Cisco Security Cloud Control の基本

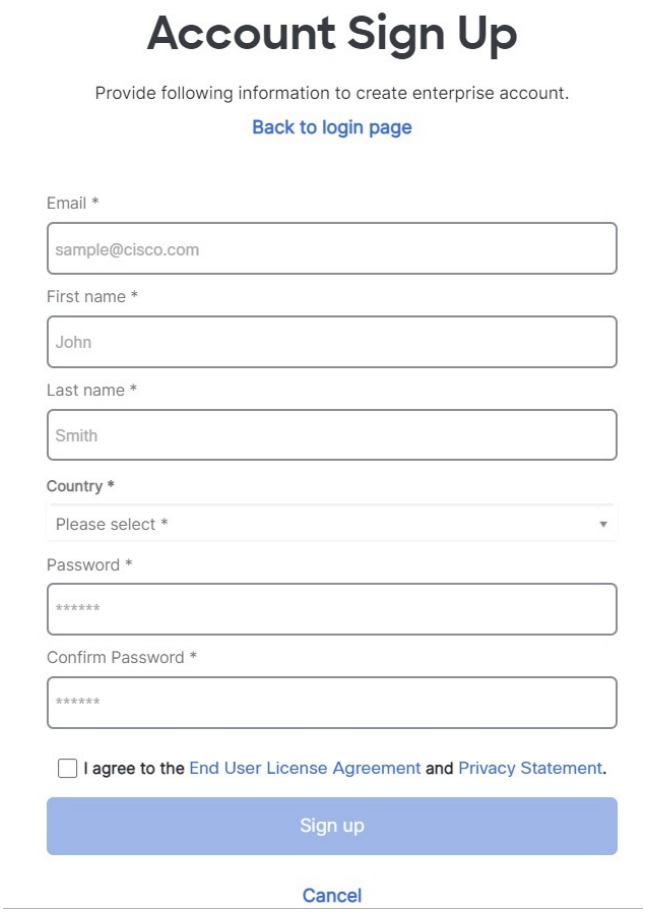
この章は、次のセクションで構成されています。

Security Cloud Control テナントの作成

新しい Security Cloud Control テナントをプロビジョニングして、デバイスをオンボーディングおよび管理できます。オンプレミス Firewall Management Center バージョン 7.2 以降を使用していて、Cisco Security Cloud と統合する場合は、統合ワークフローの一部として Security Cloud Control テナントを作成することもできます。

手順

1. https://manage.security.cisco.com/provisionに進みます。
2. Security Cloud Control テナントをプロビジョニングするリージョンを選択して、[サインアップ（Sign Up）] をクリックします。
3. [Security Cloud Sign On] ページで、ログイン情報を入力します。
4. Security Cloud Sign On アカウントをお持ちでなく、作成する場合は、[今すぐサインアップ（Sign up now）] をクリックします。
   1. アカウントを作成するため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。

2. [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。
3. E メールを開き、E メールと [Security Cloudサインオン（Security Cloud Sign On）] ページの両方で [アカウントのアクティブ化（Activate account）] をクリックします。
4. 任意のデバイスで Duo を使用して多要素認証を設定し、[Duo でログイン（Log in with Duo）] と [終了（Finish）] をクリックします。

（注） 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。

5. テナントの名前を入力し、[新しいアカウントの作成（Create new account）] をクリックします。
6. 選択したリージョンに新しい Security Cloud Control テナントが作成されます。また、作成中の Security Cloud Control テナントに関する詳細が記載された電子メールが届きます。すでに複数の Security Cloud Control テナントに関連付けられている場合は、[テナントの選択（Choose a tenant）]ページで、作成したテナントを選択してログインします。新しい Security Cloud Control テナントを初めて作成した場合は、そのテナントに直接ログインします。

   初めて Security Cloud Control テナントにログオンする方法については、「新規 Security Cloud Control テナントへの初回ログイン」を参照してください。

   Security Cloud Control テナントの管理とさまざまなテナント設定については、「テナント管理」を参照してください。

Security Cloud Control テナントの完全バージョンへのアップグレード

無料トライアルバージョンの Security Cloud Control を使用している場合は、[CDOの無料トライアル期間（You are in a free Trial of Security Cloud Control）] バナーが表示され、トライアル期間の残り日数が示されます。トライアル期間中はいつでも、Security Cloud Control テナントを完全バージョンにアップグレードできます。シスコのセールス担当者またはシスコセールス窓口に連絡してください。代理で発注し、SO 番号を取得します。

SO 番号を取得したら、バナーの [完全バージョンにアップグレード（Upgrade to full version）] をクリックし、注文番号を入力して完全バージョンの Security Cloud Control の使用を開始します。

Security Cloud Control のトライアル期間延長の要求

トライアルバージョンの使用を 30 日間継続する場合は、[延長の要求（Request for an extension）] をクリックします。

Security Cloud Control へのサインイン

Security Cloud Control にログインするには、SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）、多要素認証プロバイダー、および Security Cloud Control でのユーザーの管理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 アイデンティティ プロバイダーがない限り、アイデンティティ プロバイダーは Security Cloud Sign On です。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 SAML シングルサインオンと Security Cloud Control の統合できます。

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 Security を使用して多要素認証（MFA）を設定し、テナントのネットワーク管理者に Security Cloud Control レコードの作成を依頼する必要があります。

2019 年 10 月 14 日、Security Cloud Control は、既存のすべてのテナントを、ID プロバイダーとして Cisco Security Cloud Sign On を使用し、MFA に Duo を使用するように変換しました。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して Security Cloud Control にサインインする場合、この Cisco Security Cloud Sign On への移行は影響しません。独自のサインオンソリューションを引き続き使用できます。
- Security Cloud Control の無料試用期間中であれば、この移行の影響はあります。

Security Cloud Control テナントが 2019 年 10 月 14 日以降に作成された場合は、新規 Security Cloud Control テナントへの初回ログイン （5 ページ）を参照してください。

2019 年 10 月 14 日より前に Security Cloud Control テナントが存在していた場合は、Cisco Security Cloud Sign On ID プロバイダーへの移行 （6 ページ）を参照してください。

新規 Security Cloud Control テナントへの初回ログイン

はじめる前に

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。

Security Cloud Control は、Cisco Security Cloud Sign On を ID 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。。Cisco Security Cloud Sign On アカウントがない場合、https://manage.security.cisco.com/provision を使用して新しい Security Cloud Control テナントを作成すると、プロビジョニングフローには、 Security Cloud Sign On アカウントの作成や Duo を使用した MFA の設定など、さまざまな手順が必要になります。

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。

重要 **2019 年 10 月 14 日より前に Security Cloud Control テナントが存在していた場合は、**この項目の代わりにCisco Security Cloud Sign On ID プロバイダーへの移行 （6 ページ）をログイン手順として使用してください。

次の手順

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 （84 ページ） に進みます。これは 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。

リージョンごとの Security Cloud Control へのサインイン

こちらは、Security Cloud Control へのサインインに使用する AWS リージョンごとの URL です。

表 *1 :* リージョンごとの *Security Cloud Control URL*

地域	Security Cloud Control URL
アジア太平洋および日本（APJ）	https://apj.manage.security.cisco.com
オーストラリア（AUS）	https://au.manage.security.cisco.com

地域	Security Cloud Control URL
ヨーロッパ、中東、アフリカ（EMEA）	https://eu.manage.security.cisco.com
インド（IN）	https://in.manage.security.cisco.com
アメリカ合衆国（US）	https://us.manage.security.cisco.com

ログインの失敗のトラブルシューティング

正しくない Security Cloud Control リージョンに誤ってログインしているため、ログインに失敗する

適切な Security Cloud Control リージョンにログインしていることを確認してください。https://sign-on.security.cisco.com にログインすると、アクセスするリージョンを選択できます。

サインインするリージョンについては、リージョンごとの Security Cloud Control へのサインイン （5 ページ）を参照してください。

Cisco Security Cloud Sign On ID プロバイダーへの移行

2019 年 10 月 14 日時点で、Security Cloud Control では、すべてのテナントが ID プロバイダーとして Cisco Security Cloud Sign On に変換されており、多要素認証（MFA）には Duo を使用しています。**Security Cloud Control にログインするには、まず Cisco Secure Sign-On でアカウントをアクティブ化し、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。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して Security Cloud Control にサインインする場合、この Cisco Security Cloud Sign On および Duo への移行は影響しません。独自のサインオンソリューションを引き続き使用できます。
- Security Cloud Control の無料トライアル期間中であれば、この移行が適用されます。
- **2019 年 10 月 14 日以降に Security Cloud Control テナントが作成されていた場合は、**この項目の代わりに新規 Security Cloud Control テナントへの初回ログイン （5 ページ）をログイン手順として使用してください。

はじめる前に

移行する前に、次の手順を実行することを強くお勧めします。

- **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。
- 新しい Cisco Secure Sign-On アカウントを作成し、Duo 多要素認証を設定します。これは 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。

移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、Security Cloud Control へのログインに失敗する

解決法 Security Cloud Control にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Security Cloud Sign On アカウントを作成せずにログインを試みた可能性があります。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 （84 ページ）の手順に従って、新しい Cisco Security Cloud Sign On アカウントにサインアップする必要があります。

Cisco Security Cloud Sign On ダッシュボードへのログインは成功するが、Security Cloud Control を起動できない

解決法 Security Cloud Control テナントとは異なるユーザー名で Cisco Security Cloud Sign On アカウントを作成している可能性があります。Security Cloud Control と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center（TAC）に連絡してください。

保存したブックマークを使用したログインに失敗する

解決法 ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが https://cdo.onelogin.com を指している可能性があります。

解決法 https://sign-on.security.cisco.com にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定します。
- **解決法** Cisco Secure Sign-On の新規アカウントを作成した場合は、テナントが作成されたリージョンに対応するダッシュボードの Security Cloud Control タイルをクリックします。
  - **解決法** Cisco Security Cloud Control APJ

- **解決法** Cisco Security Cloud Control オーストラリア
- **解決法** Cisco Security Cloud Control EU
- **解決法** Cisco Security Cloud Control インド
- **解決法** Cisco Security Cloud Control 米国

- **解決法** https://sign-on.security.cisco.com を指すようにブックマークを更新します。

Security Cloud Control テナントの起動

手順

ステップ 1 Cisco Security Cloud Sign On ダッシュボードで、該当するリージョンの Security Cloud Control ボタンをクリックします。

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、マルチテナントポータルの管理 （69 ページ）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。

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、Security Cloud Control でのユーザーの管理 を確認して、他のユーザーの役割を「管理者」に変更します。

Security Cloud Control スタートアップ ガイド

スタートアップガイドSecurity Cloud Controlは、ファイアウォールを効率的にセットアップして設定する一連のタスクが示される直感的なインターフェイスです。

Security Cloud Control にサインインし、上にあるメニューで（  ）をクリックします。

- [オンプレミス管理（On-premises Management）]ページには、以下へのリンクがあります。
  - Security Cloud Control を使用して、脅威に対する防御 デバイスを オンプレミス Management Center にオンボードします。
  - オンプレミス Management Center によって管理されている 脅威に対する防御 デバイスを クラウド提供型 Firewall Management Center に移行します。
  - デバイステンプレートを使用して、クラウド提供型 Firewall Management Center への複数の Threat Defense デバイスの一括プロビジョニングを実行します。
  - ポリシーを分析し、異常を検出し、キュレーションされた修復の推奨事項を受け取ります。

- [ファイアウォールの管理（Manage Firewalls）]ページには、以下へのリンクがあります。
  - 脅威に対する防御、Cisco Secure Firewall ASA 、Cisco Meraki MX ファイアウォールをオンボードして管理します。
  - サイト間 VPN 接続を設定します。
  - Cisco AI Assistant を活用して、必要に応じてファイアウォールポリシーとアクセス関連のドキュメントを管理します。
  - 一般的な問題の障害対応に関する通知を受信するために登録します。
- [クラウド資産の保護（Protect Cloud Assets）] ページには、以下へのリンクがあります。
  - Multicloud Defense を使用した一貫したセキュリティ対策を使用してマルチクラウド環境全体のデータとアプリケーションを保護することで、クラウド資産を保護します。

Security Cloud Control ライセンスについて

Security Cloud Control では、テナント資格の基本サブスクリプションと、デバイスを管理するためのデバイスライセンスが必要です。必要なテナント数に基づいて 1 つ以上の Security Cloud Control 基本サブスクリプションを購入し、デバイスモデル番号と数量に基づいてデバイスライセンスを購入できます。つまり、基本サブスクリプションを購入すると Security Cloud Control テナントが得られ、Security Cloud Control を使用して管理することを選択したデバイスごとに、個別のデバイスライセンスが必要になります。

展開を計画するために、各 Security Cloud Control テナントは Secure Device Connector（SDC）を介して約 500 台のデバイスを管理でき、Cloud Connector を使用して任意の数のデバイスを管理できることに注意してください。詳細については、「Secure Device Connector（SDC）」を参照してください。

Security Cloud Control からデバイスをオンボードして管理するには、管理するデバイスに基づいて、基本サブスクリプションとデバイス固有の期間ベースのサブスクリプションを購入する必要があります。

サブスクリプション

Cisco Security Cloud Control サブスクリプションは期間ベースです。

- **基本**：1 年、3 年、および 5 年のサブスクリプションを提供して、Security Cloud Control テナントにアクセスし、適切にライセンスされたデバイスを搭載する資格を提供します。
- **デバイスライセンス**：管理することを選択したサポート対象デバイスについて、1 年、3 年、および 5 年のサブスクリプションを提供します。たとえば、Cisco Firepower 1010 デバイスの 3 年のソフトウェア サブスクリプションを購入した場合、Security Cloud Control を使用して Cisco Firepower 1010 デバイスを 3 年間管理することを選択できます。

Security Cloud Control がサポートするシスコのセキュリティデバイスの詳細については、「Security Cloud Control でサポートされるソフトウェアとハードウェア」を参照してください。

重要 Security Cloud Control 高可用性デバイスペアを管理するために、2 つの個別のデバイスライセンスは必要ありません。 の高可用性ペアがある場合、Security Cloud Control では高可用性デバイスのペアを 1 つのデバイスと見なすため、1 つの デバイスライセンスを購入するだけで十分です。

（注） Cisco Smart Licensing ポータルから Security Cloud Control ライセンスを管理することはできません。

ソフトウェア サブスクリプションのサポート

Security Cloud Control 基本サブスクリプションには、サブスクリプション期間中有効なソフトウェア サブスクリプション サポートが含まれており、ソフトウェアアップデート、メジャーアップグレード、および Cisco Technical Assistance Center（TAC）へのアクセスを追加料金なしで提供します。ソフトウェアサポートがデフォルトで選択されていますが、要件に基づいて Security Cloud Control ソリューションサポートを活用することもできます。

Security Cloud Control 評価ライセンス

SecureX アカウントから 30 日間の Security Cloud Control トライアルをリクエストできます。詳細については、「Request a Security Cloud Control Tenant」[英語] を参照してください。

クラウド提供型 Firewall Management Center および Threat Defense ライセンス

Security Cloud Control で クラウド提供型 Firewall Management Center を使用するために別のライセンスを購入する必要はありません。Security Cloud Control テナントの基本サブスクリプションには、クラウド提供型 Firewall Management Center の料金が含まれています。

クラウド提供型 Firewall Management Center 評価ライセンス

クラウド提供型 Firewall Management Center には 90 日間の評価ライセンスがプロビジョニングされており、その後は 脅威に対する防御 サービスがブロックされます。

Security Cloud Control テナントでプロビジョニングされた クラウド提供型 Firewall Management Center を取得する方法については、「Request a クラウド提供型 Firewall Management Center for your Security Cloud Control Tenant」を参照してください。

（注） クラウド提供型 Firewall Management Center は、エアギャップネットワーク内のデバイスの特定のライセンス予約（SLR）をサポートしていません。

クラウド提供型 Firewall Management Center の Threat Defense ライセンス

クラウド提供型 Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense デバイスごとに個別のライセンスが必要です。詳細については、『*Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control*』[英語] の「Licensing」を参照してください。

クラウド提供型 Firewall Management Center に移行されたデバイスのライセンスを Security Cloud Control が処理する方法については、「Migrate Threat Defense from Management Center to Cloud」を参照してください。

Secure Device Connector

Secure Device Connector（SDC）は、シスコデバイスが Security Cloud Control と通信できるようにするインテリジェントプロキシです。インターネット経由で直接到達できないデバイスをデバイスのログイン情報を使用して Security Cloud Control にオンボーディングする場合は、ネットワークに SDC を展開して、デバイスと Security Cloud Control の間の通信をプロキシできます。または、必要に応じて、デバイスが Security Cloud Control からの外部インターフェイスを介して直接通信を受信できるようにすることができます。適応型セキュリティアプライアンス（ASA）、Meraki MX、Cisco Secure Firewall Threat Defense デバイス、Firepower Management Center デバイス、汎用 SSH および IOS デバイスはすべて、SDC を使用して Security Cloud Control に対して導入準備できます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、Security Cloud Control を監視します。SDC は、Security Cloud Control に代わってこのコマンドを実行し、管理対象デバイスに代わって Security Cloud Control にメッセージを送信し、管理対象デバイスからの応答を Security Cloud Control に返します。

SDC は、AES-128-GCM over HTTPS（TLS 1.3）を使用して署名および暗号化された安全な通信メッセージを使用して、Security Cloud Control と通信します。導入準備されたデバイスとサービスのすべてのログイン情報は、ブラウザから SDC に直接暗号化されるだけでなく、AES-128-GCM を使用して保存時にも暗号化されます。SDC だけがデバイスのログイン情報にアクセスできます。他の Security Cloud Control サービスはログイン情報にアクセスできません。SDC と Security Cloud Control 間の通信を許可する方法については、管理対象デバイスへの Security Cloud Control の接続 （13 ページ）を参照してください。

SDC は、任意の Ubuntu インスタンスにインストールできます。便宜上、SDC CLIがプリインストールされた、強化された Ubuntu 22 インスタンス用の OVA を提供しています。CLI を使用すると、VM を設定し、必要なすべてのシステムパッケージをインストールし、SDC を Docker コンテナとしてホストにブートストラップできます。または、独自の Ubuntu インスタ

ンス（バージョン 20 ー 24 が現在テストされています）をロールし、CLI を個別にダウンロードすることもできます。

各 Security Cloud Control テナントは、無制限の数の SDC を持つことができます。これらの SDC はテナント間で共有されず、1 つのテナント専用です。1 つの SDC が管理できるデバイスの数は、それらのデバイスに導入された機能と、設定ファイルのサイズによって異なります。ただし、展開を計画するために、1 つの SDC が約 500 台のデバイスをサポートすることを想定してください。

テナントに複数の SDC を展開すると、次の利点もあります。

- パフォーマンスを低下させることなく、Security Cloud Control テナントでより多くのデバイスを管理できます。
- ネットワーク内の隔離されたネットワークセグメントに SDC を展開し、そのセグメント内のデバイスを同じ Security Cloud Control テナントで引き続き管理できます。複数の SDC がない場合、これらの隔離されたネットワークセグメント内のデバイスを、異なる Security Cloud Control テナントで管理する必要があります。

単一のホストで複数の SDC を実行できます。実行する各 SDC のブートストラップ手順に従ってください。テナントの最初の SDC には、テナントの名前と番号 1 が組み込まれており、Security Cloud Control の [サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブに表示されます。追加の各 SDC には、順番に番号が付けられます。

詳細については、Security Cloud Control の VM イメージを使用した Secure Device Connector の展開 （15 ページ）および自身の VM 上での Secure Device Connector の展開 （19 ページ）を参照してください。

関連情報：

- 管理対象デバイスへの Security Cloud Control の接続
- Secure Device Connector の更新 （35 ページ）
- Secure Device Connector の削除 （33 ページ）

管理対象デバイスへの Security Cloud Control の接続

Security Cloud Control は、クラウドコネクタまたは Secure Device Connector（SDC）を介して管理対象デバイスに接続します。

インターネットからデバイスに直接アクセスできる場合は、クラウドコネクタを使用してデバイスに接続する必要があります。デバイスを設定できる場合は、クラウドリージョンの Security Cloud Control IP アドレスからのポート 443 でのインバウンドアクセスを許可します。

インターネットからデバイスにアクセスできない場合は、ネットワークにオンプレミスの SDC を展開して、Security Cloud Control がデバイスと通信できるようにすることができます。

ポート 443（またはデバイス管理用に設定したポート）のデバイスサブネット/IP から完全なインバウンドアクセスを許可するようにデバイスを設定します。

オンボードするには、ネットワークにオンプレミスの SDC が必要です。

- Cisco IOS デバイス。

他のすべてのデバイスとサービスには、オンプレミス SDC は必要ありません。Security Cloud Control はクラウドコネクタを使用して接続します。インバウンドアクセスの許可が必要な IP アドレスについては、次のセクションを参照してください。

Cloud Connector を介したデバイスの Security Cloud Control への接続

クラウドコネクタを介して Security Cloud Control をデバイスに直接接続する場合、EMEA、米国、または APJ 地域のさまざまな IP アドレスに、ポート 443（またはデバイス管理用に設定したポート）でのインバウンドアクセスを許可する必要があります。

アジア - 太平洋 - 日本（APJ）地域のお客様が https://apj.manage.security.cisco.com で Security Cloud Control に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 54.199.195.111
- 52.199.243.0

オーストラリア（AUS）地域のお客様が https://au.manage.security.cisco.com で Security Cloud Control に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 13.55.73.159
- 13.238.226.118

ヨーロッパ、中東、またはアフリカ（EMEA）地域のお客様で、https://eu.manage.security.cisco.com で Security Cloud Control に接続している場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 35.157.12.126
- 35.157.12.15

インド（IN）地域のお客様が https://in.manage.security.cisco.com で Security Cloud Control に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 35.154.115.175
- 13.201.213.99

米国（US）地域のお客様が https://us.manage.security.cisco.com で Security Cloud Control に接続する場合は、次の IP アドレスからのインバウンドアクセスを許可します。

- 52.34.234.2
- 52.36.70.147

SDC への Security Cloud Control の接続

SDC を介して Security Cloud Control をデバイスに接続する場合、Security Cloud Control で管理するデバイスが、ポート 443（またはデバイス管理用に設定したポート）の SDC ホストからの

完全なインバウンドアクセスを許可する必要があります。この許可は、管理アクセス制御ルールを使用して設定されます。

また、SDC が展開されている仮想マシンが、管理対象デバイスの管理インターフェイスにネットワーク接続されていることを確認する必要があります。

Security Cloud Control の VM イメージを使用した Secure Device Connector の展開

デバイスのログイン情報を使用して Security Cloud Control をデバイスに接続する場合、Security Cloud Control とデバイス間の通信を管理するために、ネットワークに SDC をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。適応型セキュリティアプライアンス（ASA）、FDM による管理デバイス、Firepower Management Center（FMC）、SSH および IOS デバイスはすべて、SDC を使用して Security Cloud Control に導入準備できます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、Security Cloud Control を監視します。SDC は、Security Cloud Control に代わってこのコマンドを実行し、管理対象デバイスに代わって Security Cloud Control にメッセージを送信し、管理対象デバイスからの応答を Security Cloud Control に返します。

1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500 台のデバイスをサポートできることを想定しています。詳細については、単一の Security Cloud Control テナントで複数の SDC を使用する （36 ページ）を参照してください。

この手順では、Security Cloud Control の VM イメージを使用してネットワークに SDC をインストールする方法について説明します。これは、SDC を作成するために推奨される、最も簡単で信頼できる方法です。作成した VM を使用して SDC を作成する必要がある場合は、自身の VM 上での Secure Device Connector の展開 （19 ページ）の手順に従います。

始める前に

SDC を展開する前に、次の前提条件を確認してください。

- Security Cloud Control は、厳密な証明書チェックを必要とし、Secure Device Connector（SDC）とインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、SDC と Security Cloud Control の間のトラフィックの検査を無効にします。
- SDC には、TCP ポート 443 またはデバイス管理用に設定したポートでのインターネットへの完全なアウトバウンドアクセスが必要です。Security Cloud Control によって管理されているデバイスは、このポートからのインバウンドトラフィックも許可する必要があります。
- 適切なネットワークアクセスを確保するため、「管理対象デバイスへの Security Cloud Control の接続」を参照してください。

- Security Cloud Control は、vSphere Web クライアントまたは ESXi Web クライアントを使用した SDC VM OVF イメージのインストールをサポートしています。
- Security Cloud Control は、vSphere デスクトップクライアントを使用した SDC VM OVF イメージのインストールをサポートしていません。
- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- SDC を 1 つだけ持つ VMWare ESXi ホストのシステム要件。
  - VMware ESXi ホストには 2 つの vCPU が必要です。
  - VMware ESXi ホストには 2 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64 GB のディスク容量が必要です。
- Docker IP は、SDC の IP 範囲**および**デバイスの IP 範囲とは異なるサブネットにある必要があります。
- インストールを開始する前に、次の情報を収集します。
  - SDC に使用する静的 IP アドレス。
  - インストールプロセス中に作成する `root` ユーザーと `cdo` ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- SDC 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

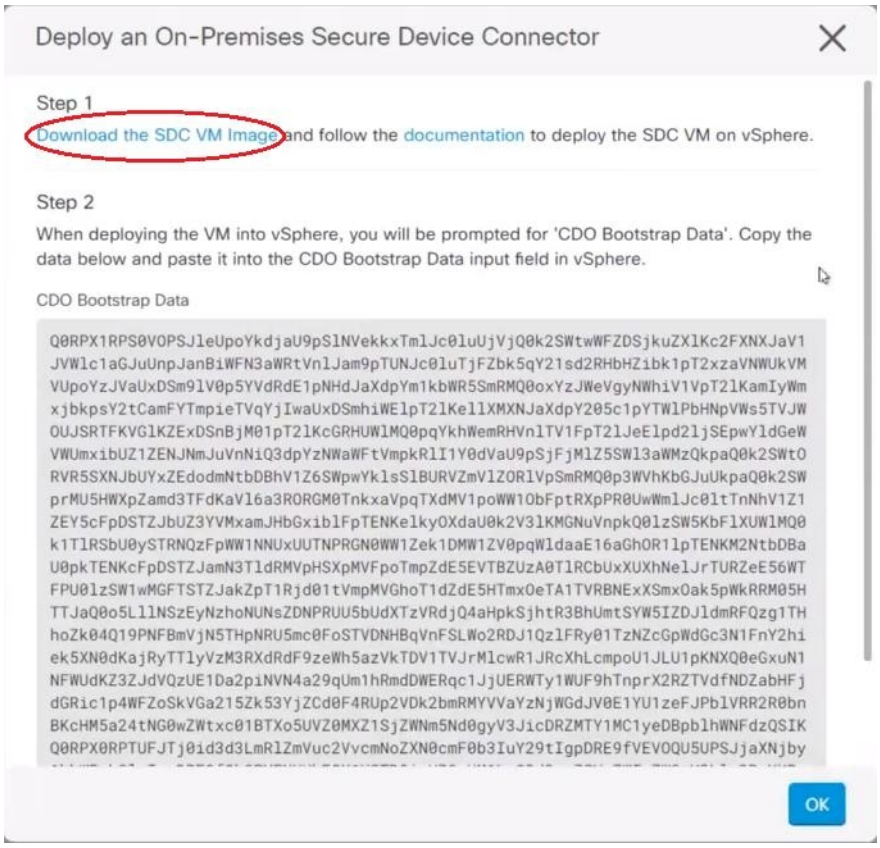
手順

ステップ 1 SDC を作成する Security Cloud Control テナントにログオンします。

ステップ 2 左側のペインで **[管理（Administration）] > [セキュアコネクタ（Secure Connectors）]** をクリックします。

ステップ 3 [サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブで、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。

ステップ 4 手順 1 で [SDC VMイメージのダウンロード（Download the SDC VM image）] をクリックします。すると別のタブが表示されます。



ステップ 5 .zip ファイルからすべてのファイルを抽出します。これらは、次のようなものです。

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

ステップ 6 vSphere Web クライアントを使用して、管理者として VMware サーバーにログオンします。

（注）
ESXi Web クライアントは使用しないでください。

ステップ 7 プロンプトに従って、OVF テンプレートから Secure Device Connector 仮想マシンを展開します。

ステップ 8 セットアップが完了したら、SDC VM の電源を入れます。

ステップ 9 新しい SDC VM のコンソールを開きます。

ステップ 10 ユーザー名「CDO」でログインします。デフォルトのパスワードは **adm123** です。

ステップ 11 プロンプトで、`sudo sdc-onboard setup` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

ステップ 12 パスワードのプロンプトが表示されたら、`adm123` と入力します。

ステップ 13 プロンプトに従って、`root` ユーザーの新しいパスワードを作成します。root ユーザーのパスワードを入力します。

ステップ 14 プロンプトに従って、Security Cloud Control ユーザーの新しいパスワードを作成します。ユーザーのパスワードを入力します

ステップ 15 [接続するSecurity Cloud Controlドメインを選択してください（Please choose the CDO domain you connect to）] というプロンプトが表示されたら、Security Cloud Control のドメイン情報を入力します。

ステップ 16 プロンプトが表示されたら、SDC VM の次のドメイン情報を入力します。

a) IP アドレス/CIDR
b) ゲートウェイ
c) DNS サーバー
d) NTP サーバーまたは FQDN
e) Docker ブリッジ

または、Docker ブリッジが適用されない場合は Enter キーを押します。

ステップ 17 [これらの値は正しいですか？（はい/いいえ）（Are these values correct? (y/n)）] というプロンプトが表示されたら、[はい] を入力してエントリを確認します。

ステップ 18 入力内容を確定します。

ステップ 19 [今すぐSDCを設定しますか？（はい/いいえ）（Would you like to setup the SDC now? (y/n)]というプロンプトが表示されたら、[n] を入力します。

ステップ 20 VM コンソールから自動的にログアウトします。

ステップ 21 SDC への SSH 接続を作成します。CDO としてログインし、パスワードを入力します。

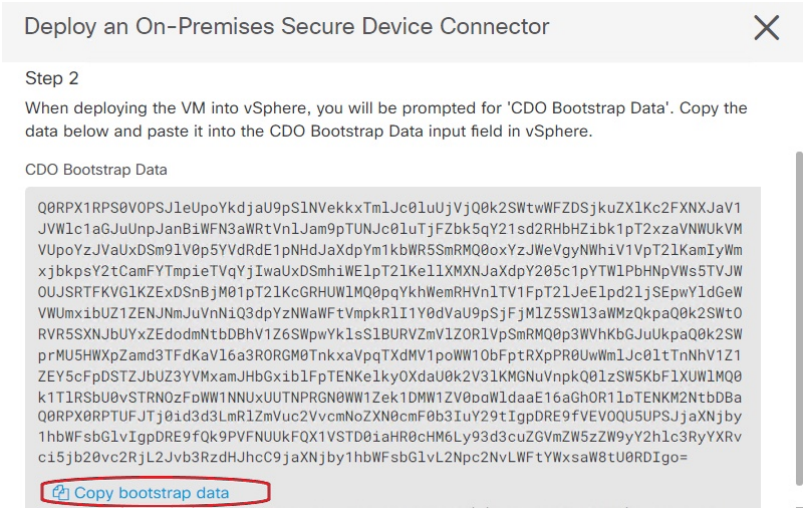
ステップ 22 プロンプトで、`sudo sdc-onboard bootstrap` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

ステップ 23 [sudo] パスワードの入力を求められたら、ステップ 14 で作成したパスワードを入力します。

ステップ 24 [Security Cloud Controlのセキュアコネクタページからブートストラップデータをコピーしてください（Please copy the bootstrap data form the Secure Connector Page of CDO）] というプロンプトが表示されたら、次の手順に従います。

1. Security Cloud Control にログインします。
2. [アクション（Actions）] ペインで、[オンプレミスの Secure Device Connector の展開（Deploy an On-Premises Secure Device Connector）] をクリックします。
3. ダイアログボックスのステップ 2 で [ブートストラップデータをコピー] をクリックし、SSH ウィンドウに貼り付けます。



ステップ 25 [これらの設定を更新しますか？（はい/いいえ）（Do you want to update these setting? (y/n)）] というプロンプトが表示されたら、[n] を入力します。

ステップ 26 [Secure Device Connector] ページに戻ります。新しい SDC のステータスが [アクティブ（Active）] に変更されるまで、画面を更新します。

自身の VM 上での Secure Device Connector の展開

デバイスのログイン情報を使用して Security Cloud Control をデバイスに接続する場合、Security Cloud Control とデバイス間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。適応型セキュリティアプライアンス（ASA）、FDM による管理デバイス、および Firepower Management Center（FMC）デバイスはすべて、デバイスのログイン情報を使用して Security Cloud Control に対して導入準備することができます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、Security Cloud Control を監視します。SDC は、Security Cloud Control に代わってこのコマンドを実行し、管理対象デバイスに代わって Security Cloud Control にメッセージを送信し、管理対象デバイスからの応答を Security Cloud Control に返します。

1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500 台のデバイスをサポートできることを想定しています。詳細については、単一の Security Cloud Control テナントで複数の SDC を使用する （36 ページ）を参照してください。

この手順では、独自の仮想マシンイメージを使用してネットワークに SDC をインストールする方法について説明します。

（注） SDC をインストールするために推奨される、最も簡単で信頼できる方法は、Security Cloud Control の SDC OVA イメージをダウンロードしてインストールすることです。手順については、Security Cloud Control の VM イメージを使用した Secure Device Connector の展開 （15 ページ） を参照してください。

始める前に

- Security Cloud Control は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシをサポートしていません。
- SDC が Security Cloud Control と通信するためには、TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。
- SDC を介して Security Cloud Control に到達するデバイスは、ポート 443 で SDC からのインバウンドアクセスを許可する必要があります。
- ネットワークのガイドラインについては、「管理対象デバイスへの Security Cloud Control の接続」を参照してください。
- vCenter Web クライアントまたはr ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

（注） vSphere デスクトップクライアントを使用したインストールはサポートしていません。

- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- SDC のみを持つ VM のシステム要件：
  - VMware ESXi ホストには 2 つの CPU が必要です。
  - VMware ESXi ホストには 2 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64 GB のディスク容量が必要です。これは、必要に応じてディスク領域を拡張できるように、パーティションで論理ボリューム管理（LVM）を使用していることを想定した値です。
- VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。
- この手順を実行するユーザーは、Linux 環境の操作に親しんでおり、vi ビジュアルエディタを使用してファイルを編集している必要があります。

- オンプレミスの SDC を CentOS 仮想マシンにインストールする場合は、Yum セキュリティパッチを定期的にインストールすることをお勧めします。Yum の更新を取得するための設定に応じて、ポート 443 だけでなくポート 80 でもアウトバウンドアクセスを開く必要がある場合があります。また、更新をスケジュールするために yum-cron または crontab も設定する必要があります。セキュリティ運用チームと連携して、Yum の更新を取得するためにセキュリティポリシーを変更する必要があるかどうかを判断します。

（注） **始める前に**：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があり、コマンドが失敗する原因となります。

手順

ステップ 1 SDC を作成する Security Cloud Control テナントにログオンします。

ステップ 2 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

ステップ 3 [サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブで、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。

ステップ 4 ウィンドウの手順 2 のブートストラップデータをメモ帳にコピーします。

ステップ 5 少なくとも次の RAM とディスク領域が SDC に割り当てられている **CentOS 7 仮想マシン**をインストールします。

- 8 GB の RAM
- 10 GB のディスクスペース

ステップ 6 インストールしたら、SDC の IP アドレス、サブネットマスク、ゲートウェイの指定など、ネットワークの基本設定を行います。

ステップ 7 DNS（ドメインネームサーバー）を設定します。

ステップ 8 NTP（ネットワーク タイム プロトコル）サーバーを設定します。

ステップ 9 SDC の CLI と簡単にやり取りできるように、CentOS に SSH サーバーをインストールします。

ステップ 10 Yum の更新を実行し、**open-vm-tools**、**nettools**、および **bind-utils** パッケージをインストールします。

```
[root@sdc-vm ~]# yum update -y
                [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

ステップ 11 AWS CLI パッケージをインストールします。https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html を参照してください。

（注）
--user フラグは使用しないでください。

ステップ 12 Docker CE パッケージをインストールします。https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ceを参照してください。

（注）
「リポジトリを使用したインストール」方法を使用します。

ステップ 13 Docker サービスを開始し、起動時に開始できるようにします。

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

ステップ 14 「CDO」と「sdc」の 2 つのユーザーを作成します。CDO ユーザーは、管理機能を実行するためにログインするユーザーです（つまり root ユーザーを直接使用する必要はありません）。sdc ユーザーは、SDC docker コンテナを実行するユーザーです。

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

ステップ 15 CDO ユーザーのパスワードを設定します。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

ステップ 16 CDO ユーザーを「wheel」グループに追加し、管理者（sudo）権限を付与します。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

ステップ 17 Docker がインストールされると、ユーザーグループが作成されます。CentOS/Docker のバージョンに応じて、「docker」または「dockerroot」と呼ばれます。/etc/group ファイルでどのグループが作成されたかを確認したら、sdc ユーザーをそのグループに追加します。

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

ステップ 18 /etc/docker/daemon.json ファイルが存在しない場合は作成し、以下の内容を入力します。作成したら、docker デーモンを再起動します。

（注）
「group」キーに入力したグループ名が、前の手順の /etc/group ファイルで見つけたグループと一致していることを確認してください。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
```

```
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

ステップ 19 現在 vSphere コンソールセッションを使用している場合は、SSH に切り替えて、「CDO」ユーザーでログインします。ログインしたら、「sdc」ユーザーに切り替えます。パスワードの入力を求められたら、「CDO」ユーザーのパスワードを入力します。

```
[CDO@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

ステップ 20 ディレクトリを **/usr/local/CDO** に変更します。

ステップ 21 `bootstrapdata` という新しいファイルを作成し、[オンプレミスの Secure Device Connector の展開（Deploy an On-Premises Secure Device Connector）] ウィザードの手順2 のブートストラップデータを、このファイルに貼り付けます。[保存（Save）] をクリックしてファイルを保存します。[vi] または [nano] を使用してファイルを作成できます。

ステップ 22 ブートストラップデータは base64 でエンコードされていますので、復号して `extractedbootstrapdata` というファイルにエクスポートします。

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/ CDO/bootstrapdata > /usr/local/CDO/extractedbootstrapdata
                [sdc@sdc-vm ~]$
```

cat コマンドを実行して復号したデータを表示します。コマンドおよび復号したデータは次のようになります。

```
[sdc@sdc-vm ~]$ cat /usr/local/ CDO/extractedbootstrapdata
                CDO_TOKEN="<token string>"
                CDO_DOMAIN="www.defenseorchestrator.com"
                CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

ステップ 23 以下のコマンドを実行して、復号したブートストラップデータの一部を環境変数にエクスポートします。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
                [sdc@sdc-vm ~]$
```

ステップ 24 Security Cloud Control からブートストラップバンドルをダウンロードします。

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
                100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
                [sdc@sdc-vm ~]$ ls -l /usr/local/ CDO/*SDC
                -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/CDO/tenant-name-SDC
```

ステップ 25 SDC tarball を展開し、`bootstrap.sh` ファイルを実行して SDC パッケージをインストールします。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
                <snipped - extracted files>
                [sdc@sdc-vm ~]$
                [sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
                [2018-07-23 13:54:02] environment properly configured
                download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
                toolkit.sh
                common.sh
                [2018-07-23 13:54:04] startup new container
                Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
                sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458: Pulling
from
```

```
ciscodefenseorchestrator/sdc_prod
08d48e6f1cff: Pull complete
ebbd10b629b1: Pull complete
d14d580ef2ed: Pull complete
45421d451ab8: Pull complete
<snipped - downloads>
no crontab for sdc
```

すると、Security Cloud Control で SDC が「アクティブ」と表示されるはずです。

次のタスク

-

Ubuntu 仮想マシンでの Secure Device Connector と Secure Event Connector の展開

デバイスのログイン情報を使用して Security Cloud Control をデバイスに接続する場合、Security Cloud Control とデバイス間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。通常、これらのデバイスは非境界ベースであり、パブリック IP アドレスを持たないか、外部インターフェイスに開かれたポートを持っています。適応型セキュリティアプライアンス（ASA）、FDM による管理デバイス、および Firepower Management Center（FMC）デバイスはすべて、デバイスのログイン情報を使用して Security Cloud Control に対して導入準備することができます。

SDC は、管理対象デバイスで実行する必要があるコマンドと、管理対象デバイスに送信する必要があるメッセージについて、Security Cloud Control を監視します。SDC は、Security Cloud Control に代わってこのコマンドを実行し、管理対象デバイスに代わって Security Cloud Control にメッセージを送信し、管理対象デバイスからの応答を Security Cloud Control に返します。

Secure Event Connector（SEC）は、ASA と FTD からのイベントを Cisco Cloud に転送するため、ライセンスに応じて、[イベントロギング（Event Logging）] ページでイベントを表示し、Cisco Secure Cloud Analytics で調査できます。

SDC を展開した後は、簡単な操作で SEC コンテナを追加できます。SEC サービスは、Cisco ASA、Cisco IOS、FDM による管理デバイスから syslog メッセージを受信し、Cisco Cloud に安全に送信するように設計されています。これにより、Security Cloud Control Analytics や Cisco XDR などのイベントサービスでログメッセージを簡単に保存、強化、分析できます。

CiscoDevNet サイト [英語] で提供されているスクリプトを実行して、Linux Ubuntu システムに SDC および SEC をインストールできます。

始める前に

- Security Cloud Control は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシをサポートしていません。
- SDC には TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。

- ネットワークのガイドラインについては、「管理対象デバイスへの Security Cloud Control の接続」を参照してください。
- vCenter Web クライアントまたは ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

（注） vSphere デスクトップクライアントを使用したインストールはサポートしていません。

- ESXi 5.1 ハイパーバイザ。
- 仮想マシンに Ubuntu オペレーティング システム バージョン 20.04 以降がインストールされている。

  SDC：

  - CPU：2 コア
  - RAM：2 GB 以上

  SDC および SEC：

  - CPU：4 コア
  - RAM：8 GB 以上

- SDC を実行している Ubuntu 仮想マシンには、ASA および Cisco IOS デバイスの管理インターフェイスへのネットワークアクセスが必要です。

手順

ステップ 1 SDC を作成する Security Cloud Control テナントにログオンします。

ステップ 2 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

ステップ 3 [サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブで、＋ をクリックし、[Secure Device Connector] を選択します。

ステップ 4 ウィンドウの手順 2 のブートストラップデータをメモ帳にコピーします。

ステップ 5 CiscoDevNet を開いて SDC を展開します。

ステップ 6 [コード（Code）] をクリックし、[HTTPS] タブの URL をコピーします。

ステップ 7 Ubuntu システムで Ctrl+Alt+T を押して、端末ウィンドウを開きます。

ステップ 8 端末で **git** と入力し、先ほどコピーした HTTPS URL を貼り付けます。

```
[sdc@vm]:~$ git https://github.com/CiscoDevNet/cdo-deploy-sdc.git
Resolving deltas: 100% (22/22). done.
```

ステップ 9 「cdo-deploy-sdc」ディレクトリに移動します。

```
[sdc@vm]:~$ cd cdo-deploy-sdc.
```

ステップ 10 **ls -la** を実行して、ファイルとスクリプトを表示します。

- **delete_sdc.sh**：以前にシステムにインストールされた SDC を削除します。
- **deploy_sdc.sh**：システムに SDC を展開します。
- **install_docker.sh**：推奨バージョンの Docker をシステムに展開します。

ステップ 11 スクリプトを実行して Docker をインストールします。

```
[sdc@vm]:~/cdo-deploy-sdc$ ./install_docker.sh

Remove docker docker.io docker-compose docker-compose-v2 docker-doc podmand-docker {y/n] n
Active: active (running) since date time UTC; 32s ago
Adding the current user to the docker permmissions group
Done!
```

ステップ 12 SDC を展開するスクリプトを実行します。

./deploy_sdc.sh と入力し、Security Cloud Control UI からコピーしたブートストラップデータを貼り付けます。

```
[sdc@vm]:~/cdo-deploy-sdc$ ./deploy_sdc.sh <bootstap data>.

If the docker container is up and running, the status of the SDC should go to 'Active' in the
Security Cloud Control Event Connectors panel.
```

Secure Device Connector が Security Cloud Control で [アクティブ（Active）] と表示される必要があります。

次のタスク

-

Terraform を使用した vSphere への Secure Device Connector の展開

始める前に

この手順では、vSphere 用 Security Cloud Control SDC Terraform モジュールを Security Cloud Control Terraform プロバイダーと組み合わせて使用して、vSphere に SDC を展開する方法について詳しく説明します。このタスク手順を実行する前に、次の前提条件を確認してください。

- vSphere データセンターバージョン 7 以降が必要です
- 次を実行する権限を持つデータセンターの管理者アカウントが必要です。
  - VM の作成
  - フォルダの作成
  - コンテンツライブラリの作成

- コンテンツライブラリへのファイルのアップロード
- Terraform の知識

手順

ステップ 1 Security Cloud Control で API のみのユーザーを作成し、API トークンをコピーします。API のみのユーザーの作成方法については、「API のみのユーザーを作成する」を参照してください。

ステップ 2 「Security Cloud Control Terraform Provider」の手順に従って、Terraform リポジトリで Security Cloud Control Terraform プロバイダーを構成します。

例：

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = “<the CDO URL you use to access CDO>”
  api_token = “<the API Token generated in step 1>”
}
```

ステップ 3 Security Cloud Control Terraform プロバイダーを使用して `cdo_sdc` リソースを作成するための Terraform コードを記述します。詳細については、Security Cloud Control-sdc リソースの Terraform レジストリを参照してください。

例：

```
Resource “cdo_sdc” “my-sdc” {
  name = “my-sdc-in-vsphere”
}
```

このリソースの `bootstrap_data` 属性には、Security Cloud Control ブートストラップデータの値が入力され、次のステップで `cdo_sdc` Terraform モジュールに提供されます。

ステップ 4 Security Cloud Control_sdc Terraform モジュールを使用して、vSphere で SDC を作成するための Terraform コードを記述します。

例：

```
data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source               = "CiscoDevNet/cdo-sdc/vsphere"
  version              = "1.0.0"
  vsphere_username     = "<replace-with-username-with-admin-privileges>"
  vsphere_password     = "<super-secure-password>"
  vsphere_server       = "<replace-with-address-of-vsphere-server>"
  datacenter           = "<replace-with-datacenter-name>"
  resource_pool        = "<replace-with-resource-pool-name>"
  cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
```

```
  datastore            = "<replace-with-name-of-datastore-to-deploy-vm-in>"
  network              = "<replace-with-name-of-network-to-deploy-vm-in>"
  host                 = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does not have a valid SSL
certificate>
  ip_address           = "<sdc-vm-ip-address; must be in the subnet of the assigned network for the
 VM>"
  gateway              = "<replace-with-network-gateway-address>"
  cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
  cdo_bootstrap_data   = cdo_sdc.sdc-in-vsphere.bootstrap_data
}
```

作成された VM には 2 人のユーザー（`root` ユーザーと `cdo` というユーザー）があり、VM の IP アドレスは静的に設定されていることに注意してください。`cdo_bootstrap_data` 属性には、`cdo_sdc` リソースの作成時に生成された `bootstrap_data` 属性の値が指定されます。

ステップ 5 通常どおり、`terraform plan` と `terraform apply` を使用して Terraform を計画および適用します。

完全な例については、CiscoDevNet の「Security Cloud Control Automation Repository」[英語] を参照してください。

SDC がオンボーディング状態のままである場合は、リモートコンソールを使用して vSphere VM に接続し、CDO ユーザーとしてログインして、次のコマンドを実行します。

```
sudo su
/opt/cdo/configure.sh startup
```

（注） Security Cloud Control Terraform モジュールは、Apache 2.0 ライセンスの下でオープンソースソフトウェアとして公開されています。サポートが必要な場合は、GitHub で問題を報告できます。

Terraform モジュールを使用した AWS VPC 上での Secure Device Connector の展開

始める前に

AWS VPC に SDC を展開する前に、次の前提条件を確認してください。

- Security Cloud Control は、厳密な証明書チェックを必要とし、SDC とインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、Secure Device Connector（SDC）と Security Cloud Control の間のトラフィックの検査を無効にします。
- 適切なネットワークアクセスを確保するため、「管理対象デバイスへの Security Cloud Control の接続」を参照してください。

- AWS アカウント、少なくとも 1 つのサブネットを持つ AWS VPC、および AWS Route53 でホストされるゾーンが必要です。
- Security Cloud Control ブートストラップデータ、AWS VPC ID、およびそのサブネット ID が手元にあることを確認します。
- SDC を展開するプライベートサブネットに NAT ゲートウェイが接続されていることを確認します。
- ファイアウォール管理HTTPインターフェイスが実行されているポートで、ファイアウォールから NAT ゲートウェイに接続された Elastic IP へのトラフィックを開きます。

手順

ステップ 1 Terraform ファイルに次のコード行を追加します。変数の入力は手動で入力してください。

```
module "example-sdc" {
  source            = "git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"

  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id              = <replace-with-vpc-id>
  subnet_id           = <replace-with-private-subnet-id>
}
```

入力変数と説明のリストについては、「Secure Device Connector Terraform module」を参照してください。

ステップ 2 Terraform コードの出力として `instance_id` を登録します。

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

`instance_id` を使用して SDC インスタンスに接続し、AWS Systems Manager Session Manager（SSM）を使用してトラブルシューティングを行うことができます。使用可能な出力のリストについては、「Secure Device Connector Terraform module」の「Outputs」を参照してください。

次のタスク

SDC のトラブルシューティングでは、AWS SSM を使用して SDC インスタンスに接続する必要があります。インスタンスへの接続方法の詳細については、「AWS Systems Manager Session Manager」を参照してください。SSH を使用して SDC インスタンスに接続するためのポートは、セキュリティ上の理由により公開されないことに注意してください。

（注） Security Cloud Control Terraform モジュールは、Apache 2.0 ライセンスの下でオープンソースソフトウェアとして公開されています。サポートが必要な場合は、GitHub で問題を報告できます。

プロキシを使用するための Secure Device Connector の設定

プロキシサーバーはアウトバウンドトラフィックをフィルタ処理する仲介の役割を果たすため、プロキシサーバーを使用することでセキュリティが強化されます。ネットワークデバイスがインターネットに直接さらされるのを防ぎ、攻撃のリスクを軽減します。プロキシサーバーは、SDC から Security Cloud Control へのすべてのアウトバウンド通信向けに Secure Device Connector（SDC）と統合できます。この手順では、ホストの Linux OS 設定ではなく、SDC に固有の Docker コンテナ構成の変更を取り上げます。

（注） 変更は、SDC の Docker コンテナにのみ影響します。Linux サーバーに関する組織の標準手続きに従って、ホスト Linux システムのプロキシ設定を行います。

始める前に

- Linux コマンド ライン インターフェイス（CLI）の知識が必要です。
- config.json ファイルを編集する前にバックアップを作成することを推奨します。

手順

ステップ 1 SSH を使用して SDC にアクセスし、次のコマンドを使用して SDC ユーザーに切り替えます。

```
$ sudo su - sdc
```

ステップ 2 `/usr/local/cdo/data/<your_sdc_name>/data/config.json` にある構成ファイルに移動します。

ステップ 3 JSON キーと値のペアを config.json ファイルに挿入します。

プロキシをプロキシサーバーの IP アドレスまたは FQDN に、ポートをプロキシサーバーのリスニングポートに置き換えます。

```
"awsProxy":"https://proxy:port"
```

ステップ 4 変更を保存し、SDC コンテナを再起動します。SDC コンテナを再起動するには、Docker コンテナ自体を再起動するか、SDC をホストしている仮想マシンを再起動します。

a) Docker コンテナを再起動するには、まず次のコマンドを使用して SDC コンテナ識別子を特定します。

```
[sdc@localhost cdo] $ docker ps
```

b) 次のコマンドを使用してコンテナを再起動します。

```
[sdc@localhost cdo] $ docker restart <container_id>
```

このとき、<*container_id*> は SDC コンテナの識別子です。

ステップ 5 次のコマンドを使用してステータスを確認し、SDC コンテナが正常に再起動し、動作していることを確認します。

```
[sdc@localhost cdo] $ docker ps | grep sdc
```

次のコマンドを使用して、logs/lar.log ファイル内のプロキシ設定に間違いがないことを確認します。

```
[sdc@localhost cdo] $ less /usr/local/cdo/data/<your_sdc_name>/logs/lar.log
```

SDC は、プロキシサーバーを使用して通信するように正しく設定されています。

Secure Device Connector の IP アドレスの変更

始める前に

- このタスクを実行するには、管理者である必要があります。
- SDC には、TCP ポート 443 またはデバイス管理用に設定したポートでのインターネットへの完全なアウトバウンドアクセスが必要です。

（注） SDC の IP アドレスを変更した後、デバイスを Security Cloud Control に再度オンボーディングする必要はありません。

手順

ステップ 1 SDC への SSH 接続を作成するか、仮想マシンのコンソールを開き、Security Cloud Control ユーザーとしてログインします。

ステップ 2 IP アドレスを変更する前に SDC VM のネットワーク インターフェイス設定情報を表示するには、`ifconfig` コマンドを使用します。

```
[cdo@localhost ~]$ ifconfig
```

ステップ 3 インターフェイスの IP アドレスを変更するには、`sudo sdc-onboard setup` コマンドを入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

ステップ 4 プロンプトが表示されたら、パスワードを入力します。

```
[sudo] password for Security Cloud Control:
```

ステップ 5 root パスワードと Security Cloud Control パスワードをリセットするプロンプトで `n` を入力します。

```
Would you like to reset the root and cdo passwords? (y/n):
```

ステップ 6 ネットワークを再設定するためのプロンプトで y と入力します。

```
Would you like to re-configure the network? (y/n):
```

ステップ 7 SDC に割り当てる新しい IP アドレスと、プロンプトが表示されたら SDC VM の他のドメイン情報を入力します。

a) IP Address
b) ゲートウェイ
c) DNS サーバー
d) NTP サーバーまたは FQDN

または、NTP サーバーまたは FQDN が適用されない場合は、Enter キーを押します。

e) Docker ブリッジ

または、Docker ブリッジが適用されない場合は Enter キーを押します。

ステップ 8 値が正しいことを求めるプロンプトが表示されたら、y でエントリを確認します。

```
Are these values correct? (y/n):
```

（注）
このコマンドの後、古い IP アドレスへの SSH 接続が失われるため、y を入力する前に値が正しいことを確認してください。

ステップ 9 SDC に割り当てた新しい IP アドレスを使用して SSH 接続を作成し、ログインします。

ステップ 10 接続ステータスのテストコマンドを実行して、SDC が稼働していることを確認できます。

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

すべてのチェックが緑色で [OK] と表示されている必要があります。

（注）
VM のコンソールでこの手順を実行している場合、値が正しいことを確認すると、接続ステータスのテストが自動的に実行され、ステータスが表示されます。

ステップ 11 Security Cloud Control ユーザーインターフェイスを介して SDC の接続を確認することもできます。確認するには、Security Cloud Control アプリケーションを開き、**[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** ページに移動します。

ステップ 12 ページを一度更新し、IP アドレスを変更したセキュアコネクタを選択します。

ステップ 13 [操作（Actions）] ペインで、[ハートビートの要求（Request heartbeat）] をクリックします。

ハートビートが正常に要求されたというメッセージが表示され、[最後のハートビート（Last Heartbeat）] に現在の日付と時刻が表示されるはずです。

重要
行った IP アドレスの変更は、GMT の午前 3 時以降にのみ SDC の [詳細（Details）] ペインに反映されます。

VM に SDC を展開する方法については、「自身の VM 上での Secure Device Connector の展開 （19 ページ）」を参照してください。

Secure Device Connector の削除

警告 この手順により、Secure Device Connector（SDC）が削除されます。この操作は元に戻せません。この操作を行った後は、新しい SDC をインストールしてデバイスを再接続するまで、その SDC に接続されているデバイスを管理できなくなります。デバイスを再接続するには、再接続が必要なデバイスごとに管理者ログイン情報を再入力する必要がある場合があります。

テナントから SDC を削除するには、次の手順を実行します。

手順

ステップ 1 削除する SDC に接続されているデバイスをすべて削除します。

1. SDC で使用されるすべてのデバイスを特定するには、同じ SDC を使用する Security Cloud Control デバイスを参照してください。
2. [インベントリ（Inventory）] ページで、識別したすべてのデバイスを選択します。
3. [デバイス アクション（Device Actions）] ウィンドウで [削除（Remove）] をクリックし、[OK] をクリックして操作を確定します。

ステップ 2 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

ステップ 3 [サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブが選択された状態で、青いプラスボタンをクリックし、[Secure Device Connector] を選択します。

ステップ 4 [セキュアコネクタ（Secure Connectors）] テーブルで、削除する SDC を選択します。これで、デバイス数はゼロになっているはずです。

ステップ 5 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。次の警告が表示されます。

警告
<sdc_name> を削除しようとしています。SDC の削除は元に戻せません。SDC を削除すると、デバイスをオンボーディングまたは再オンボーディングする前に、新しいSDCを作成してオンボーディングする必要があります。

現在オンボーディング済みのデバイスがあるため、SDCを削除するには、これらのデバイスを再接続し、新しい SDC を設定した後にログイン情報を再度入力する必要があります。

- ご質問や懸念事項がある場合は、[キャンセル（Cancel）] をクリックして、Security Cloud Control サポートにお問い合わせください。
- 続行するには、下のテキストボックスに <sdc_name> を入力して、[OK] をクリックします。

ステップ 6 続行する場合は、警告メッセージに記載されている SDC の名前を確認ダイアログボックスに入力します。

ステップ 7 [OK] をクリックして、SDC の削除を確定します。

ある SDC から別の SDC への ASA の移動

Security Cloud Control では、単一の Security Cloud Control テナントで複数の SDC を使用する。次の手順を使用して、管理対象 ASA を、ある SDC から別の SDC に移動できます。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [ASA] タブをクリックします。

ステップ 3 別の SDC に移動する 1 つ以上の ASA を選択します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[資格情報の更新（Update Credentials）] をクリックします。

ステップ 5 [セキュアデバイスコネクタ（Secure Device Connector）] ボタンをクリックし、デバイスの移動先の SDC を選択します。

ステップ 6 Security Cloud Control がデバイスにログインするために使用する管理者のユーザー名とパスワードを入力し、[更新（Update）] をクリックします。変更されていない限り、管理者のユーザー名とパスワードは、ASA のオンボードに使用したログイン情報と同じです。これらの変更をデバイスに展開する必要はありません。

（注）
すべての ASA が同じログイン情報を使用している場合、複数の ASA を、ある SDC から別の SDC に一括で移動できます。複数の ASA のログイン情報が異なる場合、各 ASA をある SDC から別の SDC に 1つずつ移動する必要があります。

Secure Device Connector の名前変更

手順

ステップ 1 左側のペインで**[ツールとサービス（Tools & Services）]** > **[セキュアコネクタ（Secure Connectors）]**を選択します。

ステップ 2 名前を変更する SDC を選択します。

ステップ 3 詳細ペインで、SDC の名前の横にある編集アイコン をクリックします。

ステップ 4 SDC の名前を変更します。

この新しい名前は、[インベントリ（Inventory）] ペインの Secure Device Connector フィルタなど、Security Cloud Control インターフェイス内の SDC 名が表示される場所に表示されます。

Secure Device Connector の更新

この手順は、トラブルシューティング ツールとして使用してください。通常、SDC は自動的に更新されるため、この手順を使用する必要はありません。ただし、VM の時刻設定が正しくない場合、SDC は AWS への接続を確立して更新を受信できませんが、この手順により、SDC の更新が開始され、時刻同期の問題によるエラーが解決されます。

手順

ステップ 1 SDC に接続します。SSH を使用して接続するか、VMware Hypervisor のコンソールビューを使用できます。

ステップ 2 **cdo** ユーザーとして SDC にログインします。

ステップ 3 SDC ユーザーに切り替えて、SDC Docker コンテナを更新します。

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

ステップ 4 SDC ツールキットをアップグレードします。

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

ステップ 5 SDC をアップグレードします。

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

（注）
SDC 仮想マシンで推奨される更新およびメンテナンス

必ず、組織の内部 IT セキュリティおよびパッチ管理ポリシーに従って、Ubuntu Linux で動作する SDC VM をモニターし、更新を適用してください。ネットワーク環境内で SDC VM のセキュリティ保護と最適な機

能が維持されるように、関連するセキュリティパッチを定期的に確認して適用することを強くお勧めします。

単一の Security Cloud Control テナントで複数の SDC を使用する

テナントに複数の SDC を展開すると、パフォーマンスを低下させることなく、より多くのデバイスを管理できます。1つのSDCが管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。

テナントにインストールできる SDC の数に制限はありません。各 SDC は 1 つのネットワークセグメントを管理できます。これらの SDC は、それらのネットワークセグメント内のデバイスを同一の Security Cloud Control テナントに接続します。複数の SDC がない場合、隔離されたネットワークセグメント内のデバイスを、異なる Security Cloud Control テナントで管理する必要があります。

2 番目以降の SDC を展開する手順は、最初の SDC を展開する手順と同じです。Security Cloud Control の VM イメージを使用した Secure Device Connector の展開か、自身の VM 上での Secure Device Connector の展開ことができます。テナントの最初の SDC には、テナントの名前と番号 1 が組み込まれています。追加の各 SDC には、順番に番号が付けられます。

同じ SDC を使用する Security Cloud Control デバイス

次の手順に従って、同じ SDC を使用して Security Cloud Control に接続するすべてのデバイスを識別します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 フィルタ基準がすでに指定されている場合は、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、Security Cloud Control で管理しているすべてのデバイスとサービスを表示します。

ステップ 5 フィルタボタン をクリックして、フィルタ メニューを展開します。

ステップ 6 フィルタの [Secure Device Connector] セクションで、必要な SDC の名前をクリックします。インベントリテーブルには、フィルタでチェックした SDC を使用して Security Cloud Control に接続しているデバイスのみが表示されます。

ステップ 7 （オプション）検索をさらに絞り込むには、フィルタメニューで追加のフィルタをチェックします。

ステップ 8 （オプション）完了したら、インベントリテーブルの上部にある [クリア（Clear）] ボタンをクリックして、Security Cloud Control で管理しているすべてのデバイスとサービスを表示します。

SDC のオープンソースおよびサードパーティライセンス

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License（MIT）

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/>

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/>

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files（the"Software"）, to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files（the "Software"）, to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT,

TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such

entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor

harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files（the"Software"）, to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** when ***

Open Source Initiative OSI - The MIT License

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

Permission is hereby granted, free of charge, to any person obtainginga copy of this software and associated documentation files（the"Software"）, to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Security Cloud Control でサポートされるデバイス、ソフトウェア、ハードウェア

Security Cloud Control は、複数のセキュリティ プラットフォームにおけるセキュリティポリシーとデバイス設定を管理できるクラウドベースの管理ソリューションです。Security Cloud Control は、以下のポリシーと設定を集中管理します。

- Cisco Secure Firewall ASA（オンプレミスと仮想）
- Cisco Secure Firewall Threat Defense（FTD）（オンプレミスと仮想）
- Cisco Secure Firewall Management Center（オンプレミス）
- Cisco Meraki MX
- Cisco IOS デバイス
- Cisco Umbrella
- AWS セキュリティグループ

ドキュメントでは、デバイス、ソフトウェア、およびハードウェア Security Cloud Control サポートについて説明しています。Security Cloud Control がサポートしていないソフトウェアやデバイスについては触れていません。ソフトウェアのバージョンまたはデバイスタイプのサポートを明示的に記載していない場合、それはサポートされません。

Cisco Secure Firewall ASA

Cisco 適応型セキュリティアプライアンス（ASA）は、ファイアウォール、VPN、および侵入防御機能を統合したセキュリティデバイスです。不正アクセス、サイバー脅威、データ侵害からネットワークを保護し、単一のプラットフォームで堅牢なセキュリティサービスを提供します。Security Cloud Control は、Cisco ASA デバイスの管理をサポートし、設定管理を合理化してネットワーク インフラストラクチャ全体で規制遵守を確保する機能を提供します。

Cisco Secure Firewall Threat Defense

Firewall Threat Defense は、従来のファイアウォール機能と高度な脅威防御機能を統合します。侵入防御、アプリケーション制御、URL フィルタリング、高度なマルウェア防御などを含む包括的なセキュリティ機能を提供します。FTD は、ASA ハードウェアアプライアンス、Cisco ファイアウォール ハードウェア アプライアンス、および仮想環境に展開できます。Threat Defense デバイスの管理は、Cisco Firewall Management Center、Security Cloud Control、Firewall Device Manager などのさまざまな管理インターフェイスを介して実行できます。

ソフトウェアおよびハードウェア互換性の詳細については、Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

Firewall Device Manager は、Threat Defense デバイス管理用に明示的に設計された Web ベースの管理インターフェイスです。Threat Defense デバイスを設定およびモニターするためのシンプルなアプローチを提供するため、小規模な展開や、直感的なインターフェイスを求める組織に最適です。

FDM は、ネットワーク設定、アクセス コントロール ポリシー、NAT ルール、VPN 設定、モニタリング、および基本的なトラブルシューティングに関する基本的な設定機能を提供します。通常、Web ブラウザを介してアクセスする FDM は、FTD デバイスで直接使用できるため、追加の管理サーバーやアプライアンスは必要ありません。

Cisco Secure Firewall Management Center

Security Cloud Control は、セキュアな統合を確立し、デバイスインベントリを検出し、一元化されたポリシー管理を有効にすることで、オンプレミスの Firewall Management Center の管理を簡素化します。ファイアウォールルール、VPN 設定、侵入防御ポリシーなどのセキュリティポリシーを、FMC 下にあるすべてのデバイスにわたって効率的に管理および展開できます。

Cisco Meraki MX

Cisco Meraki MX アプライアンスは、分散型展開用に設計されたエンタープライズグレード セキュリティおよび SD-WAN の次世代ファイアウォール アプライアンスです。Security Cloud Control は、Cisco Meraki MX デバイス上のレイヤ 3 ネットワークルールの管理をサポートします。Meraki デバイスを Security Cloud Control にオンボーディングすると、Meraki ダッシュボードと通信してそのデバイスを管理します。Security Cloud Control は設定要求を Meraki ダッシュボードに安全に転送し、新しい設定をデバイスに適用します。Cisco Meraki MX をサポートする Security Cloud Control の主な機能には、ポリシーの一元管理、バックアップと復元、モニタリングとレポート、コンプライアンスチェック、自動化機能などがあります。

Cisco IOS デバイス

Cisco IOS は、ルーティング、スイッチング、その他のネットワーキングプロトコルなどのネットワーク機能を管理および制御できます。シスコのネットワークデバイスを設定および維持するための一連の機能とコマンドを提供し、さまざまな規模および複雑さのネットワークでの効率的な通信と管理を可能にします。

Cisco Umbrella

Security Cloud Control は、Cisco Umbrella ASA 統合などの統合を通じて Cisco Umbrella を管理します。これにより管理者は、インターフェイスごとのポリシーを使用して、Cisco 適応型セキュリティアプライアンス（ASA）を Cisco Umbrella 設定に含めることができます。この統合により、ASA が DNS クエリを Cisco Umbrella にリダイレクトすることが可能になり、Cisco Umbrella の DNS セキュリティ、Web フィルタリング、および脅威インテリジェンス機能を活用してネットワークセキュリティを強化できます。

AWS セキュリティグループ

Security Cloud Control は、Amazon Web Services（AWS）仮想プライベートクラウド（VPC）向けの簡素化された管理インターフェイスを提供します。主な機能には、AWS サイト間 VPN 接続のモニタリング、AWS デバイスへの変更の追跡、AWS サイト間 VPN トンネルの表示が含まれます。

スイッチングとルーティングのサポートの詳細

次の表では、スイッチングおよびルーティング用デバイスを対象にした Cisco IOS ソフトウェアとデバイスタイプのサポートについて記載します。次の表の関連リンクで、デバイスタイプのオンボーディングと機能や特長に関する詳細な情報を確認してください。

デバイスタイプ	注記
Cisco IOS	Security Cloud Control は、Cisco IOS バージョン 12.4 以降を実行しているデバイスをサポートします。

Security Cloud Control でサポートされるブラウザ

Security Cloud Control は、次のブラウザの最新バージョンをサポートしています。

- Google Chrome
- Mozilla Firefox

Security Cloud Control プラットフォームのメンテナンススケジュール

Security Cloud Control は、新機能と品質の改善により、プラットフォームを毎週更新します。更新は、このスケジュールに従って 3 時間以内に行われます。

曜日（Day of the Week）	時刻 （24 時間表記、UTC）
Thursday	09:00 UTC - 12:00 UTC

このメンテナンス期間中、テナントには引き続きアクセスでき、クラウド提供型 Firewall Management Center または Multicloud Defense Controller がある場合はこれらのポータルにもアクセスできます。さらに、Security Cloud Control にオンボーディングしたデバイスは、引き続きセキュリティポリシーを適用します。

（注）
- メンテナンス期間中は、管理対象のデバイスに構成の変更を展開するために Security Cloud Control を使用しないことをお勧めします。
- Security Cloud Control の通信を停止する障害が発生した場合、その障害に対しては、メンテナンス期間外であっても、影響を受けるすべてのテナントで可能な限り迅速に対処いたします。

クラウド提供型 Firewall Management Center メンテナンススケジュール

テナントにクラウド提供型 Firewall Management Center をデプロイしているお客様には、Security Cloud Control でクラウド提供型 Firewall Management Center 環境が更新される約 1 週間前に通知されます。テナントのネットワーク管理者および管理者ユーザーには、電子メールで通知が届きます。また、Security Cloud Control のホームページにも、すべてのユーザーに今後の更新を通知するバナーが表示されます。

（注）
- メンテナンス期間中は、管理対象のデバイスに構成の変更を展開するためにクラウド提供型 Firewall Management Center を使用しないことをお勧めします。
- Security Cloud Control またはクラウド提供型 Firewall Management Center の通信を停止する障害が発生した場合、その障害に対しては、メンテナンス期間外であっても、影響を受けるすべてのテナントで可能な限り迅速に対処いたします。

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。

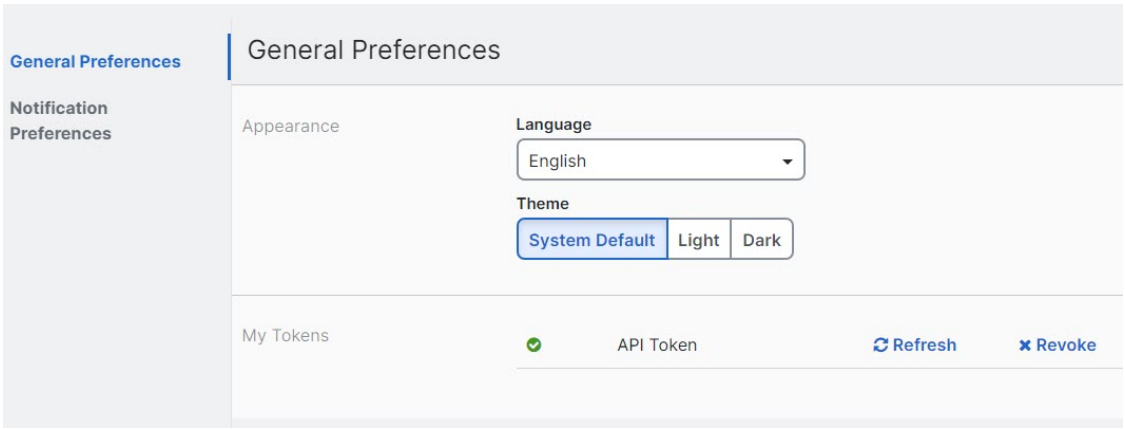
全般設定

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 （50 ページ）
- マイトークン（My Tokens）については、API トークン （65 ページ）を参照してください。
- [テナント設定（Tenant Settings）] については、以下を参照してください。
  - 変更リクエストのトラッキングの有効化 （51 ページ）
  - シスコサポートによるテナントの表示の防止 （51 ページ）
  - デバイスの変更を自動承認するオプションの有効化 （52 ページ）
  - デフォルトの競合検出間隔 （52 ページ）
  - Web 分析 （53 ページ）
  - テナント ID （54 ページ）
  - テナント名 （54 ページ）

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**

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。

テナント設定

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。変更要求トラッキングを有効にするには、次の手順に従います。

手順

ステップ 1 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

ステップ 2 [変更要求トラッキング（Change Request Tracking）] の下のスライダをクリックします。

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。

シスコサポートによるテナントの表示の防止

シスコサポートは、ユーザーをテナントに関連付けて、サポートチケットを解決したり、複数の顧客に影響する問題を積極的に修正したりします。ただし、必要に応じて、アカウント設定を変更して、シスコサポートがテナントにアクセスしないようにすることができます。そのためには、[シスコサポートがこのテナントを表示できないようにする（Prevent Cisco support from viewing this tenant）] の下にあるトグルボタンをスライドして、緑色のチェックマークを表示します。

Cisco サポートにテナントを表示させないようにするには、次の手順に従います。

手順

ステップ 1 左側のペインで **[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

ステップ 2 [シスコサポートがこのテナントを表示できないようにする（Prevent Cisco support from viewing this tenant）] の下のスライダをクリックします。

デバイスの変更を自動承認するオプションの有効化

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、次の手順に従います。

手順

ステップ 1 左側のペインで **[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

ステップ 2 [デバイスの変更を自動承認するオプションの有効化（Enable the Option to Auto-accept Device Changes）] の下にあるスライダをクリックします。

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。この選択は、このテナントで管理されるすべてのデバイスに影響し、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、[インベントリ] ページから利用できる [競合検出] 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 左側のペインで **[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

ステップ 2 [デフォルトの競合検出間隔（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にする

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。有効にすると、一回限りまたは繰り返しの自動展開をスケジュールできます。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、デバイス自体  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ないことに注意してください。デバイスが [競合検出（Conflict Detected）] または [非同期（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。

[自動展開をスケジュールするオプションを有効にする（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、次の手順に従います。

手順

ステップ 1 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

ステップ 2 [自動展開をスケジュールするオプションを有効にする（Enable the Option to Schedule Automatic Deployments）] の下のスライダをクリックします。

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。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。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 分析を無効にしたり、その後に有効にするには、次の手順を実行します。

手順

ステップ 1 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

ステップ 2 [Web分析（Web Analytics）] の下にあるトグルをクリックします。

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。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。

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起動ツールです。シスコの次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 か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。Workflows は、シスコとサードパーティの両方のアプリケーションで反復的でエラーが発生しやすいタスクを合理化することで、シスコをご利用中のお客様にクロスドメイン自動化機能を提供します。シスコが提供するまたは独自に作成できるカスタムおよび事前作成された自動化テンプレートと、シスコが提供するまたは独自に作成できる多数のアダプタオプションを使用して、クラウドまたはオンプレミスのターゲットに到達できます。

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に対するファイルのインスタントチェックを実行し、セキュリティアナリストがアウトブレイクの最初のソースを特定して分離できるようにします。また、悪意のあるファイルに対するレトロスペクティブ隔離を実行します。
- **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。

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

[概要（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。優先順位の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（Backup Failed）
- アップグレードが失敗する。
- 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

[すべて（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。

ユーザー通知の基本設定

通知は、テナントに関連付けられているデバイスで特定のイベントが発生したとき、デバイス証明書の期限が近いときや期限切れになったとき、またはバックグラウンドログ検索が開始、終了、または失敗するときに、Security Cloud Control によって生成されます。次の通知はデフォルトで有効になっており、ユーザーロールに関係なく、テナントに関係しているすべてのユーザーに対して表示されます。関心のあるアラートのみを表示するように個人の通知設定を変更できます。これらの設定はユーザー専用であり、テナントに関連付けら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。

[ユーザー名 ID（Username ID）] > [設定（Preferences）] > [通知設定（Notification Preferences）] ページで個人設定を表示します。ユーザー名 ID は、Security Cloud Control のすべてのページの右上隅に常に表示されます。このページから、次の [Security Cloud Controlで通知する条件（Notify Me in CDO When）] アラートを設定できます。

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 による管理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 による管理 デバイスにのみ適用されます。
- [クラウドへのFTDの移行（Migrate to Cloud）]：このアクションは、 FTD の変更時に適用可能です。

  デバイスマネージャを FMC 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。

バックグラウンドログ検索のアラートの送信

- [検索開始（Search started）]：検索が開始されたときに通知を受信します。これは、即時検索とスケジュール済み検索の両方に適用されます。
- [検索完了（Search completed）]：検索が終了したときに通知を受信します。これは、即時検索とスケジュール済み検索の両方に適用されます。
- [検索失敗（Search failed）]：検索が失敗したときに通知を受信します。これは、即時検索とスケジュール済み検索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 アラート

上記のアラートのいずれかを受信するには、[電子メールアラート（Email Alerts）] 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。

テナント通知設定

左側のナビゲーションバーから、**[設定（Settings）]** > **[通知設定（Notification Settings）]**の順にクリックします。

テナントに関連付けられているすべてのユーザーは、これらのアラートを自動的に受信します。また、これらのアラートの一部またはすべてを特定の電子メールまたはサービス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、**ネットワーク管理者**ユーザーロールが必要です。詳細については、「Security Cloud Control のユーザーロール」を参照してください。

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 （59 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 通知用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 左側のペインで **[管理（Administration）]** > **[通知設定（Notification Settings）]** 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 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 4 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 5 [保存（Save）] をクリックします。[キャンセル（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 左側のペインで **[管理（Administration）]** > **[通知設定（Notification Settings）]** をクリックします。

ステップ 2 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 3 [編集（Edit）] アイコンをクリックします。

ステップ 4 次の属性を編集します。

- メール アドレス
- 次の場合にアラートを送信...デバイスワークフロー（Send Alerts When.… Device Workflows）
- 次の場合にアラートを送信... [デバイス イベント（Device Events）]
- 次の場合にアラートを送信... バックグラウンドログ検索（Send Alerts When...Background Log Search）

ステップ 5 [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 左側のペインで **[管理（Administration）]** > **[通知設定（Notification Settings）]** をクリックします。

ステップ 2 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 3 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 4 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 と 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 **[管理（Administration）]** > **[通知設定（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。

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。[着信ウェブフック（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 [設定（Settings）] 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 左側のペインで **[管理（Administration）] > [通知設定（Notification Settings）]** をクリックします。

ステップ 10 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 11 [サービス統合（Service Integrations）] までスクロールします。

ステップ 12 青色のプラスボタンをクリックします。

ステップ 13 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 14 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 15 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 16 [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 左側のペインで **[管理（Administration）]** > **[通知設定（Notification Settings）]** をクリックします。

ステップ 4 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 5 [サービス統合（Service Integrations）] までスクロールします。

ステップ 6 青色のプラスボタンをクリックします。

ステップ 7 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 8 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 9 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 10 [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。

[使用履歴の表示（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すべてのロギングを表示します。

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。

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 認証ヘッダーに挿入する必要があります。API トークンは、有効期限のない「長期的な」アクセストークンですが、更新したり、取り消したりできます。

Security Cloud Control 内から API トークンを生成できます。生成されたトークンは、生成直後に、[一般設定（General Settings）] ページが開いている間のみ表示されます。Security Cloud Control で別のページを開いてから [一般設定（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。

個々のユーザーは、特定のテナントに対して独自のトークンを作成できます。あるユーザーが別のユーザーに代わってトークンを生成することはできません。トークンはアカウントとテナントのペアに固有であり、他のユーザーとテナントの組み合わせには使用できません。

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

トークンの管理

API トークンの生成

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）]**>**[一般設定（General Preferences）]** をクリックします。

ステップ 2 [マイトークン（My Tokens）] で、[API トークンの生成（Generate API Token）] をクリックします。

ステップ 3 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、トークンを安全な場所に保存します。

API トークンの確認

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、API トークンの更新を選択できます。

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）]**>**[一般設定（General Preferences）]** をクリックします。

ステップ 2 [マイトークン（My Tokens）] で、[更新（Renew）] をクリックします。Security Cloud Control は新しいトークンを生成します。

ステップ 3 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。

API トークンの取り消し

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）]**>**[一般設定（General Preferences）]** をクリックします。

ステップ 2 [マイトークン（My Tokens）] で、[取り消し（Revoke）] をクリックします。Security Cloud Control はトークンを取り消します。

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SAML シングルサインオンと Security Cloud Control の統合できます。

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://sign-on.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

SAML シングルサインオンと Security Cloud Control の統合は、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
- Security Cloud Control でのユーザーの管理
- Security Cloud Control のユーザーロール

マルチテナントポータルの管理

Security Cloud Control マルチテナント ポータル ビューには、複数のテナントにまたがるすべてのデバイスから取得された情報が表示されます。このマルチテナントポータルには、デバイスのステータス、デバイスで実行中のソフトウェアバージョンなどが表示されます。

はじめる前に

- マルチテナントポータルは、テナントでこの機能が有効になっている場合にのみ使用できます。テナントでマルチテナントポータルを有効にするには、Cisco TAC でサポートチケットを開きます。
- サポートチケットが解決され、ポータルが作成されると、ポータルで [ネットワーク管理者（Super Admin）] のロールを持つユーザーが、テナントを追加できるようになります。
- 発生する可能性のある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。

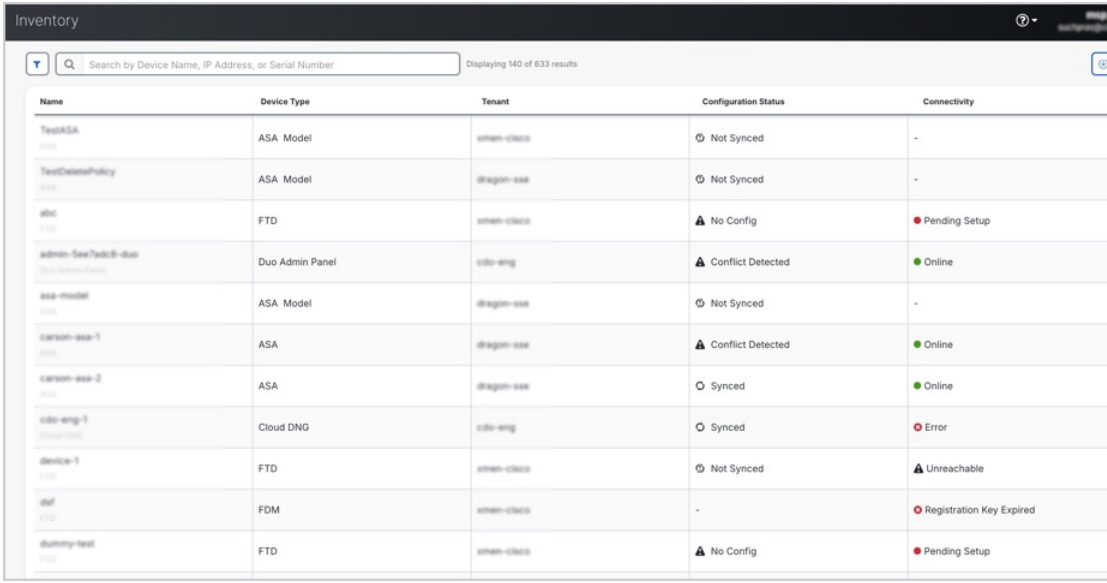
マルチテナントポータル

マルチテナントポータルには、次のメニューが用意されています。

- **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済みのすべてのデバイスが表示されます。[検索（Search）] および [フィルタ（Filter）] オプションを使用して、デバイスを検索します。
  - デバイスをクリックすると、[モデル（Model）]、[オンボーディング方式（Onboarding Method）]、[ファイアウォールモード（Firewall Mode）]、[ソフトウェアバージョン（Software Version）] などの詳細を表示できます。
  - デバイスを管理する Security Cloud Control テナントからのみデバイスを管理できます。マルチテナントポータルには、Security Cloud Control テナントページに移動するための [デバイスの管理（Manage Devices）] リンクが用意されています。

    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、[デバイスの管理（Manage Devices）] 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。
  - 詳細をカンマ区切り値（.csv）ファイルにエクスポートできます。この情報は、デバイスを分析したり、アクセス権のないユーザーに送信したりするのに役立ちます。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。作成されるファイル名には日付と時刻が含まれます。
  - 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。

図 *1*:セキュリティ デバイス



（注） デバイスを管理しているテナントが別のリージョン内にある場合は、そのリージョンの Security Cloud Control にサインインするためのリンクが表示されます。そのリージョン内の Security Cloud Control またはそのリージョン内のテナントにアクセスする権限のない場合は、デバイスを管理できません。

- テナント
  - ポータルに追加されたすべてのテナントが表示されます。
  - [ネットワーク管理者（Super Admin）] ロールを持つユーザーのみが、ポータルにテナントを追加できます。
  - 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。
- 設定
  - [一般設定（General Settings）] で、[ポータル設定（Portal Settings）] の詳細を表示できます。
  - [ユーザー管理（User Management）] では、すべての [ユーザー（Users）]、[Active Directoryグループ（Active Directory Groups）]、および [監査ログ（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） マルチテナントポータルの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ことができます。

- 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

マルチテナントポータルにテナントを追加する

[ネットワーク管理者（Super Admin）] ロールを持つユーザーは、ポータルにテナントを追加できます。複数のリージョンにまたがってテナントを追加できます。たとえば、ヨーロッパリージョンから米国リージョンにテナントを追加したり、米国リージョンからヨーロッパリージョンに追加したりできます。

重要 テナントに API のみのユーザーを作成するし、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 [Add Tenant] 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。

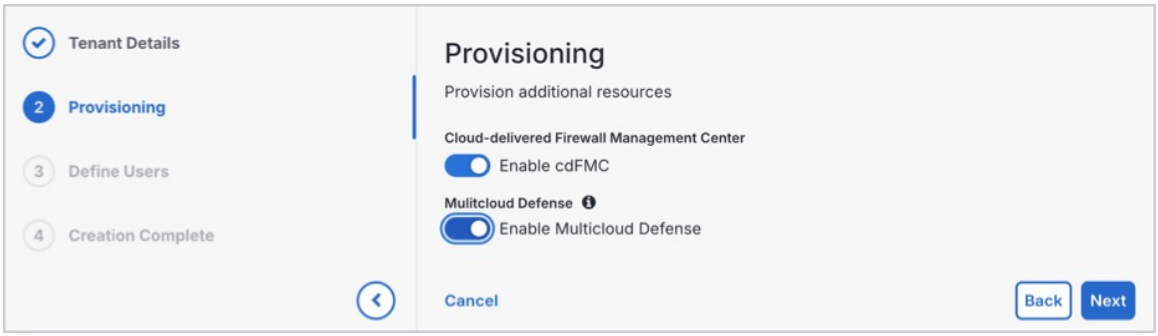
（注）

1. 既存のテナントをインポートするには、[既存のテナントをインポートしますか?（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 [テナントの詳細（Tenant Details）] で、[表示名（Display Name）] と [テナント名（Tenant Name）] を入力します。[次へ（Next）] をクリックします。

ステップ 5 [プロビジョニング（Provisioning）] で、

- [Cisco Multicloud Defense を有効化（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。
- [クラウド提供型 Firewall Management Center を有効化（Enable クラウド提供型 Firewall Management Center）] トグルを有効にして、テナントの クラウド提供型 Firewall Management Center をプロビジョニングします。
- [次へ（Next）] をクリックします。



ステップ 6 [ユーザーの定義（Define Users）] で、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、[ユーザーリスト（User list）] セクションに表示されます。

ステップ 7 [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。

マルチテナント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 右側に表示される対応する削除アイコンをクリックして、必要な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。

Manage-Tenant ポータルの設定

Security Cloud Control では、[設定（Settings）] ページのマルチテナント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 [設定（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

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。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、機密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分析を無効に、将来的に有効にするには、次の手順に従います。

1. 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。
2. [Web分析（Web Analytics）] の下にあるスライダをクリックします。

[ユーザー管理（User Management）]

マルチテナントポータル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（User Management）] 画面で確認できます。ユーザーアカウントは追加、編集または削除できます。詳細については、「Security Cloud Control でのユーザーの管理」を参照してください。

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 マルチテナントポータルで、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 [スイッチテナント（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）
- 脅威に対する防御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。

テナントに関連付けられているユーザーレコードの表示

手順

左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

（注）
シスコサポートがテナントにアクセスできないようにするには、[一般設定（General Settings）] ページで [シスコサポートがこのテナントを表示できないようにする（Prevent Cisco support from viewing this tenant）] トグルボタンを有効にします。全般設定 （50 ページ）

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、「Security Cloud Control のユーザーロール」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、**[[管理（Administration）]** > **[ユーザー管理（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

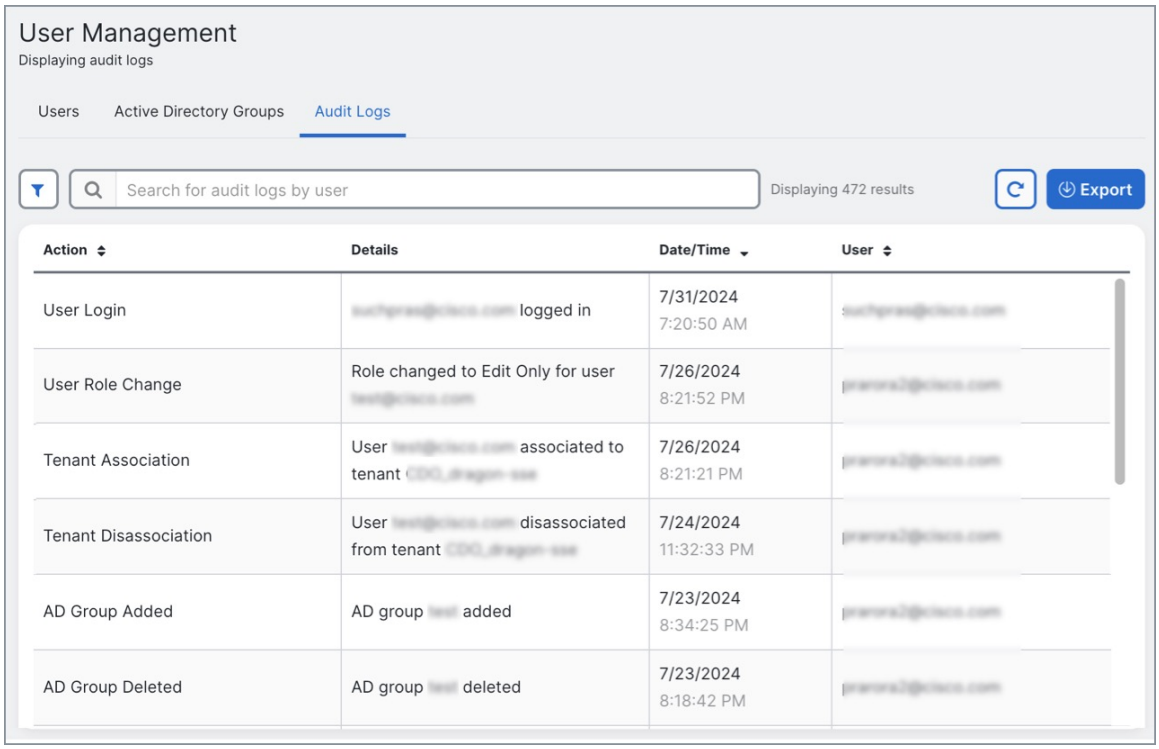
Security Cloud Control の [監査ログ（Audit Logs）] には、ユーザー関連およびシステムレベルのアクションが記録されます。[監査ログ（Audit Logs）] によってキャプチャされる主なイベントは次のとおりです。

- **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 **[管理（Administration）]** > **[ユーザー管理（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 *2:* 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

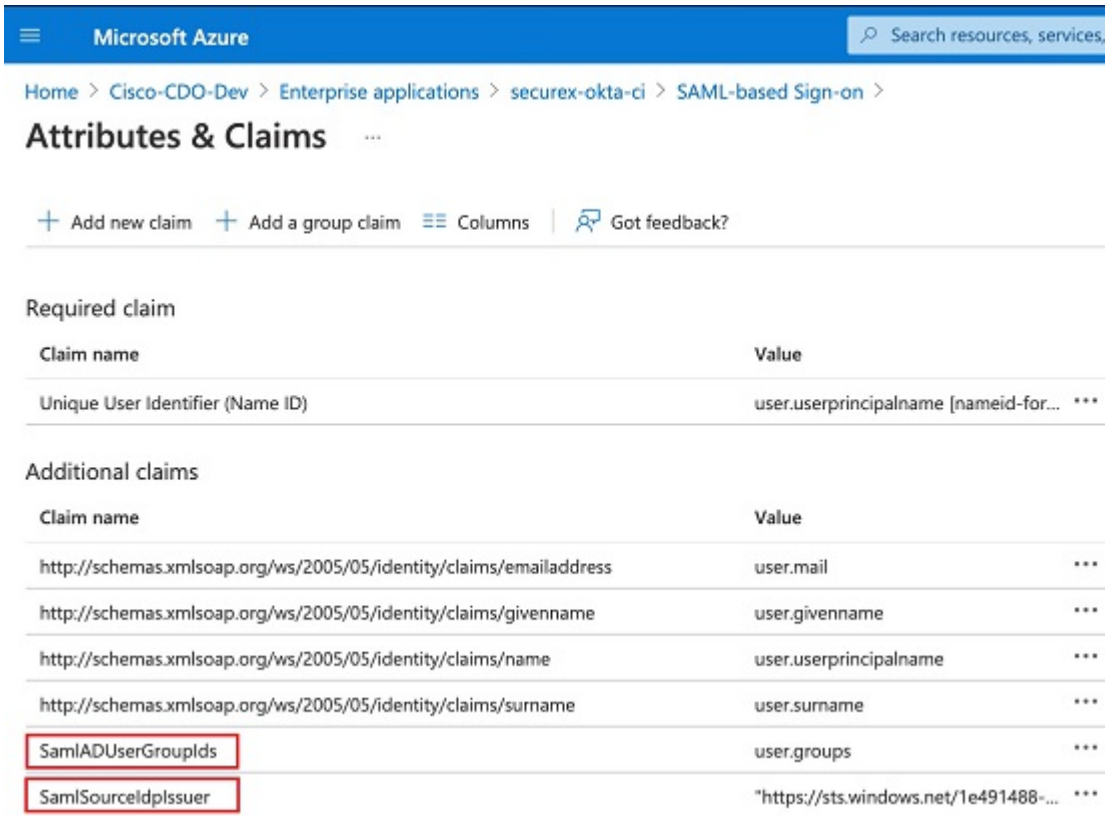
ユーザー管理の一種として Active Directory グループマッピングを Security Cloud Control に追加するには、まず Security Cloud Sign On に統合済みの Active Directory が必要です。Active Directory ID プロバイダー（IdP）がまだ統合されていない場合は、「Identity provider integration guide」[英語] を参照して、カスタム Active Directory IdP 統合に次の情報を統合します。

- 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。

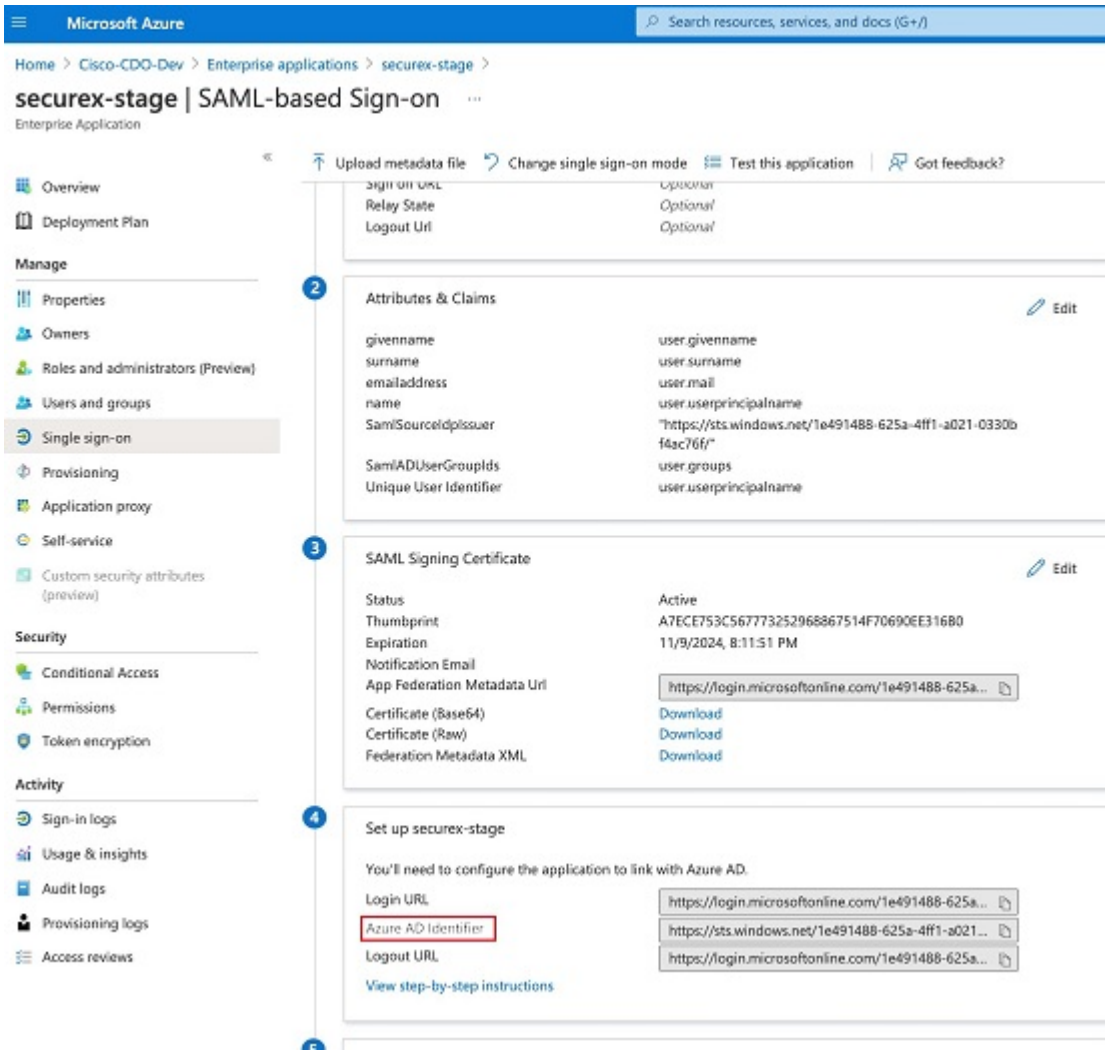
- **SamlADUserGroupIds**：この属性は、ユーザーが Active Directory 上で持つすべてのグループの関連付けを記述します。たとえば、次のスクリーンショットに示すように、Azure で [+グループ要求の追加（+ Add groups claim）] を選択します。

図 *3 : 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 *4 : 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 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 [Active Directoryグループ（Active Directory Groups）] タブをクリックします。

ステップ 4 Active Directory グループの追加（  ）ボタンをクリックします。

ステップ 5 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、「Security Cloud Control のユーザーロール」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 6 **[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 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 [Active Directory グループ（Active Directory Groups）] タブをクリックします。

ステップ 4 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 5 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 6 [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 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。
ステップ 3 [Active Directory グループ（Active Directory Groups）] タブをクリックします。
ステップ 4 削除する Active Directory グループを指定します。
ステップ 5 [Delete] アイコンをクリックします。
ステップ 6 [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 Security Cloud Sign On アカウントの作成
- Security Cloud Control ユーザー名での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 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 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。

重要 **2019 年 10 月 14 日より前に Security Cloud Control テナントが存在していた場合は、**この項目の代わりにCisco Security Cloud Sign On ID プロバイダーへの移行 （6 ページ）をログイン手順として使用してください。

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

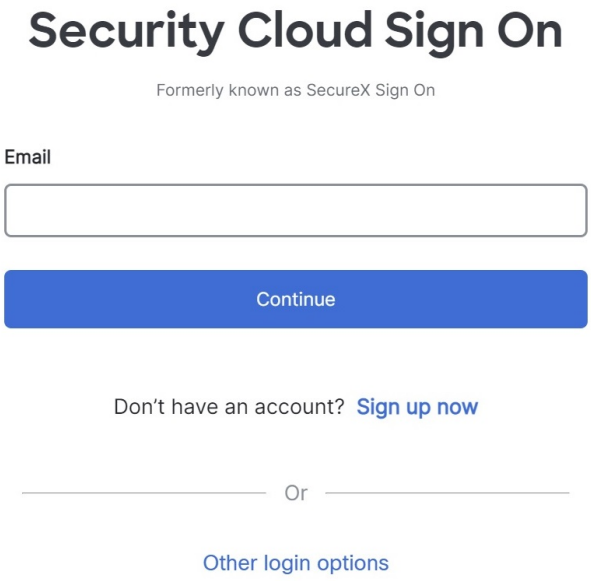
最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

手順

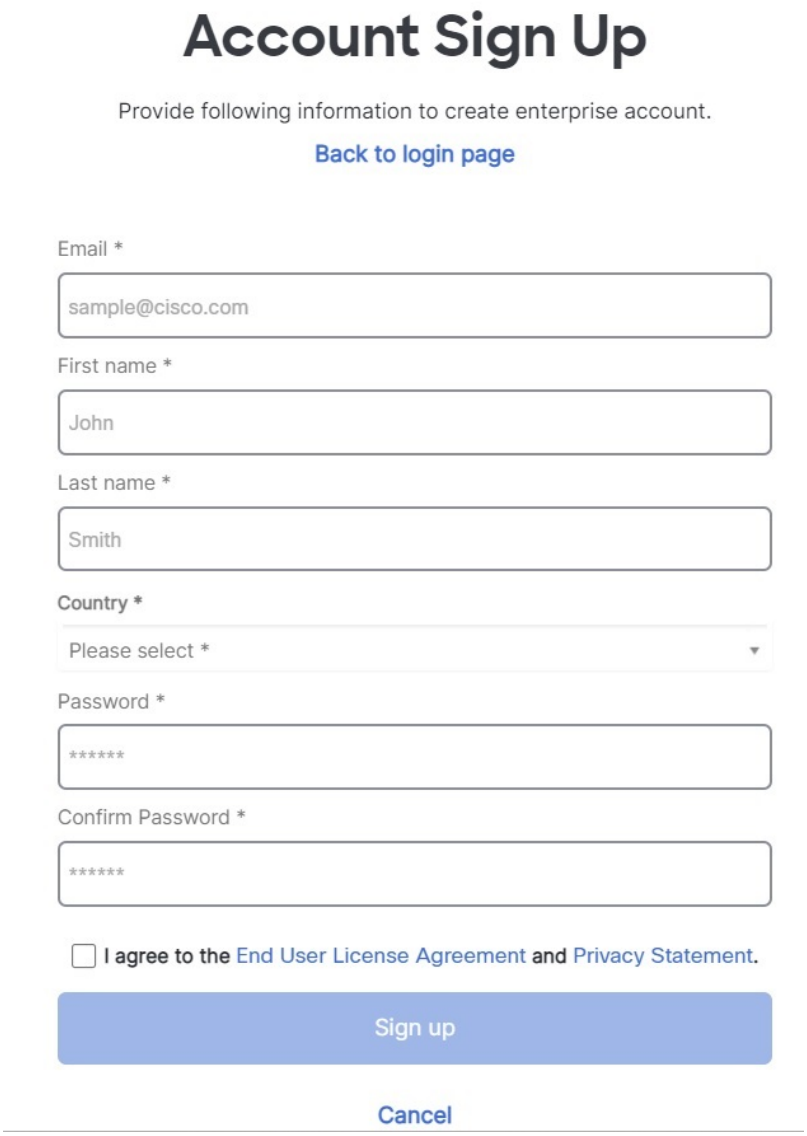
ステップ 1 新しい **Cisco Security Cloud Sign On** アカウントにサインアップします。

1. https://sign-on.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 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 3 + 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 4 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 5 [ロール（Role）] ドロップダウンリストから、ユーザーのSecurity Cloud Control のユーザーロールを選択します。

ステップ 6 [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、「マルチテナントポータルの管理」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。

（注） スーパー管理者は Security Cloud Control ユーザーレコードを作成できますが、そのユーザーレコードだけではユーザーがテナントにログインするには不十分です。テナントが使用する ID プロバイダーのアカウントも必要になります。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。ユーザーは Cisco Security Cloud Sign On アカウントに自己登録することができます。詳細については、新規 Security Cloud Control テナントへの初回ログイン （5 ページ）を参照してください。

- 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、「Security Cloud Control でのユーザーの管理」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://sign-on.security.cisco.com に移動し、サインイン画面の下部にある [サインアップ（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 でネットワーク管理者ロール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 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 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 4 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 5 ドロップダウンメニューからユーザーのSecurity Cloud Control のユーザーロールを選択します。

ステップ 6 [v] をクリックします。

（注）
スーパー管理者は Security Cloud Control ユーザーレコードを作成できますが、そのユーザーレコードだけではユーザーがテナントにログインするには不十分です。テナントが使用する ID プロバイダーのアカウン

トも必要になります。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 Secure Sign-on です。ユーザーは Cisco Secure Sign-On アカウントに自己登録することができます。詳細については、新規 Security Cloud Control テナントへの初回ログイン （5 ページ）を参照してください。

API のみのユーザーを作成する

手順

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

ステップ 2 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 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 4 [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 5 [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 6 ドロップダウンメニューからユーザーのSecurity Cloud Control のユーザーロールを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [ユーザー管理（User Management）] タブをクリックします。

ステップ 9 新しい API のみのユーザーの [トークン（Token）] 列で、[API トークンの生成（Generate API Token）] をクリックして API トークンを取得します。

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 でネットワーク管理者ロール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、スーパー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 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 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 4 [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Security Cloud Control のユーザーロール を選択します。

ステップ 5 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 6 [v] をクリックします。

ステップ 7 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。

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 でネットワーク管理者ロール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

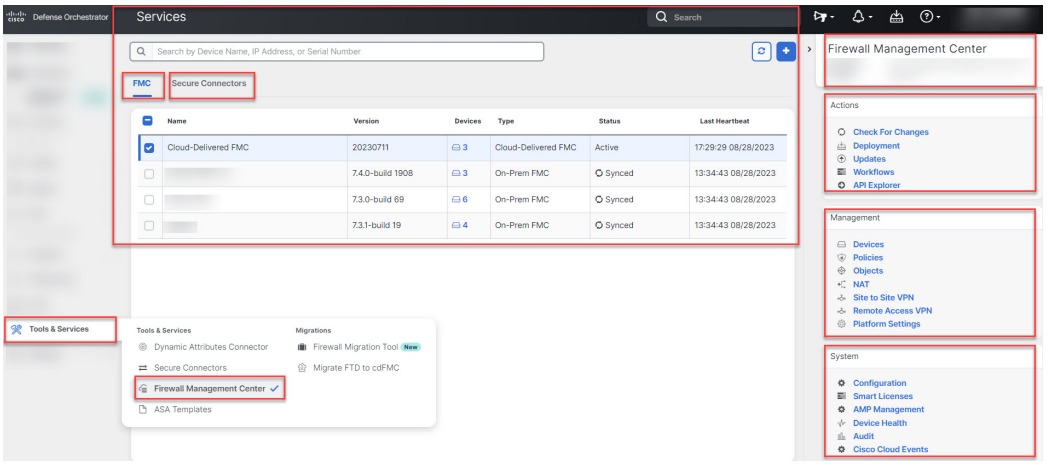
ステップ 1 Security Cloud Control にログインします。
ステップ 2 左側のペインで **[管理（Administration）]** > **[ユーザー管理（User Management）]** をクリックします。
ステップ 3 削除するユーザーの行のごみ箱アイコン をクリックします。
ステップ 4 [OK] をクリックします。
ステップ 5 [OK] をクリックして、テナントからアカウントを削除することを確認します。

Security Cloud Control の [サービス（Services）] ページ

[サービス（Services）] ページには、Security Cloud Control が提供するサービスのリストが表示されます。[FMC] タブを選択すると、Security Cloud Control アカウントにリンクされている クラウド提供型 Firewall Management Center と、Security Cloud Control にオンボーディングされているすべての オンプレミス Management Center が一覧表示されます。これらのオンプレミス Management Center によって管理されるデバイスは、[インベントリ（Inventory）] ページに表示されます。[サービス（Services）] ページの [セキュアコネクタ（Secure Connectors）] タブには、セキュアコネクタも一覧表示されます。

[FMC] タブをクリックし、青色のプラスアイコン（ ）をクリックして オンプレミス Management Center をオンボーディングし、右側のペインのオプションを使用してデバイスアクションを実行できます。また、バージョン、Management Center で管理されているデバイスの数、デバイスタイプ、デバイスの同期ステータスなどのデバイス情報を確認することもできます。管理対象デバイスのアイコンをクリックすると、[インベントリ（Inventory）] ページが表示され、選択した オンプレミス Management Center によって管理されているデバイスが自動的にフィルタリングされて表示されます。[サービス（Services）] ページでは、一度に複数の オンプレミス Management Center を選択して、Management Center のグループですべて一度にアクションを実行することもできます。クラウド提供型 Firewall Management Center が選択されている間は、オンプレミス Management Center を選択できません。新しいセキュアコネクタを追加したり、既存のセキュアコネクタでアクションを実行したりするには、[セキュアコネクタ（Secure Connectors）] タブを選択して をクリックします。

[管理（Administration）] > **[Firewall Management Center]** に移動します。



クラウド提供型 Firewall Management Center の場合、[サービス（Services）] ページには、次の情報が表示されます。

- テナントに クラウド提供型 Firewall Management Center が展開されていない場合は、[クラウド提供型FMCの有効化（Enable Cloud-Delivered FMC）] をクリックします。詳細については、「Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant」[英語] を参照してください。
- クラウド提供型 Firewall Management Center に展開された Cisco Secure Firewall Threat Defense デバイスの数。
- Security Cloud Control と クラウド提供型 Firewall Management Center ページ間の接続のステータス。
- クラウド提供型 Firewall Management Center の最後のハートビート。これは、クラウド提供型 Firewall Management Center 自体のステータスと管理するデバイスの数がこのページのテーブルと最後に同期された時刻を表します。
- 選択した クラウド提供型 Firewall Management Center のホスト名。

[クラウド提供型FMC（Cloud-Delivered FMC）] を選択し、[アクション（Actions）]、[管理（Management）]、または [設定（Settings）] ペインのリンクを使用して クラウド提供型 Firewall Management Center ユーザーインターフェイスを開き、クリックしたリンクに関連付けられている設定タスクを実行します。

[アクション（Actions）]：

- [変更の確認（Check For Changes）]：テーブルのデバイス数とステータスの情報は、このページと クラウド提供型 Firewall Management Center が最後に同期されたときに使用可能な情報で更新されます。同期は 10 分ごとに行われます。
- [展開（Deployment）]：クラウド提供型 Firewall Management Center のデバイス設定展開ページが表示されます。「設定変更の展開」を参照してください。

- [ワークフロー（Workflows）]：デバイスと通信するときに Security Cloud Control が実行するすべてのプロセスをモニターするための、[ワークフロー（Workflows）] ページが表示されます。「[ワークフロー（Workflows）] ページ」を参照してください。https://docs.defenseorchestrator.com/#!c-workflows-page.html
- [APIエクスプローラ（API Explorer）]：クラウド提供型 Firewall Management Center の REST API が一覧表示されるページが表示されます。Secure Firewall Management Center REST API のガイドを参照してください。

[管理（Management）]：

- [デバイス（Devices）]：クラウド提供型 Firewall Management Center ポータルの 脅威に対する防御 デバイス一覧表示ページが表示されます。「Configure Devices」を参照してください。
- [ポリシー（Policies）]：システム付属のアクセス コントロール ポリシーを編集したり、カスタム アクセス コントロール ポリシーを作成したりするための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Manage Access Control Policies」を参照してください。
- [オブジェクト（Objects）]：再利用可能オブジェクトを管理するための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Object Management」を参照してください。
- [NAT]：脅威に対する防御 デバイスでネットワーク アドレス変換ポリシーを設定するための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Manage NAT policies」を参照してください。
- [サイト間VPN（Site to Site VPN）]：2 つのサイト間のサイト間 VPN ポリシーを設定するための、クラウド提供型 Firewall Management Center ポータルのサイト間 VPN ダッシュボードページが表示されます。「Site-to-Site VPNs」を参照してください。
- [リモートアクセスVPN（Remote Access VPN）]：リモートアクセス VPN 設定を指定するための、クラウド提供型 Firewall Management Center ポータルのリモートアクセス VPN ダッシュボードページが表示されます。「Remote Access VPN」を参照してください。
- [プラットフォーム設定（Platform Settings）]：互いに関連しないさまざまな機能を設定し、いくつかのデバイス間でその値を共有するための、クラウド提供型 Firewall Management Center ポータルのプラットフォーム設定ページが表示されます。「Platform Settings」を参照してください。

[システム（System）]：

- [設定（Configuration）]：システム構成設定を指定するための、クラウド提供型 Firewall Management Center ポータルのシステム設定ページが表示されます。「System Configuration」を参照してください。
- [スマートライセンス（Smart Licenses）]：デバイスにライセンスを割り当てるための、クラウド提供型 Firewall Management Center ポータルのスマートライセンスページが表示されます。「Assign Licenses to Devices」を参照してください。

- [AMP管理（AMP Management）]：ネットワーク上のマルウェアを検出してブロックするためにシステムが使用するインテリジェンスを提供する、クラウド提供型 Firewall Management Center ポータルの AMP 管理ページが表示されます。「Cloud Connections for Malware Protection」を参照してください。
- [デバイスの正常性（Device Health）]：さまざまな正常性インジケータを追跡してシステムのハードウェアおよびソフトウェアの正常な動作を確保する、クラウド提供型 Firewall Management Center ポータルのヘルスモニタリングページが表示されます。「About Health Monitoring」を参照してください。
- [監査（Audit）]：Webインターフェイスとユーザーとの対話のそれぞれに対して生成される監査レコードを表示するための、クラウド提供型 Firewall Management Center ポータルの監査ログページが表示されます。
- [Cisco Cloudイベント（Cisco Cloud Events）]：イベントを SAL（SaaS）に直接送信するように クラウド提供型 Firewall Management Center を設定するための、Security Cloud Control ポータルの Cisco Cloud イベント設定ページが表示されます。「Send Events to SAL (SaaS)」を参照してください。

クラウド提供型 Firewall Management Center で、青い疑問符ボタンをクリックし、[ページレベルのヘルプ（Page-level Help）] を選択して、表示しているページの詳細と、さらに実行できるアクションを確認します。

異なるタブで Security Cloud Control と クラウド提供型 Firewall Management Center アプリケーションを開く機能のサポート

クラウド提供型 Firewall Management Center で 脅威に対する防御 デバイスまたはオブジェクトを設定するときに、追加のブラウザタブで適切な設定ページを開いて、ログオフせずに Security Cloud Control と クラウド提供型 Firewall Management Center ポータルで同時に作業できます。たとえば、クラウド提供型 Firewall Management Center でオブジェクトを作成し、同時にセキュリティポリシーから生成されたイベントログを Security Cloud Control でモニターできます。

この機能は、クラウド提供型 Firewall Management Center ポータルに移動するすべての Security Cloud Control リンクで使用できます。新しいタブで クラウド提供型 Firewall Management Center ポータルを開くには、次の手順を実行します。

Security Cloud Control ポータルで、**Ctrl**（Windows）または **Command**（Mac）ボタンを押したまま、対応するリンクをクリックします。

（注） 1 回クリックすると、同じタブで [クラウド提供型 Firewall Management Center] ページが開きます。

新しいタブで クラウド提供型 Firewall Management Center ポータルページを開く例を次に示します。

- [ツールとサービス（Tools & Services）] > [Firewall Management Center] を選択し、[クラウド提供型FMC（Cloud-Delivered FMC）] を選択します。

右側のペインで、**Ctrl**（Windows）または**Command**（Mac）ボタンを押したまま、アクセスするページをクリックします。

- [オブジェクト（Objects）] > [その他のFTDオブジェクト（Other FTD Objects）] を選択します。
- Security Cloud Control ページの右上隅にある検索アイコンをクリックし、表示される検索フィールドに検索文字列を入力します。

  検索結果から、**Ctrl**（Windows）または**Command**（Mac）ボタンを押したまま、矢印アイコンをクリックします。
- [ダッシュボード（Dashboard）]、[クイックアクション（Quick Actions）] の順に選択します。

  Ctrl（Windows）または **Command**（Mac）ボタンを押したまま、[FTDポリシーの管理（Manage FTD Policies）] または [FTDオブジェクトの管理（Manage FTD Objects）] をクリックします。

（注） 新しい Security Cloud Control テナントに切り替えると、新しいタブですでに開いている対応する クラウド提供型 Firewall Management Center ポータルがログアウトします。

関連項目

- Cisco Security Cloud Control を使用したオンプレミス Firewall Management Center の管理
- オンプレミス Firewall Management Center のオンボード
- Security Cloud Control テナントのクラウド提供型 Firewall Management Center のリクエスト
- Secure Device Connector
- Secure Event Connector

Security Cloud Control デバイスとサービスの管理

Security Cloud Control を使用すると、[インベントリ（Inventory）] ページでオンボード済みのデバイスを表示、管理、フィルタ処理、および評価できます。[インベントリ（Inventory）] ページから、次の操作を実行できます。

- Security Cloud Control 管理用のデバイスとサービスをオンボードします。
- 管理対象のデバイスとサービスの設定状態と接続状態を表示します。
- オンボードしたデバイスとテンプレートを個別のタブに分類して表示します。「Security Cloud Control インベントリ情報 （110 ページ）」を参照してください。
- 個々のデバイスとサービスを評価し、アクションを実行します。

- デバイスとサービスに固有の情報を表示し、問題を解決します。
- 次によって管理される脅威防御デバイスの正常性ステータスを表示します。
  - クラウド提供型 Firewall Management Center
  - オンプレミス Management Center

  クラウド提供型 Firewall Management Center によって管理される脅威防御デバイスの場合は、クラスタ内のデバイスのノードステータスも表示できます。
- 名前、タイプ、IPアドレス、モデル名、シリアル番号またはラベルで、デバイスまたはテンプレートを検索します。検索では大文字と小文字が区別されません。複数の検索条件を入力すると、少なくとも1つの条件に一致するデバイスとサービスが表示されます。「ページレベルの検索 （113 ページ）」を参照してください。
- デバイス タイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルで、デバイスまたはテンプレートのフィルタを絞り込みます。「フィルタ」を参照してください。

Security Cloud Control のデバイスの IP アドレスの変更

IP アドレスを使用してデバイスを Security Cloud Control にオンボードすると、Security Cloud Control ではその IP アドレスがデータベースに保存され、デバイスとの通信に使用されます。デバイスの IP アドレスが変更された場合は、Security Cloud Control に保存されている IP アドレスを更新して、新しいアドレスに一致させることができます。Security Cloud Control でデバイスの IP アドレスを変更しても、デバイスの構成は変更されません。

Security Cloud Control でデバイスとの通信に使用する IP アドレスを変更するには、次の手順を実行します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 4 IP アドレスを変更するデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインの上で、デバイスの IP アドレスの横にある編集ボタンをクリックします。

ステップ 6 フィールドに新しい IP アドレスを入力し、青色のチェックボタンをクリックします。

デバイス自体は変更されないため、デバイスの [設定ステータス（Configuration Status）] には、引き続き [同期済み（Synced）] と表示されます。

関連情報：

- テナント間でのデバイスの移動 （109 ページ）
- Security Cloud Control へのデバイス一括再接続 （108 ページ）

Security Cloud Control でのデバイスの名前の変更

すべてのデバイス、モデル、テンプレート、およびサービスには、Security Cloud Control へのオンボード時または作成時に名前が付けられます。デバイス自体の設定を変更せずに、その名前を変更することができます。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Device）] タブをクリックしてデバイスを見つけます。

ステップ 3 名前を変更するデバイスを選択します。

ステップ 4 [デバイスの詳細（Device Details）] ペインの上で、デバイス名の横にある編集ボタンをクリックします。

ステップ 5 フィールドに新しい名前を入力し、青色のチェックボタンをクリックします。

デバイス自体は変更されないため、デバイスの [設定ステータス（Configuration Status）] には、引き続き [同期済み（Synced）] と表示されます。

デバイスとサービスのリストのエクスポート

この記事では、デバイスとサービスのリストをコンマ区切り値（.csv）ファイルにエクスポートする方法について説明します。この形式にしたら、Microsoft Excel などのスプレッドシートアプリケーションでファイルを開いて、リスト内のアイテムを並べ替えたり、フィルタ処理したりできます。

エクスポートボタンは、デバイスとテンプレートタブで使用できます。選択したデバイスタイプタブで、デバイスの詳細をエクスポートすることもできます。

デバイスとサービスのリストをエクスポートする前に、フィルタペインを見て、エクスポートしたい情報がインベントリテーブルに表示されているかどうかを確認します。すべてのフィルタをクリアしてすべての管理対象デバイスとサービスを表示するか、情報をフィルタしてすべ

てのデバイスとサービスの一部を表示します。エクスポート機能は、インベントリテーブルに表示される内容をエクスポートします。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプタブをクリックして、そのタブのデバイスの詳細をエクスポートするか、[すべて（All）] をクリックしてすべてのデバイスから詳細をエクスポートします。

フィルタおよびページレベルの検索機能を使用して、必要なデバイスを見つけることができます。

ステップ 4 [CSV にリストエクスポート（Export list to CSV）] をクリックします。

ステップ 5 プロンプトが表示されたら、.csv ファイルを保存します。

ステップ 6 スプレッドシートアプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

デバイス設定のエクスポート

一度にエクスポートできるデバイス設定は1つだけです。次の手順を使用して、デバイスの設定を JSON ファイルにエクスポートします。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

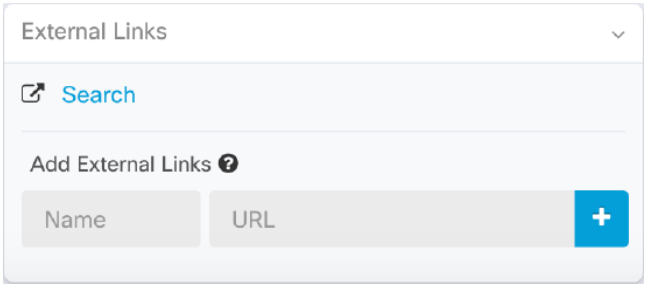
ステップ 4 必要なデバイスを選択して、強調表示します。

ステップ 5 [アクション（Actions）] ペインで、[設定のエクスポート（Export Configuration）] を選択します。

ステップ 6 [確認（Confirm）] を選択して、設定を JSON ファイルとして保存します。

デバイスの外部リンク

外部リソースへのハイパーリンクを作成し、Security Cloud Control で管理するデバイスに関連付けることができます。この機能を使用して、いずれかのデバイスのローカルマネージャへの便利なリンクを作成できます（。この機能を使用して、検索エンジン、ドキュメントリソース、企業 wiki、または選択したその他の URL へのリンクを作成できます。必要な数の外部リンクをデバイスに関連付けることができます。同じリンクを同時に複数のデバイスに関連付けることもできます。



作成したリンクはどこにでも到達できますが、企業のセキュリティ要件は変わりません。たとえば、普段オンプレミスで、または VPN 接続を介して特定の URL にアクセスすることによって企業ネットワークに接続する必要がある場合、この要件は維持されます。企業が特定の URL をブロックしている場合、それらの URL は引き続きブロックされます。制限されていない URL は引き続き制限されません。

location変数

URL に組み込むことができる {location} 変数を作成しました。この変数には、デバイスの IP アドレスが入力されます。次に例を示します。

```
https://{location}
```

に到達します。

関連情報：

- デバイスノートを書く （109 ページ）
- デバイスとサービスのリストのエクスポート （103 ページ）

デバイスからの外部リンクの作成

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 デバイスまたはモデルを選択します。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンクの名前を入力します。

ステップ 7 [URL] フィールドにリンクの URL を入力します。完全な URL を指定する必要があります。たとえばシスコの場合、http://www.cisco.com と入力します。

ステップ 8 [+] をクリックして、リンクとデバイスを関連付けます。

への外部リンクの作成

を Security Cloud Control から直接開く便利な方法を次に示します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 4 デバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 などのリンクの名前を入力します。

ステップ 7 https://{location} を [URL] フィールドに入力します。{location} 変数には、デバイスの IP アドレスが入力されます。

ステップ 8 [+] ボックスをクリックします。

複数デバイスの外部リンクの作成

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 4 複数のデバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンクの名前を入力します。

ステップ 7 次のいずれかの方法を使用して、アクセスする URL を入力します。

- 以下をURL フィールドに入力します。

  ```
  https://{location}
  ```

  URL フィールドに入力します。{location} 変数には、デバイスの IP アドレスが入力されます。入力後、デバイスの ASDM への自動リンクが作成されます。

- [URL] フィールドにリンクの URL を入力します。完全な URL を指定する必要があります。たとえばシスコの場合、http://www.cisco.com と入力します。

ステップ 8 [+] をクリックして、リンクとデバイスを関連付けます。

外部リンクの編集または削除

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 4 デバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンク名の上にカーソルを置くと、編集アイコンと削除アイコンが表示されます。

ステップ 7 該当するアイコンをクリックし、外部リンクを編集または削除して、アクションを確認します。

複数のデバイスへの外部リンクの編集または削除

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタとページレベルの検索を使用して、必要なデバイスを見つけることができます。

ステップ 4 複数のデバイスまたはモデルを選択します。

ステップ 5 右側の詳細ペインから、[外部リンク（External Links）] セクションに移動します。

ステップ 6 リンク名の上にカーソルを置くと、編集アイコンと削除アイコンが表示されます。

ステップ 7 該当するアイコンをクリックし、外部リンクを編集または削除して、アクションを確認します。

Security Cloud Control へのデバイス一括再接続

Security Cloud Control を使用すると、管理者は複数の管理対象デバイスを Security Cloud Control に同時に再接続を試みることができます。Security Cloud Control が管理するデバイスが「到達不能」とマークされている場合、Security Cloud Control は帯域外構成の変更を検出したり、デバイスを管理したりできなくなります。切断については、さまざまな原因が考えられます。デバイスの再接続を試みることは、Security Cloud Control によるデバイスの管理を復元するための簡単な最初のステップです。

（注） 新しい証明書を持つデバイスを再接続する場合、Security Cloud Control は、デバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。ただし、再接続するデバイスが 1 つだけの場合、Security Cloud Control は、それとの再接続を続行するために、証明書を手動で確認して受け入れることを求めます。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

フィルタを使用して、接続ステータスが「到達不能」であるデバイスを見つけてください。

ステップ 4 フィルタ処理の結果から、再接続を試みるデバイスを選択します。

ステップ 5 [再接続（Reconnect）] をクリックします。Security Cloud Control では、選択したすべてのデバイスに適用できるアクションのコマンドボタンのみ提供されることに注意してください。

ステップ 6 [通知（notifications）] タブで一括デバイス再接続アクションの進行状況を確認します。一括デバイス再接続ジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして Security Cloud Control でのジョブのモニタリング に移動します。

ヒント

デバイスの証明書またはログイン情報が変更されたために再接続に失敗した場合は、それらのデバイスに個別に再接続して、新しいログイン情報を追加し、新しい証明書を受け入れる必要があります。

テナント間でのデバイスの移動

デバイスを Security Cloud Control テナントに導入準備すると、そのデバイスは、別の Security Cloud Control テナントに移行できません。デバイスを新しいテナントに移動させる場合は、古いテナントからデバイスを削除して、新しいテナントに導入準備し直す必要があります。

デバイス証明書の有効期限の検出

管理証明書は Security Cloud Control から FDM による管理および ASA デバイスへのアクセスに使用されますが、Security Cloud Control から ASA、FDM による管理、および FTD デバイスの仮想プライベートネットワーク機能を使用するには Cisco Secure Client（旧称 AnyConnect）が必要です。

Security Cloud Control は、これらの証明書の有効期限ステータスをアクティブにモニターし、証明書の期限日が近づくと、または期限切れになるとユーザーに通知します。これにより、証明書の期限切れによるデバイス操作の中断を回避できます。対応する証明書を更新して、この問題に対処する必要があります。

管理証明書の有効期限チェックは ASA および FDM 管理対象デバイスに適用され、Secure Client 証明書の有効期限チェックは ASA、FDM による管理、および FTD デバイスに適用されます。

証明書の有効期限通知の表示

右上隅の [通知（Notifications）]（  ）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。[優先順位：高（High Priority）] セクションには、証明書の有効期限通知が表示されます。

これらの通知は、証明書の期限日の 30 日前、14 日前、および 7 日前に送信され、その後は証明書が期限切れになるか、有効な証明書で更新されるまで毎日送信されます。ユーザー設定ページの [通知設定（Notification Settings）] セクションで、これらの通知を電子メールで受信するように登録することもできます。詳細については、「ユーザー通知の基本設定」を参照してください。

デバイスノートを書く

以下の手順で、デバイス用に単一のプレーンテキストのノートファイルを作成します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 ノートを作成するデバイスまたはモデルを選択します。

ステップ 5 右側の [管理（Management）] ペインで、[ノート（Notes）] をクリックします。 Notes。

ステップ 6 右側のエディター ボタンをクリックして、既定のテキストエディタ（Vim または Emacs テキストエディタ）を選択します。

ステップ 7 [ノート（Notes）] ページを編集します。

ステップ 8 [保存（Save）] をクリックします。
ノートはタブに保存されます。

Security Cloud Control インベントリ情報

[インベントリ（Inventory）] ページには、すべての物理および仮想オンボードデバイスと、オンボードデバイスから作成されたテンプレートが表示されます。[インベントリ（Inventory）] ページでは、デバイスとテンプレートがそれぞれのタイプに基づいて分類され、各デバイスタイプ専用の対応するタブに表示されます。ページレベルの検索機能を使用するか、フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

[インベントリ（Inventory）] ページには、次の詳細情報が表示されます。

- [デバイス（Devices）] タブには、Security Cloud Control にオンボードされているすべてのライブデバイスが表示されます。
- [テンプレート（Templates）] には、ライブデバイスから、または Security Cloud Control にインポートされた構成ファイルから作成されたすべてのテンプレートデバイスが表示されます。

Security Cloud Control ラベルとフィルタ処理

ラベルは、デバイスまたはオブジェクトをグループ化するために使用されます。オンボーディング中またはオンボーディング後のいつでも、1 つ以上のデバイスにラベルを適用できます。ラベルをオブジェクトに適用するには、まずラベルを作成します。デバイスまたはオブジェクトにラベルを適用したら、そのラベルごとにデバイステーブルまたはオブジェクトテーブルの内容をフィルタリングできます。

（注） デバイスに適用されたラベルは、その関連オブジェクトには拡張されません。また、共有オブジェクトに適用されたラベルは、その関連オブジェクトには拡張されません。

ラベルグループは、次の構文「group name:label」を使用して作成できます。たとえば、Region:East または Region:West などです。これらの 2 つのラベルを作成する場合、グループラベルは Region になり、そのグループの East または West から選択できます。

デバイスとオブジェクトにラベルを適用する

デバイスにラベルを適用するには、以下の手順を実行します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックして、ラベルをデバイスに追加します。

ステップ 2 左側のペインで [オブジェクト（Objects）] をクリックして、ラベルをオブジェクトに追加します。

ステップ 3 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 4 適切なデバイスタイプのタブをクリックします。

ステップ 5 生成された表で 1 つ以上のデバイスまたはモデルを選択します。

ステップ 6 右側の [グループとラベルの追加（Add Groups and Labels）] フィールドで、デバイスのラベルを指定します。

ステップ 7 青色の + アイコンをクリックします。

フィルタ

[セキュリティデバイス（Security Devices）] ページと [オブジェクト（Objects）] ページのさまざまなフィルタを使用して、探しているデバイスやオブジェクトを検索できます。

フィルタ処理するには、[セキュリティデバイス（Security Devices）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Objects）] タブの左側のペインで をクリックします。

セキュリティ デバイス フィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルでフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

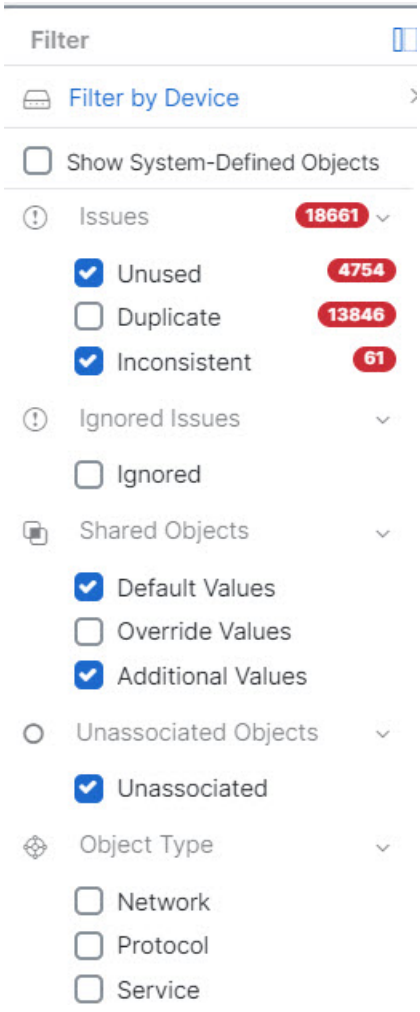
オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブ

ジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IPアドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

オブジェクトタイプフィルタを使用すると、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなどのタイプによってオブジェクトをフィルタ処理できます。共有オブジェクトフィルタを使用すると、デフォルト値またはオーバーライド値を持つオブジェクトをフィルタ処理できます。

デバイスとオブジェクトをフィルタ処理する場合、検索語を組み合わせて、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

次の例では、「問題（使用されている、または、不整合）があるオブジェクト、かつ、追加の値を持つ共有オブジェクト」であるようなオブジェクトを検索するフィルタが適用されます。



Security Cloud Control の検索機能の使用

Security Cloud Control プラットフォームにはきわめて効率的な検索機能があり、必要なものが簡単に見つかります。各ページの検索バーはそのページの内容に合わせてカスタマイズされたものであり、一方グローバル検索では、テナント全体を包括的に検索できます。この検索機能により、必要な情報をすばやく見つけられるため、時間と手間を省けます。

ページレベルの検索

ページレベルの検索では、[インベントリ（Inventory）]、[ポリシー（Policies）]、[オブジェクト（Objects）]、[VPN]、[変更ログ（Change Log）]、および [ジョブ（Jobs）] ページで特定の項目を検索できます。

- [インベントリ] スペースでは、検索バーに入力を開始するだけで、検索条件に一致するデバイスが表示されます。デバイスの名前の一部、IP アドレス、または物理デバイスのシリアル番号を入力して、デバイスを見つけることができます。
- [ポリシー（Policies）] スペースでは、名前、コンポーネント、または使用されているオブジェクトでポリシーを検索できます。
- [オブジェクト（Objects）] スペースでは、オブジェクト名の一部、または IP アドレス、ポート、プロトコルの一部を入力してオブジェクトを検索できます。
- [VPN] スペースでは、VPN ポリシーで使用されるトンネル名、デバイス名、および IP アドレスで検索できます。
- [変更ログ（Change log）] スペースでは、イベント、デバイス名、またはアクションに基づいてログを検索できます。

手順

ステップ 1 インターフェイスの上部近くにある検索バーに移動します。
ステップ 2 検索バーに検索条件を入力すると、対応する結果が表示されます。

オブジェクト

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

デバイスをオンボードすると、Security Cloud Control はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

Security Cloud Control は、複数のデバイスで使用されるオブジェクトを**共有オブジェクト**と呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである 2 つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。
- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。2024 年 6 月 28 日までは、関連付けられていないオブジェクトをルールまたはポリシーで使用すると、Security Cloud Control ではそのコピーが作成され、そのコピーが使用されます。この動作により、[オブジェクト（Objects）] メニューに同じオブジェクトの 2 つのインスタンスが表示されることがあります。一方、Security Cloud Control ではこの動作は行われなくなります。関連付けられていないオブジェクトをルールまたはポリシーで使用することはできますが、Security Cloud Control によってオブジェクトが重複して作成されることはありません。

[オブジェクト（Objects）] メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、Security Cloud Control によって管理されているオブジェクトを表示できます。

Security Cloud Control を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。Security Cloud Control を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してオブジェクトフィルタします。
- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。

- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが Security Cloud Control にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

（注） オブジェクトに対して行われたアウトオブバンド変更は、オブジェクトに対するオーバーライドとして検出されます。このような変更が発生すると、編集された値がオーバーライドとしてオブジェクトに追加されます（オブジェクトを選択すると表示できます）。デバイスのアウトオブバンド変更の詳細については、デバイスのアウトオブバンド変更を参照してください。

オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、Security Cloud Control のトラブルシューティングを参照してください。

オブジェクト タイプ

以下の表では、デバイス用に作成し、Security Cloud Control を使用して管理できるオブジェクトについて説明します。

表 *2:* 共通のオブジェクト

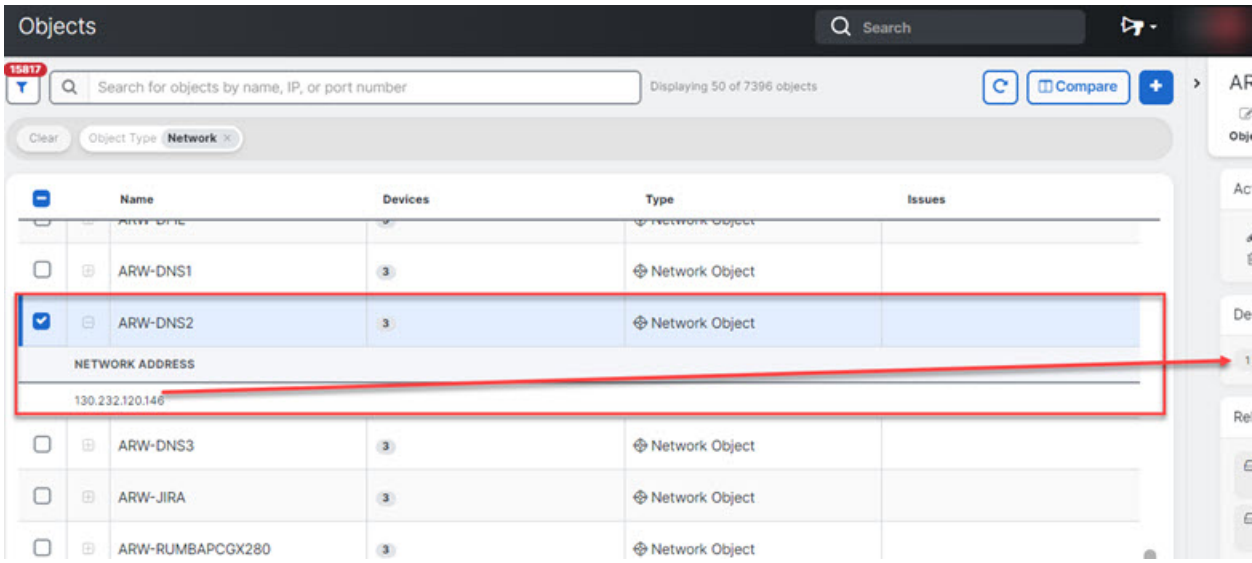
オブジェクト タイプ	説明
ネットワーク（Network）	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
URL	URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

共有オブジェクト

Security Cloud Control では、複数のデバイス上の同じ名前と同じ内容のオブジェクトを「共有オブジェクト」と呼びます。共有オブジェクトはこのアイコンで識別されます。

これは、[オブジェクト（Objects）]ページに表示されます。共有オブジェクトを使用すると、1 か所でオブジェクトを変更でき、その変更がそのオブジェクトを使用する他のすべてのポリシーに影響するため、ポリシーの維持が容易になります。共有オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

共有オブジェクトを調査する場合、Security Cloud Control ではオブジェクトの内容がオブジェクトテーブルに表示されます。共有オブジェクトの内容はまったく同じです。Security Cloud Control では、オブジェクトの要素の結合された、つまり「フラット化された」ビューが詳細ペインに表示されます。詳細ペインでは、ネットワーク要素が単純なリストにフラット化されており、名前付きオブジェクトに直接関連付けられていないことに注意してください。



オブジェクトのオーバーライド

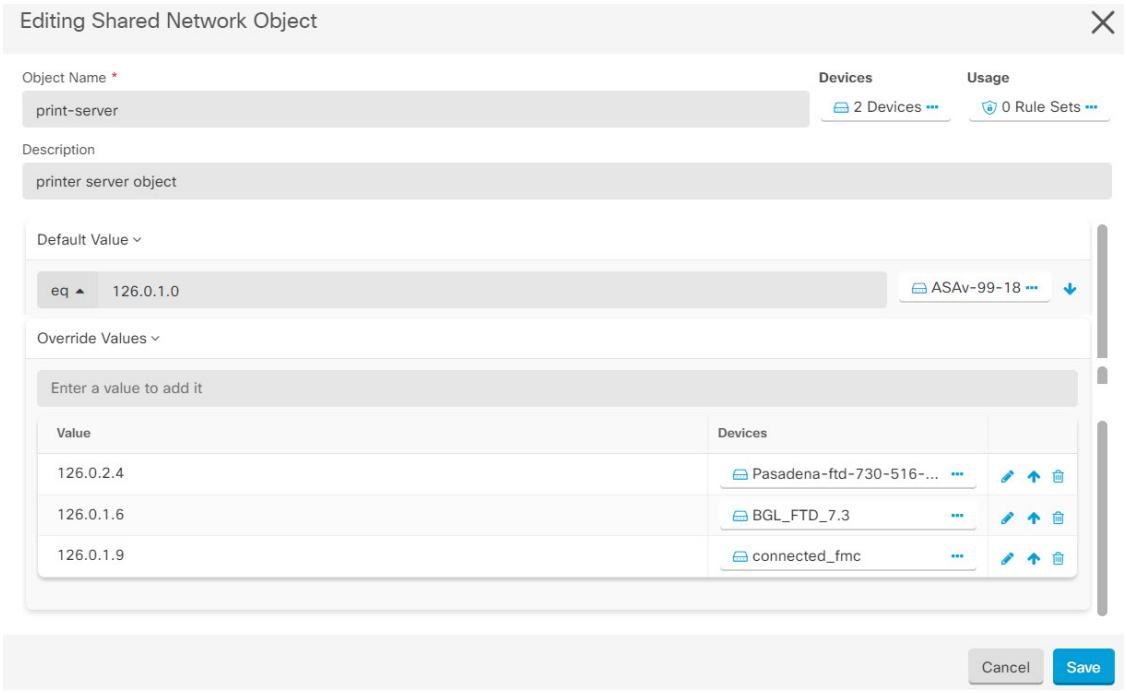
オブジェクトのオーバーライドを使用すると、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。Security Cloud Control は、オーバーライドの設定時に指定したデバイスに対応する値を使用します。これらのオブジェクトは、名前は同じで値が異なる複数のデバイス上にありますが、Security Cloud Control は、これらの値がオーバーライドとして追加されただけでは、それらを**不整合オブジェクト**として識別しません。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクトオーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、各オフィスにプリンタサーバーがあり、プリンタ サーバー オブジェクト `print-server` を作成しているシナリオを考えてみましょう。ACL には、プリンタサーバーのインターネットへのアクセスを拒否するルールを設定しています。プリンタ サーバー オブジェクトには、オ

フィスごとに変更できるデフォルト値があります。これを行うには、オブジェクトのオーバーライドを使用し、すべての場所でルールと「printer-server」オブジェクトの一貫性を維持します（値は異なる場合があります）。

オブジェクトに対して行われたアウトオブバンド変更は、オブジェクトに対するオーバーライドとして検出されます。このような変更が発生すると、編集された値がオーバーライドとしてオブジェクトに追加されます（オブジェクトを選択すると表示できます）。アウトオブバンド変更の詳細については、デバイスのアウトオブバンド変更を参照してください。



（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを1つの共有オブジェクトに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

関連付けのないオブジェクト

ルールやポリシーですぐに使用するためのオブジェクトを作成できますが、ルールやポリシーに関連付けないオブジェクトを作成することもできます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、Security Cloud Control ではそのコピーが作成され、そのコピーが使用されます。関連付けられていない元のオブジェクトは、夜間のメンテナンスジョブで削除されるか、ユーザーが削除するまで、使用可能な一連のオブジェクト内に残ります。

関連付けられていないオブジェクトはコピーとして Security Cloud Control に残り、オブジェクトに関連付けられたルールまたはポリシーが誤って削除された場合にすべての設定が失われないようにします。

左側のペインで、[オブジェクト（Objects）] > [ ] の順にクリックし、[関連付けなし（Unassociated）] チェックボックスをオンにします。

オブジェクトの比較

手順

ステップ 1 左側のペインで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 ページのオブジェクトをフィルタ処理して、比較するオブジェクトを見つけます。

ステップ 3 [比較（Compare）] Compare ボタンをクリックします。

ステップ 4 比較するオブジェクトを最大 3 つまで選択します。

ステップ 5 画面の下部にオブジェクトを並べて表示します。

- [オブジェクトの詳細（Object Details）] タイトルバーの上下の矢印をクリックして、表示するオブジェクト詳細を調整します。
- [詳細（Details）] ボックスと [関係（Relationships）] ボックスを展開するか折りたたんで、表示する情報を調整します。

ステップ 6 （オプション）[関係（Relationships）] ボックスには、オブジェクトの使用方法が表示されます。オブジェクトはデバイスまたはポリシーに関連付けられている場合があります。オブジェクトがデバイスに関連付けられている場合は、デバイス名をクリックしてから [構成の表示（View Configuration）] をクリックして、デバイスの構成を表示できます。Security Cloud Control はデバイスの構成ファイルを表示し、そのオブジェクトのエントリをハイライトします。

フィルタ

[セキュリティデバイス（Security Devices）] ページと [オブジェクト（Objects）] ページのさまざまなフィルタを使用して、探しているデバイスやオブジェクトを検索できます。

フィルタ処理するには、[セキュリティデバイス（Security Devices）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Objects）] タブの左側のペインで をクリックします。

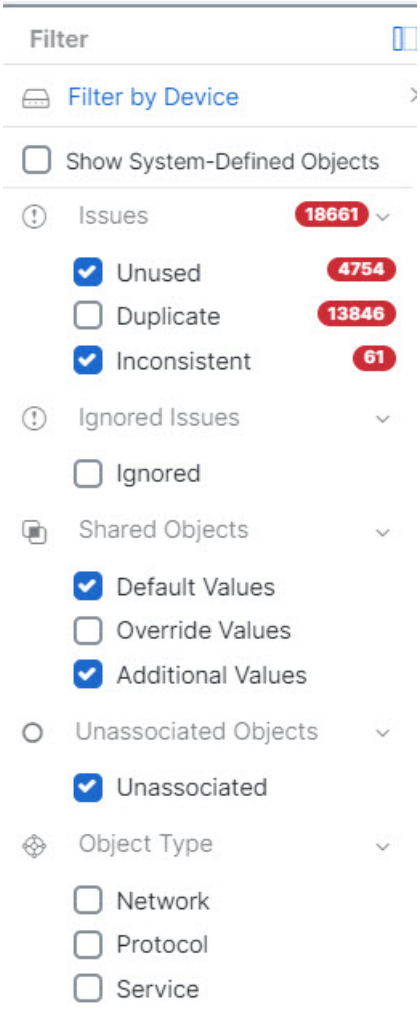
セキュリティ デバイス フィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルでフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IP アドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

オブジェクトタイプフィルタを使用すると、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなどのタイプによってオブジェクトをフィルタ処理できます。共有オブジェクトフィルタを使用すると、デフォルト値またはオーバーライド値を持つオブジェクトをフィルタ処理できます。

デバイスとオブジェクトをフィルタ処理する場合、検索語を組み合わせて、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

次の例では、「問題（使用されている、または、不整合）があるオブジェクト、かつ、追加の値を持つ共有オブジェクト」であるようなオブジェクトを検索するフィルタが適用されます。



オブジェクトフィルタ

フィルタ処理するには、[オブジェクト（Object）] タブの左側のペインで をクリックします。

- [デバイスごとのフィルタ（Filter by Device）]：特定のデバイスを選択して、選択したデバイスで見つかったオブジェクトを表示できます。
- [問題（Issues）]：未使用のオブジェクト、重複するオブジェクト、および一貫性のないオブジェクトを選択して表示できます。
- [無視された問題（Ignored Issues）]：不整合を無視したすべてのオブジェクトを表示できます。
- [共有オブジェクト（Shared Objects）]：複数のデバイスで共有されていることが Security Cloud Control によって検出されたすべてのオブジェクトを表示できます。デフォルト値またはオーバーライド値のみ、あるいはその両方を持つ共有オブジェクトを表示することを選択できます。
- [関連付けられていないオブジェクト（Unassociated Objects）]：ルールまたはポリシーに関連付けられていないすべてのオブジェクトを表示できます。
- [オブジェクトタイプ（Object Type）]：オブジェクトタイプを選択して、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなど、選択したタイプのオブジェクトのみを表示できます。

サブフィルタ–各メインフィルタ内には、選択をさらに絞り込むために適用できるサブフィルタがあります。これらのサブフィルタは、オブジェクトタイプ（ネットワーク、サービス、プロトコルなど）に基づいています。

このフィルタバーで選択されたフィルタは、以下の条件に一致するオブジェクトを返します。

***** 2 つのデバイスのいずれかにあるオブジェクト（[デバイスでフィルタ処理（Filter by Device）] をクリックしてデバイスを指定します）。および

***** **一貫性のない**オブジェクト。および

***** **ネットワーク**オブジェクトまたは**サービス**オブジェクト。 および

***** オブジェクトの命名規則に「**グループ**」という単語が含まれているオブジェクト。

[システムオブジェクトの表示（Show System Objects）] がオンになっているため、結果にはシステムオブジェクトとユーザー定義オブジェクトの両方が含まれます。

[システム定義オブジェクトの表示（Show System-Defined Objects）] フィルタ

一部のデバイスには、一般的なサービス用に事前定義されたオブジェクトがあります。これらのシステム オブジェクトは既に作成されており、ルールやポリシーで使用できるので便利です。オブジェクトテーブルには多くのシステムオブジェクトが含まれる場合があります。システムオブジェクトは編集または削除できません。

[システム定義オブジェクトの表示（Show System-Defined Objects）] は、デフォルトでは**オフ**になっています。オブジェクトテーブルにシステムオブジェクトを表示するには、フィルタバーで [システム定義オブジェクトの表示（Show System-Defined Objects）] をオンにします。オブジェクトテーブルでシステムオブジェクトを非表示にするには、フィルタバーで [システムオブジェクトを表示（Show System Objects）] をオフのままにします。

システムオブジェクトを非表示にすると、それらは検索およびフィルタ処理の結果に含まれなくなります。システムオブジェクトを表示すると、それらはオブジェクトの検索とフィルタ処理の結果に含まれます。

オブジェクトフィルタを設定する

条件を必要な数だけ設定してフィルタリングできます。フィルタリングするカテゴリが多いほど、予想される結果は少なくなります。

手順

ステップ 1 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 2 ページ上部のフィルタアイコン をクリックして、フィルタパネルを開きます。オブジェクトが誤って除外されないように、チェック付きのフィルタのチェックを外します。さらに、検索フィールドを見て、検索フィールドに入力された可能性のあるテキストを削除します。

ステップ 3 結果を特定のデバイスで見つかったものに限定したい場合：

1. **[デバイスでフィルタ処理（Filter By Device）]** をクリックします。
2. すべてのデバイスを検索するか、デバイスタブをクリックして特定の種類のデバイスのみを検索します。
3. フィルタ条件に含めるデバイスのチェックボックスをオンにします。
4. [OK] をクリックします。

ステップ 4 検索結果にシステムオブジェクトを含めるには、[システムオブジェクトを表示（Show System Objects）] をオンにします。検索結果でシステムオブジェクトを除外するには、[システムオブジェクトを表示（Show System Objects）] をオフにします。

ステップ 5 [問題（Issues）] で、フィルタリングするオブジェクトの問題のチェックボックスをオンにします。複数の問題をオンにすると、オンにしたいずれかのカテゴリのオブジェクトがフィルタ結果に含まれます。

ステップ 6 問題があったが管理者によって無視されたオブジェクトを表示する場合は、[無視（Ignored）] の問題をチェックします。

ステップ 7 2つ以上のデバイス間で共有されるオブジェクトをフィルタリングする場合は、[共有オブジェクト（Shared Objects）] で必要なフィルタをオンにします。

- [デフォルト値（Default Values）]：デフォルト値のみを持つオブジェクトをフィルタリングします。
- [オーバーライド値（Override Values）]：オーバーライドされた値を持つオブジェクトをフィルタリングします。

• [追加の値（Additional Values）]：追加の値を持つオブジェクトをフィルタリングします。

ステップ 8 ルールまたはポリシーの一部ではないオブジェクトをフィルタリングする場合は、[関連付けなし（Unassociated）] をオンにします。

ステップ 9 フィルタリングする [オブジェクトタイプ（Object Types）] をオンにします。

ステップ 10 オブジェクト名、IP アドレス、またはポート番号を [オブジェクト（Objects）] 検索フィールドに追加して、フィルタリングされた結果の中から検索条件に一致するオブジェクトを見つけることもできます。

フィルタ基準からデバイスを除外する場合

デバイスをフィルタリング基準に追加すると、結果にはデバイス上のオブジェクトは表示されますが、それらのオブジェクトと他のデバイスとの関係は表示されません。たとえば、**ObjectA** が ASA1 と ASA2 の間で共有されている場合、オブジェクトをフィルタリングして ASA1 上の共有オブジェクトを検索すると、**ObjectA** は見つかりますが、[関係（Relationships）] ペインには、オブジェクトが ASA1 にあることだけが表示されます。

オブジェクトが関連するすべてのデバイスを表示するには、検索条件でデバイスを指定しないでください。他の条件でフィルタリングし、必要に応じて検索条件を追加します。Security Cloud Control が識別するオブジェクトを選択し、[関係（Relationships）] ペインを調べます。そのオブジェクトに関連するすべてのデバイスとポリシーが表示されます。

オブジェクトの無視の解除

未使用、重複、不整合のオブジェクトを解決する方法の 1 つは、それらを無視することです。オブジェクトが未使用、重複、または不整合であっても、その状態には正当な理由があると判断し、オブジェクトの問題を未解決のままにすることを選択する場合もあります。将来のある時点で、これらの無視されたオブジェクトを解決することが必要になる場合があります。オブジェクトの問題を検索するときに Security Cloud Control は無視されたオブジェクトを表示しないため、無視されたオブジェクトのオブジェクトリストをフィルタリングし、結果に基づいて操作する必要があります。

手順

ステップ 1 左側のペインで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 オブジェクトフィルタ。

ステップ 3 [オブジェクト（Object）] テーブルで、無視を解除するオブジェクトをすべて選択します。一度に 1 つのオブジェクトの無視を解除できます。

ステップ 4 詳細ペインで [無視の解除（Unignore）] をクリックします。

ステップ 5 要求を確認します。これで、オブジェクトを問題でフィルタリングすると、以前は無視されていたオブジェクトが見つかるはずです。

オブジェクトの削除

1 つのオブジェクトまたは複数のオブジェクトを削除できます。

1 つのオブジェクトの削除

⚠

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応するクラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっているオンプレミス Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがあるオンプレミス Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、削除するオブジェクトを見つけ、それを選択します。

ステップ 3 [関係（Relationships）] ペインを確認します。オブジェクトがポリシーまたはオブジェクトグループで使用されている場合は、そのポリシーまたはグループから削除するまでオブジェクトを削除できません。

ステップ 4 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 5 [OK] をクリックしてオブジェクトの削除を確認します。

ステップ 6 行った変更をレビューして展開するか、待機してから複数の変更を一度に展開します。

未使用オブジェクトのグループの削除

デバイスをオンボードしてオブジェクトの問題解決に取り組むと、多くの未使用のオブジェクトが見つかります。一度に最大 50 個の未使用オブジェクトを削除できます。

手順

ステップ 1 [問題（Issues）] フィルタを使用して、**未使用のオブジェクト**を見つけます。デバイスフィルタを使用する際に [デバイスなし（No Device）] を選択し、デバイスに関連付けられていないオブジェクトを検索することもできます。オブジェクトリストをフィルタリングすると、オブジェクトのチェックボックスが表示されます。

ステップ 2 オブジェクト テーブル ヘッダーの [すべて選択（Select all）] チェックボックスをオンにして、フィルタによって検出されオブジェクトテーブルに表示されるすべてのオブジェクトを選択するか、削除する個々のオブジェクトの個々のチェックボックスをオンにします。

ステップ 3 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 4 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

ネットワーク オブジェクト

1 つのネットワークオブジェクトには、ホスト名、ネットワーク IP アドレス、IP アドレスの範囲、完全修飾ドメイン名（FQDN）または CIDR 表記のサブネットワークのいずれか 1 つを入れることができます。[ネットワークグループ（Network groups）] は、ネットワークオブジェクトと、グループに追加するその他の個々のアドレスまたはサブネットワークのコレクションです。ネットワークオブジェクトとネットワークグループは、アクセスルール、ネットワークポリシー、および NAT ルールで使用されます。Security Cloud Control を使用して、ネットワークオブジェクトとネットワークグループを作成、更新、および削除できます。

すべてのプラットフォームが Cisco Meraki や Multicloud Defense などのネットワークオブジェクトをサポートしているわけではないことに注意してください。ダイナミックオブジェクトを共有すると、Security Cloud Control は、発信元のプラットフォームまたはデバイスからの適切な情報を、Security Cloud Control が使用できる一連の使用可能な情報に自動的に変換します。

製品間でのネットワークオブジェクトの再利用

クラウド提供型 Firewall Management Center とテナントにオンボーディングされている 1 つ以上の オンプレミス Management Center を含む Security Cloud Control テナントがある場合は、次の手順を実行します。

- Cisco Secure Firewall Threat Defense、FDM による管理脅威に対する防御、Cisco ASA、または Cisco Meraki ネットワークオブジェクトまたはグループを作成すると、そのオブジェクトのコピーが、クラウド提供型 Firewall Management Center の設定時に使用する [オブジェクト（Objects）] ページのオブジェクトリストにも追加されます。その逆も同様です。
- Cisco Secure Firewall Threat Defense、FDM による管理脅威に対する防御、または ASA ネットワークオブジェクトまたはグループを作成すると、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている各オンプレミス Firewall Management Center の [保留中の変更があるデバイス（Devices with Pending Changes）] ページにエントリが作成されます。このリストから、オブジェクトを選択して、そのオブジェクトを使用するオンプレミス Management Center に展開し、不要なオブジェクトを破棄できます。、**[管理（Administration）] > [Firewall Management Center]** に移動し オンプレミス Management Center を選択します。[オブジェクト（Objects）] をクリックし、オンプレミス Firewall Management Center ユーザーインターフェイスでオブジェクトを確認して、ポリシーに割り当てます。

いずれかのページのネットワークオブジェクトやグループに加えた変更は、両方のページのオブジェクトまたはグループインスタンスに適用されます。1 つのページからオブジェクトを削除すると、そのオブジェクトの対応するコピーも他のページから削除されます。

例外：

- 同じ名前のネットワークオブジェクトがすでにクラウド提供型 Firewall Management Center に存在する場合、新しい Cisco Secure Firewall Threat Defense、FDM による管理 脅威に対する防御、Cisco ASA、または Cisco Meraki ネットワークオブジェクトは、Security Cloud Control の [オブジェクト（Objects）] ページには複製されません。
- オンプレミスの Cisco Secure Firewall Management Center によって管理されるオンボード済み脅威に対する防御デバイスのネットワークオブジェクトおよびグループは複製されず、クラウド提供型 Firewall Management Center で使用できません。

  クラウド提供型 Firewall Management Center に移行したオンプレミスの Cisco Secure Firewall Management Center インスタンスの場合、ネットワークオブジェクトとグループは、FTD デバイスに展開されたポリシーで使用されていれば、Security Cloud Control オブジェクトページに複製されることに注意してください。
- Security Cloud Control と クラウド提供型 Firewall Management Center の間のネットワークオブジェクトの共有は、新しいテナントでは自動的に有効になりますが、既存のテナントでは要求する必要があります。ネットワークオブジェクトが クラウド提供型 Firewall Management Center と共有されていない場合は、TAC に連絡して、テナントで機能を有効にしてもらいます。
- Security Cloud Control とオンプレミス Management Center の間のネットワークオブジェクトの共有は、Security Cloud Control に対して導入準備された新しいオンプレミス Management Center の Security Cloud Control では自動的に有効になりません。ネットワークオブジェクトがオンプレミス Management Center と共有されていない場合は、[設定（Settings）] でオンプレミス Management Center の [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンが有効になっていることを確認するか、TAC に連絡してテナントで機能を有効にしてもらいます。

ネットワークオブジェクトの表示

Security Cloud Control を使用して作成するネットワークオブジェクトと、オンボーディングしたデバイスの設定から Security Cloud Control が認識するネットワークオブジェクトは、[オブジェクト（Objects）] ページに表示されます。これらのネットワークオブジェクトには、それぞれのオブジェクトタイプのラベルが付けられています。これにより、オブジェクトタイプでフィルタリングして、探しているオブジェクトをすばやく見つけることができます。

[オブジェクト（Objects）]ページでネットワークオブジェクトを選択すると、オブジェクトの値が [詳細（Detail）] ペインに表示されます。[関係（Relationships）] ペインには、オブジェクトがポリシーで使用されているかどうか、およびオブジェクトが保存されているデバイスが表示されます。

ネットワークグループをクリックすると、そのグループの内容が表示されます。ネットワークグループは、ネットワークオブジェクトによってグループに与えられたすべての値の集合体です。

サービス オブジェクト

プロトコルオブジェクト

プロトコルオブジェクトは、使用頻度の低いプロトコルやレガシープロトコルを含むサービスオブジェクトの一種です。プロトコルオブジェクトは、名前とプロトコル番号によって識別されます。Security Cloud Control は、ASA および Firepower（FDM による管理 デバイス）設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「プロトコル」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

ICMP オブジェクト

Internet Control Message Protocol（ICMP）オブジェクトは、ICMP および IPv6-ICMP メッセージ専用のサービスオブジェクトです。Security Cloud Control は、ASA および Firepower がオンボードされたときにデバイスの設定でこれらのオブジェクトを認識し、これらに Security Cloud Control が独自のフィルタ「ICMP」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

Security Cloud Control を使用して、ASA 設定から ICMP オブジェクトの名前を変更したり、ICMP オブジェクトを削除したりできます。Security Cloud Control を使用して、Firepower 設定の ICMP および ICMPv6 オブジェクトを作成、更新、および削除できます。

（注） ICMPv6 プロトコルの場合、AWS は特定の引数の選択をサポートしていません。すべての ICMPv6 メッセージを許可するルールのみがサポートされます。

関連情報：

- オブジェクトの削除 （123 ページ）

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。