Cisco Security Cloud Control を使用した SSH デバイスの管理

最終更新：2025 年 4 月 15 日

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

Cisco Security Cloud Control を使用した SSH デバイスの管理

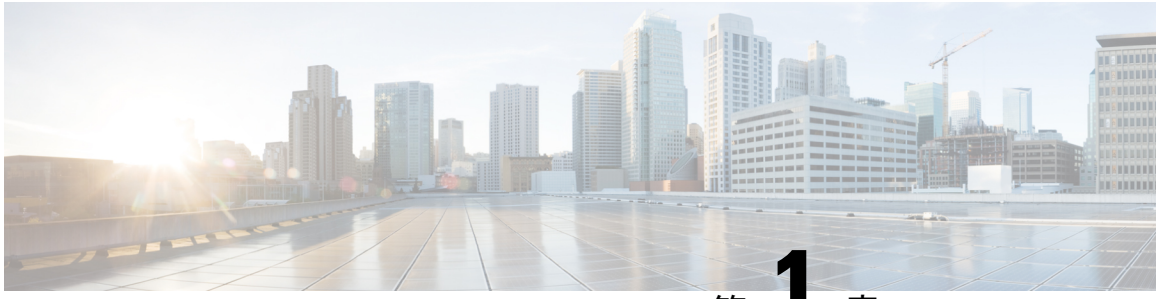
Cisco Security Cloud Control を使用した SSH デバイスの管理

Cisco Security Cloud Control（旧称 Cisco Defense Orchestrator）を使用すると、SSH を介してデバイスを管理できます。これらのデバイスでサポートされている機能は次のとおりです。

- SSH デバイスのオンボーディング。SSH デバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。
- Security Cloud Control デバイスとサービスの管理デバイス コンフィギュレーション ファイルを表示できます。
- デバイスからのポリシーと設定の変更を確認します。Cisco IOS または SSH から Security Cloud Control への変更の読み取り （151 ページ）SSH デバイスからコンフィギュレーション ファイルが読み取られると、Security Cloud Control のデータベースに保存されます。
- デバイスのアウトオブバンド変更。デバイスで [競合検出（Conflict Detection）] を有効にすると、Security Cloud Control は 10 分ごとにデバイスの設定の変更をチェックします。変更がある場合、デバイスのステータスは [競合検出（Conflict Detected）] に変わり、競合を解決可能になります。
- Security Cloud Control コマンドライン インターフェイス。Security Cloud Control のコマンド ライン インターフェイスを介して、すべての SSH デバイスコマンドをデバイスに発行できます。
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能な「コマンド ライン インターフェイス マクロ」に変換可能。Security Cloud Control が提供するシステム定義マクロを使用して、頻繁に実行するタスク用に独自のマクロを作成できます。

Cisco Security Cloud Control を使用した SSH デバイスの管理

- 新規フィンガープリント検出ステータスの解決。デバイスのログイン情報またはプロパティが変更され、それによってSSHフィンガープリントが変更された場合、Security Cloud Control はその変更を検出し、新しいフィンガープリントを確認して許可する機会を提供します。
- Security Cloud Control での変更ログの管理。変更ログには、SSH デバイスに発行するすべてのコマンドがキャプチャされます。



第 1 章

Security Cloud Control の基本

Security Cloud Control は、明確で簡潔なインターフェイスを通じてポリシーを管理するための独自のビューを提供します。Security Cloud Control を初めて使用する場合の基本的な事柄について以下で取り上げます。

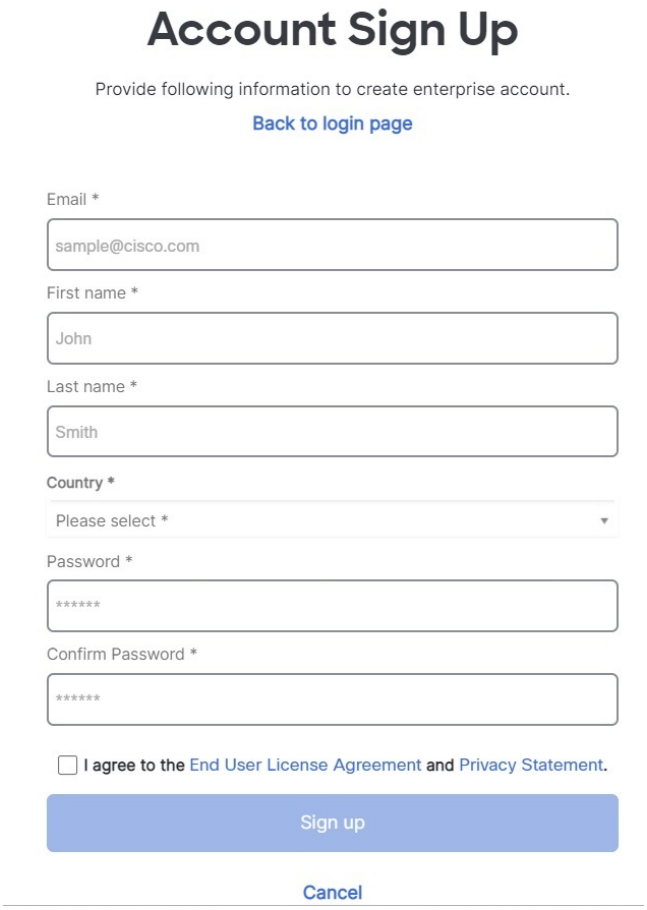
• オブジェクト （114 ページ）

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
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 （6 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 （70 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 （14 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、シスコでは、SDC CLI がプリインストールされている強化された Ubuntu 22 インスタンス用の OVA を提供しています。CLI は、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 をホストで Docker コンテナとしてブートストラップするのに役立ちます。また、独自の Ubuntu インスタンス（バージョン 20 ー 24 が現在テスト済み）をロールし、CLI を個別にダウンロードできます。

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。

- SSH アクセスのあるデバイス。

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。

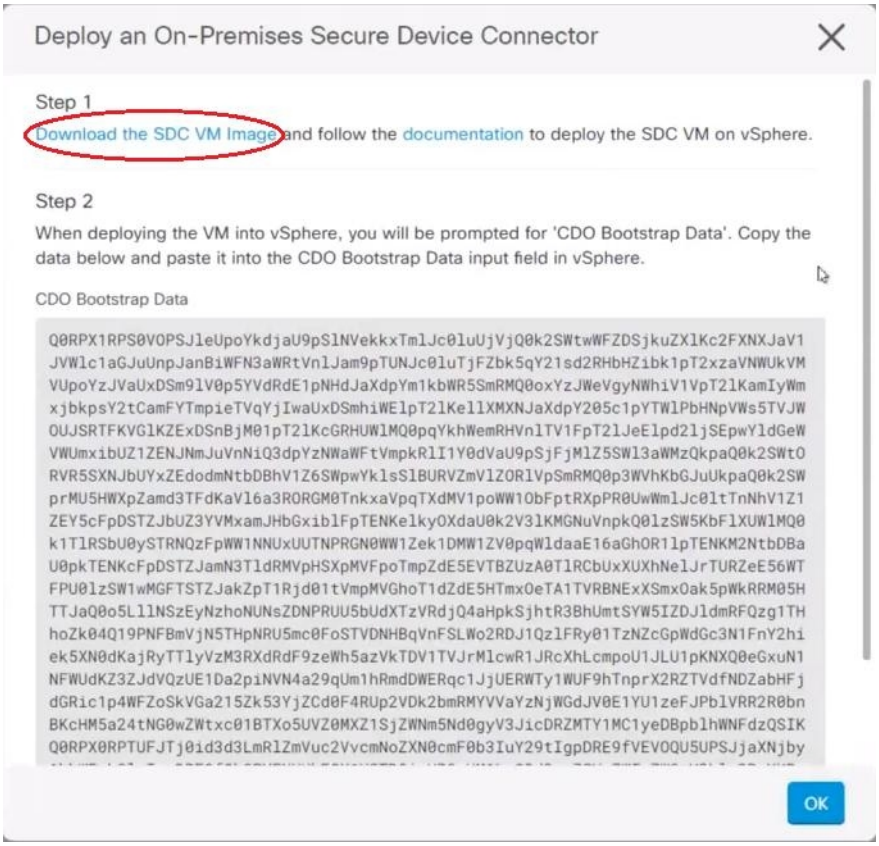
手順

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。

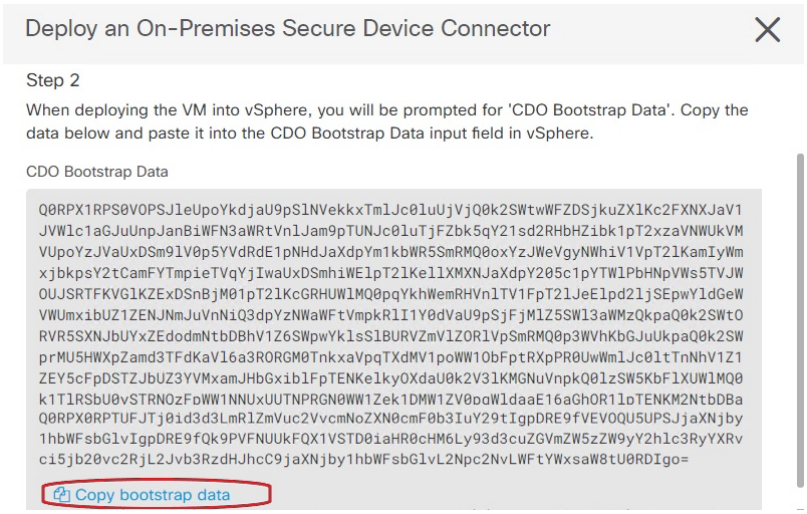
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

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AWSVPC上でのSecureDeviceConnector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 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.

====

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,

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。

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。

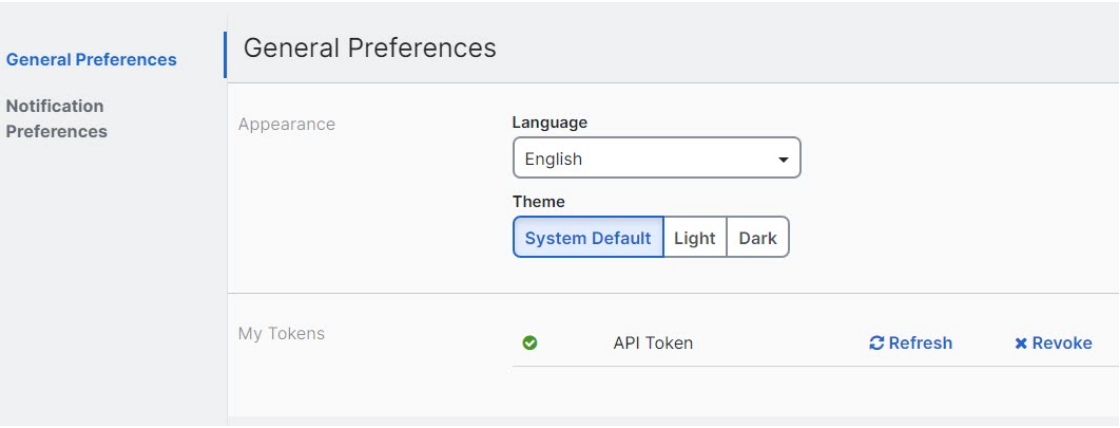
全般設定

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 （66 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Security Cloud Control での変更ログの管理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 のお客様が TAC でサポートチケットを開く方法を開き、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。

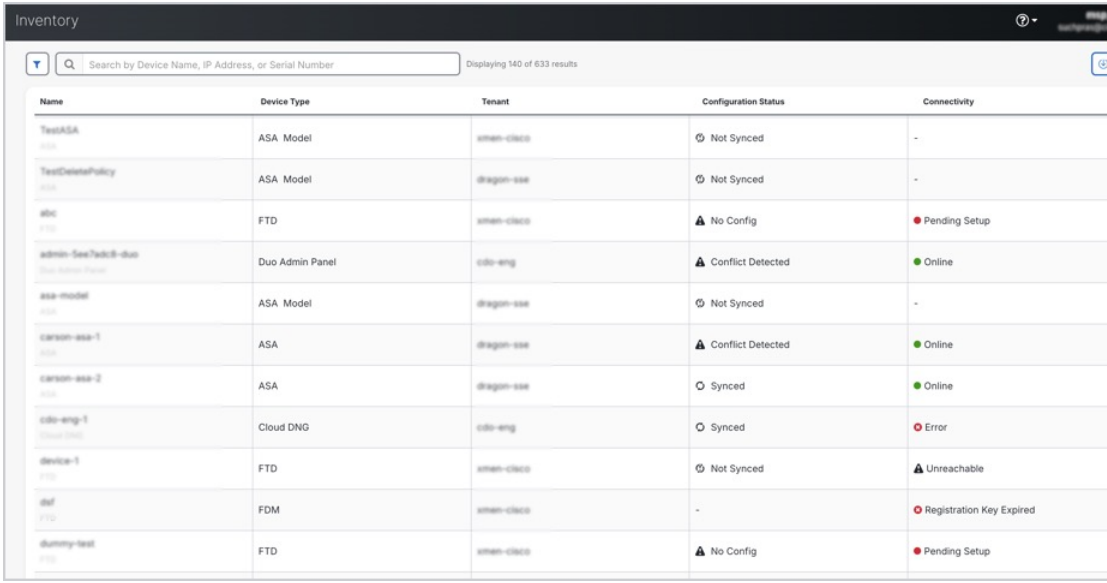
マルチテナントポータル

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。

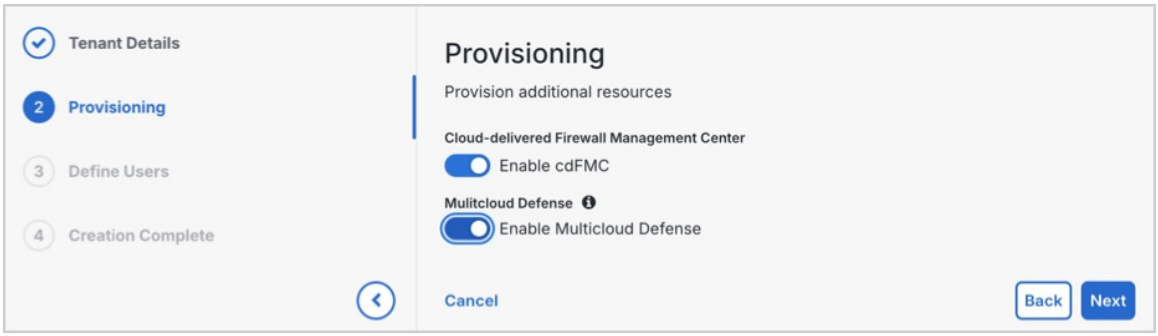
（注）

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

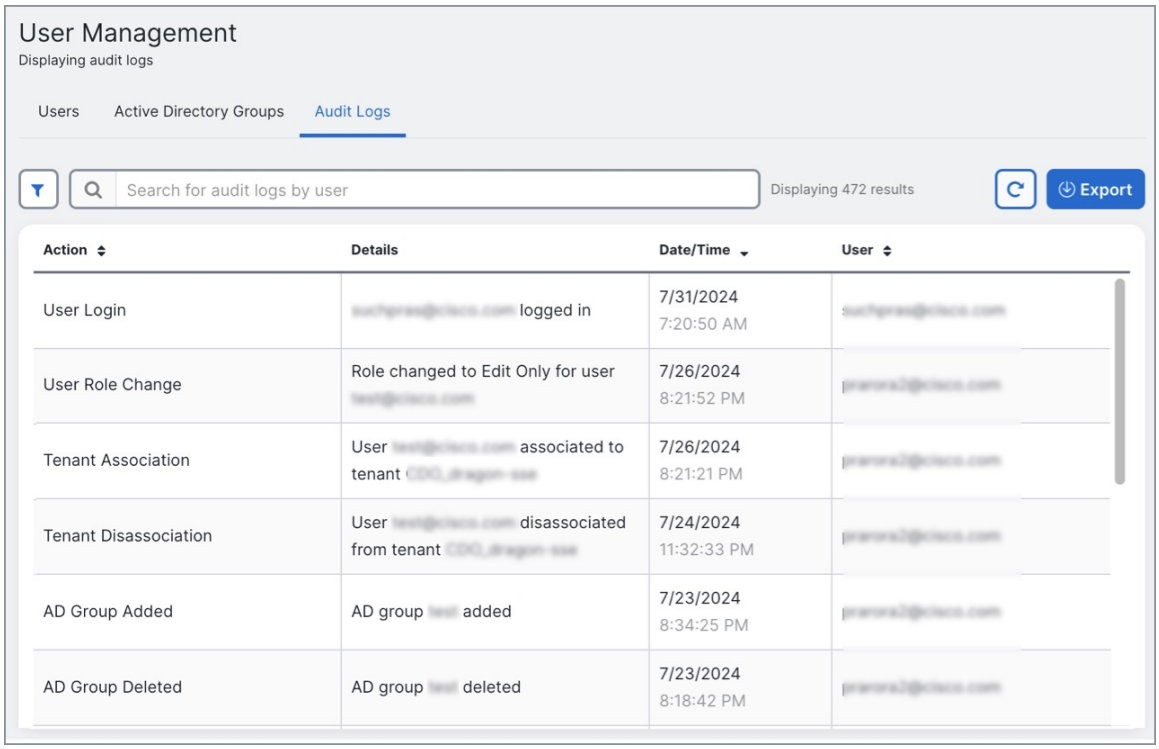
Security Cloud Control の [監査ログ（Audit Logs）] には、ユーザー関連およびシステムレベルのアクションが記録されます。[監査ログ（Audit Logs）] によってキャプチャされる主なイベントは次のとおりです。

- **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

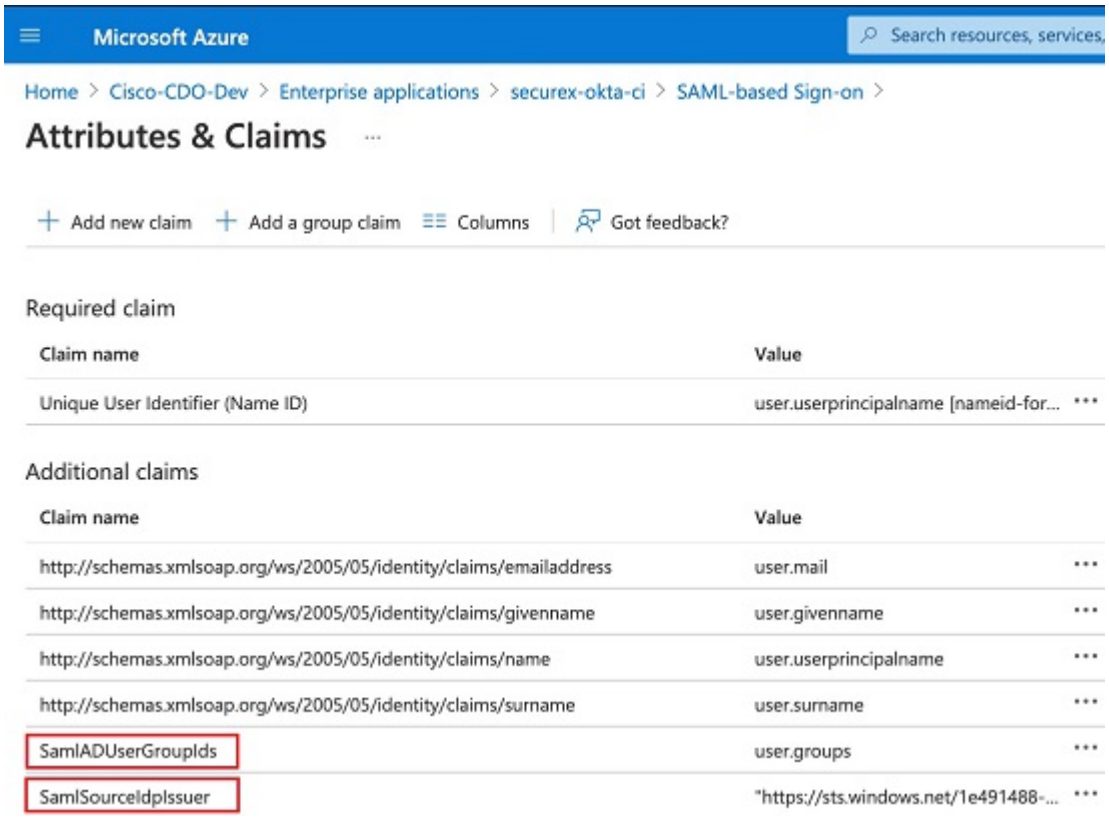
ユーザー管理の一種として Active Directory グループマッピングを Security Cloud Control に追加するには、まず Security Cloud Sign On に統合済みの Active Directory が必要です。Active Directory ID プロバイダー（IdP）がまだ統合されていない場合は、「Identity provider integration guide」[英語] を参照して、カスタム Active Directory IdP 統合に次の情報を統合します。

- 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。

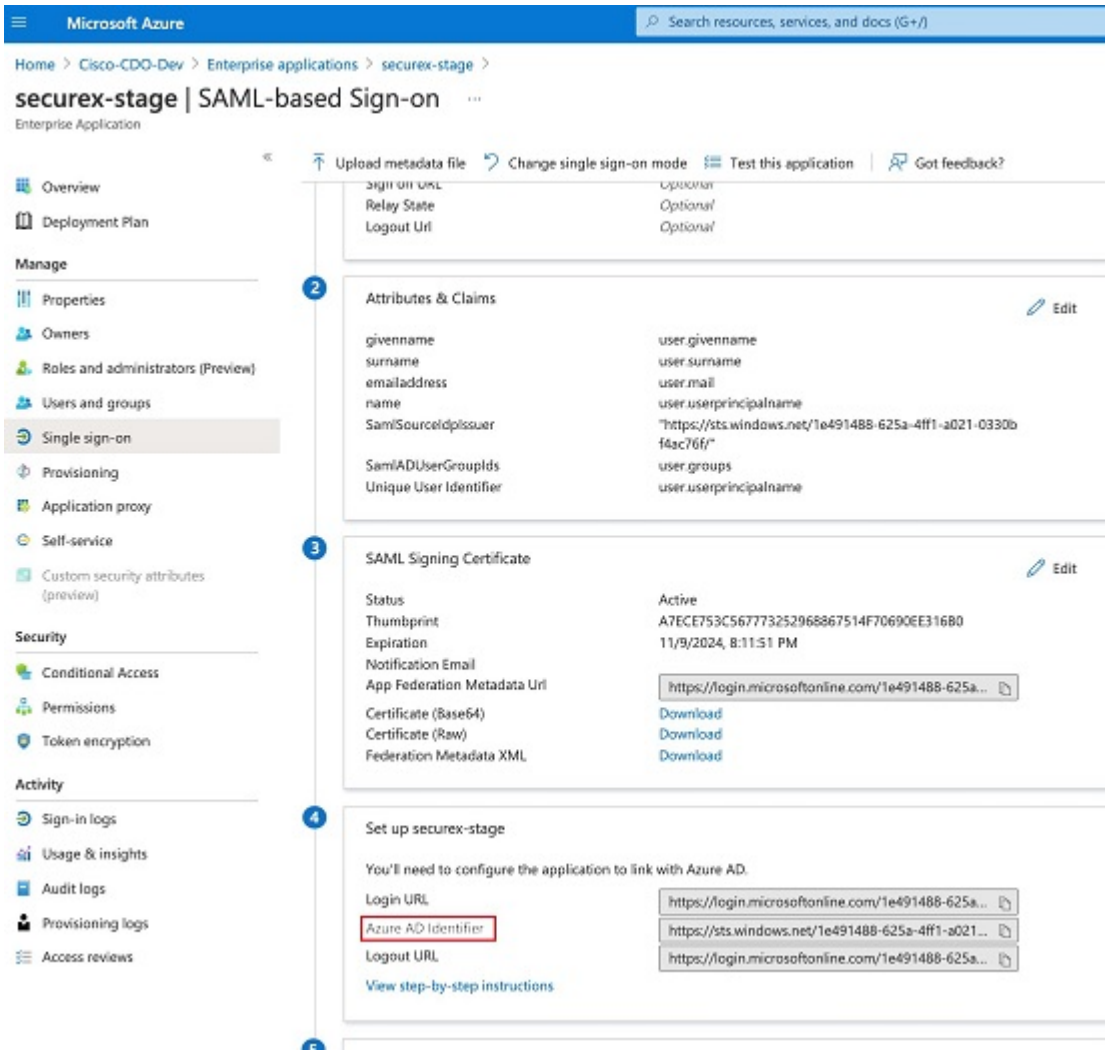
- **SamlADUserGroupIds**：この属性は、ユーザーが Active Directory 上で持つすべてのグループの関連付けを記述します。たとえば、次のスクリーンショットに示すように、Azure で [+グループ要求の追加（+ Add groups claim）] を選択します。

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。

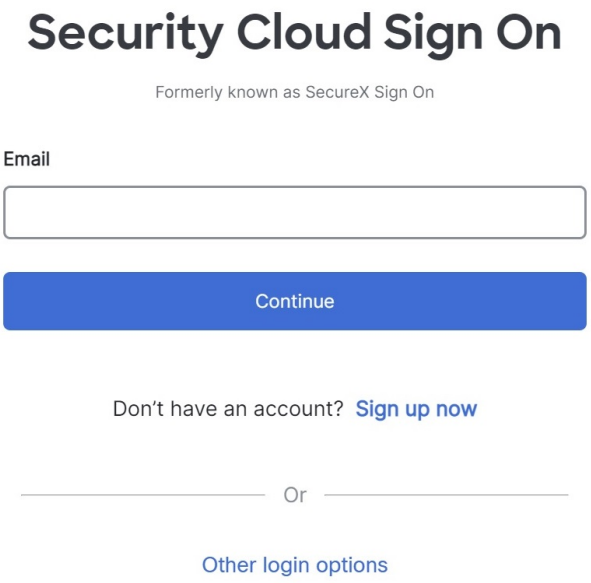
新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定

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。

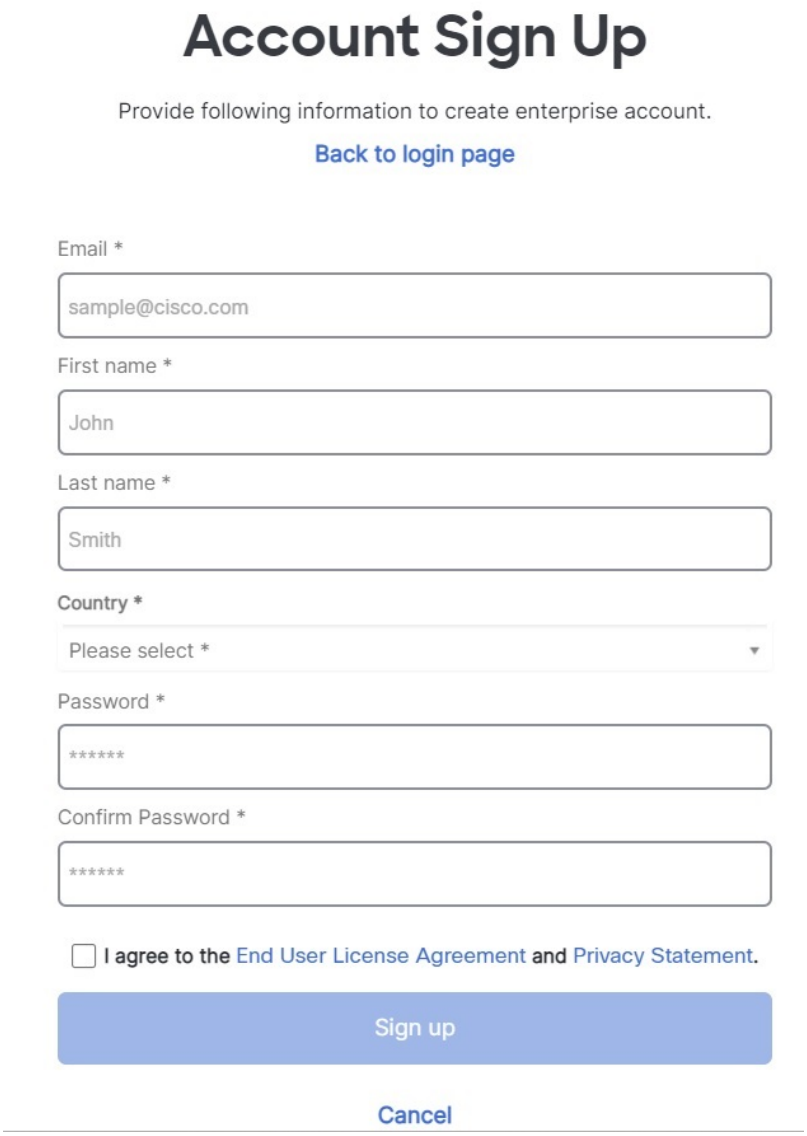
手順

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 のお客様が TAC でサポートチケットを開く方法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。

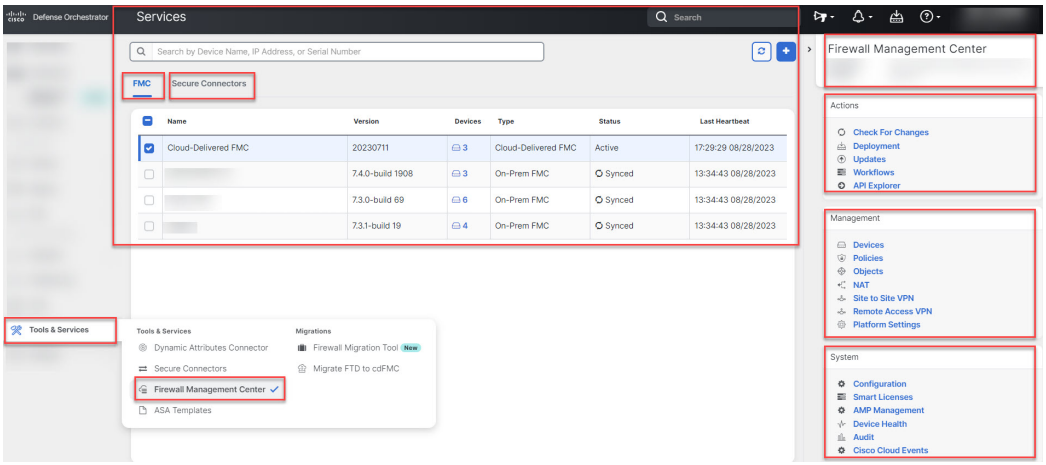
Security Cloud Control の [サービス（Services）] ページ

[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 （111 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。

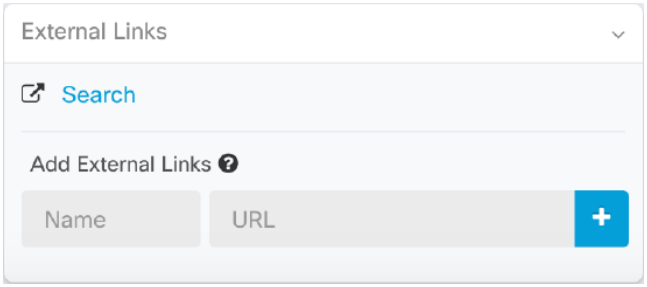
ステップ 4 必要なデバイスを選択して、強調表示します。

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 （110 ページ）
- デバイスとサービスのリストのエクスポート （104 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 （177 ページ） 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。

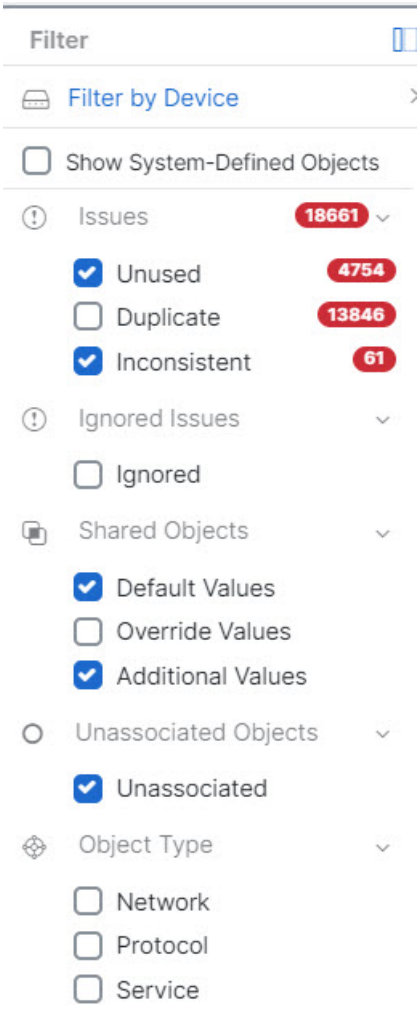
セキュリティ デバイス フィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルでフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

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（158ページ）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（193 ページ）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

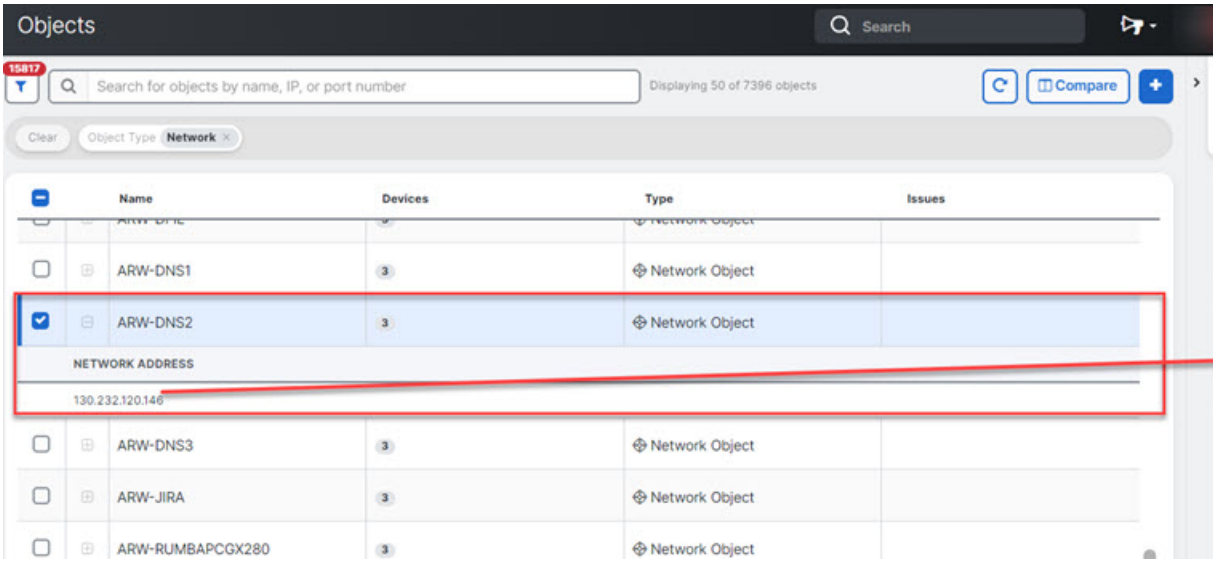
オブジェクト タイプ	説明
ネットワーク（Network）	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
URL	URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

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

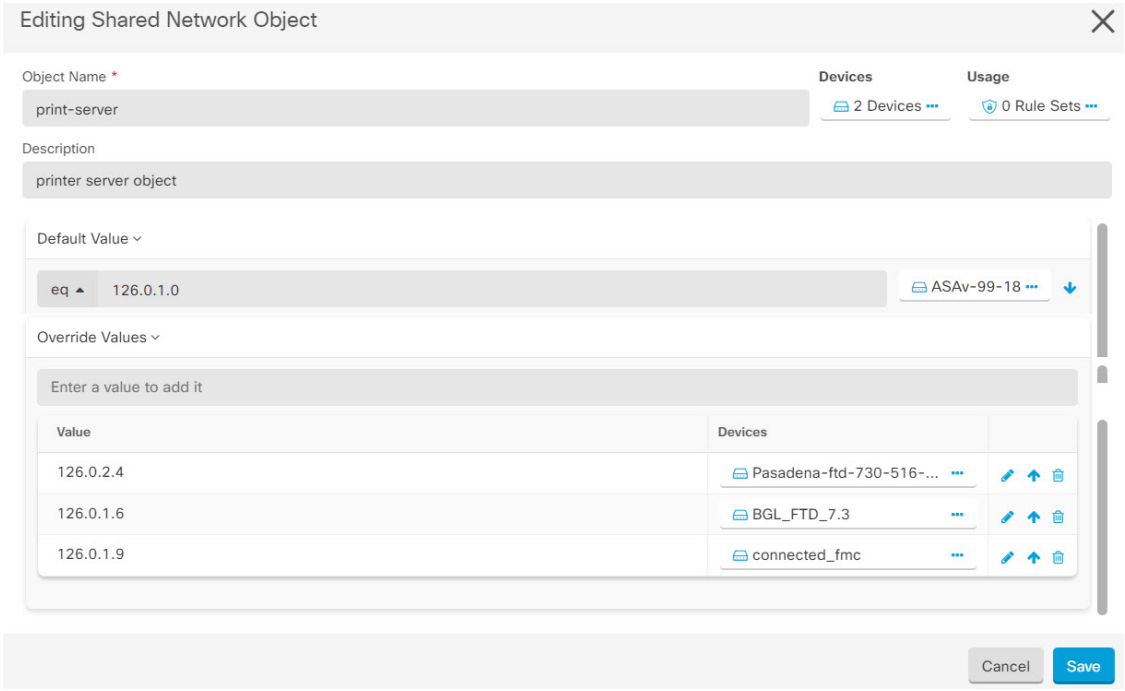
オブジェクトのオーバーライドを使用すると、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。Security Cloud Control は、オーバーライドの設定時に指定したデバイスに対応する値を使用します。これらのオブジェクトは、名前は同じで値が異なる複数のデバイス上にありますが、Security Cloud Control は、これらの値がオーバーライドとして追加されただけでは、それらを**不整合オブジェクト**として識別しません。

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（158ページ）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（200ページ）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。

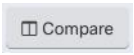
左側のペインで、[オブジェクト（Objects）] > [ ] の順にクリックし、[関連付けなし（Unassociated）] チェックボックスをオンにします。

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）] 

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。

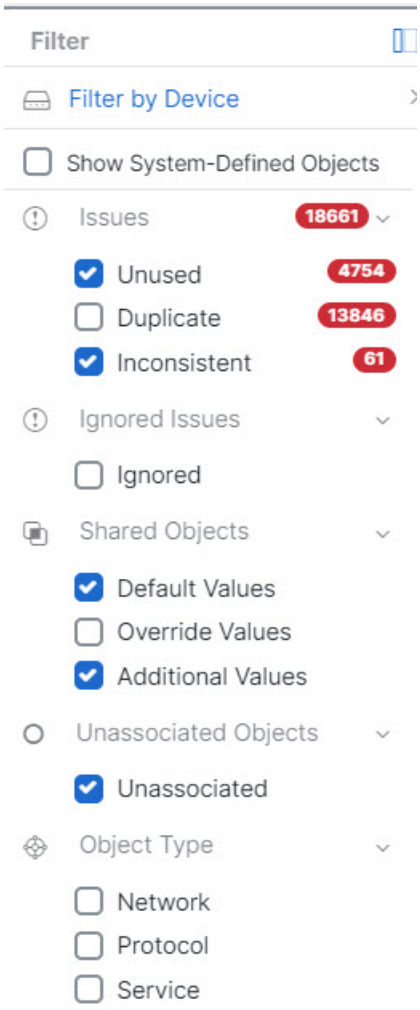
オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IP アドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

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オブジェクトの問題の解決、重複オブジェクトの問題の解決、または不整合オブジェクトの問題を解決するであっても、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 行った変更をすべてのデバイスの設定変更のプレビューと展開か、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すべてのデバイスの設定変更のプレビューと展開か、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、Security Cloud Control のお客様が TAC でサポートチケットを開く方法して、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、Security Cloud Control のお客様が TAC でサポートチケットを開く方法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

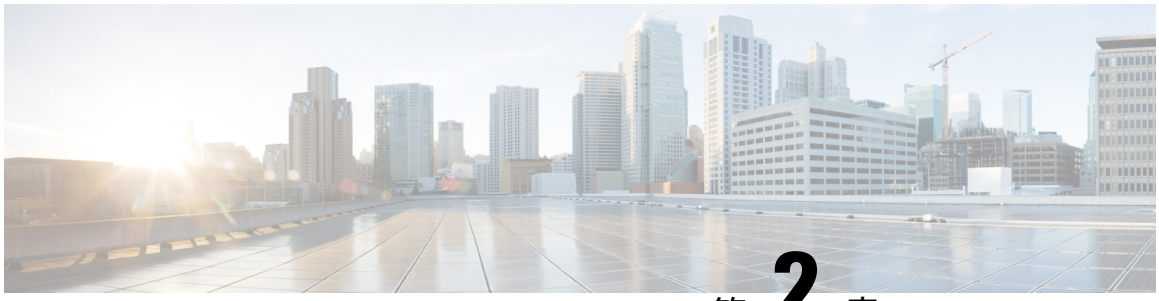
Internet Control Message Protocol（ICMP）オブジェクトは、ICMP および IPv6-ICMP メッセージ専用のサービスオブジェクトです。Security Cloud Control は、ASA および Firepower がオンボードされたときにデバイスの設定でこれらのオブジェクトを認識し、これらに Security Cloud Control が独自のフィルタ「ICMP」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

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）



第 2 章

デバイスとサービスのオンボーディング

ライブデバイスとモデルデバイスの両方を Security Cloud Control に導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、Security Cloud Control を使用して表示および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が Security Cloud Control をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、Secure Device Connector （12 ページ） を参照してください。

この章は、次のセクションで構成されています。

SSH デバイスのオンボーディング

SSHデバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。

SSH デバイスのオンボーディング

始める前に

実行する前に、次の前提条件を満たしていることを確認してください。

- SSH デバイスがサポートする暗号が Security Cloud Control でサポートされていることを確認してください。現時点では、Security Cloud Control は、SSH デバイスのオンボーディング用に限定された暗号セットをサポートしています。サポートされている暗号は次のとおりです：`aes128-ctr`、`aes192-ctr`、`aes256-ctr`、`aes128-gcm`、`aes128-gcm@openssh.com`、`aes256-gcm`、`aes256-gcm@openssh.com`。サーバーがサポートする暗号を確認するには、SDC にログインし、コマンド `ssh -vv <ip_address>` を実行します。
- Cisco IOS デバイスをオンボーディングするには、ネットワーク内にオンプレミス Secure Device Connector（SDC）が必要です。SDC の説明と展開シナリオへのリンクについては、Secure Device Connector （12 ページ）を参照してください。

- デバイスをオンボーディングする前に、「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。

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 青色のプラスボタン  をクリックして、デバイスをオンボーディングします。

ステップ 3 [統合（Integrations）] タイルをクリックします。グレー表示されている場合は、ネットワークに展開されていて、Security Cloud Control テナントで使用されているアクティブな Secure Device Connector がないことを意味します。

ステップ 4 Secure Device Connector （12 ページ） ボタンをクリックして、このデバイスが通信するネットワーク内の SDC を選択します。デフォルトの SDC が表示されますが、SDC 名をクリックすることで SDC を変更できます。

ステップ 5 デバイスに名前を付けます。

ステップ 6 [統合（Integrations）] ドロップダウンメニューで、[汎用SSH（Generic SSH）] を選択します。

ステップ 7 デバイスの場所として FDQN または IPv4 アドレスを入力します。デフォルト SSH ポートは 22 です。

ステップ 8 [実行（Go）] をクリックします。Security Cloud Control はデバイスを特定し、設定を統合する準備をします。

ステップ 9 SSH フィンガープリントを [ダウンロード（Download）] し、ローカルに保存します。これまでに SSH 経由でこのデバイスに接続したことがない場合は、このフィンガープリントを使用してデバイスを確認できます。

ステップ 10 オンボーディングするデバイスの [ユーザー名（Username）] と [パスワード（Password）] にログイン情報を入力します。Security Cloud Control は、正しいログイン情報がないと既存の設定を正常に読み取ることができません。

ステップ 11 （オプション）このデバイスに以前に [イネーブルパスワード（Enable Password）] を設定した場合は、それを入力します。

ステップ 12 （オプション）ドロップダウンメニューから [設定コマンド（Configuration Command）] を選択するか、テキストボックスにカスタムコマンドを入力します。このコマンドは、デバイスの設定として使用されます。OOB が有効になっている場合、Security Cloud Control は変更をチェックします。[設定（Configuration）] ページで現在の値を表示できます。デバイスが Security Cloud Control に正常にオンボーディングされた後に、このコマンドの変更が可能になることに注意してください。

ステップ 13 [接続（Connect）] をクリックします。

（注）
ログイン情報が正しくない場合は、接続の詳細を確認するように求められます。ここでログイン情報を再入力できます。ログイン情報を修正せずに確認を終了すると、デバイスの [インベントリ] ページに統合インスタンスが表示されますが、デバイスは導入準備または同期されていません。

ステップ 14 （オプション）このデバイスにラベルを追加します。

ステップ 15 [続行（Continue）] をクリックします。

ステップ 16 デバイスは Security Cloud Control にオンボーディングされます。[終了（Finish）] をクリックします。

ステップ 17 [インベントリ]ページに戻ります。デバイスが正常にオンボーディングされると、設定ステータスが [同期（Synced）]、接続状態が [オンライン（Online）] と表示されます。

（注）
デバイスがオンボーディングされると、実行する設定コマンドの変更が可能になります。カスタムコマンドを使用するか、CLI マクロを作成できます。

ステップ 18 （オプション）必要に応じて、デバイスの [ノート（Notes）] ページにデバイスに関するノートを入力できます。詳細については、「デバイスノートを書く」を参照してください。

関連情報：

- コマンド ライン インターフェイス マクロ
-
- Cisco IOS または SSH から Security Cloud Control への変更の読み取り （151 ページ）
- デバイス設定変更について

Security Cloud Control からデバイスを削除

Security Cloud Control からデバイスを削除するには、次の手順を使用します。

手順

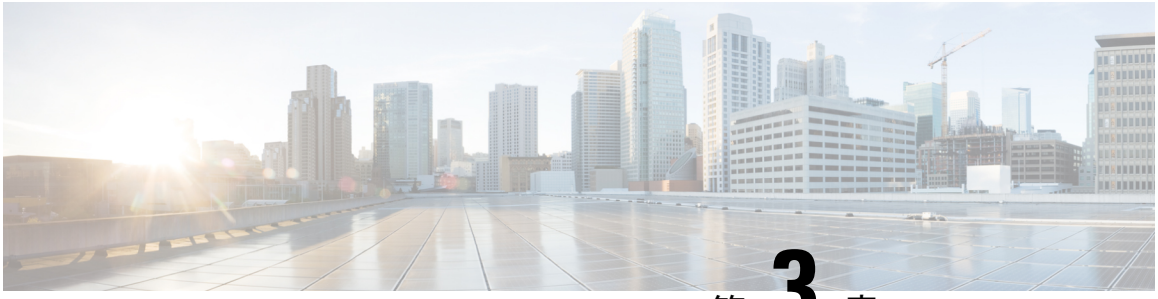
ステップ 1 Security Cloud Control にログインします。

ステップ 2 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション（Device Actions）] パネルで、[削除（Remove）] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル（Cancel）] を選択して、デバイスをオンボードしたままにします。



第 3 章

Cisco Security Cloud Control による SSH デバイスの管理

Cisco Security Cloud Control（Security Cloud Control）を使用すると、SSH を介してデバイスを管理できます。これらのデバイスでサポートされている機能は次のとおりです。

- SSH デバイスのオンボーディング。SSH デバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。
- デバイス設定の表示。デバイス コンフィギュレーション ファイルを表示できます。
- デバイスからのポリシーと設定の変更を確認します。SSH デバイスからコンフィギュレーション ファイルが読み取られると、Security Cloud Control のデータベースに保存されます。
- アウトオブバンド変更検出。デバイスで [競合検出（Conflict Detection）] を有効にすると、Security Cloud Control は 10 分ごとにデバイスの設定の変更をチェックします。変更がある場合、デバイスのステータスは [競合検出（Conflict Detected）] に変わり、競合を解決可能になります。
- コマンド ライン インターフェイスのサポート。Security Cloud Control のコマンド ライン インターフェイスを介して、すべての SSH デバイス コマンドをデバイスに発行できます。
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能な「マクロ」に変換できます。Security Cloud Control が提供するシステム定義マクロを使用して、頻繁に実行するタスク用に独自のマクロを作成できます。
- SSH フィンガープリントの変更を検出および管理します。デバイスのログイン情報またはプロパティが変更され、それによって SSH フィンガープリントが変更された場合、Security Cloud Control はその変更を検出し、新しいフィンガープリントを確認して許可する機会を提供します。
- 変更ログ。変更ログには、SSH デバイスに発行するすべてのコマンドがキャプチャされます。

- Security Cloud Control コマンドライン インターフェイス （134 ページ）

Security Cloud Control コマンドライン インターフェイス

Security Cloud Control は、、SSH 管理デバイスを管理するためのコマンドライン インターフェイス（CLI）をユーザーに提供します。コマンドは、単一のデバイスに送信することも、複数のデバイスに同時に送信することも可能です。

コマンドライン インターフェイスの使用

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] タブをクリックします。

ステップ 3 コマンドラインインターフェイス（CLI）を使用して管理するデバイスを見つけるには、デバイスタブとフィルタボタンを使用します。

ステップ 4 デバイスを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] タブをクリックします。

ステップ 7 コマンドペインにコマンドを入力して、[送信（Send）] をクリックします。コマンドに対するデバイスの応答は、「応答ペイン」の下に表示されます。

（注）

実行できるコマンドに制限がある場合、それらの制限はコマンドペインの上に一覧表示されます。

関連トピック

コマンドラインインターフェイスでのコマンドの入力 （135 ページ）

コマンドラインインターフェイスでのコマンドの入力

1 つのコマンドを 1 行に入力することも、複数のコマンドを複数の行に連続して入力することもでいます。Security Cloud Control では、入力順にコマンドが実行されます。次の ASA の例では、3つのネットワークオブジェクトと、それらのネットワークオブジェクトを含むネットワーク オブジェクト グループを作成するコマンドのバッチを送信します。

コマンド履歴での動作

CLI コマンドを送信すると、Security Cloud Control はそのコマンドを [コマンドラインインターフェイス（Command Line Interface）] ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。

手順

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

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 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 履歴ペインがまだ展開されていない場合は、時計アイコン をクリックして展開します。

ステップ 6 [履歴（History）] ペインで変更または再送信するコマンドを選択します。

ステップ 7 コマンドをそのまま再利用するか、コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。Security Cloud Control は、応答ペインにコマンドの結果を表示します。

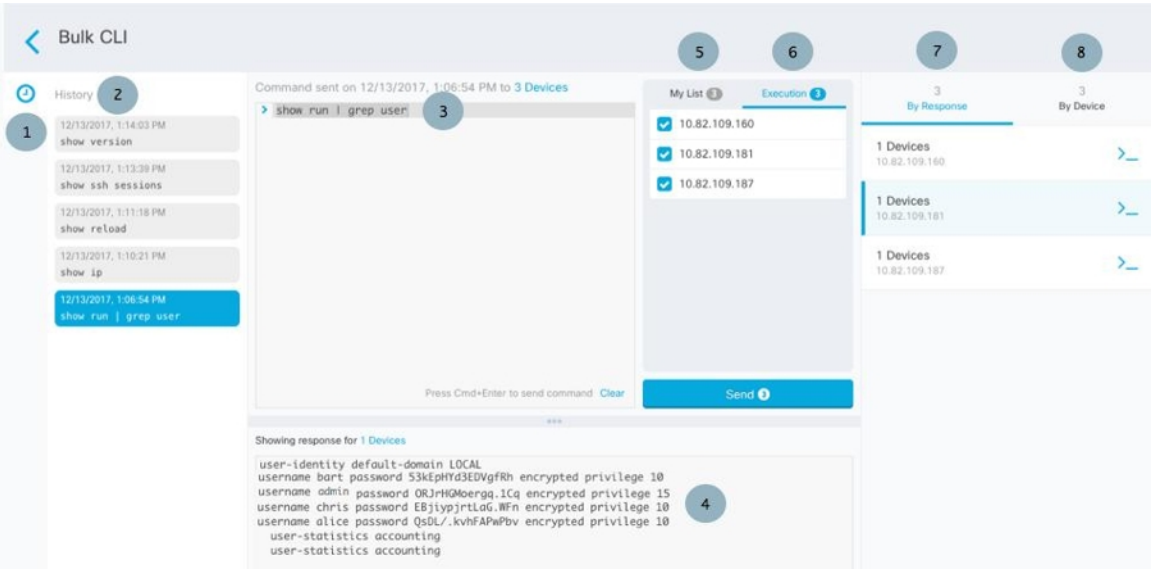
（注）
次の 2 つの状況で「完了しました（Done!）」というメッセージが Security Cloud Control の応答ペインに表示されます。

- コマンドが正常に実行された後。
- コマンドの返すべき結果が何もなかった場合。たとえば、設定エントリを検索する正規表現を含む show コマンドを発行したとします。正規表現の条件に一致する設定エントリがなかった場合、Security Cloud Control は「完了しました（Done!）」を返します。

一括コマンド ライン インターフェイス

Security Cloud Control では、コマンドラインインターフェイス（CLI）を使用してSecure Firewall ASA、FDM による管理、脅威防御、SSH、および Cisco IOS デバイスを管理できます。コマンドは、単一のデバイスに送信することも、同じ種類の複数のデバイスに同時に送信することも可能です。このセクションでは、CLI コマンドを複数のデバイスに一度に送信する方法について説明します。

一括 CLI インターフェイス



（注） 次の 2 つの状況で「完了しました（Done!）」というメッセージが Security Cloud Control に表示されます。

- コマンドがエラーなしで正常に実行された後。
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。正規表現の条件に一致する設定エントリがなかった場合、Security Cloud Control は「完了しました（Done!）」を返します。

ケース	説明
1	コマンド履歴ペインを展開したり折りたたんだりするには、時計アイコンをクリックします。
2	コマンド履歴。コマンドを送信すると、Security Cloud Control はこの履歴ペインにコマンドを記録するため、コマンドをもう一度選択して再度実行できます。
3	コマンドペイン。このペインのプロンプトにコマンドを入力します。
4	応答ペイン。Security Cloud Control は、コマンドに対するデバイスの応答と Security Cloud Control メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「Xデバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが Security Cloud Control に表示されます。 （注） 次の 2 つの状況で「完了しました（Done!）」というメッセージが Security Cloud Control に表示されます。 • コマンドがエラーなしで正常に実行された後。 • コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。正規表現の条件に一致する設定エントリがなかった場合、Security Cloud Control は「完了しました（Done!）」を返します。
5	[マイリスト（My List）] タブには、[**セキュリティデバイス**] テーブルから選択したデバイスが表示されます。このタブで、コマンドの送信先デバイスを含めたり、除外したりできます。

ケース	説明
[6]	上の図で強調表示されている [実行（Execution）] タブには、履歴ペインで選択されているコマンドの対象デバイスが表示されます。この例では、履歴ペインで show run | grep user コマンドが選択され、[実行（Execution）] タブに、10.82.109.160、10.82.109.181、および 10.82.10.9.187 に送信されたことが表示されます。
7	[応答別（By Response）] タブをクリックすると、コマンドによって生成された応答のリストが表示されます。同一の応答は 1 行にグループ化されます。[応答別] タブで行を選択すると、Security Cloud Control はそのコマンドへの応答を応答ペインに表示します。
8	[デバイス別（By Device）] タブをクリックすると、各デバイスからの個別の応答が表示されます。リスト内のいずれかのデバイスをクリックすると、特定のデバイスからのコマンドへの応答を表示できます。

コマンドの一括送信

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 コマンド ライン インターフェイスを使用して設定するデバイスを見つけるには、適切なデバイスタブを選択し、フィルタボタンを使用します。

ステップ 4 デバイスを選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 6 [マイリスト（My List）] フィールドで、コマンドを送信するデバイスをオンまたはオフにすることができます。

ステップ 7 コマンドペインにコマンドを入力して、[送信（Send）] をクリックします。コマンド出力が応答ペインに表示されます。コマンドは変更ログに記録され、Security Cloud Control コマンドはコマンドを [一括CLI（Bulk CLI）] ウィンドウの [履歴（History）] ペインに記録します。

一括コマンド履歴での動作

一括 CLI コマンドを送信すると、Security Cloud Control がそのコマンドを [一括CLIページ（Bulk CLI page）] の履歴ページに記録します。一括 CLI インターフェイス（136 ページ）履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することも

できます。履歴ペインのコマンドは、それらが実行された元のデバイスに関連付けられています。

手順

ステップ 1 ナビゲーションウィンドウで、**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、フィルタアイコンをクリックして、設定するデバイスを見つけます。

ステップ 4 デバイスを選択します。

ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 [履歴（History）] ペインで変更または再送信するコマンドを選択します。選択したコマンドは特定のデバイスに関連付けられており、最初のステップで選択したものとは限らないことに注意してください。

ステップ 7 [マイリスト（My List）] タブを見て、送信しようとしているコマンドが対象のデバイスに送信されることを確認します。

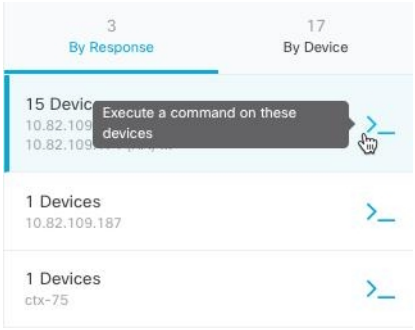
ステップ 8 コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。Security Cloud Control の応答ペインにコマンドの結果が表示されます。

一括コマンドフィルタでの動作

一括 CLI コマンドを実行後、[応答別（By Response）] フィルタと [デバイス別（By Device）] フィルタを使用して、デバイスの設定を続行できます。

応答別フィルタ

一括コマンドの実行後、Security Cloud Control は [応答別（By Response）] タブに、コマンドを送信したデバイスから返された応答のリストを入力します。同じ応答のデバイスは 1 行にまとめられます。[応答別（By Response）] タブの行をクリックすると、応答ペインにデバイスからの応答が表示されます。応答ペインに複数のデバイスの応答が表示される場合、「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[X デバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが Security Cloud Control に表示されます。



コマンド応答に関連付けられたデバイスのリストにコマンドを送信するには、次の手順に従います。

手順

ステップ 1 [応答別（By Response）] タブの行にあるコマンドシンボルをクリックします。

ステップ 2 コマンドペインでコマンドを確認し、[送信（Send）] をクリックしてコマンドを再送信するか、[クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力してデバイスに送信してから、[送信（Send）] をクリックします。

ステップ 3 コマンドから受け取った応答を確認します。

ステップ 4 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに `write memory` と入力し、[送信（Send）] をクリックします。この操作により、実行コンフィギュレーションがスタートアップコンフィギュレーションに保存されます。

デバイス別フィルタ

一括コマンドの実行後、Security Cloud Control は [実行（Execution）] タブと [デバイス別（By Device）] タブに、コマンドを送信したデバイスのリストを入力します。[デバイス別（By Device）] タブの行をクリックすると、各デバイスの応答が表示されます。

同じデバイスリストでコマンドを実行するには、次の手順に従います。

手順

ステップ 1 [デバイス別（By Device）] タブをクリックします。

ステップ 2 [>_これらのデバイスでコマンドを実行（>_Execute a command on these devices）] をクリックします。

ステップ 3 [クリア（Clear）] をクリックしてコマンドペインをクリアし、新しいコマンドを入力します。

ステップ 4 [マイリスト（My List）] ペインで、リスト内の個々のデバイスを選択または選択解除して、コマンドを送信するデバイスのリストを指定します。

ステップ 5 [送信（Send）]をクリックします。コマンドへの応答が応答ペインに表示されます。応答ペインに複数のデバイスの応答が表示される場合、「Xデバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが Security Cloud Control に表示されます。

ステップ 6 選択したデバイスの実行コンフィギュレーションファイルに変更が反映されていることが確実な場合は、コマンドペインに `write memory` と入力し、[送信（Send）] をクリックします。

コマンド ライン インターフェイス マクロ

CLI マクロは、すぐに使用できる完全な形式の CLI コマンド、または実行前に変更できる CLI コマンドのテンプレートです。すべてのマクロは、1 つ以上の SSH デバイスで同時に実行できます。

テンプレートに似た CLI マクロを使用して、複数のデバイスで同じコマンドを同時に実行します。CLI マクロは、デバイスの設定と管理の一貫性を促進します。完全な形式の CLI マクロを使用して、デバイスに関する情報を取得します。SSH デバイスですぐに使用できるさまざまな CLI マクロがあります。

頻繁に実行するタスクを監視するための CLI マクロを作成できます。詳細については、「新規コマンドからの CLI マクロの作成」を参照してください。

CLI マクロは、システム定義またはユーザー定義です。システム定義マクロは Security Cloud Control によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。

（注） デバイスが Security Cloud Control にオンボードされた後にのみ、デバイスのマクロを作成できます。

例として ASA を使用すると、いずれかの ASA で特定のユーザーを検索する場合は、次のコマンドを実行できます。

```
show running-config | grep username
```

このコマンドを実行すると、検索しているユーザーのユーザー名が username に置き換わります。このコマンドからマクロを作成するには、同じコマンドを使用して、username を中括弧で囲みます。

```
> show running-config | grep {{username}}
```

パラメータには任意の名前を付けることができ、そのパラメータ名で同じマクロを作成することもできます。

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

パラメータ名は説明的な名前にでき、英数字と下線を使用する必要があります。この場合、コマンドシンタックスは次のようになります。

```
show running-config | grep
```

コマンドの一部として、コマンドの送信先のデバイスに適したCLIシンタックスを使用する必要があります。

新規コマンドからの CLI マクロの作成

手順

ステップ 1 CLI マクロを作成する前に Security Cloud Control のコマンドライン インターフェイスでコマンドをテストして、コマンドの構文が正しく、信頼できる結果が返されることを確認します。

（注）

ステップ 2 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 3 [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 4 適切なデバイスタイプのタブをクリックし、オンラインかつ同期されているデバイスを選択します。

ステップ 5 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI マクロのお気に入りのスター ★ をクリックして、すでに存在するマクロを確認します。

ステップ 7 プラスボタン  をクリックします。

ステップ 8 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 9 [コマンド（Command）] フィールドにコマンドを入力します。

ステップ 10 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 11 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、『CLI マクロの実行』を参照してください。

CLI 履歴または既存の CLI マクロからの CLI マクロの作成

この手順では、すでに実行したコマンド、別のユーザー定義マクロ、またはシステム定義マクロからユーザー定義マクロを作成します。

手順

ステップ 1 左側のペインで [インベントリ（Inventory）]**セキュリティデバイス**をクリックします。

（注）
CLI 履歴からユーザー定義マクロを作成する場合は、コマンドを実行したデバイスを選択します。CLI マクロは、同じアカウントのデバイス間で共有されますが、CLI 履歴は共有されません。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、オンラインかつ同期されているデバイスを選択します。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 CLI マクロを作成するコマンドを見つけて選択します。次のいずれかの方法を使用してください。

- クロック をクリックして、そのデバイスで実行したコマンドを表示します。マクロに変換するコマンドを選択すると、コマンドペインにそのコマンドが表示されます。
- CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。変更するユーザー定義またはシステム定義の CLI マクロを選択します。コマンドがコマンドペインに表示されます。

ステップ 6 コマンドがコマンドペインに表示された状態で、CLI マクロの金色の星 をクリックします。このコマンドが、新しい CLI マクロの基礎になります。

ステップ 7 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド（Command）] フィールドのコマンドを確認し、必要な変更を加えます。

ステップ 9 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 10 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、CLI マクロの実行を参照してください。

CLI マクロの実行

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] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、1 つ以上のデバイスを選択します。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

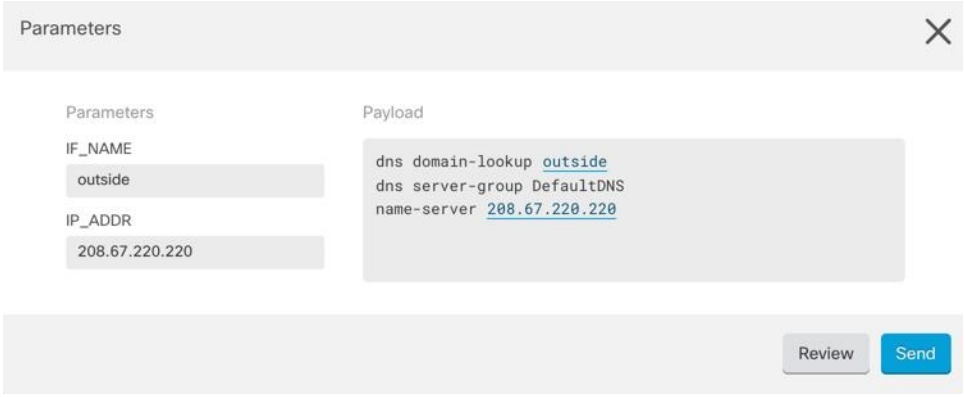
ステップ 5 コマンドパネルで、スター ★ をクリックします。

ステップ 6 コマンドパネルから CLI マクロを選択します。

ステップ 7 次のいずれかの方法でマクロを実行します。

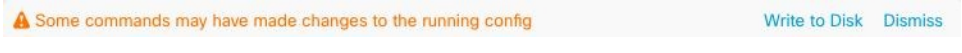
- 定義するパラメータがマクロに含まれていない場合は、[送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。これで完了です。
- マクロにパラメータが含まれている場合（下の Configure DNS マクロなど）、[>_ パラメータの表示（>_ View Parameters）] をクリックします。

ステップ 8 [パラメータ（Parameters）] ペインで、パラメータの値を [パラメータ（Parameters）] の各フィールドに入力します。



ステップ 9 [送信（Send）] をクリックします。Security Cloud Control が正常にコマンドを送信し、デバイスの構成を更新すると、「完了（Done!）」というメッセージが表示されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行コンフィギュレーションに変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。



- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行コンフィギュレーションのその他の変更がデバイスのスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

CLI マクロの編集

ユーザー定義の CLI マクロは編集できますが、システム定義のマクロは編集できません。CLI マクロを編集すると、すべての SSH デバイスでマクロが変更されます。マクロは特定のデバイス固有のものではありません。

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] タブをクリックします。
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 デバイスを選択します。
ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。
ステップ 6 編集するユーザー定義マクロを選択します。
ステップ 7 マクロラベルの編集アイコンをクリックします。
ステップ 8 [マクロの編集（Edit Macro）] ダイアログボックスで CLI マクロを編集します。
ステップ 9 [保存（Save）] をクリックします。

CLI マクロの実行方法については、「CLI マクロの実行」を参照してください。

CLI マクロの削除

ユーザー定義の CLI マクロは削除できますが、システム定義のマクロは削除できません。CLI マクロを削除すると、すべてのデバイスでマクロが削除されます。マクロは特定のデバイス固有のものではありません。

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] タブをクリックします。
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 デバイスを選択します。
ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。
ステップ 6 削除するユーザー定義 CLI マクロを選択します。
ステップ 7 CLI マクロラベルのゴミ箱アイコン をクリックします。
ステップ 8 CLI マクロを削除することを確認します。

Security Cloud Control CLI コマンドの結果のエクスポート

スタンドアロンデバイスまたは複数のデバイスに発行されたCLIコマンドの結果をコンマ区切り値（.csv）ファイルにエクスポートして、必要に応じて情報をフィルタリングおよび並べ替えることができます。単一のデバイスまたは多数のデバイスのCLI結果を一度にエクスポートできます。エクスポートされた情報には、次のものが含まれます。

- デバイス
- 日付
- ユーザー
- コマンド
- 出力

CLI コマンドの結果のエクスポート

コマンドウィンドウで実行したコマンドの結果を .csv ファイルにエクスポートできます。

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] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] ペインでコマンドを入力し、[送信（Send）] をクリックしてデバイスに送ります。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI マクロの結果のエクスポート

コマンドウィンドウで実行されたマクロの結果をエクスポートできます。次の手順で、1 つまたは複数のデバイスで実行された CLI マクロの結果を .csv 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] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、>_ [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI コマンド履歴のエクスポート

次の手順を使用して、1 つまたは複数のデバイスの CLI 履歴を .csv 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] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 履歴ペインがまだ展開されていない場合は、[時計（Clock）] アイコン をクリックして展開します。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

関連情報：

- Security Cloud Control コマンドライン インターフェイス （134 ページ）
- 新規コマンドからの CLI マクロの作成
- CLI マクロの削除
- CLI マクロの編集
- CLI マクロの実行
- 一括コマンド ライン インターフェイス

CLI マクロのリストをエクスポートする

コマンドウィンドウで実行されたマクロのみをエクスポートできます。次の手順で、1 つまたは複数のデバイスの CLI マクロを .csv 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] タブをクリックします。
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 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの[デバイスアクション]ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。
ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。
ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。
ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。
ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。

デバイス設定変更について

デバイスを管理するために、Security Cloud Control は、デバイスの設定のコピーを独自のデータベースに保存する必要があります。Security Cloud Control は、管理対象デバイスから設定を「読み取る」とき、デバイス設定のコピーを作成し、それを保存します。Security Cloud Control が最初にデバイスの設定のコピーを読み取って保存するのは、デバイスが導入準備されたときです。以下 の選択肢のように、さまざまな目的に応じて設定を読み取ります。

- [変更の破棄（Discard Changes）]：このアクションは、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が Security Cloud Control で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができます。保留中の変更は削除され、Security Cloud Control は設定のコピーをデバイスに保存されている設定のコピーで上書きします。
- [変更の確認（Check for Changes）]：このアクションは、デバイスの設定ステータスが同期済みの場合に使用できます。[変更の確認（Checking for Changes）] をクリックすると、Security Cloud Control は、デバイスの設定のコピーを、デバイスに保存されている設定のコピーと比較するように指示します。違いがある場合、Security Cloud Control はデバイスに保存されているコピーでそのデバイスの設定のコピーをすぐに上書きします。
- [競合の確認（Review Conflict）] と [レビューなしで承認（Accept Without Review）]：デバイスで [競合検出（Conflict Detection）] を有効にすると、Security Cloud Control はデバイスに加えられた設定の変更を 10 分ごとにチェックします。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/Basics_of_Cisco_Defense_Orchestrator/Synchronizing_Configurations_Between_Defense_Orchestrator_and_Device/0010_Conflict_Detectionデバイスに保存されている設定のコピーが変更された場合、Security Cloud Control は「競合が検出されました」という設定ステータスを表示して通知します。
  - [競合の確認（Review Conflict）]：[競合の確認（Review Conflict）] をクリックすると、デバイスで直接行われた変更を確認し、それらを受け入れるか拒否するかを選択できます。
  - [レビューなしで承認（Accept Without Review）]：このアクションにより、Security Cloud Control がもつ、デバイスの構成のコピーが、デバイスに保存されている構成の最新のコピーで上書きされます。Security Cloud Control では、上書きアクションを実行する前に、構成の 2 つのコピーの違いを確認するよう求められません。

[すべて読み取り（Read All）]：これは一括操作です。任意の状態にある複数のデバイスを選択し、[すべて読み取り（Read All）] をクリックして、Security Cloud Control に保存されているすべてのデバイスの設定を、デバイスに保存されている設定で上書きできます。

- [変更の展開（Deploy Changes）]：デバイスの設定に変更を加えると、Security Cloud Control では、加えた変更が独自のコピーに保存されます。これらの変更は、デバイスに展開されるまで Security Cloud Control で「保留」されています。デバイスの設定に変更があり、それがデバイスに展開されていない場合、デバイスは未同期構成状態になります。

保留中の設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、Security Cloud Control がデバイスに展開した後にのみ影響を及ぼします。Security Cloud Control がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。

- [すべて破棄（Discard All）] は、[プレビューして展開...（Preview and Deploy..）] をクリックした後にのみ使用できるオプションです。。[プレビューして展開（Preview and Deploy）] をクリックすると、Security Cloud Control で保留中の変更のプレビューが Security Cloud Control に表示されます。[すべて破棄（Discard All）] をクリックすると、保留中のすべての変更が Security Cloud Control から削除され、選択したデバイスには何も展開されません。上述の [変更の破棄（Discard Changes）] とは異なり、保留中の変更を削除すると操作が終了します。

すべてのデバイス設定の読み取り

Security Cloud Control の外部にあるデバイスの設定が変更された場合、Security Cloud Control に保存されているデバイスの設定と、当該デバイスの設定のローカルコピーは同じではなくなります。多くの場合、Security Cloud Control にあるデバイスの設定のコピーをデバイスに保存されている設定で上書きして、設定を再び同じにしたいと考えます。[すべて読み取り（Read All）] リンクを使用して、多くのデバイスでこのタスクを同時に実行できます。

Security Cloud Control によるデバイス設定の 2 つのコピーの管理方法の詳細については、「デバイス設定変更について」を参照してください。

[すべて読み取り（Read All）] をクリックした場合に、Security Cloud Control にあるデバイスの設定のコピーがデバイスの設定のコピーで上書きされる 3 つの設定ステータスを次に示します。

- [競合検出（Conflict Detected）]：競合検出が有効になっている場合、Security Cloud Control は、設定に加えられた変更について、管理するデバイスを 10 分ごとにポーリングします。Security Cloud Control がデバイスの設定が変更されたことを検出した場合、Security Cloud Control はデバイスの [競合検出（Conflict Detected）] 設定ステータスを表示します。
- [同期（Synced）]：デバイスが [同期（Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、Security Cloud Control はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り（Read All）] をクリックすると、Security Cloud Control はデバイスの設定のコピーを上書きすることを確認し、その後 Security Cloud Control が上書きを実行します。
- [非同期（Not Synced）]：デバイスが [非同期（Not Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、Security Cloud Control は、Security Cloud Control を使用したデバイスの設定に対する保留中の変更があること、および[すべて読み取り（Read All）] 操作を続行すると保留中の変更が削除されてから、Security Cloud Control にある設定のコピーがデバイス上の設定で上書きされることを警告します。この [すべて読み取り

（Read All）] は、[変更の破棄（Discard Changes）] と同様に機能します。設定変更の破棄（157 ページ）

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] タブをクリックします。

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 （任意）変更ログでこの一括アクションの結果を簡単に識別できるように、変更要求管理を作成します。

ステップ 5 Security Cloud Control を保存する設定のデバイスを選択します。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 [すべて読み取り（Read All）] をクリックします。

ステップ 7 選択したデバイスのいずれかについて、Security Cloud Control で設定変更がステージングされている場合、Security Cloud Control は警告を表示し、設定の一括読み取りアクションを続行するかどうかを尋ねられます。[すべて読み取り（Read All）] をクリックして続行します。

ステップ 8 設定の [すべて読み取り（Read All）] 操作の進行状況については、Security Cloud Control でのジョブのモニタリングで確認します。一括操作の個々のアクションの成功または失敗に関する詳細を確認する場合は、青色の[レビュー（Review）]リンクをクリックすると、[ジョブ（Jobs）] ページに移動します。 Security Cloud Control でのジョブのモニタリング （177 ページ）

ステップ 9 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

関連情報

- デバイス設定変更について
- 設定変更の破棄
- 設定変更の確認

Cisco IOS または SSH から Security Cloud Control への変更の読み取り

Cisco IOS または SSH デバイスを管理するために、Security Cloud Control は、デバイスの構成ファイルのコピーを独自で保存している必要があります。Security Cloud Control が最初にデバイスの構成ファイルのコピーを読み取って保存するのは、デバイスがオンボードされたときです。その後、Security Cloud Control は、デバイスからの設定をチェックするときに、デバイスの構成ファイルのコピーを取得し、独自のデータベースに保持している構成ファイルのコピー

を完全に上書きします。詳細については、「デバイス設定変更について」を参照してください。

Security Cloud Control の外部で Cisco IOS または SSH デバイスに直接加えられた変更を検出する方法の詳細については、「設定変更の確認」を参照してください。

Security Cloud Control で開始したものの IOS または SSH デバイスに展開していない設定変更を「元に戻す」方法の詳細については、「設定変更の破棄」を参照してください。

すべてのデバイスの設定変更のプレビューと展開

テナント上のデバイスに構成変更を加えたものの、その変更をまだ展開していない場合に、

Security Cloud Control は展開アイコン にオレンジ色のドットを表示して通知します。これらの変更の影響を受けるデバイスには、[デバイスとサービス（Devices and Services）] ページに「非同期（Not Synced）」のステータスが表示されます。[展開（Deploy）] をクリックすると、保留中の変更があるデバイスを確認し、それらのデバイスに変更を展開できます。

（注） 作成および変更を行う新しい FDM または FTD ネットワークオブジェクトまたはグループごとに、Security Cloud Control は、Security Cloud Control によって管理されるすべての オンプレミス Management Centerに対してこのページにエントリを作成します。

この展開方法は、サポートされているすべてのデバイスで使用できます。

この展開方法を使用して、単一の構成変更を展開することも、待機して複数の変更を一度に展開することもできます。

手順

ステップ 1 画面の右上で [デプロイ（Deploy）] アイコン をクリックします。

ステップ 2 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。

ステップ 3 （オプション）保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示（View Detailed Changelog）] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開（Deploy）] アイコンをクリックして、[保留中の変更があるデバイス（Devices with Pending Changes）] ページに戻ります。

ステップ 4 （オプション）[保留中の変更があるデバイス（Devices with Pending Changes）] ページを離れずに、変更を追跡する変更要求管理します。

ステップ 5 [今すぐ展開（Deploy Now）] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ（Jobs）] トレイの [アクティブなジョブ（Active jobs）] インジケータに進行状況が表示されます。

ステップ 6 （オプション）展開が完了したら、Security Cloud Control ナビゲーションバーの [ジョブ（Jobs）] をクリックします。展開の結果を示す最近の「変更の展開（Deploy Changes）」ジョブが表示されます。

ステップ 7 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

次のタスク

- スケジュールされた自動展開について

デバイス設定の一括展開

共有オブジェクトを編集するなどして複数のデバイスに変更を加えた場合、影響を受けるすべてのデバイスにそれらの変更を一度に適用できます。

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] タブをクリックします。

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 Security Cloud Control で設定を変更した、すべてのデバイスを選択します。これらのデバイスは、「未同期」ステータスが表示されているはずです。

ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- 画面の右上にある ボタンをクリックして、[保留中の変更があるデバイス（Devices with Pending Changes）] ウィンドウを表示します。これにより、選択したデバイス上の保留中の変更を展開する前に確認することができます。変更を展開するには、[今すぐ展開（Deploy Now）] をクリックします。

  （注）
  [保留中の変更があるデバイス（Devices with Pending Changes）] 画面でデバイスの横に黄色の警告三角形が表示されている場合、そのデバイスに変更を展開することはできません。そのデバイスに変更を展開できない理由を確認するには、警告三角形の上にマウスカーソルを置きます。

- 詳細ペインで [すべて展開（Deploy All）] をクリックします。 すべての警告を確認し、[OK] をクリックします。一括展開は、変更を確認せずにすぐに開始します。

ステップ 6 （任意）ナビゲーションバーの [ジョブ（Jobs）] アイコン  をクリックして、一括展開の結果を表示します。

スケジュールされた自動展開について

Security Cloud Control を使用すると、CDO が管理する 1 つ以上のデバイスの構成を変更し、都合のよいタイミングでそれらのデバイスに変更を展開するようにスケジュールできます。

[設定（Settings）] ページの [テナント設定（Tenant Settings）] タブで 自動展開をスケジュールするオプションを有効にする （53 ページ） をした場合のみ、展開をスケジュールできます。このオプションを有効にすると、展開スケジュールを作成、編集、削除できます。展開スケジュールによって、Security Cloud Control に保存されたすべてのステージング済みの変更が、設定した日時に展開されます。[ジョブ]ページから、展開スケジュールを表示および削除することもできます。

Security Cloud Control にデバイス設定変更についてデバイスに直接変更が加えられた場合、その競合が解決されるまで、展開スケジュールはスキップされます。[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。

注意 複数のデバイスの新しい展開をスケジュールし、それらのデバイスの一部に展開が既にスケジュールされている場合、既存の展開スケジュールが新しい展開スケジュールで上書きされます。

（注） 展開スケジュールを作成すると、スケジュールはデバイスのタイムゾーンではなく現地時間で作成されます。展開スケジュールは、サマータイムに合わせて自動的に調整されません。

自動展開のスケジュール

展開スケジュールは、単一のイベントまたは繰り返し行われるイベントにすることができます。繰り返し行われる自動展開は、繰り返し行われる展開をメンテナンス期間に合わせるための便利な方法です。次の手順に従って、単一のデバイスに対して1回限りまたは繰り返し行われる展開をスケジュールします。

（注） 既存の展開がスケジュールされているデバイスへの展開をスケジュールすると、新しくスケジュールされた展開によって既存の展開が上書きされます。

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] タブをクリックします。

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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[スケジュール（Schedule）] をクリックします。

ステップ 6 展開をいつ実行するかを選択します。

- 1 回限りの展開の場合は、[1回限り（Once on）] オプションをクリックして、カレンダーから日付と時刻を選択します。
- 繰り返し展開する場合は、[定期（Every）] オプションをクリックします。日に 1 回と週に 1 回のいずれかの展開を選択できます。展開を実行する [曜日（Day）] と [時刻（Time）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

手順

ステップ 1 左側のペインで **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] タブをクリックします。

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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[編集（Edit）] をクリックします。

ステップ 6 スケジュールされた展開の繰り返し回数、日付、または時刻を編集します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。

（注） 複数のデバイスの展開をスケジュールしてから、一部のデバイスのスケジュールを変更または削除した場合は、残りのデバイスの元のスケジュールされた展開が保持されます。

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] タブをクリックします。
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 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細（Device Details）] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[削除（Delete）] をクリックします。

次のタスク

- デバイス設定変更について
- すべてのデバイス設定の読み取り （150 ページ）
- すべてのデバイスの設定変更のプレビューと展開 （152 ページ）

設定変更の確認

[変更の確認（Check for Changes）] をクリックして、デバイスの設定がデバイス上で直接変更されているか、Security Cloud Control に保存されている設定のコピーと異なっているかどうかを確認します。このオプションは、デバイスが [同期（Synced）] 状態のときに表示されます。

変更を確認するには、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] タブをクリックします。
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 設定がデバイス上で直接変更された可能性があるデバイスを選択します。

ステップ 5 右側の [同期（Synced）] ペインで [変更の確認（Check for Changes）] をクリックします。

ステップ 6 次の動作は、デバイスによって若干異なります。

- デバイスの場合、デバイスの設定に変更があった場合、次のメッセージが表示されます。

```
Reading the policy from the device. If there are active deployments on the device,
reading will start after they are finished.
```

  - [OK] をクリックして、先へ進みます。デバイスの設定で、Security Cloud Control に保存されている設定が上書きされます。
  - 操作をキャンセルするには、[キャンセル（Cancel）] をクリックします。

- SSH デバイスの場合：

1. 提示された 2 つの設定を比較します。[続行（Continue）] をクリックします。**最後に認識されたデバイス設定（Last Known Device Configuration）**というラベルの付いた設定は、Security Cloud Control に保存されている設定です。[デバイスで検出（Found on Device）] というラベルの付いた設定は、ASA に保存されている設定です。
2. 次のいずれかを選択します。
   1. [拒否（Reject）] : アウトオブバンド変更を拒否して、「最後に認識されたデバイス設定（Last Known Device Configuration）」を維持します。
   2. [承認（Accept）] : アウトオブバンド変更を承認して、Security Cloud Control に保存されているデバイスの設定を、デバイスで見つかった設定で上書きします。
3. [続行（Continue）] をクリックします。

設定変更の破棄

Security Cloud Control を使用してデバイスの構成に加えた、展開されていない構成変更のすべてを「元に戻す」場合は、[変更の破棄（Discard Changes）] をクリックします。[変更の破棄（Discard Changes）] をクリックすると、Security Cloud Control は、デバイスに保存されている構成でデバイスの構成のローカルコピーを完全に上書きします。

[変更の破棄（Discard Changes）] をクリックすると、デバイスの構成ステータスは [非同期（Not Synced）] 状態になります。変更を破棄すると、Security Cloud Control 上の構成のコピーは、デバイス上の構成のコピーと同じになり、Security Cloud Control の構成ステータスは [同期済み（Synced）] に戻ります。

デバイスの展開されていない構成変更のすべてを破棄する（つまり「元に戻す」）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] タブをクリックします。

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 構成変更を実行中のデバイスを選択します。

ステップ 5 右側の [未同期（Not Synced）] ペインで [変更の破棄（Discard Changes）] をクリックします。

- FDM による管理 デバイスの場合は、Security Cloud Control で「Security Cloud Control 上の保留中の変更は破棄され、このデバイスに関する Security Cloud Control 構成は、デバイス上の現在実行中の構成に置き換えられます（Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device）」という警告メッセージが表示されます。[続行（Continue）] をクリックして変更を破棄します。
- Meraki デバイスの場合は、Security Cloud Control で変更がすぐに削除されます。
- AWS デバイスの場合は、Security Cloud Control で削除しようとしているものが表示されます。[同意する（Accept）] または [キャンセル（Cancel）] をクリックします。

デバイスのアウトオブバンド変更

アウトオブバンド変更とは、Security Cloud Control を使用せずにデバイス上で直接行われた変更を指します。アウトオブバンド変更は、SSH 接続を介してデバイスのコマンド ライン インターフェイスを使用して、または、ASA の場合は Adaptive Security Device Manager（ASDM）、FDM による管理 デバイスの場合は FDM、オンプレミス Firewall Management Center ユーザー インターフェイス上の オンプレミス Firewall Management Center などのローカルマネージャを使用して行うことができます。アウトオブバンド変更により、Security Cloud Control に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

デバイスでのアウトオブバンド変更の検出

ASA、FDM による管理デバイス、Cisco IOS デバイス、またはオンプレミス Firewall Management Center に対して競合検出が有効になっている場合、Security Cloud Control は 10 分ごとにデバイスをチェックし、Security Cloud Control の外部でデバイスの設定に直接加えられた新たな変更を検索します。

Security Cloud Control は、Security Cloud Control に保存されていないデバイスの設定に対する変更を検出した場合、そのデバイスの [設定ステータス（Configuration Status）] を [競合検出（Conflict Detected）] 状態に変更します。

Security Cloud Control が競合を検出した場合、次の 2 つの状態が考えられます。

- Security Cloud Control のデータベースに保存されていない設定変更が、デバイスに直接加えられています。
- FDM による管理 デバイスの場合、FDM による管理 デバイスに展開されていない「保留中」の設定変更がある可能性があります。
- オンプレミス Firewall Management Center の場合、たとえば、Security Cloud Control との同期が保留されている Security Cloud Control の外部で行われた変更や、オンプレミス Firewall Management Center への展開が保留されている Security Cloud Control で行われた変更がある可能性があります。

Security Cloud Control とデバイス間の設定を同期する

設定の競合について

[セキュリティデバイス（Security Devices）] ページで、デバイスまたはサービスのステータスが [同期済み（Synced）]、[未同期（Not Synced）]、または [競合検出（Conflict Detected）] になっていることがあります。Security Cloud Control を使用して管理するオンプレミス Firewall Management Center のステータスを確認するには、**[ツールとサービス（Tools & Services）]** > **[Firewall Management Center]** に移動します。

- デバイスが [同期済み（Synced）] の場合、Security Cloud Control の設定と、デバイスにローカルに保存されている設定は同じです。
- デバイスが [未同期（Not Synced）] の場合、Security Cloud Control に保存された設定が変更され、デバイスにローカルに保存されている設定とは異なっています。Security Cloud Control からデバイスに変更を展開すると、Security Cloud Control のバージョンに一致するようにデバイスの設定が変更されます。
- Security Cloud Control の外部でデバイスに加えられた変更は、**アウトオブバンドの変更**と呼ばれます。デバイスの競合検出が有効になっている場合、アウトオブバンドの変更が行われると、デバイスのステータスが [競合が検出されました（Conflict Detected）] に変わります。アウトオブバンドの変更を受け入れると、Security Cloud Control の設定がデバイスの設定と一致するように変更されます。

競合検出

競合検出が有効になっている場合、Security Cloud Control はデフォルトの間隔でデバイスをポーリングして、Security Cloud Control の外部でデバイスの構成が変更されたかどうかを判断します。変更が行われたことを検出すると、Security Cloud Control はデバイスの構成ステータスを [競合検出（Conflict Detected）] に変更します。Security Cloud Control の外部でデバイスに加えられた変更は、「アウトオブバンドの」変更と呼ばれます。

Security Cloud Control によって管理されているオンプレミス Firewall Management Center で、ステージングされた変更があり、デバイスが [未同期（Not Synced）] 状態の場合、Security Cloud

Control はデバイスのポーリングを停止して変更を確認します。Security Cloud Control との同期が保留されている Security Cloud Control の外部で行われた変更と、オンプレミス Management Center への展開が保留されている Security Cloud Control で行われた変更がある場合、Security Cloud Control は オンプレミス Management Centerが [競合検出（Conflict Detected）] 状態であることを宣言します。

このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、デバイス変更のポーリングのスケジュール（164 ページ）を参照してください。

競合検出の有効化

競合検出を有効にすると、Security Cloud Control の外部でデバイスに変更が加えられた場合に警告が表示されます。

手順

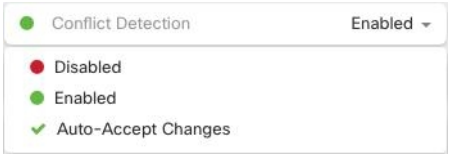
ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブを選択します。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 デバイステーブルの右側にある [競合検出（Conflict Detection）] ボックスで、リストから [有効（Enabled）] を選択します。



デバイスからのアウトオブバンド変更の自動的な受け入れ

変更の自動的な受け入れを有効にすることで、管理対象デバイスに直接加えられた変更を自動的に受け入れるように Security Cloud Control を設定できます。Security Cloud Control を使用せずにデバイスに直接加えられた変更は、アウトオブバンド変更と呼ばれます。アウトオブバンドの変更により、Security Cloud Control に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、Security Cloud Control は 10 分ごとに変更をチェックして、デバイスの

設定に対してアウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、Security Cloud Control は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

Security Cloud Control で行われたいずれかの設定変更がデバイスにまだ展開されていない場合、Security Cloud Control は設定変更を自動的に**受け入れません**。画面上のプロンプトに従って、次のアクションを決定します。

変更の自動承認を使用するには、最初に、[セキュリティデバイス（Security Devices）] ページの [競合検出（Conflict Detection）] メニューで自動承認オプションをテナントが表示できるようにします。次に、個々のデバイスでの変更の自動承認を有効にします。

Security Cloud Control でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに競合検出 （159ページ） を有効にします。

自動承認変更の設定

手順

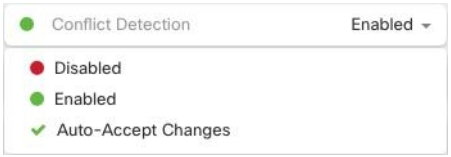
ステップ 1 管理者またはネットワーク管理者権限を持つアカウントを使用して Security Cloud Control にログインします。

ステップ 2 左側のペインで **[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

ステップ 3 [テナント設定（Tenant Settings）] エリアで、[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）] のトグルをクリックします。[セキュリティデバイス（Security Devices）] ページの [競合検出（Conflict Detection）] メニューに [変更の自動承認（Auto-Accept Changes）] メニューオプションが表示されます。

ステップ 4 左側のペインで **セキュリティデバイス** をクリックして、アウトオブバンドの変更を自動承認するデバイスを選択します。

ステップ 5 [競合の検出（Devices & Services）] メニューで、ドロップダウンメニューから [変更の自動承認（Auto-Accept Changes）] を選択します。



テナント上のすべてのデバイスの自動承認変更の無効化

手順

ステップ 1 [管理者（Admin）] または [ネットワーク管理者（Super Admin）] 権限を持つアカウントを使用して 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）] > [一般設定（General Settings）]** をクリックします。

ステップ 3 [テナント設定（Tenant Settings）] 領域で、トグルを左にスライドして灰色の X を表示し、[デバイスの変更を自動承認するオプションを有効にする（Enable the option to auto-accept device changes）] を無効にします。これにより、競合検出メニューの [変更の自動承認（Auto-Accept Changes）] オプションが無効になり、テナント上のすべてのデバイスでこの機能が無効になります。

（注）
[自動承認（Auto-Accept）] を無効にした場合、Security Cloud Control で承認する前に、各デバイスの競合を確認する必要があります。これまで変更の自動承認が設定されていたデバイスも対象になります。

設定の競合の解決

このセクションでは、デバイスで発生する設定の競合の解決に関する情報を提供します。

未同期ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）] > [Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

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 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期（Not synced）] パネルで、次のいずれかを選択します。

- [プレビューして展開...（Preview and Deploy..）]：設定の変更を Security Cloud Control からデバイスにプッシュする場合は、今行った変更をすべてのデバイスの設定変更のプレビューと展開か、待ってから一度に複数の変更を展開します。
- [変更の破棄（Discard Changes）]：設定の変更を Security Cloud Control からデバイスに**プッシュしない**場合、または Security Cloud Control で開始した設定の変更を「元に戻す」場合。このオプションは、Security Cloud Control に保存されている設定を、デバイスに保存されている実行構成で上書きします。

競合検出ステータスの解決

Security Cloud Control を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。競合検出 （159 ページ） が有効になっていて、Security Cloud Control を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出（Conflict Detected）] と表示されます。

[競合検出（Conflict Detected）] ステータスを解決するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）]** > **[Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

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 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認（Review Conflict）] をクリックします。

ステップ 5 [デバイスの同期（Device Sync）] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。

- 「最後に認識されたデバイス設定（Last Known Device Configuration）」というラベルの付いたパネルは、Security Cloud Control に保存されているデバイス設定です。
- [デバイスで検出（Found on Device）] というラベルの付いたパネルは、ASA の実行コンフィギュレーションに保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認（Accept Device changes）]：設定と、Security Cloud Control に保存されている保留中の変更がデバイスの実行コンフィギュレーションで上書きされます。

  （注）
  Security Cloud Control はコマンド ライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認（Accept Without Review）] です。

- [デバイスの変更を拒否（Reject Device Changes）]：デバイスに保存されている設定を Security Cloud Control に保存されている設定で上書きします。

（注）
拒否または承認されたすべての設定変更は、変更ログに記録されます。

デバイス変更のポーリングのスケジュール

競合検出 （159 ページ） を有効にしている場合、または [設定（Settings）] ページで [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）] オプションを有効にしている場合、Security Cloud Control はデフォルトの間隔でデバイスをポーリングして、Security Cloud Control の外部でデバイスの設定に変更が加えられたかどうかを判断します。Security Cloud Control による変更のポーリング間隔は、デバイスごとにカスタマイズできます。ポーリング間隔の変更は、複数のデバイスに適用できます。

デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。

（注） [セキュリティデバイス（Security Devices）] ページでデバイスごとの間隔をカスタマイズすると、[一般設定（General Settings）] ページの [デフォルトの競合検出間隔（Default Conflict Detection Interval）] で選択したポーリング間隔がオーバーライドされます。デフォルトの競合検出間隔 （52 ページ）

[セキュリティデバイス（Security Devices）] ページで [競合検出（Conflict Detection）] を有効にするか、[設定（Settings）] ページで [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）] オプションを有効にしたら、次の手順に従い Security Cloud Control によるデバイスのポーリング間隔をスケジュールします。

手順

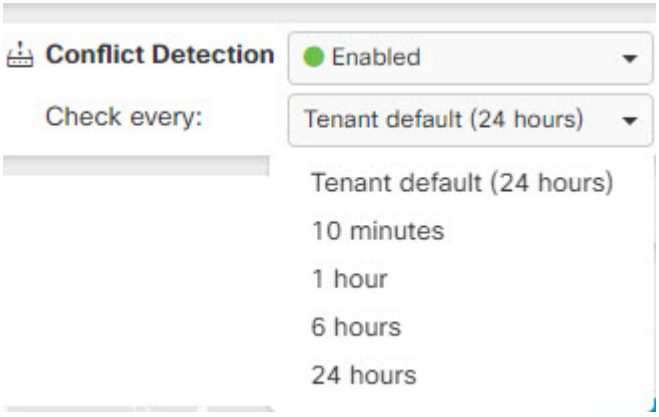
ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

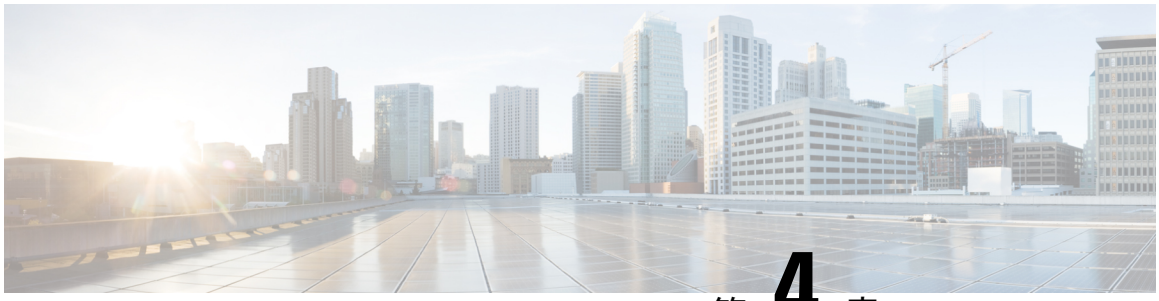
ステップ 2 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

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 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 [競合検出（Conflict Detection）] と同じ領域で、[チェック間隔（Check every）] のドロップダウンメニューをクリックし、目的のポーリング間隔を選択します。





第 4 章

変更ログ、ワークフロー、およびジョブのモニタリングとレポート

Security Cloud Control は、設定変更ログ、一括デバイス操作、およびデバイスとの通信時に実行されるプロセスを効果的にモニタリングします。これは、ネットワークの既存のポリシーがセキュリティ態勢にどのように影響するかを理解するのに役立ちます。

Security Cloud Control での変更ログの管理

変更ログは、Security Cloud Control で行われた設定変更をキャプチャし、サポート対象のすべてのデバイスとサービスの変更を表示する単一のビューを提供します。変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較を示します。
- すべての変更ログエントリのラベルを示します。
- デバイスのオンボーディングと削除を記録します。
- Security Cloud Control の外部で発生するポリシー変更の競合を検出します。
- インシデントの調査またはトラブルシューティング中に、「誰が」、「何を」、「いつ」に回答します。
- 変更ログ全体またはその一部のみを CSV ファイルとしてダウンロードできます。

変更ログの容量の管理

Security Cloud Control は、変更ログ情報を 1 年間保持し、1 年以上経過したデータを削除します。

Security Cloud Control のデータベースに保存される変更ログ情報と、エクスポートした変更ログに表示される情報には違いがあります。詳細については、変更ログのエクスポート（170ページ）を参照してください。

変更ログエントリ

変更ログエントリには、単一のデバイス設定への変更、デバイスで実行されたアクション、または Security Cloud Control の外部でデバイスに加えられた変更が反映されます。

- 設定の変更を含む変更ログエントリの場合、対応する行の任意の場所をクリックして変更の詳細を表示できます。
- Security Cloud Control の外部で行われ、競合として検出されたアウトオブバンド変更の場合、**システムユーザー**は**最後のユーザー**として報告されます。
- Security Cloud Control 上のデバイスの設定がデバイス上の設定と同期された後、またはデバイスが Security Cloud Control から削除されたときに、Security Cloud Control は変更ログエントリを閉じます。設定は、デバイスから Security Cloud Control に設定を読み取った後に、または Security Cloud Control からデバイスに設定を展開した後に同期されたと見なされます。
- Security Cloud Control は、変更が成功したか失敗したかに関係なく、既存のエントリを完了した直後に新しい変更ログエントリを作成します。追加の設定変更は、開いている新しい変更ログエントリに追加されます。
- デバイスに対する読み取り、展開、および削除アクションのイベントが表示されます。これらのアクションで、デバイスの変更ログが閉じられます。
- Security Cloud Control が（読み取りまたは展開によって）デバイスの設定と同期されると、または Security Cloud Control がデバイスを管理しなくなると、変更ログは閉じられます。
- Security Cloud Control の外部でデバイスに変更が加えられた場合、[競合検出（Conflict Detected）] エントリが変更ログに含まれます。

保留中および完了した変更ログエントリ

変更ログには、[保留中（Pending）] または [完了（Completed）] のステータスがあります。Security Cloud Control を使用してデバイスの設定を変更すると、変更は [保留中（Pending）] 変更ログエントリに記録されます。次のアクティビティによって保留中の変更ログが完了し、その後、将来の変更を記録するために新しい変更ログが作成されます。

- デバイスから Security Cloud Control への設定の読み取り
- Security Cloud Control からデバイスへの変更の展開
- Security Cloud Control からのデバイスの削除

- 実行コンフィギュレーション ファイルを更新する CLI コマンドの実行

変更ログエントリの検索とフィルタ処理

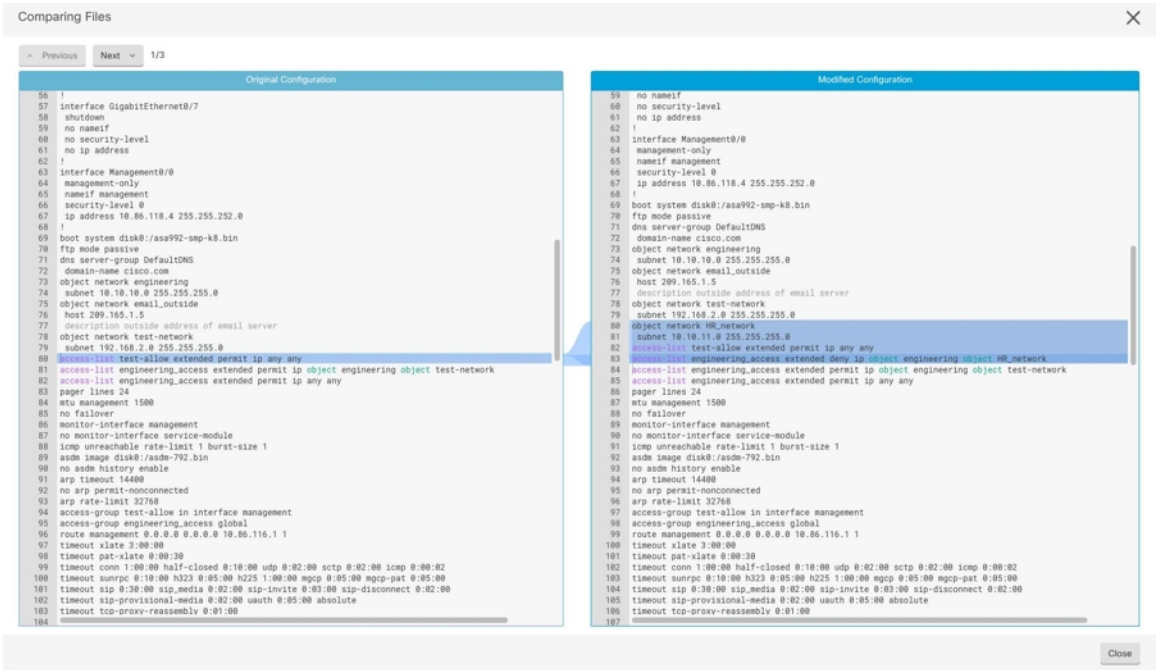
変更ログエントリを検索およびフィルタ処理できます。検索フィールドを使用してイベントを検索します。フィルタ（）を使用して、指定した条件を満たすエントリを検索します。また、変更ログをフィルタ処理し、検索フィールドにキーワードを追加して、2 つのタスクを組み合わせることで、フィルタ処理された結果内のエントリを検索できます。

変更ログの差異の表示

変更ログにある [差分（Diff）] をクリックすると、デバイスの実行コンフィギュレーション ファイル内の変更が並べて表示されるため、変更を対比できます。

次の図で、[元の設定（Original Configuration）] 列は、変更が ASA に書き込まれる前の実行コンフィギュレーション ファイルです。[変更済みの設定（Modified Configuration）] 列には、変更が書き込まれた後の実行コンフィギュレーション ファイルが表示されます。この場合、[元の設定（Original Configuration）] 列は、実行コンフィギュレーション ファイルの行を強調表示します。この行は変更されていませんが、[変更された設定（Modified Configuration）] 列の参照点をとなります。

左から右の列に向かって線をたどると、*HR_network* オブジェクトの追加と、「*engineering*」ネットワークのアドレスが「*HR_network*」ネットワークのアドレスに到達することを防止するアクセスルールを確認できます。[前へ（Previous）] および [次へ（Next）] ボタンをクリックして、ファイル内の変更を確認します。



関連項目

- Security Cloud Control での変更ログの管理 （167 ページ）

変更ログのエクスポート

Security Cloud Control 変更ログのすべてまたは一部をコンマ区切り値（.csv）ファイルにエクスポートして、必要に応じて情報をフィルタリングおよび並べ替えることができます。

変更ログを .csv ファイルにエクスポートするには、次の手順を実行します。

手順

ステップ 1 左側のペインで、[変更ログ（Change Log）]**[イベントとログ（Events & Logs）]** > **[変更ログ（Change Log）]**をクリックします。

ステップ 2 次のいずれかのタスクを実行して、エクスポートする変更を見つけます。

- フィルタリング（）フィールドと検索フィールドを使用して、エクスポートするものを見つけます。たとえば、デバイスでフィルタリングして、選択した 1 つまたは複数のデバイスの変更のみを表示します。
- 変更ログのすべてのフィルタリングおよび検索条件をクリアします。これにより、変更ログ全体をエクスポートできます。

（注）
Security Cloud Control は 1 年間の変更ログデータを保持します。1 年間分の変更ログ履歴全体をダウンロードするよりも、変更ログの内容をフィルタリングし、その結果を .csv ファイルとしてダウンロードことをお勧めします。

ステップ 3 ページの右上隅にあるエクスポート アイコンをクリックします。

ステップ 4 .csv ファイルにわかりやすい名前を付けてローカルファイルシステムに保存します。

Security Cloud Control の変更ログのキャパシティとエクスポートした変更ログのサイズの差異

Security Cloud Control の [変更ログ（Change Log）] ページからエクスポートする情報は、Security Cloud Control がデータベースに保存する変更ログ情報とは異なります。

すべての変更ログについて、Security Cloud Control はデバイスの設定の 2 つのコピーを保存します。1 つは「開始」設定、もう 1 つはクローズされた変更ログの場合は「終了」設定、オープンな変更ログの場合は「最新」設定です。これにより、Security Cloud Control は設定の違い

を並べて表示できます。さらに、Security Cloud Control は、変更を行ったユーザー名、変更が行われた時刻、およびその他の詳細とともに、すべてのステップ（「変更イベント」）を追跡して保存します。

ただし、変更ログをエクスポートする場合、エクスポートには設定の2つの完全なコピーは含まれません。これには「変更イベント」のみが含まれるため、エクスポートファイルはSecurity Cloud Control に保存されている変更ログよりもはるかに小さくなります。

Security Cloud Control は、1年分の変更ログ情報を保存します。これには、設定の2つのコピーが含まれます。

変更要求管理

変更要求管理を使用すると、**変更要求**とそのビジネス上の正当性を**変更ログ**イベントにリンクできます。**変更要求**は、サードパーティのチケット生成システムで開かれます。

変更要求管理を使用して、Security Cloud Control で**変更要求**を作成し、変更ログイベントに関連付けます。この変更要求は、変更ログ内で**名前**で検索できます。

（注） Security Cloud Control では、**変更要求トラッキング**と**変更要求管理**は同じ機能を指しています。

変更要求管理の有効化

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。

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

有効にすると、[変更リクエスト（Change Request）] メニューが左下隅に表示され、[変更ログ（Change Log）] ページの [変更リクエスト（Change Request）] ドロップダウンリストが使用できるようになります。

変更リクエストの作成

手順

ステップ 1 Security Cloud Control で、左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

[名前（Name）] が組織で使用する予定の [変更リクエスト（Change Request）] 名に対応していること、そして [説明（Description）] に変更の目的が記載されていることを確認します。

（注）
作成後に [変更リクエスト（Change Request）] の名前を変更することはできません。

ステップ 3 [保存（Save）] をクリックします。

（注）
[変更リクエスト（Change Request）] が保存されると、Security Cloud Control はすべての新しい変更を対応する [変更リクエスト（Change Request）] 名に関連付けます。この関連付けは、変更リクエスト管理の無効化か、メニューから変更リクエストツールバーをクリアするまで続きます。

変更リクエストと変更ログイベントの関連付け

手順

ステップ 1 左側のペインで、[変更ログ（Change Log）]**[イベントとログ（Events & Logs）]** > **[変更ログ（Change Log）]**をクリックします。

ステップ 2 変更ログを展開して、[変更リクエスト（Change Request）] に関連付けるイベントを表示します。

ステップ 3 対応する変更ログエントリの横にあるドロップダウンリストをクリックします。

（注）
最新の変更リクエストが変更リクエストリストの一番上に表示されます。

ステップ 4 変更リクエストを選択して、[選択（Select）] をクリックします。

変更リクエストがある変更ログイベントの検索

手順

ステップ 1 左側のペインで、[変更ログ（Change Log）]**[イベントとログ（Events & Logs）]** > **[変更ログ（Change Log）]**をクリックします。

ステップ 2 [変更ログ（Change Log）] 検索フィールドに、変更リクエストの名前を入力して、関連付けられた変更ログイベントを検索します。

Security Cloud Control は、完全に一致する変更ログイベントを強調表示します。

変更リクエストの検索

手順

ステップ 1 Security Cloud Control で、左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 [検索（Search）] フィールドに [変更リクエスト（Change Request）] の名前または関連するキーワードを入力します。値を入力すると、入力内容と部分的に一致する結果が [名前（Name）] フィールドと [説明（Description）] フィールドの両方に表示されます。

フィルタ変更リクエスト

手順

ステップ 1 左側のペインで、[変更ログ（Change Log）]**[イベントとログ（Events & Logs）]** > **[変更ログ（Change Log）]**をクリックします。

ステップ 2 フィルタアイコンをクリックすると、すべてのオプションが表示されます。

ステップ 3 [検索（search）] フィールドに、[変更リクエスト（Change Request）] の名前を入力します。

値を入力すると、入力した値と部分一致する結果が表示されます。

ステップ 4 対応するチェックボックスをオンにして、変更リクエストを選択します。

一致したものが [変更ログ（Change Log）] テーブルに表示されます。Security Cloud Control により、完全一致の変更ログイベントが強調表示されます。

変更リクエストツールバーをクリアする

変更ログイベントが既存の変更リクエストに自動的に関連付けられるのを避けるため、変更リクエストツールバーの情報をクリアします。

手順

ステップ 1 Security Cloud Control で、左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 [クリア（Clear）] をクリックします。

[変更リクエスト（Change Request）] メニューに [なし（None）] と表示されます。

変更ログイベントと関連付けられた変更リクエストのクリア

手順

ステップ 1 左側のペインで、[変更ログ（Change Log）]**[イベントとログ（Events & Logs）]** > **[変更ログ（Change Log）]**をクリックします。

ステップ 2 [変更ログ（Change Log）] を展開して、[変更リクエスト（Change Requests）] との関連付けを解除するイベントを表示します。

ステップ 3 対応する変更ログエントリの横にあるドロップダウンリストをクリックします。

ステップ 4 [クリア（Clear）] をクリックします。

変更リクエストの削除

[変更リクエスト（Change Request）] を削除するときは、[変更ログ（Change Log）] からではなく変更リクエストリストから削除します。

手順

ステップ 1 左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 変更リクエストを選択し、ゴミ箱アイコンをクリックして削除します。

ステップ 3 チェックマークをクリックして確定します。

変更リクエスト管理の無効化

[変更リクエスト管理（Change Request Management）] または [変更リクエストのトラッキング（Change Request Tracking）] を無効にすると、アカウントのすべてのユーザーに影響します。

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 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを無効化します。

変更リクエスト管理のユースケース

これらのユースケースは、変更リクエスト管理が有効化されていることを前提としています。

外部システムで維持されているチケットを解決するために行われたファイアウォールデバイスの変更を追跡する

このユースケースでは、外部システムで維持されているチケットを解決するためにファイアウォールデバイスに変更を加え、これらのファイアウォールの変更から生じる変更ログイベントを変更リクエストに関連付けるシナリオについて説明します。次の手順に従って変更リクエストを作成し、変更ログイベントを関連付けます。

1. 変更リクエストの作成 （172 ページ）。
2. 外部システムのチケット名またはチケット番号を変更リクエストの名前に使用し、[説明（Description）] フィールドに変更の理由とその他の関連情報を追加します。
3. 新しい変更リクエストが変更リクエストツールバーに表示されることを確認します。
4. ファイアウォールデバイスを変更します。
5. ナビゲーションウィンドウで [変更ログ（Change Log）] をクリックし、新しい変更リクエストに関連付けられている変更ログイベントを見つけます。

6. 変更リクエストツールバーをクリアする （174 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

ファイアウォールデバイスの変更が行われた後、個々の変更ログイベントを手動で更新する

このユースケースでは、ファイアウォールデバイスの変更を行って外部システムで維持されているチケットを解決したものの、変更リクエスト管理機能を使用して変更リクエストを変更ログイベントに関連付けるのを忘れたというシナリオについて説明します。チケット番号を使用して変更ログイベントを更新します。変更リクエストを変更ログイベントに関連付けるには、次の手順に従います。

1. 変更リクエストの作成 （172 ページ）。変更リクエストの名前として、外部システムからのチケット名または番号を使用します。[説明（Description）] フィールドを使用して、変更の理由とその他の関連情報を追加します。
2. ナビゲーションウィンドウで [変更ログ（Change Log）] をクリックし、変更に関連付けられている変更ログイベントを検索します。
3. 変更リクエストと変更ログイベントの関連付け （172 ページ）。
4. 変更リクエストツールバーをクリアする （174 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

変更リクエストに関連付けられた変更ログイベントを検索する

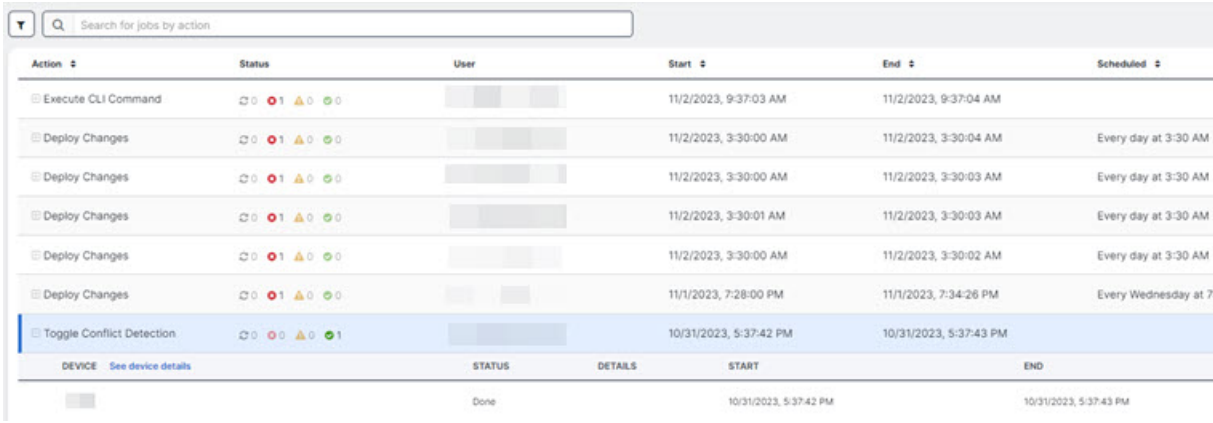
このユースケースでは、外部システムで維持されているチケットを解決するために行われた作業の結果として、どのような変更ログイベントが変更ログに記録されたかを知りたいというシナリオについて説明します。変更リクエストに関連付けられている変更ログイベントを検索するには、次の手順に従います。

1. ナビゲーションウィンドウで、[変更ログ（Change Log）] をクリックします。
2. 次のいずれかの方法を使用して、変更リクエストに関連付けられた変更ログイベントを検索します。
   - [変更ログ（Change Log）] 検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ログイベントを検索します。Security Cloud Control により、完全一致の変更ログイベントが強調表示されます。
   - フィルタ変更リクエスト （173 ページ） を実行して変更ログイベントを検索します。
3. 各変更ログを表示して、関連する変更リクエストを示す強調表示された変更ログイベントを見つけます。

Security Cloud Control でのジョブのモニタリング

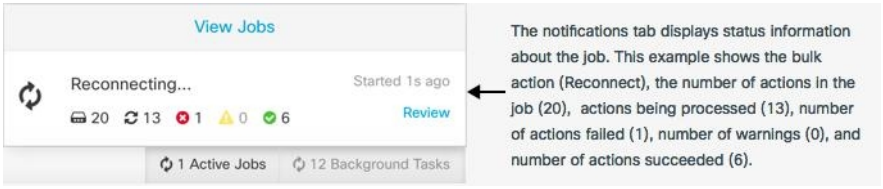
[ジョブ（Jobs）] ページには、一括操作（複数のデバイスの再接続、複数のデバイスからの設定の読み取り、複数のデバイスの同時アップグレードなど）の進捗状況の概要が表示されます。[ジョブ（Jobs）]テーブルでは、個々のアクションのステータスと合わせて色分けされた行が使用され、アクションが成功したか失敗したかを示します。

表の 1 行は、1 回の一括操作を表します。この 1 回の一括操作は、たとえば、20 台のデバイスを再接続する試みだった可能性があります。[ジョブ（Jobs）] ページの行を展開すると、一括操作の影響を受ける各デバイスの結果が表示されます。



[ジョブ（Jobs）] ページには、次の 2 つの方法でアクセスできます。

- [通知（Notification）] タブで、新しいジョブ通知があるときに、[確認（Review）] リンクをクリックします。[ジョブ（Jobs）] ページにリダイレクトされ、通知に対応する特定のジョブが表示されます。



- 左側のペインで **[イベントとログ（Events & Logs）]** > **[ジョブ（Jobs）]** をクリックします。この表には、Security Cloud Control で実行される一括操作の完全なリストが示されます。

Security Cloud Control でのジョブの検索

[ジョブ（Jobs）] ページでは、異なるアクション、アクションを実行したユーザー、アクションのステータスによってフィルタ処理および検索を実行できます。

一括アクションの再開

[ジョブ（Jobs）] ページを確認して、一括アクションの 1 つまたは複数のアクションの失敗が判明した場合は、必要な修正を行ってから一括アクションを再試行できます。Security Cloud Control は、失敗したアクションのみを対象にジョブを再度実行します。一括アクションを再度実行するには、次の手順に従います。

手順

ステップ 1 [ジョブ（Jobs）] ページで、アクションの失敗を示す行を選択します。

ステップ 2 [再試行（Retry）]（↻）アイコンをクリックします。

一括アクションのキャンセル

複数のデバイスで現在進行中の一括アクションをキャンセルできます。たとえば、4 台の管理対象デバイスを再接続しようとして、そのうち 3 台が正常に再接続されたが、4 台目のデバイスがまだ接続も切断もされていない場合は、一括アクションをキャンセルできます。

一括操作をキャンセルするには、次の手順を実行します。

手順

ステップ 1 左側のペインで **[イベントとログ（Events & Logs）]** > **[ジョブ（Jobs）]** をクリックします。

ステップ 2 実行中の一括アクションを特定し、右側にある [キャンセル（Cancel）] リンクをクリックします。

（注）
一括アクションの一部が成功している場合、それを元に戻すことはできません。進行中のアクションがキャンセルされます。

Security Cloud Control でのワークフローのモニタリング

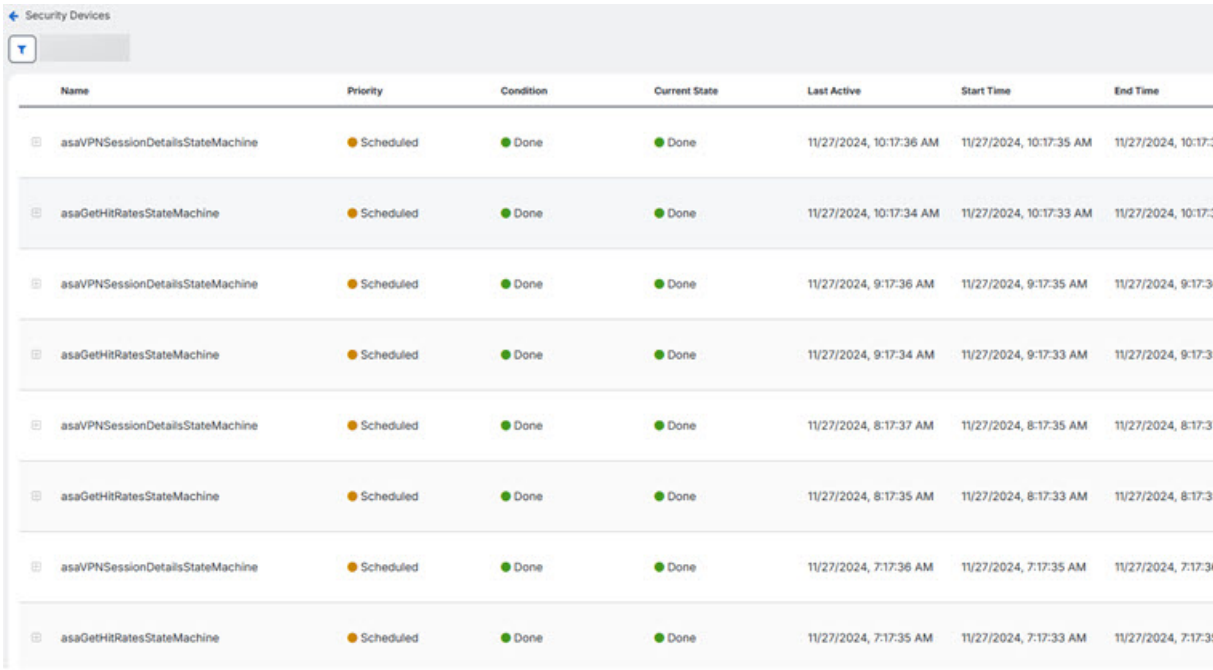
[ワークフロー（Workflows）] ページでは、デバイス、Secure Device Connector（SDC）、または Secure Event Connector（SEC）と通信するとき、およびルールセットの変更をデバイスに適用するときに、Security Cloud Control が実行するすべてのプロセスを監視できます。Security Cloud Control は、各ステップのワークフローテーブルにエントリを作成し、その結果をこのページに表示します。エントリには、Security Cloud Control によって実行されるアクションに

ついての情報のみが含まれており、CDO がデータをやり取りしているデバイスについての情報は含まれません。

Security Cloud Control は、デバイスでタスクの実行に失敗した場合にエラーを報告します。詳細については、[ワークフロー（Workflows）] ページに移動して、エラーが発生したステップを確認してください。

このページでは他にも必要に応じて、エラーの特定とトラブルシュートや TAC との情報共有ができます。

[ワークフロー（Workflows）] ページに移動するには、左側のペインの [セキュリティデバイス（Security Devices）] をクリックして、[デバイス（Devices）] タブをクリックします。適切なデバイスタイプタブをクリックしてデバイスを特定し、必要なデバイスを選択します。右側のペインの [デバイスとアクション（Devices and Actions）] で、[ワークフロー（Workflows）] をクリックします。次の図は、[ワークフロー（Workflows）] テーブルのエントリが表示された [ワークフロー（Workflows）] ページを示しています。



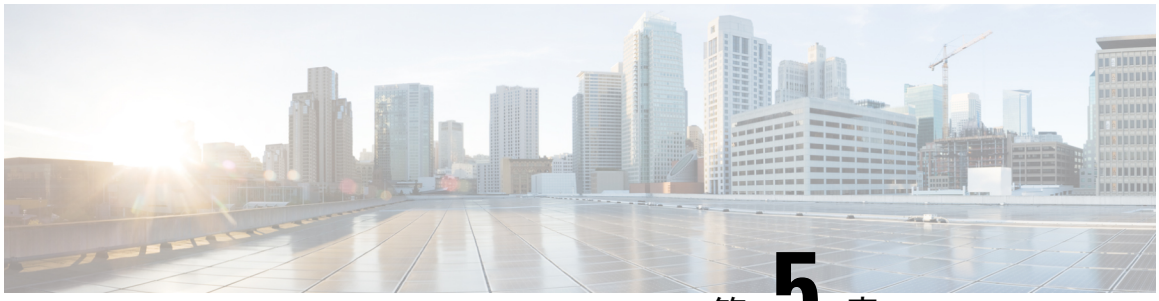
デバイスワークフローのエクスポート

完全なワークフロー情報を JSON ファイルにダウンロードして、TAC チームから詳細な分析情報を求められたときに提供できます。ワークフロー情報をエクスポートするには、該当するデバイスを選択してその [ワークフロー（Workflows）] ページに移動し、右上隅に表示されるエクスポート（ ）アイコンをクリックします。

スタックトレースのコピー

解決できないエラーがあって TAC に問い合わせた場合、TAC からスタックトレースのコピーを求められる場合があります。エラーのスタックトレースを収集するには、[スタックトレー

ス（Stack Trace）] リンクをクリックし、[スタックトレースのコピー（Copy Stacktrace）] をクリックして、画面に表示されるスタックをクリップボードにコピーします。



第 5 章

Terraform

Terraform について

Security Cloud Control のお客様は、Security Cloud Control Terraform プロバイダーと Security Cloud Control Terraform モジュールを使用して、繰り返し可能でバージョン管理されたコードを使用してテナントを迅速にセットアップできます。Security Cloud Control Terraform プロバイダーを使用すると、ユーザーは次のことができます。

- ユーザーの**管理**
- クラウド提供型 Firewall Management Center、Cisco Secure ASA デバイス、および iOS デバイスでの Secure Firewall Threat Defense デバイスの**オンボーディング**
- vSphere および AWS での Secure Device Connector の**オンボーディング**
- AWS での Secure Event Connector の**オンボーディング**

詳細については、以下のページを参照してください。

- Security Cloud Control Terraform プロバイダーのページ
- Security Cloud Control SDC モジュール（vSphere）のページ
- Security Cloud Control SDC モジュール（AWS）のページ
- Security Cloud Control SEC モジュール（AWS）のページ
- Devnet ラーニングラボでの学習
- 「Automating Security Infrastructure Management Using the Cisco Security Cloud Control Terraform Provider」：学習ラボ
- GitHub での Security Cloud Control 自動化の例

サポート

Security Cloud Control Terraform プロバイダーとモジュールは、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 の以下のリポジトリで問題を報告してください。

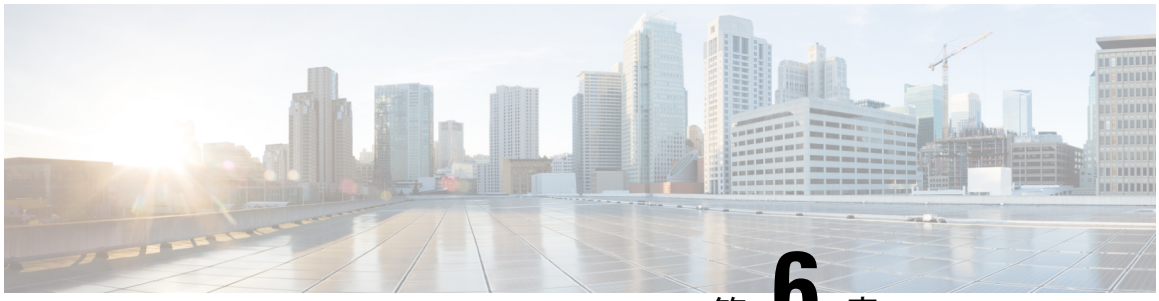
モジュール	リポジトリ
Security Cloud Control Terraform プロバイダー	https://github.com/ciscodevnet/terraform-provider-SecurityCloud Control
Security Cloud Control SDC モジュール（vSphere）	https://github.com/CiscoDevNet/terraform-vsphere-SecurityCloud Control-sdc
Security Cloud Control SDC モジュール（AWS）	https://github.com/CiscoDevNet/terraform-aws-SecurityCloud Control-sdc
Security Cloud Control SEC モジュール（AWS）	https://github.com/CiscoDevNet/terraform-aws-SecurityCloud Control-sec

リポジトリへの貢献

Security Cloud Control チームは、上記のリポジトリへの貢献を歓迎します。プロバイダーとモジュールの改善に貢献する場合は、これらの GitHub リポジトリでプルリクエストを作成してください。

関連項目

- Deploy an SDC to vSphere Using Terraform
- Deploy an SDC to AWS VPC Using Terraform
- Deploy an SEC to AWS VPC Using Terraform



第 6 章

トラブルシューティング

この章は、次のセクションで構成されています。

Secure Device Connector のトラブルシュート

オンプレミスの Secure Device Connector（SDC）のトラブルシューティングを行うには、以下のトピックを参照してください。

いずれのシナリオにも当てはまらない場合は、Security Cloud Control のお客様が TAC でサポートチケットを開く方法。

SDC に到達不能

Security Cloud Control からの 2 回のハートビート要求に連続して応答しなかった場合、SDC の状態は [到達不能（Unreachable）] になります。SDC に到達不能な場合、テナントは、オンボーディングしたどのデバイスとも通信できません。

Security Cloud Control は、次の方法で SDC に到達不能であることを示します。

- 「一部の Secure Device Connector（SDC）に到達できません。該当する SDC に関連付けられたデバイスとは通信できません（Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs）」というメッセージが Security Cloud Control のホームページに表示されます。
- [サービス（Services）] ページの SDC のステータスが [到達不能（Unreachable）] になります。

この問題を解決するには、まず SDC とテナントの再接続を試行してください。

1. SDC 仮想マシンが実行中で、地域の Security Cloud Control IP アドレスに到達できることを確認します。管理対象デバイスへの Security Cloud Control の接続 （14 ページ）を参照してください。

2. ハートビートを手動で要求して、Security Cloud Control と SDC の再接続を試行します。SDC がハートビート要求に応答すると、[アクティブ（Active）] ステータスに戻ります。ハートビートを手動で要求するには、次の手順に従います。
   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。
   2. 到達不能な SDC をクリックします。
   3. [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。
   4. [再接続（Reconnect）] をクリックします。
3. SDC を手動でテナントに再接続しようとしても、SDC が [アクティブ（Active）] ステータスに戻らない場合は、「展開後 Security Cloud Control で SDC ステータスが [アクティブ（Active）] にならない （184 ページ）」の指示に従ってください。

.

展開後Security Cloud ControlでSDCステータスが[アクティブ（Active）]にならない

展開して約 10 分たっても SDC がアクティブになったことを Security Cloud Control が示さない場合は、SDC の展開時に作成した `Security Cloud Control` ユーザーおよびパスワードにより、SSH を使用して SDC VM に接続します。

手順

ステップ 1 `/opt/cdo/configure.log` を確認します。ここには、入力した SDC の構成設定と、それらが正常に適用されたかどうかが示されます。セットアッププロセスでエラーが発生している場合または値が正しく入力されていない場合は、sdc-onboard setup を再度実行します。

a) プロンプトで、`sudo sdc-onboard setup` と入力します。
b) `cdo` ユーザーのパスワードを入力します。
c) プロンプトに従います。セットアップスクリプトの指示に従って、セットアップウィザードで行ったすべての設定手順を確認し、入力した値を変更することができます。

ステップ 2 ログを確認し、`sudo sdc-onboard setup` を実行しても、Security Cloud Control で SDC が [アクティブ（Active）] にならない場合は、Security Cloud Control サポートへの問い合わせ。

SDC の変更された IP アドレスが Security Cloud Control に反映されない

SDC の IP アドレスを変更した場合、GMT の午前 3 時以降まで変更は Security Cloud Control に反映されません。

デバイスと SDC の接続に関するトラブルシューティング

このツールを使用して、Secure Device Connector（SDC）を介した Security Cloud Control からデバイスへの接続をテストします。デバイスがオンボーディングに失敗した場合、またはオンボーディングの前に Security Cloud Control がデバイスに到達できるかどうかを判断する場合は、この接続をテストすることができます。

手順

ステップ 1 左側のペインで **[管理（Administration）]** > **[Firewall Management Center]** をクリックし、[セキュアコネクタ（Secure Connectors）] タブをクリックします。

ステップ 2 SDC を選択します。

ステップ 3 右側の [トラブルシューティング（Troubleshooting）] ペインで、[デバイスの接続（Device Connectivity）] をクリックします。

ステップ 4 トラブルシューティングまたは接続しようとしているデバイスの有効な IP アドレスまたは FQDN とポート番号を入力し、[実行（Go）] をクリックします。Security Cloud Control は次の検証を実行します。

a) [DNS解決（DNS Resolution）]：IP アドレスの代わりに FQDN を指定すると、SDC がドメイン名を解決でき、IP アドレスを取得できることを確認します。

b) [接続テスト（Connection Test）]：デバイスが到達可能であることを確認します。

c) [TLSサポート（TLS support）]：デバイスと SDC の両方がサポートする TLS バージョンと暗号を検出します。

- [サポートされていない暗号（Unsupported Cipher）]：デバイスと SDC の両方でサポートされている TLS バージョンがない場合、Security Cloud Control は、SDC ではなくデバイスでサポートされている TLS バージョンと暗号についてもテストします。

d) SSL 証明書：トラブルシューティングでは、証明書情報が提供されます。

ステップ 5 デバイスのオンボーディングまたはデバイスへの接続の問題が解消しない場合は、Security Cloud Control サポートへの問い合わせ。

SDC との断続的な接続または接続がない

このセクションで説明するソリューションは、オンプレミスの Secure Device Connector（SDC）にのみ適用されます。

症状：SDC との断続的な接続または接続がない。

診断：この問題は、ディスク領域がほぼいっぱい（80%以上）の場合に発生する可能性があります。

次の手順を実行して、ディスク容量の使用状況を確認します。

1. Secure Device Connector（SDC）VM のコンソールを開きます。
2. ユーザー名 **cdo** でログインします。
3. 初回ログイン時に作成したパスワードを入力します。
4. まず、**df -h**と入力して空きディスク容量をチェックし、空きディスク容量がないことを確認します。

   Dockerによってディスク容量が消費されたことを確認できます。通常のディスク使用量は 2 ギガバイト未満であると予想されます。
5. **Docker** フォルダーのディスク使用量を表示するには、

   sudo du -h /var/lib/docker | sort -h を実行します。

   Docker フォルダーのディスク使用量を確認できます。

手順

Dockerフォルダーのディスク使用量がほぼいっぱいの場合は、docker設定ファイルで次のように定義します。

- Max-size：現在のファイルが最大サイズに達したら、ログローテーションを強制します。
- Max-file：上限に達したら、ローテーションされた余分なログファイルを削除します。

次の手順を実行します。

1. **sudo vi /etc/docker/daemon.json** を実行します。
2. 次の行をファイルに挿入します。

   ```
   {
   "log-driver": "json-file",
   "log-opts": {"max-size": "100m", "max-file": "5" }
   }
   ```
3. **Esc** キーを押してから **:wq!** と入力し、変更を書き込んでファイルを閉じます。

（注） **sudo cat /etc/docker/daemon.json** を実行して、ファイルに加えられた変更を確認できます。

4. **sudo systemctl restart docker** を実行して docker ファイルを再起動します。

   変更が適用されるまでに数分かかる場合があります。**sudo du -h /var/lib/docker | sort -h** を実行して、docker フォルダーの更新されたディスク使用量を表示します。
5. **df -h** を実行して、空きディスクサイズが増加したことを確認します。

6. SDC のステータスを [到達不能（Unreachable）] から [アクティブ（Active）] に変更する前に、**[管理（Administration）]** > **[Firewall Management Center]** から [セキュアコネクタ（Secure Connectors）] タブに移動して、[アクション（Actions）] メニューから [再接続の要求（Request Reconnect）] をクリックする必要があります。

Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性：cisco-sa-20190215-runc

Cisco Product Security Incident Response Team（PSIRT）は、Docker のシビラティ（重大度）の高い脆弱性について説明するセキュリティアドバイザリ **cisco-sa-20190215-runc** を公開しました。脆弱性の完全な説明については、PSIRT チームのアドバイザリ全体をお読みください。

この脆弱性は、すべての Security Cloud Control ユーザーに影響します。

- Security Cloud Control のクラウド展開された Secure Device Connector（SDC）を使用しているお客様は、修復手順が Security Cloud Control オペレーションズチームによってすでに実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。アップグレードするには、次の手順を使用します。
  - Security Cloud Control 標準の SDC ホストの更新 （187 ページ）
  - カスタム SDC ホストを更新する （188 ページ）
  - バグトラッキング （188 ページ）

Security Cloud Control 標準の SDC ホストの更新

Security Cloud Control の VM イメージを使用した Secure Device Connector の展開した場合は、次の手順を使用します。

手順

ステップ 1 SSH またはハイパーバイザコンソールを使用して SDC ホストに接続します。

ステップ 2 次のコマンドを実行して、Docker サービスのバージョンを確認します。

```
docker version
```

ステップ 3 最新の仮想マシン（VM）のいずれかを実行している場合、次のような出力が表示されます。

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
```

```
 OS/Arch: linux/amd64
 Experimental: false
```

ここで古いバージョンが表示される可能性があります。

ステップ 4 次のコマンドを実行して Docker を更新し、サービスを再起動します。

```
> sudo yum update docker-ce
> sudo service docker restart
```

（注）
Docker サービスの再起動中、Security Cloud Control とデバイス間の接続が短時間停止します。

ステップ 5 docker version コマンドを再度実行します。次の出力が表示されます。

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

ステップ 6 これで追加されました。パッチが適用された最新バージョンの Docker にアップグレードされました。

カスタム SDC ホストを更新する

独自の SDC ホストを作成している場合は、Docker のインストール方法に基づいた更新手順に従う必要があります。CentOS、yum、Docker-ce（コミュニティ版）を使用した場合は、前述の手順で動作します。

Docker-ee（エンタープライズ版）をインストールした場合、または別の方法を使用して Docker をインストールした場合は、Docker の修正バージョンが異なる場合があります。正しいインストールバージョンは、Docker のページ（Docker Security Update and Container Security Best Practices）で確認できます。

バグトラッキング

シスコでは、この脆弱性を引き続き評価し、追加情報が利用可能になり次第、アドバイザリを更新します。アドバイザリが最終とマークされたら、次の関連する Cisco バグを参照して詳細を確認できます。

CSCvo33929-CVE-2019-5736：runC コンテナのブレークアウト

無効なシステム時刻

Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。

（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

Security Cloud Control のオペレーションズチームが SDC を移行しようとしましたが、SDC システム時刻が AWS システム時刻より 15 分進んでいるか遅れていたため、移行できませんでした。

システム時刻の問題を修正するには、以下の手順に従ってください。この問題が解決したら、移行を続行できます。

手順

ステップ 1 VM 端末を介して、または SSH 接続を確立して、SDC VM にログインします。

ステップ 2 プロンプトに `sudo sdc-onboard setup` と入力して、認証を行います。

ステップ 3 SDC の初回セットアップ時と同様に、SDC セットアップに関する質問に回答します。以前と同じパスワードとネットワーク情報をすべて再入力します。このとき、NTP サーバーアドレスをメモしておきます。

a) SDC のセットアップに使用したものと同じパスワードを使用して、ルートおよび Security Cloud Control ユーザーのパスワードをリセットします。
b) プロンプトが表示されたら、**y** と入力してネットワークを再設定します。
c) 以前と同じ IP アドレスまたは CIDR の値を入力します。
d) 以前と同じネットワークゲートウェイの値を入力します。
e) 以前と同じドメインネームシステム（DNS）サーバーの値を入力します。
f) NTP サーバーの入力を求められたら、有効な NTP サーバーアドレス（`time.aws.com`など）を入力してください。
g) 入力した値を確認し、間違いなければ **y** と入力します。

ステップ 4 プロンプトに `date` と入力して、時刻サーバーが到達可能か、SDC と同期しているかを検証します。日時（UTC）が表示され、SDC の時刻と比較できます。

次のタスク

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center（TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが SDC の新通信方式への移行を完了できます。

SDC のバージョンが 202311**** より前

Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。

（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

Security Cloud Control のオペレーションズチームは SDC を移行しようとしましたが、テナントが 202311**** よりも前のバージョンを実行しているため失敗しました。

SDC の現在のバージョンは、Security Cloud Control のメニューバーから**[ツールとサービス（Tools & Services）]** > **[セキュアコネクタ（Secure Connectors）]**の順に移動して、[セキュアコネクタ（Secure Connectors）] ページに記載されています。SDC を選択すると、画面右側の [詳細（Details）] ペインにバージョン番号が表示されます。

SDCバージョンをアップグレードするには、次の手順に従ってください。この問題が解決したら、Security Cloud Control オペレーションズチームが移行プロセスを再度実行できるようになります。

手順

ステップ 1 SDC VM にログインし、認証を行います。

ステップ 2 プロンプトに `sudo su - sdc` と入力して、認証を行います。

ステップ 3 プロンプトに `crontab -r` と入力します。

`no crontab for sdc` というメッセージが表示された場合、無視して次の手順に進めます。

ステップ 4 プロンプトに `./toolkit/toolkit.sh upgrade` と入力します。Security Cloud Control は、アップグレードが必要かどうかを判断し、ツールキットをアップグレードします。コンソールでエラーが報告されていないことを確認します。

ステップ 5 SDC の新しいバージョンを確認します。

a) Security Cloud Control にログインします。

b) Security Cloud Control のメニューバーから**[ツールとサービス（Tools & Services）]** > **[セキュアコネクタ（Secure Connectors）]**の順に移動して、[セキュアコネクタ（Secure Connectors）] ページを開きます。

c) SDC を選択して、[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。

d) SDC のバージョンが 202311**** 以降であることを検証します。

次のタスク

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center（TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが移行プロセスを再度実行できます。

AWS サーバーの証明書または接続エラー

Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。

（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

Security Cloud Control のオペレーションズチームが SDC を移行しようとしましたが、接続の問題が発生したため失敗しました。

接続の問題を修正するには、次の手順に従ってください。この問題が解決したら、移行を続行できます。

手順

ステップ 1 ポート 443 で、リージョン内のドメインへのアウトバウンドプロキシ接続を許可するファイアウォールルールを作成します。

- オーストラリアリージョンの実稼働テナント：
  - cognito-identity.ap-southeast-2.amazonaws.com
  - cognito-idp.ap-southeast-2.amazonaws.com
  - sns.ap-southeast-2.amazonaws.com
  - sqs.ap-southeast-2.amazonaws.com
- インドリージョンの実稼働テナント：
  - cognito-identity.ap-south-1.amazonaws.com
  - cognito-idp.ap-south-1.amazonaws.com
  - sns.ap-south-1.amazonaws.com
  - sqs.ap-south-1.amazonaws.com
- 米国リージョンの実稼働テナント：
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- EU リージョンの実稼働テナント：

- cognito-identity.eu-central-1.amazonaws.com
- cognito-idp.eu-central-1.amazonaws.com
- sns.eu-central-1.amazonaws.com
- sqs.eu-central-1.amazonaws.com

- APJ リージョンの実稼働テナント：
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

ステップ 2 次のいずれかのコマンドを使用して、ファイアウォールの「許可リスト」に追加する必要がある IP アドレスの全リストを確認できます。

（注）
次のコマンドは、**jq** がインストールされているユーザー向けです。IP アドレスが 1 つのリストに表示されます。

- 米国リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
 (.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- EU リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
 (.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- APJ リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
 (.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

（注）
jq がインストールされていない場合は、次の短縮バージョンのコマンドを使用できます。

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

次のタスク

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center（TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが SDC の新通信方式への移行を完了できます。

Security Cloud Control のトラブルシューティング

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 （6 ページ）を参照してください。

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。

アクセスと証明書のトラブルシューティング

新規フィンガープリント検出ステータスの解決

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] タブをクリックします。

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 [新しいフィンガープリントを検出（New Fingerprint Detected）] ステータスのデバイスを選択します。

ステップ 5 [新しい指紋が検出されました（New Fingerprint Detected）] ペインで [フィンガープリントの確認（Review Fingerprint）] をクリックします。

ステップ 6 フィンガープリントを確認して許可するように求められたら、以下の手順を実行します。

1. [フィンガープリントのダウンロード（Download Fingerprint）] をクリックして確認します。
2. フィンガープリントに問題がなければ [許可（Accept）] をクリックします。 問題がある場合は、[キャンセル（Cancel）] をクリックします。

ステップ 7 新しいフィンガープリントの問題を解決した後、デバイスの接続状態が [オンライン（Online）] と表示され、構成ステータスが「非同期（Not Synced）」または「競合検出（Conflict Detected）」と表示される場合があります。[構成の競合の解決（Resolve Configuration Conflicts）]設定の競合の解決 （162 ページ） を確認し、Security Cloud Control とデバイス間の構成の差異を確認して解決します。

SecurityandAnalyticsLoggingイベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題にトラブルシューティングを実行するための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユー

ザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているか把握しています。

（注） このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FDM による管理デバイスであることも想定しています。Security Analytics and Logging は、他のデバイスタイプからログ情報を収集しません。

手順

ステップ 1 左側のペインで **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** をクリックします。

ステップ 2 [履歴（Historic）] タブをクリックします。

ステップ 3 [時間範囲（Time Range）] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴（Historical）] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了（End）] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。

ステップ 4 [センサーID（Sensor ID）] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで**属性:値**のペアを使用してイベントをフィルタ処理します。2つのエントリを作成し、それらを OR ステートメントで結合します。例: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

ステップ 5 イベントフィルタバーの [ソースIP（Source IP）] フィールドにユーザーの IP アドレスを入力します。

ステップ 6 ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [宛先IP（Destination IP）] フィールドに入力します。

ステップ 7 結果に表示されるイベントを展開し、その詳細を確認します。以下の詳細に注意してください。

- **AC_RuleAction** - ルールがトリガーされたときに実行されたアクション（許可、信頼、ブロック）。
- **FirewallPolicy** - イベントをトリガーしたルールが存在するポリシー。
- **FirewallRule** - イベントをトリガーしたルールの名前。値が Default Action の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
- **UserName** - イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスはソース IP アドレスと同じです。

ステップ 8 ルールのアクションがアクセスをブロックしている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシーのルールを特定します。

SSL 暗号解読の問題のトラブルシューティング

復号再署名がブラウザでは機能するがアプリでは機能しないWebサイトの処理（SSLまたは認証局ピニング）

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL（または認証局）ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバー証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense デバイスから受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Web サイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Web ブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で https://www.facebook.com を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

詳細の表示

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション（Facebook など）は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラート メッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - `SSL フロー フラグには ALERT_SEEN が含まれます。`
  - `SSL フロー フラグには APP_DATA_C2S または APP_DATA_S2C は含まれません。`
  - `SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE です。`
- グループ 2 のアプリケーション（Dropbox など）はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
  - `SSL フロー フラグには ALERT_SEEN、APP_DATA_C2S または APP_DATA_S2C は含まれません。`

- SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED です。

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。

オブジェクトのトラブルシューティング

重複オブジェクトの問題の解決

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誤って作成され、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。重複オブジェクトの問題を解決した後、Security Cloud Control は、残されたオブジェクト名に対する、影響を受けるすべてのオブジェクト参照を更新します。

重複オブジェクトの問題を解決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、[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 次に、オブジェクトをオブジェクトフィルタして、重複するオブジェクトの問題を見つけます。

ステップ 3 結果の中から 1 つを選択します。オブジェクトの詳細パネルに、該当する重複の数を示す [重複（DUPLICATE）] フィールドが表示されます。

ステップ 4 [解決（Resolve）] をクリックします。Security Cloud Control は、重複オブジェクトを比較できるように表示します。

ステップ 5 比較するオブジェクトを 2 つ選択します。

ステップ 6 以下のオプションがあります。

- オブジェクトの 1 つを別のオブジェクトに置き換える場合は、保持するオブジェクトで [選択（Pick）] をクリックし、[解決（Resolve）] をクリックして影響を受けるデバイスとネットワークポリシーを確認し、変更に問題がなければ [確認（Confirm）] をクリックします。Security Cloud Control は、選択したオブジェクトに置き換えて保持し、重複を削除します。
- リストにあるオブジェクトを無視する場合は、[無視（Ignore）] をクリックします。オブジェクトを無視すると、Security Cloud Control が表示する重複オブジェクトのリストから削除されます。
- オブジェクトを保持するものの、重複オブジェクトの検索で Security Cloud Control に表示してほしくない場合は、[すべて無視（Ignore All）] をクリックします。

ステップ 7 重複オブジェクトの問題が解決したら、行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、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問題の解決

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。

関連情報：

- デバイスとサービスのリストのエクスポート （104 ページ）
- Security Cloud Control へのデバイス一括再接続 （108 ページ）

未使用オブジェクトの問題の解決

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 次に、オブジェクトをオブジェクトフィルタして、未使用オブジェクトの問題を見つけます。

ステップ 3 1 つ以上の未使用のオブジェクトを選択します。

ステップ 4 以下のオプションがあります。

- 操作ウィンドウで [削除（Remove）] をクリックして、未使用のオブジェクトを Security Cloud Control から削除します。
- [問題（Issues）]ペインで、[無視（Ignore）]をクリックします。 オブジェクトを無視すると、Security Cloud Control は未使用のオブジェクトの結果にそのオブジェクトを表示しなくなります。

ステップ 5 未使用のオブジェクトを削除した場合は、行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開 （152 ページ）か、待機してから複数の変更を一度に展開します。

（注）
未使用のオブジェクトの問題を一括で解決するには、「オブジェクトの問題を一度に解決する」を参照してください。

未使用オブジェクトの一括削除

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 次に、オブジェクトをオブジェクトフィルタして、未使用オブジェクトの問題を見つけます。

ステップ 3 削除する未使用のオブジェクトを選択します。

- ページ上のすべてのオブジェクトを選択するには、オブジェクトテーブルのヘッダー行にあるチェックボックスをクリックします。

- オブジェクトテーブルで未使用のオブジェクトを個別に選択します。

ステップ 4 右側の [アクション（Actions）] ペインで [削除（Remove）] をクリックして、Security Cloud Control で選択した未使用のオブジェクトをすべて削除します。99 個のオブジェクトを同時に削除できます。

ステップ 5 [OK] をクリックして、未使用のオブジェクトを削除することを確認します。

ステップ 6 これらの変更の展開には、つぎの 2 つの方法があります。

- 行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。
- [インベントリ]ページを開き、変更の影響を受けたデバイスを特定します。変更の影響を受けるすべてのデバイスを選択し、[管理（Management）] ペインで [すべて展開（Deploy All）] をクリックします。警告を読み、適切なアクションを実行します。

不整合オブジェクトの問題を解決する

不整合オブジェクト INCONSISTENT 2 Resolve | Ignore 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。ユーザーが異なる構成の中で、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。

注：不整合オブジェクトの問題を一括で解決するには、「オブジェクトの問題を一度に解決する」を参照してください。

不整合オブジェクトに対して次のことを実行できます。

- [無視（Ignore）]：Security Cloud Control は、オブジェクト間の不整合を無視し、それらの値を保持します。このオブジェクトは、不整合カテゴリに表示されなくなります。
- [マージ（Merge）]：Security Cloud Control は、選択されているすべてのオブジェクトとその値を 1 つのオブジェクトグループに結合します。
- [名前の変更（Rename）]：Security Cloud Control で、不整合オブジェクトの 1 つの名前を変更し、新しい名前を付けることができます。
- [共有ネットワークオブジェクトのオーバーライドへの変換（Convert Shared Network Objects to Overrides）]：Security Cloud Control で、不整合のある共有オブジェクトを（オーバーライドの有無にかかわらず）、オーバーライドのある単一の共有オブジェクトに結合できます。不整合オブジェクトの最も一般的なデフォルト値が、新しく形成されるオブジェクトのデフォルトとして設定されます。

（注） 共通のデフォルト値が複数ある場合は、そのうちの一つがデフォルトとして選択されます。残りのデフォルト値とオーバーライド値は、そのオブジェクトのオーバーライドとして設定されます。

- [共有ネットワークグループの追加の値への変換（Convert Shared Network Group to Additional Values）]：Security Cloud Control で、不整合のある共有ネットワークグループを、追加の値のある単一の共有ネットワークグループに結合できます。この機能の基準は、「変換される不整合ネットワークグループに、同じ値を持つ少なくとも 1 つの共通オブジェクトが必要である」というものです。この基準に一致するすべてのデフォルト値がデフォルト値になり、残りのオブジェクトは、新しく形成されるネットワークグループの追加の値として割り当てられます。

  たとえば、不整合のある 2 つの共有ネットワークグループがあるとします。1 つ目のネットワークグループ「shared_network_group」は、「object_1」（192.0.2.x）と「object_2」（192.0.2.y）で形成されています。また、追加の値「object_3」（192.0.2.a）も含まれています。2つ目のネットワークグループ「shared_network_group」は、「object_1」（192.0.2.x）と追加の値「object_4」（192.0.2.b）で形成されます。共有ネットワークグループを追加の値に変換すると、新しく形成されるグループ「shared_network_group」には、デフォルト値として「object_1」（192.0.2.x）と「object_2」（192.0.2.y）が含まれ、追加の値として「object_3」（192.0. 2.a）と「object_4」（192.0.2.b）が含まれます。

（注） 新しいネットワークオブジェクトを作成すると、Security Cloud Control は、その値を同じ名前の既存の共有ネットワークオブジェクトへのオーバーライドとして自動的に割り当てます。これは、新しいデバイスが Security Cloud Control にオンボードされる場合にも当てはまります。

自動割り当ては、次の条件が満たされている場合にのみ発生します。

1. 新しいネットワークオブジェクトがデバイスに割り当てられる必要があります。
2. テナントには、同じ名前とタイプの共有オブジェクトが 1 つだけ存在する必要があります。
3. 共有オブジェクトには、すでにオーバーライドが含まれている必要があります。

不整合オブジェクトの問題を解決するには、次の手順を実行します。

手順

ステップ 1 左側の Security Cloud Control ナビゲーションバーで、[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 次に、オブジェクトをオブジェクトフィルタして、不整合オブジェクトの問題を見つけます。

ステップ 3 不整合オブジェクトを選択します。オブジェクトの詳細パネルに、該当するオブジェクトの数を示す [不整合（INCONSISTENT）] フィールドが表示されます。

ステップ 4 [解決（Resolve）] をクリックします。Security Cloud Control は、不整合オブジェクトを比較できるように表示します。

ステップ 5 以下のオプションがあります。

- **[すべて無視（Ignore All）]**：
  1. 提示されるオブジェクトを比較し、いずれかのオブジェクトで [無視（Ignore）] をクリックします。または、すべてのオブジェクトを無視するために、[すべて無視（Ignore All）] をクリックします。
  2. [OK] をクリックして確認します。
- **[オブジェクトをマージして解決（Resolve by merging objects）]**：
  1. [X つのオブジェクトをマージして解決（Resolve by Merging X Objects）] をクリックします。
  2. [確認（Confirm）] をクリックします。
- **[名前の変更（Rename）]**：
  1. [名前の変更（Rename）] をクリックします。
  2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認（Confirm）] をクリックします。
- **[オーバーライドへの変換（Convert to Overrides）]（不整合のある共有オブジェクトの場合）**：共有オブジェクトをオーバーライドと比較する場合、比較パネルには、[不整合のある値（Inconsistent Values）] フィールドのデフォルト値のみが表示されます。
  1. [オーバーライドへの変換（Convert to Overrides）] をクリックします。すべての不整合オブジェクトは、オーバーライドを持つ単一の共有オブジェクトに変換されます。
  2. [確認（Confirm）] をクリックします。[共有オブジェクトの編集（Edit Shared Object）] をクリックすると、新しく形成されたオブジェクトの詳細が表示されます。上向き矢印と下向き矢印を使用して、デフォルトとオーバーライドの間で値を移動することができます。
- **[追加の値への変換（Convert to Additional Values）]（不整合のあるネットワークグループの場合）**：
  1. [追加の値への変換（Convert to Additional Values）] をクリックします。すべての不整合オブジェクトは、追加の値を持つ単一の共有オブジェクトに変換されます。
  2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認（Confirm）] をクリックします。

ステップ 6 不整合を解決したら、行った変更を今すぐすべてのデバイスの設定変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

オブジェクトの問題を一度に解決する

未使用オブジェクトの問題の解決、重複オブジェクトの問題の解決、不整合オブジェクトの問題を解決する （200 ページ）の問題のある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。オブジェクトに複数の問題がある場合でも、複数のオブジェクトを選択して無視できます。たとえば、オブジェクトに一貫性がなく、さらに未使用の場合、一度に無視できる問題タイプは 1 つだけです。

重要 後でオブジェクトが別の問題タイプに関連付けられた場合も、実行した無視アクションは、その時に選択した問題にのみ影響します。たとえば、重複していたためにオブジェクトを無視し、後でそのオブジェクトが不整合としてマークされた場合、そのオブジェクトを重複オブジェクトとして無視しても、不整合のオブジェクトとして無視されるわけではありません。

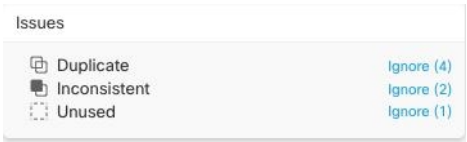
問題を一括で無視するには、以下の手順に従ってください。

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 検索を絞り込むために、オブジェクトの問題をオブジェクトフィルタできます。

ステップ 3 オブジェクトテーブルで、無視するオブジェクトをすべて選択します。問題ペインでは、問題タイプごとにオブジェクトがグループ化されます。



ステップ 4 [無視（Ignore）] をクリックして、問題をタイプごとに無視します。各問題をタイプごとに**無視**する必要があります。

ステップ 5 [OK] をクリックして、それらのオブジェクトを無視することを確認します。

デバイスの接続状態

Security Cloud Control テナントにオンボードされたデバイスの接続状態を表示できます。このトピックは、さまざまな接続状態を理解するのに役立ちます。[インベントリ] ページの [接続] 列に、デバイスの接続状態が表示されます。

デバイスの接続状態が「オンライン」の場合、デバイスの電源がオンになっていて、Security Cloud Control に接続されていることを意味します。以下の表に記載されているその他の状態は、通常、さまざまな理由でデバイスに問題が発生した場合になります。この表は、このような問題から回復する方法を示しています。接続障害の原因となっている問題が複数ある可能性

があります。再接続を試みると、Security Cloud Control は、再接続を実行する前に、まずこれらの問題をすべて解決するように求めます。

デバイスの接続状態	考えられる原因	解像度
オンライン（Online）	デバイスの電源が入っていて、Security Cloud Control に接続されています。	NA
オフライン	デバイスの電源が切れているか、ネットワーク接続が失われています。	デバイスがオフラインかどうかを確認します。
Insufficient licenses	デバイスに十分なライセンスがありません。	ライセンス不足のトラブルシュート （204 ページ）
クレデンシャルが無効である	Security Cloud Control がデバイスに接続するために使用するユーザー名とパスワードの組み合わせが正しくありません。	無効なログイン情報のトラブルシューティング （205 ページ）
オンボーディング	デバイスのオンボーディングが開始されましたが、完了していません。	デバイスの接続を確認し、デバイスの登録を完了させてください。
New Certificate Detected	このデバイスの証明書が変更されました。デバイスが自己署名証明書を使用している場合、これはデバイスの電源を再投入したために発生した可能性があります。	新規証明書の問題のトラブルシュート （206 ページ）
オンボーディングエラー	Security Cloud Control がオンボーディング時にデバイスとの接続を失った可能性があります。	オンボーディングエラーのトラブルシュート （215 ページ）

ライセンス不足のトラブルシュート

デバイスの接続ステータスに[ライセンスが不足しています（Insufficient License）]と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。

- デバイスのステータスが変わらない場合は、Security Cloud Control からサインアウトしてから再度サインインすることで Security Cloud Control ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の不具合を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。

手順

ステップ 1 Cisco Smart Software Manager から新しいトークンを生成し、コピーします。詳細については、スマートライセンスの生成に関するビデオをご覧ください。

ステップ 2 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 3 [デバイス] タブをクリックします。

ステップ 4 適切なデバイスタイプのタブをクリックし、ステータスが [ライセンスが不足しています（Insufficient License）] のデバイスを選択します。

ステップ 5 [デバイスの詳細（Device Details）] ペインで、[ライセンスが不足しています（Insufficient License）] に表示される [ライセンスの管理（Manage Licenses）] をクリックします。[ライセンスの管理（Manage Licenses）] ウィンドウが表示されます。

ステップ 6 [アクティブ化（Activate）] フィールドで、新しいトークンを貼り付けて [デバイスの登録（Register Device）] をクリックします。

トークンがデバイスに正常に適用されると、接続状態が [オンライン（Online）] に変わります。

無効なログイン情報のトラブルシューティング

無効なログイン情報によるデバイスの切断を解決するには、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] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、ステータスが [無効なログイン情報（Invalid Credentials）] のデバイスを選択します。

ステップ 4 [デバイスの詳細（Device Details）] ペインで、[無効なログイン情報（Invalid Credentials）] に表示される [再接続（Reconnect）] をクリックします。Security Cloud Control は、デバイスとの再接続を試みます。

ステップ 5 デバイスの新しいユーザー名とパスワードの入力を求められたら、

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 デバイスがオンラインになり、使用できる状態となったら、[閉じる（Close）] をクリックします。

ステップ 8 Security Cloud Control がデバイスへの接続に誤った間違ったログイン情報を使用しようとしたため、デバイスへの接続に Security Cloud Control が使用するユーザー名とパスワードの組み合わせが、デバイス上で直接変更された可能性があります。デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました（Conflict Detected）] であることがわかります。[構成の競合の解決（Resolve Configuration Conflicts）] を使用して、Security Cloud Control とデバイス間の構成の差異を確認して解決します。設定の競合の解決 （162 ページ）

新規証明書の問題のトラブルシュート

Security Cloud Control の証明書の使用

Security Cloud Control は、デバイスに接続するときに証明書の有効性をチェックします。具体的には、Security Cloud Control は次のことを要求します。

1. デバイスで TLS バージョン 1.0 以降を使用している。
2. デバイスにより提示される証明書が有効期限内であり、発効日が過去の日付である（すなわち、すでに有効になっており、後日に有効化されるようにスケジュールされていない）。
3. 証明書は、SHA-256 証明書であること。SHA-1 証明書は受け入れられません。
4. 次のいずれかが該当すること。
   - デバイスは自己署名証明書を使用し、その証明書は認可されたユーザーにより信頼された最新の証明書と同じである。
   - デバイスは、信頼できる認証局（CA）が署名した証明書を使用し、提示されたリーフ証明書から関連 CA にリンクしている証明書チェーンを形成している。

これらは、ブラウザとは異なる Security Cloud Control の証明書の使用方法です。

- 自己署名証明書の場合、Security Cloud Control は、デバイスのオンボーディングまたは再接続時に、ドメイン名チェックを無効にして、代わりに、その証明書が承認ユーザーによって信頼された証明書と完全に一致することをチェックします。
- Security Cloud Control は、まだ内部 CA をサポートしていません。現時点では、内部 CA によって署名された証明書をチェックする方法はありません。

  ASA デバイスの証明書チェックを、デバイスごとに無効にすることができます。ASA の証明書を Security Cloud Control が信頼できない場合、そのデバイスの証明書チェックを無効にするオプションがあります。デバイスの証明書チェックの無効化を試みても依然としてデバイスをオンボードできない場合は、デバイスに関して指定した IP アドレスおよびポートが正しくないか到達可能ではない可能性があります。証明書チェックをグローバルに無効にする方法、またはサポートされている証明書を持つデバイスの証明書チェックを

無効にする方法はありません。非 ASA デバイスの証明書チェックを無効にする方法はありません。

デバイスの証明書チェックを無効にしても、Security Cloud Control は、引き続き TLS を使用してデバイスに接続しますが、接続の確立に使用される証明書を検証しません。つまり、パッシブ中間者攻撃者は接続を盗聴できませんが、アクティブ中間攻撃者は、無効な証明書を Security Cloud Control に提供することによって、接続を傍受する可能性があります。

証明書の問題の特定

いくつかの理由で Security Cloud Control がデバイスをオンボードできない場合があります。UI に「Security Cloud Control は、提示された証明書を使用してデバイスに接続できません（CDO cannot connect to the device using the certificate presented）」というメッセージが表示される場合は、証明書に問題があります。このメッセージが UI に表示されない場合は、問題が接続の問題(デバイスに到達できない)またはその他のネットワークエラーに関連している可能性が高くなります。

Security Cloud Control が特定の証明書を拒否する理由を判断するには、SDC ホスト、または関連デバイスに到達できる別のホストで、openssl コマンドラインツールを使用します。次のコマンドを使用して、デバイスによって提示された証明書を示すファイルを作成します。

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

このコマンドでは、対話型セッションが開始されるため、数秒後に Ctrl+C キーを押して終了する必要があります。

次のような出力を含むファイルが作成されます。

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
```

```
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

この出力では、最初に、**確認リターン（verify return）コード**が示されている最後の行に注目してください。証明書に関する問題が存在する場合、このリターンコードはゼロ以外になり、エラーの説明が表示されます。

この証明書エラーコードのリストを展開して、一般的なエラーとその修正方法を確認してください。

0 X509_V_OK：操作が成功しました。

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT：信頼できない証明書の発行者証明書が見つかりませんでした。

3 X509_V_ERR_UNABLE_TO_GET_CRL：証明書の CRL が見つかりませんでした。

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE：証明書の署名を復号できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。これは、RSA キーについてのみ意味を持ちます。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE：CRL の署名を復号できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。未使用。

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY：証明書 SubjectPublicKeyInfo の公開キーを読み取れませんでした。

7 X509_V_ERR_CERT_SIGNATURE_FAILURE：証明書の署名が無効です。

8 X509_V_ERR_CRL_SIGNATURE_FAILURE：証明書の署名が無効です。

9 X509_V_ERR_CERT_NOT_YET_VALID：証明書がまだ有効ではありません（notBefore の日付が現在時刻より後です）。詳細については、この後の「確認リターンコード：9（証明書がまだ有効ではありません）」を参照してください。

10 X509_V_ERR_CERT_HAS_EXPIRED：証明書の有効期限が切れています（notAfter の日付が現在時刻より前です）。詳細については、この後の「確認リターンコード：10（証明書の有効期限が切れています）」を参照してください。

11 X509_V_ERR_CRL_NOT_YET_VALID：CRL がまだ有効ではありません。

12 X509_V_ERR_CRL_HAS_EXPIRED：CRL の有効期限が切れています。

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD：証明書の notBefore フィールドに無効な時刻が含まれています。

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD：証明書の notAfter フィールドに無効な時刻が含まれています。

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD：CRL の lastUpdate フィールドに無効な時刻が含まれています。

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD：CRL の nextUpdate フィールドに無効な時刻が含まれています。

17 X509_V_ERR_OUT_OF_MEM：メモリを割り当てようとしてエラーが発生しました。これは決して発生しないはずの問題です。

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT：渡された証明書は自己署名済みであり、信頼できる証明書のリストに同じ証明書が見つかりません。

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN：信頼できない証明書を使用して証明書チェーンを構築できましたが、ルートがローカルで見つかりませんでした。

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY：ローカルでルックアップされた証明書の発行者証明書が見つかりませんでした。これは、通常、信頼できる証明書のリストが完全ではないことを意味します。

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE：チェーンに証明書が 1 つしか含まれておらず、それが自己署名済みでないため、署名を検証できませんでした。詳細については、この後の「確認リターンコード：21（最初の証明書を検証できません）」を参照してくだ

さい。詳細については、この後の「確認リターンコード：21（最初の証明書を検証できません）」を参照してください。

22 X509_V_ERR_CERT_CHAIN_TOO_LONG：証明書チェーンの長さが、指定された最大深度を超えています。未使用。

23 X509_V_ERR_CERT_REVOKED：証明書が失効しています。

24 X509_V_ERR_INVALID_CA：CA 証明書が無効です。CA ではないか、その拡張領域が、提供された目的と一致していません。

25 X509_V_ERR_PATH_LENGTH_EXCEEDED：basicConstraints の pathlength パラメータを超えています。

26 X509_V_ERR_INVALID_PURPOSE：提供された証明書を、指定された目的に使用できません。

27 X509_V_ERR_CERT_UNTRUSTED：ルート CA が、指定された目的に関して信頼できるものとしてマークされていません。

28 X509_V_ERR_CERT_REJECTED：ルート CA が、指定された目的を拒否するようにマークされています。

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH：件名が現在の証明書の発行者名と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

30 X509_V_ERR_AKID_SKID_MISMATCH：件名キー識別子が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH：発行者名とシリアル番号が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN：keyUsage 拡張領域が証明書の署名を許可していないため、現在の候補発行者証明書が拒否されました。

50 X509_V_ERR_APPLICATION_VERIFICATION：アプリケーション固有のエラーです。未使用。

「New Certificate Detected」メッセージ

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、Security Cloud Control で、[設定（Configuration）] ステータスと [接続（Connectivity）] ステータスの両方として、「新しい証明書が検出されました（New Certificate Detected）」というメッセージが生成されることがあります。このデバイスを引き続き Security Cloud Control から管理するには、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。

（注） 複数の管理対象デバイスを Security Cloud Control に同時にSecurity Cloud Control へのデバイス一括再接続すると、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。

新しい証明書を解決するには、次の手順を使用します。

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。
2. フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました（New Certificate Detected）] であるデバイスを表示し、必要なデバイスを選択します。
3. 操作ウィンドウで、[証明書の確認（Review Certificate）] をクリックします。Security Cloud Control では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
4. [デバイス同期（Device Sync）] ウィンドウで [承認（Accept）] をクリックするか、[デバイスへの再接続（Reconnecting to Device）] ウィンドウで [続行（Continue）] をクリックします。

   Security Cloud Control は、デバイスを新しい自己署名証明書と自動的に同期します。 場合によっては、同期されたデバイスを表示するためにページを手動で更新する必要があります。

証明書エラーコード

確認リターンコード：0（OK）（ただし、Security Cloud Control は証明書エラーを返します）

Security Cloud Control は、証明書を取得すると、「https://<device_ip>:<port>」への GET コールを実行することにより、デバイスの URL への接続を試みます。これが機能しない場合、Security Cloud Control は証明書エラーを表示します。証明書が有効である（openssl が 0 つまり OK を返します）ことがわかった場合、接続しようとしているポートで別のサービスがリッスンしている可能性があります。この場合、次のコマンドを使用できます。

```
 curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

これにより、次のように、ASA と確実に通信しているかどうかを確認することができ、HTTPS サーバーが ASA の正しいポートで動作しているかどうかをチェックすることもできます。

```
 # show asp table socket
Protocol         Socket         State         Local Address              Foreign Address

SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

確認リターンコード：9（証明書がまだ有効ではありません）

このエラーは、提供された証明書の発行日が将来の日付であるため、クライアントがそれを有効なものとして扱わないことを意味します。これは、証明書の不完全な作成が原因である可能

性があります。また、自己署名証明書の場合は、証明書生成時のデバイスの時刻が間違っていたことが原因である可能性があります。

エラーには、証明書の notBefore の日付が含まれた行があります。

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

このエラーから、証明書がいつ有効になるかを判別できます。

修復

証明書の notBefore の日付は過去の日付である必要があります。notBefore の日付をより早い日付にして証明書を再発行できます。この問題は、クライアントまたは発行デバイスのいずれかで時刻が正しく設定されていない場合にも発生する可能性があります。

確認リターンコード：10（証明書の有効期限が切れています）

このエラーは、提供された証明書の少なくとも 1 つの期限が切れていることを意味します。エラーには、証明書の notBefore の日付が含まれた行があります。

```
 error 10 at 0 depth lookup:certificate has expired
```

この有効期限は、証明書の本文に含まれています。

修復

証明書が本当に期限切れの場合、唯一の修復方法は、別の証明書を取得することです。証明書の有効期限が将来の日付であるのに、openssl が期限切れであると主張する場合は、コンピュータの日付と時刻をチェックしてください。たとえば、証明書が 2020 年に期限切れになるように設定されているのに、コンピュータの日付が 2021 年になっている場合、そのコンピュータは証明書を期限切れとして扱います。

確認リターンコード：21（最初の証明書を検証できません）

このエラーは、証明書チェーンに問題があることと、デバイスによって提示された証明書を信頼できることを openssl が検証できないことを示しています。ここで、上記の例の証明書チェーンを調べて、証明書チェーンがどのように機能するのかを見てみましょう。

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
```

```
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

証明書チェーンとは、サーバーによって提示される証明書のリストです。このリストは、サーバー自体の証明書から始まり、そのサーバーの証明書を認証局の最上位の証明書に結び付ける、段階的により上位の中間証明書が含まれます。各証明書には、その件名（「s:」で始まる行）とその発行者（「i」で始まる行）のリストが示されています。

件名は、証明書によって識別されるエンティティです。これには、組織名が含まれており、場合によっては証明書の発行先エンティティの共通名も含まれます。

発行者は、証明書を発行したエンティティです。これには、組織フィールドも含まれており、場合によっては共通名も含まれます。

サーバーは、信頼できる認証局によって直接発行された証明書を持っている場合、証明書チェーンに他の証明書を含める必要がありません。次のような 1 つの証明書が表示されます。

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

この証明書を提供すると、openssl は、***.example.com** の ExampleCo 証明書が、openssl の組み込み信頼ストアに存在する信頼できる認証局の証明書によって正しく署名されていることを検証します。その検証の後に、openssl は、デバイスに正常に接続します。

ただし、ほとんどのサーバーには、信頼できる CA によって直接署名された証明書がありません。代わりに、最初の例のように、サーバーの証明書は 1 つ以上の中間証明書によって署名されており、最上位の中間証明書が、信頼できる CA によって署名された証明書を持ちます。OpenSSL は、デフォルトでは、これらの中間 CA を信頼せず、信頼できる CA で終わる完全な証明書チェーンが提供されている場合にのみ、それらを検証できます。

中間認証局によって署名された証明書を持つサーバーが、信頼できる CA に結び付けられたすべての証明書（すべての中間証明書を含む）を提供することが非常に重要です。このチェーン全体が提供されない場合、openssl からの出力は次のようなものになります。

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1
```

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

この出力は、サーバーが 1 つの証明書のみを提供しており、提供された証明書が信頼されたルート認証局ではなく中間認証局によって署名されていることを示しています。この出力には、特性検証エラーも示されています。

修復

この問題は、デバイスによって提示された証明書の設定が間違っているために発生します。この問題を修正して Security Cloud Control またはその他のプログラムがデバイスに安全に接続できるようにする唯一の方法は、正しい証明書チェーンをデバイスにロードして、接続しているクライアントに完全な証明書チェーンを提示することです。

中間 CA をトラストポイントに含めるには、次のいずれか（CSR が ASA で生成されたかどうかに応じて）のリンク先に記載されている手順に従ってください。

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

「New Certificate Detected」メッセージ

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、Security Cloud Control で、[設定（Configuration）] ステータスと [接続（Connectivity）] ステータスの両方として、「新しい証明書が検出されました（New Certificate Detected）」というメッセージが生成されることがあります。このデバイスを引き続き Security Cloud Control から管理するには、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。

（注） Security Cloud Control へのデバイス一括再接続により、複数の管理対象デバイスを Security Cloud Control に同時に再接続すると、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。

新しい証明書を解決するには、次の手順を使用します。

手順

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

ステップ 2 [デバイス] タブをクリックします。

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 フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました（New Certificate Detected）] であるデバイスを表示し、必要なデバイスを選択します。

ステップ 5 操作ウィンドウで、[証明書の確認（Review Certificate）] をクリックします。Security Cloud Control では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。

ステップ 6 [デバイス同期（Device Sync）] ウィンドウで [承認（Accept）] をクリックするか、[デバイスへの再接続（Reconnecting to Device）] ウィンドウで [続行（Continue）] をクリックします。

Security Cloud Control は、デバイスを新しい自己署名証明書と自動的に同期します。 場合によっては、同期されたデバイスを表示するためにページを手動で更新する必要があります。

オンボーディングエラーのトラブルシュート

デバイスのオンボーディングエラーは、さまざまな理由で発生する可能性があります。

次の操作を実行できます。

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 適切なデバイスタイプのタブをクリックし、エラーが発生しているデバイスを選択します。場合によっては、右側にエラーの説明が表示されます。説明に記載されている必要なアクションを実行します。

または

ステップ 3 Security Cloud Control からデバイスインスタンスを削除し、デバイスのオンボーディングを再試行します。

競合検出ステータスの解決

Security Cloud Control を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。競合検出 （159 ページ） が有効になっていて、Security Cloud Control を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出（Conflict Detected）] と表示されます。

[競合検出（Conflict Detected）] ステータスを解決するには、次の手順に従います。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）]** > **[Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

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 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認（Review Conflict）] をクリックします。

ステップ 5 [デバイスの同期（Device Sync）] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。

- 「最後に認識されたデバイス設定（Last Known Device Configuration）」というラベルの付いたパネルは、Security Cloud Control に保存されているデバイス設定です。

- [デバイスで検出（Found on Device）] というラベルの付いたパネルは、ASA の実行コンフィギュレーションに保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認（Accept Device changes）]：設定と、Security Cloud Control に保存されている保留中の変更がデバイスの実行コンフィギュレーションで上書きされます。

  （注）
  Security Cloud Control はコマンド ライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認（Accept Without Review）] です。

- [デバイスの変更を拒否（Reject Device Changes）]：デバイスに保存されている設定を Security Cloud Control に保存されている設定で上書きします。

（注）
拒否または承認されたすべての設定変更は、変更ログに記録されます。

未同期ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

手順

ステップ 1 ナビゲーションバーで **セキュリティデバイス** をクリックします。

（注）
オンプレミス Firewall Management Center の場合は、**[管理（Administration）]** > **[Firewall Management Center]** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

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。

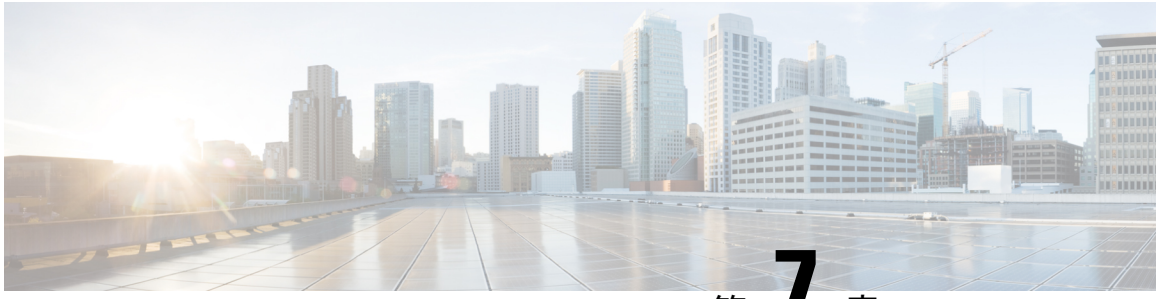
ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期（Not synced）] パネルで、次のいずれかを選択します。

- [プレビューして展開...（Preview and Deploy..）]：設定の変更を Security Cloud Control からデバイスにプッシュする場合は、今行った変更をすべてのデバイスの設定変更のプレビューと展開か、待ってから一度に複数の変更を展開します。

- [変更の破棄（Discard Changes）]：設定の変更を Security Cloud Control からデバイスに**プッシュしない**場合、または Security Cloud Control で開始した設定の変更を「元に戻す」場合。このオプションは、Security Cloud Control に保存されている設定を、デバイスに保存されている実行構成で上書きします。



第 7 章

FAQ とサポート

この章は、次の項で構成されています。

Cisco Security Cloud Control

Cisco Security Cloud Controlとは

Cisco Security Cloud Control（旧称 Cisco Defense Orchestrator）は、ネットワーク管理者がさまざまなセキュリティデバイス間で一貫したセキュリティポリシーを作成および維持できるクラウドベースのマルチデバイスマネージャです。

Security Cloud Control を使用して、次のデバイスを管理できます。

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS デバイス
- Amazon Web Services（AWS）インスタンス

- SSH 接続を使用して管理されるデバイス

Security Cloud Control 管理者は、これらすべてのデバイスタイプを単一のインターフェイスで監視および保守できます。

Security Cloud Control へのデバイスのオンボーディングに関する FAQ

Secure Firewall ASA の Security Cloud Control へのオンボーディングに関する FAQ

資格情報を使用して ASA をオンボードするにはどうすればよいですか？

ASA のオンボーディングは、一度に 1 つずつ、またはまとめて実行できます。デバイスを一度に。高可用性ペアの一部である ASA をオンボーディングする場合は、「Onboard an ASA Device」を使用してペアのプライマリデバイスのみをオンボーディングします。セキュリティコンテキストまたは管理コンテキストをオンボーディングする方法は、他の ASA をオンボーディングする場合と同じです。

一度に複数の ASA をオンボードするにはどうすればよいですか？

CSV ファイルを使用して ASA のリストを作成できます。Security Cloud Control はリスト内のすべての ASA をオンボーディングします。ASA を一括でオンボーディングする方法については、「Onboard ASAs in Bulk」を参照してください。

ASA をオンボーディングした後はどうすればよいですか？

開始するには、『Managing ASA with Cisco Security Cloud Control』[英語] を参照してください。

Security Cloud Control への FDM 管理対象デバイスのオンボーディングに関する FAQ

FDM 管理対象デバイスをオンボーディングするにはどうすればよいですか。

FDM 管理対象デバイスのオンボーディングにはさまざまな方法があります。登録キー方式を使用することが推奨されます。開始するには、「Onboard an FDM-Managed Device」を参照してください。

Secure Firewall Threat Defense の クラウド提供型 Firewall Management Center へのオンボーディングに関する FAQ

Secure Firewall Threat Defense をオンボーディングするにはどうすればよいですか。

CLI登録キー、ゼロタッチプロビジョニング、またはシリアル番号を使用して、FTDデバイスをオンボードできます。

Secure Firewall Threat Defense のオンボーディング後は何をすればよいですか。

デバイスが同期されたら、[ツールとサービス（Tools & Services）]>[Firewall Management Center]に移動し、[アクション（Actions）]、[管理（Management）]、または[設定（Settings）]ペインからアクションを選択して、クラウド提供型 Firewall Management Center で Threat Defense デバイスの設定を開始します。開始するには「Cloud-delivered Firewall Management Center Application Page」を参照してください。

Secure Firewall Threat Defense のトラブルシューティング方法を教えてください。

「Troubleshoot Onboarding your Secure Firewall Threat Defense」を参照してください。

オンプレミスの Secure Firewall Management Center に関する FAQ

オンプレミス Management Center のオンボーディング方法

オンプレミス Management Center を Security Cloud Control にオンボードできます。オンプレミス Management Center をオンボードすると、そのオンプレミス Management Center に登録されているすべてのデバイスもオンボードされます。Security Cloud Control は、オンプレミス Management Center またはオンプレミス Management Center に登録されたデバイスに関連付けられたオブジェクトまたはポリシーの作成や変更をサポートしていません。これらの変更は、オンプレミス Management Center UI で行う必要があります。開始するには、「Onboard an On-Prem Management Center 」を参照してください。

Security Cloud Control への Meraki デバイスのオンボーディングに関する FAQ

Meraki デバイスをオンボーディングするにはどうすればよいですか。

MXデバイスは、Security Cloud Control と Meraki ダッシュボードの両方で管理できます。Security Cloud Control は、設定の変更を Meraki ダッシュボードに展開します。これにより、設定がデバイスに安全に展開されます。開始するには、「Meraki MX デバイスのオンボーディング」を参照してください。

Security Cloud Control への SSH デバイスのオンボーディングに関する FAQ

SSH デバイスをオンボードするにはどうすればよいですか？

SSHデバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスを Secure Device Connector（SDC）でオンボーディングできます。開始するには、「SSH デバイスのオンボーディング」を参照してください。

デバイスの削除方法

[セキュリティデバイス（Security Devices）] ページからデバイスを削除できます。

Security Cloud Control への IOS デバイスのオンボーディングに関する FAQ

Cisco IOS デバイスをオンボードするにはどうすればよいですか？

Secure Device Connector（SDC）を使用して、Cisco IOS（Internetwork Operating System）を実行しているライブ Cisco デバイスをオンボードできます。開始するには、「Cisco IOS デバイスのオンボーディング」を参照してください。

デバイスの削除方法

[セキュリティデバイス（Security Devices）] ページからデバイスを削除できます。

デバイスタイプ

適応型セキュリティアプライアンス（ASA）とは何ですか。

Cisco ASA は、追加モジュールとの統合サービスに加え、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティコンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール オペレーション、高度なインスペクションエンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。ASA は、仮想マシンまたはサポートされているハードウェアにインストールできます。

ASA モデルとは何ですか。

ASA モデルは、Security Cloud Control にオンボードされた ASA デバイスの実行構成ファイルのコピーです。ASA モデルを使用すると、デバイス自体をオンボードせずに ASA デバイスの設定を分析することができます。

デバイスが「同期済み（Synced）」であるのは、どのような場合ですか。

Security Cloud Control の設定と、デバイスにローカルに保存されている設定が同じになっているときです。

デバイスが「非同期（Not Synced）」であるのは、どのような場合ですか。

Security Cloud Control に保存されている設定が変更され、デバイスにローカルに保存されている設定と異なっているときです。

デバイスが「競合検出（Conflict Detected）」状態であるのは、どのような場合ですか。

デバイスの設定が Security Cloud Control の外部（アウトオブバンド）で変更され、Security Cloud Control に保存されている設定と異なっているときです。

アウトオブバンド変更とは何ですか。

Security Cloud Control の外部でデバイスに変更が加えられることです。この変更は、CLI コマンドを使用するか、ASDM や FDM などのデバイス上のマネージャを使用して、デバイス上で直接行われたものです。アウトオブバンド変更が行われると、デバイスが [競合検出（Conflict Detected）] 状態であると Security Cloud Control が通知します。

変更をデバイスに展開するとは、どういう意味ですか。

デバイスを Security Cloud Control にオンボードすると、Security Cloud Control はその設定のコピーを保持します。Security Cloud Control に変更を加えると、Security Cloud Control は、デバイスの設定のコピーに変更を加えます。その変更をデバイスに「展開」すると、Security Cloud Control は、加えた変更をデバイスの設定のコピーにコピーします。次のトピックを参照してください。

- すべてのデバイスの設定変更のプレビューと展開 （152 ページ）

現在、どの ASA コマンドがサポートされていますか。

すべてのコマンドです。ASA CLI を使用するには、[デバイスアクション（Device Actions）] の [コマンドラインインターフェイス（Command Line Interface）] をクリックしてください。

デバイスの管理に関して規模の制約はありますか。

Security Cloud Control のクラウドアーキテクチャにより、数千台のデバイスにまで規模を拡張できます。

Security Cloud Control は、Cisco サービス統合型ルータおよびアグリゲーション サービス ルータを管理できますか。

Security Cloud Control では ISR および ASR 用のモデルデバイスを作成して、その設定をインポートできます。次に、インポートされた設定に基づいてテンプレートを作成し、その設定を標準の設定としてエクスポートできます。この標準の設定を、ISR および ASR の新規または既存のデバイスに展開して、セキュリティの一貫性を確保できます。

Security Cloud Control は SMA を管理できますか。

いいえ、現時点では、Security Cloud Control は SMA を管理しません。

セキュリティ

Security Cloud Control は安全ですか？

Security Cloud Control は、次の機能を通じて顧客データのエンドツーエンドのセキュリティを実現します。

- 新規 Security Cloud Control テナントへの初回ログイン （5 ページ）
- API およびデータベース操作の認証呼び出し
- 転送中および保存中のデータ分離
- 役割分担

Security Cloud Control では、ユーザーがクラウドポータルに接続するために多要素認証が必要です。多要素認証は、顧客の ID を保護するために必要な重要な機能です。

すべてのデータは、転送中も保存中も暗号化されます。顧客構内のデバイスと Security Cloud Control からの通信は SSL で暗号化され、顧客テナントのデータボリュームはすべて暗号化されます。

Security Cloud Control のマルチテナント アーキテクチャは、テナントデータを分離し、データベースとアプリケーション サーバー間のトラフィックを暗号化します。Security Cloud Control へのアクセス権が認証されると、ユーザーにトークンが送られます。このトークンは、キー管理サービスからキーを取得するために使用され、このキーはデータベースへのトラフィックを暗号化するために使用されます。

Security Cloud Control はお客様に価値を素早く提供すると同時に、お客様のログイン情報の安全性を確保します。これは、クラウドまたはお客様自身のネットワーク（ロードマップ）に「Secure Data Connector」を展開することによって実現されます。Secure Data Connector は、インバウンドおよびアウトバウンドトラフィックを制御して、クレデンシャルデータが顧客構内から離れることがないようにします。

Security Cloud Control に初めてログインしたときに、「OTP を検証できませんでした（Could not validate your OTP）」というエラーが表示されました。

デスクトップまたはモバイルデバイスの時計がワールドタイムサーバーと同期していることを確認します。時計が 1 分以上ずれていると、誤った OTP が生成される可能性があります。

デバイスは Security Cloud Control クラウドプラットフォームに直接接続されるのですか？

はい。デバイスと Security Cloud Control プラットフォームの間でプロキシとして機能する Security Cloud Control SDC を使用することで、セキュアな接続が実現します。セキュリティを最優先に

設計された Security Cloud Control アーキテクチャにより、デバイスとの間を行き来するデータを完全に分離できます。

パブリック IP アドレスを持たないデバイスを接続するにはどうすればよいですか？

ネットワーク内に展開でき、外部ポートを開く必要がない Security Cloud Control Secure Device Connectorを利用できます。SDC が展開されると、内部（インターネットでルーティングできない）IP アドレスを持つデバイスをオンボードできます。

SDC には追加のコストやライセンスが必要ですか？

番号

トンネルステータスはどのように確認できますか？状態オプション

Security Cloud Control はトンネル接続チェックを 1 時間ごとに自動的に実行しますが、トンネルを選択して接続チェックを要求することで、アドホックの VPN トンネル接続チェックを実行できます。結果の処理には数秒かかる場合があります。

デバイス名とそのピアの片方の IP アドレスに基づいてトンネルを検索できますか？

はい。名前とピア IP アドレスの両方で利用可能なフィルタ機能と検索機能を使用して、特定の VPN トンネルの詳細を検索してピボットします。

トラブルシューティング

Security Cloud Control から管理対象デバイスへのデバイス構成の完全な展開を実行しているときに、「変更をデバイスに展開できません（Cannot deploy changes to device）」という警告が表示されます。解決するにはどうすればよいですか？

完全な構成（Security Cloud Control でサポートされているコマンドを超えて実行された変更）をデバイスに展開するときにエラーが発生した場合は、[変更の確認（Check for changes）] をクリックして、デバイスから使用可能な最新の構成をプルします。これによって問題が解決されたら、Security Cloud Control で引き続き変更を加えて展開することができます。問題が解決しない場合は、[サポートに連絡（Contact Support ）] ページから Cisco TAC に連絡してください。

アウトオブバンドの問題（Security Cloud Control の外部で、デバイスに対して直接実行された変更）を解決しているときに、Security Cloud Control に存在する構成をデバイスの構成と比較すると、Security Cloud Control は、私が追加または変更していない追加のメタデータを提示します。どうしてですか。

Security Cloud Control がその機能を拡張すると、デバイスの構成から追加情報が収集され、ポリシーとデバイス管理の分析を改善するために必要なすべてのデータを充実させて維持します。これらは管理対象デバイスで発生した変更ではなく、既存の情報です。[競合が検出され

ました（Conflict Detected）] の状態の解決は、デバイスからの変更を確認し、発生した変更を確認することで簡単に解決できます。

Security Cloud Control が私の証明書を拒否するのはなぜですか？

「新規証明書の問題のトラブルシュート」を参照してください。

ゼロ タッチ プロビジョニング で使用される用語および定義

- **要求（Claimed）**：Security Cloud Control でシリアル番号のオンボーディングのコンテキストで使用されます。シリアル番号が Security Cloud Control テナントにオンボードされている場合、そのデバイスは「要求」されています。
- **パーク（Parked）**：Security Cloud Control でシリアル番号のオンボーディングのコンテキストで使用されます。デバイスが Cisco Cloud に接続されていて、Security Cloud Control テナントがそのデバイスのシリアル番号を要求していない場合、そのデバイスは「パーク」されています。
- **初期プロビジョニング（Initial provisioning）**：初期 FTD セットアップのコンテキストで使用されます。このフェーズでは、デバイスの EULA を受け入れ、新しいパスワードを作成し、管理 IP アドレス、FQDN、および DNS サーバーを設定し、FDM を使用してデバイスをローカルで管理することを選択します。
- **ゼロ タッチ プロビジョニング**：FTD を工場からお客様のサイト（通常は分散拠点）に出荷するプロセスであり、サイトの従業員が FTD をネットワークに接続し、デバイスを Cisco Cloud に接続します。その時点で、シリアル番号がすでに「要求」されている場合、デバイスは Security Cloud Control テナントにオンボードされます。また、FTD は、Security Cloud Control テナントが要求するまで Cisco Cloud に「パーク」されます。

ポリシーの最適化

2 つ以上のアクセスリスト（同じアクセスグループ内）で相互にシャドウイングが発生しているケースを特定するにはどうすればよいですか。

Security Cloud Control のネットワークポリシー管理（NPM）を使用することで、ルールセット内で上位のルールが別のルールをシャドーイングしている場合に、ユーザーを特定して警告することができます。ユーザーは、すべてのネットワークポリシー間を移動するか、フィルタ処理を実行してすべてのシャドー問題を特定できます。

（注） Security Cloud Control は、完全にシャドーイングされたルールのみをサポートします。

接続性

Secure Device Connector により IP アドレスが変更されましたが、これは Security Cloud Control 内に反映されませんでした。変更を反映するにはどうすればよいですか。

Security Cloud Control 内で新しい Secure Device Connector（SDC）を取得して更新するには、次のコマンドを使用してコンテナを再起動する必要があります。

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh
restartSDC <tenant-name>
```

Security Cloud Control がデバイス（FTD または ASA）を管理するために使用する IP アドレスが変更された場合はどうなりますか。

デバイスの IP アドレスが何らかの理由で変更された場合、それが静的 IP アドレスの変更であるか、DHCP による IP アドレスの変更であるかにかかわらず、Security Cloud Control がデバイスへの接続に使用する IP アドレスを変更して（Security Cloud Control のデバイスの IP アドレスの変更 （102 ページ）を参照）、デバイスを再接続できます（Security Cloud Control へのデバイス一括再接続（108 ページ）を参照）。デバイスを再接続するときに、デバイスの新しい IP アドレスの入力と、認証の資格情報の再入力を求められます。

ASA を Security Cloud Control に接続するには、どのようなネットワークが必要ですか。

- ASDM イメージが存在し、ASA に対して有効になっている。
- 52.25.109.29、52.34.234.2、52.36.70.147 へのパブリック インターフェイス アクセス。
- ASA の HTTPS ポートは 443、または 1024 以上の値に設定する必要があります。たとえば、ポート 636 に設定することはできません。
- 管理下の ASA も AnyConnect VPN クライアント接続を受け入れるように設定されている場合は、ASA HTTPS ポートを 1024 以上の値に変更する必要があります。

データインターフェイスについて

デバイスとの通信には、専用の管理インターフェイス、または通常のデータインターフェイスを使用できます。データインターフェイスでの Security Cloud Control アクセスは、外部インターフェイスからリモートで FTD を管理する場合、または別の管理ネットワークがない場合に便利です。Security Cloud Control は、データインターフェイスからリモートで管理される FTD での高可用性をサポートします。

データインターフェイスからの FTD 管理アクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを FTD と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- データインターフェイスでは SSH がデフォルトで有効になっていないため、後で Security Cloud Control を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。

Security Cloud Control による個人情報の処理方法

Security Cloud Control が個人を特定できる情報を処理する方法については、『Cisco Security Cloud Control Privacy Data Sheet』[英語] を参照してください。

Security Cloud Control サポートへの問い合わせ

この章は、次のセクションで構成されています。

ワークフローのエクスポート

サポートチケットを開く前に、問題が発生しているデバイスのワークフローをエクスポートすることを強くお勧めします。この追加情報は、サポートチームがトラブルシューティング作業を迅速に特定して修正するのに役立ちます。

ワークフローをエクスポートするには、次の手順を使用します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** 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、トラブルシューティングが必要なデバイスを選択します。

フィルタまたは**検索バー**を使用して、トラブルシューティングが必要なデバイスを見つけます。デバイスを選択して強調表示します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[ワークフロー（Workflows）] を選択します。

ステップ 5 ページ右上のイベントテーブルの上にある [エクスポート（Export）] ボタンをクリックします。ファイルは、**.json** ファイルとしてローカルに自動的に保存されます。このファイルを、TAC で開いた電子メールまたはチケットに添付します。

TAC でサポートチケットを開く

30 日間のトライアルか、ライセンス取得済み Security Cloud Control アカウントを使用しているお客様は、シスコのテクニカル アシスタンス センター（TAC）でサポートチケットを開くことができます。

- Security Cloud Control のお客様が TAC でサポートチケットを開く方法。
- Security Cloud Control のトライアルのお客様が TAC でサポートチケットを開く方法。

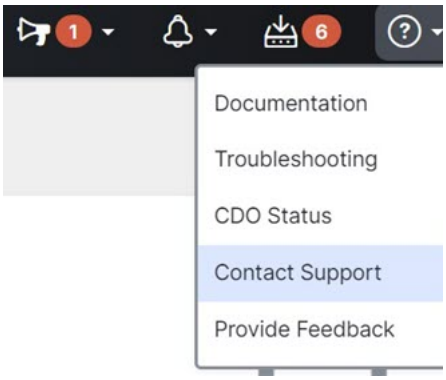
Security Cloud Control のお客様が TAC でサポートチケットを開く方法

このセクションでは、ライセンス取得済み Security Cloud Control テナントを使用しているお客様が、シスコのテクニカル アシスタンス センター（TAC）でサポートチケットを開く方法について説明します。

手順

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

ステップ 2 テナント名の横にある [ヘルプ（help）] ボタンをクリックし、[サポートに連絡（Contact Support）] を選択します。



ステップ 3 [サポートケースマネージャ（Support Case Manager）] をクリックします。

ステップ 4 青色の [新しいケースを開く（Open New Case）] ボタンをクリックします。

ステップ 5 [ケースをオープン（Open Case）] をクリックします。

ステップ 6 [製品およびサービス（Products and Services）] を選択し、[ケースを開く（Open Case）] をクリックします。

ステップ 7 [リクエストタイプ（Request Type）] を選択します。

ステップ 8 [サービス契約による製品の検索（Find Product by Service Agreement）] 行を展開します。

ステップ 9 すべてのフィールドに入力します。多くのフィールドは明らかで説明するまでもありませんが、追加の情報を以下に記載します。

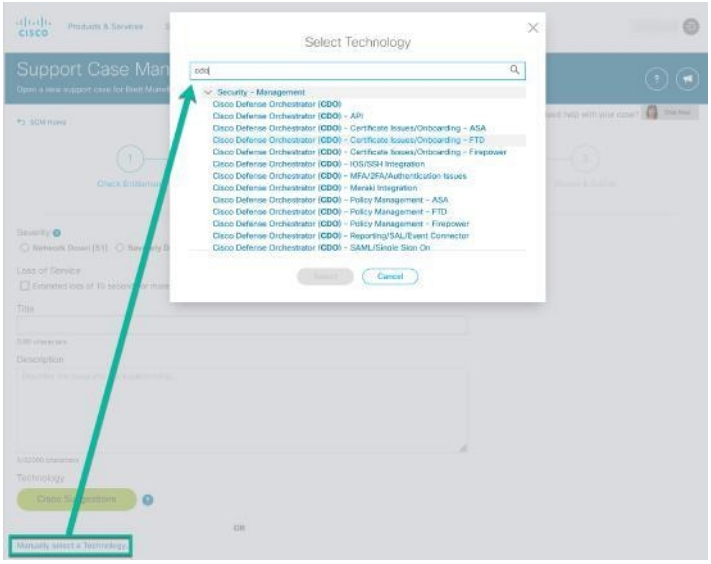
- [製品名（PID）（Product Name (PID)）]：この番号がわからない場合は、『Cisco Security Cloud Control Data Sheet』を参照してください。
- [製品の説明（Product Description）]：PID の説明です。
- [サイト名（Site Name）]：サイト名を入力します。シスコパートナーがお客様に代わってケースを開いている場合は、お客様の名前を入力します。
- [サービス契約（Service Contract）]：サービス契約番号を入力します。
  - **重要**：ケースを Cisco.com アカウントに関連付けるには、契約番号を Cisco.com プロファイルに関連付ける必要があります。契約番号を Cisco.com プロファイルに関連付けるには、次の手順を実行します。
    1. Cisco Profile Manager を開きます。
    2. [アクセス管理（Access Management）] タブをクリックします。
    3. [アクセス権の追加（Add Access）] をクリックします。
    4. [Cisco.comのTACおよびRMAケース作成、ソフトウェアダウンロード、サポートツール、および権限付きコンテンツ（TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com）] を選択し、[実行（Go）] をクリックします。
    5. 指定されたスペースにサービス契約番号を入力し、[送信（Submit）] をクリックします。サービス契約の関連付けが完了したことが電子メールで通知されます。サービス契約の関連付けは、完了までに最長 6 時間かかる場合があります。

重要
重要：以下のリンクのいずれにもアクセスできない場合は、シスコ認定のパートナーや再販業者、シスコのアカウント担当者、または社内でシスコサービスの契約情報を管理する担当者にお問い合わせください。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [問題の説明（Describe Problem）] 画面を下にスクロールして [テクノロジーを手動で選択（Manually select a Technology）] をクリックし、検索フィールドに **Security Cloud Control** と入力します。

ステップ 12 リクエストに最も一致するカテゴリを選択し、[選択（Select）] をクリックします。



ステップ 13 サービスリクエストの残りの部分をすべて入力し、[送信（Submit）] をクリックします。

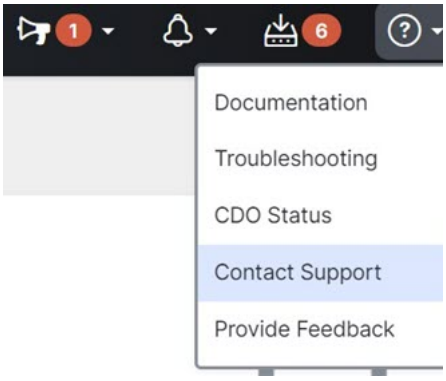
Security Cloud Control のトライアルのお客様が TAC でサポートチケットを開く方法

このセクションでは、無料トライアルの Security Cloud Control テナントを使用しているお客様が、シスコのテクニカル アシスタンス センター（TAC）でサポートチケットを開く方法について説明します。

手順

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

ステップ 2 テナント名とアカウント名の横にある [ヘルプ（help）] ボタンをクリックし、[サポートに連絡（Contact Support）] を選択します。



ステップ 3 [問題またはリクエストを下に入力（Enter Issue or request below）] フィールドで、直面している問題またはリクエストを指定し、[送信（Submit）] をクリックします。

リクエストと技術情報がサポートチームに送信され、テクニカル サポート エンジニアが質問に回答します。

Security Cloud Control サービスステータスページ

Security Cloud Control は顧客向けのサービスステータスページを維持しており、このページには、Security Cloud Control サービスが稼働しているかどうかと、サービスの中断があったかどうかが表示されます。稼働時間情報を日次、週次、または月次のグラフで表示できます。

Security Cloud Control の任意のページのヘルプメニューで [CDOステータス（Security Cloud Control Status）] をクリックすると、Security Cloud Control ステータスページにアクセスできます。

ステータスページで、[更新の登録（Subscribe to Updates）] をクリックして、Security Cloud Control サービスがダウンした場合に通知を受け取ることができます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。