

Cisco Security Cloud Control：Cisco Meraki の管理

最終更新：2026 年 11 月 12 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

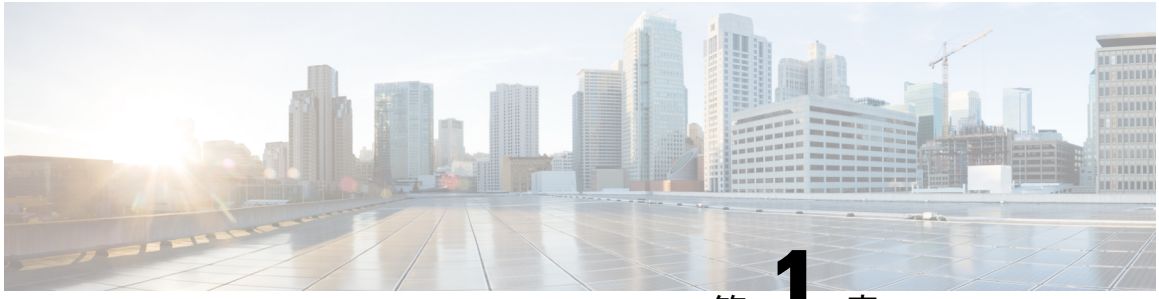
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2026 Cisco Systems, Inc. All rights reserved.



第 1 章

はじめに

Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのプラットフォームで、Cisco のファイアウォールおよびデバイス全体でセキュリティポリシー管理を統合し、簡素化します。ポリシーの一貫性が合理化され、直感的で高度なインターフェイスが提供され、複数のデバイスマネージャ間での設定の変更が調整されます。

- Security Cloud Control を使用した Meraki の管理, on page 1
- Cisco Security Cloud Control の概要 （4 ページ）
- Security Cloud Control によってサポートされる製品およびソリューション （5 ページ）
- Security Cloud Control Firewall Management の概要 （6 ページ）
- ファイアウォール管理ダッシュボード （7 ページ）

Security Cloud Control を使用した Meraki の管理

Cisco Meraki デバイスを Security Cloud Control にオンボードすると、Security Cloud Control は Cisco 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 MX デバイスと直接通信しません。

Security Cloud Control は設定要求を Cisco Meraki ダッシュボードに安全に転送し、その後ダッシュボードが新しい設定をデバイスに適用します。詳細については、Security Cloud Control と Meraki の通信方法, on page 3を参照してください。

Security Cloud Control は、オブジェクトとポリシーの問題を特定し、考えられる修正や代替オプションを提案することで、Cisco Meraki 環境を最適化するツールを提供します。これは、デバイスとテンプレートの両方に関連付けられたポリシーに適用されます。Security Cloud Control を使用して次のことができます。

- 1 つ以上の Meraki デバイスでポリシーを同時に管理します。
- 包括的な環境で、FTD および Cisco ASA デバイスとともに Cisco Meraki ポリシーまたはテンプレートを監視および管理します。
- Meraki テンプレートを使用して複数のネットワークを管理します。
- FTD や Cisco ASA デバイスなど、サポートされている他のプラットフォームとの互換性のあるオブジェクトを使用してアクセスルールをカスタマイズします。

Meraki MX デバイスのオンボーディング

デバイスを Security Cloud Control にオンボードする前に、Cisco Meraki ダッシュボードでアカウントを作成し、デバイスまたはテンプレートをダッシュボードにオンボードする必要があります。API トークンを生成して Security Cloud Control と通信するためには、組織が Cisco Meraki ダッシュボードにアカウントを持っている必要があります。

Cisco Meraki MX デバイスまたは Cisco Meraki テンプレートを Security Cloud Control にオンボードできます。

Security Cloud Control コンソールを介して Cisco Meraki MX のログイン情報と権限を処理します。正しいログイン情報または権限がないと、Security Cloud Control は Meraki デバイスと通信できません。

詳細については、「Cisco Meraki MX ログイン情報の更新」および「Cisco Meraki API キーの生成と取得」を参照してください。

Meraki レイヤ 3 ルールと Security Cloud Control

現時点では、Security Cloud Control はレイヤ 3 ファイアウォールルールのみをサポートしています。レイヤ 3 ルールは、OSI モデルのネットワーク層でポリシーを管理することを可能にします。詳細については、「Using Layer 3 Firewall Rules」を参照してください。

Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki ダッシュボードで定義されたレイヤ 3 ルールを読み取ります。その後、Security Cloud Control で、FTD または ASA ルールを管理する場合と同じ方法でこれらのルールを管理できます。詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

オブジェクト

オブジェクトを使用して、新しいアクセス コントロール ポリシーを最適化できます。Cisco Meraki ダッシュボードでは、プロトコルと IP アドレスのグループまたは IP アドレス範囲を使用します。対照的に、Security Cloud Control ではさまざまなオブジェクトを使用してルールを管理します。Security Cloud Control が Cisco Meraki プロトコルをオブジェクトに移行する方法を理解するには、「Cisco Meraki デバイスに関連付けられたオブジェクト」を参照してください。次のオブジェクトを Security Cloud Control で作成し、Cisco Meraki ダッシュボードの IP グループに変換できます。

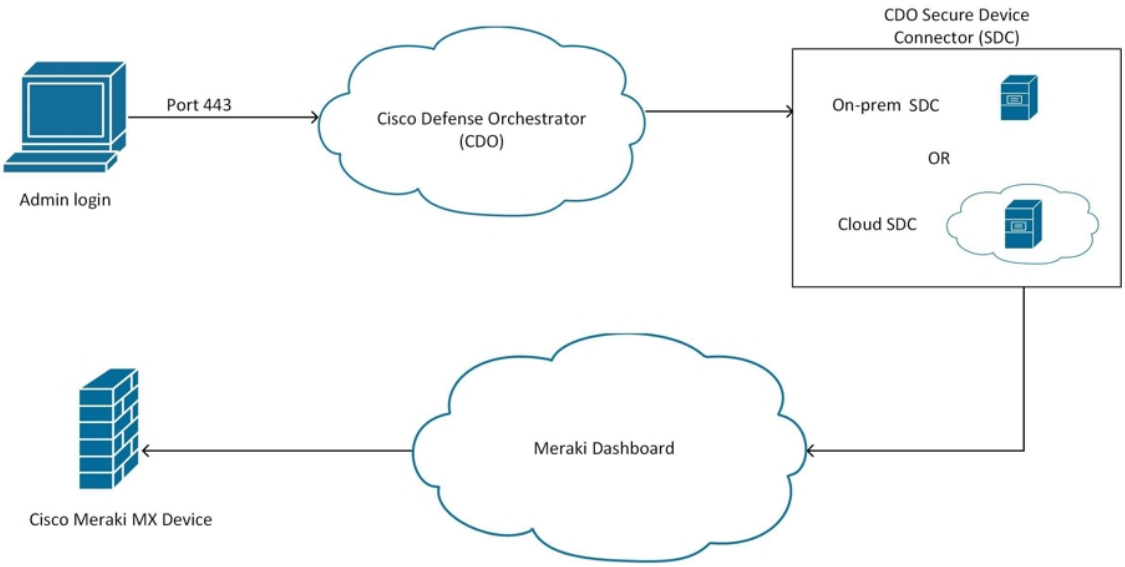
- ネットワークオブジェクトまたはオブジェクトグループ
- ネットワークサービス（ポート）オブジェクト

Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki ダッシュボードで定義したレイヤ 3 ルールを読み取ります。その後、Security Cloud Control で FTD または ASA ルールを管理する場合と同様に、これらのルールを管理できます。Cisco Meraki アクセス コントロール ポリシーの詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

Security Cloud Control と Meraki の通信方法

Security Cloud Control から Meraki デバイスへの展開

Security Cloud Control は、設定の変更を Cisco Meraki MX デバイスに直接展開しません。展開は複数のステップからなるプロセスです。次の図は、デプロイメントプロセスを示しています。



Cisco Meraki MX デバイスの Security Cloud Control で行った設定の変更は、展開を決定するまで Security Cloud Control でステージングされます。設定の変更を展開すると、Security Cloud Control から Cisco Meraki ダッシュボードに転送され、Cisco Meraki MX デバイスに実装されます。Security Cloud Control はファイアウォールポリシーを管理し、Cisco Meraki ダッシュボードはポリシーが適用されるネットワークを管理します。どちらの操作も、Cisco Meraki MX デバイスがネットワークトラフィックを管理および処理する方法に影響を与えます。

古いテナントを持つ一部のお客様は、SDC を介して Meraki MX デバイスを Security Cloud Control に接続する場合があります。そのようなお客様は、この方法を引き続き使用できます。あるいは、Cisco Meraki MX を再オンボーディングするか、接続ログイン情報を更新して SDC を削除できます。Security Cloud Control を Meraki MX に接続するために SDC は必要ありません。

Security Cloud Control と Cisco Meraki ダッシュボードの違いの 1 つは、オブジェクトの使用です。Cisco Meraki ダッシュボードで作成されたルールの場合、Security Cloud Control は Meraki の IP アドレスグループまたは IP アドレス範囲を取得し、それらをルールやデバイスポリシーに添付または関連付けできるオブジェクトに変換します。Security Cloud Control で作成されたオブジェクトを Meraki アプライアンスに展開すると、Cisco Meraki ダッシュボードはそれらのオブジェクトを IP アドレスグループまたは IP アドレス範囲に変換し直します。Security Cloud Control 内のオブジェクトは、他のデバイスプラットフォームと互換性があるため、固有かつ汎用性の高いオブジェクトです。Security Cloud Control でオンボードされた他のデバイスがある場合、すべてのデバイスに対して単一のオブジェクトを作成できる場合があります。Cisco Meraki デバイスに関連付けられているオブジェクトの詳細については、「Meraki デバイスに関連付けられるオブジェクト, on page 98」を参照してください。

Cisco Security Cloud Control の概要

Security Cloud Control は、単一の統合インターフェイスからセキュリティ製品を管理し、セキュリティの成果を達成できるようにするセキュリティ プラットフォームです。

プラットフォームにセキュリティ製品を統合すると、エクスペリエンスが合理化になります。Cisco セキュリティ製品のサブスクリプションを購入すると、購入したすべてのサブスクリプションに関する単一の要求コードが記載された電子メールが 1 件届きます。新しい Security Cloud Control 組織に要求コードを入力すると、すべての製品が同時に Cisco Security Cloud Control にプロビジョニングされます。

Security Cloud Control では、ユーザーとグループの管理はプラットフォームレベルで行われます。これらのユーザーとグループにロールが割り当てられ、Security Cloud Control および統合製品を管理する権限が定義されます。

製品とツール間の移動は直感に行うことができ、すべての統合製品に共通のプラットフォームメニューとツールバーが標準化されています。

Security Cloud Control は、プラットフォーム上のすべての統合製品に次のコアサービスを提供します。

- **プラットフォーム管理**：ロールベースのアクセス制御の管理、サブスクリプションの要求、製品インスタンスの標準化された地域展開などの一般的なサービスは、Security Cloud Control によって提供されます。Security Cloud Control では、これらの機能を一元化することで、プラットフォームから管理されるすべての Cisco Security 製品間でのプロビジョニングおよびアクセス管理における一貫したユーザーエクスペリエンスが保証されます。管理者は、Security Cloud Control のメインナビゲーションバーにある プラットフォーム管理 メニューからこれらの共通サービスにアクセスします。
- **人工知能アシスタント**：Security Cloud Control の Cisco AI Assistant は、AI 中心のインサイト、自動化、およびコンテキストガイダンスを提供することにより、セキュリティ業務を合理化するように設計されています。管理者がセキュリティポリシーを管理し、問題をトラブルシュートし、Firewall、Duo、および Secure Access などの Cisco のセキュリティ製品全体で設定を最適化するのに役立ちます。Cisco Assistant は、自然言語処理とクロスプラットフォーム インテリジェンスを活用することで、効率を向上させ、インシデント対応を迅速化し、セキュリティワークフローを簡素化します。
- **Global Search**：プラットフォーム内の製品全体の値を検索する機能です。
- **Shared Objects**：デバイスやポリシー間で共有できるオブジェクトを作成および管理します。
- **Unified documentation portal**：すべてのドキュメントにアクセスできる、ドキュメントの「ヘルプ」エクスペリエンス。

Security Cloud Control と統合される製品：

Security Cloud Control からは、次のすべてのセキュリティ製品を管理できます。

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- セキュアなアクセス

Security Cloud Control から起動できる製品

Security Cloud Control から、これらのセキュリティ製品を起動できます。起動後、これらの製品はスタンドアロン製品として動作するため、Security Cloud Control を介して管理することはできません。このような製品のライセンスは Security Cloud Control からのみ要求または非アクティブ化できます。

[Cisco Security Cloud Control] ツールバーで、9 ドットメニュー をクリックすると、次の製品が起動します：

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control によってサポートされる製品およびソリューション

現在、Security Cloud Control と統合できる製品は次のとおりです。

AI Defense：AI Defense はAIのユーザーとプロバイダーのリスクに対処します。Security Cloud Controlのネットワーク可視性と適用ポイントを使用して、AI Defense では、分散クラウド環境全体で承認済みおよび未承認の AI ワークロード、アプリケーション、モデル、データ、およびユーザーアクセスを検出するための検出と適用の手順が追加されます。AI を搭載したサービスを開発および提供する組織の場合、AI Defense は提供前に AI モデルの脆弱性を検出します。プロンプトインジェクション、サービス妨害（DoS）、データ漏洩といった急速に進化する脅威から AI アプリケーションを保護します。詳細については、「AI Defenseのドキュメント」を参照してください。

Security Cloud Control Firewall Management： Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのセキュリティポリシーマネージャで、シスコのファイアウォールやその他のデバイス全体でポリシーを簡素化および統合します。詳細については、『Cisco Security Cloud Control ドキュメント』の「ファイアウォール」を参照してください。

Multicloud Defense：Multicloud Defense は、マルチクラウドセキュリティに対する簡素化および高度に自動化されたアプローチを提供します。このソリューションにより、組織は単一の

SaaS 提供コントロールプレーンと、一元化または分散された PaaS 提供データプレーンアーキテクチャを使用して、マルチクラウド環境を管理および保護できます。 Multicloud Defense では、すべての主要なクラウドプロバイダーで継続的な可視性、統合された保護、およびダイナミックなポリシー更新が提供されるため、各クラウドプロバイダーごとにソリューションごとに個別のポイントソリューションを用意する必要がなくなります。詳細については、「Multicloud Defenseのドキュメント」を参照してください。

セキュアなアクセス：Cisco セキュアなアクセス は、インターネットベースの脅威に対して複数のレベルの防御を提供するクラウドベースのプラットフォームです。組織のネットワークから接続する場合でも、ネットワークからローミングする場合でも、インターネット、SaaSアプリケーション、およびプライベート デジタル リソースに安全に接続できます。ポリシールールを使用して、リソース、ユーザー、デバイスのコレクションにセキュリティ管理を構成および適用します。 詳細については、「Secure Access Documentation」を参照してください。セキュアなアクセス サブスクリプションには、追加料金なしで Security Cloud Control を介した アイデンティティ インテリジェンス 統合も含まれます。これには、スタンドアロン アイデンティティインテリジェンス ダッシュボードへのアクセスは含まれません。詳細については、「Cisco Identity Intelligence と Cisco Secure Access の統合」を参照してください。

Cisco XDR (Extended Detection and Response)：Cisco XDR は、セキュリティ運用を簡素化し、インシデント対応を迅速化するように設計されたクラウドネイティブの拡張可能なセキュリティソリューションです。エンドポイント、ネットワーク、ファイアウォール、電子メール、アイデンティティ、およびDNSを含む複数のソースからテレメトリを収集および分析し、Cisco Talos から提供される強化されたコンテキストと脅威インテリジェンスを使用して高度な脅威を検出します。

Cisco XDR は潜在的なリスクと影響に基づいて脅威に優先順位を付け、誤検出を減らし、AI 中心のガイダンスと自動化を提供して調査と修復を合理化します。この統合アプローチにより、セキュリティ オペレーション センター（SOC）チームは、マルチベクトル、マルチベンダー環境でシスコおよびサードパーティのセキュリティツールの両方を統合することで、より迅速に行動でき、生産性を向上させ、サイバーレジリエンスを構築できます。詳細については、「Cisco XDR ヘルプセンター」を参照してください。

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management、旧 Cisco Defense Orchestrator は、分散環境でのセキュリティポリシー管理を簡素化します。これにより、管理対象のファイアウォールやデバイス間で一貫したポリシーを維持できます。Security Cloud Control では、**ファイアウォール**は**製品（Products）**に表示されます。

Security Cloud Control Firewall Management は、不整合を特定し、解決ツールを提供することにより、セキュリティポリシーを最適化します。また、オブジェクト共有、ポリシー共有、および設定テンプレートもサポートされているため、デバイス間で一貫した設定を適用できます。

Security Cloud Control Firewall Management は、Adaptive Security Device Manager（ASDM）などのローカルデバイスマネージャと共存できます。他のマネージャが行った設定変更を追跡し、必要に応じて違いを調整します。

このプラットフォームには、脅威防御 デバイスを オンプレミス Firewall Management Center または クラウド提供型 Firewall Management Center にオンボーディングするのに役立つガイド付き Day 0 エクスペリエンスが含まれています。主要な機能に焦点を当てており、それらの機能をアクティブ化および設定するのに役立ちます。

デバイスのオンボーディング要件

デバイスをオンボーディングする前に、次の前提条件を満たしてください。

- インストールウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスをオンボーディングします。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスをオンボーディングした後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

ファイアウォール管理ダッシュボード

ファイアウォールダッシュボードは、さまざまなカテゴリ全体でテナントレベルの詳細をモニタリングおよび管理するための中心ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

左側のペインで、[ダッシュボード（Dashboard）] をクリックします。

ダッシュボードのカスタマイズ

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードに表示するウィジェットを選択または選択解除します。

3. ウィジェットをドラッグアンドドロップして、希望に応じて配置できます。

ダッシュボードは、**[Top Insights & Alerts]**、**[Top Actions]**、および **[Top Information]**の 3 つの主要なセクションに分割されています。各セクションでは、最適なセキュリティおよび運用管理を維持するために役立つさまざまなカテゴリのインサイトが提供されます。

上位のインサイトとアラート

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。エレメントフロー、RA VPN 予測、アクセス制御ポリシーの異常、CPU およびメモリの使用率が高い、Snort CPU およびメモリの使用率が原因で発生する高トラフィックに関連するインサイトを表示できます。

上位アクション

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。有効にすると、次のウィジェットが表示できます。

- **[ポリシーアナライザおよびオプティマイザ（Policy Analyzer and Optimizer）]**：セキュリティポリシーを分析し、異常を検出し、ファイアウォールのパフォーマンスを向上させるための最適化推奨事項を提供します。

  詳細については、「ポリシーアナライザおよびオプティマイザ」を参照してください。

- **Insights**：設定、正常性と操作、トラフィックとキャパシティなどのカテゴリごとに、アクティブなインサイトと傾向を表示します。

  詳細については、「 Insights」を参照してください。

- **[機能の導入（Feature Adoption）]**：使用状況を評価して改善できる機能の導入率を示します。

  詳細については、「機能の導入状況の評価と改善」を参照してください。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。テナントに対して有効になっている機能に応じて、次のウィジェットを表示できます。

- **設定状態（Configuration States）**：デバイス設定を Security Cloud Control によって維持される設定と比較して、不整合や競合を特定できます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理（Change Log Management）**：完了した変更ログと保留中の変更ログを表示して、運用の変更を追跡できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「変更ログ」を参照してください。

- **RA VPN セッション（RA VPN Sessions）**：リモートアクセス VPN セッションのアクティビティを表示します。

詳細については、「RA VPN セッション」を参照してください。

- **インベントリ全体（Overall Inventory）**：デバイスの総数を表示し、問題、保留中のアクション、その他、およびオンラインに分けてデバイスをグループ化します。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN（Site-to-Site VPN）**：VPN トンネルの総数と、アクティブおよびアイドルのトンネルの割合が表示されます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

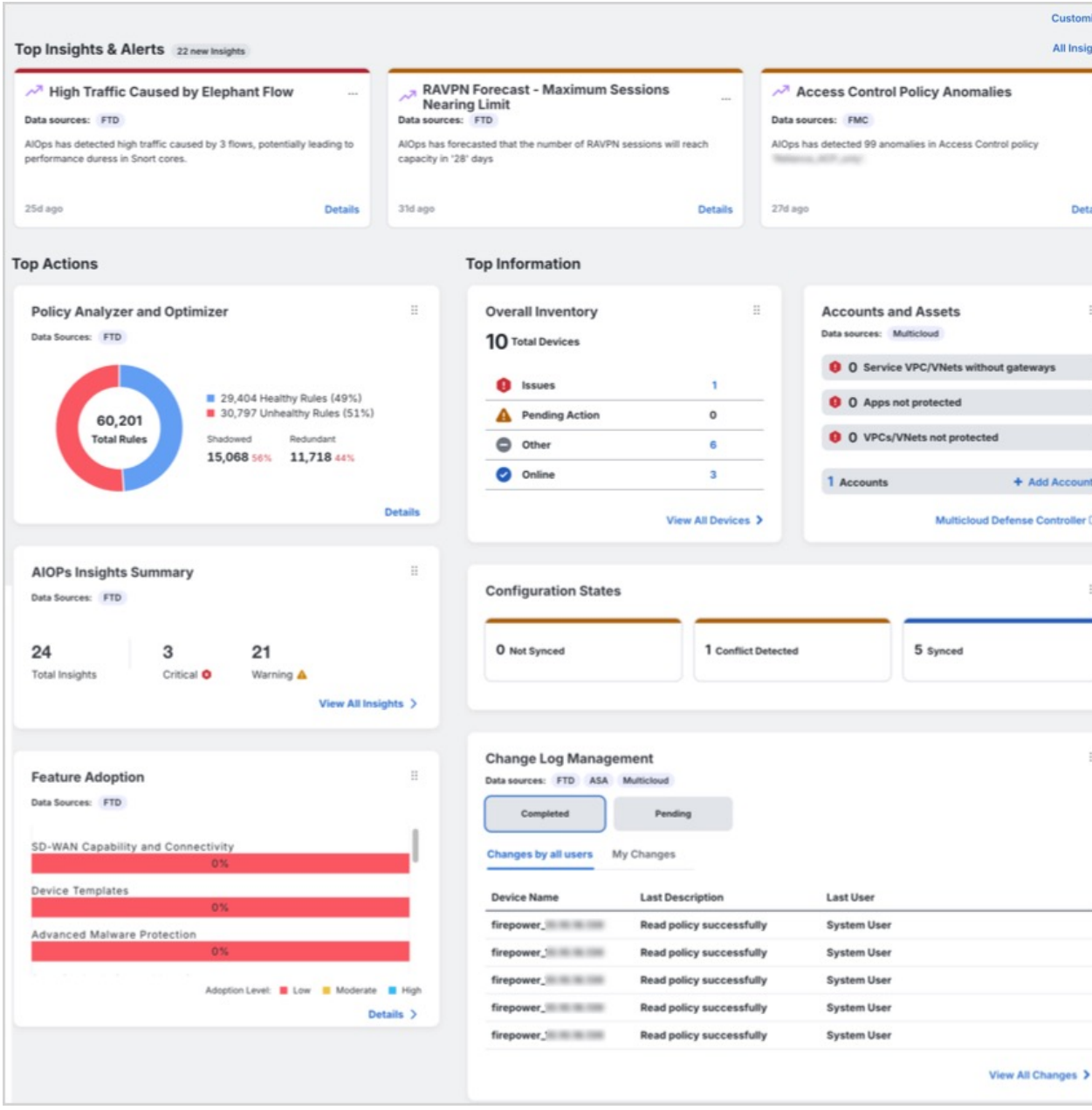
  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：
  - マルチクラウドのアカウントとリソースを効果的に追跡して管理するのに役立ちます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

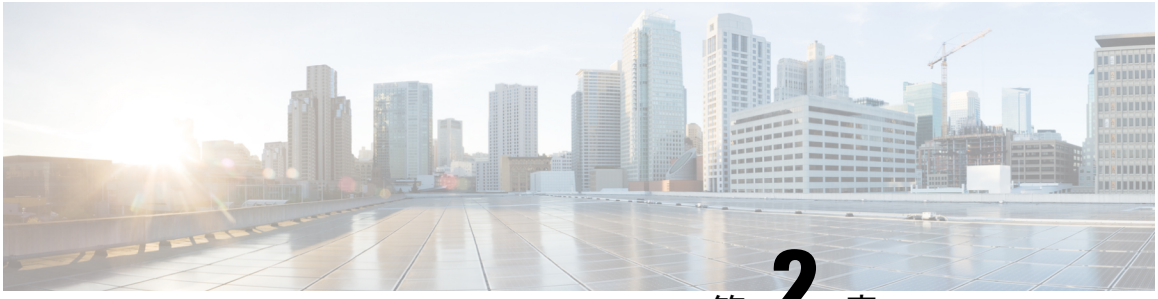
- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。許可されたトラフィック（デフォルト）とブロックされたトラフィックの間でフィルタ処理できます。

- **トップ侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。許可されたイベント（デフォルト）とブロックされたイベントの間でフィルタ処理できます。



アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目に関する詳細を知りたい場合は、関連するドキュメントへのリンクが提供されます。



第 2 章

Security Cloud Control Firewall Management のスタートアップガイド

- Cisco Security Cloud Control の概要 （11 ページ）
- Security Cloud Control Firewall Management の概要 （14 ページ）
- クラウド提供型 Firewall Management Center の概要 （17 ページ）
- Security Cloud Control Firewall Management のプロビジョニング （24 ページ）
- Security Cloud Control Firewall Management を開く （25 ページ）
- ファイアウォール管理ダッシュボード （26 ページ）

Cisco Security Cloud Control の概要

Security Cloud Control は、単一の統合インターフェイスからセキュリティ製品を管理し、セキュリティの成果を達成できるようにするセキュリティ プラットフォームです。

プラットフォームにセキュリティ製品を統合すると、エクスペリエンスが合理化になります。Cisco セキュリティ製品のサブスクリプションを購入すると、購入したすべてのサブスクリプションに関する単一の要求コードが記載された電子メールが 1 件届きます。新しい Security Cloud Control 組織に要求コードを入力すると、すべての製品が同時に Cisco Security Cloud Control にプロビジョニングされます。

Security Cloud Control では、ユーザーとグループの管理はプラットフォームレベルで行われます。これらのユーザーとグループにロールが割り当てられ、Security Cloud Control および統合製品を管理する権限が定義されます。

製品とツール間の移動は直感に行うことができ、すべての統合製品に共通のプラットフォームメニューとツールバーが標準化されています。

Security Cloud Control は、プラットフォーム上のすべての統合製品に次のコアサービスを提供します。

- **プラットフォーム管理**：ロールベースのアクセス制御の管理、サブスクリプションの要求、製品インスタンスの標準化された地域展開などの一般的なサービスは、Security Cloud Control によって提供されます。Security Cloud Control では、これらの機能を一元化することで、プラットフォームから管理されるすべての Cisco Security 製品間でのプロビジョニ

ングおよびアクセス管理における一貫したユーザーエクスペリエンスが保証されます。管理者は、Security Cloud Control のメインナビゲーションバーにある プラットフォーム管理メニューからこれらの共通サービスにアクセスします。

- **人工知能アシスタント**：Security Cloud Control の Cisco AI Assistant は、AI 中心のインサイト、自動化、およびコンテキストガイダンスを提供することにより、セキュリティ業務を合理化するように設計されています。管理者がセキュリティポリシーを管理し、問題をトラブルシュートし、Firewall、Duo、および Secure Access などの Cisco のセキュリティ製品全体で設定を最適化するのに役立ちます。Cisco Assistant は、自然言語処理とクロスプラットフォームインテリジェンスを活用することで、効率を向上させ、インシデント対応を迅速化し、セキュリティワークフローを簡素化します。
- **Global Search**：プラットフォーム内の製品全体の値を検索する機能です。
- **Shared Objects**：デバイスやポリシー間で共有できるオブジェクトを作成および管理します。
- **Unified documentation portal**：すべてのドキュメントにアクセスできる、ドキュメントの「ヘルプ」エクスペリエンス。

Security Cloud Control と統合される製品：

Security Cloud Control からは、次のすべてのセキュリティ製品を管理できます。

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- セキュアなアクセス

Security Cloud Control から起動できる製品

Security Cloud Control から、これらのセキュリティ製品を起動できます。起動後、これらの製品はスタンドアロン製品として動作するため、Security Cloud Control を介して管理することはできません。このような製品のライセンスは Security Cloud Control からのみ要求または非アクティブ化できます。

[Cisco Security Cloud Control] ツールバーで、9 ドットメニュー をクリックすると、次の製品が起動します：

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control によってサポートされる製品およびソリューション

現在、Security Cloud Control と統合できる製品は次のとおりです。

AI Defense：AI Defense はAIのユーザーとプロバイダーのリスクに対処します。Security Cloud Controlのネットワーク可視性と適用ポイントを使用して、AI Defense では、分散クラウド環境全体で承認済みおよび未承認の AI ワークロード、アプリケーション、モデル、データ、およびユーザーアクセスを検出するための検出と適用の手順が追加されます。AI を搭載したサービスを開発および提供する組織の場合、AI Defense は提供前に AI モデルの脆弱性を検出します。プロンプトインジェクション、サービス妨害（DoS）、データ漏洩といった急速に進化する脅威から AI アプリケーションを保護します。詳細については、「AI Defenseのドキュメント」を参照してください。

Security Cloud Control Firewall Management： Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのセキュリティポリシーマネージャで、シスコのファイアウォールやその他のデバイス全体でポリシーを簡素化および統合します。 詳細については、『Cisco Security Cloud Control ドキュメント』の「ファイアウォール」を参照してください。

Multicloud Defense：Multicloud Defense は、マルチクラウドセキュリティに対する簡素化および高度に自動化されたアプローチを提供します。このソリューションにより、組織は単一の SaaS 提供コントロールプレーンと、一元化または分散された PaaS 提供データプレーンアーキテクチャを使用して、マルチクラウド環境を管理および保護できます。 Multicloud Defense では、すべての主要なクラウドプロバイダーで継続的な可視性、統合された保護、およびダイナミックなポリシー更新が提供されるため、各クラウドプロバイダーごとにソリューションごとに個別のポイントソリューションを用意する必要がなくなります。詳細については、「Multicloud Defenseのドキュメント」を参照してください。

セキュアなアクセス：Cisco セキュアなアクセス は、インターネットベースの脅威に対して複数のレベルの防御を提供するクラウドベースのプラットフォームです。組織のネットワークから接続する場合でも、ネットワークからローミングする場合でも、インターネット、SaaS アプリケーション、およびプライベート デジタル リソースに安全に接続できます。ポリシールールを使用して、リソース、ユーザー、デバイスのコレクションにセキュリティ管理を構成および適用します。 詳細については、「Secure Access Documentation」を参照してください。セキュアなアクセス サブスクリプションには、追加料金なしで Security Cloud Control を介した アイデンティティ インテリジェンス 統合も含まれます。これには、スタンドアロン アイデンティティ インテリジェンス ダッシュボードへのアクセスは含まれません。詳細については、「Cisco Identity Intelligence と Cisco Secure Access の統合」を参照してください。

Cisco XDR (Extended Detection and Response)：Cisco XDR は、セキュリティ運用を簡素化し、インシデント対応を迅速化するように設計されたクラウドネイティブの拡張可能なセキュリティソリューションです。エンドポイント、ネットワーク、ファイアウォール、電子メール、アイデンティティ、およびDNSを含む複数のソースからテレメトリを収集および分析し、Cisco Talos から提供される強化されたコンテキストと脅威インテリジェンスを使用して高度な脅威を検出します。

Cisco XDR は潜在的なリスクと影響に基づいて脅威に優先順位を付け、誤検出を減らし、AI 中心のガイダンスと自動化を提供して調査と修復を合理化します。この統合アプローチにより、セキュリティ オペレーション センター（SOC）チームは、マルチベクトル、マルチベンダー環境でシスコおよびサードパーティのセキュリティツールの両方を統合することで、より迅速に行動でき、生産性を向上させ、サイバーレジリエンスを構築できます。詳細については、「Cisco XDR ヘルプセンター」を参照してください。

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management、旧 Cisco Defense Orchestrator は、分散環境でのセキュリティポリシー管理を簡素化します。これにより、管理対象のファイアウォールやデバイス間で一貫したポリシーを維持できます。Security Cloud Control では、**ファイアウォール**は**製品**（**Products**）に表示されます。

Security Cloud Control Firewall Management は、不整合を特定し、解決ツールを提供することにより、セキュリティポリシーを最適化します。また、オブジェクト共有、ポリシー共有、および設定テンプレートもサポートされているため、デバイス間で一貫した設定を適用できます。

Security Cloud Control Firewall Management は、Adaptive Security Device Manager（ASDM）などのローカルデバイスマネージャと共存できます。他のマネージャが行った設定変更を追跡し、必要に応じて違いを調整します。

このプラットフォームには、脅威防御 デバイスを オンプレミス Firewall Management Center または クラウド提供型 Firewall Management Center にオンボーディングするのに役立つガイド付き Day 0 エクスペリエンスが含まれています。主要な機能に焦点を当てており、それらの機能をアクティブ化および設定するのに役立ちます。

デバイスのオンボーディング要件

デバイスをオンボーディングする前に、次の前提条件を満たしてください。

- インストールウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスをオンボーディングします。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスをオンボーディングした後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

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

Security Cloud Control Firewall Management 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	時刻 （24 時間表記、UTC）
Thursday	09:00 UTC - 12:00 UTC

Security Cloud Control Firewall Management のアップグレード期間中も、引き続き組織と クラウド提供型 Firewall Management Center にアクセスできます。さらに、Security Cloud Control Firewall Management 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）

- Security Cloud Control Firewall Managementのメンテナンス期間中は、管理対象デバイスへの設定の作成または展開を行わないでください。
- Security Cloud Control Firewall Management 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、Cisco は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 Firewall Management ライセンス

Security Cloud Control Firewall Management では、組織の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 Firewall Management 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 Firewall Management 組織が提供されます。Security Cloud Control Firewall Management 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です。

Security Cloud Control Firewall Management 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

Security Cloud Control Firewall Management 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 Firewall Management 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 Firewall Management 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 Firewall Management 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 Firewall Management 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 Firewall Management の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 Firewall Management 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）

- Catalyst SD-WAN には Security Cloud Control Firewall Management と統合するために追加のライセンスは必要ありません。Cisco Digital Network Architecture（DNA）または WAN Essentials ライセンスを持つお客様は、他のライセンスは必要なく、これらの既存のライセンスを統合に使用できます。
-

（注） Cisco Smart Licensing ポータルから Security Cloud Control Firewall Management 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 Firewall Management 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

セスが追加料金なしで利用できます。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 Firewall Management ソリューションサポートを活用することもできます。

その他のサポート対象デバイスとライセンス

クラウド提供型 Firewall Management Center を通じて Cisco Secure Firewall Threat Defense デバイスをサポートすることに加えて、Security Cloud Control は次のデバイスも管理します。

- Cisco Secure Firewall ASA
- オンプレミスの Cisco Secure Firewall Management Center
- Cisco Meraki セキュリティアプライアンス
- Cisco IOS デバイス
- SSH を使用してアクセス可能なデバイス
- Amazon Web Services（AWS）仮想プライベートクラウド（VPC）
- Umbrella 組織

Security Cloud Control 基本資格ライセンスと、管理するデバイスに固有のライセンスが必要です。

クラウド提供型 Firewall Management Center の概要

クラウド提供型 Firewall Management Center は、Security Cloud Control Firewall Management を介して Cisco Secure Firewall Threat Defense デバイスを管理する Software-as-a-Service（SaaS） 製品です。オンプレミス Firewall Management Center と同じ機能の多くが用意されています。

クラウド提供型 Firewall Management Center は オンプレミス Firewall Management Center と外観および動作が同じであり、同じ FMC API を使用します。

SaaS 製品であるため、Security Cloud Control Firewall Management オペレーションズチームが クラウド提供型 Firewall Management Center ソフトウェアを展開し、保守します。新機能が導入されると、オペレーションズチームがお客様の Security Cloud Control Firewall Management 組織のクラウド提供型 Firewall Management Center を更新します。

移行とオンボーディングの詳細

脅威防御 デバイスを オンプレミス Firewall Management Center から クラウド提供型 Firewall Management Center に移行するために、移行ウィザードを使用できます。

デバイスは、移行する前に次のいずれかの 脅威防御 ソフトウェアリリースを実行する必要があります。

- オンプレミス Firewall Management Center の最小リリース：7.2

- 脅威防御 の最小リリース：7.2.x（バージョン 7.1 ではサポート対象外）

脅威防御 7.1 リリースは移行ではサポートされていません。

シリアル番号を入力するか、登録キーを含むCLIコマンドを使用するなど、使い慣れた方法を使用して、Security Cloud Control Firewall Management の 脅威防御 デバイスをオンボーディングします。

オンボーディング後

- デバイスは Security Cloud Control Firewall Management と クラウド提供型 Firewall Management Center の両方に表示されます。
- クラウド提供型 Firewall Management Center でデバイスを設定します。
- Security Cloud Control Firewall Management では、バージョン、設定ステータス、接続、正常性ステータス、ノードステータスなどのデバイス情報を確認できます。
- Security Cloud Control Firewall Management で正常性ステータスをクリックすると、クラウド提供型 Firewall Management Center ユーザーインターフェイスで、デバイスのヘルスモニタリングページが開きます。

可用性およびセキュリティ分析

Security Cloud Control Firewall Management は、データインターフェイスを介して管理する 脅威防御 デバイスの高可用性をサポートします。この機能は、ソフトウェアバージョン 7.2 以降を実行するデバイスでサポートされています。

Security Analytics and Logging（SaaS）または Security Analytics and Logging（オンプレミス）を使用して、オンボーディングされた Threat Defense デバイスで生成されたセキュリティイベントを分析できます。

- Security Analytics and Logging （SaaS）では、イベントがクラウドに保存され、それらのイベントは Security Cloud Control Firewall Management で表示します。
- Security Analytics and Logging（オンプレミス）では、オンプレミスの Secure Network Analytics アプライアンスでイベントが保存され、分析は オンプレミス Firewall Management Center で行われます。

どちらの場合も、選択したログコレクタにファイアウォールから引き続きログを直接送信できます。

ライセンス

クラウド提供型 Firewall Management Center のライセンスはデバイスごとに管理されるライセンスであるため、クラウド提供型 Firewall Management Center 自体のライセンスは不要です。既存の Cisco Secure Firewall Threat Defense デバイスは既存のスマートライセンスを再利用し、新しい Cisco Secure Firewall Threat Defense デバイスは Cisco Secure Firewall Threat Defense に導入された各機能に対して新しいスマートライセンスをプロビジョニングします。詳細については、「クラウド提供型 Firewall Management Center ライセンス」を参照してください。

既存のお客様は、引き続き Security Cloud Control を使用して、Cisco Secure Firewall ASA、Meraki、Cisco IOS デバイス、Umbrella、AWS 仮想プライベートクラウドなどの他のデバイスタイプを管理できます。Security Cloud Control を使用して、Firepower Device Manager によるローカル管理用に構成された Cisco Secure Firewall Threat Defense デバイスを管理する場合、Security Cloud Control で引き続き管理できます。

テナントで クラウド提供型 Firewall Management Center をプロビジョニングする方法については、「Cisco Security Cloud Control テナントでのクラウド提供型 Firewall Management Center の有効化」を参照してください。

クラウド提供型 Firewall Management Center の完全な管理者ガイドについては、『Managing Cisco Secure Firewall Threat Defense with Cloud-delivered Firewall Management Center』を参照してください。

クラウド提供型 Firewall Management Center を有効にする

Cisco Secure Firewall Threat Defense デバイスを管理する場合は、テナントでクラウド提供型 Firewall Management Center を有効にすることができます。このタスクを実行するには、管理者またはネットワーク管理者のユーザーロールが必要です。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 Security Cloud Control メニューから、**管理（Administration）** > **統合（Integrations）** > **Firewall Management Center**の順に選択し、[クラウド提供型FMCの有効化（Enable Cloud-Delivered FMC）] をクリックします。

Security Cloud Control はバックグラウンドでクラウド提供型 Firewall Management Center インスタンスのプロビジョニングを開始します。通常、これが完了するまでに 15 ～ 30 分かかります。プロビジョニングの進行状況は、[クラウド提供型FMC（Cloud-Delivered FMC）] の [ステータス（Status）] 列で追跡できます。

プロビジョニングが完了すると、ステータスが [アクティブ（Active）] に変わります。また、Security Cloud Control 通知パネルと、着信ウェブフックを設定したアプリケーションにも、[クラウド提供型Firewall Management Centerの準備ができました（クラウド提供型 Firewall Management Center is Ready）] の通知が届きます。詳細については、「Notification Settings」を参照してください。

Note [クラウド提供型Firewall Management Centerの準備ができました（クラウド提供型 Firewall Management Center is Ready）] の通知を受信したら、テナントからログアウトして再度ログインし、[クラウド提供型FMC（Cloud-Delivered FMC）] の右側のペインオプション（[アクション（Actions）]、[管理（Management）]、[システム（System）] など）を確認します。

次に行う作業：

a. Cisco Smart Software Manager（CSSM）に クラウド提供型 Firewall Management Center を登録して、スマートライセンスをアクティブ化します。詳細な手順については、「Smart Software Manager への クラウド提供型 Firewall Management Center の登録」を参照してください。

b. Firewall Threat Defense デバイスを クラウド提供型 Firewall Management Center に対してオンボーディングし、管理します。

Security Cloud Control Firewall Management で クラウド提供型 Firewall Management Center バージョンを確認する

クラウド提供型 Firewall Management Center バージョンに関する情報は、主に移行計画、機能サポートの検証、障害対応、ライセンス、および運用管理に必要です。

Security Cloud Control Firewall Management で使用している クラウド提供型 Firewall Management Center の現在のバージョンを確認するには、この手順を使用します。

始める前に

組織でクラウド提供型 Firewall Management Center を有効化します。

手順の概要

1. Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
2. 左側のペインで、**[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** の順にクリックします。
3. [FMC] タブの [バージョン（Version）] 列にバージョンが表示されます。

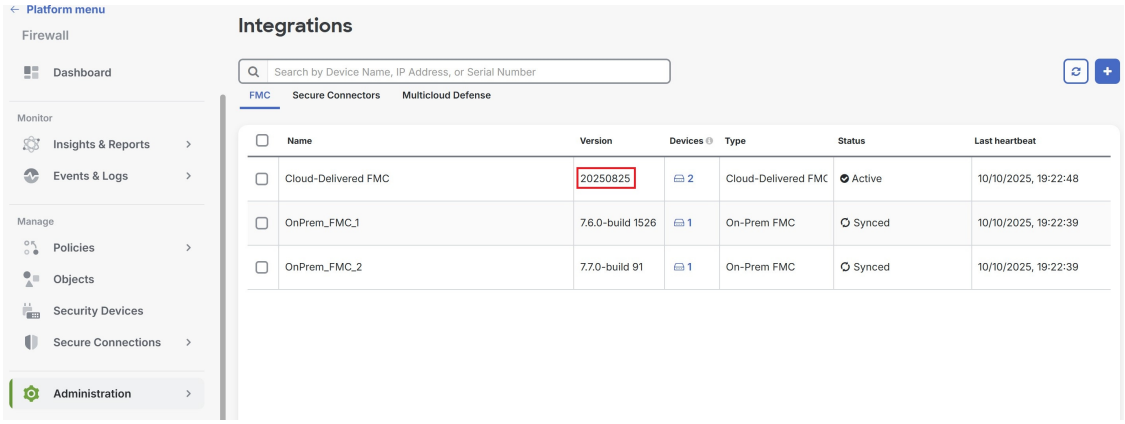
手順の詳細

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、**[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** の順にクリックします。

ステップ 3 [FMC] タブの [バージョン（Version）] 列にバージョンが表示されます。



クラウド提供型 Firewall Management Center のバージョンの詳細については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

クラウド提供型 Firewall Management Center ライセンスと登録

クラウド提供型 Firewall Management Center の場合と同じように、オンプレミス Firewall Management Center を Cisco Smart Licensing に登録します。

概要

クラウド提供型 Firewall Management Center は、Security Cloud Control Firewall Management の基本サブスクリプションおよびトライアルに含まれています。クラウド提供型 Firewall Management Center のライセンスを個別に購入する必要はありません。基本サブスクリプションまたはトライアルは クラウド提供型 Firewall Management Center をカバーしており、クラウドを介して Firewall Threat Defense のデバイスを管理できます。

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います。

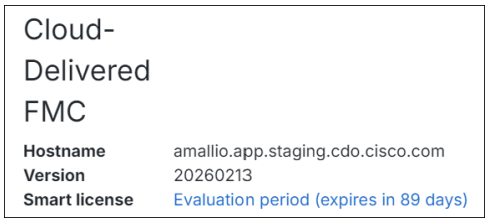
重要 RAVPN や SSL VPN などのエクスポート暗号化を必要とする機能を含むすべての機能にアクセスするには、展開後すぐに Cisco Smart Software Manager に クラウド提供型 Firewall Management Center を登録することを強く推奨します。早期登録により、機能の制限や展開の中断が防止されます。

評価ライセンス

- リモートアクセス VPN、SSL VPN、およびその他の暗号化依存オプションなど、エクスポート暗号化を必要とする機能は、クラウド提供型 Firewall Management Center を Cisco Smart Software Manager（CSSM）に登録するまで無効のままです。

- 90 日間の評価期間が終了した後も、Firewall Threat Defense デバイスのオンボーディングを続行できますが、CSSM への登録が完了するまで、手動でトリガーされた展開またはスケジュールされた展開はブロックされます。
- 評価ライセンスの有効期限が近づいている場合、Security Cloud Control Firewall Management はアラート通知を送信します。

（注） 評価ライセンスの期限が切れると、[スマートライセンス（Smart license）] フィールドに警告が表示されます。



この期間が終了すると、クラウド提供型 Firewall Management Center は登録解除されます。Cisco Smart Software Manager に クラウド提供型 Firewall Management Center を登録すると、評価モードから完全にライセンスされた状態に変換されます。

評価警告のリンクをクリックしてスマートライセンシングの登録ページを開き、クラウド提供型 Firewall Management Center を Cisco Smart Software Manager に登録します。

Cisco Smart Software Manager（CSSM）

- クラウド提供型 Firewall Management Center と同じプロセスに従って、オンプレミス Firewall Management Center をスマート ライセンス アカウントに接続します。このセクションでは、手順の概要を示します。
- クラウド提供型 Firewall Management Center に対してライセンスを個別に購入する必要はありません。ライセンスは登録時に自動的に適用されます。
- スマートライセンスに登録すると、暗号化エクスポート機能が有効になります。
- 登録すると、コンプライアンスが保証され、展開の問題が防止されます。

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。

Firewall Threat Defense デバイスのライセンス

- クラウド提供型 Firewall Management Center には、ライセンスを個別に購入する必要はありません。

- クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスにはそれぞれ個別のライセンスが必要です。
- クラウド提供型 Firewall Management Center を CSSM に登録すると、管理者はセキュリティデバイスに機能ライセンスを適用できます。

登録ステップバイステップ

手順の概要は次のとおりです。詳細は「スマート ソフトウェア マネージャーで管理センターを登録する」を参照してください。

1. スマートアカウントの作成またはアクセス：

   Cisco Smart Software Manager アカウントを持っていることを確認します。次がない場合は、Smart Software Manager で作成します。

2. 登録トークンの生成または登録トークンの使用：

   Smart Software Manager で、既存の有効な登録トークンを使用するか、クラウド提供型 Firewall Management Center を登録する仮想アカウントの登録トークンを生成します。

   1. **[Inventory] > [New Token]** の順に選択します。
   2. 説明を入力し、有効期限を設定します（シスコでは 30 日を推奨）。
   3. トークンを作成し、コピーします。

3. クラウド提供型 Firewall Management Center をトークンに登録します。

   1. クラウド提供型 Firewall Management Center インターフェイスにログインします。
   2. **[System] > [Licenses] > [Smart Licenses]** に移動します。
   3. **[Register]** をクリックし、**[Product Instance Registration Token]** フィールドに登録トークンを貼り付けます。
   4. トークンの前後に余分なスペースや空白行がないことを確認してください。
   5. [変更を適用（Apply Changes）] をクリックします。

4. 登録の確認

   登録後、**[System] > [Licenses] > [Smart Licenses]** でライセンスステータスを確認し、登録が成功し、ライセンスが適用され、「輸出規制機能」が有効になっていることを確認します。

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

組織に クラウド提供型 Firewall Management Center を展開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）
- クラウド提供型 Firewall Management Center のメンテナンス期間中は、管理対象デバイスへの設定の作成または展開を行わないでください。
- 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 Firewall Management のプロビジョニング

このトピックでは、Security Cloud Control 内でファイアウォールをプロビジョニングするために必要な手順の概要について説明します。ファイアウォールのプロビジョニングには、組織のファイアウォール機能の有効化、サブスクリプションの要求、およびセキュアなネットワーク管理のための環境の準備が含まれます。このプロセスにより、組織のファイアウォールサービスが正しくセットアップされ、設定とポリシー展開の準備が整います。

手順

ステップ 1 Security Cloud Sign On アカウントを使用して Security Cloud Control にサインインします。アカウントを持っていない場合は作成します。

Security Cloud Sign On アカウントを作成するには、アカウント有効化メールの送信先メールアドレスを入力する必要があります。すべての Security Cloud Sign On ユーザーアカウントで、Duo 多要素認証（MFA）を使用する必要があります。Duo MFA は、Security Cloud Sign On アカウントに無料で含まれています。

Security Cloud Sign On アカウントの作成方法の詳細については、「Security Cloud Sign On」を参照してください。.

（注） Security Cloud Sign On アカウントをすでにお持ちの場合は、「Signing in to Security Cloud Control」を参照してください。

ステップ 2 組織を作成し、優先地域を設定します。「組織の作成」を参照してください。

ステップ 3 （オプション）Security Cloud Control でファイアウォール管理を有効にします。

新しい Security Cloud Control 組織があり、Security Cloud Control のファイアウォールの使用権限はあるものの、まだサブスクリプションコードがない場合は、この手順を使用してファイアウォール アプリケーションを有効にできます。詳細については、「Security Cloud Control Firewall Management の有効化」を参照してください。

ステップ 4 サブスクリプションコードを受け取ったら、製品インスタンスのサブスクリプションを要求するために、Security Cloud Control のウェルカムメールで受信した要求コードを入力します。詳細については、「Claim your Product Subscription」を参照してください。新しい製品インスタンスをアクティブにします。

（注） 請求サブスクリプションプロセスを理解する必要がある場合は、「Overview of the Claim Subscription」を参照してください。

ステップ 5 製品組織にドメインを追加します。詳細については、「Add and Claim your Domain」を参照してください。

ステップ 6 アイデンティティ プロバイダーを Security Cloud Sign On アカウントと統合します。詳細については、「アイデンティティ プロバイダーとの統合」を参照してください。

ステップ 7 ユーザーとグループを作成し、正確な製品管理と制御用のロールを割り当てます。ロールベースアクセスの詳細については、「Role-based Access Control」を参照してください。

Security Cloud Control Firewall Management を開く

このトピックでは、Security Cloud Control でファイアウォール アプリケーションに移動する手順について説明します。

Cisco Security Cloud Sign-On アカウントがあり、ファイアウォールが組織の Security Cloud Control 内でプロビジョニングされていることを確認してください。詳細については、「Security Cloud Control Firewall Management のプロビジョニング」を参照してください。

手順

ステップ 1 https://security.cisco.com/ にアクセスして、Security Cloud Control を開きます。

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

ステップ 3 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ファイアウォール管理ダッシュボード

ファイアウォールダッシュボードは、さまざまなカテゴリ全体でテナントレベルの詳細をモニタリングおよび管理するための中心ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

左側のペインで、[ダッシュボード（Dashboard）] をクリックします。

ダッシュボードのカスタマイズ

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードに表示するウィジェットを選択または選択解除します。
3. ウィジェットをドラッグアンドドロップして、希望に応じて配置できます。

ダッシュボードは、**[Top Insights & Alerts]**、**[Top Actions]**、および **[Top Information]** の 3 つの主要なセクションに分割されています。各セクションでは、最適なセキュリティおよび運用管理を維持するために役立つさまざまなカテゴリのインサイトが提供されます。

上位のインサイトとアラート

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。エレメントフロー、RA VPN 予測、アクセス制御ポリシーの異常、CPU およびメモリの使用率が高い、Snort CPU およびメモリの使用率が原因で発生する高トラフィックに関連するインサイトを表示できます。

上位アクション

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。有効にすると、次のウィジェットが表示できます。

- **[ポリシーアナライザおよびオプティマイザ（Policy Analyzer and Optimizer）]**：セキュリティポリシーを分析し、異常を検出し、ファイアウォールのパフォーマンスを向上させるための最適化推奨事項を提供します。

  詳細については、「ポリシーアナライザおよびオプティマイザ」を参照してください。

- **Insights**：設定、正常性と操作、トラフィックとキャパシティなどのカテゴリごとに、アクティブなインサイトと傾向を表示します。

  詳細については、「 Insights」を参照してください。

- **[機能の導入（Feature Adoption）]**：使用状況を評価して改善できる機能の導入率を示します。

  詳細については、「機能の導入状況の評価と改善」を参照してください。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。テナントに対して有効になっている機能に応じて、次のウィジェットを表示できます。

- **設定状態（Configuration States）**：デバイス設定を Security Cloud Control によって維持される設定と比較して、不整合や競合を特定できます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理（Change Log Management）**：完了した変更ログと保留中の変更ログを表示して、運用の変更を追跡できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「変更ログ」を参照してください。

- **RA VPN セッション（RA VPN Sessions）**：リモートアクセス VPN セッションのアクティビティを表示します。

  詳細については、「RA VPN セッション」を参照してください。

- **インベントリ全体（Overall Inventory）**：デバイスの総数を表示し、問題、保留中のアクション、その他、およびオンラインに分けてデバイスをグループ化します。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN（Site-to-Site VPN）**：VPN トンネルの総数と、アクティブおよびアイドルのトンネルの割合が表示されます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

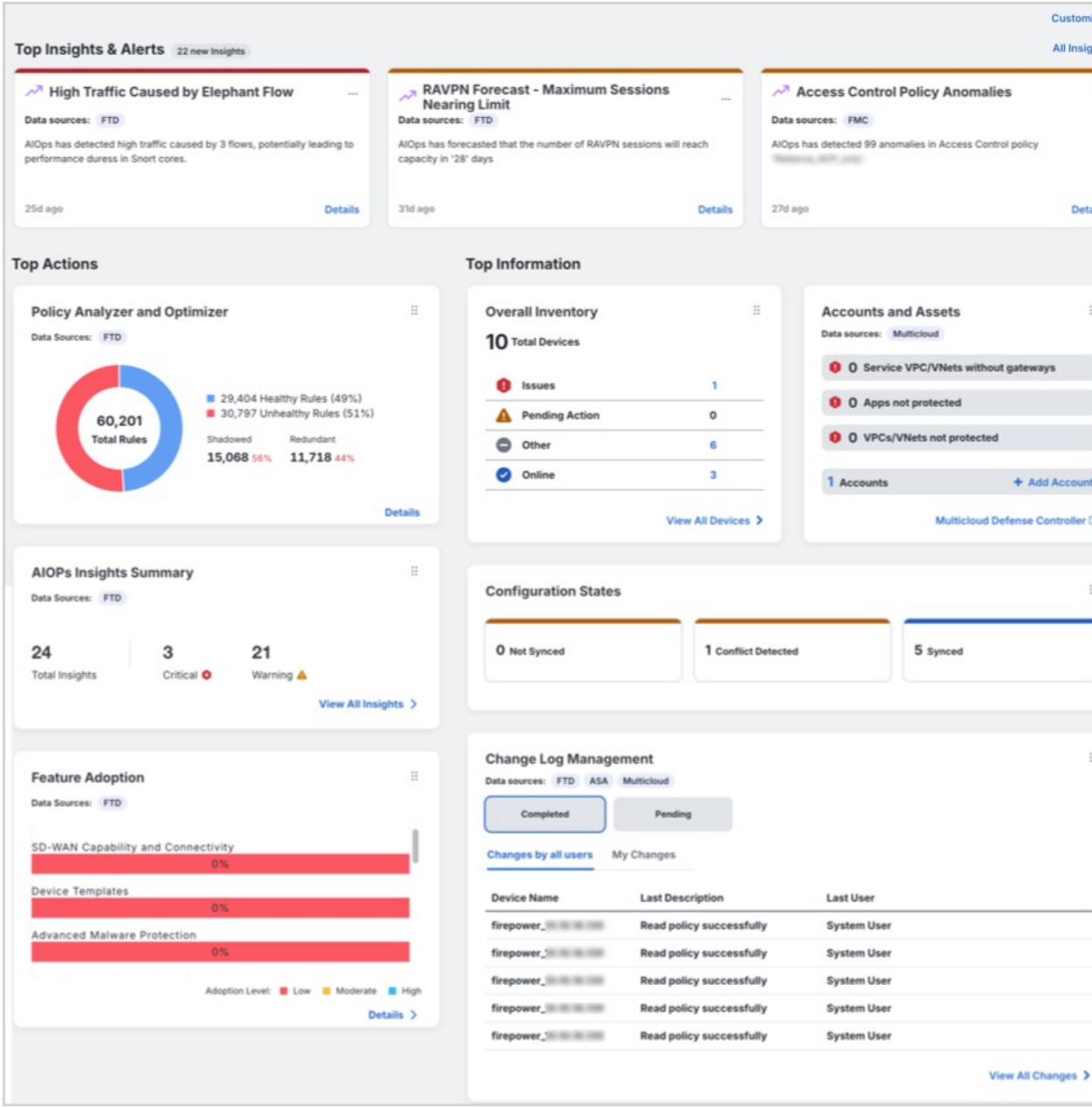
- **アカウントとアセット**：

  - マルチクラウドのアカウントとリソースを効果的に追跡して管理するのに役立ちます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

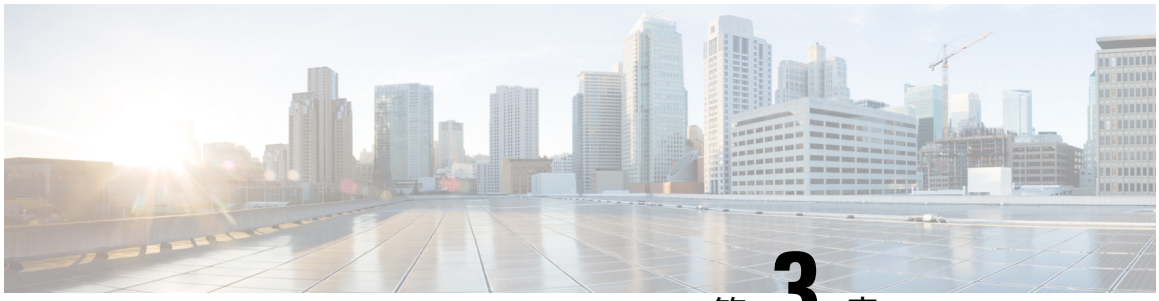
- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。許可されたトラフィック（デフォルト）とブロックされたトラフィックの間でフィルタ処理できます。

- **トップ侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。許可されたイベント（デフォルト）とブロックされたイベントの間でフィルタ処理できます。



アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目に関する詳細を知りたい場合は、関連するドキュメントへのリンクが提供されます。



第 3 章

Security Cloud Control Firewall Management でのファイアウォール管理

組織の Security Cloud Control Firewall Management を管理する場合に、この章を活用してください。組織全体のファイアウォール設定、ユーザーアクセス、通知、ロギングの可視性、およびロールの権限を管理する方法について説明します。

ここでは、次の情報を提供します。

- 全般設定
- APIユーザー管理
- ロギングの設定

ファイアウォール管理設定で制御する対象

ファイアウォール管理設定は管理対象の組織全体に適用され、複数のデバイスやユーザーに影響を与える可能性があります。一部のトグルボタンは、管理対象組織に対して関連機能が有効になっている場合にのみ表示されます。

- 一般設定の設定, on page 29
- Security Cloud Control 組織内のユーザーとグループの管理 （39 ページ）
- Security Cloud Control Firewall Management の API 専用ユーザーの管理 （39 ページ）
- Security Cloud Control 通知の表示 （40 ページ）
- ロギング設定の表示, on page 43
- **Security Cloud Control Firewall Management のユーザーロールを理解する**, on page 44
- セキュリティデバイス、ポリシー、およびオブジェクトページのフィルタ処理 （48 ページ）

一般設定の設定

管理対象組織内の複数の管理対象デバイスとユーザーに影響する組織全体の設定を管理するには、**管理（Administration）** > **一般設定（General Settings）** を使用します。

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

ファイアウォールのAI Assistantの有効化

人工知能アシスタントは、セキュリティポリシー、問題のトラブルシュート、および設定の最適化を管理するためのコンテキストガイダンスとインサイトを提供する、AI 中心のバーチャルコンパニオンです。詳細については、「Cisco AI Assistantのオンボーディング」を参照してください。

デフォルトでは 人工知能アシスタント は有効に設定されています。人工知能アシスタント を有効または無効にすると、管理対象組織のすべてのユーザーが影響を受けます。

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。
ステップ 3 **[Enable 人工知能アシスタントfor Firewall]** トグルボタンをオフにして、人工知能アシスタント を無効にします。

デバイスの変更を自動承認するオプションを有効にします

この設定を有効にすると、Security Cloud Control Firewall Management はユーザーがデバイスで直接行った変更を自動的に受け入れます。この設定を無効のままにするか、後で無効にする場合は、変更を承認する前に各デバイスの競合を確認する必要があります。

デバイスの変更の自動承認を有効にするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。
ステップ 3 **[Enable the option to auto-accept device changes]** トグルボタンをオンにします。

Multicloud Defense SCC 機能の有効化

この機能を有効にすると、Multicloud Defense と、Security Cloud Control Firewall Management によって管理される ASA デバイスおよび Firewall Threat Defense デバイスとの間にサイト間 IPsec VPN トンネルを設定できます。この機能を有効にした後、これらの管理対象デバイス間で VPN 設定を確立して展開することで、マルチクラウドインフラストラクチャ全体のセキュアな接続を向上させることができます。

Multicloud Defense Security Cloud Control Firewall Management 機能を有効にするには、次の手順を実行します。

Procedure

ステップ 1 左側のペインで、**[Settings]** > **[General Settings]** の順に選択します。

ステップ 2 [Multicloud Defense SCC機能の有効化（Enable Multicloud Defense SCC features）] トグルボタンをオンにします。

Multicloud Defense とのオブジェクト共有の有効化

Security Cloud Control Firewall Management から Multicloud Defense ネットワークオブジェクトを共有するには、この設定を有効にします。

Multicloud Defense とのオブジェクト共有を有効にするには、次の手順を実行します。

手順の概要

1. **管理（Administration）** > **一般設定（General Settings）** の順に選択します。
2. **[Enable object sharing with Multicloud Defense]** トグルボタンをオンにします。

手順の詳細

手順

ステップ 1 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 2 **[Enable object sharing with Multicloud Defense]** トグルボタンをオンにします。

ASAヘルスモニタリングの有効化

管理対象組織レベルでデバイス正常性メトリックを有効にする必要があります。Secure Device Connector によって管理される Cisco ASA デバイスについては、個々のデバイスレベルでも機

能を有効にする必要があります。これらの手順により、正常性データが収集され、ダッシュボード内で分析できるようになります。

この機能を有効にして使用するには、**ネットワーク管理者**のユーザーロールが必要です。

管理対象組織に対してCisco ASAヘルスモニタリングを有効にするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）**を選択します。

ステップ 3 **[Enable ASA Health Monitoring]** トグルボタンをオンにして、管理対象組織のデバイス正常性メトリック機能を有効にします。

デバイスタイプに関する考慮事項

- クラウドデバイスゲートウェイ（CDG）によって管理される Cisco ASA デバイスの場合、**[General Settings]**で**[Enable Device Health Metricsの]** トグルを有効にすると、正常性メトリックは有効になります。
- Secure Device Connector（SDC）によって管理される Cisco ASA デバイスについて、各デバイスの正常性メトリックを手動で有効にします。
  a. **[Security Devices]**を選択します。
  b. SDC 管理対象 Cisco ASA デバイスを選択します。
  c. **[Device Actions]** ペインで、**[Opt-in to Health Metrics]** を選択します。

  デバイスがすでにオプトインしている場合は、代わりに **[Opt-out of Health Metrics]** オプションが表示されます。

Note 各 SDC は、最大 50 台の Cisco ASA デバイスの正常性メトリックのコレクションをサポートできます。

デフォルトの競合検出間隔の設定

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

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

デフォルトの競合検出間隔を設定するには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。
ステップ 3 **[Default Conflict Detection Interval]** のドロップダウンメニューをクリックし、時間の値を選択します。

自動展開をスケジュールするオプションを有効にする

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。このオプションを有効にすると、単一の自動展開をスケジュールしたり、定期的な自動展開を設定したりできます。

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

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

Important 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。

スケジュールされた自動展開を有効にするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 管理（**Administration**）> 一般設定（**General Settings**）を選択します。

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

Web 分析の管理

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

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

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 管理（**Administration**）> 一般設定（**General Settings**）を選択します。

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

FDM デフォルトの定期バックアップスケジュールを設定する

この設定を使用して、デバイスのデフォルトの定期バックアップスケジュールを設定します。デバイスのバックアップをスケジュールする際に、デフォルト値を使用するか、カスタマイズすることができます。デフォルトの定期バックアップスケジュールを変更しても、既存のスケジュールされたバックアップはそのままの設定を保持します。

FDM のデフォルトの定期バックアップスケジュールを設定するには、次の手順に従います。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 管理（**Administration**）> 一般設定（**General Settings**）を選択します。

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

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

ステップ 5 毎週バックアップする場合は、バックアップする曜日を選択します。毎月バックアップする場合は、**[Days of Month]** フィールドを選択し、バックアップを実行する日数を追加します。31 日未満の月に「31 日」と

入力した場合、その月のバックアップは実行されません。バックアップスケジュールの名前と説明を入力します。

ステップ 6 [保存（Save）] をクリックします。

Cisco Security Cloudからのオンプレミスfmcの自動オンボード

自動オンボーディング機能を無効にすると、Cisco Security Cloud テナントから新しい オンプレミス Firewall Management Center が自動的に追加されなくなります。

（注） ネットワーク管理者または管理者のみが、Security Cloud Control でこの機能を有効または無効にできます。

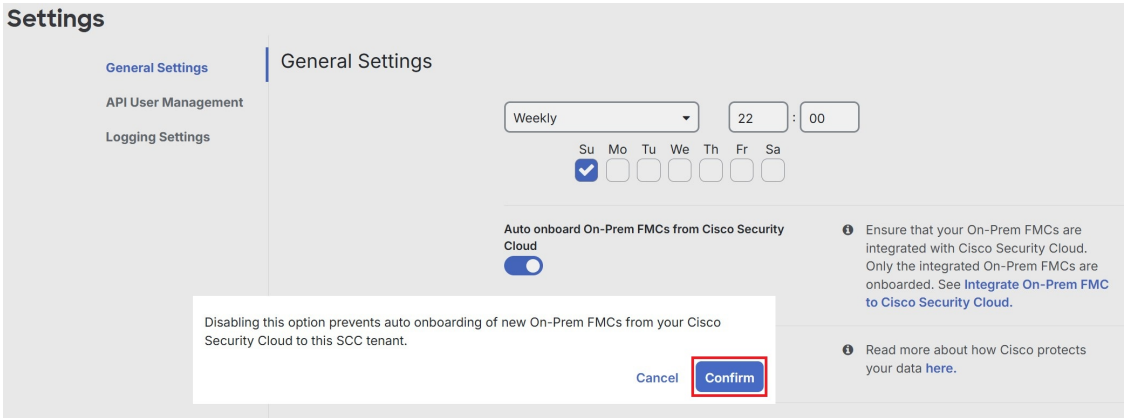
手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。

ステップ 3 [Cisco Security CloudオンプレミスFMCの自動オンボード（Auto onboard On-Prem FMCs from Cisco Security Cloud）] トグルボタンをオフにして、オンプレミス Firewall Management Center の自動オンボーディングを無効にします。

ステップ 4 [確認（Confirm）] をクリックします。



Talosとのイベントデータ共有の有効化

Ciscoの脅威インテリジェンス組織であるTalosと、デバイスからの悪意のあるイベントデータを共有します。イベントデータを共有することで、Talos の脅威インテリジェンス機能が向上

し、ネットワークにターゲットを絞ったセキュリティインサイトを提供して、新たな脅威に対する保護を強化できます。

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

（注） Security Cloud Control の [Talosとのイベントデータ共有を有効にする（Enable event data sharing with Talos）] 設定と、クラウド提供型 Firewall Management Center の [Talos脅威ハンティングテレメトリ（Talos Threat Hunting Telemetry）] オプションは別の設定です。Security Cloud Control の設定は、デバイスからの悪意のあるイベントのデータを Talos と共有します。

グローバル侵入ポリシーに脅威ハンティングルールを追加し、それらのルールからのイベントを Talos に送信するには、[Talos脅威ハンティングテレメトリ（Talos Threat Hunting Telemetry）] をクラウド提供型 Firewall Management Center の [管理（Administration）]>[設定（Configuration）]>[侵入ポリシーの設定（Intrusion Policy Preferences）] で有効にします。

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

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

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）**を選択します。

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

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

ファイアウォール管理インスタンスの詳細の表示

[ファイアウォール管理インスタンスの詳細（Firewall Management Instance Details）] は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。コピーアイコンをクリックすると、これらのテナントの詳細をコピーできます。

- [ファイアウォール管理インスタンス名（Firewall Management Instance Name）]：ファイアウォール管理インスタンスの表示名。
- [ファイアウォール管理インスタンスID（Firewall Management Instance ID）]：Cisco Security Cloud Controlのファイアウォール管理インスタンスでシステム生成された一意の識別子。
- [Secure Services Exchange ID]：Secure Services Exchange 環境内のファイアウォール管理インスタンスの一意の識別子。シスコは、クラウドサービス間でのサービス統合とバックエンドの相関にこの値を使用します。
- [Security Cloud Control Organization ID]：ファイアウォール管理インスタンスに関連付けられた Security Cloud Control 組織の一意の識別子。

Security Cloud Control Firewall Management プラットフォームナビゲータの使用

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

ネットワーキング アプリケーション

- **Cisco Catalyst**：Cisco Catalyst 製品は、さまざまなネットワークスイッチ、ワイヤレスコントローラ、ワイヤレスアクセスポイント、およびエッジプラットフォームとルータを含み、耐久性が高く堅牢なネットワーキング環境を必要とするエンタープライズクラスのビジネスニーズをサポートします。
- **Cisco Intersight**：Cisco Intersight はクラウド運用プラットフォームであり、先進的なインフラストラクチャのモジュラ型機能、ワークロードの最適化、およびKubernetesサービスなどのオプションで構成されます。Cisco Intersight インフラストラクチャ サービスには、物理および仮想インフラストラクチャの展開、モニタリング、管理、サポートが含まれます。Cisco Unified Computing System（Cisco UCS）、Cisco HyperFlex ハイパーコンバージドインフラストラクチャ（HCI）、およびその他 Intersight に接続されたサードパーティ製のターゲットをサポートします。
- **IoT Operations Dashboard**：Cisco IoT Operations Dashboard は、クラウドベースの IoT サービスプラットフォームであり、オペレーションズチームが産業用ネットワークデバイスおよび接続された大規模な産業資産に安全に接続し、接続を維持し、インサイトを得られるようにします。接続されているすべての産業資産が 1 ヵ所にまとめて表示されるため、業務チームは運用の合理化と事業継続に役立つ有益なインサイトを引き出すことができます。
- **Cisco Meraki**：Cisco Meraki は、Cisco Meraki デバイスの中央管理プラットフォームを提供する、IT および IoT クラウド管理型プラットフォームです。
- **Cisco Spaces**：Cisco Spaces はクラウドベースのロケーション サービス プラットフォームであり、組織は物理スペース内における人や物の移動に関するインサイトを得られます。

こうしたインサイトをもとに、有益で関連性の高い、コンテキストに応じたエンゲージメントを提供できます。組織は、人の移動を把握するだけでなく、資産の場所、移動、使用状況をモニタリングすることで、業務効率を向上させることができます。

- **Cisco ThousandEyes**：Cisco ThousandEyes は、Web アプリケーション、サービス、およびネットワークの可用性とパフォーマンスのモニタリングと測定をサポートするクラウドサービススイートです。任意のユーザーに対し、あらゆるネットワーク上のあらゆるアプリケーションがエンドツーエンドで可視化されるため、企業は問題の発生源を迅速に特定し、迅速に解決し、パフォーマンスを効果的に管理できます。
- **Cisco Workflows**：Cisco Workflows は、大規模な Cisco Networking Cloud ビジョンの一部であるクラウドホスト型自動化アプリケーションです。これは、Cisco のお客様に、クロスドメイン自動化機能を提供する権限を提供します。カスタムおよび既作成の自動化テンプレートと、Cisco が提供またはシスコが独自に構築するさまざまなアダプタオプションを使用して、Cisco アプリケーションとサードパーティアプリケーションの両方でエラーが発生しやすい反復的なタスクを合理化して、クラウドまたはオンプレミスのターゲットに到達します。

セキュリティ アプリケーション

- **Duo Security**：Cisco Duo は、すべてのユーザー、デバイス、およびアプリケーションを対象に、機密データへのアクセスを保護する二要素認証を備えた、ユーザー中心のゼロトラストセキュリティプラットフォームです。適応型ポリシー、シングルサインオン（SSO）、高度なエンドポイントの可視性などの機能を提供する、リモートアクセスの保護と事業継続性の維持のための包括的なソリューションです。
- **Cisco Secure Access**：Cisco Secure Access は、単一のクラウド管理コンソール、統合クライアント、一元化されたポリシー作成、および集約されたレポート作成機能によって IT の運用を簡素化します。1つのソリューションに統合された広範なセキュリティ機能（ZTNA、SWG、CASB、FWaaS、DNS セキュリティ、RBI など）により、ゼロトラストの原則を適用し、きめ細かいセキュリティポリシーを適用することで、セキュリティリスクを軽減します。市場をリードする Talos 脅威インテリジェンスによって比類のない脅威ブロッキングが促進され、リスクを軽減し、迅速な調査を可能にします。
- **Cisco Secure Endpoint**：Cisco Secure Endpoint（旧 Cisco AMP for Endpoints）は、侵害を防止し、脅威を迅速に検出、封じ込め、修復するように設計されたクラウド管理型のエンドポイント セキュリティ ソリューションです。高度な追跡機能を備えたクラウドベースのスキャナでファイルを即座にチェックできます。これらの機能により、セキュリティアナリストは初期のアウトブレイクソースを識別して隔離できます。このソリューションでは、悪意のあることがわかったファイルのレトロスペクティブ検疫も提供されます。
- **Cisco Security Provisioning and Administration**：Cisco Security Provisioning and Administration は、Cisco Security Cloud 全体で Cisco Secure 製品インスタンス、ユーザーアイデンティティ、およびユーザーアクセス管理を中央管理するための Web アプリケーションです。Security Cloud Control の管理者は、新しい Security Cloud エンタープライズの作成、エンタープライズ内のユーザーの管理、ドメインの要求、組織の SSO ID プロバイダーの統合などのタスクを実行できます。

- **Cisco XDR**：Cisco XDR は、セキュリティ運用を簡素化し、セキュリティチームが高度な脅威を検出、優先順位付けし、対応できるように設計されたクラウドベースのソリューションです。シスコとサードパーティの両方のセキュリティソリューションを統一されたプラットフォームに統合することで、Cisco XDR は脅威管理のための包括的なアプローチを提供します。Talos が提供する脅威インテリジェンスとの統合により、Cisco XDR は追加のコンテキストや資産に関するインサイトを使用してインシデントデータを強化し、誤検出を減らし、脅威検出、対応、およびフォレンジック機能全般を強化します。

Security Cloud Control 組織内のユーザーとグループの管理

このタスクの目的は、ロールベース アクセス コントロール（RBAC）を介してシスコ セキュリティ製品全体のユーザーアクセスを一元的かつ自動的に管理することです。

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

さらに、Security Cloud Control Firewall Management の API 専用ユーザーを作成できます。API 専用ユーザーを使用すると、システムは API 経由で Security Cloud Control と対話できるため、ユーザーインターフェイスは不要になります。

手順

ステップ 1 Security Cloud Control ホームページから、[プラットフォーム管理（Platform Management）] をクリックします。

ステップ 2 **[プラットフォーム管理（Platform Management）] > [アクセス管理（Access Management）] > [管理者アクセス（Administrator Access）]** を選択します。

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

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

開発者は、Security Cloud Control Firewall Management REST API 呼び出しを行うときに Security Cloud Control Firewall Management API トークンを使用します。呼び出しを成功させるには、API トークンを REST API 認証ヘッダーに含める必要があります。API 専用ユーザーは API トーク

ンを生成できます。通常のユーザーは、自分自身または他のユーザーの API トークンを作成できません。

Security Cloud Control Firewall Management で API 専用ユーザーを作成する目的は、API トークンを使用してシステムへのセキュアなプログラムによるアクセスを有効にすることです。

API 専用ユーザーロールを使用すると、ユーザーはユーザーインターフェイスを使用せずに、API を使用して Security Cloud Control Firewall Management を操作できます。API 専用ユーザーは、Security Cloud Control インターフェイスに直接ログインできません。このロールは組織にメリットがあり、API 専用ユーザーロールは、自動化されたプロセスと統合が必要な組織で役立ちます。

API 専用ユーザーのみが API トークンを生成できます。通常のユーザーは、自分自身または他のユーザーの API トークンを作成できません。

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、**管理（Administration）** > **APIユーザー管理（API User Management）** を選択します。

ステップ 3 **[Add a new user]**（）アイコンをクリックして、新しいユーザーをテナントに追加します。

ステップ 4 [ユーザー名（Username）] フィールドに、API 専用ユーザーの名前を入力します。

ステップ 5 [ロール（Role）] ドロップダウンリストから、API 専用ユーザーのロールを選択し、[追加（Add）] をクリックします。

ステップ 6 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。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。

（注） [編集（Edit）] をクリックして、既存の API 専用ユーザーのロールを変更します。

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）] ページで選択した設定によって、Security Cloud Control Firewall Management に表示される通知のタイプが決まります。

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

[概要（Overview）] タブ

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

- 展開に失敗しました
- バックアップに失敗しました
- アップグレードに失敗しました
- FTD から クラウド提供型 Firewall Management Center 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

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

解除した通知を表示します。個々の通知を非表示にするには、通知の [x] をクリックします。

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

通知の検索

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

通知設定の表示

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

ユーザー通知の基本設定

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

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

デバイス ワークフロー アラート

- [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Firewall Threat Defenseの移行（Migrate to Cloud）]：このアクションは、Firewall Threat Defense の変更時に適用可能です。

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

デバイスイベントアラート

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

イベント検索レポートアラート

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

アプリケーションインサイトアラート

- **アプリケーションが使用可能（Application available）**：モニター対象のアプリケーションが使用可能になると通知されます。
- **アプリケーションを使用できません（Application unavailable）**：モニター対象アプリケーションが使用できなくなると通知されます。

通知のオプトアウト

デフォルトでは、すべての通知タイプが有効になっています。通知タイプの受信を停止するには、その通知のチェックを外してから **[Save]** をクリックします。

電子メール通知の管理

選択したアラートに関する電子メールを受信するには、[Email notifications]トグルボタンを有効にします。

デフォルトでは、**[Use Security Cloud Control notification settings above]** が選択されています。このオプションを選択すると、電子メール通知は **[Notify Me in Security Cloud Control When]** セクションで選択したものと同じ通知およびイベントと一致します。

一部のアラートのみを電子メールで通知する場合は、**[Use Security Cloud Control notification settings above]** を解除し、電子メールで受信するアラートタイプを選択してから、**[Save]** をクリックします。

ロギング設定の表示

[ロギング設定（Logging Settings）] を使用して、テナントの現在のロギング使用状況を確認します。

このページには、次の情報が表示されます。

- 月間のイベントロギング制限。

- 制限がリセットされるまでの日数。
- Cisco Cloud が受信した圧縮されたイベントデータを表す、保存されたロギング使用状況。

[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。

このページには、追加のストレージをリクエストするためのリンクも含まれています。

Security Cloud Control Firewall Management のユーザーロールを理解する

Security Cloud Control Firewall Management は、ユーザーごと、および組織ごとにロールを割り当てます。1 人の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。たとえば、ユーザーは、ある組織で「読み取り専用」ロールを持ち、別の組織で「ネットワーク管理者」ロールを持つことができます。

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、または「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を意味しています。

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、次の操作を実行できます。

- Security Cloud Control の任意のページまたは設定を確認する。
- 証明書、PSK、ログイン情報など、デバイス設定内の機密値を含むすべてのデバイス設定の詳細を表示します。

Note 注：ASA デバイスの場合、ベストプラクティスとしてパスワード暗号化を有効にすることを推奨します。パスワードの暗号化により、PSK やログイン情報が設定内にクリアテキストで表示されることを防ぎます。

- 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。
- 任意のページのコンテンツを検索およびフィルタリングする。
- 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」ロールを持つユーザーは、次の操作を実行できません。

- 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。

編集専用ロールを持つユーザーは、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する。
- 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。

展開専用ロールを持つユーザーは、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する。
- 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ロールを持つユーザーは、次のことができません。

- 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。

管理者ロール

「管理者」ロールを持つユーザーには、Security Cloud Control Firewall Management のほとんどのエリアへの完全なアクセス権があります。

- Security Cloud Control Firewall Management 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

ネットワーク管理者ロールを持つユーザーは、Security Cloud Control Firewall Management のあらゆるエリアに完全にアクセスできます。

ネットワーク管理者ロールを持つユーザーは、以下を実行できます。

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

セキュリティデバイス、ポリシー、およびオブジェクトページのフィルタ処理

[セキュリティデバイス（Security Devices）]ページ、[ポリシー（Policies）]ページ、および[オブジェクト（Objects）]ページでフィルタを使用して、デバイスとオブジェクトを検索します。フィルタリングするには、左側のペインでフィルタアイコンを選択します。

[セキュリティデバイス（Security Devices）]ページのフィルタパネルでは、デバイスタイプ、ハードウェアバージョン、ソフトウェアバージョン、Snort バージョン、設定ステータス、接

続状態、競合検出、Secure Device Connector、およびラベルなどの条件でデバイスをフィルタリングできます。選択したデバイスタイプのタブ内でフィルタを適用できます。

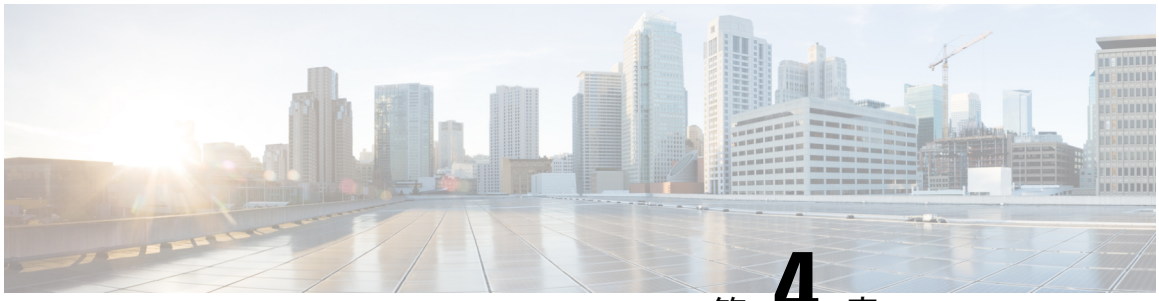
[FTD] タブを開いている場合、フィルタパネルでは、Security Cloud Control が FTD デバイスへのアクセスに使用する管理アプリケーションで、それらのデバイスをフィルタリングすることもできます。

フィルタリングするには、[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 [フィルタ処理（Filter）] をクリックします。



（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、Security Cloud Control からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FDM による管理 デバイスが表示されます。

- FDM：FTD API または Firewall Device Manager を使用して管理されるデバイス。
- FMC-FTD：Firepower Management Center を使用して管理されるデバイス。
- FTD：FTD 管理を使用して管理されるデバイス。



第 4 章

デバイスオンボーディング用の Secure Connector の展開および管理

- セキュアコネクタの概要 （51 ページ）

セキュアコネクタの概要

セキュアコネクタは、ネットワークまたはサポートされているクラウド環境で実行され、Security Cloud Control Firewall Management と管理対象リソースとの間にセキュアな通信経路を提供する、コネクタインスタンスです。セキュアコネクタは、Security Cloud Control Firewall Management がインターネットから直接到達できないデバイスを管理するのに役立ち、ロギングおよび分析ワークフローでのイベント転送をサポートします。

[セキュアコネクタ（Secure Connector）]ページを使用して、テナントのコネクタインスタンスを表示、展開、および管理します。

セキュアコネクタのタイプ

[セキュアコネクタ（Secure Connector）]ページには、次のコネクタタイプを含めることができます。

- セキュアデバイスコネクタ（SDC）：Security Cloud Control Firewall Management とサポートされている管理対象デバイスとの間にセキュアな通信パスを提供します。
- セキュアイベントコネクタ（SEC）：サポートされているデバイスからイベントを受信し、ロギングおよび分析のために、それらのイベントを Cisco Cloud に転送します。

Secure Device Connector について

Secure Device Connector（SDC）は、デバイスがインターネットから直接到達できない場合にシスコデバイスが Security Cloud Control Firewall Management 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。デバイスログイン情報を使用してデバイスをオンボーディングする場合、ネットワークに SDC を展開して、デバイスと Security Cloud Control Firewall Management 間の通信をプロキシできます。デバイスがインターネットから直接到達可能である場合、SDC

を使用する代わりにデバイスの外部インターフェイスを介した直接通信を許可できます。SDC は、次の機能を実行します。

- 管理対象デバイスのコマンドとメッセージを Security Cloud Control Firewall Management でモニターします。
- Security Cloud Control Firewall Management の代わりにコマンドを実行します。
- 管理対象デバイスにメッセージをリレーします。
- デバイス応答を返します。

SDC と Security Cloud Control Firewall Management 間の通信では、TLS 1.3 および AES-128-GCM を使用した HTTPS が使用されます。オンボードされたデバイスとサービスのクレデンシャルは、ブラウザから SDC に暗号化され、AES-128-GCM を使用して保存時にも暗号化されます。SDC のみがこれらのログイン情報にアクセスできます。

ネットワーク管理者ロールを持つユーザーは、Secure Device Connector またはセキュアイベントコネクタ（SEC）を作成する必要があります。

これらのデバイスを SDC を介して Secure Device Connector にオンボーディングできます。

- ログイン情報メソッドを使用した オンプレミス Firewall Management Center
- Meraki MX デバイス
- 汎用 SSH デバイス
- Cisco IOS デバイス

クラウド提供型 Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense デバイスは SDC を必要とせず、プロキシを介したオンボーディングをサポートしません。これらのデバイスが クラウド提供型 Firewall Management Center に接続できるように、適切な DNS 設定とアウトバウンド インターネット接続があることを確認してください。

SDC と Security Cloud Control 間の通信を許可する方法については、直接クラウド接続のインバウンドアクセスを許可 （54 ページ）を参照してください。

詳細については、Secure Device Connector および Secure Event Connector を実行するための VM の展開 （55 ページ）を参照してください。

デバイス接続の計画

Security Cloud Control Firewall Management はクラウドコネクタを介して、または SDC を介して管理対象デバイスに接続します。

表 *1*:

接続方法	次の場合に使用	必要なネットワークアクセス
ダイレクトクラウドコネクタ	デバイスはインターネットから直接到達可能です。	ポート443、またはデバイス管理に使用するポートで、クラウドリージョンの Security Cloud Control Firewall Management IPアドレスからのインバウンドアクセスを許可します。
SDC	デバイスがインターネットから直接到達できないか、送信元にオンプレミス SDC が明示的に必要です。	ポート 443 またはデバイス管理に使用するポートで、SDC ホストからのフルインバウンドアクセスを許可します。SDC VM がデバイス管理インターフェイスに到達できることを確認します。

FDM による管理 デバイスは、インターネットから直接アクセスできるかどうかに関係なく、デバイスのログイン情報、登録キー、またはシリアル番号を使用して Security Cloud Control Firewall Management へのオンボーディングを実行できます。デバイスがインターネットに直接アクセスできないものの、インターネットに直接アクセスできるネットワーク上に存在する場合、このデバイスの一部として提供される Security Services Exchange コネクタは Security Services Exchange クラウドに到達できるため、FDM による管理 デバイスのオンボーディングが可能になります。

送信元は、以下をオンボーディングするにはオンプレミス SDC が必要であると明示的に記載しています。

- クラウドからアクセスできない ASA デバイス
- ログイン情報のオンボード方式を使用する場合にクラウドからアクセスできない FDM による管理 デバイス
- Cisco IOS デバイス
- SSH でアクセスするデバイス

Security Cloud Control Firewall Management はクラウドコネクタを使用して接続するため、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。

SDC に関する Docker ネットワークの考慮事項

SDC は Docker コンテナとして実行されます。Docker は通常、デフォルトのブリッジネットワークである docker0 に `172.17.0.0/16` サブネットを使用します。

`172.17.0.0/16`または Docker によって割り当てられたネットワークスペースの一部が既存のネットワーク IP スペースと重複している場合は、SDC を展開する前に Docker ネットワークのデ

フォルト値を変更します。代替ネットワークを使用するには、/etc/docker/daemon.json の設定を編集します。

たとえば、Docker ネットワークアドレスプールでスーパーネット 10.198.0.1/24 を使用し、サブネット 10.198.0.0/24 から、IP アドレス 10.198.128.0/17 をデフォルト Docker ブリッジインターフェイスである docker0 として使用します。

```
sudo vi /etc/docker/daemon.json

{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "100m",
    "max-file": "5"
  },
    "bip": "10.198.0.1/24",
    "default-address-pools": [
        {
            "base": "10.198.128.0/17",
            "size": 24
        }
    ]
}

(save and exit)

sudo reboot (required)
```

詳細については、「ネットワークの概要」を参照してください。

直接クラウド接続のインバウンドアクセスを許可

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。

クラウドコネクタを介して Security Cloud Control Firewall Management 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。

Table 2:

地域	URL	次からのインバウンドアクセスを許可
アジア太平洋日本（APJ）	https://security.cisco.com	54.199.195.111 52.199.243.0
オーストラリア（AUS）	https://security.cisco.com	13.55.73.159 13.238.226.118
ヨーロッパ、中東、アフリカ（EMEA）	https://security.cisco.com	35.157.12.126 35.157.12.15
インド（IN）	https://security.cisco.com	35.154.115.175 13.201.213.99

地域	URL	次からのインバウンドアクセスを許可
アメリカ合衆国（US）	https://security.cisco.com	52.34.234.2 52.36.70.147

SDC キャパシティとホストの要件を計画

各 Security Cloud Control Firewall Management 組織は SDC の数に制限はありません。SDC は 1 つの組織にのみ属しており、組織間で共有されることはありません。展開プランでは、1 つの SDC は約 500 台のデバイスをサポートすると予想されます。実際のキャパシティは、該当デバイスで有効になっている機能と、構成ファイルのサイズによって異なります。

複数の SDC を展開すると、次のことが可能になります。

- パフォーマンスを低下させることなく、デバイス管理を拡張できます。
- SDC を隔離されたネットワークセグメントに配置し、デバイスを同じ Security Cloud Control Firewall Management 組織内に配置します。
- 追加の SDC ごとにブートストラップ手順に従い、ホスト上で複数の SDC を実行します。

最初の SDC の名前にはテナント名と数値 1 が含まれています。SDC が追加されるたびに、シーケンスが番号付けされます。

Secure Device Connector および Secure Event Connector を実行するための VM 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。

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、展開を計画するために、1 つの SDC で約 500 台のデバイスをサポートす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」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、最も信頼できる方法です。

はじめる前に

- 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 または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 によって管理されるデバイスは、SDC VM の IP アドレスからのインバウンドトラフィックを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、「直接クラウド接続のインバウンドアクセスを許可 （54 ページ） の Secure Device Connector への接続」を参照してください。
- ネットワークでプロキシを使用している場合は、ホストセットアップコマンドを実行する前に、必要なすべての詳細情報があることを確認します。ほとんどの問題は、誤ったプロキシ設定に関連しています。重要な詳細情報は次のとおりです。
  - プロキシの IP/ホスト名。
  - プロキシが、トラフィックを代行受信し、独自の証明書を使用してそれを再暗号化するかどうか。この詳細情報が、SDC VM セットアップに関する複雑さのほとんどの原因です。
    - プロキシがトラフィックを代行受信する場合は、VM を設定するときにルート証明書を準備します。プロンプトが表示されたら、それを貼り付けることで、プロキシによって生成された証明書をホストと SDC が認識して信頼できるようになります。
    - プロキシがトラフィックを代行受信しない場合、ここでは他に何もする必要はありません。
  - 以下の項目は、ほとんどの場合、プロキシされる HTTP および HTTPS 接続で同じです。ただし、プロトコルごとに異なるプロキシを使用する場合は、それぞれに次のすべてが必要になります。
    - プロキシの IPアドレス
    - プロキシが使用するポート
    - プロキシが、プロキシ自体への接続が HTTPS を介したものである必要があるかどうか（通常はそうではありません）。たとえば、プロキシのアドレスが https://proxy.corp.com:80 と表示された場合は、「はい」と応答します。表示されるアドレスが http://proxy.corp.com:80 の場合は、「いいえ」と応答します。どちらの URL もポート 80 を使用しますが、プロトコルが異なることに注意してください。
    - 以下を含むプロキシの認証の詳細情報：
      - プロキシに認証が必要かどうか（ほとんどの場合、必要ありません）
      - 必要な場合は、ホストを設定するときに使用できるユーザー名とパスワードが必要です。

サポートされているインストール

- 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。
- Security Cloud Control は、独自の Ubuntu インスタンスへの SDC のインストールをサポートしています。現在、バージョン 20LTS ～ 24LTS がサポートされています。
- ESXi 5.1 ハイパーバイザ。

システム要件

- 1 つの SDC を持つ VM のシステム要件は、次のとおりです。
  - 2 vCPU
  - 2 GB のメモリ
  - 64 GB のディスク容量
- ホストに追加する各 SDC には、追加の 1 つの vCPU と 1 GB の RAM が必要です。
- 1 つの SEC（Cisco Security Analytics and Logging で使用されるコンポーネント）を持つ VM のシステム要件は、次のとおりです。
  - 4 つの vCPU（最小）
  - 8 GB のメモリ
- ホストに追加する SEC ごとにリソースを倍にする必要があります。そのため、これらは 1 つの SDC と 1 つの SEC を持つ VMware ESXi ホストの要件です。
  - 6 vCPU
  - 10 GB のメモリ
  - 64 GB のディスク容量

設置の準備

- ホストにおいてネットワーキングを手動で設定するには、次の情報を収集します。
  - VM に使用する静的 IP アドレス
  - `cdo` ユーザー（または sudo アクセスを持つユーザー）と sdc ユーザー（Docker を実行するユーザー）に使用するパスワード
  - 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/NTP 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。

  ネットワークでアウトバウンド接続に許可/拒否リストを使用している場合は、ubuntu.com への接続を許可して、それらのセキュリティ更新を適用できるようにする必要があります。

（注） Ubuntu はチェックサムで更新を保護し、HTTPS ではなく HTTP のみを使用します。セキュリティ更新をプルするには、ubuntu.com への HTTP 接続を許可する必要があります。

VM の展開

SDC と SEC の実行に使用される VM を展開するには、2 つのオプションがあります。

1. Security Cloud Control が提供する VMware イメージをダウンロードするには、次の手順を実行します。
2. Ubuntu 20、22、または 24 を自分で展開する場合、独自の Ubuntu インスタンスを展開するときは、次のセクションをスキップして、「VM の設定」セクションに進むことができます。

手順

1. Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
2. 左側のペインで **管理（Administration）** > **統合（Integrations）** > **セキュアコネクタ（Secure Connectors）** をクリックします。
3. [Services] ページの [Secure Connectors] タブを選択し、青いプラスボタンをクリックして、[Secure Device Connector] を選択します。
4. **[Download the SDC VM]** のイメージをクリックします。新しいタブで表示されます。
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
6. vSphere Web クライアントを使用して、管理者として VMware サーバーにログインします。

（注） ESXi Web クライアントは使用しないでください。

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。

7. セットアップが完了したら、SDC VM の電源を入れます。
8. 新しい SDC VM のコンソールを開きます。
9. `cdo` というユーザー名でログインします。デフォルトのパスワードは `adm123` です。

VM の設定

これで、展開した VM イメージのコンソールを起動できます（また、VM を自作しており、SSH を有効にしている場合は、その VM に SSH 接続できます）。ホストで SDC または SEC Docker コンテナを実行できるようにするには、設定スクリプトを実行する必要があります。

1. Security Cloud Control 提供の VM をダウンロードした場合は、CLI がすでにインストールされているため、手順 2 に進むことができます。独自の VM を展開した場合は、その VM に SSH 接続し、次のコマンドを実行して CLI をインストールします。

   ```
   curl -O
   https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
    && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
   ```

2. 次のコマンドを実行して、ホストの構成を開始します：

   ```
   sudo sdc host configure
   ```

3. パスワードの入力を求められたら、Security Cloud Control 提供の VM 場合は adm123 を入力し、独自の VM の場合は、選択した管理者パスワードを入力します。
4. プロンプトに従って、`sdc` ユーザーを設定します。
5. ネットワークの設定を求められたら、次のいずれかを選択します。
   - [このホストを静的 IP で手動設定する（Manually configure this host with a static IP）]：このホストの IP、ゲートウェイ、DNS サーバーなどを指定し、それを VM 上のシステム設定に書き込みます。
   - [DHCP]：VM に静的 IP を割り当てる DHCP サーバーがある場合。
   - [静的 IP が設定済みで、今すぐネットワーキングを変更したくない。（Static IP is already configured and I don't want to change my networking now.）]
6. プロンプトが表示されたら、プロキシ設定に関する質問に回答します。このトピックの上部にある詳細なリストで、すべての前提条件と、可能なプロキシ設定オプションを確認してください。

7. プロキシが設定済みである場合は、すべてのプロキシ設定を有効にするために VM を再起動することを求められます。設定していない場合は、再起動することを求められず、手順 8 に進むことができます。

8. カスタム インターネット アクセス テスト URL を設定します。これを行う必要があるのは、デフォルトですべてのアウトバウンド接続を拒否する場合のみです。その場合は、許可リストにある https://google.com などのパブリックにアクセス可能な Web URL を指定します。

9. 最新のセキュリティパッチをインストールします。一部のパッチにはOS ツールと Docker サーバーが必要です。

10. プロンプトが表示されたら、スクリプトでSSH設定を強化するかどうかを指定します。

    シスコの VM を使用している場合は、続行します。独自の VM を使用しており、SSH を自分で設定している場合は、現在の設定を変更しないように、この手順をスキップすることができます。

11. SDC、SEC、CLI 自体の自動更新を有効にするように求められた場合は、これを実行して、バグ修正、パッチ、および新機能を最新の状態に保つことを推奨します。ポリシーによって自動更新が許可されない場合は、「Secure Device Connector の更新」を参照してください。

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 に対してオンボーディング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、単一の組織で複数の Secure Device Connector を使用 （75 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。

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、「Secure Device Connector を使用した Security Cloud Control への接続」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。
- Ubuntu 22.04 および Ubuntu 24.04 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 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 左側のペインで **管理（Administration）** > **統合（Integrations）** > **セキュアコネクタ（Secure Connectors）** をクリックします。

ステップ 4 [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 5 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 6 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 7 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 8 DNS（ドメインネームサーバー）を設定します。

ステップ 9 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 10 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 11 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 12 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 13 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 14 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 15 cdo と sdc の 2 つのユーザーを作成します。cdo ユーザーを使用すれば、ルートユーザーに直接アクセスせずに管理タスクを実行できます。sdcユーザーは、SDC docker コンテナを実行するために指定します。

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

ステップ 16 sdc 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 17 sdc ユーザーを wheel グループに追加して、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 18 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 19 /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 20 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 21 ディレクトリを **/usr/local/CDO** に変更します。

ステップ 22 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 23 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 24 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 25 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 26 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。

展開されたホストでの Secure Device Connector のブートストラップ

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

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

ステップ 3 [Services] ページの [Secure Connectors] タブで、[+] アイコンをクリックし、[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 管理者ユーザー（通常は `cdo`）と選択したパスワードを使用して、VM に SSH で接続します。

ステップ 6 「sudo su - sdc」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 7 次のコマンドを使用して、新しい SDC をブートストラップします。

```
sdc bootstrap <paste-your-bootstrap-data-here>
```

ステップ 8 使用する SDC のバージョンを選択します。

SDC バージョンには 3 つのオプションがあります。

- SDC 2024：これは、ほとんどの場合に実行を希望されるバージョンです。
- FIPS が有効な SDC 2024：FedRamp 準拠の条件を満たす場合は、このバージョンを選択します。
- SDC レガシー：このバージョンは機能の更新を受信しなくなったため、代わりに SDC 2024 を実行することを推奨します。

ステップ 9 CLI はコンテナイメージをプルして SDC を起動します。また、以下を実行して、SDC がアクティブでユーザーインターフェイスおよびホスト上で動作していることを検証できます。

```
sdc show running
```

テナントの SDC が表示されます。

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。

```
sdc host status
```

資料によっては、以下を手動で実行する必要がある場合があります。

```
sdc host configure
```

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

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

始める前に

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

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

次に行う作業：

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。

オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行

Security Cloud Control のオンプレミス Secure Device Connector（SDC）は、これまで CentOS 7 仮想マシンにインストールされていました。CentOS 7 はサポートが終了し、Security Cloud Control によって廃止されたため、すべての SDC を CentOS 7 から Ubuntu 仮想マシンに移行できるように、こちらの移行プロセスを準備しました。

移行する前に

- 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。
- SDC を実行している Ubuntu 仮想マシンには、ASA や Cisco IOS デバイスなど、通信する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。
- デバイスに到達するため、元の SDC VM の IP アドレスまたは FQDN で作成されたネットワークルールを、新しい SDC VM の IP アドレスまたは FQDN を使用して作成し直す必要があります。
- 移行には 10 ～ 15 分かかります。移行中、デバイスは引き続きセキュリティポリシーを適用し、ネットワークトラフィックを回送しますが、SDC を介した通信はできません。

前提条件

「Secure Device Connector および Secure Event Connector を実行するための VM の展開」の手順に従って新しいホストを展開します。

ホストの設定

SDC や SEC を移行する場合は、次の手順に従います。

1. こちらから新しい VM イメージをダウンロードします。
2. CDO-SDC_VM.zip ファイルを解凍します。次のような名前の 3 つの VM ファイルが表示されます。
   - CDO-SDC-VM-708cd33-2024-05-30-2031-disk1.vmdk
   - CDO-SDC-VM-708cd33-2024-05-30-2031.mf
   - CDO-SDC-VM-708cd33-2024-05-30-2031.ovf
3. ダウンロードした VM を展開します。
4. 新しい VM に割り当てられた静的 IP アドレスまたは FQDN をメモします。
5. SSH を使用して、CDO ユーザーとして新しい VM にログインします。
6. プロンプトに次のコマンドを入力します。

```
sudo sdc host configure
```

（注）
- 移行スクリプトのプロンプトに厳密に従ってください。このスクリプトは適切に文書化されており、手順ごとの説明で移行プロセスをガイドします。
- 移行スクリプトの最後に、SDC が新しい VM に移行されたことを示すメッセージが表示されます。SDC の名前は、移行後も保持されます。

SDC の移行

手順：

1. SSH を使用して、CDO ユーザーとして元の（CentOS）SDC にログインします。
2. 次のコマンドを使用して CLI をインストールします。

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
```

3. 次のコマンドを実行し、プロンプトに従います。

```
sudo sdc migrate now
```

確認：

1. Security Cloud Control テナントにログインします。
2. 移行先の 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。

（注） SDC が [アクティブ（Active）] 状態であることを確認します。

SEC の移行

手順：

1. SSH を使用して、CDO ユーザーとして元の（CentOS）SDC にログインします。
2. 次のコマンドを使用して CLI をインストールします。

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
```

3. 次のコマンドを実行し、プロンプトに従います。

```
sudo sdc eventing migrate
```

4. SEC の新しい IP アドレスをポイントするようにデバイスを設定するか、元のホストをシャットダウンし、新しいホストに元のホストと同じ IP アドレスを割り当てます（この場合、デバイスの更新は不要です）。

確認：

SEC の状態に関する詳細は、「Secure Event Connector の状態を把握するためのヘルスチェックの使用」を参照してください。

追加手順

古い SDC を再起動しない

移行が完了したら、元の仮想マシンで古い SDC を再起動しないでください。

失敗した移行を元に戻す

何らかの理由で移行が失敗した場合、または期待どおりの結果でなかったため、元の SDC に戻す場合は、次の手順に従います。

1. 新しい VM にログインし、**SDC** ユーザーにスイッチします。
2. 次のコマンドを使用して、SDC が現在新しい VM で実行されていないことを確認します。

```
docker ps
```

3. SDC が実行されている場合は、次のコマンドを実行します。

```
sdc stop
```

4. 再度 `docker ps` を実行して、SDC が実行を停止したことを確認します。
5. 古い VM にログインし、次のコマンドを実行します。

```
sdc migrate revert
```

6. 古い SDC がアクティブで UI に表示されたら、新しい VM に戻り、次のコマンドを実行します。

   ```
   sdc delete <your-tenant-name-here>
   ```

7. ブラウザを完全に更新し、SDC をクリックして、古いホストの IP がサイドバーに表示されていることを確認します。

   これらの手順を実行しても、新しいIPが表示される場合は、新しいヘルスチェックを要求し、ブラウザを更新して、もう一度確認してください。

8. SEC 移行を元に戻すには、以下のコマンドを実行します。

   ```
   sdc eventing revert
   ```

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、**CDO** 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、コマンドを使用します。

```
[cdo@localhost ~]$ ip addr
```

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、次のコマンドを使用してホスト設定を再度開始します。

```
[cdo@localhost ~]$ sdc host configure network
```

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。

ステップ 5 設定スクリプトは、ネットワーク設定について尋ね、新しい IP を使用して新しい設定ファイルを書き込み、その設定を適用します。

（注） この時点で、SSH 接続は失われます。

ステップ 6 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 7 SDC は自動的に起動しますが、起動しない場合は以下のコマンドを実行します。

```
[cdo@localhost ~]$ sudo su - sdc
[cdo@localhost ~]$ sdc start
```

（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 8 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）**>**統合（Integrations）**>**セキュアコネクタ（Secure Connectors）** ページに移動します。

ステップ 9 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 10 [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、**[Last Heartbeat]** に現在の日付と時刻が表示されるはずです。

ある Secure Device Connector SDC から別の SDC への ASA の移動

Security Cloud Control Firewall Management では、1 つのテナントあたり 1 つ以上の SDC の使用がサポートされます。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 [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、**管理（Administration）**>**統合（Integrations）**>**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、Security Cloud Control インターフェース内の SDC 名が表示される場所に、**[Security Devices]** ペインの Secure Device Connector フィルタを含めて表示されます。

Secure Device Connector を手動で更新

このタスクは、障害対応ツールとして使用します。この送信元では、SDC は通常自動的に更新され、エラーが発生しない限り手動で更新する必要はないと説明しています。

Procedure

ステップ 1 SDC に接続します。SSH を使用して接続するか、ハイパーバイザのコンソールビューを使用できます。

ステップ 2 SDC に管理者ユーザー（通常は **cdo**）としてログインします。

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 をアップグレードします。

```
sdc upgrade
```

Note **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。

単一の組織で複数の Secure Device Connector を使用

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。複数の SDC により、より多くのデバイスを管理し、それらのデバイスを同じ Security Cloud Control Firewall Management テナントに配置したまま、コネクタを異なるネットワークセグメントに配置できます。2 つ目以降の SDC を展開する手順は、最初の SDC の手順と同じです。最初の SDC 名前にはテナント名と数字の「1」が含まれています。追加の各 SDC には、順番に番号が付けられます。

- 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。
- 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 Secure Device Connector を介するデバイスを検索

同じ SDC を介して接続するデバイスを検索するには、次の手順を実行します。

Procedure

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、[セキュリティデバイス（Security Devices）] ページの上部にある [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（Filter）] 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。[セキュリティデバイス（Security Devices）] ページには、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、[セキュリティデバイス（Security Devices）] ページの上部にある [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。

Secure Device Connector を削除

SDC の削除は元に戻せません。削除後、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に接続されていたデバイスは管理できません。デバイスを再接続する場合、管理者のログイン情報を再度入力する必要がある場合があります。

SDC を削除する前に、接続されているデバイスを別の SDC に移動するか、Security Cloud Control Firewall Management から削除してください。

Procedure

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。この操作は、次の 2 つの方法で実行できます。

- 削除する SDC に接続されているすべてのデバイスを Security Cloud Control から削除します。
  - **a.** SDC で使用されるすべてのデバイスを特定するには、「同一 SDC を使用した Security Cloud Control に接続するすべてのデバイスを見つける」を参照してください。
  - **b.** [セキュリティデバイス（Security Devices）] ページで、識別したすべてのデバイスを選択します。
  - **c.** [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 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 左側のペインで **管理（Administration）** > **統合（Integrations）** > **セキュアコネクタ（Secure Connectors）** をクリックします。

ステップ 4 [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 5 [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 6 [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。

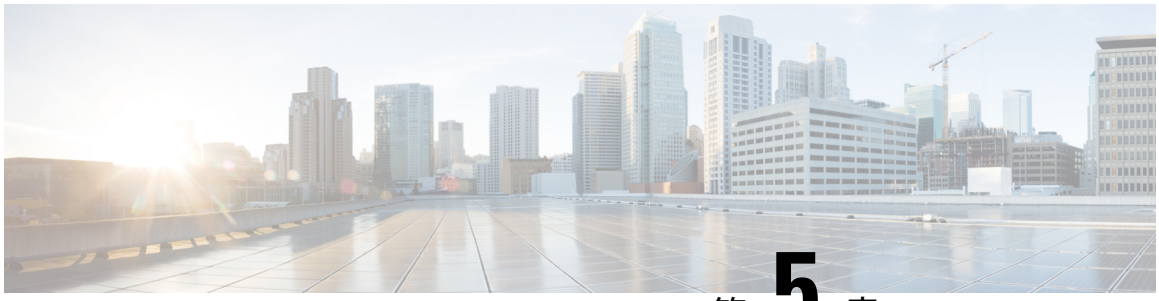
Warning <sdc_name> を削除しようとしています。SDC の削除は元に戻せません。SDC を削除すると、デバイスをオンボーディングまたは再オンボーディングする前に、新しい SDC を作成してオンボーディングする必要があります。

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 7 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 8 [OK] をクリックして、SDC の削除を確定します。



第 5 章

Security Cloud Control Firewall Management でのデバイ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 Firewall Management にオンボーディングできます。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 Firewall Management 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 Firewall Management 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 について （51 ページ） を参照してください。

• Cisco Meraki MX デバイスのオンボーディング （79 ページ）

Cisco Meraki MX デバイスのオンボーディング

この章では、Cisco Meraki MX デバイスをオンボーディングする手順について説明します。

Meraki MX の Security Cloud Control へのオンボーディング

MX デバイスは、Security Cloud Control と Cisco 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 Cisco Meraki ダッシュボードに展開します。ダッシュボードはその設定をデバイスに安全に展開します。

Before you begin

- Security Cloud Control の管理対象デバイスへの接続については、「直接クラウド接続のインバウンドアクセスを許可 , on page 54」を参照してください。
- まず、Meraki ダッシュボードで Meraki MX を登録する必要があります。Cisco Meraki ダッシュボードにアクセスできないと、組織は Cisco Meraki クラウドによって認識されません。その結果、デバイスをオンボードするための API トークンを生成できません。

- Security Cloud Control は、ホストに関連付けられたすべてのビットをゼロに設定することにより、無効な CIDR プレフィックス表記の IP アドレスと IP アドレス範囲を有効な形式に変換します。
- Meraki MX デバイスまたはテンプレートのオンボーディングでは、Secure Device Connector（SDC）を介した接続は必要なくなりました。以前にオンボーディングされた Meraki MX デバイスがあり、SDC を使用して Security Cloud Control に接続する場合、その接続は引き続き機能します。デバイスを削除して再度オンボーディングするか、接続ログイン情報を更新すると、接続が停止します。
- MX デバイスを Security Cloud Control で管理するために Cisco Meraki クラウドに接続する必要はありません。MX デバイスがクラウドに接続したことがない場合、デバイスの接続は**到達不能**としてリストされます。このステータスは正常であり、デバイスを管理したり、ポリシーをデバイスに展開したりする機能には影響しません。

Procedure

ステップ 1 Meraki MX デバイスをオンボードするときは、Meraki API キーを生成する必要があります。このキーにより、ダッシュボードが要求を認証できるようになります。これにより、デバイスを安全にオンボーディングできます。Meraki API キーの生成と取得の詳細については、「Meraki API キーの生成と取得」を参照してください。

ステップ 2 API キーを使用して Cisco Meraki デバイスを Security Cloud Control にオンボードします。

Meraki API キーの生成と取得

以下の手順に従って、API アクセスによる Security Cloud Control の Meraki ダッシュボードへのアクセスを有効にします。

Before you begin

Meraki MX の Security Cloud Control へのオンボーディング, on page 79 に関する注意事項と前提条件を確認します。

Procedure

ステップ 1 Meraki ダッシュボードにログインします。

ステップ 2 **[組織（Organization）] > [設定（Settings）]** の順に選択します。

ステップ 3 [ダッシュボードAPIアクセス（Dashboard API Access）] セクションで、[Cisco MerakiダッシュボードAPIへのアクセスを有効にする（Enable access to the Cisco Meraki Dashboard API）] をオンにします。このオプションをオンにしないと、MX デバイスを Security Cloud Control にオンボーディングするための API キーを生成できません。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

ステップ 5 Cisco Meraki ダッシュボードで、**ユーザー名**をクリックしてから、[マイプロファイル（My Profile）] をクリックします。

ステップ 6 API アクセスヘッダーを見つけて、[新しいAPIキーの生成（Generate new API key）] をクリックします。API キーをコピーし、使用する準備が整うまでメモに貼り付けておきます。API キーを貼り付ける前にその API キーを含むウィンドウまたはタブを閉じると、コピーした API キーにアクセスできなくなります。

Note デバイスごとに必要な API キーは 1 つのみです。新しいキーを生成せずに、Meraki デバイスを再オンボーディングできます。

「Meraki デバイスの Security Cloud Control へのオンボーディング」に進みます。

Security Cloud Control への MX デバイスのオンボード

次の手順を使用して、Cisco Meraki デバイスをオンボードします。

Before you begin

Meraki API キーの生成と取得, on page 80。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 青色の追加ボタン（）をクリックします。

ステップ 4 [Meraki] タイルをクリックします。

ステップ 5 このデバイスが通信する Secure Device Connector について , on page 51 を選択します。デフォルトの SDC が表示されますが、青色の [変更（Change）] リンクをクリックして変更できます。

ステップ 6 [Cisco Merakiへの接続（Connect to Cisco Meraki）] ページで、次の手順を実行します。

a) コピーした API アクセスキーを貼り付けて、[接続（Connect）] をクリックします。
キーが不完全または正しくない場合、デバイスをオンボードできません。

b) ドロップダウンリストを使用して、正しい組織を選択します。生成された組織のリストはCisco Meraki ダッシュボードから取得され、このリストにはデバイスとテンプレートが含まれています。[選択（Select）] をクリックします。

c) ドロップダウンリストを使用して、正しいネットワークを選択します。生成されたネットワークのリストは、Cisco Meraki ネットワークから取得されます。[選択（Select）] をクリックします。

d) （オプション）デバイスに固有のラベルを追加します。これらのラベルでデバイスのリストをフィルタリングできます。[続行（Continue）] をクリックします。

デバイスのオンボーディングプロセスが開始されます。プロセスが完了すると、[セキュリティデバイス（Security Devices）] ページにリダイレクトされます。

Meraki テンプレートの Security Cloud Control へのオンボーディング

Cisco Meraki テンプレートは、単一のポリシーで複数の場所またはネットワークを管理するための優れた方法です。これらのテンプレートは、Security Cloud Control と Cisco Meraki ダッシュボードの両方を使用して管理できます。Security Cloud Control は設定の変更を Cisco Meraki ダッシュボードにデプロイし、その後ダッシュボードは設定をテンプレートに安全にデプロイします。Security Cloud Control が Meraki と通信する方法の詳細。

Note テンプレートを Security Cloud Control にオンボーディングするには、まず Meraki ダッシュボードでテンプレートを作成する必要があります。Cisco Meraki ダッシュボードへのアクセス権がない場合、Cisco Meraki クラウドは組織を認識せず、ユーザーはデバイスの API トークンを生成できません。Cisco Meraki ダッシュボードで、**[組織（Organization）] > [設定テンプレート（Configuration templates）]** をクリックします。詳細については、「設定テンプレートを使用してネットワークを一括管理する」を参照してください。

Meraki テンプレートを導入するには、次の 3 つの手順を完了する必要があります。

Procedure

ステップ 1 Meraki ダッシュボードでテンプレートネットワークを作成します。Cisco Meraki テンプレートのベストプラクティスの詳細については、「Meraki Templates Best Practices」を参照してください。

ステップ 2 Meraki API キーを生成して取得します。Meraki テンプレートをオンボーディングするときは、Meraki API キーを生成する必要があります。このキーでダッシュボードを認証し、デバイスを安全にオンボーディングすることができます。

ステップ 3 このキーを使用して Meraki テンプレートを Security Cloud Control にオンボーディングします。

Meraki API キーの生成と取得

以下の手順に従って、API アクセスによる Security Cloud Control の Meraki ダッシュボードへのアクセスを有効にします。

Procedure

ステップ 1 Meraki ダッシュボードにログインします。

ステップ 2 **[組織（Organization）] > [設定（Settings）]** の順に選択します。

ステップ 3 [ダッシュボードAPIアクセス（Dashboard API Access）] セクションで、[Cisco MerakiダッシュボードAPIへのアクセスを有効にする（Enable access to the Cisco Meraki Dashboard API）] をオンにします。このオプションをオンにしないと、MX デバイスを Security Cloud Control にオンボーディングするための API キーを生成できません。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

ステップ 5 Cisco Meraki ダッシュボードで、**ユーザー名**をクリックしてから、[マイプロファイル（My Profile）] をクリックします。

ステップ 6 API アクセスヘッダーを見つけて、[新しいAPIキーの生成（Generate new API key）] をクリックします。API キーをコピーし、使用する準備が整うまでメモに貼り付けておきます。API キーを貼り付ける前にその API キーを含むウィンドウまたはタブを閉じると、コピーした API キーにアクセスできなくなります。

Note テンプレートごとに必要な API キーは 1 つのみです。テンプレートの再オンボーディングに新しいキーを生成する必要はありません。

Meraki テンプレートの Security Cloud Control へのオンボーディング

以下の手順に従って、Cisco Meraki テンプレートをオンボーディングします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 青色の追加ボタン（）をクリックします。

ステップ 4 [Cisco Merakiへの接続（Connect to Cisco Meraki）] をクリックします。

ステップ 5 コピーした API アクセスキーを貼り付けます。キーが不完全または正しくない場合、デバイスをオンボードできません。[接続（Connect）] をクリックします。

ステップ 6 ドロップダウンリストを使用して、テンプレート名として [組織（Organization）] を選択します。生成された組織のリストは Cisco Meraki ダッシュボードから取得され、このリストにはデバイスとテンプレートが含まれています。目的のテンプレートを選択し、[選択] をクリックします。

ステップ 7 （オプション）デバイスに固有のラベルを追加できます。これらのラベルでデバイスのリストをフィルタリングできます。

ステップ 8 [続行（Continue）] をクリックします。

デバイスのオンボーディングプロセスが開始されます。完了すると、Security Cloud Control により [セキュリティデバイス（Security Devices）] にリダイレクトされます。テンプレートが Security Cloud Control に同期されると、[セキュリティデバイス（Security Devices）] ページにテンプレートに関連付けられたデバイ

スの名前が表示され、[デバイスの詳細（Device Details）] ウィンドウにテンプレートにバインドされたネットワークの数が表示されます。

Meraki MX の接続ログイン情報の更新

Meraki ダッシュボードから新しい API キーを生成する場合は、Security Cloud Control Firewall Management で接続ログイン情報を更新する必要があります。

Security Cloud Control Firewall Management では、デバイス自体の接続ログイン情報を更新することはできません。必要に応じて、Cisco Meraki ダッシュボードで API キーを手動で更新します。ログイン情報を更新して通信を復元するには、Security Cloud Control Firewall Management UI で API キーを手動で更新する必要があります。

Note Security Cloud Control がデバイスの同期に失敗した場合、Security Cloud Control の接続ステータスに [無効なログイン情報（Invalid Credentials）] と表示されることがあります。この状況では、API キーを使用しようとした可能性があります。選択した Meraki MX の API キーが正しいことを確認します。

次の手順を使用して、Cisco Meraki MX デバイスのログイン情報を更新します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [デバイス（Devices）] タブをクリックし、[Cisco Meraki（Meraki）] タブをクリックします。

ステップ 4 接続ログイン情報を更新する Meraki MX 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、[ログイン情報の更新（Update Credentials）] をクリックします。

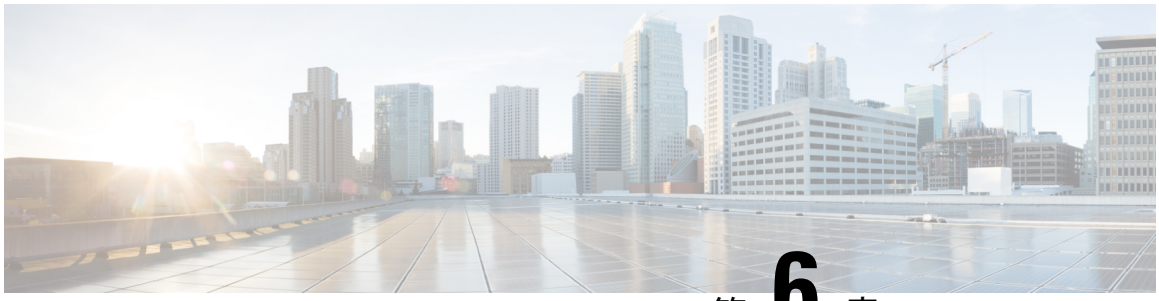
ステップ 6 Security Cloud Control Firewall Management がデバイスにログインするために使用する **API キー**を入力し、[更新（Update）] をクリックします。この API キーは、変更されていない限り、Cisco Meraki MX のオンボーディングに使用したのと同じログイン情報です。これらの変更は、デバイスに展開する必要はありません。

Security Cloud Control Firewall Management からのデバイスの削除

Security Cloud Control Firewall Management からデバイスを削除するには、次の手順を実行します。

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
ステップ 2 **セキュリティデバイス**を選択します。
ステップ 3 削除するデバイスを選択します。
ステップ 4 [デバイスアクション（Device Actions）] ペインで、[削除（Remove）] をクリックします。
ステップ 5 デバイスの削除を確認するには、[OK] をクリックします。
デバイスをオンボーディングされたままにするには、[キャンセル（Cancel）] をクリックします。



第 6 章

Meraki デバイスの設定

- Security Cloud Control Firewall Management でのセキュリティポリシーの管理 （87 ページ）
- Meraki テンプレート, on page 89
- 共有オブジェクト, on page 90
- オブジェクトフィルタ, on page 91
- Meraki ローカル ネットワーク オブジェクトの作成 （93 ページ）
- Meraki デバイスに関連付けられるオブジェクト, on page 98

Security Cloud Control Firewall Management でのセキュリティポリシーの管理

セキュリティポリシーは、目的の宛先へのトラフィックを許可するか、セキュリティ脅威が特定された場合にトラフィックをドロップすることを最終的な目標として、ネットワークトラフィックを検査します。Security Cloud Control を使用して、さまざまな種類のデバイスでセキュリティポリシーを設定できます。

Meraki アクセスコントロールポリシー

Meraki MX デバイスは、Security Cloud Control にオンボーディングする前に Meraki ダッシュボードによって管理されていた可能性があり、デバイスにはすでにいくつかのアウトバウンドルールが設定されている可能性があります。これらのルールは、Security Cloud Control でアクセス制御ルールとして表示されます。

これらのルールを変更し、アクセスコントロールポリシー内に追加のルールを作成できます。アクセスコントロールポリシーをカスタマイズするには、オブジェクトを作成してアタッチします。関連情報については、関連する記事のセクションを参照してください。

Note Meraki アクセスコントロールポリシーのアクションは、デフォルトで [許可（Allow）] です。このアクションを変更することはできません。

Security Cloud Control を使用して Meraki アクセス コントロール ポリシーを編集するには、次の手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [テンプレート（Templates）] タブをクリックします。

ステップ 4 [Meraki] タブをクリックし、アクセス コントロール ポリシーを編集する Meraki MX デバイステンプレートを選択します。

ステップ 5 [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 6 次のいずれかを実行します。

- 新しいルールを作成するには、追加ボタン（）をクリックします。
- 既存のルールを編集するには、ルールを選択し、**[アクション（Actions）]**ペインの編集ボタン（）をクリックします。編集モードに入らずに簡単なインライン編集を行うことができます。
- 不要になったルールを削除するには、ルールを選択し、[アクション（Actions）] ペインで [削除（Remove）] ボタン をクリックします。
- ポリシー内でルールを移動させるには、アクセス コントロール テーブルでルールを選択し、ルールの行の最後にある上下の矢印をクリックしてルールを移動します。

ステップ 7 [順序（Order）] フィールドで、ポリシー内のルールの位置を選択します。ネットワークトラフィックは、ルールのリストに照らして 1 から「最後」の番号までの順に評価されます。

ルールは最初の一致に基づいて適用されます。特定のトラフィック一致基準を持つルールは、同じトラフィックに適用される一般的な基準を持つポリシーよりも前に配置する必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 8 ルール名を入力します。英数字、スペース、および次の特殊文字を使用できます：+ . _ -

Note アクセス制御ルールの [名前（Name）] は Security Cloud Control のルール名として使用されます。一方、**[備考（Remark）]**フィールドは Meraki ダッシュボードのルール名として扱われます。この 2 つのフィールドは互いに依存していません。

ステップ 9 ネットワークトラフィックがルールに一致する場合に適用するアクションを選択します。

- [Block]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

- [Allow]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。



Note ルールアクションのみを設定または変更できます。デフォルトポリシーのアクションを Security Cloud Control から変更することはできません。

ステップ 10 次のタブ内の属性を任意に組み合わせて、トラフィック一致基準を定義します。

- **[Source]**：**[送信元（Source）]** タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック発信元ポートを追加または削除します。デフォルト値は、[任意（Any）] です。
- [Destination]：[宛先（Destination）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック着信ポートを追加または削除します。デフォルト値は、[任意（Any）] です。



Note 送信元および宛先のネットワークは、設定されたいずれかの VLAN サブネット内にある必要があります。または、VLAN サブネットが手動で設定されていない場合は、デフォルトの VPN サブネット内にある必要があります。無効な送信元または接続先ネットワークを含むルールの展開は失敗します。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Meraki テンプレート

Meraki テンプレートは、複数のサイト/ネットワークで共有できるネットワーク設定です。個々のサイトネットワークをテンプレートネットワークにバインドできます。単一のテンプレートに変更を加えると、バインドされるすべてのネットワークが自動的に更新されます。バインドされたネットワークは、Security Cloud Control のバインドされたデバイスとして表示できます。この設定は、異なる場所にある複数のネットワークに 1 つのポリシーを適用する場合に最適です。

1 つのテンプレートに対して複数のネットワークを設定する方法については、「設定テンプレートを使用した複数のネットワークの管理」を参照してください。.Cisco Meraki テンプレート、テンプレートの計画、およびセットアップの詳細については、「Meraki Templates Best Practices」を参照してください。

Cisco Meraki デバイスの管理と同じ方法で、Meraki テンプレートを管理します。最初に、Cisco Meraki ダッシュボードを使用してテンプレートを設定し、Security Cloud Control にオンボーディ

ングします。テンプレートを Security Cloud Control にオンボーディングすると、既存のルールまたは IP のグループが Security Cloud Control に読み込まれ、オブジェクトに変換されます。同期後、[セキュリティデバイス（Security Devices）]ページの[デバイスの詳細（Device Details）]ペインで、テンプレート名と関連するネットワークの数が（バインドされたデバイスとして）表示されます。テンプレートに関連付けられたポリシーとバインドされたネットワークを Security Cloud Control から管理、変更、デプロイすることも可能です。Security Cloud Control への Cisco Meraki テンプレートのオンボーディングの詳細については、「Security Cloud Control へのCisco Meraki テンプレートのオンボーディング」を参照してください。

共有オブジェクト

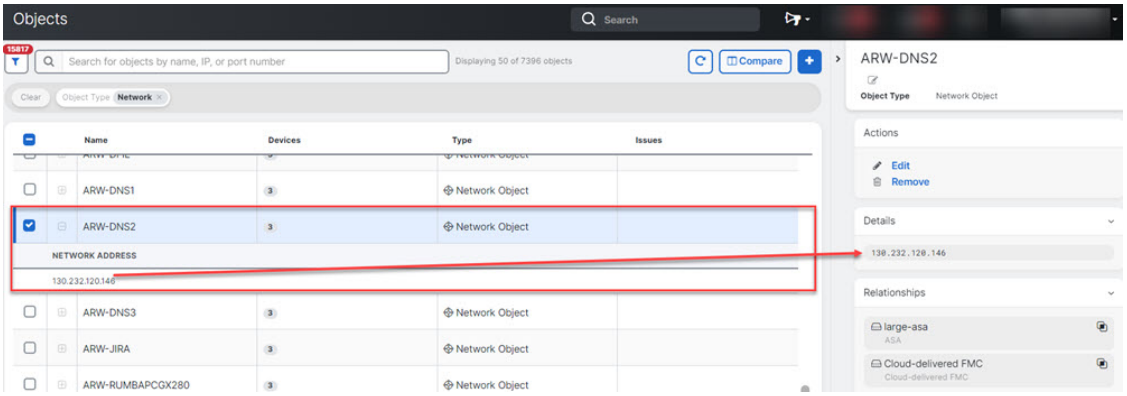
共有オブジェクトは、複数のデバイス上の同じ名前と同じ内容を持つオブジェクトです。1 つの共有オブジェクトの変更がそのオブジェクトを使用するすべてのポリシーに影響するため、共有オブジェクトはポリシーの維持に役立ちます。

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 ヵ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。

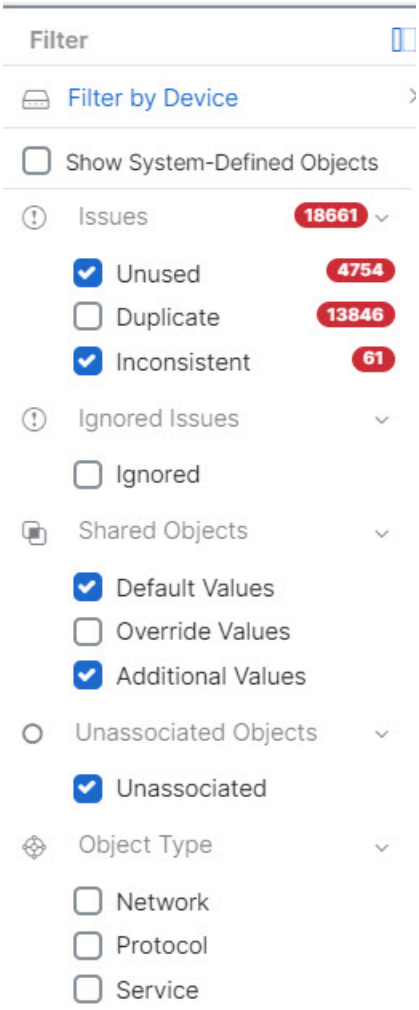


オブジェクトフィルタ

[オブジェクト（Objects）]ページのフィルタを使用して、デバイス、問題、共有状態、関連付け状態、オブジェクトタイプ、または検索値でオブジェクトを検索します。また、システム定義オブジェクトを含めたり除外したり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オブジェクトタイプでフィルタリングできます。共有オブジェクトフィルタを使用すると、デフォルト値、オーバーライド値、または追加の値を持つオブジェクトをフィルタリングできます。

デバイスフィルタとオブジェクトフィルタを組み合わせて、焦点を絞った検索ストラテジーを作成できます。たとえば、次のロジックに一致するオブジェクトを検索できます。[問題（Issues）] は [未使用（Unused）] OR [不整合（Inconsistent）] であり、AND [共有オブジェクト（Shared Objects）] は [デフォルト値（Default Values）] OR [追加の値（Additional Values）] で、AND [関連付けられていないオブジェクト（Unassociated Objects）] が選択されます。



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

- [デバイスでフィルタリング（Filter by Device）]：選択したデバイスで見つかったオブジェクトを表示します。
- [システム定義オブジェクトの表示（Show System-Defined Objects）]：検索およびフィルタリングの結果に事前定義されたシステムオブジェクトが含められます。システムオブジェクトは編集または削除できません。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。
- [問題（Issues）]：未使用の、重複している、または不整合なオブジェクトを表示します。複数の問題を選択した場合、選択したすべての問題カテゴリのオブジェクトが含められます。

- [無視された問題（Ignored Issues）]：管理者によって無視された問題を含むオブジェクトを表示します。
- [共有オブジェクト（Shared Objects）]：共有オブジェクトを表示します。デフォルト値、オーバーライド値、追加の値、またはこれらの組み合わせでフィルタリングできます。
- [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します。
- [オブジェクトタイプ（Object Type）]：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を表示します。

メインフィルタ内でサブフィルタを使用して、ネットワーク、サービス、プロトコルなどのオブジェクトタイプで結果をさらに絞り込めます。複数のカテゴリでのフィルタリングは、AND 関係と組み合わされます。1 つのカテゴリ内での複数選択は、OR 関係と組み合わせることができます。

たとえば、フィルタセットで、次のロジックに一致するオブジェクトを検索できます：選択したデバイス上のオブジェクト AND 不整合オブジェクト AND 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 AND [group] を含むオブジェクト名。

Meraki ローカル ネットワーク オブジェクトの作成

ローカルの Meraki ネットワークオブジェクトは、Cisco Meraki ダッシュボードで作成する必要があります。Security Cloud Control にまだオンボードされていない Meraki デバイスがある場合、既存のローカルオブジェクトはすべてデバイスと一緒にオンボードされます。**オンボード済みの** Meraki デバイスがある場合は、Security Cloud Control でデバイスを同期して、新しい構成とローカルオブジェクトを読み取ります。

（注） Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス構成が Security Cloud Control UI でオンボードまたは同期されると、これらのオブジェクトは **FTD ネットワーク**オブジェクトまたはオブジェクトグループとして表示されます。

これらのオブジェクトおよびオブジェクトグループは、Security Cloud Control では**読み取り専用**になります。

始める前に

Meraki の**オープン ベータ ネットワーク オブジェクト**を有効にしていない場合は、Cisco Meraki ダッシュボードにログインし、**組織** > **ポリシーオブジェクト** に移動して、ローカルオブジェクトとオブジェクトグループに登録してアクセスします。

手順

ステップ 1 Meraki ダッシュボードにログインし、ローカルオブジェクトまたはローカルオブジェクト グループを作成します。詳細については、『Network Objects Configuration Guide』を参照してください。

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

注：Meraki デバイスを Security Cloud Control にまだオンボードしていない場合は、詳細についてSecurity Cloud Control への MX デバイスのオンボード（81 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と、既存のすべてのオブジェクトもオンボーディングされます。

ステップ 3 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 4 Meraki デバイスを見つけて選択し、デバイスの行が強調表示されるようにします。デバイスのステータスは [競合が検出されました] になっています。右側のペインで、[競合の確認] を選択してデバイスの構成に追加された変更を確認するか、[確認せずに承認] を選択してすべての構成変更を承認します。

Merakiネットワークオブジェクトまたはネットワークグループの作成または編集

MX デバイスは Firepower および ASA **ネットワークオブジェクト**と同じ形式を使用し、CIDR 表記で表されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**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、読み取り、更新、および削除できます。

ネットワークオブジェクトに追加できる IP アドレス

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	完全修飾ドメイン名	CIDR 表記法によるサブネット
MX	IPv4	対応	対応	非対応	対応

Note 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：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。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 Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Note 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 Firewall 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 Firewall 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。

Meraki ネットワークオブジェクトの作成

Note 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：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。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 Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 をクリックしてから、**[FTD]** > **[ネットワーク（Network）]**または**[ASA]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークオブジェクトの作成（Create a network object）] を選択します。

ステップ 6 [値（Value）] セクションで、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Meraki ネットワークグループの作成

ネットワークグループは、複数のネットワークオブジェクトまたは IP アドレスで構成されます。

ネットワークグループをネットワークオブジェクトで構成する場合は、上記の「ネットワークオブジェクトの作成」の手順を使用して、IP アドレスごとに個別のネットワークオブジェクトを作成します。

Note 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：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。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 Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側の Security Cloud Control ナビゲーションバーで、**オブジェクト** をクリックします。

ステップ 3 をクリックしてから、**[FTD]** > **[ネットワーク（Network）]**または**[ASA]** > **[ネットワーク（Network）]** のいずれかをクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 6 [オブジェクトの追加（Add Object）] をクリックし、リストからネットワークオブジェクトを選択して、[選択（Select）] をクリックします。必要なすべてのネットワークオブジェクトを追加するまで、この操作を繰り返します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Firepower ネットワークオブジェクトまたはネットワークグループの編集

Note 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 Firewall 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 Firewall 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

ステップ 5 [詳細（details）] ペインの [編集（edit）] ボタン をクリックします。

ステップ 6 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Security Cloud Control のネットワークオブジェクトとグループの削除

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：

オブジェクト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、クラウド提供型 Firewall Management Center の **オブジェクト** ページから重複するネットワークオブジェクトまたはグループが削除されます。その逆も同様です。

Meraki デバイスに関連付けられるオブジェクト

Meraki デバイスで使用されるオブジェクトについて

Meraki ダッシュボードは、アウトバウンドアクセス制御ルールの送信元および宛先フィールドに指定された IP アドレス、プロトコル、またはポート範囲のグループを利用します。オンボーディングすると、Security Cloud Control は、IP アドレスをネットワークオブジェクトに変換し、アプリケーションレイヤのプロトコル値をサービスオブジェクトまたはプロトコルオブジェクトに変換します。

Security Cloud Control の 1 つのルールがダッシュボードで複数のルールに変換される可能性があります。たとえば、TCP プロトコルと UDP プロトコルの両方を含む ASA プロトコルグループを Security Cloud Control の単一のアクセス制御ルールに追加すると、Security Cloud Control は 1 つの Security Cloud Control ルールをダッシュボード内の複数のルールに変換します。変換後のルールは、TCP プロトコルを含む 1 つのルールと UDP プロトコルを含む 1 つのルールになります。

Meraki ダッシュボードと Security Cloud Control はどちらも CIDR サブネット表記をサポートしていることに注意してください。レイヤ 3 スイッチインターフェイスと MX デバイスレイアウトの詳細については、Meraki ナレッジベースを参照してください。

Security Cloud Control の Meraki デバイスで使用できるオブジェクト

Security Cloud Control には、MX デバイス専用のオブジェクトはありません。代わりに、FTD、FDM および ASA オブジェクトを作成または共有し、デバイスに展開されるルールにこれらのオブジェクトを関連付けることができます。Meraki には FTD および ASA オブジェクトとの完全な互換性がないため、MX デバイスがオブジェクトを使用する方法に影響するいくつかの制限がある可能性があります。

FTD、FDM または ASA オブジェクトを MX デバイスに関連付けると、そのオブジェクトが共有されるようになることに注意してください。関連付けられたオブジェクトへの変更は、そのオブジェクトが共有されているすべてのデバイスに影響し、デバイスの設定ステータスには [未同期（Not Synced）] と表示されます。詳細については、「共有オブジェクト」を参照してください。オブジェクトに影響する付加的なオブジェクト状態については、このページの下部に表示されている「**関連記事**」セクションを参照してください。

Meraki は、IPv6 アドレスまたは FQDN を含むオブジェクトをサポートしていません。

Security Cloud Control のオブジェクト	Meraki との互換性あり
プロトコルオブジェクト	TCP、UDP、ICMP
ネットワーク オブジェクト	○

Security Cloud Control のオブジェクト	Meraki との互換性あり
ネットワーク グループ	○
サービス オブジェクト	○
ASA サービスグループ	×
FTD サービスグループ	×

Meraki クラウドのローカル ネットワーク オブジェクトおよびオブジェクトグループ

ネットワークオブジェクトとオブジェクトグループを使用すると、Merakiデバイスのファイアウォールルールを簡単に管理できます。これらは、ファイアウォールルールなどのアクセスポリシーで使用できるIPサブネットおよびFQDNのラベルとして機能します。同じIPサブネットやFQDNを使用する複数のアクセスポリシーを変更する必要がある場合は、ネットワークオブジェクトを変更して、すべてのポリシーに反映させるだけです。現時点では、Meraki ダッシュボードを使用して、これらのオブジェクトを作成および変更する必要があります。お使いの環境でネットワークオブジェクトを使って何ができるのかについては、Meraki の『ネットワークオブジェクトのハイライト』[英語] を参照してください。

Note Meraki ネットワークオブジェクトやネットワーク オブジェクト グループを参照するデバイス設定が Security Cloud Control UI にオンボードまたは同期されると、これらのオブジェクトは**FTD ネットワークオブジェクト**として表示されます。

これらのオブジェクトおよびオブジェクトグループは、Security Cloud Control では**読み取り専用**になります。

Security Cloud Control での Meraki ルールの表示

デバイスのポリシーページからオブジェクトを表示するか、デバイスに基づいてオブジェクトページをフィルタ処理できます。ポリシーページから、アクセス制御ルールの表示、編集、および並べ替えを実行できます。Security Cloud Control は、Meraki ダッシュボードからのアウトバウンドルールをオブジェクトへのアクセス制御ルールに変換するため、Meraki ダッシュボードからのルールとプロトコルの表示が変更される場合があります。次の表は、Security Cloud Control へのデバイスのオンボーディングを完了した後のプロトコルの新しい名前を示しています。

Meraki ダッシュボードでのルールまたはプロトコルのヘッダー	Security Cloud Control でのルールまたはオブジェクトのヘッダー
ポリシー	操作
[ソースIP（Source IP）]	ネットワークオブジェクトまたはネットワークグループ

Meraki ダッシュボードでのルールまたはプロトコルのヘッダー	Security Cloud Control でのルールまたはオブジェクトのヘッダー
[宛先 IP アドレス（Destination IP）]	ネットワークオブジェクトまたはネットワークグループ
送信元ポート（Source Port）	ネットワークオブジェクトまたはネットワークグループ
[宛先ポート（Destination Port）]	ネットワークオブジェクトまたはネットワークグループ
レイヤ 3 アプリケーションプロトコル	ポート（プロトコルグループ、ポートグループ、またはサービスオブジェクト）

次の例は、Meraki ダッシュボードからのアウトバウンドルールが Security Cloud Control でどのように表示されるかを示しています。



Meraki サービスオブジェクトの作成または編集

サービスオブジェクトの概要

サービスオブジェクトは、TCP/IP プロトコルとポートを指定する再利用可能なコンポーネントです。Security Cloud Control は、これらのオブジェクトをサービスオブジェクトとして分類します。MX デバイスに展開すると、Security Cloud Control はオブジェクトをプロトコルまたはポート範囲に変換します。Security Cloud Control が Meraki プロトコルをオブジェクトとして処理する方法の詳細については、Meraki デバイスに関連付けられるオブジェクト, on page 98を参照してください。

サービスオブジェクトの作成

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3  をクリックしてから、**[FTD]** > **[サービス（Service）]** または **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 4 オブジェクト名と説明を入力します。

ステップ 5 [サービスオブジェクトの作成（Create a service object）] を選択します。

ステップ 6 [サービスタイプ（Service Type）] ボタンをクリックし、オブジェクトを作成するプロトコルを選択します。

ステップ 7 次のいずれかのアクションを実行して、プロトコルを識別する情報を入力します。

- TCP または UDP ポートの特定のポート番号を入力します。
- ICMP または ICMPv6 メッセージタイプを選択します。
- 「その他」のサービスタイプを選択した場合は、リストから TCP/IP プロトコルの 1 つを選択します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

サービスグループを作成する

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3  をクリックしてから、**[FTD]** > **[サービス（Service）]** をクリックします。



Note Meraki は ASA サービスグループをサポートしていません。

ステップ 4 オブジェクト名と説明を入力します。

ステップ 5 [サービスグループの作成（Create a service group）] を選択します。

ステップ 6 [オブジェクトの追加（Add Object）] をクリックし、オブジェクトを選択して [選択（Select）] をクリックすることで既存のオブジェクトを追加します。このステップを繰り返してさらにオブジェクトを追加します。

ステップ 7 サービスオブジェクトとサービス値のサービスグループへの追加が完了したら、[追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

サービスオブジェクトまたはサービスグループの編集

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトをフィルタリングして編集するオブジェクトを見つけ、オブジェクトテーブルでオブジェクトを選択します。

ステップ 4 詳細ペインで、[編集（Edit）] をクリックします。

ステップ 5 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。これで、オブジェクトを Meraki ポリシーで使用する準備ができました。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

Firepowerネットワークオブジェクトまたはネットワークグループの編集

Note 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 Firewall 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 Firewall 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **オブジェクト** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

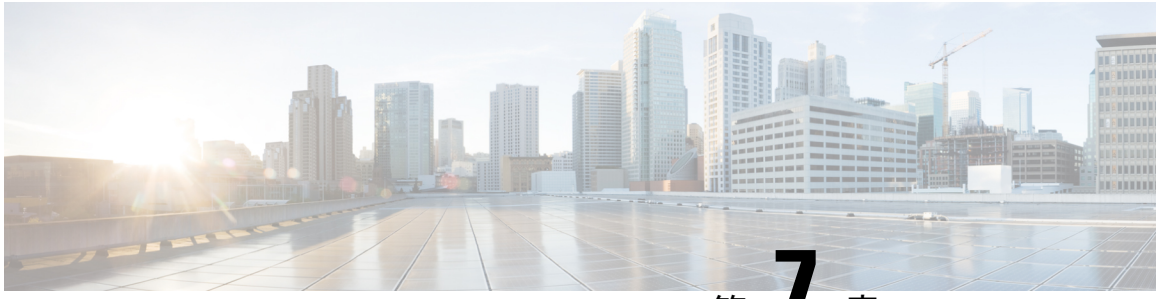
ステップ 5 [詳細（details）] ペインの [編集（edit）] ボタン をクリックします。

ステップ 6 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。



第 7 章

オンボーディングされたデバイス設定の管理

この章では、オンボーディングされたデバイスのデバイス設定の管理について説明します。

- Security Cloud Control Firewall Management でのデバイスの IP アドレスの変更, on page 105
- Security Cloud Control Firewall Management でのデバイス名の変更, on page 106
- デバイスとサービスのリストのエクスポート, on page 107
- デバイス設定のエクスポート （108 ページ）
- デバイスの外部リンク, on page 108
- Security Cloud Control Firewall Management へのデバイス一括再接続, on page 112
- 組織間でのデバイスの移動, on page 113
- デバイス証明書の有効期限の検出 （113 ページ）
- デバイスノートの作成, on page 113
- Security Cloud Control Firewall Management からのデバイスの削除 （114 ページ）
- Firewall Threat Defense デバイスのバックアップ （114 ページ）
- Security Cloud Control Firewall Management を介した Firewall Threat Defense デバイスの管理 （115 ページ）
- セキュリティデバイスの概要 （116 ページ）
- Security Cloud Control Firewall Management ラベルおよびフィルタリング （118 ページ）
- Security Cloud Control Firewall Management の検索機能の使用 （119 ページ）

Security Cloud Control Firewall Management でのデバイスの 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 Firewall Management にオンボードすると、Security Cloud Control Firewall Management 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 Firewall Management 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 Firewall Management 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。

Procedure

ステップ 1 **セキュリティデバイス** を選択します。

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。

フィルタ機能と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 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。

Security Cloud Control Firewall Management でのデバイス名の変更

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 Firewall Management 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。

Procedure

ステップ 1 **セキュリティデバイス**を選択します。

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（Devices）] タブと [テンプレート（Templates）] タブの両方で使用できます。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 [セキュリティデバイス（Security Devices）] ページ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、フィルタを適用してデバイスとサービスの一部を表示します。エクスポート機能には現在 [セキュリティデバイス（Security Devices）] ページに表示されている情報のみが含まれます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

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 5 [CSVにリストをエクスポート（Export list to CSV）] をクリックします。



ステップ 6 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 7 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 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

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。

フィルタ機能と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。

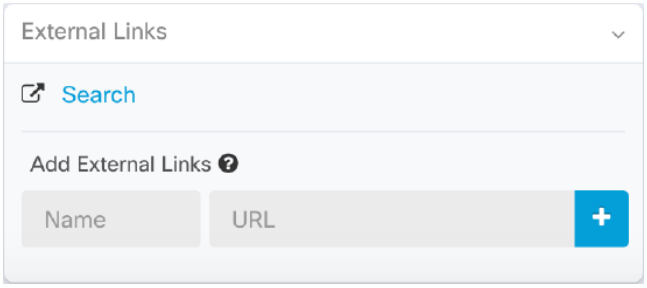
ステップ 5 必要なデバイスを選択して、強調表示します。

ステップ 6 [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 7 [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。

デバイスからの外部リンクの作成

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

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 デバイスまたはモデルを選択します。

フィルタ機能と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 6 [外部リンク（External Links）] セクションの [詳細（Details）] ペインに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。

Procedure

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。

フィルタ機能と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 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

Procedure

ステップ 1 **セキュリティデバイス**を選択します。

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。

フィルタ機能と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 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

Procedure

ステップ 1 **セキュリティデバイス**を選択します。

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。

フィルタ機能と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 デバイスまたはモデルを選択します。

ステップ 5 詳細ペインで、[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

Procedure

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。

フィルタ機能と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 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 Firewall Management へのデバイス一括再接続

Security Cloud Control Firewall Management 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 Firewall Management に同時に再接続を試みることができます。Security Cloud Control Firewall Management 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 Firewall Management 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 Firewall Management 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。

Note 新しい証明書を持つデバイスを再接続する場合、Security Cloud Control Firewall Management 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 Firewall Management 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。

Procedure

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 でのジョブモニタリング, on page 155 に移動します。

Tip 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。

組織間でのデバイスの移動

Security Cloud Control Firewall Management 組織にデバイスをオンボードした後は、デバイスを 1 つの Security Cloud Control Firewall Management 組織から別の組織に移行することはできません。デバイスを新しい組織に移動する場合は、古いテナントからデバイスを削除して、新しい組織に再オンボードする必要があります。

デバイス証明書の有効期限の検出

管理証明書は Security Cloud Control Firewall Management 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 Firewall Management 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 Firewall Management 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、「ユーザー通知設定」を参照してください。

デバイスノートの作成

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。

Procedure

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 Firewall Management からのデバイスの削除

Security Cloud Control Firewall Management からデバイスを削除するには、次の手順を実行します。

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 削除するデバイスを選択します。

ステップ 4 [デバイスアクション（Device Actions）] ペインで、[削除（Remove）] をクリックします。

ステップ 5 デバイスの削除を確認するには、[OK] をクリックします。
デバイスをオンボーディングされたままにするには、[キャンセル（Cancel）] をクリックします。

Firewall Threat Defense デバイスのバックアップ

Security Cloud Control 管理対象 Firewall Threat Defense デバイスタイプをバックアップする方法については、以下を参考にしてください。

クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスのバックアップ

- Security Cloud Control 左ペインで、管理（**Administration**）> **Firewall Management Center** を選択します。
- **[FMC]** タブで **[Cloud-delivered FMC]** を選択します。
- 右側のペインで **[Device]** をクリックして、クラウド提供型 Firewall Management Center に移動します。
- 引き続き「クラウド提供型 Firewall Management Center からの Threat Defense デバイスのバックアップ」の手順に従います。

Security Cloud Control Firewall Management にオンボーディング済みの オンプレミス Firewall Management Center によって管理される Firewall Threat Defense デバイスのバックアップ

- Security Cloud Control 左ペインで、管理（**Administration**）> **Firewall Management Center** を選択します。
- バックアップする オンプレミス Firewall Management Center の Firewall Threat Defense デバイスを選択します。
- 右側のペインで **[FMC Cross Launch URL]** をクリックして オンプレミス Firewall Management Center に移動するか、オンプレミス Firewall Management Center に手動でログインします。
- 引き続き『*Cisco Secure Firewall Management Center Administration Guide*』の「Back Up the Management Center」の指示に従ってください。

Security Cloud Control Firewall Management にオンボーディング済みの Firewall Device Manager によって管理される Firewall Threat Defense デバイスのバックアップ

「FDM 管理対象デバイスのバックアップ」の手順に従います。

Security Cloud Control Firewall Management を介した Firewall Threat Defense デバイスの管理

始める前に

Security Cloud Control Firewall Management は、ハードウェア形式と仮想形式の両方で Firewall Threat Defense デバイスを管理するための統合インターフェイスを提供します。

次の 3 つの管理アプリケーションに関連付けられている Firewall Threat Defense デバイスは、Cisco Security Cloud Control プラットフォームで管理できます。

- セキュア Firewall Device Manager
- Cisco Secure Firewall Management Center

- セキュア クラウド提供型 Firewall Management Center

手順

ステップ 1 Security Cloud Control プラットフォームにログインします。

ステップ 2 左側のペインで、[セキュリティデバイス（Security Devices）] をクリックします。

ステップ 3 [FTD] タブをクリックします。

ステップ 4 左上隅にある [フィルタ処理（Filter）] をクリックします。

[Devices/Services] の下で、フィルタペインは Security Cloud Control からアクセスされる管理アプリケーションに基づいて Firewall Threat Defense デバイスを表示するフィルタを提供します。

- **FDM**：Firewall Device Manager で管理されている Firewall Threat Defense デバイス
- **FMC-FTD**：Firewall Management Center によって管理される Firewall Threat Defense デバイス
- **FTD**：クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイス

ステップ 5 管理アプリケーションの Firewall Threat Defense デバイスを表示するには、対応するチェックボックスをオンにします。

セキュリティデバイスの概要

[Security Devices] 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。

[Security Devices] ページで、次の詳細を確認できます。

- [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。
- [Templates] タブには、ライブデバイスから、または Security Cloud Control にインポートされた設定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。

セキュリティデバイスのフィルタ

[Filter] パネルには、**[Security Devices]** ページで結果を絞り込み、特定の属性に基づいてデバイスを検索するための複数のオプションがあり、**デバイス/サービス、ハードウェアバージョン、デバイスのサポート終了、ソフトウェアバージョン、Snortバージョン、設定ステータス、接続の状態、競合検出、正常性ステータス、Secure Device Connector、およびラベル** に基づいてデバイスを検索できます。

ハードウェアのサポート終了（EoL）フィルタ

[Hardware End-of-Life (EoL)] フィルタを使用すると、ハードウェアサポートの最終日に近づいているデバイス、または最終日に達したデバイスを特定できます。この日付以降、Cisco はソフトウェアアップデート、セキュリティパッチ、またはテクニカルサポートを提供しません。これにより、運用上およびセキュリティ上のリスクが生じる可能性があります。



（注） [Hardware End-of-Life (EoL)] フィルタは現在、オンプレミス Firewall Management Center およびクラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスと、ASA デバイスをサポートしています。

手順

1. **[Devices]** タブで、フィルタアイコンをクリックします。
2. 使用可能なフィルタのリストから、**[Device End-of-Life]** で、**[Hardware End-of-Life]** を選択します。

   このリストには、ハードウェアのサポート終了が近づいている、またはハードウェアのサポート終了に達したすべてのデバイスが表示されるようになりました。
3. 右側のペインで詳細情報を表示するデバイスを選択します。
4. **[Device End of Life]** セクションまで下にスクロールすると、次の詳細が表示されます。
   - 正確なサポート終了日。
   - サポート終了日までの残り期間
5. **[Know more]** をクリックします。

   次の情報を含む詳細ページを表示できます。
   - Cisco の推奨交換デバイスと製品仕様の両方に、公式データシートを表示するためのリンクが含まれています。
   - [Contact Cisco page] ページを介してリクエストを送信するためのガイダンス、および Cisco の専門家に直接連絡するオプション。
   - Cisco の製品再利用プログラムに関する情報。
6. **[Export]** をクリックすると、デバイスレポートが CSV 形式でダウンロードされ、オフラインで分析できます。

Security Cloud Control Firewall Management ラベルおよびフィルタリング

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、対応するラベルを使用して、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。

構文 group name:label を使用してラベルグループを作成できます。たとえば、Region:East または Region:West です。これらの 2 つのラベルを作成した場合、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）] をクリックします。

ステップ 3 [Devices] タブをクリックしてデバイスを見つけるか、[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 1 つ以上のデバイスを選択します。

ステップ 6 右側の [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 アイコンをクリックします。

セキュリティデバイス、ポリシー、およびオブジェクトページのフィルタ処理

[セキュリティデバイス（Security Devices）]ページ、[ポリシー（Policies）]ページ、および[オブジェクト（Objects）]ページでフィルタを使用して、デバイスとオブジェクトを検索します。フィルタリングするには、左側のペインでフィルタアイコンを選択します。

[セキュリティデバイス（Security Devices）] ページのフィルタパネルでは、デバイスタイプ、ハードウェアバージョン、ソフトウェアバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルなどの条件でデバイスをフィルタリングできます。選択したデバイスタイプのタブ内でフィルタを適用できます。

[FTD] タブを開いている場合、フィルタパネルでは、Security Cloud Control が FTD デバイスへのアクセスに使用する管理アプリケーションで、それらのデバイスをフィルタリングすることもできます。

フィルタリングするには、[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 [フィルタ処理（Filter）] をクリックします。

（注） [FTD] タブを開くと、フィルタペインでフィルタを使用できます。これにより、Security Cloud Control からデバイスにアクセスするために使用されている管理アプリケーションに基づいて FDM による管理 デバイスが表示されます。

- FDM：FTD API または Firewall Device Manager を使用して管理されるデバイス。
- FMC-FTD：Firepower Management Center を使用して管理されるデバイス。
- FTD：FTD 管理を使用して管理されるデバイス。

Security Cloud Control Firewall Management の検索機能の使用

Security Cloud Control Firewall Management 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、[セキュリティデバイス（Security Devices）]、[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。

- [セキュリティデバイス（Security Devices）] 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。

Procedure

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。

グローバル検索

グローバル検索機能を使用すると、Security Cloud Control の管理対象のデバイスをすばやく見つけてナビゲートできます。

（注） 現在、Security Cloud Control は、Cisco ASA、クラウド提供型 Firewall Management Center、Security Cloud Control で管理されるオンプレミス Firewall Management Center、Firewall Threat Defense、および Cisco Meraki のグローバル検索をサポートしています。

グローバル検索は、Security Cloud Control Firewall Management が Security Cloud Control にオンボードされている場合にのみ使用できます。

すべての検索結果は、選択したインデックス作成オプションに基づいています。インデックス作成オプションは次のとおりです。

- フルインデックス作成：フルインデックス作成プロセスを呼び出す必要があります。このプロセスは、システム内のすべてのデバイスとオブジェクトをスキャンし、インデックス作成を呼び出した後にのみ、それらを検索インデックスに表示します。フルインデックス作成を呼び出すには、管理者権限が必要です。

  詳細については、フルインデックス作成の開始 （122 ページ）を参照してください。

- 増分インデックス作成：イベントベースのインデックス作成プロセスで、デバイスまたはオブジェクトが追加、変更、または削除されるたびに検索インデックスが自動的に更新されます。

検索フィールドに入力する情報では、大文字と小文字が区別されません。次のエンティティを使用して、グローバル検索を実行できます。

- [デバイス名（Device Name）]：部分的なデバイス名、URL、IP アドレス、または範囲をサポートします。
- [オブジェクトタイプ（Object Types）]：オブジェクト名、オブジェクトの説明、および構成された値をサポートします。
- [ポリシータイプ（Policy Types）]：ポリシー名、ポリシーの説明、ルール名、およびルールコメントをサポートします。

  クラウド提供型 Firewall Management Center および、Security Cloud Control で管理されるオンプレミス Firewall Management Center は、次のポリシータイプをサポートします。

  - アクセス コントロール ポリシー（Access Control Policy）
  - プレフィルタポリシー（Prefilter Policy）
  - Threat Defense NAT ポリシー

検索式を入力すると、インターフェイスに検索結果の表示が開始され、検索を実行するために Enter キーを押す必要はありません。

検索結果には、検索語に一致するすべてのデバイスとオブジェクトが表示されます。検索語が複数のデバイスやオブジェクトに一致する場合、結果はカテゴリ（Devices、Objects、および connected_fmc）の下に表示されます。

デフォルトでは、検索結果の最初の項目が強調表示され、その項目の関連情報が右側のペインに表示されます。検索結果をスクロールして項目をクリックすると、対応する情報を表示できます。項目の横にある矢印アイコンをクリックして、対応するページに移動できます。

（注）

- グローバル検索では、重複する検索結果は表示されません。オブジェクトの場合、共有オブジェクトの UID は、オブジェクトビューに移動するために使用されます。
- Security Cloud Control からデバイスを削除すると、関連するすべてのオブジェクトがグローバル検索インデックスから削除されます。
- ポリシーからオブジェクトを削除し、デバイスを保持した状態でフルインデックス作成を開始すると、削除したオブジェクトはデバイスに関連付けられているため、グローバル検索インデックスに残ります。

フルインデックス作成の開始

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

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 グローバル検索で、[フルインデックス作成の開始（Initiate Full Indexing）] をクリックしてインデックス作成をトリガーします。



（注） フルインデックスの作成を開始すると、Security Cloud Control テナントの既存のインデックスがクリアされます。

ステップ 4 ここをクリックして、グローバル検索ワークフローを表示します。

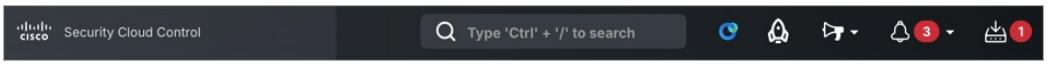
グローバル検索の実行

手順

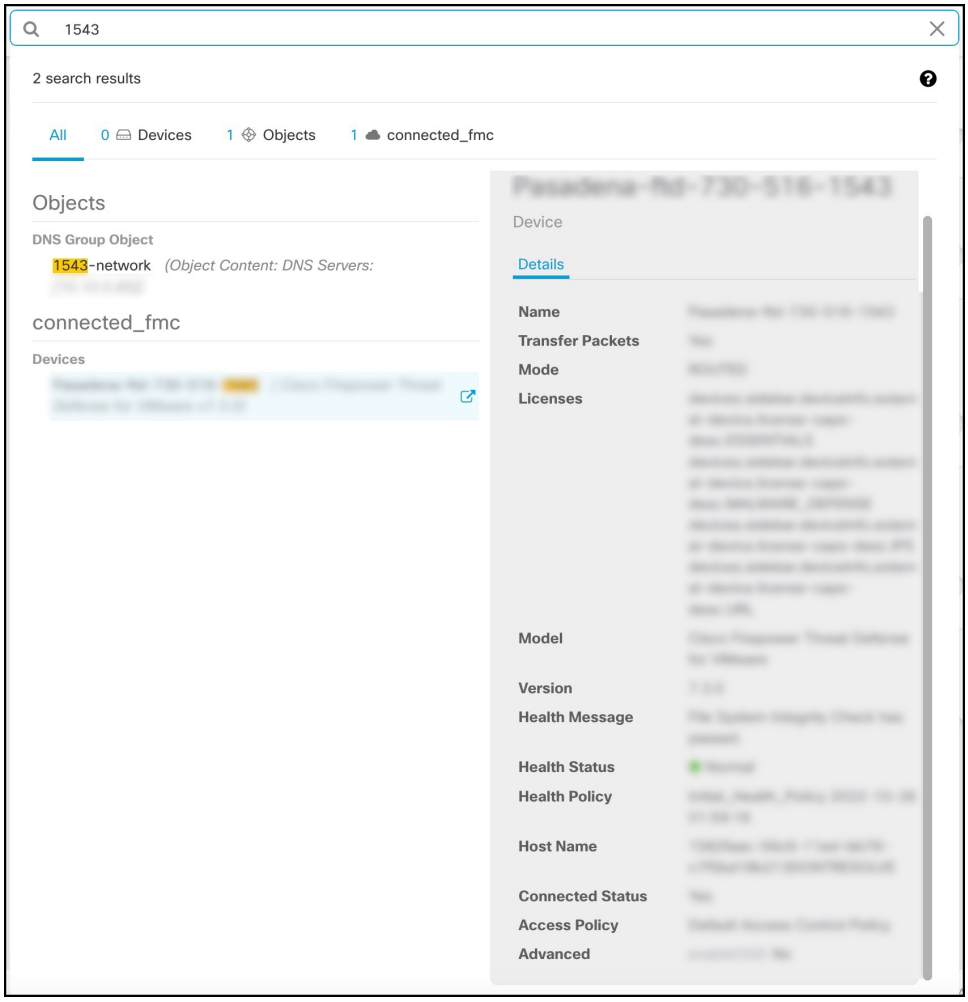
ステップ 1 Security Cloud Control にログインします。

ステップ 2 Security Cloud Control ページにある検索アイコンをクリックし、表示される [Search] フィールドに検索文字列を入力します。

または、Windows の場合は **Ctrl** キーを押しながら / キーを押す、Mac の場合は **Command** キーを押しながら / キーを押して検索バーを開くこともできます。



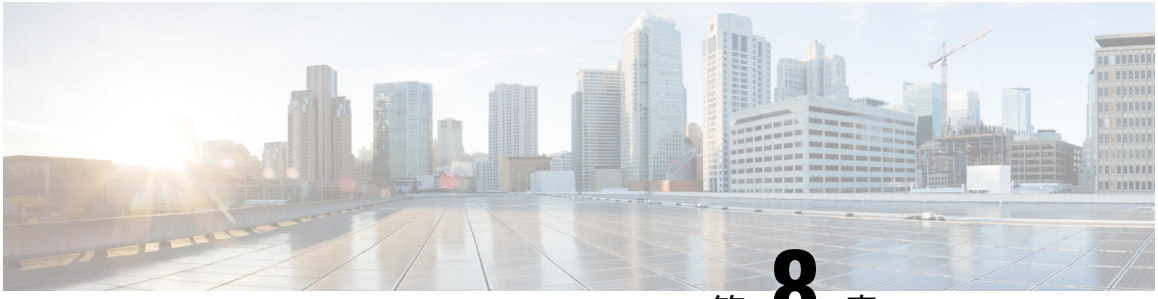
検索文字列の入力を開始すると、可能性のある項目のリストが表示されます。検索結果は、[すべて（All）]、[デバイス（Devices）]、[オブジェクト（Objects）]、[ポリシー（Policies）]、およびクラウド提供型 Firewall Management Center の 4 つのカテゴリの下に表示されます。右ペインには、選択した検索結果の情報が表示されます。



ステップ 3 検索結果からデバイスまたはオブジェクトを選択し、矢印アイコンをクリックして、検索結果から対象のデバイスおよびオブジェクトのページに移動します。検索結果からオブジェクトを選択し、矢印アイコンをクリックして、検索結果から対象のページに移動します。

（注） クラウド提供型 Firewall Management Center でデバイスの検索結果を選択すると、Security Cloud Control 内の クラウド提供型 Firewall Management Center ユーザーインターフェイスに移動できます。

ステップ 4 [X] をクリックして検索バーを閉じます。



第 8 章

デバイス設定の管理

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 が管理対象デバイスから設定を読み取ると、設定をコピーして保存します。

Security Cloud Control はデバイスが導入されたときに、デバイスの設定のコピーを読み取って保存します。これらのアクションにはそれぞれ特定の目的があります。

- [変更の破棄（Discard Changes）]：このアクションは、デバイス設定のステータスが [未同期（Not Synced）] の場合に使用できます。[未同期（Not Synced）] の状態では、デバイス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、デバイス設定のステータスが [同期済み（Synced）] 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、そのデバイス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。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）]：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するには、[競合の確認（Review Conflict）] をクリックします。

  - [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 のデバイス設定のコピーが、デバイスに保存されている最新の設定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 2 つの設定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 はその変更を自らの設定のコピーに保存します。これらの変更は、デバイスに展開するまで Security Cloud Control で [保留中（Pending）] のままです。展開されていない保留中の変更がある場合、デバイスの設定状態は [未同期（Not Synced）] になります。

  保留中の設定変更は、ネットワークトラフィックには影響しません。これらは、Security Cloud Control がデバイスに展開した後にのみ有効になります。

  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。デバイス構成ファイル全体が上書きされることはありません。1つまたは複数のデバイスに変更を同時に展開できます。

- [すべて破棄（Discard All）]：このオプションは、[プレビューして展開...（Preview and Deploy...）] をクリックした後に表示されます。[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、保留中の変更すべてを、選択したデバイスに展開せずに Security Cloud Control から削除できます。[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。

- 設定変更の読み取り、破棄、および展開 （126 ページ）
- Security Cloud Control とデバイス間の設定を同期する （136 ページ）

設定変更の読み取り、破棄、および展開

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、「設定変更の読み取り、破棄、チェック、および展開」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。
- [未同期（Not Synced）]：デバイスが [未同期（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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

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ます。

ステップ 5 （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、変更リクエストラベルを作成します。

ステップ 6 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。

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。

ステップ 7 [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 **[Read All]** 操作の進行状況については、[notifications] タブ 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 **[Review]** リンクをクリックすると、[Jobs] ページに移動します。

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。

すべてのデバイスの設定変更のプレビューと展開

Security Cloud Control は、組織のデバイスに設定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、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

の影響を受ける各デバイスについて、[セキュリティデバイス（Security Devices）]ページに「未同期（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。

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、単一の設定変更を展開できます。または、待機して複数の変更を一度に展開することもできます。

このデプロイメントメソッドは、Security Cloud Control Firewall Management が Security Cloud Control にオンボードされている場合にのみ使用できます。

手順

ステップ 1 Security Cloud Control のメニューバーで、[展開（Deploy）] ボタン 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。黄色の三角の注意マークにマウスのポインタを合わせて、理由を確認します。

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、**[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 [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 5 （オプション）展開が完了したら、[プラットフォーム（Platform）] メニューで [ファイアウォール（Firewall）]をクリックし、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[ジョブ（Jobs）]** の順に選択します。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。

デバイスへの変更の展開

Procedure

ステップ 1 Security Cloud Control を使用してデバイスの設定を変更して保存すると、その変更はデバイスの設定の Security Cloud Control インスタンスに保存されます。

ステップ 2 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **セキュリティデバイス**を選択します。

ステップ 4 [デバイス] タブをクリックします。

ステップ 5 適切なデバイスタイプのタブをクリックします。変更を加えると、デバイスの設定ステータスに [未同期（Not synced）] と表示されます。

ステップ 6 次のいずれかの方法を使用して、変更を展開します。

- デバイスを選択し、[未同期（Not Synced）] ペインで [プレビューして展開（Preview and Deploy）] をクリックします。[保留中の変更（Pending Changes）] 画面で、変更を確認します。保留中のバージョンに問題がなければ、[今すぐ展開（Deploy Now）] をクリックします。

  変更が正常に展開されたら、変更ログを表示して、展開の結果を確認できます。

- [展開（Deploy）] アイコン をクリックします。詳細については、すべてのデバイスの設定変更のプレビューと展開, on page 127を参照してください。

変更をキャンセルする

Security Cloud Control からデバイスに変更を展開するときに [キャンセル（Cancel）] をクリックすると、行った変更はデバイスに展開されません。プロセスはキャンセルされます。行った変更はまだ Security Cloud Control で保留中であり、最終的に FDM による管理 デバイスに展開する前に編集を加えることができます。

変更の破棄

変更をプレビューしているときに [すべて破棄（Discard all）] をクリックすると、自分が行った変更と、他のユーザーが行ったもののデバイスに展開しなかったその他の変更が削除されます。Security Cloud Control は、保留中の構成を、変更が行われる前の最後の読み取りまたは展開された構成に戻します。

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。

Procedure

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。

Note [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, on page 33 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 に読み取られていない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。

Caution 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。

Note 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。このオプションを有効にすると、単一の自動展開をスケジュールしたり、定期的な自動展開を設定したりできます。

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

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



Important 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。

スケジュールされた自動展開を有効にするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** を選択します。

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

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。



Important この手順は、Cisco ASA および FDM-managed デバイスにのみ適用されます。

[on-premises Firewall Management Center] または [Cloud-Delivered Firewall Management Center] によって管理される [Cisco Secure Firewall Threat Defense] デバイスの展開をスケジュールするには、「スケジュール」を参照してください。

Note 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。

Procedure

ステップ 1 Cisco Security Cloud Control ホームページから、**セキュリティデバイス** を選択します。

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。

Procedure

ステップ 1 Cisco Security Cloud Control ホームページから、**セキュリティデバイス** を選択します。

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。



Note 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] 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。

- 設定変更の読み取り、破棄、チェック、および展開
- すべてのデバイス設定の読み取り, on page 126
- すべてのデバイスの設定変更のプレビューと展開, on page 127

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。

Procedure

ステップ 1 Cisco Security Cloud Control ホームページから、**セキュリティデバイス** を選択します。

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。

- Meraki 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。

- デバイスの場合：

a. 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。

b. 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。

c. [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 [未同期（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。

Procedure

ステップ 1 Cisco Security Cloud Control ホームページから、**セキュリティデバイス** を選択します。

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、**管理（Administration）** > **統合（Integrations）** > **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 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場合、Security Cloud Control は オンプレミス Firewall 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, on page 141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。

Procedure

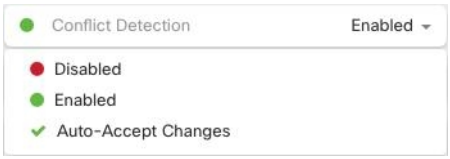
ステップ 1 **セキュリティデバイス**を選択します。

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, on page 136 を有効にします。

自動承認変更の設定

Procedure

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。

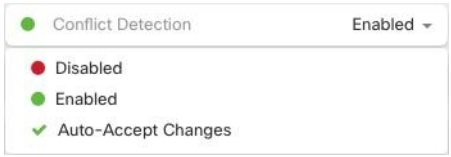
ステップ 2 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 4 [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 5 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 6 [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

Procedure

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 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 3 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 4 [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。

Note [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

ここでは、デバイスで発生する設定の競合を解決する方法について説明します。

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。

Procedure

ステップ 1 **セキュリティデバイス**を選択します。

Note オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **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、今行った変更をプレビューして展開するか、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, on page 136 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

Note オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **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 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ます。

ステップ 5 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 6 [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 7 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。

Note 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。

Note 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, on page 136 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。デバイスごとに、Security Cloud Control が変更をポーリングする頻度を設定できます。このカスタマイズは複数のデバイスに適用できます。

この間隔が設定されていないデバイスについては、間隔が「テナントのデフォルト」に自動的に設定されます。

Note [セキュリティデバイス（Security Devices）] ページでデバイスごとのカスタム間隔を設定すると、[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）]デフォルトの競合検出間隔の設定, on page 32で選択したポーリング間隔が上書きされます。

[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できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

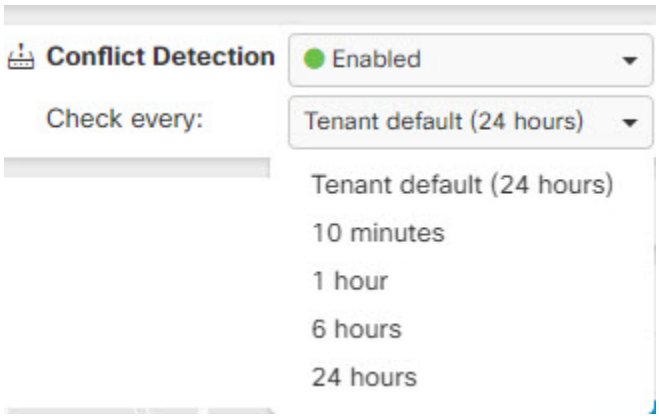
ステップ 2 **セキュリティデバイス**を選択します。

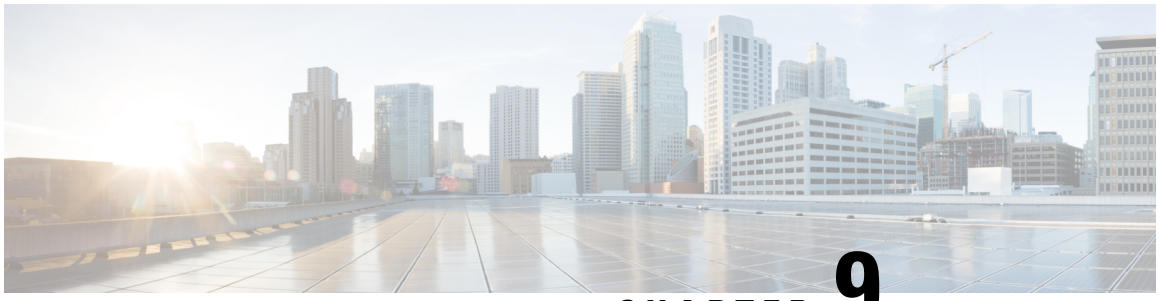
ステップ 3 [デバイス（Devices）] タブをクリックして、デバイスを見つけます。

ステップ 4 適切なデバイスタイプのタブをクリックします。

ステップ 5 競合検出を有効にするデバイスを選択します。

ステップ 6 [競合検出（Conflict Detection）] の横にある [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。





CHAPTER 9

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 の変更ログ （143 ページ）
- 変更ログの差異の表示 （145 ページ）
- 変更リクエスト管理 （146 ページ）
- 変更ログのエクスポート, on page 154
- Security Cloud Control でのジョブモニタリング （155 ページ）
- Security Cloud Control でのワークフローのモニタリング （157 ページ）

Security Cloud Control の変更ログ

変更ログは、次のような設定追跡機能です。

- 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。
- デバイス構成に加えられた変更の対照比較を示します。
- 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。

変更ログの管理機能

変更ログには、設定管理および障害対応に関する次の機能が用意されています。

- すべての変更ログエントリのラベルを示します。
- インシデントの調査または障害対応中に、「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。

（注） クラウド提供型 Firewall Management Center で行われた変更は、変更ログに反映されません。

[変更ログの容量（Change log capacity）]：Security Cloud Control は変更ログ情報を 1 年間保持し、1 年を超える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（154ページ）を参照してください。

[変更ログエントリ（Change log entries）]： 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（Pending and completed change log entries）]： 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。保留中の変更ログを完了するアクティビティは次のとおりです。

- 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（Search and filter change log entries）]：変更ログエントリの検索とフィルタ処理ができます。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（フィルタアイコン）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

変更ログの差異を表示し、実行構成ファイルの変更前後の状態を調べることで、デバイスに加えられた設定変更を分析します。

変更ログの差異では、元の構成ファイルと変更された構成ファイルの詳細な比較が提供され、デバイス設定にどのような変更が加えられたかを把握できます。左右のビューでは、実行構成内で追加、変更、および削除された箇所が強調表示されます。

手順

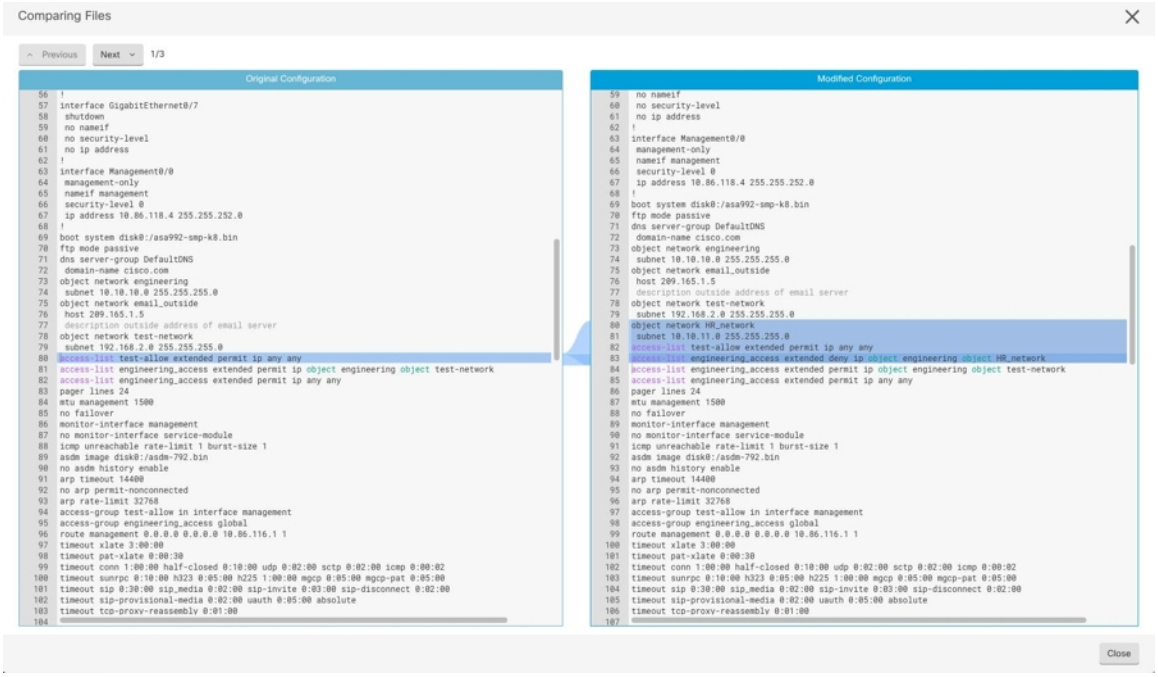
ステップ 1 変更ログで [差分（Diff）] をクリックします。

対象デバイスの実行構成ファイル内の変更が並べて表示されます。

[元の設定（Original Configuration）] 列には、変更が ASA デバイスに書き込まれる前の実行構成ファイルが表示されます。[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。

ステップ 2 左の列から右の列まで線をたどって、変更を確認します。

比較ビューでは、HR_network オブジェクトや、engineering ネットワーク内のアドレスが HR_network ネットワーク内のアドレスに到達するのを防ぐアクセスルールなどの追加箇所を確認できます。[元の設定（Original Configuration）] 列では、[変更された設定（Modified Configuration）] 列の変更内容を把握するための参照ポイントとなる行が強調表示されます。



ステップ 3 [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。

元のデバイス設定と変更されたデバイス設定の差分を表示して分析し、設定の更新プロセス中にどのような変更が行われたかを正確に把握できます。

変更リクエスト管理

変更リクエスト管理には次のような機能があります。

- [変更リクエスト（Change Request）] とそのビジネス上の正当性を [変更ログ（Change Log）] イベントにリンクできます。
- サードパーティのチケットシステムで [変更リクエスト（Change Request）] を開きます。
- Security Cloud Control での [変更リクエスト（Change Request）] の作成を許可し、変更ログイベントに関連付けます。

変更リクエスト管理の使用方法

[変更リクエスト管理（Change Request Management）] を使用して、Security Cloud Control で [変更リクエスト（Change Request）] 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。

変更リクエスト管理の有効化

変更リクエストの追跡を有効にすると、組織内のすべてのユーザーが行った設定変更を可視化し、制御できます。

変更要求トラッキングの有効化は、組織のすべてのユーザーに影響を及ぼします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

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



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。

組織で変更リクエストの追跡が有効になりました。[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）] ページに [変更リクエスト（Change Request）] ドロップダウンリストが表示されます。

変更リクエストの作成

変更リクエストを作成し、ネットワーク内のデバイスに加えられる設定変更を整理して追跡することで、変更を適切に文書化して監視できるようになります。

変更リクエストでは、関連する設定変更をグループ化し、変更の監査証跡を維持するための構造化された方法が提供されます。一度作成されると、後続のすべての変更は、アクティブな変更リクエストがクリアされるか無効になるまで、その変更リクエストに関連付けられます。

Procedure

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。

Note 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。

Note [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、変更リクエストを無効化するか、メニューから変更リクエストをクリアするまで続きます。

変更リクエストが作成され、アクティブな変更リクエストになります。変更リクエスト管理を無効にするか、変更リクエストの詳細をクリアするまで、後続の設定変更はすべて、この変更リクエストに関連付けられます。

変更リクエストと変更ログイベントの関連付け

変更リクエストを変更ログイベントに関連付けて、監査証跡を残し、設定変更の理由を追跡します。

設定変更の承認と理由を文書化するために、変更リクエストを特定の変更ログイベントにリンクする必要がある場合は、この手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 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 4 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。

Note 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 5 変更リクエストを選択して、[選択（Select）] をクリックします。

変更リクエストが変更ログイベントに関連付けられ、承認と設定変更の間にトレース可能なリンクが作成されます。

変更リクエストを使用した変更ログイベントの検索

このタスクでは、関連する変更リクエスト名を検索することによって、特定の変更ログイベントを見つけることができ、変更とそれに対応するドキュメントを追跡できるようになります。

監査、追跡、または分析の目的で、特定の変更リクエストにリンクされている変更ログイベントを検索する必要がある場合に、この手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 [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。

検索条件に一致する変更ログイベントが表示されます。完全一致は強調表示され、簡単に特定できます。

変更リクエストの検索

部分一致を使用して名前や説明で検索することにより、ユーザーは既存の変更リクエストをすばやく見つけることができます。

システム内の複数のエントリ間で特定の変更リクエストを見つける必要がある場合は、この検索機能を使用します。

Procedure

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。

検索条件に一致する変更リクエストが名前フィールドと説明フィールドの両方に表示されるため、目的の変更リクエストをすばやく見つけることができます。

変更リクエストのフィルタ処理

変更リクエストをフィルタ処理して、セキュリティ環境内の特定の設定変更やイベントをすばやく見つけて確認できます。

変更ログのフィルタ機能を使用して、特定の基準に基づいて変更リクエストのリストを絞り込むことができます。この操作により、デバイス全体の設定変更を効率的に確認および管理できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 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 4 [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 5 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。

[変更ログ（Change Log）] テーブルには、検索条件に一致するフィルタ処理された変更リクエストのみが表示されます。完全一致は強調表示され、簡単に特定できます。

変更リクエストツールバーのクリア

変更リクエストツールバーをクリアすると、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ことを防ぐことができます。

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防ぐ必要がある場合は、変更リクエストツールバーの情報をクリアします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 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 3 [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。

変更リクエストツールバーがクリアされ、[なし（None）] と表示され、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くなります。

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

このタスクでは、接続が不要になった場合や誤って作成された場合に、変更リクエストと変更ログイベント間の関連付けを削除できます。

この手順は、変更ログインターフェイスで変更ログイベントから変更リクエストの関連付けを解除する必要がある場合に使用します。不要な接続を削除することで、変更を正確に追跡し、整理できるようになります。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 [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 4 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 5 [クリア（Clear）] をクリックします。

変更リクエストと選択した変更ログイベントとの関連付けが正常に解除され、それらの項目間の接続が削除されました。

変更リクエストの削除

変更リクエストが不要になった場合は、変更リクエストを削除して、アクティブな変更リクエストリストから削除します。

[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。

変更リクエストは変更リクエストリストから削除されますが、履歴参照用に変更ログには引き続き表示されます。

変更リクエスト管理の無効化

このタスクでは、アカウントで変更リクエスト管理機能が不要になった場合、その機能を無効にします。

[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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 3 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを無効化します。

変更リクエスト管理および変更リクエスト追跡の機能が、アカウント内のすべてのユーザーに対して無効になります。

変更リクエストの管理と変更ログイベントの関連付け

このタスクは、ファイアウォールデバイスに加えられた変更を追跡し、それらを変更リクエストに関連付けて、外部システムで維持されているチケットを解決するのに役立ちます。変更リクエストを作成し、変更ログイベントを関連付けて、特定の変更リクエストに関連するイベントを検索できます。

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。さまざまなシナリオで変更リクエスト管理を使用して、監査証跡を維持し、ファイアウォールの変更を外部のチケットシステムに関連付けることができます。

手順

ステップ 1 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加えられた変更を追跡します。

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。

1. 変更リクエストの作成 （147 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のクリア （150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。

ステップ 2 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します。

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。

1. 変更リクエストの作成 （147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 （148 ページ）。
4. 変更リクエストツールバーのクリア （150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。

ステップ 3 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。

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。

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。
   - 変更リクエストのフィルタ処理 （150 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。

変更リクエストが正常に管理され、変更ログイベントが外部チケットに関連付けられました。変更ログには、変更リクエストにリンクされた追跡可能なイベントが含まれるようになり、ファイアウォール変更の監査証跡が提供されます。

変更ログのエクスポート

変更ログデータをカンマ区切り値（.csv）ファイルにエクスポートして、システム外での変更レコードのフィルタリング、ソート、分析を可能にします。

Security Cloud Control 変更ログのすべてまたは一部をカンマ区切り値（.csv）ファイルにエクスポートし、必要に応じて情報をフィルタリングしたり、並べ替えたりできます。

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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 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（フィルタアイコン）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。

Note 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することをお勧めします。

ステップ 4 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 5 .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。

変更ログデータはローカルシステム上の CSV ファイルにエクスポートされ、必要に応じて追加のフィルタリング、ソート、および分析を実行できます。

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

変更ログのキャパシティの違いとは、次のようなデータストレージの相違点です。

- Security Cloud Control のデータベースに保存されている完全な変更ログ情報と、エクスポートされたファイルに含まれる情報のサブセットを区別します。
- データベース操作とエクスポート機能ではストレージ要件が異なることに起因します。
- ユーザーが変更ログデータをエクスポートするときのファイルサイズに影響します。

変更ログのストレージ構造

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。

Security Cloud Control でのジョブモニタリング

Security Cloud Control でのジョブモニタリングは、次のことを行う管理インターフェイスです。

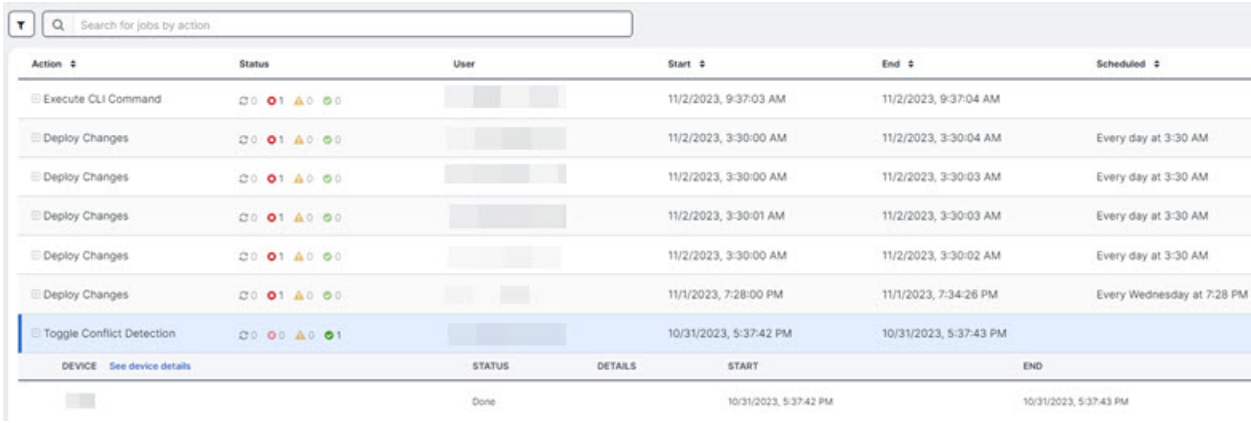
- 複数デバイスの再接続、複数デバイスからの設定の読み取り、複数デバイスの同時アップグレードなど、一括操作の進行状況の概要を示します。
- 個々のアクションのステータスとともに色分けされた行を使用し、それぞれが成功したか失敗したかを示します。
- 行を展開すると、一括操作の影響を受ける各デバイスの結果が表示されます。

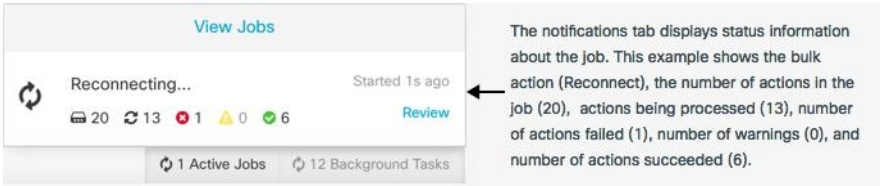
ジョブへのアクセス方法

[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）** > **イベント（Events）] 見出し** > **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。

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

このタスクでは、ジョブ全体を再実行せずに、一括操作内の失敗したアクションを再試行できます。

[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。

Procedure

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。

元の一括操作で失敗したアクションのみが再試行され、ジョブのステータスはそれに応じて更新されます。

一括アクションのキャンセル

想定よりも時間がかかっている可能性がある、または不要になった複数のデバイスで進行中の操作を停止する必要がある場合、現在進行中の一括アクションをキャンセルします。

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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **イベントとログ（Events & Logs）** > **イベント（Events）] 見出し** > **ジョブ（Jobs）** をクリックします。

ステップ 3 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。

Note 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。

一括アクションがキャンセルされ、進行中の操作は停止しますが、正常に完了した部分は保持されます。

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

ワークフローモニタリングは、次のような Security Cloud Control 機能です。

- 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追跡します。

- 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、その結果を表示します。
- 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、通信対象のデバイスについての情報は含まれません。

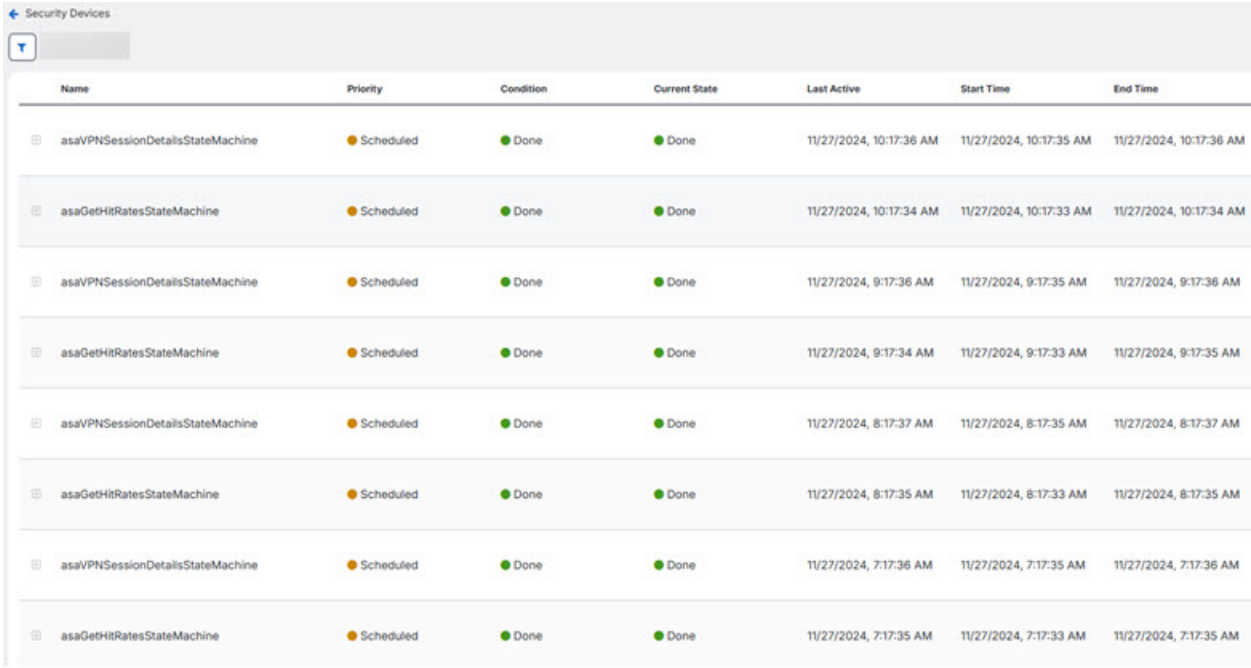
ワークフローエラーのレポートと障害対応

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。

図 *1 :* ワークフローテーブルにエントリが表示される *[*ワークフロー（*Workflows*）*]* ページ



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 10 章

Terraform

この章では、Security Cloud Control を設定および管理する方法について説明します。

- Terraform について （161 ページ）

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 Cisco 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 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 11 章

トラブルシューティング

この章では、Security Cloud Control Firewall Management のさまざまなコンポーネントを使用するときに発生する可能性のあるエラーをトラブルシュートする方法について詳しく説明しています。

- Secure Device Connector のトラブルシュート （163 ページ）
- Security Cloud Control のトラブルシューティング, on page 174
- デバイスの接続状態, on page 176

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、Cisco Technical Assistance Center でケースを開いてください。

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。

   直接クラウド接続のインバウンドアクセスを許可 （54 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、**管理（Administration）** > **統合（Integrations）** > **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 [Active] にならない （164 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 [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。

Procedure

ステップ 1 Security Cloud Control で、アクティブと表示されていない SDC をクリックし、**[Request Heartbeat]** をクリックします。

ステップ 2 次のコマンドを使用して、コンテナが実行されていることを確認します。

```
docker ps
```

ステップ 3 SDC ログを表示し、次のコマンドを使用してエラーを確認します。

```
sdc show logs
```

ステップ 4 次のコマンドを使用してコンテナを再起動します。

```
sdc restart
```

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

SDC の更新された IP アドレスを表示するには、前述の手順を使用してハートビートを要求し、ブラウザを更新します。

ハートビートの要求

Security Cloud Control で、アクティブと表示されていない SDC をクリックし、サイドバーで **[Request Heartbeat]**をクリックします。

1. 次のコマンドを使用してコンテナが実行されていることを確認します：`docker ps`
2. SDCログを表示し、`sdc show logs` コマンドを使用してエラーを確認します
3. 次のコマンドを使用してコンテナを再起動します：`sdc restart`

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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **管理（Administration）** > **統合（Integrations）** > **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 3 SDC を選択します。

ステップ 4 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 5 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 6 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 サポートまでお問い合わせください。

SDC との断続的な接続または接続がない

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、オンプレミスの SDC で、CentOS を引き続き使用している場合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）** > **統合（Integrations）** > **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 （168 ページ）
  - カスタム SDC ホストを更新する （169 ページ）

• バグトラッキング （169 ページ）

Security Cloud Control 標準の SDC ホストの更新

• Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

• Security Cloud Control イメージを使用して SDC を展開した場合は、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

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- 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

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- 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。

以下の手順を実行します。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。

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

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォー

ルでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- 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 [Tools & Services] [Secure Connectors] の順に移動して、[Secure Connectors] ページに記載されています。**管理（Administration）** > **統合（Integrations）** > **セキュアコネクタ（Secure Connectors）** 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。

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
```

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

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

Procedure

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。

a. [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。

b. 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, on page 139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。

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、知っている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://security.cisco.com にログインします。

- **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** Security Cloud Control APJ
  - **解決法** Security Cloud Control オーストラリア
  - **解決法** Security Cloud Control EU
  - **解決法** Security Cloud Control インド
  - **解決法** Security Cloud Control 米国
- **解決法** https://security.cisco.com を指すようにブックマークを更新します。

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。**[Security Devices]** ページの **[Connectivity]** カラムに、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, on page 178
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, on page 178
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。
不明（Unknown）	デバイスのオンボーディングに失敗し、Security Cloud Control はデバイスの接続状態を取得できません。	**セキュリティデバイス** ページでデバイスを選択し、右側のペインから **[Check for Changes]** を選択して、そのデバイスから最新の設定の取得を試みます。
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, on page 179
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, on page 189

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。

Procedure

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。

Procedure

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 プロンプトが表示されたら、デバイスの新しいユーザー名とパスワードを入力します。

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, on page 139

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。

Note 複数の管理対象デバイスを Security Cloud Control に同時に一括再接続すると、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） デバイスの一括再接続により、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。

Procedure

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, on page 136 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。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

Note オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **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 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ます。

ステップ 5 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 6 [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 7 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。



Note 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。



Note 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。

Procedure

ステップ 1 **セキュリティデバイス**を選択します。



Note オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **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。

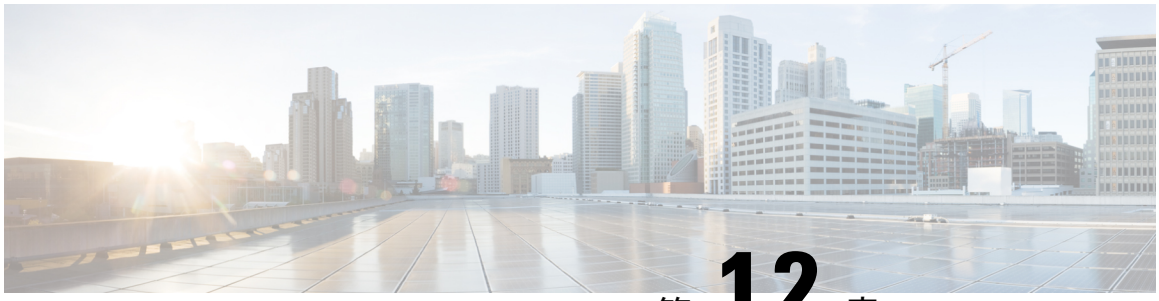
ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

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、今行った変更をプレビューして展開するか、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 12 章

FAQ とサポート

この章は、次の項で構成されています。

- Security Cloud Control, on page 193
- Security Cloud Control へのデバイスのオンボーディングに関する FAQ （194 ページ）
- デバイスタイプ, on page 196
- セキュリティ, on page 197
- トラブルシューティング, on page 198
- 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, on page 199
- ポリシーの最適化, on page 199
- 接続性, on page 200
- データインターフェイスについて （200 ページ）
- Security Cloud Control による個人情報の処理方法 （201 ページ）
- Security Cloud Control サポートへのお問い合わせ, on page 201

Security Cloud Control

Security Cloud Controlとは

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。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 Security Cloud Control』[英語] を参照してください。

Cisco 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

Cisco Secure Firewall Threat Defense をオンボード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。

Cisco Secure Firewall Threat Defense のオンボーディング後はどうすればよいですか？

デバイスが同期されたら、**管理（Administration）** > **統合（Integrations）** > **Firewall Management Center** に移動し、[Actions]、[Management]、または [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。

Cisco Secure Firewall Threat Defense をトラブルシュートするにはどうすればよいですか？

「オンボーディングのトラブルシュートCisco Secure Firewall Threat Defense」を参照してください。

オンプレミスFirewallManagementCenterに関するよくある質問（FAQ）

どうすれば オンプレミス Firewall Management Center をオンボーディングできますか？

オンプレミス Firewall Management Center は Security Cloud Control にオンボーディングできます。オンプレミス Firewall Management Center へのオンボーディングでは、オンプレミス Firewall Management Center に登録されたすべてのデバイスもオンボーディングします。Security Cloud Control では、オンプレミス Firewall Management Center に関連付けられたオブジェクトまたはポリシー、または オンプレミス Firewall Management Center に登録されたデバイスの作成や変更をサポートしていません。そのような変更は オンプレミス Firewall Management Center UI で行う必要があります。詳細については、「オンプレミス Management Center のオンボード」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, on page 127

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 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（SDC）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。

詳細については、「Secure Device Connector（SDC）」を参照してください。

SDC には追加のコストやライセンスが必要ですか？

いいえ。

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。

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。

Note 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 Firewall Management でのデバイスの IP アドレスの変更, on page 105を参照）、デバイスを再接続できます（Security Cloud Control Firewall Management へのデバイス一括再接続, on page 112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、『Security Cloud Control Privacy Data Sheet』[英語] を参照してください。

Security Cloud Control サポートへのお問い合わせ

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。

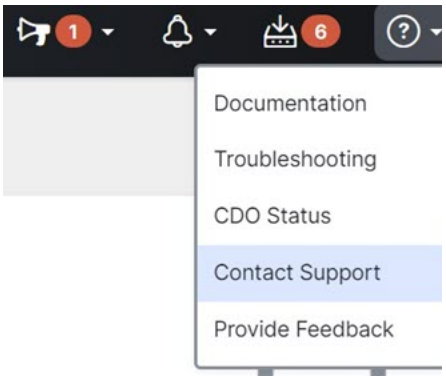
Security Cloud Control のお客様が TAC でサポートチケットを開く方法

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。

Procedure

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、『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。
    a. Cisco Profile Manager を開きます。
    b. [アクセス管理（Access Management）] タブをクリックします。
    c. [アクセス権の追加（Add Access）] をクリックします。
    d. [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。
    e. 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。

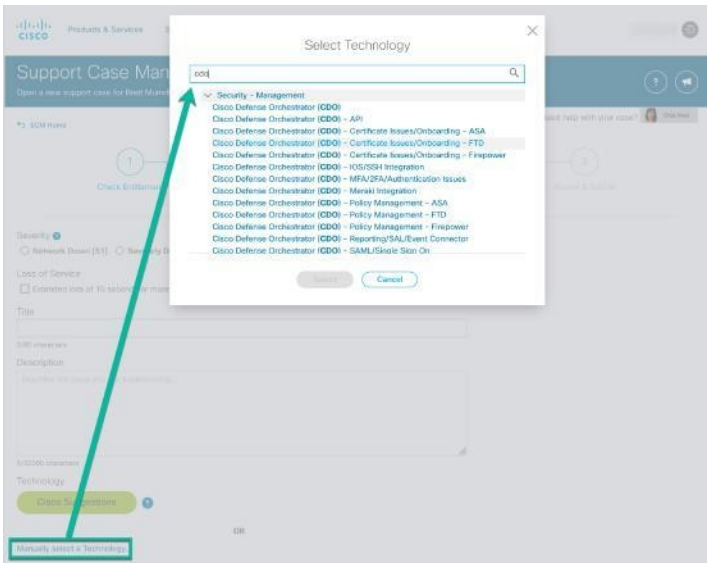


Important 重要：以下のリンクのいずれにもアクセスできない場合は、シスコ認定のパートナーや再販業者、シスコのアカウント担当者、または社内でシスコサービスの契約情報を管理する担当者にお問い合わせください。

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。

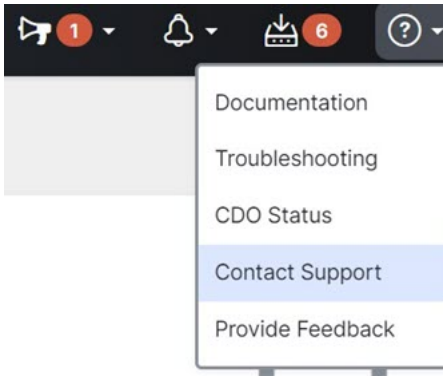
Security Cloud Control のトライアルのお客様が TAC でサポートチケットを開く方法

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。