

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 1
- Security Cloud Control 組織内のユーザーとグループの管理 （11 ページ）
- Security Cloud Control Firewall Management の API 専用ユーザーの管理 （11 ページ）
- Security Cloud Control 通知の表示 （12 ページ）
- ロギング設定の表示, on page 15
- **Security Cloud Control Firewall Management のユーザーロールを理解する**, on page 16
- 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 （20 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。

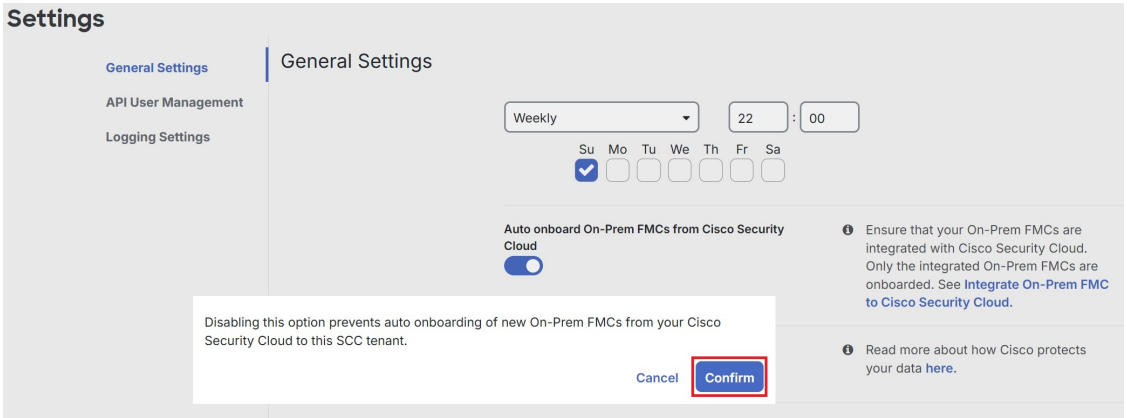
手順

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。

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。