

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

- Cisco Security Cloud Control の概要 （1 ページ）
- Security Cloud Control Firewall Management の概要 （4 ページ）
- クラウド提供型 Firewall Management Center の概要 （7 ページ）
- Security Cloud Control Firewall Management のプロビジョニング （14 ページ）
- Security Cloud Control Firewall Management を開く （15 ページ）
- ファイアウォール管理ダッシュボード （16 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。

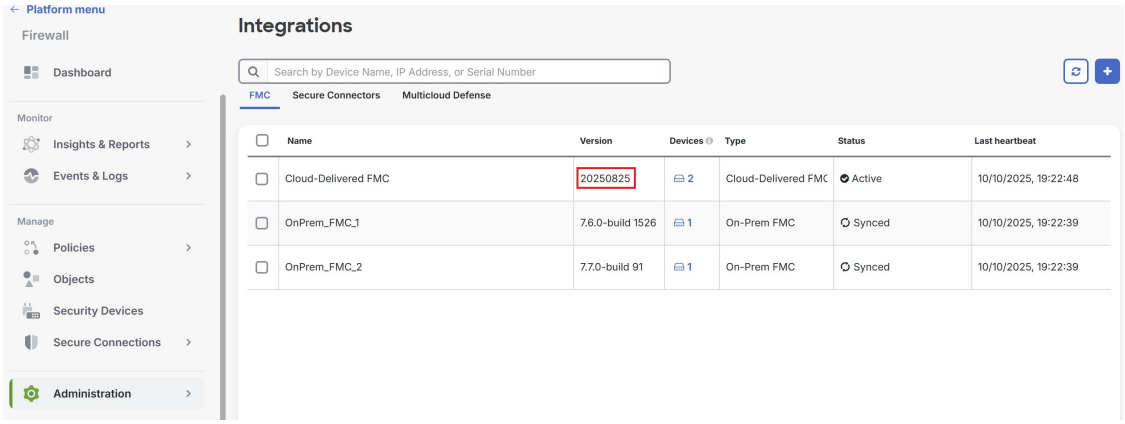
手順の詳細

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。

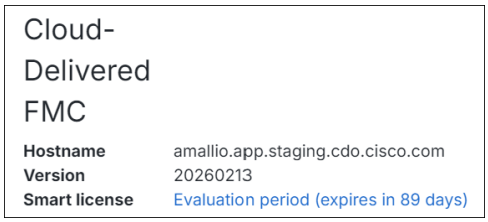
重要 RAVPN や SSL VPN などのエクスポート暗号化を必要とする機能を含むすべての機能にアクセスするには、展開後すぐに Cisco Smart Software Manager に クラウド提供型 Firewall Management Center を登録することを強く推奨します。早期登録により、機能の制限や展開の中断が防止されます。

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。

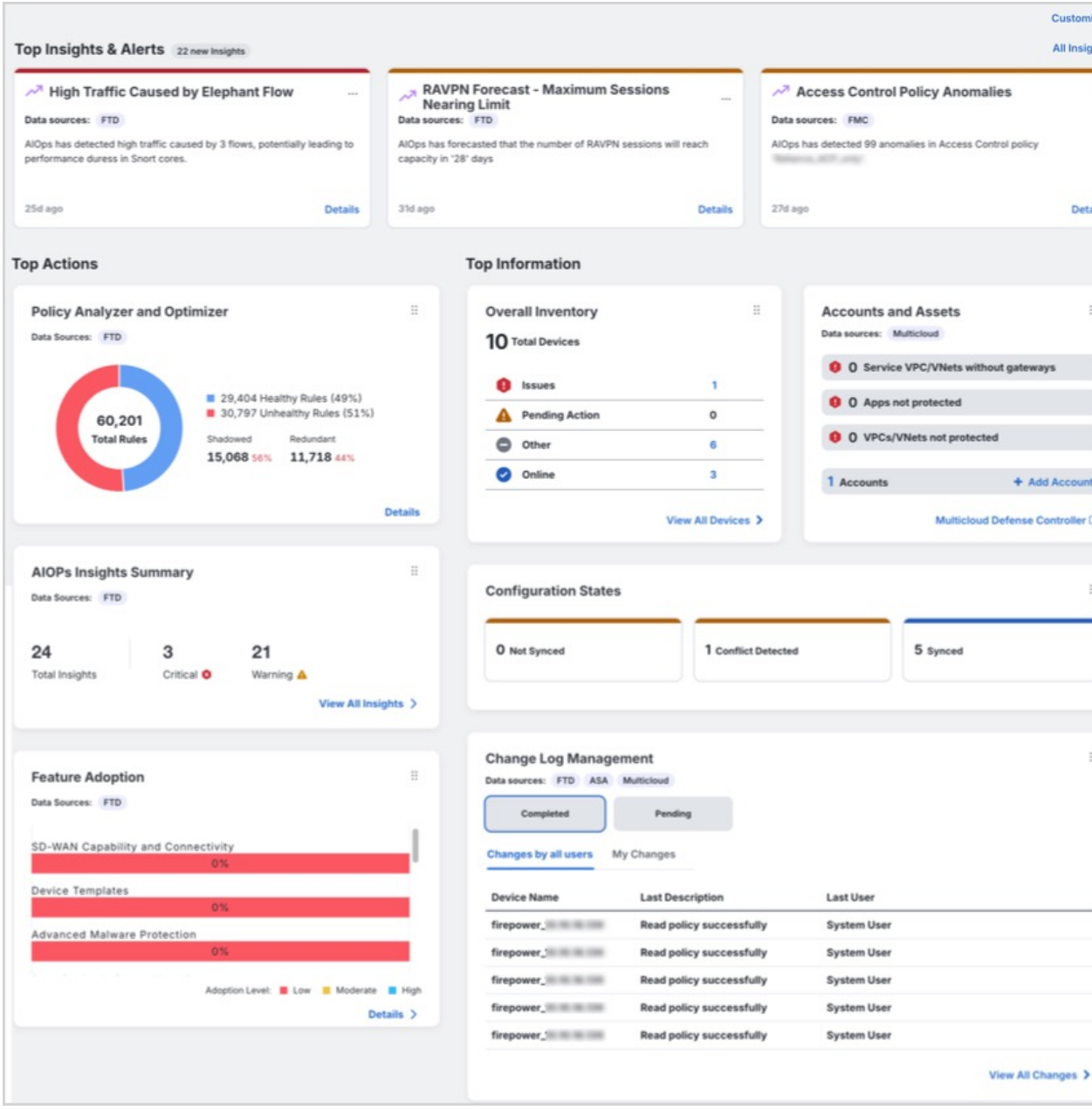
  詳細については、「サイト間 VPN」を参照してください。

- **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。

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。