改訂：2025 年 11 月 20 日

Cisco Catalyst Center リリース 3.1.3 用 Stealthwatch セキュリティ分析サービス ユーザーガイド

Catalyst Center の Stealthwatch セキュリティ分析サービス

Catalyst Center 用 Stealthwatch セキュリティ分析 サービス

Catalyst Center 用 Stealthwatch セキュリティ分析サービスは、Cisco Stealthwatch と連携して、すべてのネットワークトラフィックのリアルタイムモニタリングを提供します。

（注）

Cisco Stealthwatch は、Cisco Secure Network Analytics とも呼ばれます。

Stealthwatch セキュリティ分析サービスを使用して暗号化トラフィック分析 を有効にすると、暗号化された脅威に対するネットワークの保護をトラフィックを復号せずに強化できます。

Catalyst Center 用 Stealthwatch セキュリティ分析サービスは、（ベストプラクティスを使用して）ネットワーク要素のプロビジョニングを自動化します。この自動化により、ネットワーク要素は Cisco Stealthwatch にデータを送信できます。その結果、可視性が向上し、マルウェア検出機能が向上します。

Stealthwatch セキュリティ分析 を使用すると、次を実行できます。

- 導入に向けたネットワークの準備状況の評価
- Stealthwatch セキュリティ分析 の有効化
- 展開のステータスのモニタリング
- サイトあたり最大 1,000 台のデバイスのモニタリング

Stealthwatch セキュリティ分析 がサポートされているバージョン

次の表に、Stealthwatch セキュリティ分析 に関する最小ソフトウェアバージョンと必要なライセンスを示します。

製品ファミリ	最小バージョン	必要な製品コンポーネント	必要なライセンスとキャパシティ
Stealthwatch Enterprise	7.0	• Stealthwatch Management Console • Flow Collector	『*Stealthwatch Management Console VE and Flow Collector VE Installation and Configuration Guide*』を参照してください。

Stealthwatch セキュリティ分析 がサポートされているデバイス

暗号化トラフィック分析 の有効化がサポートされているデバイス

次の表に、暗号化トラフィック分析 の有効化がサポートされているデバイス、最小バージョン、およびライセンスの要件を示します。

（注）

一部のデバイスは暗号化トラフィック分析 と Flexible NetFlowの両方をサポートしています。これらのデバイスでは、[ETA Telemetry] トグルボタンを使用して 暗号化トラフィック分析 を無効にすることができます。暗号化トラフィック分析 を無効にすると、Flexible NetFlow のみが有効になります。

製品ファミリ	最小バージョン	必要なライセンス
Cisco Catalyst 9300 シリーズ スイッチ	Cisco IOS XE リリース 16.9.1	DNA Advantage
Cisco Catalyst 9400 シリーズ スイッチ	Cisco IOS XE リリース 16.9.1	DNA Advantage
Cisco 4000 シリーズ サービス統合型ルータ	Cisco IOS XE リリース 16.6.4	デバイスには、次のいずれかのライセンスが必要です。 • DNA Advantage • SEC/K9
Cisco 1000 シリーズ アグリゲーション サービス ルータ	Cisco IOS XE リリース 16.6.4	デバイスには、次のいずれかのライセンスが必要です。 • DNA Advantage • SEC/K9

Flexible NetFlow の有効化がサポートされているデバイス

次の表に、Flexible NetFlow の有効化がサポートされるデバイス、最小バージョン、およびライセンスの要件を示します。

製品ファミリ	最小バージョン	必要なライセンス
Cisco Catalyst 9200 シリーズ スイッチ	Cisco IOS XE リリース 16.9.1	DNA Advantage
Cisco Catalyst 3850 シリーズ スイッチ	Cisco IOS XE リリース 16.9.1	DNA Advantage
Cisco Catalyst 3650 シリーズ スイッチ	Cisco IOS XE リリース 16.9.1	DNA Advantage

Stealthwatch セキュリティ分析の設定

Stealthwatch セキュリティ分析 のインストール

ステップ 1 メインメニューから次を選択します。**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Available Applications for the release] エリアの [Stealthwatch Security Analytics] の横にあるチェックボックスをオンにします。

ステップ 3 [Install] をクリックします。

インストールが完了したら、[View Installed Applications] をクリックして、Stealthwatch セキュリティ分析サービスが表示されていることを確認します。

Stealthwatch セキュリティ分析 のアクセス制御

Catalyst Center での Stealthwatch セキュリティ分析 のアクセス制御は、次の設定を使用して管理できます。

設定	説明
ロール	ユーザーが Catalyst Center 機能にアクセスするために使用できる権限を定義します。 カスタムロールを作成し、**Stealthwatch**に必要な権限を選択できます。**Stealthwatch** の権限を選択すると、Catalyst Center は、ネットワーク設計、ネットワーク管理、ネットワークプロビジョニング、システムなどの依存機能に必要な権限を自動的に割り当てます。これらの権限は、必要に応じて変更できます。
アクセスグループ	サイト階層に基づいて、ロールのアクセス権を特定の範囲に制限します。 カスタムロールの場合、 **Stealthwatch** 権限を **[Read]** または **[Write]**に設定する場合は、対応するアクセスグループの **[Global]** 範囲を選択します。
ユーザー	ユーザー名、パスワード、および関連情報を定義します。アクセスグループに基づいて機能へのアクセスを制限します。

ロール、アクセスグループ、およびユーザーを作成するには、『*Cisco Catalyst Center* 管理者ガイド』の「ユーザーの管理」を参照してください。

Stealthwatch セキュリティ分析 に対する権限の要件

次の表に、ユーザーがデバイスで Stealthwatch セキュリティ分析をプロビジョニングするために最低限必要な権限を示します。

アクセス	説明	権限
[Security] > **[Stealthwatch]**	暗号化されたトラフィックに含まれる脅威も検出して軽減できるようにするために、ネットワーク要素から Cisco Stealthwatch にデータを送信するように設定します。	書き込み
[Network Design] > **[Profiles and Settings]**	AAA、NTP、DHCPなどのサイト全体のネットワーク設定を管理します。テレメトリとプロファイルを管理します。	書き込み
[Network Management] > **[Hierarchy]**	地理的な場所に基づいてエリア、ビルディング、フロアのネットワーク階層を作成します。このロールには、CMXサーバーの設定も含まれます。	読み取り
[Network Management] > **[Inventory]**	ネットワーク上のデバイスを追加、更新、または削除します。デバイス属性を管理し、ネットワークトポロジと設定を表示および管理します。	読み取り
[Network Provision] > **[Device Provision]**	サイト固有の設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。	書き込み
[System] > [System Administration]	HA、ディザスタリカバリ、バックアップおよび復元など、コアシステムの管理機能を管理します。	読み取り
[System] > **[System Settings]**	コアシステムの接続設定を管理します。このロールには、整合性検証、統合設定、デバッグログ、テレメトリ収集、システムの EULA、IPAM、データプラットフォーム、シスコのクレデンシャル、スマートアカウント、スマートライセンス、SSM接続モード、デバイスの EULAが含まれます。	読み取り

Stealthwatch の登録

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。

ステップ 2 左側のペインで、[Search Settings] バーに Stealthwatch と入力します。

ステップ 3 左側のペインで [Stealthwatch] をクリックします。

ステップ 4 Stealthwatch Management Console の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 5 Stealthwatch Management Console へのアクセスに使用するユーザーアカウントのユーザー名とパスワードを入力します。

（注） Stealthwatch Management Console に新しいユーザーを追加したら、そのユーザーが Cisco Stealthwatch と統合する前に Stealthwatch Management Console に少なくとも 1 回ログインしていることを確認します。最初のログイン時に、ユーザーは新しいパスワードを設定し、APIアクセスをアクティブにするように求められます。

Stealthwatch ユーザーアカウントに最低限必要な権限は次のとおりです。

- データロール：読み取り専用
- 機能ロール：設定マネージャとネットワークエンジニア

（注） Catalyst Center でカスタムユーザーロールを作成して、別のユーザーがデバイスで Stealthwatch セキュリティ分析をプロビジョニングできるように設定することができます。詳細については、Stealthwatch セキュリティ分析 のアクセス制御 （3 ページ）を参照してください。

ステップ 6 [Save] をクリックします。

Stealthwatch が正常に登録されると、[IP Address] フィールドのすぐ上にステータスが [Active | Registered and Running] と表示されます。

UDP Director のセットアップ

User Datagram Protocol（UDP）Director は、NetFlow やその他のトラフィックを受信して複数の宛先に複製します。

UDP Director をインストールし、StealthWatch 管理コンソールで設定する必要があります。詳細については、『*UDP Director Virtual Edition インストールおよびコンフィギュレーション ガイド（Stealthwatch System v6.9.0 用）*』を参照してください。

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。

ステップ 2 （任意） 左側の階層ツリーから、以下を選択しますを使用して、Stealthwatch Flow Destination を設定するサイトまでドリルダウンします。

ステップ 3 [Servers] タブで、[Stealthwatch Flow Destination] エリアを展開します。

ステップ 4 フローの接続先を追加するには、次のいずれかのオプションを選択します。

選択した内容	結果
Stealthwatchで設定されたフローの宛先から選択	[Select flow destination] ドロップダウンリストからフローの宛先を選択します。 「No Stealthwatch flow destination server configured」というエラーが表示される場合は、Stealthwatch の登録 （4 ページ）を参照してください。
外部フロー宛先サーバーを追加	対応するフィールドに、フロー宛先の IP アドレスとポートを入力します。

ステップ 5 [Save] をクリックします。

Stealthwatch セキュリティ分析 を有効にする

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Stealthwatch Security]**の順に選択します。

ステップ 2 左側のペインで、ドロップダウンリストを使用して目的のオプションを選択します。

Stealthwatch セキュリティ分析 を有効にする対象	選択するもの
サイト	[All Sites]
ファブリック	[All Fabrics]

デフォルトでは、[All Sites] が選択されています。

ステップ 3 Stealthwatch セキュリティ分析 を有効にするサイトまたはファブリックに対して、左側の階層ツリーから、以下を選択しますします。

または、検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 4 サイトカードをクリックして、Stealthwatch セキュリティ分析を有効にするサイトまたはファブリックを選択します。

必要に応じて、サイトおよびファブリックの階層を特定のフロアまで移動できます。

サイトカードには、[Enabled]、[Ready]、および [Not Ready] のデバイスの数が表示されます。

（注） Stealthwatch セキュリティ分析を有効にするには、少なくとも 1 つのデバイスを待受中の状態にする必要があります。

ステップ 5 事前チェックを確認し、[Get Started] をクリックします。

ステップ 6 選択したサイトまたはファブリックに対して設定されているフローの宛先を確認します。

次の場合は...	次の操作...
フローの接続先を変更する場合	1. **[設定の変更（Change Settings）]**をクリックします。 2. 新しいフローの宛先を設定し、ワークフローを再開します。
Select a flow destination for the site to proceed エラーが表示された場合	1. **[設定の更新 (Update Settings)]** をクリックします。 2. フローの宛先を設定し、ワークフローを再開します。

ステップ 7 [Next] をクリックします。

ステップ 8 デバイステーブルで [Ready] タブが選択されていることを確認します。

ステップ 9 Stealthwatch セキュリティ分析を有効にするデバイスのリストを確認します。

Stealthwatch セキュリティ分析 の有効化を除外する対象	結果
すべてのデバイス	[Exclude all devices] トグルボタンをクリックします。
特定のデバイス	[Exclude Device] 列の下にある、対応するトグルボタンをクリックします。

ステップ 10 [ETA Telemetry] 列のトグルボタンを使用して、暗号化トラフィック分析 テレメトリデータの収集を有効または無効にします。

デフォルトでは、このオプションは 暗号化トラフィック分析 対応デバイスに対して有効になっています。暗号化トラフィック分析 と互換性のあるデバイスのリストについては、Stealthwatch セキュリティ分析 を有効にする （5 ページ）を参照してください。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （10 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （10 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

（注）

プロビジョニングアクションをすぐに実行する場合も後で実行する場合も、実行前に一連の事前チェックが追加で実行されます。次の場合はタスクが失敗します。

- その時点でデバイスの CPU が 70% を超えている
- アクセススイッチで NBAR が有効になっている
- Stealthwatch セキュリティ分析 に適用可能なインターフェイスがスイッチにない
- ルータのルート情報がない

Stealthwatch セキュリティ分析 事前チェック

Stealthwatch セキュリティ分析 サービスは、サイトとファブリックのデバイスが展開基準を満たしていることを確認するために自動事前チェックを実施します。

このサービスでは、次のチェックが行われます。

- [Required Software]：デバイスで実行されているソフトウェアが最小要件を満たしている必要があります。
- [Required Device Role]：デバイスロールでサービスの展開がサポートされている必要があります。
  - Cisco ASR および ISR シリーズのルータを使用している場合は、[Device Role] を [Border Router] に設定します。
  - Cisco Catalyst 9300または9400シリーズ スイッチの場合は、[Device Role] を [Access] に設定します。
- [Required Hardware]：デバイスハードウェアでサービスの展開がサポートされている必要があります。
- [Required Licenses]：サイトのデバイスのアクティブなライセンスが最小要件を満たしている必要があります。
- [No conflicts with existing configurations]：他のサービスとの互換性の問題がないことを確認します。

  このチェックは次の場合に失敗します

- デバイスが vManage で管理されている
- デバイスで NBAR が有効になっている
- デバイスの 1 つ以上のインターフェイスで既存の NetFlow モニターが有効になっている

（注）

NBAR 競合は、Enable Flexible NetFlow が有効になっているデバイスと、Cisco IOS XE リリース 17.3.1 より前のバージョンを実行している Cisco Catalyst 9300 および Cisco Catalyst 9400 スイッチに適用されます。

これらの基準をすべて満たしているデバイスのステータスとして [Ready] と表示されます。

（注）

要件（ハードウェア、ソフトウェア、およびライセンス）の詳細については、Stealthwatch セキュリティ分析 がサポートされているデバイス （2 ページ） を参照してください。

準備ができていないデバイスの確認

ソフトウェア、互換性、またはライセンスのチェックに失敗したデバイスには、 **[Not Ready]** のラベルが付けられます。Stealthwatch セキュリティ分析 の有効化の準備ができていないデバイスを表示するには、この手順を完了します。

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Stealthwatch Security]**の順に選択します。

ステップ 2 左側のペインで、左側の階層ツリーから、以下を選択しますを有効にする準備ができていないデバイスを表示するサイトまたはファブリックまでドリルダウンします。

検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 3 準備ができていないデバイスを表示するサイトまたはファブリックのサイトカードをクリックします。

ステップ 4 [Get Started] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 デバイステーブルで、[Not Ready] をクリックします。

Stealthwatch セキュリティ分析 の有効化の準備ができていないデバイスのリストが表示され、それぞれのデバイスに対する各チェックのステータスが示されます。

ステップ 7 赤色のアイコンにカーソルを合わせて、失敗したチェックに関する詳細情報を確認します。

Stealthwatch Cloud への Flexible NetFlow エクスポートの有効化

Stealthwatch Cloud への Flexible NetFlow エクスポートを有効にするように Stealthwatch セキュリティ分析 を設定できます。

Stealthwatch Cloud は、Cisco IOS XE リリース 17.3.1 以降を実行している Cisco Catalyst 9200 および 9300 デバイスをサポートします。

- Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認します。

- Stealthwatch セキュリティ分析のユーザーロールに設定マネージャとネットワークエンジニアの権限があることを確認します。
- インベントリにまだデバイスが存在しない場合は、検出機能を使用してデバイスをインベントリに追加し、サイトに割り当てます。

ステップ 1 Stealthwatch Cloud ポータルで、次の手順を実行します。

a) **[Settings]** > **[Sensors]** > **[Service key]** の順に選択します。

b) [Service key] フィールドで、サービスキーをコピーし、後で使用するために保存します。

Stealthwatch Cloud では、次の地域に Flexible NetFlow データを送信できます。

- アメリカ合衆国（US）
- 欧州連合（EU）
- アジア太平洋、日本、中国（APJC）

サービスキーは地域によって異なります。サイトに応じて、最大 3 つの異なるサービスキーを使用できます。

ステップ 2 Catalyst Center で Stealthwatch フローの宛先を Stealthwatch Cloud に設定します。

a) メインメニューから次を選択します。**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

b) 左側の階層ツリーから、以下を選択しますを使用して、Stealthwatch Flow Destination を設定するサイトまでドリルダウンします。

c) 下にスクロールして、[Stealthwatch Flow Destination] 領域を展開します。

d) [Stealthwatch Cloud] オプションボタンをクリックします。

e) [Service key] フィールドに、前にコピーしたサービスキーを貼り付けます。

f) [Save] をクリックします。

ステップ 3 Stealthwatch セキュリティ分析 を有効化し、フローの宛先が **Stealthwatch Cloud** に設定されていることを確認します。

詳細については、「Stealthwatch セキュリティ分析 を有効にする （5 ページ）」を参照してください。

ステップ 4 [Enabled] タブには、SWC ステータスが [Enabled] になっている新しいデバイスが表示されます。

ステップ 5 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （10 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （10 ページ）を参照してください。

ステップ 6 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 7 Stealthwatch Cloud ポータルに戻り、**[Settings]** > **[Sensors]** の順に選択します。

新しいセンサーを探します。

センサー名はデバイスのホスト名です。

ヒント

データが Stealthwatch Cloud ポータルにアップロードされると、センサーのステータスインジケータは緑色になります。データが送信されていない場合、センサーのステータスインジケータは赤色になります。

Stealthwatch Cloud ポータルで、センサーが緑色に変わると、トラフィックの詳細がダッシュボードに表示されます。

デバイス構成を今すぐまたは後で展開する

設定の可視性と制御をサポートするワークフローのスケジュールの手順で、次の手順を完了してデバイス設定を今すぐ、または後で展開します。

設定で [Visibility and Control of Configurations] が無効になっていることを確認してください。

ステップ 1 [Now] または [Later] をクリックします。必要に応じてタスクの名前を更新します。

（注） 可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Preview and Deploy (Recommended)] がデフォルトで選択されます。[Now] および [Later] オプションはグレー表示されます。

ステップ 2 [Performing Initial Checks] ウィンドウで、展開するためのタスクを準備して送信します。

a) すべての問題に対処し、デバイス設定を展開します。

[Recheck] をクリックし、すべての検証が成功したことを確認します。

b) [Submit] をクリックします。

デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認します。

デバイス設定のプレビューと展開

設定の可視性と制御をサポートするワークフローのスケジュールの手順まで来たら、この手順を実行してデバイス設定のプレビューと展開を行います。

設定で [Visibility and Control of Configurations] が有効になっていることを確認してください。

ステップ 1 [Preview and Deploy (Recommended)] をクリックし、必要に応じてタスク名を更新します。

（注） デフォルトでは、可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Preview and Deploy (Recommended)] が選択されます。[Now] および [Later] オプションはグレー表示されます。

ステップ 2 [Performing Initial Checks] ウィンドウで、すべての問題に対処して、現在の展開を続行します。

ウィンドウの右下隅にある [Recheck] をクリックし、すべての検証が成功したことを確認します。

ステップ 3 [Preparing Devices and Configuration Models] ウィンドウで、システムがデバイスを準備してデバイス設定を生成するのを待ちます。


ヒント

準備には時間がかかる場合があります。[Exit and Preview Later] をクリックすると、[Tasks] ウィンドウで作業項目を確認できます。

ステップ 4 [Preview Configuration] ウィンドウでデバイス設定を確認します。ウィンドウに展開オプションが表示されます。

クリックする対象	目的
[Deploy] または [Submit for Approval]	デバイス構成を展開します。
[Exit and Preview Later]	後でデバイス構成を確認して展開します。 後で、[Tasks] ウィンドウに移動して作業項目を開き、[Deploy] または [Submit for Approval] をクリックします。


（注）

ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

ステップ 5 展開のスケジュールを設定します。

a) 設定を展開するタイミングと場所（該当する場合）を指定します。

確認のために設定を送信する場合は、IT 管理者へのメモを追加します。

b) [Submit] をクリックします。

作業項目の承認ステータスまたはタスクの展開ステータスは、[Tasks] ウィンドウで確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信します。承認された作業項目は、スケジュールされた時刻に展開されます。


（注）

タスクを送信したら、タスク名をクリックして **[Activities]** > **[Tasks]** ウィンドウの [Task Progress] バーでプロビジョニングタスクの進行状況を確認します。

Stealthwatch セキュリティ分析の管理

サイトとファブリックのステータスの確認

Stealthwatch セキュリティ分析を使用すると、各サイトまたはファブリックのデバイスのステータスを表示できます。

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Stealthwatch Security]**の順に選択します。

ステップ 2 左側のペインで、ステータスを表示するサイトまたはファブリックを選択します。

各サイトまたはファブリックカードは次の色を表示します。

- 青：Stealthwatch セキュリティ分析 が有効になっているデバイスの場合。
- 緑：事前チェックに合格し、Stealthwatch セキュリティ分析 を有効にできるデバイスが対象。
- 赤：事前チェックに失敗し、Stealthwatch セキュリティ分析 を有効にできないデバイス用。
- 紫：ETA テレメトリが有効になっているデバイスの場合。

ステップ 3 デバイスステータスを表示するには、サイトまたはファブリックカードをクリックします。

[Ready]、[Not Ready]、または [Enabled] のデバイスを表示し、対応するタブをクリックします。

サイトまたはファブリック内のデバイスには、次のステータスがあります。

- [Enabled Devices]：これらのデバイスでは Stealthwatch セキュリティ分析が有効になっています。
- [Not ready Devices]：事前チェックに 1 つ以上失敗したデバイス。

  緑色のチェックマークは、デバイスが合格した事前チェックを示します。赤色のアイコンは、デバイスが失敗した事前チェックを示します。赤色のアイコンにカーソルを合わせて、失敗した事前チェックに関する詳細情報を確認します。
- Ready Devices：すべての事前チェックに合格し、Stealthwatch セキュリティ分析 に対して有効にできるデバイス。

スケジュールされたタスクの表示

ステップ 1 メインメニューから次を選択します。**[Activities]** > **[Tasks]**の順に選択します。

デフォルトでは、[Tasks] ウィンドウには次が表示されます。

- 今後のタスク、進行中のタスク、失敗したタスク、および成功したタスク
- 既存の作業項目、レビュー待ちの作業項目、および失敗した作業項目。

ステップ 2 左側のペインの [Type] で、[Task] をクリックしてタスクのみを表示します。

ステップ 3 左側のペインの [Status] で [Upcoming] チェックボックスをオンにして、スケジュール済みのタスクのみを表示します。

ステップ 4 左側のペインで、次の手順を実行してスケジュール済みの Stealthwatch セキュリティ分析 タスクのみを表示します。

1. [Categories] を展開します。
2. [Show all] をクリックします。
3. [Search] フィールドに **SSA** と入力します。
4. [SSA] チェックボックスをオンにします。

ステップ 5 タスクをクリックすると、詳細情報を表示できます。

タスクの管理の詳細については、『*Cisco Catalyst Center Administrator Guide*』の「View, Edit, and Delete Tasks」を参照してください。

の更新 Stealthwatch セキュリティ分析

Stealthwatch セキュリティ分析 では、以前に有効にしたデバイスの設定を更新できます。時間の経過とともにネットワークの変更が発生する可能性があります。

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Stealthwatch Security]**の順に選択します。

ステップ 2 左側のペインで、ドロップダウンリストを使用して該当するオプションを選択します。

Stealthwatch セキュリティ分析 を有効にする対象	**選択するもの**
サイト	[All Sites]
ファブリック	[All Fabrics]

デフォルトでは、[All Sites] が選択されています。

ステップ 3 Stealthwatch セキュリティ分析 を更新するサイトまたはファブリックに対して、左側の階層ツリーから、以下を選択しますします。

または、検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 4 サイトカードをクリックして、Stealthwatch セキュリティ分析 を更新するサイトまたはファブリックを選択します。

サイトカードには、**Enabled**、**Ready**、および **Not Ready** のデバイスの数が表示されます。

（注） Stealthwatch セキュリティ分析 を更新するには、少なくとも 1 つのデバイスを有効にする必要があります。

ステップ 5 [Get Started] をクリックします。

ステップ 6 選択したサイトまたはファブリックに対して設定されているフローの宛先を確認します。

Stealthwatch セキュリティ分析 の更新を除外する対象	**結果**
すべてのデバイス	[Exclude all devices] トグルボタンをクリックします。
特定のデバイス	[Exclude Device] 列の下にある、対応するトグルボタンをクリックします。

ステップ 7 [Next] をクリックします。

ステップ 8 デバイステーブルで [Enabled] タブが選択されていることを確認します。

ステップ 9 [Update] オプションボタンをクリックします。

（注） デバイスの更新では、関連するネットワークデバイスで必要な変更のみを設定します。たとえば、これまで 10 個のアクセスインターフェイスが有効になっていたものの、現在関連性のあるインターフェイスは 1 つのみである場合、デバイスを更新すると、その新しいインターフェイスにのみ設定変更がプッシュされます。

デバイスの更新には次の内容が含まれます。

- 新しいラインカードの追加
- アクセスポイントが接続されているインターフェイスに対する変更
- VLAN に対する変更

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （10 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（10 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Stealthwatch セキュリティ分析 の無効化

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Stealthwatch Security]**の順に選択します。

ステップ 2 左側のペインで、ドロップダウンリストから必要なオプションを選択します。

Stealthwatch セキュリティ分析 を無効化する対象	**選択するもの**
サイト	[All Sites]
ファブリック	[All Fabrics]

デフォルトでは、[All Sites] が選択されています。

ステップ 3 Stealthwatch セキュリティ分析 を有効にするサイトまたはファブリックに対して、左側の階層ツリーから、以下を選択しますします。

または、検索バーを使用してサイトまたはファブリックを検索することもできます。

ステップ 4 サイトまたはファブリックの Stealthwatch セキュリティ分析 を無効化するには、サイトカードをクリックします。

サイトカードには、**Enabled**、**Ready**、および **Not Ready** のデバイスの数が表示されます。

（注） Stealthwatch セキュリティ分析 を無効にするには、少なくとも 1 つのデバイスを有効にする必要があります。

ステップ 5 事前チェックを確認します。[Get Started] をクリックします。

ステップ 6 選択したサイトまたはファブリックに対して設定されているフローの宛先を確認します。

次の場合は...	次の操作...
フローの接続先を変更する場合	1. **[設定の変更（Change Settings）]**をクリックします。 2. 新しいフローの宛先を設定し、ワークフローを再開します。
Select a flow destination for the site to proceed エラーが表示された場合	1. **[設定の更新 (Update Settings)]** をクリックします。 2. フローの宛先を設定し、ワークフローを再開します。

ステップ 7 [Next] をクリックします。

ステップ 8 デバイステーブルで **[Enabled]** タブが選択されていることを確認します。

ステップ 9 Stealthwatch セキュリティ分析 を無効にするデバイスのリストを確認します。

Stealthwatch セキュリティ分析 の有効化を除外する対象	結果
すべてのデバイス	[Exclude all devices] トグルボタンをクリックします。
特定のデバイス	[Exclude Device] 列の下にある、対応するトグルボタンをクリックします。

ステップ 10 [Disable] オプションボタンをクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （10 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（10 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Stealthwatch セキュリティ分析のトラブルシューティング

Stealthwatch セキュリティ分析サービスでは、GUI 内にエラーメッセージを表示して、アプリケーションの使用に可能な限り問題がないことを確認します。エラーメッセージとは別に、この章の情報を使用して、発生している可能性のある問題をトラブルシューティングできます。

監査ログの表示

監査ログは、Catalyst Centerで実行されているさまざまなアプリケーションに関する情報を取得します。

ステップ 1 メインメニューから次を選択します。**[Activities]** > **[Audit Logs]** の順に選択します。

[Audit Logs] ウィンドウが開くと、システム アクティビティのログを表示できます。

この情報は、次の各監査ログに表示されます。

- **Description**：監査ログの説明
- **Site**：特定の監査ログのサイトの名前
- **Device**：監査ログのデバイス
- **Requestor**：ログに記録されているアクションを要求するユーザー
- **Source**：監査ログの送信元
- **Created On**：監査ログが作成された日付

ステップ 2 監査ログのドロップダウンを展開して、子の監査ログを表示します。

（注） 監査ログは、Catalyst Center によって実行されたタスクに関するデータをキャプチャします。子監査ログは、Catalyst Center によって実行されたタスクのサブタスクです。

ステップ 3 監査ログのフィルタ処理

a) [Filter] アイコンをクリックします。
b) 監査ログをフィルタ処理するための特定のパラメータを入力します。
c) [Apply] をクリックします。

ステップ 4 （任意） ウィンドウの右上にあるデュアル矢印アイコンをクリックして、データを更新します。

ステップ 5 （任意） [Log ID]をクリックしてログの ID を表示し、クリップボードにコピーします。

タスクマネージャを使用したトラブルシューティング

ステップ 1 メインメニューから次を選択します。**[Activities]** > **[Tasks]**の順に選択します。

ステップ 2 リストで問題のあるタスクを特定します。[Failed] をクリックして詳細を表示します。

（注） 1 つのタスクに複数のデバイスを含めることができます。タスクに含まれる他のデバイスが成功しても、1 つのデバイスで障害が発生した場合、タスクの全体的なステータスは [Failed] と表示されます。

サポート対象デバイスのトラブルシューティング

これらの問題は、サポートされているデバイスでトラブルシュートできる一般的な問題です。

デバイスがリストされていない

Catalyst Center に Stealthwatch セキュリティ分析を有効または無効にするデバイスがリストされていない場合は、デバイスロールを確認してください。

使用しているルータ	デバイスロールが次に設定されていることを確認してください...
Cisco ASR および ISR シリーズ ルータ	境界ルータ
Cisco Catalyst 9300 および 9400 シリーズ スイッチ	アクセス
ファブリックの一部ではないデバイス	ディストリビューション

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。