変更ログ、ワークフロー、およびジョブのモニタリングとレポート

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

Security Cloud Control での変更ログの管理

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

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

変更ログの容量の管理

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

Security Cloud Control のデータベースに保存される変更ログ情報と、エクスポートした変更ログに表示される情報には違いがあります。詳細については、変更ログのエクスポート（4ページ）を参照してください。

変更ログエントリ

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

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

保留中および完了した変更ログエントリ

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

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

- 実行コンフィギュレーション ファイルを更新する CLI コマンドの実行

変更ログエントリの検索とフィルタ処理

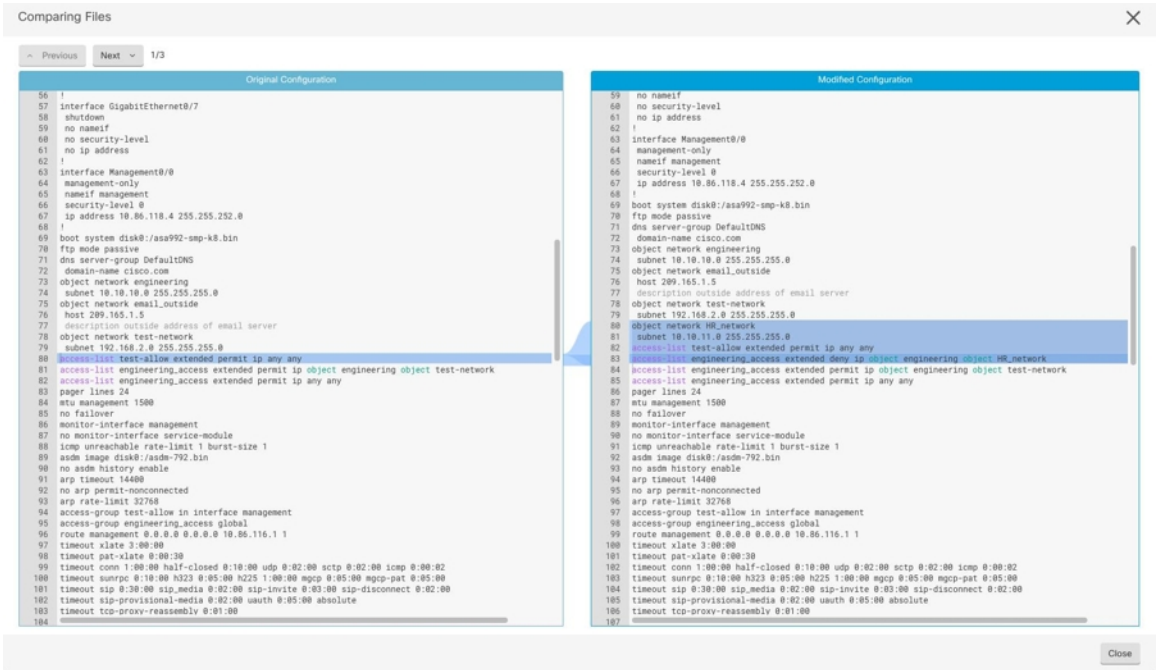
変更ログエントリを検索およびフィルタ処理できます。検索フィールドを使用してイベントを検索します。フィルタ（）を使用して、指定した条件を満たすエントリを検索します。また、変更ログをフィルタ処理し、検索フィールドにキーワードを追加して、2 つのタスクを組み合わせることで、フィルタ処理された結果内のエントリを検索できます。

変更ログの差異の表示

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

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

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



関連項目

- Security Cloud Control での変更ログの管理 （1 ページ）

変更ログのエクスポート

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

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

手順

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

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

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

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

ステップ 3 ページの右上隅にあるエクスポート アイコンをクリックします。

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

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

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

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

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

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

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

変更要求管理

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

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

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

変更要求管理の有効化

変更要求トラッキングの有効化は、テナントのすべてのユーザーに影響を及ぼします。

手順

ステップ 1 左側のペインで、**[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

ステップ 2 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを有効にします。

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

変更リクエストの作成

手順

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

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

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

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

ステップ 3 [保存（Save）] をクリックします。

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

変更リクエストと変更ログイベントの関連付け

手順

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

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

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

（注）
最新の変更リクエストが変更リクエストリストの一番上に表示されます。

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

変更リクエストがある変更ログイベントの検索

手順

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

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

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

変更リクエストの検索

手順

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

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

フィルタ変更リクエスト

手順

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

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

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

値を入力すると、入力した値と部分一致する結果が表示されます。

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

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

変更リクエストツールバーをクリアする

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

手順

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

ステップ 2 [クリア（Clear）] をクリックします。

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

変更ログイベントと関連付けられた変更リクエストのクリア

手順

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

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

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

ステップ 4 [クリア（Clear）] をクリックします。

変更リクエストの削除

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

手順

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

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

ステップ 3 チェックマークをクリックして確定します。

変更リクエスト管理の無効化

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

手順

ステップ 1 左側のペインで、**[管理（Administration）] > [一般設定（General Settings）]** をクリックします。

ステップ 2 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを無効化します。

変更リクエスト管理のユースケース

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

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

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

1. 変更リクエストの作成 （6 ページ）。
2. 外部システムのチケット名またはチケット番号を変更リクエストの名前に使用し、[説明（Description）] フィールドに変更の理由とその他の関連情報を追加します。
3. 新しい変更リクエストが変更リクエストツールバーに表示されることを確認します。
4. ファイアウォールデバイスを変更します。
5. ナビゲーションウィンドウで [変更ログ（Change Log）] をクリックし、新しい変更リクエストに関連付けられている変更ログイベントを見つけます。

6. 変更リクエストツールバーをクリアする （8 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

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

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

1. 変更リクエストの作成 （6 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 （6 ページ）。
4. 変更リクエストツールバーをクリアする （8 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

変更リクエストに関連付けられた変更ログイベントを検索する

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

1. ナビゲーションウィンドウで、[変更ログ（Change Log）] をクリックします。
2. 次のいずれかの方法を使用して、変更リクエストに関連付けられた変更ログイベントを検索します。
   - [変更ログ（Change Log）] 検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ログイベントを検索します。Security Cloud Control により、完全一致の変更ログイベントが強調表示されます。
   - フィルタ変更リクエスト （7 ページ） を実行して変更ログイベントを検索します。
3. 各変更ログを表示して、関連する変更リクエストを示す強調表示された変更ログイベントを見つけます。

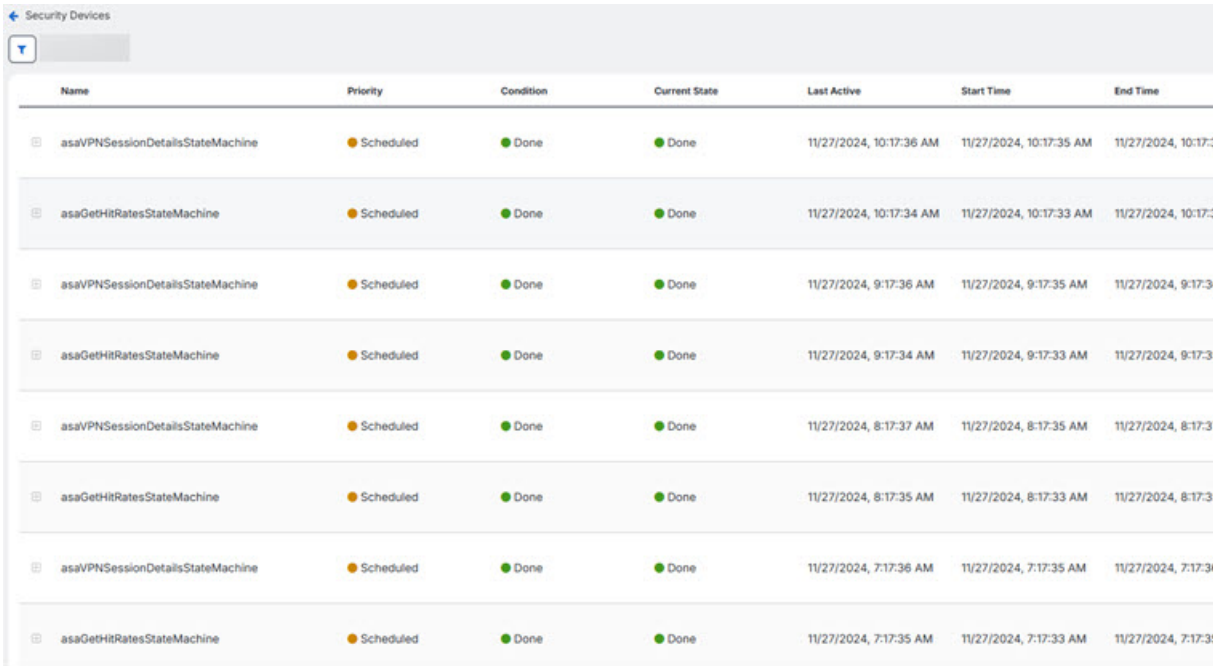
Security Cloud Control でのワークフローのモニタリング

[ワークフロー（Workflows）] ページでは、デバイス、Secure Device Connector（SDC）、または Secure Event Connector（SEC）と通信するとき、およびルールセットの変更をデバイスに適用するときに、Security Cloud Control が実行するすべてのプロセスを監視できます。Security Cloud Control は、各ステップのワークフローテーブルにエントリを作成し、その結果をこのページに表示します。エントリには、Security Cloud Control によって実行されるアクションについての情報のみが含まれており、CDO がデータをやり取りしているデバイスについての情報は含まれません。

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

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

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



デバイスワークフローのエクスポート

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

スタックトレースのコピー

解決できないエラーがあって TAC に問い合わせた場合、TAC からスタックトレースのコピーを求められる場合があります。エラーのスタックトレースを収集するには、[スタックトレース（Stack Trace）] リンクをクリックし、[スタックトレースのコピー（Copy Stacktrace）] をクリックして、画面に表示されるスタックをクリップボードにコピーします。

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。