モニタリングとレポート

CDO の監視およびレポート機能は、既存のポリシーの影響とその結果として生じるセキュリティ態勢に関する貴重なインサイトをもたらします。

この章は、次のセクションで構成されています。

- 変更ログ （1 ページ）
- 変更ログの差分の表示 （3 ページ）
- 変更ログを CSV ファイルにエクスポートする （4 ページ）
- 変更リクエスト管理 （5 ページ）
- [ジョブ（Jobs）] ページ （10 ページ）
- [ワークフロー（Workflows）] ページ （11 ページ）

変更ログ

変更ログについて

変更ログは、CDO で行われた設定変更を継続的にキャプチャします。この単一のビューには、サポートされているすべてのデバイスとサービスにわたる変更が含まれます。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。
- すべての変更ログエントリの平易な英語のラベル。
- デバイスの導入準備と削除の記録。
- CDO の外部で発生するポリシー変更の競合の検出。
- 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、いつに関する問に回答可能。
- 完全な変更ログまたは一部のみを CSV ファイルとしてダウンロード可能。

変更ログの容量

CDO は、変更ログの情報を 1 年間保持します。1 年以上前の情報は削除されます。

CDO がデータベースに保存する変更ログ情報と、変更ログをエクスポートしたときに表示される情報には違いがあります。詳細については、変更ログを CSV ファイルにエクスポートする （4 ページ）を参照してください。

[変更ログ] ページの変更ログエントリ

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 CDO 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、行の任意の場所をクリックして変更を展開できます。
- 競合として検出された CDO の外部で行わ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。
- CDO 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 CDO から削除されたときに、CDO は変更ログエントリを閉じます。設定は、デバイスから CDO に設定を「読み取った」後に、または CDO からデバイスに設定を展開することによって同期されます。
- CDO は、既存のエントリを閉じ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。
- CDO 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 CDO 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。
- CDO 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書き込まれます。

アクティブおよび完了した変更ログエントリ

変更ログには、**アクティブ**または**完了**のステータスがあります。CDO を使用してデバイスの設定を変更すると、変更は**アクティブ**な変更ログエントリに記録されます。デバイスから CDO への設定の読み取り、CDO からデバイスへの変更の展開、CDO からのデバイスの削除が完了するか、または実行構成ファイルを更新する CLI コマンドを実行すると、アクティブな変更ログが完了し、将来の変更のために新しいログが作成されます。

変更ログでのエントリの検索

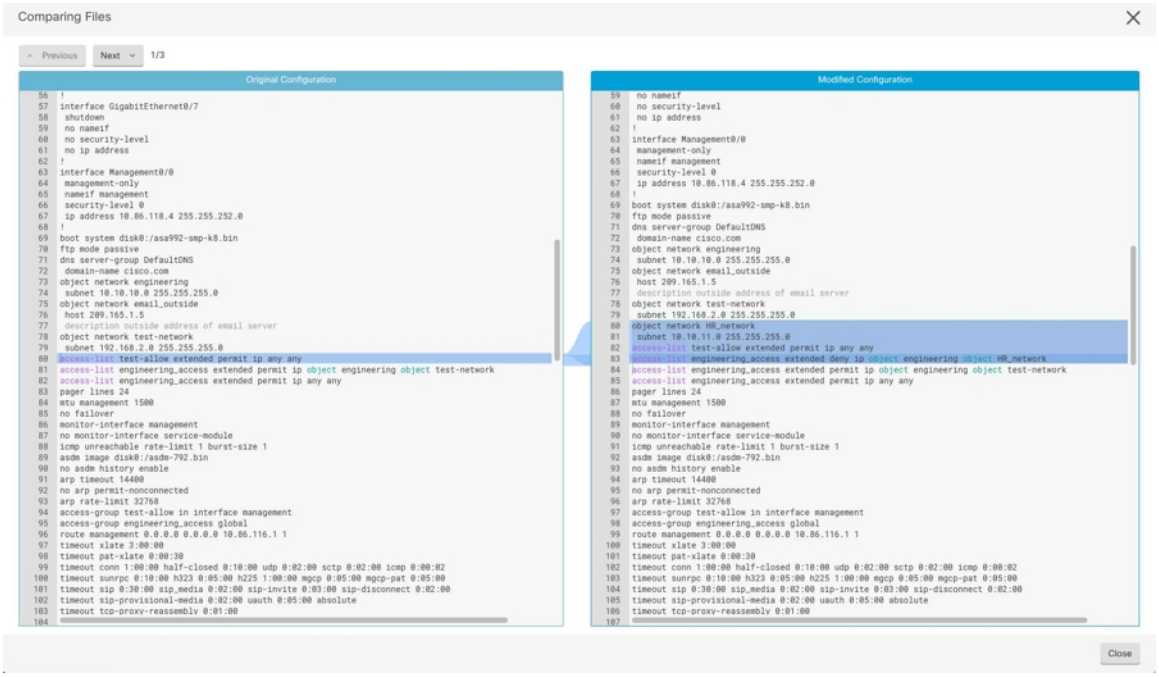
変更ログイベントは検索およびフィルタリングできます。検索バーを使用して、キーワードに一致するイベントを検索します。フィルタ を使用して、指定したすべての条件を満たすエントリを検索します。また、変更ログをフィルタリングし、[検索]フィールドにキーワードを

追加して、操作を組み合わせることで、フィルタリングされた結果内のエントリを検索できます。

変更ログの差分の表示

変更ログにある青色の [差分（Diff）] リンクをクリックすると、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るため、変更を対比できます。2 つのバージョンの違いがわかります。

次の図では、[元の設定（Original Configuration）] は変更が ASA に書き込まれる前の実行構成ファイルであり、[変更された設定（Modified Configuration）] 列は変更が書き込まれた後の実行構成ファイルを示しています。この場合、[元の設定（Original Configuration）] 列は、実際には変更されていない実行構成ファイルの行を強調表示しますが、[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] ボタンを使用して、ファイル内の変更を確認します。



関連項目

- 変更ログ （1 ページ）

変更ログを CSV ファイルにエクスポートする

CDO 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処理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 ナビゲーションウィンドウで、[変更ログ] をクリックします。

ステップ 2 次のいずれかのアクションを実行して、エクスポートする変更を見つけます。

- フィルタ フィールドと検索フィールドを使用して、エクスポート対象を正確に見つけます。たとえば、デバイスでフィルタ処理して、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） CDO は 1 年間の変更ログデータを保存することに注意してください。最大限の 1 年間分の変更ログ履歴をダウンロードするよりも、変更ログの内容をフィルタ処理し、その結果を .csv ファイルとしてダウンロードする方がよい場合があります。

ステップ 3 変更ログの右上にある青色のエクスポートボタン 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、ファイルをローカルファイルシステムに保存します。

CDO 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

CDO の変更ログページからエクスポートする情報は、CDO 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、CDO はデバイスの設定の 2 つのコピーを保存します。クローズされた変更ログの場合は「開始」設定と「終了」設定のいずれかとなり、オープンな変更ログの場合は「最新」設定となります。これにより、CDO は設定の違いを並べて表示できます。さらに、CDO 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、すべてのステップの「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変更ログ CDO ストアよりもはるかに小さくなります。

CDOは最大1年分の変更ログ情報を保存し、この情報には設定の2つのコピーが含まれます。

変更リクエスト管理

変更リクエスト管理により、サードパーティのチケットシステムで開かれた変更リクエストとそのビジネス上の正当性を、変更ログのイベントに関連付けることができます。変更リクエスト管理を使用して、CDO で変更リクエストを作成し、作成した変更リクエストを一意の名前で識別し、変更の説明を入力して、変更リクエストを変更ログイベントに関連付けます。後で変更リクエスト名を変更ログで検索できます。

（注） CDO の変更リクエストトラッキングへの参照も表示される場合があります。変更リクエストトラッキングと変更リクエスト管理は、同じ機能を参照します。

変更リクエスト管理の有効化

変更リクエスト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。変更リクエストトラッキングを有効にするには、次の手順に従います。

手順

ステップ1 ユーザーメニューから、[設定（Settings）] を選択します。

ステップ2 ユーザーメニューで、[一般設定（General Settings）] をクリックします。

ステップ3 [変更リクエストトラッキング（Change Request Tracking）] 下のスライダをクリックします。

確認が完了すると、Defense Orchestrator インターフェイスの左下隅と、[変更ログ] の [変更リクエスト] ドロップダウンメニューに、[変更リクエスト] ツールバーが表示されます。

変更リクエストの作成

手順

ステップ1 任意の CDO ページから、ページの左下隅にある変更リクエストツールバーの青色の [+] ボタンをクリックします。

ステップ2 変更リクエストに名前を付け、説明を入力します。変更リクエスト名に、組織が実装する変更リクエスト ID を反映させます。説明フィールドを使用して、変更の目的を記述します。

（注） 作成した変更リクエストの名前は変更できません。

ステップ 3 変更リクエストを保存します。

（注） CDO は変更リクエストを保存し、その変更リクエストを無効にするか、変更リクエストツールバーの変更リクエスト情報をクリアするまで、すべての新しい変更をその変更リクエスト名に関連付けます。

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 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。

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

ステップ 3 [変更リクエスト]列で、イベントのドロップダウンメニューをクリックします。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ることに注意してください。

ステップ 4 変更リクエストの名前をクリックし、[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 ナビゲーションウィンドウで、[変更ログ] 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。CDO 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 変更リクエストツールバーの変更リクエストメニューをクリックします。

ステップ 2 検索する変更リクエスト名またはキーワードの入力を開始します。名前フィールドと説明フィールド両方での部分一致の結果が、変更リクエストのリストに表示されるようになります。

フィルタ変更リクエスト

フィルタトレイには、変更ログイベントの検索に使用できる変更リクエストフィルタがあります。

手順

ステップ 1 [変更ログ] ページの左側にあるフィルタトレイで、[変更リクエスト（Change Requests）] 領域を探します。

ステップ 2 フィルタを展開し、[検索（search）] フィールドに変更リクエストの名前の入力を開始します。[検索（Search）] フィールドの下に、部分一致が表示され始めます。

ステップ 3 変更リクエスト名を選択し、対応するチェックボックスをオンにすると、[変更ログ]テーブルに一致したものが表示されます。CDO 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。

手順

ステップ 1 変更リクエストツールバーの変更リクエストメニューを選択します。

ステップ 2 [クリア（Clear）] をクリックします。変更リクエストメニューが [なし] に変わります。

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

手順

ステップ 1 ナビゲーションウィンドウで、[変更ログ] をクリックします。

ステップ 2 変更ログを拡大して、変更リクエスト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 [変更リクエスト] 列で、イベントのドロップダウンメニューをクリックします。

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

変更リクエストを削除するときは、変更ログからではなく、変更リクエストリストから削除します。

手順

ステップ 1 変更リクエストツールバーの変更リクエストメニューをクリックします。
ステップ 2 変更リクエスト名をクリックします。
ステップ 3 その行の [削除（delete）] アイコンをクリックします。
ステップ 4 緑色のチェックマークをクリックして、変更リクエストを削除することを確認します。

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。変更リクエスト管理を無効にするには、次の手順に従います。

手順

ステップ 1 ユーザー名のメニューから、[設定] を選択します。
ステップ 2 [変更リクエストのトラッキング（Change Request Tracking）] の下にあるボタンをスライドして、灰色の X を表示します。

使用例

これらのユースケースは、上記の手順に従って変更リクエスト管理を前もって有効にし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の変更を追跡する

このユースケースでは、ユーザーがファイアウォールの変更を行って、外部システムで維持されているチケットを解決します。ユーザーは、ファイアウォールの変更に起因する変更ログイベントを変更リクエストに関連付けたいと考えています。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 （5 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。説明フィールドを使用して、変更の理由やその他の関連情報を追加します。
2. 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ていることを確認します。

3. ファイアウォールを変更します。
4. ナビゲーションウィンドウで[変更ログ]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。
5. 完了したら、変更リクエストツールバーのクリア （7 ページ）を実行します。

ファイアウォール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、ユーザーがファイアウォール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ましたが、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ていました。ユーザーは、変更ログに戻って、チケット番号で変更ログイベントを更新したいと考えています。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 （5 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。説明フィールドを使用して、変更の理由や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]をクリックし、ファイアウォールの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. 完了したら、変更リクエストツールバーをクリアします。

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

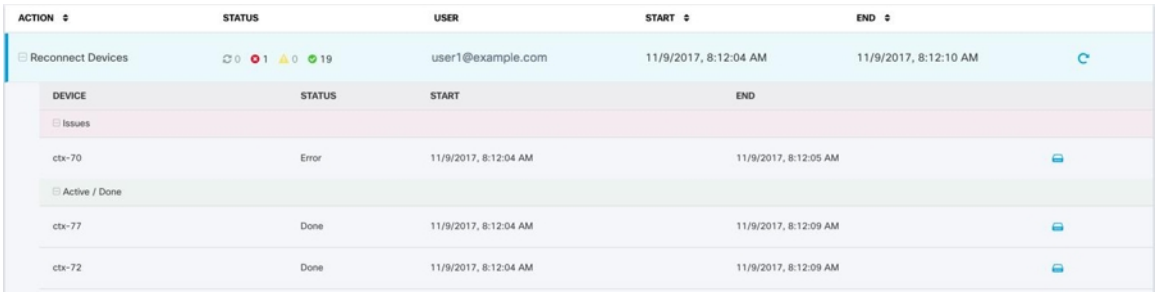
このユースケースでは、ユーザーは、外部システムで維持されているチケットを解決するために行われた作業の結果として、どの変更ログイベントが変更ログに記録されたかを知りたいと考えています。変更リクエストに関連付けられている変更ログイベントを検索するには、次の手順に従います。

1. ナビゲーションウィンドウで、[変更ログ] 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] 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。CDOは、完全に一致する変更ログイベントを強調表示します。
   - 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。

[ジョブ（Jobs）] ページ

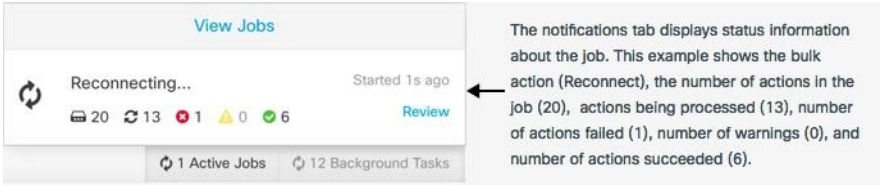
[ジョブ]ページには、一括操作のステータスに関する情報が表示されます。一括操作には、複数のデバイスの再接続、複数のデバイスからの設定の読み取り、複数のデバイスの同時アップグレードなどがあります。ジョブテーブルの色分けされた行は、成功または失敗した個々のアクションを示します。

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]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] ページには、次の 3 つの方法でアクセスできます。

- 通知タブで、通知行の [確認] リンクをクリックします。[ジョブ]ページにリダイレクトされ、その通知に対応する特定のジョブが表示されます。



- [通知（Notifications ）] タブの上部にある [ジョブを表示（View jobs）] リンクをクリックすると、[ジョブ] ページに移動します。
- CDO のメニューから、**[モニターリング（Monitoring）]** > **[ジョブ]** を選択します。この表には、CDO で実行される一括操作の完全なリストが示されます。

フィルタリングと検索

[ジョブ]ページでは、操作タイプ、操作を実行したユーザー、および操作ステータスによってフィルター処理および検索を実行できます。

いずれかのアクションに失敗した一括操作の再開

ジョブのページを確認して、一括操作で1つ以上のアクションに失敗したことがわかった場合は、必要な修正を行った後に一括操作を再実行できます。CDO は、失敗したアクションのみでジョブを再実行します。一括操作を再実行するには、次の手順に従います。

手順

ステップ 1 アクションの失敗を示すジョブページの行を選択します。

ステップ 2 再開 アイコンをクリックします。

一括操作のキャンセル

複数のデバイスで実行したアクティブな一括操作をキャンセルできるようになりました。 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、3台のデバイスが正常に再接続したが、4 台目のデバイスは再接続に成功も失敗もしていないとします。

一括操作をキャンセルするには、次の手順を実行します。

手順

ステップ 1 CDO ナビゲーションメニューで、[ジョブ] をクリックします。

ステップ 2 まだ実行中の一括操作を見つけて、ジョブの行の右側にある [キャンセル] リンクをクリックします。

一括操作のいずれかの部分が成功した場合、それらの操作は元に戻されません。まだ実行中の操作はすべてキャンセルされます。

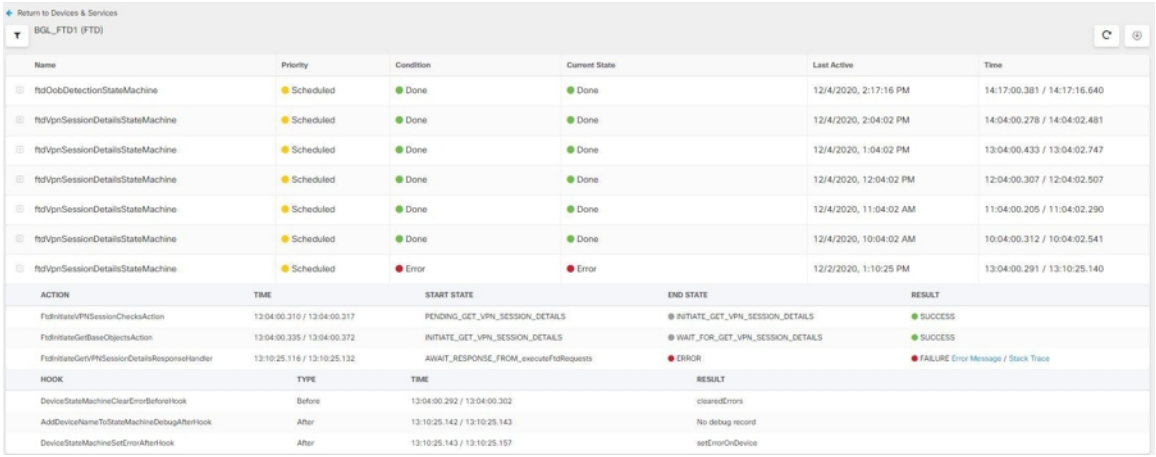
[ワークフロー（Workflows）] ページ

[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、CDOが実行するすべてのプロセスを監視できます。CDO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、CDO 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。

CDO は、デバイスでのタスクの実行に失敗するとエラーを報告します。[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とエラーの詳細を確認できます。

このページにアクセスして、エラーを特定してトラブルシューティングしたり、TACに要求された情報を TAC と共有したりすることができます。

[ワークフロー（Workflows）] ページに移動するには、[デバイスとサービス] ページで、[デバイス] 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。



ワークフロー情報のダウンロード

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。この情報をダウンロードするには、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ボタン をクリックします。

スタックトレースの生成

解決できないエラーがある場合、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。