



## トラブルシューティング

この章は、次のセクションで構成されています。

- [Firepower Threat Defense \(FTD\) のトラブルシューティング \(1 ページ\)](#)
- [Secure Device Connector のトラブルシューティング \(13 ページ\)](#)
- [Secure Event Connector のトラブルシューティング \(17 ページ\)](#)
- [CDO のトラブルシューティング \(30 ページ\)](#)
- [デバイスの接続状態 \(41 ページ\)](#)
- [SecureX のトラブルシューティング \(58 ページ\)](#)

## Firepower Threat Defense (FTD) のトラブルシューティング

FTD デバイスのトラブルシューティングを行う際、以下を参考にしてください。

- [登録キーを使用したオンボーディング中にデバイス登録の問題のトラブルシューティングを実行する](#)
- [FTD HA 作成のトラブルシューティング \(13 ページ\)](#)

## エグゼクティブ サマリー レポートのトラブルシューティング

ネットワーク運用レポートを作成しようとしても、期待どおりの結果が表示されない場合や、データがまったく表示されない場合があります。場合によっては、サマリーに「**使用可能なデータがありません (No data available)**」と表示されることがあります。次のシナリオを考えます。

- CDO は、デバイスがオンボーディングされてから **1 時間**ごとにイベントをポーリングします。一部のスケジュール済みイベントは、10 分ごと、60 分ごと、6 時間ごと、または 24 時間ごとのさまざまな時間間隔でポーリングされる複数のジョブをトリガーできます。選択したデバイスがオンボーディングされたばかりの場合、データを収集してコンパイルする十分な時間がない可能性があります。

- スマートライセンスが不足している可能性があります。十分なライセンスのあるデバイスのみがデータを生成します。「[FTD のライセンスタイプ](#)」を参照して、目的のデータの生成に必要なスマートライセンスを確認してください。
- アクセス制御ルールのロギングが有効になっていません。詳細については、[FTD アクセスコントロールルールのロギング設定](#)を参照してください。
- 選択した時間範囲に関して表示するデータの量が不足しているか、選択した時間範囲の間にアクセス制御ルールがトリガーされていない可能性があります。[時間範囲 (TimeRange)] オプションを切り替えて、別の期間がレポートに影響しているかどうかを判断します。

## FTD のオンボーディングのトラブルシュート

### 接続性

- ping でデバイスの接続を確認します。ASA から直接 FP 管理 IP アドレスに ping を実行してみてください。ICMP が外部からの通信をブロックする場合、インターネットから FP 管理インターフェイスに対して ping を実行できません。cUrl または wget を使用すると、設定された IP やポートで FP 管理インターフェイスにアクセスできるかどうかを確認できます。
- ASA/ASDM ソフトウェアバージョンの互換性の確認詳細については、「[CDO 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。
- ASA ログを使用して、CDO トラフィックが ASA によってブロックされているかどうかを判断します。SSH を介して FP HTTP 管理インターフェースへの接続を試みると、`/var/log/httpd/httpd_access_log` にログが記録されます。

### モジュールの不良構成

- Unsupported configuration. モジュールが特定の要件を満たしていない場合、CDO はデバイス構成をサポートできない場合があります。

### HTTP Authentication

- CDO は、オンボーディングプロセス中に ASA デバイスを認証するためにトークンベースの SSO を発行します。マルチコンテキストモードの ASA の場合、管理コンテキスト以外から FP モジュールをオンボードしようとする、トークンが発生する可能性があります。無効なトークンは、`/var/log/mojo/mojo.log a` で ASDM SSO ログインとして識別されます。

## ライセンス不足のために失敗

デバイスの接続ステータスに[ライセンスが不足しています (Insufficient License)]と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。
- デバイスのステータスが変わらない場合は、CDO からサインアウトしてから再度サインインすることで CDO ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の不具合を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。

#### 手順

- ステップ 1** Cisco Smart Software Manager から新しい登録キーを生成し、コピーします。詳細については、[スマートライセンスの生成](#)に関するビデオをご覧ください。
- ステップ 2** CDO のナビゲーションバーで、[デバイスとサービス (Devices & Services)] ページをクリックします。
- ステップ 3** [デバイス] タブをクリックします。
- ステップ 4** 適切なデバイスタイプのタブをクリックし、ステータスが [ライセンスが不足しています (Insufficient License)] のデバイスを選択します。
- ステップ 5** [デバイスの詳細 (Device Details)] ペインで、[ライセンスが不足しています (Insufficient License)] に表示される [ライセンスの管理 (Manage Licenses)] をクリックします。[ライセンスの管理 (Manage Licenses)] ウィンドウが表示されます。
- ステップ 6** [アクティブ化 (Activate)] フィールドで、新しい登録キーを貼り付けて [デバイスの登録 (Register Device)] をクリックします。

新しい登録キーがデバイスに正常に適用されると、接続状態が [オンライン (Online)] に変わります。

#### 関連情報 :


- [FTD のオンボーディング](#)
- [ユーザー名、パスワード、IP アドレスを使用した FTD のオンボーディング](#)
- [スマートライセンスの適用または更新](#)

## 登録解除されたデバイスのトラブルシューティング

FTD デバイスが、FDM 経由でクラウドから登録解除されていることがあります。

以下の手順を実行して、デバイスをクラウドに再登録します。

## 手順

- 
- ステップ 1** [インベントリ (Inventory)] ページで [デバイス (Devices)] タブをクリックします。
- ステップ 2** [FTD] タブをクリックし、[デバイスの登録が解除されました (Device Unregistered)] 状態のデバイスを選択し、右側でエラーメッセージを確認します。
- ステップ 3** 登録解除されたデバイスが登録キーを使用してオンボーディングされた場合、以前に適用されたキーの有効期限が切れているため、CDO は新しい登録キーを生成するように求めます。
- [更新 (Refresh)] ボタンをクリックして新しい登録キーを生成し、コピーアイコン  をクリックします。
  - CDO に再登録する FTD の FDM にログインします。
  - [システム設定 (System Settings)] で、[クラウドサービス (Cloud Services)] をクリックします。
  - [Cisco Defense Orchestrator] 領域で、[始める (Get Started)] をクリックします。
  - [登録キー (Registration Key)] フィールドに、CDO で生成した登録キーを貼り付けます。
  - [登録 (Register)] をクリックし、[シスコの開示情報を受け入れる (Accept the Cisco Disclosure)] をクリックします。FDM が CDO に登録要求を送信します。
  - デバイスの接続状態が [読み取りエラー (Read Error)] に変わるまで、CDO の [インベントリ (Inventory)] ページを更新します。
  - CDO の [設定の読み取り (Read Configuration)] をクリックして、デバイスから設定を読み取ります。
- ステップ 4** 登録解除されたデバイスがシリアル番号を使用してオンボーディングされた場合、CDO は FDM からデバイスを自動登録するように求めます。
- CDO に再登録する FTD の FDM にログインします。
  - [システム設定 (System Settings)] で、[クラウドサービス (Cloud Services)] をクリックします。
  - [Cisco Defense Orchestrator からテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] オプションを選択して [登録 (Register)] をクリックします。
  - デバイスの接続状態が [読み取りエラー (Read Error)] に変わるまで、CDO の [インベントリ (Inventory)] ページを更新します。
  - CDO の [設定の読み取り (Read Configuration)] をクリックして、デバイスから設定を読み取ります。
- 

## 登録キーを使用したオンボーディング中にデバイス登録の問題のトラブルシューティングを実行する

### クラウドサービスの FQDN を解決できない

クラウドサービスの FQDN の解決に失敗したためにデバイスの登録が失敗した場合は、ネットワーク接続または DNS 構成を確認して、デバイスのオンボーディングを再試行してください。

### 無効な登録キーのために失敗する

無効な登録キーが原因でデバイスの登録に失敗した場合、FDM に間違った登録キーを貼り付けている可能性があります。

同じ登録キーを CDO から再度コピーして、デバイスの登録を試行します。デバイスにすでにスマートライセンスがある場合は、FDM に登録キーを貼り付ける前にスマートライセンスを削除してください。

### ライセンス不足のために失敗する

デバイスの接続ステータスに [ライセンスが不足しています (Insufficient License) ] と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。
- デバイスのステータスが変わらない場合は、CDO からサインアウトしてから再度サインインすることで CDO ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の問題を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。
  1. Cisco Smart Software Manager から新しい登録キーを生成し、コピーします。詳細については、[スマートライセンスの生成](#)に関するビデオをご覧ください。
  2. CDO ナビゲーションバーで、[インベントリ (Inventory) ] ページをクリックします。
  3. ステータスが [ライセンスが不足しています (Insufficient License) ] のデバイスを選択します。
  4. [デバイスの詳細 (Device Details) ] ペインで、[ライセンスが不足しています (Insufficient License) ] に表示される [ライセンスの管理 (Manage Licenses) ] をクリックします。[ライセンスの管理 (Manage Licenses) ] ウィンドウが開きます。
  5. [アクティブ化 (Activate) ] フィールドで、新しい登録キーを貼り付けて [デバイスの登録 (Register Device) ] をクリックします。
- 新しい登録キーがデバイスに正常に適用されると、接続状態が [オンライン (Online) ] に変わります。

## 侵入防御システムのトラブルシューティング

### IPS ポリシーのオプションは何ですか？

すべてのオンボーディング済みデバイスは、「デフォルトオーバーライド」と呼ばれる CDO 提供の IPS ポリシーに自動的に関連付けられます。CDO はすべての FTD デバイスに対して新しい IPS ポリシーを生成するため、この名前のポリシーが複数存在する場合があります。デフォルトの IP ポリシーを使用し、署名のオーバーライドオプションを変更する場合は、

『[Firepower 侵入ポリシーの署名のオーバーライド](#)』を参照してください。デバイスごとに異なる署名オーバーライドを構成すると、デフォルトのオーバーライドポリシーに不整合が発生する可能性があることに注意してください。

**すべてのデバイスに異なる IPS ポリシーを構成するにはどうすればよいですか？**

CDO はすべての FTD デバイスに対して新しい IPS ポリシーを生成するため、この名前のポリシーが複数存在する場合があります。各デバイスのオンボーディング後に、CDO が提供する IPS ポリシーの名前を変更する必要はありません。ポリシーを拡大すると、それに関連付けられているデバイスが表示されます。また、デバイスまたはポリシーごとに脅威イベントページと署名オーバーライドページをフィルタ処理することもできます。デフォルトのオーバーライドポリシーをカスタマイズするには、デバイスごとに署名のオーバーライドを構成します。これにより、デフォルトのオーバーライド侵入ポリシーに不整合が生じますが、これによって機能が阻害されることはありません。

**FDM からオーバーライドが構成されているデバイスをオンボーディングしました。**

CDO の外部で構成されたオーバーライドは、デバイスの構成または機能に問題を引き起こしません。

すでにオーバーライドが構成されているデバイスをオンボーディングし、この新しいデバイスがオーバーライドが構成されていないデバイスと IPS ポリシーを共有している場合、IPS ポリシー不整合として表示されます。不整合に対処するには、『[Firepower 侵入ポリシーの署名のオーバーライド](#)』のステップ 3 を参照してください。

## SSL 暗号解読の問題のトラブルシューティング

**復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理 (SSL または認証局 ピニング)**

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL (または認証局) ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバー証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense デバイスから受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Web サイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Web ブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で <https://www.facebook.com/> を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

- アプリケーションのユーザをサポートします。この場合は、サイトへのトラフィックを復号できません。[SSL 復号 (SSL Decryption)] ルールの [アプリケーション (Application)] タブで、サイトのアプリケーションの [復号しない (Do Not Decrypt)] ルールを作成し、

そのルールが、接続に適用される [再署名の復号 (Decrypt Re-sign) ] ルールの前に適用されることを確認します。

- ユーザにブラウザだけを使用させます。サイトへのトラフィックを復号する必要がある場合は、ネットワーク経由での接続にサイトのアプリケーションを使用できないため、ブラウザのみを使用しなければならないことをユーザーに通知する必要があります。

## 詳細

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション (Facebook など) は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラートメッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN が含まれます。
  - SSL フロー フラグには APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE です。
- グループ 2 のアプリケーション (Dropbox など) はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN、APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE、CLIENT\_KEY\_EXCHANGE、CLIENT\_CHANGE\_CIPHER\_SPEC、CLIENT\_FINISHED、SERVER\_CHANGE\_CIPHER\_SPEC、SERVER\_FINISHED です。

## CA 証明書のダウンロードボタンが無効になっている

CDO でステージングされているが、まだデバイスに展開されていない証明書 (自己署名およびアップロード) のダウンロードボタンが無効になっています。証明書は、デバイスへの展開後のみダウンロードできます。

# シリアル番号を使用した FTD オンボーディングのトラブルシューティング

- プロビジョニングエラー
  - デバイスパスワードが変更されていない
  - デバイスパスワードがすでに変更されている
- 要求エラー
  - 無効なシリアル番号
  - デバイスのシリアル番号がすでに要求されている
  - デバイスがオフラインである
  - デバイスの要求に失敗した

## 要求エラー

### 無効なシリアル番号



CDO でデバイスを要求するときに、間違ったシリアル番号が入力されました。

#### 対処法

1. CDO で FTD デバイスインスタンスを削除します。
2. 正しいシリアル番号を入力して新しい FTD デバイスインスタンスを作成し、デバイスを要求します。

### デバイスのシリアル番号がすでに要求されている

シリアル番号を使用して FTD デバイスをオンボーディングすると、次のエラーが発生します。



#### 原因

このエラーは次のいずれかの理由で発生することがあります。

- デバイスが外部ベンダーから購入された可能性があり、デバイスがそのベンダーのテナントにあります。
- デバイスが、以前に他の地域にある別の CDO インスタンスによって管理されていた可能性があり、そのクラウドテナントに登録されています。



## 対処法

デバイスのシリアル番号を他のクラウドテナントから登録解除した後に、テナントで再要求する必要があります。

## 前提条件

デバイスは、クラウドテナントに到達できるインターネットに接続されている必要があります。

## 外部ベンダーから購入したデバイス

外部ベンダーから購入したデバイスは、そのベンダーのクラウドテナントに登録されている可能性があります。

1. CDO からデバイスインスタンスを削除します。
2. デバイスに FXOS イメージをインストールします。詳細については、『[Cisco FXOS Troubleshooting Guide for the Firepower 1000/21000 with FTD](#)』の「Reimage Procedures」の章を参照してください。
3. コンソールポートから FXOS CLI に接続します。
4. 現在の管理者パスワードを使用して FXOS にログインします。
5. FXOS CLI で、local-mgmt に接続します。firepower # **connect local-mgmt**
6. コマンドを実行して、クラウドテナントからデバイスを登録解除します。  
firepower(local-mgmt) # **cloud deregister**
7. 登録解除が成功すると、CLI インターフェイスは成功メッセージを返します。

例 : firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success  
MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9

デバイスがクラウドテナントからすでに登録解除されている場合、CLI インターフェイスは、デバイスのシリアル番号がクラウドテナントに登録されていないことを示します。

RESULT=success MESSAGE=DEVICE\_NOT\_FOUND: Device with serial number JAD213082x9 is not registered with SSE, X-Flow-Id: 63e48b4c-8426-48fb-9bd0-25fcd7777b99

8. デバイスのシリアル番号を入力して、CDO でデバイスを再度要求します。詳細については、「[デバイスのシリアル番号を使用した FTD のオンボーディング](#)」を参照してください。
9. デバイスに FTD アプリケーション（バージョン 6.7 以降）をインストールします。ロータッチプロビジョニングがデバイス上で開始され、デバイスが Cisco Cloud に登録されます。CDO がデバイスをオンボーディングします。

## 別の地域の別のクラウドテナントによってすでに管理されている FTD デバイスのオンボーディング

デバイスが、以前に他の地域にある別の CDO インスタンスによって管理されていた可能性があります。そのクラウドテナントに登録されています。

ケース 1 : デバイスを所有するテナントにアクセスできる。

1. 地域 1 の CDO からデバイスインスタンスを削除します。
2. FDM で、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページに移動します。デバイスが CDO から削除されたことを示す警告メッセージが表示されます。
3. をクリックし、ドロップダウンリストから [クラウドサービスの登録解除 (Unregister Cloud Services)] を選択します。
4. 警告を確認してから、[登録解除 (Unregister)] をクリックします。
5. 地域 2 の CDO からデバイスを要求します。
6. FDM で、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] に移動し、[Cisco Defense Orchestratorからテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] オプションを選択して [登録 (Register)] をクリックします。デバイスは、新しい地域に属する新しいテナントにマッピングされ、CDO によってオンボーディングされます。

ケース 2 : デバイスを所有するテナントにアクセスできない。

1. コンソールポートから FXOS CLI に接続します。
2. 現在の管理者パスワードを使用して FXOS にログインします。
3. FXOS CLI で、local-mgmt に接続します。firepower # **connect local-mgmt**
4. コマンドを実行して、クラウドテナントからデバイスを登録解除します。  
firepower(local-mgmt) # **cloud deregister**
5. 登録解除が成功すると、CLI インターフェイスは成功メッセージを返します。

例 : **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

デバイスがクラウドから登録解除されます。

6. 地域 2 の CDO からデバイスを要求します。
7. FDM で、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] に移動し、[Cisco Defense Orchestratorからテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] オプションを選択して [登録 (Register)] をクリックします。デバイスは、新しい地域に属する新しいテナントにマッピングされ、CDO によってオンボーディングされます。

デバイスがオフラインである



原因

次のいずれかの理由により、デバイスが Cisco Cloud に到達できません。

- デバイスのケーブル接続が正しくありません。
- ネットワークには、デバイスのスタティック IP アドレスが必要な場合があります。
- ネットワークでカスタム DNS が使用されているか、顧客のネットワークに外部 DNS ブロッキングが設定されています。
- PPPoE 認証が必要です。（欧州地域共通）
- FTD がプロキシの背後に配置されています。

#### 対処法

1. デバイスにサインインし、ブートストラップ CLI プロセスまたは FDM の簡単なセットアッププロセスを実行して、まずインターネットに接続できるようにデバイスを設定します。
2. ケーブル接続とネットワーク接続を確認します。
3. ファイアウォールがトラフィックをブロックしていないことを確認してください。
4. SSE ドメインが到達可能であることを確認してください。詳細については、「[ハードウェア設置に関する設定の前提条件](#)」を参照してください。

#### デバイスの要求に失敗した

##### 原因

このエラーは次のいずれかの理由で発生することがあります。

- SSE に一時的な問題が発生している可能性があります。
- サーバーがダウンしている可能性があります。

##### 対処法

1. CDO で FTD デバイスインスタンスを削除します。
2. 新しい FTD デバイスインスタンスを作成し、しばらくしてから再度デバイスを要求します。



(注) デバイスを要求できない場合は、ワークフローに移動してエラーメッセージを確認し、詳細を CDO サポートチームに送信します。

## プロビジョニングエラー

### デバイスのパスワードは変更されていません

CDO からデバイスを要求すると、デバイスの初期プロビジョニングが失敗し、[インベントリ (Inventory)] ページに「プロビジョニングされていません」というメッセージが表示される場合があります。

#### 原因

デフォルトパスワードが変更されていない新しい FTD デバイスに対して、CDO FTD シリアル オンボーディング ウィザードで [デフォルトパスワードが変更された (Default Password Changed)] オプションを選択した可能性があります。

#### 対処法

デバイスのパスワードを変更するには、[インベントリ (Inventory)] ページで [パスワードの入力 (Enter Password)] をクリックする必要があります。CDO は新しいパスワードで続行し、デバイスの導入準備をします。

### デバイスパスワードがすでに変更されている

CDO からデバイスを要求すると、デバイスの初期プロビジョニングが失敗し、[インベントリ (Inventory)] ページに「プロビジョニングされていません」というメッセージが表示される場合があります。

#### 原因

デフォルトパスワードがすでに変更されている FTD デバイスに対して、CDO FTD シリアル オンボーディング ウィザードで [デフォルトパスワードが変更されていない (Default Password Not Changed)] オプションを選択した可能性があります。

#### 対処法

シリアル オンボーディング ウィザードで指定された新しいパスワードを無視するには、[インベントリ (Inventory)] ページで [確認して続行 (Confirm and Proceed)] をクリックする必要があります。CDO は古いパスワードで続行し、デバイスの導入準備をします。

### その他のエラーの場合

その他すべてのプロビジョニングエラーについては、[再試行 (Retry)] をクリックしてプロビジョニングを再開できます。複数回再試行しても失敗する場合は、次の手順を実行します。

1. CDO から FTD デバイスインスタンスを削除し、新しいインスタンスを作成します。オンボーディングの手順については、『[Onboard an FTD using the Device's Serial Number](#)』を参照してください。
2. FDM で、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] に移動し、[Cisco Defense Orchestratorからテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] オプションを選択して [登録 (Register)] をクリックします。

## FTD HA 作成のトラブルシューティング

### イベントの説明エラー

CDO で FTD HA ペアをオンボードまたは作成しようとする、HA ペアの形成に失敗し、次のメッセージとともにエラーが表示される場合があります。

[ イベントの説明 (Event description) ] : CD App Sync エラーは、Cisco Threat Response がアクティブデバイスで有効になっていて、スタンバイでは有効になっていない場合に表示されます (CD App Sync error is Cisco Threat Response is enabled on Active but not on Standb)。

このエラーが表示された場合、HA ペア内の一方または両方のデバイスが、イベントを CDO、Firepower Threat Response、または Cisco Success Network などの Cisco Cloud サーバーに送信できるように設定されていません。

FDM UI から、[ Cisco Cloud にイベントを送信 (Send Events to the Cisco Cloud) ] 機能を有効にする必要があります。詳細については、実行しているバージョンの Firepower Device Manager 設定ガイド [英語] の「Configuring Cloud Services」の章を参照してください。

<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html>

HA を作成後、デバイスの 1 つが不良状態になります。

HA の作成中にいずれかのデバイスが異常または障害状態になった場合は、HA ペアを解除してデバイスの状態を解決してから、HA を再作成します。フェールオーバーの履歴は、問題の診断に役立つ場合があります。[FTD の高可用性フェールオーバーの履歴](#)

## Secure Device Connector のトラブルシューティング

オンプレミスの Secure Device Connector (SDC) のトラブルシューティングを行うには、以下のトピックを参照してください。

いずれのシナリオにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースを開いてください。

### SDC に到達不能

CDO からの 2 回のハートビート要求に連続して応答しなかった場合、SDC の状態は [到達不能 (Unreachable)] になります。SDC に到達不能な場合、テナントは、オンボーディングしたどのデバイスとも通信できません。

CDO は、次の方法で SDC に到達不能であることを示します。

- 「一部の Secure Device Connector (SDC) に到達できません。該当する SDC に関連付けられたデバイスとは通信できません (Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs)」というメッセージが CDO のホームページに表示されます。

- [セキュアコネクタ (Secure Connectors) ] ページの SDC のステータスが [到達不能 (Unreachable) ] になります。

この問題を解決するには、まず SDC とテナントの再接続を試行してください。

1. SDC 仮想マシンが実行中で、地域の CDO IP アドレスに到達できることを確認します。  
[Cisco Defense Orchestrator の管理対象デバイスへの接続](#)を参照してください。
2. ハートビートを手動で要求して、CDO と SDC の再接続を試行します。SDC がハートビート要求に応答すると、[アクティブ (Active) ] ステータスに戻ります。ハートビートを手動で要求するには、次の手順に従います。
  1. ユーザーメニューから、[セキュアコネクタ (Secure Connectors) ] を選択します。
  2. 到達不能な SDC をクリックします。
  3. [操作 (Actions) ] ウィンドウで、[ハートビートの要求 (Request heartbeat) ] をクリックします。
  4. [再接続 (Reconnect) ] をクリックします。
3. SDC を手動でテナントに再接続しようとしても、SDC が [アクティブ (Active) ] ステータスに戻らない場合は、「[展開後 CDO で SDC ステータスがアクティブになりません \(14 ページ\)](#)」の指示に従ってください。

## 展開後 CDO で SDC ステータスがアクティブになりません

展開から約 10 分過ぎても SDC がアクティブであると CDO で示されない場合は、SDC の展開時に作成した cdo ユーザーおよびパスワードを使用して、SDC VM に SSH 接続します。

### 手順

---

**ステップ 1** /opt/cdo/configure.log を確認します。ここでは、入力した SDC の構成設定と、それらが正常に適用されたかどうかを示されます。セットアッププロセスでエラーが発生した場合や値が正しく入力されていない場合は、sdc-onboard setup を再度実行します。

- a) [cdo@localhost cdo]\$ プロンプトで、sudo sdc-onboard setup と入力します。
- b) cdo ユーザーのパスワードを入力します。
- c) プロンプトに従います。セットアップスクリプトの指示に従って、セットアップウィザードで行ったすべての設定手順を確認し、入力した値を変更できます。

**ステップ 2** ログを確認し、sudo sdc-onboard setup を実行しても、SDC がアクティブであることが CDO で示されない場合は、[CDO サポートに連絡してください](#)。

---

## SDC の変更した IP アドレスが CDO に反映されない

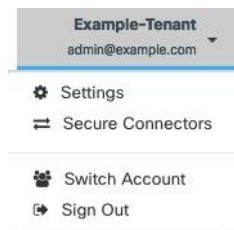
SDC の IP アドレスを変更した場合、GMT の午前 3 時以降まで変更は CDO に反映されません。

### デバイスと SDC の接続に関するトラブルシューティング

このツールを使用して、Secure Device Connector (SDC) を介した CDO からデバイスへの接続をテストします。デバイスがオンボーディングに失敗した場合、またはオンボーディングの前に CDO がデバイスに到達できるかどうかを判断する場合は、この接続をテストすることができます。

#### 手順

**ステップ 1** [アカウント (Account)] メニューをクリックし、[セキュアコネクタ (Secure Connectors)] を選択します。



**ステップ 2** SDC を選択します。

**ステップ 3** 右側の [トラブルシューティング (Troubleshooting)] ペインで、[デバイスの接続 (Device Connectivity)] をクリックします。

**ステップ 4** トラブルシューティングまたは接続しようとしているデバイスの有効な IP アドレスまたは FQDN とポート番号を入力し、[実行 (Go)] をクリックします。CDO は次の検証を実行します。

- a) [DNS解決 (DNS Resolution)] : IP アドレスの代わりに FQDN を指定すると、SDC がドメイン名を解決でき、IP アドレスを取得できることを確認します。
- b) [接続テスト (Connection Test)] : デバイスが到達可能であることを確認します。
- c) [TLSサポート (TLS support)] : デバイスと SDC の両方がサポートする TLS バージョンと暗号を検出します。

- [サポートされていない暗号 (Unsupported Cipher)] : デバイスと SDC の両方でサポートされている TLS バージョンがない場合、CDO は、SDC ではなくデバイスでサポートされている TLS バージョンと暗号についてもテストします。

d) SSL 証明書 : トラブルシューティングでは、証明書情報が提供されます。

**ステップ 5** デバイスのオンボーディングまたはデバイスへの接続の問題が解消しない場合は、[Defense Orchestrator サポート](#)までお問い合わせください。

## Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性 : cisco-sa-20190215-runc

Cisco Product Security Incident Response Team (PSIRT) は、Docker の重大度の高い脆弱性について説明するセキュリティアドバイザリ **cisco-sa-20190215-runc** を公開しました。脆弱性の完全な説明については、[PSIRT チームのアドバイザリ全体をお読みください](#)。

この脆弱性は、すべての CDO ユーザーに影響します。

- CDO のクラウド展開された Secure Device Connector (SDC) を使用しているお客様は、修復手順が CDO 運用チームによってすでに実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。アップグレードするには、次の手順を使用します。
  - [CDO 標準の SDC ホストの更新 \(16 ページ\)](#)
  - [カスタム SDC ホストを更新する \(17 ページ\)](#)
  - [バグトラッキング \(17 ページ\)](#)

### CDO 標準の SDC ホストの更新

[CDO イメージを使用して SDC を展開した場合は](#)、次の手順を使用します。

#### 手順

**ステップ 1** SSH またはハイパーバイザコンソールを使用して SDC ホストに接続します。

**ステップ 2** 次のコマンドを実行して、Docker サービスのバージョンを確認します。

```
docker version
```

**ステップ 3** 最新の仮想マシン (VM) のいずれかを実行している場合、次のような出力が表示されます。

```
> docker version
Client:
 Version: 18.06.1-ce
 API version: 1.38
 Go version: go1.10.3
 Git commit: e68fc7a
 Built: Tue Aug 21 17:23:03 2018
 OS/Arch: linux/amd64
 Experimental: false
```

ここで古いバージョンが表示される可能性があります。

**ステップ 4** 次のコマンドを実行して Docker を更新し、サービスを再起動します。

```
> sudo yum update docker-ce
> sudo service docker restart
```



(注) Docker サービスの再起動中、CDO とデバイス間の接続が短時間停止します。

**ステップ 5** `docker version` コマンドを再度実行します。次の出力が表示されます。

```
> docker version
Client:
 Version: 18.09.2
 API version: 1.39
 Go version: go1.10.6
 Git commit: 6247962
 Built: Sun Feb XX 04:13:27 2019
 OS/Arch: linux/amd64
 Experimental: false
```

**ステップ 6** これで追加されました。パッチが適用された最新バージョンの Docker にアップグレードされました。

## カスタム SDC ホストを更新する

独自の SDC ホストを作成している場合は、Docker のインストール方法に基づいた更新手順に従う必要があります。CentOS、yum、Docker-ce (コミュニティ版) を使用した場合は、前述の手順で動作します。

Docker-ee (エンタープライズ版) をインストールした場合、または別の方法を使用して Docker をインストールした場合は、Docker の修正バージョンが異なる場合があります。正しいインストールバージョンは、Docker のページ ([Docker Security Update and Container Security Best Practices](#)) で確認できます。

## バグトラッキング

シスコでは、この脆弱性を引き続き評価し、追加情報が利用可能になりしだい、アドバイザリを更新します。アドバイザリに最終とマーキングされた後は、詳細については次の関連 Cisco Bug を参照してください。

[CSCvo33929-CVE-2019-5736 : runC コンテナのブレイクアウト](#)

# Secure Event Connector のトラブルシューティング

いずれのシナリオにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースを開いてください。

## SEC オンボーディング失敗のトラブルシューティング

以下のトラブルシューティングのトピックでは、Secure Event Connector (SEC) のオンボーディングの失敗に関連するさまざまな症状について説明します。

### SEC のオンボーディングに失敗しました

症状：SEC のオンボーディングに失敗しました。

修復：SEC を取り外して、再度オンボードします。

このエラーが表示された場合：

1. 仮想マシンコンテナから [Secure Event Connector](#) とそのファイルを削除します。
2. [Secure Device Connector](#) の更新。通常、SDC は自動的に更新されるためこの手順を行う必要はありませんが、トラブルシューティングではこの手順が役立ちます。
3. [SDC 仮想マシンへの Secure Event Connector のインストール](#)。



ヒント SECをオンボードするときは、常にコピーリンクを使用してブートストラップデータをコピーします。



(注) この手順で問題が解決しない場合は、[イベントロギングのトラブルシューティング ログ ファイル](#)し、マネージド サービス プロバイダーまたは [Cisco Technical Assistance Center](#) に連絡してください。

### SEC ブートストラップデータが指定されていません

メッセージ：ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

診断：プロンプトが表示されたときに、ブートストラップデータがセットアップスクリプトに入力されませんでした。

修復：オンボーディング時にブートストラップデータの入力を求められたら、CDO UI で生成された SEC ブートストラップデータを指定します。

### ブートストラップ構成ファイルが存在しません

メッセージ：ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant\_name>, bootstrap config file ("/usr/local/cdo/es\_bootstrapdata") does not exist, exiting.

診断：SEC ブートストラップ データ ファイル ("/usr/local/cdo/es\_bootstrapdata") が存在しません。

修復：CDO UI で生成された SEC ブートストラップデータをファイル `/usr/local/cdo/es_bootstrapdata` に配置し、オンボーディングを再試行します。

1. オンボーディング手順を繰り返します。

2. ブートストラップデータをコピーします。
3. 「sdc」ユーザーとして SEC VM にログインします。
4. CDO UI で生成された SEC ブートストラップデータをファイル `/usr/local/cdo/es_bootstrapdata` に配置し、オンボーディングを再実行します。

#### ブートストラップデータのデコードに失敗しました

メッセージ : ERROR cannot bootstrap Secure Event Connector for tenant: <tenant\_name>, failed to decode SEC bootstrap data, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
failed to decode SEC bootstrap data, exiting.
```

診断 : ブートストラップデータのデコードに失敗しました

修復 : SEC ブートストラップデータを再生成し、オンボーディングを再実行します。

#### ブートストラップデータに SEC をオンボードするために必要な情報がありません

メッセージ :

- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant\_name>, SSE\_FQDN not set, exiting.
- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant\_name>, SSE\_OTP not set, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
SSE_FQDN not set, exiting.

[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
SSE_FQDN not set, exiting.
```

診断 : ブートストラップデータに SEC をオンボードするために必要な情報がありません。

修復 : ブートストラップデータを再生成し、オンボーディングを再実行します。

#### ツールキット cron が現在実行中

メッセージ : ERROR SEC toolkit already running, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

診断 : ツールキット cron が現在実行中です。

修復 : オンボーディングコマンドを再実行します。

#### 十分な CPU とメモリがない

メッセージ : ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and
8 GB ram required, exiting.
```

**診断**：十分な CPU とメモリがありません。

**修復**：VM の SEC 専用に最低 4 つの CPU と 8 GB の RAM がプロビジョニングされていることを確認し、オンボーディングを再試行します。

### SEC がすでに実行中

**メッセージ**：ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup'
before onboarding a new Secure Event Connector, exiting.
```

**診断**：SEC がすでに実行中です。

**修復**：新しい SEC をオンボードする前に、[SEC クリーンアップコマンド](#)を実行します。

### SEC ドメインに到達不能

**メッセージ**：

- Failed connect to api-sse.cisco.com:443; Connection refused
- ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain
api-sse.cisco.com unreachable, exiting.
```

**診断**：SEC ドメインに到達できません。

**修復**：オンプレミス SDC にインターネット接続があることを確認し、オンボーディングを再試行します。

オンボーディング SEC コマンドはエラーなしで成功しましたが、**SEC Docker** コンテナが起動していません

**症状**：オンボーディング SEC コマンドはエラーなしで成功しましたが、SEC Docker コンテナが起動していません

**診断**：オンボーディング SEC コマンドはエラーなしで成功しましたが、SEC docker コンテナが起動していません

**修復**：

1. 「sdc」ユーザーとして SEC にログインします。
2. SEC Docker コンテナの起動ログ (/usr/local/cdo/data/<tenantDir>/event\_streamer/logs/startup.log) でエラーがないか確認してください。
3. エラーがある場合は、[SEC クリーンアップコマンド](#)を実行して、オンボーディングを再試行してください。

### CDO サポートに連絡する

いずれのシナリオにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースを開いてください。

## Secure Event Connector の登録失敗のトラブルシューティング

**症状**：クラウドイベントサービスへの Cisco Secure Event Connector の登録が失敗します。

**診断**：SEC がイベントクラウドサービスに登録できない最も一般的な理由は、次のとおりです。

- SEC が SEC からイベントクラウドサービスに到達できない

**修復**：インターネットがポート 443 でアクセス可能であり、DNS が正しく設定されていることを確認します。

- SEC ブートストラップデータの無効または期限切れのワンタイムパスワードによる登録の失敗

**修復**：

### 手順

**ステップ 1** 「sdc」ユーザーとして SDC にログオンします。

**ステップ 2** コネクタログ (/usr/local/cdo/data/<tenantDir>/event\_streamer/logs/connector.log) を表示して、登録状態を確認します。

無効なトークンが原因で登録に失敗した場合は、ログファイルに次のようなエラーメッセージが表示されます。

**context:(\*contextImpl).handleFailed] registration - CE2001: Registration failed - Failed to register the device because of invalid token. Retry with a new valid token. - Failed"**

**ステップ 3** SDC VM で [SEC クリーンアップコマンド](#) 手順を実行して、[セキュアコネクタ (Secure Connectors) ] ページから SEC を削除します。

**ステップ 4** 新しい SEC ブートストラップデータを生成し、SEC オンボーディング手順を再試行します。

## Security and Analytics Logging イベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題にトラブルシューティングを実行するための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユー

ザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているか把握しています。



(注) このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FTD デバイスであることも想定しています。Security Analytics and Logging は、他のデバイスタイプからログ情報を収集しません。

## 手順

- ステップ 1 ナビゲーションウィンドウで、[モニタリング (Monitoring)] > [イベントロギング (Event Logging)] をクリックします。 >
- ステップ 2 [履歴 (Historic)] タブをクリックします。
- ステップ 3 [時間範囲 (Time Range)] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴 (Historical)] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了 (End)] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。
- ステップ 4 [センサーID (Sensor ID)] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで属性:値のペアを使用してイベントをフィルタ処理します。2つのエントリを作成し、それらを OR ステートメントで結合します。例: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`。
- ステップ 5 イベントフィルタバーの [ソースIP (Source IP)] フィールドにユーザーの IP アドレスを入力します。
- ステップ 6 ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [宛先IP (Destination IP)] フィールドに入力します。
- ステップ 7 結果に表示されるイベントを展開し、その詳細を確認します。以下の詳細に注意してください。
  - **AC\_RuleAction** - ルールがトリガーされたときに実行されたアクション (許可、信頼、ブロック)。
  - **FirewallPolicy** - イベントをトリガーしたルールが存在するポリシー。
  - **FirewallRule** - イベントをトリガーしたルールの名前。値が **Default Action** の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
  - **UserName** - イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスはソース IP アドレスと同じです。

- ステップ 8** ルールのアクションがアクセスをブロックしている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシーのルールを特定します。

## NSEL データフローのトラブルシューティング

したら、次の手順を使用して、NSEL イベントが ASA から Cisco Cloud に送信されていること、および Cisco Cloud がそれらのイベントを受信していることを確認します。

NSEL イベントを Secure Event Connector (SEC) に送信してから Cisco Cloud に送信するように ASA を設定すると、データはすぐには流れないことに注意してください。ASA で NSEL 関連のトラフィックが生成されていると仮定すると、最初の NSEL パケットが到着するまでに数分かかることがあります。



- (注) このワークフローは、「flow-export counters」コマンドと「capture」コマンドを単純に使用して NSEL データフローをトラブルシューティングする方法を示しています。これらのコマンドの使用法の詳細については、[CLI ブック 1 : Cisco ASA シリーズ CLI コンフィギュレーションガイド \(一般的な操作\) \[英語\]](#) および [Cisco ASA NetFlow 実装ガイド \[英語\]](#) の「Monitoring NSEL」を参照してください。

次のタスクを実行します。

- NetFlow パケットが SEC に送信されていることを確認する
- NetFlow パケットが Cisco Cloud 受信されていることを確認する

## イベントロギングのトラブルシューティング ログ ファイル

Secure Event Connector (SEC) の `troubleshoot.sh` は、すべてのイベントストリーマログを収集して、単一の `.tar.gz` ファイルに圧縮します。

次の手順を使用して、`compressed.tar.gz` ファイルを作成し、ファイルを解凍します。

1. [トラブルシューティング スクリプトの実行 \(23 ページ\)](#)。
2. [sec\\_troubleshoot.tar.gz ファイルの圧縮解除 \(24 ページ\)](#)。

## トラブルシューティング スクリプトの実行

Secure Event Connector (SEC) の `troubleshoot.sh` は、すべてのイベントストリーマログを収集して、単一の `.tar.gz` ファイルに圧縮します。次の手順に従って、`troubleshoot.sh` スクリプトを実行します。

## 手順

**ステップ1** VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。

**ステップ2** ログインしてから、[ルート (root) ] ユーザーに切り替えます。

```
[cdo@localhost ~]$sudo su root
```

(注) SDCユーザーに切り替える一方でrootとして操作することもできます。その場合、IPテーブルの情報も受信することになります。IPテーブルの情報には、デバイス上でファイアウォールが実行中であることと、すべてのファイアウォールルートが表示されます。ファイアウォールが Secure Event Connector TCPポートまたはUDPポートをブロックしている場合、[イベントロギング (Event Logging) ]テーブルにイベントが表示されません。IPテーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。

**ステップ3** プロンプトで、トラブルシューティングスクリプトを実行し、テナント名を指定します。コマンド構文は次のとおりです。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

コマンド出力で、sec\_troubleshoot ファイルが SDC の /tmp/troubleshoot ディレクトリに保存されていることがわかります。ファイル名は、**sec\_troubleshoot-timestamp.tar.gz** の表記法に従います。

**ステップ4** ファイルを取得するには、CDOユーザーとしてログインし、SCPまたはSFTPを使用してダウンロードします。

次に例を示します。

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

## 次のタスク

[sec\\_troubleshoot.tar.gz ファイルの圧縮解除 \(24 ページ\)](#) に進みます。

## sec\_troubleshoot.tar.gz ファイルの圧縮解除

Secure Event Connector (SEC) の [トラブルシューティング スクリプトの実行](#) は、すべてのイベントストリーマログを収集して、単一の sec\_troubleshoot.tar.gz ファイルに圧縮します。

sec\_troubleshoot.tar.gz ファイルの圧縮を解凍するには、次の手順を実行します。

1. VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。
2. ログインしてから、[ルート (root) ] ユーザーに切り替えます。

```
[cdo@localhost ~]$sudo su root
```





(注) **sdc** ユーザーに切り替える一方で **root** として操作することもできます。その場合、IP テーブルの情報も受信することになります。IP テーブルの情報には、デバイス上でファイアウォール実行中であることと、すべてのファイアウォールルートが表示されます。ファイアウォール Secure Event Connector TCP ポートまたは UDP ポートをブロックしている場合、[ イベントロギング (Event Logging) ] テーブルにイベントが表示されません。IP テーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。

3. プロンプトで、次のコマンドを入力します。

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

ログファイルは、テナント名に基づいて名付けられたディレクトリに保存されます。このタイプのログは、sec\_troubleshoot-timestamp.tar.gz ファイルに保存されます。root ユーザーとしてすべてのログファイルを収集した場合は、iptables ファイルが含まれています。



SEC ブートストラップデータの生成に失敗しました。

## SEC ブートストラップデータの生成に失敗しました。

**症状：** CDO で SEC ブートストラップデータを生成しているときに、「ブートストラップの生成」ステップでエラーが発生し、次のメッセージが表示されます。「ブートストラップデータの取得中にエラーが発生しました。再試行してください」。

**修復：** ブートストラップデータの生成を再試行します。それでも失敗する場合は、[CDO サポートまでお問い合わせください](#)。

## オンボーディング後、[CDOセキュアコネクタ (CDO Secure Connectors)] ページで SEC ステータスが [非アクティブ (Inactive)] になる

**症状：** 次のいずれかの理由により、[CDOセキュアコネクタ (CDO Secure Connectors)] ページで Secure Event Connector のステータスが [非アクティブ (Inactive)] と表示されます。

- ハートビートに失敗した
- コネクタの登録に失敗した

**修復：**

- **ハートビートに失敗した：** SEC ハートビートを要求し、[セキュアコネクタ (Secure Connector)] ページを更新して、ステータスが [アクティブ (Active)] に変わるか確認します。変わらない場合は、Secure Device Connector の登録が失敗していないか確認します。
- **コネクタの登録に失敗した：** [「Secure Event Connector の登録失敗のトラブルシューティング」](#) を参照してください。

## SEC は「オンライン」ですが、CDO イベントログページにはイベントがありません

**症状：** Secure Event Connector の CDO セキュアコネクタページには「アクティブ」と表示されているのに、CDO イベントビューアにイベントが表示されません。

**解決策または回避策：**

**手順**

**ステップ 1** オンプレミス SDC の VM に「sdc」ユーザーとしてログインします。プロンプトで、**sudo su - sdc** と入力します。

**ステップ 2** 次のチェックを実行します。

- SEC コネクタのログ (`/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log`) を確認し、SEC 登録が成功していることを確認します。成功していない場合は、[「Secure Event Connector の登録失敗のトラブルシューティング」](#) を参照してください。

- SEC イベントのログ (/usr/local/cdo/data/<tenantDir>/event\_streamer/logs/events-plugin.log)を確認し、イベントが処理されていることを確認します。処理されていない場合は、[CDO サポートにお問い合わせ](#)ください。
- SEC Docker コンテナにログインし、コマンド「`supervisorctl -c /opt/cssp/data/conf/supervisord.conf`」を実行します。出力が以下のようになり、すべてのプロセスが RUNNING 状態であることを確認します。そうでない場合は、[CDO サポートにお問い合わせ](#)ください。

**estreamer-connector RUNNING pid 36, uptime 5:25:17**

**estreamer-cron RUNNING pid 39, uptime 5:25:17**

**estreamer-plugin RUNNING pid 37, uptime 5:25:17**

**estreamer-rsyslog RUNNING pid 38, uptime 5:25:17**

- オンプレミス SDC のファイアウォールルールが、[セキュアコネクタ (Secure Connectors)] ページの SEC に表示される UDP および TCP ポートをブロックしていないことを確認します。どのポートを開くかを判断するには、「[Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索](#)」を参照してください。

ID	Type	Deployment	Status	Last Heartbeat
CDO_solution_es1-SDC	Secure Device Connector	On-Prem	Active	5/31/2019, 3:00:21 PM
6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b	Secure Event Connector	On-Prem	Active	5/31/2019, 3:00:23 PM

6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b	
Details	
Version	83a49e199bdd85b7cdfb8dd05972e50c5929abf4
IP Address	192.168.0.191
TCP Port	10125
UDP Port	10025

- 独自の CentOS 7 VM を使用して SDC を手動でセットアップし、ファイアウォールが着信要求をブロックするように設定している場合は、次のコマンドを実行して UDP および TCP ポートのブロックを解除できます。

**firewall-cmd --zone=public --add-port=<udp\_port>/udp --permanent**

**firewall-cmd --zone=public --add-port=<tcp\_port>/tcp --permanent**

**firewall-cmd --reload**

- 選択した Linux ネットワークツールを使用して、これらのポートでパケットが受信されているかどうかを確認します。受信していない場合は、FTD ログ設定を再確認してください。

上記のいずれの修復も機能しない場合は、[CDO サポートにサポートチケットを提出](#)します。

## SEC クリーンアップコマンド

Secure Event Connector (SEC) クリーンアップコマンドは、SEC コンテナとその関連ファイルを Secure Device Connector (SDC) VM から削除します。このコマンドは、[Secure Event Connector の登録失敗のトラブルシューティング \(21 ページ\)](#) またはオンボーディングが失敗した場合に実行できます。

このコマンドを実行するには、次の手順を実行します。

### 始める前に

このタスクを実行するには、自分のテナントの名前を知っている必要があります。テナント名を見つけるには、CDO でユーザーメニューを開き、[設定 (Settings)] をクリックします。ページを下にスクロールして、[テナント名 (Tenant Name)] を見つけます。

### 手順

**ステップ 1** 「sdc」ユーザーとして SDC にログインします。プロンプトで、`sudo su - sdc` と入力します。

**ステップ 2** `/usr/local/cdo/toolkit` ディレクトリに接続します。

**ステップ 3** `sec.sh removetenant_name` を実行し、SEC を削除することを確認します。

例：

```
[sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

### 次のタスク

このコマンドで SEC の削除に失敗した場合は、[SEC クリーンアップコマンドの失敗 \(28 ページ\)](#) に進みます。

## SEC クリーンアップコマンドの失敗

[SEC クリーンアップコマンド \(28 ページ\)](#) が失敗した場合は、この手順を使用します。

**メッセージ：** SEC が見つかりません。終了します。

**症状：** Cleanup SEC コマンドが既存の SEC のクリーンアップに失敗します。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42]
SEC not found, exiting.
```

**修復：** クリーンアップコマンドが失敗した場合、Secure Event Connector を手動でクリーンアップします。

すでに実行中の SEC docker コンテナを削除します。

### 手順

- ステップ1 「sdc」ユーザーとしてSDCにログインします。プロンプトで、`sudo su - sdc`と入力します。
- ステップ2 `docker ps` コマンドを実行して、SEC コンテナの名前を探します。SEC名は、"es\_name"の形式になります。
- ステップ3 `docker stop` コマンドを実行して、SEC コンテナを停止します。
- ステップ4 `rm` コマンドを実行して、SEC コンテナを削除します。

例：

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

## Secure Event Connector の状態を把握するためのヘルスチェックの使用

Secure Event Connector (SEC) のヘルスチェックスクリプトは、SEC の状態に関する情報を提供します。

ヘルスチェックを実行するには、次の手順に従います。

### 手順

- ステップ1 VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。
- ステップ2 「CDO」ユーザーとしてSDCにログインします。
- ステップ3 「SDC」ユーザーに切り替えます。

```
[cdo@tenant]$sudo su sdc
```

- ステップ4 プロンプトで `healthcheck.sh` スクリプトを実行し、テナント名を指定します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

スクリプトの出力には、次のような情報が表示されます。

```
=====
Running SEC health check for tenant [redacted]
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

ヘルスチェック出力の値：

- [SECクラウドURL (SEC Cloud URL)] : CDO クラウド URL と、SEC が CDO に到達できるかどうかを表示します。
- [SECコネクタ (SEC Connector)] : SEC コネクタが正しくオンボーディングされ、開始されている場合は、「実行中 (Running)」と表示されます。
- [SEC UDP syslogサーバー (SEC UDP syslog server)] : UDP syslog サーバーが UDP イベントを送信する準備ができている場合は、「実行中 (Running)」と表示されます。
- [SEC TCP syslogサーバー (SEC TCP syslog server)] : TCP syslog サーバーが TCP イベントを送信する準備ができている場合は、「実行中 (Running)」と表示されます。
- [SECコネクタのステータス (SEC Connector status)] : SEC が実行中で、CDO へのオンボーディングが完了している場合は、[アクティブ (Active)] と表示されます。
- [SEC送信サンプルイベント (SEC Send sample event)] : ヘルスチェックの終了時点ですべてのステータスチェックが「緑色」になっている場合、ツールはサンプルイベントを送信します。(いずれかのプロセスが [停止中 (Down)] になっている場合、ツールはテストイベントの送信をスキップします)。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。

## CDO のトラブルシューティング

### ログインの失敗のトラブルシューティング

正しくない CDO リージョンに誤ってログインしているため、ログインに失敗する

適切な CDO リージョンにログインしていることを確認してください。

<https://sign-on.security.cisco.com> にログインすると、アクセスするリージョンを選択できます。[CDO] タイルをクリックして [defenseorchestrator.com](https://defenseorchestrator.com) にアクセスするか、[CDO (EU)] をクリックして [defenseorchestrator.eu](https://defenseorchestrator.eu) にアクセスします。

### 移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、CDO へのログインに失敗する

**解決法** CDO にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Secure Sign-On アカウントを作成せずにログインを試みた可能性があります。[新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定](#) の手順に従って、新しい Cisco Secure Sign-On アカウントにサインアップする必要があります。

**Cisco Secure Sign-On ダッシュボードへのログインは成功するが、CDO を起動できない**

**解決法** CDO アカウントとは異なるユーザー名で Cisco Secure Sign-On アカウントを作成している可能性があります。CDO と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center (TAC) に連絡してください。 <http://cdo.support@cisco.com>

#### 保存したブックマークを使用したログインに失敗する

**解決法** ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが <https://cdo.onelogin.com> を指している可能性があります。

**解決法** <https://sign-on.security.cisco.com> にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、[アカウントを作成](#) します。
- **解決法** 新しいアカウントを作成している場合は、ダッシュボードで Cisco Defense Orchestrator (米国)、Cisco Defense Orchestrator (欧州)、または Cisco Defense Orchestrator (アジア太平洋/日本/中国) に対応する CDO タイルをクリックします。
- **解決法** <https://sign-on.security.cisco.com> を指すようにブックマークを更新します。

## アクセスと証明書のトラブルシューティング

### 新規フィンガープリント検出ステータスの解決

#### 手順

- 
- ステップ 1** ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
  - ステップ 2** [デバイス] タブをクリックします。
  - ステップ 3** 適切なデバイスタイプのタブをクリックします。
  - ステップ 4** [新しいフィンガープリントを検出 (New Fingerprint Detected)] ステータスのデバイスを選択します。
  - ステップ 5** [新しい指紋が検出されました (New Fingerprint Detected)] ペインで [フィンガープリントの確認 (Review Fingerprint)] をクリックします。
  - ステップ 6** フィンガープリントを確認して許可するように求められたら、以下の手順を実行します。
    1. [フィンガープリントのダウンロード (Download Fingerprint)] をクリックして確認します。
    2. フィンガープリントに問題がなければ [許可 (Accept)] をクリックします。問題がある場合は、[キャンセル (Cancel)] をクリックします。
  - ステップ 7** 新しいフィンガープリントの問題を解決した後、デバイスの接続状態が [オンライン (Online)] と表示され、構成ステータスが「非同期 (Not Synced)」または「競合検出 (Conflict Detected)」と表示される場合があります。[構成の競合の解決 (Resolve Configuration Conflicts)] を確認し、CDO とデバイス間の構成の差異を確認して解決します。 [設定の競合の解決](#)
-

## Security and Analytics Logging イベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題にトラブルシューティングを実行するための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユーザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているか把握しています。



(注) このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FTD デバイスであることも想定しています。Security Analytics and Logging は、他のデバイスタイプからログ情報を収集しません。

### 手順

- ステップ 1** ナビゲーションウィンドウで、[モニタリング (Monitoring)] > [イベントロギング (Event Logging)] をクリックします。 >
- ステップ 2** [履歴 (Historic)] タブをクリックします。
- ステップ 3** [時間範囲 (Time Range)] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴 (Historical)] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了 (End)] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。
- ステップ 4** [センサー ID (Sensor ID)] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで **属性:値** のペアを使用してイベントをフィルタ処理します。2 つのエントリを作成し、それらを OR ステートメントで結合します。例: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`。
- ステップ 5** イベントフィルタバーの [ソース IP (Source IP)] フィールドにユーザーの IP アドレスを入力します。
- ステップ 6** ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [宛先 IP (Destination IP)] フィールドに入力します。
- ステップ 7** 結果に表示されるイベントを展開し、その詳細を確認します。以下の詳細に注意してください。
  - **AC\_RuleAction** - ルールがトリガーされたときに実行されたアクション (許可、信頼、ブロック)。
  - **FirewallPolicy** - イベントをトリガーしたルールが存在するポリシー。



- **FirewallRule** - イベントをトリガーしたルールの名前。値が **Default Action** の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
- **UserName** - イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスはソース IP アドレスと同じです。

**ステップ 8** ルールのアクションがアクセスをブロックしている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシーのルールを特定します。

## SSL 暗号解読の問題のトラブルシューティング

### 復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理 (SSL または認証局ピニング)

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL (または認証局) ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバー証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense デバイスから受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Web サイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Web ブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で <https://www.facebook.com> を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

#### 詳細の表示

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション (Facebook など) は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラートメッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN が含まれます。
  - SSL フロー フラグには APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE です。

- グループ 2 のアプリケーション（Dropbox など）はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
  - SSL フロー フラグには ALERT\_SEEN、APP\_DATA\_C2S または APP\_DATA\_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT\_HELLO、SERVER\_HELLO、SERVER\_CERTIFICATE、SERVER\_KEY\_EXCHANGE、SERVER\_HELLO\_DONE、CLIENT\_KEY\_EXCHANGE、CLIENT\_CHANGE\_CIPHER\_SPEC、CLIENT\_FINISHED、SERVER\_CHANGE\_CIPHER\_SPEC、SERVER\_FINISHED です。

## 侵入防御システムのトラブルシューティング

### IPS ポリシーのオプションは何ですか？

すべてのオンボーディング済みデバイスは、「デフォルトオーバーライド」と呼ばれる CDO 提供の IPS ポリシーに自動的に関連付けられます。CDO はすべての FTD デバイスに対して新しい IPS ポリシーを生成するため、この名前のポリシーが複数存在する場合があります。デフォルトの IP ポリシーを使用し、署名のオーバーライドオプションを変更する場合は、『[Firepower 侵入ポリシーの署名のオーバーライド](#)』を参照してください。デバイスごとに異なる署名オーバーライドを構成すると、デフォルトのオーバーライドポリシーに不整合が発生する可能性があることに注意してください。

### すべてのデバイスに異なる IPS ポリシーを構成するにはどうすればよいですか？

CDO はすべての FTD デバイスに対して新しい IPS ポリシーを生成するため、この名前のポリシーが複数存在する場合があります。各デバイスのオンボーディング後に、CDO が提供する IPS ポリシーの名前を変更する必要はありません。ポリシーを拡大すると、それに関連付けられているデバイスが表示されます。また、デバイスまたはポリシーごとに脅威イベントページと署名オーバーライドページをフィルタ処理することもできます。デフォルトのオーバーライドポリシーをカスタマイズするには、デバイスごとに署名のオーバーライドを構成します。これにより、デフォルトのオーバーライド侵入ポリシーに不整合が生じますが、これによって機能が阻害されることはありません。

### FDM からオーバーライドが構成されているデバイスをオンボーディングしました。

CDO の外部で構成されたオーバーライドは、デバイスの構成または機能に問題を引き起こしません。

すでにオーバーライドが構成されているデバイスをオンボーディングし、この新しいデバイスがオーバーライドが構成されていないデバイスと IPS ポリシーを共有している場合、IPS ポリシー不整合として表示されます。不整合に対処するには、『[Firepower 侵入ポリシーの署名のオーバーライド](#)』のステップ 3 を参照してください。

## 移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、CDO へのログインに失敗する

**解決法** CDO にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Secure Sign-On アカウントを作成せずにログインを試みた可能性があります。新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定の手順に従って、新しい Cisco Secure Sign-On アカウントにサインアップする必要があります。

**Cisco Secure Sign-On ダッシュボードへのログインは成功するが、CDO を起動できない**

**解決法** CDO アカウントとは異なるユーザー名で Cisco Secure Sign-On アカウントを作成している可能性があります。CDO と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center (TAC) に連絡してください。 <http://cdo.support@cisco.com>

**保存したブックマークを使用したログインに失敗する**

**解決法** ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが <https://cdo.onelogin.com> を指している可能性があります。

**解決法** <https://sign-on.security.cisco.com> にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、[アカウントを作成](#)します。
- **解決法** 新しいアカウントを作成している場合は、ダッシュボードで Cisco Defense Orchestrator (米国)、Cisco Defense Orchestrator (欧州)、または Cisco Defense Orchestrator (アジア太平洋/日本/中国) に対応する CDO タイルをクリックします。
- **解決法** <https://sign-on.security.cisco.com> を指すようにブックマークを更新します。

## オブジェクトのトラブルシューティング

### 重複オブジェクトの問題の解決

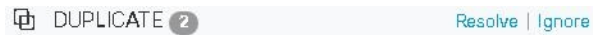
重複オブジェクトとは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは誤って作成され、同じ目的を果たし、さまざまなポリシーによって使用されます。重複オブジェクトの問題を解決した後、CDO は、残されたオブジェクト名に対する、影響を受けるすべてのオブジェクト参照を更新します

重複オブジェクトの問題を解決するには以下の手順を実行します。

#### 手順

- ステップ 1** [オブジェクト (Objects) ] ページを開き、オブジェクトを [フィルタ処理](#) して、重複するオブジェクトの問題を見つけます。

**ステップ 2** 結果の中から 1 つを選択します。オブジェクトの詳細パネルに、該当する重複の数を示す [重複 (DUPLICATE)] フィールドが表示されます。



**ステップ 3** [解決 (Resolve)] をクリックします。CDO は、重複オブジェクトを比較できるように表示します。

**ステップ 4** 比較するオブジェクトを 2 つ選択します。

**ステップ 5** 以下のオプションがあります。

- オブジェクトの 1 つを別のオブジェクトに置き換える場合は、保持するオブジェクトで [選択 (Pick)] をクリックし、[解決 (Resolve)] をクリックして影響を受けるデバイスとネットワークポリシーを確認し、変更の問題がなければ [確認 (Confirm)] をクリックします。CDO は、選択したオブジェクトに置き換えて保持し、重複を削除します。
- リストにあるオブジェクトを無視する場合は、[無視 (Ignore)] をクリックします。オブジェクトを無視すると、CDO が表示する重複オブジェクトのリストから削除されます。
- オブジェクトを保持するものの、重複オブジェクトの検索で CDO に表示してほしくない場合は、[すべて無視 (Ignore All)] をクリックします。

**ステップ 6** 重複オブジェクトの問題が解決したら、行った変更を今すぐ [レビューして展開する](#) か、待機してから複数の変更を一度に展開します。


## 不整合または未使用のセキュリティゾーンオブジェクトを解決する

セキュリティゾーンオブジェクトは、他のオブジェクトと同様に、不整合または未使用としてマークできます。これらの問題を解決する方法については、「[未使用オブジェクトの問題の解決](#)」と「[不整合オブジェクトの問題を解決する](#)」を参照してください。

関連情報：

- [セキュリティゾーンオブジェクト](#)
- [Firepower インターフェイスをセキュリティゾーンに割り当てる](#)
- [オブジェクトの削除](#)

## 未使用オブジェクトの問題の解決


未使用オブジェクト  は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。

関連情報：

- [デバイスとサービスのリストのエクスポート](#)
- [CDO へのデバイス一括再接続](#)


## 未使用オブジェクトの問題の解決

### 手順

- 
- ステップ 1** メニューバーで[オブジェクト (Objects)]をクリックし、オブジェクトを[フィルタ処理](#)して、未使用のオブジェクトの問題を見つけます。
- ステップ 2** 1つ以上の未使用のオブジェクトを選択します。
- ステップ 3** 以下のオプションがあります。
- 操作ウィンドウで[削除 (Remove)]  をクリックして、未使用のオブジェクトを CDO から削除します。
  - [問題 (Issues)] ペインで、[無視 (Ignore)] をクリックします。オブジェクトを無視すると、CDO は未使用のオブジェクトの結果にそのオブジェクトを表示しなくなります。
- ステップ 4** 未使用のオブジェクトを削除した場合は、行った変更を今すぐ[すべてのデバイスの設定変更のプレビューと展開](#)か、待機してから複数の変更を一度に展開します。
- (注) 未使用のオブジェクトの問題を一度に解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。
- 



## 未使用オブジェクトの一括削除

### 手順

- 
- ステップ 1** [オブジェクト (Objects)] ページを開き、オブジェクトを[フィルタ処理](#)して、未使用オブジェクトの問題を見つけます。
- ステップ 2** 削除する未使用のオブジェクトを選択します。
- ページ上のすべてのオブジェクトを選択するには、オブジェクトテーブルのヘッダー行にあるチェックボックスをクリックします。
  - オブジェクトテーブルで未使用のオブジェクトを個別に選択します。
- ステップ 3** 右側の[アクション (Actions)] ペインで[削除 (Remove)]  をクリックして、CDO で選択した未使用のオブジェクトをすべて削除します。99 個のオブジェクトを同時に削除できます。
- ステップ 4** [OK] をクリックして、未使用のオブジェクトを削除することを確認します。
- ステップ 5** これらの変更の展開には、つぎの 2 つの方法があります。
- 行った変更を今すぐ[レビューして展開する](#)か、待機してから複数の変更を一度に展開します。
  - [デバイスとサービス (Devices & Services)] ページを開き、変更の影響を受けたデバイスを特定します。変更の影響を受けるすべてのデバイスを選択し、[管理 (Management)] ペ

インで [すべて展開 (Deploy All)] をクリックします。警告を読み、適切なアクションを実行します。

## 不整合オブジェクトの問題を解決する

不整合オブジェクト  INCONSISTENT  とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーが異なる構成の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。

注：不整合オブジェクトの問題を一度に解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。

不整合オブジェクトに対して次のことを実行できます。

- [無視 (Ignore)]：CDO はオブジェクト間の不整合を無視して、その値を保持します。このオブジェクトは、不整合カテゴリに表示されなくなります。
- [マージ (Merge)]：CDO は選択されているすべてのオブジェクトとその値を 1 つのオブジェクトグループに結合します。
- [名前の変更 (Rename)]：ユーザーは不整合オブジェクトの 1 つの名前を変更し、新しい名前を付けることができます。
- [共有ネットワークオブジェクトのオーバーライドへの変換 (Convert Shared Network Objects to Overrides)]：ユーザーは不整合のある共有オブジェクトを（オーバーライドの有無にかかわらず）オーバーライドのある単一の共有オブジェクトに結合できます。不整合オブジェクトの最も共通するデフォルト値が、新しく形成されるオブジェクトのデフォルト値として設定されます。



(注) 共通するデフォルト値が複数ある場合は、そのうちの 1 つがデフォルトとして選択されます。残りのデフォルト値とオーバーライド値は、そのオブジェクトのオーバーライドとして設定されます。

- [共有ネットワークグループの追加の値への変換 (Convert Shared Network Group to Additional Values)]：ユーザーは不整合のある共有ネットワークグループを、追加の値のある単一の共有ネットワークグループに結合できます。この機能の条件は、「変換される不整合ネットワークグループに、同じ値を持つ共通オブジェクトが少なくとも 1 つあること」です。この条件を満たすすべてのデフォルト値がデフォルト値になり、残りのオブジェクトは、新しく形成されるネットワークグループの追加の値として割り当てられます。

たとえば、不整合のある 2 つの共有ネットワークグループがあるとします。1 つ目のネットワークグループ「shared\_network\_group」は、「object\_1」(192.0.2.x) と「object\_2」(192.0.2.y) で形成されています。また、追加の値「object\_3」(192.0.2.a) も含まれてい

ます。2つ目のネットワークグループ「shared\_network\_group」は、「object\_1」(192.0.2.x)と追加の値「object\_4」(192.0.2.b)で形成されています。共有ネットワークグループを追加の値に変換すると、新しく形成されるグループ「shared\_network\_group」には、デフォルト値として「object\_1」(192.0.2.x)と「object\_2」(192.0.2.y)が含まれ、追加の値として「object\_3」(192.0.2.a)と「object\_4」(192.0.2.b)が含まれます。




(注) 新しいネットワークオブジェクトを作成すると、CDOは、その値を同じ名前前の既存の共有ネットワークオブジェクトへのオーバーライドとして自動的に割り当てます。これは、新しいデバイスがCDOにオンボードされる場合にも当てはまります。

自動割り当ては、次の条件が満たされている場合にのみ発生します。

1. 新しいネットワークオブジェクトがデバイスに割り当てられる必要があります。
2. テナントには、同じ名前とタイプの共有オブジェクトが1つだけ存在する必要があります。
3. 共有オブジェクトには、すでにオーバーライドが含まれている必要があります。

不整合オブジェクトの問題を解決するには、次の手順を実行します。

#### 手順

- ステップ 1** [オブジェクト (Objects)] ページを開き、オブジェクトを [フィルタ処理](#) して、不整合オブジェクトの問題を見つけます。
- ステップ 2** 不整合オブジェクトを選択します。オブジェクトの詳細パネルに、該当するオブジェクトの数を示す [不整合 (INCONSISTENT)] フィールドが表示されます。  

- ステップ 3** [解決 (Resolve)] をクリックします。CDO は、不整合オブジェクトを比較できるように表示します。
- ステップ 4** 以下のオプションがあります。
  - [すべて無視 (Ignore All)] :
    1. 提示されるオブジェクトを比較し、いずれかのオブジェクトで [無視 (Ignore)] をクリックします。または、すべてのオブジェクトを無視するには、[すべて無視 (Ignore All)] をクリックします。
    2. [OK] をクリックして確認します。
  - [オブジェクトをマージして解決 (Resolve by merging objects)] :
    1. [Xつのオブジェクトをマージして解決 (Resolve by Merging X Objects)] をクリックします。

2. [確認 (Confirm)] をクリックします。
- [名前の変更 (Rename)] :
    1. [名前の変更 (Rename)] をクリックします。
    2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm)] をクリックします。
  - [オーバーライドへの変換 (Convert to Overrides)] (不整合のある共有オブジェクトの場合) : 共有オブジェクトをオーバーライドと比較する場合、比較パネルには、[不整合のある値 (Inconsistent Values)] フィールドのデフォルト値のみが表示されます。
    1. [オーバーライドへの変換 (Convert to Overrides)] をクリックします。すべての不整合オブジェクトは、オーバーライドを持つ単一の共有オブジェクトに変換されます。
    2. [確認 (Confirm)] をクリックします。[共有オブジェクトの編集 (Edit Shared Object)] をクリックすると、新しく形成されたオブジェクトの詳細が表示されます。上向き矢印と下向き矢印を使用して、デフォルトとオーバーライドの間で値を移動することができます。
  - [追加の値への変換 (Convert to Additional Values)] (不整合のあるネットワークグループの場合) :
    1. [追加の値への変換 (Convert to Additional Values)] をクリックします。すべての不整合オブジェクトは、追加の値を持つ単一の共有オブジェクトに変換されます。
    2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm)] をクリックします。

**ステップ 5** 不整合を解決したら、行った変更を今すぐ **レビューして展開する** か、待機してから複数の変更を一度に展開します。

## オブジェクトの問題を一度に解決する

未使用オブジェクトの問題の解決、重複オブジェクトの問題の解決、不整合オブジェクトの問題を解決する (38 ページ) の問題のあるオブジェクトを解決する方法の 1 つは、それらを見捨てることです。オブジェクトに複数の問題がある場合でも、複数のオブジェクトを選択して無視できます。たとえば、オブジェクトに一貫性がなく、さらに未使用の場合、一度に無視できる問題タイプは 1 つだけです。



**重要** 後でオブジェクトが別の問題タイプに関連付けられた場合も、実行した無視アクションは、その時に選択した問題にのみ影響します。たとえば、重複していたためにオブジェクトを見捨て、後でそのオブジェクトが不整合としてマークされた場合、そのオブジェクトを重複オブジェクトとして無視しても、不整合のオブジェクトとして無視されるわけではありません。

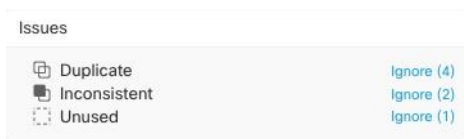


問題を一括で無視するには、以下の手順に従ってください。

手順

**ステップ 1** [オブジェクト (Objects) ]ページを開きます。検索を絞り込むために、オブジェクトの問題を [フィルタ処理](#) できます。

**ステップ 2** オブジェクトテーブルで、無視するオブジェクトをすべて選択します。問題ペインでは、問題タイプごとにオブジェクトがグループ化されます。



**ステップ 3** [無視 (Ignore) ]をクリックして、問題をタイプごとに無視します。各問題をタイプごとに無視する必要があります。

**ステップ 4** [OK] をクリックして、それらのオブジェクトを無視することを確認します。

## デバイスの接続状態

CDO テナントにオンボードされたデバイスの接続状態を表示できます。このトピックは、さまざまな接続状態を理解するのに役立ちます。[デバイスとサービス (Devices & Services) ]ページの [接続 (Connectivity) ] カラムに、デバイスの接続状態が表示されます。

デバイスの接続状態が「オンライン」の場合、デバイスの電源がオンになっていて、CDO に接続されていることを意味します。以下の表に記載されているその他の状態は、通常、さまざまな理由でデバイスに問題が発生した場合になります。この表は、このような問題から回復する方法を示しています。接続障害の原因となっている問題が複数ある可能性があります。再接続を試みると、CDO は、再接続を実行する前に、まずこれらの問題をすべて解決するように求めます。

デバイスの接続状態	考えられる原因	解像度
オンライン (Online)	デバイスの電源が入っていて、CDO に接続されています。	NA
オフライン	デバイスの電源が切れているか、ネットワーク接続が失われています。	デバイスがオフラインかどうかを確認します。
Insufficient licenses	デバイスに十分なライセンスがありません。	<a href="#">ライセンス不足のトラブルシューティング (43 ページ)</a>


デバイスの接続状態	考えられる原因	映像度
クレデンシャルが無効である	CDO がデバイスに接続するために使用するユーザー名とパスワードの組み合わせが正しくありません。	<a href="#">無効なログイン情報のトラブルシューティング (44 ページ)</a>
New Certificate Detected	このデバイスの証明書が変更されました。デバイスが自己署名証明書を使用している場合、これはデバイスの電源を再投入したために発生した可能性があります。	<a href="#">新規証明書の問題のトラブルシューティング (45 ページ)</a>
Device Unregistered	FTD デバイスが、FDM 経由でクラウドから登録解除されました。	<a href="#">登録解除されたデバイスのトラブルシューティング (3 ページ)</a>
Claim Error	CDO が FTD デバイスの要求に失敗しました。考えられる理由として、無効なシリアル番号が入力されたか、デバイスのシリアル番号がすでに要求されていることが考えられます。	<a href="#">要求エラー</a>
オンボーディングエラー	CDO がオンボーディング時にデバイスとの接続を失った可能性があります。	<a href="#">オンボーディングエラーのトラブルシューティング (54 ページ)</a>
Provisioning Error	FTD デバイスの初期プロビジョニングが失敗しました。	<a href="#">プロビジョニングエラー</a>
[到達不要 (Unreachable) ]	<ul style="list-style-type: none"> <li>• Device is powered down.</li> <li>• デバイスの IP アドレスが変更されました。</li> <li>• デバイスが Cisco Cloud から削除されました。</li> </ul>	<a href="#">到達不能の接続状態のトラブルシューティング (56 ページ)</a>

## 登録解除されたデバイスのトラブルシューティング

FTD デバイスが、FDM 経由でクラウドから登録解除されていることがあります。

以下の手順を実行して、デバイスをクラウドに再登録します。

## 手順

- 
- ステップ 1** [インベントリ (Inventory)] ページで [デバイス (Devices)] タブをクリックします。
- ステップ 2** [FTD] タブをクリックし、[デバイスの登録が解除されました (Device Unregistered)] 状態のデバイスを選択し、右側でエラーメッセージを確認します。
- ステップ 3** 登録解除されたデバイスが登録キーを使用してオンボーディングされた場合、以前に適用されたキーの有効期限が切れているため、CDO は新しい登録キーを生成するように求めます。
- [更新 (Refresh)] ボタンをクリックして新しい登録キーを生成し、コピーアイコン  をクリックします。
  - CDO に再登録する FTD の FDM にログインします。
  - [システム設定 (System Settings)] で、[クラウドサービス (Cloud Services)] をクリックします。
  - [Cisco Defense Orchestrator] 領域で、[始める (Get Started)] をクリックします。
  - [登録キー (Registration Key)] フィールドに、CDO で生成した登録キーを貼り付けます。
  - [登録 (Register)] をクリックし、[シスコの開示情報を受け入れる (Accept the Cisco Disclosure)] をクリックします。FDM が CDO に登録要求を送信します。
  - デバイスの接続状態が [読み取りエラー (Read Error)] に変わるまで、CDO の [インベントリ (Inventory)] ページを更新します。
  - CDO の [設定の読み取り (Read Configuration)] をクリックして、デバイスから設定を読み取ります。
- ステップ 4** 登録解除されたデバイスがシリアル番号を使用してオンボーディングされた場合、CDO は FDM からデバイスを自動登録するように求めます。
- CDO に再登録する FTD の FDM にログインします。
  - [システム設定 (System Settings)] で、[クラウドサービス (Cloud Services)] をクリックします。
  - [Cisco Defense Orchestrator からテナントへの自動登録 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)] オプションを選択して [登録 (Register)] をクリックします。
  - デバイスの接続状態が [読み取りエラー (Read Error)] に変わるまで、CDO の [インベントリ (Inventory)] ページを更新します。
  - CDO の [設定の読み取り (Read Configuration)] をクリックして、デバイスから設定を読み取ります。
- 

## ライセンス不足のトラブルシューティング

デバイスの接続ステータスに [ライセンスが不足しています (Insufficient License)] と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。

- デバイスのステータスが変わらない場合は、CDO からサインアウトしてから再度サインインすることでCDO ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の不具合を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。

#### 手順

---

- ステップ 1** Cisco Smart Software Manager から新しいトークンを生成し、コピーします。詳細については、[スマートライセンスの生成](#)に関するビデオをご覧ください。
- ステップ 2** CDO のナビゲーションバーで、[デバイスとサービス (Devices & Services)] ページをクリックします。
- ステップ 3** [デバイス] タブをクリックします。
- ステップ 4** 適切なデバイスタイプのタブをクリックし、ステータスが [ライセンスが不足しています (Insufficient License)] のデバイスを選択します。
- ステップ 5** [デバイスの詳細 (Device Details)] ペインで、[ライセンスが不足しています (Insufficient License)] に表示される [ライセンスの管理 (Manage Licenses)] をクリックします。[ライセンスの管理 (Manage Licenses)] ウィンドウが表示されます。
- ステップ 6** [アクティブ化 (Activate)] フィールドで、新しいトークンを貼り付けて [デバイスの登録 (Register Device)] をクリックします。

トークンがデバイスに正常に適用されると、接続状態が [オンライン (Online)] に変わります。

---

## 無効なログイン情報のトラブルシューティング

無効なログイン情報によるデバイスの切断を解決するには、次の手順を実行します。

#### 手順

---

- ステップ 1** [デバイスとサービス (Devices & Services)] ページを開きます。
- ステップ 2** [デバイス] タブをクリックします。
- ステップ 3** 適切なデバイスタイプのタブをクリックし、ステータスが [無効なログイン情報 (Invalid Credentials)] のデバイスを選択します。
- ステップ 4** [デバイスの詳細 (Device Details)] ペインで、[無効なログイン情報 (Invalid Credentials)] に表示される [再接続 (Reconnect)] をクリックします。CDO がデバイスとの再接続を試行します。
- ステップ 5** デバイスの新しいユーザー名とパスワードの入力を求められたら、
- ステップ 6** [続行 (Continue)] をクリックします。

- ステップ7** デバイスがオンラインになり、使用できる状態となったら、[閉じる (Close)] をクリックします。
- ステップ8** CDO がデバイスへの接続に誤った間違っただログイン情報を使用しようとしたため、デバイスへの接続に CDO が使用するユーザー名とパスワードの組み合わせが、デバイス上で直接変更された可能性があります。デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました (Conflict Detected)] であることがわかります。[構成の競合の解決 (Resolve Configuration Conflicts)] を使用して、CDO とデバイス間の構成の差異を確認して解決します。  
[設定の競合の解決](#)

## 新規証明書の問題のトラブルシューティング

### CDO での証明書の使用

CDO は、デバイスに接続するときに証明書の有効性をチェックします。具体的には、CDO は次のことを要求します。

1. デバイスで TLS バージョン 1.0 以降を使用している。
2. デバイスにより提示される証明書が有効期限内であり、発効日が過去の日付である（すなわち、すでに有効になっており、後日に有効化されるようにスケジューリングされていない）。
3. 証明書は、SHA-256 証明書であること。SHA-1 証明書は受け入れられません。
4. 次のいずれかが該当すること。
  - デバイスは自己署名証明書を使用し、その証明書は認可されたユーザーにより信頼された最新の証明書と同じである。
  - デバイスは、信頼できる認証局 (CA) が署名した証明書を使用し、提示されたリーフ証明書から関連 CA にリンクしている証明書チェーンを形成している。

これらは、ブラウザとは異なる CDO の証明書の使用方法です。

- 自己署名証明書の場合、CDO は、デバイスのオンボーディングまたは再接続時に、ドメイン名チェックを無効にして、代わりに、その証明書が承認ユーザーによって信頼された証明書と完全に一致することをチェックします。
- CDO は、まだ内部 CA をサポートしていません。現時点では、内部 CA によって署名された証明書をチェックする方法はありません。

ASA デバイスの証明書チェックを、デバイスごとに無効にすることができます。ASA の証明書を CDO が信頼できない場合、そのデバイスの証明書チェックを無効にするオプションがあります。デバイスの証明書チェックの無効化を試みても依然としてデバイスをオンボードできない場合は、デバイスに関して指定した IP アドレスおよびポートが正しくないか到達可能ではない可能性があります。証明書チェックをグローバルに無効にする方法、またはサポートされている証明書を持つデバイスの証明書チェックを無効にする方法はありません。非 ASA デバイスの証明書チェックを無効にする方法はありません。

デバイスの証明書チェックを無効にしても、CDO は、引き続き TLS を使用してデバイスに接続しますが、接続の確立に使用される証明書を検証しません。つまり、パッシブ中間者攻撃者は接続を盗聴できませんが、アクティブ中間攻撃者は、無効な証明書を CDO に提供することによって、接続を傍受する可能性があります。

### 証明書の問題の特定

いくつかの理由で CDO がデバイスをオンボードできない場合があります。UI に「CDO cannot connect to the device using the certificate presented」というメッセージが表示される場合は、証明書に問題があります。このメッセージが UI に表示されない場合は、問題が接続の問題(デバイスに到達できない)またはその他のネットワークエラーに関連している可能性が高くなります。

CDO が特定の証明書を拒否する理由を判断するには、SDC ホスト、または関連デバイスに到達できる別のホストで、`openssl` コマンドラインツールを使用します。次のコマンドを使用して、デバイスによって提示された証明書を示すファイルを作成します。

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

このコマンドでは、対話型セッションが開始されるため、数秒後に `Ctrl+C` キーを押して終了する必要があります。

次のような出力を含むファイルが作成されます。

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAKGA1UE
...lots of base64...
tzw9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdba0/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIx CzAJBgNVBAYTA1VT
...lots of base64...
tzw9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdba0/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDervmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjAlBOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
```

```

Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o].
0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[...eo..
0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.....3(
0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n.....c...c.d.6
0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "...:Y...!\...R(E.
0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
00a0 - 72 a4 ad
00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---

```

この出力では、最初に、**確認リターン (verify return)** コードが示されている最後の行に注目してください。証明書に関する問題が存在する場合、このリターンコードはゼロ以外になり、エラーの説明が表示されます。

この証明書エラーコードのリストを展開して、一般的なエラーとその修正方法を確認してください。

0 X509\_V\_OK : 操作が成功しました。

2 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT : 信頼できない証明書の発行者証明書が見つかりませんでした。

3 X509\_V\_ERR\_UNABLE\_TO\_GET\_CRL 証明書の CRL が見つかりませんでした。

4 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CERT\_SIGNATURE 証明書の署名を復号化できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。これは、RSA キーに対してのみ意味があります。

5 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CRL\_SIGNATURE CRL 署名を復号化できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。未使用。

- 6 X509\_V\_ERR\_UNABLE\_TO\_DECODE\_ISSUER\_PUBLIC\_KEY : 証明書 SubjectPublicKeyInfo の公開キーを読み取れませんでした。
- 7 X509\_V\_ERR\_CERT\_SIGNATURE\_FAILURE : 証明書の署名が無効です。
- 8 X509\_V\_ERR\_CRL\_SIGNATURE\_FAILURE : 証明書の署名が無効です。
- 9 X509\_V\_ERR\_CERT\_NOT\_YET\_VALID : 証明書がまだ有効ではありません (notBefore の日付が現在時刻より後です)。詳細については、この後の「[確認リターンコード : 9 \(証明書がまだ有効ではありません\)](#)」を参照してください。
- 10 X509\_V\_ERR\_CERT\_HAS\_EXPIRED : 証明書の有効期限が切れています (notAfter の日付が現在時刻より前です)。詳細については、この後の「[確認リターンコード : 10 \(証明書の有効期限が切れています\)](#)」を参照してください。
- 11 X509\_V\_ERR\_CRL\_NOT\_YET\_VALID : CRL がまだ有効ではありません。
- 12 X509\_V\_ERR\_CRL\_HAS\_EXPIRED : CRL の有効期限が切れています。
- 13 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_BEFORE\_FIELD : 証明書の notBefore フィールドに無効な時刻が含まれています。
- 14 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_AFTER\_FIELD : 証明書の notAfter フィールドに無効な時刻が含まれています。
- 15 X509\_V\_ERR\_ERROR\_IN\_CRL\_LAST\_UPDATE\_FIELD : CRL の lastUpdate フィールドに無効な時刻が含まれています。
- 16 X509\_V\_ERR\_ERROR\_IN\_CRL\_NEXT\_UPDATE\_FIELD : CRL の nextUpdate フィールドに無効な時刻が含まれています。
- 17 X509\_V\_ERR\_OUT\_OF\_MEM : メモリを割り当てようとしてエラーが発生しました。これは決して発生しないはずの問題です。
- 18 X509\_V\_ERR\_DEPTH\_ZERO\_SELF\_SIGNED\_CERT : 渡された証明書は自己署名済みであり、信頼できる証明書のリストに同じ証明書が見つかりません。
- 19 X509\_V\_ERR\_SELF\_SIGNED\_CERT\_IN\_CHAIN : 信頼できない証明書を使用して証明書チェーンを構築できましたが、ルートがローカルで見つかりませんでした。
- 20 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT\_LOCALLY : ローカルでルックアップされた証明書の発行者証明書が見つかりませんでした。これは、通常、信頼できる証明書のリストが完全ではないことを意味します。
- 21 X509\_V\_ERR\_UNABLE\_TO\_VERIFY\_LEAF\_SIGNATURE : チェーンに証明書が 1 つしか含まれておらず、それが自己署名済みでないため、署名を検証できませんでした。詳細については、この後の「[確認リターンコード : 21 \(最初の証明書を検証できません\)](#)」を参照してください。詳細については、この後の「[確認リターンコード : 21 \(最初の証明書を検証できません\)](#)」を参照してください。
- 22 X509\_V\_ERR\_CERT\_CHAIN\_TOO\_LONG : 証明書チェーンの長さが、指定された最大深度を超えています。未使用。
- 23 X509\_V\_ERR\_CERT\_REVOKED : 証明書が失効しています。



24 X509\_V\_ERR\_INVALID\_CA : CA 証明書が無効です。CA ではないか、その拡張領域が、提供された目的と一致していません。

25 X509\_V\_ERR\_PATH\_LENGTH\_EXCEEDED : basicConstraints の pathlength パラメータを超えています。

26 X509\_V\_ERR\_INVALID\_PURPOSE : 提供された証明書を、指定された目的に使用できません。

27 X509\_V\_ERR\_CERT\_UNTRUSTED : ルート CA が、指定された目的に関して信頼できるものとしてマークされていません。

28 X509\_V\_ERR\_CERT\_REJECTED : ルート CA が、指定された目的を拒否するようにマークされています。

29 X509\_V\_ERR\_SUBJECT\_ISSUER\_MISMATCH : 件名が現在の証明書の発行者名と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。

30 X509\_V\_ERR\_AKID\_SKID\_MISMATCH : 件名キー識別子が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。

31 X509\_V\_ERR\_AKID\_ISSUER\_SERIAL\_MISMATCH : 発行者名とシリアル番号が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer\_checks オプションが設定されている場合にのみ表示されます。

32 X509\_V\_ERR\_KEYUSAGE\_NO\_CERTSIGN : keyUsage 拡張領域が証明書の署名を許可していないため、現在の候補発行者証明書が拒否されました。

50 X509\_V\_ERR\_APPLICATION\_VERIFICATION : アプリケーション固有のエラーです。未使用。

### 新しい証明書が検出されました

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDOは、設定 (Configuration) ]ステータスおよび[接続 (Connectivity) ]の両方のステータスとして、「新しい証明書が検出されました (New Certificate Detected) 」メッセージを生成する場合があります。このデバイスを CDO から管理する前に、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



- (注) 複数の管理対象デバイスを CDO に同時に一括再接続すると、CDO は、デバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。

新しい証明書を解決するには、次の手順を使用します。

1. [デバイスとサービス (Device & Services) ] ページに移動します。

2. フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました (New Certificate Detected) ] であるデバイスを表示し、必要なデバイスを選択します。
3. [アクション (Action) ] ペインで、[証明書の確認 (Review Certificate) ] をクリックします。CDOでは、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
4. [デバイス同期 (Device Sync) ] ウィンドウで[承認 (Accept) ] をクリックするか、[デバイスへの再接続 (Reconnecting to Device) ] ウィンドウで[続行 (Continue) ] をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス (Devices & Services) ] ページを手動で更新する必要があります。

### 証明書エラーコード

**確認リターンコード : 0 (OK) (ただし、CDO は証明書エラーを返します)**

CDO は、証明書を取得すると、「https://<device\_ip>:<port>」への GET コールを実行することにより、デバイスの URL への接続を試みます。これが機能しない場合、CDO は証明書エラーを表示します。証明書が有効である (openssl が 0 つまり OK を返します) ことがわかった場合、接続しようとしているポートで別のサービスがリスンしている可能性があります。この場合、次のコマンドを使用できます。

```
curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

これにより、次のように、ASA と確実に通信しているかどうかを確認することができ、HTTPS サーバーが ASA の正しいポートで動作しているかどうかをチェックすることもできます。

```
# show asp table socket
```

Protocol	Socket	State	Local Address	Foreign Address
SSL	00019b98	LISTEN	192.168.1.5:443	0.0.0.0:*
SSL	00029e18	LISTEN	192.168.2.5:443	0.0.0.0:*
TCP	00032208	LISTEN	192.168.1.5:22	0.0.0.0:*

**確認リターンコード : 9 (証明書がまだ有効ではありません)**

このエラーは、提供された証明書の発行日が将来の日付であるため、クライアントがそれを有効なものとして扱わないことを意味します。これは、証明書の不完全な作成が原因である可能性があります。また、自己署名証明書の場合は、証明書生成時のデバイスの時刻が間違っていたことが原因である可能性があります。

エラーには、証明書の notBefore の日付が含まれた行があります。

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
```

```
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

このエラーから、証明書がいつ有効になるかを判別できます。

### 修復

証明書の `notBefore` の日付は過去の日付である必要があります。`notBefore` の日付をより早い日付にして証明書を再発行できます。この問題は、クライアントまたは発行デバイスのいずれかで時刻が正しく設定されていない場合にも発生する可能性があります。

### 確認リターンコード：10（証明書の有効期限が切れています）

このエラーは、提供された証明書の少なくとも1つが期限切れであることを意味します。エラーには、証明書の `notBefore` の日付が含まれた行があります。

```
error 10 at 0 depth lookup:certificate has expired
```

この有効期限は、証明書の本文に含まれています。

### 修復

証明書が本当に期限切れの場合、唯一の修復方法は、別の証明書を取得することです。証明書の有効期限が将来の日付であるのに、`openssl` が期限切れであると主張する場合は、コンピュータの日付と時刻をチェックしてください。たとえば、証明書が2020年に期限切れになるように設定されているのに、コンピュータの日付が2021年になっている場合、そのコンピュータは証明書を期限切れとして扱います。

### 確認リターンコード：21（最初の証明書を検証できません）

このエラーは、証明書チェーンに問題があり、デバイスによって提示された証明書が信頼できるものであることを `openssl` が検証できないことを示しています。ここで、上記の例の証明書チェーンを調べて、証明書チェーンがどのように機能するののかを見てみましょう。

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTALVT
....lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDFTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTALVT
....lots of base64...
```

```
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
```

証明書チェーンとは、サーバーによって提示される証明書のリストです。このリストは、サーバー自体の証明書から始まり、そのサーバーの証明書を認証局の最上位の証明書に結び付ける、段階的により上位の中間証明書が含まれます。各証明書には、その件名（「s:」で始まる行）とその発行者（「i:」で始まる行）のリストが表示されています。

件名は、証明書によって識別されるエンティティです。これには、組織名が含まれており、場合によっては証明書の発行先エンティティの共通名も含まれます。

発行者は、証明書を発行したエンティティです。これには、組織フィールドも含まれており、場合によっては共通名も含まれます。

サーバーは、信頼できる認証局によって直接発行された証明書を持っている場合、証明書チェーンに他の証明書を含める必要がありません。次のような1つの証明書が表示されます。

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdba0/Bf
-----END CERTIFICATE-----
```

この証明書を提供すると、**openssl** は、**\*.example.com** の ExampleCo 証明書が、**openssl** の組み込み信頼ストアに存在する信頼できる認証局の証明書によって正しく署名されていることを検証します。その検証の後に、**openssl** は、デバイスに正常に接続します。

ただし、ほとんどのサーバーには、信頼できる CA によって直接署名された証明書がありません。代わりに、最初の例のように、サーバーの証明書は1つ以上の中間証明書によって署名されており、最上位の中間証明書が、信頼できる CA によって署名された証明書を持ちます。**OpenSSL** は、デフォルトでは、これらの中間 CA を信頼せず、信頼できる CA で終わる完全な証明書チェーンが提供されている場合にのみ、それらを検証できます。

中間認証局によって署名された証明書を持つサーバーが、信頼できる CA にリンクするすべての証明書(すべての中間証明書を含む)を提供することが非常に重要です。このチェーン全体を提供しない場合、**openssl** からの出力は次のようになります。

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1
```

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1
```

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1
```

```
CONNECTED(00000003)
```

```
---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
```

```
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

この出力は、サーバーが1つの証明書のみを提供しており、提供された証明書が信頼されたルート認証局ではなく中間認証局によって署名されていることを示しています。出力には、特性検証エラーも表示されます。

### 修復

この問題は、デバイスによって提示された証明書の設定が間違っているために発生します。この問題を修正してCDOまたはその他のプログラムがデバイスに安全に接続できるようにする唯一の方法は、正しい証明書チェーンをデバイスにロードして、接続しているクライアントに完全な証明書チェーンを提示することです。

中間CAをトラストポイントに含めるには、次のいずれか（CSRがASAで生成されたかどうかに応じて）のリンク先に記載されている手順に従ってください。

- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-1.html#anc13>
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-1.html#anc15>

## 新しい証明書が検出されました

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDOは、設定（Configuration）]ステータスおよび[接続（Connectivity）]の両方のステータスとして、「新しい証明書が検出されました（New Certificate Detected）」メッセージを生成する場合があります。このデバイスを CDO から管理する前に、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



(注) 複数の管理対象デバイスを同時に **CDO に一括再接続**すると、CDO はデバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。

新しい証明書を解決するには、次の手順を使用します。

### 手順

- ステップ1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）]をクリックします。
- ステップ2 [デバイス]タブをクリックします。
- ステップ3 適切なデバイスタイプのタブをクリックします。
- ステップ4 フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました（New Certificate Detected）]であるデバイスを表示し、必要なデバイスを選択します。
- ステップ5 [アクション（Action）]ペインで、[証明書の確認（Review Certificate）]をクリックします。CDO では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
- ステップ6 [デバイス同期（Device Sync）]ウィンドウで[承認（Accept）]をクリックするか、[デバイスへの再接続（Reconnecting to Device）]ウィンドウで[続行（Continue）]をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス（Devices & Services）]ページを手動で更新する必要がある場合があります。

## オンボーディングエラーのトラブルシューティング

デバイスのオンボーディングエラーは、さまざまな理由で発生する可能性があります。次の操作を実行できます。

### 手順

- ステップ1 [インベントリ（Inventory）]ページで[デバイス（Devices）]タブをクリックします。

**ステップ2** 適切なデバイスタイプのタブをクリックし、エラーが発生しているデバイスを選択します。場合によっては、右側にエラーの説明が表示されます。説明に記載されている必要なアクションを実行します。

または

**ステップ3** CDO からデバイスインスタンスを削除し、デバイスのオンボーディングを再試行します。

## [競合検出 (Conflict Detected) ]ステータスの解決

CDO を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。[競合検出](#)が有効になっていて、CDO を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出 (Conflict Detected) ]と表示されます。

[競合検出 (Conflict Detected) ]ステータスを解決するには、次の手順に従います。

### 手順

**ステップ1** ナビゲーションバーで、[デバイスとサービス (Devices & Services) ]をクリックします。

**ステップ2** [デバイス (Devices) ]タブをクリックして、デバイスを見つけます。

**ステップ3** 適切なデバイスタイプのタブをクリックします。

**ステップ4** 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認 (Review Conflict) ]をクリックします。

**ステップ5** [デバイスの同期 (Device Sync) ]ページで、強調表示されている相違点を確認して、2つの設定を比較します。

- 「最後に認識されたデバイス設定 (Last Known Device Configuration) 」というラベルの付いたパネルは、CDO に保存されているデバイス設定です。
- 「デバイスで検出 (Found on Device) 」というラベルの付いたパネルは、ASA の実行コンフィギュレーションに保存されている設定です。

**ステップ6** 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認 (Accept Device changes) ]: 設定と、CDO に保存されている保留中の変更がデバイスの実行コンフィギュレーションで上書きされます。

(注) CDO はコマンドライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認 (Accept Without Review) ]です。

- [デバイスの変更を拒否 (Reject Device Changes) ]: デバイスに保存されている設定を CDO に保存されている設定で上書きします。

(注) 拒否または承認されたすべての設定変更は、変更ログに記録されます。

## 「未同期」ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。


### 手順

- ステップ1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ2 [デバイス (Devices)] タブをクリックしてデバイスを見つけるか、[テンプレート (Templates)] タブをクリックしてモデルデバイスを見つけます。
- ステップ3 適切なデバイスタイプのタブをクリックします。
- ステップ4 未同期と報告されたデバイスを選択します。
- ステップ5 右側の [未同期 (Not synced)] パネルで、次のいずれかを選択します。
  - [プレビューして展開... (Preview and Deploy..)] : 設定の変更を CDO からデバイスにプッシュする場合は、今行った変更を **プレビューして展開する** か、待ってから一度に複数の変更を展開します。
  - [変更の破棄 (Discard Changes)] : 設定の変更を CDO からデバイスにプッシュしたくない場合、または CDO で開始した設定の変更を「元に戻す」場合。このオプションは、CDO に保存されている設定を、デバイスに保存されている実行中の設定で上書きします。

## 到達不能の接続状態のトラブルシューティング

デバイスは、さまざまな理由で「到達不能」になる可能性があります。

### 手順

- ステップ1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ2 [デバイス (Devices)] タブをクリックして、デバイスを見つけます。
- ステップ3 適切なデバイスタイプのタブをクリックし、[到達不能 (Unreachable)] 状態のデバイスを選択します。
- ステップ4  [再接続 (Reconnect)] をクリックします。
- ステップ5 右側に表示されるメッセージに基づいて、次のいずれかのアクションを実行します。
  1. IP アドレスとデバイスログイン情報を使用して FTD デバイスをオンボードした場合、次のメッセージが表示されます。



「このデバイスには到達できません。IPアドレスとポートを確認してください」その後、メッセージボックスにデバイスの新しいIPアドレスまたは新しいポート情報を入力します。CDOが無効なIPアドレスに接続しようとしたため、デバイスのIPアドレスがデバイス上で直接変更された可能性があります。

(注) デバイスが再起動され、他に保留中の変更がない場合、デバイスはオンライン接続状態に戻ります。それ以上のアクションは必要ありません。

デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました (Conflict Detected) ] であることがわかります。[構成の競合の解決 (Resolve Configuration Conflicts) ] を使用して、CDO とデバイス間の構成の差異を確認して解決します。 [設定の競合の解決](#)

2. 登録トークンまたはシリアル番号を使用してFTDデバイスをオンボードしている場合、次のメッセージが表示されます。

「このデバイスは Cisco Cloud から削除されました。返品許可 (RMA) プロセスの一部として削除された可能性があります」。これは、RMA チームに返品された障害のあるデバイスが、RMA プロセスの一部として Cisco Cloud から削除されたことを意味します。

その結果、CDO でのデバイスの接続ステータスが「到達不能」となっています。

- RMA ケースの場合、CDO で次の手順を実行する必要があります。
    1. デバイスが正常にオンボードされた場合は、デバイス構成をテンプレートとして保存する必要があります。「[FTD テンプレートの設定](#)」を参照してください。  
CDO からデバイスインスタンスを削除します。
    2. RMA チームから受け取った新しい交換用デバイスの電源を入れ、CDOにオンボードします。「[デバイスのシリアル番号を使用したFTDの導入準備](#)」を参照してください。
- 重要** 交換用デバイスのシリアル番号は異なる可能性が高いため、新しいデバイスとしてオンボードする必要があります。

デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました (Conflict Detected) ] であることがわかります。

3. [構成の競合の解決 (Resolve Configuration Conflicts) ] を使用して、CDO とデバイス間の構成の差異を確認して解決します。 [設定の競合の解決](#)  
以前に保存したテンプレートを新しいデバイスに適用します。「[FTD テンプレートの適用](#)」を参照してください。
- デバイスを売却した場合、またはデバイスの構成を消去せずにテナントの外部の別のユーザーに所有権を譲渡した場合、デバイスの所有者ではなくなります。このエラーは、購入者がデバイスのイメージを再作成したときに発生します。デバイスが前もつ

て正しく構成されて同期されている場合は、デバイス構成をテンプレートとして保存し、その後でデバイスインスタンスを CDO から削除できます。

## SecureX のトラブルシューティング

SecureX と組み合わせて CDO を使用しようとする時、エラーや警告が表示されたり、問題が発生したりする場合があります。SecureX UI に表示される問題については、SecureX のマニュアルを参照する必要があります。詳細については、SecureX の [Support](#) を参照してください。

CDO 内の SecureX リボン機能、または SecureX リボンへのテナントアクセシビリティに関するケースを開くには、[CDO Cisco TAC](#) を参照してください。テナント ID の入力を求められる場合があります。

### SecureX UI のトラブルシューティング

#### SecureX ダッシュボードに重複した CDO モジュールが表示される

SecureX では、単一製品の複数のモジュールを手動で設定できます。たとえば、複数の CDO テナントがある場合、テナントごとに 1 つの CDO モジュールを作成できます。重複モジュールは、同じ CDO テナントからの 2 つの異なる API トークンがあることを意味します。この冗長性により、混乱が生じ、ダッシュボードが乱雑になる可能性があります。

SecureX で CDO モジュールを手動で設定し、CDO の [一般設定 (General Settings)] ページで [SecureX に接続 (Connect SecureX)] を選択した場合、1 つのテナントが SecureX に複数のモジュールを持つ可能性があります。

回避策として、SecureX から元の CDO モジュールを削除し、複製したモジュールで CDO のパフォーマンスの監視を続けることをお勧めします。このモジュールは、より安全で、SecureX リボンと互換性のある、より堅牢な API トークンを使用して生成されます。

### CDO UI のトラブルシューティング

SecureX 内の CDO モジュールに関するケースを開く場合、詳細については、SecureX の [Terms](#)、[Privacy](#)、[Support](#) の「サポート」セクションを参照してください。

#### OAuth エラー

メッセージ「ユーザーは必要なすべてのスコープまたは十分な権限を持っていないようです (The user does not seem to have all the required scopes or sufficient privilege)」が表示されて、OAuth エラーが発生する場合があります。この問題が発生した場合は、次の可能性を検討してください。

- アカウントがアクティブ化されていない可能性。<https://visibility.test.iroh.site/> を参照し、登録したメールアドレスを使用して、アカウントがアクティブ化されているか確認します。アカウントがアクティブ化されていない場合、CDO アカウントは SecureX とマージされ

ない可能性があります。この問題を解決するには、Cisco TACに連絡する必要があります。詳細については、[Contact Cisco TAC](#)を参照してください。

#### 組織の間違ったログイン情報で SecureX にログインしている

[一般設定 (General Settings)] ページの [テナント設定 (Tenant Settings)] セクションで [SecureX に接続 (Connect SecureX)] オプションを使用して CDO イベントを SecureX に送信することを選択したが、間違ったログイン情報を使用して SecureX にログインした場合、間違ったテナントからのイベントが SecureX ダッシュボードに表示されることがあります。

回避策として、CDO の [一般設定 (General Settings)] ページで [SecureX の切断 (Disconnect SecureX)] をクリックします。SecureX 組織、つまり SecureX ダッシュボードとの情報の送受信に使用される読み取り専用 API ユーザーが終了します。

次に、[テナントを SecureX に接続 (Connect Tenant to SecureX)] を再度有効にし、SecureX へのログインを求められたら、正しい組織のログイン情報を使用する必要があります。

#### 間違ったアカウントでリボンにログインしている

現時点では、間違ったアカウント情報でリボンにログインすると、リボンからログアウトできません。リボンのログインを手動でリセットするには、[Support Case Manager](#) でケースを開く必要があります。

#### SecureX リボンを起動できない

適切なスコープにアクセスできない可能性があります。この問題を解決するには、Cisco TACに連絡する必要があります。詳細については、[Contact Cisco TAC](#)を参照してください。

SecureX リボンの動作の詳細については、[SecureX ribbon documentation](#)を参照してください。

