



# 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。

- [Secure Device Connector のトラブルシュート](#) (1 ページ)
- [CDO のトラブルシューティング](#) (5 ページ)
- [デバイスの接続状態](#) (9 ページ)
- [SecureX のトラブルシューティング](#) (23 ページ)

## Secure Device Connector のトラブルシュート

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 \(2 ページ\)](#)」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。

**ステップ 1** /opt/cdo/configure.log を確認します。ここには、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が表示されます。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](#)。

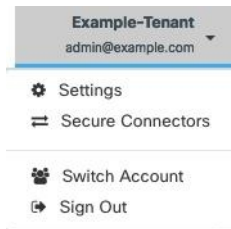
## SDC の変更した IP アドレスが CDO に反映されない

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。

**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 \(4 ページ\)](#)
  - [カスタム SDC ホストを更新する \(5 ページ\)](#)
  - [バグトラッキング \(5 ページ\)](#)

## 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。

**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](#)

# 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](#) にアクセスするか、[CDO (EU)] をクリックして [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

**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。

- 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 SSLALERT 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。

## 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。

## 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 (10 ページ)</a>
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 (11 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 (11 ページ)</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 (21 ページ)</a>

## 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。

**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。

- 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、使用できる状態になったら、[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ルされていない）。
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...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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+Y7mHhD8S
-----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:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FFBEBAB1B6

    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-----
MIID8DCCAtigAwIBAgIDAjqsMA0GCSqGSIb3DQEBCwUAMEIx CzAJBgNVBAYTA1VT
...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-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
...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...
tzw9TylihJpZc14qihFVTgFM7rMU2VHulpJgA59gdbaO/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
```

新しい証明書が検出されました

```

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

**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。

- 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。

- 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。

**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。

# 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、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。