

# トラブルシューティング

この章では、Security Cloud Control Firewall Management のさまざまなコンポーネントを使用するときに発生する可能性のあるエラーをトラブルシュートする方法について詳しく説明しています。


- Secure Device Connector のトラブルシュート （1 ページ）
- Security Cloud Control のトラブルシューティング, on page 12
- デバイスの接続状態, on page 14


# 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

Security Cloud Control 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。

Security Cloud Control 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 Security Cloud Control のホームページに表示されます。
- [サービス（Services）] 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 Security Cloud Control IP アドレスに到達できることを確認します。

   直接クラウド接続のインバウンドアクセスを許可を参照してください。

2. ハートビートを手動で要求して、Security Cloud Control 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. 左側のペインで、**管理（Administration）** > **統合（Integrations）** > **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）] ペインで、[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 Security Cloud Control で SDC ステータスが [Active] にならない （2 ページ）」の指示に従ってください。

   .

# 展開後 Security Cloud Control で SDC ステータスが [Active] にならない

展開して約 10 分たっても SDC がアクティブになったことを Security Cloud Control が示さない場合は、SDC の展開時に作成した `Security Cloud Control` ユーザーおよびパスワードにより、SSH を使用して SDC VM に接続します。

**Procedure**

**ステップ 1** Security Cloud Control で、アクティブと表示されていない SDC をクリックし、**[Request Heartbeat]** をクリックします。

**ステップ 2** 次のコマンドを使用して、コンテナが実行されていることを確認します。

```
docker ps
```

**ステップ 3** SDC ログを表示し、次のコマンドを使用してエラーを確認します。

```
sdc show logs
```

**ステップ 4** 次のコマンドを使用してコンテナを再起動します。

```
sdc restart
```

# SDC の変更された IP アドレスが Security Cloud Control に反映されない

SDC の更新された IP アドレスを表示するには、前述の手順を使用してハートビートを要求し、ブラウザを更新します。

### ハートビートの要求

Security Cloud Control で、アクティブと表示されていない SDC をクリックし、サイドバーで **[Request Heartbeat]**をクリックします。

1. 次のコマンドを使用してコンテナが実行されていることを確認します：`docker ps`
2. SDCログを表示し、`sdc show logs` コマンドを使用してエラーを確認します
3. 次のコマンドを使用してコンテナを再起動します：`sdc restart`

# 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 Security Cloud Control 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 Security Cloud Control 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。

### Procedure

**ステップ 1** Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

**ステップ 2** 左側のペインで **管理（Administration）** > **統合（Integrations）** > **Firewall Management Center** をクリックし、[セキュアコネクタ（Secure Connectors）] タブをクリックします。

**ステップ 3** SDC を選択します。

**ステップ 4** 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 5** 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。Security Cloud Control 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、Security Cloud Control 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 6** 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、Security Cloud Control サポートまでお問い合わせください。

# SDC との断続的な接続または接続がない

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、オンプレミスの SDC で、CentOS を引き続き使用している場合にのみ適用されます。

**症状**：SDC との断続的な接続または接続がない。

**診断**：この問題は、ディスク領域がほぼいっぱい（80% 以上）の場合に発生する可能性があります。

次の手順を実行して、ディスク容量の使用状況を確認します。

1. Secure Device Connector（SDC）VM のコンソールを開きます。
2. ユーザー名 **cdo** でログインします。
3. 初回ログイン時に作成したパスワードを入力します。
4. まず、**`df -h`** と入力して空きディスク容量をチェックし、空きディスク容量がないことを確認します。

   Docker によってディスク容量が消費されたことを確認できます。通常のディスク使用量は 2 ギガバイト未満であると予想されます。
5. **Docker** フォルダーのディスク使用量を表示するには、

   **`sudo du -h /var/lib/docker | sort -h`** を実行します。

   **Docker** フォルダーのディスク使用量を確認できます。

### 手順

Docker フォルダーのディスク使用量がほぼいっぱいの場合は、docker 設定ファイルで次のように定義します。

- Max-size：現在のファイルが最大サイズに達したら、ログローテーションを強制します。
- Max-file：上限に達したら、ローテーションされた余分なログファイルを削除します。

次の手順を実行します。

1. **sudo vi /etc/docker/daemon.json** を実行します。
2. 次の行をファイルに挿入します。

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. **Esc** キーを押してから **:wq!** と入力し、変更を書き込んでファイルを閉じます。

（注） **sudo cat /etc/docker/daemon.json** を実行して、ファイルに加えられた変更を確認できます。

4. **sudo systemctl restart docker** を実行して docker ファイルを再起動します。

   変更が適用されるまでに数分かかる場合があります。**sudo du -h /var/lib/docker | sort -h** を実行して、docker フォルダーの更新されたディスク使用量を表示します。
5. **df -h** を実行して、空きディスクサイズが増加したことを確認します。
6. SDC のステータスを [到達不能（Unreachable）] から [アクティブ（Active）] に変更する前に、**管理（Administration）** > **統合（Integrations）** > **Firewall Management Center** から [セキュアコネクタ（Secure Connectors）] タブに移動して、[アクション（Actions）] メニューから [再接続の要求（Request Reconnect）] をクリックする必要があります。

# 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 のシビラティ（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 Security Cloud Control ユーザーに影響します。

- Security Cloud Control 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 Security Cloud Control オペレーションズ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。
  - Security Cloud Control 標準の SDC ホストの更新 （6 ページ）
  - カスタム SDC ホストを更新する （7 ページ）

• バグトラッキング （7 ページ）

# Security Cloud Control 標準の SDC ホストの更新

- Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

  詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

  この手順は、まだ CentOS を使用している場合に適用されます。

- Security Cloud Control 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、Security Cloud Control 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

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- 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次第、アドバイザリを更新します。アドバイザリが最終とマークされたら、次の関連する Cisco バグを参照して詳細を確認できます。

CSCvo33929-CVE-2019-5736：runC コンテナのブレークアウト

# 無効なシステム時刻

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォールでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。

（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

- Security Cloud Control のオペレーションズチームが SDC を移行しようとしましたが、SDC システム時刻が AWS システム時刻より 15 分進んでいるか遅れていたため、移行できませんでした。

以下の手順を実行します。この問題が解決したら、移行を続行できます。

**手順**

**ステップ 1** VM 端末を介して、または SSH 接続を確立して、SDC VM にログインします。

**ステップ 2** プロンプトに `sudo sdc-onboard setup` と入力して、認証を行います。

**ステップ 3** SDC の初回セットアップ時と同様に、SDC セットアップに関する質問に回答します。以前と同じパスワードとネットワーク情報をすべて再入力します。このとき、NTP サーバーアドレスをメモしておきます。

a) SDC のセットアップに使用したものと同じパスワードを使用して、ルートおよび Security Cloud Control ユーザーのパスワードをリセットします。
b) プロンプトが表示されたら、**y** と入力してネットワークを再設定します。
c) 以前と同じ IP アドレスまたは CIDR の値を入力します。
d) 以前と同じネットワークゲートウェイの値を入力します。
e) 以前と同じドメインネームシステム（DNS）サーバーの値を入力します。
f) NTP サーバーの入力を求められたら、有効な NTP サーバーアドレス（`time.aws.com`など）を入力してください。
g) 入力した値を確認し、間違いなければ **y** と入力します。

**ステップ 4** プロンプトに `date` と入力して、時刻サーバーが到達可能か、SDC と同期しているかを検証します。日時（UTC）が表示され、SDC の時刻と比較できます。

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center （TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが SDC の新通信方式への移行を完了できます。

# SDC のバージョンが 202311**** より前

Secure Device Connector（SDC）は、これまでは CentOS 7 仮想マシンにインストールされていました。ただし、CentOS はサポート終了になり、Cisco Security Cloud Control のファイアウォー

ルでサポートされなくなるため、CentOS 7 から Ubuntu 仮想マシンにすべての SDC を移行することを推奨します。

詳細については、「オンプレミス Secure Device Connector および Secure Event Connector の CentOS 7 仮想マシンから Ubuntu 仮想マシンへの移行」を参照してください。

この手順は、まだ CentOS を使用している場合に適用されます。

- Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。



（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

- Security Cloud Control のオペレーションズチームは SDC を移行しようとしましたが、テナントが 202311**** よりも前のバージョンを実行しているため失敗しました。
- SDC の現在のバージョンは、Security Cloud Control のメニューバーから [Tools & Services] [Secure Connectors] の順に移動して、[Secure Connectors] ページに記載されています。**管理（Administration）** > **統合（Integrations）** > **セキュアコネクタ（Secure Connectors）** SDC を選択すると、画面右側の [詳細（Details）] ペインにバージョン番号が表示されます。

SDC バージョンをアップグレードするには、次の手順に従ってください。この問題が解決したら、Security Cloud Control オペレーションズチームが移行プロセスを再度実行できるようになります。

### 手順

**ステップ 1** SDC VM にログインし、認証を行います。

**ステップ 2** プロンプトに `sudo su - sdc` と入力して、認証を行います。

**ステップ 3** プロンプトに `crontab -r` と入力します。

`no crontab for sdc` というメッセージが表示された場合、無視して次の手順に進めます。

**ステップ 4** プロンプトに `./toolkit/toolkit.sh upgrade` と入力します。Security Cloud Control は、アップグレードが必要かどうかを判断し、ツールキットをアップグレードします。コンソールでエラーが報告されていないことを確認します。

**ステップ 5** SDC の新しいバージョンを確認します。

a) Security Cloud Control にログインします。

b) Security Cloud Control のメニューバーから**[ツールとサービス（Tools & Services）]** > **[セキュアコネクタ（Secure Connectors）]**の順に移動して、[セキュアコネクタ（Secure Connectors）] ページを開きます。

c) SDC を選択して、[操作（Actions）] ペインで [ハートビートの要求（Request Heartbeat）] をクリックします。

d) SDC のバージョンが 202311**** 以降であることを検証します。

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center （TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが移行プロセスを再度実行できます。

# AWS サーバーの証明書または接続エラー

Security Cloud Control は、Secure Device Connector（SDC）との新しい通信方式を採用します。そのため、Security Cloud Control は 2024 年 2 月 1 日までに既存の SDC を新しい通信方式に移行する必要があります。

（注） 2024 年 2 月 1 日までに SDC が移行されない場合、Security Cloud Control は SDC を介してデバイスと通信できなくなります。

Security Cloud Control のオペレーションズチームが SDC を移行しようとしましたが、接続の問題が発生したため失敗しました。

接続の問題を修正するには、次の手順に従ってください。この問題が解決したら、移行を続行できます。

### 手順

**ステップ 1** ポート 443 で、リージョン内のドメインへのアウトバウンドプロキシ接続を許可するファイアウォールルールを作成します。

- オーストラリアリージョンの実稼働テナント：
  - cognito-identity.ap-southeast-2.amazonaws.com
  - cognito-idp.ap-southeast-2.amazonaws.com
  - sns.ap-southeast-2.amazonaws.com
  - sqs.ap-southeast-2.amazonaws.com
- インドリージョンの実稼働テナント：
  - cognito-identity.ap-south-1.amazonaws.com
  - cognito-idp.ap-south-1.amazonaws.com
  - sns.ap-south-1.amazonaws.com
  - sqs.ap-south-1.amazonaws.com

- 米国リージョンの実稼働テナント：
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- EU リージョンの実稼働テナント：
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- APJ リージョンの実稼働テナント：
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

**ステップ 2** 次のいずれかのコマンドを使用して、ファイアウォールの「許可リスト」に追加する必要がある IP アドレスの全リストを確認できます。



（注） 次のコマンドは、**jq** がインストールされているユーザー向けです。IP アドレスが 1 つのリストに表示されます。

- 米国リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service
 == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- EU リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service
 == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- APJ リージョンの実稼働テナント：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service
 == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

（注） **jq** がインストールされていない場合は、次の短縮バージョンのコマンドを使用できます。

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

これらの手順が完了したら、またはエラーが発生した場合は、Cisco Technical Assistance Center （TAC）までご連絡ください。これらの手順が正常に完了すると、Security Cloud Control オペレーションズチームが SDC の新通信方式への移行を完了できます。

# Security Cloud Control のトラブルシューティング

## 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

**Procedure**

**ステップ 1** 左側のペインで **セキュリティデバイス** 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。

**a.** [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。

**b.** 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）]設定の競合の解決を確認し、Security Cloud Control とデバイス間の構成の差異を確認して解決します。

# 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。`

# 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、Security Cloud Control へのログインに失敗する

**解決法** Security Cloud Control にログインしようとして、知っている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 Security Cloud 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。新しい Cisco Security Cloud Sign On アカウントにサインアップする必要があります。

### Cisco Security Cloud Sign On ダッシュボードへのログインは成功するが、Security Cloud Control を起動できない

**解決法** Security Cloud Control テナントとは異なるユーザー名で Cisco Security Cloud Sign On アカウントを作成している可能性があります。Security Cloud Control 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。

### 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://security.cisco.com にログインします。

- **解決法** Cisco Secure Sign-On の新規アカウントを作成した場合は、テナントが作成されたリージョンに対応するダッシュボードの Security Cloud Control タイルをクリックします。
  - **解決法** Security Cloud Control APJ
  - **解決法** Security Cloud Control オーストラリア
  - **解決法** Security Cloud Control EU
  - **解決法** Security Cloud Control インド
  - **解決法** Security Cloud Control 米国
- **解決法** https://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

Security Cloud Control 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。**[Security Devices]** ページの **[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、Security Cloud Control 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、Security Cloud Control 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、Security Cloud Control 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。 | ライセンス不足のトラブルシュート, on page 16 |
| クレデンシャルが無効である | Security Cloud Control 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。 | 無効なログイン情報のトラブルシューティング, on page 16 |
| オンボーディング | デバイスのオンボーディングが開始されましたが、完了していません。 | デバイスの接続を確認し、デバイスの登録を完了させてください。 |
| 不明（Unknown） | デバイスのオンボーディングに失敗し、Security Cloud Control はデバイスの接続状態を取得できません。 | **セキュリティデバイス** ページでデバイスを選択し、右側のペインから **[Check for Changes]** を選択して、そのデバイスから最新の設定の取得を試みます。 |
| 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。 | 新規証明書の問題のトラブルシュート, on page 17 |
| オンボーディングエラー | Security Cloud Control 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。 | オンボーディングエラーのトラブルシュート, on page 27 |

# ライセンス不足のトラブルシュート

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、Security Cloud Control からサインアウトしてから再度サインインすることで Security Cloud Control 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。

**Procedure**

**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** 左側のペインで **セキュリティデバイス** 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。

**Procedure**

**ステップ 1** 左側のペインで **セキュリティデバイス** 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、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。Security Cloud Control は、デバイスとの再接続を試みます。

**ステップ 5** プロンプトが表示されたら、デバイスの新しいユーザー名とパスワードを入力します。

**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** Security Cloud Control がデバイスへの接続に誤った間違った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 Security Cloud Control 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、Security Cloud Control 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ト

### Security Cloud Control の証明書の使用

Security Cloud Control 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、Security Cloud Control 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 Security Cloud Control の証明書の使用方法です。

- 自己署名証明書の場合、Security Cloud Control 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。
- Security Cloud Control 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 Security Cloud Control 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、Security Cloud Control 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 Security Cloud Control 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 Security Cloud Control がデバイスをオンボードできない場合があります。UI に「Security Cloud Control は、提示された証明書を使用してデバイスに接続できません（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。

Security Cloud Control 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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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-----
---
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 キーについてのみ意味を持ちます。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE：CRL の署名を復号できませんでした。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。

### 「New Certificate Detected」メッセージ

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、Security Cloud Control で、[設定（Configuration）] ステータスと [接続（Connectivity）] ステータスの両方として、「新しい証明書が検出されました（New Certificate

Detected）」というメッセージが生成されることがあります。このデバイスを引き続き Security Cloud Control から管理するには、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。

**Note** 複数の管理対象デバイスを Security Cloud Control に同時に一括再接続すると、Security Cloud Control 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. 左側のペインで **セキュリティデバイス** をクリックします。
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. 操作ウィンドウで、[証明書の確認（Review Certificate）] をクリックします。Security Cloud Control 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。

   Security Cloud Control 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。 場合によっては、同期されたデバイスを表示するために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、Security Cloud Control は証明書エラーを返します）

Security Cloud Control 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、Security Cloud Control 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ッ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 つの期限が切れてい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ることと、デバイスによって提示された証明書を信頼できることを 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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/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 に結び付けられたすべての証明書（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。このチェーン全体が提供されない場合、openssl からの出力は次のようなものになります。

```
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。この出力には、特性検証エラーも示されています。

### 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 Security Cloud Control 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

## 「New Certificate Detected」メッセージ

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、Security Cloud Control で、[設定（Configuration）] ステータスと [接続（Connectivity）] ステータスの両方として、「新しい証明書が検出されました（New Certificate Detected）」というメッセージが生成されることがあります。このデバイスを引き続き Security Cloud Control から管理するには、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） デバイスの一括再接続により、複数の管理対象デバイスを Security Cloud Control に同時に再接続すると、Security Cloud Control 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** 左側のペインで **セキュリティデバイス** 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** 操作ウィンドウで、[証明書の確認（Review Certificate）] をクリックします。Security Cloud Control 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。

Security Cloud Control 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。 場合によっては、同期されたデバイスを表示するためにページを手動で更新する必要があります。

# オンボーディングエラーのトラブルシュート

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。

**Procedure**

**ステップ 1** 左側のペインで **セキュリティデバイス** 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** Security Cloud Control 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。

# 競合検出ステータスの解決

Security Cloud Control 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、Security Cloud Control 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。

**Procedure**

**ステップ 1** Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

**ステップ 2** **セキュリティデバイス**を選択します。

**Note** オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **Firewall Management Center** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

**ステップ 3** [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 4** 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 5** 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 6** [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、Security Cloud Control 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 7** 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、Security Cloud Control 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。

**Note** Security Cloud Control 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 Security Cloud Control に保存されている設定で上書きします。

**Note** 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。

**Procedure**

**ステップ 1** **セキュリティデバイス**を選択します。

**Note** オンプレミス Firewall Management Center の場合は、**管理（Administration）** > **統合（Integrations）** > **Firewall Management Center** をクリックして、[未同期（Not Synced）] 状態の FMC を選択し、ステップ 5 から続行します。

**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 Security Cloud Control 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 Security Cloud Control からデバイスに**プッシュしない**場合、または Security Cloud Control 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、Security Cloud Control 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構成で上書きします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。