macOSサービスのISEポスチャ条件の理解および設定

内容

はじめに

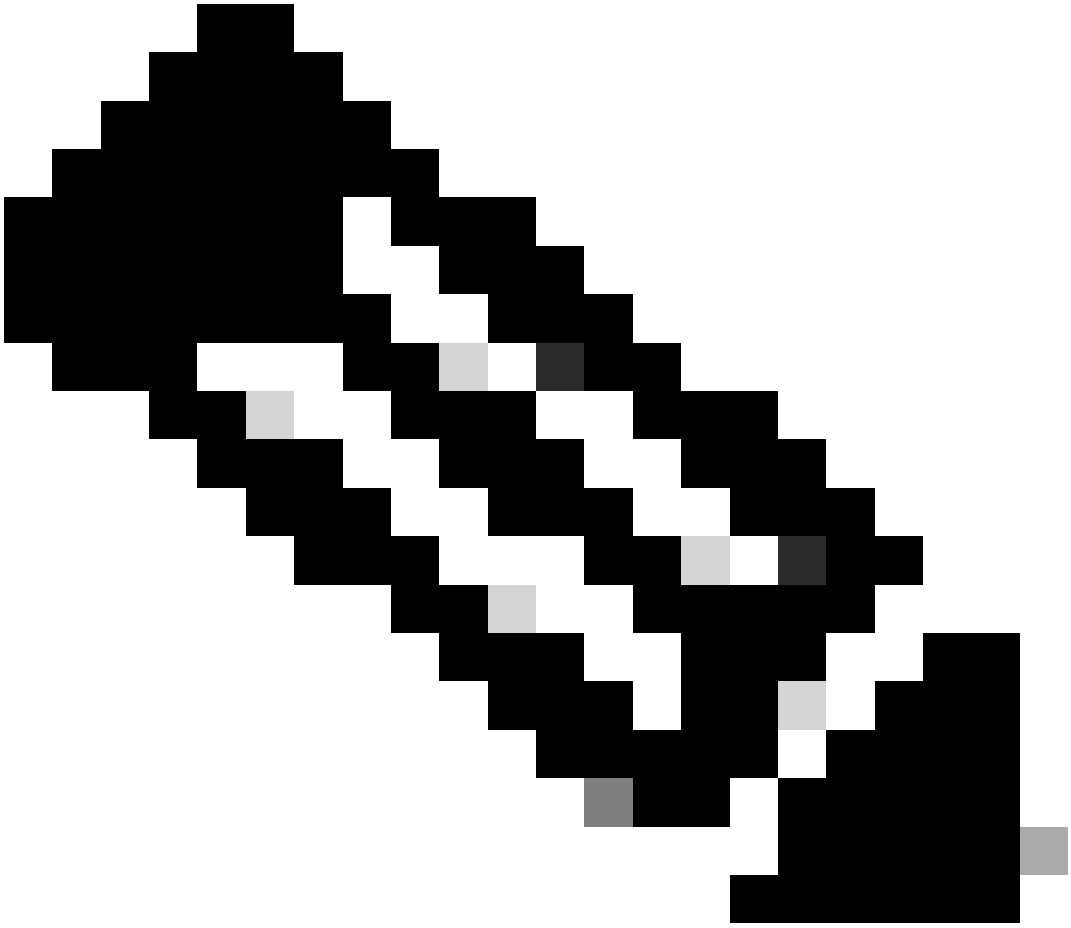
このドキュメントでは、Cisco ISEでmacOSサービス条件を設定するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- macOSに関する基礎知識
- ISEポスチャフローに関する知識



注：このドキュメントでは、macOSサービス条件の設定について説明します。初期ポスチャ設定については、このドキュメントでは説明しません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE 3.3パッチ1
- sonoma 14.3.1を実行するMacOSデバイス
- Cisco Secureクライアント5.1.2.42
- コンプライアンスモジュールバージョン4.3.3432.64000

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

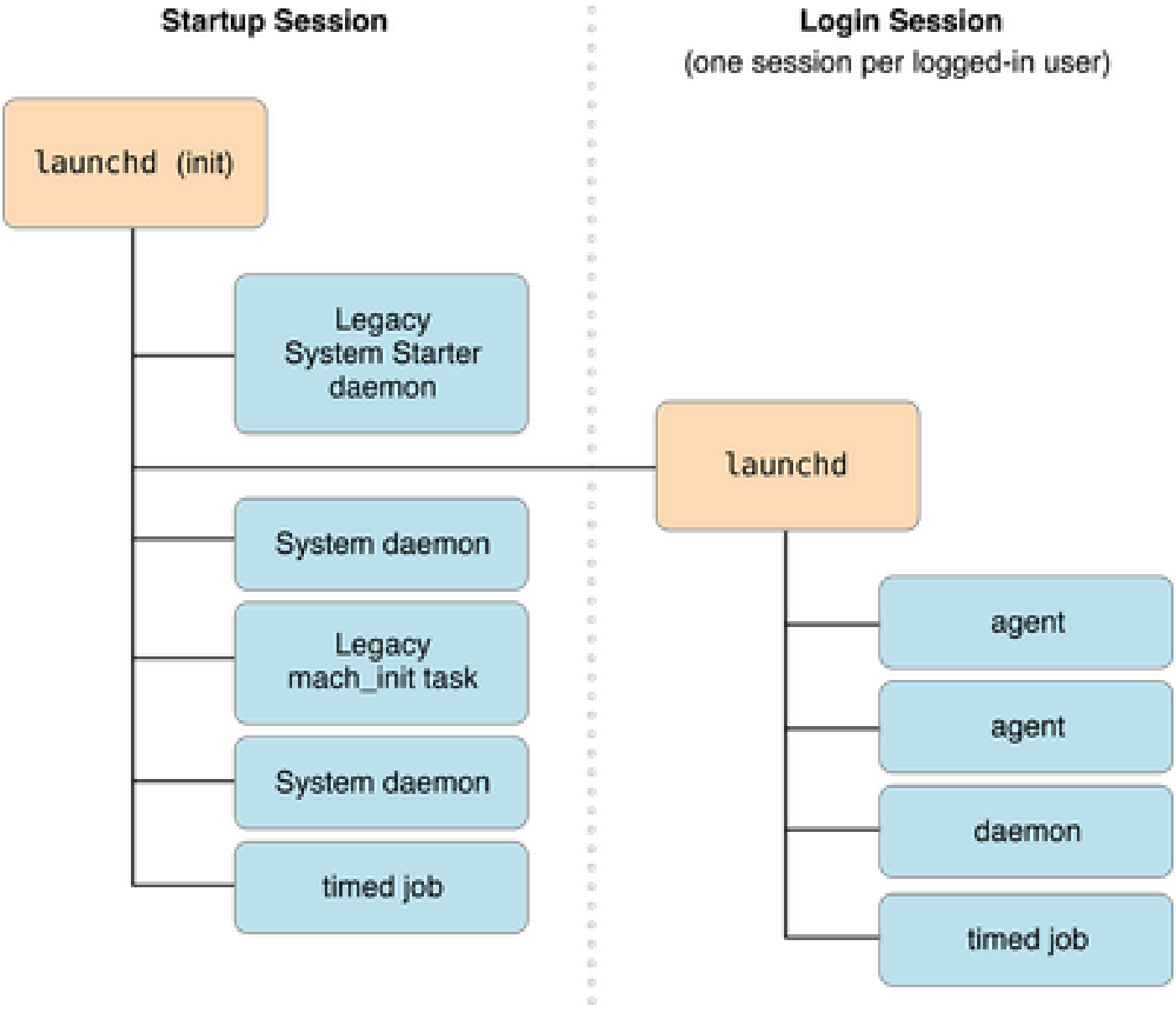
背景説明

macOSサービス条件は、サービスリクエストを使用して、サービスがmacOSデバイスにロードされているかどうかをチェックする必要がある場合に便利です。また、サービスが実行中かどうかをチェックすることもできます。 macOSのサービス条件では、デーモンとエージェントという2つの異なるサービスタイプをチェックできます。

デーモンは、システム全体の一部としてバックグラウンドで実行されるプログラムです（つまり、特定のユーザーに関連付けられません）。 デーモンはGUIを表示できません。具体的には、ウィンドウサーバへの接続は許可されていません。Webサーバはデーモンの完全な例です。

エージェントは、特定のユーザの代わりにバックグラウンドで実行されるプロセスです。エージェントは、ユーザのホームディレクトリへの確実なアクセスやウィンドウサーバへの接続など、デーモンが実行できないようなことを実行できるので便利です。エージェントの良い例として、カレンダー監視プログラムがあります。

次の図では、デバイスの起動とユーザのログインに基づいてそれぞれがどのようにロードされるかを確認できます。



デーモンおよびエージェントの詳細については、Appleのドキュメントを参照してください。

macOSデバイスで使用可能なデーモンとエージェントは、次の場所にあります。

場所	説明
~/ライブラリ/起動エージェント	ユーザが提供するユーザごとのエージェント。
/Library/LaunchAgents	管理者が提供するユーザごとのエージェント。
/Library/LaunchDaemons	管理者が提供するシステム全体のデーモン。
/System/Library/LaunchAgents	OS Xのユーザごとのエージェント

/System/Library/LaunchDaemons	OS Xシステム全体のデーモン

macOS端末から各カテゴリのリストを確認するには、次のコマンドを使用します。

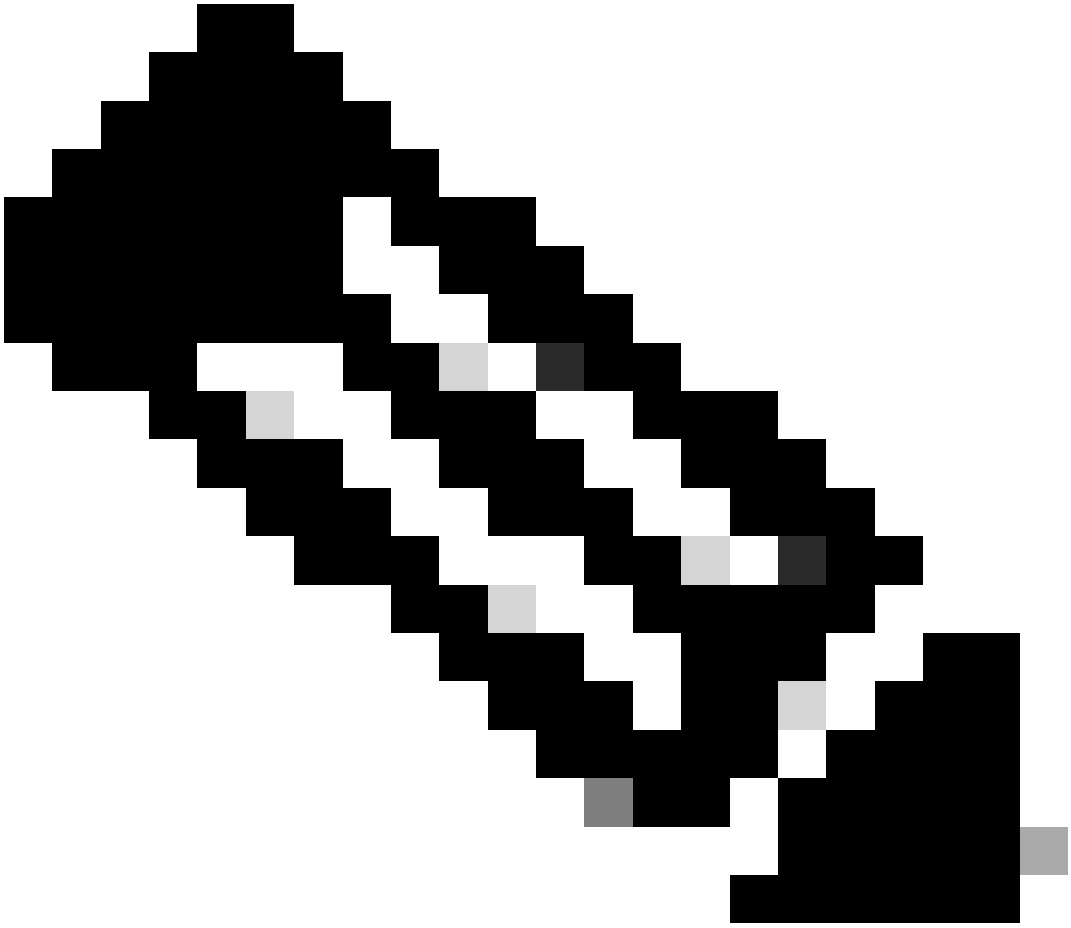
ls -ltr ~/Library/LaunchAgentsコマンド
ls -ltr /Library/LaunchAgentsコマンド
ls -ltr /Library/LaunchDaemons
ls -ltr / システム/ライブラリ/起動エージェント
ls -ltr /System/Library/LaunchDaemons

上記の場所には、macOSデバイスで使用可能なすべてのデーモンとエージェントが表示されますが、すべてがロードまたは実行されているわけではありません。

設定

macOSサービス条件の設定は、次の手順を使用して行うことができます。

1. チェックするサービス名を指定します。
2. （オプション）サービスの詳細を確認して、サービスがエージェントかデーモンかを定義します。
3. 評価するサービス演算子を選択します。
4. このような条件に対して、要件とポスチャポリシーを設定します。



注：サービスポスチャ条件が機能するには、昇格された特権が必要です。したがって、ISE PSNがCisco Secure Client（以前のAnyConnect）によって信頼されていることが必要です。『リファレンスガイド』を参照してください。

チェックするサービス名の識別

ISEポスチャコンプライアンスモジュールは、終了コードでロード、実行、ロード、および実行されたサービスを確認できます。

ロードされているサービスを確認するには、sudo launchctl dumpstateコマンドを使用します。

ロードされているサービスと終了コードを確認するには、sudo launchctl listコマンドを使用します。

上記のコマンドでは、多くの情報が突然表示される場合がありますが、実際のサービス名を表示するためだけに次のコマンドを使用します。

ロードされたサービス名だけを確認するには、次のコマンドを使用します。

```
sudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/|;s| = {$||'
```

ロードされ、終了コードが付いているサービス名だけを確認するには、次のコマンドを使用します。

```
sudo launchctl list | awk '{if (NR>1) print $3}'
```

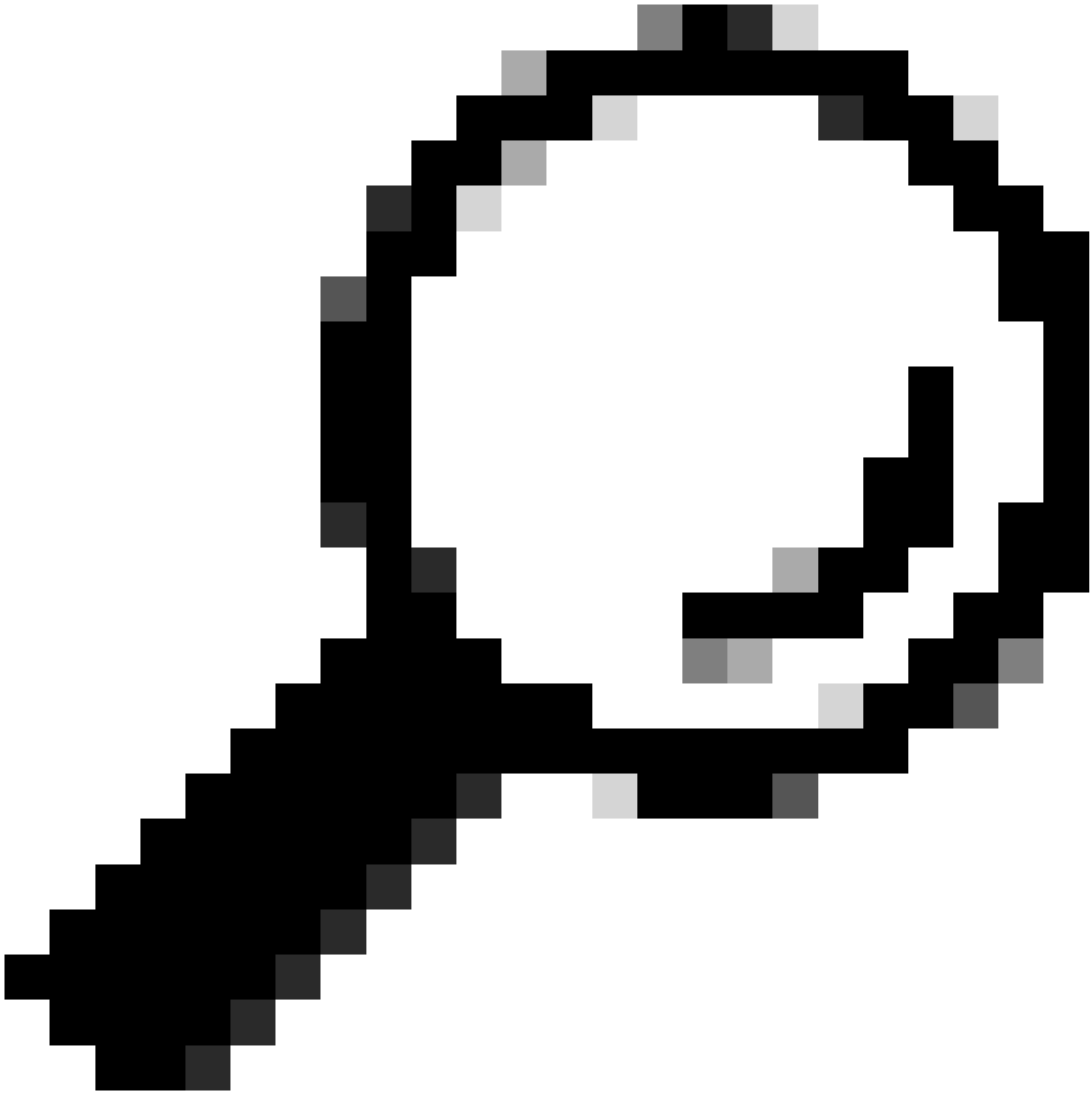
これらのコマンドは多くの情報を表示するため、各コマンドの最後に別のgrepフィルタを使用して探しているサービスを見つけることをお勧めします。
たとえば、ベンダー固有のサービスを検索する場合は、とのフィルタとしてキーワードを使用できます。

シスコサービスの場合、コマンドは次のようになります。

```
sudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/|;s| = {$||' | grep -i cisco
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i cisco
```

（オプション）サービスの詳細を確認して、サービスがエージェントであるかデーモンであるかを定義します

この条件の設定の2番目の部分では、サービスがデーモンタイプかエージェントタイプかを確認する必要があります。



ヒント:ISEではデーモンまたはユーザエージェントのオプションを選択できるため、この手順はオプションです。このオプションを選択してこの部分をスキップするだけです。

この状態で詳細を確認する場合は、次の手順を実行してタイプを確認できます。

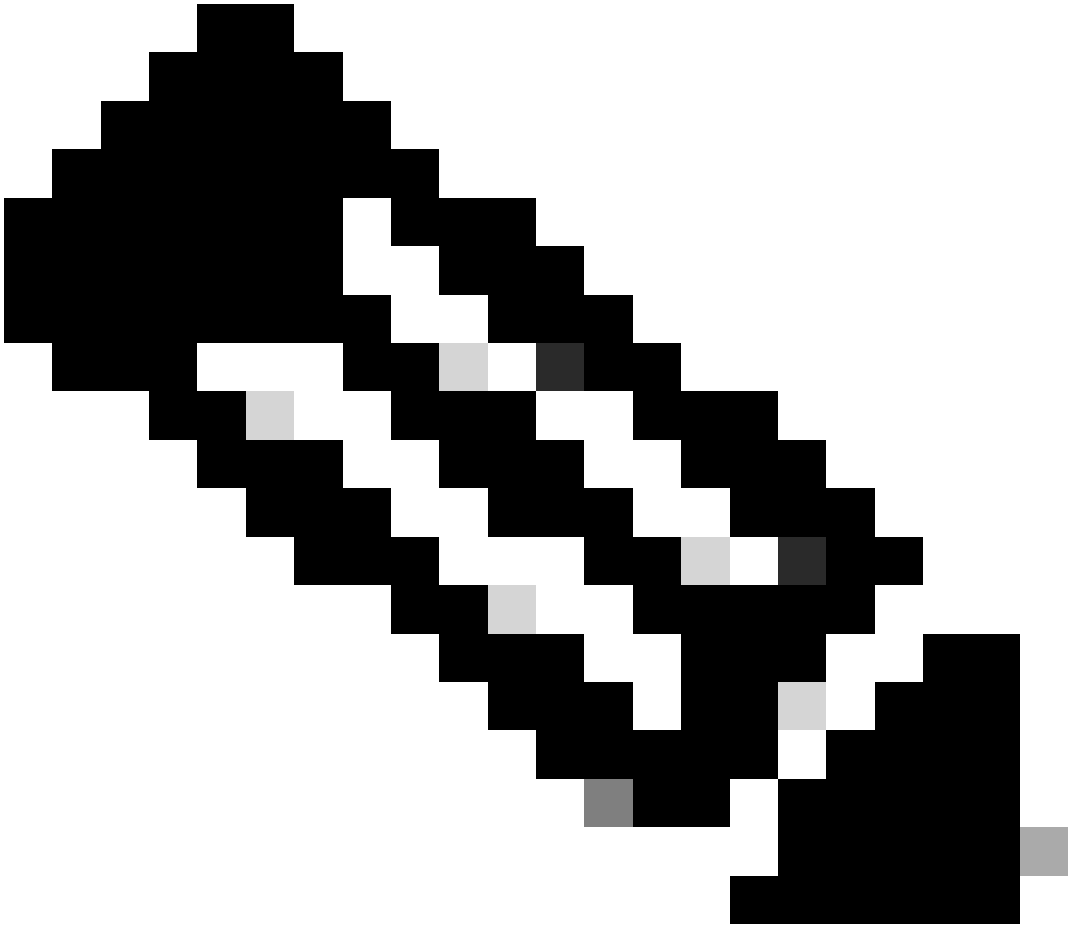
1. 最初に、コマンドsudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/|;s| = {$|' | grep -i {サービス名}

たとえば、sudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$/' | grep -i com.cisco.secureclient.isepostureコマンドの場合、出力はgui/501/com.cisco.secureclient.isepostureになります。

2. コマンドsudo launchctl print { Your launchctl service name } | grep -i 'type = Launch'を使用して、サービスタイプを確認します。

例に続き、コマンドsudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch'の場合、出力はtype = LaunchAgentです。

これは、サービスタイプが「Agent」であることを意味します。そうでない場合は、「type = LaunchDaemon」と表示されます。



注：情報が空の場合、サービスタイプの設定で、ISEのデーモンまたはユーザエージェントのオプションを選択します。

評価するサービス演算子の選択

ISEでは、次の5種類のサービスオペレータを選択できます。

- ロード済み
- ロードされていません
- ロード済みで実行中

- 終了コードで読み込まれました
- ロード済み、実行中、または終了コードあり

読み込まれたサービス

これら2つのコマンドを使用する際にリストされるサービスはすべて、

```
sudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/|;s| = {$||'
sudo launchctl list | awk '{if (NR>1) print $3}'
```

サービスがロードされていません

プロパティ・リスト(plist)が定義されているがロードされていないサービスや、プロパティ・リスト(plist)が定義されていないためにロードできないサービスがあります。

これらのサービスを特定するのは簡単ではなく、macOSデバイスに特定のサービスが存在しないことを確認する必要がある場合に最も一般的です。
たとえば、ズームサービスがmacOSデバイスにロードされないようにするには、サービスの値としてus.zoom.ZoomDaemonをここに指定します。こうすることで、ズームが実行されていないこと、またはまったくインストールされていないことを確認できます。

アンインストールできないサービスがあり、そのプロパティ一覧が定義されています。
たとえば、次のコマンドを使用すると、dhcp6d plistが定義されていることがわかります。

```
ls -ltr /System/Library/LaunchDaemons | grep com.apple.dhcp6d.plist
```

サービスリストを確認すると、がロードされていないことがわかります。

```
sudo grep -B 10 -A 10 -E "^\s*state = " <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/|;s| = {$||' | grep -i com.apple.dhcp6d
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i com.apple.dhcp6d
```

値をcom.apple.dhcp6d"に設定すると、サービスリストが定義されていてもサービスはロードされないため、macOSデバイスは準拠したものになります。

ロード済みで実行中

すべてのサービスが実行されているわけではありません。各サービスには、実行中、非実行中、待機中、終了済み、未初期化など、複数の状態があります。
実行中のすべてのサービスを確認するには、次のコマンドを使用します。

```
sudo grep -B 10 -A 10 -E "^\s*state = running" << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/|;s| = {$||'
```

上記のコマンドでリストされたサービスは、Loaded & Runningサービスオペレータ状態に該当します。

終了コードで読み込まれました

一部のサービスは、予期される終了コードまたは予期しない終了コードで終了する場合があります。このようなサービスは、次のコマンドでリストできます。

```
sudo grep -B 10 -A 10 "state = e" <<< "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//'
```

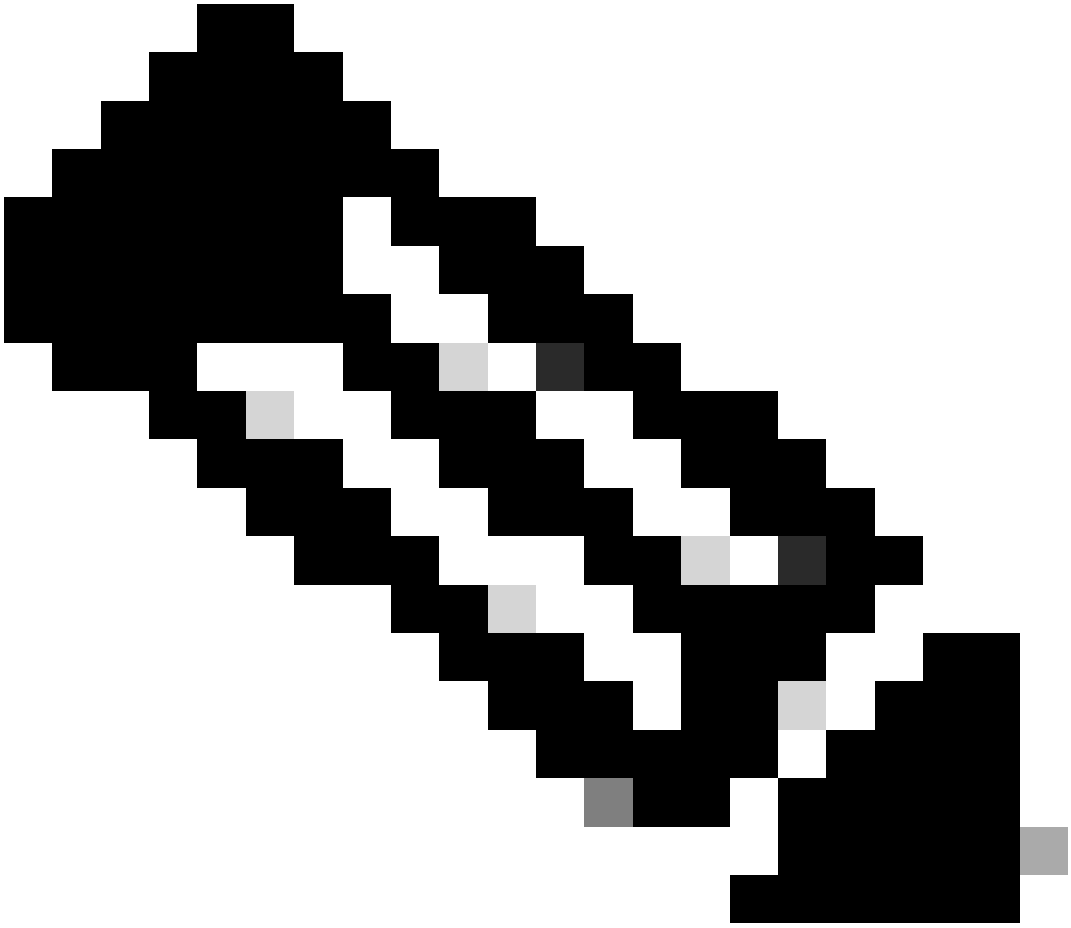
終了コードを確認するには、任意のサービスを選択して次のコマンドを使用します。

```
sudo launchctl print { Your launchctl service name } | grep -i 'last exit code'
```

例：

```
sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i 'last exit code'
```

出力は次のとおりです。last exit code = 0

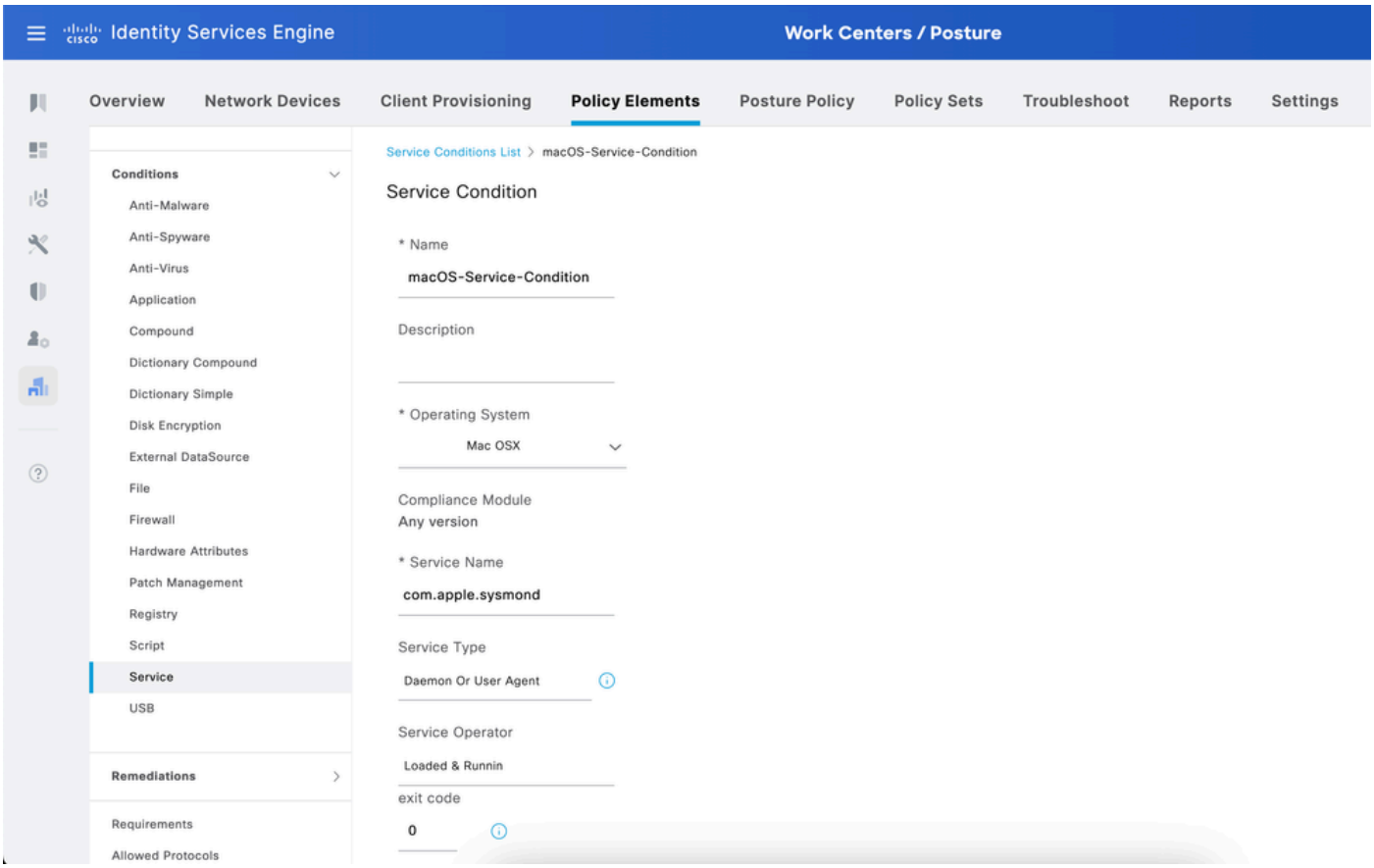


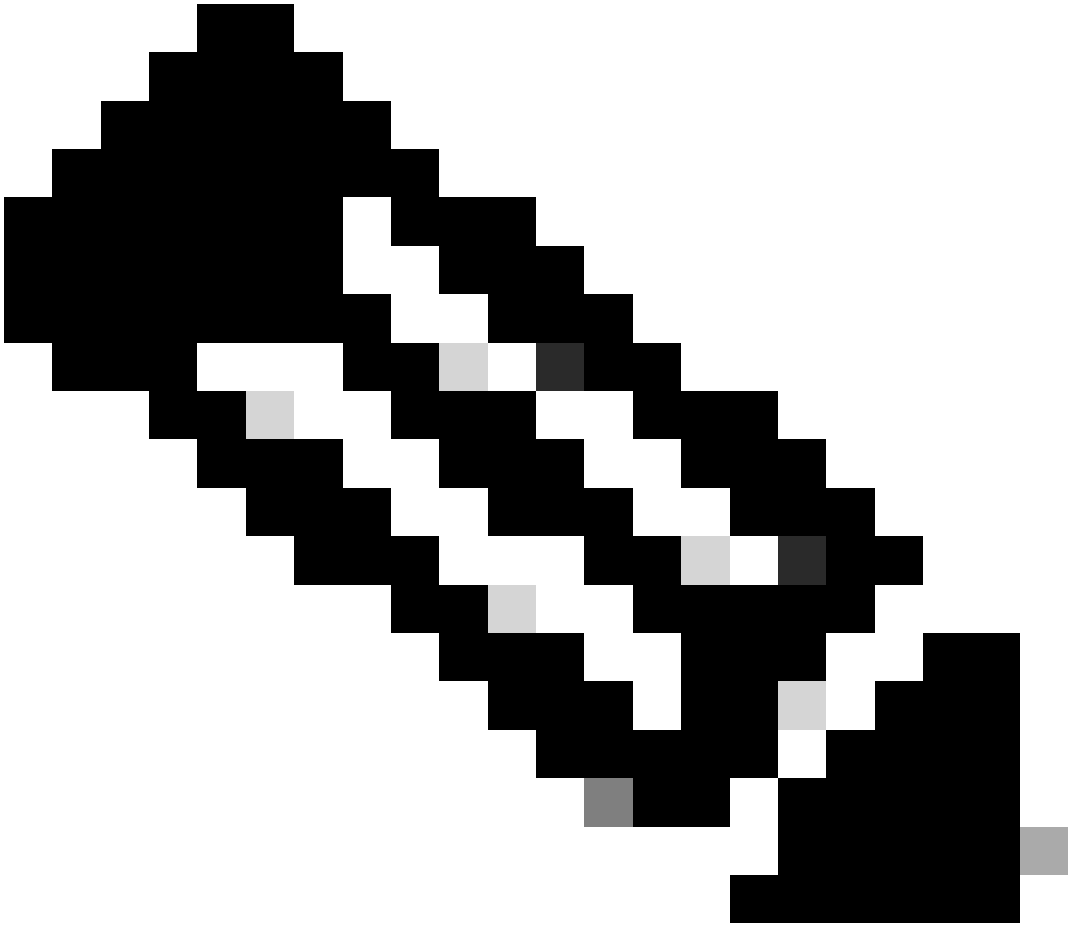
注：ここで終了コード0は、通常、すべての処理がサービスによって正しく行われたことを意味します。コンピュータが終了コードとして0に一致しない場合は、サービスが予期されたアクションを実行しなかったことを意味します。

ロード済み、実行中、または終了コードあり

この最後のオプションは、サービスがLoaded & RunningまたはLoaded with exit codeの場合に機能します。

次の図に、macOSサービス状態の例を示します。

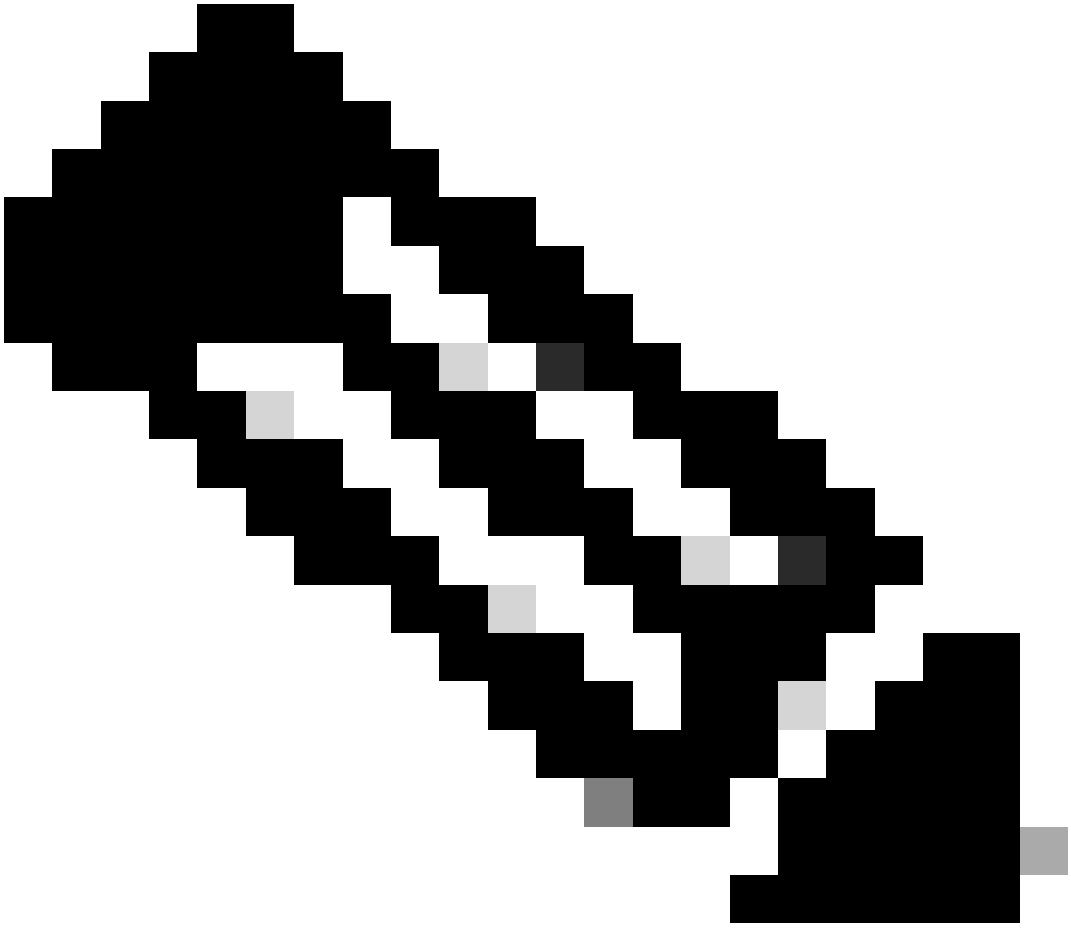

Identity Services Engine
Work Centers / Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall
Hardware Attributes
Patch Management
Registry
Script
Service
USB
Remediations
Requirements
Allowed Protocols
Service Conditions List > macOS-Service-Condition
Service Condition
* Name
macOS-Service-Condition
Description
* Operating System
Mac OSX
Compliance Module
Any version
* Service Name
com.apple.sysmond
Service Type
Daemon Or User Agent
Service Operator
Loaded & Runnin
exit code
0



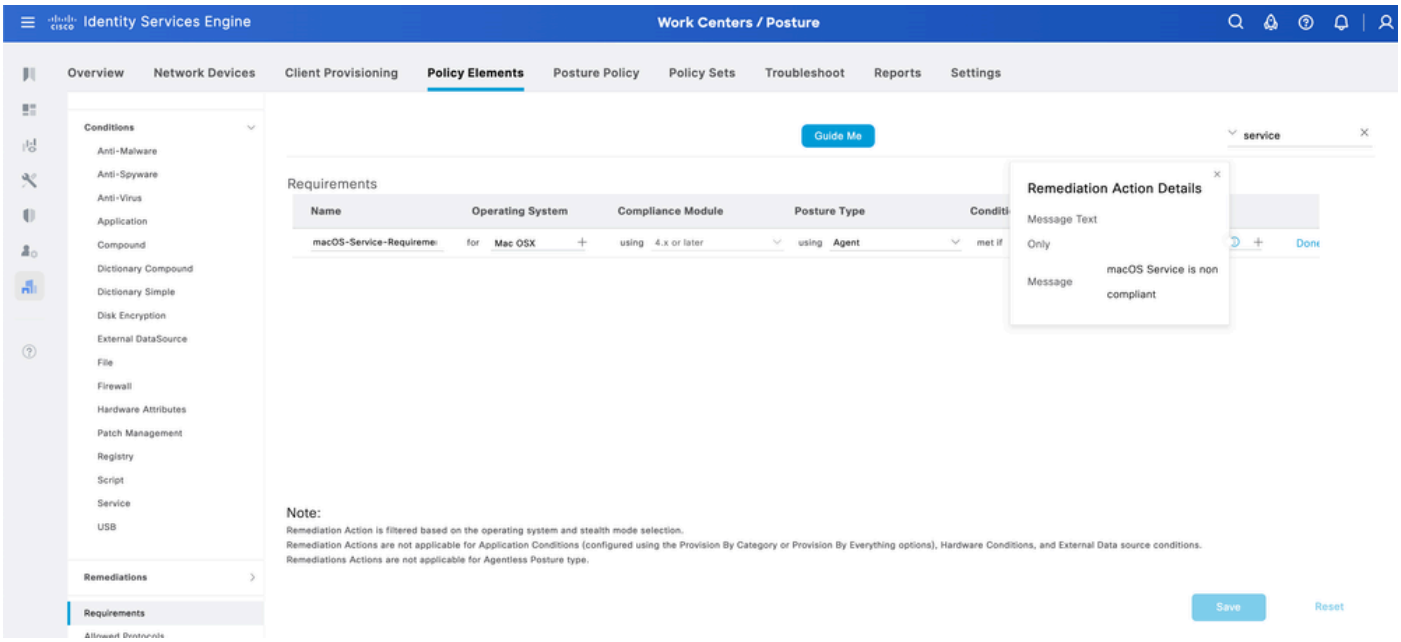
注：現在サポートされているのは、正確なサービス名だけです。サービス名でワイルドカードをサポートするための機能拡張要求があります。Cisco Bug ID CSCwf01373

このような条件に対する要件とポスチャポリシーの設定

条件を設定したら、その条件の要件を作成する必要があります。この要件に対してMessage Test Onlyオプションを使用します。
これを作成するには、ISE > Work Centers > Posture > Requirementsの順に移動します。

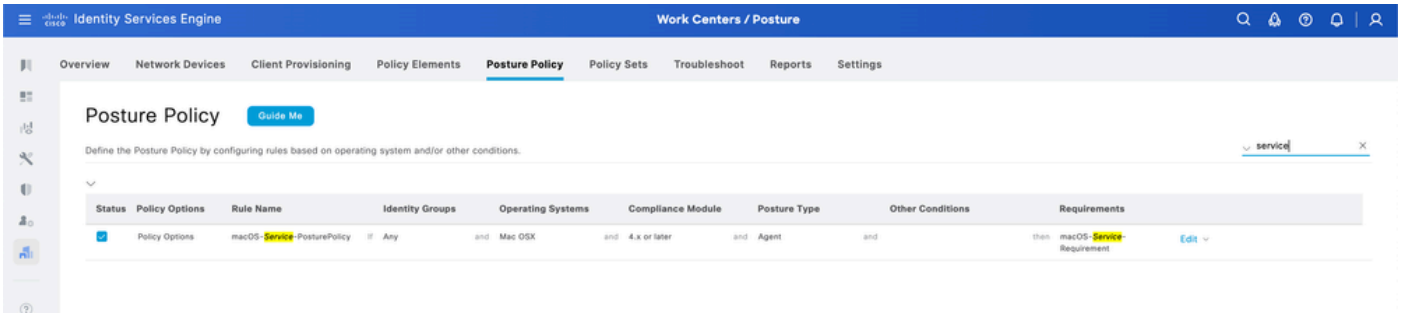


注：サービス条件に対する修正オプションはありません。



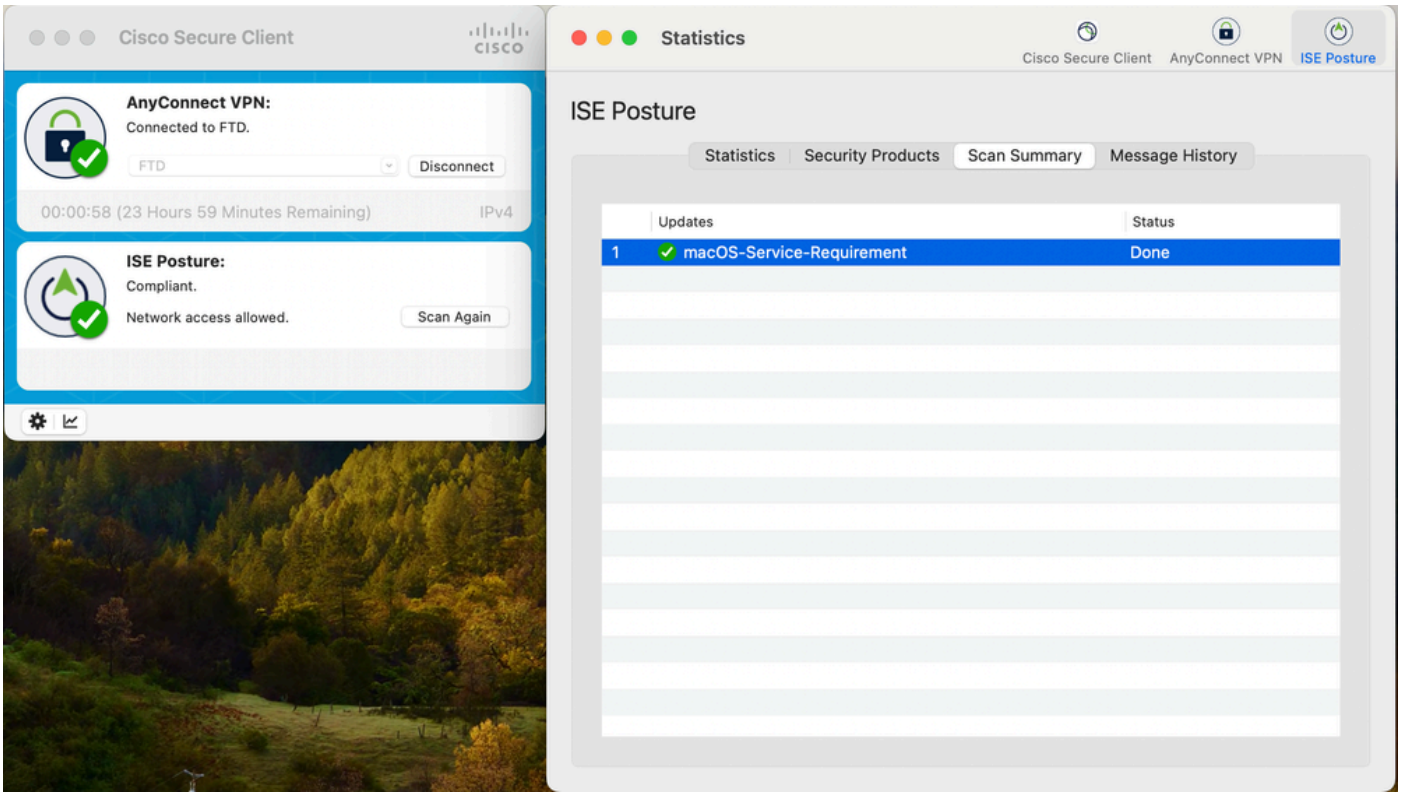
これが完了したら、最後のステップとして、作成された要件を使用するポスチャポリシーを設定します。
ISE > Work Centers > Posture > Posture Policyの順に移動し、ポリシーを作成します。

新しいポリシーを有効にし、必要な名前を付けて、作成した要件を選択します。

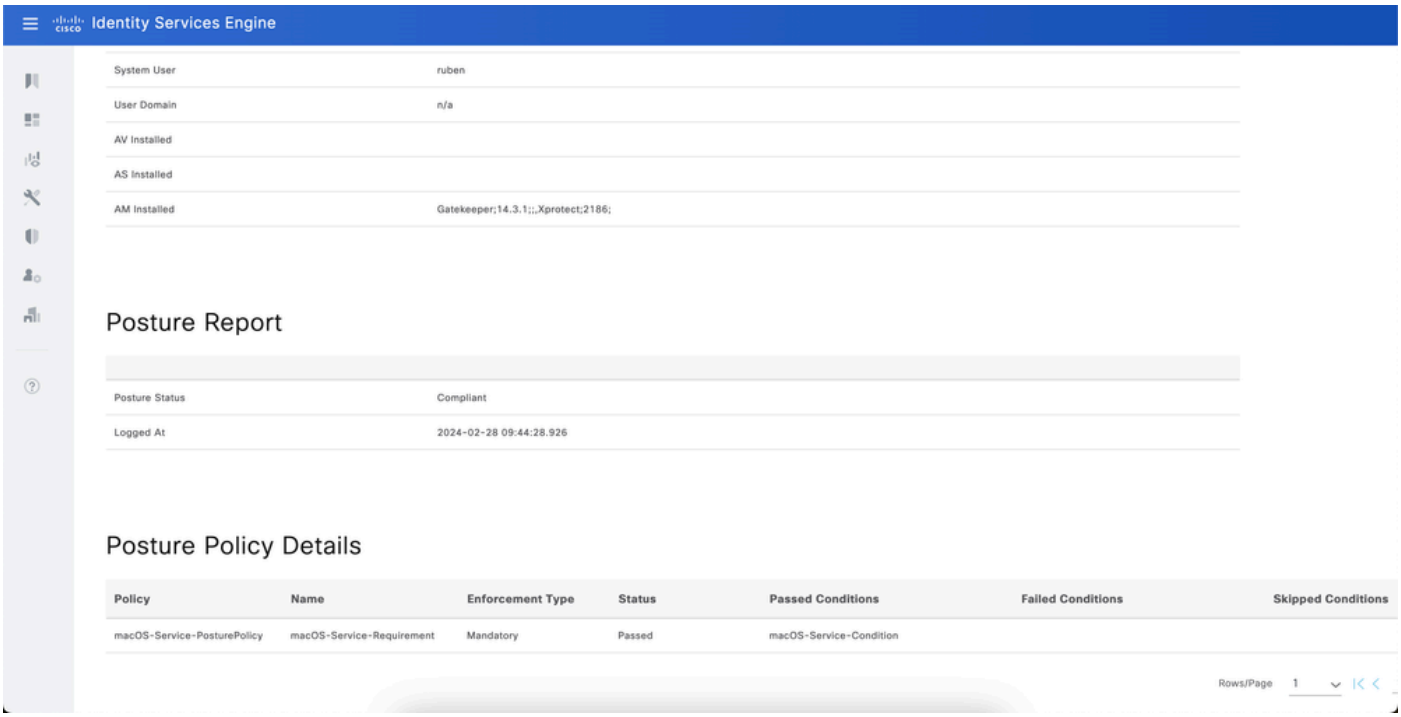


確認

Cisco Secure Client GUI自体から、macOSポスチャ条件が成功したか失敗したかを確認できます。



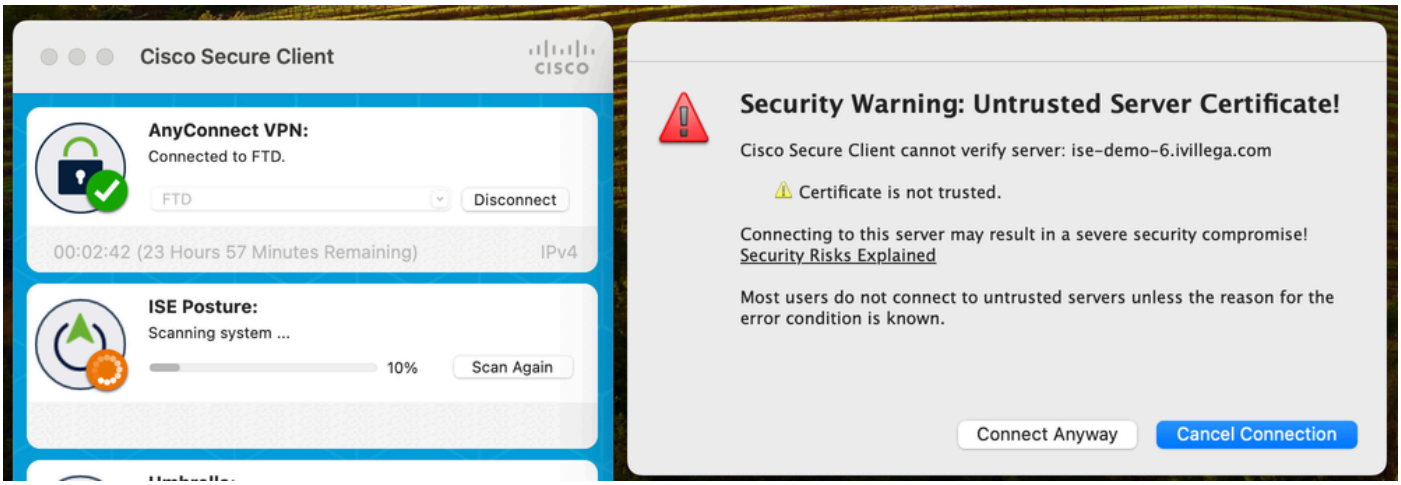
また、ISEポスチャレポートは、ISE > Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpointからも確認できます。



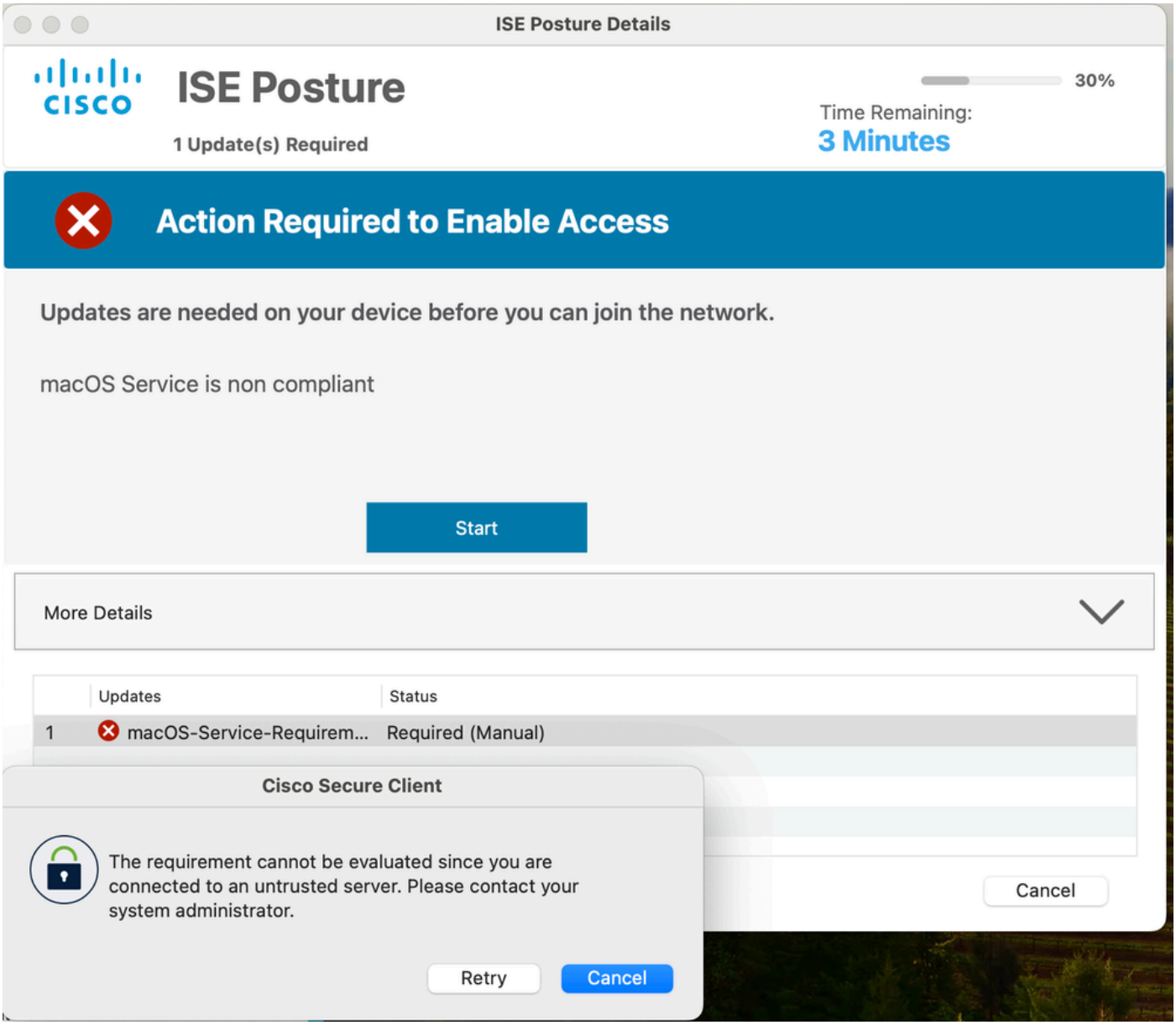
トラブルシュート

このmacOSサービスポスチャ条件の設定中に発生する可能性のある一般的な問題は次のとおりです。

信頼されていない証明書



前述したように、サービス状態には管理者特権でのアクセス許可が必要です。ポスチャスキャンプロセスの証明書がサーバによって信頼されていることが不可欠です。
そうしないと、次のエラーが発生します。



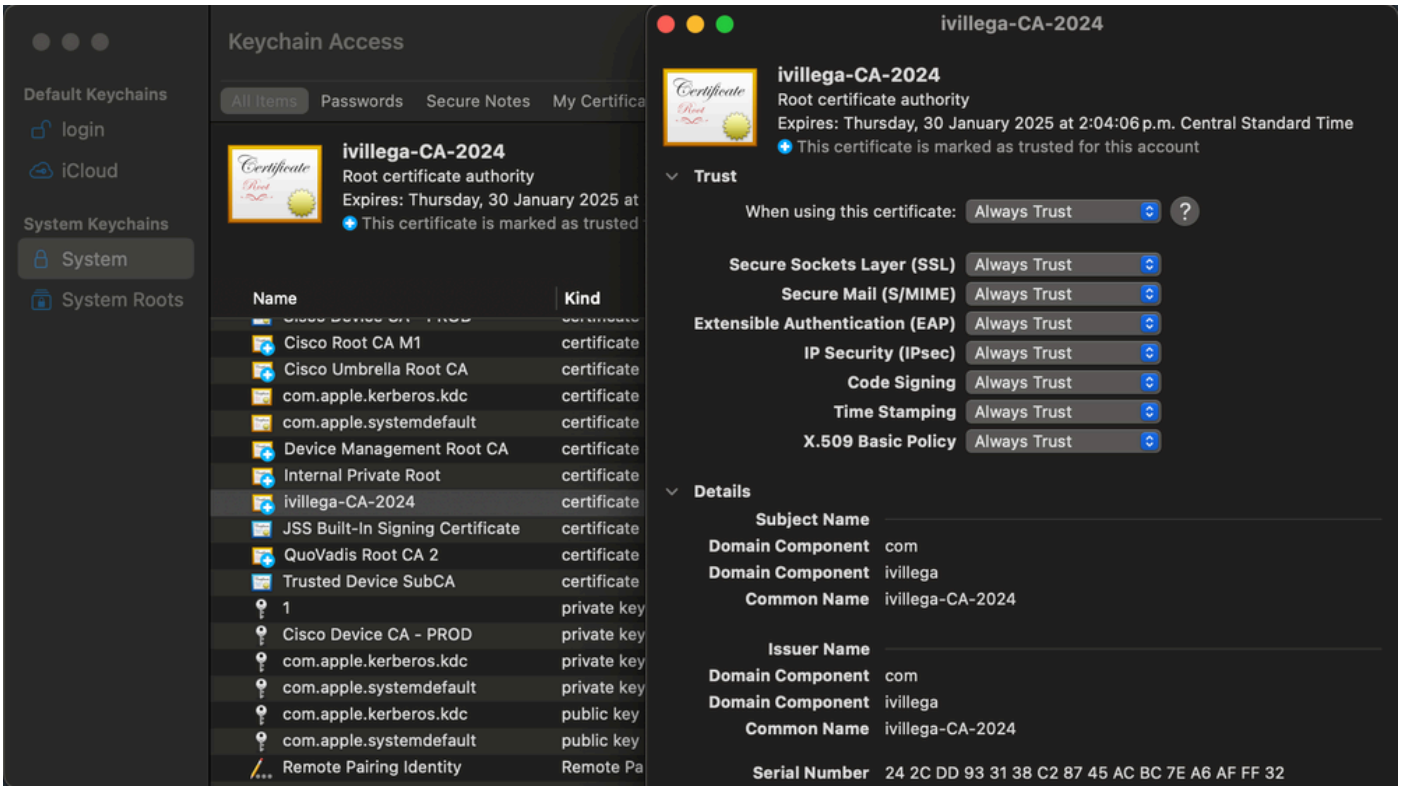
ISEポスチャモジュールは、IPアドレスまたは完全修飾ドメイン名(FQDN)のいずれかでPSNサーバを検出します。 ベストプラクティスは、ポスチャ設定ファイルを使用してFQDNによってISEノードを検出することです。このため、管理者（クライアントプロビジョニングポータル）証明書とポータル（クライアントプロビジョニングポータル）証明書のCNフィールドまたはSANフィールドにはFQDNが含まれている必要があります。これにはワイルドカード証明書も使用できます。ワイルドカード証明書はこのフローでサポートされています。

システムのセキュリティのため、CNフィールドは将来信頼できません。ベストプラクティスとして、SANフィールドにワイルドカードエントリまたはFQDNを含めてください。

FQDNではなくIPアドレスを使用してISE PSNが検出される場合、ノードのIPアドレスは、管理者およびポータルの使用にリンクされている証明書のCNフィールドまたはSANフィールドのいずれかに含まれている必要があります。

ISEポスチャモジュールは、ISEサーバによって提示される証明書を信頼します。そのCAがmacOS キーチェーンアクセスのシステム証明書ストアにある場合、このCAにはWhen using this

certificateをAlways Trustに設定する必要があります。



証明書が正しくロードされ、CNとSANの要件がすべて満たされていても、macOSシステムが証明書を信頼できないという問題が発生する場合があります。 このような場合は、キーチェーンアクセスアプリケーションを開き、システム証明書ストアタブに移動して、そこからCA証明書を削除します。

次に、macOSターミナルアプリケーションに移動し、sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychainコマンドを実行します。

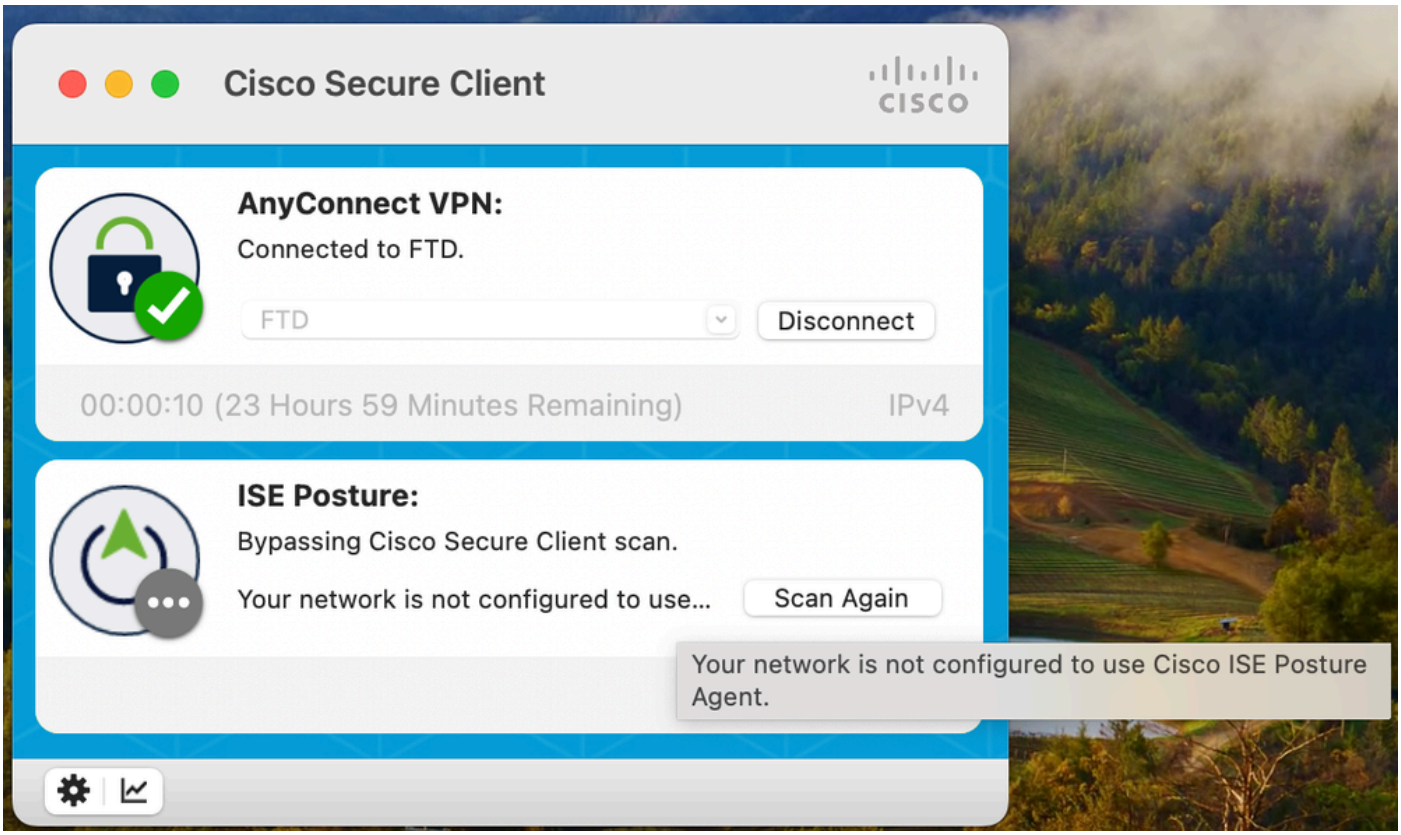
{CA証明書へのパス}

たとえば、証明書がデスクトップにある場合、コマンドは次のようになります。sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

コマンドを実行した後、コンピュータを再起動して再試行します。

Cisco Secure Clientスキャンのバイパス

また、「Bypassing Cisco Secure Client Scan」および「Your network is not configured to use Cisco ISE Posture Agent」というエラーメッセージが表示される場合もあります。



このメッセージが表示されるのは、ISE > Work Centers > Posture > Client Provisioning > Client Provisioning Policiesでクライアントプロビジョニングが設定されていないためです。
Mac OSXオペレーティングシステムの状態が発生する場合でも、すべてのmacOSバージョンを対象としているわけではありません。

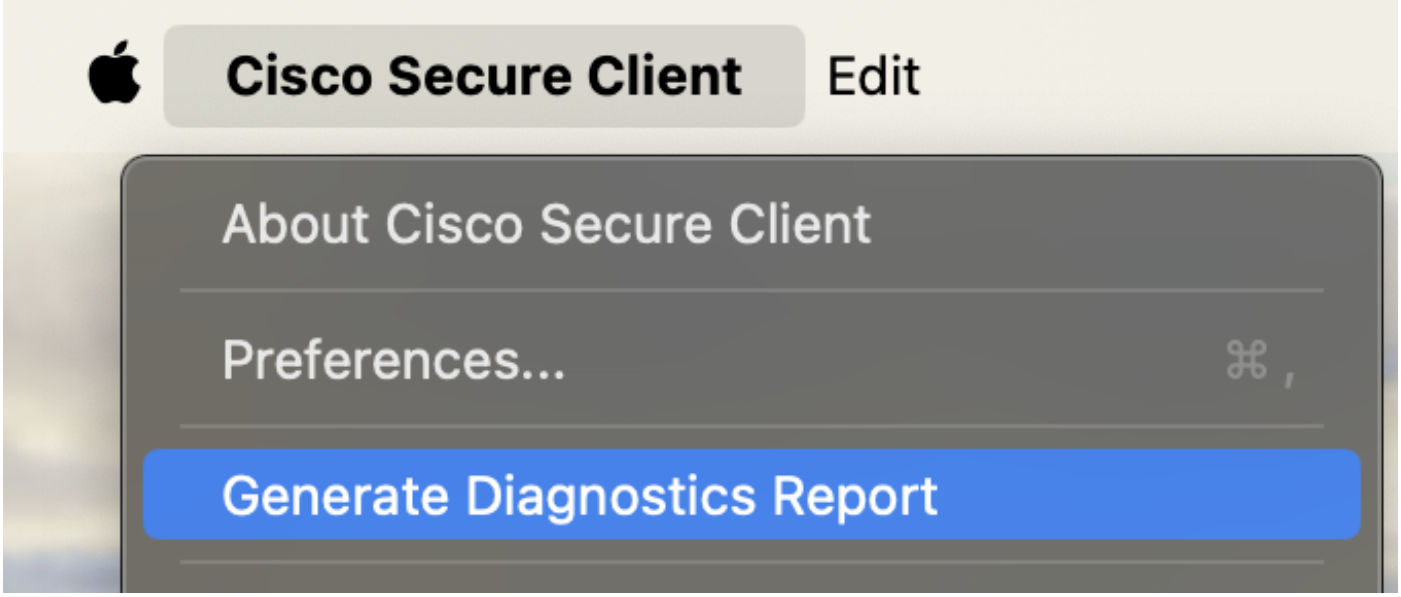
デフォルトでは、ISEにはSequoia(15.6.x)などの最新のmacOSバージョンが含まれないため、このようなメッセージを回避して、ポスチャが確実に更新されるようにします。

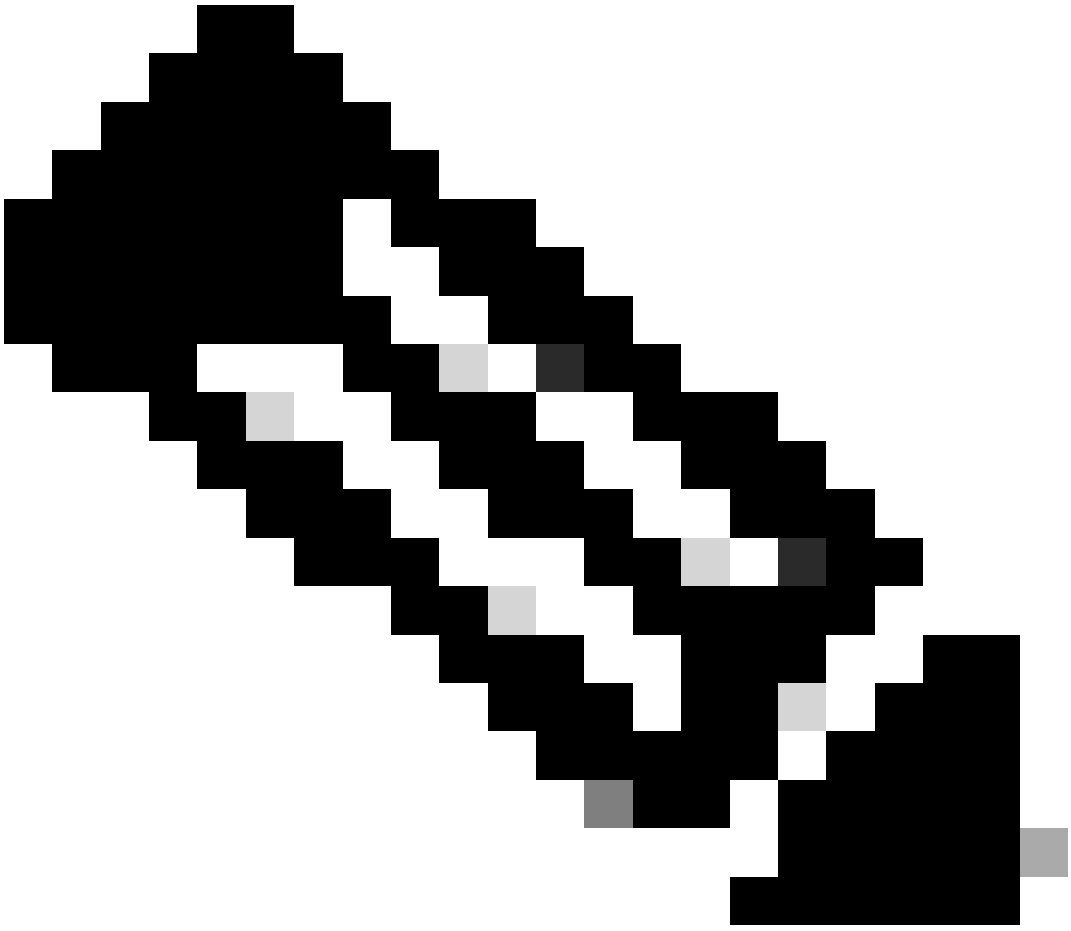
ポスチャフィードは、ISE > Work Centers > Posture > Settings > Software Updates > Posture Updatesから更新する必要があります。

これは、ISEからオンラインで直接更新するか、Posture Offlineサイトからここにダウンロードできるzipファイルを使用してオフラインにできます

その他の問題

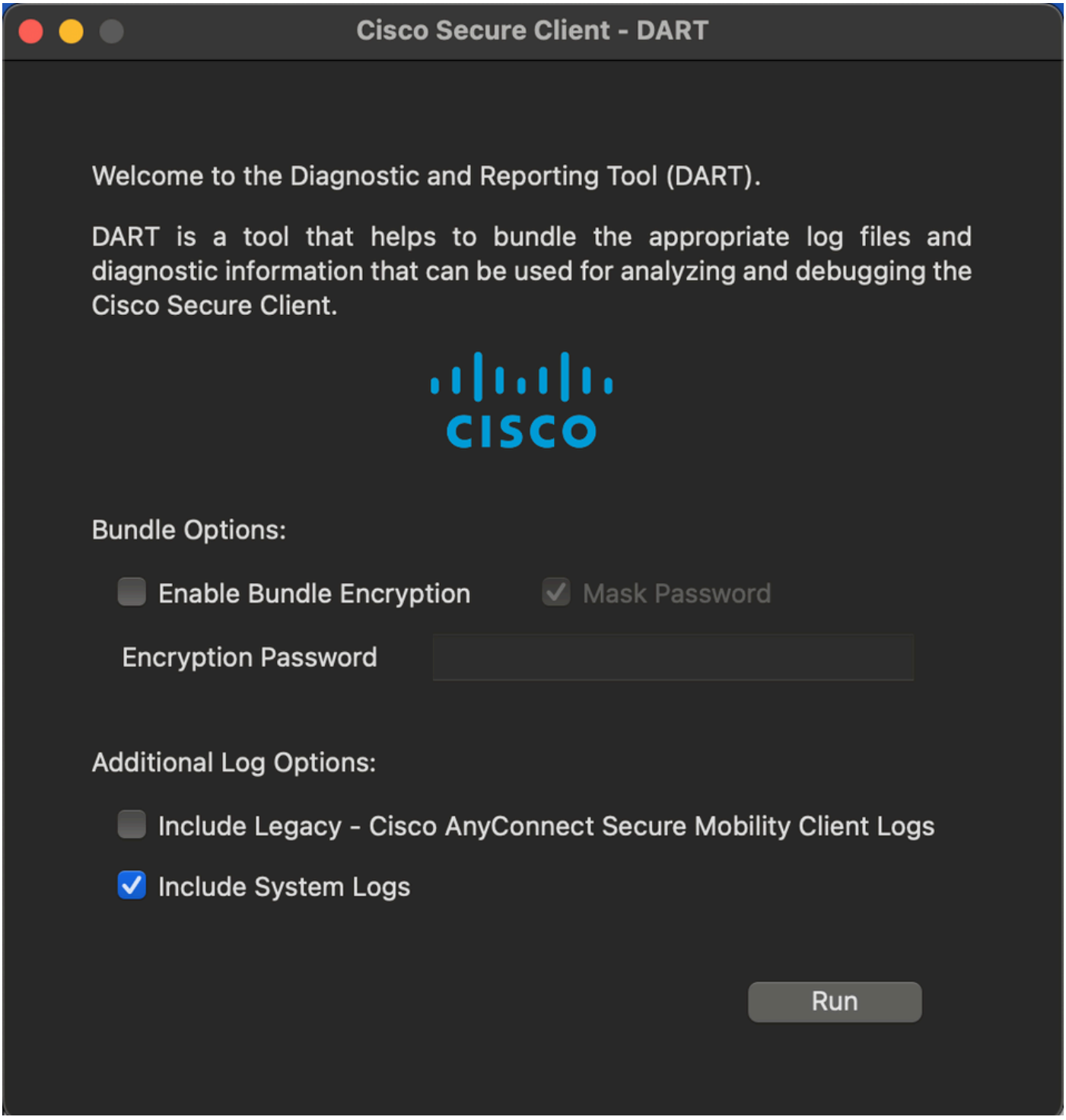
詳細を確認する場合は、姿勢のmacOSデバイスからDARTバンドルを収集できます。そのためには、DARTモジュールをインストールし、Cisco Secure Clientアプリケーションをアクティブにした状態で、メニューバーに移動してCisco Secure Clientをクリックし、Generate Diagnostics Reportsで次のコマンドを実行する必要があります。



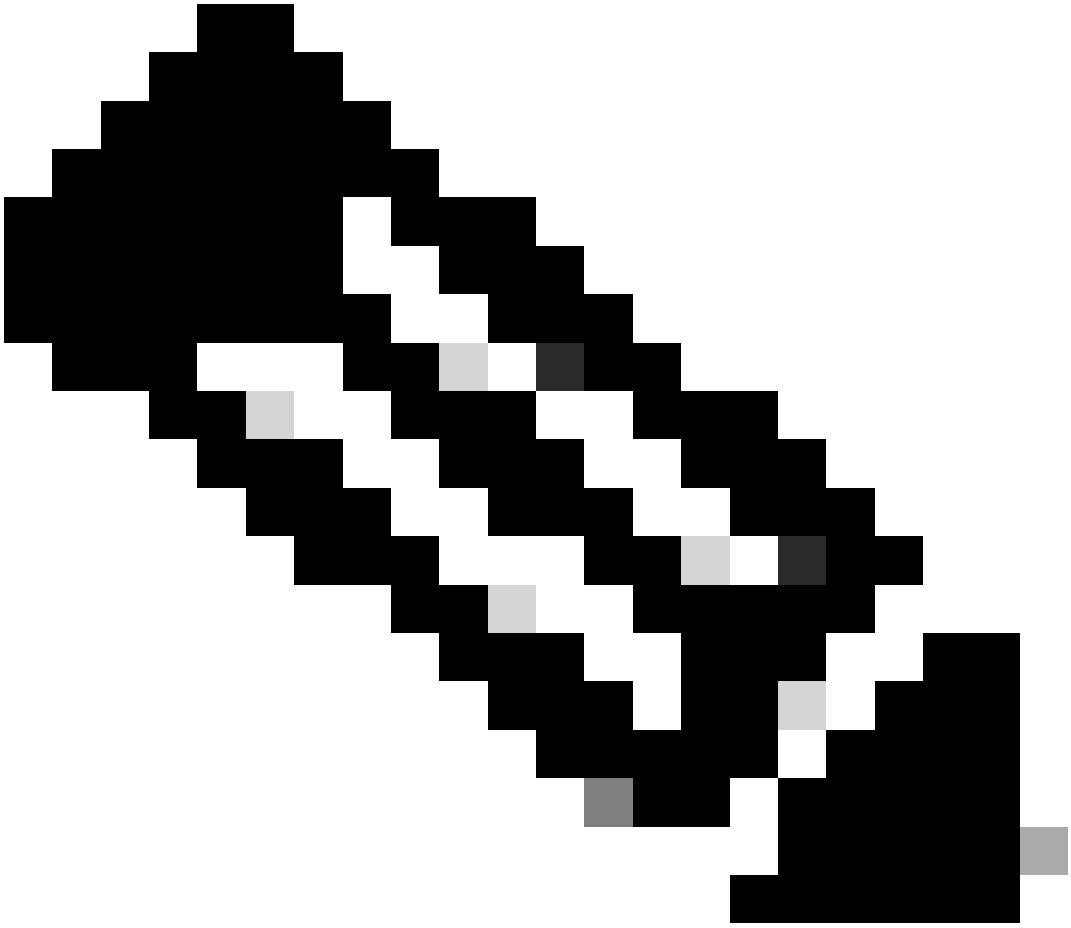


注:DARTバンドルの生成時には、Include System Logsオプションを有効にしておくこと

が重要です。有効にしていないと、DARTバンドルにはISEポスチャモジュール情報が含まれません。



セキュリティ上の理由から、一部のログは暗号化されて表示されない場合がありますが、DARTバンドルのunified_log.logには、次のようなログが表示される場合があります。



注：このログの例は、このドキュメントで設定したmacOSサービス条件のものです。

```
[Tue Feb 27 10:30:58.576 2024][csc_iseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 File
```

```
macOS-Service-Condition
```

```
3
```

303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: processPostureData Thread Id: 0x4A9FD7C0 File: Au

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: SMP_initCheck Thread Id: 0x4A9FD7C0 File: SMNavPo

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

",isElevationAllowed:1,nRemediationTimeLeft:0}
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 Fi

macOS-Service-Condition

3

303

```
        com.apple.sysmond

         running

         0

)
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: Rqmt.cpp
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: CheckSvc.
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: completeCheck Thread Id: 0x4A9FD7C0 File: Rqm
```

また、エンドポイントの認証とポスチャを行うISE PSNノードで、デバッグログレベルのポスチャコンポーネントを設定することもできます。

このログレベルは、ISE > Operations > Troubleshoot > Debug Wizard > Debug Log Configurationの順に選択して設定できます。 PSN Hostnameをクリックし、ポスチャコンポーネントのログレベルをINFOからDEBUGに変更します。

macOSサービス条件に対して同じ例を使用すると、ise-psc.log内で同様のログを確認できます。

```
2024-02-27 10:30:58.658 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.runtime.Pos

         ISE: 3.3.0.430

         ISE: 2.x
```

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

2024-02-27 10:30:58.659 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.util.Status

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

]

2024-02-27 10:31:06.044 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-8][[]] cisco.cpm.posture.util.AgentU

それでも問題が解決しない場合は、シスコチームにTACチケットを提出してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。