# Verständnis und Konfiguration des Status des macOS-Service für die ISE

## Inhalt


- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Konfigurieren
  - Identifizieren des zu überprüfenden Dienstnamens
  - (Optional) Überprüfen Sie die Details des Diensts, um festzulegen, ob der Dienst ein Agent oder ein Demon ist.
  - Wählen Sie den auszuwertenden Service Operator aus.
  - Geladene Services
  - Nicht geladene Services
  - Geladen und aktiv
  - Mit Exitcode geladen
  - Geladen und ausgeführt oder mit Exit-Code
  - Konfigurieren Sie die Anforderungs- und Statusrichtlinie für diesen Zustand.
- Überprüfung
- Fehlerbehebung
  - Zertifikat nicht vertrauenswürdig
  - Umgehen von Cisco Secure Client Scan
  - Sonstige Fragen


## Einleitung

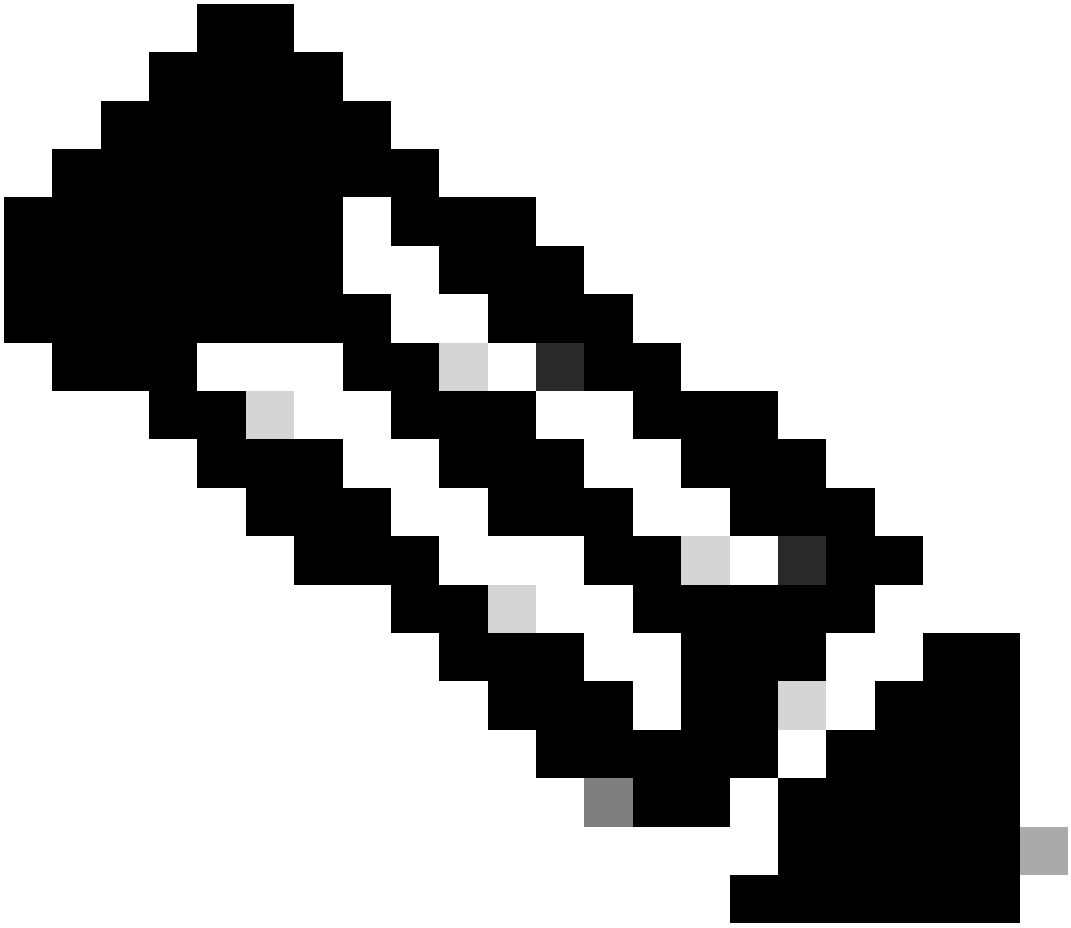
Dieses Dokument beschreibt den Prozess der Konfiguration der macOS-Servicebedingungen in der Cisco ISE.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse von macOS.
- Bekannt für ISE-Statusflow.



Anmerkung: In diesem Dokument wird die Konfiguration für den macOS-Dienstzustand beschrieben. Die anfängliche Statuskonfiguration wird in diesem Dokument nicht behandelt.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 3.3 Patch 1
- MacoOS-Gerät mit Sonoma 14.3.1
- Cisco Secure Client 5.1.2.42
- Compliance-Modul Version 4.3.3432.64000

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

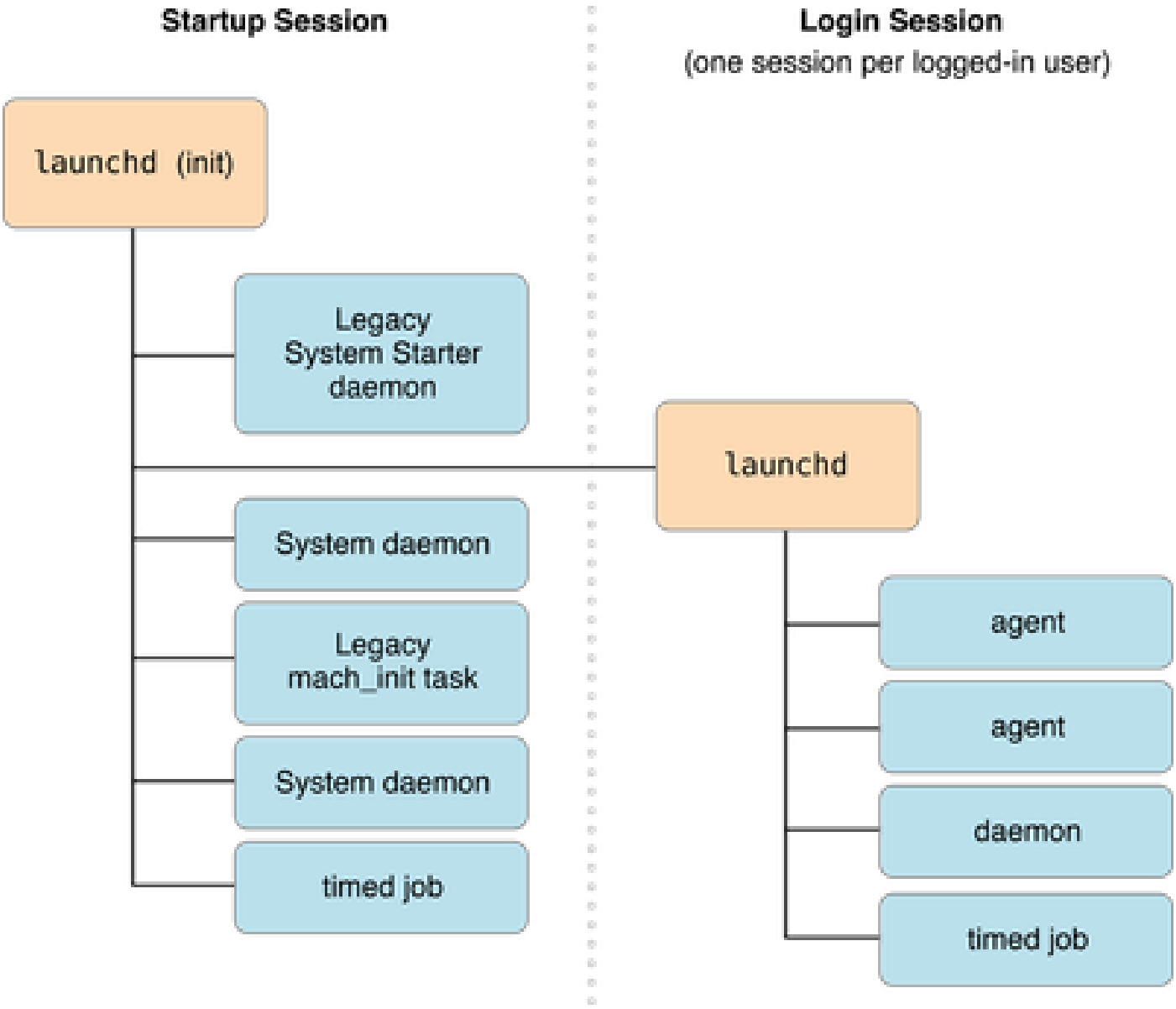
## Hintergrundinformationen

Die macOS-Dienstbedingung ist nützlich, wenn Sie case verwenden müssen, um zu überprüfen, ob ein Dienst im macOS-Gerät geladen ist. Außerdem können Sie überprüfen, ob er ausgeführt wird oder nicht. Die macOS-Dienstbedingung kann zwei verschiedene Diensttypen überprüfen: Daemons und Agenten.

Ein Daemon ist ein Programm, das im Hintergrund als Teil des Gesamtsystems läuft (d.h. nicht an einen bestimmten Benutzer gebunden ist). Ein Daemon kann keine GUI anzeigen; Genauer gesagt, ist es nicht erlaubt, eine Verbindung zum Window-Server herzustellen. Ein Webserver ist das perfekte Beispiel für einen Daemon.

Ein Agent ist ein Prozess, der im Hintergrund für einen bestimmten Benutzer ausgeführt wird. Agenten sind nützlich, weil sie Dinge tun können, die Daemons nicht können, wie zuverlässigen Zugriff auf das Home-Verzeichnis des Benutzers oder verbinden sich mit dem Window-Server. Ein Kalenderüberwachungsprogramm ist ein gutes Beispiel für einen Agenten.

Im folgenden Diagramm sehen Sie, wie die einzelnen Module je nach Gerätestart und Benutzeranmeldung geladen werden:




Weitere Informationen zu Daemons und Agenten finden Sie hier in der [Apple-Dokumentation]

Die auf Ihrem macOS-Gerät verfügbaren Dämonen und Agenten befinden sich an folgenden Stellen:

| Location (Standort) | Beschreibung |
|---|---|
| ~/Library/LaunchAgents | Vom Benutzer bereitgestellte benutzerspezifische Agenten. |
| /Library/LaunchAgents | Vom Administrator bereitgestellte benutzerspezifische Agenten. |
| /Library/LaunchDaemons | Systemweite Daemons, die vom Administrator bereitgestellt werden. |

| | |
|---|---|
| /System/Library/LaunchAgents | OS X-Agenten pro Benutzer |
| /System/Library/LaunchDaemons | OS X Systemweite Daemons |

Sie können die Liste der einzelnen Kategorien von macOS Terminal mit den folgenden Befehlen überprüfen:

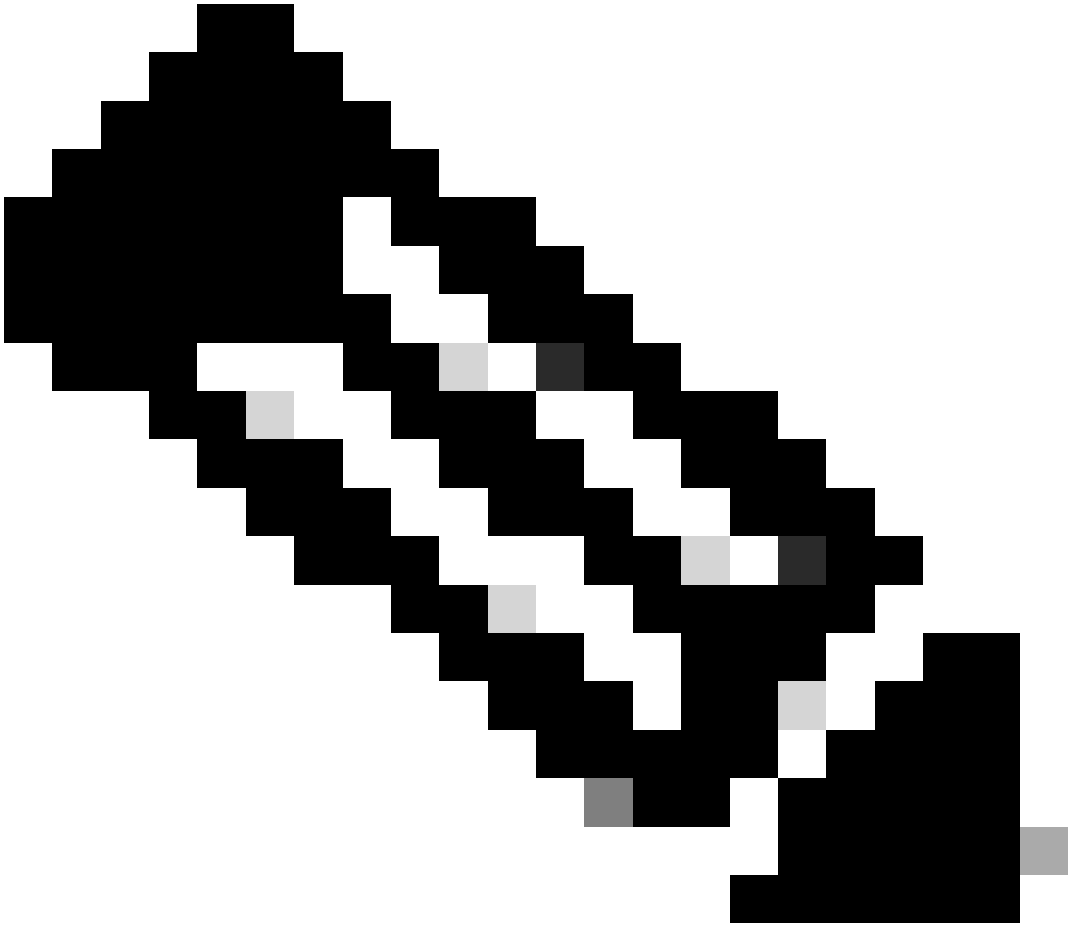
ls -ltr ~/Library/LaunchAgents
ls -ltr /Library/LaunchAgents
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

Die vorherigen Standorte können Ihnen alle Daemons und Agenten anzeigen, die auf dem macOS-Gerät verfügbar sind, aber nicht alle sind geladen oder laufen.

# Konfigurieren

Die Konfiguration für den MacOS-Dienstzustand kann wie folgt durchgeführt werden:

1. Geben Sie den zu überprüfenden Dienstnamen an.
2. (Optional) Überprüfen Sie die Details des Dienstes, um zu bestimmen, ob es sich um einen Agenten oder einen Demon handelt.
3. Wählen Sie den auszuwertenden Service-Operator.
4. Konfigurieren Sie die Anforderungs- und Statusrichtlinie für diese Bedingung.



Anmerkung: Der Service-Schwachstellenzustand erfordert eine erhöhte Berechtigung, damit er funktioniert. Daher MUSS ISE PSN vom Cisco Secure Client (ehemals AnyConnect) als vertrauenswürdig eingestuft werden - Referenzhandbuch

## Identifizieren des zu überprüfenden Dienstnamens

Das ISE Posture Compliance Module ist in der Lage, Services zu prüfen, die mit einem Exitcode geladen, ausgeführt und geladen wurden und ausgeführt werden.

Um die geladenen Dienste zu überprüfen, verwenden Sie den Befehl sudo launchctl dumpstate.

Um zu überprüfen, welche Dienste geladen sind und über einen Exitcode verfügen, verwenden Sie den Befehl sudo launchctl list.

Die vorherigen Befehle können abrupt viele Informationen anzeigen. Verwenden Sie stattdessen diese Befehle, um nur den tatsächlichen Dienstnamen anzuzeigen:

Verwenden Sie den folgenden Befehl, um nur die geladenen Dienstnamen zu überprüfen:

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

Verwenden Sie den folgenden Befehl, um nur die Dienstnamen zu überprüfen, die geladen wurden und über einen Exitcode verfügen:

sudo launchctl-Liste | awk "{if (NR>1) print $3}"

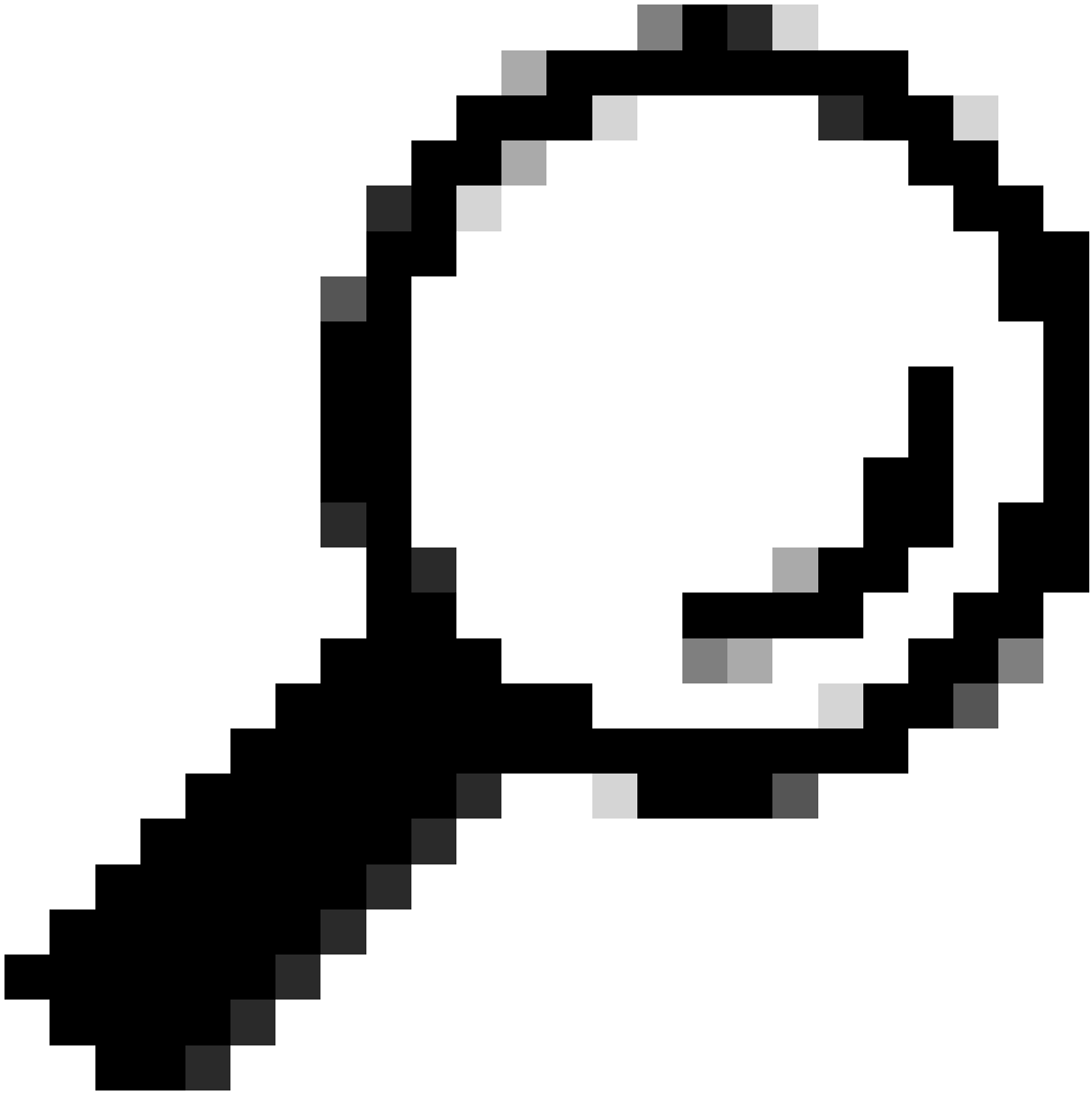
Diese Befehle zeigen viele Informationen an, daher wird empfohlen, am Ende jedes Befehls einen anderen grep-Filter zu verwenden, um den gesuchten Dienst zu finden.
Wenn Sie beispielsweise nach einem anbieterspezifischen Service suchen, können Sie ein Schlüsselwort als Filter im und verwenden.

Im Fall von Cisco Services sind die Befehle in etwa wie folgt:

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

## (Optional) Überprüfen Sie die Details des Diensts, um festzulegen, ob der Dienst ein Agent oder ein Demon ist.

Im zweiten Teil der Konfiguration dieser Bedingung müssen Sie überprüfen, ob es sich bei Ihrem Dienst um einen Daemon- oder einen Agent-Typ handelt.



Tipp: Dieser Schritt ist optional, da Sie mit der ISE die Option für Daemon or User Agent auswählen können. Sie können diese Option also einfach auswählen und diesen Teil überspringen.

---

Wenn Sie in diesem Zustand granular sein möchten, können Sie den Typ wie folgt überprüfen:

1. Überprüfen Sie zuerst den vollständigen launchctl-Namen des Diensts mit dem Befehl sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$|| | grep -i {Ihr Dienstname}

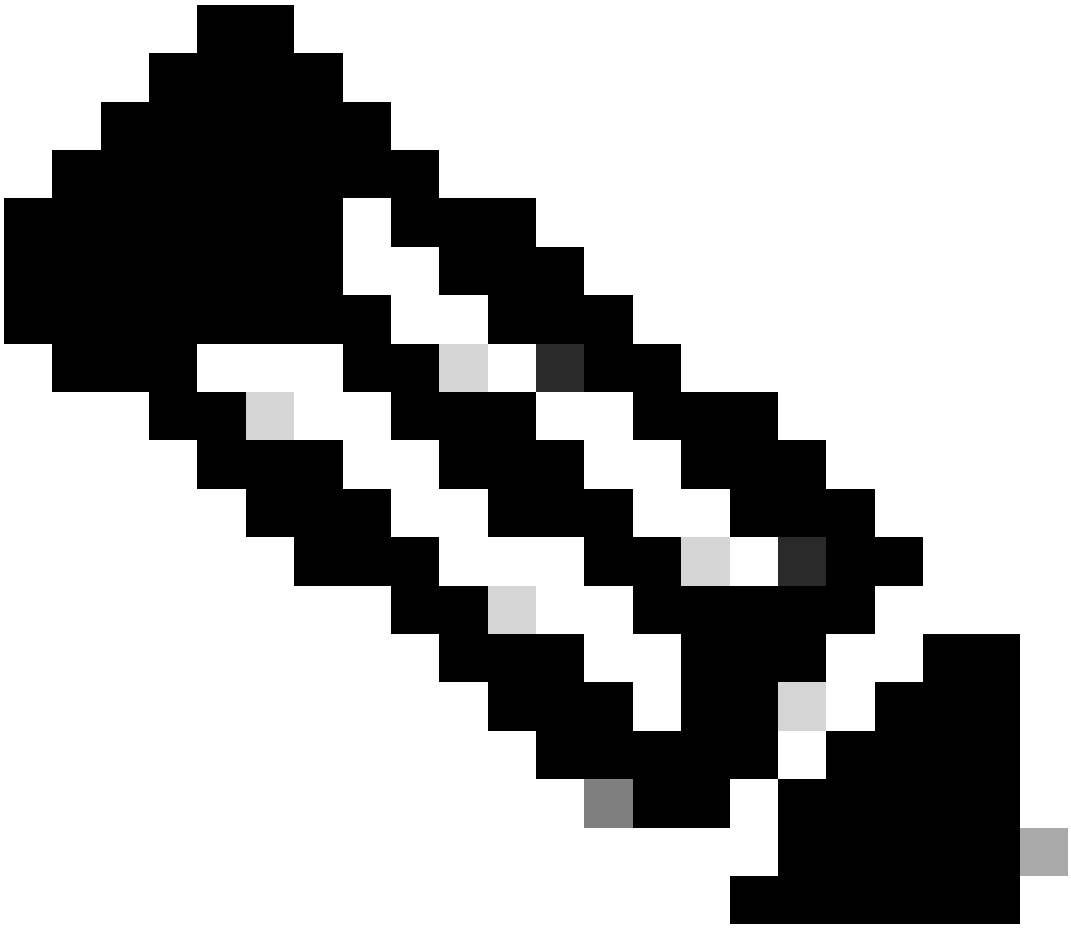
Für den Befehl sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | s/.\{3\}$// verwendet | grep -i com.cisco.secureclient.iseposture, die Ausgabe lautet: gui/501/com.cisco.secureclient.iseposture.

2. Überprüfen Sie den Servicetyp mit dem Befehl sudo launchctl print { Ihr launchctl-Servicename } | grep -i 'type = Launch'

Im folgenden Beispiel für den Befehl: sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch', die Ausgabe ist: type = LaunchAgent.

Das bedeutet, dass der Diensttyp Agent ist, andernfalls wird Typ = LaunchDaemon angezeigt.

---



> Anmerkung: Wenn die Informationen leer sind, wählen Sie die Option für Daemon or User Agent in ISE für die Einstellung des Diensttyps aus.

---

## Wählen Sie den auszuwertenden Service Operator aus.

Mit der ISE können Sie fünf verschiedene Service Provider auswählen:

- Geladen
- Nicht geladen
- Geladen und aktiv
- Mit Exitcode geladen
- Geladen und ausgeführt oder mit Exitcode

## Geladene Services

Sind alle Dienste aufgeführt, die mit diesen beiden Befehlen aufgerufen werden:

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

## Nicht geladene Services

Sind alle Dienste, deren Eigenschaftsliste (plist) definiert ist, aber nicht geladen wurde, oder Dienste, deren Eigenschaftsliste (plist) noch nicht definiert ist, also überhaupt nicht geladen werden kann.

Diese Dienste sind nicht leicht zu identifizieren, und es ist am häufigsten für den Anwendungsfall, wenn Sie überprüfen möchten, dass ein bestimmter Dienst nicht im macOS-Gerät vorhanden sein sollte.
Wenn Sie beispielsweise verhindern möchten, dass der Zoom-Dienst auf das macOS-Gerät geladen wird, können Sie us.zoom.ZoomDaemon als Wert für den Dienst hier einfügen. Auf diese Weise stellen Sie sicher, dass Zoom nicht ausgeführt wird oder gar nicht installiert ist.

Es gibt Dienste, die nicht deinstalliert werden können, und die zugehörige Eigenschaftenliste ist definiert.
Mit diesem Befehl können Sie beispielsweise sehen, dass dhcp6d plist definiert ist:

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

Wenn Sie die Liste der Dienste überprüfen, sehen Sie, dass nicht geladen wurde:

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

Wenn Sie den Wert auf "com.apple.dhcp6d" setzen, ist das macOS-Gerät kompatibel, da der Dienst trotz der Definition der Dienstliste nicht geladen wird.

## Geladen und aktiv

Nicht alle Dienste werden ausgeführt. Es gibt mehrere Zustände für jeden Dienst, z. B. "Wird ausgeführt", "Wird nicht ausgeführt", "Warten", "Beendet", "Nicht initialisiert" usw.
Verwenden Sie den folgenden Befehl, um alle ausgeführten Dienste zu überprüfen:

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

Dienste, die mit dem obigen Befehl aufgelistet sind, haben auf Loaded & Running service operator condition geklickt.

## Mit Exitcode geladen

Einige Dienste werden möglicherweise mit einem erwarteten oder unerwarteten Exitcode beendet. Diese Dienste können mit folgendem Befehl aufgelistet werden:

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

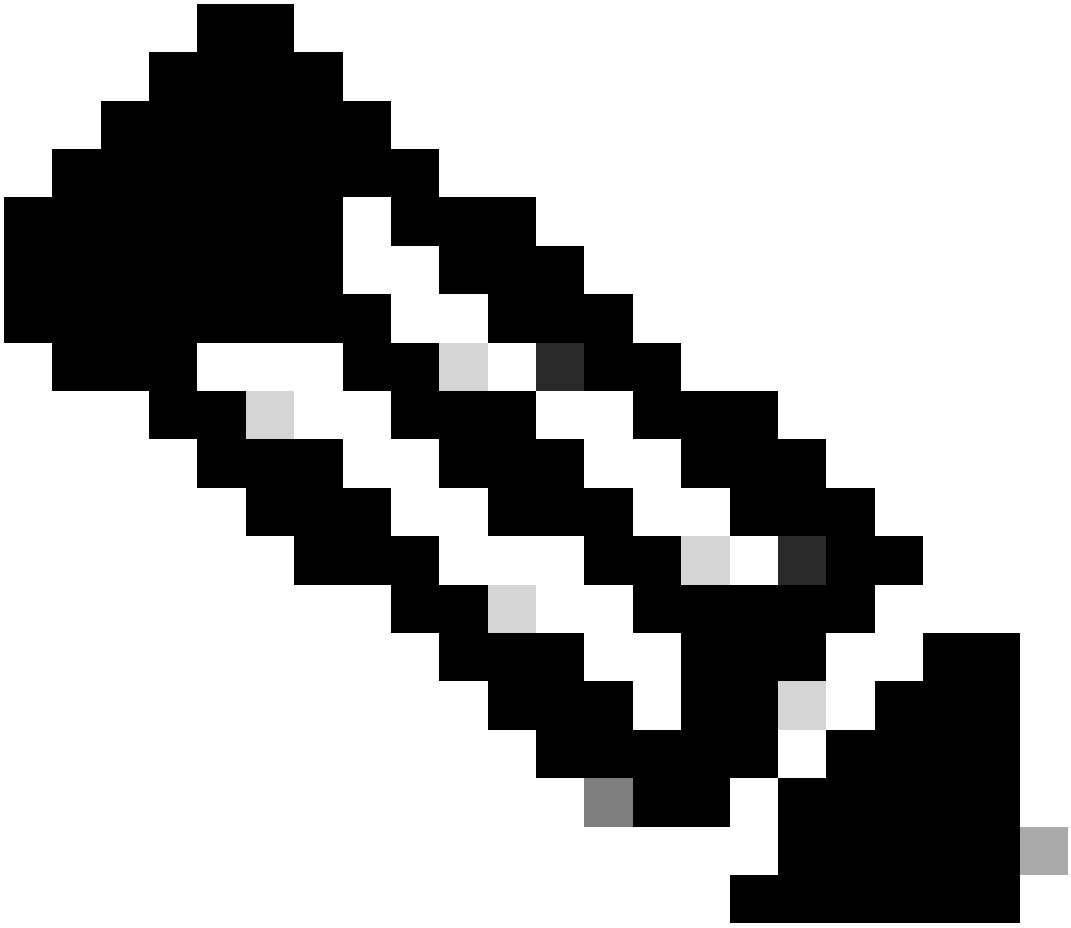
Um den Exitcode zu kennen, können Sie einen beliebigen Dienst auswählen und den folgenden Befehl verwenden:

sudo launchctl print { Ihr launchctl-Dienstname } | grep -i 'letzter Exitcode'

Beispiele:

sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i 'letzter Exitcode'

dessen Ausgabe lautet: last exit code = 0

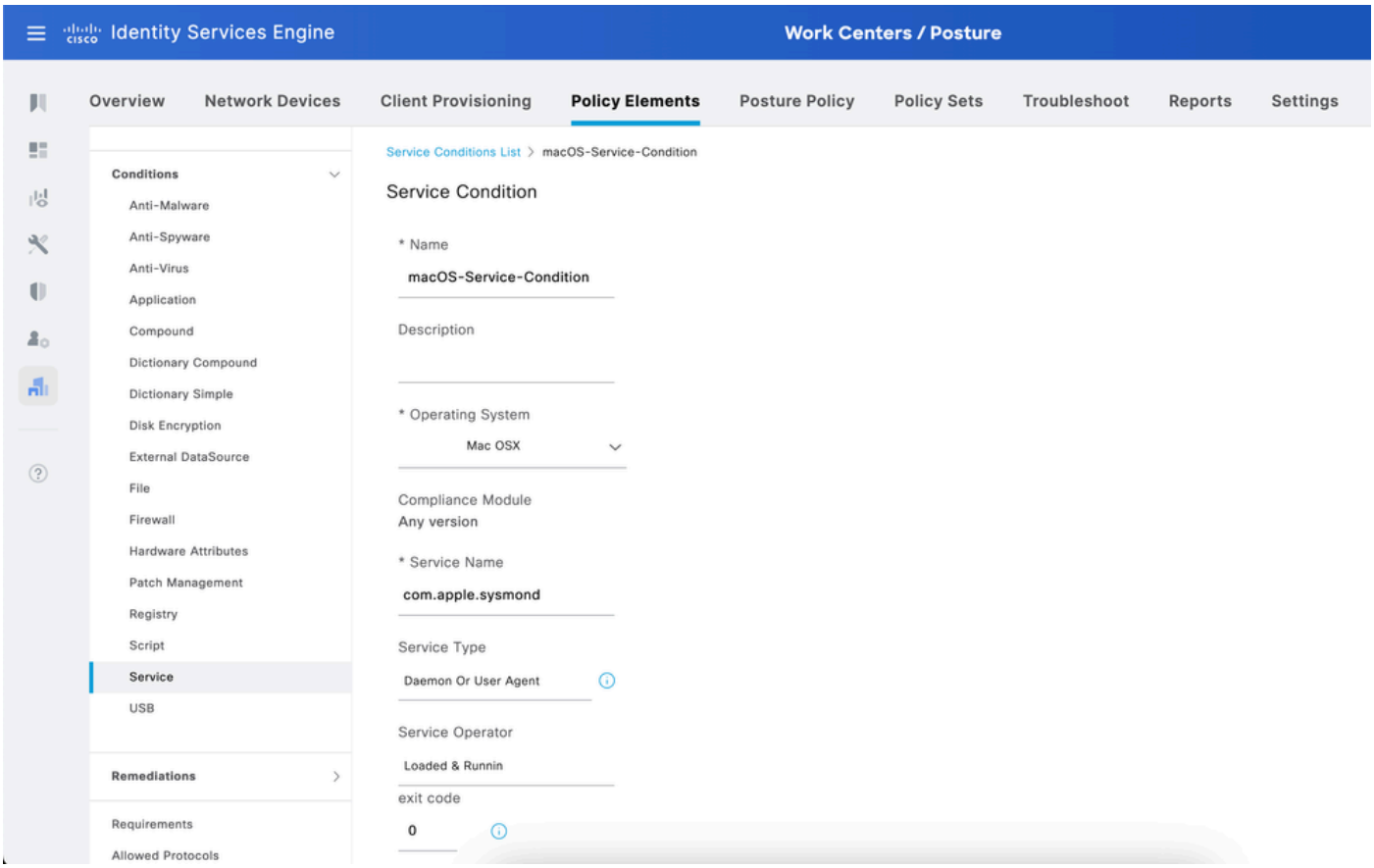


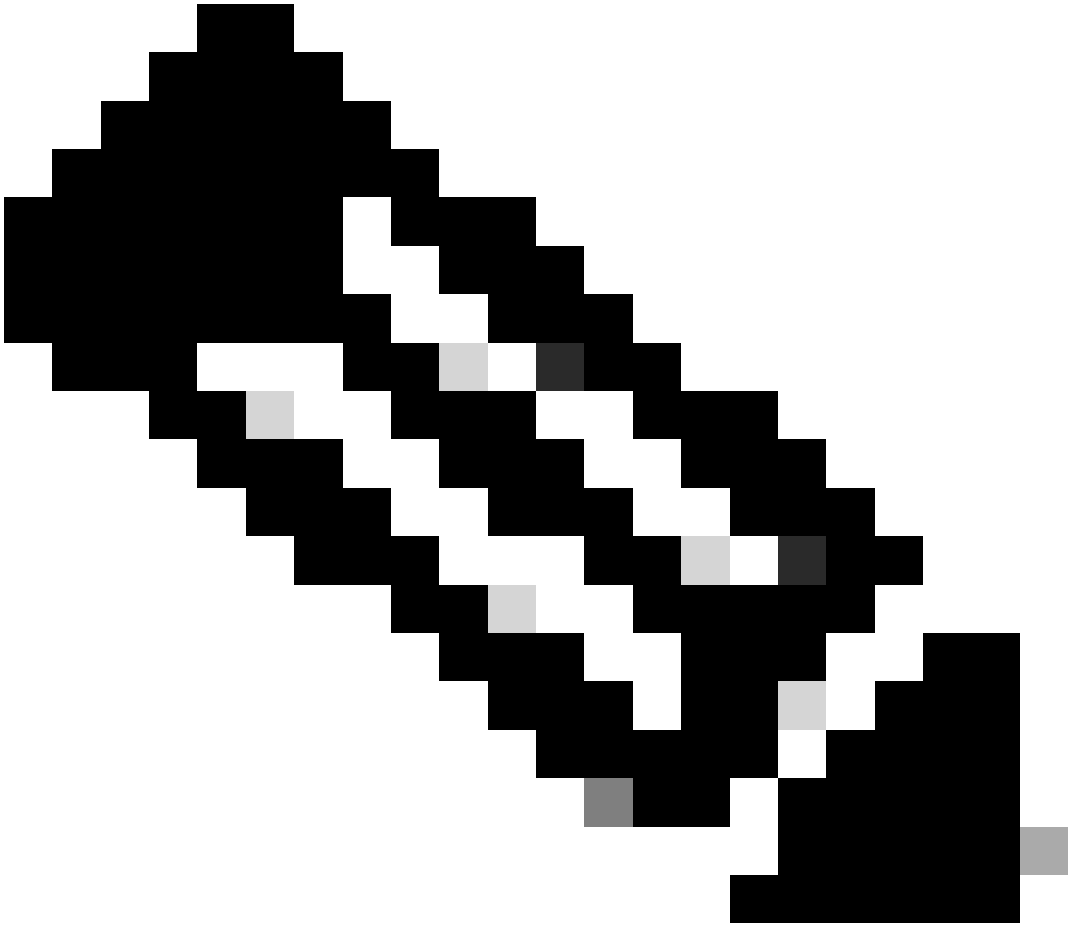
Anmerkung: Hier bedeutet der Exitcode 0 normalerweise, dass alles vom Dienst richtig gemacht wurde. Wenn ein Computer nicht mit 0 als Exitcode übereinstimmt, bedeutet dies, dass der Dienst die erwartete Aktion nicht ausgeführt hat.

## Geladen und ausgeführt oder mit Exit-Code

Diese letzte Option funktioniert, wenn der Dienst entweder geladen und ausgeführt oder mit Exitcode geladen ist.

Dieses Bild zeigt ein Beispiel für einen macOS-Dienstzustand.


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

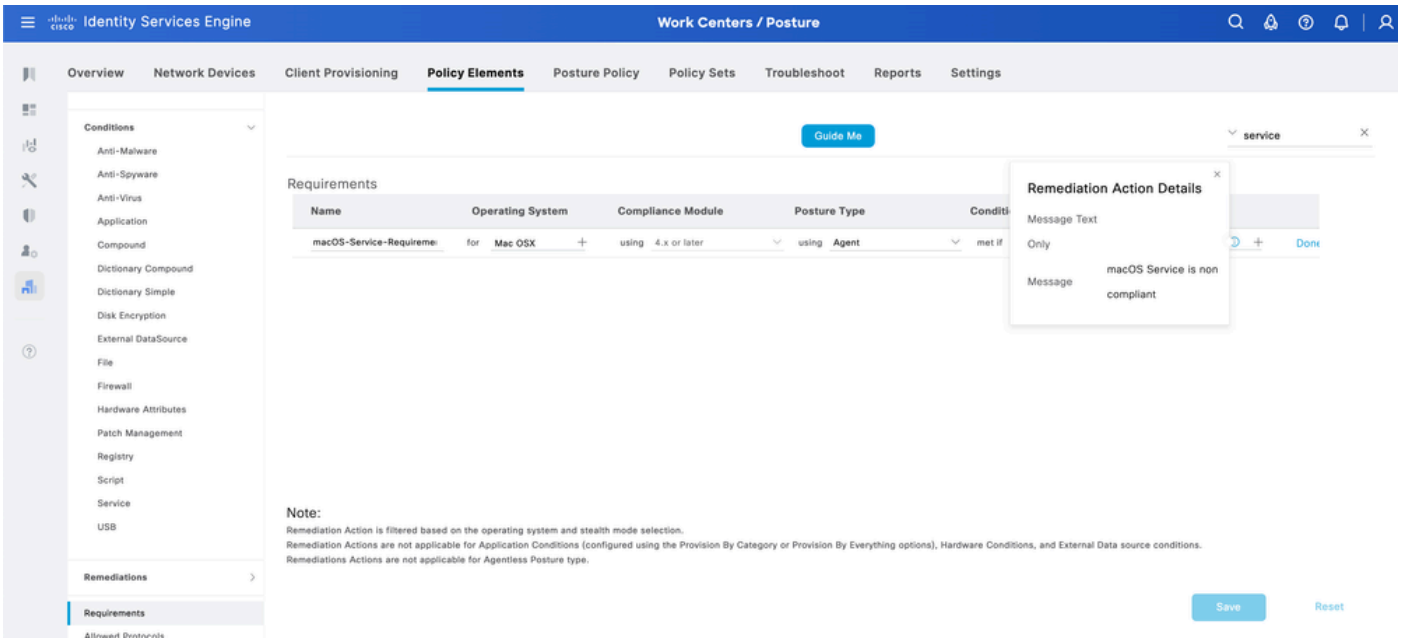


Anmerkung: Derzeit wird nur der genaue Dienstname unterstützt. Es liegt eine Erweiterungsanforderung vor, die Platzhalter in den Servicenamen unterstützt: Cisco Bug-ID CSCwf01373.

## Konfigurieren Sie die Anforderungs- und Statusrichtlinie für diesen Zustand.

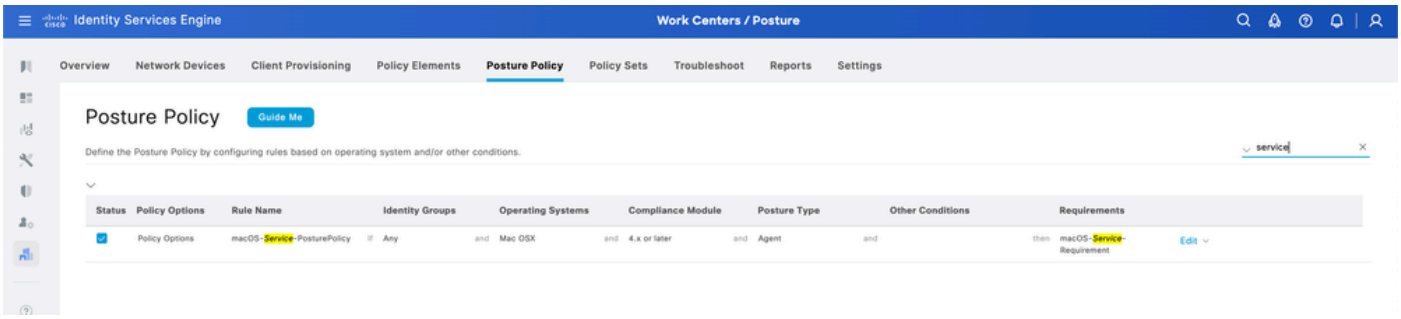
Nachdem die Bedingung konfiguriert wurde, müssen Sie eine Anforderung für diese Bedingung erstellen. Verwenden Sie für diese Anforderung die Option Nachrichtentest.
Navigieren Sie zu ISE > Work Centers > Posture > Requirements, um sie zu erstellen.

Anmerkung: Es gibt keine Sanierungsoptionen für Servicebedingungen.



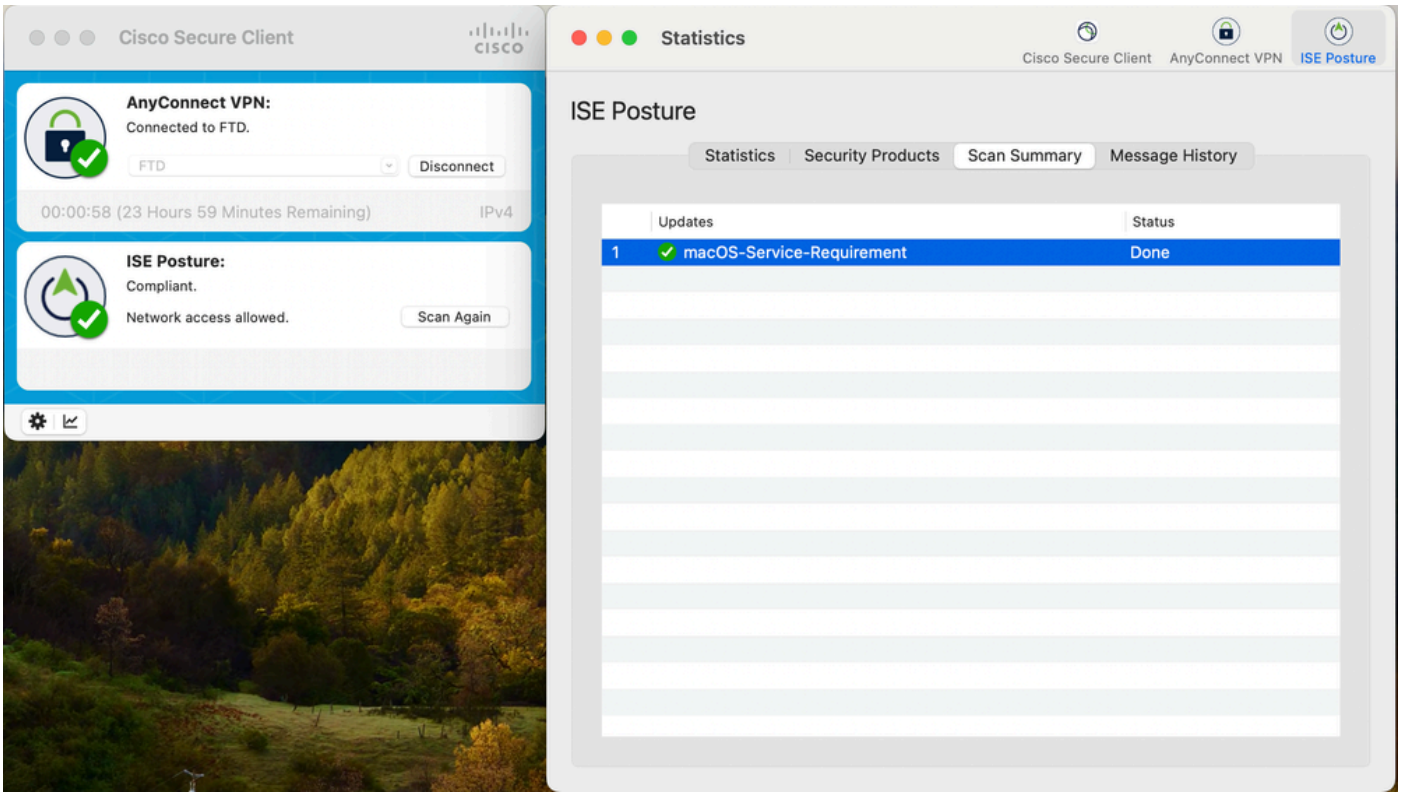
Danach besteht der letzte Schritt darin, die Statusrichtlinie zu konfigurieren, die die erstellte Anforderung verwendet.
Navigieren Sie zu ISE > Work Centers > Posture > Posture Policy, um die Richtlinie zu erstellen.

Aktivieren Sie die neue Richtlinie, benennen Sie sie nach Belieben, und wählen Sie die gerade erstellte Anforderung aus.

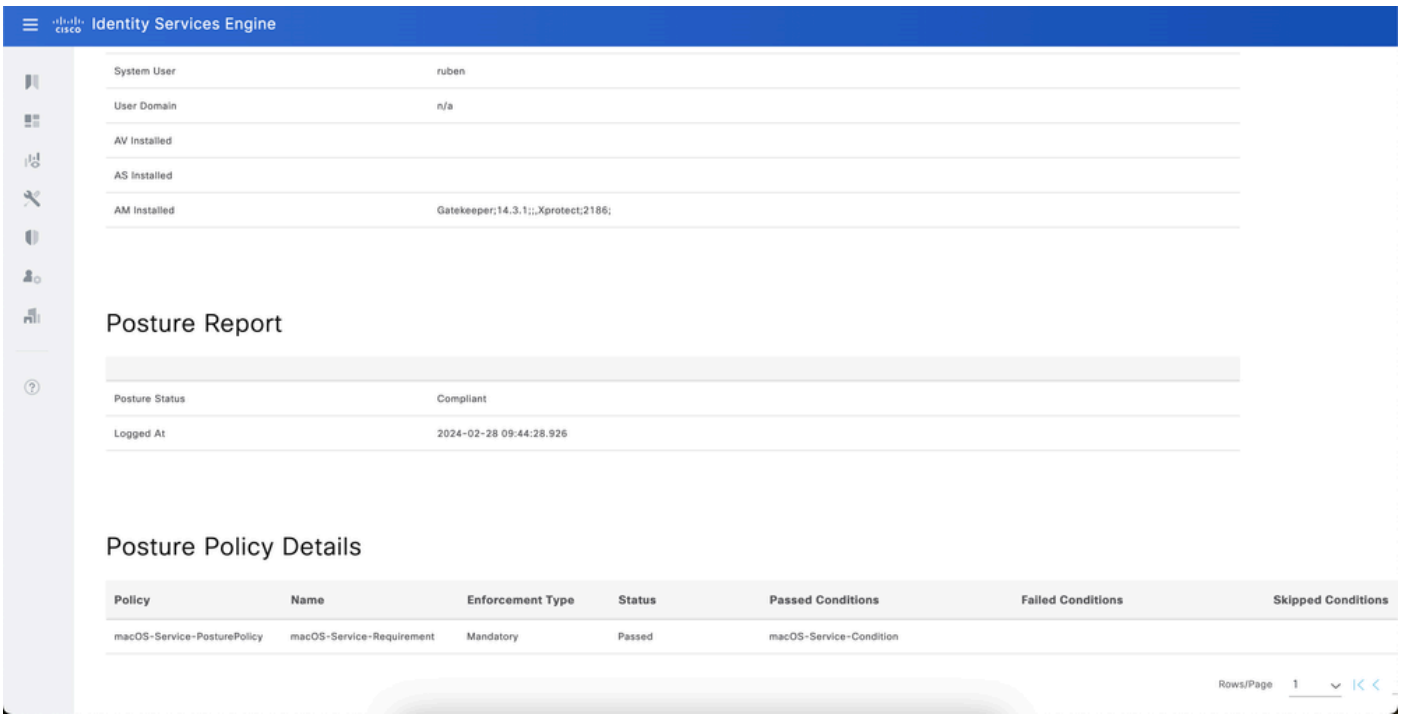



# Überprüfung

Sie können überprüfen, ob der macOS-Status erfolgreich war oder fehlgeschlagen ist. Dies erfolgt über die Benutzeroberfläche des Cisco Secure Client.



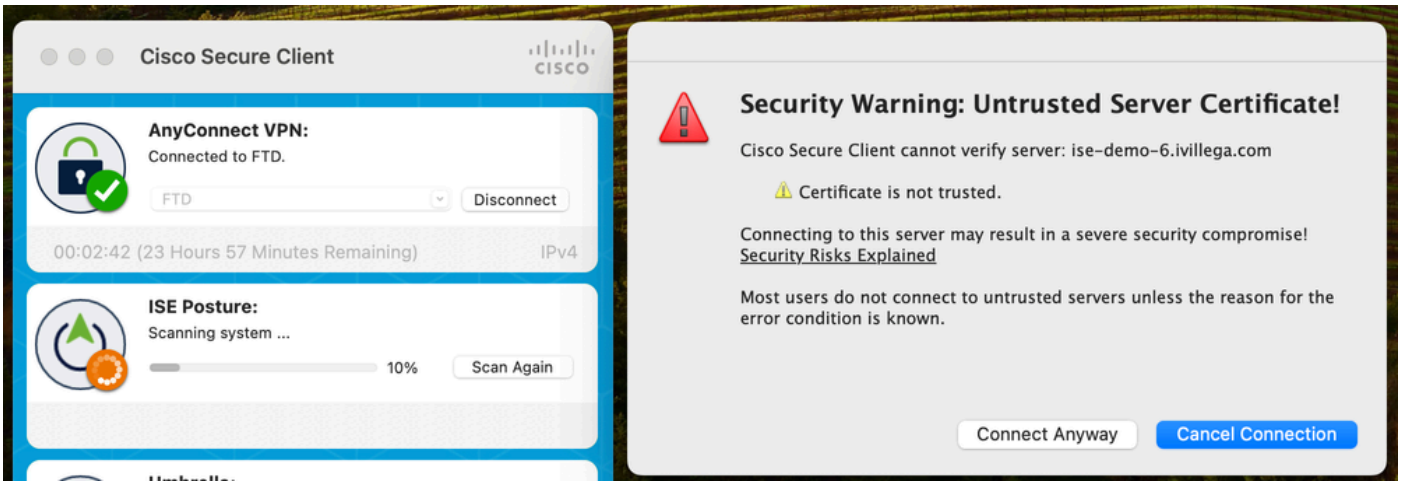
Sie können den ISE-Statusbericht auch unter ISE > Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint überprüfen.




# Fehlerbehebung

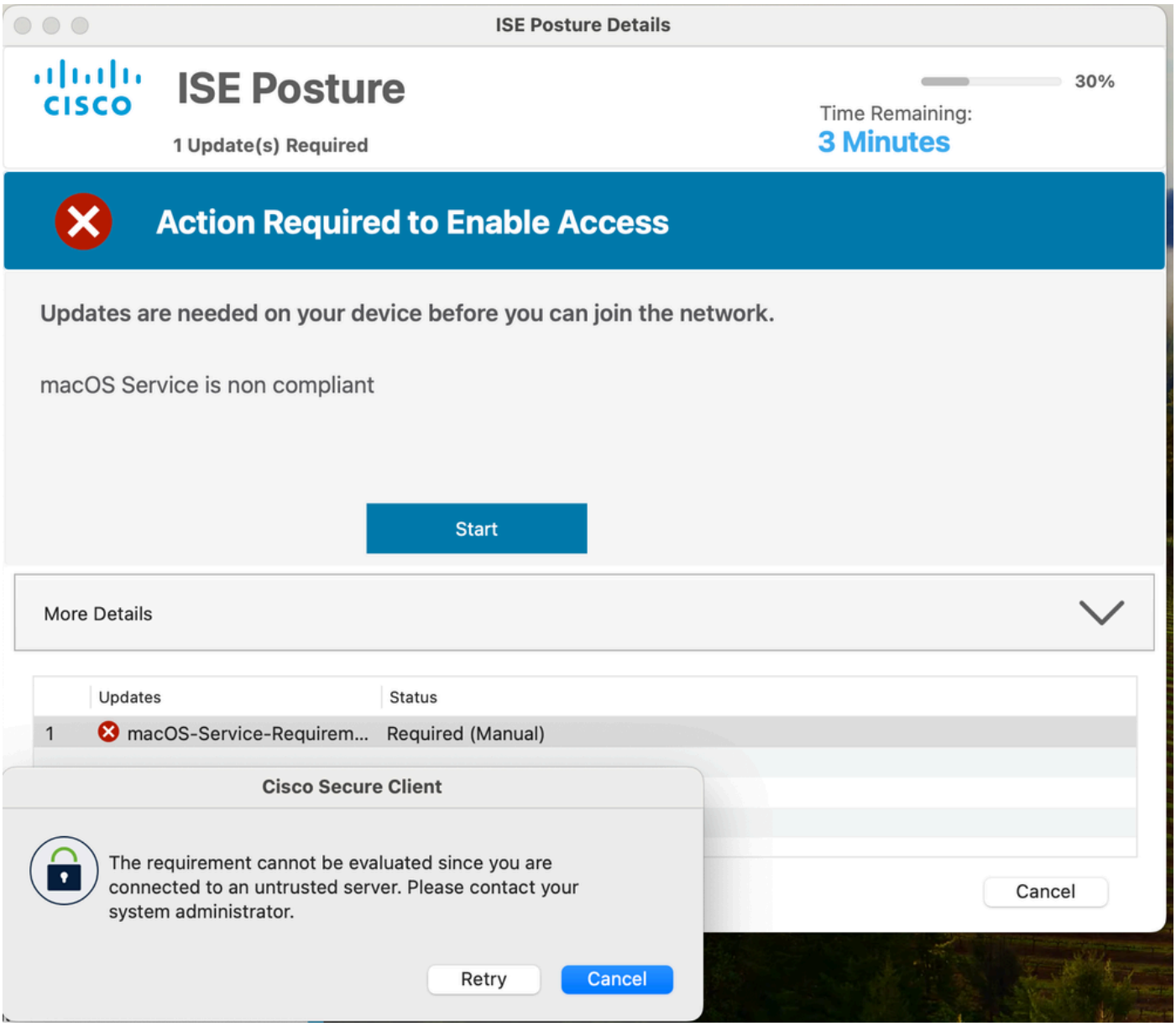
Häufige Probleme, die bei der Konfiguration dieses MACOS-Service-Status auftreten können, sind:

## Zertifikat nicht vertrauenswürdig




Wie bereits erwähnt, sind für den Dienstzustand erhöhte Berechtigungen erforderlich. Das Zertifikat für den Statusüberprüfungsprozess muss vom Server als vertrauenswürdig eingestuft

werden.
Andernfalls tritt dieser Fehler auf:



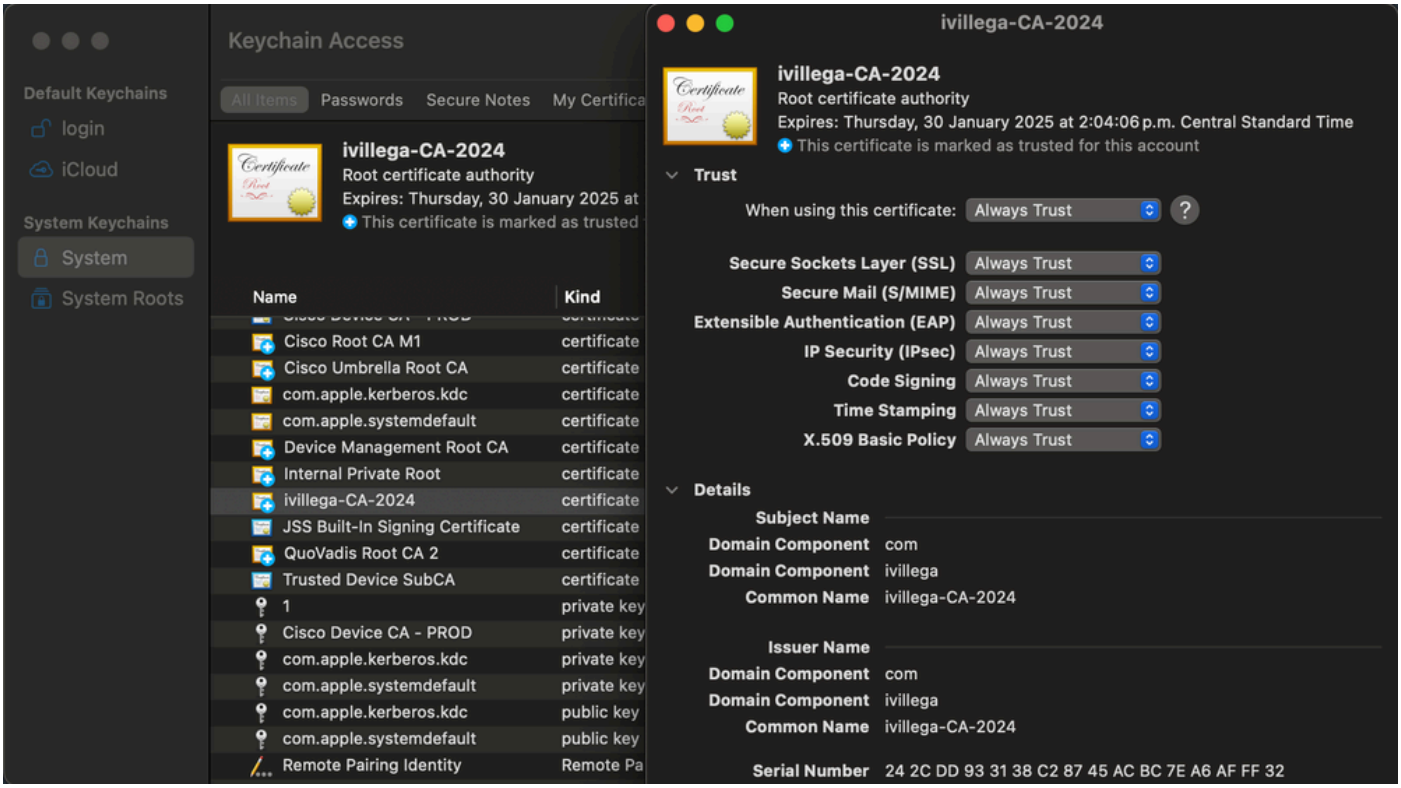

Das ISE Posture-Modul erkennt die PSN-Server entweder anhand der IP-Adresse oder des vollqualifizierten Domänennamens (FQDN). Als Best Practice sollten Sie die Posture-Konfigurationsdateien verwenden, um die ISE-Knoten über FQDN zu erkennen. Daher sollten die Admin- und Portal-Zertifikate (Client Provisioning Portal) den FQDN in das CN- oder SAN-Feld einschließen. Sie können auch hierfür ein Platzhalterzertifikat verwenden. Platzhalterzertifikate werden für diesen Fluss unterstützt.

Aufgrund von Systemsicherheiten kann das CN-Feld in Zukunft nicht mehr als vertrauenswürdig angesehen werden. Fügen Sie als Best Practice den Platzhaltereintrag oder den FQDN in das SAN-Feld ein.

Falls die ISE-PSNs über die IP-Adresse statt über FQDN erkannt werden, muss die IP-Adresse der Knoten entweder im CN-Feld oder im SAN-Feld der Zertifikate enthalten sein, die mit der

Admin- und Portalnutzung verknüpft sind.

ISE-Statusmodule vertrauen dem vom ISE-Server vorgelegten Zertifikat. Wenn sich die Zertifizierungsstelle im Systemzertifikatsspeicher des macOS-Schlüsselbundzugriffs befindet, sollte für diese Zertifizierungsstelle die Einstellung Bei Verwendung dieses Zertifikats auf Immer vertrauen festgelegt sein.




Sie können auf das Fehlverhalten stoßen, dass selbst wenn das Zertifikat korrekt geladen wird und alle CN- und SAN-Anforderungen erfüllt sind, das macOS-System dem Zertifikat immer noch nicht vertraut. Öffnen Sie in diesem Fall die Keychain-Anwendung, navigieren Sie zur Registerkarte System certificate store, und löschen Sie das CA-Zertifikat von dort.

Navigieren Sie anschließend zur macOS-Terminalanwendung, und führen Sie den folgenden Befehl aus: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

{Pfad zu Ihrem Zertifizierungsstellenzertifikat}

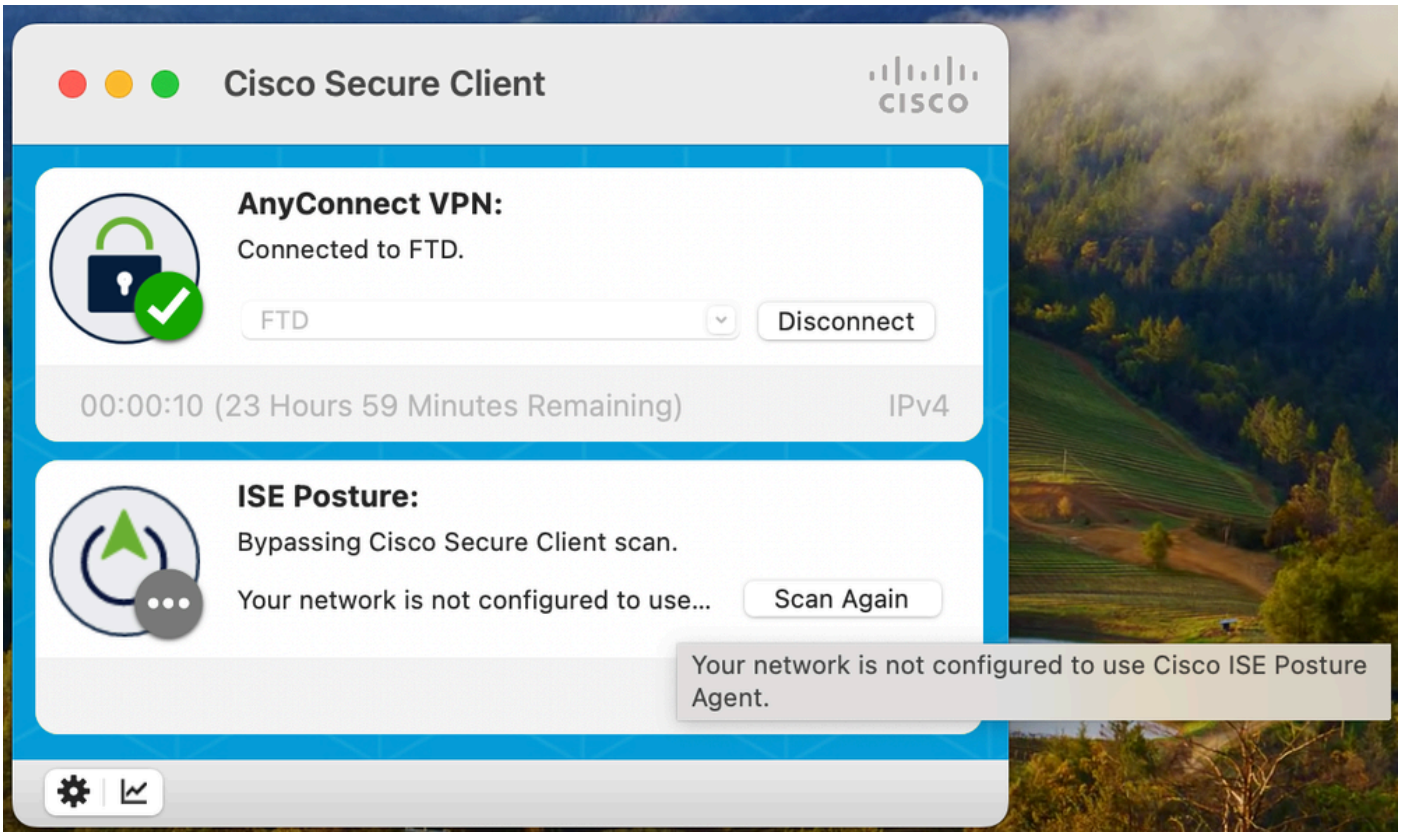
Wenn sich Ihr Zertifikat z. B. in Ihrem Desktop befindet, lautet der Befehl: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

Starten Sie den Computer nach Ausführung des Befehls neu, und versuchen Sie es erneut.

## Umgehen von Cisco Secure Client Scan

Sie können auch die Fehlermeldungen "Umgehen der Cisco Secure Client-Suche" und "Ihr

Netzwerk ist nicht für die Verwendung des Cisco ISE Posture Agent konfiguriert" erhalten:




Diese Meldung wird angezeigt, da in der Client-Bereitstellung unter ISE > Work Centers > Posture > Client Provisioning > Client Provisioning Policies keine Profile konfiguriert wurden.
Auch wenn Sie eine Bedingung für Mac OSX-Betriebssysteme sehen, bedeutet dies nicht, dass Sie alle MacOS-Versionen abdecken.

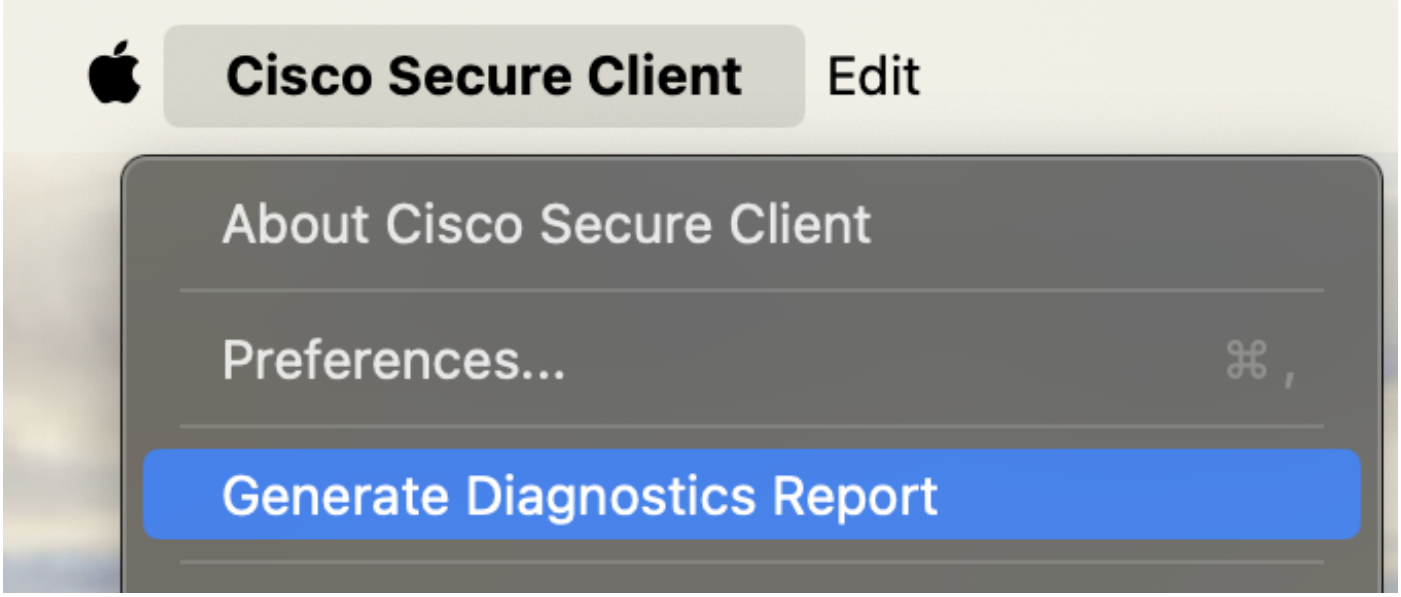
Standardmäßig enthält ISE keine aktuellen macOS-Versionen, wie Sequoia (15.6.x), um solche Nachrichten zu vermeiden, stellen Sie sicher, dass der Status aktualisiert wird.

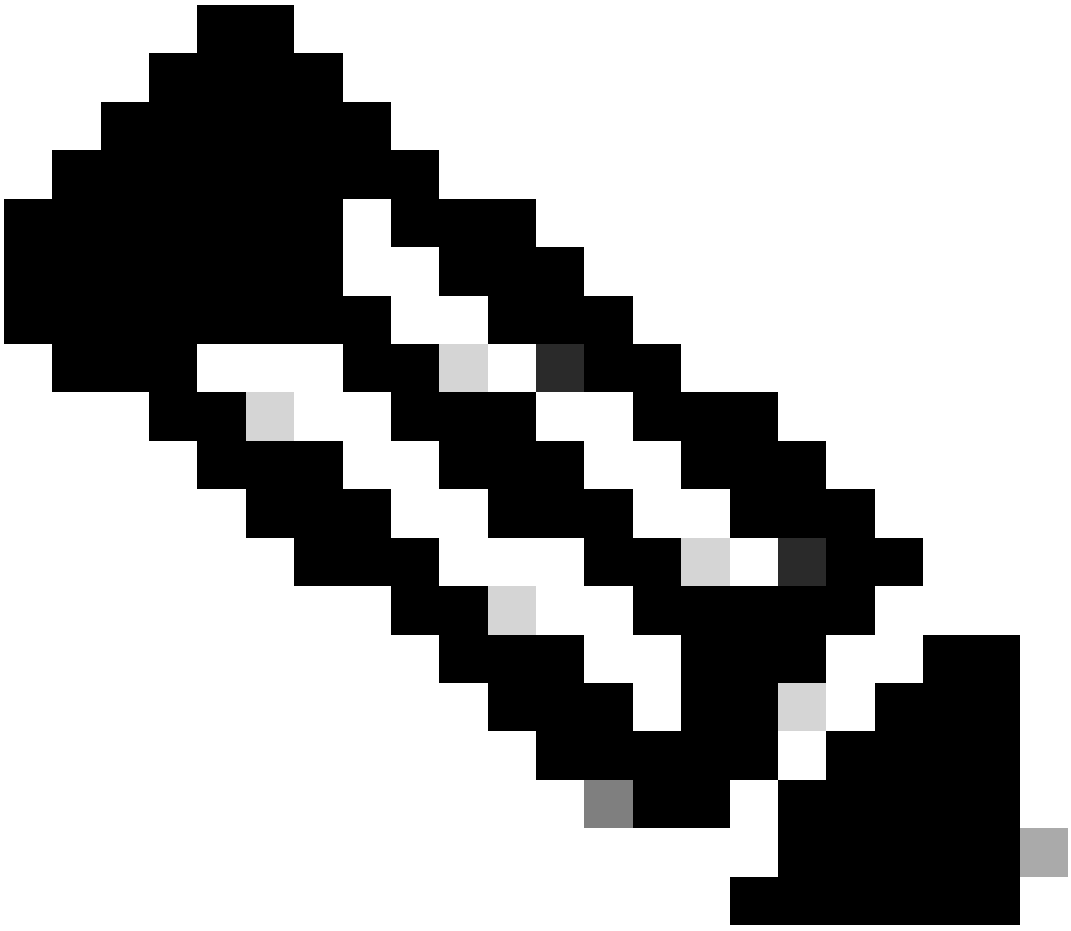
Sie müssen den Status-Feed von ISE aktualisieren > Work Centers > Posture > Settings > Software Updates > Posture Updates.

Dies kann online direkt von der ISE oder offline über eine ZIP-Datei aktualisiert werden, die hier von der Posture Offline-Website heruntergeladen werden kann.

## Sonstige Fragen

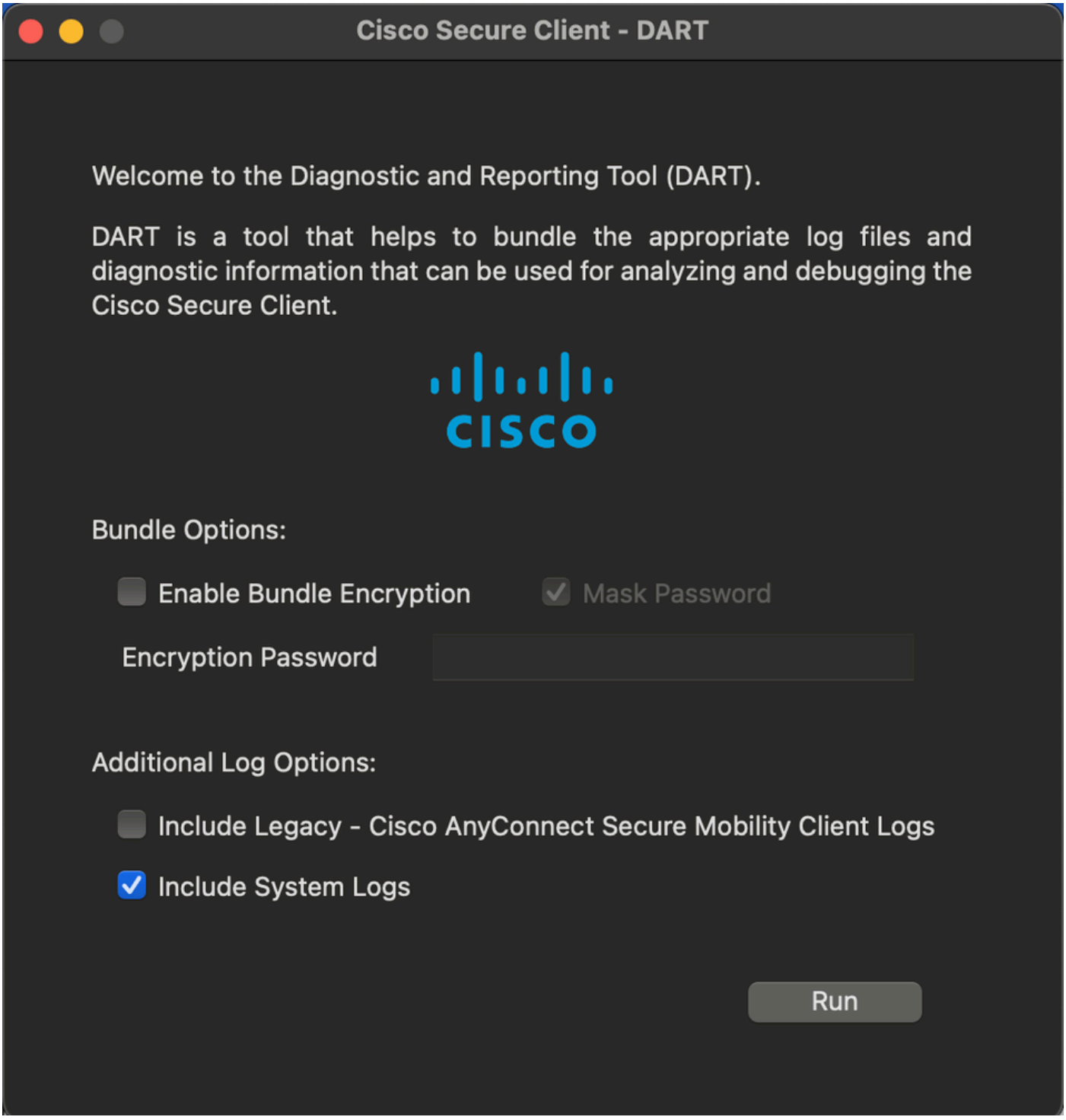
Wenn Sie in die Details gehen möchten, können Sie ein DART-Paket von der postured macOS Gerät sammeln. Dazu muss das DART-Modul installiert sein. Navigieren Sie dann bei aktivierter Cisco Secure Client-Anwendung zur Menüleiste, und klicken Sie auf Cisco Secure Client und dann auf Diagnoseberichte generieren.



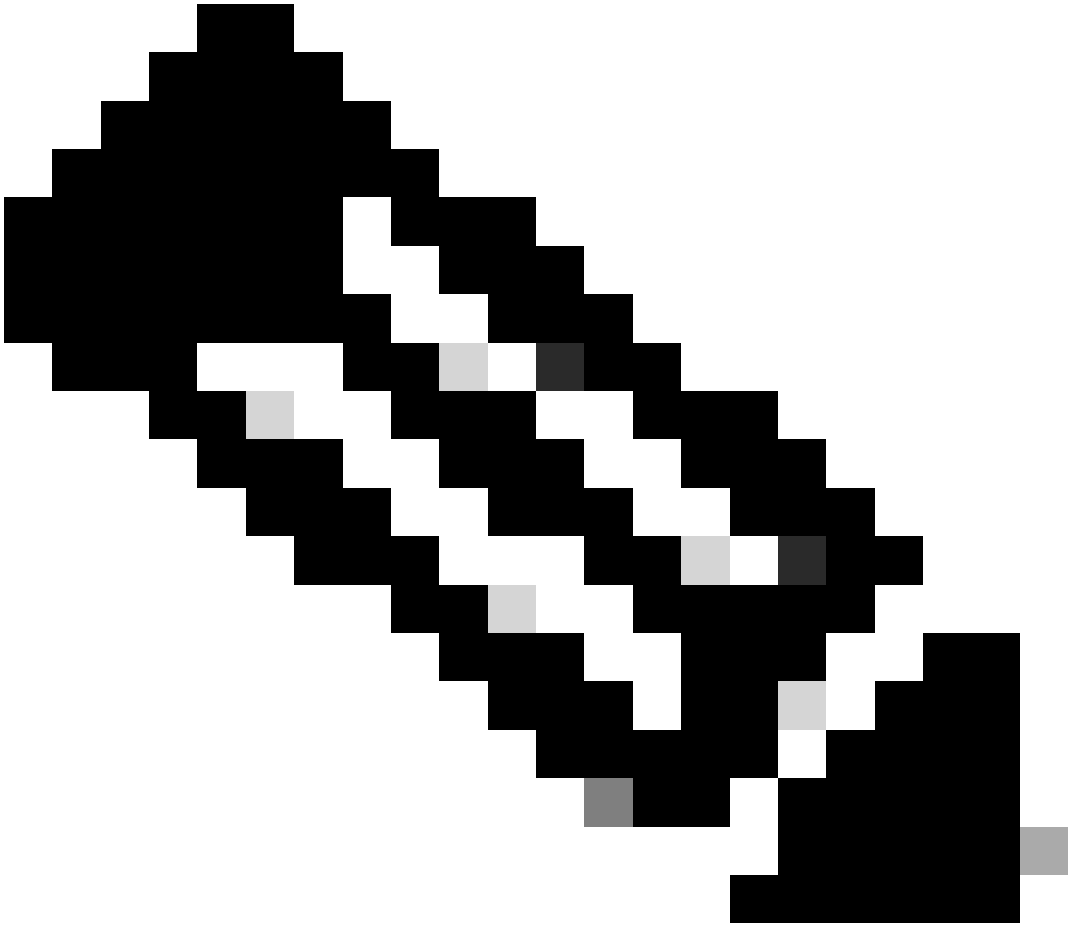



Anmerkung: Es ist wichtig, dass die Option Systemprotokolle einbeziehen beim

Generieren des DART-Pakets aktiviert ist, da sonst das DART-Paket keine ISE-Statusmodulinformationen enthält.




Aus Sicherheitsgründen sind einige der Protokolle möglicherweise verschlüsselt und nicht sichtbar. Im Paket "unified_log.log" des DART werden jedoch möglicherweise ähnliche Protokolle angezeigt, wie hier gezeigt:



Anmerkung: Dieses Protokollbeispiel bezieht sich auf die in diesem Dokument konfigurierte MacOS-Dienstbedingung.

---

```
[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
```

Außerdem können Sie die Statuskomponente auf Debug-Protokollebene im ISE PSN-Knoten festlegen, der den Endpunkt authentifiziert und den Status wiederherstellt.

Sie können diese Protokollstufe über ISE > Vorgänge > Fehlerbehebung > Debug-Assistent > Debug-Protokollkonfiguration konfigurieren. Klicken Sie auf den PSN-Hostnamen, und ändern Sie die Protokollstufe der Posture-Komponente von INFO in DEBUG.

Mit dem gleichen Beispiel für die macOS-Dienstbedingung können Sie ähnliche Protokolle in ise-psc.log sehen:

```
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
```

Falls das Problem weiterhin besteht, erstellen Sie ein TAC-Ticket mit dem Cisco Team.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.