

瞭解和配置macOS服務ISE終端安全評估條件

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[確定要檢查的服務名稱](#)

[（可選）檢查服務的詳細資訊，以定義其是代理還是代理](#)

[選擇要評估的服務運營商](#)

[已載入的服務](#)

[未載入的服務](#)

[已載入並運行](#)

[已載入退出代碼](#)

[已載入並正在運行或帶有退出代碼](#)

[為此條件配置要求和狀態策略](#)

[驗證](#)

[疑難排解](#)

[證書不受信任](#)

[繞過思科安全客戶端掃描](#)

[其他問題](#)

簡介

本文檔介紹在思科ISE中配置macOS服務條件的過程。

必要條件

需求

思科建議您瞭解以下主題：

- MacOS基礎知識。
- 瞭解ISE終端安全評估流程。



附註：本文檔介紹macOS服務條件的配置。本文檔未涵蓋初始狀態配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE 3.3補丁1
- 運行Sonoma 14.3.1的MacOS裝置
- 思科安全使用者端5.1.2.42
- 合規性模組版本4.3.3432.64000

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

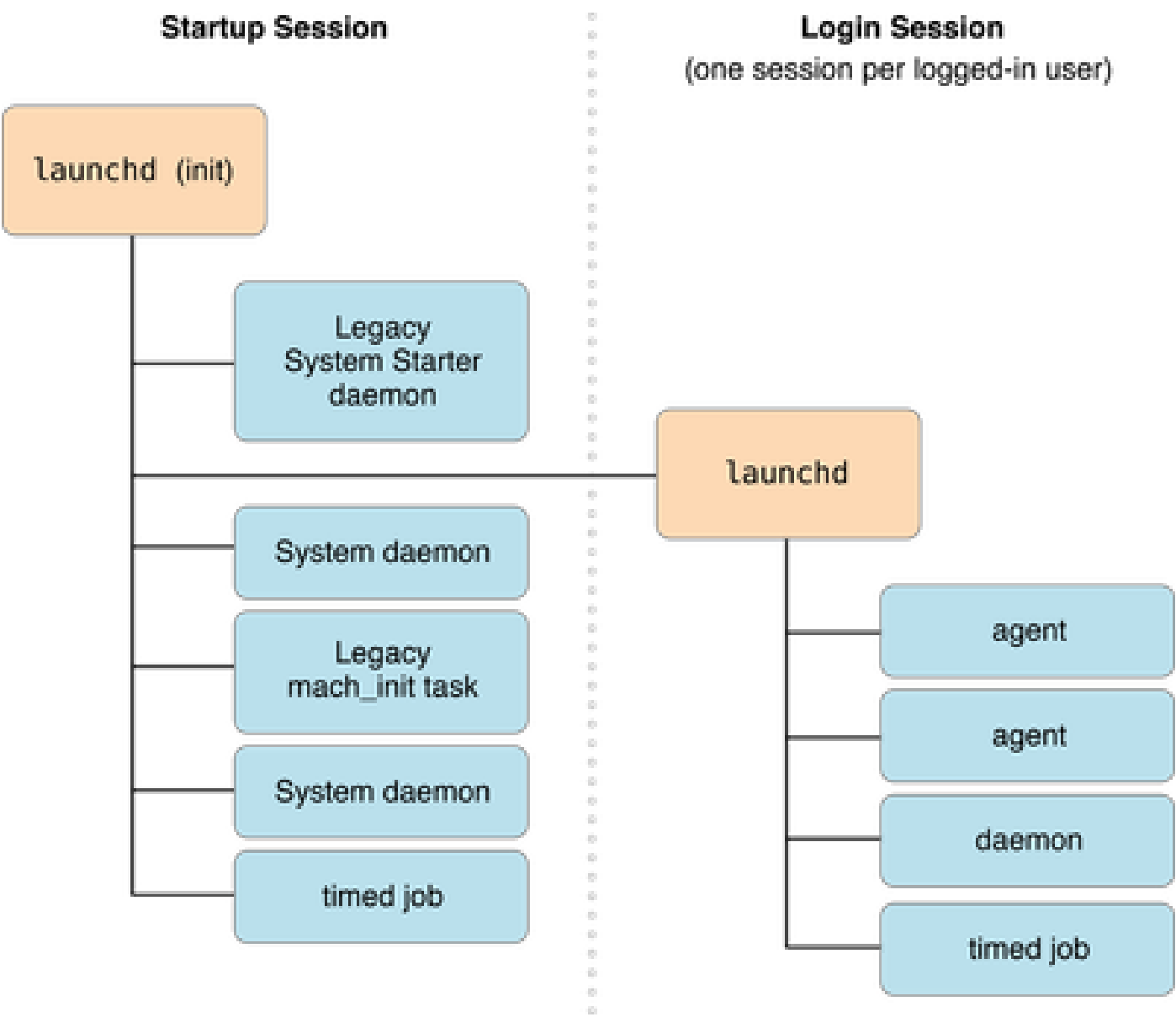
當您必須使用用例檢查服務是否載入到macOS裝置時，macOS服務條件非常有用，還允許您檢查

服務是否正在運行或未運行。macOS服務條件可以檢查兩種不同的服務型別：守護程式和代理。

守護程式是在後台作為整個系統的一部分運行的程式（也就是說，它不與特定使用者相關聯）。守護程式無法顯示任何GUI;更具體地說，它不允許連線到window伺服器。Web伺服器是守護程式的完美示例。

代理是在後台代表特定使用者運行的進程。代理非常有用，因為它們可以做守護程式無法做到的事情，例如可靠地訪問使用者的主目錄或連線到視窗伺服器。日曆監視程式是代理程式的良好示例。

在下圖中，您可以看到每個裝置如何根據裝置啟動和使用者登入進行載入：



有關守護程式和代理的更多資訊，請參閱[Apple文檔](#)

在以下位置可以找到MacOS裝置上可用的請求和代理：

位置	說明
----	----

~/庫/啟動代理	使用者提供的按使用者代理。
/Library/LaunchAgents	由管理員提供的按使用者代理。
/Library/LaunchDaemons	由管理員提供的系統範圍守護程式。
/System/Library/LaunchAgents	OS X每使用者代理
/System/Library/LaunchDaemons	OS X系統範圍守護程式

可以使用以下命令從macOS終端檢查每個類別的清單：

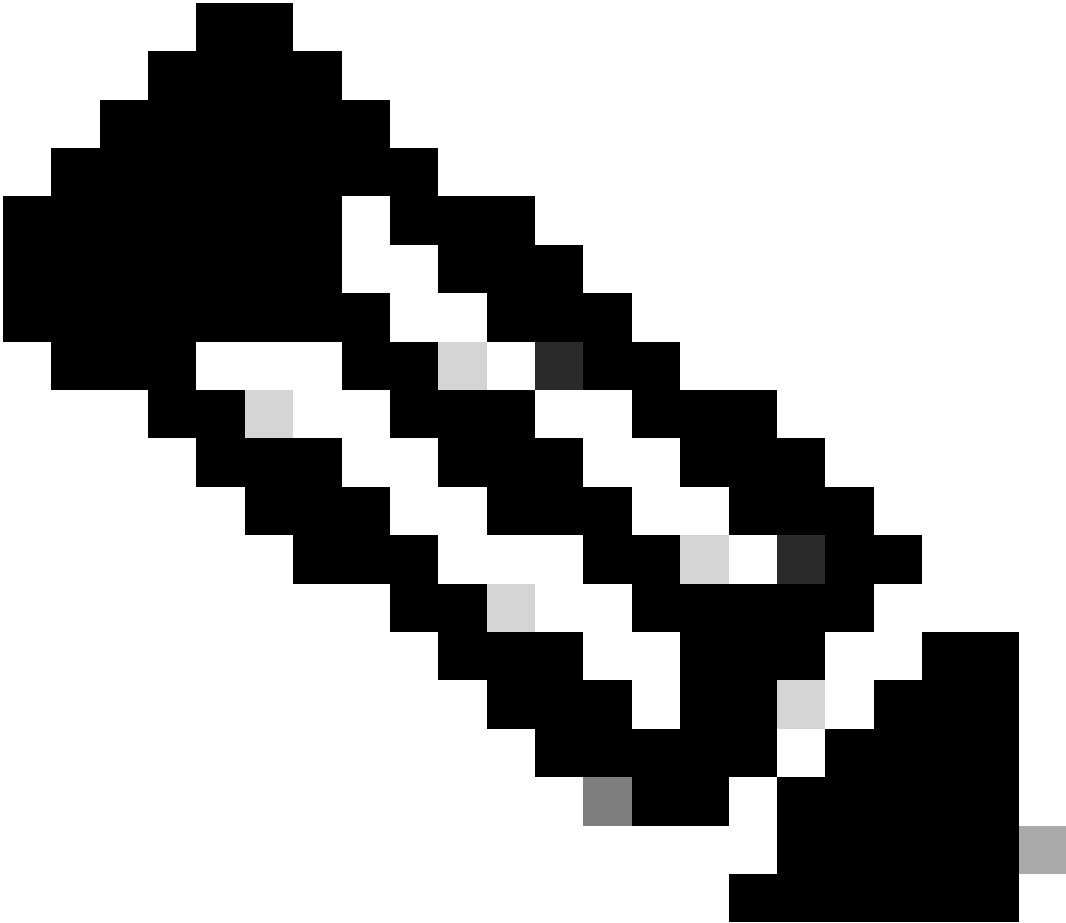
```
ls -ltr ~/Library/LaunchAgent
ls -ltr /Library/LaunchAgent
ls -ltr /庫/啟動守護程式
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/Launch守護程式
```

前面的位置可以顯示macOS裝置上可用的所有守護程式和代理，但並非所有守護程式和代理都已載入或運行。

設定

可以使用以下步驟配置macOS服務條件：

- 1.確定要檢查的服務名稱。
- 2.（可選）檢查服務的詳細資訊，以定義其是座席還是管理員。
- 3.選擇要評估的服務運營商。
- 4.為此條件配置需求和狀態策略。



附註：服務狀態條件需要提升的許可權才能工作，因此，思科安全客戶端（以前稱為 AnyConnect）必須信任ISE PSN — [參考指南](#)

確定要檢查的服務名稱

ISE終端安全評估合規性模組能夠檢查載入、運行和載入的服務以及運行退出代碼。

使用`sudo launchctl dumpstate` 命令檢查已載入的服務。

要檢查已載入的服務並具有退出代碼，請使用命令`sudo launchctl list`。

前面的命令可以突然顯示許多資訊，而使用這些命令只顯示實際的服務名稱：

要僅檢查已載入的服務名稱，請使用以下命令：

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

要僅檢查已載入的服務名稱並具有退出代碼，請使用以下命令：

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

這些命令會顯示大量資訊，因此建議您在每個命令的結尾使用另一個grep過濾器來查詢要查詢的服務。

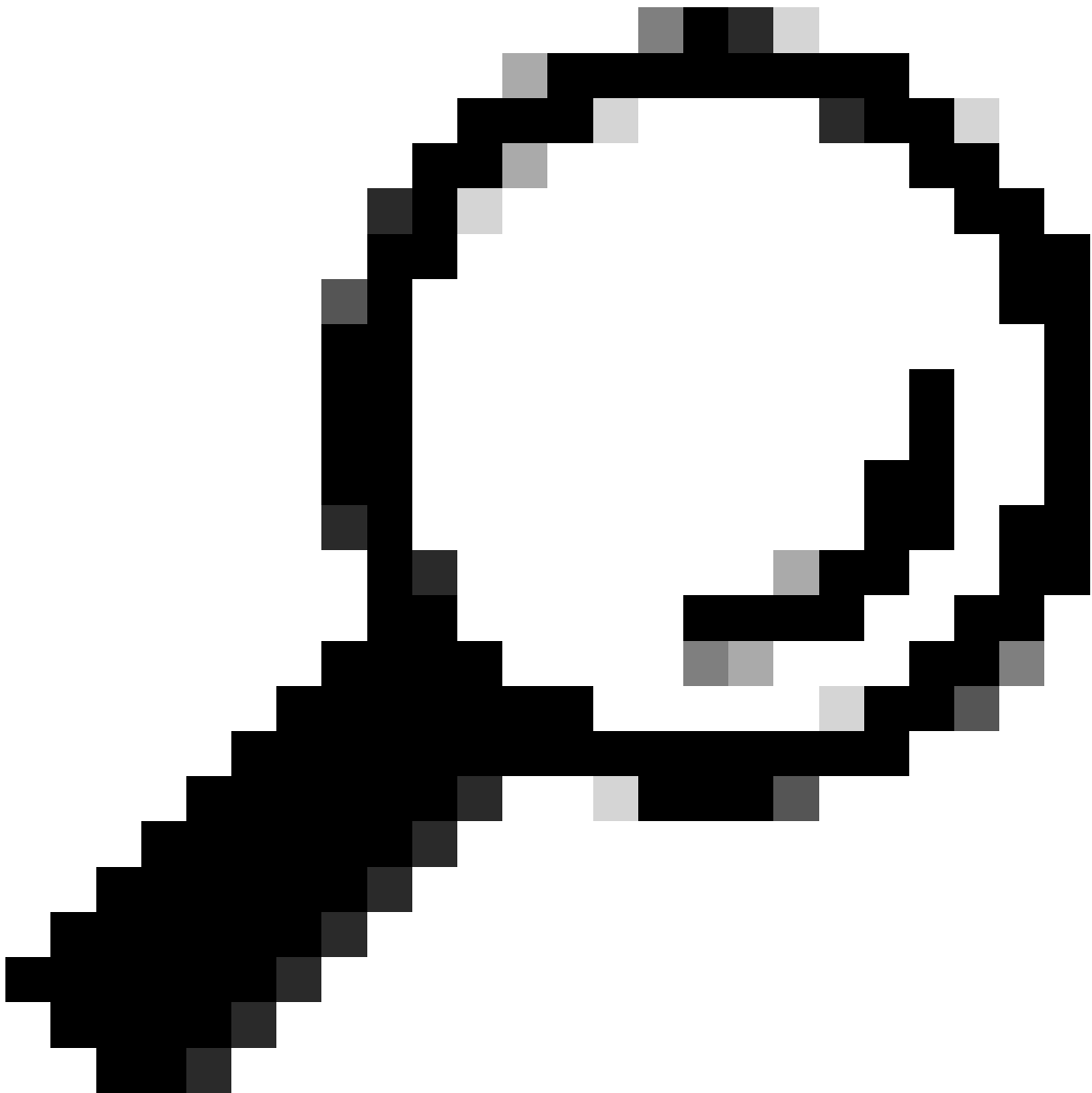
例如，如果您正在查詢供應商特定的服務，則可以在和處使用關鍵字作為過濾器。

對於思科服務，命令如下所示：

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

(可選) 檢查服務的詳細資訊，以定義其是代理還是代理

在此條件配置的第二部分，您需要檢查您的服務是守護程式型別還是代理型別。



提示：此步驟是可選的，因為ISE允許您為守護程式或使用代理選擇選項，因此您可以只選擇該選項並跳過此部分。

如果要在此情況下具有精細度，可以執行以下操作來檢查型別：

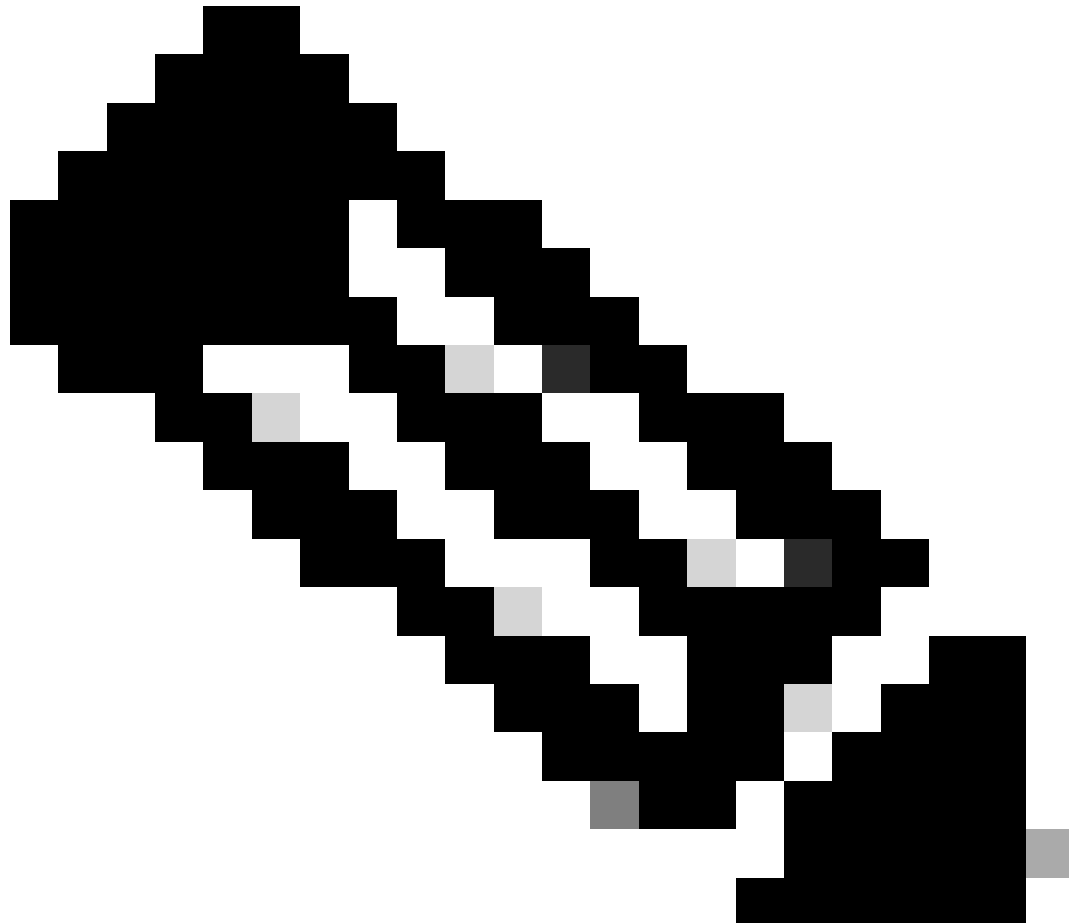
1. 首先，使用命令`sudo grep -B 10 -A 10 -E "^s*state = " << "$(launchctl dumpstate)"`檢查服務的launchctl全名 | `grep -aiE "V.*= {" | sed 's|.|/|;s| = {|'| | grep -i {您的服務名}`

例如，對於命令`sudo grep -B 10 -A 10 -E "^s*state = " << "$(launchctl dumpstate)" | grep -aiE "V.*= {" | sed 's|.|{3}|$/' | grep -i com.cisco.secureclient.iseposture`，輸出為：
：gui/501/com.cisco.secureclient.iseposture。

2. 使用`sudo launchctl print { Your launchctl service name } | grep -i 'type = Launch'`命令檢查服務型別

以下示例中的命令：`sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch'`，輸出為：`type = LaunchAgent`。

這表示服務型別為Agent，否則將顯示`type = LaunchDaemon`。



附註：如果資訊為空，請選擇ISE中Daemon或User Agent的選項作為服務型別設定。

選擇要評估的服務運營商

ISE允許您選擇5個不同的服務運營商：

- 已載入
- 未載入
- 已載入並運行
- 已載入退出代碼
- 已載入並正在運行或使用退出代碼

已載入的服務

使用這兩個命令時列出的所有服務是：

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

未載入的服務

是定義了其屬性清單(plist)但尚未載入的所有服務，還是甚至未定義屬性清單(plist)因而根本無法載入的服務。

這些服務不易識別，當您需要檢查特定服務是否不應存在於macOS裝置時，最常用於使用案例。例如，如果要阻止在macOS裝置上載入縮放服務，可以將us.zoom.ZoomDaemon作為該服務的值，這樣可以確保縮放未運行或根本沒有安裝。

存在無法解除安裝的服務，並且已定義其屬性清單。

例如，使用此命令，您可以看到dhcp6d plist已定義：

```
ls -ltr /System/Library/Launch守護程式 | grep com.apple.dhcp6d.plist
```

在檢查服務清單時，可以看到未載入的項：

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

如果將該值設定為com.apple.dhcp6d"，則macOS裝置是相容的，因為即使定義了服務清單，系統也不會載入該服務。

已載入並運行

並非所有服務都在運行，每個服務有多個狀態，如正在運行、未運行、等待、退出、未初始化等。要檢查所有正在運行的服務，請使用以下命令：

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

使用上述命令列出的服務命中Loaded & Running service operator條件。

已載入退出代碼

某些服務可能會以預期或意外的退出代碼終止，此類服務可以通過命令列出：

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

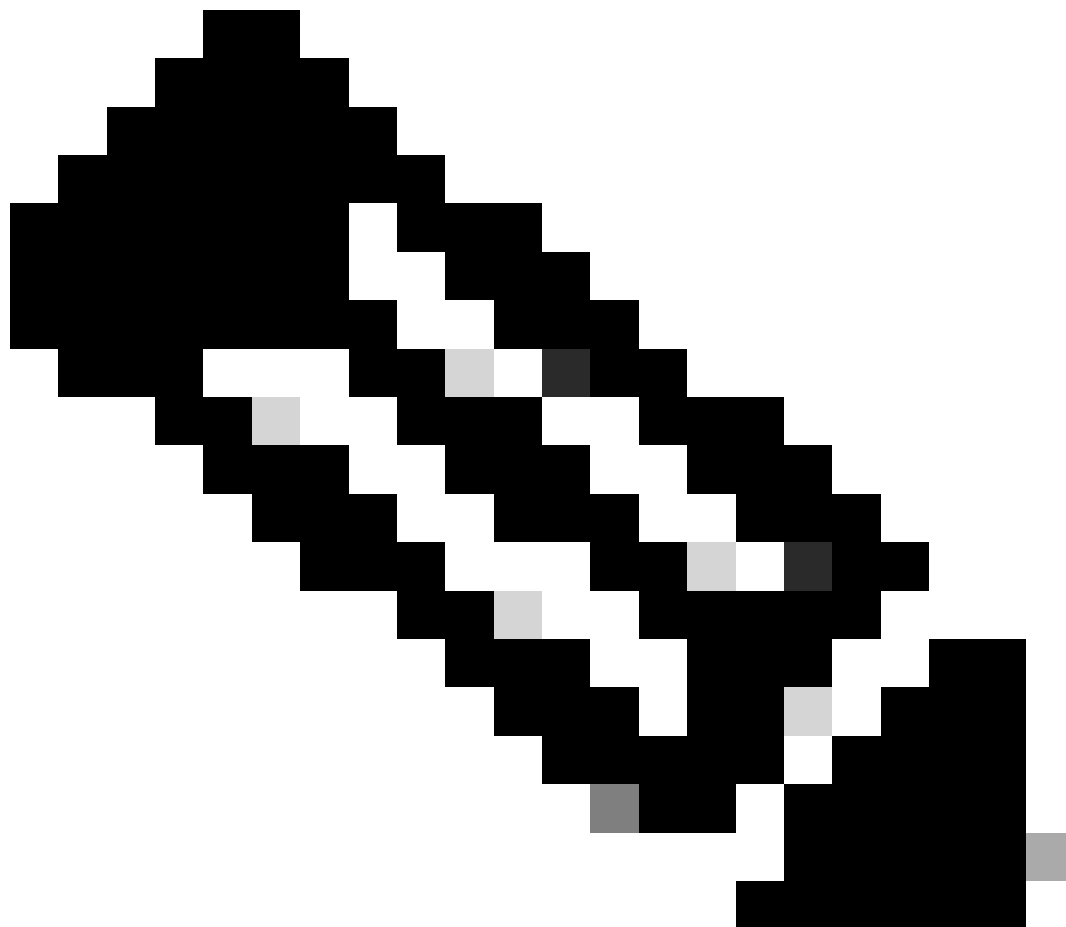
要瞭解其退出代碼，您可以選取任何服務並使用命令：

```
sudo launchctl print {您的launchctl服務名} | grep -i '上次退出代碼'
```

舉例來說：

```
sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i '上次退出代碼'
```

其輸出為：最後一個退出代碼= 0



附註：在這裡，退出代碼0通常表示服務已正確執行所有操作。如果電腦與退出代碼的0不匹配，則表示服務未執行預期操作。

已載入並正在運行或帶有退出代碼

當服務為Loaded & Running或Loaded with exit code時，最後一個選項起作用。

此圖顯示macOS服務條件的示例。

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

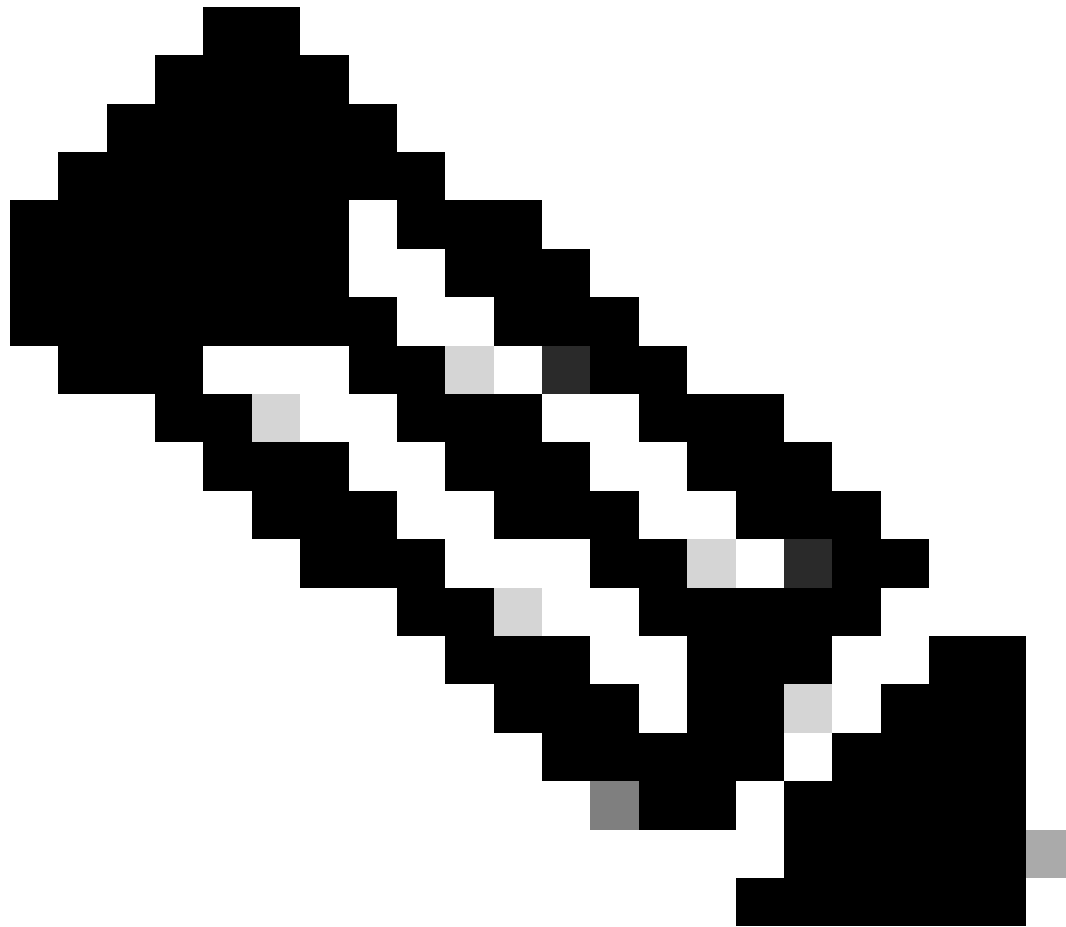
Daemon Or User Agent

Service Operator

Loaded & Runnin

exit code

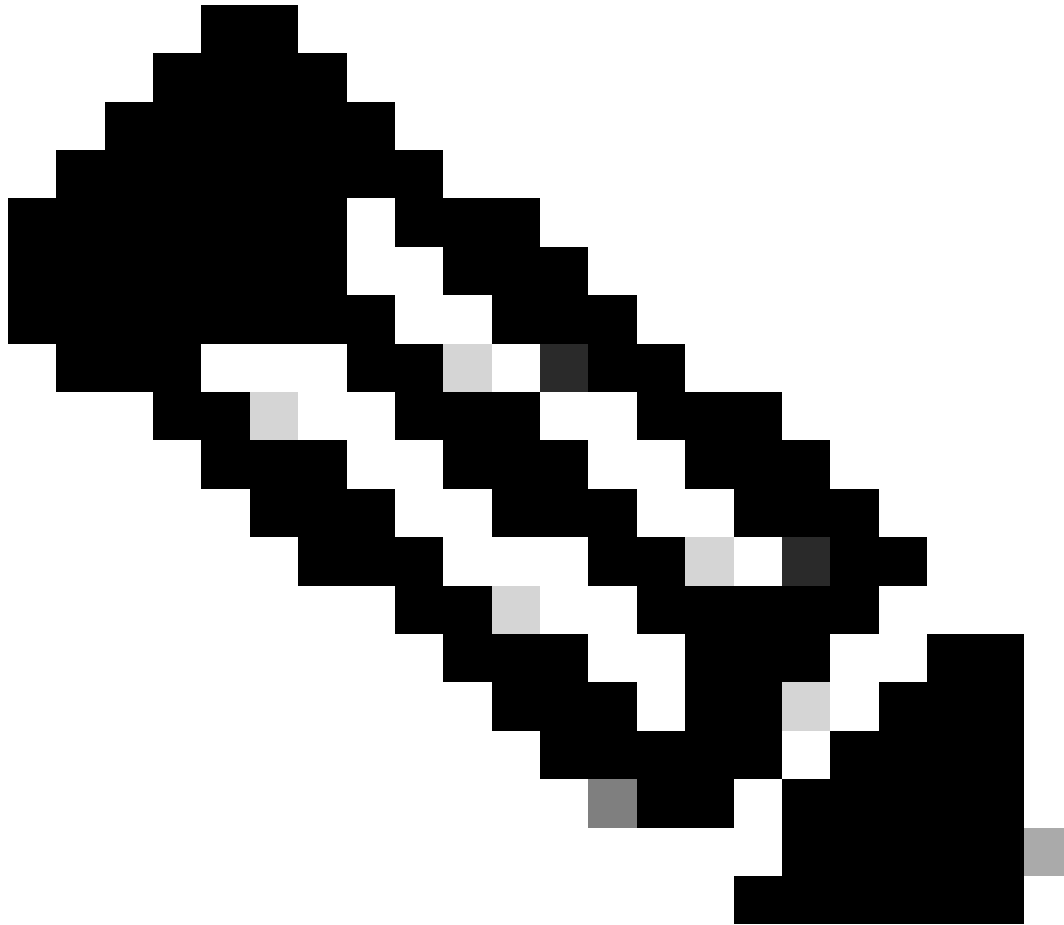
0



附註：目前，僅支援確切的服務名稱。服務名稱中有支援萬用字元的功能增強要求，思科錯誤ID [CSCwf01373](#)

為此條件配置要求和狀態策略

配置完條件後，您需要為此條件建立要求，並為此要求使用Message Test Only選項。
導航到ISE >工作中心>狀態>要求以建立它。



附註：沒有針對服務條件的補救選項。

Identity Services Engine

Work Centers / Posture

Q 🔔 ⓘ 🔔 🔍

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Conditions

Anti-MalwareAnti-SpywareAnti-VirusApplicationCompoundDictionary CompoundDictionary SimpleDisk EncryptionExternal DataSourceFileFirewallHardware AttributesPatch ManagementRegistryScriptServiceUSB

Remediations

Requirements

Guide Me

service

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions
macOS-Service-Requireme	for Mac OS X	using 4.x or later	using Agent	met if

Remediation Action Details

Message TextOnly

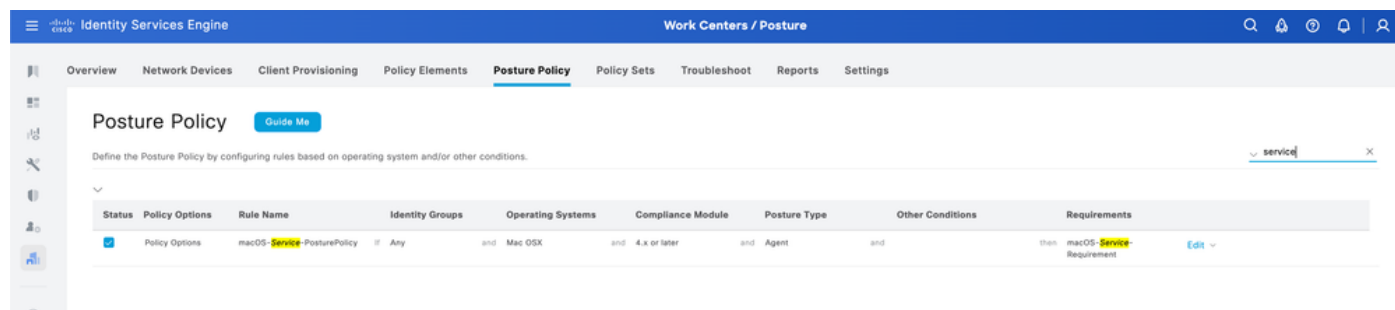
MessagemacOS Service is non compliant

Note:
Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

SaveReset

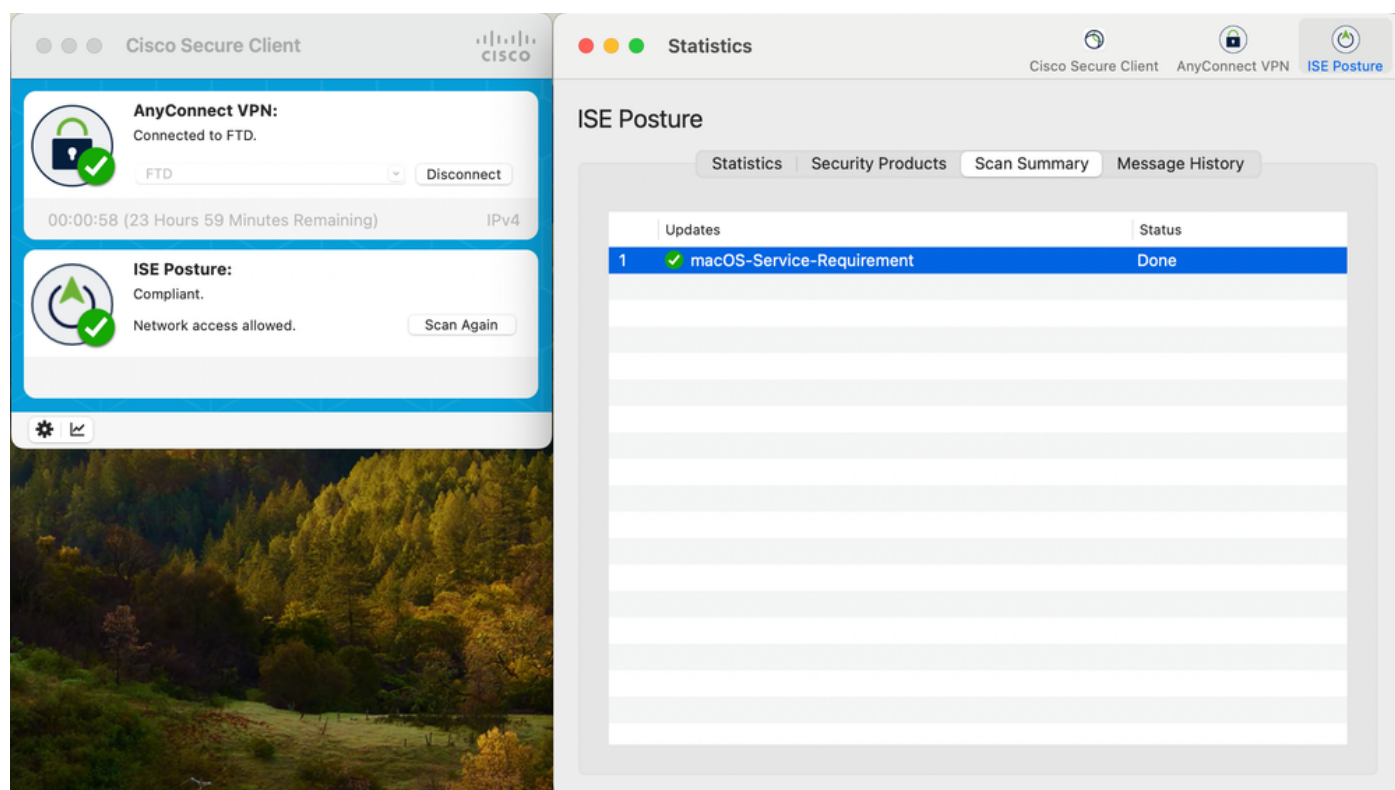
完成此操作後，最後一步是配置使用建立要求的終端安全評估策略。
導航到ISE > Work Centers > Posture > Posture Policy建立策略。

啟用新策略，根據需要命名它，然後選擇剛創建的要求。

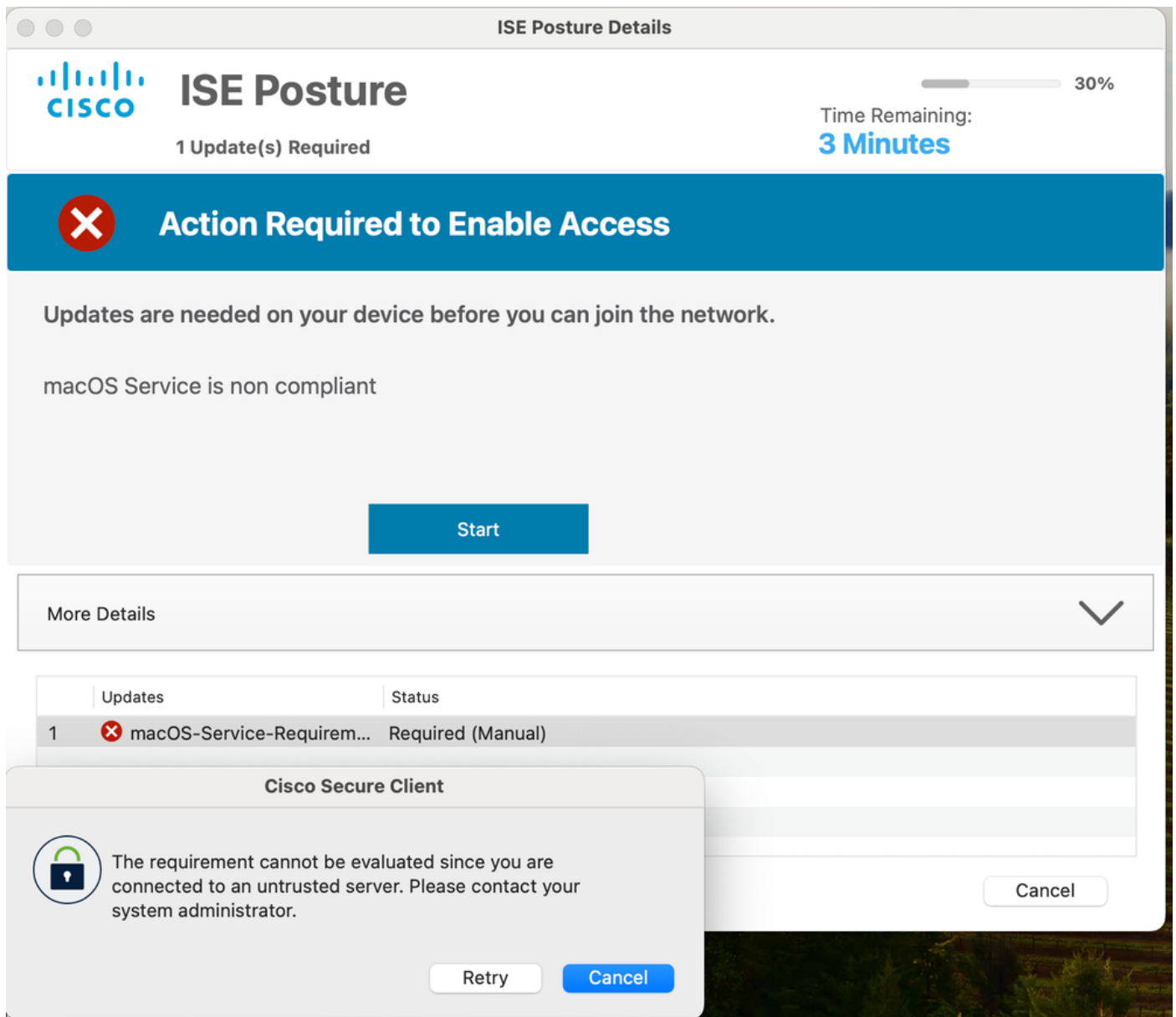


驗證

您可以從Cisco安全客戶端GUI本身驗證macOS狀態條件通過或失敗。



此外，您可以從ISE > Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint檢查ISE終端安全評估。

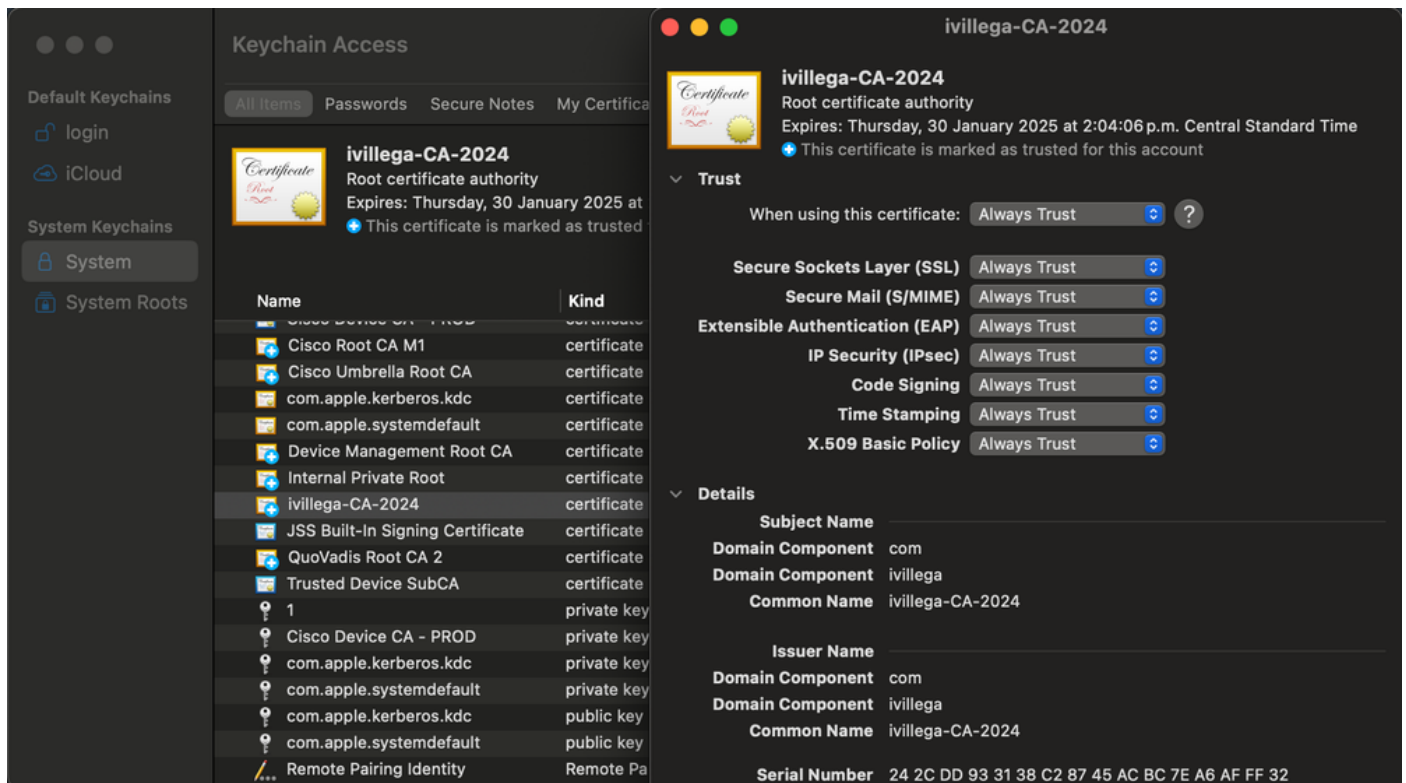


ISE終端安全評估模組通過IP地址或完全限定域名(FQDN)發現PSN伺服器。最佳實踐是使用Posture配置檔案通過FQDN發現ISE節點，因此Admin和Portal(Client Provisioning Portal)證書應將FQDN包含在CN欄位或SAN欄位中。您也可以為此使用萬用字元證書，此流支援萬用字元證書。

由於系統安全原因，CN欄位在將來不可信。最佳做法是在SAN欄位中包括萬用字元項或FQDN。

如果通過IP地址而不是FQDN發現ISE PSN，則要求節點的IP地址包含在與管理員和門戶使用相關的證書的CN欄位或SAN欄位中。

ISE終端安全評估模組信任由ISE伺服器提供的證書。如果其CA在macOS Keychain access的系統證書儲存中，則此CA應將When using this certificate設定為Always Trust。



您可能會遇到以下錯誤行為：即使正確載入了證書，並且滿足了所有CN和SAN要求，macOS系統仍不信任證書。在這種情況下，請開啟Keychain access應用程式，導航到「System certificate store」頁籤，然後從那裡刪除CA證書。

然後，導航到macOS終端應用程式並執行以下命令：`sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain`

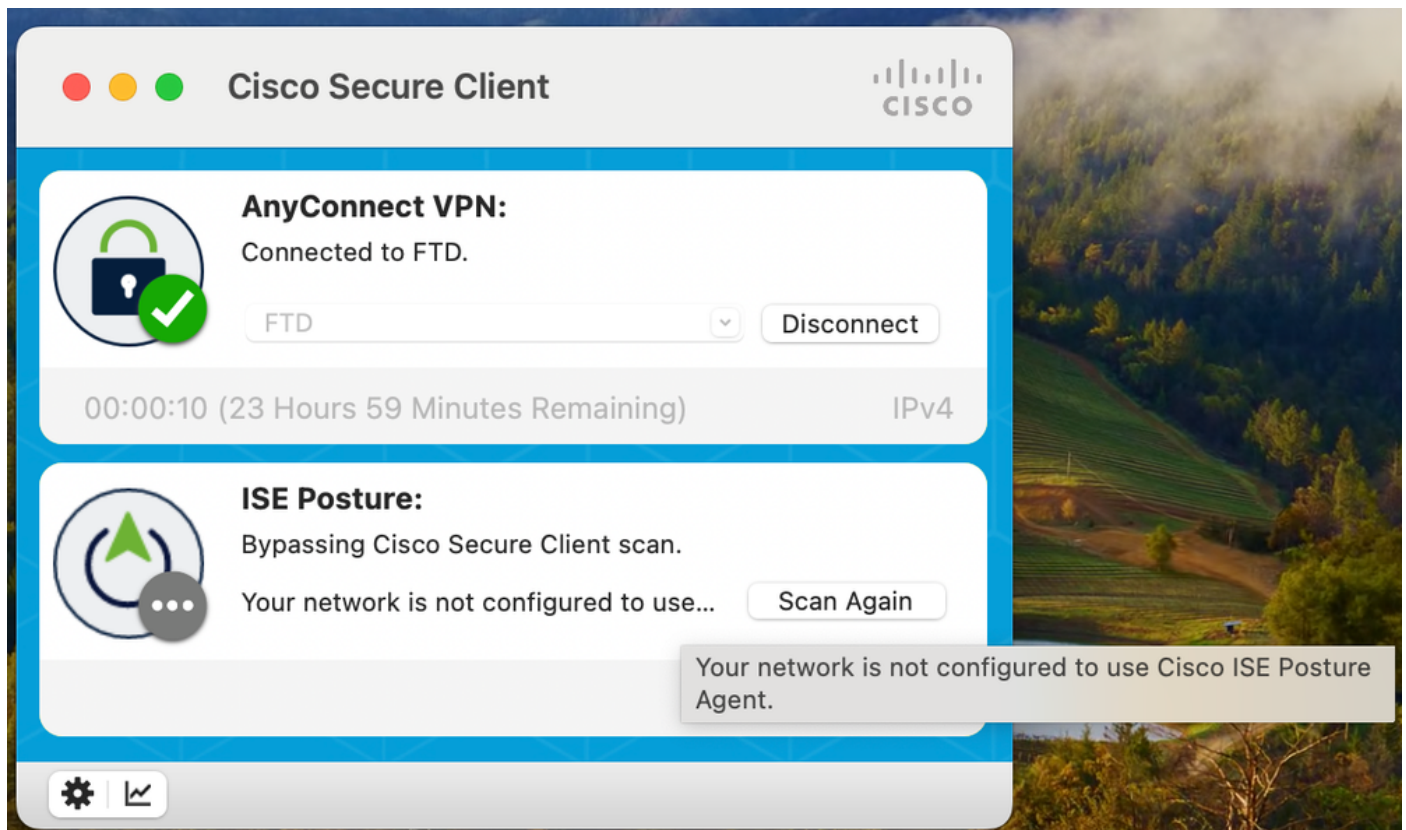
{CA證書的路徑}

例如，如果您的憑證位於您的案頭中，命令如下：`sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt`

執行命令後，請重新啟動電腦並重試。

繞過思科安全客戶端掃描

您還可能遇到錯誤消息「Bypassing Cisco Secure Client Scan」和「Your network is not configured to use Cisco ISE Posture Agent」：



出現此消息是因為在ISE > Work Centers > Posture > Client Provisioning > Client Provisioning Policies的客戶端調配中沒有配置配置檔案。

雖然您可能看到Mac OSX作業系統的情況，但這並不意味著您涵蓋了所有的macOS版本。

預設情況下，ISE不包含最新的macOS版本，例如Sequoia(15.6.x)，以避免此類消息以確保該狀態更新。

您必須從ISE > Work Centers > Posture > Settings > Software Updates > Posture Updates更新Posture feed。

可以直接從ISE線上更新，也可以通過可從狀態離線站點下載的zip文件[離線更新](#)

其他問題

如果您想瞭解詳細資訊，可以從姿勢的macOS裝置收集DART捆綁包。為此，您必須安裝DART模組，然後啟用Cisco Secure Client應用程式，導航到Menu欄並按一下Cisco Secure Client，然後在Generate Diagnostics Reports中按一下。



Cisco Secure Client

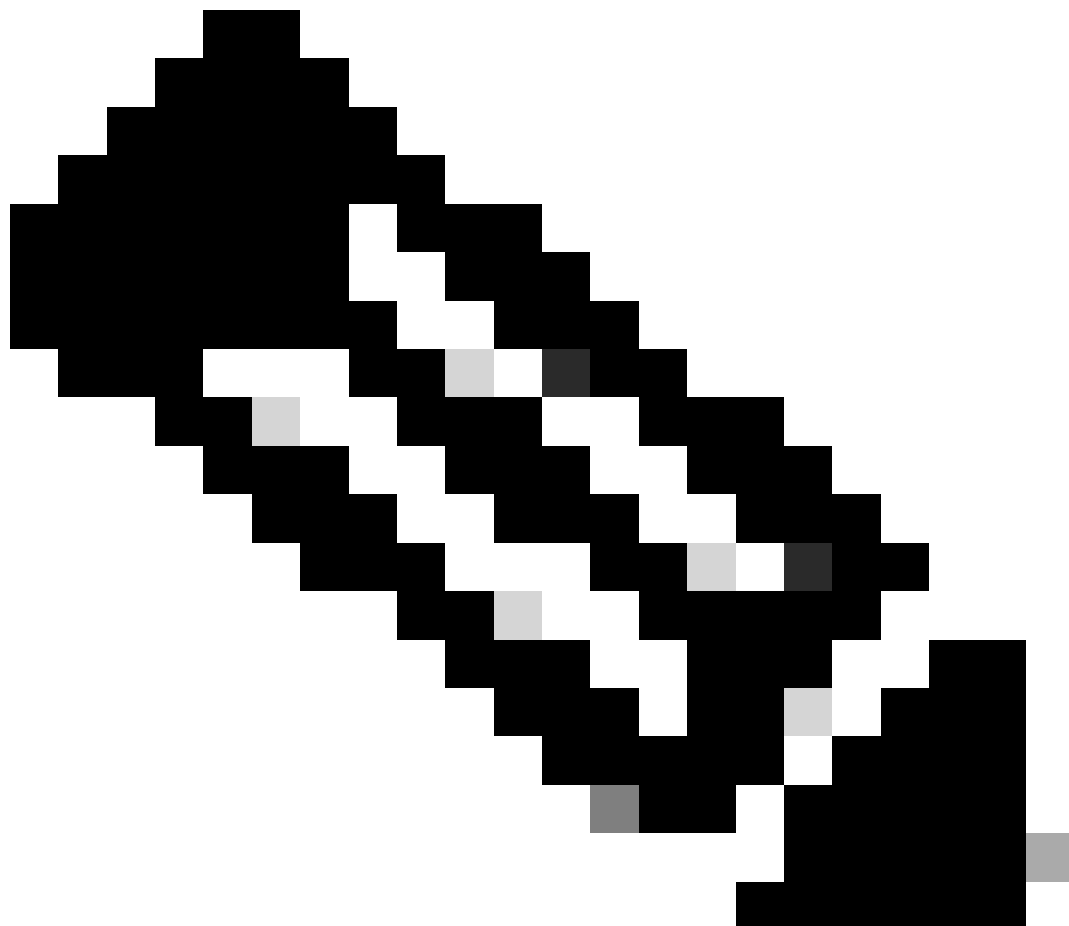
Edit

About Cisco Secure Client

Preferences...



Generate Diagnostics Report

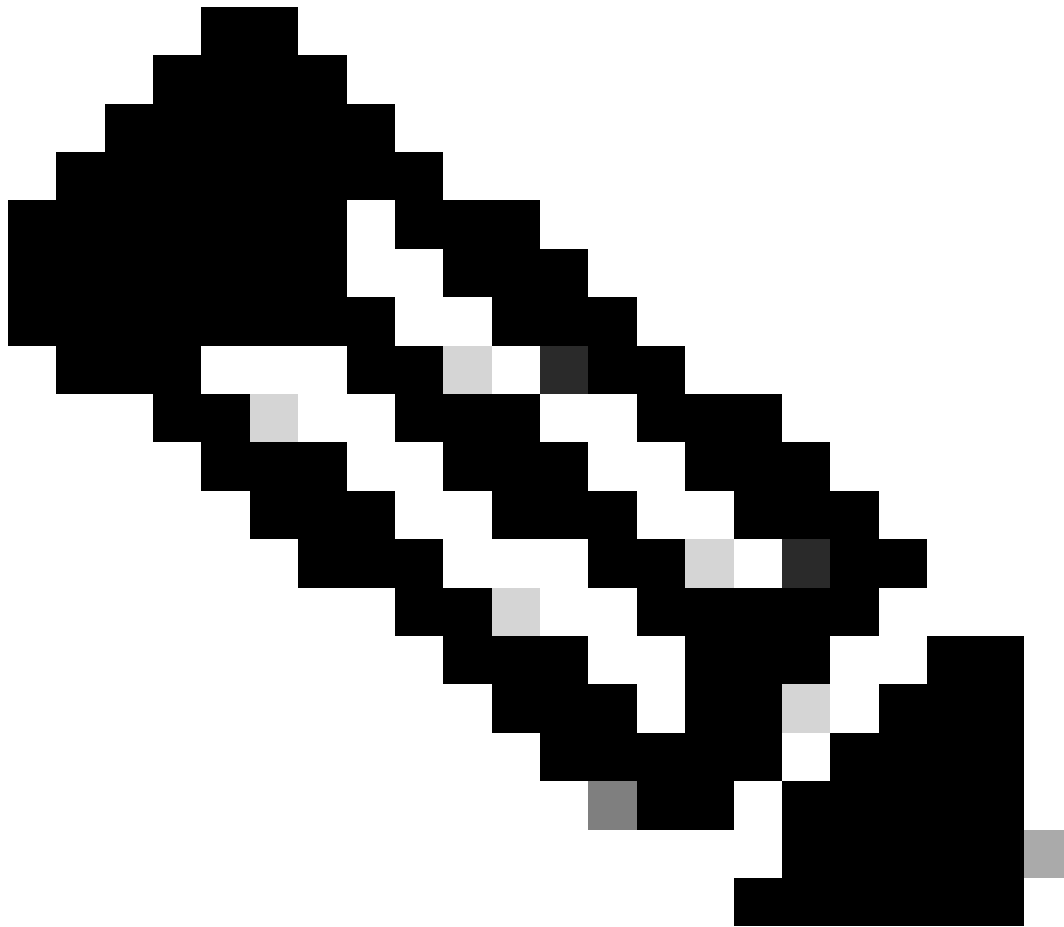


附註：在生成DART捆綁包時，必須啟用Include System Logs選項，否則DART捆綁包不會

包含ISE終端安全評估模組資訊。



由於安全原因，某些日誌可能已被加密且不可見，但在DART捆綁包的unified_log.log中，您可能會看到類似日誌，如下所示：



附註：此日誌示例適用於本文檔中配置的macOS服務條件。

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

macOS-Service-Condition

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: Rqmt.cpp
```

此外，您還可以在ISE PSN節點中將posture元件設定為調試日誌級別，該節點對終端進行身份驗證和定位。

您可以通過ISE > Operations > Troubleshoot > Debug Wizard > Debug Log Configuration配置此日誌級別。單擊PSN Hostname並將Posture component 日誌級別從INFO更改為DEBUG。

使用與macOS服務條件相同的示例，您可以在ise-psc.log中看到類似的日誌：

```
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)

]

如果問題仍然存在，請向思科團隊提出TAC通知單。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。