Entender e Configurar a Condição de Postura do ISE do Serviço macOS

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configurar
  - Identificar o Nome do Serviço a Ser Verificado
  - (Opcional) Verifique os detalhes do serviço para definir se é um agente ou um deamon
  - Selecione o operador de serviço a ser avaliado
  - Serviços carregados
  - Serviços não carregados
  - Carregado e em execução
  - Carregado com código de saída
  - Carregado e em execução ou com código de saída
  - Configurar a Política de Requisito e Postura para Tal Condição
- Verificar
- Troubleshooting
  - Certificado não confiável
  - Ignorando o Cisco Secure Client Scan
  - Outros problemas

Introdução

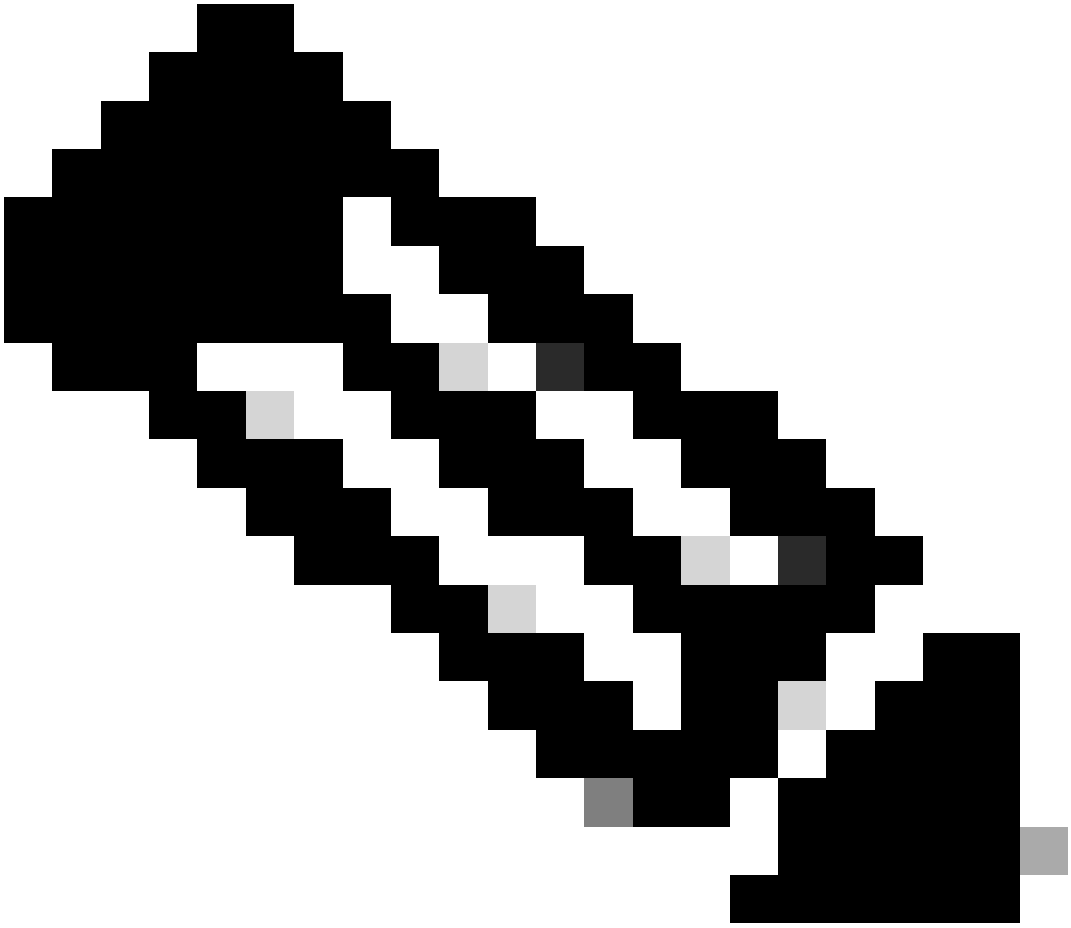
Este documento descreve o processo de configuração da condição de serviço do macOS no Cisco ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do macOS.
- Conhecimento sobre o fluxo de postura do ISE.



Note: Este documento aborda a configuração para a condição de serviço do macOS. A configuração inicial da postura não é abordada neste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Patch 1 do Cisco ISE 3.3
- dispositivo macoOS executando Sonoma 14.3.1
- Cisco Secure Client 5.1.2.42
- Módulo de conformidade versão 4.3.3432.64000

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

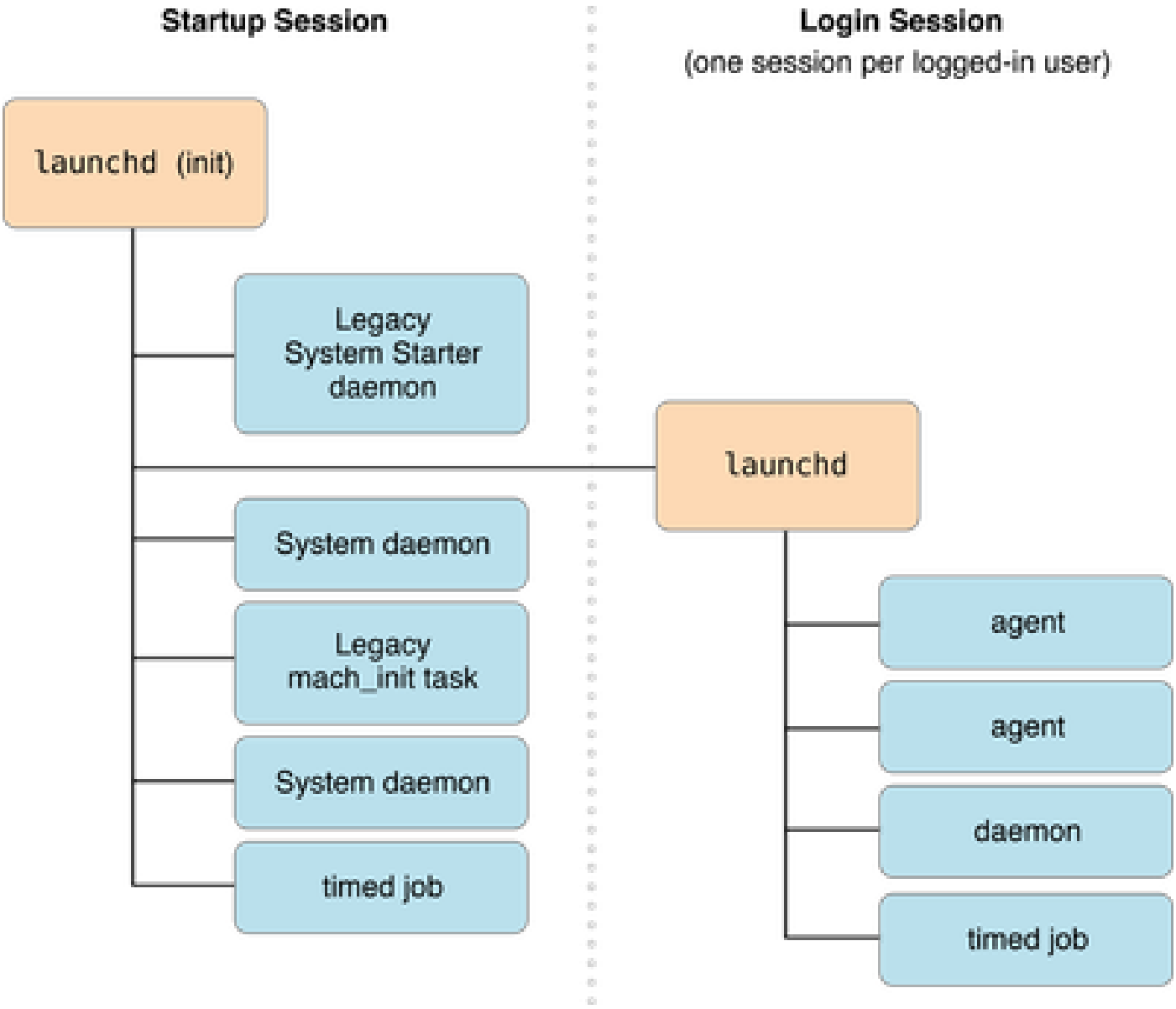
Informações de Apoio

a condição de serviço macOS é útil quando você tem que usar um caso para verificar se um serviço está carregado no dispositivo macOS e também permite verificar se ele está em execução ou não. A condição de serviço macOS pode verificar dois tipos de serviço diferentes: daemons e agentes.

Um daemon é um programa executado em segundo plano como parte do sistema geral (ou seja, não está vinculado a um usuário específico). Um daemon não pode exibir nenhuma GUI; mais especificamente, não é permitido conectar-se ao servidor windows. Um servidor web é o exemplo perfeito de um daemon.

Um agente é um processo executado em segundo plano em nome de um usuário específico. Os agentes são úteis porque podem fazer coisas que os daemons não podem, como acessar com segurança o diretório inicial do usuário ou conectar-se ao servidor de janelas. Um programa de monitoramento de calendário é um bom exemplo de agente.

No diagrama abaixo, você pode ver como cada um é carregado com base na inicialização do dispositivo e no login do usuário:



Mais informações sobre daemons e agentes podem ser encontradas aqui na [documentação da Apple]

Deamons e Agentes disponíveis em seu dispositivo macOS são encontrados nos seguintes locais:

Local	Descrição
~/Biblioteca/AgentesDeLançamento	Agentes por usuário fornecidos pelo usuário.
/Library/LaunchAgents	Agentes por usuário fornecidos pelo administrador.
/Library/LaunchDaemons	Daemons de todo o sistema fornecidos pelo administrador.

/System/Library/LaunchAgents	Agentes por usuário do OS X
/System/Library/LaunchDaemons	Daemons do sistema OS X

Você pode verificar a lista de cada categoria do terminal macOS usando estes comandos:

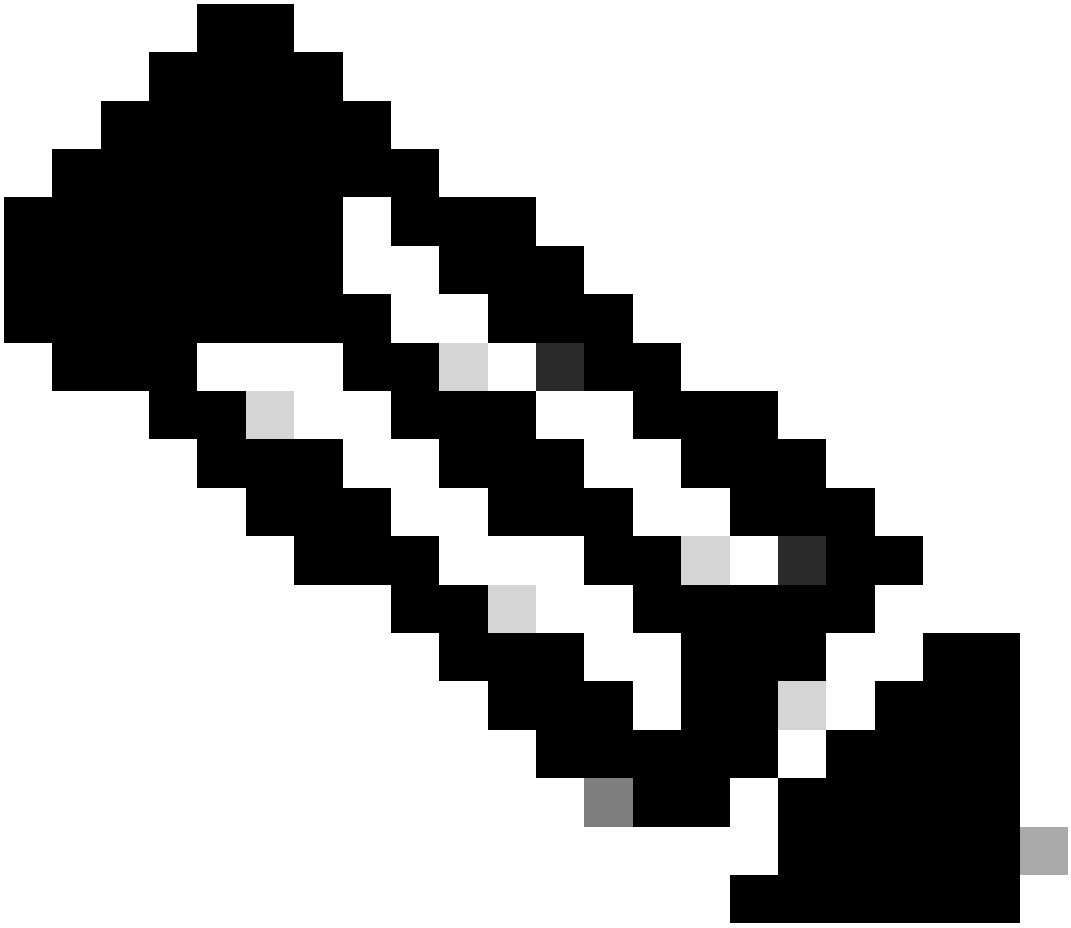
ls -ltr ~/Library/LaunchAgents
ls -ltr /Library/LaunchAgents
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

Os locais anteriores podem mostrar todos os daemons e agentes que estão disponíveis no dispositivo macOS, no entanto nem todos estão carregados ou em execução.

Configurar

A configuração para a condição de serviço do macOS pode ser feita usando estas etapas:

1. Identifique o nome do serviço a ser verificado.
2. (Opcional) Verifique os detalhes do serviço para definir se é um Agente ou um Deamon.
3. Selecione o operador de serviçoa ser avaliado.
4. Configure o requisito e a política de postura para tal condição.



Note: A condição de postura de serviço requer privilégio elevado para funcionar, portanto, é OBRIGATÓRIO que a PSN do ISE seja confiável pelo Cisco Secure Client (antigo AnyConnect) - Guia de referência

Identificar o Nome do Serviço a Ser Verificado

O Módulo de conformidade com procedimentos do ISE pode verificar os serviços que foram carregados, executados, carregados e executados com o código de saída.

Para verificar os serviços carregados, use o comando sudo launchctl dumpstate.

Para verificar os serviços que estão carregados e têm um código de saída, use o comando sudo launchctl list.

Os comandos anteriores podem mostrar muitas informações abruptamente; em vez disso, use esses comandos para apenas exibir o nome do serviço real:

Para verificar apenas os nomes de serviço carregados, use este comando:

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

Para verificar apenas os nomes de serviço que estão carregados e têm um código de saída, use este comando:

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

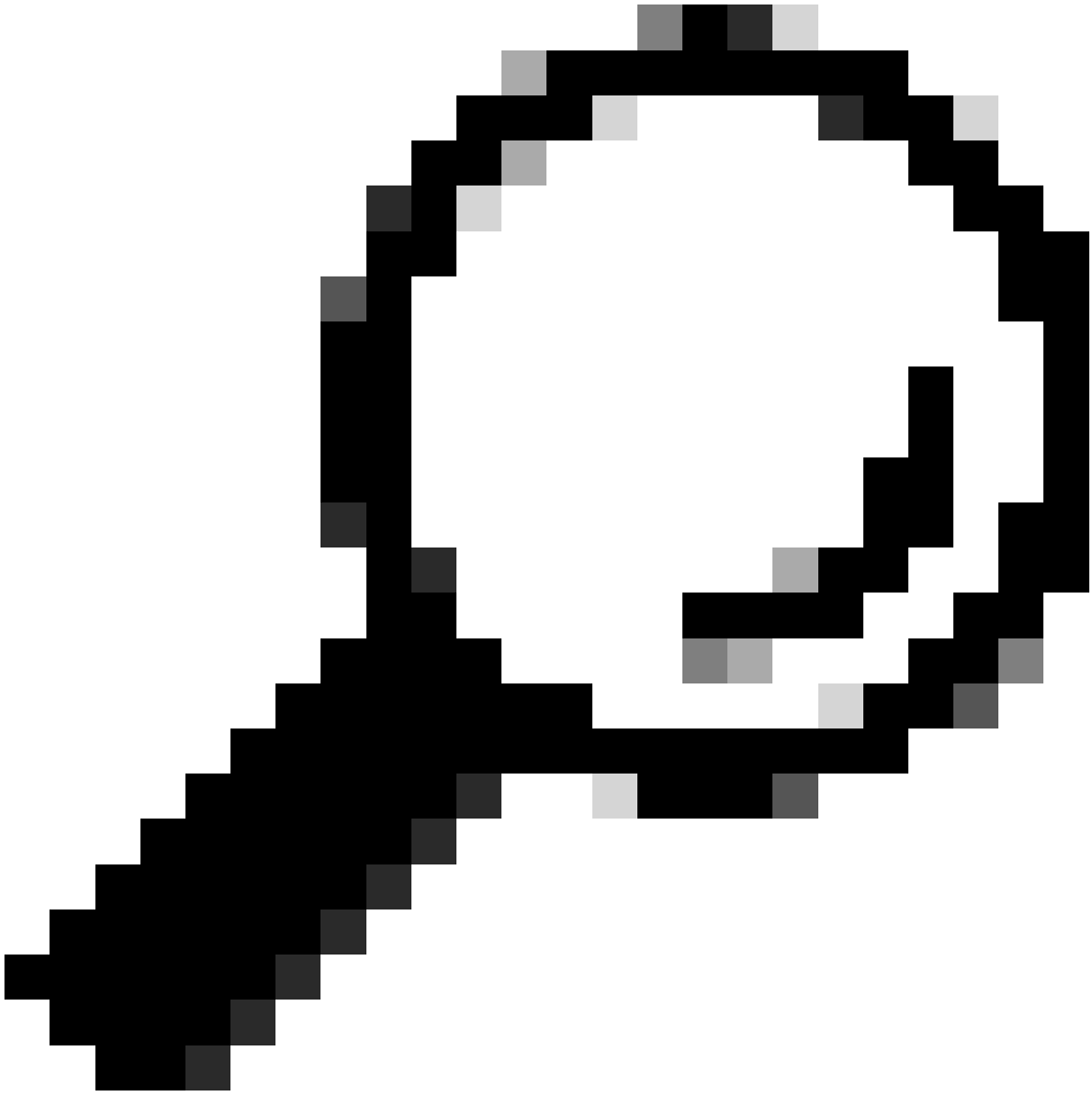
Esses comandos mostram muitas informações, portanto, ao final de cada comando é recomendável usar outro filtro grep para encontrar o serviço que você está procurando.
Por exemplo, se estiver procurando um serviço específico de fornecedor, você pode usar uma palavra-chave como um filtro no e.

Para o caso dos serviços Cisco, os comandos seriam algo como:

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

(Opcional) Verifique os detalhes do serviço para definir se é um agente ou um deamon

Na segunda parte da configuração dessa condição, você precisa verificar se o serviço é do tipo daemon ou do tipo de agente.



Tip: Esta etapa é opcional, pois o ISE permite selecionar a opção para Daemon ou agente de usuário, assim você pode apenas selecionar essa opção e ignorar esta parte.

Caso queira ser granular nessa condição, você pode verificar o tipo fazendo isso:

1. Primeiro, verifique o nome launchctl completo do serviço com o comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i {Nome do serviço}

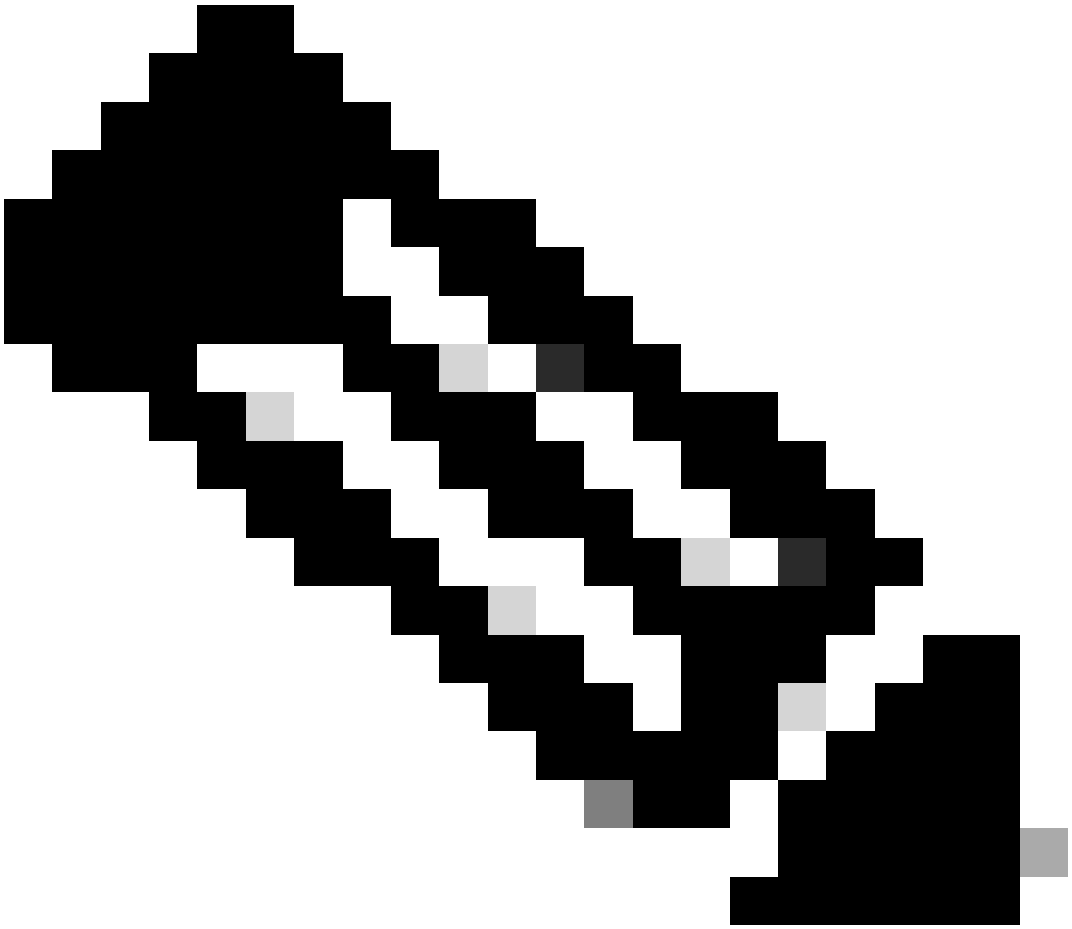
Por exemplo, para o comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//' | grep -i com.cisco.secureclient.iseposture, a saída é: gui/501/com.cisco.secureclient.iseposture.

2. Verifique o tipo de serviço com o comando sudo launchctl print { Seu nome de serviço launchctl

} | grep -i 'type = Launch'

Seguindo o exemplo, para o comando: sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch', a saída é: type = LaunchAgent.

Isso significa que o tipo de serviço é Agente, caso contrário, ele mostraria type = LaunchDaemon.



Note: Caso as informações estejam vazias, selecione a opção Daemon ou agente de usuário no ISE para a configuração de tipo de serviço.

Selecione o operador de serviço a ser avaliado

O ISE permite selecionar 5 operadores de serviço diferentes:

- Carregado
- Não carregado

- Carregado e em execução
- Carregado com o código de saída
- Carregado e em execução ou com código de saída

Serviços carregados

Todos os serviços listados ao usar esses dois comandos são:

```
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}'
```

Serviços não carregados

Todos os serviços que têm sua lista de propriedades (plist) definida, mas que não foram carregados, ou serviços que nem mesmo têm uma lista de propriedades (plist) definida, portanto, não podem ser carregados.

Esses serviços não são fáceis de serem identificados, e é mais comum para o caso de uso quando você deseja verificar se um serviço específico não deve existir no dispositivo macOS. Por exemplo, se você deseja impedir que o serviço de zoom seja carregado no dispositivo macOS, você pode colocar aqui us.zoom.ZoomDaemon como o valor do serviço, dessa forma, você verifica se o zoom não está sendo executado ou não está instalado.

Há serviços que não podem ser desinstalados e sua lista de propriedades está definida.
Por exemplo, com esse comando, você pode ver que dhcp6d plist está definido:

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

Verificando a lista de serviços, você pode ver que não está carregada:

```
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
```

Se você definir o valor como com.apple.dhcp6d", o dispositivo macOS será compatível, pois mesmo que a lista de serviços esteja definida, o serviço não será carregado.

Carregado e em execução

Nem todos os serviços estão em execução, há vários estados para cada serviço, como em execução, não em execução, em espera, encerrado, não inicializado, etc.
Para verificar todos os serviços em execução, use este comando:

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

Os serviços listados com o comando acima atingem a condição do operador de serviço Loaded & Running.

Carregado com código de saída

Alguns serviços podem terminar com um código de saída esperado ou inesperado; esses serviços podem ser listados com o comando:

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

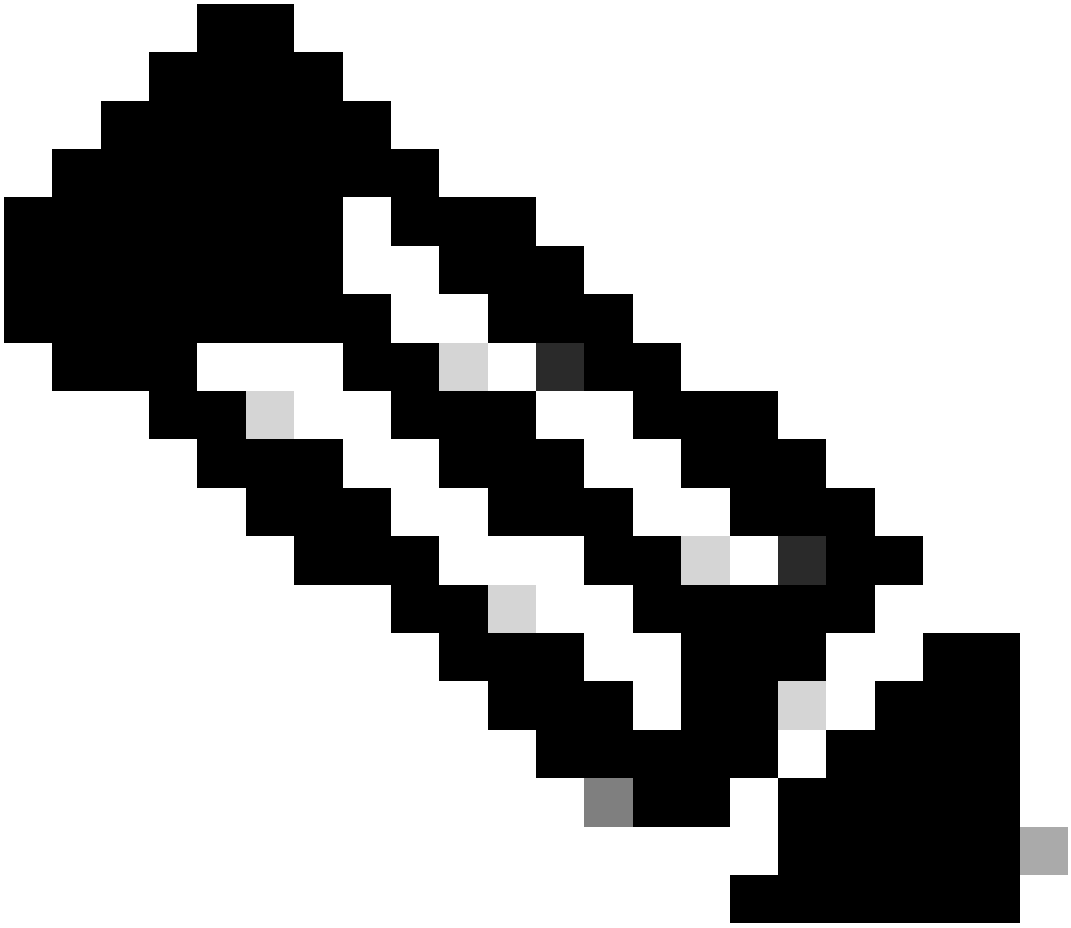
Para saber o código de saída, você pode escolher qualquer serviço e usar o comando:

sudo launchctl print { Seu nome de serviço launchctl } | grep -i 'último código de saída'

Por exemplo:

sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i 'último código de saída'

qual é a saída: último código de saída = 0

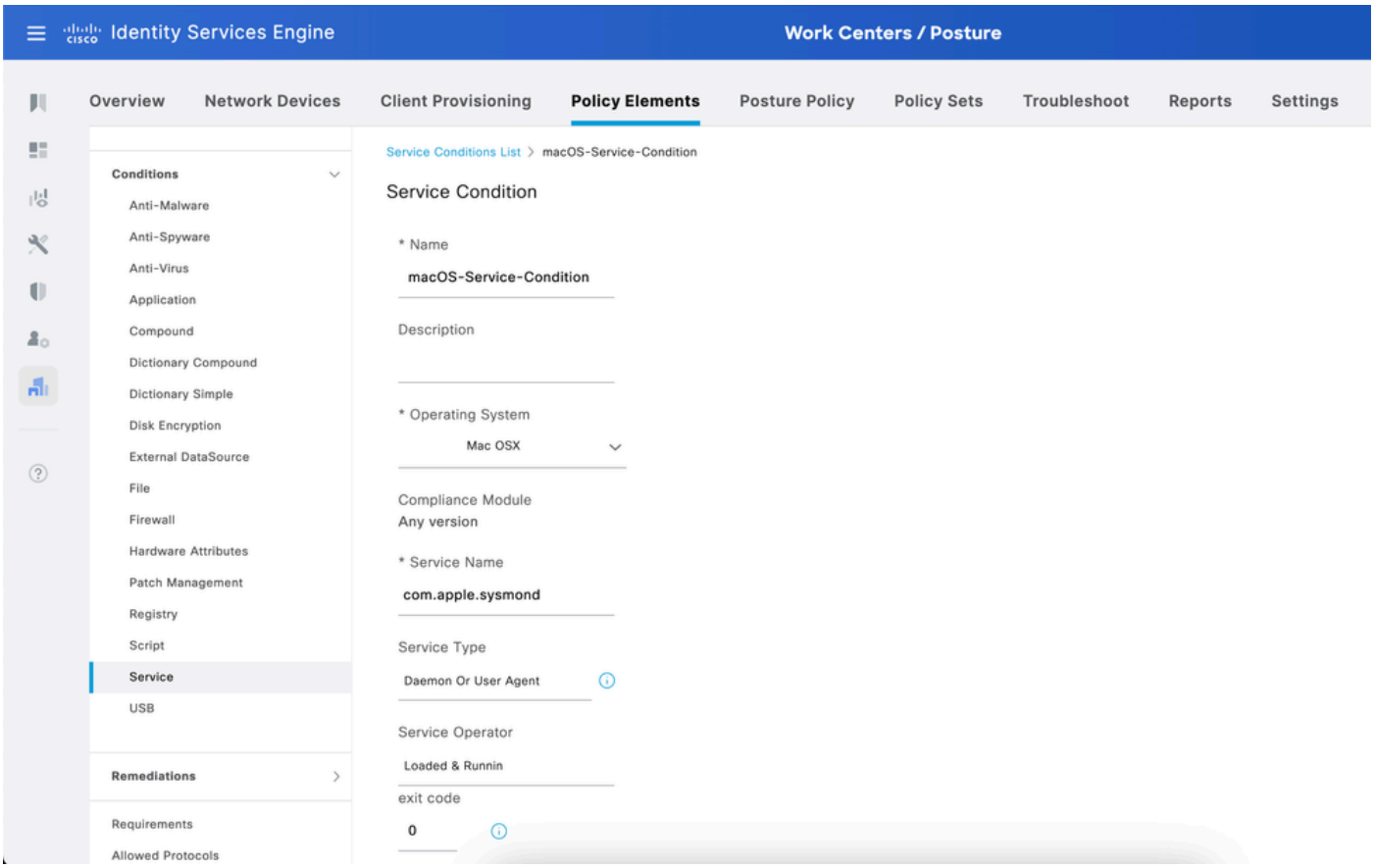


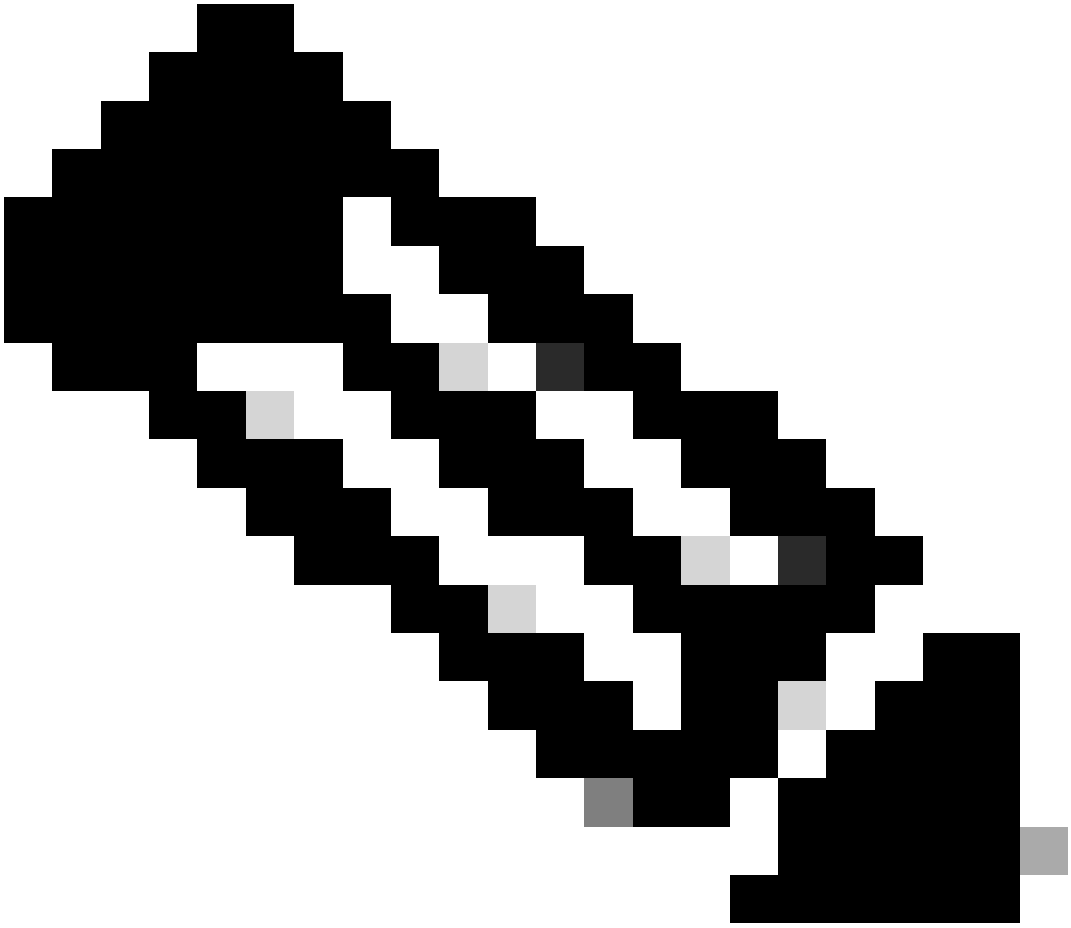
Note: Aqui, o código de saída 0 geralmente significa que tudo foi feito corretamente pelo serviço. Se um computador não corresponder a 0 como o código de saída, significa que o serviço não executou a ação esperada.

Carregado e em execução ou com código de saída

Esta última opção funciona quando o serviço está carregado e em execução ou carregado com código de saída.

Esta imagem mostra um exemplo de uma condição de serviço do macOS.


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

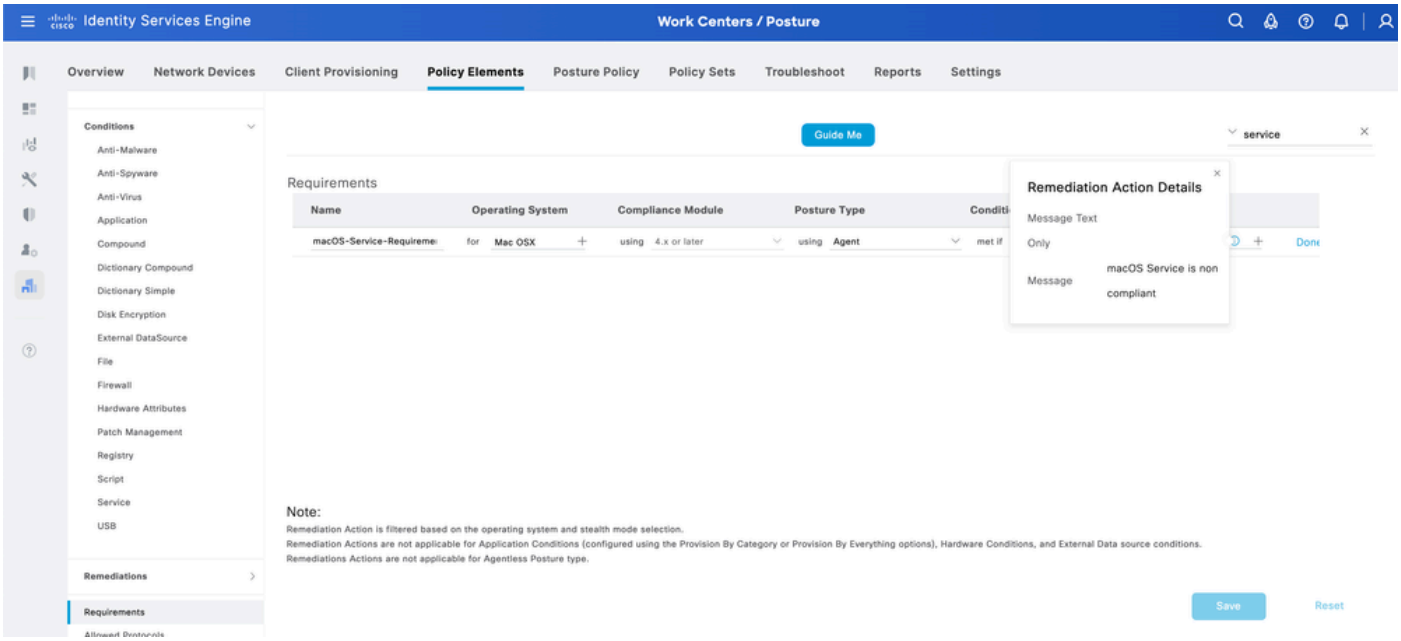


Note: No momento, há suporte apenas para o nome de serviço exato. Há uma solicitação de aprimoramento para suportar o curinga nos nomes de serviço, ID de bug da Cisco CSCwf01373

Configurar a Política de Requisito e Postura para Tal Condição

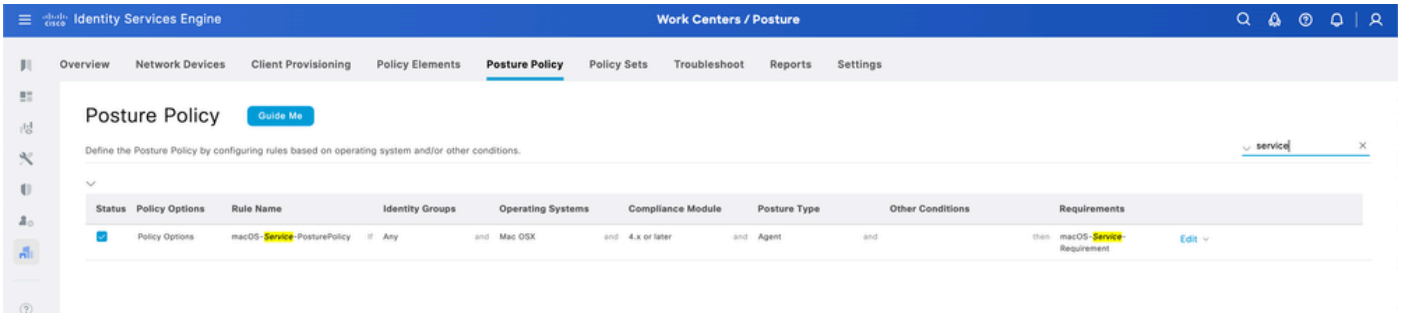
Depois que a condição for configurada, será necessário criar um requisito para essa condição. Use a opção Message Test Only para esse requisito.
Navegue até ISE > Centros de trabalho > Postura > Requisitos para criá-lo.

Note: Não há opções de correção para as condições de Serviço.



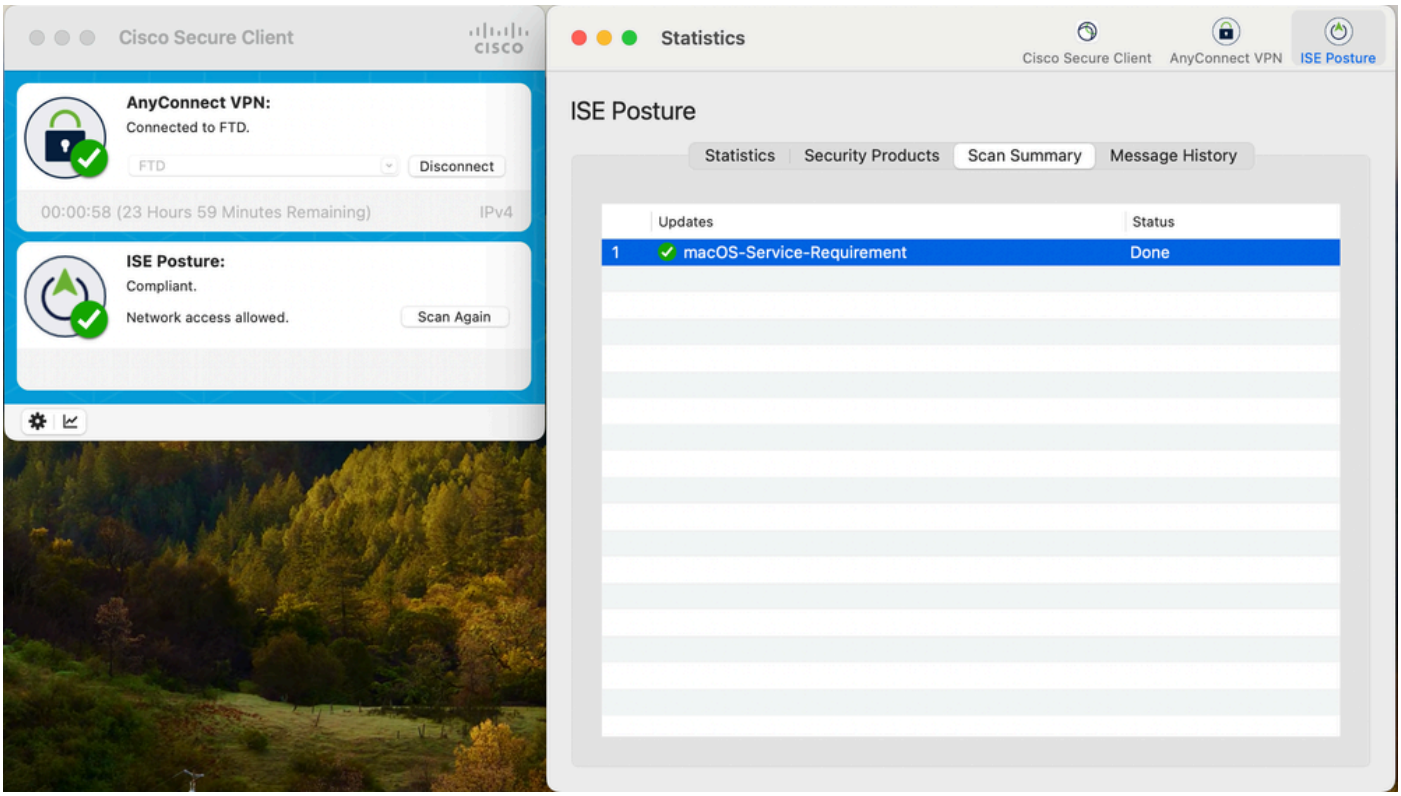
Depois que isso for feito, a última etapa será configurar a Política de postura que usa o requisito criado.
Navegue até ISE > Centros de trabalho > Postura > Política de postura para criar a política.

Habilite a nova política, nomeie-a como desejar e selecione o requisito que você acabou de criar.

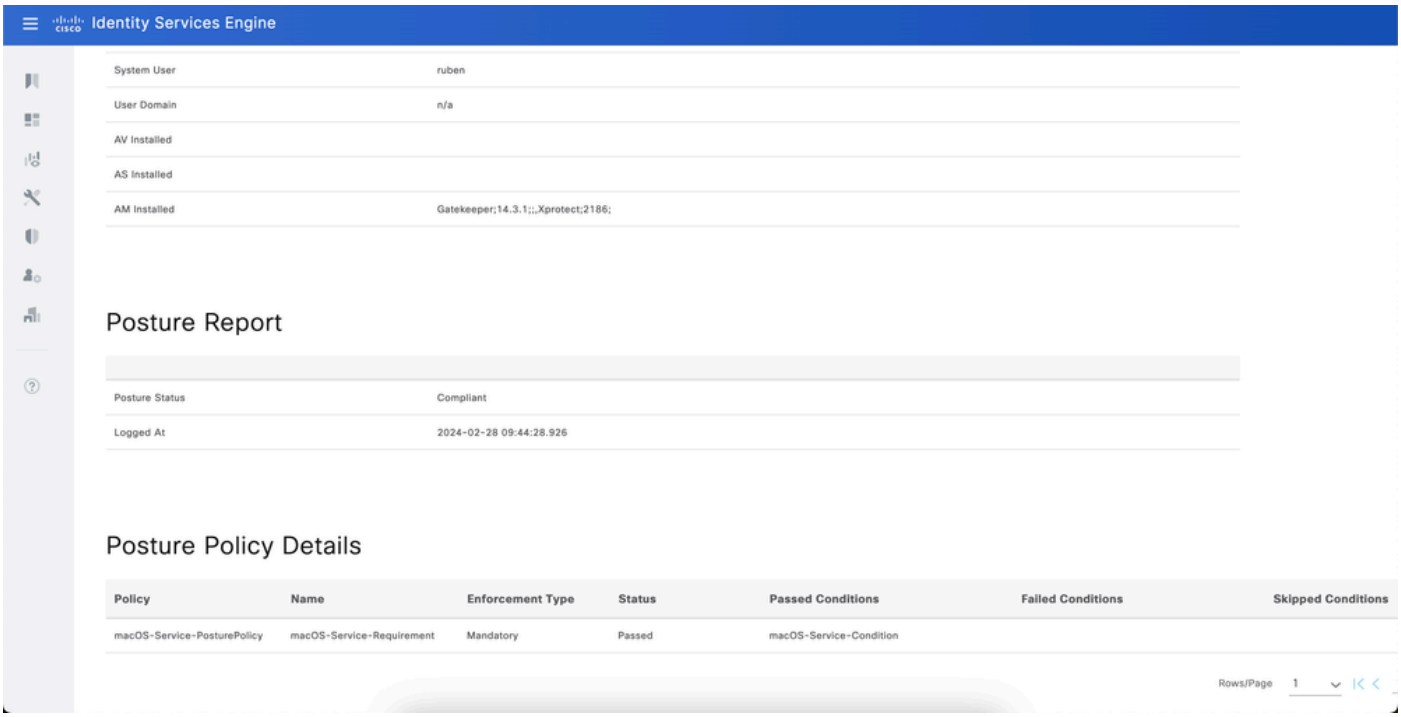


Verificar

Você pode verificar se a condição de postura do macOS foi aprovada ou falhou na própria GUI do Cisco Secure Client.



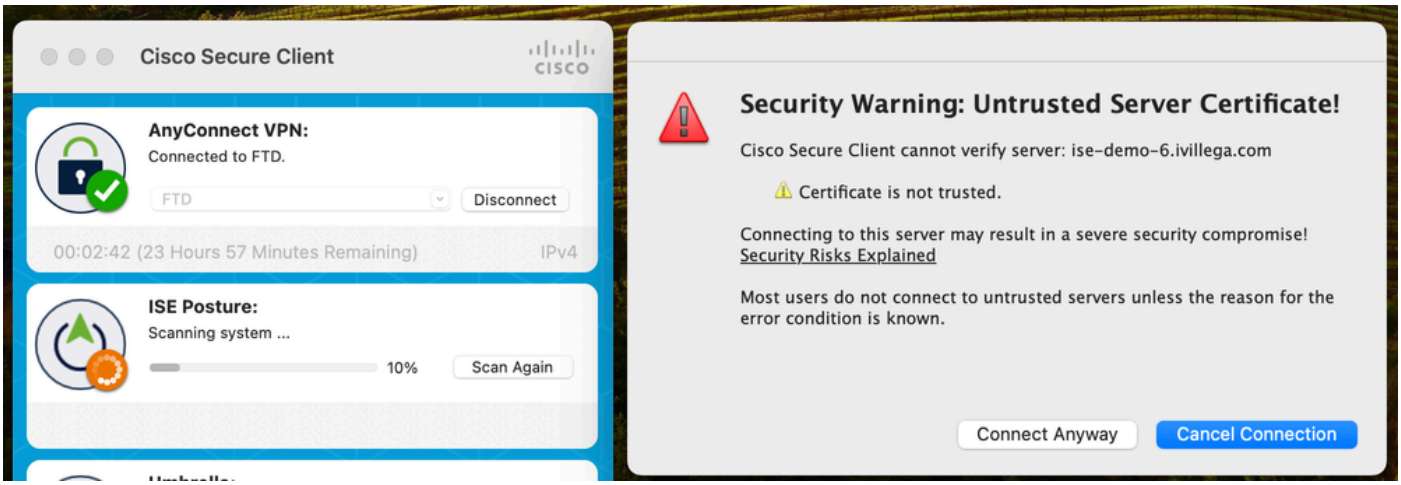
Além disso, você pode verificar o relatório de postura do ISE em ISE > Operações > Relatórios > Relatórios > Endpoints e Usuários > Avaliação de postura por endpoint.



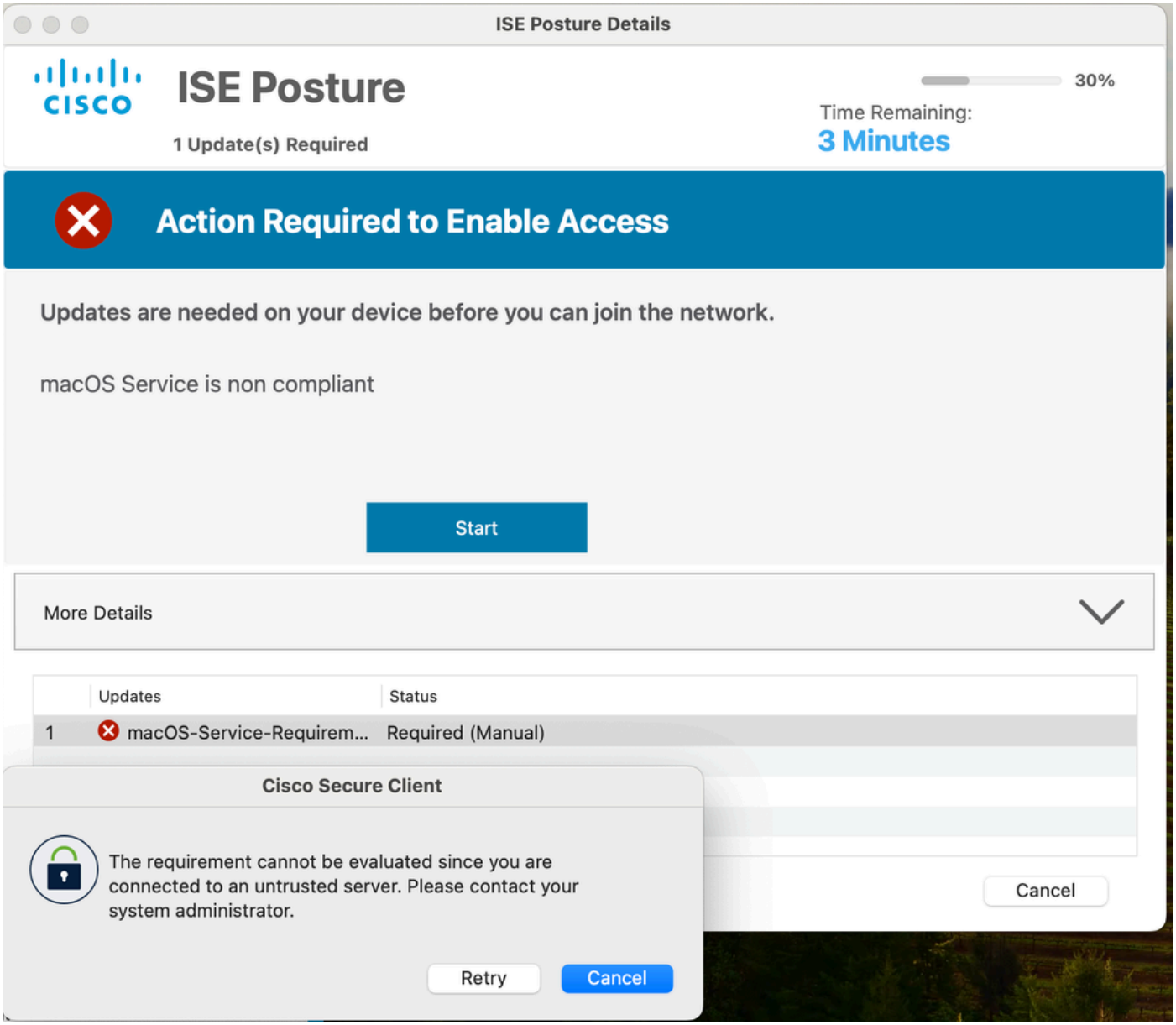
Troubleshooting

Os problemas comuns que você pode encontrar ao configurar essa condição de postura de serviço do macOS são:

Certificado não confiável



Como indicado anteriormente, a condição de serviço requer permissões elevadas. É imperativo que o certificado para o processo de verificação de postura seja confiável para o servidor. Caso contrário, você encontrará este erro:

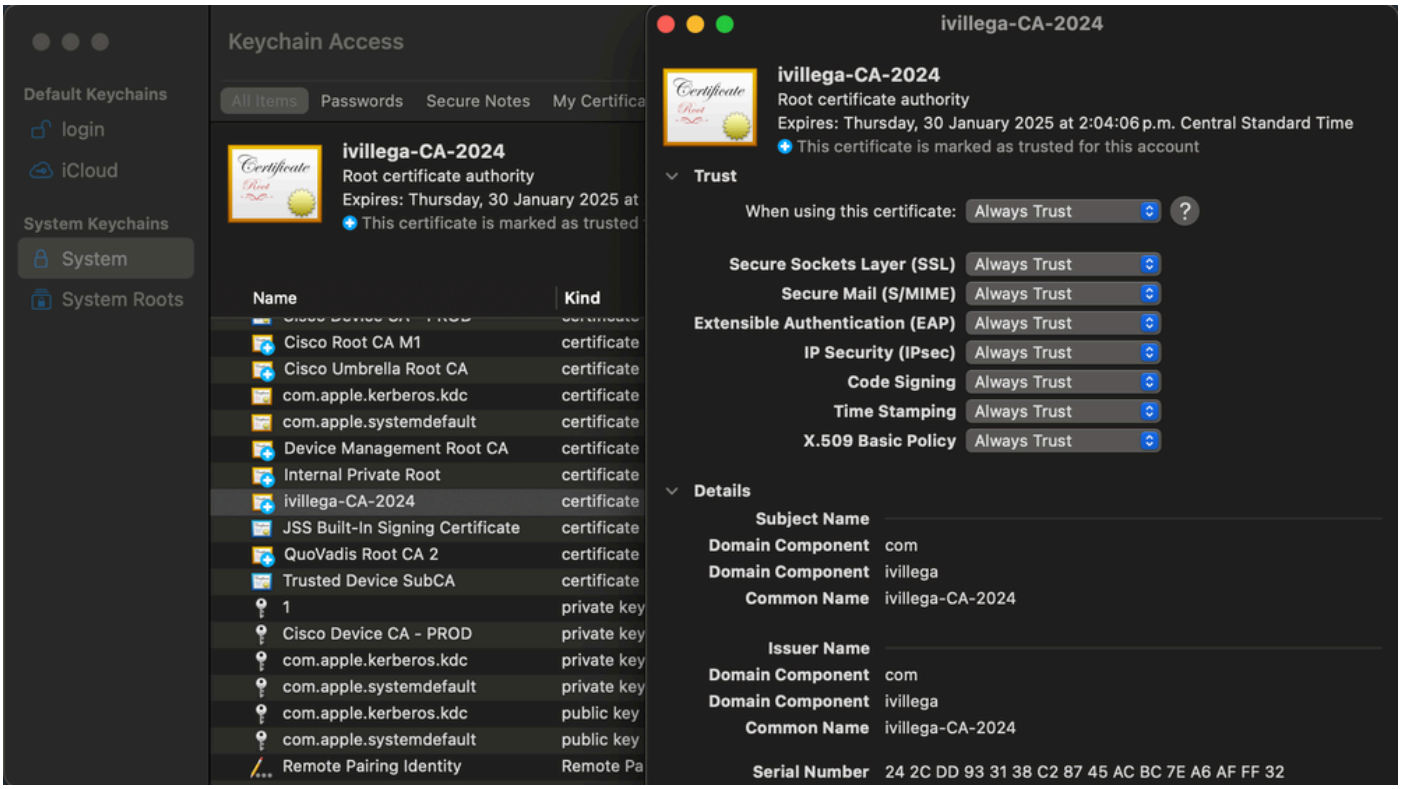


O módulo de postura ISE descobre os servidores PSN por endereço IP ou Nome de domínio totalmente qualificado (FQDN). A prática recomendada é ter os arquivos de configuração Posture para descobrir os nós ISE por meio do FQDN, de modo que os certificados Admin e Portal (Client Provisioning Portal) devem incluir o FQDN no campo CN ou no campo SAN. Você também pode usar certificados curinga para isso, pois esses certificados são compatíveis com esse fluxo.

Devido aos títulos do sistema, o campo CN não pode ser confiável no futuro. Inclua a entrada curinga ou o FQDN no campo SAN como prática recomendada.

Caso as PSNs do ISE sejam descobertas por meio do endereço IP em vez do FQDN, é necessário que o endereço IP dos nós seja incluído no campo CN ou no campo SAN do(s) certificado(s) vinculado ao uso do Administrador e do Portal.

Os módulos de postura do ISE confiam no certificado apresentado pelo servidor ISE. Se sua CA estiver no armazenamento de certificados do sistema do acesso de cadeia de chaves do Mac OS, essa CA deverá ter a configuração Ao usar esse certificado definida como Sempre Confiar.



Você pode encontrar o comportamento incorreto que, mesmo quando o certificado é carregado corretamente e todos os requisitos de CN e SAN são atendidos, o sistema macOS ainda não confia no certificado. Nesses casos, abra o aplicativo Acesso ao conjunto de chaves, navegue até a guia Armazenamento de certificados do sistema e exclua o certificado CA de lá.

Em seguida, navegue até o aplicativo terminal do macOS e execute este comando: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

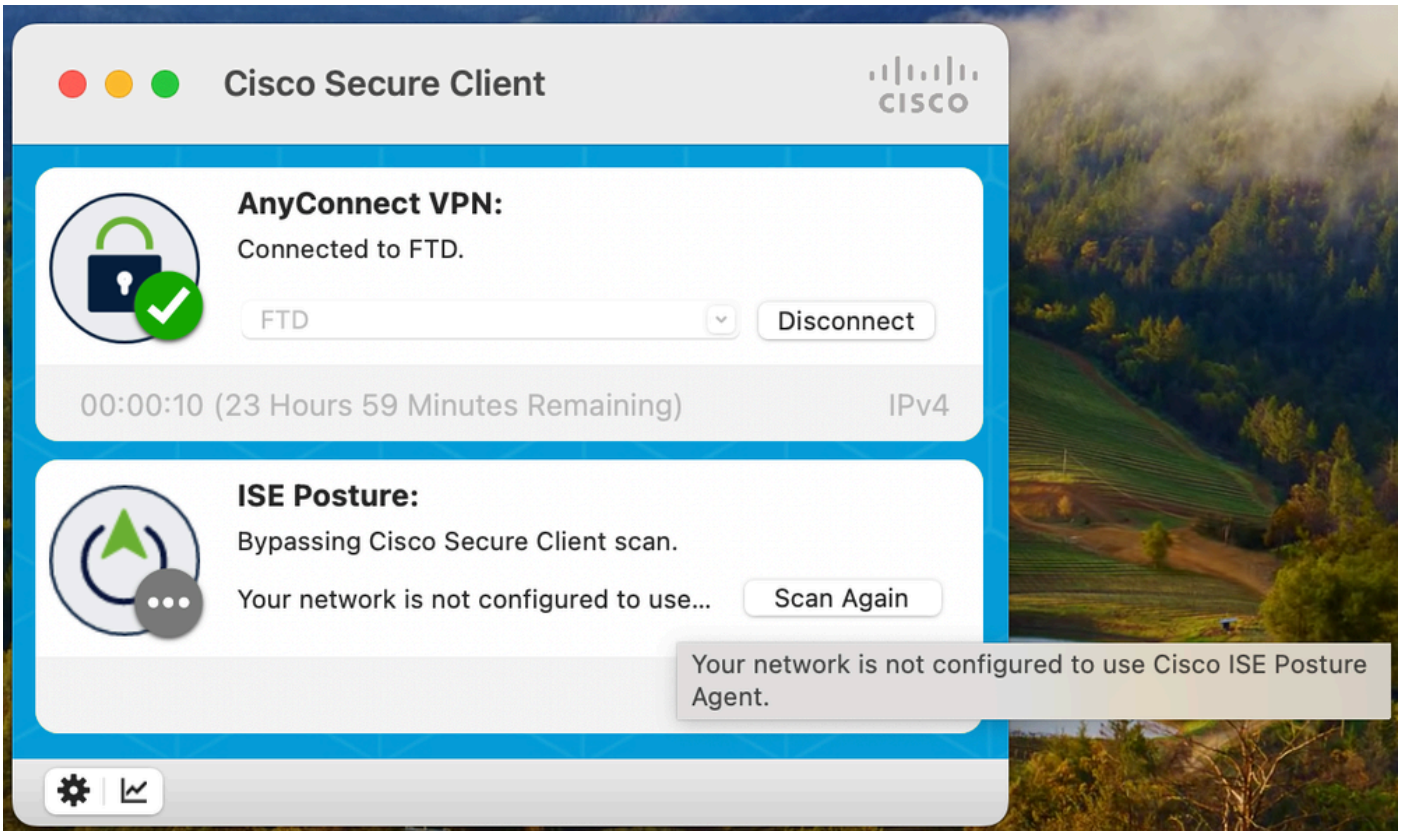
{Caminho para o certificado da autoridade de certificação}

Por exemplo, se o certificado estiver na área de trabalho, o comando será: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

Depois de executar o comando, reinicie o computador e tente novamente.

Ignorando o Cisco Secure Client Scan

Você também pode encontrar as mensagens de erro "Bypassing Cisco Secure Client Scan" (Ignorando a verificação de segurança do Cisco) e "Your network is not configured to use Cisco ISE Posture Agent" (Sua rede não está configurada para usar o Cisco ISE Posture Agent):



Esta mensagem é exibida porque não há perfis configurados no Provisionamento de cliente no ISE > Centros de trabalho > Postura > Provisionamento de cliente > Políticas de provisionamento de cliente.
Embora você possa ver uma condição para os sistemas operacionais Mac OSX, isso não significa que você está cobrindo todas as versões do macOS.

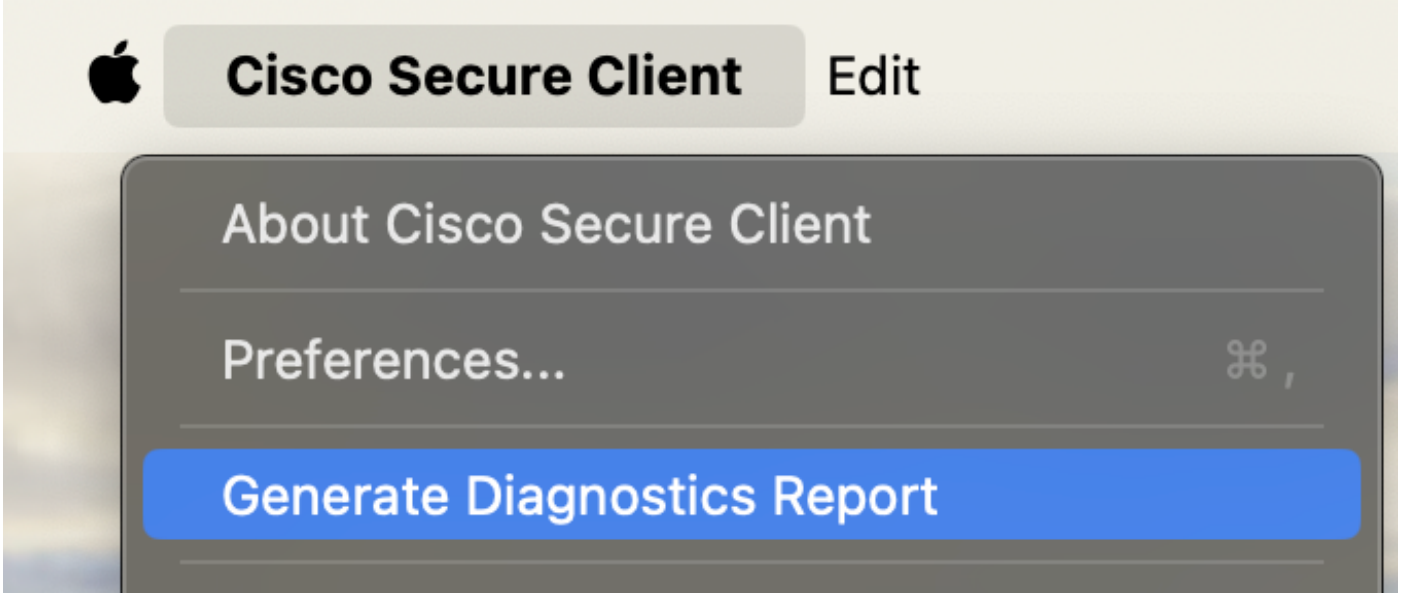
Por padrão, o ISE não inclui as versões mais recentes do macOS, como Sequoia (15.6.x), para evitar essa mensagem, certifique-se de que a postura seja atualizada.

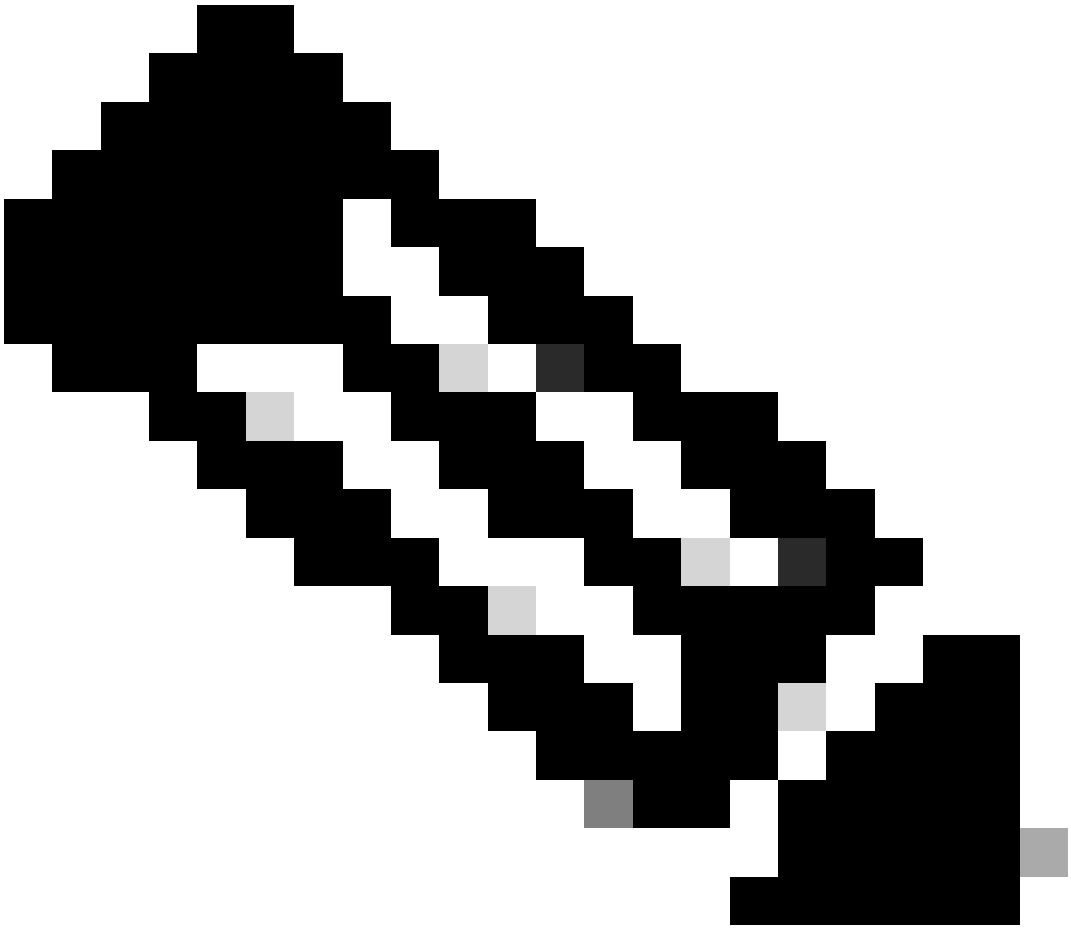
Você deve atualizar o feed Posture no ISE > Centros de trabalho > Postura > Configurações > Atualizações de software > Atualizações de postura.

Isso pode ser atualizado on-line diretamente do ISE ou off-line por meio de um arquivo zip que pode ser baixado aqui do site Posture Offline

Outros problemas

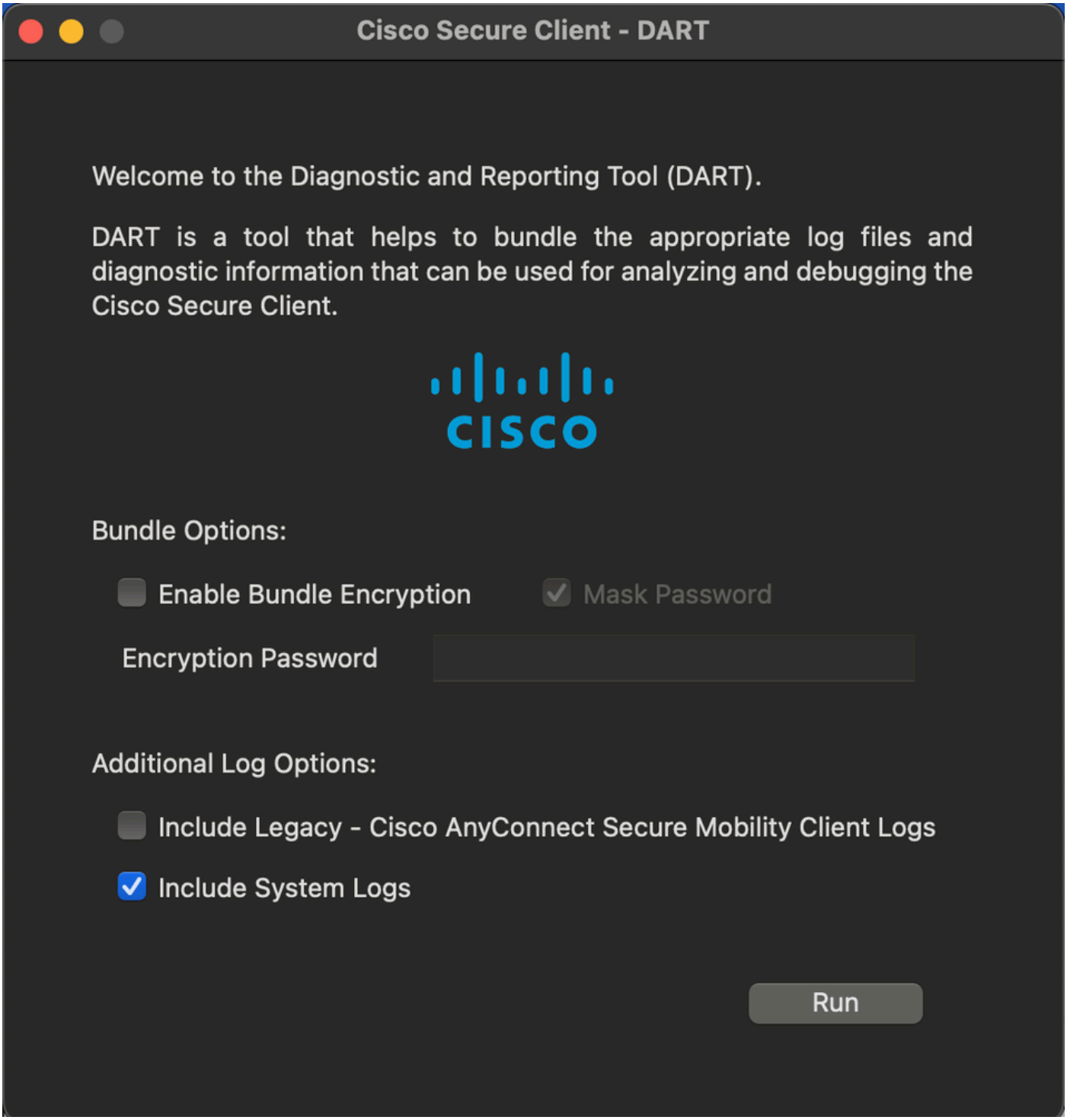
Se quiser entrar nos detalhes, você pode coletar um pacote DART do dispositivo postured macOS. Para isso, você deve ter o módulo DART instalado e, em seguida, com o aplicativo Cisco Secure Client ativo, navegue até a barra Menu e clique em Cisco Secure Client e, em seguida, em Gerar Relatórios de Diagnóstico.



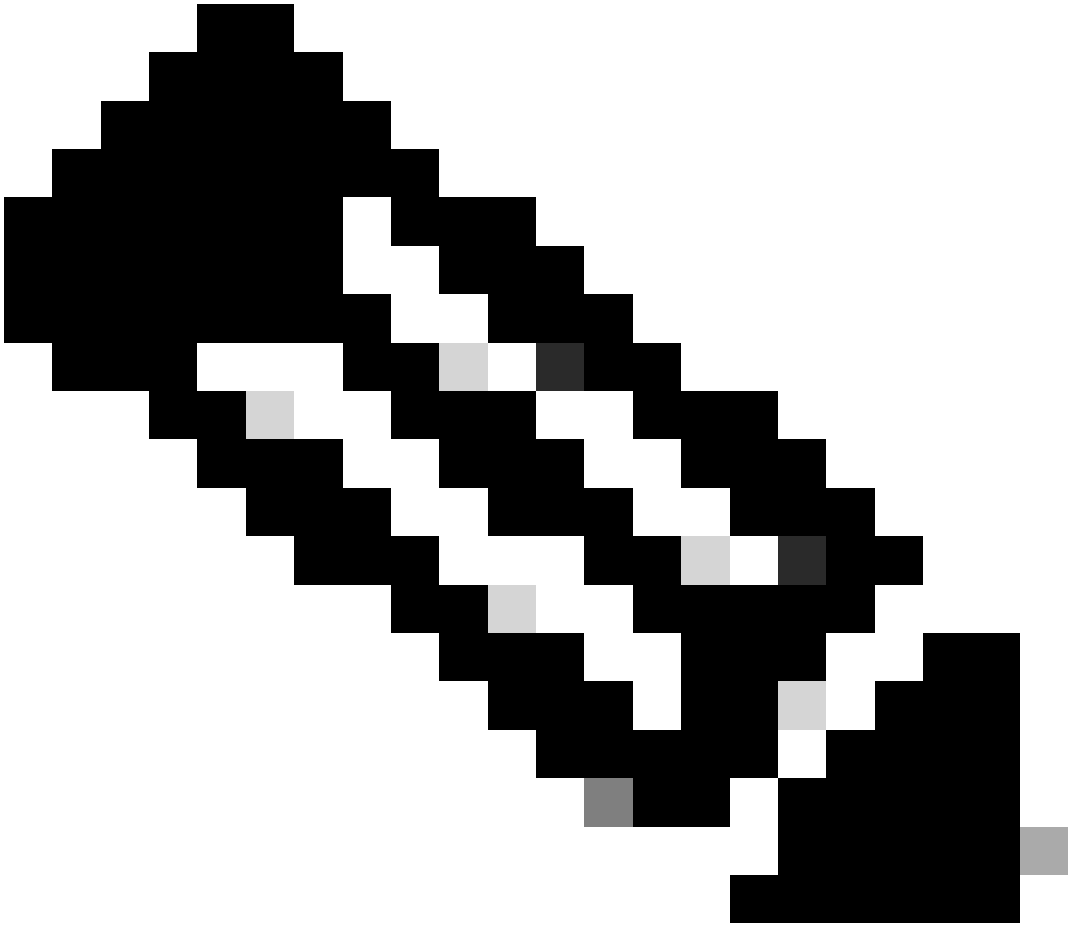


Note: É importante ter a opção Incluir logs do sistema habilitada ao gerar o pacote DART,

caso contrário o pacote DART não incluirá informações do módulo de postura do ISE.



Por motivos de segurança, alguns dos logs podem estar criptografados e não visíveis, mas no arquivo unified_log.log do pacote DART você pode ver logs semelhantes como mostrado:



Note: Este exemplo de log é para a condição de serviço macOS configurada neste documento.

```
[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

Além disso, você pode definir o componente posture no nível do log de depuração no nó PSN do ISE que autentica e posiciona o endpoint.

Você pode configurar esse nível de log no ISE > Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração. Clique no nome de host PSN e altere o nível de log do componente Postura de INFO para DEBUG.

Usando o mesmo exemplo para a condição de serviço macOS, você pode ver logs semelhantes no ise-psc.log:

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
```

Se os problemas persistirem, aumente o valor do TAC com a equipe da Cisco.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.