

Implementação de postura sem redirecionamento do ISE

Contents

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Connectiondata.xml](#)
[Lista do Call Home](#)
[Projeto](#)
[Configurar](#)
[Grupos de dispositivos de rede \(opcional\)](#)
[Dispositivo de rede](#)
[Provisionamento de clientes](#)
[Provisionamento manual \(pré-implantação\)](#)
[Portal de provisionamento do cliente \(implantação na Web\)](#)
[Política de provisionamento do cliente](#)
[Autorização](#)
[Perfil de autorização](#)
[Política de Autorização](#)
[Troubleshooting](#)
[Compatível com o Cisco Secure Client e postura não aplicável \(pendente\) no ISE](#)
[Sessões obsoletas/fantasmas](#)
[Identificar](#)
[Solução](#)
[Desempenho](#)
[Identificar](#)
[Solução](#)
[Relatório](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve o uso e a configuração do fluxo de postura sem redirecionamento e dicas de Troubleshooting.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxo de postura no ISE
- Configuração de componentes de postura no ISE
- Redirecionamento para portais ISE

Para compreender melhor os conceitos descritos mais adiante, é recomendável passar por:

[Comparar versões anteriores do ISE com o fluxo de postura do ISE no ISE 2.2](#)
[Postura e gerenciamento de sessões do ISE](#)

Componentes Utilizados

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

- Cisco ISE versão 3.1
- Cisco Secure Client 5.0.01242

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

O fluxo de postura do ISE consiste nas seguintes etapas:

0. Autenticação/Autorização. Geralmente executado logo antes do fluxo de postura ser iniciado, mas pode ser ignorado para certos casos de uso, como a Reavaliação de postura (PRA). Como a própria autenticação não aciona a descoberta de postura, isso não é considerado essencial para cada fluxo de postura.

1. Descoberta. Processo executado pelo módulo Secure Client ISE Posture para encontrar o proprietário PSN da **sessão ativa atual**.
2. Provisionamento de clientes. Processo executado pelo ISE para provisionar o cliente com as versões correspondentes do módulo de postura do ISE do Cisco Secure Client (antigo AnyConnect) e do módulo de conformidade. Nesta etapa, a cópia local do perfil de postura contida e assinada pela PSN específica também é enviada ao cliente.
3. Verificação do sistema. As políticas de postura configuradas no ISE são avaliadas pelo módulo de conformidade.
4. Correção (opcional). Executado no caso de qualquer política de postura não estar em conformidade.
5. CoA É necessária uma nova autorização para conceder acesso final à rede (em conformidade ou não em conformidade).

Este documento concentra-se no processo de descoberta do fluxo de postura do ISE.

A Cisco recomenda usar o redirecionamento para o processo de descoberta, no entanto, há alguns casos em que o redirecionamento não é possível de implementar, como o uso de dispositivos de rede de terceiros, em que o redirecionamento não é suportado. Este documento tem como objetivo fornecer uma orientação geral e práticas recomendadas para implementar e solucionar problemas de postura sem redirecionamento nesses ambientes.

A descrição completa do fluxo sem redirecionamento está descrita em [Comparar versões anteriores do ISE com o fluxo de postura do ISE no ISE 2.2](#).

Há dois tipos de testes de descoberta de postura que não usam redirecionamento:

1. Connectiondata.xml
2. Lista do Call Home

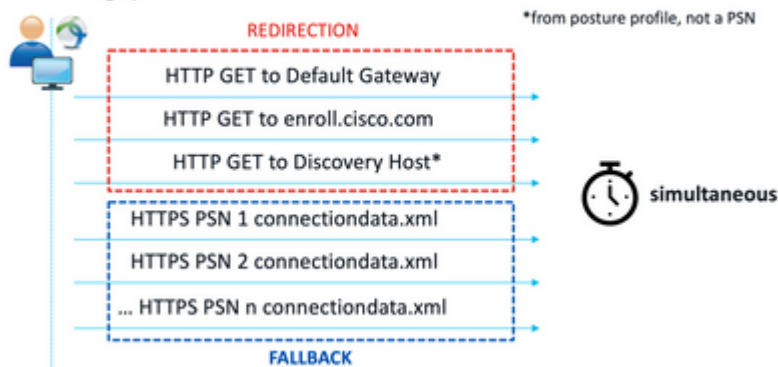
Connectiondata.xml

O Connectiondata.xml é um arquivo criado e mantido automaticamente pelo Cisco Secure Client. Ele consiste em uma lista de PSNs às quais o cliente se conectou anteriormente com êxito para fins de postura. Portanto, esse é apenas um arquivo local e seu conteúdo não é persistente em todos os endpoints.

A finalidade principal do connectiondata.xml é trabalhar como um mecanismo de backup para os testes de descoberta dos Estágios 1 e 2. Caso os testadores de redirecionamento ou de lista de call home não consigam encontrar um PSN com uma sessão ativa, o Cisco Secure Client envia uma solicitação direta a cada um dos servidores listados em connectiondata.xml.

Stage 1 discovery probes

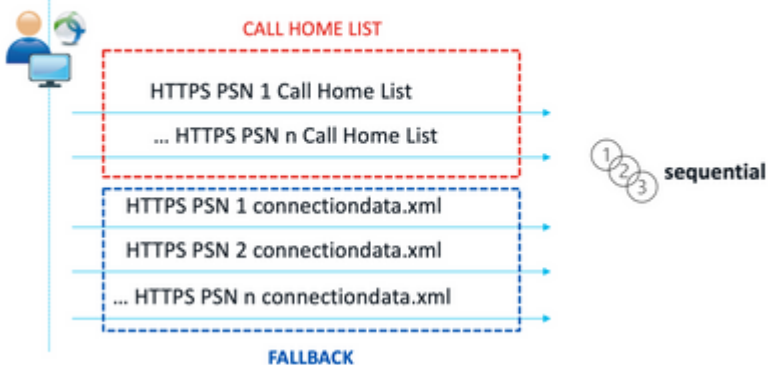
No-MnT stage probes



Sondas de descoberta do estágio 1

Stage 2 discovery probes

MnT stage probes



Sondas de descoberta do estágio 2

Um problema comum causado pelo uso de testes connectiondata.xml é uma sobrecarga da implantação do ISE devido a um grande número de solicitações HTTPS enviadas pelos pontos de extremidade. É importante considerar que, embora o connectiondata.xml seja eficaz como um mecanismo de backup para evitar interrupções completas para mecanismos de postura de redirecionamento e sem redirecionamento, ele não é uma solução sustentável para um ambiente de postura; portanto, é necessário diagnosticar e resolver os problemas de design e configuração que causam a falha dos principais testes de descoberta e que resultam em problemas de descoberta.

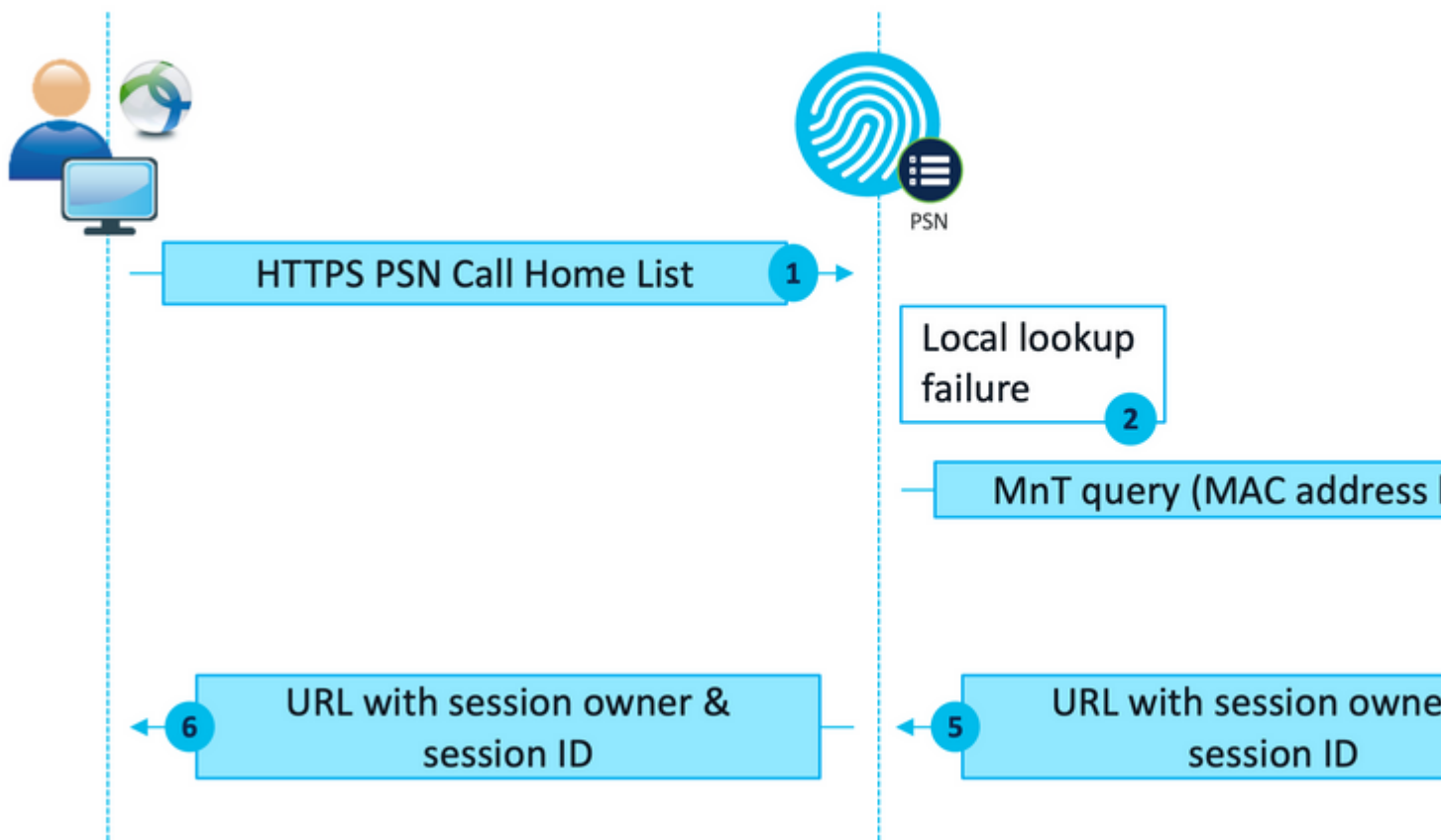
Lista do Call Home

Call Home List é uma seção do perfil de postura em que uma lista de PSNs é especificada para ser usada para postura. Diferentemente do connectiondata.xml, ele é criado e mantido por um administrador do ISE e

pode exigir uma fase de projeto para a configuração ideal. A lista de PSNs na lista Call Home deve corresponder à lista de servidores de autenticação e contabilização configurada no dispositivo de rede ou balanceador de carga para RADIUS.

Os testadores Call Home List permitem o uso de uma pesquisa MnT durante a pesquisa de sessão ativa em caso de falha de pesquisa local em um PSN. A mesma funcionalidade se estende aos testes connectiondata.xml somente quando eles são usados durante a descoberta do estágio 2. Por esse motivo, todos os testes do Estágio 2 também são chamados de testes de Nova Geração.

MnT lookup



Fluxo de pesquisa MnT

Projeto

Como um processo de descoberta sem redirecionamento geralmente envolve um fluxo mais complexo e uma quantidade maior de processamento em PSNs e MnT em comparação a um fluxo de redirecionamento, há dois desafios comuns que podem surgir durante a implementação:

1. Detecção eficaz
2. Desempenho da implantação do ISE

Para lidar com esses desafios, é recomendável projetar a lista Call Home para limitar o número de PSNs que um determinado endpoint pode usar para postura. Para implantações médias e grandes, é necessário distribuir a implantação para criar várias Listas de Call Home com número reduzido de PSNs. Consequentemente, a lista de PSNs que são usadas para autenticação RADIUS para um determinado Dispositivo de rede deve ser limitada da mesma forma para corresponder à Lista de Call Home correspondente.

Os seguintes aspectos podem ser levados em consideração durante o desenvolvimento da estratégia de distribuição da PSN para determinar o número máximo de PSNs em cada lista de Call Home:

- Número de PSNs na implantação
- Especificações de hardware de PSNs e nós MnT
- Número máximo de sessões de postura simultâneas na implantação
- Número de dispositivos de rede
- Ambientes híbridos (redirecionamento simultâneo e implementação de postura sem redirecionamento)
- Número de adaptadores usados pelos pontos de extremidade
- Localização dos dispositivos de rede e PSNs
- Tipos de conexão de rede usados para postura (com fio, sem fio, VPN)

2. No ISE, navegue até **Administração > Recursos de rede > Dispositivos de rede** e clique em **Adicionar**. Configure os grupos de dispositivos de rede de acordo com o design e habilite as **configurações de autenticação RADIUS** para configurar o **segredo compartilhado**.

* Device Profile
Cisco

Model Name

Software Version

* Network Device Group

Location WEST Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

Posture Redirectionless Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret Show

Configuração do dispositivo de rede

Provisionamento de clientes

Há duas maneiras de provisionar o cliente com o software e o perfil corretos para executar a postura em um ambiente sem redirecionamento:

1. Provisionamento manual (pré-implantação)
2. Portal de provisionamento do cliente (implantação na Web)

Provisionamento manual (pré-implantação)

1. Faça o download e instale o Cisco Secure Client Profile Editor a partir do [download do software Cisco](#).

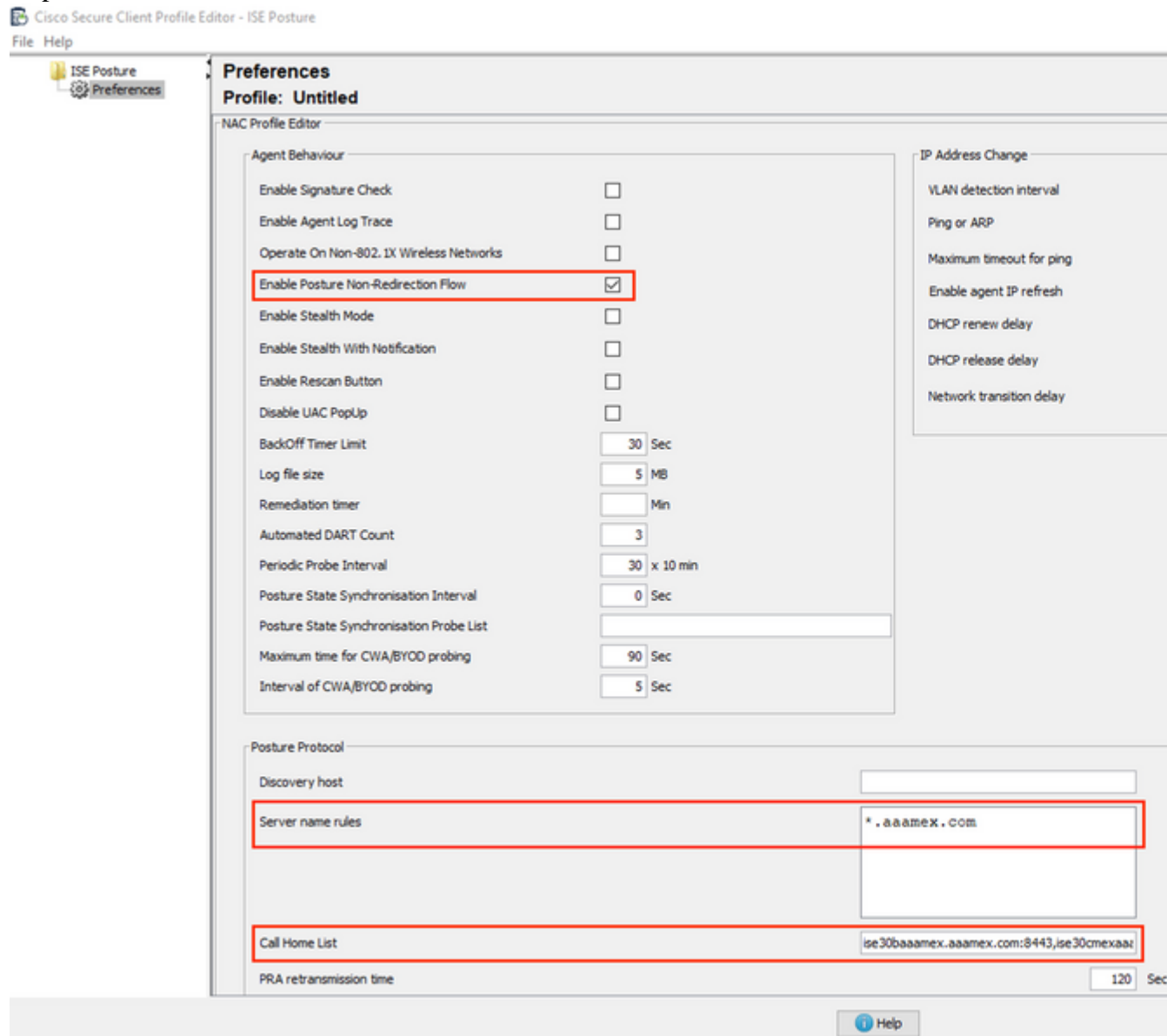
Profile Editor (Windows)	19-Dec-2022	15.74
tools-cisco-secure-client-win-5.0.01242-profileeditor-k9.msi		
Advisories		

Pacote do Editor de perfis

2. Abra o editor de perfil de postura do ISE:
 - Verifique se **Enable Posture Non-Redirection Flow** está habilitado.
 - Configure as **regras de nome do servidor** separadas por vírgulas. Use um único asterisco * para permitir a conexão a qualquer PSN, valores curinga para permitir a conexão a qualquer PSN em um domínio específico ou os FQDNs PSN para restringir a conexão a PSNs

específicos.

- Configure **Call Home List** para especificar a lista separada por vírgulas de PSNs. Certifique-se de adicionar a porta do Portal de Provisionamento do Cliente com o formato FQDN:porta ou IP:porta.



Configuração do perfil de postura com o Editor de perfis

Observação: consulte a etapa 4 da seção Client Provisioning policy para obter instruções sobre como verificar a porta do Client Provisioning Portal, se necessário.

3. Repita a etapa 2 para cada lista do Call Home em uso.
4. Faça o download do pacote de pré-implantação do Cisco Secure Client a partir do [download do software Cisco](#).

cisco-secure-client-win-5.0.01242-predeploy-k9.zip

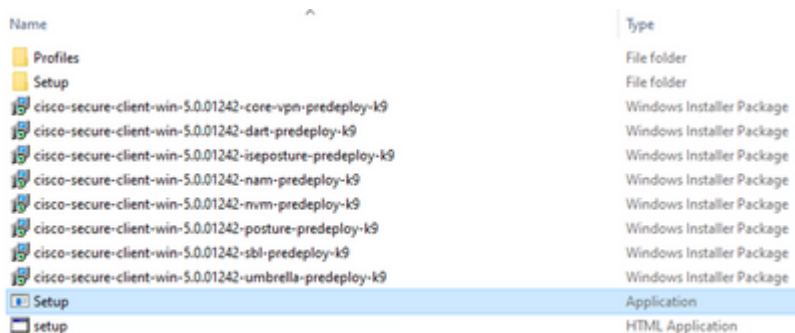
[Advisories](#) 

Pacote de pré-implantação do Cisco Secure Client

5. Salve o perfil como ISEPostureCFG.xml.
6. Distribua os arquivos de perfil e instalação em um arquivo morto ou copie os arquivos para os clientes.

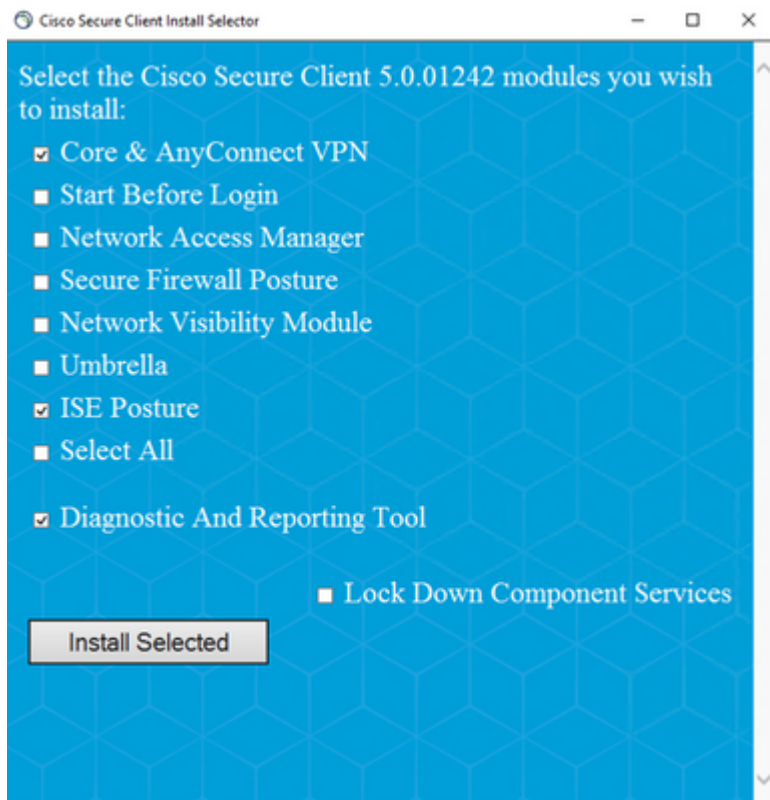
Aviso: certifique-se de que os mesmos arquivos do Cisco Secure Client também estejam nos headends aos quais você planeja se conectar: Secure Firewall ASA, ISE, etc. Mesmo quando o provisionamento manual é usado, o ISE deve ser configurado para provisionamento de clientes com a versão de software correspondente. Consulte a seção Configuração da política de provisionamento do cliente para obter instruções detalhadas.

7. No cliente, abra o arquivo zip no e execute a Instalação para instalar os módulos Core e ISE Posture. Como alternativa, os arquivos msi individuais podem ser usados para instalar cada módulo. Nesse caso, você deve certificar-se de que o módulo core-vpn seja instalado primeiro.



Name	Type
Profiles	File folder
Setup	File folder
cisco-secure-client-win-5.0.01242-core-vpn-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-dart-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-iseposture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nam-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nvm-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-posture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-sbl-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-umbrella-predeploy-k9	Windows Installer Package
Setup	Application
setup	HTML Application

Conteúdo do pacote de pré-implantação do Cisco Secure Client



instalador do Cisco Secure Client

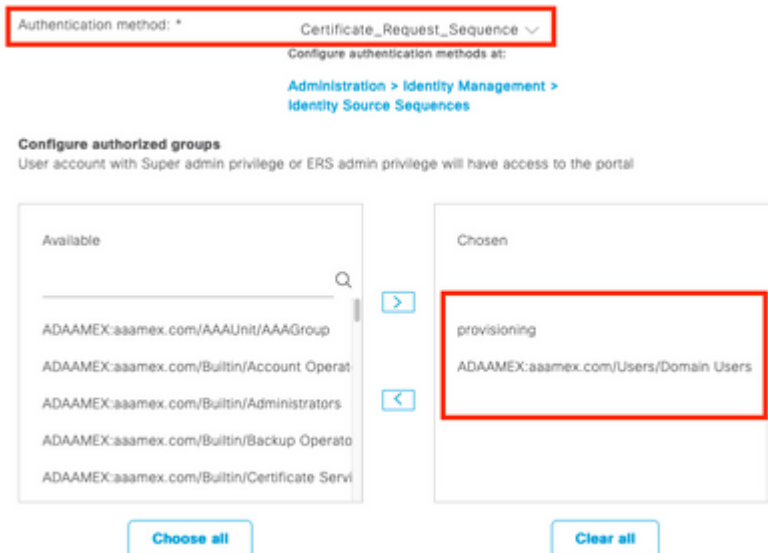
Dica: instale a ferramenta de diagnóstico e relatórios a ser usada para fins de solução de problemas.

8. Quando a instalação estiver concluída, copie o xml do perfil de postura para os seguintes locais:
- Windows: %ProgramData%\Cisco\Cisco Secure Client\Postura do ISE
 - MacOS: /opt/cisco/secureclient/iseposture/

Portal de provisionamento do cliente (implantação na Web)

O ISE Client Provisioning Portal pode ser usado para instalar o módulo de postura do Cisco Secure Client ISE e o perfil de postura do ISE. Ele também pode ser usado para enviar o perfil de postura sozinho se o módulo de postura do ISE já estiver instalado no cliente.

1. Navegue até **Centros de trabalho > Postura > Provisionamento de cliente > Portal de provisionamento de cliente** para abrir a configuração do portal. Expanda a seção **Configurações do portal** e localize o campo **Método de autenticação**, selecione a **Sequência de origem da identidade** a ser usada para autenticação no portal.
2. Configure grupos de identidade internos e externos que estejam autorizados a usar o Portal de Provisionamento de Cliente.



Método de autenticação e grupos autorizados nas configurações do portal

3. No campo **Nome de domínio totalmente qualificado (FQDN)**, configure a URL usada pelos clientes para acessar o portal. Para configurar vários FQDNs, insira os valores separados por vírgulas.

Fully qualified domain name (FQDN):

Idle timeout:
1-30 (minutes)

Display language: Use browser locale

Fallback language:

Always use:

4. Configure o(s) servidor(es) DNS para resolver a URL do portal para os PSNs da lista de Call Home correspondente.
5. Forneça o FQDN aos usuários finais para acessar o portal a fim de instalar o software ISE Posture.

Observação: para usar o FQDN do portal, os clientes devem ter a cadeia de certificados PSN Admin e a cadeia de certificados do Portal instaladas no armazenamento confiável, e o certificado Admin deve conter o FQDN do portal no campo SAN.

Política de provisionamento do cliente

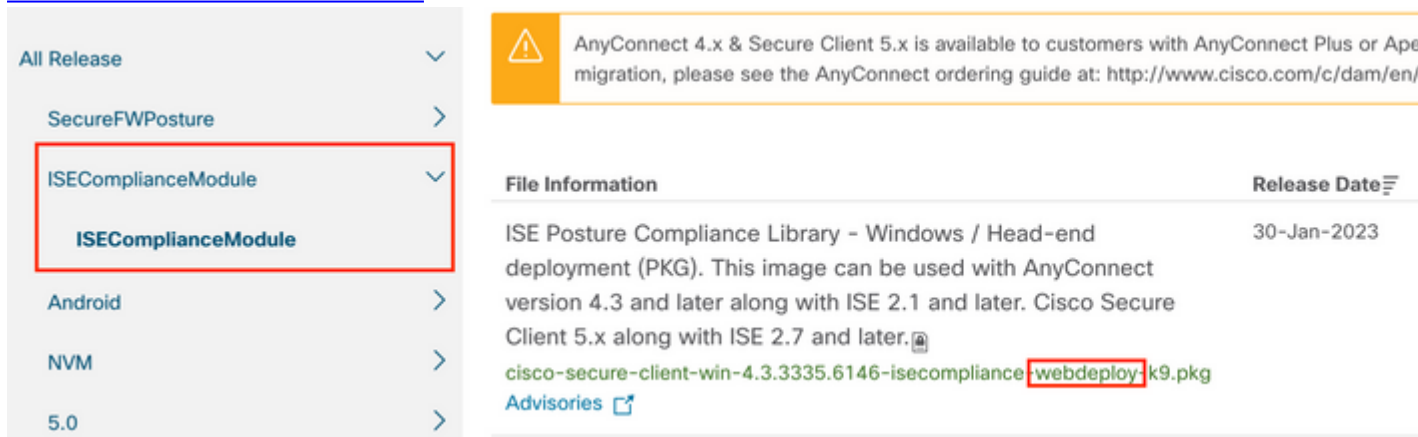
O provisionamento do cliente deve ser configurado no ISE independentemente do tipo de provisionamento (pré-implantação ou implantação na Web) usado para instalar o Cisco Secure Client nos endpoints.

1. Faça o download do pacote de implantação da Web do Cisco Secure Client a partir do [Download do Cisco Software](#).


cisco-secure-client-win-5.0.01242-**webdeploy**-k9.pkg[Advisories](#) 

Pacote de implantação na Web do Cisco Secure Client

2. Faça o download do pacote de implantação da Web do módulo de conformidade mais recente em [Download de software da Cisco](#).



The screenshot shows a software catalog interface. On the left, a navigation menu is expanded to 'ISEComplianceModule', with the sub-item 'ISEComplianceModule' highlighted by a red box. On the right, a 'File Information' table lists the package details. A yellow warning banner at the top states: 'AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Ape migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en...'. The table entry for the package is:

File Information	Release Date
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.  cisco-secure-client-win-4.3.3335.6146-isecompliance- webdeploy -k9.pkg Advisories 	30-Jan-2023

Pacote de implantação da Web do módulo de conformidade ISE

3. No ISE, navegue até Centros de trabalho > Postura > Provisionamento de cliente > Recursos e clique em Adicionar > Recursos de agente do disco local. Selecione **Cisco Provided Packages** no menu suspenso Category e carregue o pacote do Cisco Secure Client webdeploy baixado anteriormente. Repita o mesmo processo para carregar o módulo de conformidade.

Agent Resources From Local Disk

Category

Cisco Provided Packages



Browse...

cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 5.0...	AnyConnectDesktopWind...	5.0.1242.0	Cisco S

Submit

Cancel

Carregar pacotes fornecidos pela Cisco no ISE

- De volta à guia **Resources**, clique em **Add > AnyConnect Posture Profile**. No perfil:
 - Configure um **nome** que possa ser usado para identificar o perfil no ISE.
 - Configure as **regras de nome do servidor** separadas por vírgulas. Use um único asterisco * para permitir a conexão a qualquer PSN, valores curinga para permitir a conexão a qualquer PSN em um domínio específico ou os FQDNs PSN para restringir a conexão a PSNs específicos.
 - Configure **Call Home List** para especificar a lista separada por vírgulas de PSNs. Certifique-se de adicionar a porta do Portal de Provisionamento do Cliente usando o formato FQDN:porta ou IP:porta.

* Name: CSC Redirectionless

Description: Redirectionless Posture LAB - 2 PSNs

Configuração de perfil de postura do ISE I

Posture Protocol

Parameter	Value	Notes	Description
PSA retransmission time	120 secs		This is the agent retry period if there is a Passive Assessment communication failure.
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Server name rules	*.asamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cscc.com"
Call Home List	vix.asamex.com:8443	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till the max time limit is reached

Configuração II do perfil de postura do ISE

Para localizar a porta que deve ser usada na Lista de Call Home, navegue até **Centros de trabalho > Postura > Provisionamento de cliente > Portal de provisionamento de cliente**, selecione o portal em uso e expanda Configurações do portal.

Portals Settings and Customization

Portal Name:
Client Provisioning Portal (default)

Description:
Default portal and user experience user

Language File ▼

[Portal test URL](#)

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:* **8443**

(8000 - 8999)

- De volta à guia **Resources**, clique em **Add > AnyConnect Configuration**. Selecione o pacote Cisco Secure Client e o módulo de conformidade a ser usado.

Aviso: se o Cisco Secure Client tiver sido pré-implantado nos clientes, certifique-se de que a versão no ISE corresponda à versão nos endpoints. Se o ASA ou o FTD for usado para implantação na Web, a versão neste dispositivo também deve ser compatível.

- Role para baixo até a seção **Seleção de postura** e selecione o perfil que foi criado na etapa 1. Clique em **Enviar** na parte inferior da página para salvar a configuração.

* Select AnyConnect Package: CiscoSecureClientDesktopWindows 5.0 ▾

* Configuration Name: AnyConnect Configuration Redirectionless

Description: ISE Redirectionless Posture LAB

Description Value Notes

* Compliance Module: ComplianceModuleWindows 4.3.3335.6146 ▾

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input checked="" type="checkbox"/>

Configuração do AnyConnect

Profile Selection

* ISE Posture: CSC Redirectionless ▾

VPN ▾

Seleção de perfil

- Navegue até **Centros de trabalho > Postura > Provisionamento de cliente > Política de provisionamento de cliente**. Localize a diretiva usada para o sistema operacional necessário e clique em **Editar**. Clique no sinal + na coluna **Resultados** e selecione a configuração do AnyConnect na etapa 5 na seção **Configuração do agente**.

Observação: no caso de várias listas Call Home, use o campo **Other Conditions** para enviar o perfil correto para os clientes correspondentes. No exemplo, o Grupo de localização do

dispositivo é usado para identificar o perfil de postura que é enviado na política.

Dica: se várias políticas de provisionamento de clientes forem configuradas para o mesmo sistema operacional, é recomendável torná-las mutuamente exclusivas, ou seja, um determinado cliente só deve conseguir acessar uma política de cada vez. Os atributos RADIUS podem ser usados na coluna **Outras Condições** para diferenciar uma política de outra.

Agent Configuration

ect Configuration Redirectionless[▼]

Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard [▼]

Choose a Wizard Profile [▼]

Configuração do Agente de Política de Provisionamento de Cliente

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

[▼]

	Rule Name	Identity Groups	Operating Systems	Other Conditions
<input checked="" type="checkbox"/>	IOS	If Any	and Apple iOS All	and Condition(s)
<input checked="" type="checkbox"/>	Android	If Any	and Android	and Condition(s)
<input checked="" type="checkbox"/>	Windows	If Any	and Windows All	and DEVICE:Location EQUALS All Locations#US#WEST
<input checked="" type="checkbox"/>	MAC OS	If Any	and Mac OSX	and Condition(s)
<input checked="" type="checkbox"/>	Chromebook	If Any	and Chrome OS All	and Condition(s)

8. Repita as etapas de 4 a 7 para cada lista Call Home e o perfil de postura correspondente em uso. Para ambientes híbridos, os mesmos perfis podem ser usados para clientes de redirecionamento.

Autorização

Perfil de autorização

1. Navegue para Política > Elementos de política > Resultados > Autorização > ACLs que podem ser baixadas e clique em Adicionar.
2. Crie um DACL para permitir o tráfego para DNS, DHCP (se usado), ISE PSNs e bloquear outro tráfego. Certifique-se de permitir qualquer outro tráfego que seja necessário acessar antes do acesso final compatível.

* Name: redirectionless_posture

Description: DACL used for posture with ise30baaamex and ise30cmexaaa

IP version: IPv4 IPv6 Agnostic

* DACL Content:

1234567	permit udp any any eq domain
8910111	permit udp any any eq bootps
2131415	permit ip any host <pin 1 IP address>
1617181	permit ip any host <pin 2 IP address>
9202122	permit icmp any any
2324252	deny ip any any
6272829	
3031323	
3343536	
3738394	
0414243	

Check DACL Syntax

Recheck < >

DACL is valid

configuração de DACL

```
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host
```

```
permit ip any host
```

```
deny ip any any
```

Cuidado: alguns dispositivos de terceiros podem não suportar DACLs; nesses casos, é necessário usar um ID de filtro ou outros atributos específicos do fornecedor. Consulte a documentação do fornecedor para obter mais informações. Se as DACLs não forem usadas, certifique-se de configurar a ACL correspondente no dispositivo de rede.

3. Navegue para Política > Elementos de política > Resultados > Autorização > Perfis de autorização e clique em Adicionar. Dê um nome ao perfil de autorização e selecione **Nome da DACL** em **Tarefas comuns**. No menu suspenso, selecione a DACL criada na etapa 2.

[Authorization Profiles](#) > Redirectionless posture

Authorization Profile

* Name	Redirectionless posture
Description	<div style="border: 1px solid #ccc; height: 80px;"></div>
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> ⓘ
Agentless Posture	<input type="checkbox"/> ⓘ
Passive Identity Tracking	<input type="checkbox"/> ⓘ

Common Tasks

<input checked="" type="checkbox"/> DACL Name	redirectionless_posture
---	-------------------------

Perfil de autorização

Observação: se as DACLs não forem usadas, use **Filter-ID** de **Common Tasks** ou as **Advanced Attribute Settings** para enviar o nome da ACL correspondente.

4. Repita as etapas de 1 a 3 para cada lista de Call Home em uso. Para ambientes híbridos, é necessário

apenas um único perfil de autorização para o redirecionamento. A configuração do perfil de autorização para redirecionamento está fora do escopo deste documento.

Política de Autorização

1. Navegue para **Política > Conjuntos de políticas** e abra o conjunto de políticas em uso ou crie um novo.
2. Role para baixo até a seção **Política de autorização**. Crie uma política de autorização usando **Session PostureStatus NOT_EQUALS Compliant** e selecione o perfil de autorização criado na seção anterior.

Authorization Policy (4)

Status	Rule Name	Conditions	Profiles
✓	Compliant	Session-PostureStatus EQUALS Compliant	Compliant access ×
✓	Redirectionless	AND • DEVICE-Posture EQUALS Posture#Redirectionless • DEVICE-Location EQUALS All Locations#US#WEST • Session-PostureStatus NOT_EQUALS Compliant	Redirectionless posture ×
✓	Redirection	AND • Session-PostureStatus NOT_EQUALS Compliant • DEVICE-Posture EQUALS Posture#Redirection	Redirection posture ×
✓	Default		DenyAccess ×

Políticas de autorização

3. Repita a etapa 2 para cada perfil de autorização com sua lista do Call Home correspondente em uso. Para ambientes híbridos, é necessária apenas uma única política de autorização para o redirecionamento.

Troubleshooting

Compatível com o Cisco Secure Client e postura não aplicável (pendente) no ISE

Sessões obsoletas/fantasmas

A presença de sessões obsoletas ou fantasmas na implantação pode gerar falhas intermitentes e aparentemente aleatórias com descoberta de postura sem redirecionamento, que resultam em usuários presos em uma postura de acesso desconhecido/não aplicável no ISE, enquanto a IU do Cisco Secure Client mostra o acesso compatível.

[Sessões obsoletas](#) são sessões antigas que não estão mais ativas. Eles são criados por uma solicitação de autenticação e início de contabilização, mas nenhuma parada de contabilização é recebida no PSN para

limpar a sessão.

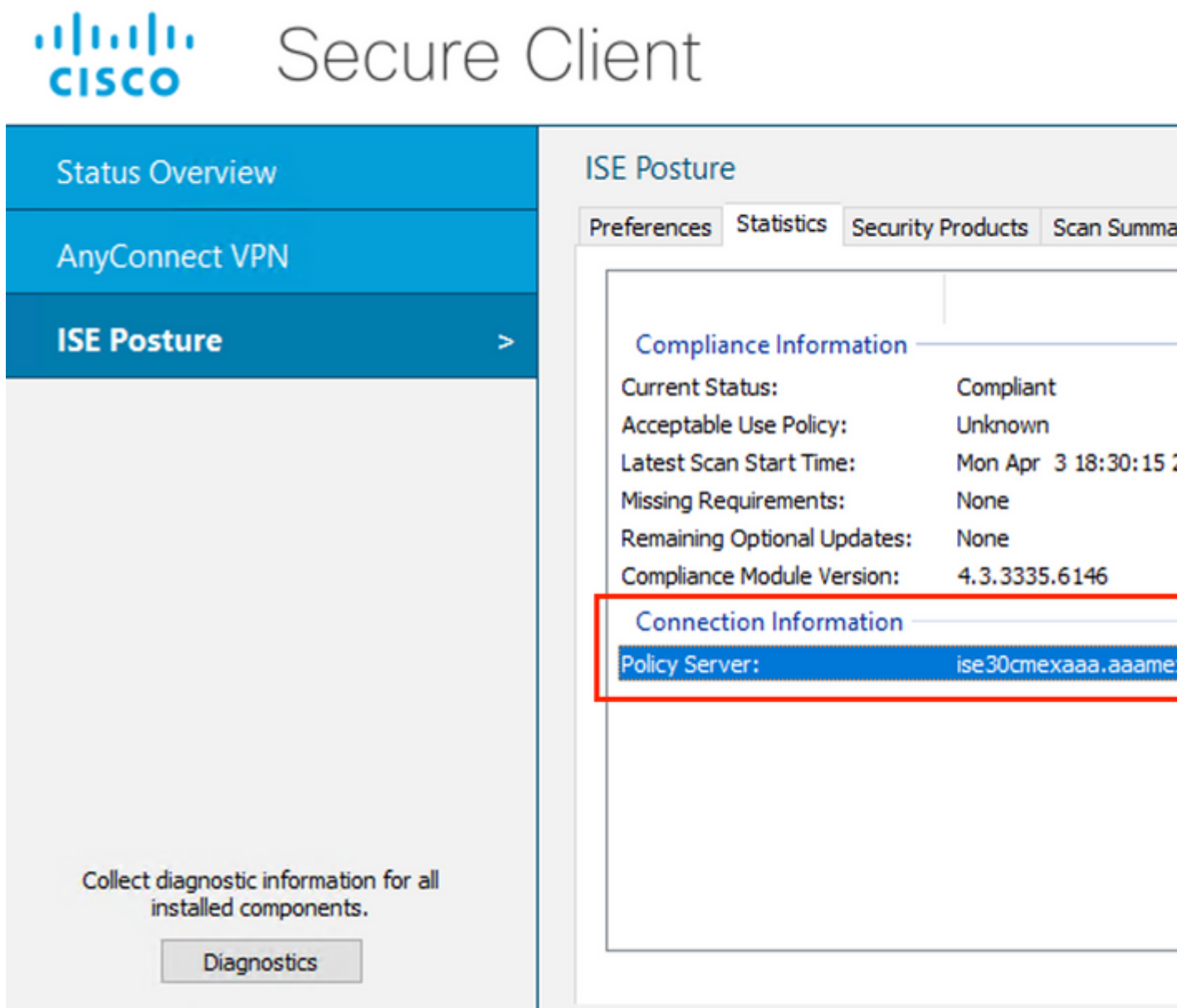
[As sessões fantasmas](#) são sessões que nunca estiveram realmente ativas em uma PSN específica. Eles são criados por uma atualização provisória de contabilização, mas nenhuma parada de contabilização é recebida no PSN para limpar a sessão.

Identificar

Para identificar um problema de sessão obsoleta/fantasma, verifique a PSN usada na verificação do sistema no cliente e compare com a PSN que está executando a autenticação:

1. Na IU do Cisco Secure Client, clique no **ícone de engrenagem** no canto inferior esquerdo. No menu esquerdo, abra a seção **ISE Posture** e navegue até a guia **Statistics**. Anote o Servidor de políticas em Informações de conexão.

 Cisco Secure Client



The screenshot displays the Cisco Secure Client interface. On the left, a navigation menu includes 'Status Overview', 'AnyConnect VPN', and 'ISE Posture' (selected). The main content area shows the 'ISE Posture' section with tabs for 'Preferences', 'Statistics', 'Security Products', and 'Scan Summary'. Under the 'Statistics' tab, there are two sections: 'Compliance Information' and 'Connection Information'. The 'Connection Information' section is highlighted with a red box and contains the following data:

Compliance Information	
Current Status:	Compliant
Acceptable Use Policy:	Unknown
Latest Scan Start Time:	Mon Apr 3 18:30:15 2
Missing Requirements:	None
Remaining Optional Updates:	None
Compliance Module Version:	4.3.3335.6146

Connection Information	
Policy Server:	ise30cmexaaa.aaame

At the bottom of the interface, there is a button labeled 'Diagnostics' with the text 'Collect diagnostic information for all installed components.' above it.

2. Nos registros ao vivo do ISE RADIUS, observe o seguinte:

- Alteração no status da postura
- Alteração no servidor
- Nenhuma alteração na Diretiva de Autorização e no Perfil de Autorização
- Nenhum log ao vivo de CoA

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baamex
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baamex

Logs ao vivo para sessão obsoleta/fantasma

3. Abrir a sessão ao vivo ou os detalhes do log ao vivo da última autenticação. Anote o Servidor de políticas, se ele for diferente do servidor observado na etapa 1, isso indica um problema com sessões obsoletas/fantasma.

Overview	
Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details	
Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691
Policy Server	ise30baamex
Event	5200 Authentication succeeded
Username	redirectionless


Servidor de política em detalhes do log ao vivo

Solução

As versões do ISE acima do ISE 2.6 patch 6 e 2.7 patch 3 implementam o [RADIUS Session Directory](#) como uma solução para cenário de sessão obsoleta/fantasma em fluxo de postura sem redirecionamento.

1. Navegue para Administration > **System** > **Settings** > Light Data Distribution e verifique se a caixa de seleção Enable RADIUS Session Directory está ativada.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Back

FIPS Mode
Security Settings
Alarm Settings
Posture >
Profiling
Protocols >
Endpoint Scripts >
Proxy
SMTP Server
SMS Gateway
System Time 
ERS Settings
API Gateway Settings
Network Success Diagnostics >
DHCP & DNS Services
Max Sessions
Light Data Distribution

RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

Enable RADIUS Session Directory



Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address in ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling sessions. The legacy Profiler owners directory option will use legacy Profiler owners directory.

Enable Endpoint Owner Directory

Advanced Settings

Configure the following options for RSD and EPOD.

Batch size
10  Items 

Ativar o diretório de sessão RADIUS

2. Na CLI do ISE, verifique se o **serviço de mensagens do ISE** está sendo executado em **todas as PSNs** executando o comando **show applications status ise**.

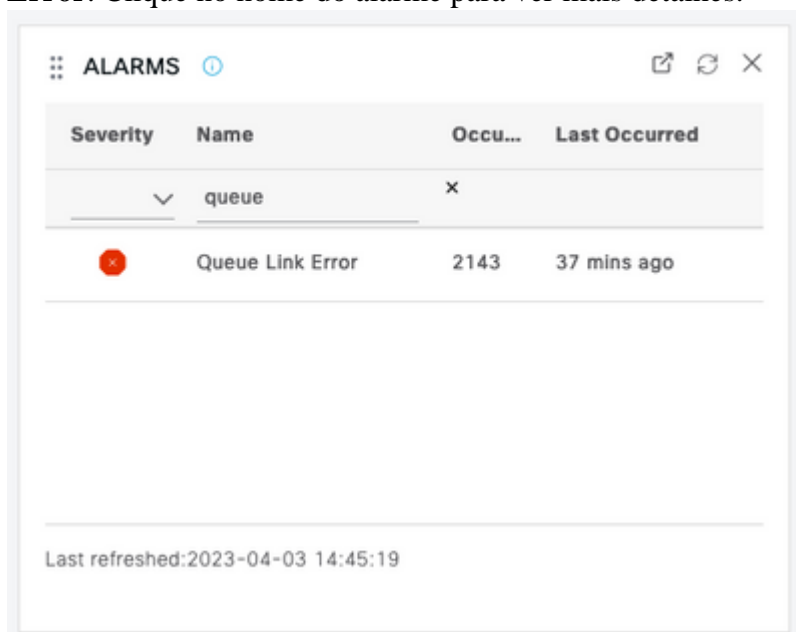
```
ise30cmexaaa/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	12434
Database Server	running	112 PROCESSES
Application Server	running	33093
Profiler Database	running	19622
ISE Indexing Engine	running	42923
AD Connector	running	60317
M&T Session Database	running	19361
M&T Log Processor	running	33283
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
Docker Daemon	running	14791
TC-NAC MongoDB Container	running	18594
TC-NAC Core Engine Container	running	18981
VA Database	running	53465
VA Service	running	53906
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	running	55480
PassiveID Syslog Service	running	56312
PassiveID API Service	running	57153
PassiveID Agent Service	running	58079
PassiveID Endpoint Service	running	59138
PassiveID SPAN Service	running	60059
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	16526
ISE API Gateway Database Service	running	18463
ISE API Gateway Service	running	23052

Serviço de mensagens do ISE em execução

Observação: esse serviço se refere ao método de comunicação usado para RSD entre PSNs e deve estar em execução independentemente do status da configuração do Serviço de mensagens do ISE para syslog que pode ser definido na interface do usuário do ISE.

3. Navegue até o **painel do ISE** e localize o dashlet **Alarms**. Verifique se há algum alarme **Queue Link Error**. Clique no nome do alarme para ver mais detalhes.



Alarmes de Erro de Link de Fila

4. Verifique se os alarmes são gerados entre as PSNs usadas para postura.

⊗ Alarms: Queue Link Error

Description

The queue link between two nodes in the ISE deployment is down.

Suggested Actions

Please check and restore connectivity between the nodes. Ensure that the nodes and the ISE Messaging Service are up and running. Ensure that ISE Messaging Service ports are not blocked by firewalls or are being registered to deployment or manually-synced from PSPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Rows/Page 100 < > 1

Refresh Acknowledge

<input type="checkbox"/> Time Stamp	Description	Cause={tls_alert;" unknown Ca" }
<input type="checkbox"/> Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={tls_alert;" unkno...	
<input type="checkbox"/> Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={tls_alert;" unkno...	

Detalhes do alarme de Erro do Link da Fila

5. Passe o mouse sobre a descrição do alarme para ver todos os detalhes e anote o campo Causa. As duas causas mais comuns para erros de link de fila são:

- Tempo limite: indica que as solicitações enviadas por um nó para outro nó na porta 8671 não são respondidas dentro do limite. Para corrigir, verifique se a porta TCP 8671 é permitida entre os nós.
- CA desconhecida: indica que a cadeia de certificados que assina o certificado de Mensagens do ISE não é válida ou está incompleta. Para corrigir esse erro:
 - a. Navegue até **Administração > Sistema > Certificados > Solicitações de assinatura de certificado**.
 - b. Clique em **Generate Certificate Signing Requests (CSR)**.
 - c. No menu suspenso, selecione **ISE Root CA** e clique em **Replace ISE Root CA Certificate chain**.
Se a CA raiz do ISE não estiver disponível, navegue para **Autoridade de certificação > Configurações internas da CA** e clique em **Habilitar autoridade de certificação**, em seguida, volte para o CSR e gere novamente a CA raiz.
 - d. Gere um novo CSR e selecione **ISE Messaging Service** no menu suspenso.
 - e. Selecione todos os nós da implantação e gere novamente o certificado.

Observação: é esperado que ele observe alarmes de Erro de link de fila com causa CA desconhecida ou Econnrejected enquanto os certificados forem regenerados. Monitore os alarmes após a geração do certificado para confirmar se o problema foi resolvido.

Desempenho

Identificar

Problemas de desempenho, como alta utilização da CPU e alta média de carga relacionada à postura sem redirecionamento, podem afetar a PSN e os nós MnT e são frequentemente acompanhados ou precedidos pelos seguintes eventos:

- Aleatório ou intermitente *Nenhum servidor de políticas detectou* erros no Cisco Secure Client
- *O limite máximo de recursos atingiu* relatórios para eventos de valor de limite de pool de threads de serviço do portal. Navegue até Operações > **Relatórios** > Relatórios > Auditoria > Auditoria de

operações para ver os relatórios.

- *Consulta de Postura para pesquisa MNT é um alto* alarme. Esses alarmes são gerados apenas no ISE 3.1 e versões superiores.

Solução





Se o desempenho da implantação for afetado por uma postura sem redirecionamento, isso geralmente indica uma implementação ineficiente. Recomenda-se a revisão dos seguintes aspectos:

- Número de PSNs usadas por lista de Call Home. Considere reduzir o número de PSNs que podem ser usadas para postura por endpoint ou dispositivo de rede de acordo com o design.
- Porta do portal de provisionamento do cliente na lista Call Home. Certifique-se de que o número da porta do portal esteja incluído após o IP ou o FQDN de cada nó.

Para atenuar o impacto:

1. Limpe `connectiondata.xml` dos endpoints removendo o arquivo da pasta do Cisco Secure Client e reinicie o serviço de postura do ISE ou o Cisco Secure Client. Se os serviços não forem reiniciados, o arquivo antigo será gerado novamente e as alterações não terão efeito. Essa ação também deve ser executada após a revisão e modificação das listas Call Home.
2. Use DACLs ou outras ACLs para bloquear o tráfego para ISE PSNs para conexões de rede onde ele não é relevante:
 - Para conexões em que a postura não é imposta nas políticas de autorização, mas que se aplicam a endpoints com o módulo de postura do Cisco Secure Client ISE instalado, bloqueie o tráfego dos clientes para todos os PSNs do ISE para as portas TCP 8905 e porta do Portal de Provisionamento de Cliente. Esta ação também é recomendada para postura com implementação de redirecionamento.
 - Para conexões em que a postura é imposta nas políticas de autorização, permita o tráfego dos clientes para a PSN de autenticação e bloqueie o tráfego para outras PSNs na implantação. Esta ação pode ser implementada temporariamente durante a revisão do projeto.

Authorization Profile

* Name	Redirectionless PSN1
Description	Authorization profile for redirectionless posture with DACL allowing traffic only to PSN1, DNS and DHCP
* Access Type	ACCESS_ACCEPT
Network Device Profile	 Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Agentless Posture	<input type="checkbox"/> 
Passive Identity Tracking	<input type="checkbox"/> 

Common Tasks

<input checked="" type="checkbox"/> DACL Name	redirectionless_posture_psn1
---	------------------------------

Perfil de autorização com DACL para PSN único

✓	Compliant		Session-PostureStatus EQUALS Compliant
✓	Redirectionless PSN1	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS Ise30baaamex.aaam
✓	Redirectionless PSN2	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS Ise30cmexaaa.aaam
✓	Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection

Políticas de autorização por PSN

Relatório

A contabilização de RADIUS é essencial para o gerenciamento de sessões no ISE. Como a postura depende de uma sessão ativa a ser executada, erros ou falta de configuração de contabilidade também podem afetar a descoberta da postura e o desempenho do ISE. É importante verificar se a contabilização está configurada corretamente no dispositivo de rede para enviar solicitações de autenticação, início de contabilização, interrupção de contabilização e atualizações de contabilização para um único PSN para cada sessão.

Para verificar os pacotes de contabilização recebidos no ISE, navegue para **Operações > Relatórios > Relatórios > Endpoints e Usuários > Contabilidade RADIUS**.

Informações Relacionadas

- [Suporte técnico e downloads 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.