Configuración y resolución de problemas de sincronización del estado de postura

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Configurar
  - Diagrama de la red
  - Configuraciones
- Verificación
  - Desde el paquete DART
  - Desde la captura de paquetes en el cliente
  - Desde ISE
  - Reinicio de postura al cambiar el estado de postura
- Troubleshoot
  - La sincronización del estado de condición no se inicia
  - La sincronización del estado de la postura falla con la alarma en el panel de ISE
    - Verificar dACL configurada para perfil de autorización de condición "compatible"
  - Problemas conocidos
    - La sincronización del estado de postura falla con la alarma en ISE

Introducción

Este documento describe la configuración y el uso de la sincronización del estado de condición introducida en la versión 3.1 de Cisco Identity Service Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Flujo de estado en Cisco ISE
- Configuración de los componentes de estado en Cisco ISE

Se supone que tiene una configuración de postura en lugar de cualquier tipo.

Para comprender mejor los conceptos descritos más adelante, se recomienda seguir estos pasos:

- Guía del administrador de Cisco Identity Services Engine, versión 3.1
- Comparación de versiones anteriores de ISE con el flujo de estado de ISE en ISE 2.2
- Gestión y estado de sesiones de ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 3.1
- Cisco Secure Client 5.0.00556

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

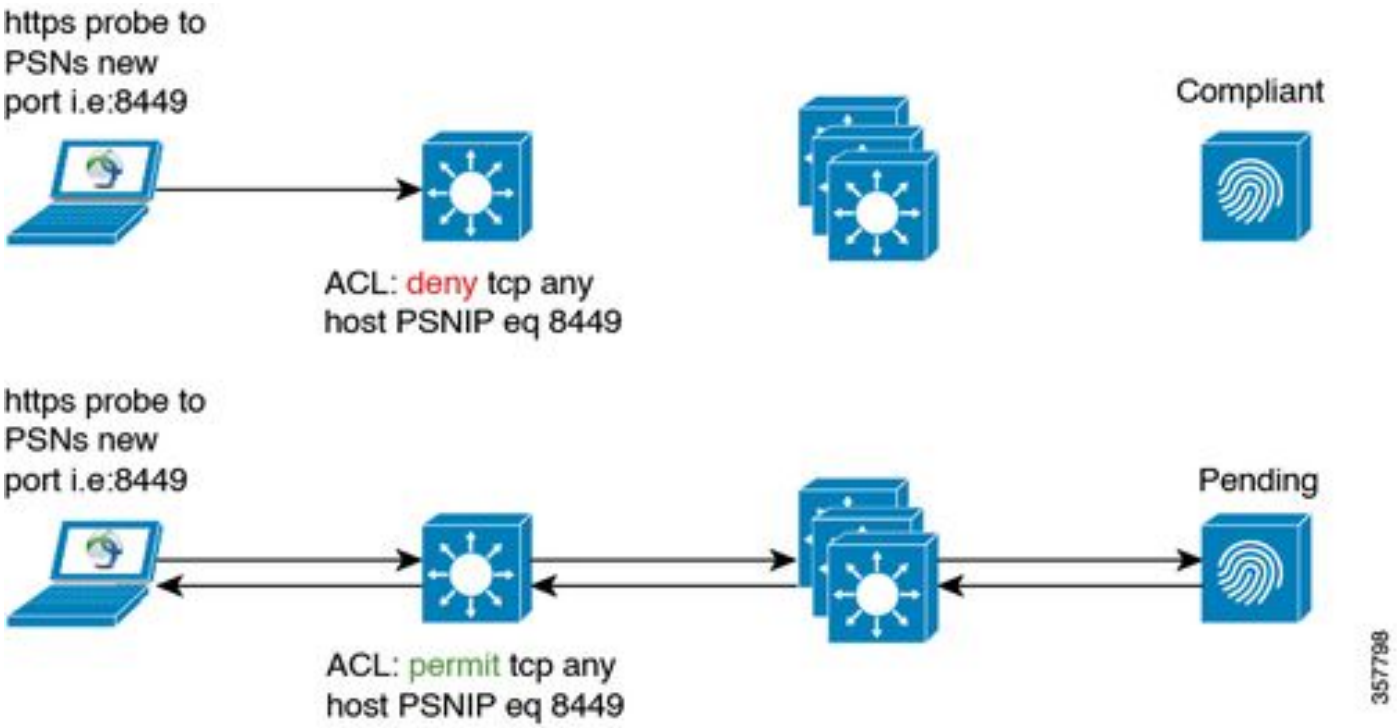
El flujo de estado de ISE normalmente no permite actualizar el estado de estado en el cliente desde ISE. Cisco Secure Client Posture Module se utiliza para evaluar el estado de estado del terminal y lo mantiene hasta que se produzca un cambio en la red, una reevaluación periódica u otros activadores en el lado del cliente. Si el estado de estado del terminal cambia en ISE debido a una terminación de sesión u otros motivos, es posible que el módulo de estado de cliente seguro no sea consciente de ese cambio, por lo que el terminal permanece en estado de estado desconocido con acceso limitado a la red hasta que se produce uno de los desencadenadores del lado del cliente.

Este documento se centra en una nueva función: Posture Status Synchronization, que se desarrolló para abordar este tipo de problemas y permitir que ISE proporcione información al módulo de postura de cliente seguro sobre el estado actual del terminal.

Configurar

El puerto de sondeo de estado de postura se introdujo en cada nodo PSN de ISE cuando la sincronización de estado de postura está habilitada: TCP 8449 de forma predeterminada. Se supone que es accesible desde el terminal si el estado de la postura del terminal es Desconocido o Pendiente y no es accesible si el estado del terminal es Conforme.

Diagrama de la red



Configuraciones

La configuración de la función de sincronización del estado de postura consta de dos partes:

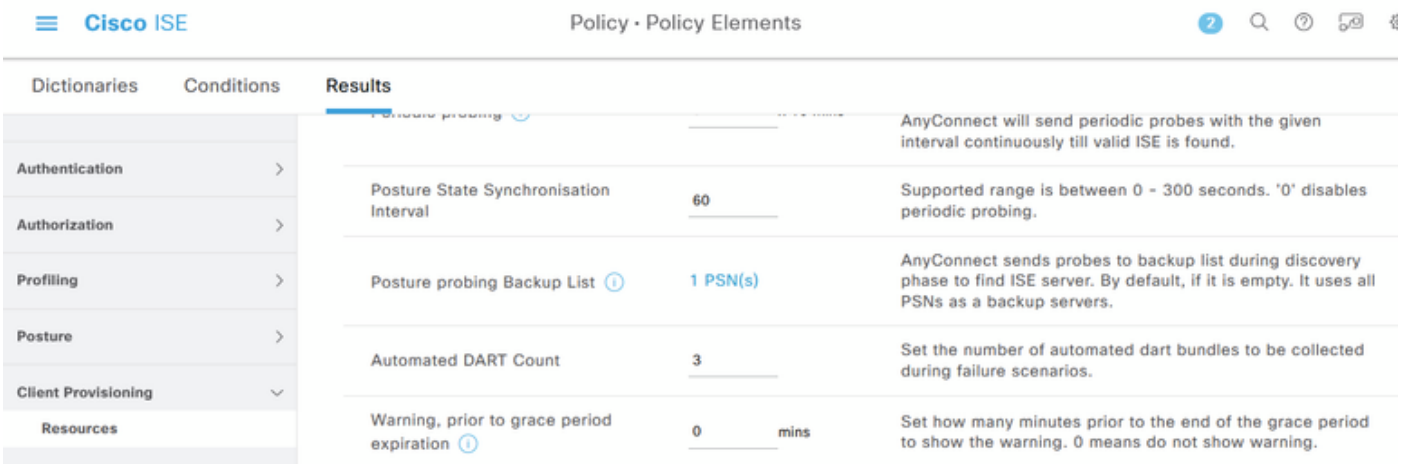
1. Configuración del perfil de postura de AnyConnect

   1.1 En la GUI de Cisco ISE, navegue hasta Política > Elementos de política > Resultados > Aprovisionamiento del cliente > Recursos.

   1.2 Seleccione el perfil de postura de AnyConnect que ya utiliza o cree uno nuevo.

   1.3 En el área Comportamiento del agente, configure el Intervalo de sincronización del estado de postura en cualquier valor entre 1 y 300 segundos, 0 - inhabilita la Sincronización del estado de postura

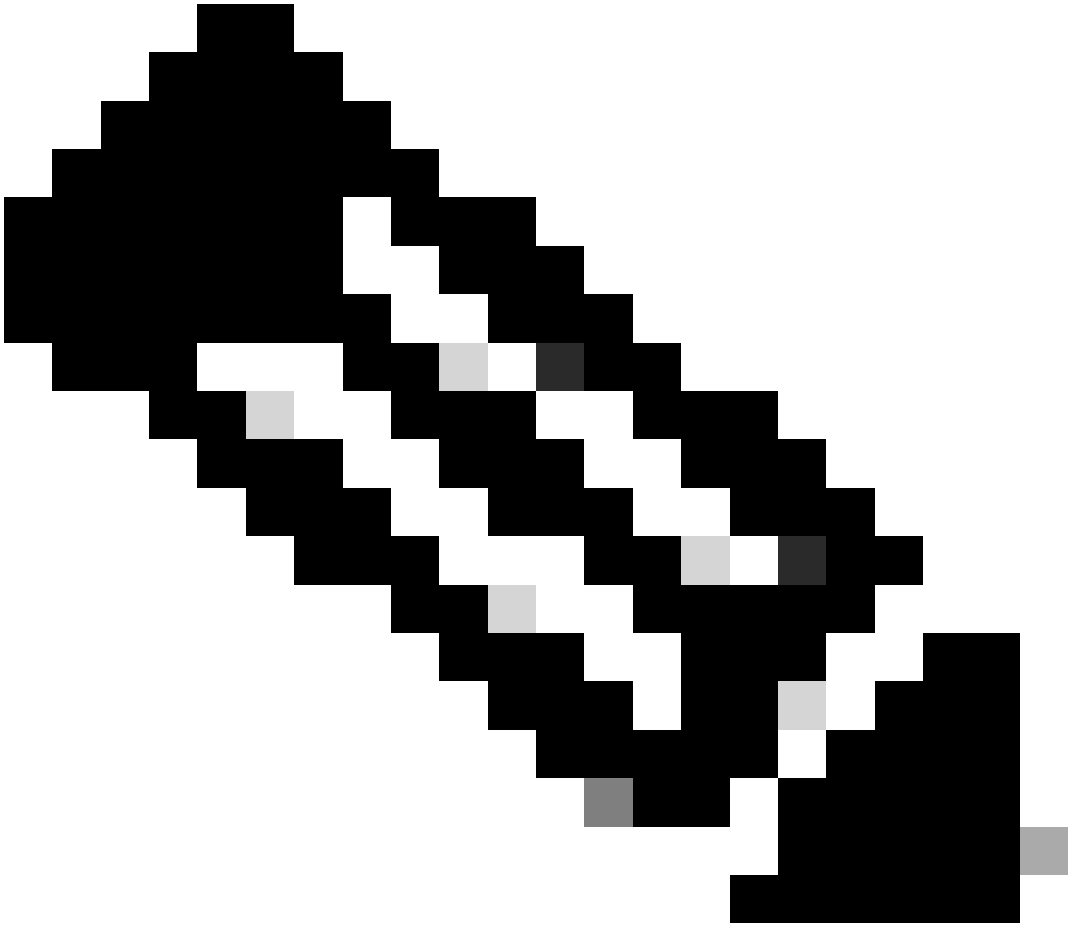
   1.4 Puede configurar la lista de respaldo de sondeo de posición: Secure Client utiliza esta lista para verificar el estado de posición en los PSN seleccionados. Si no selecciona ningún PSN, el PSN conectado y dos servidores de copia de seguridad cualesquiera se utilizan como copias de seguridad para la sincronización del estado de estado.



2. Configuración de una ACL descargable (dACL) para bloquear el acceso al puerto de sincronización del estado de postura en Cisco ISE cuando el estado del cliente es Conforme o No Conforme. Debe agregar la entrada de negación de control de acceso con el puerto de sincronización de estado de postura para cada PSN en la parte superior de las ACL utilizadas para los terminales compatibles para restringir el acceso al puerto de sincronización de estado de postura si se conoce el estado del terminal, por ejemplo:

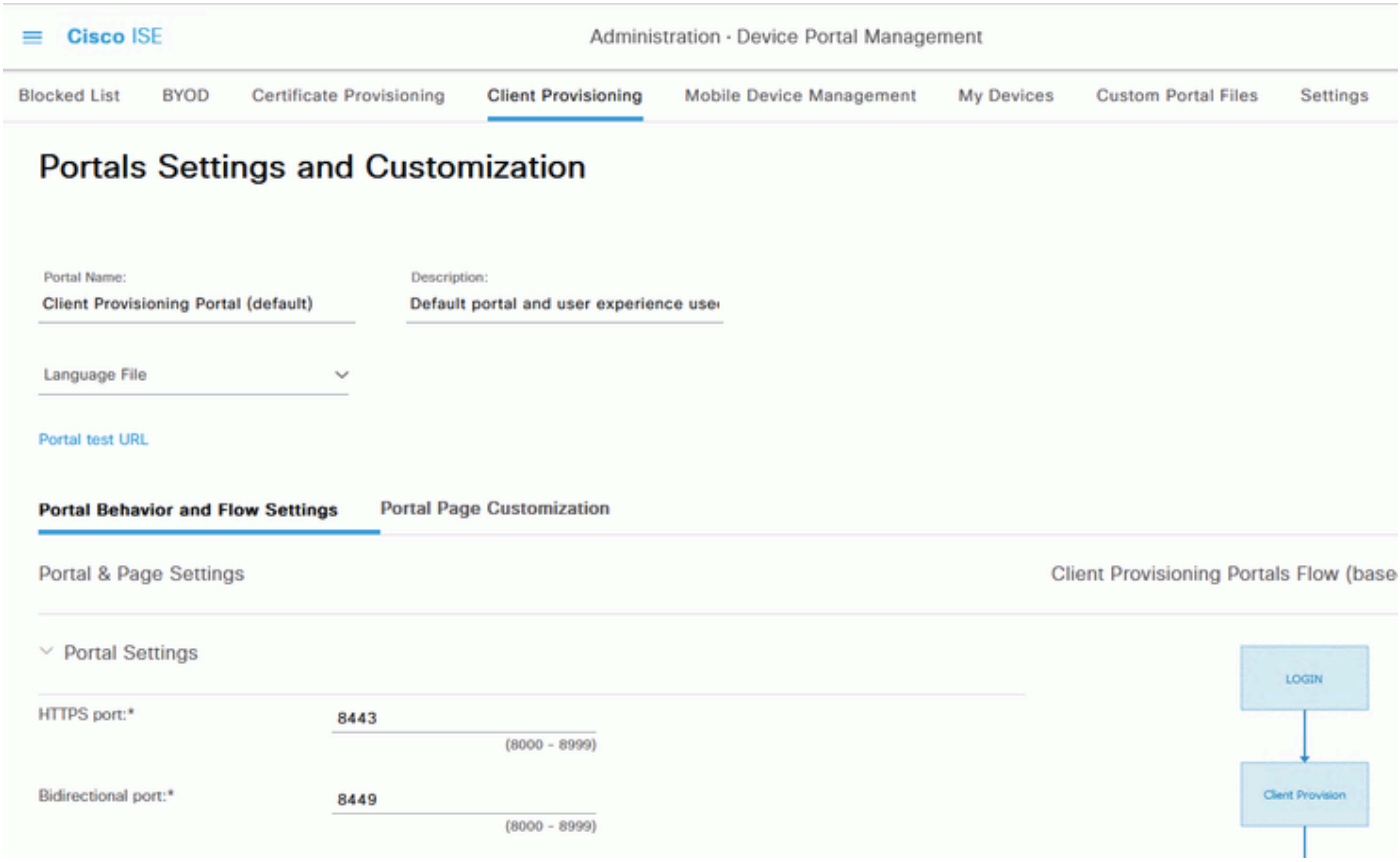
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

permit ip any any no es obligatorio, puede sustituirlo por cualquier conjunto de reglas según sus necesidades.



Nota: si no se configura la entrada de denegación en dACL, se activa la alarma de detección de configuración de posición en el panel de Cisco ISE y se desactiva la sincronización del estado de postura en el terminal hasta que se reinicie Cisco Secure Client.

El puerto de sincronización de estado de postura (puerto bidireccional) se puede cambiar en la página de configuración del portal de aprovisionamiento de clientes. Vaya a Administration > Device Portal Management > Client Provisioning > Select desired portal > Portal Behavior and Flow Settings y abra Portal Settings. No se puede cambiar el puerto de sincronización de estado de postura para el portal de aprovisionamiento de clientes predeterminado.



Verificación

Desde el paquete DART

La sincronización del estado de la postura se puede verificar desde el lado del cliente consultando los registros del módulo de estado de Cisco Secure Client (AnyConnect_ISEPosture.txt) del paquete DART:

1. La evaluación de posición ha finalizado, el estado de postura es Conforme.

```
2022/11/09 12:22:47 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xC60 Fil
```

2. Se ha iniciado el sondeo de sincronización de estado de postura.

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

3. Se inicia la conexión HTTPS con ISE PSN en el puerto de sincronización de estado de postura (8449).

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. Tiempo de espera para la sonda de sincronización de estado de postura.

```
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_winhttp_post Thread Id: 0x296C File
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_post Thread Id: 0x296C File: hs_tra
2022/11/09 12:22:54 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

Desde la captura de paquetes en el cliente

La captura de paquetes tomada en el cliente muestra los paquetes SYN enviados hacia el nodo ISE PSN en el puerto de sincronización de estado de postura (8449) sin respuesta SYN-ACK de ISE PSN:

413	2022-11-09 12:23:42.611361	192.168.255.211	192.168.48.231	TCP	66 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
421	2022-11-09 12:23:43.618040	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
423	2022-11-09 12:23:45.626811	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
430	2022-11-09 12:23:49.645454	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
474	2022-11-09 12:24:00.621182	192.168.255.211	192.168.48.231	TCP	66 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
480	2022-11-09 12:24:01.633779	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
486	2022-11-09 12:24:03.648948	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
488	2022-11-09 12:24:06.622549	192.168.255.211	192.168.48.231	TCP	66 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
490	2022-11-09 12:24:07.632488	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
493	2022-11-09 12:24:09.635802	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
505	2022-11-09 12:24:13.648698	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14

Desde ISE

No se puede verificar la configuración correcta de la sincronización del estado de postura desde el lado de ISE, ya que se supone que la conexión del puerto de sincronización del estado de postura (8449) falla.

Reinicio de postura al cambiar el estado de postura

1) Se ha recibido información del estado de la sesión de ISE con el estado de estado "Desconocido" mientras que Cisco Secure Client se encuentra en estado "Conforme".

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
```

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_http
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_http
```

2) Cisco Secure Client reconoce el cambio de estado de la postura y reinicia la detección de posición:

```
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
```

3) Cisco Secure Client detiene la sincronización del estado de postura hasta que se realiza la evaluación de estado:

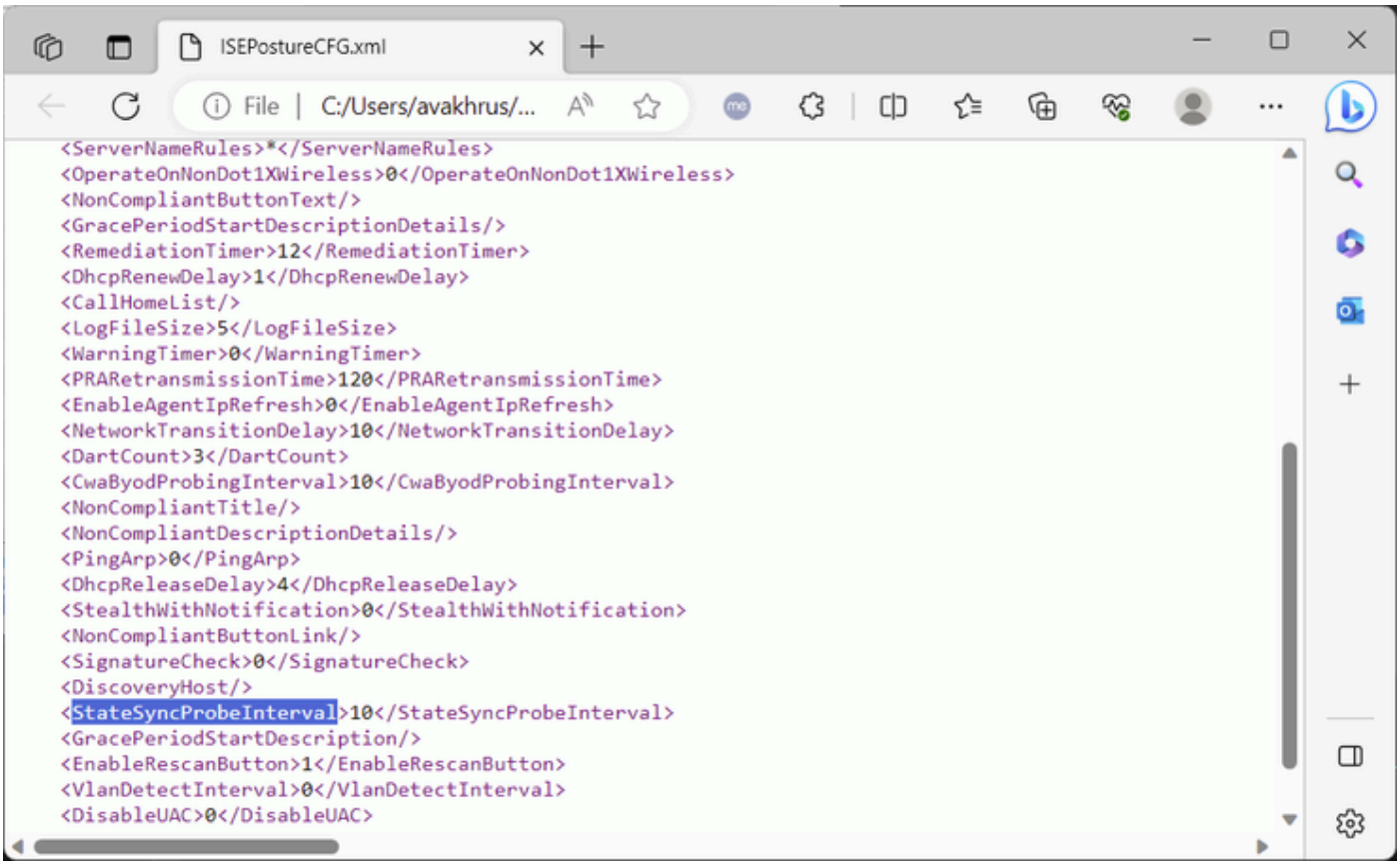
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: hs_transport_free Thread Id: 0xC60 File: hs_tran
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

Troubleshoot

La sincronización del estado de condición no se inicia

Si no hay indicación de inicio de sincronización del estado de postura en el archivo de registro AnyConnect_ISEPosture.txt y el cliente no intenta establecer una conexión con el nodo PSN de ISE en el puerto de sincronización del estado de postura (8449), compruebe el archivo de configuración de postura ISEPostureCFG.xml del paquete DART o directamente en el equipo cliente: "%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\" para un PC con Windows.

El parámetro responsable de la sincronización del estado de postura es "StateSyncProbeInterval", se supone que debe establecerse con un valor superior a 0:



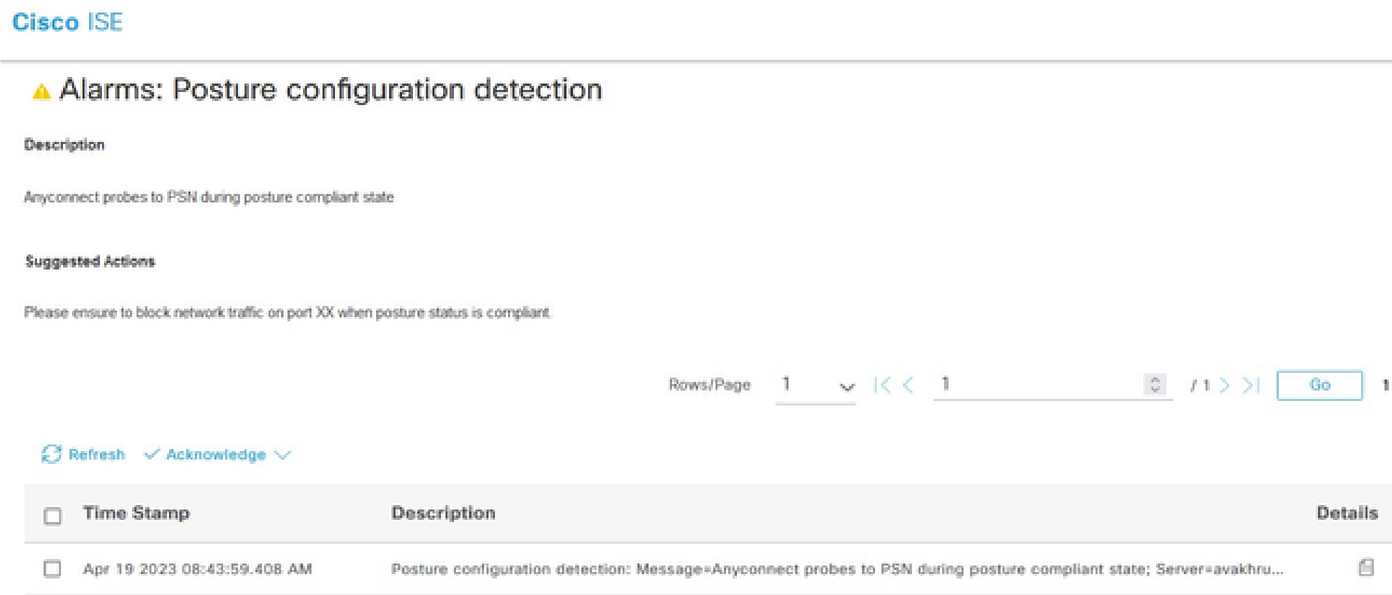
La ausencia de "StateSyncProbeInterval" o el valor "0" significa que la sincronización del estado de postura está deshabilitada.

Si se establece "Intervalo de sincronización de estado de postura" en Perfil de postura en ISE pero no se refleja en un archivo de configuración en el cliente, debe investigarse el aprovisionamiento de estado.

La sincronización del estado de la postura falla con la alarma en el panel de ISE

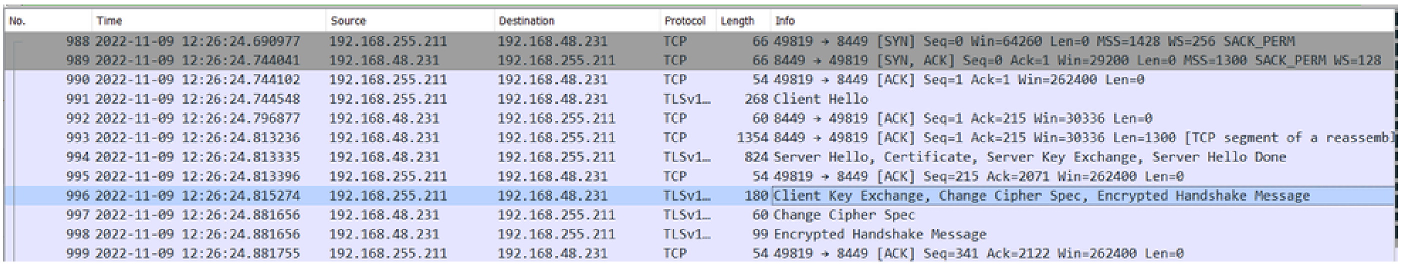
Si la sincronización de estado de postura falla con la alarma en ISE, significa que Cisco Secure Client pudo alcanzar ISE en el puerto de sincronización de estado de postura (8449) y solicitó un estado para la sesión con el estado "Conforme".

- Alarma en la GUI de ISE:



- Validar desde captura de paquetes

Se establece la conexión TCP en el puerto de sincronización de estado de postura (8449):



No.	Time	Source	Destination	Protocol	Length	Info
988	2022-11-09 12:26:24.690977	192.168.255.211	192.168.48.231	TCP	66	49819 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
989	2022-11-09 12:26:24.744041	192.168.48.231	192.168.255.211	TCP	66	8449 → 49819 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM WS=128
990	2022-11-09 12:26:24.744102	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=1 Ack=1 Win=262400 Len=0
991	2022-11-09 12:26:24.744548	192.168.255.211	192.168.48.231	TLSv1…	268	Client Hello
992	2022-11-09 12:26:24.796877	192.168.48.231	192.168.255.211	TCP	60	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=0
993	2022-11-09 12:26:24.813236	192.168.48.231	192.168.255.211	TCP	1354	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=1300 [TCP segment of a reassemb]
994	2022-11-09 12:26:24.813335	192.168.48.231	192.168.255.211	TLSv1…	824	Server Hello, Certificate, Server Key Exchange, Server Hello Done
995	2022-11-09 12:26:24.813396	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=215 Ack=2071 Win=262400 Len=0
996	2022-11-09 12:26:24.815274	192.168.255.211	192.168.48.231	TLSv1…	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
997	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	60	Change Cipher Spec
998	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	99	Encrypted Handshake Message
999	2022-11-09 12:26:24.881755	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=341 Ack=2122 Win=262400 Len=0

- Validar desde el registro del módulo de estado de Cisco Secure Client

Compruebe AnyConnect_ISEPosture.txt en el paquete DART:

1) Se inicia la conexión HTTPS con ISE PSN en el puerto de sincronización de estado de postura (8449).

```
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
```

2) Se ha recibido información del estado de la sesión de ISE con el estado de condición "Conforme".

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

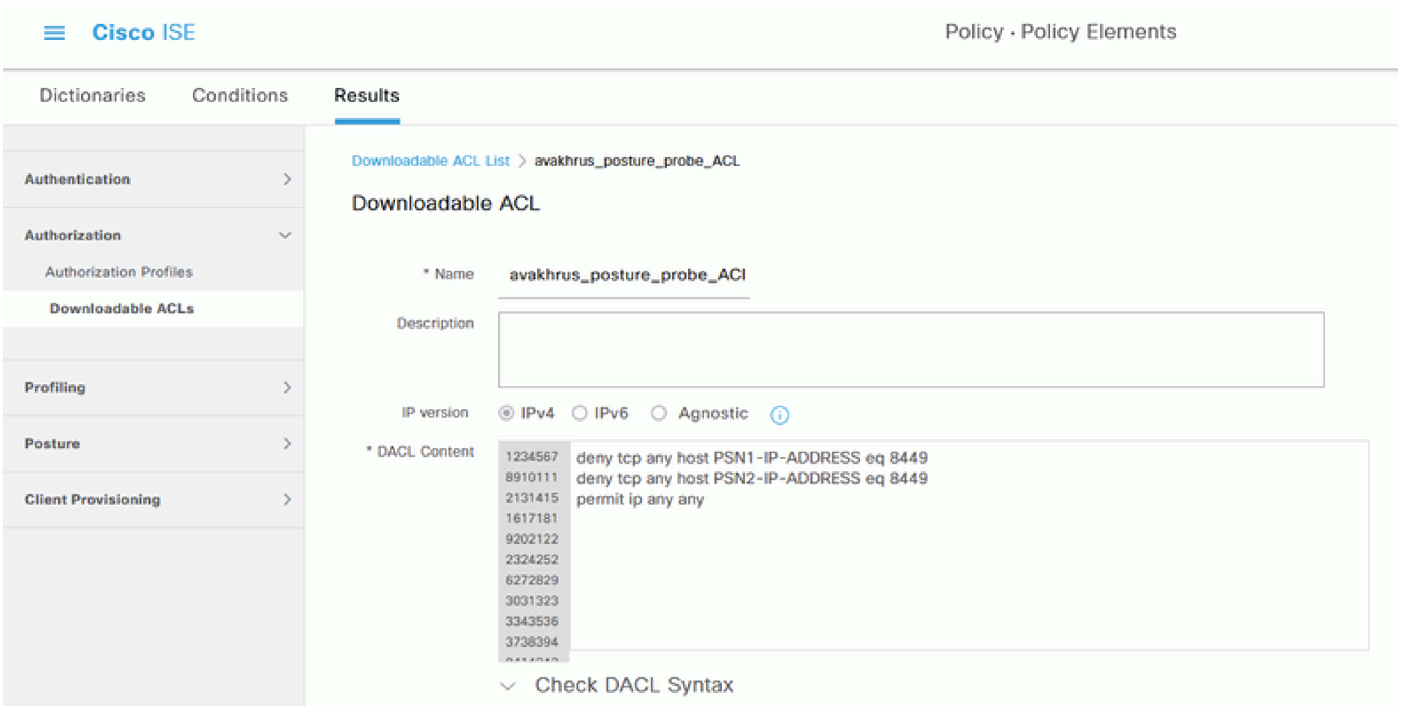
3) La sincronización del estado de postura se detiene debido a la detección de una configuración incorrecta:

```
2022/11/09 12:26:34 [Error] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750 File
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
```

La sincronización del estado de condición no se puede reiniciar desde la GUI de Cisco Secure Client reiniciando la evaluación de estado o un cambio de red. En su lugar, es necesario reiniciar Cisco Secure Client para que la sincronización del estado de postura funcione de nuevo.

Verificar dACL configurada para perfil de autorización de condición "compatible"

1. Valide que se ha configurado la dACL correcta para el perfil de autorización "Conforme" a la condición:



2. Validar el informe de autenticación detallado dACL se envió correctamente como resultado de la autenticación del terminal "Conforme".

CPMSessionID	c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0
CiscoAVPair	aaa:service=ip_admission,aaa:event=acl-download

Result

Class	CACS:c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0:ISE-PSN-FQDN/482174459/480
cisco-av-pair	ip:inacl#1=deny tcp any host PSN1-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#2=deny tcp any host PSN2-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#3=permit ip any any

3. Valide que dACL se aplique correctamente en un dispositivo de acceso a la red:

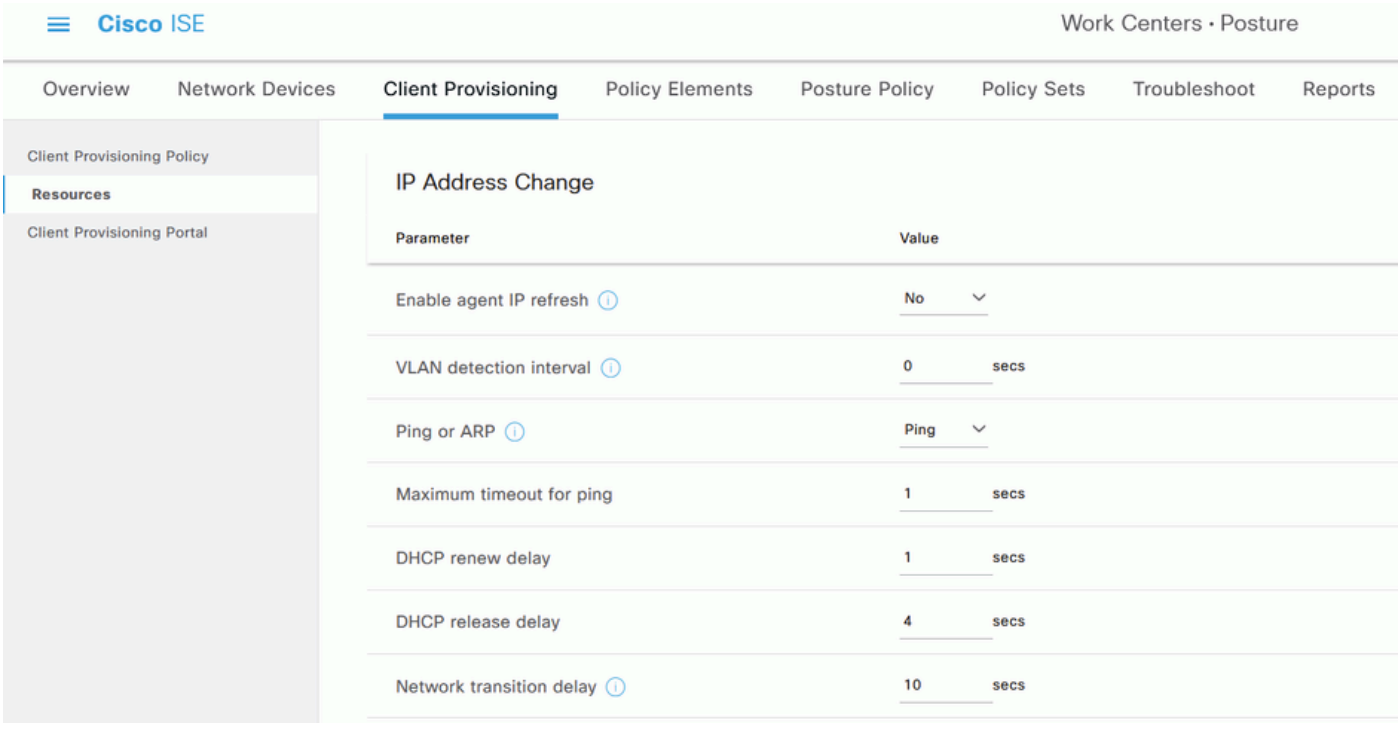
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  172800s (local), Remaining: 92111s
       Session Uptime:  1515s
    Common Session ID:  C0A8FF0C00000012679EAF14
      Acct Session ID:  0x00000012
               Handle:  0x5D000005
       Current Policy:  POLICY_Fa0/12

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
             ACS ACL:  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac

Method status list:
       Method           State

       mab              Stopped
       dot1x            Authc Success

avakhrus_3560C#sh access-lists | s  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac
Extended IP access list xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac (per-user)
```

```
1 deny tcp any host PSN1-IP-ADDRESS eq 8449
2 deny tcp any host PSN2-IP-ADDRESS eq 8449
3 permit ip any any
```

Problemas conocidos

Falla la sincronización del estado de postura con la alarma en ISE

La sincronización del estado de postura puede fallar con una alarma en ISE, incluso si se aplica una dACL adecuada en un dispositivo de acceso a la red al terminal del cliente. Sucede si la sonda de sincronización de estado de postura se realiza más rápido que la aplicación de dACL o si la sonda de sincronización de estado de postura ya está en curso cuando se aplica dACL. El problema se investigó con el Id. de error de Cisco CSCwd58316
. Como solución temporal, debe establecer "Retraso de transición de red" en 10 segundos en el perfil de estado de Anyconnect (Configuración de perfil de agente de estado de ISE).



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).