配置状态同步并对其进行故障排除

目录

简介

本文档介绍在思科身份服务引擎(ISE) 3.1版本中引入的状态状态同步的配置和使用。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE上的安全评估流程
- 在Cisco ISE的状态组件的配置

假设您具有任何类型的状态配置。

为了更好地了解下文介绍的概念，建议完成以下步骤：

- 思科身份服务引擎管理员指南，版本3.1
- 比较早期ISE版本与ISE 2.2中的ISE终端安全评估流程
- ISE会话管理和状态

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.1
- 思科安全客户端5.0.00556

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

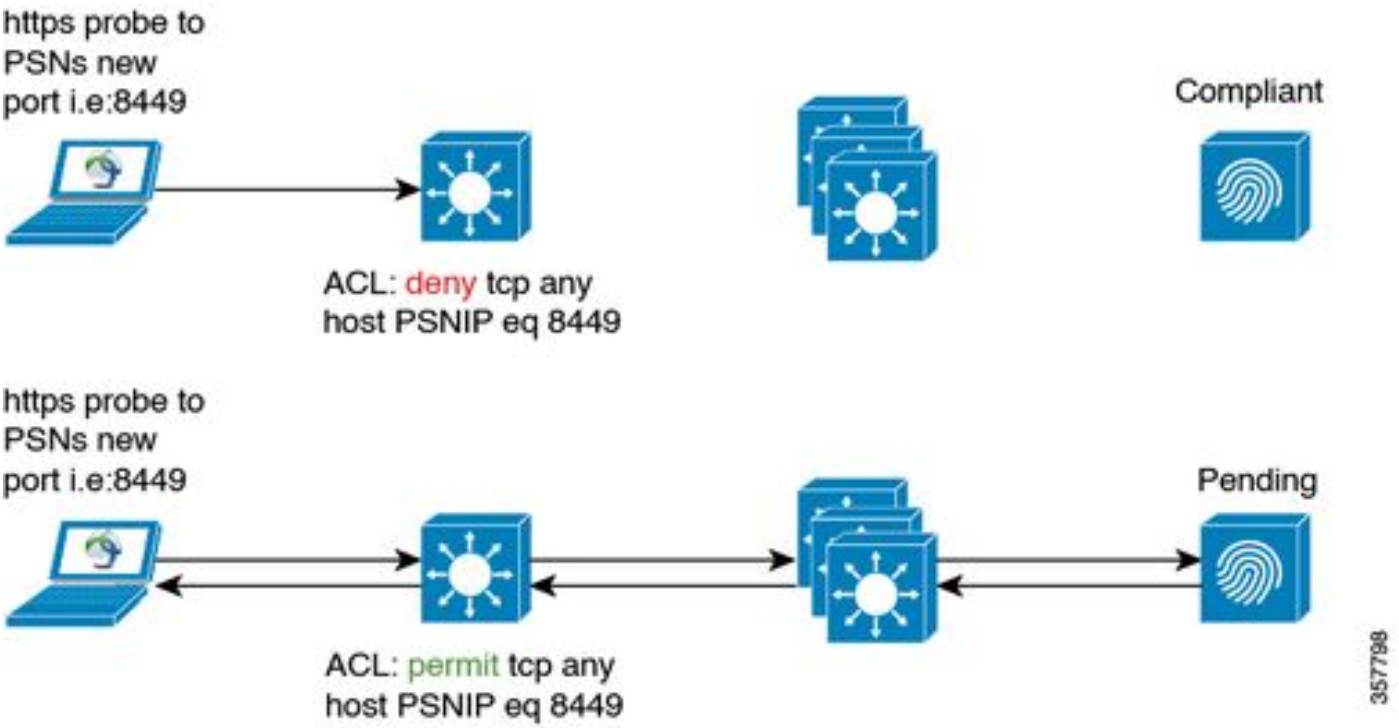
ISE终端安全评估流程通常不允许在客户端上从ISE更新终端安全评估状态。思科安全客户端状态模块用于评估终端的状态并一直保持到网络更改、定期重新评估或其他客户端触发。如果由于会话终止或其他原因，终端安全评估状态在ISE上发生更改，安全客户端安全评估模块可能不知道该更改，因此，终端将处于安全评估未知状态，网络访问受限，直到发生客户端触发事件之一。

本文档重点介绍一项新功能-安全评估状态同步，该功能旨在解决此类问题，并允许ISE向安全客户端安全评估模块提供有关终端当前安全评估状态的反馈。

配置

默认情况下，启用终端安全评估状态同步时，会在每个ISE PSN节点上引入终端安全评估状态探测端口- TCP 8449。如果终端状态为未知或待处理，则从终端应该可以访问，如果终端状态为合规，则无法访问。

网络图



配置

状态同步功能配置包括两部分：

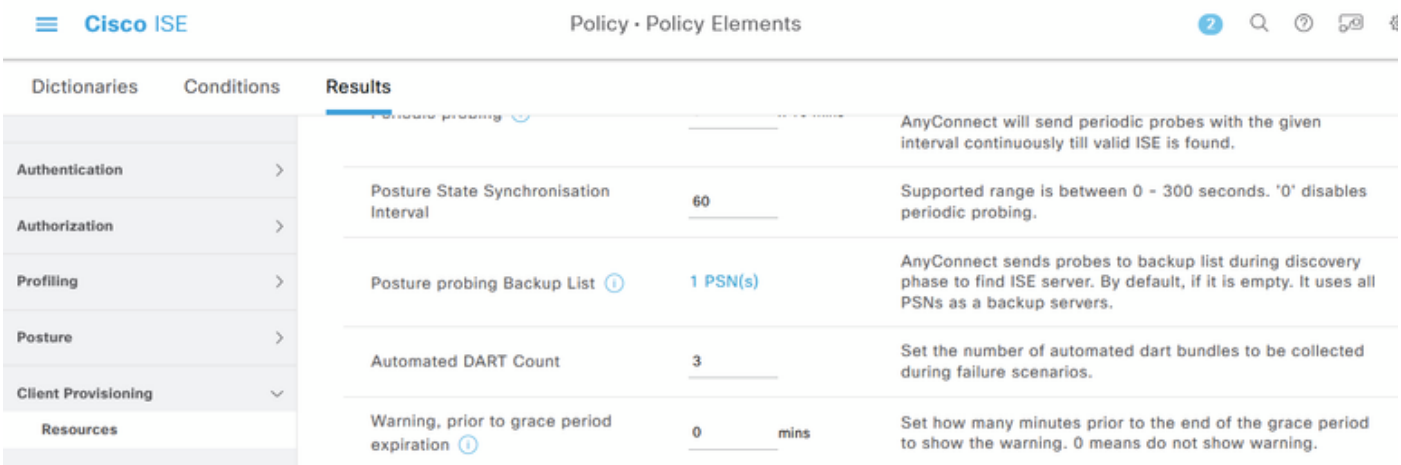
1. AnyConnect终端安全评估配置文件配置

1.1在思科ISE GUI中，导航到策略>策略元素>结果>客户端调配>资源。

1.2选择您已使用的AnyConnect终端安全评估配置文件或创建新配置文件。

1.3在Agent Behavior区域，将Posture State Synchronization Interval配置为1到300秒之间的任意值，0 -禁用状态同步

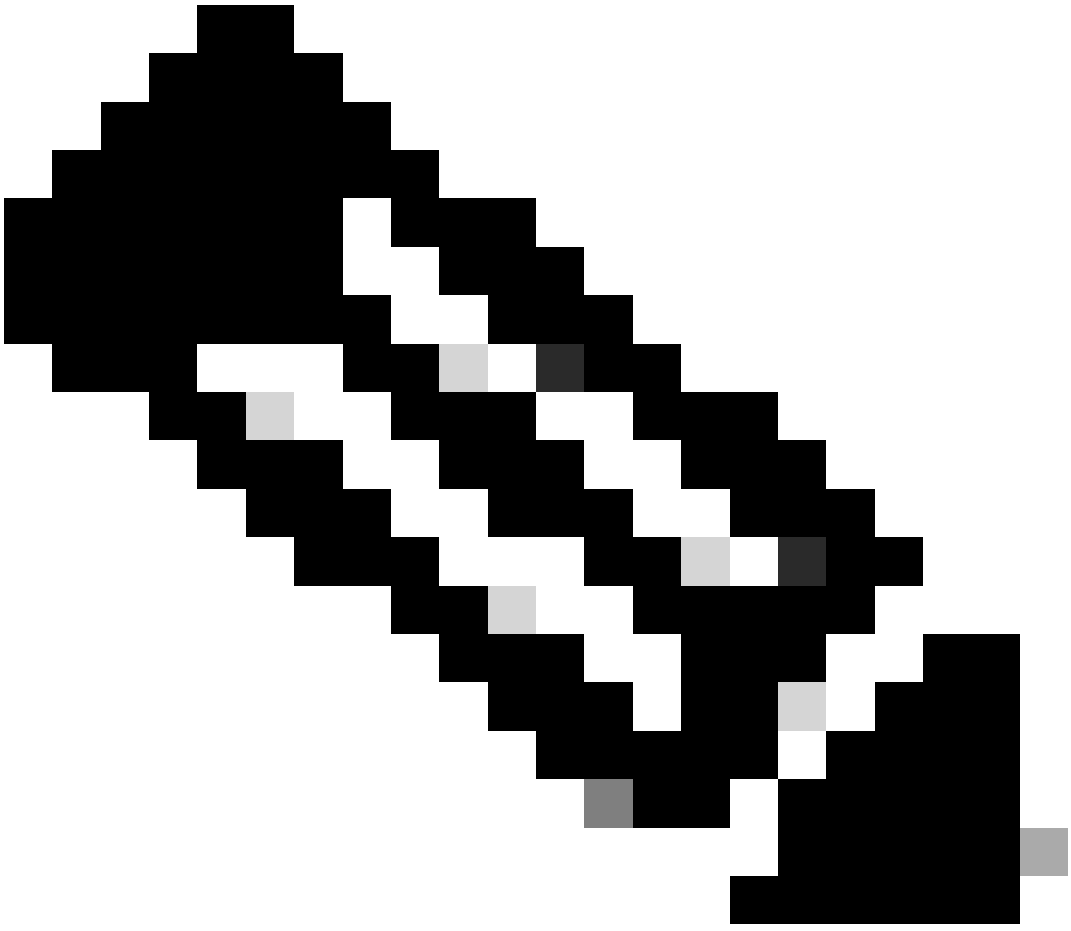
1.4 您可以配置终端安全评估探测备份列表-安全客户端使用此列表检查所选PSN上的终端安全评估状态。如果不选择任何PSN，则连接的PSN和任意两个备份服务器将用作状态同步的备份。



2. 配置可下载ACL(dACL)以阻止访问状态同步端口在Cisco ISE客户端状态合规或不合规。您需要为每个PSN添加访问控制拒绝条目，并在终端状态已知的情况下，为合规终端使用的ACL顶部提供终端状态同步端口，以限制对终端状态同步端口的访问，例如：

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

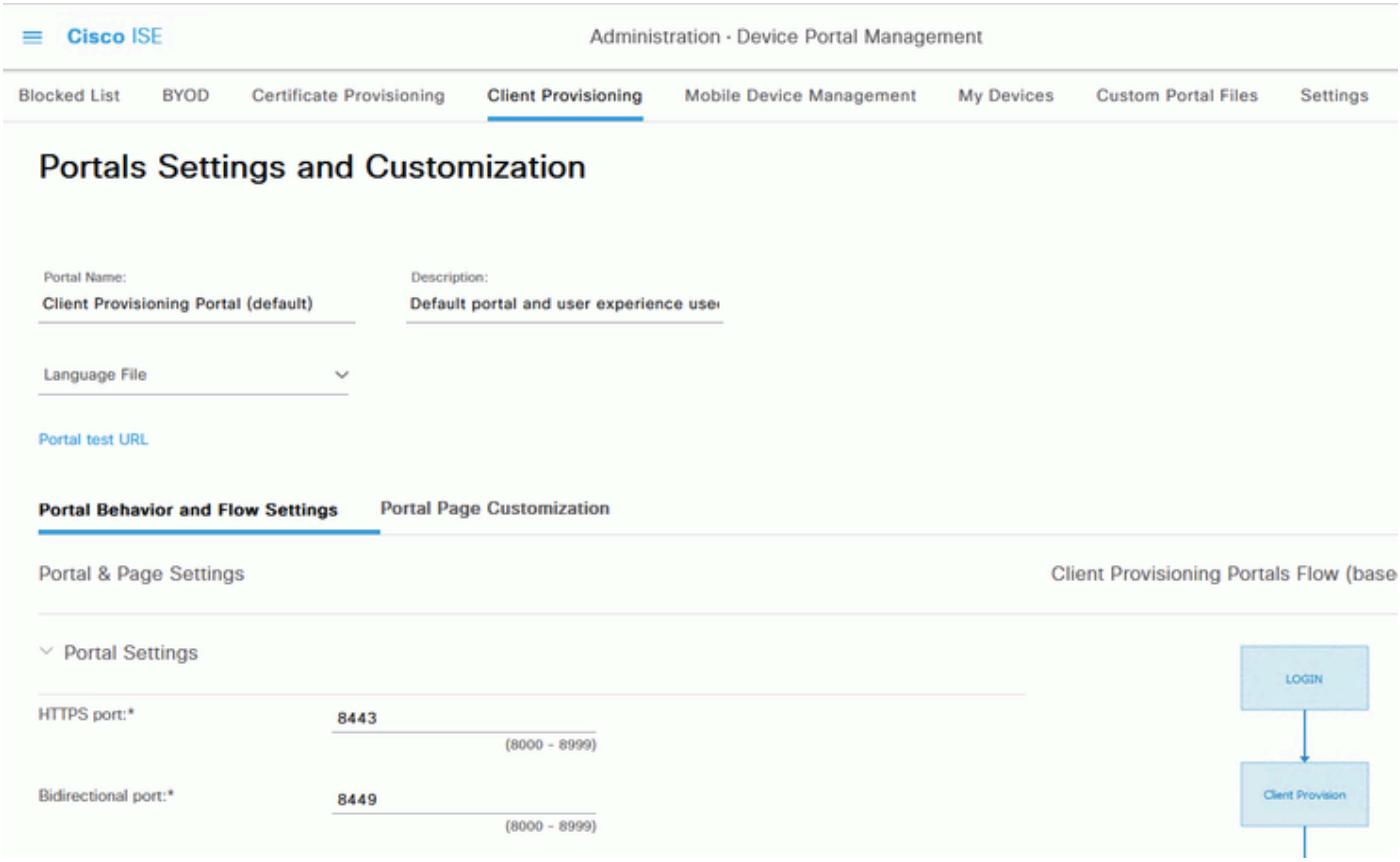
permit ip any any不是强制性的，您可以根据需要将其替换为任何规则集。



注：如果未配置dACL中的deny条目，则在Cisco ISE控制面板上触发状态配置检测警报，并且终端上的状态同步被禁用，直到Cisco安全客户端重新启动。

状态同步端口（双向端口）可以在Client Provisioning Portal配置页面更改。导航到管理>设备门户管理>客户端调配>选择所需的门户>门户行为和流量设置，然后打开门户设置。无法更改默认客户

端调配门户的状态状态同步端口。



验证

来自DART捆绑包

通过查看DART捆绑包中的思科安全客户端状态模块日志(AnyConnect_ISEPosture.txt)，可以从客户端验证状态同步：

1. 状态评估完成，状态为合规。

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

2. 状态状态同步探测启动。

```
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. 在终端安全评估状态同步端口(8449)上启动到ISE PSN的HTTPS连接。

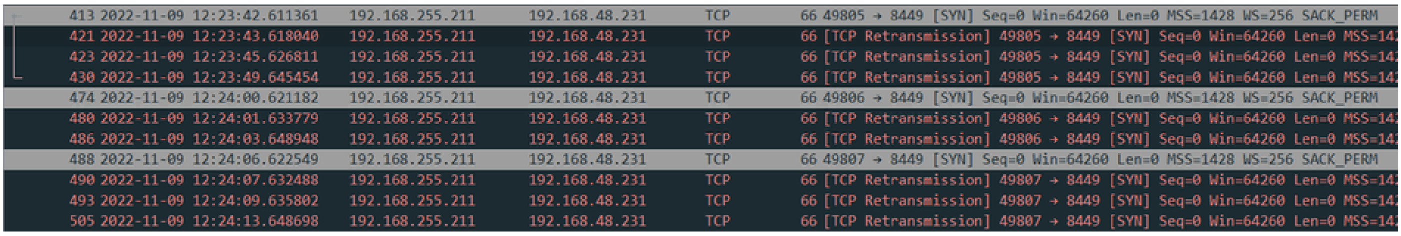
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. 状况状态同步探测超时。

```
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
```

从客户端的数据包捕获

在客户端上捕获的数据包显示在没有来自ISE PSN的SYN-ACK响应的情况下，在终端安全评估状态同步端口(8449)上向ISE PSN节点发送的SYN数据包：



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

从ISE

无法从ISE端验证正确的安全评估状态同步配置，因为安全评估状态同步端口(8449)上的连接应该失败。

状态更改时状态重启

1)当思科安全客户端处于“兼容”状态时，已从ISE接收状态状态为“未知”的会话状态信息。

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

2)思科安全客户端确认状态更改并重新启动状态发现：

```
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安全客户端停止状态同步，直到执行状态评估：

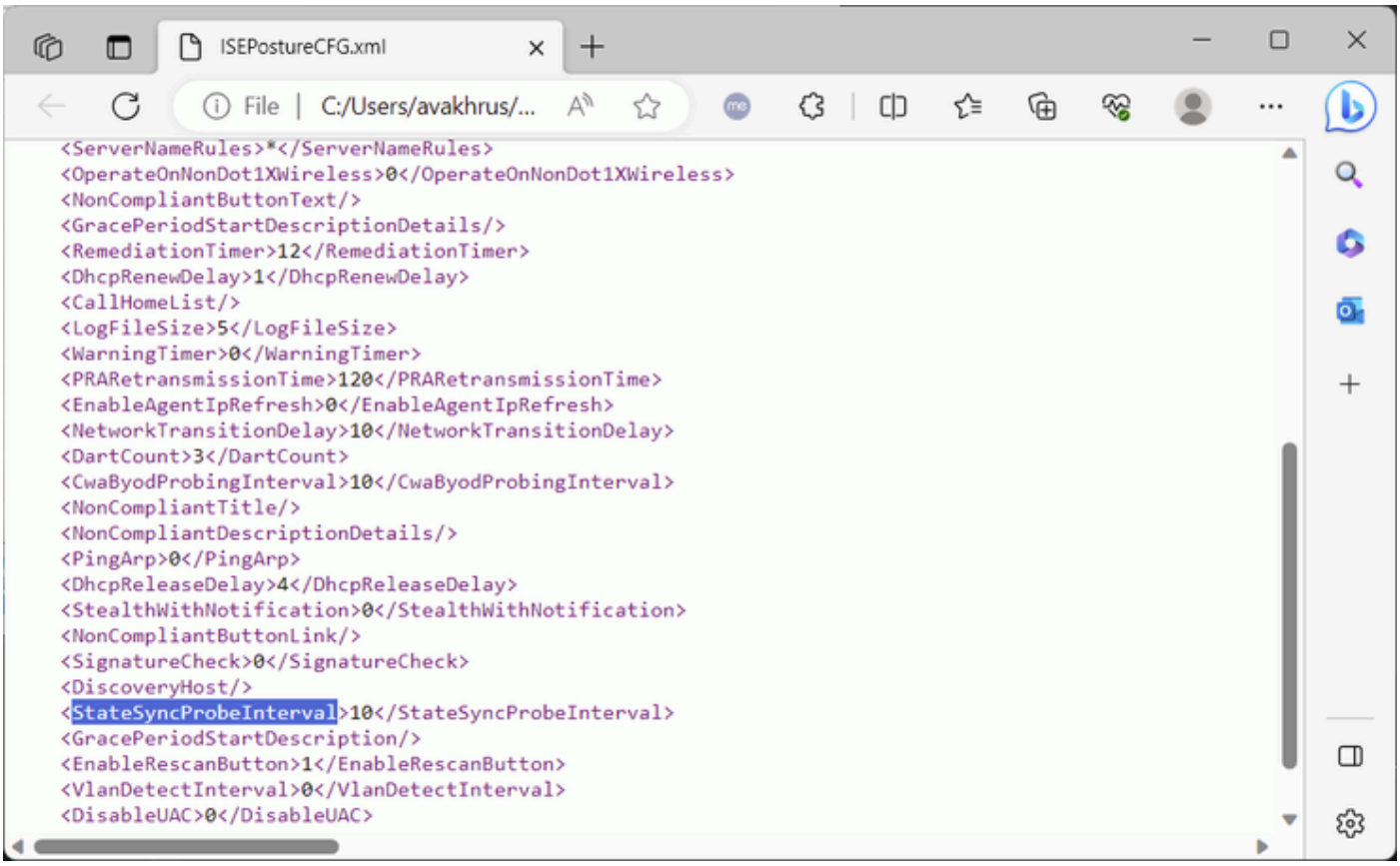
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery 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
```

故障排除

状况状态同步无法启动

如果AnyConnect_ISEPosture.txt日志文件中没有指示安全评估状态同步启动，并且客户端未尝试在安全评估状态同步端口(8449)上与ISE PSN节点建立连接，请从DART包或直接在客户端计算机上检查安全评估配置文件ISEPostureCFG.xml：“%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\”（对于Windows PC）。

负责状态同步的参数是“StateSyncProbeInterval”，应为其设置大于0的值：



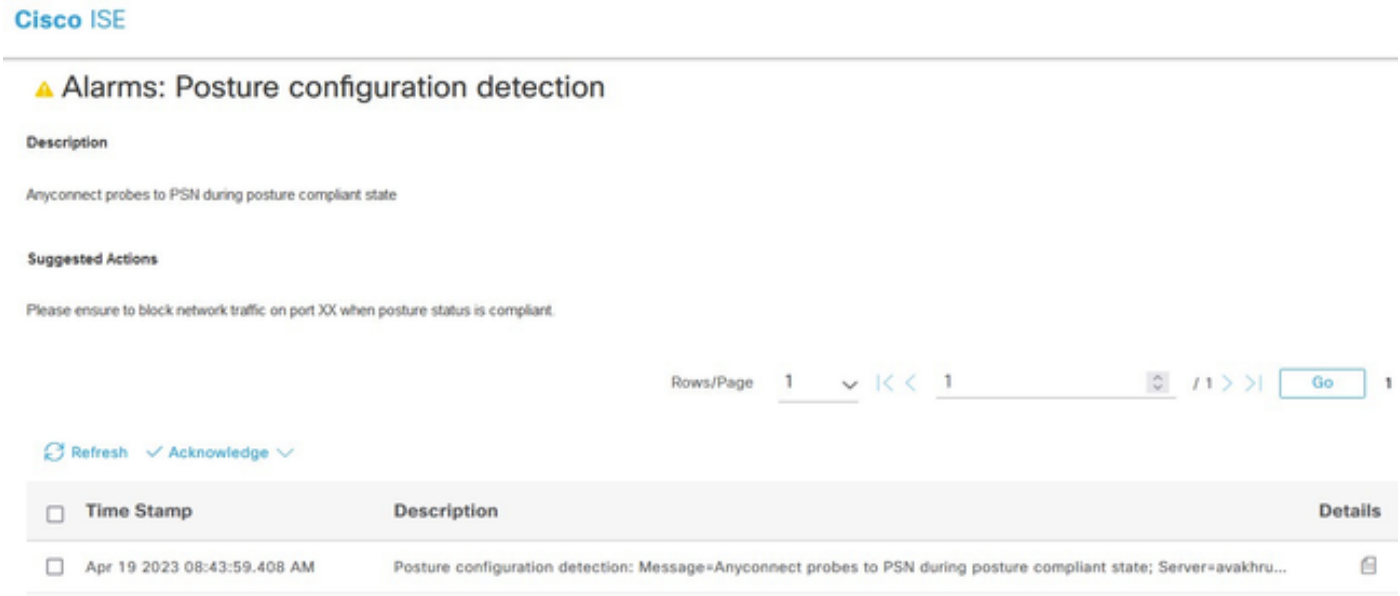
缺少“StateSyncProbeInterval”或值“0”表示状态同步已禁用。

如果在ISE的终端安全评估配置文件中设置了“终端安全评估状态同步间隔”，但该设置并未反映在客户端的配置文件中，则需要调查终端安全评估调配。

安全评估状态同步失败并在ISE控制面板上发出警报

如果ISE上的安全评估状态同步失败并发出警报，则意味着思科安全客户端能够在安全评估状态同步端口(8449)上到达ISE，并请求会话的状态为“兼容”(Compliant)。

- ISE GUI中的警报：



- 从数据包捕获进行验证

在状态状态同步端口(8449)上建立TCP连接：

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 reassembl
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

- 从思科安全客户端状态模块日志验证

从DART捆绑包检查AnyConnect_ISEPosture.txt：

1)在终端安全评估状态同步端口(8449)上发起到ISE PSN的HTTPS连接。

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

2)已收到来自ISE的会话状态信息，安全评估状态为“兼容”。

```
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
```

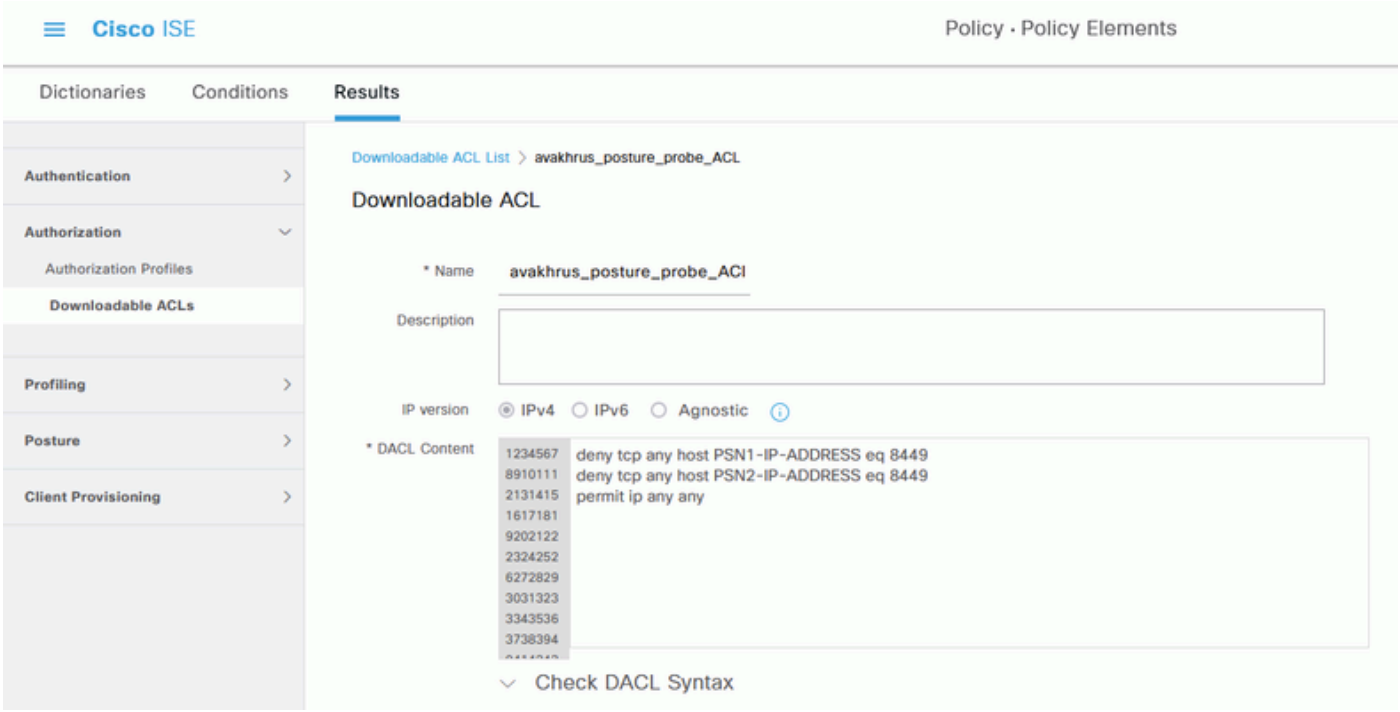
3)由于检测到不正确的配置，终端安全评估状态同步停止：

```
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
```

无法通过重新启动状态评估或网络更改从思科安全客户端GUI重新启动状态同步。相反，需要重新启动Cisco安全客户端才能使状态状态同步重新工作。

验证为状态“兼容”授权配置文件配置的dACL

1. 验证为状态“兼容”授权配置文件配置了正确的dACL：



2. 验证详细身份验证报告dACL作为“兼容”端点的身份验证结果是否正确发送。

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

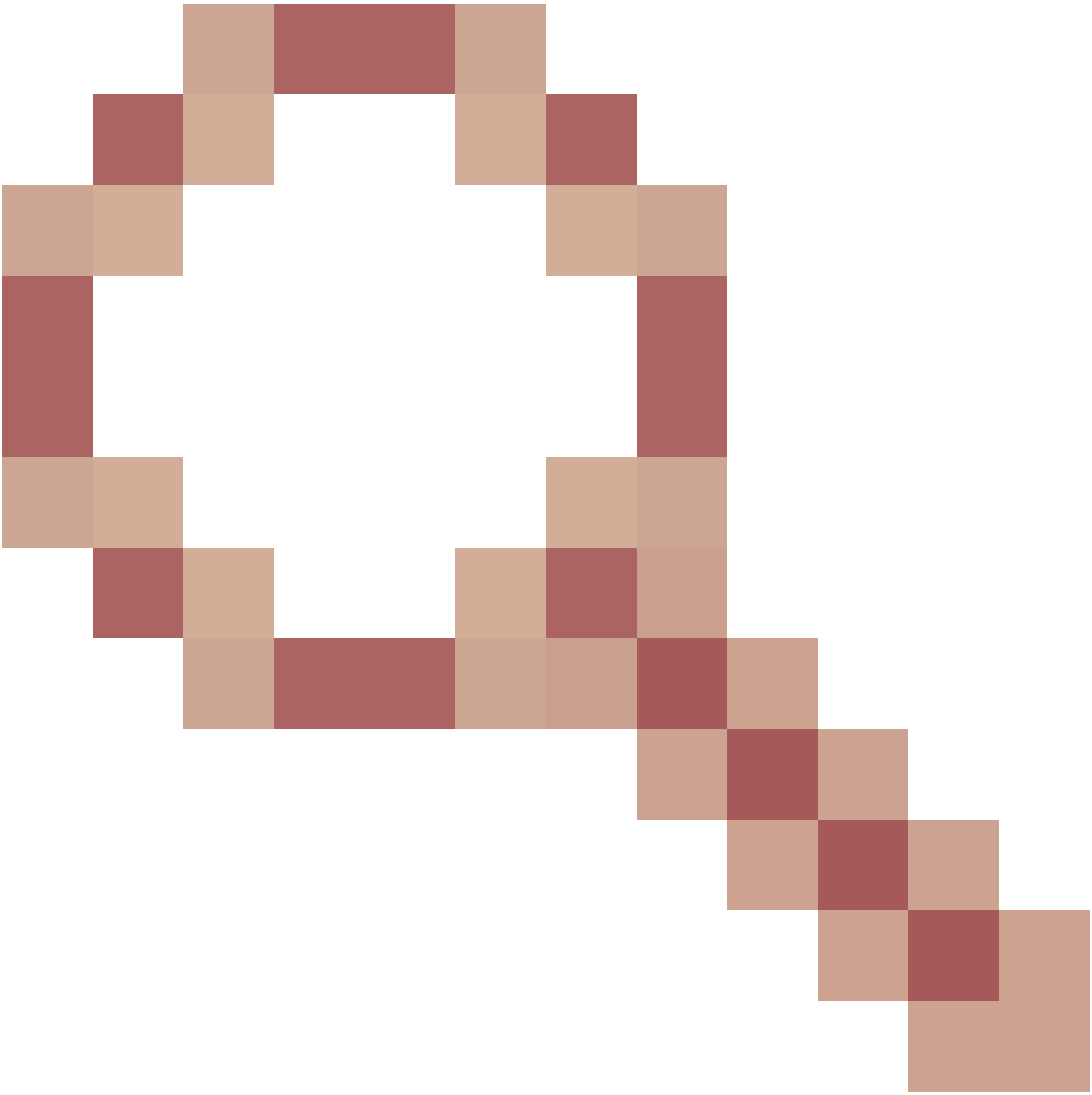
3. 验证dACL是否正确应用于网络接入设备：

```
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
```

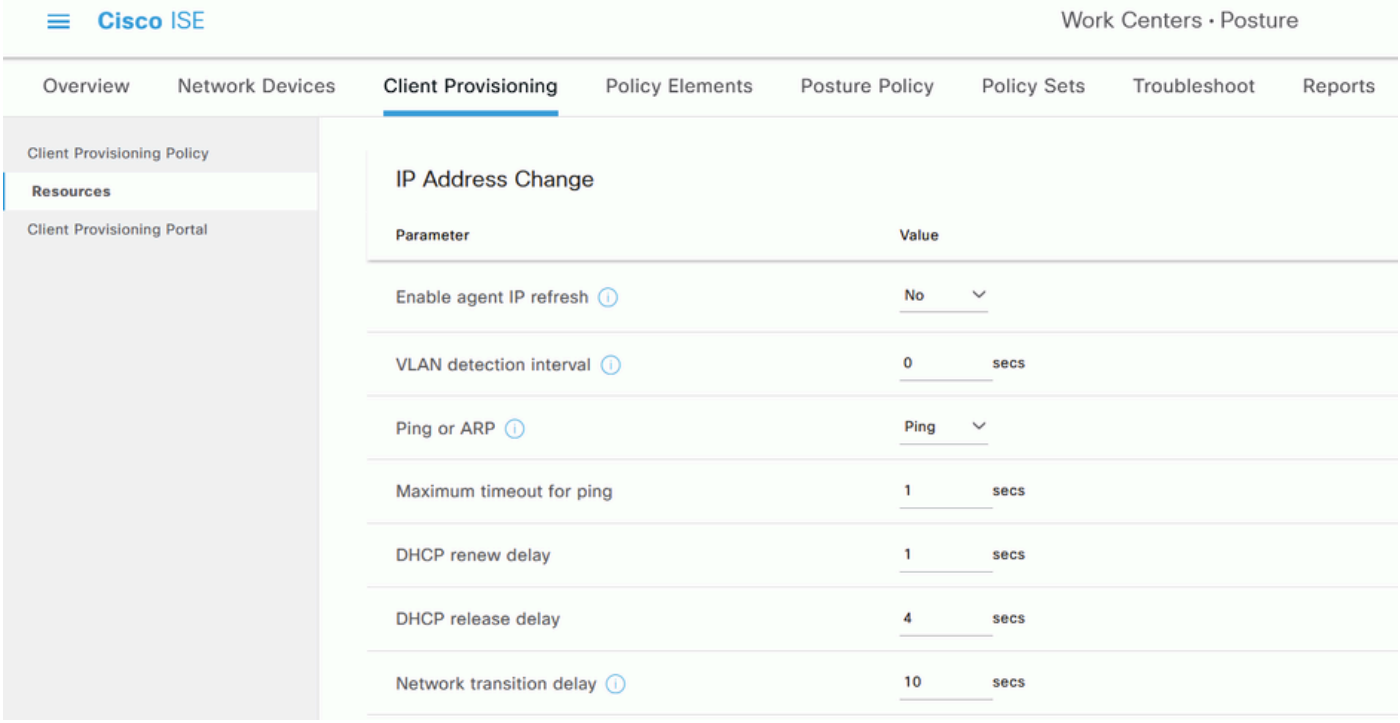
已知问题

安全评估状态同步失败，并在ISE上发出警报

即使在网络接入设备上对客户端终端应用了正确的dACL，ISE上的终端安全评估状态同步也会因警报而失败。如果终端安全评估状态同步探测的执行速度快于应用dACL的速度，或者如果应用dACL时终端安全评估状态同步探测已在进行中，则会发生此情况。思科漏洞ID CSCwd58316中调查了此问题



.作为解决方法，您需要在Anyconnect终端安全评估配置文件（ISE终端安全评估代理配置文件设置）中将“网络过渡延迟”设置为10秒。


Cisco ISE
Work Centers · Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Client Provisioning Policy
Resources
Client Provisioning Portal
IP Address Change
Parameter
Value
Enable agent IP refresh
No
VLAN detection interval
0
secs
Ping or ARP
Ping
Maximum timeout for ping
1
secs
DHCP renew delay
1
secs
DHCP release delay
4
secs
Network transition delay
10
secs

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。