

ASA 版本 9.2.1 基于 ISE 的 VPN 安全评估配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图和流量流程](#)

[配置](#)

[ASA](#)

[ISE](#)

[定期重新评估](#)

[验证](#)

[故障排除](#)

[ISE上的调试](#)

[ASA上的调试](#)

[代理的调试](#)

[NAC代理状态故障](#)

[相关信息](#)

简介

本文档介绍如何配置思科自适应安全设备(ASA)版本9.2.1，以便针对思科身份服务引擎(ISE)对VPN用户进行安全评估，而无需内联状态节点(IPN)。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA CLI配置和安全套接字层(SSL)VPN配置的基本知识
- ASA上远程访问VPN配置的基本知识
- ISE和状态服务基础知识

使用的组件

本文档中的信息基于以下软件版本：

- Cisco ASA软件9.2.1版及更高版本
- 带Cisco AnyConnect安全移动客户端版本3.1的Microsoft Windows版本7
- 带补丁5或更高版本的思科ISE版本1.2

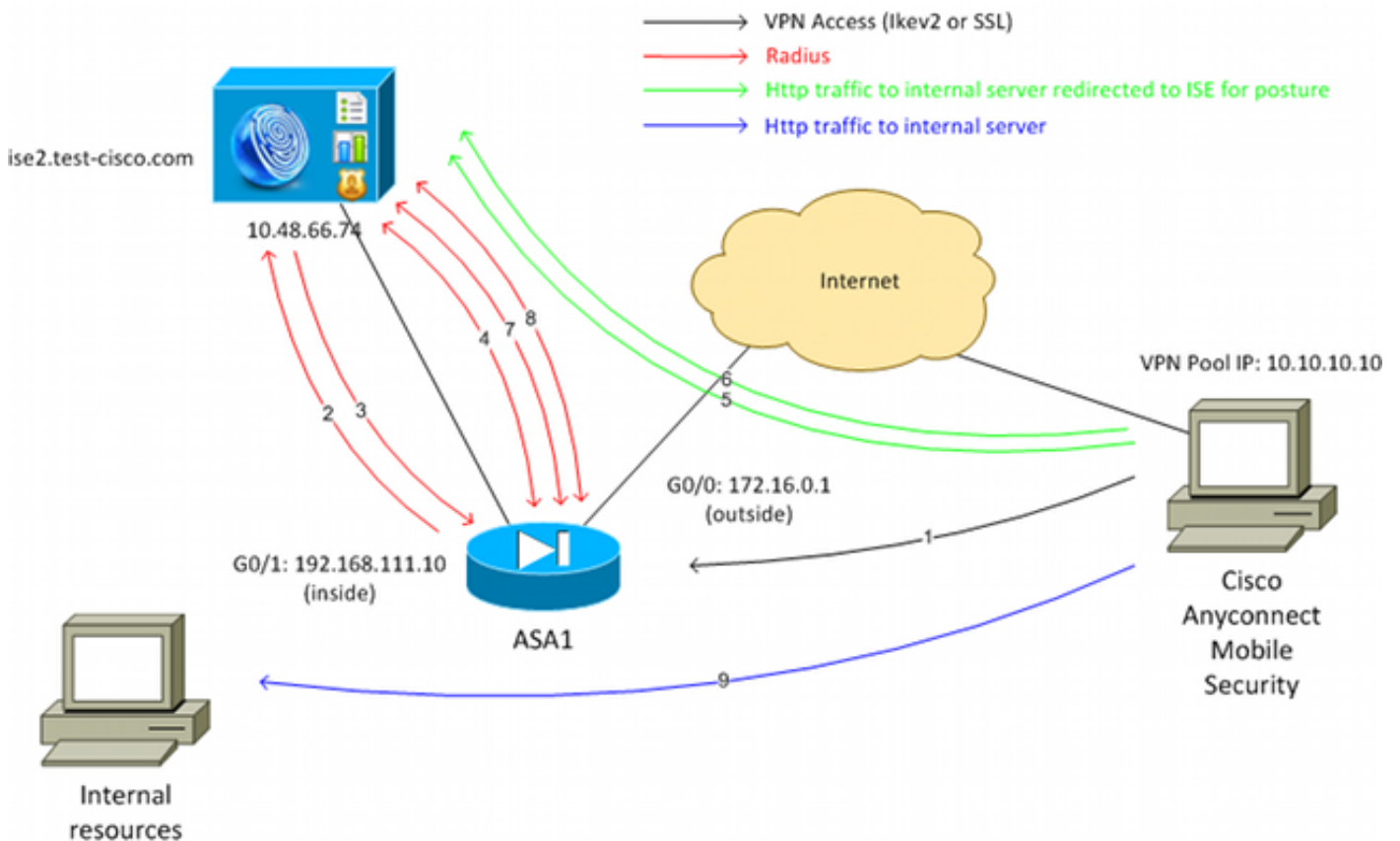
背景信息

Cisco ASA版本9.2.1支持RADIUS授权更改(CoA)(RFC 5176)。这允许对Cisco ISE进行VPN用户状态分析，无需IPN。在VPN用户登录后，ASA会将网络流量重定向到ISE，用户在此调配网络准入控制(NAC)代理或Web代理。代理对用户机器执行特定检查，以确定其是否符合一组已配置的状况规则，如操作系统(OS)、补丁、防病毒、服务、应用或注册表规则。

然后，将状态验证结果发送到ISE。如果认为计算机有投诉，则ISE可以使用新的授权策略集向ASA发送RADIUS CoA。在成功的安全状态验证和CoA后，允许用户访问内部资源。

配置

网络图和流量流程



如网络图所示，以下是流量传输：

1. 远程用户使用Cisco Anyconnect进行VPN访问ASA。
2. ASA向ISE发送该用户的RADIUS访问请求。
3. 该请求到达ISE上名为ASA92-posture的策略。因此，将返回ASA92-posture授权配置文件。ISE发送包含两个Cisco属性值对的RADIUS Access-Accept:

url-redirect-acl=redirect — 这是在ASA上本地定义的访问控制列表(ACL)名称，决定应重定向的流量。

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp — 这是远程用户应重定向到的URL。**提示**：分配给VPN客户端的域名系统(DNS)服务器必须能够解析重定向URL中返回的完全限定域名(FQDN)。如果配置VPN过滤器以限制隧道组级别的访问，请确保客户端池能够在配置的端口上访问ISE服务器(本示例中为TCP 8443)。

4. ASA发送RADIUS Accounting-Request start数据包并接收响应。要向ISE发送有关会话的所有详细信息，需要执行此操作。这些详细信息包括session_id、VPN客户端的外部IP地址和ASA的IP地址。ISE使用session_id标识该会话。ASA还会定期发送临时帐户信息，其中最重要的属性是具有ASA分配给客户端的IP的Framed-IP-Address(本示例中为10.10.10.10)。
5. 当来自VPN用户的流量与本地定义的ACL (重定向) 匹配时，会将其重定向到https://ise2.test-cisco.com:8443。根据配置，ISE会调配NAC代理或Web代理。
6. 在客户端计算机上安装代理后，代理会自动执行特定检查。在本示例中，它会搜索c:\test.txt文件。它还向ISE发送状态报告，其中可能包含使用瑞士协议和端口TCP/UDP 8905的多个交换以访问ISE。
7. 当ISE从代理收到状况报告时，它会再次处理授权规则。这次，状态结果为已知，另一个规则已命中。它会发送RADIUS CoA数据包：

如果用户兼容，则发送允许完全访问的可下载ACL(DACL)名称 (AuthZ规则ASA92-compliant) 。

如果用户不兼容，则会发送允许有限访问的DACL名称 (授权规则ASA92-non-compliant) 。
注：始终确认RADIUS CoA；即，ASA向ISE发送响应以进行确认。

8. ASA删除重定向。如果它没有缓存的DACL，则必须发送访问请求以便从ISE下载它们。特定的DACL连接到VPN会话。
9. VPN用户下次尝试访问网页时，可以访问ASA上安装的DACL允许的所有资源。
如果用户不合规，则仅授予有限的访问权限。
注意：此流量模式与大多数使用RADIUS CoA的场景不同。对于有线/无线802.1x身份验证，RADIUS CoA不包含任何属性。它只触发附加所有属性 (例如DACL) 的第二个身份验证。对于ASA VPN状态，没有第二次身份验证。所有属性都在RADIUS CoA中返回。VPN会话处于活动状态，无法更改大多数VPN用户设置。

配置

使用此部分配置ASA和ISE。

ASA

以下是Cisco AnyConnect访问的基本ASA配置：

```
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address xxxx 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
 key cisco

webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
```

对于ASA与ISE终端安全评估集成，请确保您：

- 为动态授权配置身份验证、授权和记帐(AAA)服务器以接受CoA。
- 将记帐配置为隧道组，以便向ISE发送VPN会话详细信息。
- 配置临时记帐，它将发送分配给用户的IP地址并定期更新ISE上的会话状态
- 配置重定向ACL，确定是否允许DNS和ISE流量。所有其他HTTP流量重定向到ISE进行安全评估。

以下是配置示例：

```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

aaa-server ISE protocol radius
```

authorize-only

interim-accounting-update periodic 1

dynamic-authorization

aaa-server ISE (inside) host 10.48.66.74

key cisco

tunnel-group RA general-attributes

address-pool POOL

authentication-server-group ISE

accounting-server-group ISE

default-group-policy GP-SSL

ISE

完成以下步骤以配置ISE:

1. 导航到Administration > Network Resources > Network Devices并将ASA添加为网络设备：

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded, showing 'Network Resources' as the active section. Under 'Network Resources', 'Network Devices' is selected. The main content area is titled 'Network Devices List > New Network Device'. The left sidebar shows a tree view with 'Network Devices' and 'Default Device'. The main form contains the following fields and options:

- Name:** ASA
- Description:** (empty)
- IP Address:** 192.168.111.10 / 32
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- Network Device Group:** (dropdown menu)
- Location:** All Locations (dropdown menu) with a 'Set To Default' button.
- Device Type:** All Device Types (dropdown menu) with a 'Set To Default' button.
- Authentication Settings:** (checked checkbox)
- Enable Authentication Settings:** (checked)
- Protocol:** RADIUS
- Shared Secret:** (masked password field) with a 'Show' button.

2. 导航到Policy > Results > Authorization > Downloadable ACL并配置DAACL，使其允许完全访问。默认ACL配置允许ISE上的所有IP流量：

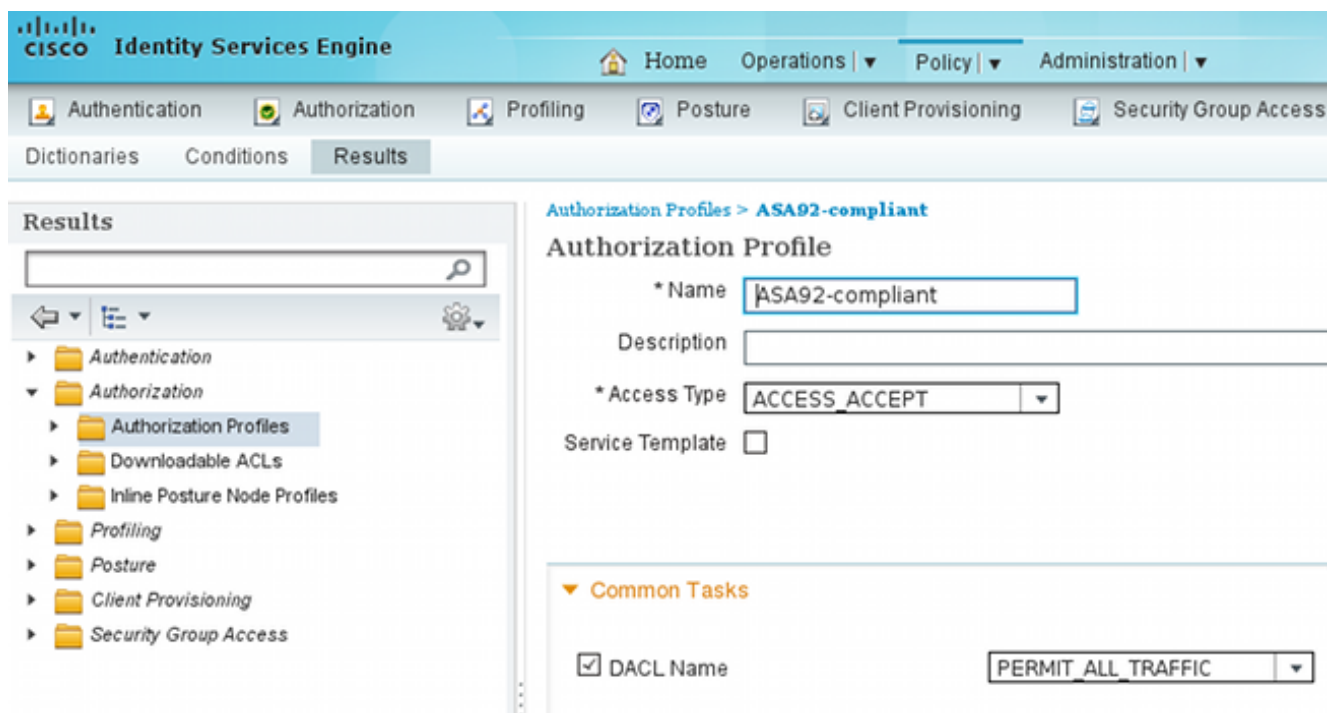
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below the navigation bar are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active, and the left sidebar shows a tree view with 'Downloadable ACLs' selected. The main content area displays the configuration for a 'Downloadable ACL' named 'PERMIT_ALL_TRAFFIC'. The description is 'Allow all Traffic'. The DACL content is shown as a list of lines, with the first line being '1 permit ip any any'. A 'Check DACL Syntax' button is visible at the bottom.

3. 配置一个类似的ACL，使其提供有限的访问权限（适用于不合规的用户）。

4. 导航到 **Policy > Results > Authorization > Authorization Profiles**，并配置名为 **ASA92-posture** 的授权配置文件，该配置文件重定向用户以进行安全评估。选中 **Web Redirection** 复选框，从下拉列表中选择 **Client Provisioning**，并确保 **redirect** 显示在 ACL 字段中（该 ACL 在 ASA 上本地定义）：

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below the navigation bar are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active, and the left sidebar shows a tree view with 'Authorization Profiles' selected. The main content area displays the configuration for an 'Authorization Profile' named 'ASA92-posture'. The description is empty. The access type is set to 'ACCESS_ACCEPT'. The 'Service Template' checkbox is unchecked. Under the 'Common Tasks' section, the 'Web Redirection (CWA, DRW, MDM, NSP, CPP)' checkbox is checked. The 'Client Provisioning (Posture)' dropdown is set to 'Client Provisioning (Posture)', and the 'ACL' field is set to 'redirect'. The 'Static IP/Host name' checkbox is unchecked.

5. 配置名为**ASA92-compliant**的授权配置文件，该配置文件应仅返回名为**PERMIT_ALL_TRAFFIC**的DACL，为合规用户提供完全访问权限：



6. 配置名为**ASA92-non-compliant**的类似授权配置文件，该配置文件应返回具有有限访问权限的DACL（适用于不合规用户）。

7. 导航到**Policy > Authorization**并配置授权规则：

创建在状况结果符合时允许完全访问的规则。结果是授权策略**符合ASA92**。

创建在状况结果不符合时允许有限访问的规则。其结果是授权策略**ASA92不兼容**。

确保前两个规则均未命中，则默认规则返回**ASA92-posture**，这会强制在ASA上重定向。

✓	ASA92 compliant	if Session:PostureStatus EQUALS Compliant	then ASA92-compliant
✓	ASA92 non compliant	if Session:PostureStatus EQUALS NonCompliant	then ASA92-noncompliant
✓	ASA92 redirect	if Radius:NAS-IP-Address EQUALS 192.168.111.10	then ASA92-posture

8. 默认身份验证规则检查内部身份库中的用户名。如果必须进行更改(例如，在Active Directory(AD)中选中)，请导航到**Policy > Authentication**并进行更改：

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Users	
<input checked="" type="checkbox"/>	Default Rule (if no match)	: Allow Protocols : Default Network Access and use : Internal Users	

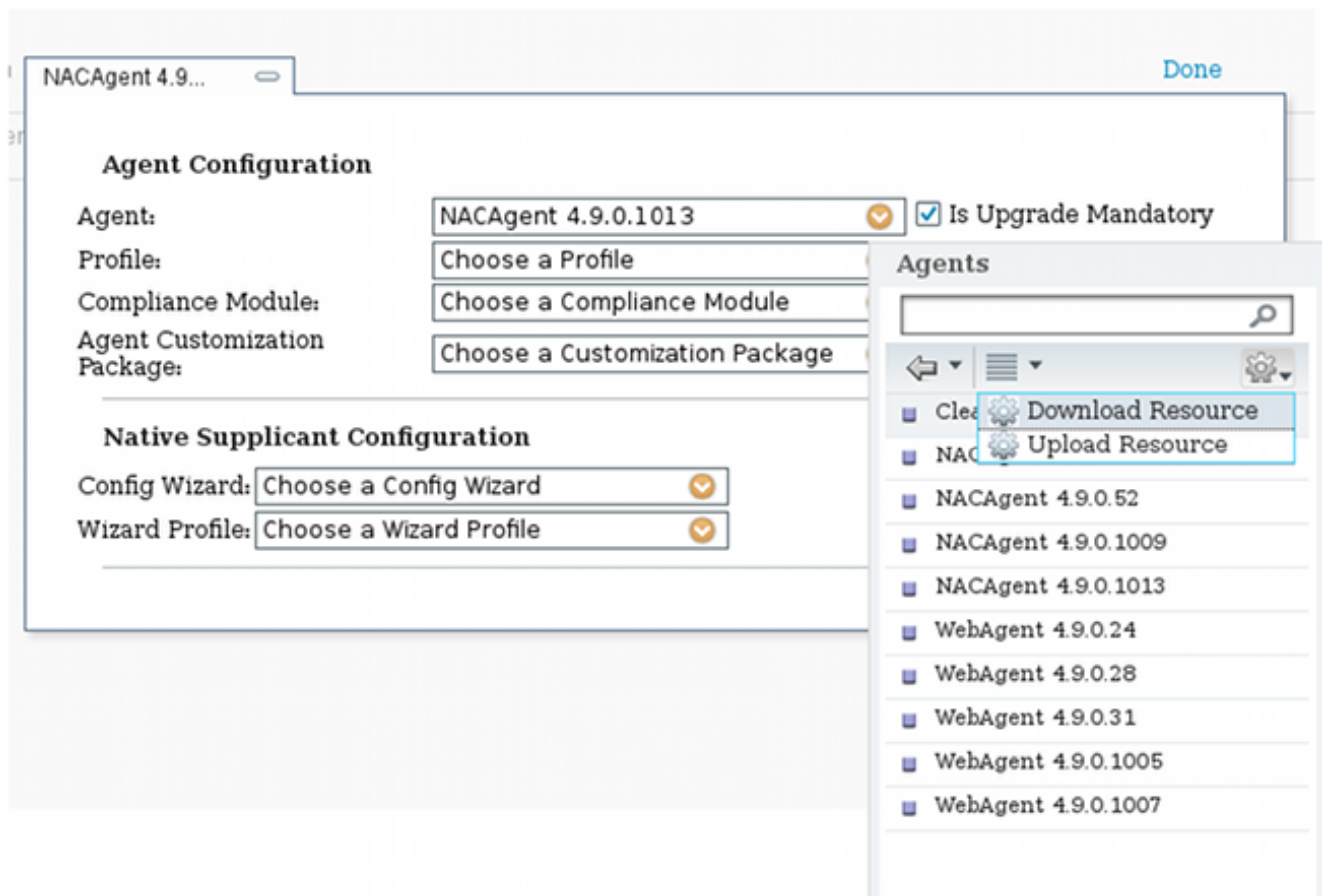
9. 导航到 **Policy > Client Provisioning** 并配置调配规则。这些规则决定应调配的代理类型。在本示例中，仅存在一个简单规则，并且ISE为所有Microsoft Windows系统选择NAC代理：

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	Results
<input checked="" type="checkbox"/> ASA92-posture	if Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1013

当代理不在ISE上时，可以下载它们：



10. 如有必要，您可以导航到**Administration > System > Settings > Proxy**并为ISE配置代理（以访问Internet）。

11. 配置状态规则，用于验证客户端配置。可以配置检查以下内容的规则：

文件 — 存在、版本、日期

注册表 — 键、值、存在

应用 — 进程名称，正在运行，未运行

service — 服务名称，正在运行，未运行

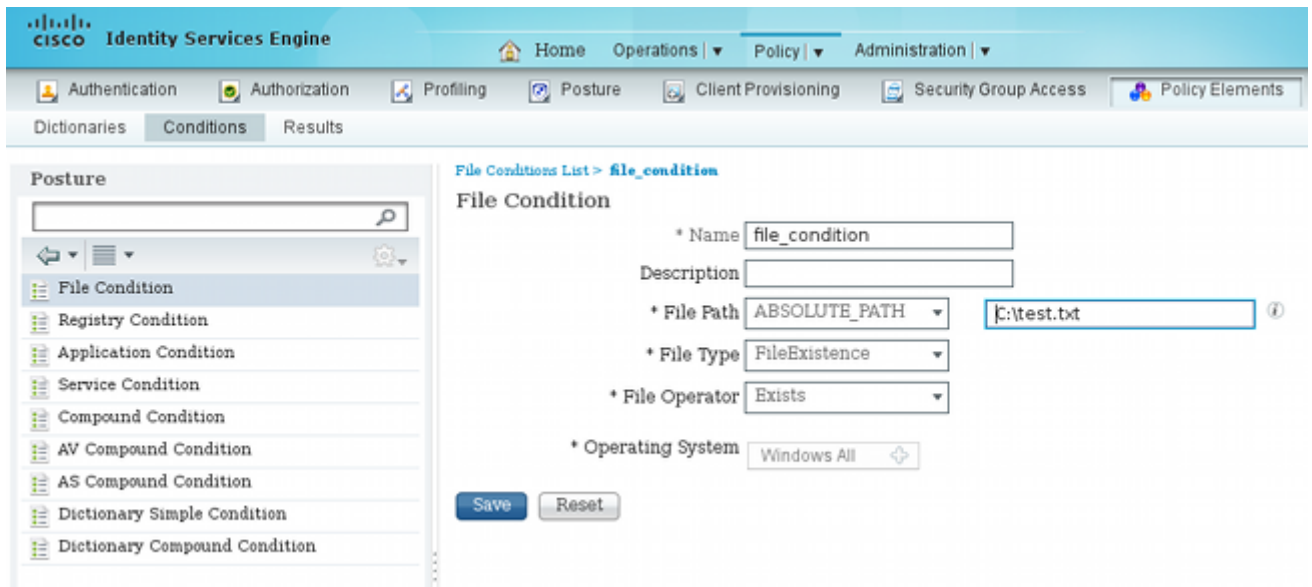
防病毒 — 更新定义时，版本支持100多家供应商

反间谍软件 — 在更新定义时，版本支持100多家供应商

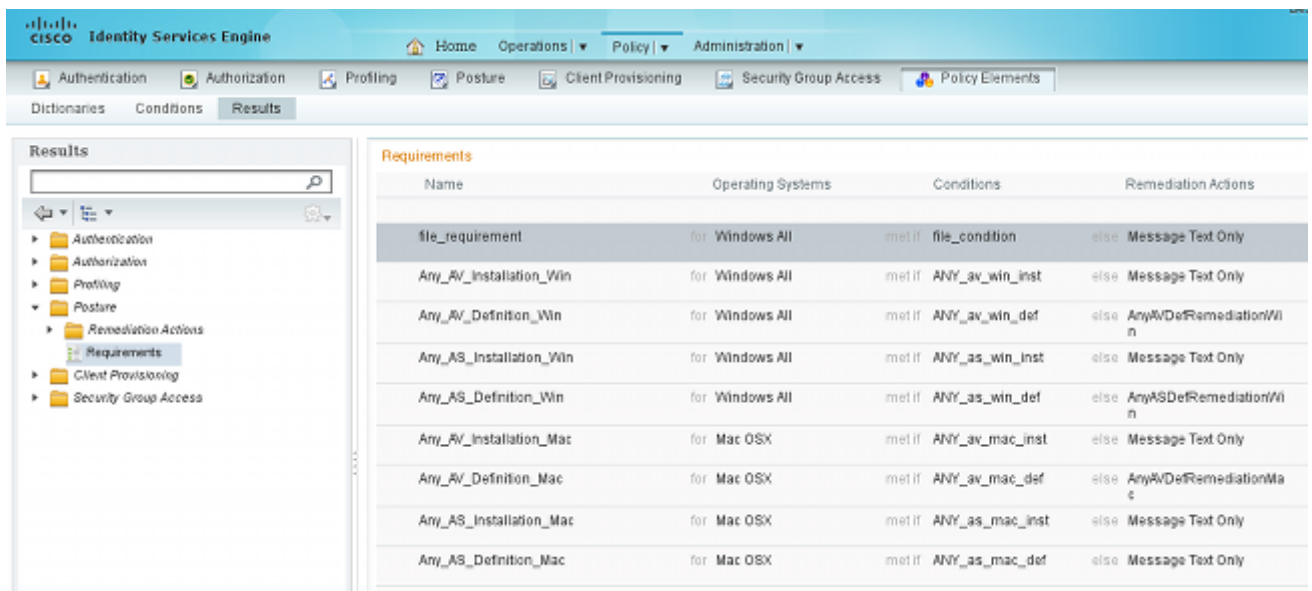
复合条件 — 混合所有

自定义词典条件 — 大部分ISE词典的使用

12. 在本示例中，只执行简单的文件存在性检查。如果客户端计算机上存在c:\test.txt文件，则该文件符合要求并允许完全访问。导航到**Policy > Conditions > File Conditions**并配置文件条件：

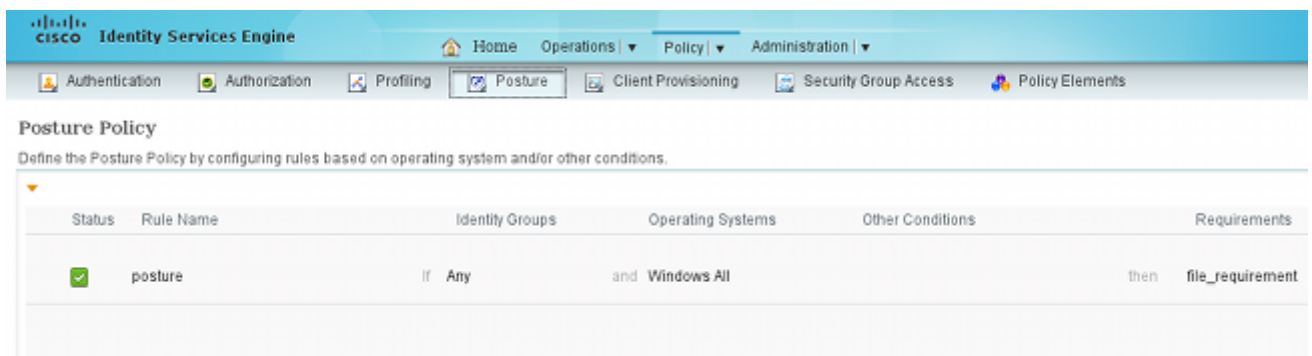


13. 导航到 **Policy > Results > Posture > Requirements** 并创建要求。当满足前一条件时，应满足此要求。如果不是，则执行补救操作。可能有许多类型的补救操作可用，但在本示例中，使用最简单的补救操作：显示特定消息。



注意：在正常情况下，可以使用File Remediation操作（ISE提供可下载的文件）。

14. 导航到 **Policy > Posture**，并使用您在上一步骤中创建的要求(命名为file_requirement)在安全评估规则。唯一的安全评估规则要求所有Microsoft Windows系统都满足file_requirement。如果满足此要求，则表示工作站合规；如果不满足，则表示工作站不合规。

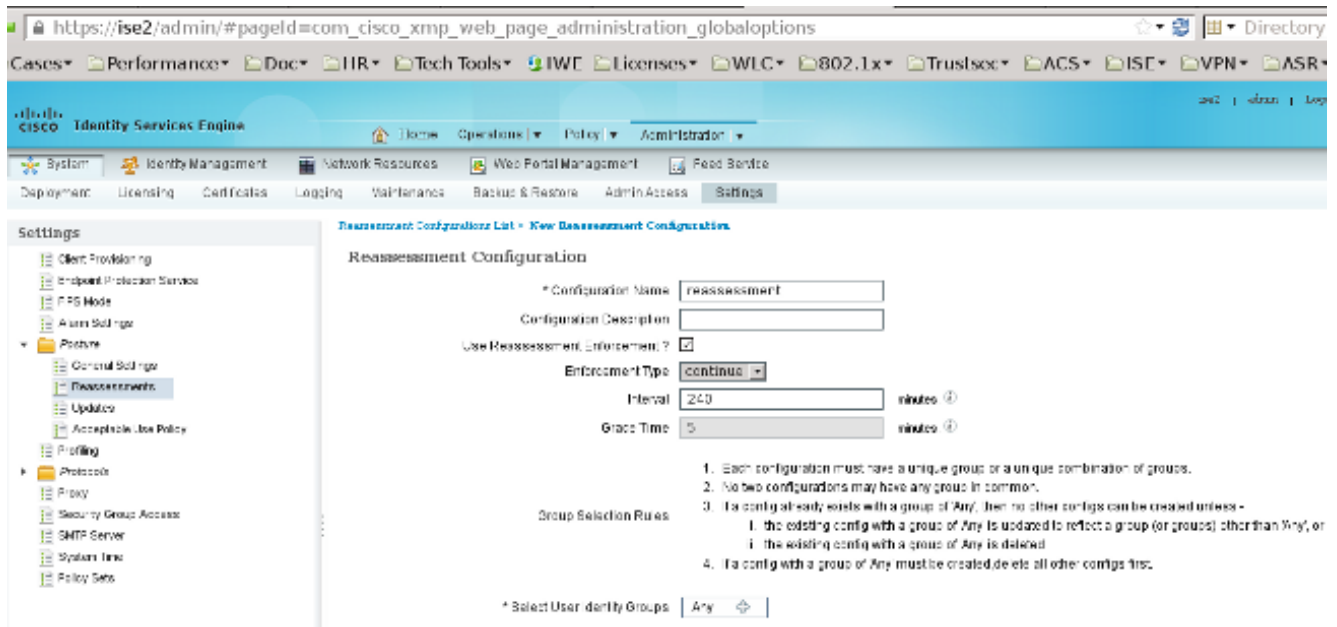


定期重新评估

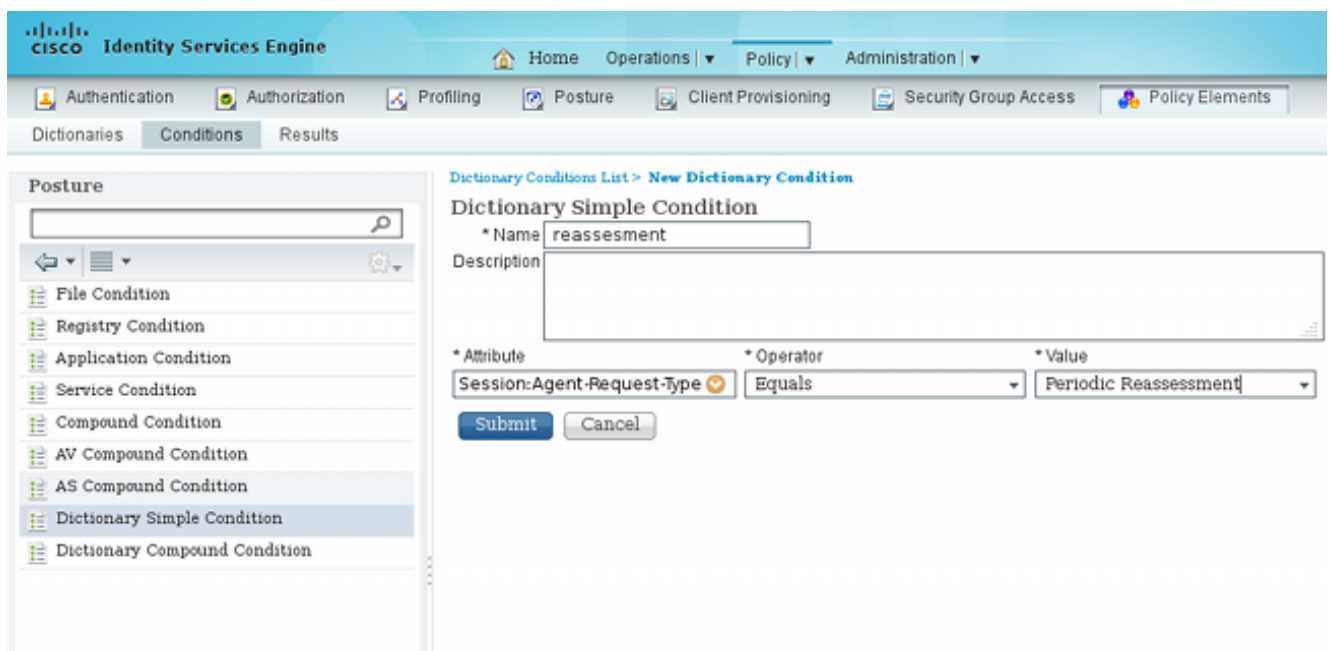
默认情况下，状态为一次性事件。但是，有时需要定期检查用户合规性并根据结果调整对资源的访问。此信息通过SWISS协议（NAC代理）推送或在应用（Web代理）中编码。

要检查用户合规性，请完成以下步骤：

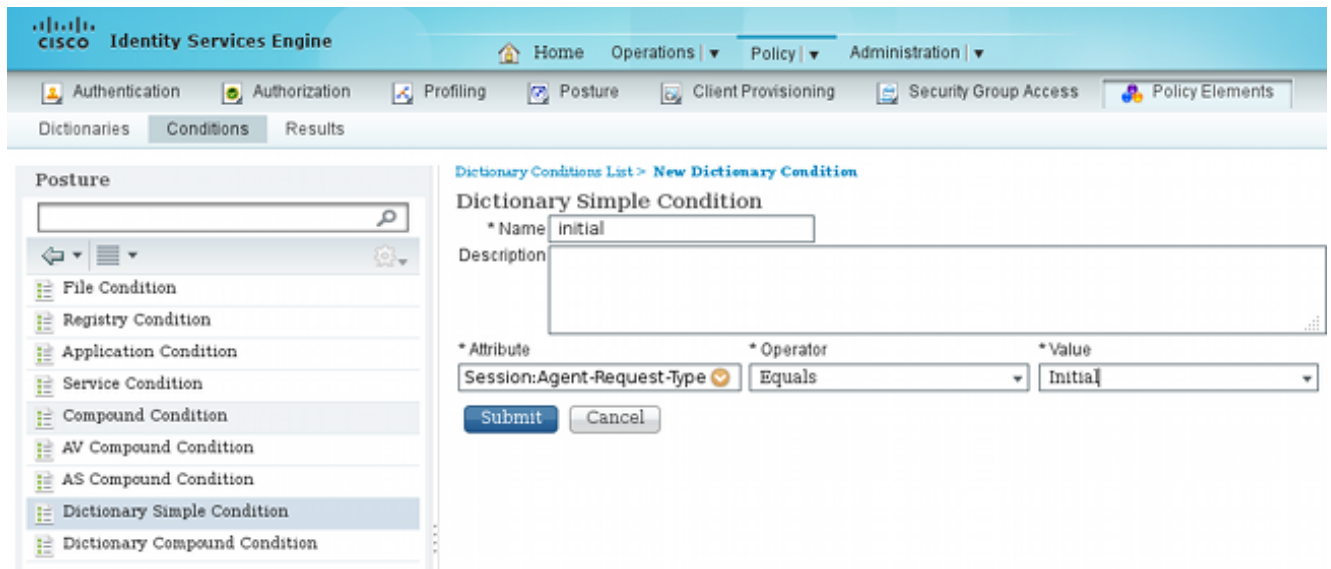
1. 导航到Administration > Settings > Posture > Reassessments并全局启用重新评估（根据身份组配置）：



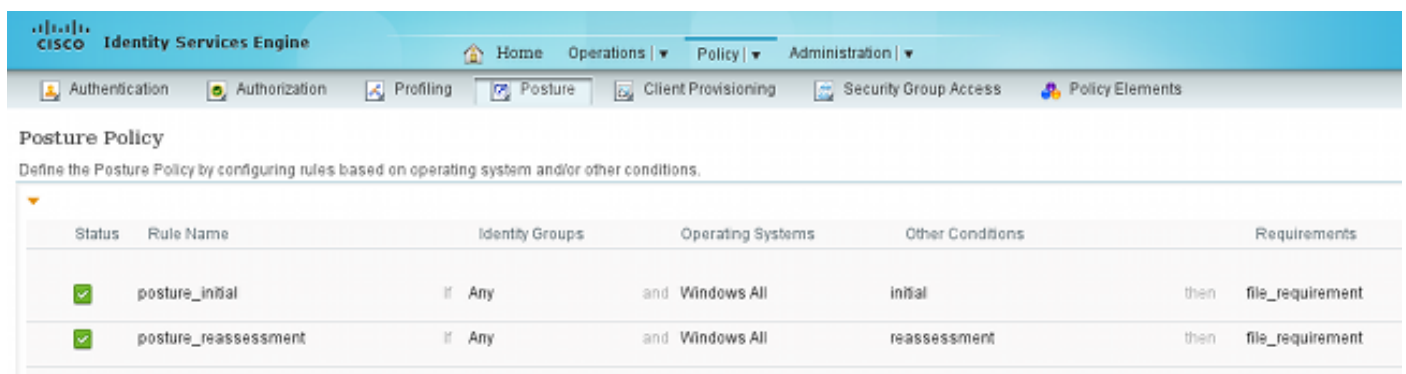
2. 创建与所有重新评估匹配的状况条件：



3. 创建仅与初始评估匹配的类似条件：



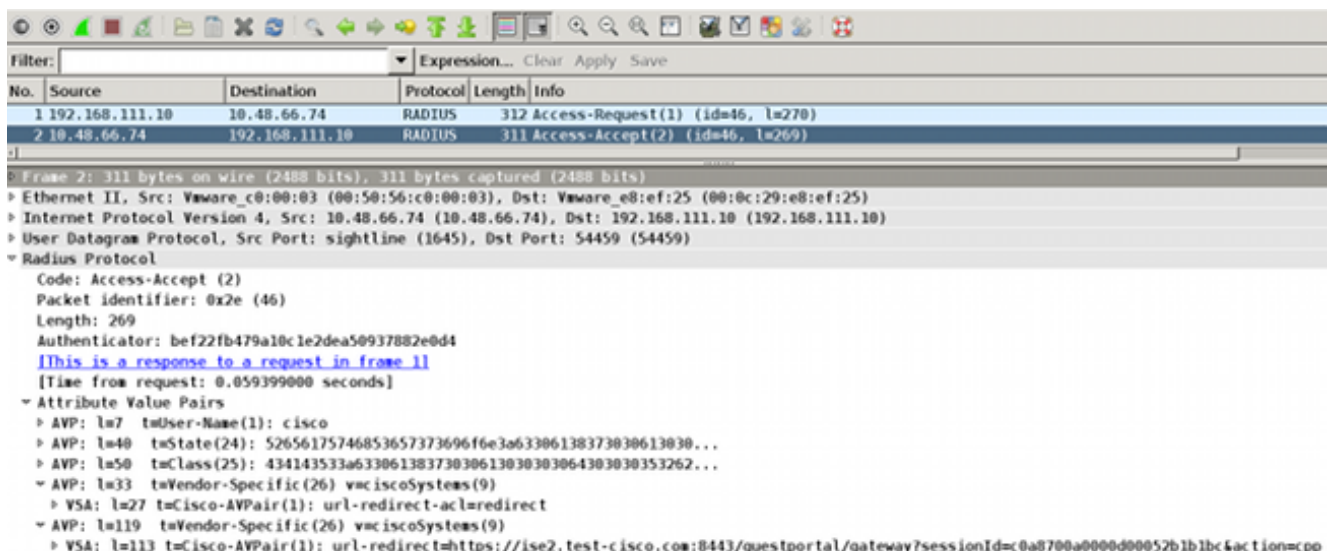
这两种情况都可用于状况规则。第一条 规则仅匹配初始评估，第二条规则匹配所有后续评估：



验证

为了确认您的配置是否正常工作，请确保按所述完成以下步骤：

1. VPN用户连接到ASA。
2. ASA发送RADIUS请求并接收具有url-redirect和url-redirect-acl属性的响应：



3. ISE日志指示授权匹配状况配置文件（第一个日志条目）：

<input checked="" type="checkbox"/>		#ACSACL#-IP-F		ASA9-2		Compliant	ise2
<input checked="" type="checkbox"/>			192.168.10.67	ASA9-2	ASA92-compliant	Compliant	ise2
<input checked="" type="checkbox"/>		0 cisco	192.168.10.67			Compliant	ise2
<input checked="" type="checkbox"/>		cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro...	Pending

4. ASA向VPN会话添加重定向：

```
aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/  
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp  
acl:redirect for 10.10.10.10
```

5. ASA上VPN会话的状态显示需要安全评估并重定向HTTP流量：

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username       : cisco                               Index          : 9  
Assigned IP    : 10.10.10.10                          Public IP       : 10.147.24.61  
Protocol       : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License       : AnyConnect Essentials  
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128  
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1  
Bytes Tx      : 16077                                Bytes Rx       : 19497  
Pkts Tx       : 43                                  Pkts Rx       : 225  
Pkts Tx Drop  : 0                                  Pkts Rx Drop  : 0  
Group Policy  : GP-SSL                               Tunnel Group   : RA  
Login Time    : 14:55:50 CET Mon Dec 23 2013  
Duration      : 0h:01m:34s  
Inactivity    : 0h:00m:00s  
VLAN Mapping  : N/A                                  VLAN           : none  
Audt Sess ID  : c0a8700a0000900052b840e6  
Security Grp  : 0
```

```
AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
```

```
Tunnel ID      : 9.1  
Public IP     : 10.147.24.61  
Encryption    : none                               Hashing        : none  
TCP Src Port  : 50025                              TCP Dst Port   : 443  
Auth Mode     : userPassword  
Idle Time Out: 30 Minutes                          Idle TO Left   : 28 Minutes  
Client OS     : win  
Client Type   : AnyConnect  
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx      : 5204                                Bytes Rx       : 779  
Pkts Tx       : 4                                  Pkts Rx       : 1  
Pkts Tx Drop  : 0                                  Pkts Rx Drop  : 0
```

```
SSL-Tunnel:
```

```
Tunnel ID      : 9.2  
Assigned IP    : 10.10.10.10                          Public IP       : 10.147.24.61  
Encryption    : RC4                                  Hashing        : SHA1  
Encapsulation: TLSv1.0                              TCP Src Port   : 50044  
TCP Dst Port  : 443                                  Auth Mode     : userPassword  
Idle Time Out: 30 Minutes                          Idle TO Left   : 28 Minutes  
Client OS     : Windows  
Client Type   : SSL VPN Client
```

Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx : 5204 Bytes Rx : 172
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 9.3
Assigned IP : 10.10.10.10 Public IP : 10.147.24.61
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 63296
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx : 5669 Bytes Rx : 18546
Pkts Tx : 35 Pkts Rx : 222
Pkts Tx Drop : 0 Pkts Rx Drop : 0

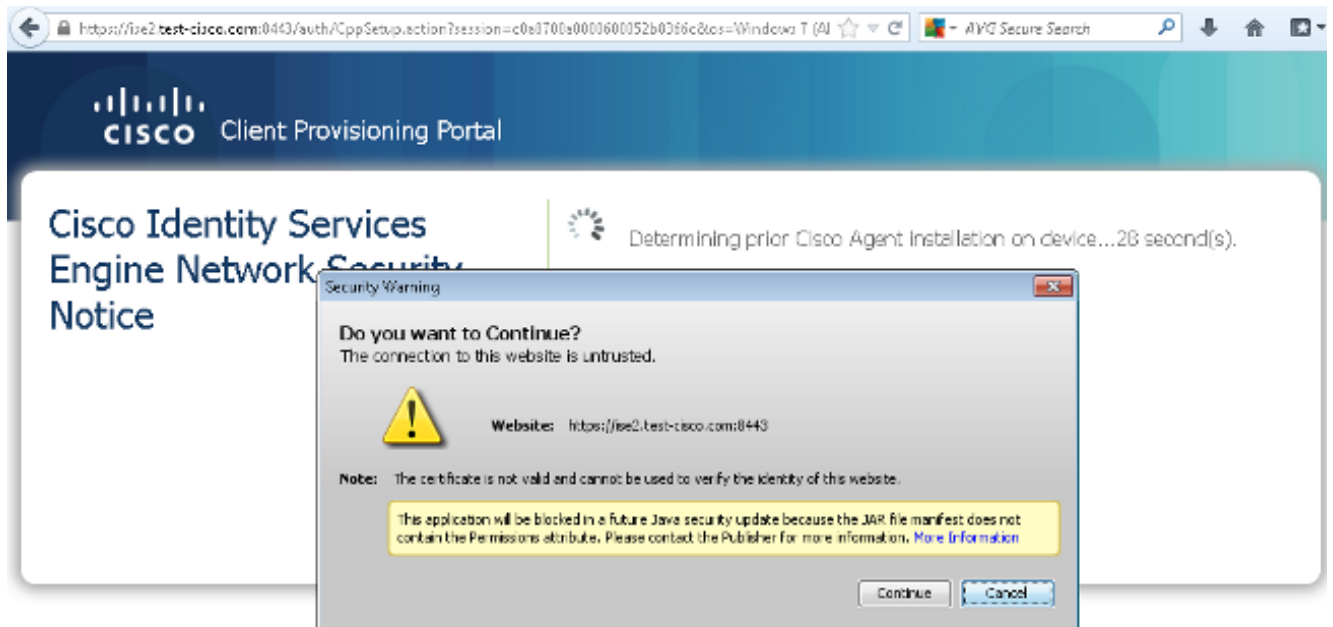
ISE Posture:

Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?
sessionId=c0a8700a0000900052b840e6&action=cpp
Redirect ACL : redirect

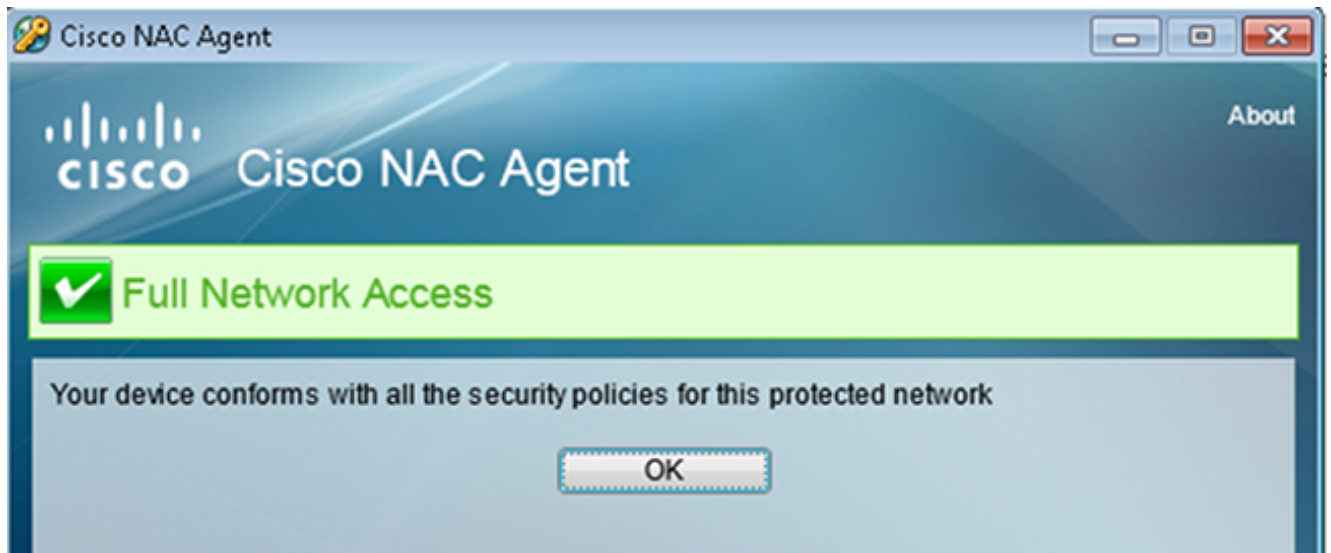
6. 启动与重定向ACL匹配的HTTP流量的客户端重定向到ISE:

aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: **Sending url redirect:**https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for 10.10.10.10

7. 客户端被重定向到ISE以进行安全评估 :



8. NAC代理已安装。安装NAC代理后，它通过SWISS协议下载安全评估规则并执行检查以确定合规性。然后，安全评估报告发送到ISE。



9. ISE接收状况报告，重新评估授权规则，并且（如果需要）更改授权状态并发送CoA。这可以在ise-psc.log中验证：

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
:::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
:::- Posture CoA is triggered for endpoint [null] with session
[c0a8700a0000900052b840e6]
```

10. ISE发送RADIUS CoA，包括session_id和允许完全访问的DACL名称：

No.	Source	Destination	Protocol	Length	Info
7	10.48.66.74	192.168.111.10	RADIUS	231	CoA-Request(43) (id=11, l=189)
8	192.168.111.10	10.48.66.74	RADIUS	62	CoA-ACK(44) (id=11, l=20)

```

> Frame 7: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)
> Ethernet II, Src: Vmware_c0:00:03 (00:50:56:c0:00:03), Dst: Vmware_e8:ef:25 (00:0c:29:e8:ef:25)
> Internet Protocol Version 4, Src: 10.48.66.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)
> User Datagram Protocol, Src Port: 44354 (44354), Dst Port: mps-raft (1700)
v Radius Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xb (11)
  Length: 189
  Authenticator: d20817c6ca828ce7db4ee54f15177b8d
  [The response to this request is in frame 8]
v Attribute Value Pairs
  > AVP: l=6 t=NAS-IP-Address(4): 10.147.24.61
  > AVP: l=15 t=Calling-Station-Id(31): 192.168.10.67
  > AVP: l=6 t=Event-Timestamp(55): Dec 18, 2013 15:32:10.000000000 CET
  > AVP: l=18 t=Message-Authenticator(80): 1ee29f1d83e5f3aa4934d60aa617ebeb
  v AVP: l=75 t=Vendor-Specific(26) v=ciscoSystems(9)
    > VSA: l=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
  v AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
    > VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc

```

这反映在ISE日志中：

第一个日志条目用于返回状态配置文件（带重定向）的初始身份验证。

在收到符合的SWISS报告后，系统会填充第二个日志条目。

发送CoA时，系统会填充第三个日志条目以及确认（描述为Dynamic Authorization Succeeded）。

当ASA下载DACL时，会创建最终日志条目。

✓	🔒	#ACSACL*-IP-F	ASA9-2	Compliant	ise2		
✓	🔒	192.168.10.67	ASA9-2	ASA92-compliant	Compliant	ise2	
🔄	🔒	0 cisco 192.168.10.67		Compliant	ise2		
✓	🔒	cisco 192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro...	Pending	ise2

11. ASA上的调试显示已接收CoA并删除重定向。如果需要，ASA下载DACL:

```
ASA# Received RAD_COA_REQUEST
```

```
RADIUS packet decode (CoA-Request)
```

```
Radius: Value (String) =
```

```
41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d | ACS:CiscoSecure-  
44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53 | Defined-ACL=#ACS  
41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41 | ACL#-IP-PERMIT_A  
4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37 | LL_TRAFFIC-51ef7  
64 62 31 | db1
```

```
Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6
```

```
Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=
```

```
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

```
aaa_url_redirect: Deleted url redirect for 10.10.10.10
```

12. 在VPN会话后，思科为用户应用了DACL（完全访问）:

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                               Index      : 9  
Assigned IP   : 10.10.10.10                          Public IP   : 10.147.24.61  
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License       : AnyConnect Essentials  
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128  
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx     : 94042                               Bytes Rx    : 37079  
Pkts Tx      : 169                                 Pkts Rx    : 382  
Pkts Tx Drop : 0                                 Pkts Rx Drop : 0  
Group Policy : GP-SSL                               Tunnel Group : RA  
Login Time   : 14:55:50 CET Mon Dec 23 2013  
Duration     : 0h:05m:30s  
Inactivity   : 0h:00m:00s  
VLAN Mapping : N/A                               VLAN        : none  
Audt Sess ID : c0a8700a0000900052b840e6  
Security Grp : 0
```

```
AnyConnect-Parent Tunnels: 1
```

```
SSL-Tunnel Tunnels: 1
```

```
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
```

```
Tunnel ID      : 9.1
```



```
Public IP      : 10.147.24.61
Encryption    : none
Hashing       : none
TCP Src Port  : 50025
TCP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Idle TO Left  : 24 Minutes
Client OS     : win
Client Type   : AnyConnect
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 5204
Bytes Rx      : 779
Pkts Tx      : 4
Pkts Rx      : 1
Pkts Tx Drop  : 0
Pkts Rx Drop  : 0
```

SSL-Tunnel:

```
Tunnel ID     : 9.2
Assigned IP   : 10.10.10.10
Public IP     : 10.147.24.61
Encryption    : RC4
Hashing       : SHA1
Encapsulation: TLSv1.0
TCP Src Port  : 50044
TCP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Idle TO Left  : 24 Minutes
Client OS     : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 5204
Bytes Rx      : 172
Pkts Tx      : 4
Pkts Rx      : 2
Pkts Tx Drop  : 0
Pkts Rx Drop  : 0
Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

DTLS-Tunnel:

```
Tunnel ID     : 9.3
Assigned IP   : 10.10.10.10
Public IP     : 10.147.24.61
Encryption    : AES128
Hashing       : SHA1
Encapsulation: DTLSv1.0
UDP Src Port  : 63296
UDP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Idle TO Left  : 29 Minutes
Client OS     : Windows
Client Type   : DTLS VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 83634
Bytes Rx      : 36128
Pkts Tx      : 161
Pkts Rx      : 379
Pkts Tx Drop  : 0
Pkts Rx Drop  : 0
Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

注：即使CoA未连接任何DACL，ASA始终删除重定向规则。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

ISE上的调试

导航到Administration > Logging > Debug Log Configuration以启用调试。Cisco建议您为以下各项启用临时调试：

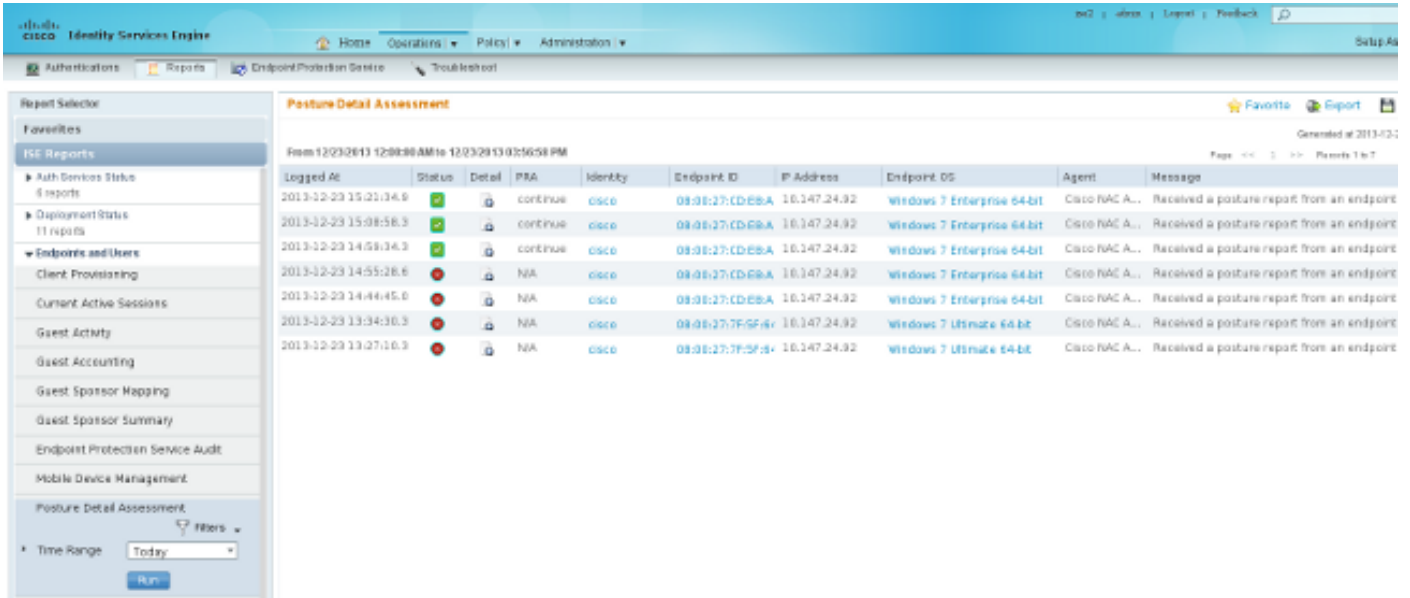
- 瑞士
- 不间断转发(NSF)
- NSF会话

- 调配
- 状态

在CLI中输入以下命令以查看调试：

```
ise2/admin# show logging application ise-psc.log tail count 100
```

导航至操作>报告> ISE报告>终端和用户>终端安全评估详细信息评估以查看终端安全评估报告：



Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	Success	Success	continue	cisco	08:08:27:CD:8B:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 15:08:58.3	Success	Success	continue	cisco	08:08:27:CD:8B:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:59:34.3	Success	Success	continue	cisco	08:08:27:CD:8B:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:55:28.6	Failure	Failure	N/A	cisco	08:08:27:CD:8B:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:44:45.0	Failure	Failure	N/A	cisco	08:08:27:CD:8B:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:34:30.3	Failure	Failure	N/A	cisco	08:08:27:7F:5F:8*	10.147.24.32	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

在Posture More Detail Assessment页面上，将显示具有要求名称的策略名称，以及结果：

Posture More Detail Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM
Generated At: 2013-12-23 15:57:31.248

Client Details

Username:	cisco
Mac Address:	08:00:27:CD:E8:A2
IP address:	10.147.24.92
Session ID:	c0a8700a0000b00052b846c0
Client Operating System:	Windows 7 Enterprise 64-bit
Client NAC Agent:	Cisco NAC Agent for Windows 4.9.0.1013
PRA Enforcement:	1
CoA:	Received a posture report from an endpoint
PRA Grace Time:	
PRA Interval:	240
PRA Action:	continue
User Agreement Status:	NotEnabled
System Name:	MGARCARZ-WS01
System Domain:	cisco.com
System User:	mgarcarz
User Domain:	CI SCO
AV Installed:	McAfee VirusScan Enterprise;8.8.0.975;7227;10/13/2013;McAfeeAV,Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Windows Defender;6.1.7600.16385;1.95.191.0;11/19/2010;MicrosoftAS

Posture Report

Posture Status:	Compliant
Logged At:	2013-12-23 15:21:34.902

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require...	Mandatory		file_condition		

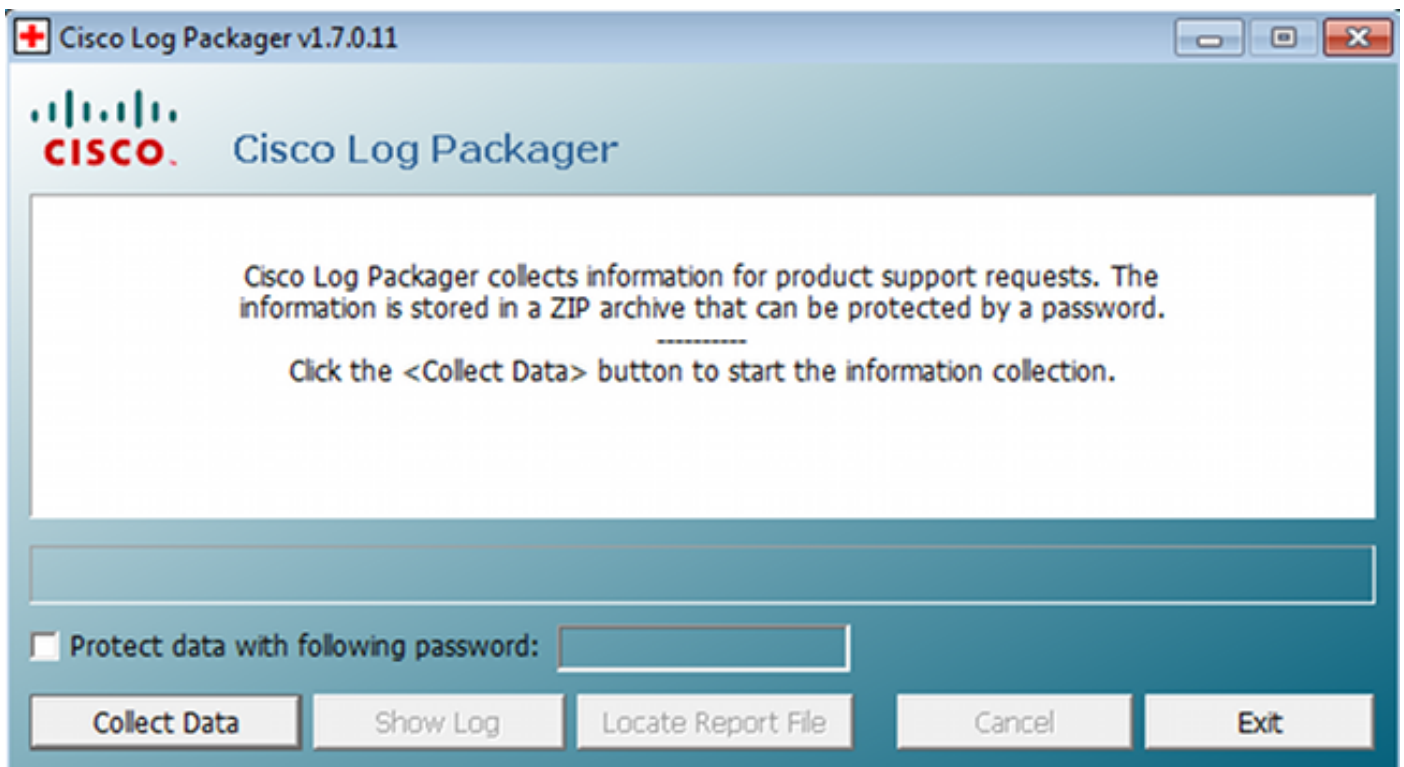
ASA上的调试

您可以在ASA上启用以下调试：

- debug aaa url-redirect
- debug aaa authorization
- debug radius dynamic-authorization
- debug radius decode
- debug radius user cisco

代理的调试

对于NAC代理，可以使用从GUI启动的Cisco Log Packager或CLI(CCAgentLogPackager.app)收集调试。



提示：您可以使用技术支持中心(TAC)工具对结果进行解码。

要检索Web代理的日志，请导航到以下位置：

- C: > Document and Settings > <user> > Local Settings > Temp > webagent.log (使用TAC工具解码)
- C: > Document and Settings > <user> > Local Settings > Temp > webagentsetup.log

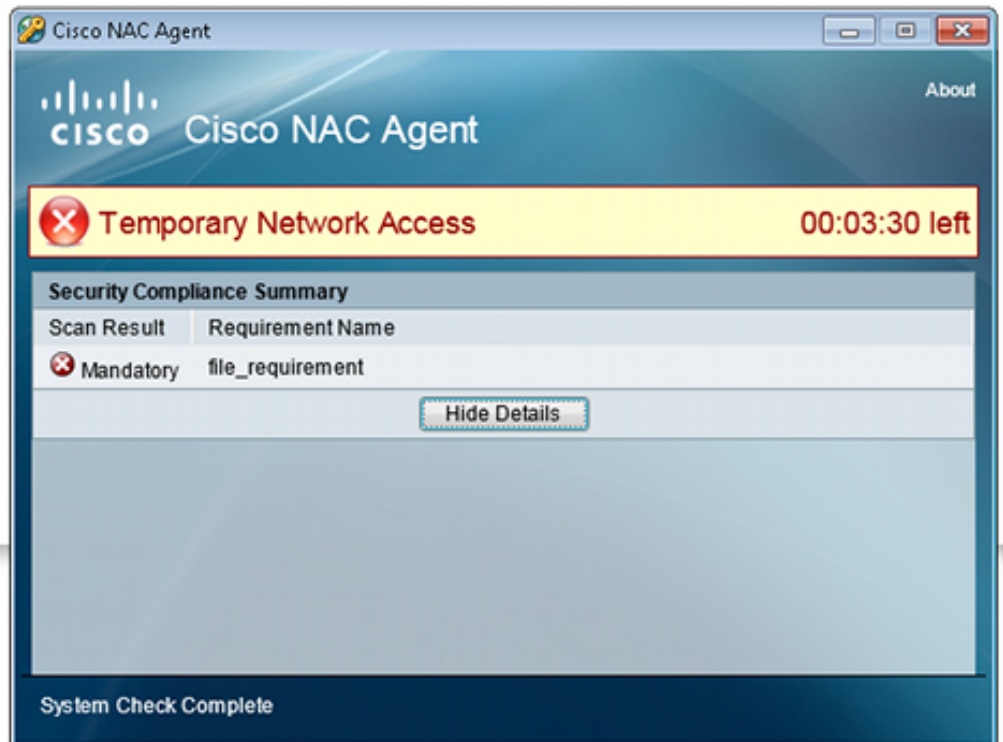
注意：如果日志不在这些位置，则验证TEMP Environment变量。

NAC代理状态故障

如果终端安全评估失败，用户会看到以下原因：



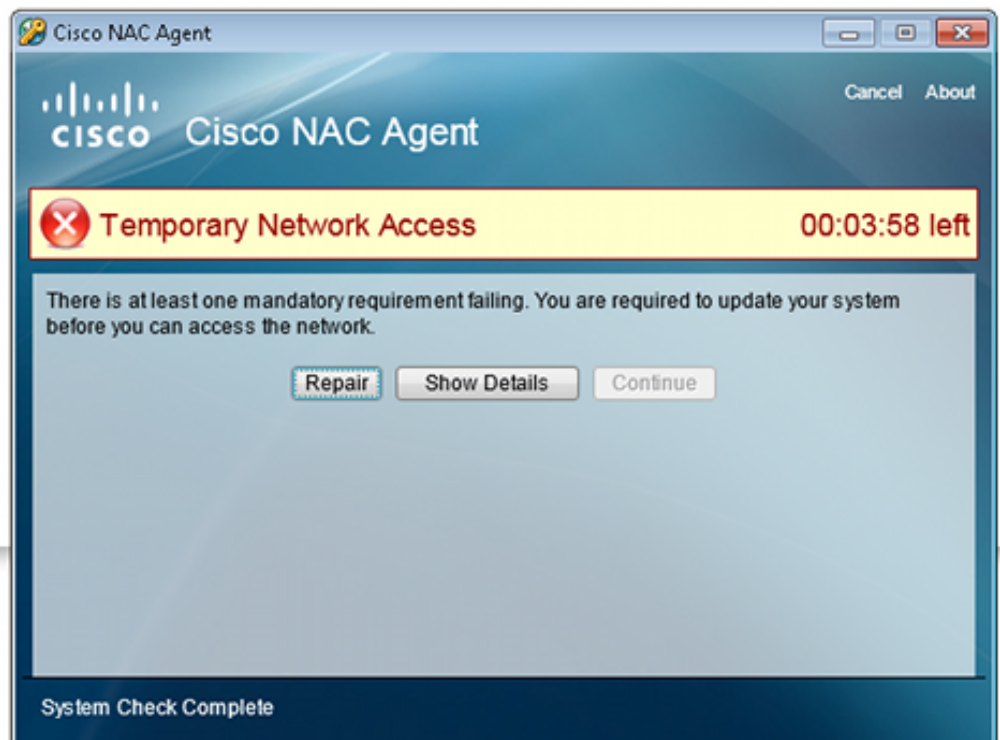
Information



然后，如果配置了以下操作，则允许用户采取补救操作：



Information



相关信息

- [为安全设备用户授权配置外部服务器](#)
- [思科 ASA 系列 VPN CLI 配置指南，版本 9.1](#)
- [思科身份服务引擎用户指南，版本 1.2](#)
- [技术支持和文档 - Cisco Systems](#)

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）。