採用ISE的ASA 9.2.1版VPN安全評估配置示例

目錄

簡介

本檔案介紹如何設定思科調適型安全裝置(ASA)版本9.2.1，以便針對思科身分識別服務引擎(ISE)對VPN使用者進行安全評估，而無需內聯狀態節點(IPN)。

必要條件

需求

思科建議您瞭解以下主題：

- ASA CLI配置和安全套接字層(SSL)VPN配置的基本知識
- ASA上遠端訪問VPN配置的基本知識
- ISE和狀態服務基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體版本9.2.1及更高版本
- 搭載Cisco AnyConnect安全行動化使用者端版本3.1的Microsoft Windows版本7
- Cisco ISE版本1.2（帶補丁5或更高版本）

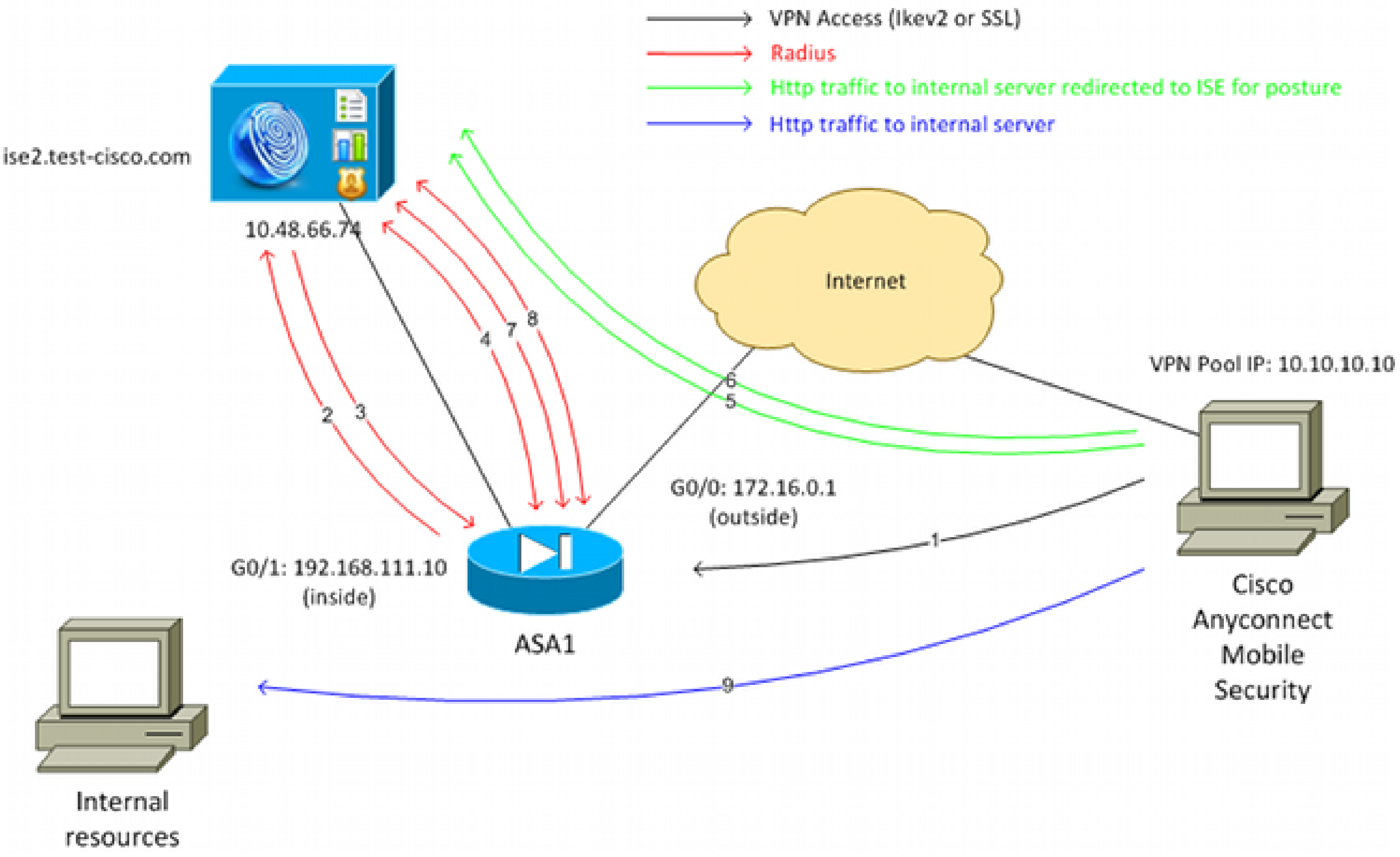
背景資訊

Cisco ASA版本9.2.1支援RADIUS授權更改(CoA)(RFC 5176)。這允許對Cisco ISE進行VPN使用者假定，而不需要IPN。在VPN使用者登入後，ASA會將網路流量重定向到ISE，使用者在此調配網路准入控制(NAC)代理或Web代理。代理對使用者機器執行特定檢查，以確定其是否符合一組已配置的狀況規則，如作業系統(OS)、修補程式、防病毒、服務、應用程式或登錄檔規則。

然後將狀態驗證結果傳送到ISE。如果電腦被視為投訴，則ISE可以使用新授權策略集向ASA傳送RADIUS CoA。成功進行狀態驗證和CoA後，允許使用者訪問內部資源。

設定

網路圖表和流量傳輸



以下是流量傳輸，如網路圖所示：

1. 遠端使用者使用Cisco Anyconnect對ASA進行VPN訪問。

2. ASA向ISE傳送該使用者的RADIUS訪問請求。

3. 該請求會到達ISE上名為**ASA92-posture**的策略。因此，將返**回ASA92-posture**授權配置檔案。ISE傳送帶有兩個Cisco屬性 — 值對的RADIUS訪問接受：

   url-redirect-acl=redirect — 這是在ASA本地定義的訪問控制清單(ACL)名稱，它決定應重定向的流量。

   url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp — 這是遠端使用者應重定向到的URL。**提示**：分配給VPN客戶端的域名系統(DNS)伺服器必須能夠解析重定向URL中返回的完全限定域名(FQDN)。如果配置了VPN過濾器以在隧道組級別限制訪問，請確保客戶端池能夠訪問已配置埠上的ISE伺服器(在本例中為**TCP 8443**)。
4. ASA傳送RADIUS Accounting-Request啟動資料包並接收響應。若要向ISE傳送會話的所有詳細資訊，需要執行此操作。這些詳細資訊包括session_id、VPN客戶端的外部IP地址和ASA的IP地址。ISE使用session_id來標識該會話。ASA還會定期傳送臨時帳戶資訊，其中最重要的屬性是Framed-IP-Address，該屬性具有ASA分配給客戶端的IP(在本例中為**10.10.10.10**)。

5. 當VPN使用者的流量與本地定義的ACL（重定向）匹配時，會將其重定向到**https://ise2.test-cisco.com:8443**。根據配置，ISE會調配NAC代理或Web代理。

6. 在客戶端電腦上安裝代理後，代理將自動執行特定的檢查。在本例中，它搜尋**c:\test.txt**檔案。它還向ISE傳送狀態報告，其中可以包含使用瑞士協定和埠TCP/UDP 8905進行多次交換以訪問ISE。

7. 當ISE收到來自代理的狀態報告時，它會再次處理授權規則。這一次，狀態結果為已知，另一規則被命中。傳送RADIUS CoA封包：

   如果使用者符合，則會傳送允許完全存取的可下載ACL(DACL)名稱（AuthZ規則ASA92-compliant）。

   如果使用者不相容，則會傳送允許有限訪問的DACL名稱（AuthZ規則ASA92-not compliant）。**註**:RADIUS CoA始終確認；即ASA向ISE傳送響應以進行確認。
8. ASA刪除重定向。如果沒有快取DACL，則必須傳送訪問請求才能從ISE下載它們。特定DACL會附加到VPN會話。

9. 下次當VPN使用者嘗試訪問網頁時，可以訪問ASA上安裝的DACL允許的所有資源。
   如果使用者不合規，則僅授予有限的訪問許可權。
   注意：此流量模型與使用RADIUS CoA的大多數方案不同。對於有線/無線802.1x身份驗證，RADIUS CoA不包括任何屬性。它只觸發附加所有屬性（如DACL）的第二個身份驗證。對於ASA VPN狀態，沒有第二個身份驗證。所有屬性都返回到RADIUS CoA中。VPN會話處於活動狀態，無法更改大多數VPN使用者設定。

組態

使用本節配置ASA和ISE。

ASA

以下是Cisco AnyConnect接入的基本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
```

對於ASA與ISE終端安全評估整合，請確保您：

- 為動態授權配置身份驗證、授權和記帳(AAA)伺服器，以便接受CoA。
- 將記帳配置為隧道組，以便向ISE傳送VPN會話詳細資訊。
- 配置臨時記帳，它將傳送分配給使用者的IP地址並定期更新ISE上的會話狀態
- 配置重定向ACL，它決定是否允許DNS和ISE流量。所有其他HTTP流量都重定向到ISE進行安全評估。

以下是組態範例：

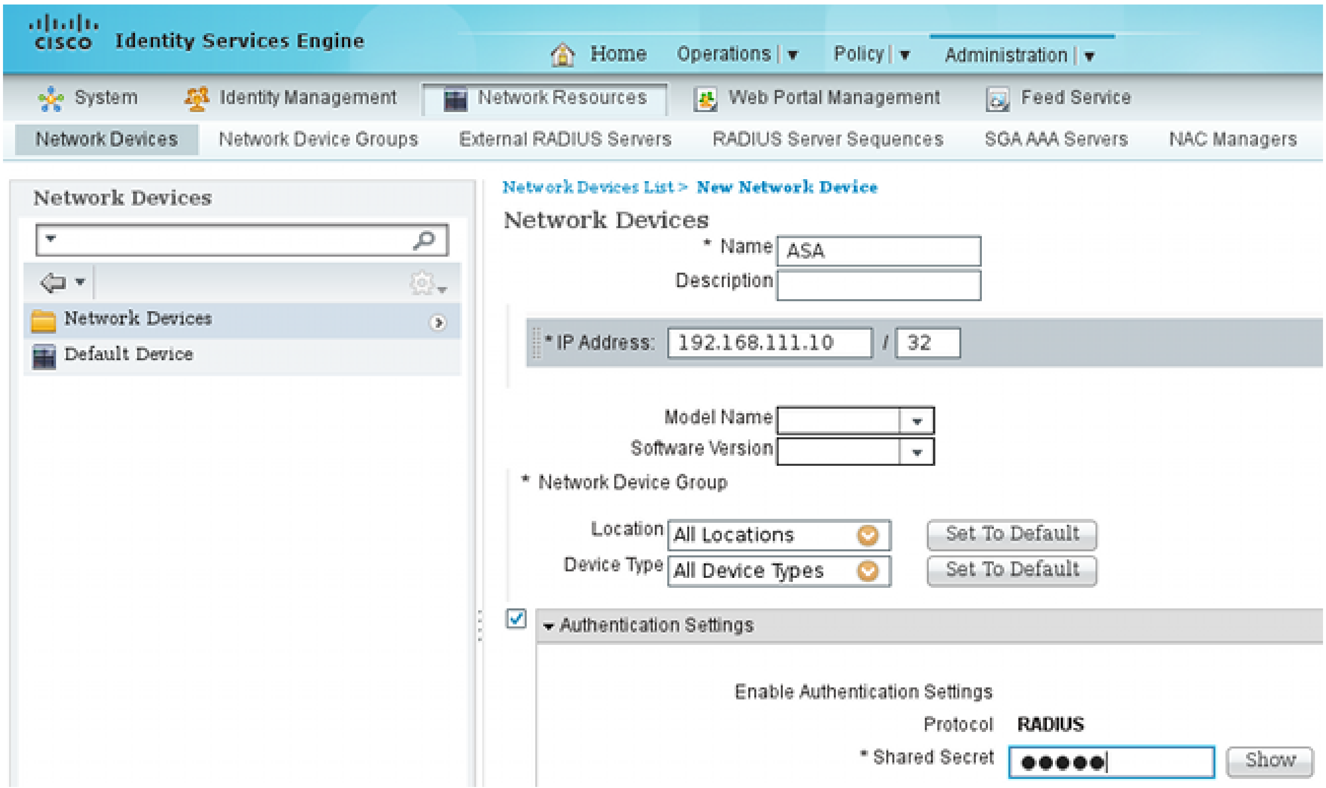
```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

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

完成以下步驟以配置ISE:

1. 導航到**Administration > Network Resources > Network Devices**，然後將ASA新增為網路裝置：



Network Devices

* Name: ASA

Description:

* IP Address: 192.168.111.10 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations

Device Type: All Device Types

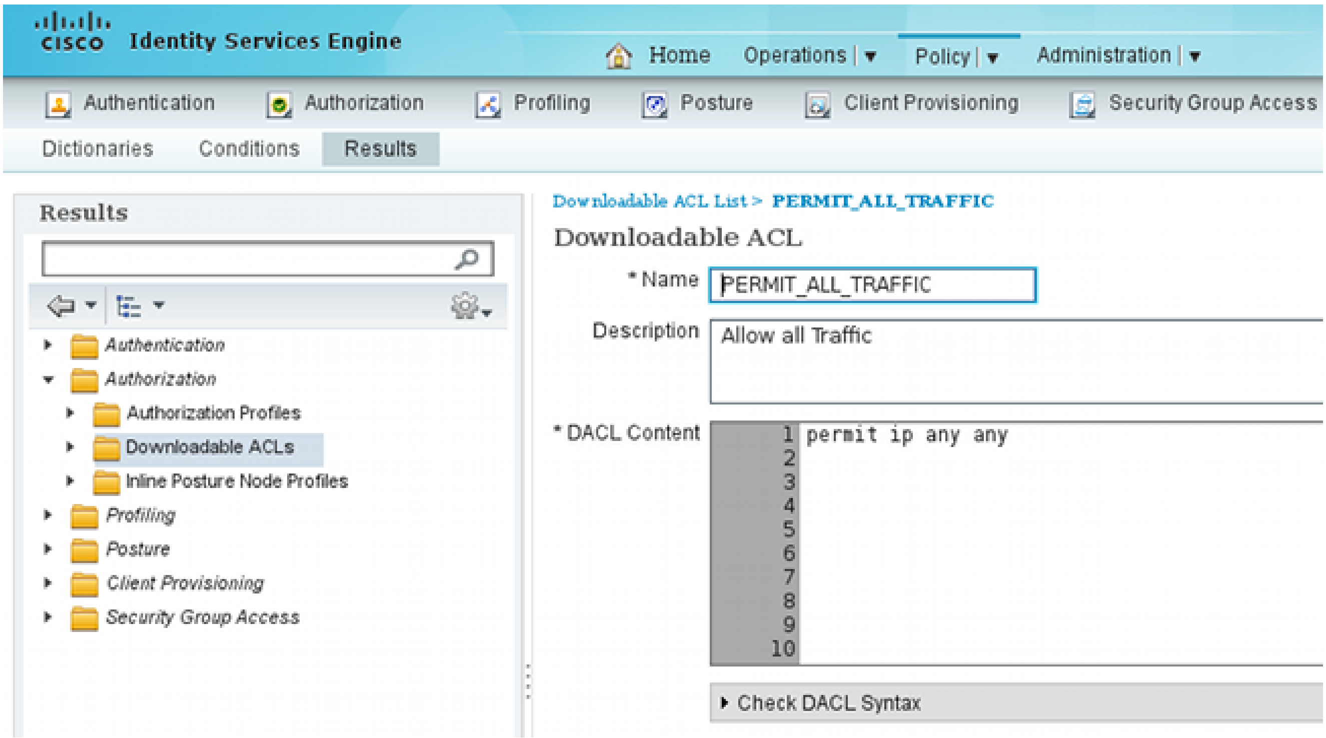
☑ Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: ●●●●●

2. 導覽至**Policy > Results > Authorization > Downloadable ACL**，並設定DACL使其允許完全存取。預設ACL配置允許ISE上的所有IP流量：



Downloadable ACL List > PERMIT_ALL_TRAFFIC

Downloadable ACL

* Name: PERMIT_ALL_TRAFFIC

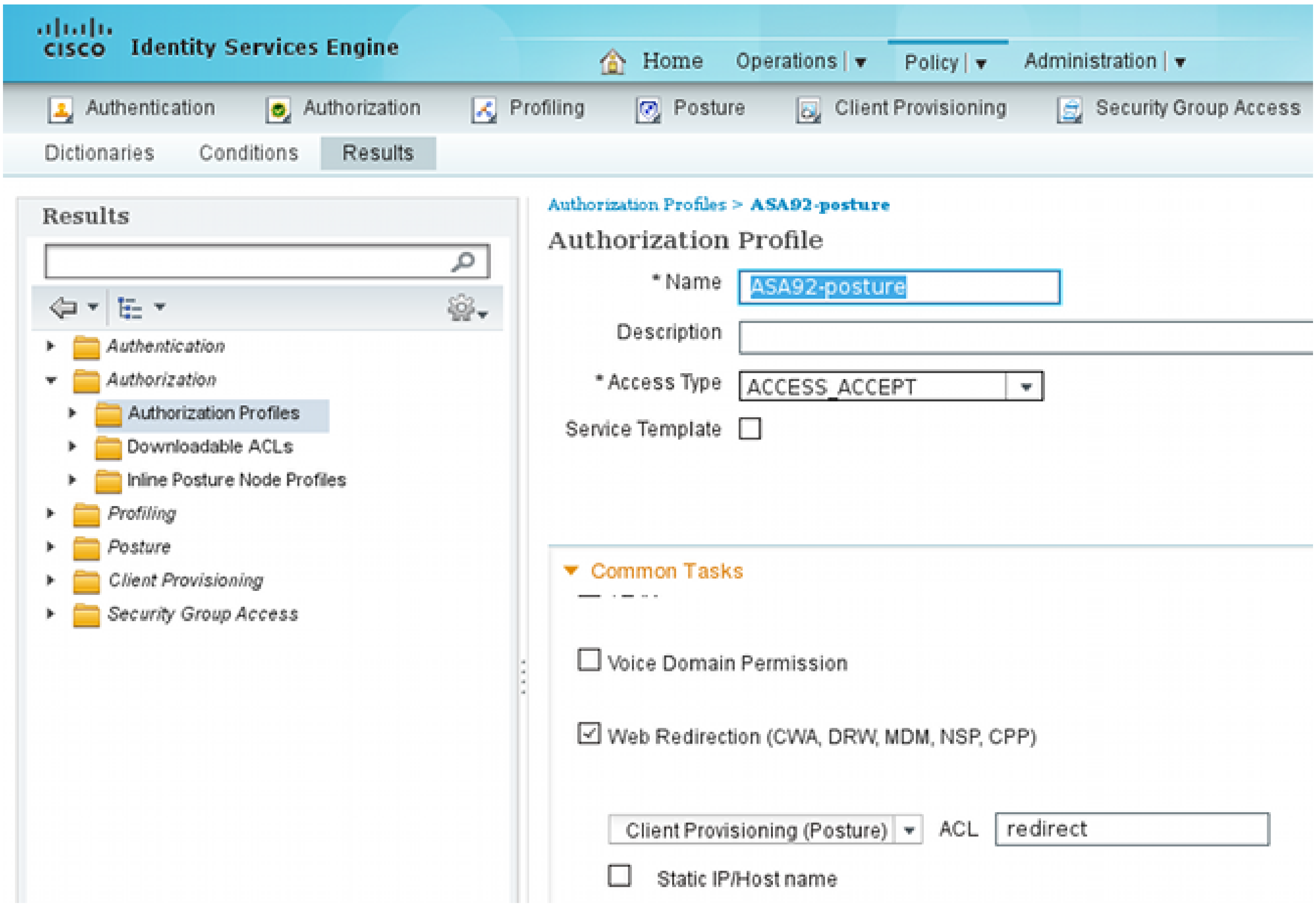
Description: Allow all Traffic

* DACL Content:

```
permit ip any any
```

3. 配置提供有限訪問的類似ACL（針對不合規使用者）。

4. 導航到**Policy > Results > Authorization > Authorization Profiles**，並配置名為**ASA92-posture**的授權配置檔案，該配置檔案重定向使用者進行安全評估。選中**Web Redirection**覈取方塊，從下拉選單中選擇**Client Provisioning**，並確保**redirect**顯示在ACL欄位中（該ACL在ASA上本地定義）：



Authorization Profiles > ASA92-posture

Authorization Profile

* Name: ASA92-posture

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

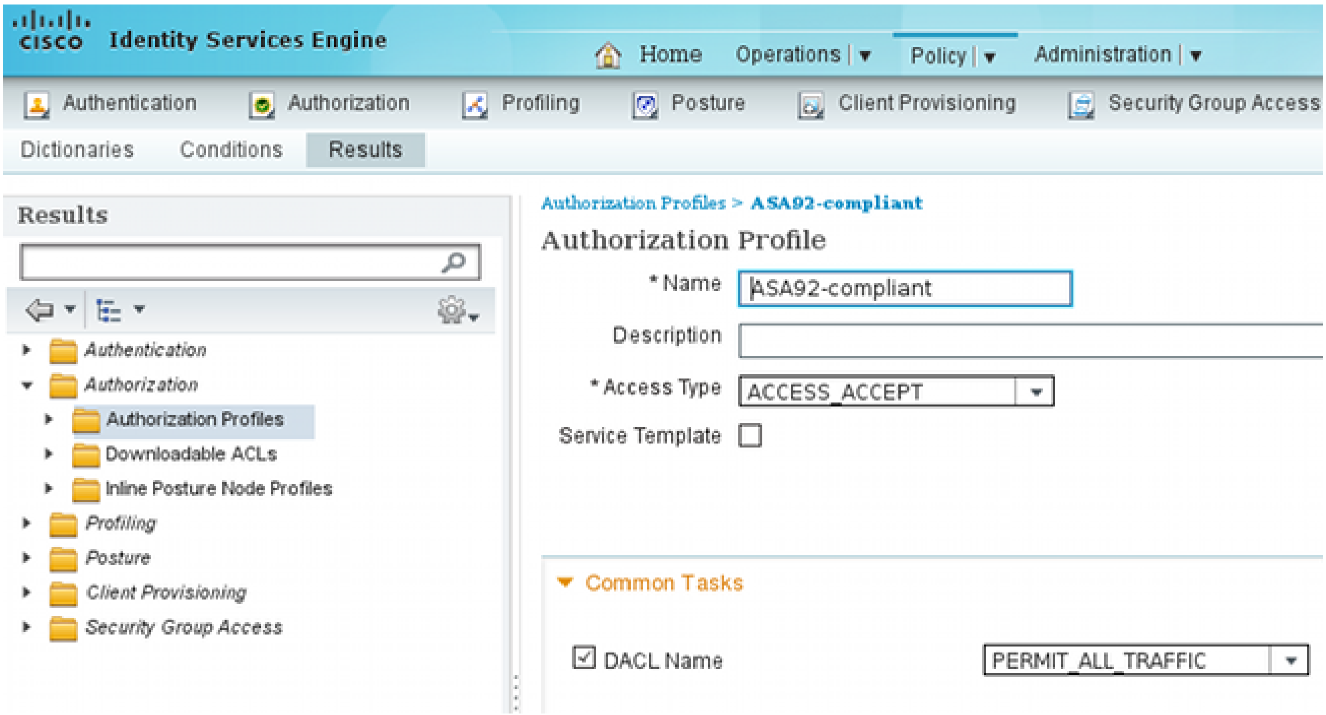
□ Voice Domain Permission

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: redirect

□ Static IP/Host name

5. 配置名為**ASA92-compliant**的授權配置檔案，該配置檔案應只返回名為**PERMIT_ALL_TRAFFIC**的DACL，為相容使用者提供完全訪問許可權：



Authorization Profiles > **ASA92-compliant**

Authorization Profile

* Name: ASA92-compliant

Description:

* Access Type: ACCESS_ACCEPT

Service Template: □

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

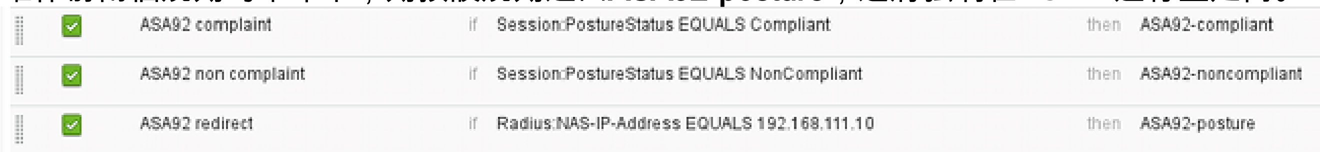
6. 配置名為**ASA92-non-compliant**的類似授權配置檔案，該配置檔案應返回具有有限訪問許可權的DACL（針對不合規使用者）。

7. 導航到**Policy > Authorization**並配置授權規則：

   建立一條規則，允許安全狀態結果符合時進行完全訪問。結果是授權策略**與ASA92相容**。

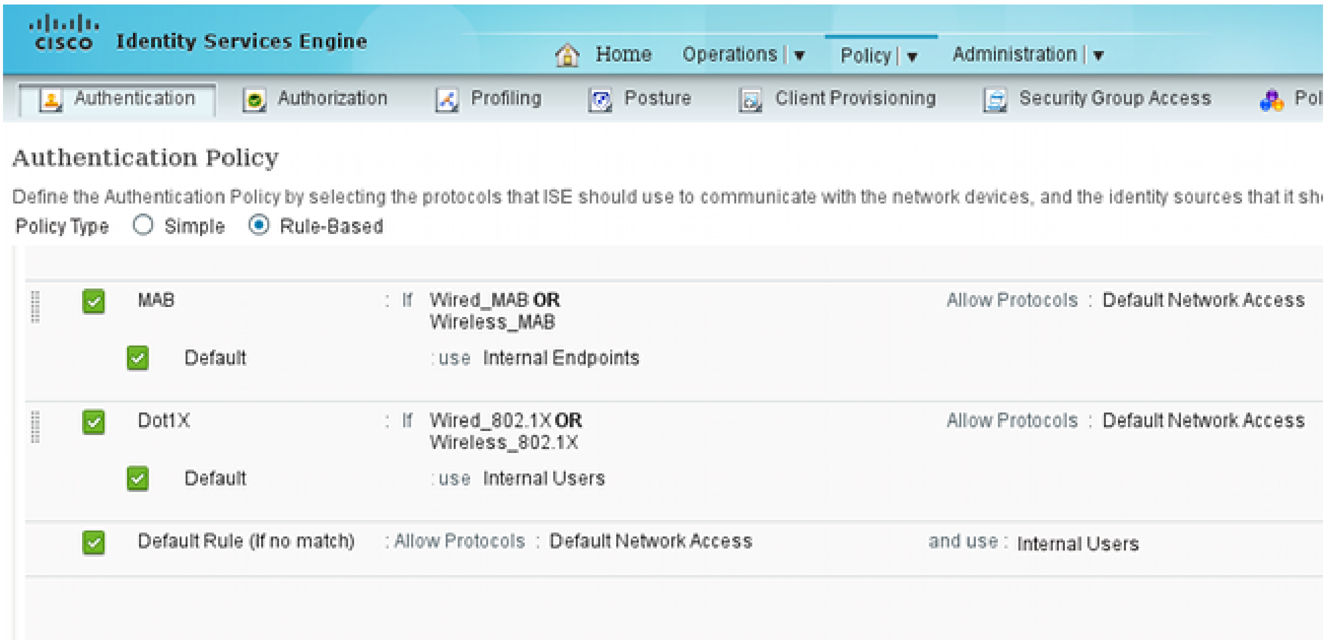
   建立在狀況結果不符合時允許有限訪問的規則。結果導致授權策略**ASA92不相容**。

   確保前兩個規則均未命中，則預設規則返回**ASA92-posture**，這將強制在ASA上進行重定向。



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

8. 預設身份驗證規則檢查內部身份庫中的使用者名稱。如果必須更改此設定(例如，在Active Directory(AD)中選中)，請導航到**Policy > Authentication**並進行更改：



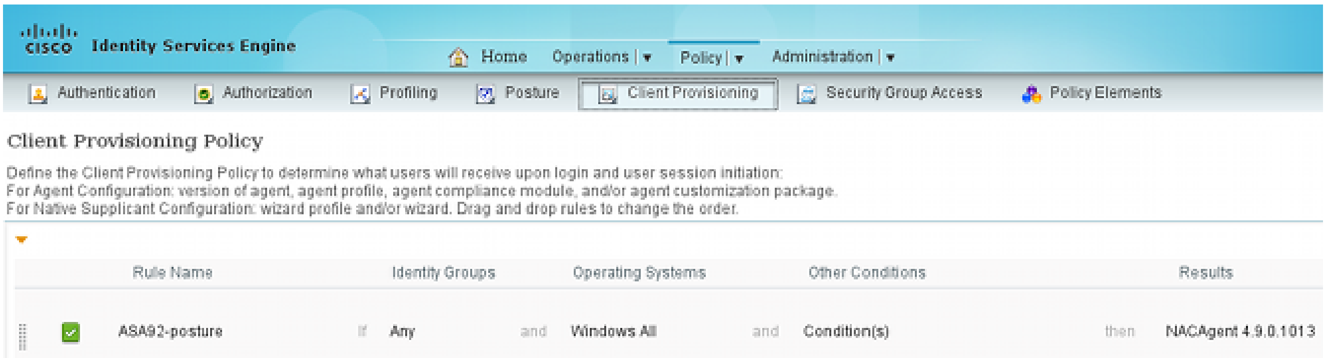
Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If	Wired_MAB **OR** Wireless_MAB	Allow Protocols :	Default Network Access
☑ Default	: use	Internal Endpoints		
☑ Dot1X	: If	Wired_802.1X **OR** Wireless_802.1X	Allow Protocols :	Default Network Access
☑ Default	: use	Internal Users		
☑ Default Rule (If no match)	: Allow Protocols :	Default Network Access	and use :	Internal Users

9. 導航到**Policy > Client Provisioning**並配置調配規則。以下是決定應調配的代理型別的規則。在此示例中，僅存在一個簡單規則，並且ISE為所有Microsoft Windows系統選擇NAC代理：

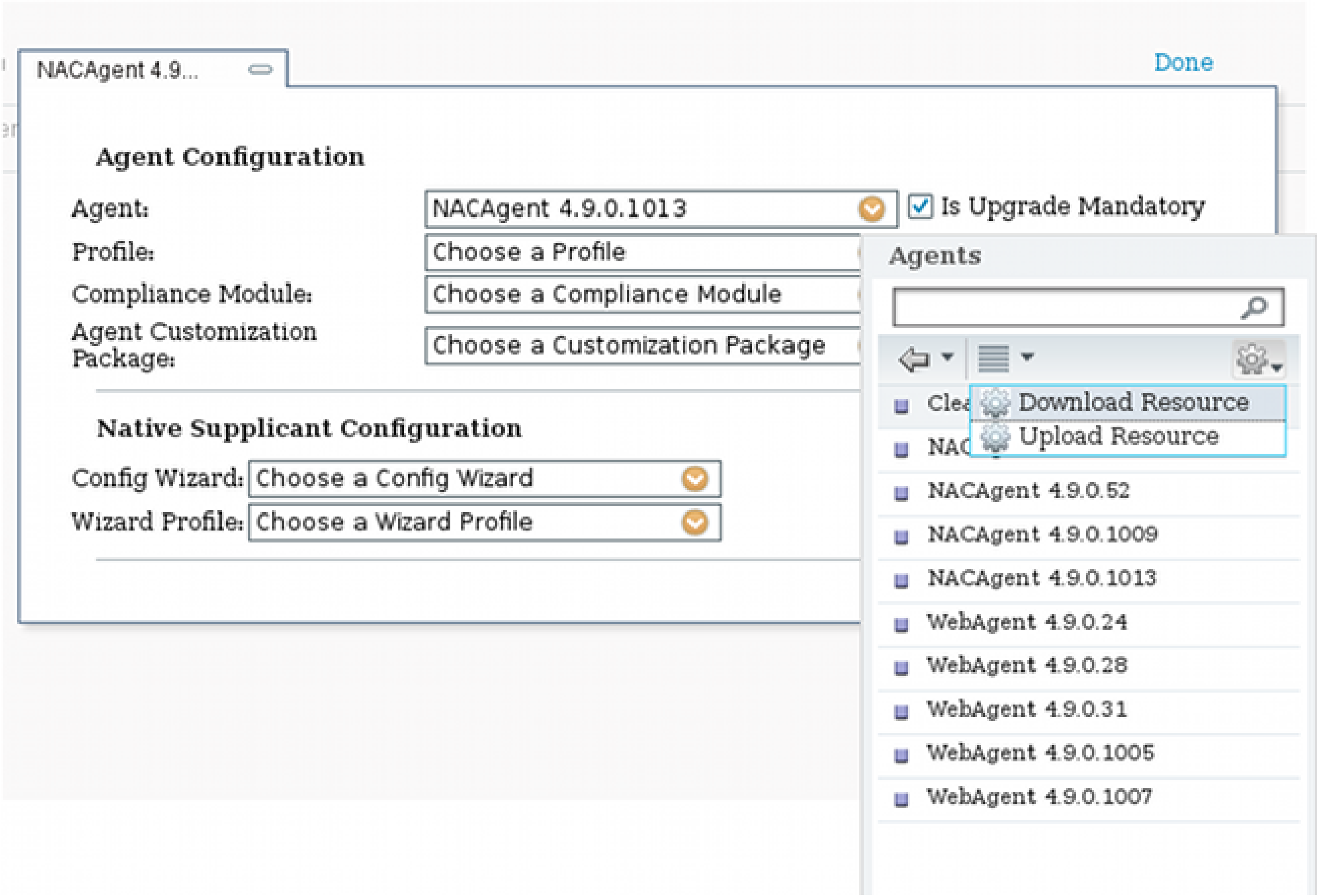


Client Provisioning Policy

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
☑ ASA92-posture	If	Any	and	Windows All	and	Condition(s)	then	NACAgent 4.9.0.1013

當Agent不在ISE上時，可以下載它們：



Agent Configuration

Agent: NACAgent 4.9.0.1013 ☑ Is Upgrade Mandatory

Profile: Choose a Profile

Compliance Module: Choose a Compliance Module

Agent Customization Package: Choose a Customization Package

Native Supplicant Configuration

Config Wizard: Choose a Config Wizard

Wizard Profile: Choose a Wizard Profile

Clea
NAC
NACAgent 4.9.0.52
NACAgent 4.9.0.1009
NACAgent 4.9.0.1013
WebAgent 4.9.0.24
WebAgent 4.9.0.28
WebAgent 4.9.0.31
WebAgent 4.9.0.1005
WebAgent 4.9.0.1007

10. 如有必要，您可以導航到**Administration > System > Settings > Proxy**，並為ISE配置代理（以訪問Internet）。

11. 配置終端安全評估規則，用於驗證客戶端配置。您可以配置檢查以下內容的規則：

    files — 存在、版本、日期

    registry — 鍵、值、存在

    application — 進程名稱，正在運行，未運行

    service — 服務名稱，正在運行，未運行

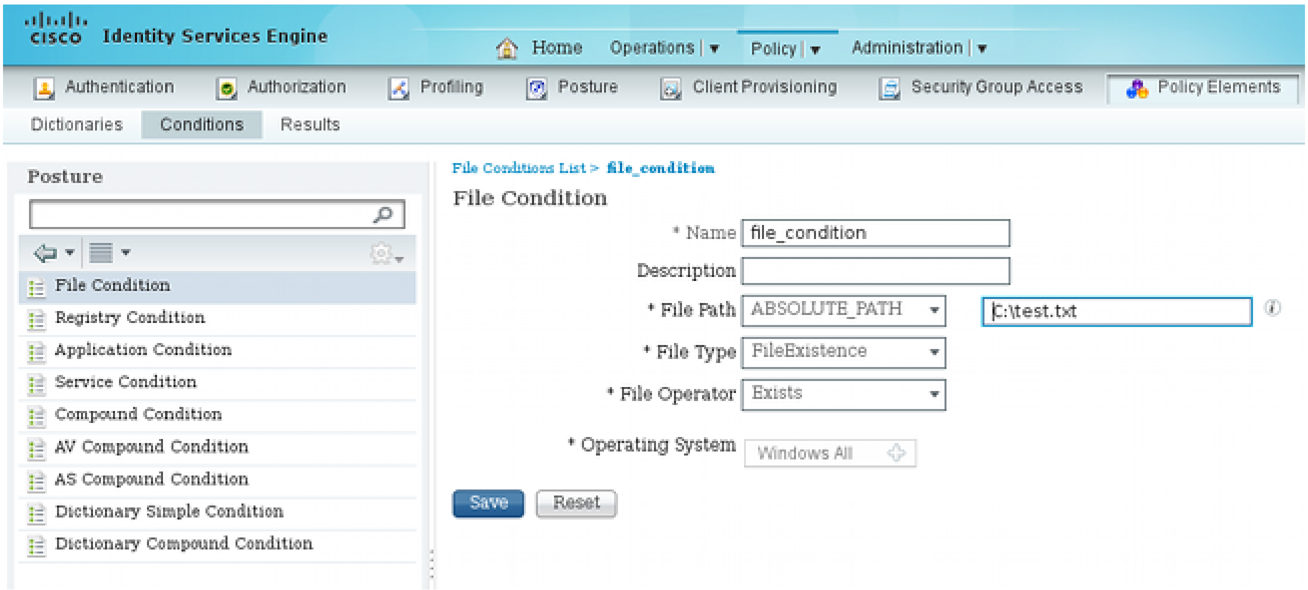
    防病毒 — 更新定義時，版本支援100多家供應商

    反間諜軟體 — 更新定義時，版本支援100多家供應商

    複合條件 — 混合所有

    自定義詞典條件 — 大多數ISE詞典的使用

12. 在此示例中，只執行簡單的檔案存在性檢查。如果客戶端電腦上存在**c:\test.txt**檔案，則該檔案符合併允許完全訪問。導覽至**Policy > Conditions > File Conditions**，並設定檔案條件：



File Conditions List > file_condition

File Condition

* Name: file_condition

Description:

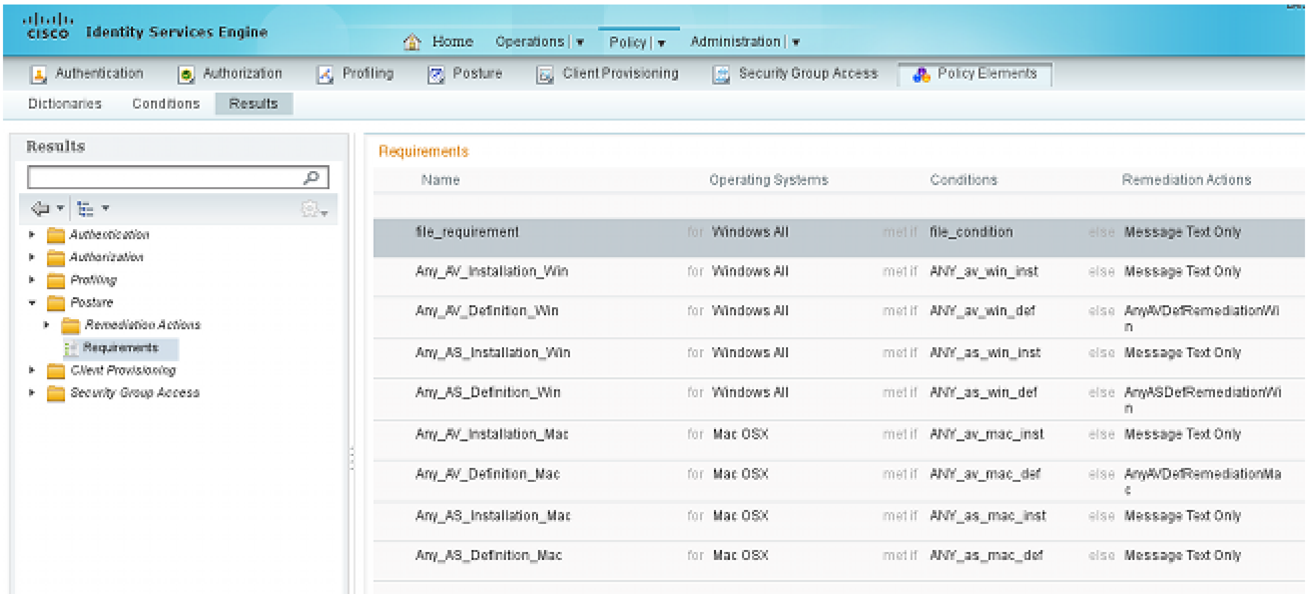
* File Path: ABSOLUTE_PATH C:\test.txt

* File Type: FileExistence

* File Operator: Exists

* Operating System: Windows All

13. 導航到**Policy > Results > Posture > Requirements**並建立需求。當滿足前一條件時，應滿足此要求。如果不是，則執行補救操作。可能有許多型別的補救操作可用，但在此示例中，使用最簡單的補救操作：顯示特定消息。

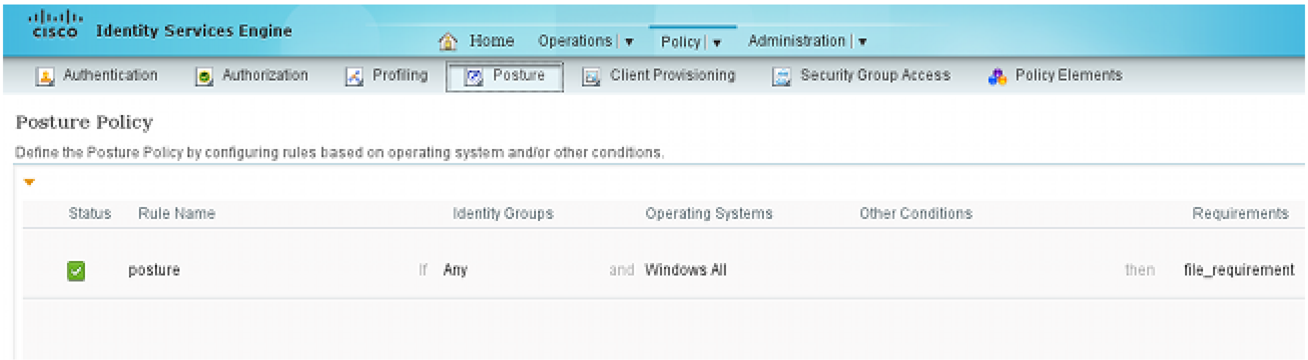


Requirements

Name		Operating Systems		Conditions		Remediation Actions
file_requirement	for	Windows All	met if	file_condition	else	Message Text Only
Any_AV_Installation_Win	for	Windows All	met if	ANY_av_win_inst	else	Message Text Only
Any_AV_Definition_Win	for	Windows All	met if	ANY_av_win_def	else	AnyAVDefRemediationWin
Any_AS_Installation_Win	for	Windows All	met if	ANY_as_win_inst	else	Message Text Only
Any_AS_Definition_Win	for	Windows All	met if	ANY_as_win_def	else	AnyASDefRemediationWin
Any_AV_Installation_Mac	for	Mac OSX	met if	ANY_av_mac_inst	else	Message Text Only
Any_AV_Definition_Mac	for	Mac OSX	met if	ANY_av_mac_def	else	AnyAVDefRemediationMac
Any_AS_Installation_Mac	for	Mac OSX	met if	ANY_as_mac_inst	else	Message Text Only
Any_AS_Definition_Mac	for	Mac OSX	met if	ANY_as_mac_def	else	Message Text Only

注意：在正常情況下，可以使用File Remediation操作（ISE提供可下載檔案）。

14. 導航到**Policy > Posture**，並在終端安全評估規則中使用您在上一步驟中建立的需求(名稱為**file_requirement**)。唯一的狀態規則要求所有Microsoft Windows系統都滿足**file_requirement**。如果滿足此要求，則工作站是相容的；如果不能滿足此要求，則工作站是不相容的。



Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

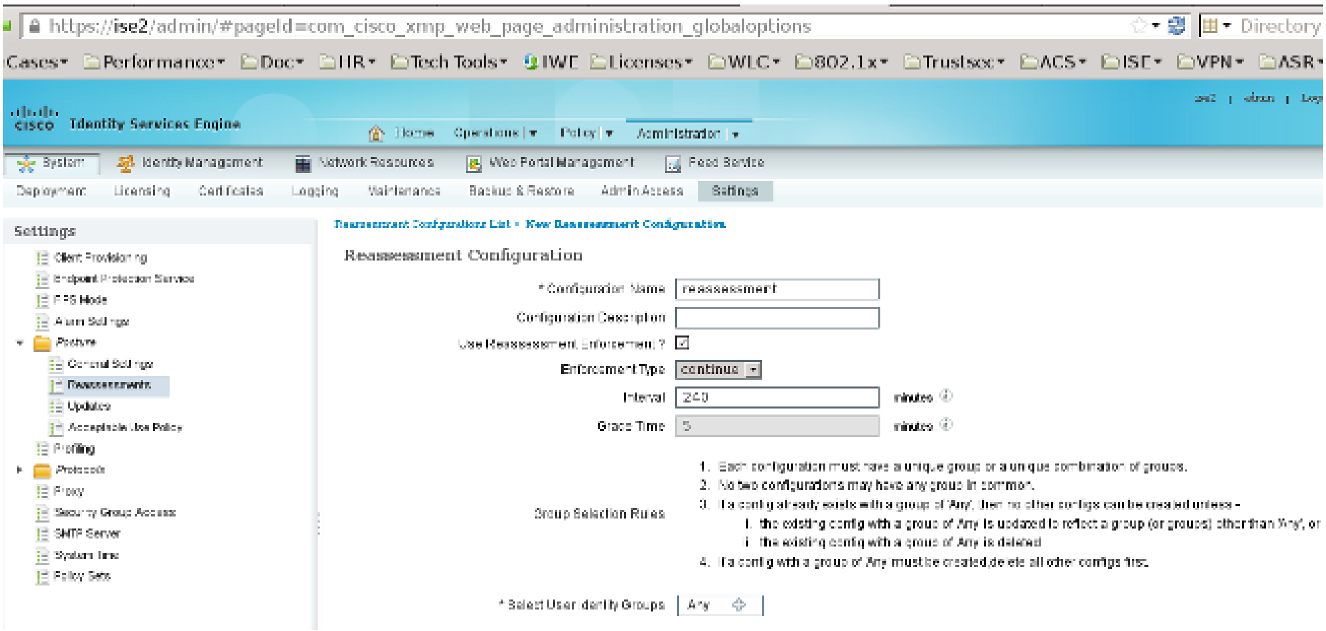
Status	Rule Name		Identity Groups		Operating Systems	Other Conditions		Requirements
✓	posture	If	Any	and	Windows All		then	file_requirement

定期重新評估

預設情況下，狀態為一次性事件。但是，有時需要定期檢查使用者符合性，並根據結果調整對資源的訪問。此資訊通過SWISS協定（NAC代理）推送或在應用程式（Web代理）中編碼。

完成以下步驟以檢查使用者符合性：

1. 導航到**Administration > Settings > Posture > Reassessments**，並全域性啟用重新評估（每個身份組配置）：


https://ise2/admin/#pageId=com_cisco_xmp_web_page_administration_globaloptions
Cases Performance Doc HR Tech Tools IWE Licenses WLC 802.1x Trustsec ACS ISE VPN ASR
Identity Services Engine
Home Operations Policy Administration
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Settings
Client Provisioning
Endpoint Protection Service
FIPS Mode
Alarm Settings
Posture
General Settings
Reassessments
Updates
Acceptable Use Policy
Profiling
Protocols
Proxy
Security Group Access
SMTP Server
System Time
Policy Sets

Reassessment Configurations List > New Reassessment Configuration

Reassessment Configuration

* Configuration Name: reassessment

Configuration Description:

Use Reassessment Enforcement ? ☑

Enforcement Type: continue

Interval: 240 minutes

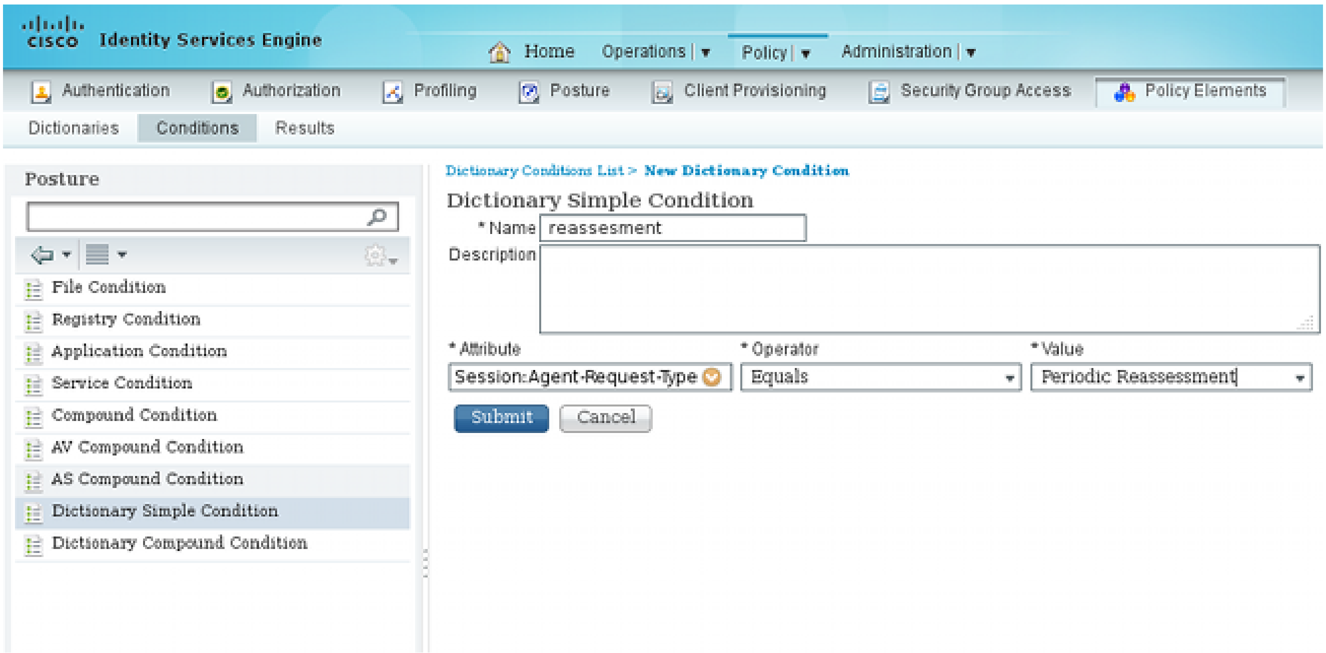
Grace Time: 5 minutes

Group Selection Rules:

1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
   i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
   ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created, delete all other configs first.

* Select User Identity Groups: Any

2. 建立與所有重新評估匹配的狀況條件：


Identity Services Engine
Home Operations Policy Administration
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Posture
File Condition
Registry Condition
Application Condition
Service Condition
Compound Condition
AV Compound Condition
AS Compound Condition
Dictionary Simple Condition
Dictionary Compound Condition
Submit
Cancel

Dictionary Conditions List > New Dictionary Condition

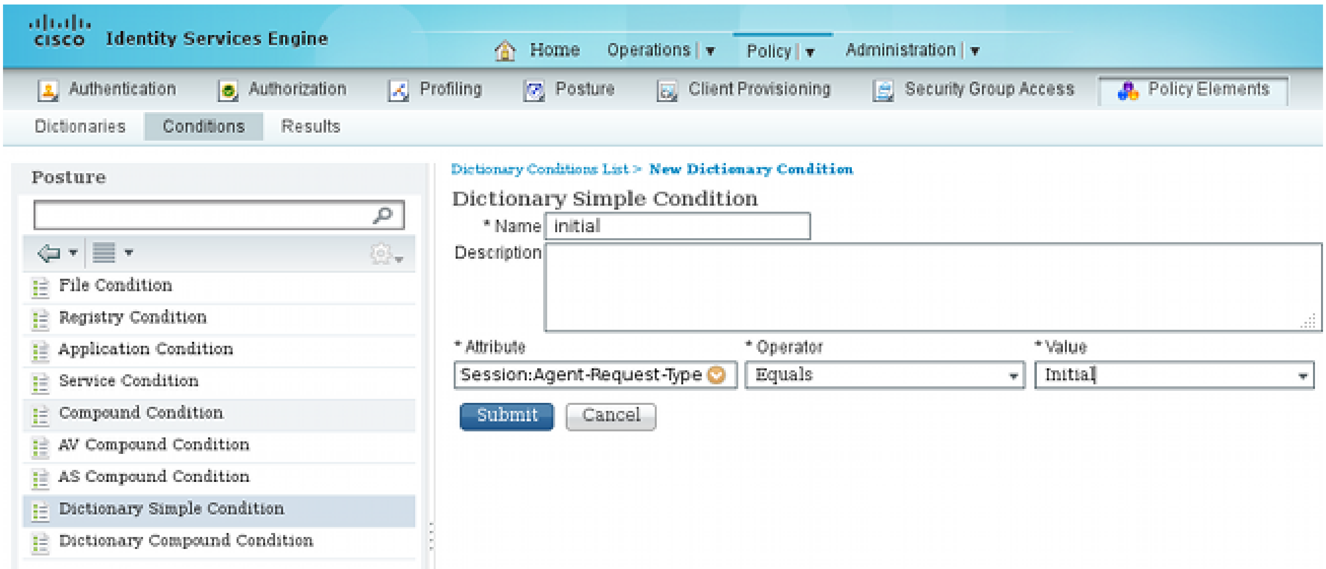
Dictionary Simple Condition

* Name: reassesment

Description:

* Attribute	* Operator	* Value
Session:Agent-Request-Type	Equals	Periodic Reassessment

3. 建立僅與初始評估匹配的類似條件：



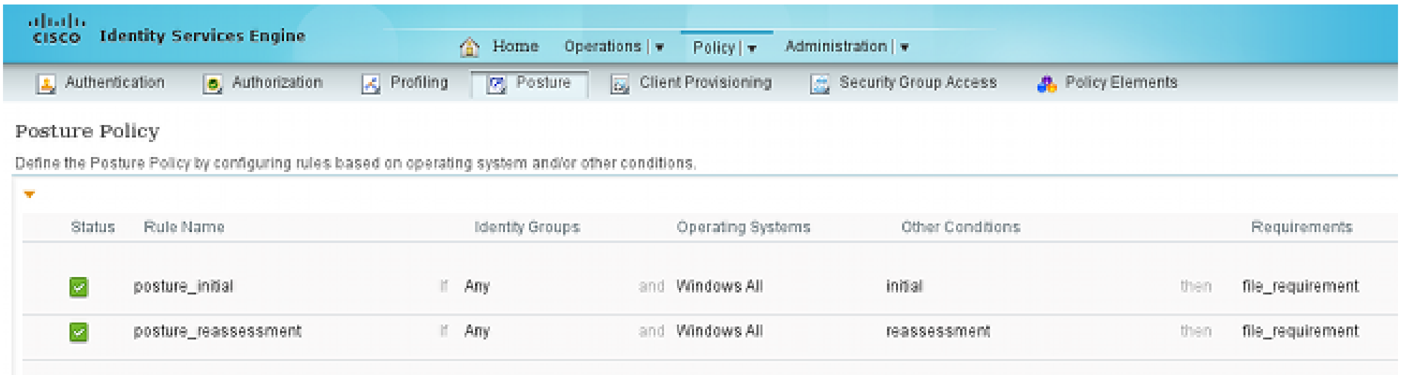
Dictionary Simple Condition

* Name: initial

Description:

* Attribute	* Operator	* Value
Session:Agent-Request-Type	Equals	Initial

這兩個條件都可以在狀態規則中使用。第一條 規則僅匹配初始評估，第二條規則匹配所有後續評估：



Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

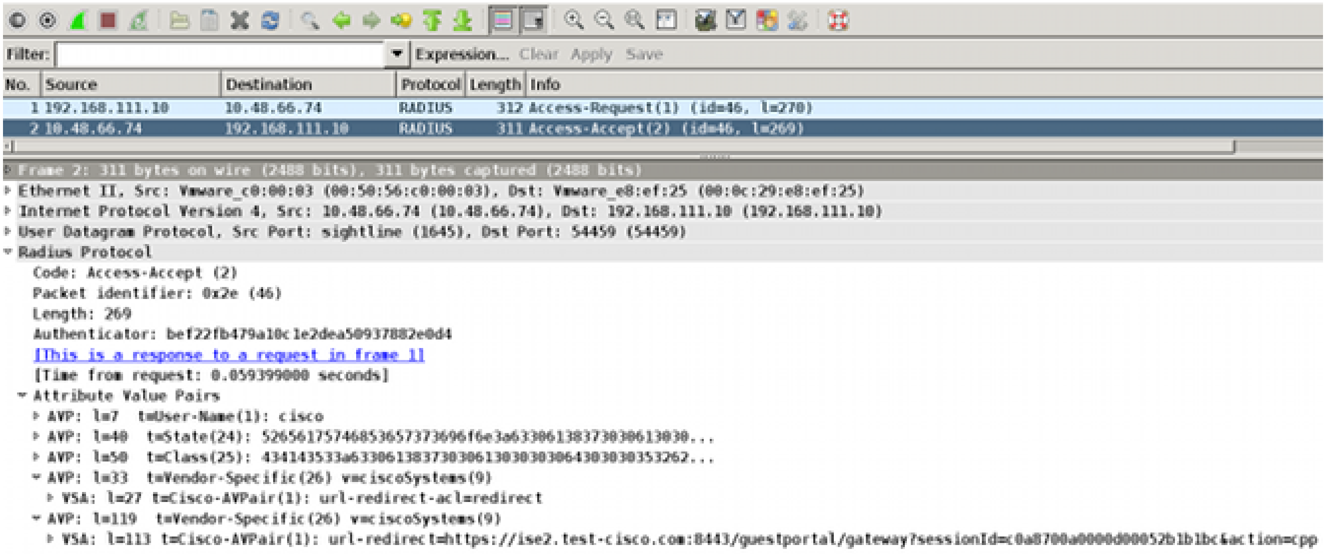
Status	Rule Name		Identity Groups		Operating Systems	Other Conditions		Requirements
✓	posture_initial	if	Any	and	Windows All	initial	then	file_requirement
✓	posture_reassessment	if	Any	and	Windows All	reassessment	then	file_requirement

驗證

若要確認您的組態是否正常運作，請確保已按說明完成以下步驟：

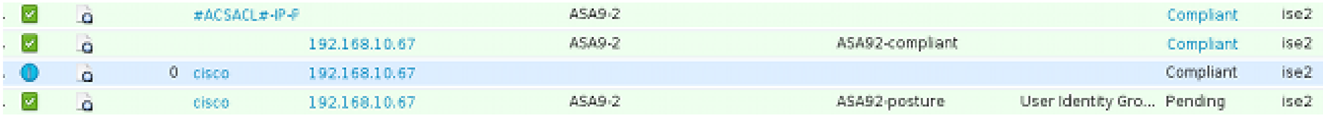
1. VPN使用者連線到ASA。

2. ASA傳送RADIUS請求並接收具有**url-redirect**和**url-redirect-acl**屬性的響應：



```
No. Source          Destination     Protocol Length Info
  1 192.168.111.10  10.48.66.74     RADIUS   312 Access-Request(1) (id=46, l=270)
  2 10.48.66.74     192.168.111.10  RADIUS   311 Access-Accept(2) (id=46, l=269)

▸ Frame 2: 311 bytes on wire (2488 bits), 311 bytes captured (2488 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: sightline (1645), Dst Port: 54459 (54459)
▾ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x2e (46)
    Length: 269
    Authenticator: bef22fb479a10c1e2dea50937882e0d4
    [This is a response to a request in frame 1]
    [Time from request: 0.059399000 seconds]
  ▾ Attribute Value Pairs
    ▸ AVP: l=7  t=User-Name(1): cisco
    ▸ AVP: l=40  t=State(24): 52656175746853657373696f6e3a63306138373030613030...
    ▸ AVP: l=50  t=Class(25): 434143533a633061383730306130303030643030303353262...
    ▾ AVP: l=33  t=Vendor-Specific(26) v=ciscoSystems(9)
      ▸ VSA: l=27 t=Cisco-AVPair(1): url-redirect-acl=redirect
    ▾ AVP: l=119  t=Vendor-Specific(26) v=ciscoSystems(9)
      ▸ VSA: l=113 t=Cisco-AVPair(1): url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a0000d00052b1b1bc&action=cpp
```

3. ISE日誌指示授權與狀態配置檔案（第一個日誌條目）匹配：



☑			#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

4. ASA將重定向新增到VPN會話：

```
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
```

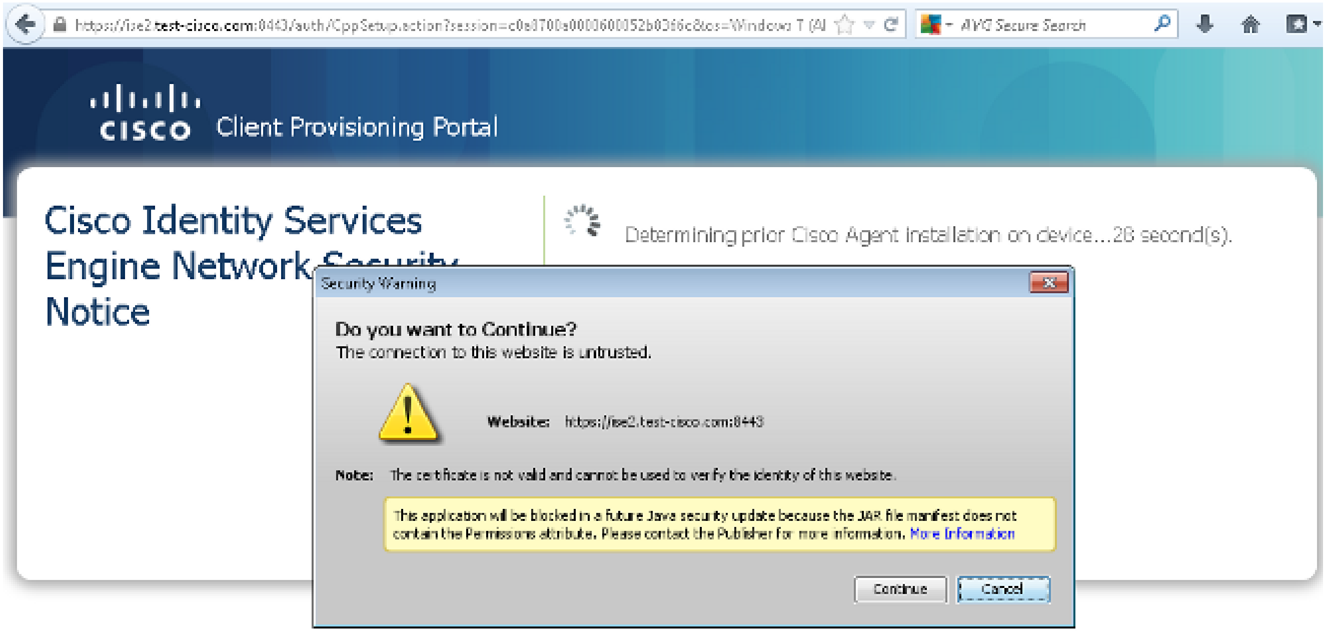
5. ASA上VPN會話的狀態顯示需要安全狀態並重定向HTTP流量：

```
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. 啟動與重定向ACL匹配的HTTP流量的客戶端重定向到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. 客戶端重定向到ISE以進行安全評估：


https://ise2.test-cisco.com:8443/auth/CppSetup.action?session=c0a8700a0000600052b0366c&os=Windows 7 (Al
AVG Secure Search
cisco
Client Provisioning Portal
Security Warning
Continue
Cancel

Cisco Identity Services Engine Network Security Notice

Determining prior Cisco Agent installation on device...28 second(s).

Do you want to Continue?

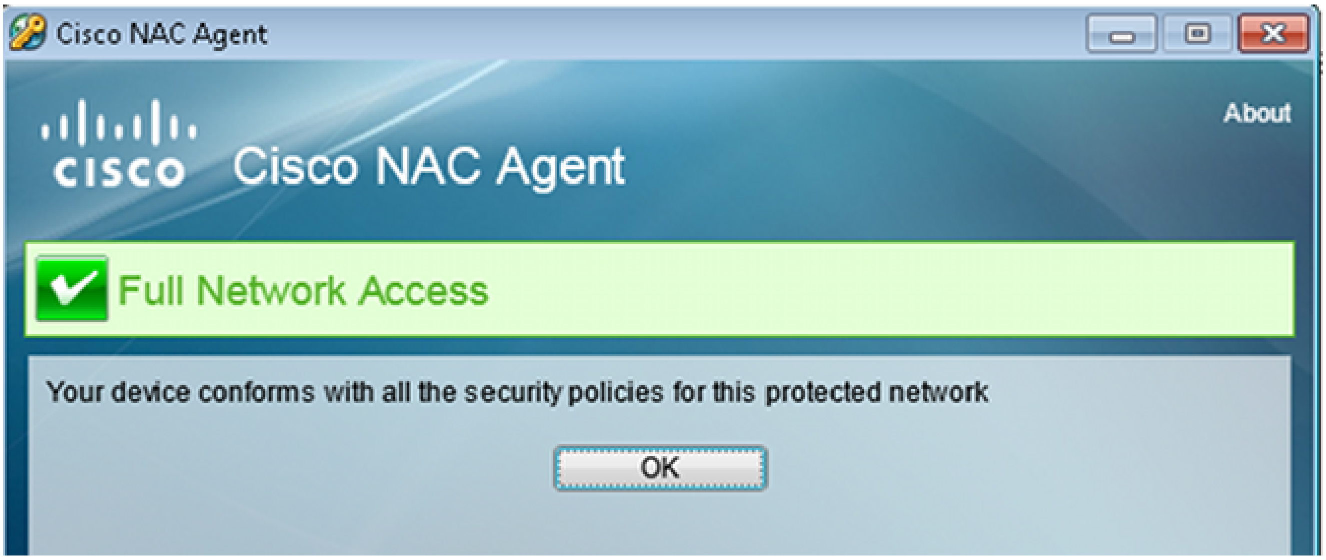
The connection to this website is untrusted.

Website: https://ise2.test-cisco.com:8443

Note: The certificate is not valid and cannot be used to verify the identity of this website.

This application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher for more information. More Information

8. 已安裝NAC代理。安裝NAC代理後，它將通過SWISS協定下載狀態規則並執行檢查以確定合規性。然後，將終端安全評估報告傳送到ISE。



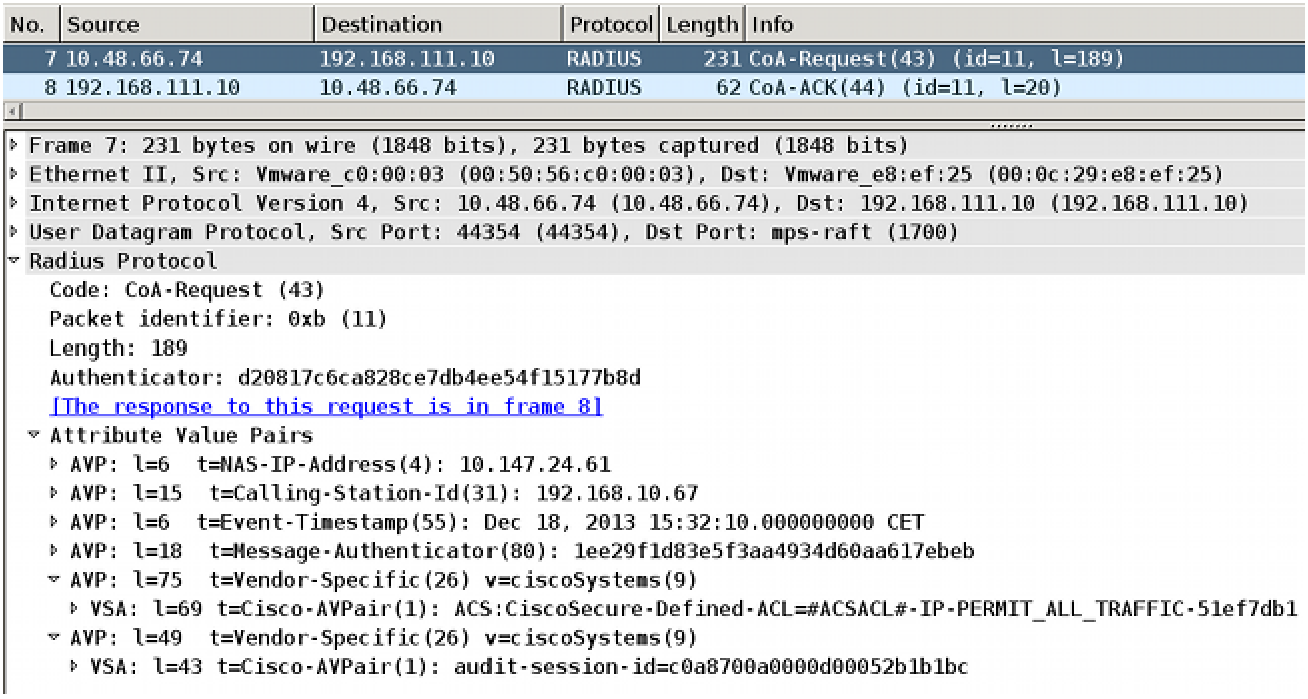
Full Network Access

Your device conforms with all the security policies for this protected network

9. ISE接收狀態報告，重新評估授權規則，並且（如果需要）更改授權狀態並傳送CoA。這可以在**ise-psc.log**中驗證：

```
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會傳送一個RADIUS CoA，其中包括**session_id**和允許完全存取的DACL名稱：



```
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)
▾ Radius Protocol
    Code: CoA-Request (43)
    Packet identifier: 0xb (11)
    Length: 189
    Authenticator: d20817c6ca828ce7db4ee54f15177b8d
    [The response to this request is in frame 8]
  ▾ 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
    ▾ 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
    ▾ AVP: l=49  t=Vendor-Specific(26) v=ciscoSystems(9)
      ▸ VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc
```

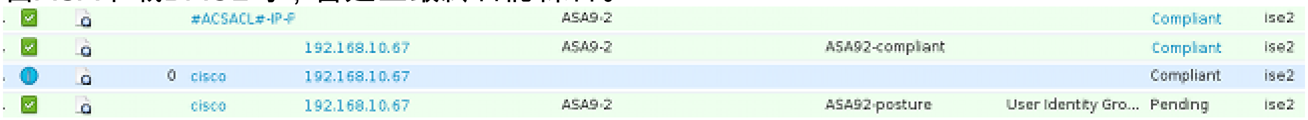
這反映在ISE日誌中：

第一個日誌條目用於返回狀態配置檔案（帶重定向）的初始身份驗證。

在收到符合的SWISS報告後，系統會填充第二個日誌條目。

第三個日誌條目在CoA傳送時與確認一起填充（描述為動態授權成功）。

當ASA下載DACL時，會建立最終日誌條目。



✓		#ACSACL#-IP-P		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上的調試顯示已接收CoA並刪除重定向。如果需要，ASA會下載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作業階段後，思科已為使用者套用DACL（完全存取許可權）：

```
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
```

注意：即使CoA未附加任何DACL，ASA始終刪除重定向規則。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

ISE上的調試

導覽至**Administration > Logging > Debug Log Configuration**以啟用調試。思科建議您為以下各項啟用臨時調試：

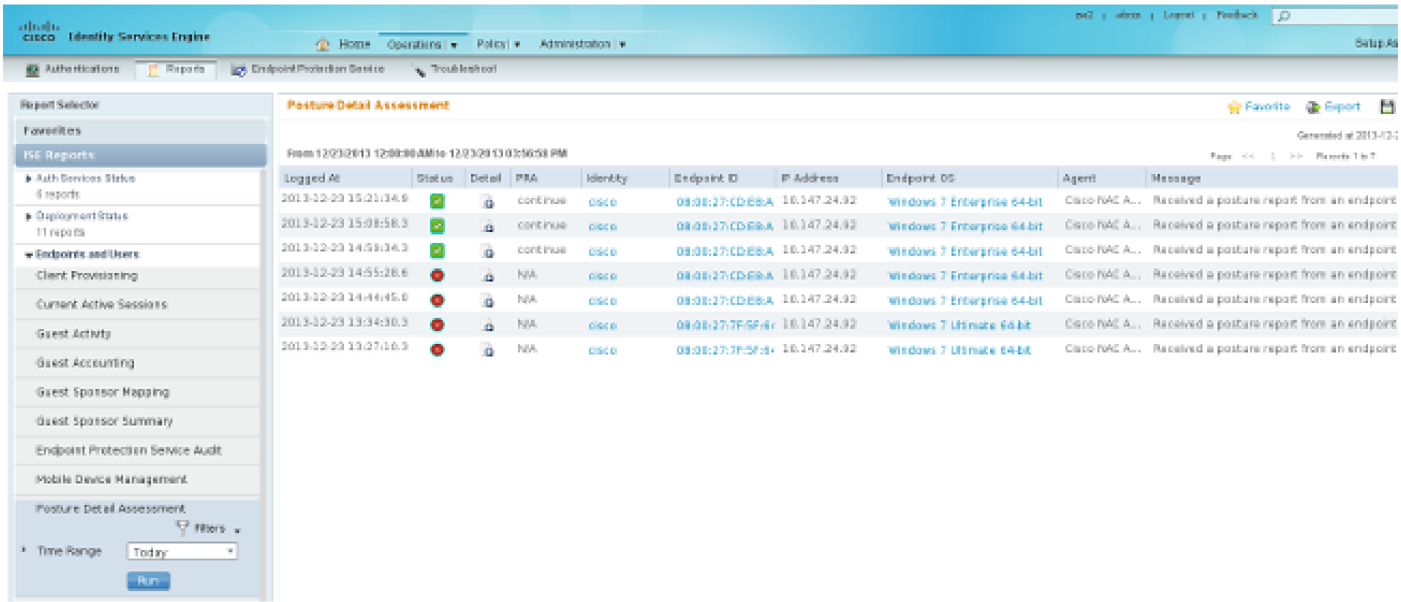
- 瑞士
- 不間斷轉發(NSF)
- NSF會話
- 提供

- 狀態

在CLI中輸入以下命令以檢視偵錯專案：

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

導航至**操作>報告> ISE報告>終端和使用者>終端安全評估詳細資訊評估**以檢視終端安全評估報告：



Posture Detail Assessment

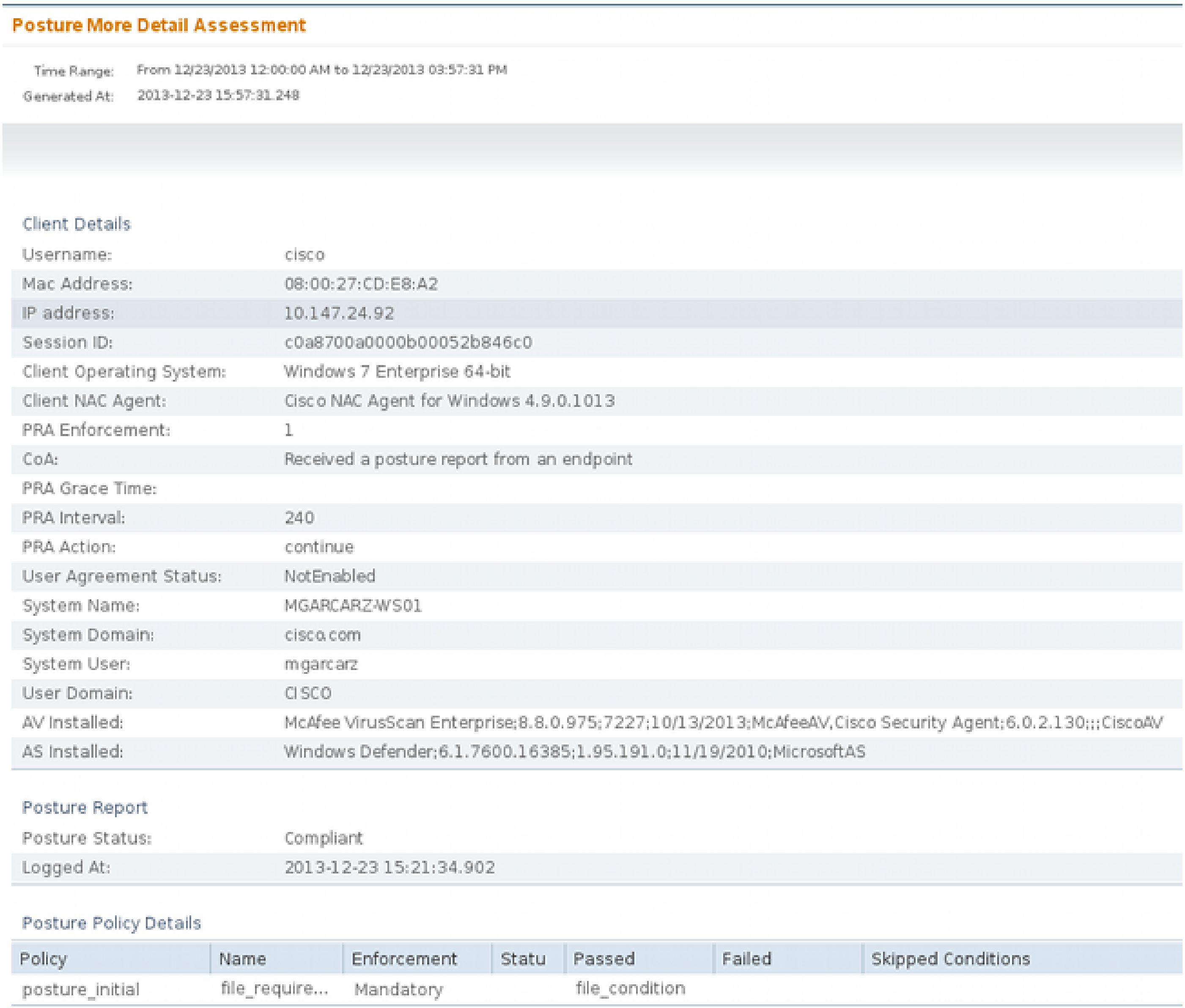
Generated at 2013-12-2

From 12/23/2013 12:00:00 AM to 12/23/2013 03:56:58 PM

Page 1 Records 1 to 7

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	✓		continue	cisco	08:00:27:CD:EB:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 15:08:58.3	✓		continue	cisco	08:00:27:CD:EB:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:59:34.3	✓		continue	cisco	08:00:27:CD:EB:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:55:28.6	●		N/A	cisco	08:00:27:CD:EB:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:44:45.0	●		N/A	cisco	08:00:27:CD:EB:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:34:30.3	●		N/A	cisco	08:00:27:7F:5F:6	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:27:10.3	●		N/A	cisco	08:00:27:7F:5F:6	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

在Posture More Detail Assessment頁面上，將顯示帶有需求名稱的策略名稱以及結果：



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:	CISCO
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		

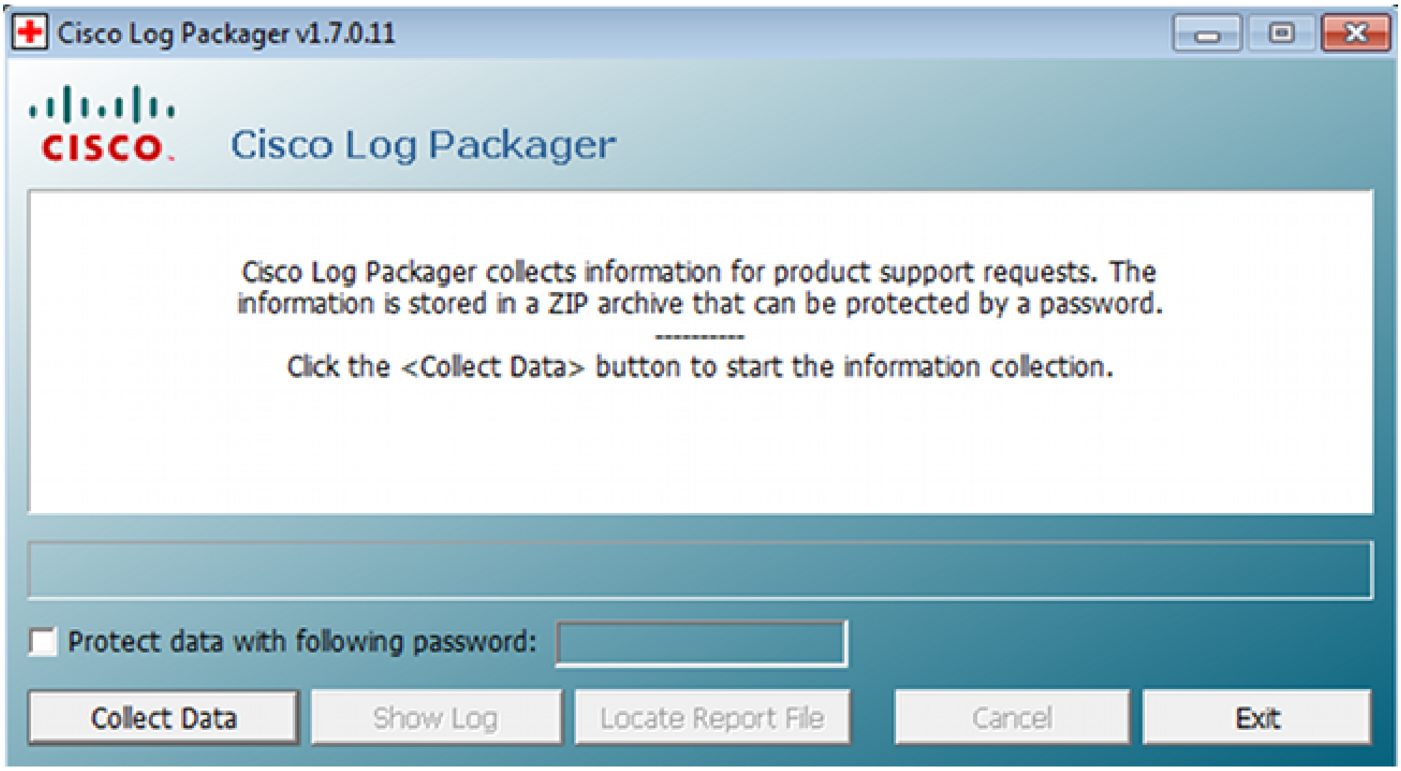
ASA上的調試

您可以在ASA上啟用這些調試：

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

代理的調試

對於NAC代理，可以使用從GUI啟動的Cisco日誌打包程式或使用CLI收集調試：CCAAgentLogPackager.app。



Cisco Log Packager collects information for product support requests. The information is stored in a ZIP archive that can be protected by a password.

Click the <Collect Data> button to start the information collection.

□ Protect data with following password:

提示：您可以使用技術援助中心(TAC)工具解碼結果。

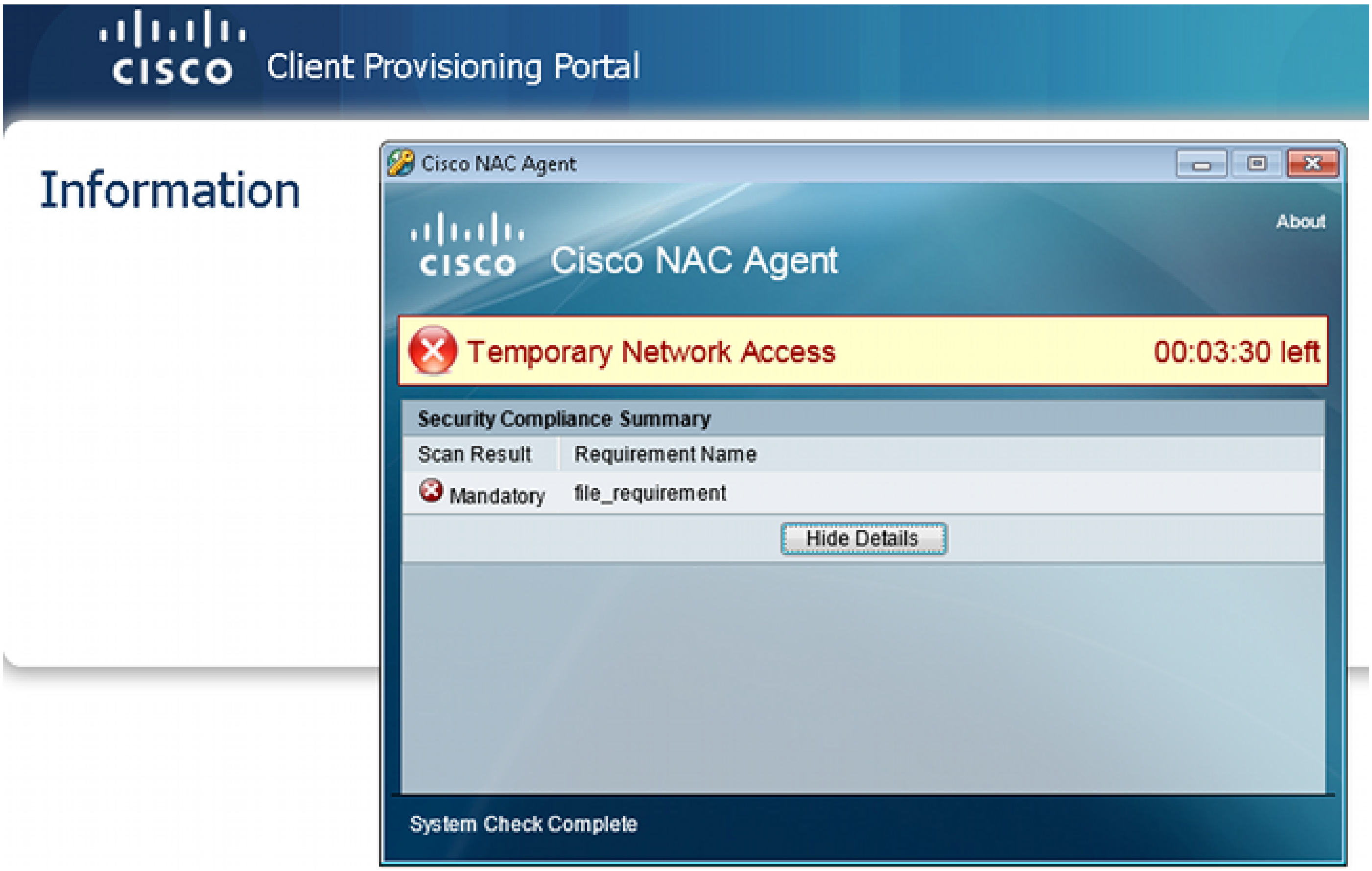
要檢索Web代理的日誌，請導航到以下位置：

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

注意：如果日誌不在這些位置，則驗證**TEMP Environment變**量。

NAC代理狀態故障

如果安全狀態失敗，則會向使用者顯示以下原因：



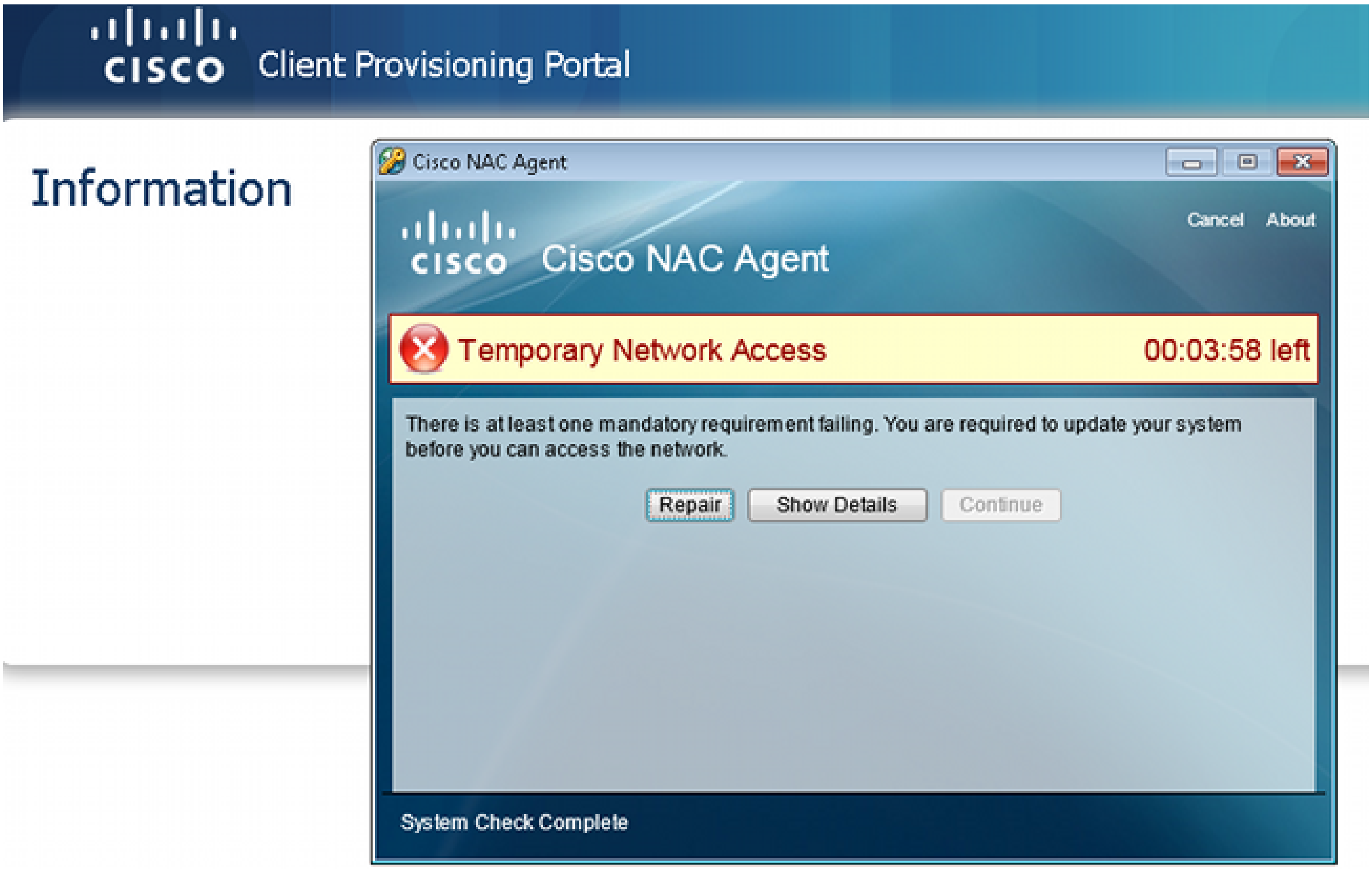
Temporary Network Access 00:03:30 left

Security Compliance Summary

Scan Result	Requirement Name
Mandatory	file_requirement

System Check Complete

如果配置了以下操作，則允許使用者採取補救操作：



Temporary Network Access 00:03:58 left

There is at least one mandatory requirement failing. You are required to update your system before you can access the network.

System Check Complete

相關資訊

- 配置外部伺服器以進行安全裝置使用者授權
- Cisco ASA系列VPN CLI配置指南9.1
- 思科身份服務引擎使用手冊，版本1.2
- 技術支援與文件 - Cisco Systems

關於此翻譯