

# Configurazione della postura della VPN ASA con ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete e flusso del traffico](#)

[Configurazioni](#)

[ASA](#)

[ISE](#)

[Rivalutazione periodica](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Debug sull'ISE](#)

[Debug dell'appliance ASA](#)

[Debug per l'agente](#)

[Errore di postura dell'agente NAC](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare l'ASA in modo che metta in postura gli utenti VPN rispetto all'ISE.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione di ASA CLI e della configurazione VPN SSL (Secure Sockets Layer)
- Conoscenze base della configurazione VPN di accesso remoto sull'appliance ASA
- Conoscenze base di ISE e servizi di postura

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA versione 9.16 e successive
- Microsoft Windows versione 7 con Cisco AnyConnect Secure Mobility Client versione 4.10
- Cisco ISE versione 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

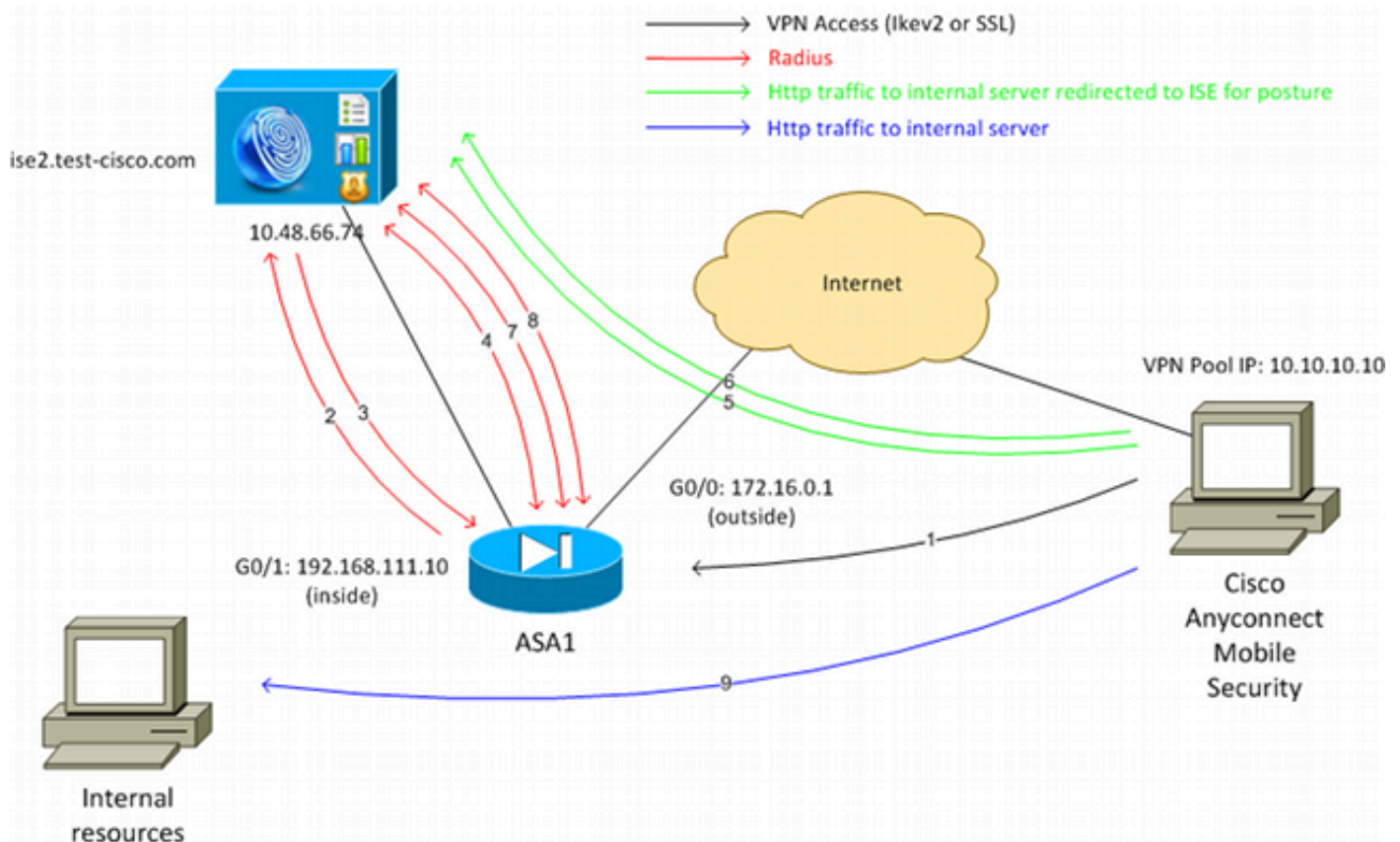
## Premesse

Cisco ASA versione 9.16 supporta Cambio di autorizzazione (CoA) RADIUS (RFC 5176). Ciò consente di posizionare gli utenti VPN rispetto a Cisco ISE. Dopo che un utente VPN ha eseguito l'accesso, l'ASA reindirizza il traffico Web all'ISE, dove all'utente viene assegnato un agente Network Admission Control (NAC) o un agente Web. L'agente esegue controlli specifici sul computer dell'utente per determinarne la conformità rispetto a un set configurato di regole di postura, quali sistema operativo (OS), patch, antivirus, di servizio, di applicazione o di registro.

I risultati della convalida della postura vengono quindi inviati all'ISE. Se il computer viene ritenuto conforme, l'ISE può inviare una richiesta RADIUS CoA all'appliance ASA con i nuovi criteri di autorizzazione. Dopo la convalida della postura e la verifica di autenticità (CoA), all'utente viene consentito l'accesso alle risorse interne.


## Configurazione

### Esempio di rete e flusso del traffico



Di seguito è riportato il flusso del traffico, come mostrato nello schema della rete:

1. L'utente remoto utilizza Cisco Anyconnect per l'accesso VPN all'appliance ASA.
2. L'ASA invia una richiesta di accesso RADIUS per l'utente all'ISE.
3. Questa richiesta è conforme alla policy denominata ASA916-posture per ISE. Di conseguenza, viene restituito il profilo di autorizzazione ASA916-postura. L'ISE invia un messaggio RADIUS Access-Accept con due coppie attributo-valore Cisco:
  - url-redirect-acl=redirect: il nome dell'elenco di controllo di accesso (ACL) definito localmente sull'appliance ASA e che determina il traffico che deve essere reindirizzato.
  - url-redirect: URL a cui l'utente remoto deve essere reindirizzato.

 **Suggerimento:** i server DNS (Domain Name System) assegnati ai client VPN devono essere in grado di risolvere il nome di dominio completo restituito nell'URL di reindirizzamento. Se i filtri VPN sono configurati in modo da limitare l'accesso a livello di gruppo di tunnel, verificare che il pool di client sia in grado di accedere al server ISE sulla porta configurata (in questo esempio, TCP 8443).

4. L'appliance ASA invia un pacchetto di avvio richiesta di accounting RADIUS e riceve una risposta. Questa operazione è necessaria per inviare tutti i dettagli relativi alla sessione all'ISE. Questi dettagli includono session\_id, l'indirizzo IP esterno del client VPN e l'indirizzo IP dell'appliance ASA. Per identificare la sessione, ISE utilizza il valore session\_id. L'ASA

invia anche informazioni periodiche sull'account provvisorio, in cui l'attributo più importante è l'indirizzo IP con frame che corrisponde all'indirizzo IP assegnato al client dall'ASA (nell'esempio, 10.10.10.10).

5. Quando il traffico proveniente dall'utente VPN corrisponde all'ACL (reindirizzamento) definito localmente. A seconda della configurazione, ISE esegue il provisioning dell'agente NAC o dell'agente Web.
6. Dopo l'installazione dell'agente sul computer client, esegue automaticamente controlli specifici. In questo esempio viene eseguita la ricerca del file c:\test.txt. Inoltre, invia un report sulla postura all'ISE, che può includere scambi multipli con l'uso del protocollo SWISS e delle porte TCP/UDP 8905 per accedere all'ISE.
7. Quando l'ISE riceve il report sulla postura dall'agente, elabora nuovamente le regole di autorizzazione. Questa volta, il risultato della postura è noto e un'altra regola viene trovata. Invia un pacchetto CoA RADIUS:
  - Se l'utente è conforme, viene inviato un nome DACL (Downloadable ACL) che consente l'accesso completo (regola AuthZ conforme a ASA916).
  - Se l'utente non è conforme, viene inviato un nome DACL che consente l'accesso limitato (regola AuthZ non conforme a ASA916).



Nota: il valore di RADIUS CoA è sempre confermato, ossia l'ASA invia una risposta all'ISE per confermare.

---

8. L'appliance ASA rimuove il reindirizzamento. Se i DACL non sono memorizzati nella cache, deve inviare una richiesta di accesso per scaricarli dall'ISE. Il DACL specifico viene collegato alla sessione VPN.
9. Al successivo tentativo di accesso alla pagina Web, l'utente VPN può accedere a tutte le risorse consentite dal DACL installato sull'appliance ASA.  
Se l'utente non è conforme, viene concesso solo un accesso limitato.



Nota: questo modello di flusso è diverso dalla maggior parte degli scenari che utilizzano RADIUS CoA. Per le autenticazioni 802.1x cablate/wireless, RADIUS CoA non include attributi. Viene attivata solo la seconda autenticazione a cui sono associati tutti gli attributi, ad esempio DACL. Per la postura della VPN ASA, non è disponibile una seconda autenticazione. Tutti gli attributi vengono restituiti nel CoA RADIUS. La sessione VPN è attiva e non è possibile modificare la maggior parte delle impostazioni utente VPN.

---

## Configurazioni

Per configurare l'ASA e l'ISE, consultare questa sezione.

## ASA

Di seguito è riportata la configurazione ASA base per l'accesso Cisco AnyConnect:

```
<#root>

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 162.168.111.10 255.255.255.0

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

key cisco

webvpn
    enable outside

anyconnect image disk0:/anyconnect-win-arm64-4.10.06079-webdeploy-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

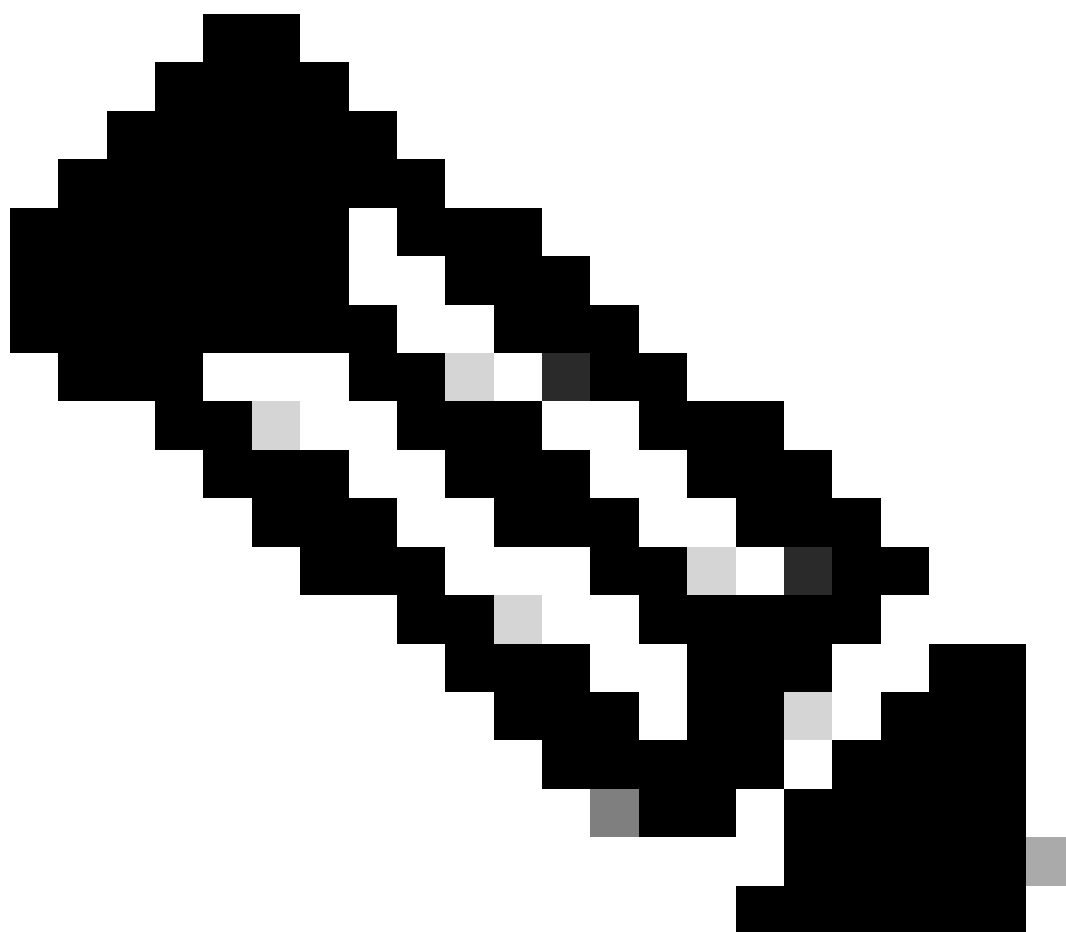
tunnel-group RA type remote-access
tunnel-group RA general-attributes
    address-pool POOL
    authentication-server-group ISE
    default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
    group-alias RA enable
```

Per l'integrazione dell'ASA con la postura ISE, accertarsi di:

- Configurare il server di autenticazione, autorizzazione e accounting (AAA) per

l'autorizzazione dinamica in modo da accettare il processo CoA.

- Configurare l'accounting come gruppo di tunnel per inviare i dettagli della sessione VPN all'ISE.
  - Configurare l'accounting provvisorio che invia l'indirizzo IP assegnato all'utente e aggiornare periodicamente lo stato della sessione su ISE
  - Configurare l'ACL di reindirizzamento, che decide se il DNS e il traffico ISE sono consentiti. Tutto il resto del traffico HTTP viene reindirizzato all'ISE per la postura.
- 



Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti Cisco interni.

---

Di seguito è riportato l'esempio di configurazione:

<#root>

```
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
```

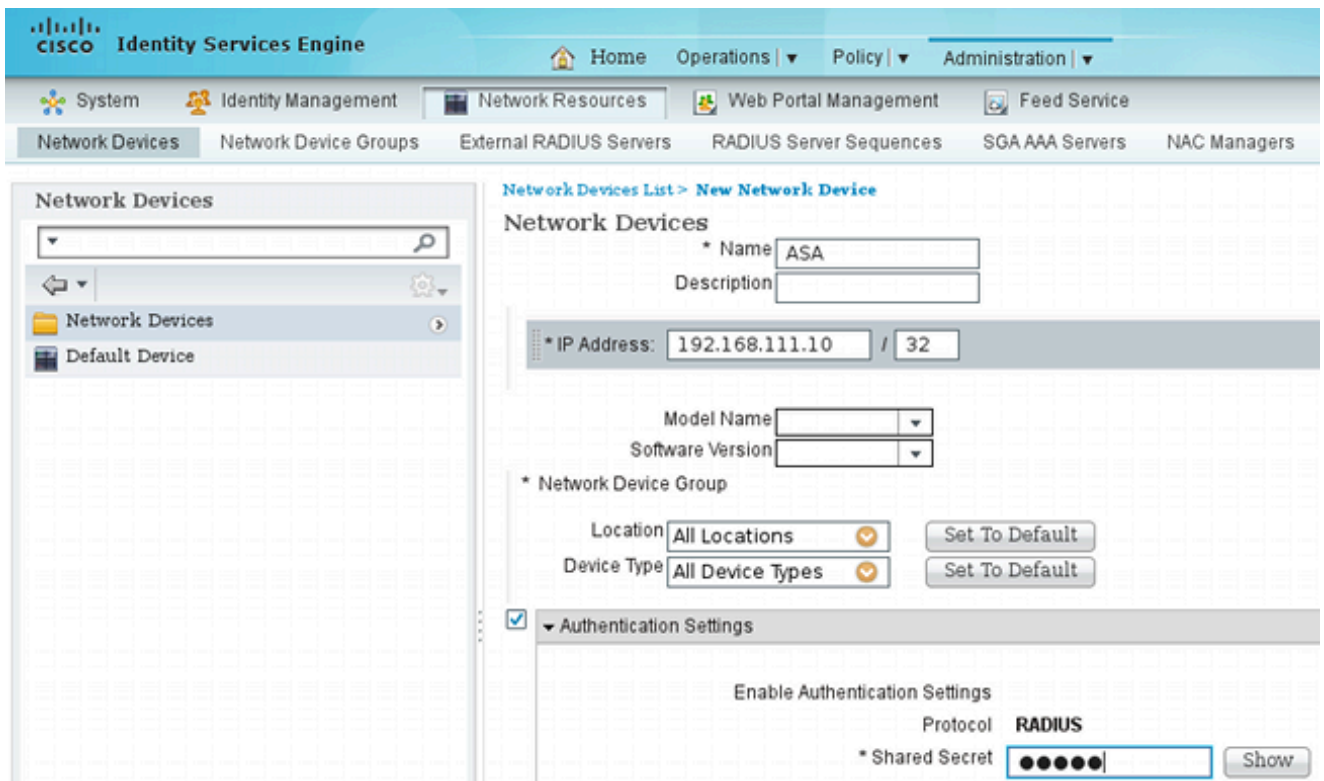
### Modalità accounting ASA:

La modalità di accounting sull'appliance ASA deve essere singola (predefinita). In caso contrario, l'appliance ASA non è in grado di elaborare correttamente le sessioni ISE; in altre parole, l'appliance ASA rifiuta la richiesta CoA con l'opzione "Azione non supportata".

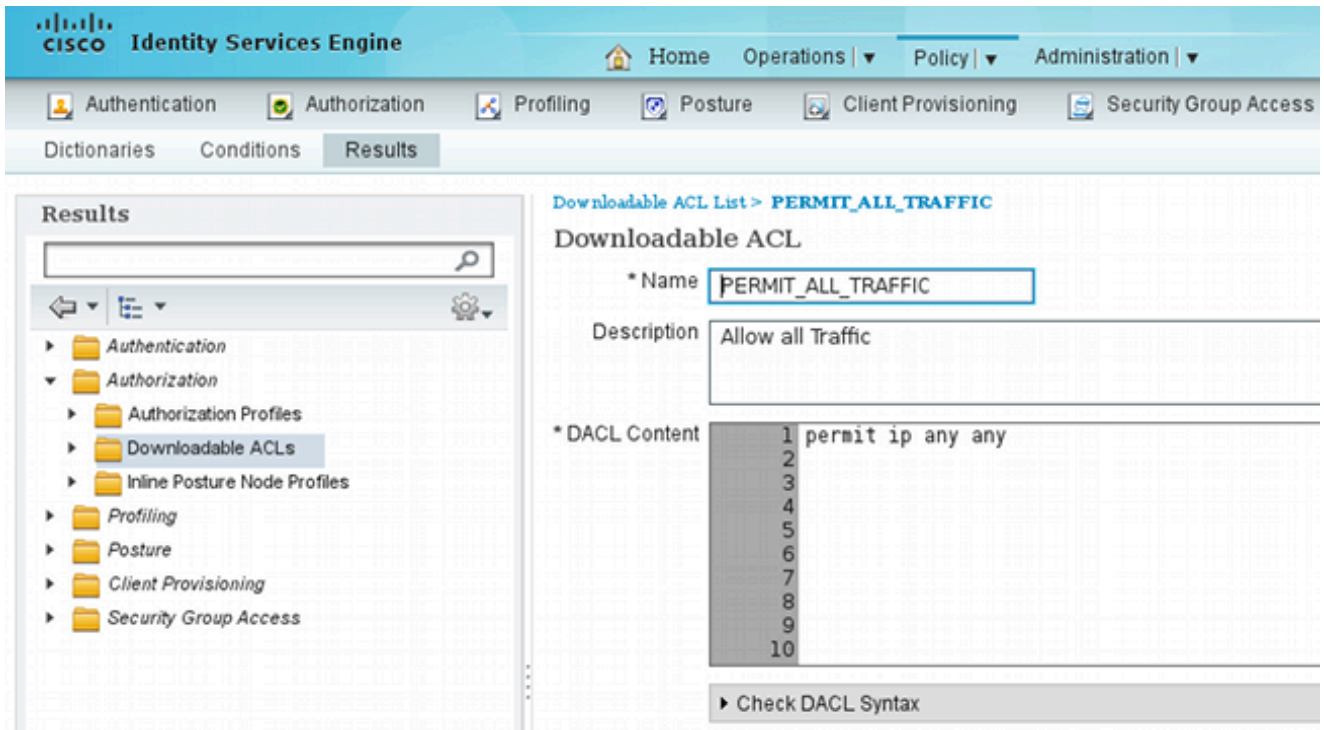
### ISE

Per configurare l'ISE, completare la procedura seguente:

1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete e aggiungere l'appliance ASA come dispositivo di rete:



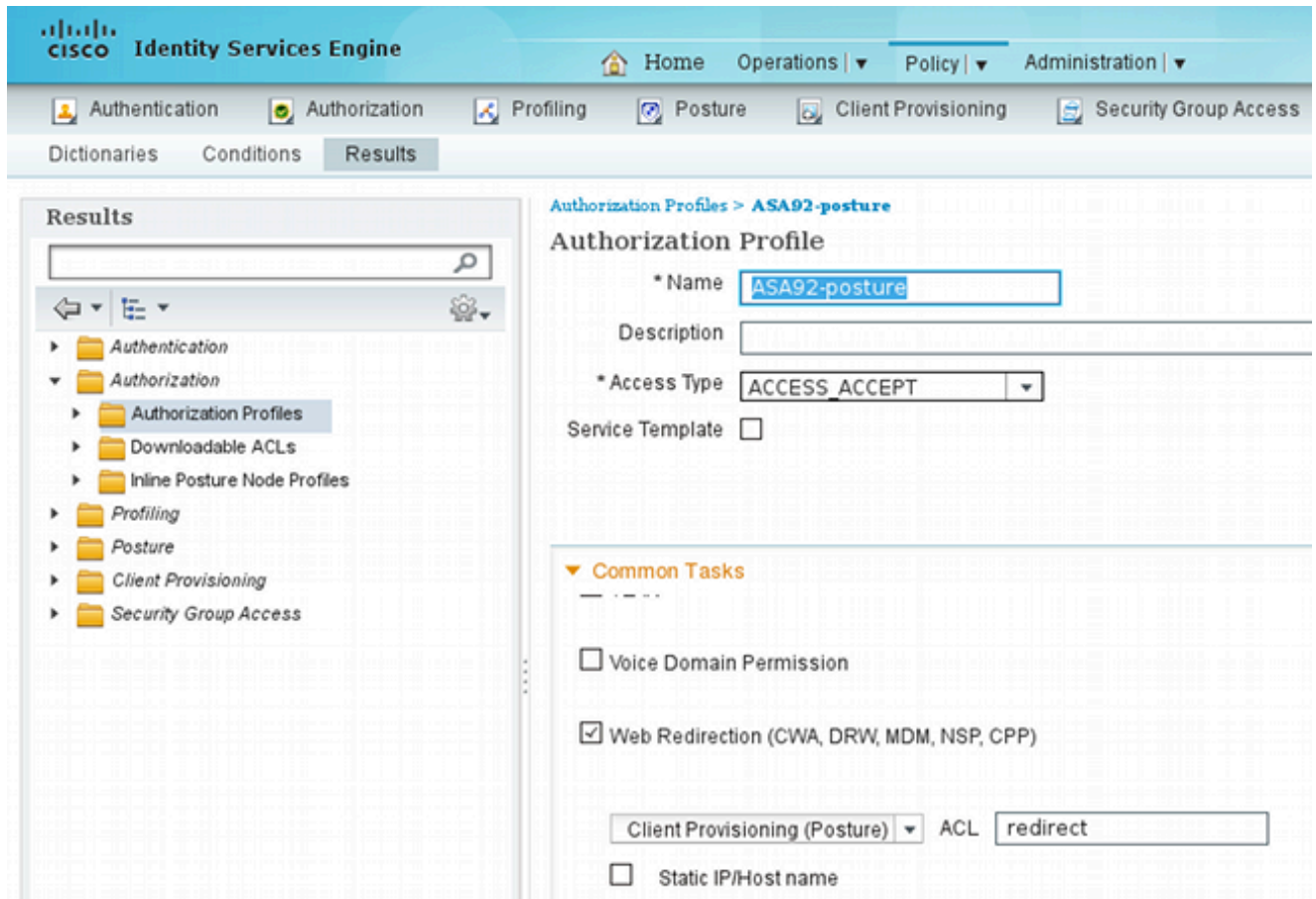
2. Selezionare Policy > Results > Authorization > Downloadable ACL (Criterio > Risultati > Autorizzazione > ACL scaricabile) e configurare l'elenco DACL in modo che consenta l'accesso completo. La configurazione ACL predefinita permette tutto il traffico IP sull'ISE:



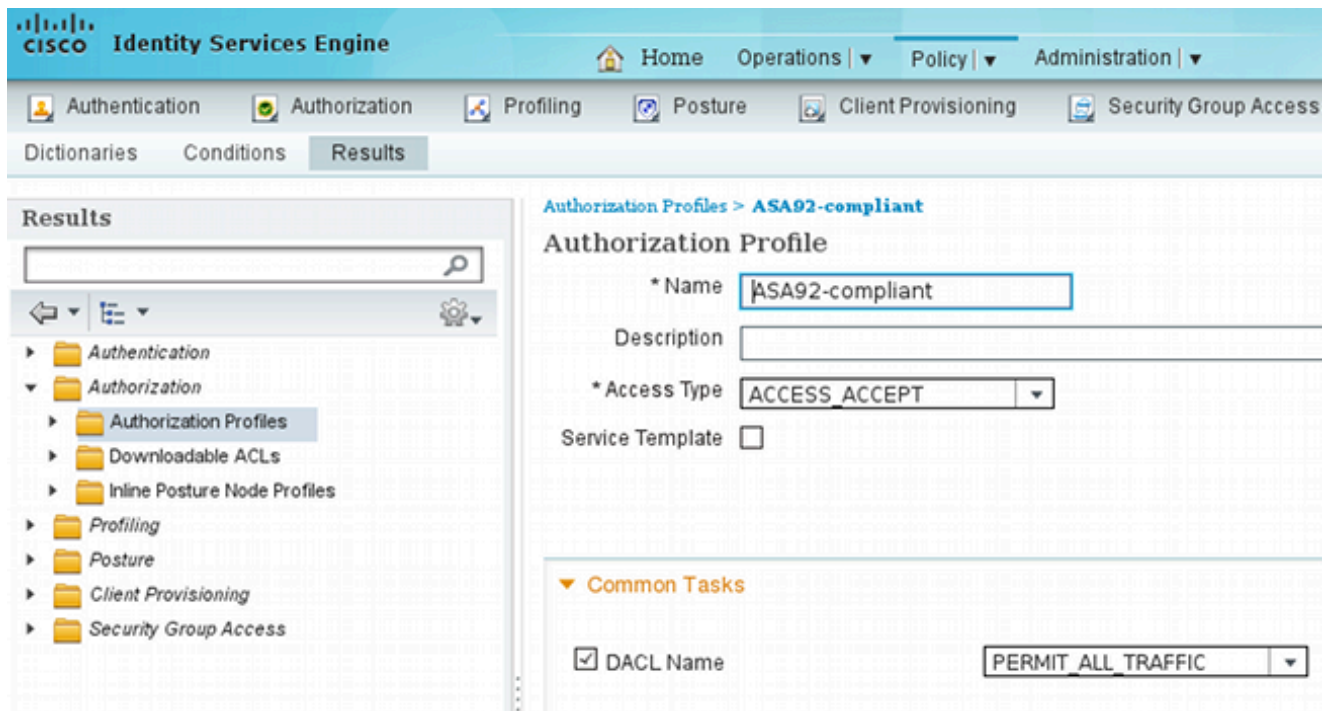
3. Configurare un ACL simile che fornisca accesso limitato (per utenti non conformi).
4. Selezionare Policy > Results > Authorization > Authorization Profiles (Criteri > Risultati > Autorizzazione > Profili di autorizzazione) e configurare il profilo di autorizzazione



denominato ASA92-posture, che reindirizza gli utenti alla postura. Selezionare la casella di controllo Web Redirection, selezionare Client Provisioning dall'elenco a discesa e verificare che il comando redirect venga visualizzato nel campo ACL (l'ACL è definito localmente sull'appliance ASA):



5. Configurare il profilo di autorizzazione conforme ad ASA92, che deve restituire solo il DACL denominato PERMIT\_ALL\_TRAFFIC che fornisce l'accesso completo agli utenti conformi:



6. Configurare un profilo di autorizzazione simile denominato ASA916 non conforme che deve restituire il DACL con accesso limitato (per gli utenti non conformi).

7. Passare a Criterio > Autorizzazione e configurare le regole di autorizzazione:

- Create una regola che consenta l'accesso completo se i risultati della postura sono conformi. Il risultato è il criterio di autorizzazione conforme a ASA916.
- Create una regola che consenta un accesso limitato se i risultati della postura non sono conformi. Il risultato è il criterio di autorizzazione non conforme ad ASA916.
- Se non viene trovata alcuna delle due regole precedenti, la regola predefinita restituisce la postura ASA916-16, che forza il reindirizzamento sull'appliance ASA.

✓	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. Le regole di autenticazione predefinite controllano il nome utente nell'archivio identità interno. Se è necessario modificare questa impostazione, ad esempio archiviata in Active Directory, passare a Criteri > Autenticazione e apportare la modifica:

**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	

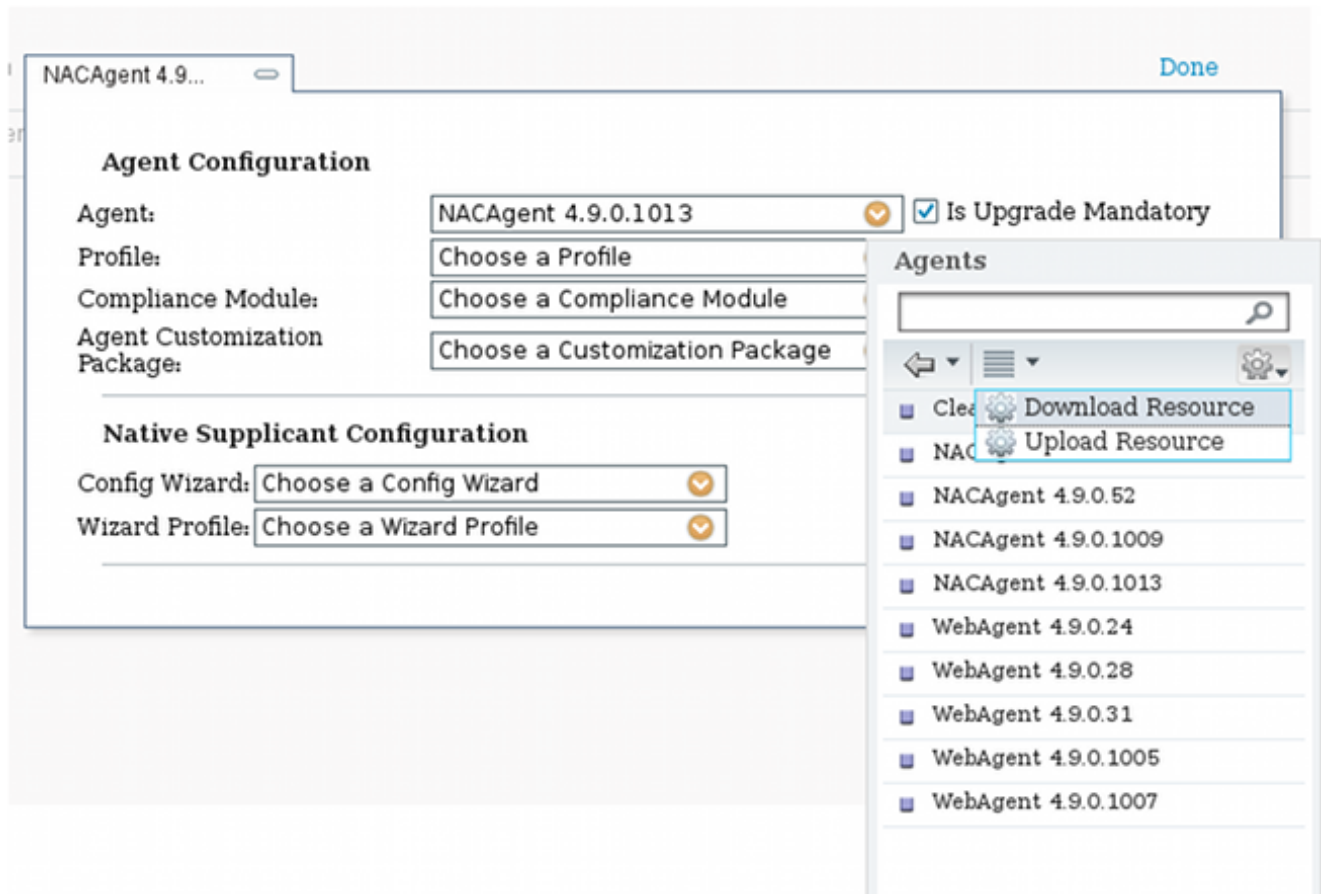
9. Passare a Policy > Client Provisioning e configurare le regole di provisioning. Queste sono le regole che determinano il tipo di agente da attivare. Nell'esempio, esiste una sola regola semplice e ISE seleziona l'agente NAC per tutti i sistemi Microsoft Windows:

**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

Quando gli agenti non sono sull'ISE, è possibile scaricarli:



10. Se necessario, è possibile selezionare Amministrazione > Sistema > Impostazioni > Proxy e configurare il proxy per ISE (per accedere a Internet).

11. Configurare le regole di postura, che verificano la configurazione del client. È possibile configurare le regole che controllano:

- file - esistenza, versione, data
- Registro di sistema - chiave, valore, esistenza
- applicazione - nome processo, in esecuzione, non in esecuzione
- servizio - nome servizio, in esecuzione, non in esecuzione
- antivirus - oltre 100 fornitori supportati, versione, quando vengono aggiornate le definizioni
- antispyware - oltre 100 fornitori supportati, versione, quando vengono aggiornate le definizioni
- condizione composta - miscela di tutti
  - condizioni del dizionario personalizzato - uso della maggior parte dei dizionari ISE

12. In questo esempio, viene eseguita solo una semplice verifica dell'esistenza dei file. Se il file

c:\test.txt è presente nel computer client, è conforme e dispone dell'accesso completo. Passare a Criterio > Condizioni > Condizioni file e configurare la condizione del file:

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Posture' section is active, and the 'File Condition' is selected in the left-hand menu. The main configuration area is titled 'File Condition List > file\_condition'. It contains the following fields:


- \* Name: file\_condition
- Description: (empty)
- \* File Path: ABSOLUTE\_PATH (dropdown), C:\test.txt (text input)
- \* File Type: FileExistence (dropdown)
- \* File Operator: Exists (dropdown)
- \* Operating System: Windows All (dropdown)

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

- Passare a Criterio > Risultati > Postura > Fabbisogni e creare un fabbisogno. Questa condizione deve essere soddisfatta quando è soddisfatta la condizione precedente. In caso contrario, viene eseguita l'azione di correzione. Possono essere disponibili molti tipi di azioni correttive, ma in questo esempio viene utilizzata la più semplice: viene visualizzato un messaggio specifico.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for 'Requirements'. The top navigation bar is the same as in the previous screenshot. The 'Results' section is active, and 'Requirements' is selected in the left-hand menu. The main area contains a table with the following columns: Name, Operating Systems, Conditions, and Remediation Actions.

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 AnyWDeRemediationWin
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 AnyASDeRemediationWin
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 AnyWDeRemediationMac
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

 Nota: in uno scenario normale, è possibile utilizzare l'azione Correzione file (ISE fornisce il file scaricabile).

- Passare a Criterio > Postura e utilizzare il requisito creato nel passo precedente (denominato file\_requirements) nelle regole di postura. L'unica regola di postura richiede che tutti i sistemi Microsoft Windows soddisfino il requisito\_file. Se questo requisito è soddisfatto, la stazione è conforme; se non lo è, la stazione non è conforme.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below this, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main content area is titled "Posture Policy" and contains a table with the following data:

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	posture	If Any	and Windows All		then file_requirement

## Rivalutazione periodica

Per impostazione predefinita, la postura è un evento singolo. Tuttavia, talvolta è necessario verificare periodicamente la conformità degli utenti e regolare l'accesso alle risorse in base ai risultati. Queste informazioni vengono inviate tramite il protocollo SWISS (agente NAC) o codificate nell'applicazione (agente Web).

Per verificare la conformità degli utenti, completare i seguenti passaggi:

1. Passare a Amministrazione > Impostazioni > Postura > Rivalutazioni e abilitare la rivalutazione a livello globale (per configurazione gruppo di identità):

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Reassessment. The left sidebar shows the navigation menu with "Settings" expanded to "Posture" > "Reassessments". The main content area is titled "Reassessment Configuration" and contains the following fields and options:

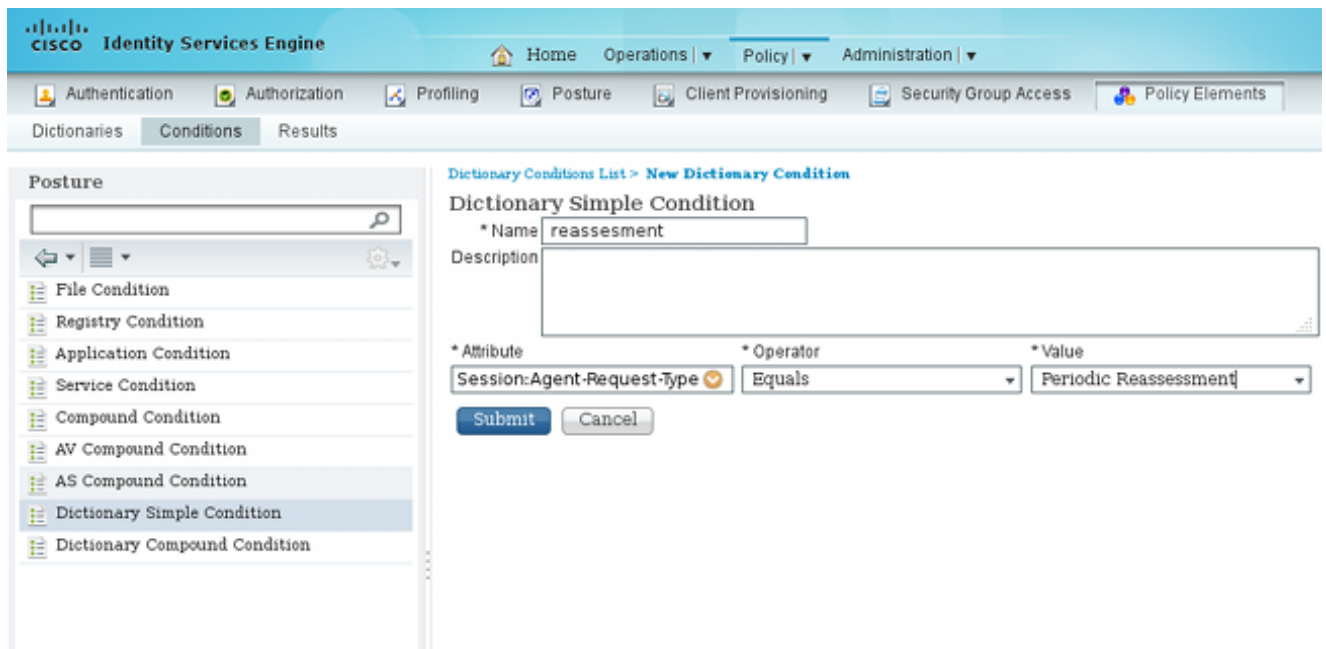
- \* Configuration Name:
- Configuration Description:
- Use Reassessment Enforcement?
- Enforcement Type:
- Interval:  minutes
- Grace Time:  minutes
- Group Selection Rules:

Below the configuration fields, there are four numbered instructions:

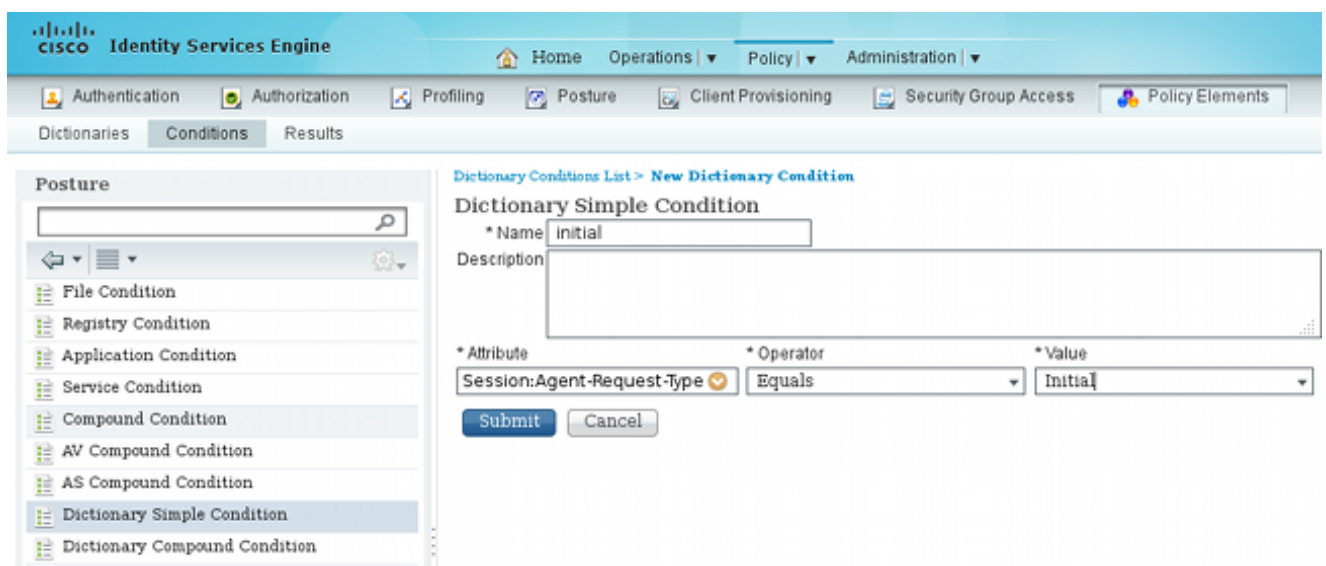
1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
  - i. the existing config with a group of 'Any' is updated to reflect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

2. Creare una condizione di postura che corrisponda a tutte le rivalutazioni:





3. Creare una condizione simile che corrisponda solo alle valutazioni iniziali:



Entrambe queste condizioni possono essere utilizzate nelle regole di postura. La prima regola corrisponde solo alle valutazioni iniziali e la seconda corrisponde a tutte le valutazioni successive:

Posture Policy

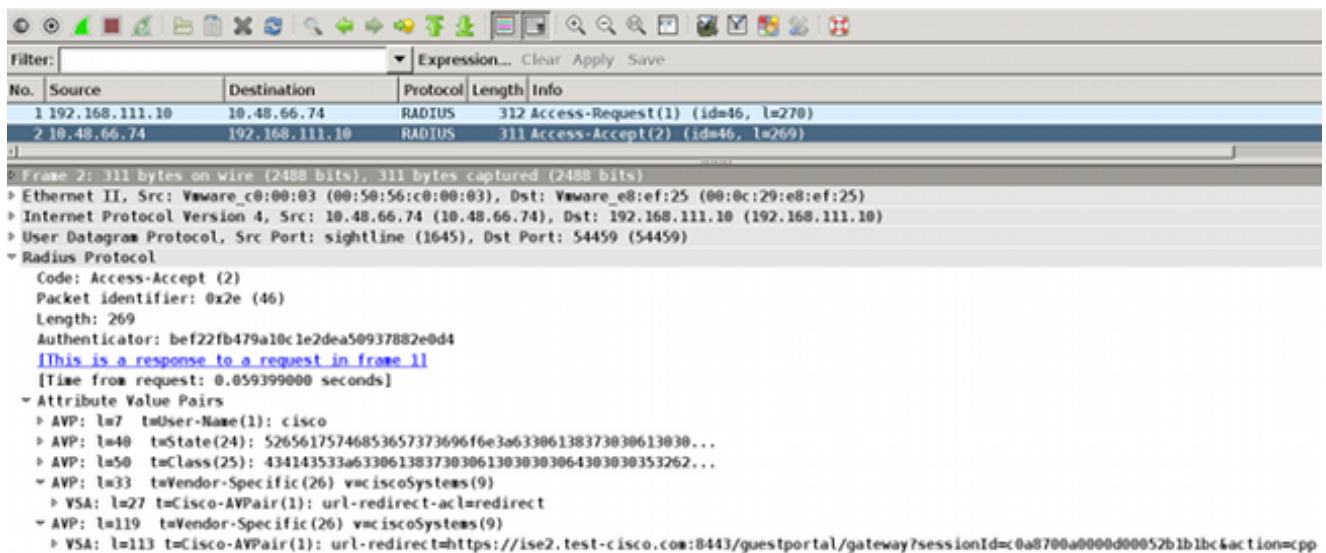
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	posture_initial	If Any	and Windows All	initial	then file_requirement
<input checked="" type="checkbox"/>	posture_reassessment	If Any	and Windows All	reassessment	then file_requirement

# Verifica

Per verificare che la configurazione funzioni correttamente, attenersi alla seguente procedura:

1. L'utente VPN si connette all'ASA.
2. L'appliance ASA invia una richiesta RADIUS e riceve una risposta con gli attributi url-redirect e url-redirect-acl:



3. I log ISE indicano che l'autorizzazione corrisponde al profilo di postura (la prima voce):

✓	🔒	#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. L'ASA aggiunge un reindirizzamento alla sessione VPN:

```
<#root>
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. Lo stato della sessione VPN sull'appliance ASA mostra che la postura è richiesta e reindirizza il traffico HTTP:

```
<#root>
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 : 16497  
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. Il client che avvia il traffico HTTP che corrisponde all'ACL di reindirizzamento viene reindirizzato all'ISE:

```
<#root>
```

```
aaa_url_redirect: Created proxy for 10.10.10.10
```

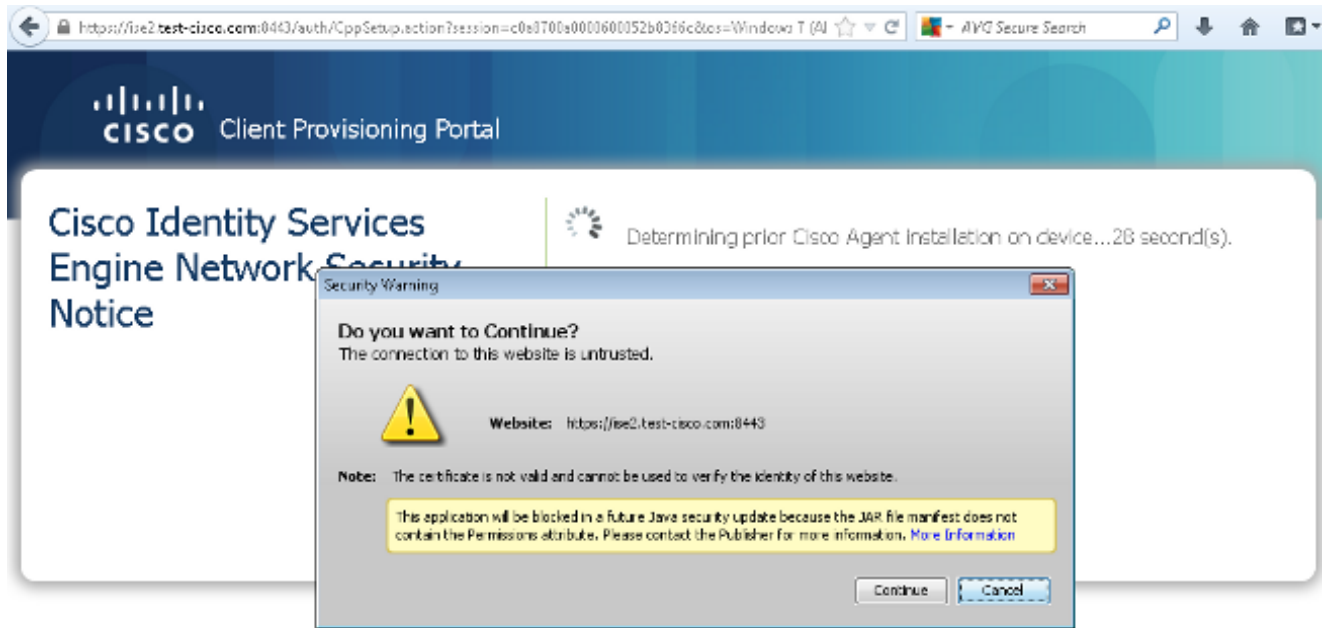
```
aaa_url_redirect:
```

```
sending url redirect
```

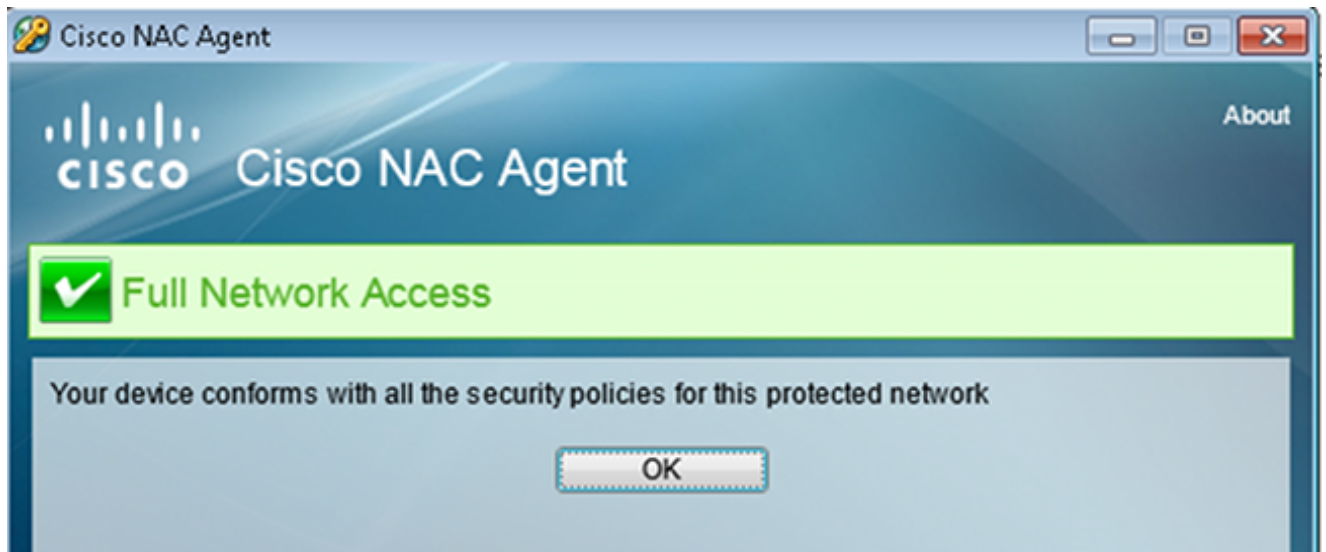
```
:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for
```

```
10.10.10.10
```

7. Il client viene reindirizzato all'ISE per la postura:



8. L'agente NAC è installato. Una volta installato, l'agente NAC scarica le regole di postura tramite il protocollo SWISS ed esegue dei controlli per determinare la conformità. Il report sulla postura viene quindi inviato all'ISE.



9. L'ISE riceve il report sulla postura, rivaluta le regole di autorizzazione e, se necessario, modifica lo stato di autorizzazione e invia un CoA. È possibile verificare questa condizione nel file ise-psc.log:

```
<#root>
```

```
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco:c0a8700a0000900052b840e6  
:::-
```

```
Decrypting report
```

```

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- U

ser 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. L'ISE invia una richiesta RADIUS CoA che include il valore session\_id e il nome DACL che consente l'accesso completo:

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

```

Ciò si riflette nei log ISE:

- La prima voce di log è per l'autenticazione iniziale che restituisce il profilo di postura (con reindirizzamento).

- La seconda voce del log viene compilata dopo la ricezione del report SWISS conforme.
- La terza voce del log viene compilata quando si invia il CoA, insieme alla conferma (descritta come Autorizzazione dinamica riuscita).
- La voce finale del log viene creata quando l'ASA scarica il DACL.

✓		#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

11. I debug sull'appliance ASA mostrano che il cavo CoA viene ricevuto e il reindirizzamento rimosso. L'ASA scarica gli ACL, se necessario:

```
<#root>
```

```
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. Dopo la sessione VPN, Cisco ha applicato il DACL (accesso completo) per l'utente:

```
<#root>
```

```
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



Nota: l'ASA rimuove sempre le regole di reindirizzamento, anche quando al CoA non è associato alcun DACL.

---

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Debug sull'ISE

Per abilitare i debug, selezionare Amministrazione > Log > Debug log Configuration. Cisco consiglia di abilitare i debug temporanei per:

- SVIZZERO
- NSF (Nonstop Forwarding)
- Sessione NSF

- Provisioning
- Postura

Immettere questo comando nella CLI per visualizzare i debug:

```
<#root>
```

```
ise2/admin#
```

```
show logging application ise-psc.log tail count 100
```

Per visualizzare i rapporti sulla postura, passare a Operazioni > Rapporti > Rapporti ISE > Endpoint e utenti > Valutazione dettagliata postura:

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	✓		continue	cisco	08:08:27:CD:8B: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	08:08:27:CD:8B:A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:58:34.3	✓		continue	cisco	08:08:27:CD:8B: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	08:08:27:CD:8B: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	08:08:27:CD:8B: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	08:08:27:7F: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	08:08:27:7F:5F:6*	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

Nella pagina Valutazione postura più dettagliata è presente un nome di criterio con un nome di requisito visualizzato insieme ai risultati:



## 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		

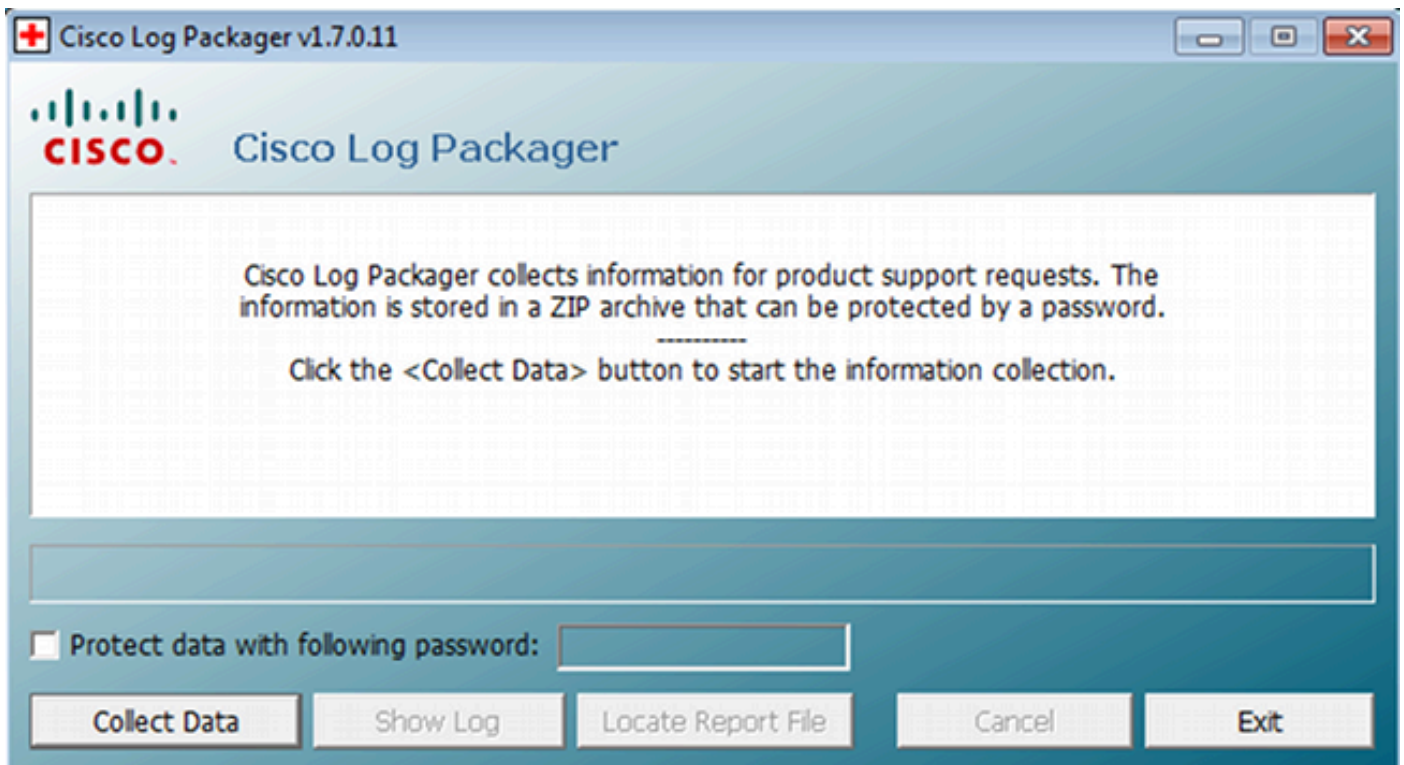
## Debug dell'appliance ASA


Sull'appliance ASA, è possibile abilitare i seguenti debug:

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

## Debug per l'agente

Per l'agente NAC, è possibile raccogliere i debug con Cisco Log Packager, che viene avviato dalla GUI o dalla CLI; utilizzare CCAgentLogPackager.app.



 Suggerimento: è possibile decodificare i risultati con lo strumento Technical Assistance Center (TAC).

Per recuperare i log per l'agente Web, passare ai percorsi seguenti:

- C: > Documento e impostazioni > <utente> > Impostazioni locali > Temp > webagent.log (decodificato con lo strumento TAC)
- C: > Documento e impostazioni > <utente> > Impostazioni locali > Temp > webagentsetup.log

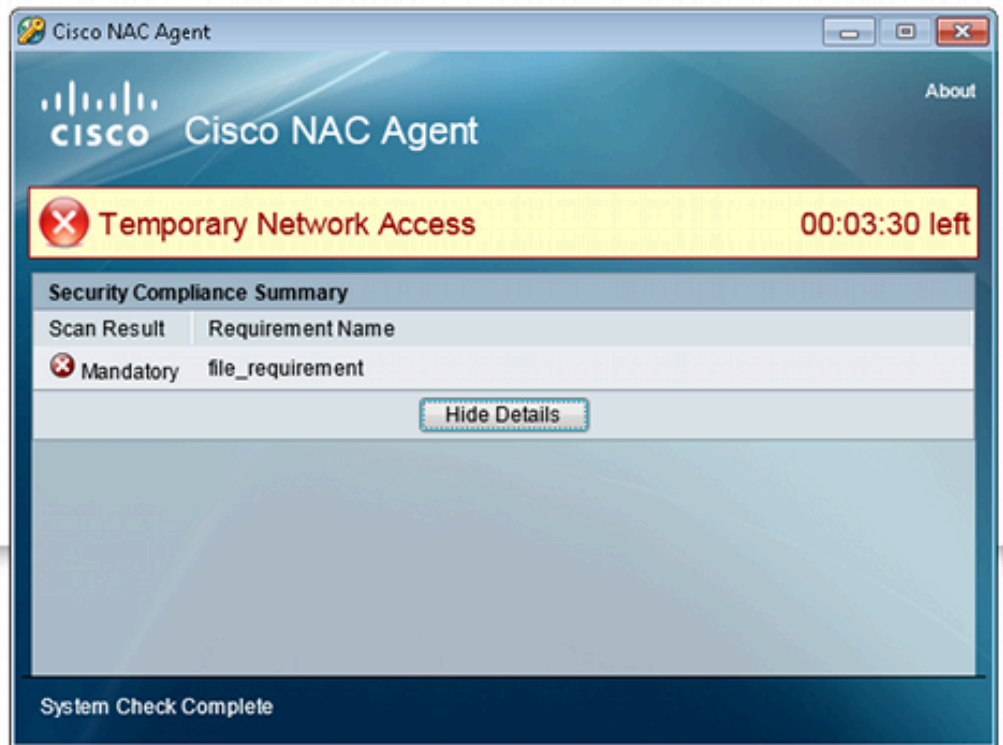
 Nota: se i log non si trovano in questi percorsi, verificare la variabile di ambiente TEMP.

Errore di postura dell'agente NAC

Se la postura non riesce, all'utente viene presentato il motivo:



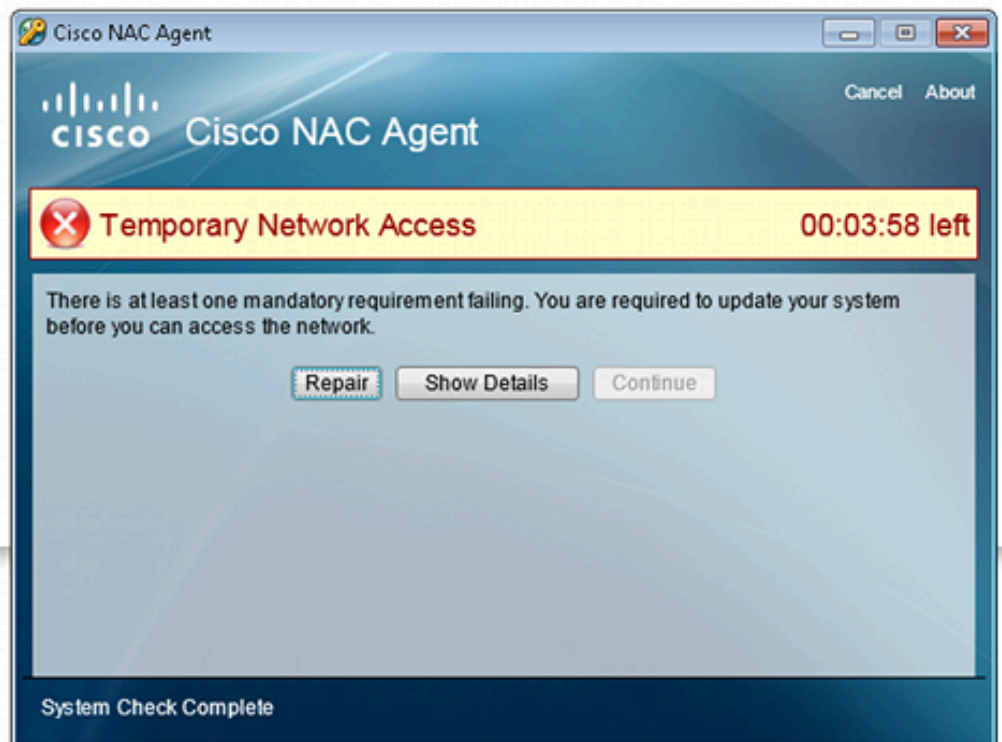
## Information



All'utente vengono quindi consentite le azioni correttive se configurate:



## Information



## Informazioni correlate

- [Guida alla configurazione di Cisco ASA serie 5500 con CLI, 8.4 e 8.6](#)
- [CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.1](#)
- [Supporto tecnico Cisco e download](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).