ASA Version 9.2.1 VPN-Status mit ISE - Konfigurationsbeispiel

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Cisco Adaptive Security Appliance (ASA) Version 9.2.1 konfigurieren, um VPN-Benutzer ohne Inline-Statusknoten (IPN) mit der Cisco Identity Services Engine (ISE) abzugleichen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der ASA CLI-Konfiguration und der SSL VPN-Konfiguration (Secure Socket Layer)
- Grundkenntnisse der VPN-Konfiguration für Remote-Zugriff auf der ASA

- Grundkenntnisse der ISE und Statusservices

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco ASA Software Version 9.2.1 und höher
- Microsoft Windows Version 7 mit Cisco AnyConnect Secure Mobility Client Version 3.1
- Cisco ISE Version 1.2 mit Patch 5 oder höher

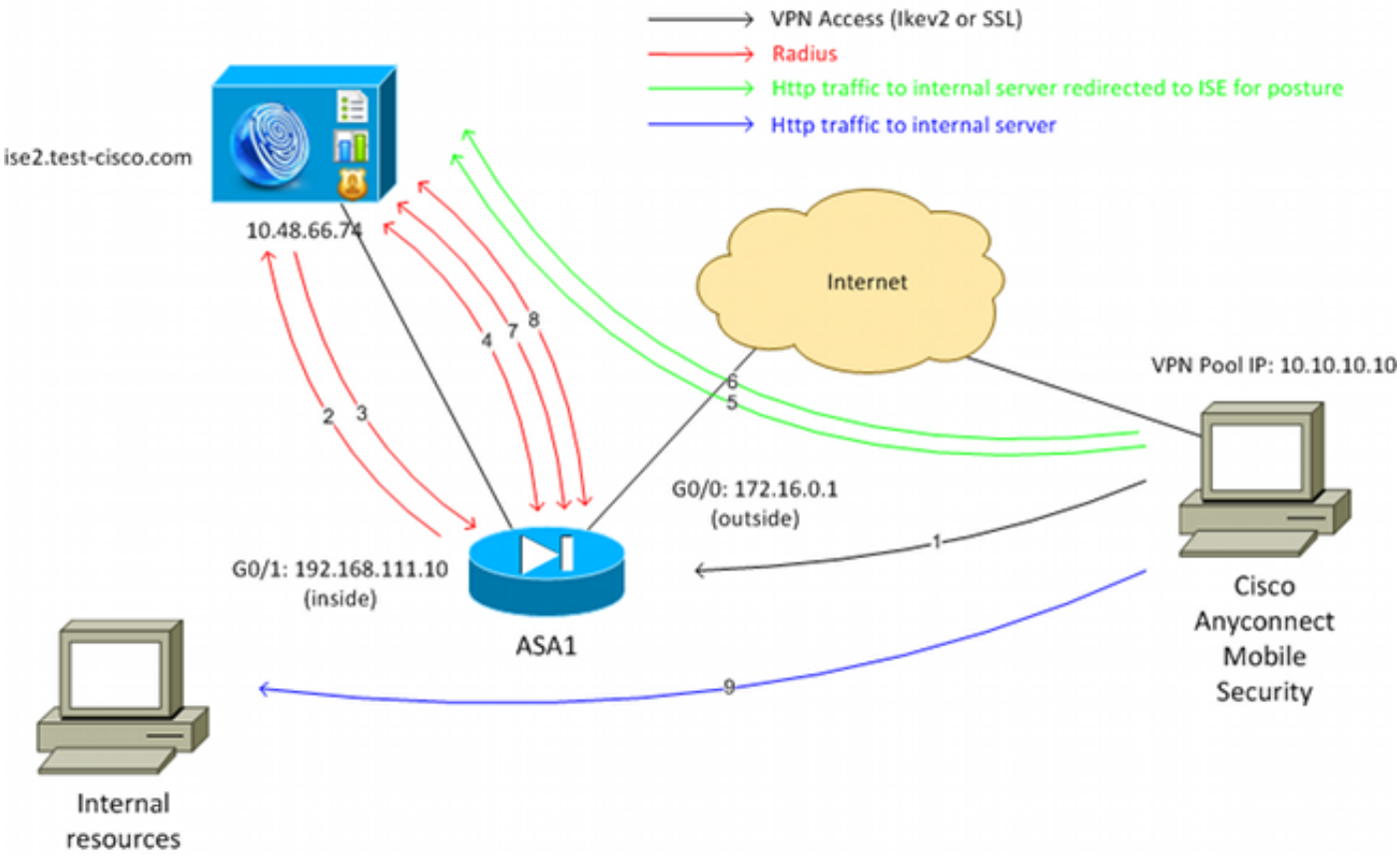
Hintergrundinformationen

Die Cisco ASA Version 9.2.1 unterstützt RADIUS Change of Authorization (CoA) (RFC 5176). Dadurch können VPN-Benutzer ohne IPN an die Cisco ISE weitergeleitet werden. Nach der Anmeldung eines VPN-Benutzers leitet die ASA den Web-Datenverkehr zur ISE um, wo dem Benutzer ein Network Admission Control (NAC)-Agent oder Web-Agent bereitgestellt wird. Der Agent führt auf dem Benutzercomputer spezifische Prüfungen durch, um die Konformität mit einem konfigurierten Satz von Statusregeln zu ermitteln, z. B. Betriebssystem, Patches, AntiVirus-, Dienst-, Anwendungs- oder Registrierungsregeln.

Die Ergebnisse der Statusüberprüfung werden dann an die ISE gesendet. Wenn das System als fehlerhaft eingestuft wird, kann die ISE eine RADIUS-CoA mit den neuen Autorisierungsrichtlinien an die ASA senden. Nach erfolgreicher Statusüberprüfung und CoA kann der Benutzer auf die internen Ressourcen zugreifen.

Konfigurieren

Netzwerkdiagramm und Datenverkehrsfluss



Der Datenverkehrsfluss sieht wie im Netzwerkdiagramm dargestellt folgendermaßen aus:

1. Der Remote-Benutzer verwendet Cisco AnyConnect für den VPN-Zugriff auf die ASA.

2. Die ASA sendet eine RADIUS-Zugriffsanforderung für diesen Benutzer an die ISE.

3. Diese Anforderung trifft auf die Richtlinie **ASA92-Posture** auf der ISE zu. Das Autorisierungsprofil für den **ASA92-Status** wird daher zurückgegeben. Die ISE sendet eine RADIUS Access-Accept-Nachricht mit zwei Cisco Attribut-Wert-Paaren:

   url-redirect-acl=redirect - Dies ist der Name der Zugriffskontrollliste (ACL), der lokal auf der ASA definiert wird und über den umzuleitenden Datenverkehr entscheidet.

   url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp - Dies ist die URL, zu der der Remote-Benutzer umgeleitet werden soll.**Tipp:** Die DNS-Server (Domain Name System), die den VPN-Clients zugewiesen sind, müssen in der Lage sein, den vollqualifizierten Domänennamen (FQDN) aufzulösen, der in der Umleitungs-URL zurückgegeben wird. Wenn die VPN-Filter so konfiguriert sind, dass der Zugriff auf Tunnelgruppenebene eingeschränkt wird, stellen Sie sicher, dass der Client-Pool auf den ISE-Server über den konfigurierten Port zugreifen kann (in diesem Beispiel **TCP 8443**).
4. Die ASA sendet ein RADIUS Accounting-Request-Startpaket und erhält eine Antwort. Dies ist erforderlich, um alle Details bezüglich der Sitzung an die ISE zu senden. Zu diesen Details gehören die session_id, die externe IP-Adresse des VPN-Clients und die IP-Adresse der ASA. Die ISE verwendet die session_id, um diese Sitzung zu identifizieren. Die ASA sendet außerdem regelmäßig Zwischenkontoinformationen, wobei das wichtigste Attribut die Framed-IP-Adresse mit der IP ist, die dem Client von der ASA zugewiesen wird (in diesem

Beispiel **10.10.10.10**).

5. Wenn der Datenverkehr vom VPN-Benutzer mit der lokal definierten ACL übereinstimmt (Redirect), wird er an **https://ise2.test-cisco.com:8443** umgeleitet. Abhängig von der Konfiguration stellt die ISE den NAC Agent oder den Web Agent bereit.

6. Nachdem der Agent auf dem Client-Computer installiert wurde, führt er automatisch bestimmte Prüfungen durch. In diesem Beispiel wird nach der Datei **c:\test.txt** gesucht. Es sendet auch einen Statusbericht an die ISE, der mehrere Tauschvorgänge unter Verwendung des SWISS-Protokolls und der Ports TCP/UDP 8905 umfassen kann, um auf die ISE zuzugreifen.

7. Wenn die ISE den Statusbericht vom Agenten erhält, verarbeitet sie die Autorisierungsregeln erneut. Dieses Mal ist das Haltungsergebnis bekannt und eine weitere Regel wird getroffen. Es sendet ein RADIUS-CoA-Paket:

   Wenn der Benutzer die Richtlinien erfüllt, wird ein Name für eine herunterladbare Zugriffskontrollliste (DACL) gesendet, die den vollständigen Zugriff erlaubt (AuthZ-Regel ASA92-konform).

   Wenn der Benutzer nicht konform ist, wird ein DACL-Name gesendet, der einen eingeschränkten Zugriff zulässt (AuthZ-Regel ASA92-konform).**Hinweis**: Die RADIUS-CoA wird immer bestätigt, d. h., die ASA sendet eine Antwort zur Bestätigung an die ISE.
8. Die ASA entfernt die Umleitung. Wenn die DACLs nicht zwischengespeichert sind, muss eine Zugriffsanforderung gesendet werden, um sie von der ISE herunterzuladen. Die jeweilige DACL ist mit der VPN-Sitzung verbunden.

9. Wenn der VPN-Benutzer das nächste Mal versucht, auf die Webseite zuzugreifen, kann er auf alle Ressourcen zugreifen, die von der auf der ASA installierten DACL zugelassen werden.
   Wenn der Benutzer die Bedingungen nicht erfüllt, wird nur eingeschränkter Zugriff gewährt.
   Hinweis: Dieses Datenflussmodell unterscheidet sich von den meisten Szenarien, in denen RADIUS-CoA verwendet wird. Für kabelgebundene/Wireless-802.1x-Authentifizierungen enthält RADIUS CoA keine Attribute. Es wird nur die zweite Authentifizierung ausgelöst, bei der alle Attribute, z. B. DACL, angefügt werden. Für den ASA VPN-Status gibt es keine zweite Authentifizierung. Alle Attribute werden in der RADIUS-CoA zurückgegeben. Die VPN-Sitzung ist aktiv, und die meisten VPN-Benutzereinstellungen können nicht geändert werden.

Konfigurationen

In diesem Abschnitt können Sie die ASA und die ISE konfigurieren.

ASA

Die ASA-Basiskonfiguration für den Cisco AnyConnect-Zugriff sieht wie folgt aus:

```
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
```

Für die ASA-Integration in die ISE müssen Sie Folgendes sicherstellen:

- Konfigurieren Sie den AAA-Server (Authentication, Authorization, and Accounting) für die dynamische Autorisierung, um CoA zu akzeptieren.
- Konfigurieren Sie die Abrechnung als Tunnelgruppe, um VPN-Sitzungsdetails an die ISE zu senden.
- Konfigurieren Sie die Zwischenabrechnung, die die dem Benutzer zugewiesene IP-Adresse sendet, und aktualisieren Sie regelmäßig den Sitzungsstatus auf der ISE.
- Konfigurieren Sie die Umleitungszugriffskontrollliste, die entscheidet, ob DNS- und ISE-Datenverkehr zulässig sind. Der gesamte andere HTTP-Datenverkehr wird auf Status zur ISE umgeleitet.

Hier ein Konfigurationsbeispiel:

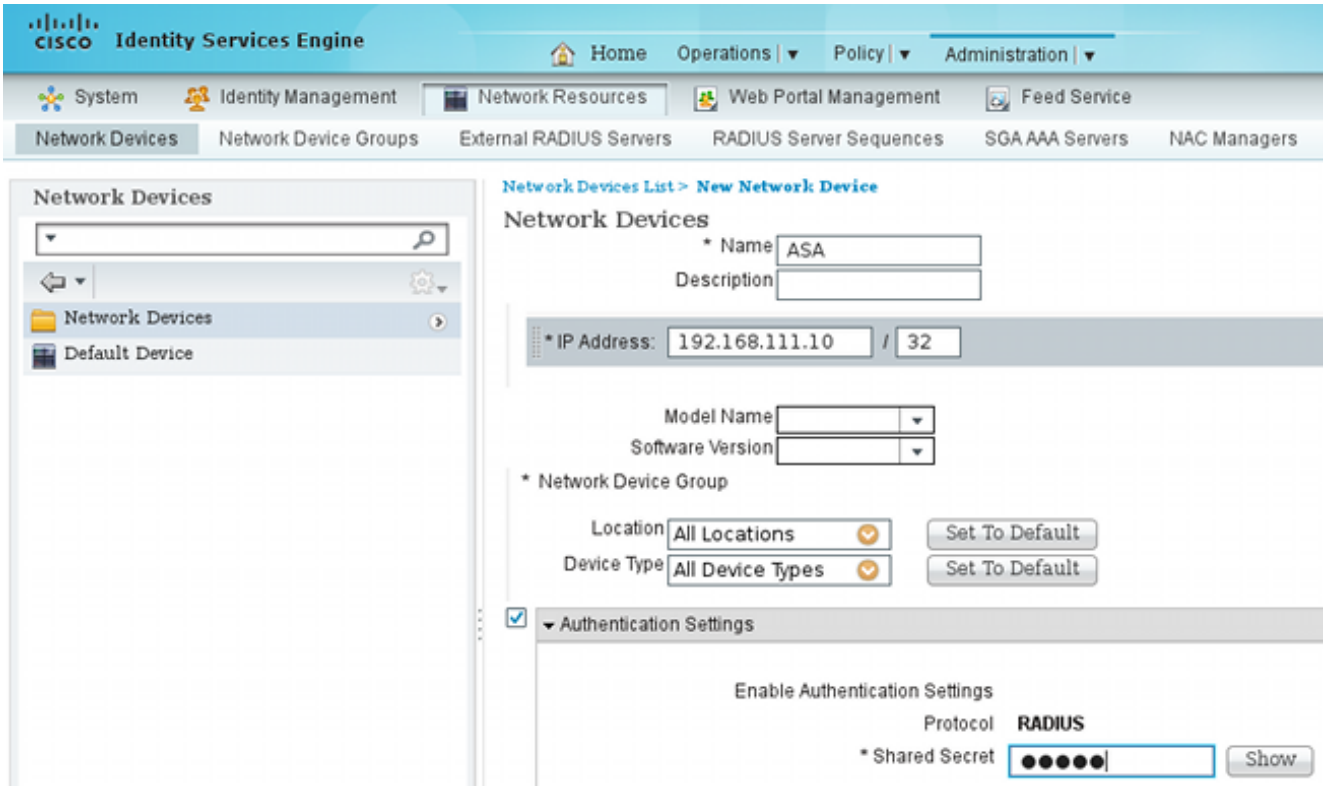
```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

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
```

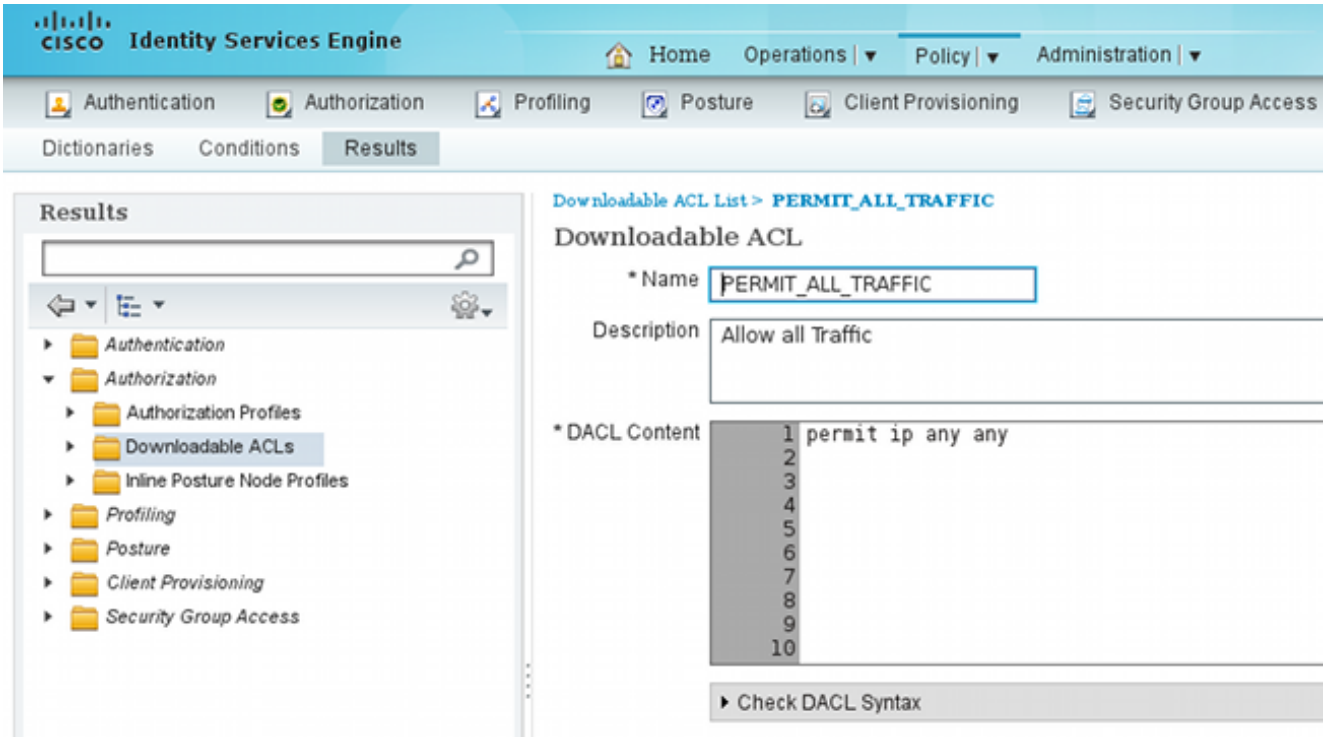
ISE

Gehen Sie wie folgt vor, um die ISE zu konfigurieren:

1. Navigieren Sie zu **Administration > Network Resources > Network Devices,** und fügen Sie die ASA als Netzwerkgerät hinzu:

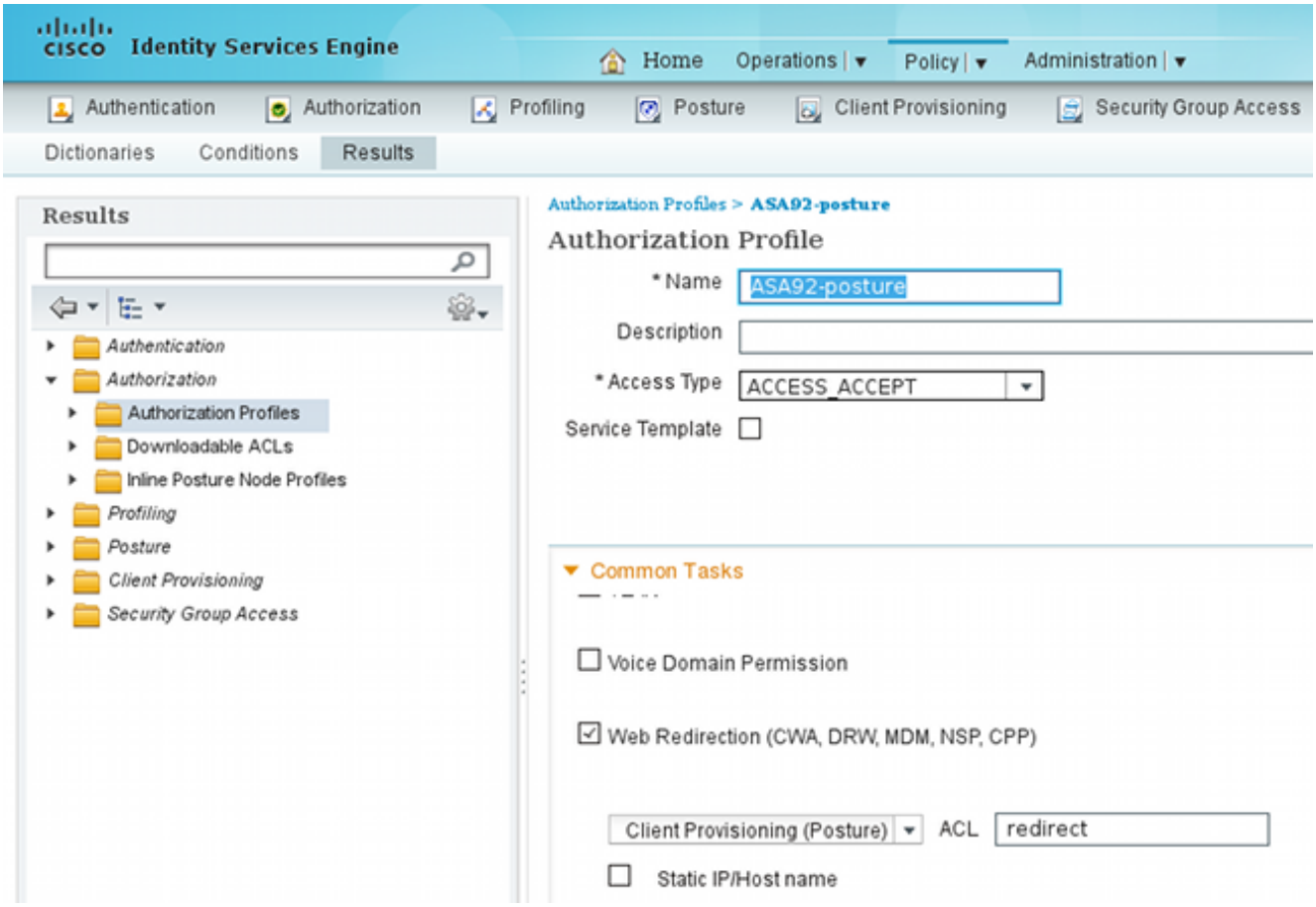


2. Navigieren Sie zu **Policy > Results > Authorization > Downloadable ACL**, und konfigurieren Sie die DACL so, dass sie den vollständigen Zugriff ermöglicht. Die ACL-Standardkonfiguration lässt den gesamten IP-Verkehr auf der ISE zu:

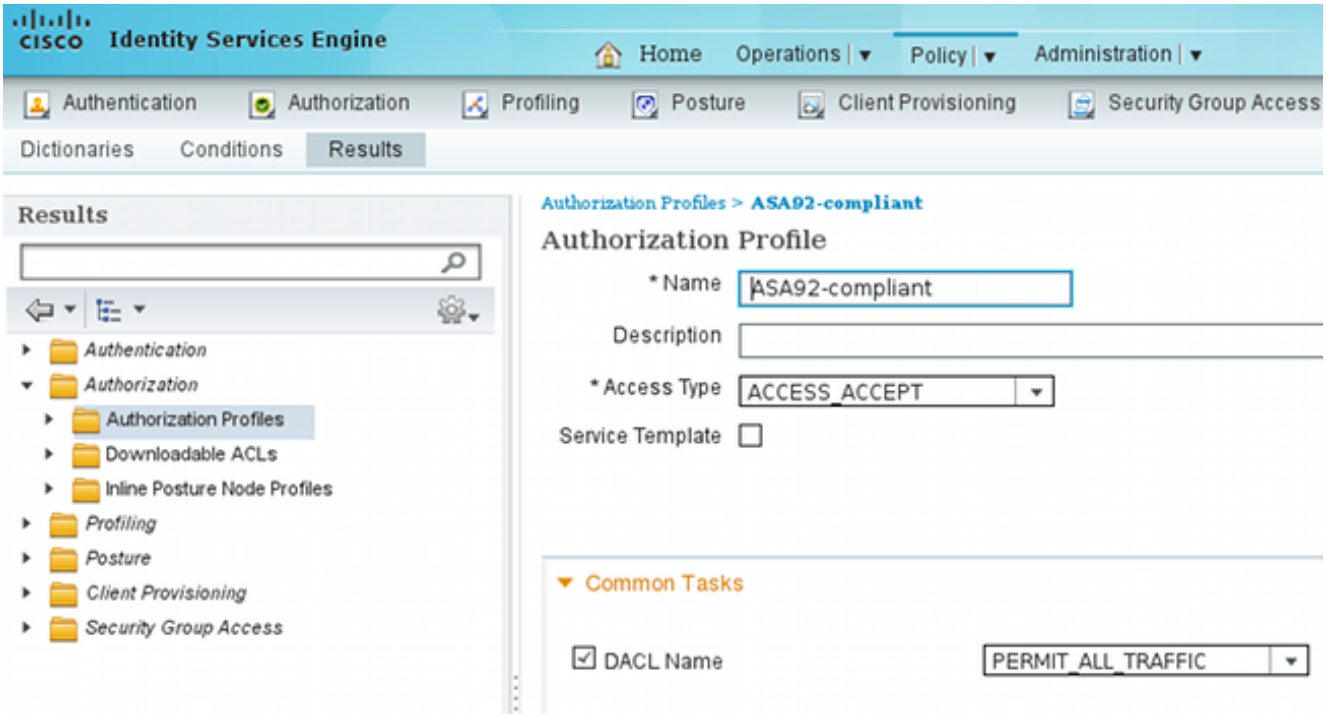


3. Konfigurieren Sie eine ähnliche ACL, die eingeschränkten Zugriff bietet (für nicht konforme Benutzer).

4. Navigieren Sie zu **Richtlinie > Ergebnisse > Autorisierung > Autorisierungsprofile,** und konfigurieren Sie das Autorisierungsprofil **ASA92-**Statusüberprüfung, das Benutzer auf Statusüberprüfungen umleitet. Aktivieren Sie das Kontrollkästchen **Web Redirection (Webumleitung)**, wählen Sie in der Dropdown-Liste die Option **Client Provisioning** aus, und stellen Sie sicher, dass **Redirect** im ACL-Feld angezeigt wird (dass ACL lokal auf der ASA definiert ist):



5. Konfigurieren Sie das **ASA92-konforme** Autorisierungsprofil, das nur die DACL **PERMIT_ALL_TRAFFIC** zurückgeben soll, die vollständigen Zugriff für die konformen Benutzer bietet:



6. Konfigurieren Sie ein ähnliches Autorisierungsprofil mit dem Namen "**ASA92-noncompliant",** das die DACL mit eingeschränktem Zugriff zurückgeben soll (für nicht kompatible Benutzer).

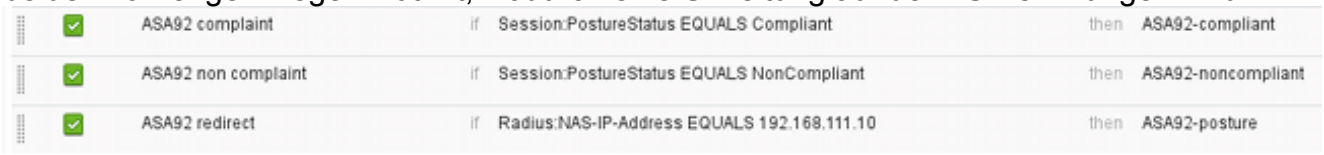
7. Navigieren Sie zu **Policy > Authorization (Richtlinie > Autorisierung**), und konfigurieren Sie

die Autorisierungsregeln:

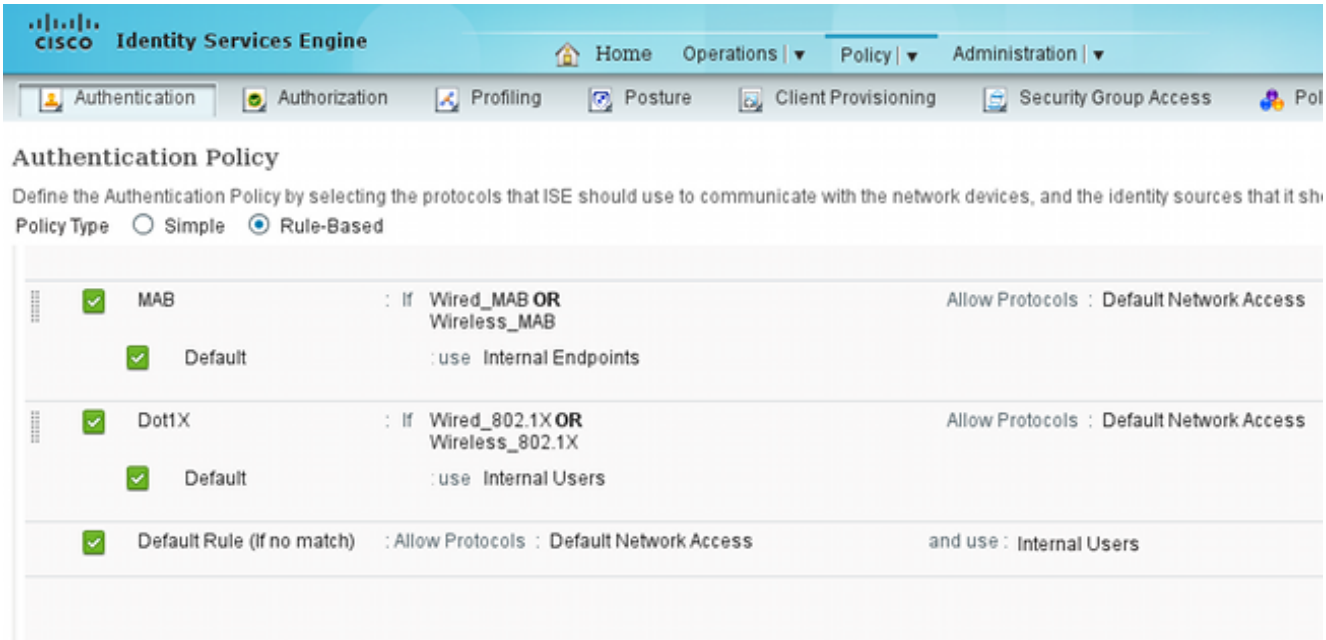
Erstellen Sie eine Regel, die vollständigen Zugriff erlaubt, wenn die Statusergebnisse konform sind. Das Ergebnis ist die **ASA92-konforme** Autorisierungsrichtlinie.

Erstellen Sie eine Regel, die eingeschränkten Zugriff erlaubt, wenn die Statusergebnisse nicht konform sind. Das Ergebnis ist, dass die Autorisierungsrichtlinie **ASA92 nicht konform ist**.

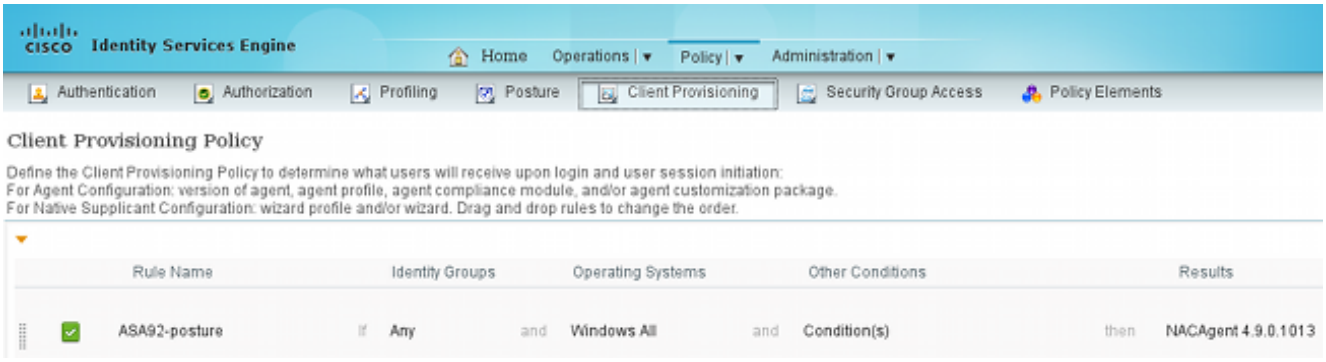
Stellen Sie sicher, dass die Standardregel den **ASA92-Status** zurückgibt, wenn keine der beiden vorherigen Regeln zutrifft, wodurch eine Umleitung auf der ASA erzwungen wird.



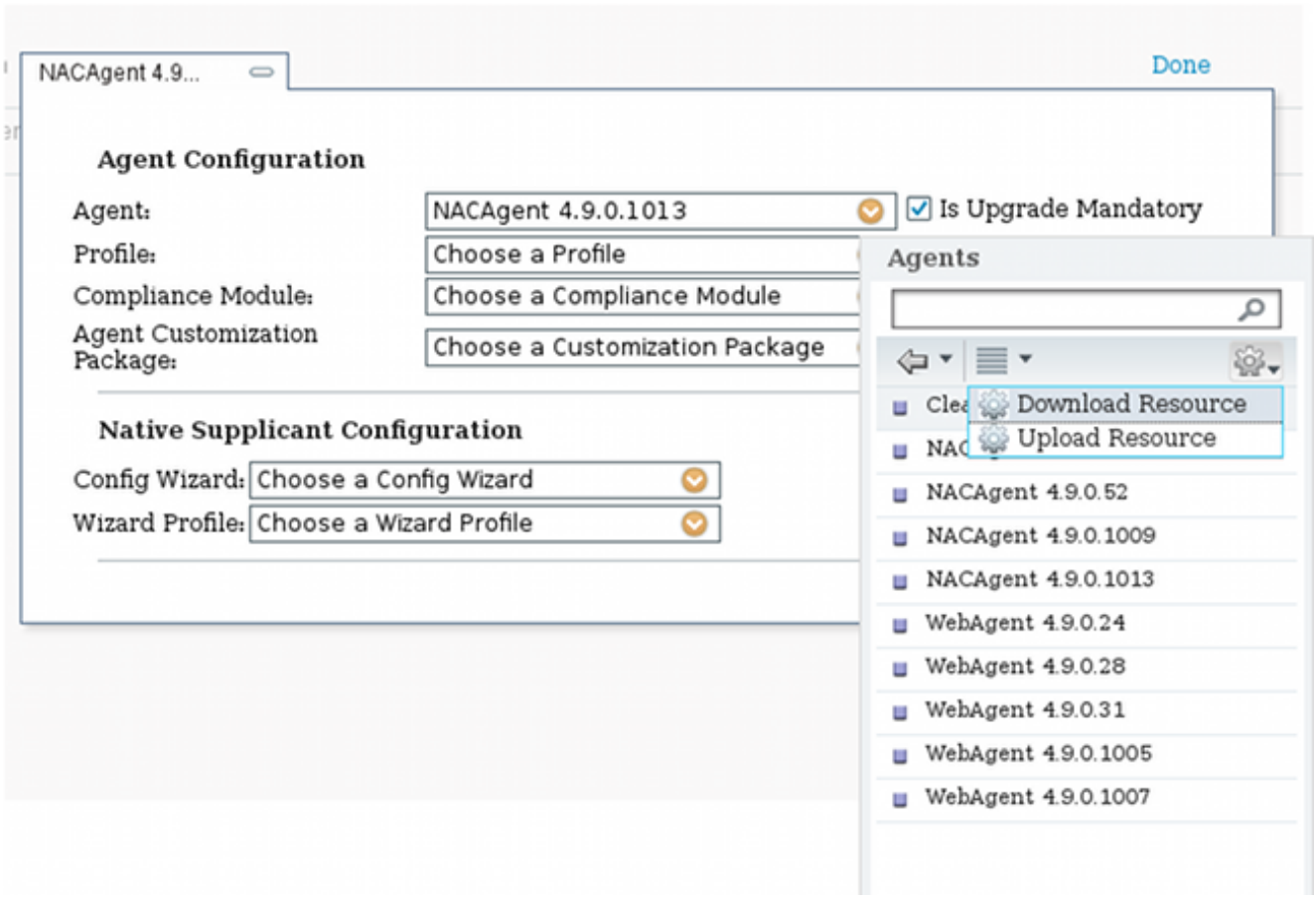
8. Die Standardauthentifizierungsregeln überprüfen den Benutzernamen im internen Identitätsspeicher. Wenn dies geändert werden muss (z. B. in Active Directory (AD) markiert), navigieren Sie zu **Policy > Authentication,** und nehmen Sie die Änderung vor:



9. Navigieren Sie zu **Policy > Client Provisioning**, und konfigurieren Sie die Bereitstellungsregeln. Diese Regeln bestimmen, welcher Agententyp bereitgestellt werden soll. In diesem Beispiel existiert nur eine einfache Regel, und die ISE wählt den NAC Agent für alle Microsoft Windows-Systeme aus:



Wenn sich die Agenten nicht auf der ISE befinden, können sie heruntergeladen werden:



10. Falls erforderlich, können Sie zu **Administration > System > Settings > Proxy** navigieren und den Proxy für die ISE konfigurieren (um auf das Internet zuzugreifen).

11. Konfigurieren Sie die Statusregeln, mit denen die Clientkonfiguration überprüft wird. Sie können Regeln konfigurieren, die Folgendes prüfen:

    Dateien - Existenz, Version, Datum

    Registry - Schlüssel, Wert, Existenz

    Anwendung - Prozessname, wird ausgeführt, wird nicht ausgeführt

    service - Dienstname, ausgeführt, nicht ausgeführt

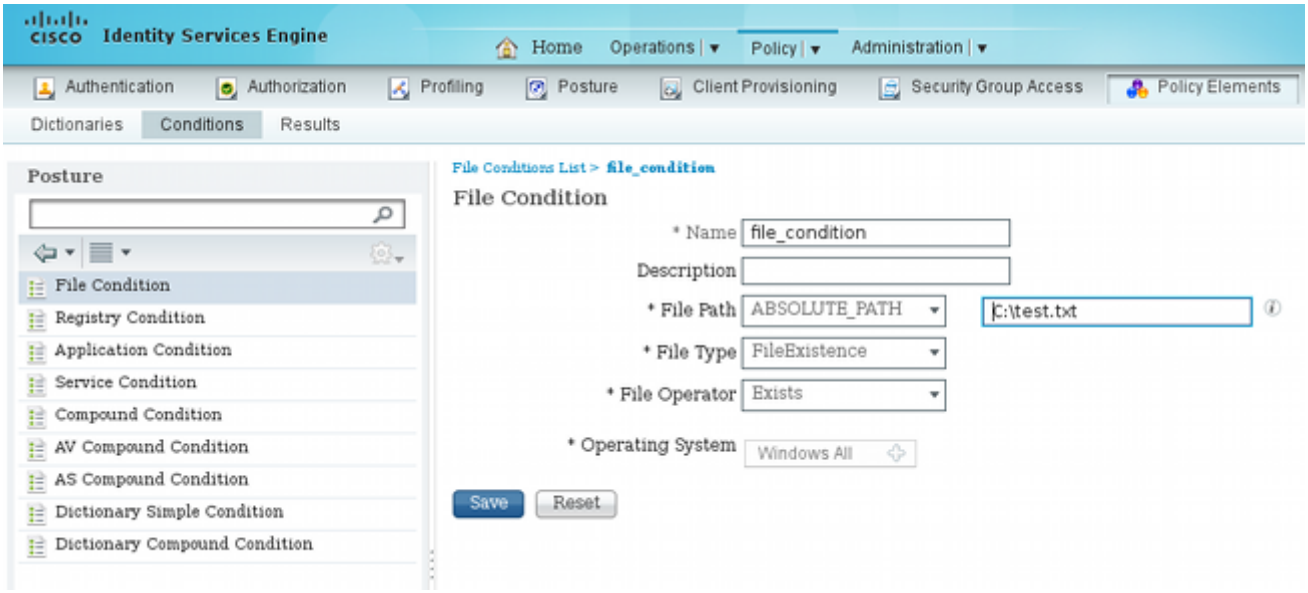
Antivirus - Unterstützung von mehr als 100 Anbietern, Version, wenn Definitionen aktualisiert werden

Antispyware - mehr als 100 Anbieter unterstützt, Version, wenn Definitionen aktualisiert werden

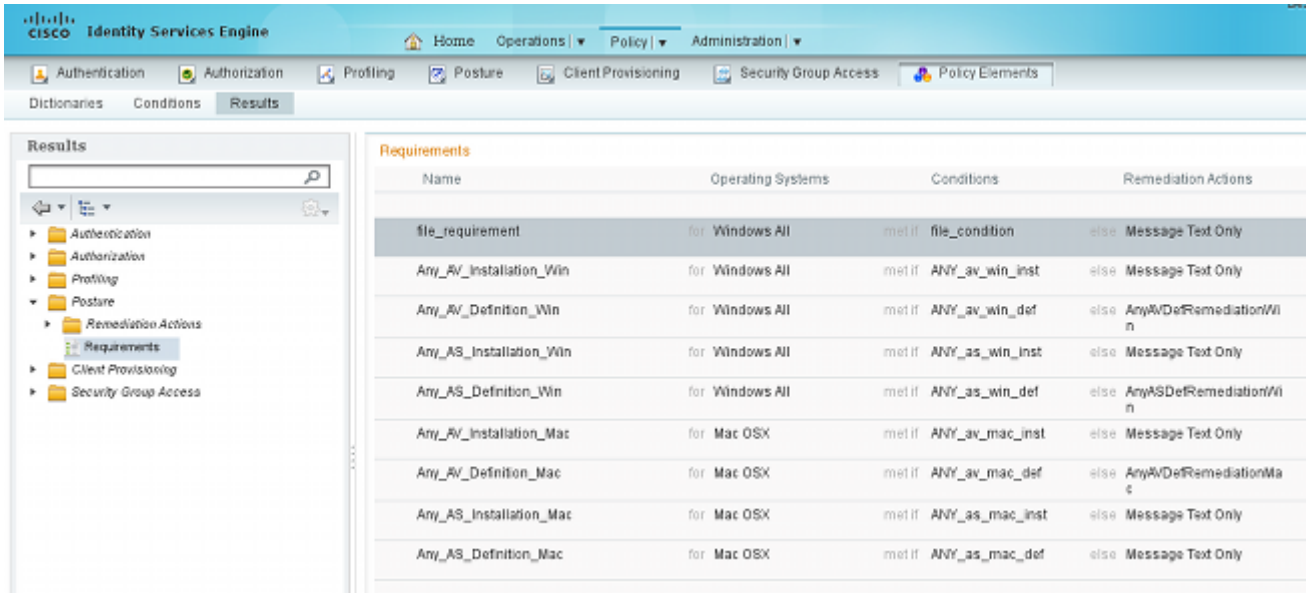
zusammengesetzter Zustand - Mischung aller

Benutzerdefinierte Wörterbuchbedingungen - Verwendung der meisten ISE-Wörterbücher

12. In diesem Beispiel wird nur eine einfache Überprüfung des Vorliegens einer Datei durchgeführt. Wenn die Datei **c:\test.txt** auf dem Client-Computer vorhanden ist, ist sie kompatibel und erhält uneingeschränkten Zugriff. Navigieren Sie zu **Policy > Conditions > File Conditions,** und konfigurieren Sie die Dateibedingung:

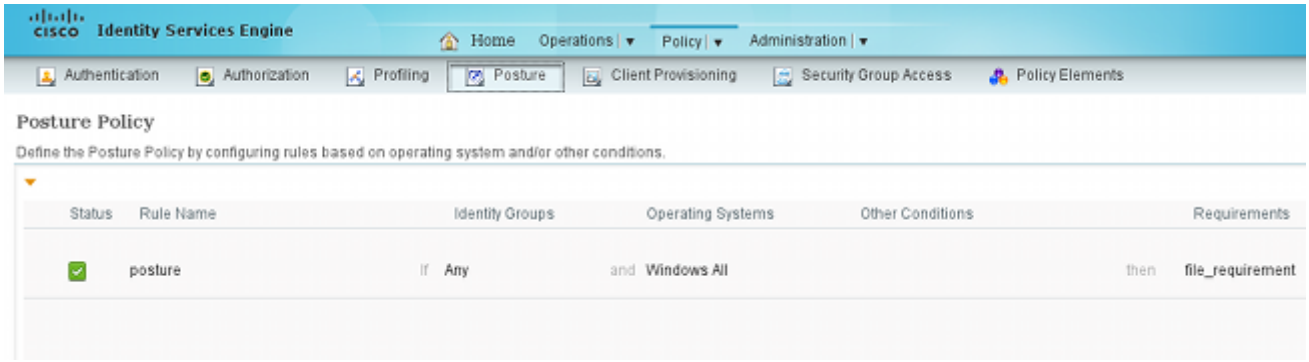


13. Navigieren Sie zu **Richtlinie > Ergebnisse > Status > Anforderungen,** und erstellen Sie eine Anforderung. Diese Anforderung muss erfüllt sein, wenn die vorherige Bedingung erfüllt ist. Ist dies nicht der Fall, wird eine Korrekturmaßnahme ausgeführt. Es gibt möglicherweise viele Arten von Korrekturmaßnahmen, aber in diesem Beispiel wird die einfachste verwendet: Eine bestimmte Meldung wird angezeigt.



Hinweis: In einem normalen Szenario kann die Aktion "Datei-Bereinigung" verwendet werden (die ISE stellt die herunterladbare Datei bereit).

14. Navigieren Sie zu **Richtlinie > Status**, und verwenden Sie die Anforderung, die Sie im vorherigen Schritt (mit dem Namen **file_requirement)** in den Statusregeln erstellt haben. Die einzige Statusregel erfordert, dass alle Microsoft Windows-Systeme die **file_requirement** erfüllen. Wenn diese Anforderung erfüllt wird, ist die Station konform. Wenn sie nicht erfüllt wird, ist die Station nicht konform.

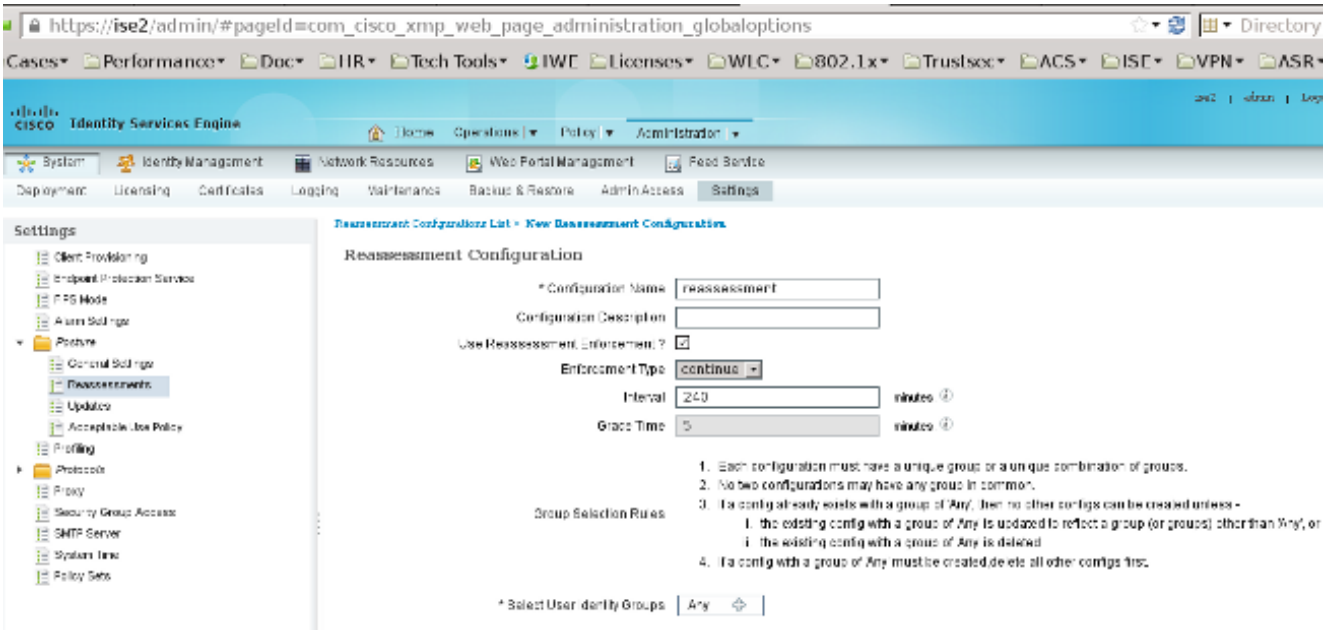


Regelmäßige Neubewertung

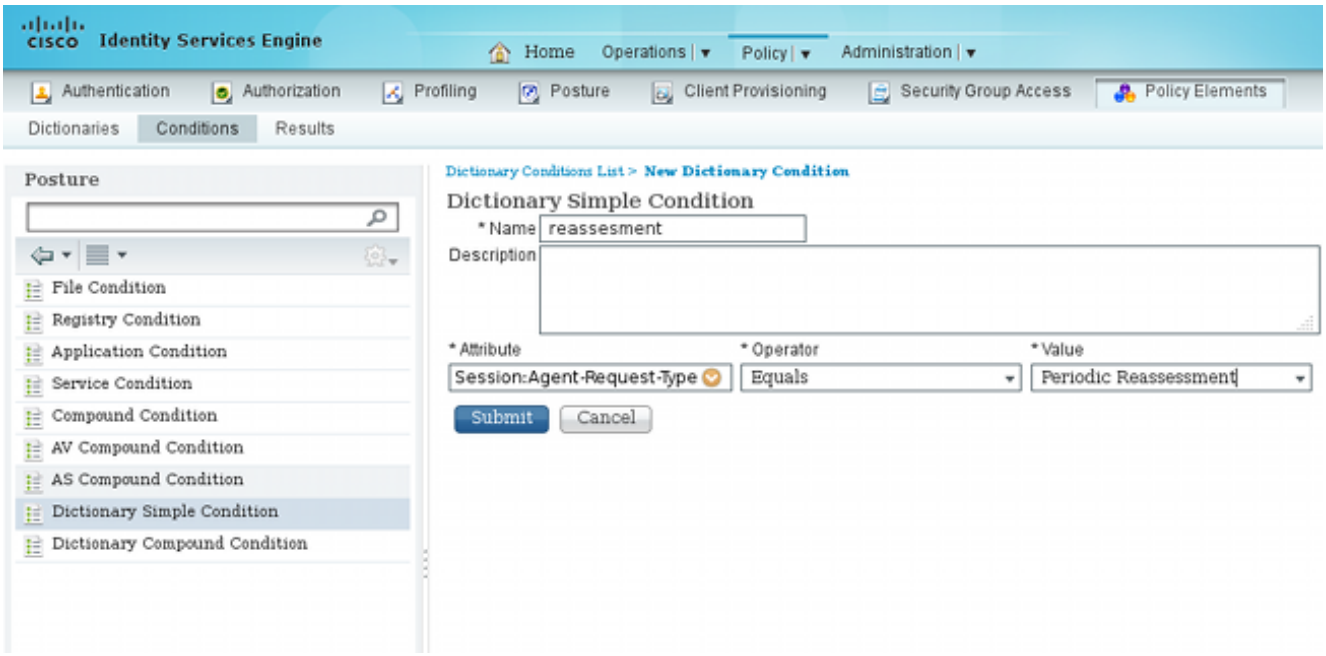
Standardmäßig ist ein Status ein einmaliges Ereignis. Manchmal ist es jedoch erforderlich, die Benutzer-Compliance regelmäßig zu überprüfen und den Zugriff auf die Ressourcen entsprechend den Ergebnissen anzupassen. Diese Informationen werden über das SWISS-Protokoll (NAC Agent) weitergeleitet oder in der Anwendung (Web Agent) codiert.

Führen Sie die folgenden Schritte aus, um die Einhaltung der Benutzerrichtlinien zu überprüfen:

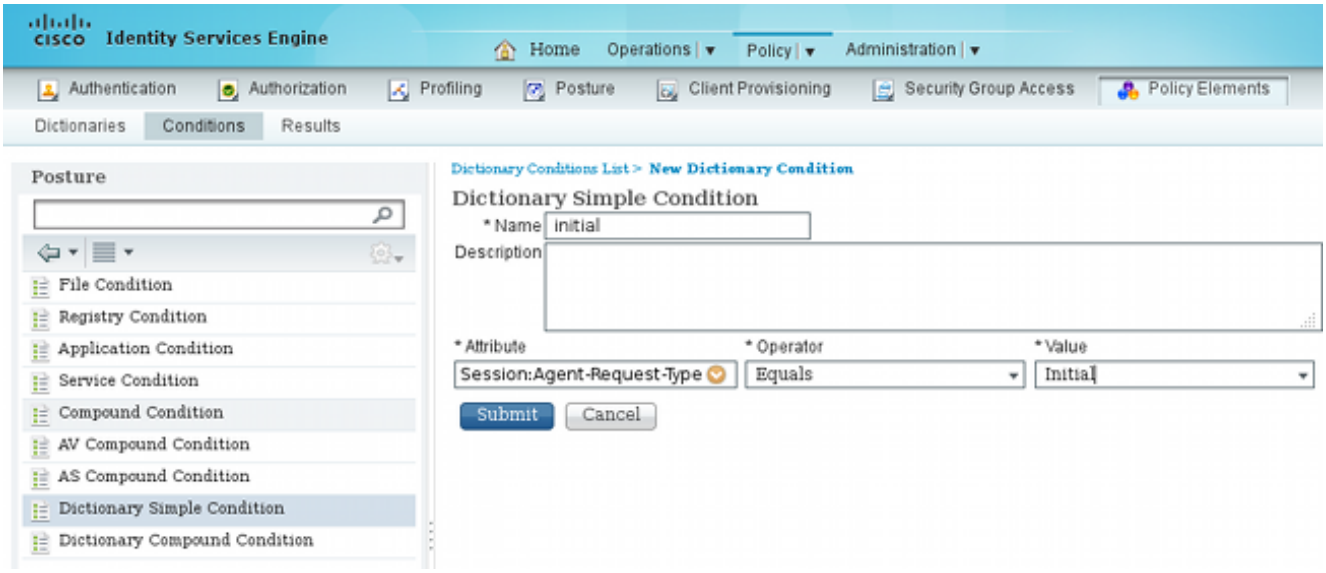
1. Navigieren Sie zu **Administration > Settings > Posture > Rereviews,** und aktivieren Sie die Neubewertung global (nach Identitätsgruppenkonfiguration):



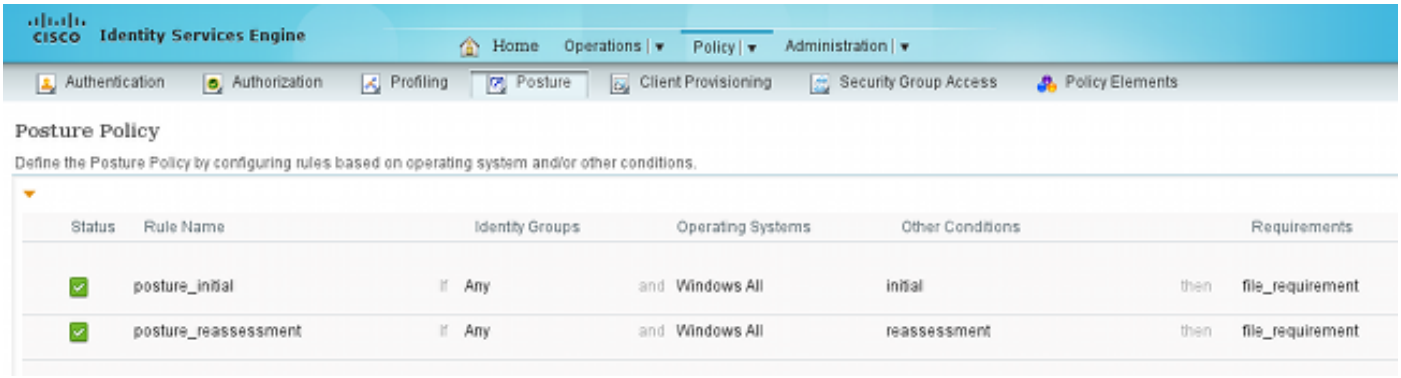
2. Erstellen Sie eine Statusbedingung, die mit allen Neubewertungen übereinstimmt:



3. Erstellen Sie eine ähnliche Bedingung, die nur mit den anfänglichen Leistungsbeurteilungen übereinstimmt:



Beide Bedingungen können in den Haltungsregeln verwendet werden. Die erste Regel stimmt nur mit der ersten Leistungsbeurteilung überein, die zweite mit allen nachfolgenden Leistungsbeurteilungen:

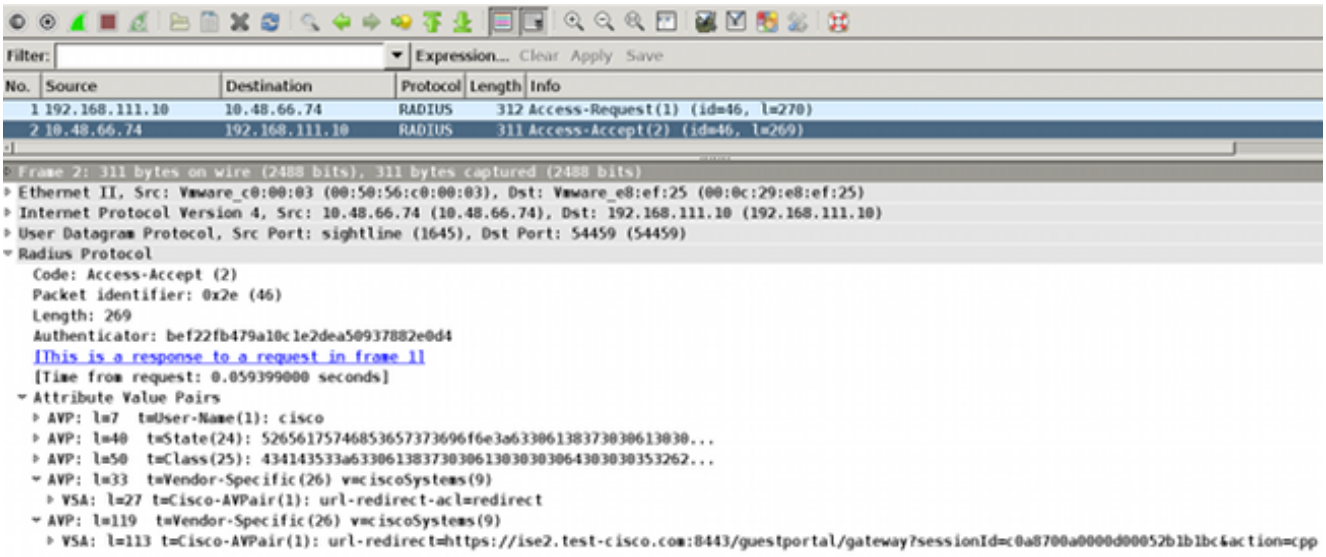


Überprüfung

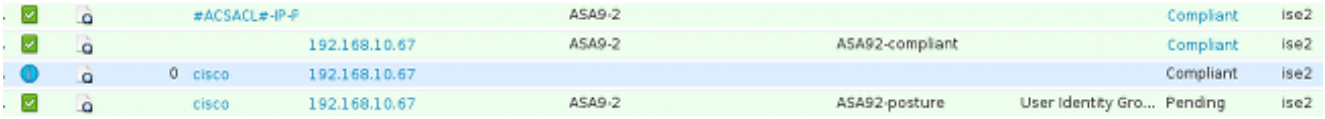
Um sicherzustellen, dass Ihre Konfiguration korrekt funktioniert, stellen Sie sicher, dass die folgenden Schritte durchgeführt werden:

1. Der VPN-Benutzer stellt eine Verbindung zur ASA her.

2. Die ASA sendet eine RADIUS-Anforderung und erhält eine Antwort mit den Attributen **url-redirect** und **url-redirect-acl**:



3. Aus den ISE-Protokollen geht hervor, dass die Autorisierung mit dem Statusprofil (dem ersten Protokolleintrag) übereinstimmt:



4. Die ASA fügt der VPN-Sitzung eine Umleitung hinzu:

```
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. Der Status der VPN-Sitzung auf der ASA zeigt, dass der Status erforderlich ist, und leitet den HTTP-Datenverkehr um:

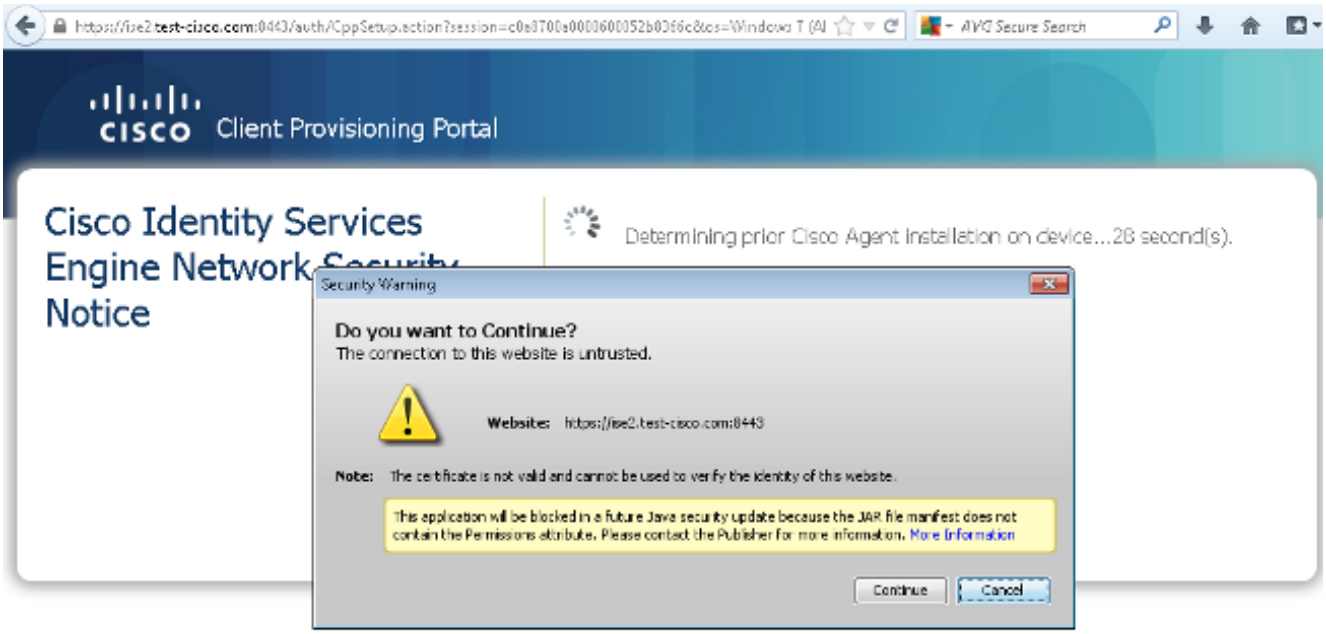
```
ASA# show vpn-sessiondb detail anyconnect

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. Der Client, der den HTTP-Datenverkehr initiiert, der mit der Umleitungs-ACL übereinstimmt, wird an die ISE umgeleitet:

```
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. Der Client wird für den Status an die ISE umgeleitet:



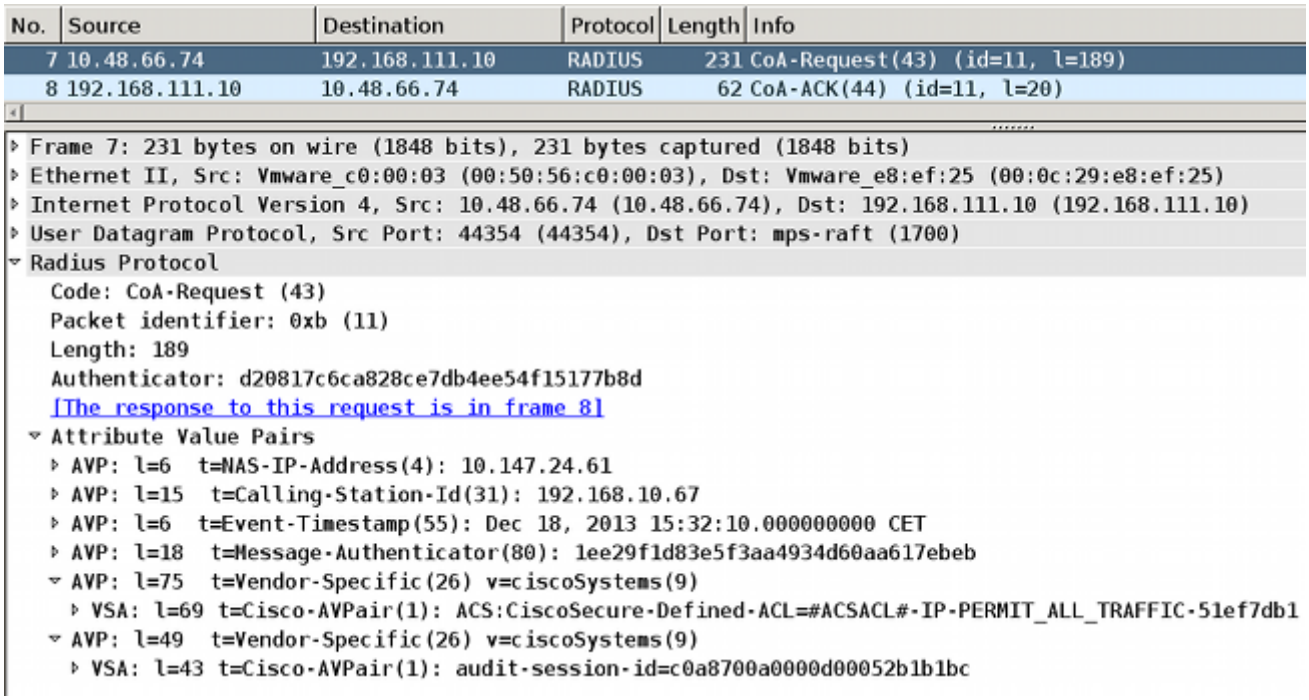
8. Der NAC Agent ist installiert. Nach der Installation des NAC Agent lädt er die Statusregeln über das SWISS-Protokoll herunter und führt Prüfungen durch, um die Konformität festzustellen. Der Statusbericht wird dann an die ISE gesendet.

9. Die ISE erhält den Statusbericht, bewertet die Autorisierungsregeln neu und ändert (falls erforderlich) den Autorisierungsstatus und sendet eine CoA. Dies kann in der Datei **ise-psc.log** überprüft werden:

```
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. Die ISE sendet eine RADIUS-CoA, die die **session_id** und den DACL-Namen enthält, die

vollständigen Zugriff ermöglichen:



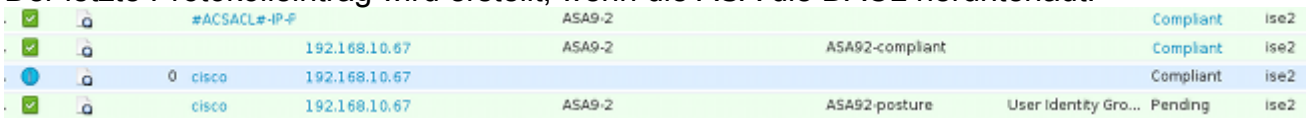
Dies spiegelt sich in den ISE-Protokollen wider:

Der erste Protokolleintrag bezieht sich auf die Erstauthentifizierung, die das Statusprofil (mit Umleitung) zurückgibt.

Der zweite Protokolleintrag wird nach Empfang des konformen SWISS-Berichts ausgefüllt.

Der dritte Protokolleintrag wird ausgefüllt, wenn die CoA gesendet wird, zusammen mit der Bestätigung (beschrieben als "Dynamic Authorization Succeeded" (dynamische Autorisierung erfolgreich).

Der letzte Protokolleintrag wird erstellt, wenn die ASA die DACL herunterlädt.



11. Die Fehlerbehebungen auf der ASA zeigen, dass die CoA empfangen und die Umleitung entfernt wurde. Die ASA lädt die DACLs bei Bedarf herunter:

```
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. Nach der VPN-Sitzung überträgt Cisco die DACL (vollständiger Zugriff) auf den Benutzer:

```
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
```

Hinweis: Die ASA entfernt die Umleitungsregeln immer, auch wenn der CoA keine DACL angehängt hat.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Debuggen auf der ISE

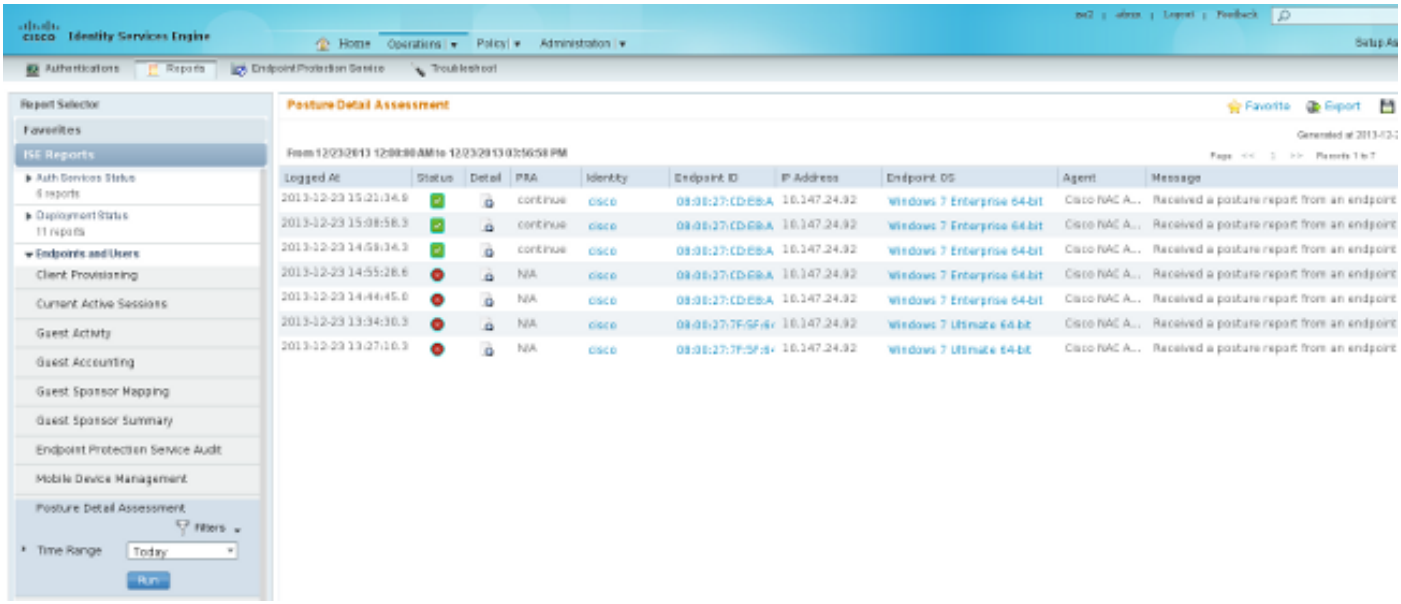
Navigieren Sie zu **Administration > Logging > Debug Log Configuration**, um Debugging zu aktivieren. Cisco empfiehlt die Aktivierung von temporären Debugging-Vorgängen für:

- SCHWEIZ
- Nonstop Forwarding (NSF)
- NSF-Sitzung
- Bereitstellung
- Status

Geben Sie den folgenden Befehl in der CLI ein, um die Debugging-Meldungen anzuzeigen:

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

Navigieren Sie zu **Operations > Reports > ISE Reports > Endpoints and Users > Statusdetailsanalyse,** um die Statusberichte anzuzeigen:



Auf der Seite "Statusprüfung mit weiteren Details" wird neben den Ergebnissen ein Richtlinienname mit einem Anforderungsnamen angezeigt:

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		

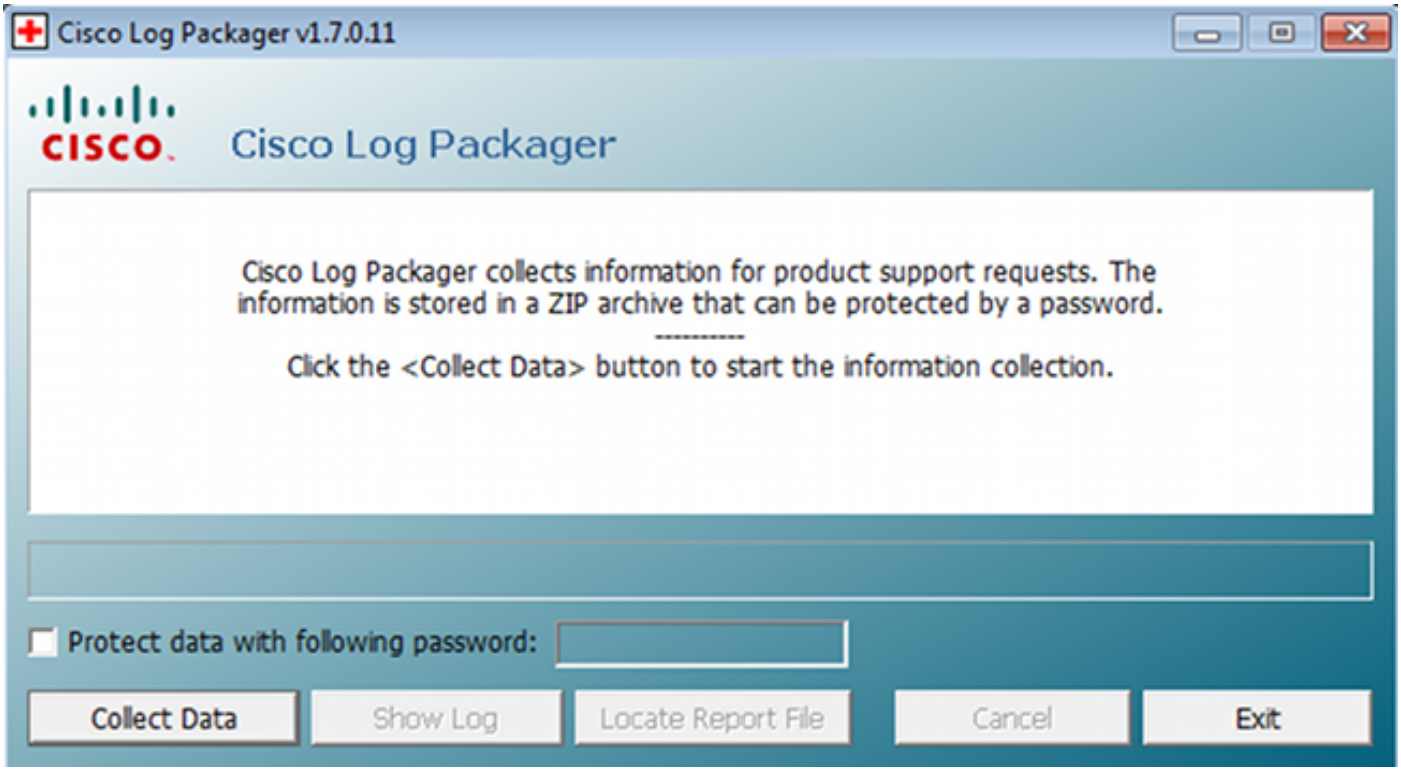
Fehlerbehebung auf der ASA

Sie können diese Debug-Funktionen auf der ASA aktivieren:

- **debug aaa url-redirect**
- **debuggen aaa-Berechtigung**
- **Debugradius dynamische Autorisierung**
- **Debug-Radius-Dekodierung**
- **debugradius benutzer cisco**

Debuggen für den Agent

Für den NAC Agent ist es möglich, die Debug-Meldungen mit dem Cisco Log Packager zu sammeln, der über die GUI oder die CLI initiiert wird: **CCAAgentLogPackager.app**.



> **Tipp:** Sie können die Ergebnisse mit dem Tool des Technical Assistance Center (TAC) entschlüsseln.

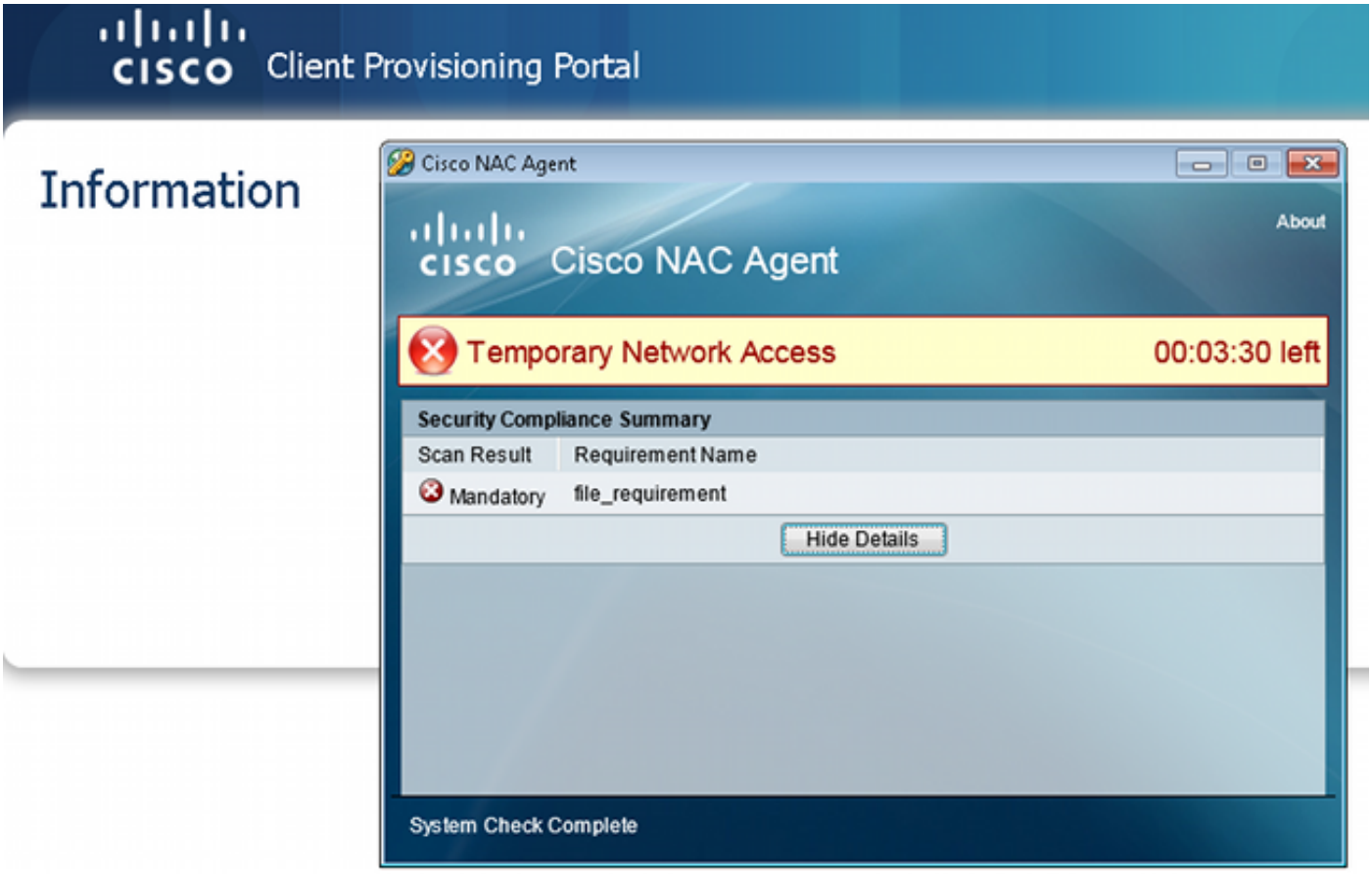
Um die Protokolle für den Web-Agent abzurufen, navigieren Sie zu den folgenden Speicherorten:

- **C: > Dokument und Einstellungen > *<Benutzer>* > Lokale Einstellungen > Temp > webagent.log** (mit dem TAC-Tool dekodiert)
- **C: > Dokument und Einstellungen > *<Benutzer>* > Lokale Einstellungen > Temp > webagentsetup.log**

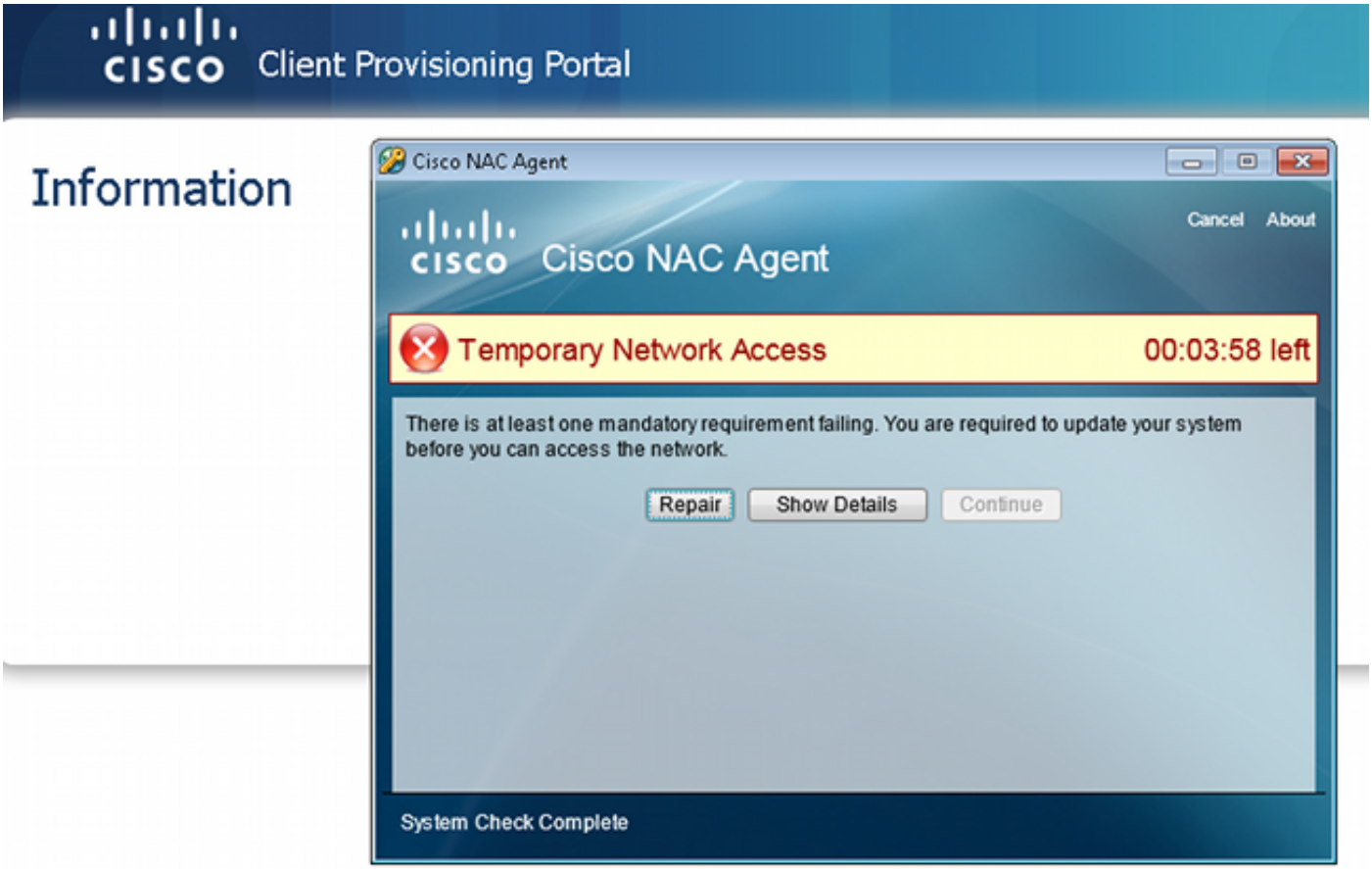
> **Hinweis**: Wenn sich die Protokolle nicht an diesen Standorten befinden, überprüfen Sie die Variable **TEMP Environment (TEMP-Umgebung)**.

NAC Agent-Statusfehler

Wenn der Status fehlschlägt, wird dem Benutzer der Grund angezeigt:



Dem Benutzer können dann Wiederherstellungsaktionen durchgeführt werden, wenn sie wie folgt konfiguriert sind:



Zugehörige Informationen

- Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance
- Konfigurationsleitfaden für die VPN-CLI der Cisco ASA-Serie, 9.1
- Cisco Identity Services Engine Benutzerhandbuch, Version 1.2
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.