ISE との ASA バージョン 9.2.1 VPN ポスチャの設定例

内容

概要

このドキュメントでは、インライン ポスチャ ノード（IPN）を使用せずに Cisco Identity Services Engine（ISE）に対して VPN ユーザをポスチャするように Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 9.2.1 を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA CLI 設定およびセキュア ソケット レイヤ（SSL）VPN 設定に関する基本的な知識
- ASA でのリモート アクセス VPN 設定に関する基本的な知識
- ISE サービスとポスチャ サービスに関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco ASA ソフトウェア バージョン 9.2.1 以降
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 3.1 を備えた Microsoft Windows Version 7
- パッチ 5 以降が適用された Cisco ISE バージョン 1.2

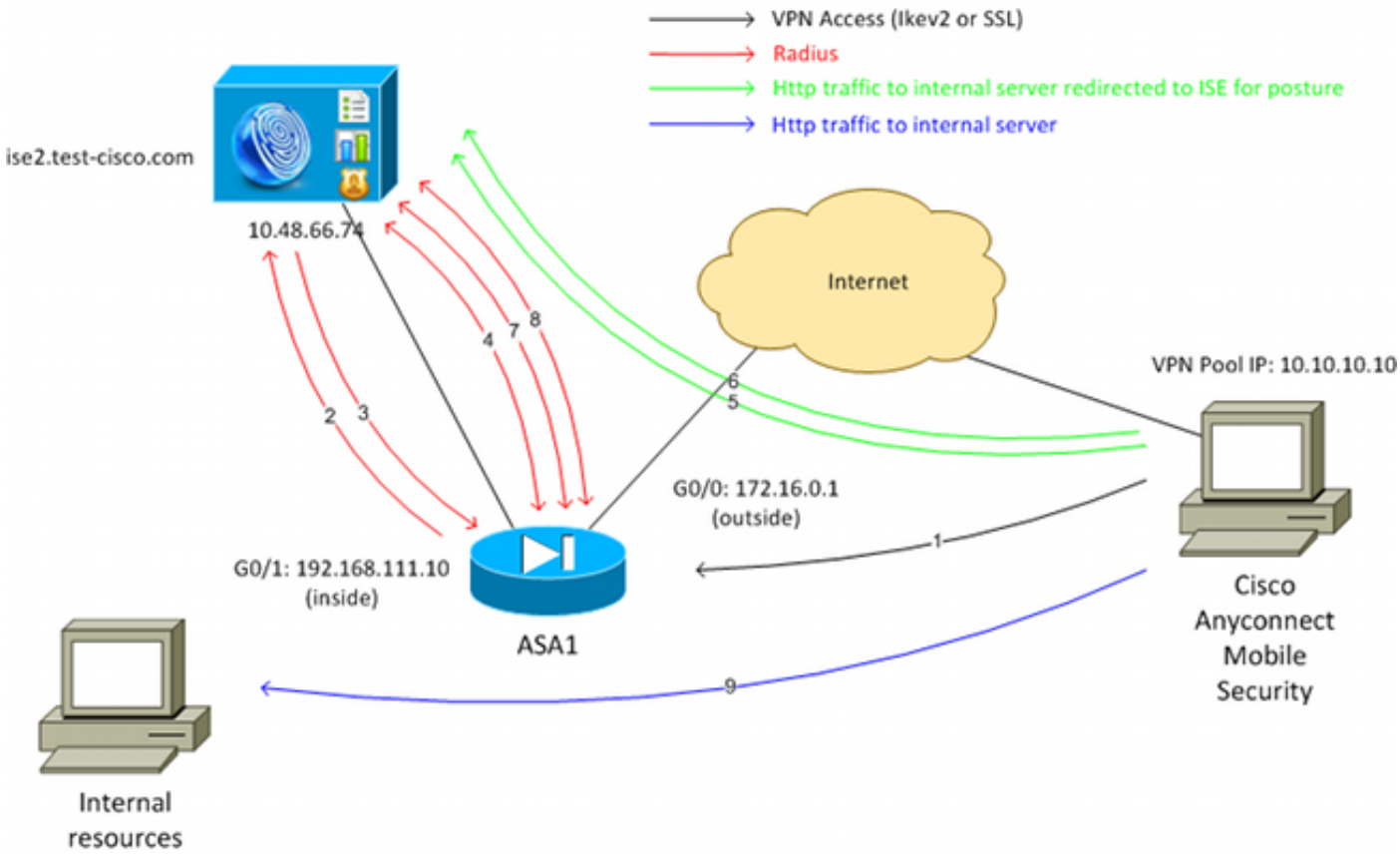
背景説明

Cisco ASA バージョン 9.2.1 は、RADIUS 認可変更（CoA）（RFC 5176）をサポートしています。これにより、IPN を使用せずに Cisco ISE に対して VPN ユーザをポスチャすることが可能になります。VPN ユーザがログインした後、ASA は Web トラフィックを ISE にリダイレクトします。そこでユーザは、ネットワーク アドミッション コントロール（NAC）エージェントまたは Web エージェントでプロビジョニングされます。エージェントは、オペレーティング システム（OS）、パッチ、ウイルス対策、サービス、アプリケーション、またはレジストリ ルールなどの一連の設定済みポスチャ ルールと照らしてコンプライアンスを確認するために、ユーザ マシンで特定のチェックを実行します。

その後、ポスチャ検証の結果が ISE に送信されます。マシンが準拠していると見なされた場合、ISE は認証ポリシーの新しいセットを使用して ASA に RADIUS CoA を送信することができます。ポスチャ検証と CoA に成功すると、ユーザは内部リソースへのアクセスが許可されます。

設定

ネットワーク図とトラフィック フロー



次のネットワーク図にトラフィック フローを示します。

1. リモート ユーザが Cisco AnyConnect を使用して ASA に VPN アクセスします。

2. ASA はそのユーザの RADIUS アクセス要求を ISE に送信します。

3. この要求に対しては、ISE で **ASA92-posture という名前のポリシーがヒットします。**その結果、**ASA92-posture 認証プロファイルが返されます。**ISE は、次の 2 つの Cisco Attribute-Value ペアを使用して、RADIUS Access-Accept を送信します。

   url-redirect-acl=redirect 。これは、ASA でローカルに定義されたアクセス コントロール リスト (ACL) の名前であり、リダイレクトするトラフィックを決定します。

   url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp 。これは、リモート ユーザのリダイレクト先となる URL です。ヒント:VPNクライアントに割り当てられたドメインネームシステム(DNS)サーバは、リダイレクトURLで返される完全修飾ドメイン名(FQDN)を解決できる必要があります。VPN フィルタがトンネル グループ レベルでアクセスを制限するように設定されている場合は、クライアント プールが設定済みポート (この例では **TCP 8443) 上で ISE サーバにアクセスできることを確認します。**
4. ASA は RADIUS Accounting-Request 開始パケットを送信し、応答を受信します。これは、ISE へのセッションに関するすべての詳細を送信するために必要です。詳細には、session_id、VPN クライアントの外部 IP アドレス、および ASA の IP アドレスが含まれます。ISE は session_id を使用してセッションを識別します。ASA はさらに、定期中間アカウント情報を送信します。この情報で最も重要な属性は、ASA によってクライアントに割り当てられている IP を持つ Framed-IP-Address です (この例では **10.10.10.10**) 。

5. VPN ユーザからのトラフィックが、ローカルに定義された ACL（リダイレクト）と一致する場合は、**https://ise2.test-cisco.com:8443** にリダイレクトされます。設定によっては、ISE は NAC Agent または Web エージェントをプロビジョニングします。

6. エージェントは、クライアント マシンにインストールされると、自動的に特定のチェックを実行します。この例では、**c:\test.txt** ファイルを探します。エージェントはまた、ISE にポスチャ レポートを送信します。このレポートには、ISE にアクセスできるようにするために、SWISS プロトコルおよびポート TCP/UDP 8905 を使用した複数の交換を含めることができます。

7. ISE がエージェントからポスチャ レポートを受信すると、認証ルールをもう一度処理します。今回は、ポスチャの結果は既知であるため、別のルールがヒットします。これにより、次のように RADIUS CoA のパケットが送信されます。

   ユーザが準拠している場合は、フル アクセスを許可するダウンロード可能 ACL（DACL）名が送信されます（AuthZ ルール ASA92 準拠）。

   ユーザが準拠していない場合は、制限付きアクセスを許可する DACL 名が送信されます（AuthZ ルール ASA92 非準拠）。**注**:RADIUS CoAは常に確認されます。つまり、ASAは確認のためにISEに応答を送信します。
8. ASA がリダイレクションを削除します。DACL がキャッシュされていない場合は、ISE からダウンロードするために Access-Request を送信する必要があります。特定の DACL が VPN セッションに付加されます。

9. VPN ユーザがもう一度 Web ページにアクセスしようとすると、ASA にインストールされている DACL によって許可されたすべてのリソースにアクセスできます。
   ユーザが準拠していない場合は、制限付きアクセスのみが付与されます。
   注：このフローモデルは、RADIUS CoAを使用するほとんどのシナリオとは異なります。有線/無線 802.1x 認証の場合は、RADIUS CoA には属性は含まれていません。これにより、すべての属性（DACL など）が付加される 2 番目の認証のみがトリガーされます。ASA VPN ポスチャの場合は、2 番目の認証は行われません。すべての属性が RADIUS CoA で返されます。VPN セッションがアクティブであるため、ほとんどの VPN ユーザ設定が変更不可になっています。

設定

ここでは、ASA および ISE を設定します。

平均応答時間

Cisco AnyConnect アクセスの基本的な ASA 設定は次のとおりです。

```
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
```

ISE ポスチャと ASA を統合する場合は、必ず次の操作を実行します。

- CoA を受け入れるため、認証、認可、およびアカウンティング（AAA）サーバを動的認証に設定します。
- VPN セッションの詳細情報を ISE へ送信できるように、アカウンティングをトンネル グループとして設定します。
- ユーザに割り当てられた IP アドレスを送信する中間アカウンティングを設定し、定期的に ISE でのセッション ステータスを更新します。
- DNS と ISE トラフィックを許可するかどうかを決定するリダイレクト ACL を設定します。他の HTTP トラフィックはすべて、ポスチャのため ISE にリダイレクトされます。

次に設定の例を示します。

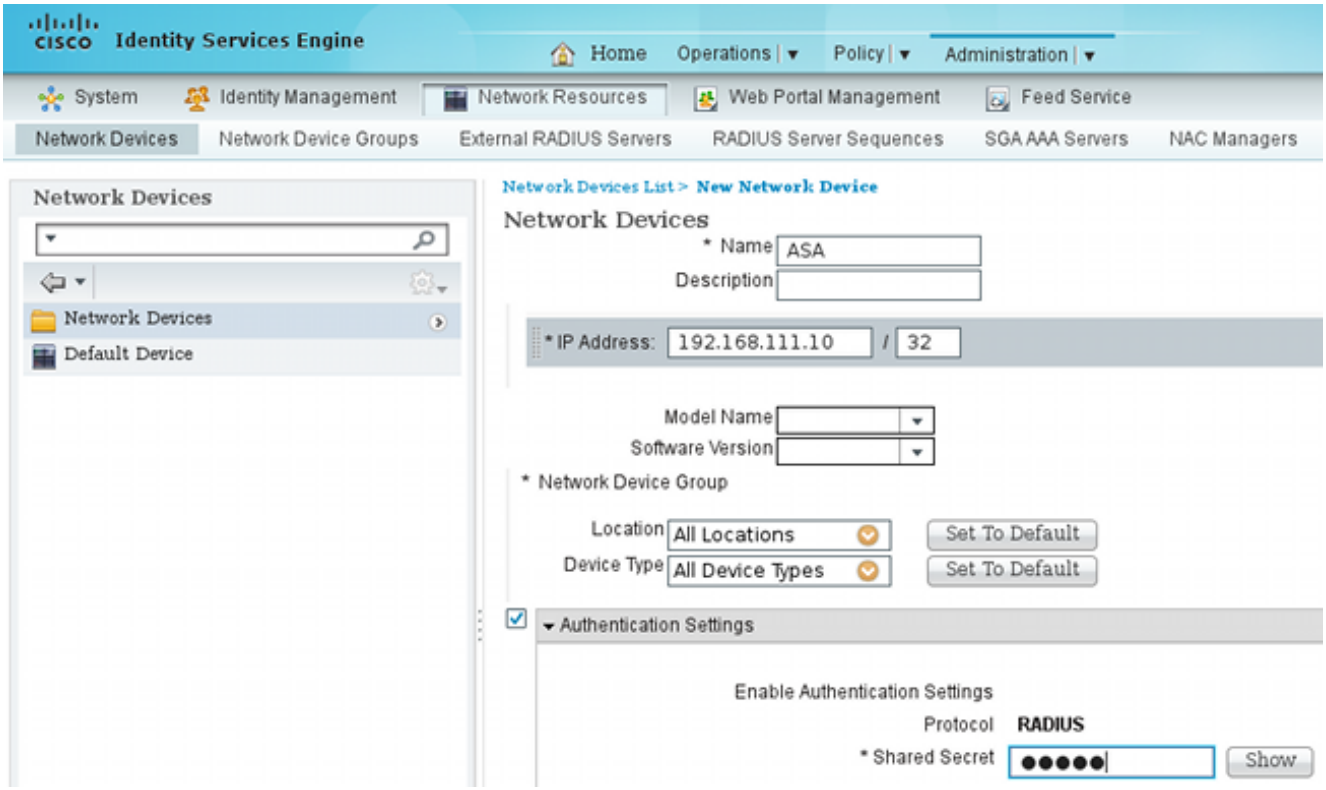
```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

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
```

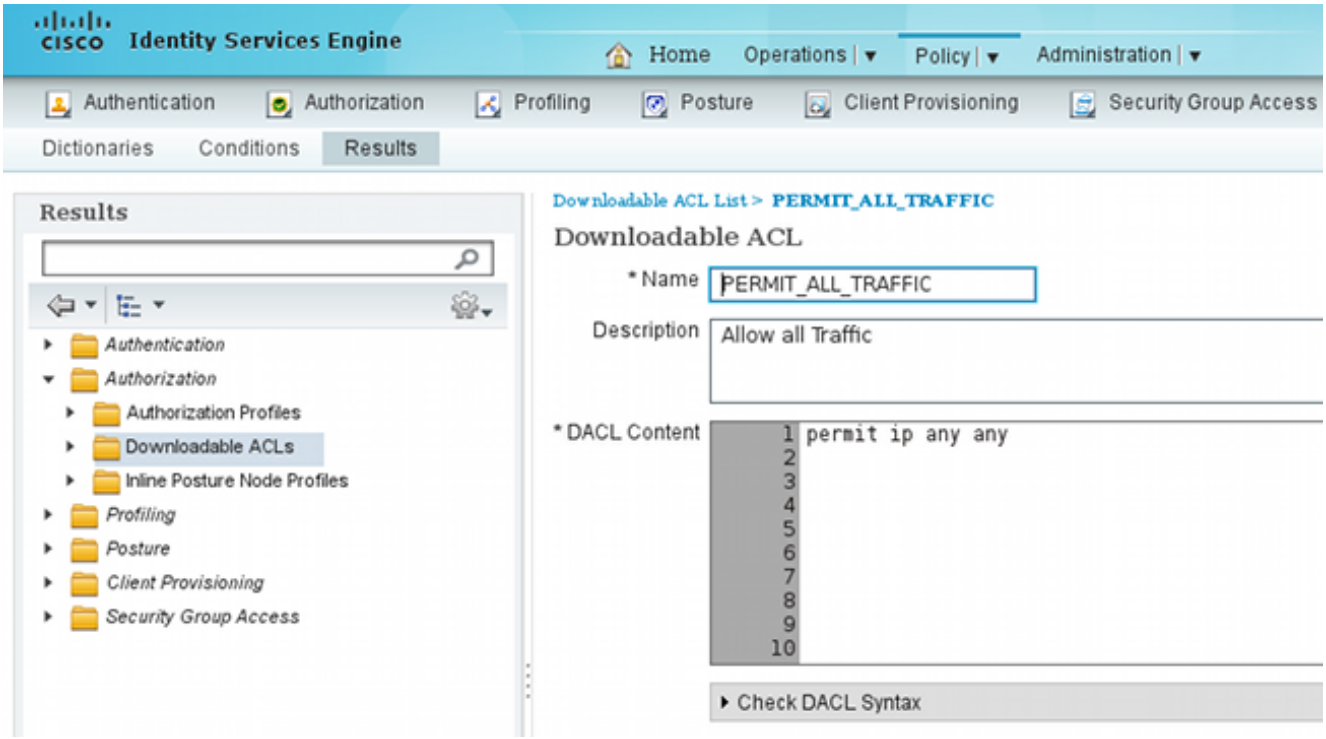
ISE

ISE を設定するには、次の手順を実行します。

1. [Administration] > [Network Resources] > [Network Devices] に移動し、ASA をネットワークデバイスとして追加します。

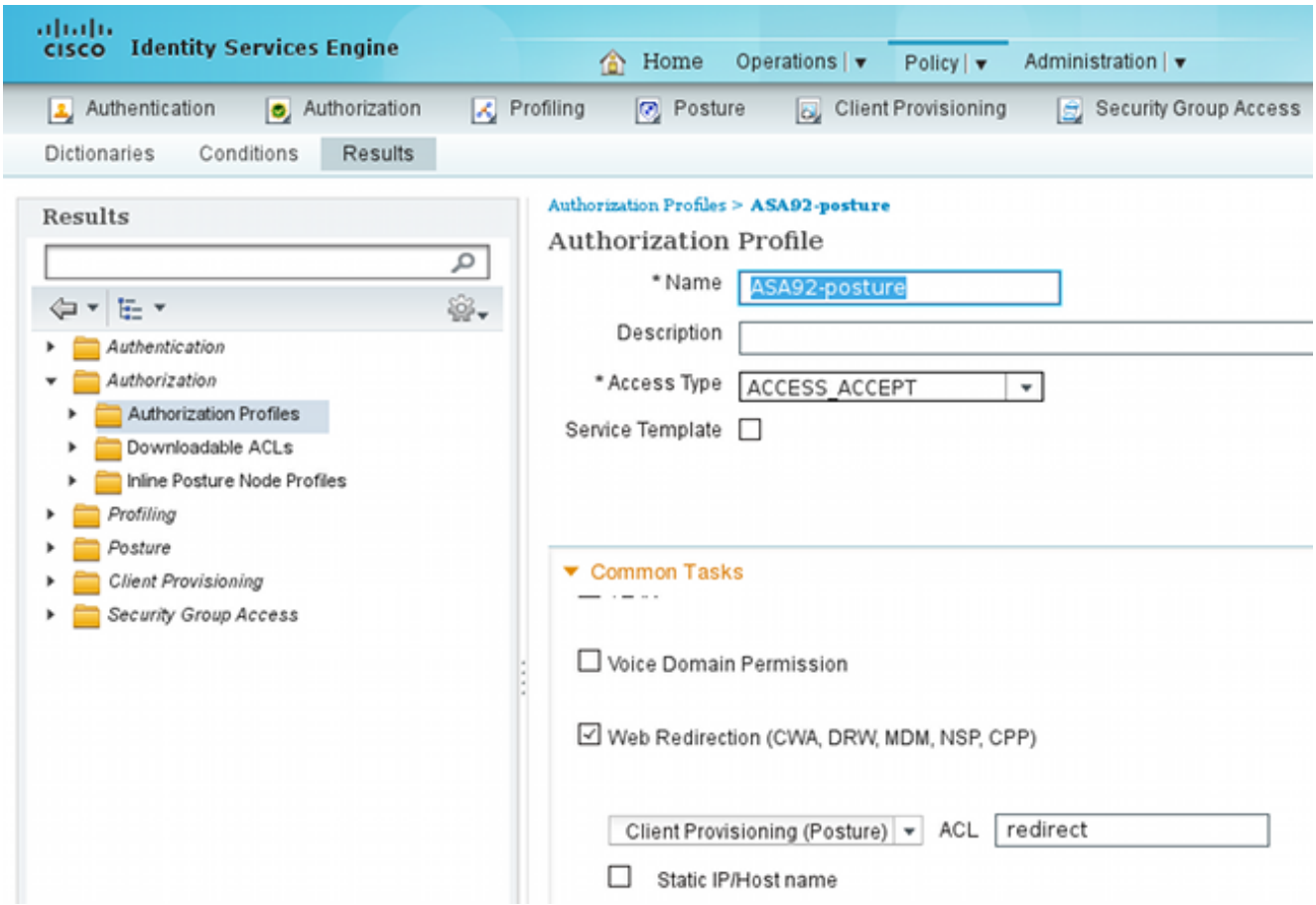


2. [Policy] > [Results] > [Authorization] > [Downloadable ACL] に移動し、フル アクセスを許可するように DACL を設定します。ACL のデフォルト設定では、ISE 上のすべての IP トラフィックを許可します。

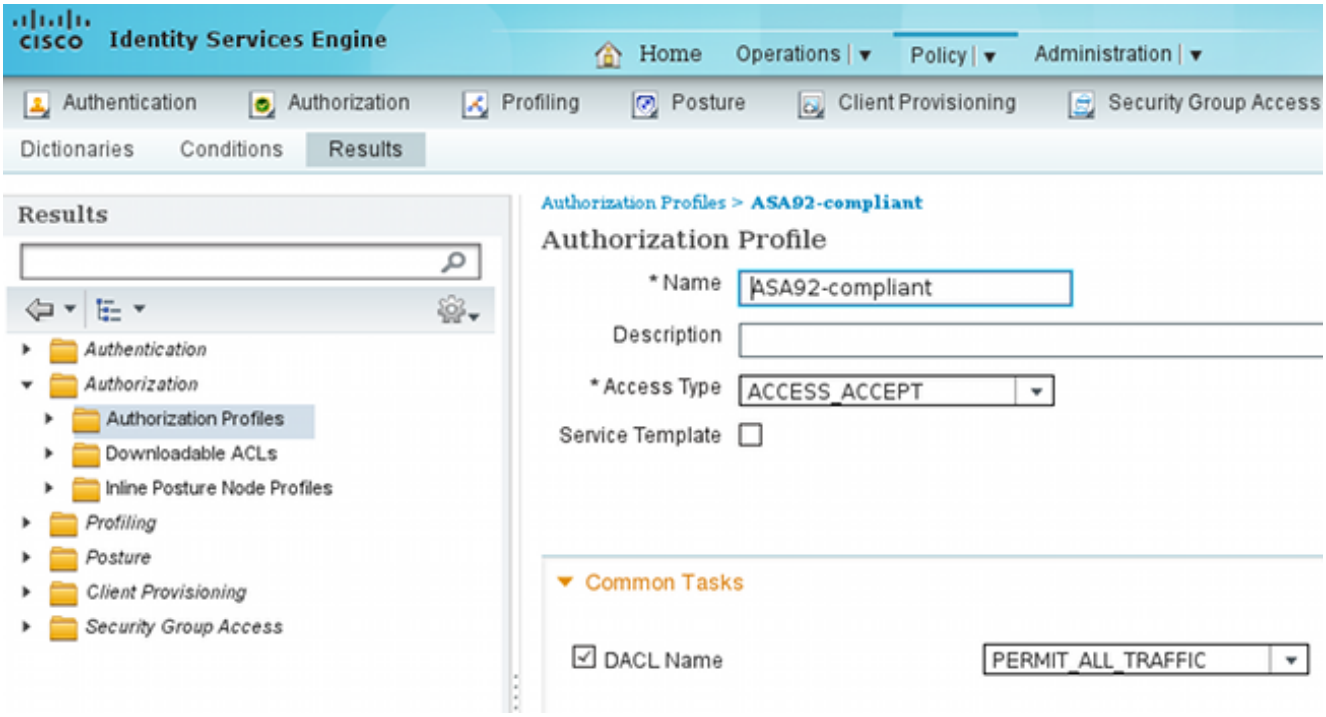


3. 制限付きアクセスを提供する同様の ACL を設定します（非準拠ユーザ向け）。

4. [Policy] > [Results] > [Authorization] > [Authorization Profiles] に移動し、**ASA92-posture という許可プロファイルを設定します。これが、ポスチャのためにユーザをリダイレクトします。**[Web Redirection] チェック ボックスをオンにし、ドロップダウン リストから [Client Provisioning] を選択し、[ACL] フィールドに **redirect** と表示されることを確認します。



5. **ASA92-compliant という名前の認証プロファイルを設定します。このプロファイルが、PERMIT_ALL_TRAFFIC という DACL だけを返すようにします。これにより、準拠するユーザにはフル アクセスが提供されます。**



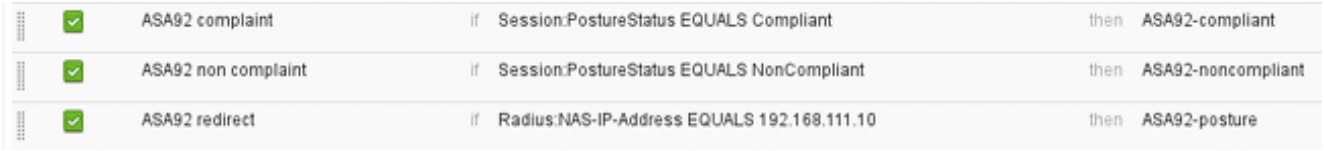
6. **ASA92-noncompliant** という名前の同様の認証プロファイルを設定します。このプロファイルは、制限付きアクセスを提供する DACL を返すようにします（非準拠ユーザ向け）。

7. [Policy] > [Authorization] に移動し、認証ルールを設定します。

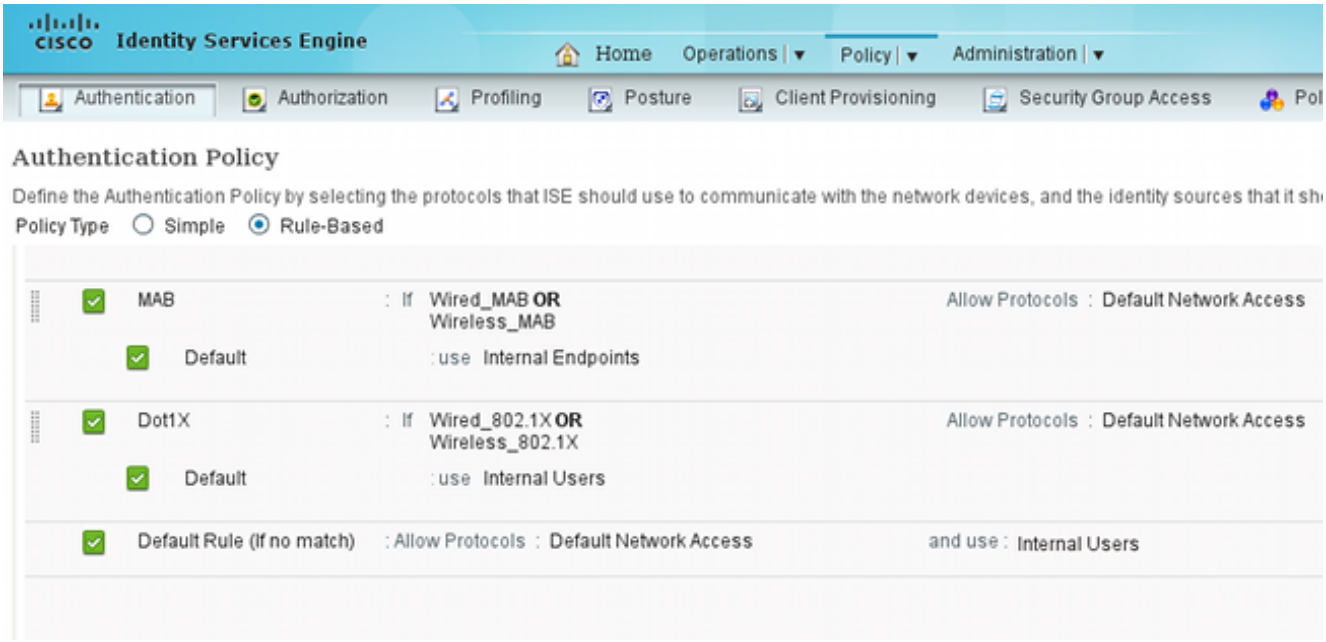
   ポスチャの結果が準拠する場合にフル アクセスを許可するルールを作成します。この結果が **ASA92-compliant** という認証ポリシーです。

   ポスチャの結果が準拠しない場合に制限付きアクセスを許可するルールを作成します。この結果が **ASA92-noncompliant** という認証ポリシーです。

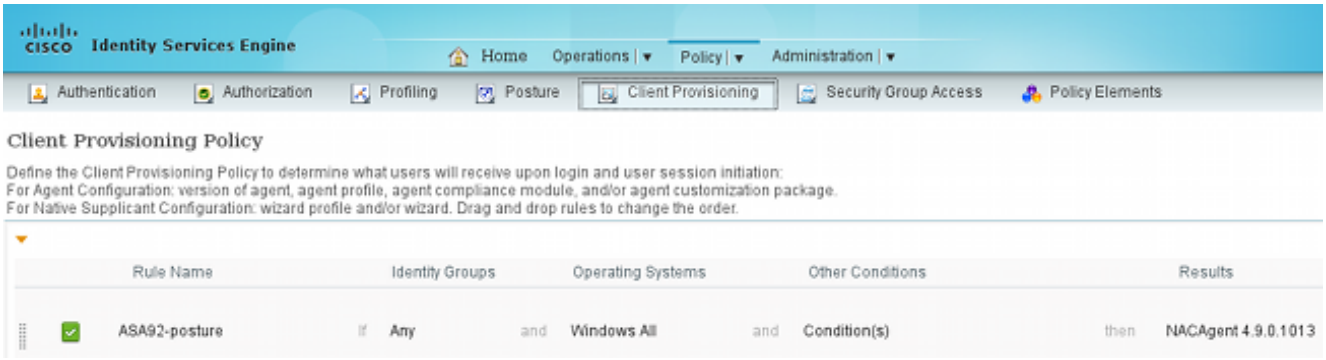
   上記の 2 つのルールのどちらにも該当しなかった場合にデフォルト ルールが **ASA92-posture** を返すようにします。これにより ASA でリダイレクションが強制的に実行されます。



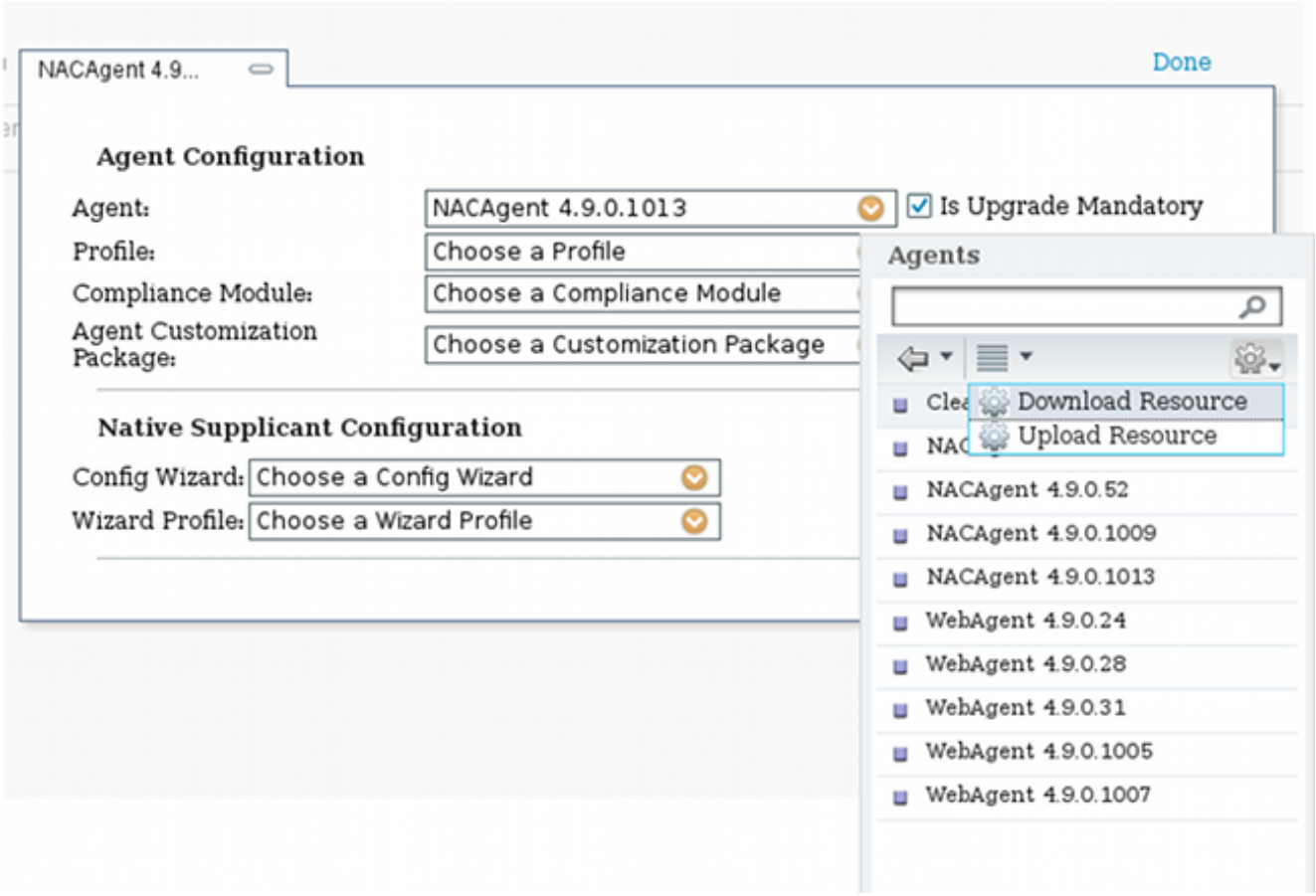
8. デフォルトの認証ルールは、内部 ID ストア内でユーザ名を確認します。この動作（たとえば、Active Directory（AD）での確認など）を変更する必要がある場合は、[Policy] > [Authentication] に移動し、変更を行います。



9. [Policy] > [Client Provisioning] に移動し、プロビジョニング ルールを設定します。これらは、プロビジョニングされるエージェントのタイプを決定するルールです。この例では、単純なルールが 1 つだけ存在し、ISE がすべての Microsoft Windows システムで NAC Agent を選択します。



エージェントが ISE 上にない場合はダウンロードできます。



10. 必要に応じて、[Administration] > [System] > [Settings] > [Proxy] に移動し、ISE のプロキシを設定できます（インターネット アクセスのための設定）。

11. クライアント設定を検証するポスチャ ルールを設定します。以下を確認するルールを設定できます。

    ファイル - 存在、バージョン、日付

    レジストリ - キー、値、存在

    アプリケーション - プロセス名、実行中、非実行中

    サービス - サービス名、実行中、非実行中

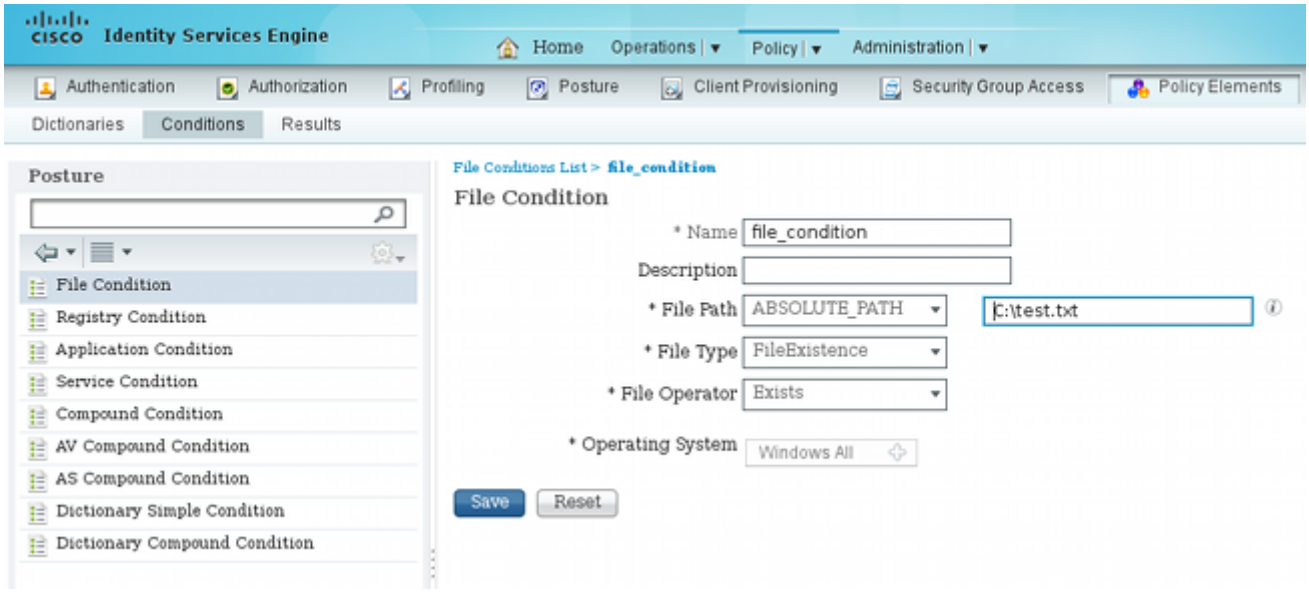
    ウイルス対策 - 100 を超えるベンダーをサポート、バージョン、定義更新のタイミング

    スパイウェア対策 - 100 を超えるベンダーをサポート、バージョン、定義更新のタイミング

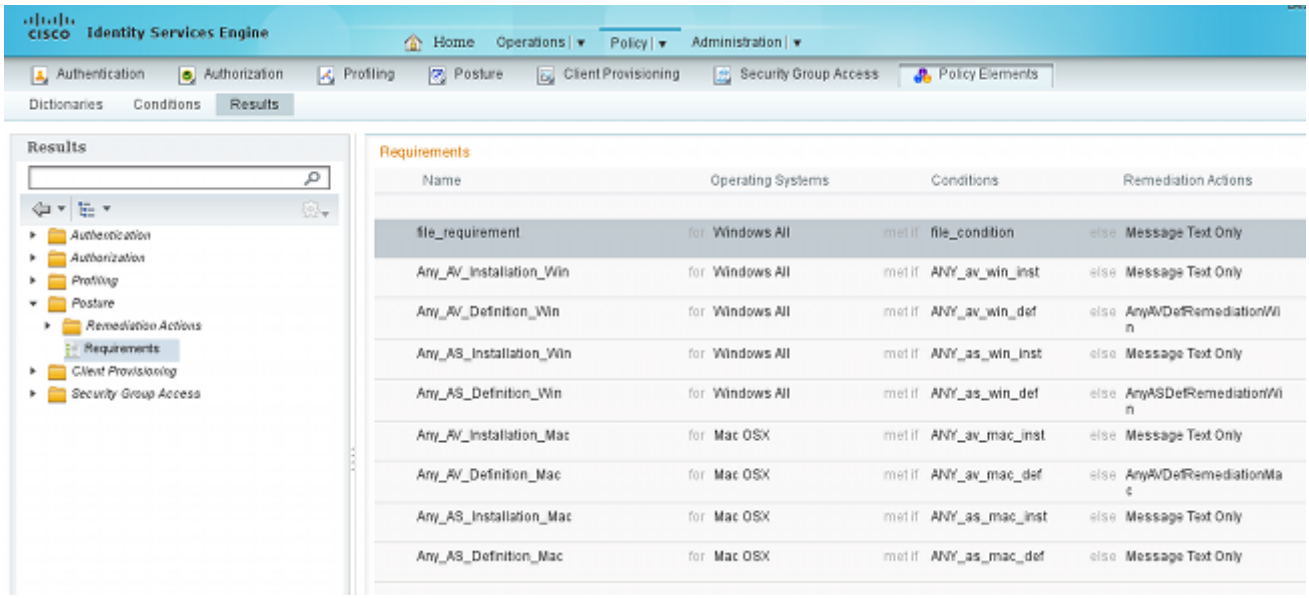
    複合条件 - すべての組み合わせ

    カスタム ディクショナリ条件 - ほとんどの ISE ディクショナリの使用状況

12. この例では、単純なファイルの存在チェックを実行します。**c:\test.txt ファイルがクライアント マシンに存在する場合は、準拠しているため、フル アクセスが許可されます。**
    [Policy] > [Conditions] > [File Conditions] に移動し、ファイル条件を設定します。

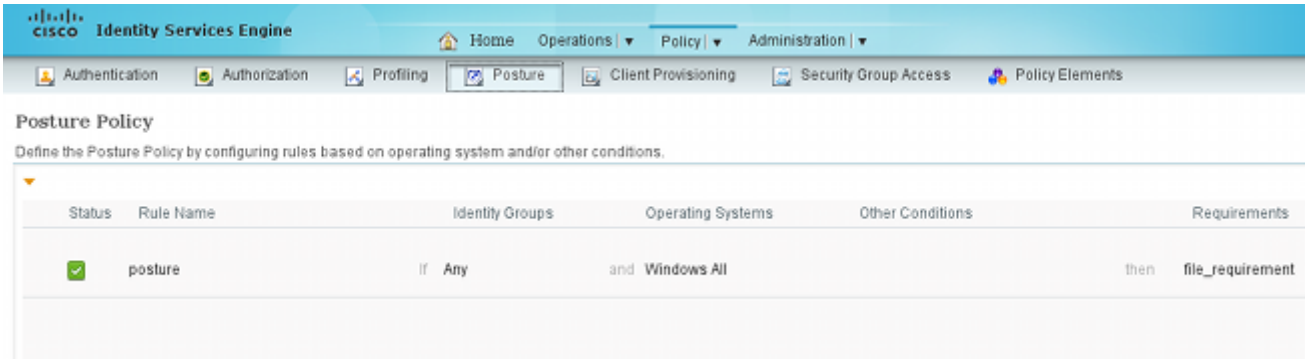


13. [Policy] > [Results] > [Posture] > [Requirements] に移動し、要件を作成します。この要件は、直前の条件を満たした場合に満たす必要があります。条件を満たさない場合は、修復アクションが実行されます。多くの種類の修復アクションを使用できますが、この例では最も単純な方法である特定のメッセージが表示されます。



注：通常のシナリオでは、ファイル修復アクションを使用できます（ISEはダウンロード可能なファイルを提供します）。

14. [Policy] > [Posture] に移動し、前の手順で作成した要件（**file_requirement**）**をポスチャ ルールに使用します。**唯一のポスチャ ルールは、すべての Microsoft Windows システムが **file_requirement** を満たすことです。この要件が満たされている場合、ステーションは準拠しています。要件が満たされていない場合、ステーションは非準拠です。

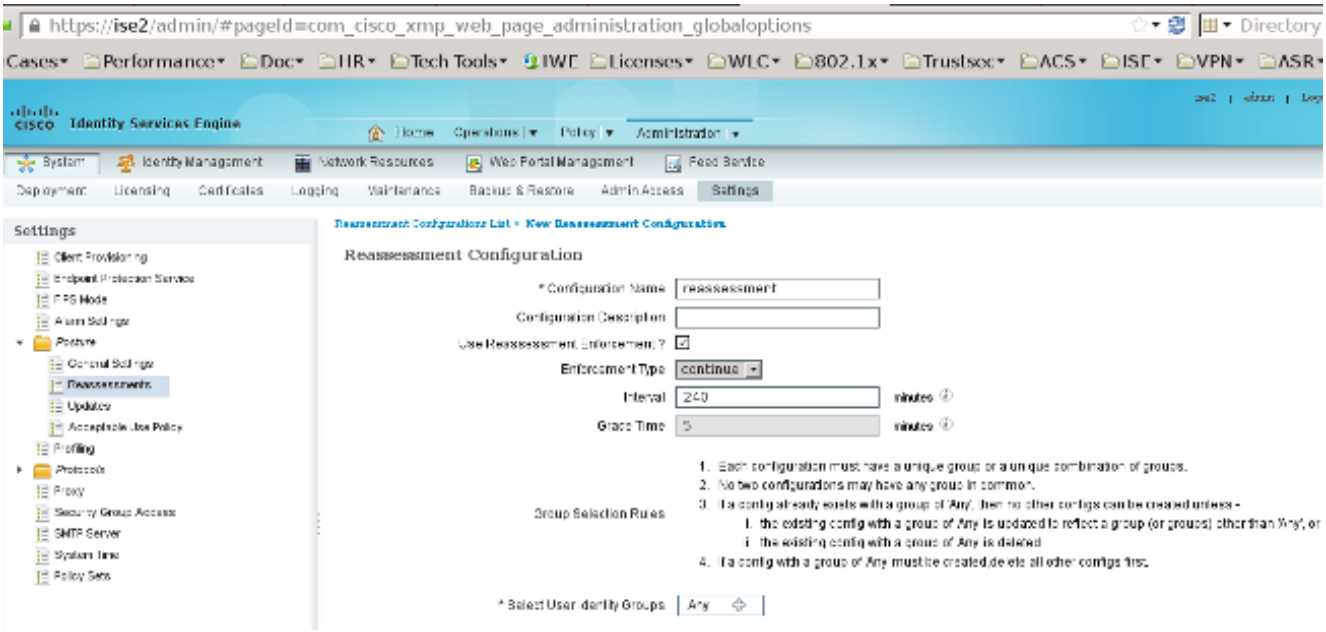


定期的再評価

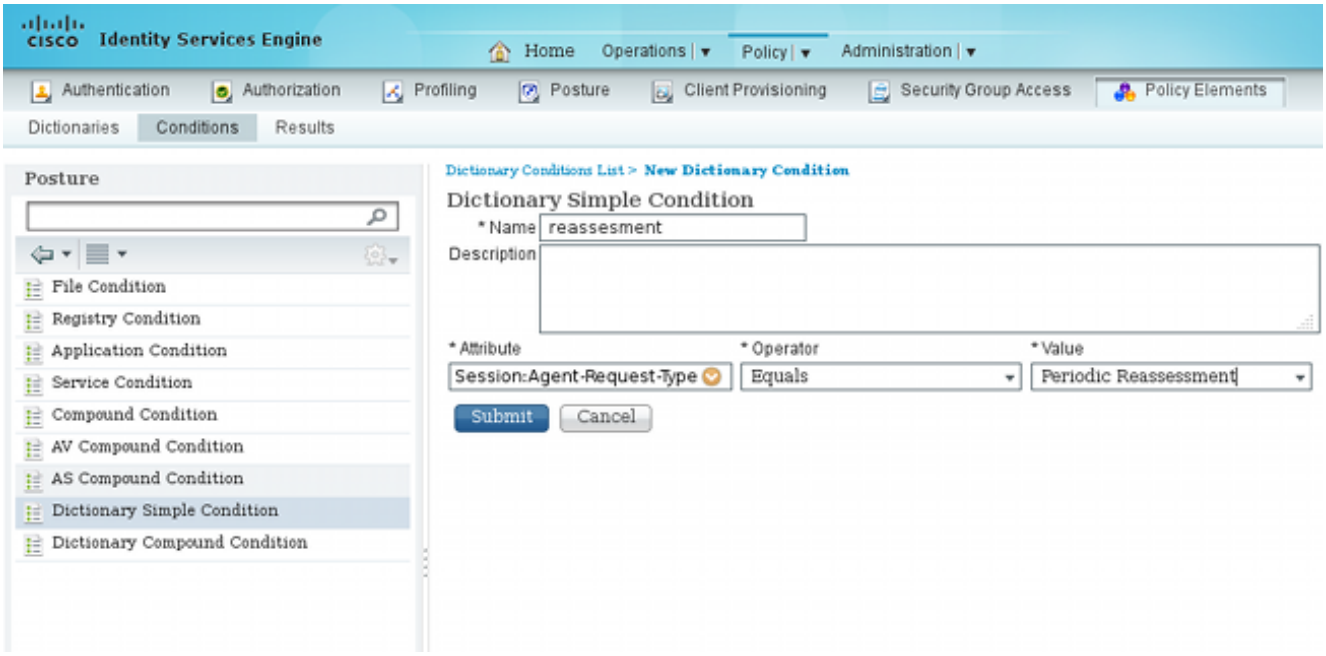
デフォルトでは、ポスチャはワンタイム イベントです。ただし、定期的にユーザの準拠性を確認し、その結果に基づいてリソースへのアクセスを調整しなければならない場合もあります。この情報は、SWISS プロトコル（NAC Agent）を介してプッシュされるか、アプリケーション（Web Agent）内にエンコードされています。

次の手順を実行して、ユーザの準拠性を確認します。

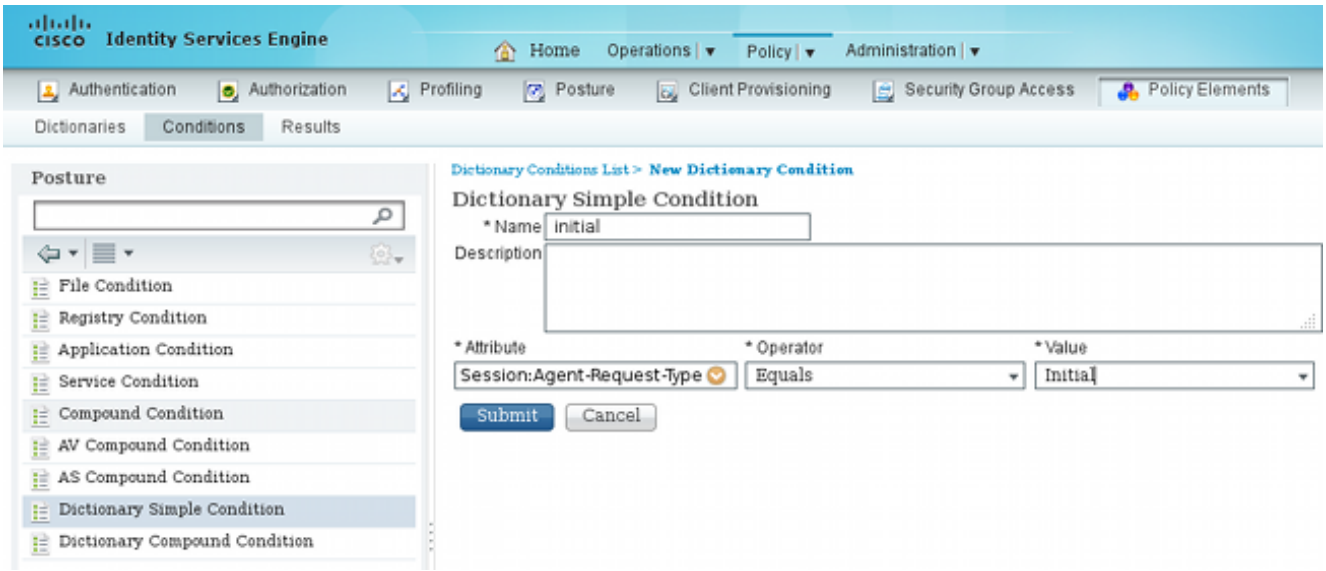
1. [Administration] > [Settings] > [Posture] > [Reassessments] に移動し、再評価をグローバルに有効にします（ID グループ設定ごと）。



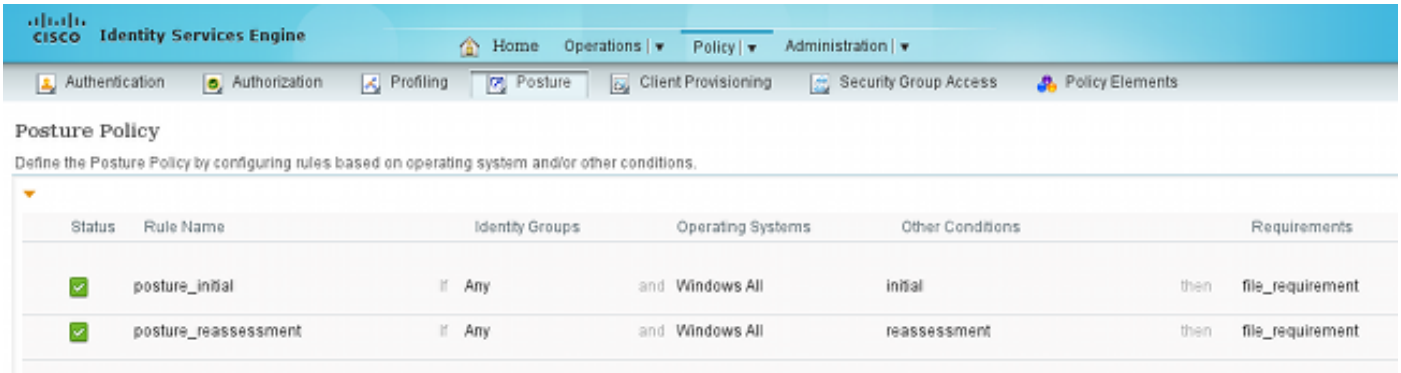
2. すべての再評価に一致するポスチャ条件を作成します。



3. 最初の評価のみと一致する同様の条件を作成します。



ポスチャ ルールではこの両方の条件を使用できます。最初のルールは最初の評価のみと一致し、2 番目のルールは後続のすべての評価と一致します。

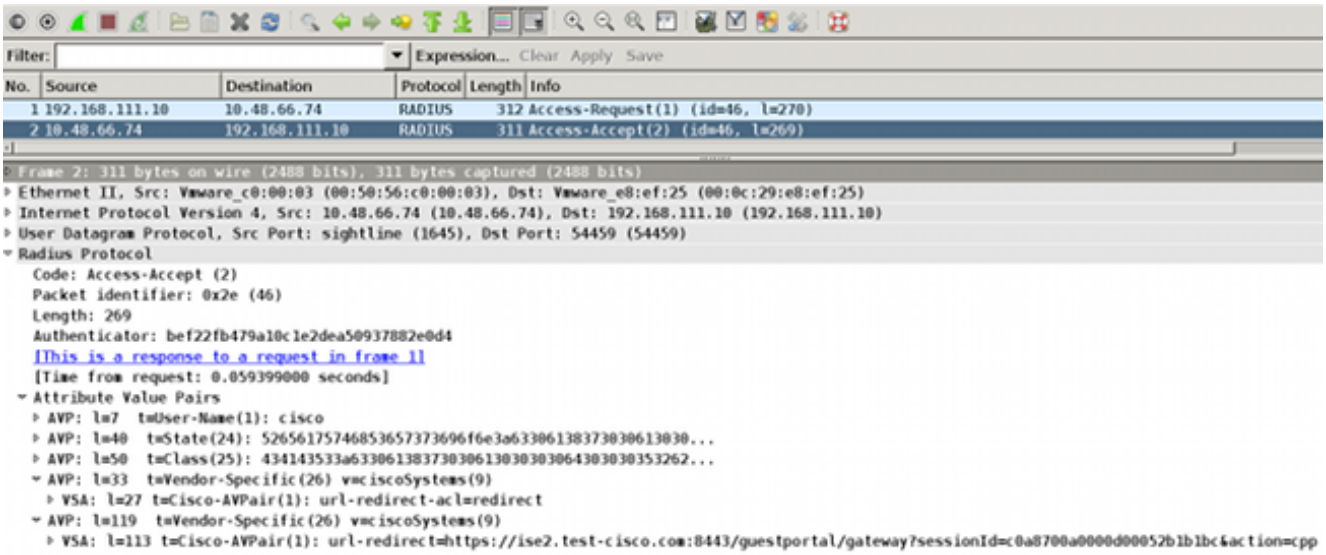


確認

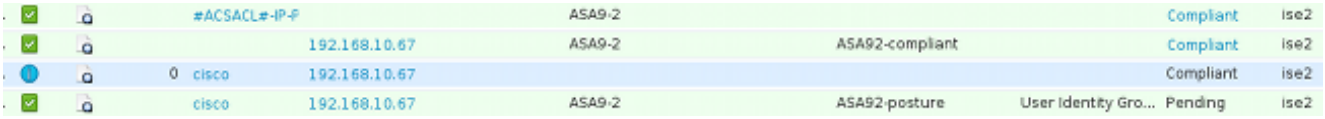
次の手順に従って、設定が正しく機能するかどうかを確認します。

1. VPN ユーザが ASA に接続します。

2. ASA が RADIUS-Request を送信し、**url-redirect 属性と url-redirect-acl 属性が含まれた応答を受信します。**



3. ISE ログには、認証がポスチャ プロファイルと一致したことが示されています（最初のログエントリ）。



4. ASA が VPN セッションにリダイレクトを追加します。

```
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 での VPN セッションのステータスにポスチャが必要であることが示され、HTTP トラフィックをリダイレクトします。

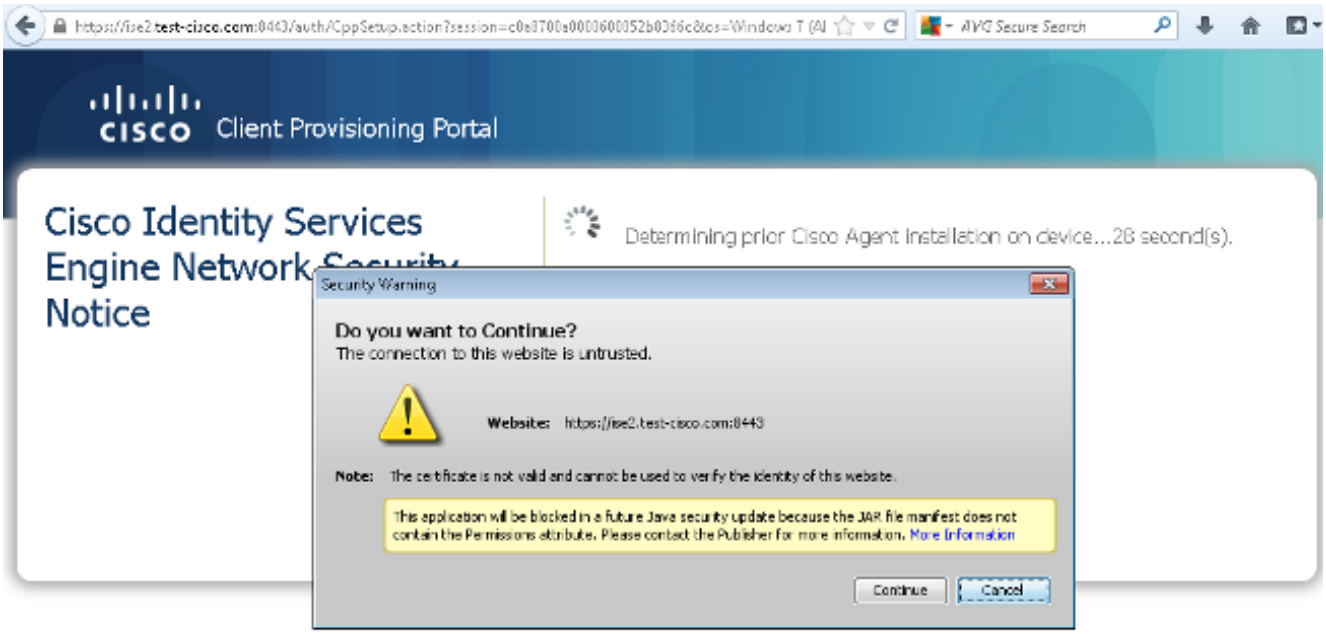
```
ASA# show vpn-sessiondb detail anyconnect

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. リダイレクト ACL と一致する HTTP トラフィックを開始するクライアントは、ISE にリダイレクトされます。

```
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. クライアントはポスチャのために ISE にリダイレクトされます。

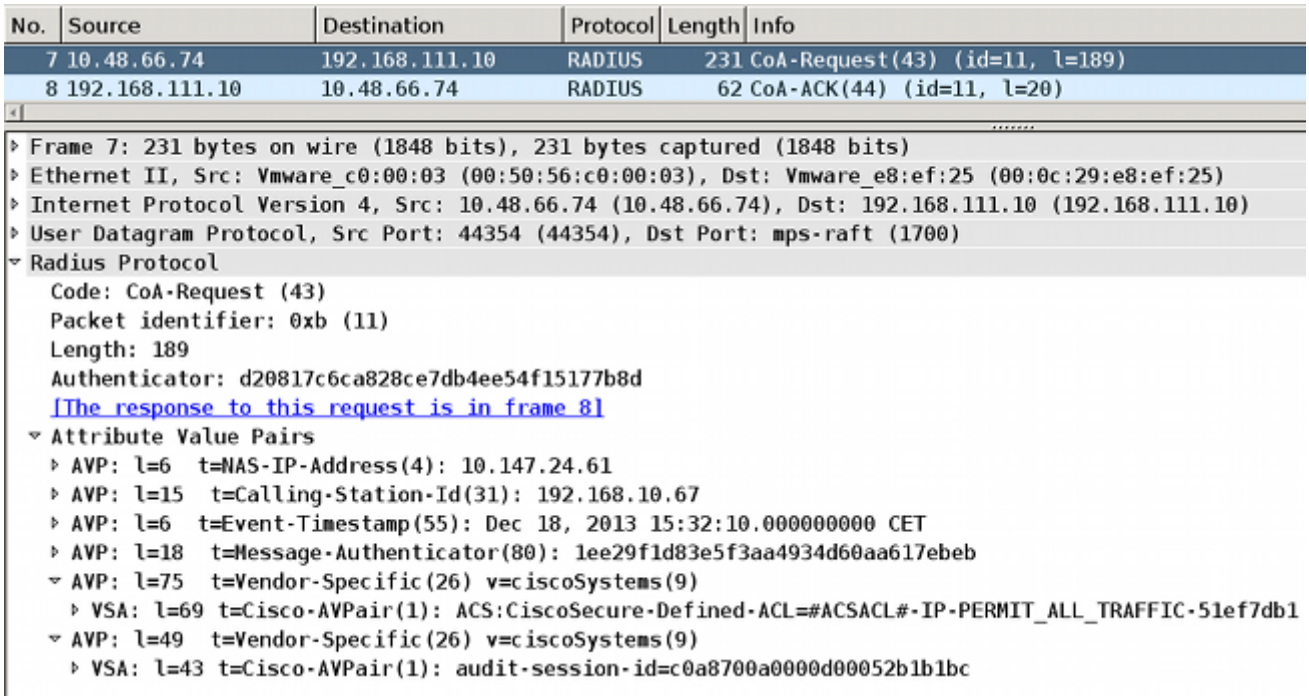


8. NAC Agent がインストールされます。NAC Agent がインストールされると、SWISS プロトコルを介してポスチャ ルールをダウンロードし、コンプライアンスを確認するためのチェックを実行します。ポスチャ レポートが ISE に送信されます。

9. ISE はポスチャ レポートを受信し、認証ルールを再評価し、（必要に応じて）認証ステータスを変更して CoA を送信します。これは **ise-psc.log** で確認できます。

```
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 は、**session_id を含む RADIUS CoA と、フル アクセスを許可する DACL 名を送信します。**



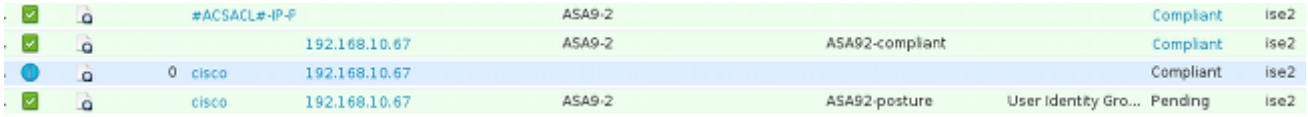
これは、ISE ログに反映されます。

最初のログ エントリは、ポスチャ プロファイルを返す（リダイレクションを伴う）最初の認証です。

2 番目のログ エントリは、準拠している SWISS レポートを受信した後に入力されます。

3 番目のログ エントリは、CoA が送信される（確認を伴う）ときに入力されます（「動的認証の成功」の説明を参照）。

最後のログ エントリは、ASA が DACL をダウンロードするときに作成されます。



11. ASA でのデバッグに、CoA を受信したこと、およびリダイレクトが削除されたことが示されています。ASA は必要に応じて DACL をダウンロードします。

```
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. VPN セッション終了後、シスコがそのユーザに DACL を適用します (フル アクセス) 。

```
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:CoAにDACLが接続されていない場合でも、ASAは常にリダイレクトルールを削除します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ISE でのデバッグ

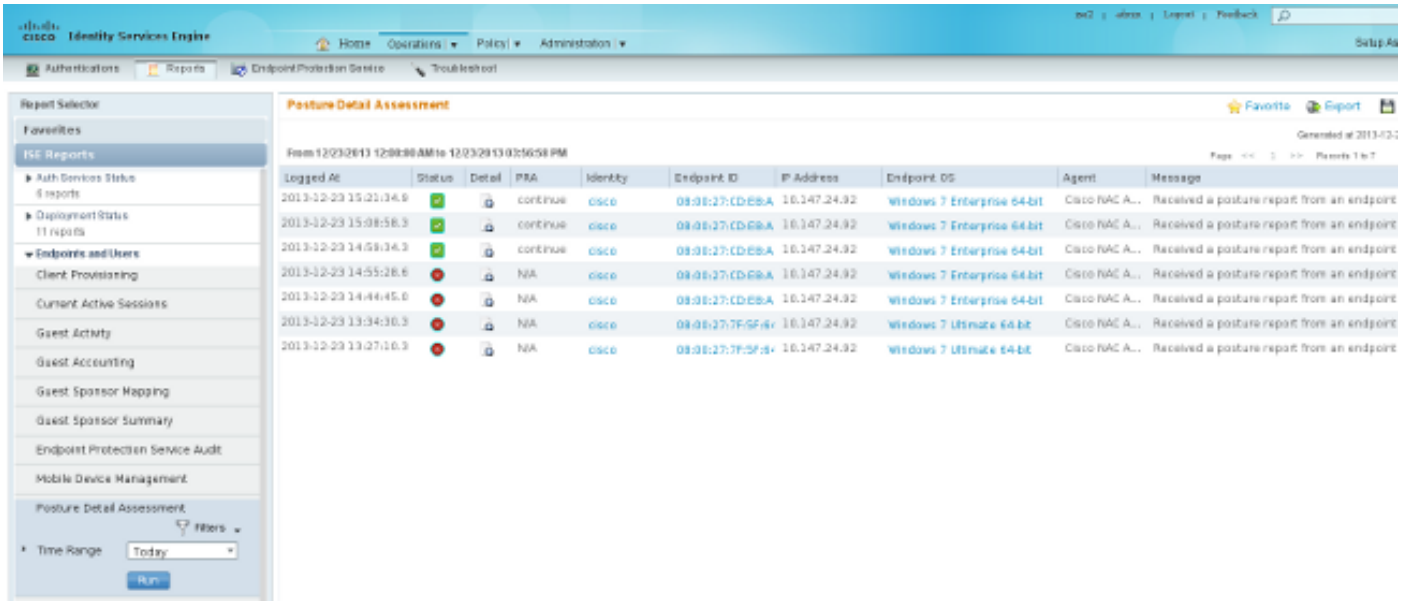
[Administration] > [Logging] > [Debug Log Configuration] に移動し、デバッグを有効にします。シスコでは、以下の一時的なデバッグを有効にすることを推奨します。

- SWISS
- Nonstop Forwarding（NSF）
- NSF-Session
- [Provision]
- ポスチャ

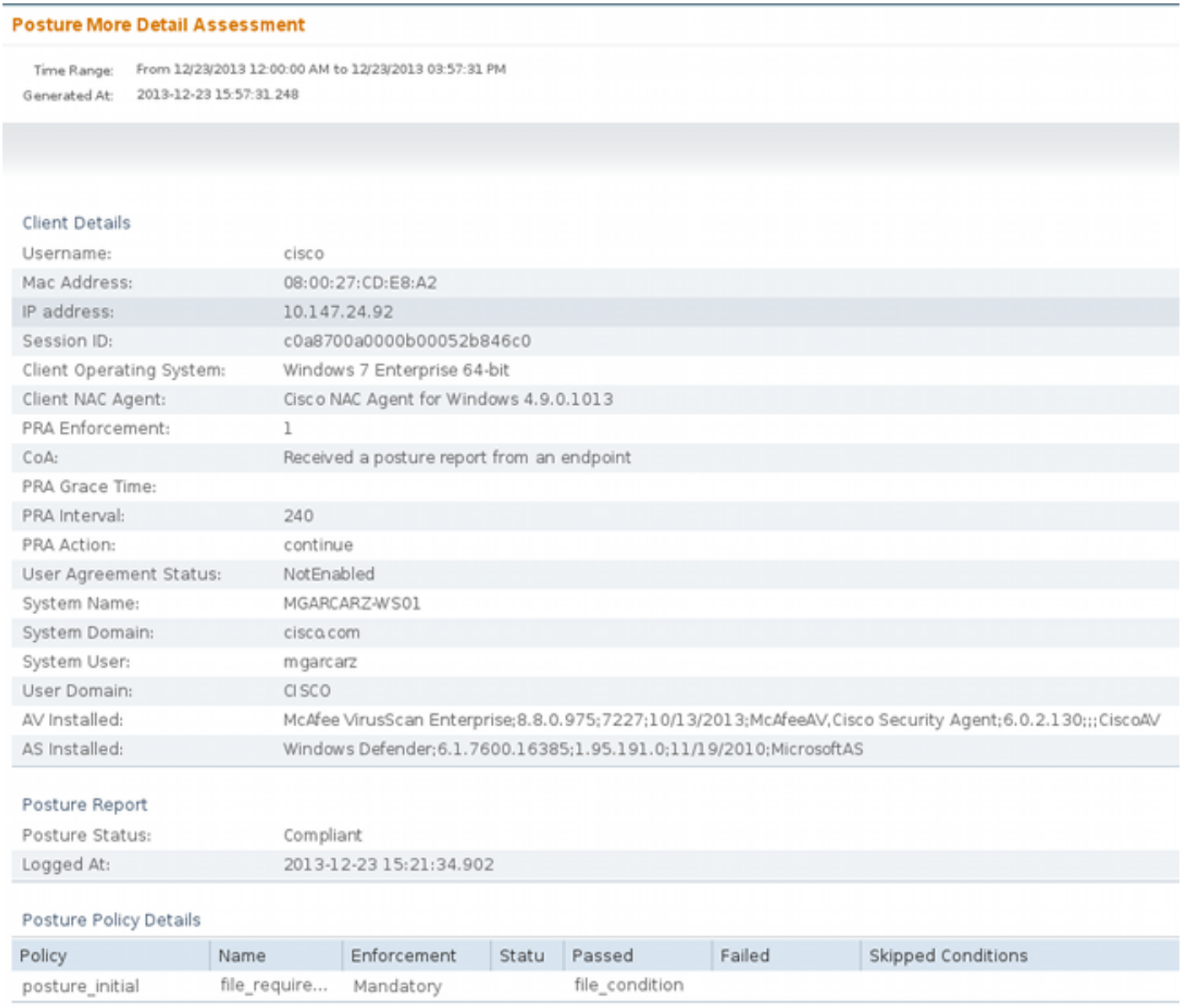
CLI で次のコマンドを入力して、デバッグを表示します。

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

[Operations] > [Reports] > [ISE Reports] > [Endpoints and Users] > [Posture Details Assessment] に移動し、ポスチャ レポートを表示します。



[Posture More Detail Assessment] ページに、ポリシー名と要件名が表示され、さらにその結果が表示されます。



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		

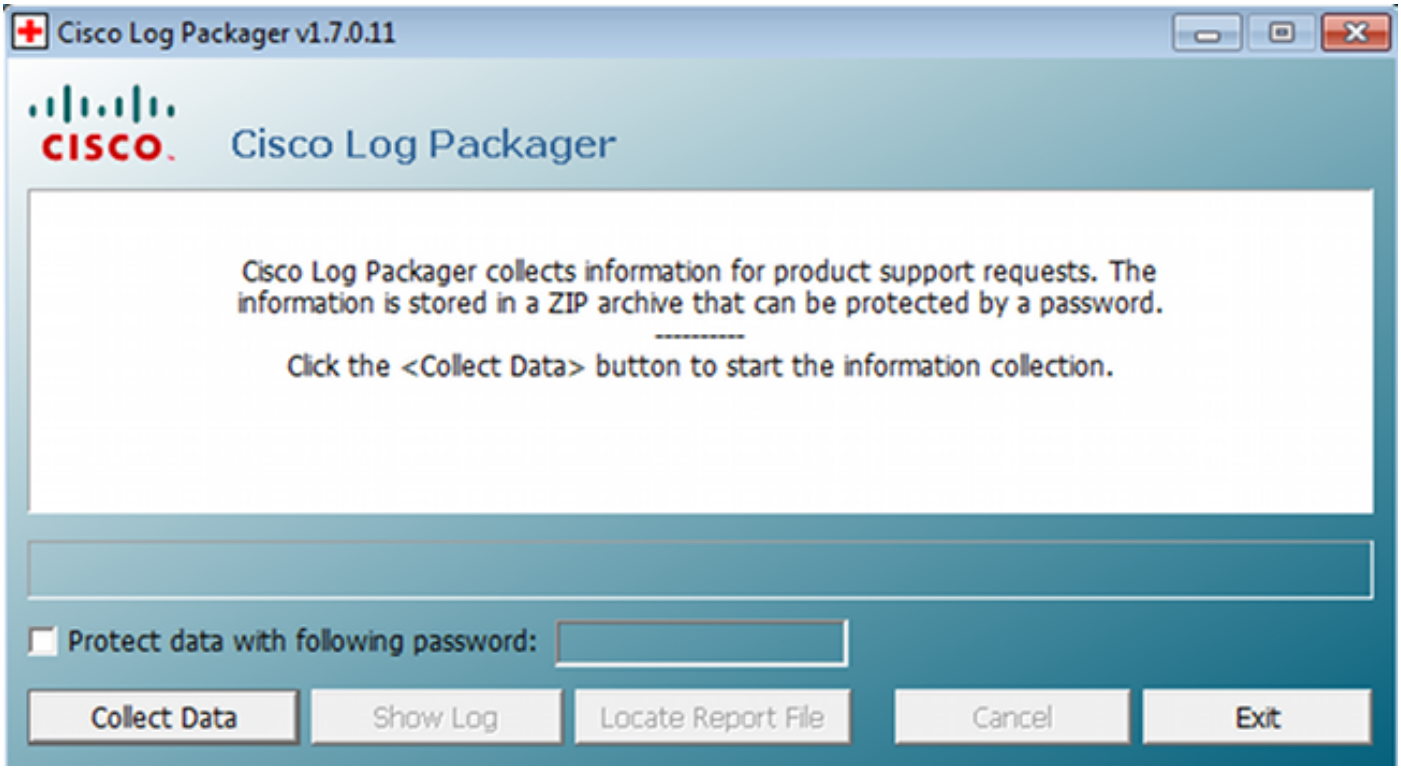
ASA でのデバッグ

ASA では以下のデバッグを有効にすることができます。

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

エージェントのデバッグ

NACエージェントの場合は、Cisco Log Packagerを使用してデバッグを収集できます。Cisco Log Packagerは、GUIまたはCLIで**CCAAgentLogPackager.app**を使用して開始します。



ヒント：結果をデコードするには、Technical Assistance Center(TAC)ツールを使用します。

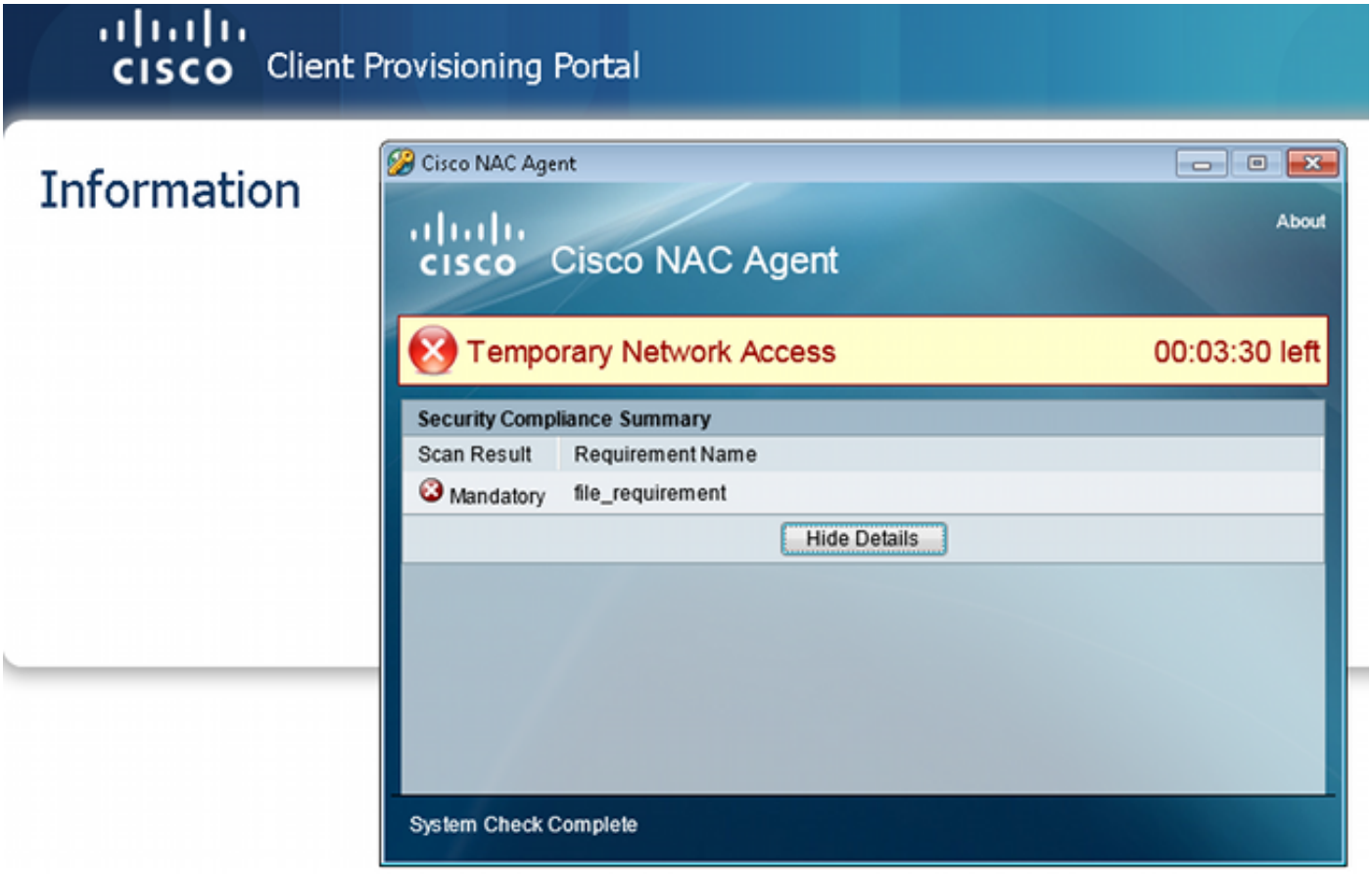
Web エージェントのログを取得するには、次の場所に移動します。

- C: > Document and Settings > ***<user> > Local Settings > Temp > webagent.log (TACツールでデコード)***
- **C: > Document and Settings > *<user>* > Local Settings > Temp > webagentsetup.log**

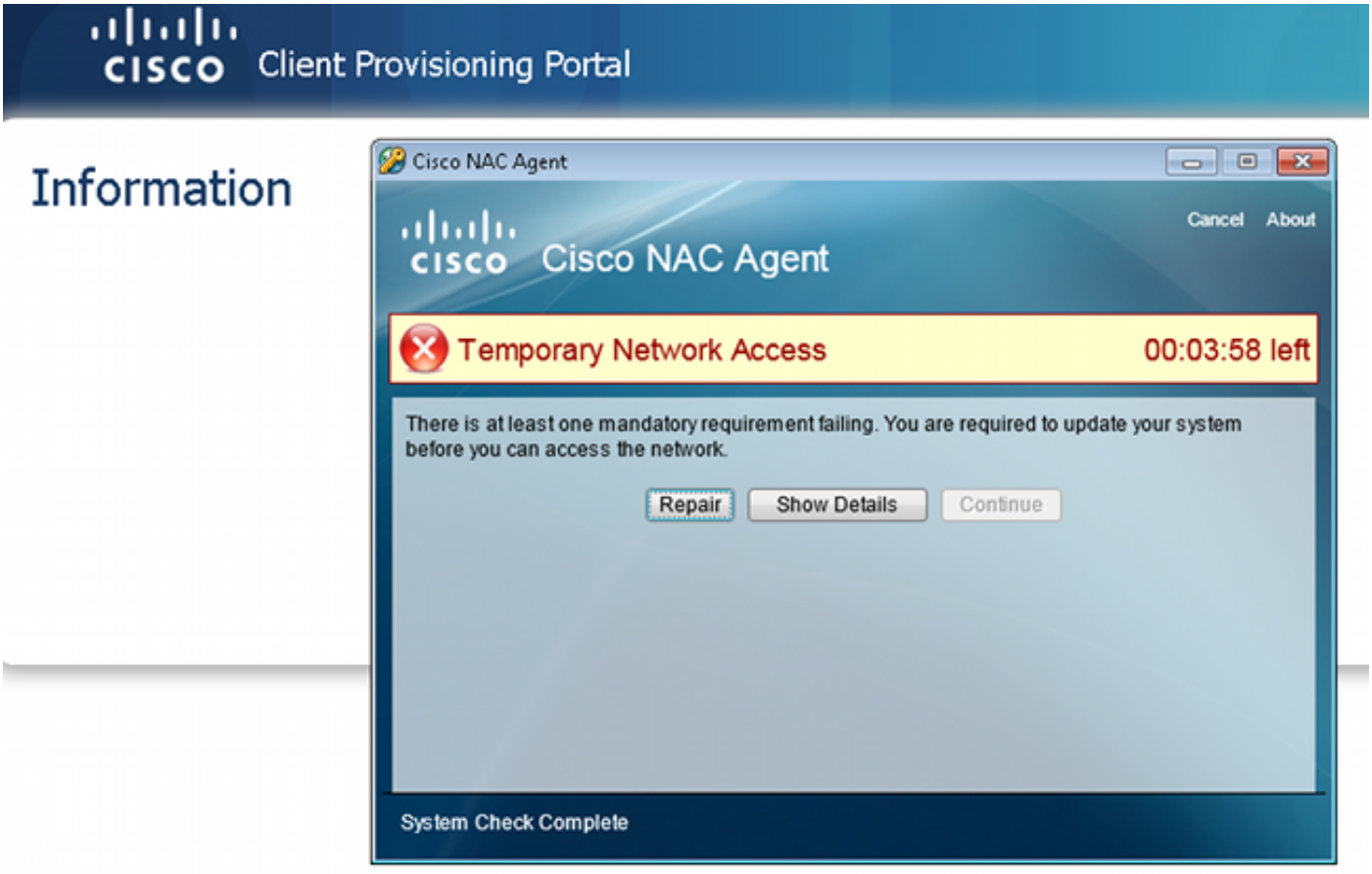
注：ログがこれらの場所にない場合は、**TEMP Environment**変数を確認します。

NAC エージェント ポスチャの障害

ポスチャが失敗した場合は、次のようにその原因が表示されます。



修復アクションが設定されている場合は、ユーザに修復アクションの実行が許可されます。



関連情報

- セキュリティ アプライアンスのユーザ認証に外部サーバを設定
- Cisco ASA シリーズ VPN CLI 構成ガイド 9.1
- 『Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2) 』
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。