带有安全状态授权变更功能的 Cisco ISE 和 ASA。

ISE/ASA CoA 集成操作指南：

目录

Cisco ISE 和 ASA 与 CoA 集成

解决方案概述

本文重点关注身份服务引擎 (ISE) 通过执行安全状态评估确定终端状态的能力。在 ASA 9.2.1 发布以前，需要安全状态功能的 VPN 用户都需要在 VPN 基础设施和受局域网保护的网络之间建立 Inline Posture 节点 (IPN)。随着 ASA 9.2.1 的发布，我们现在能够执行策略，ASA 和 ISE 也能够在安全状态评估执行之后发送“策略推送”。

本文档将向管理员逐一介绍用于授权变更的 ASA 和 ISE 的基本配置组件。

组件

- Cisco ISE 1.2 补丁 5 或更高版本
- 采用 ASDM 7.2(1) 或更高版本的 ASA 9.2.1
- AnyConnect 3.1 MR 6 或更高版本
- NAC 代理 4.x（更新版）或更高版本

网络图

使用 ASDM 针对 CoA 配置 ASA

本节将在 ASA 上启用 CoA 功能。通过启动 ASDM 客户端连接到您的 ASA。

注意：本节执行的 CLI 配置可在下一节中找到，命令在“**使用 CLI 针对 CoA 配置 ASA 9.2.1**”一节中提供。

配置隧道组和身份验证方式

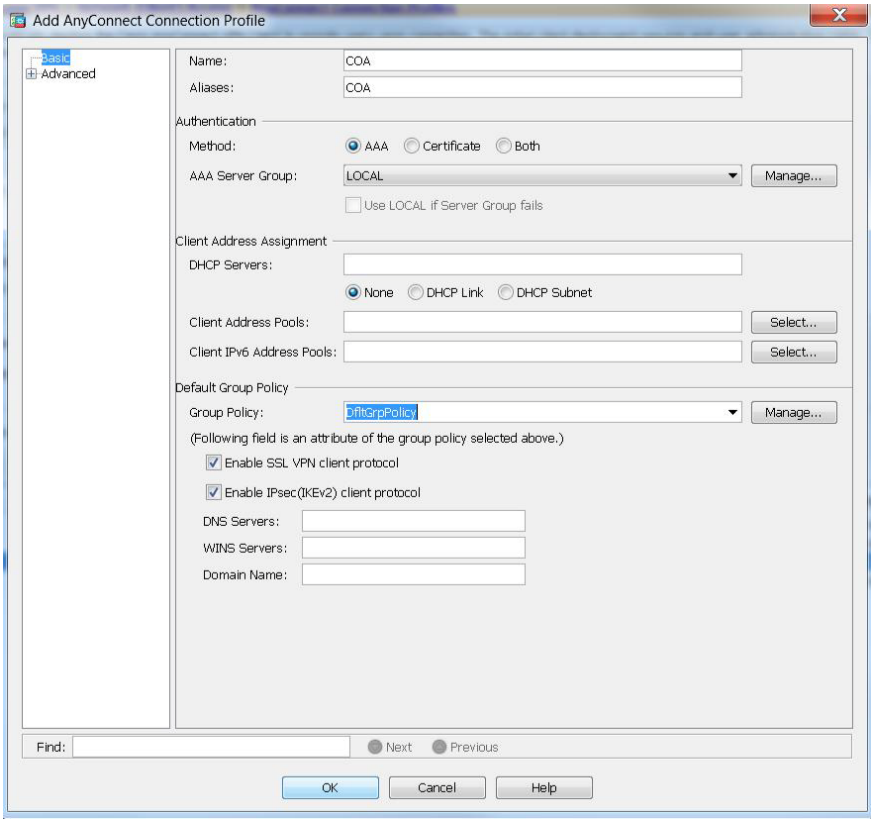
ASA 设备提供两个默认渠道组，一个用于远程访问 (DefaultRAGroup)，一个用于无客户端 (DefaultWEBVPNGroup)。在本文档中，我们将创建一个新的隧道组，并将其命名为 **COA**。我们还需要配置身份验证方式，并使其指向用于 RADIUS 身份验证的 ISE。在 VPN 用户连接到其公司头端时，其 AnyConnect 下拉列表选项中将出现一个名为 **COA** 的渠道组。

本节将指导您配置**重定向 ACL**（访问控制列表），ISE 将在初次进行 VPN 连接时使用该列表，直至用户将被置于合规状态。用户合规后，ISE 便将推送一个带有一组新访问权限的新 dACL（动态访问控制列表）。

步骤 1：导航至**配置 (Configuration) 远程访问 VPN (Remote Access VPN)→→网络（客户端）访问 (Network[Client]Access)→→AnyConnect 连接配置文件 (AnyConnect Connection Profiles)**，选择**添加 (Add)**。

步骤 2：在 **AnyConnect 连接配置文件 (AnyConnect Connection Profiles)** 中：

- 输入名称：（示例：COA）
- 输入别名：（示例：COA）



步骤 3：在“身份验证”(Authentication) 下。

根据您的公司策略，您可以在 **AAA**、**证书 (Certificate)** 或**两者 (Both)** 之间进行选择。

- 方法：为简化配置，我们选择使用 **AAA**

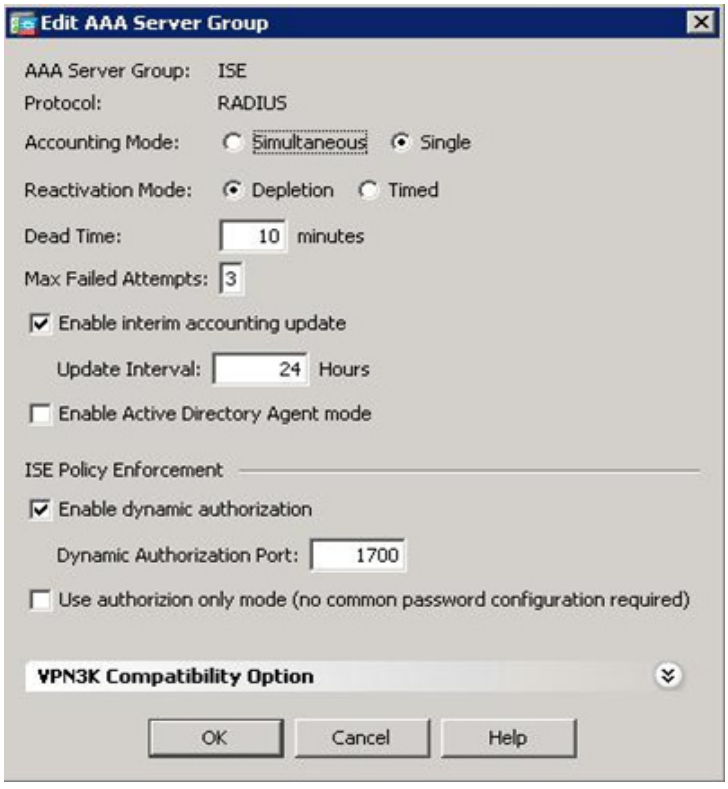
注意：如果使用证书身份验证，您必须在下面的配置中启用“使用仅授权模式”(Use Authorize only mode)。

- 在“AAA 服务器组”(AAA Server Group) 中：选择**管理 (Manage)**
  - 系统将弹出一个名为**配置 AAA 服务器组 (Configure AAA Server Groups)** 的新窗口，在 **AAA 服务器组 (AAA Server Groups)** 下选择**添加 (Add)**
    - 输入 AAA 服务器组的名称：（示例：**ISE**）
    - 协议 (Protocol)：**RADIUS**
    - 记帐模式 (Accounting mode)：Single（默认设置）
    - 重新激活模式 (Reactivation Mode)：Depletion（默认设置）
    - 停滞时间 (Dead Time)：10（默认设置）
    - 最大失败尝试次数 (Max Failed Attempts)：3（默认设置）
    - 选中方框**启用临时记帐更新 (Enable interim accounting update)**
    - 在“ISE 策略执行”(ISE Policy Enforcement) 下，选中方框**启用动态授权 (Enable dynamic authorization)**

注意：这可启用 ASA 授权变更 (CoA)

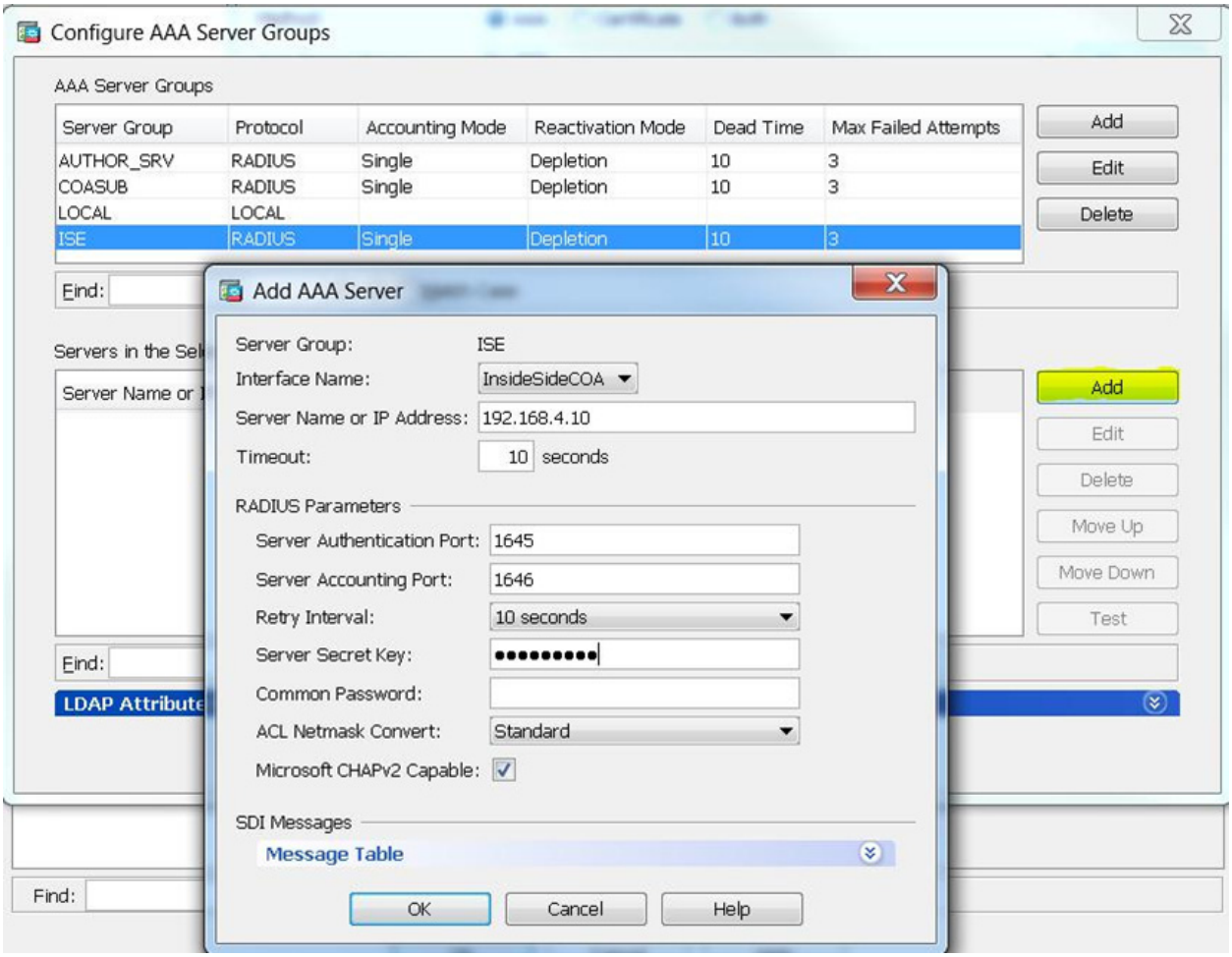
- 保留默认的 1700 端口不动，点击**确认 (OK)**

下面是配置的屏幕截图。



- 高亮显示新创建的 ISE AAA 服务器组，在**所选组中的服务器 (Server in the Selected Group)** 下选择**添加 (Add)**

  - 接口名称 (Interface Name)：选择可连接 ISE 服务器的相应接口
  - 服务器名称或 IP 地址 (Server Name or IP Address)：这是 ISE 服务器的 IP 地址
  - 超时 (Timeout)：10 秒 (10 seconds)（默认设置）
  - 服务器身份验证端口 (Server Authentication Port)：1645（默认设置）支持 1812
  - 服务器记帐端口 (Server Accounting Port)：1646（默认设置）支持 1813
  - 重试间隔 (Retry Interval)：10 秒 (10 seconds)（默认设置）
  - 服务器密钥 (Server Secret Key)：输入一个稍后将在 ISE 配置部分中用到的短语
  - 常用密码 (Common Password)：
  - ACL 子网掩码转换器 (ACL Netmask Converter)：标准 (Standard)（默认设置）
  - 支持 Microsoft CHAPv2 (Microsoft CHAPv2 Capable)：启用（默认设置）
  - 选择**确定 (OK)**，然后再次选择**确定 (OK)** 以接受**配置 AAA 服务器组 (Configure AAA Server Groups)** 弹出框，并回到**添加 AnyConnect 连接配置文件 (Add AnyConnect Connection Profile)** 弹出框

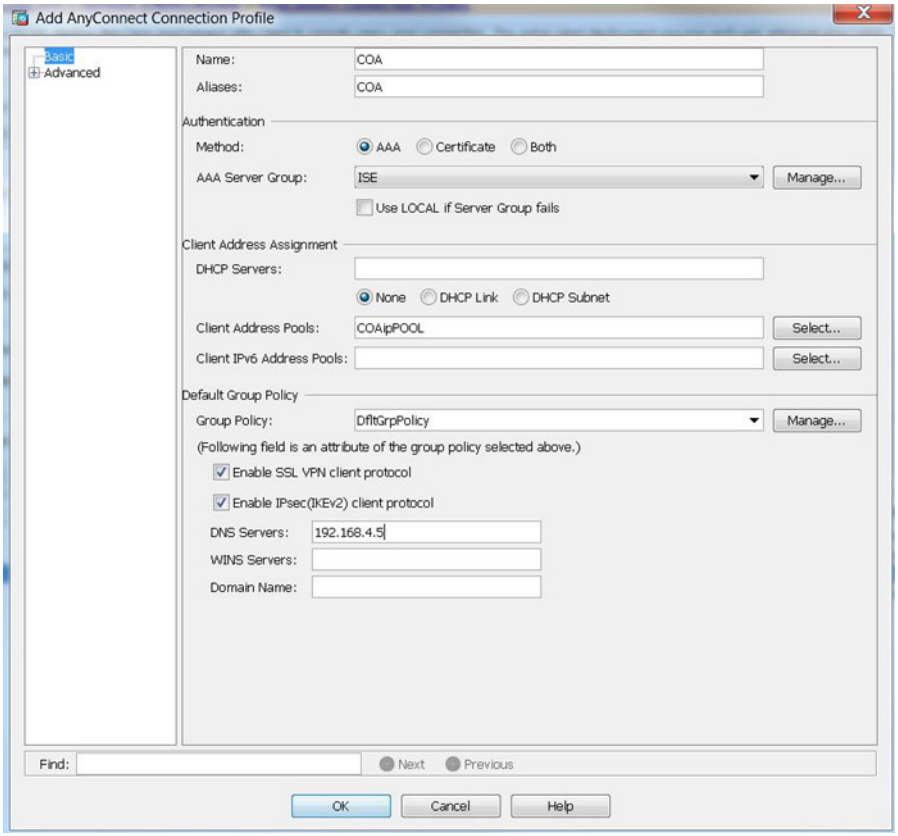


步骤 4：在“客户端地址分配”(Client Address Assignment) 下。

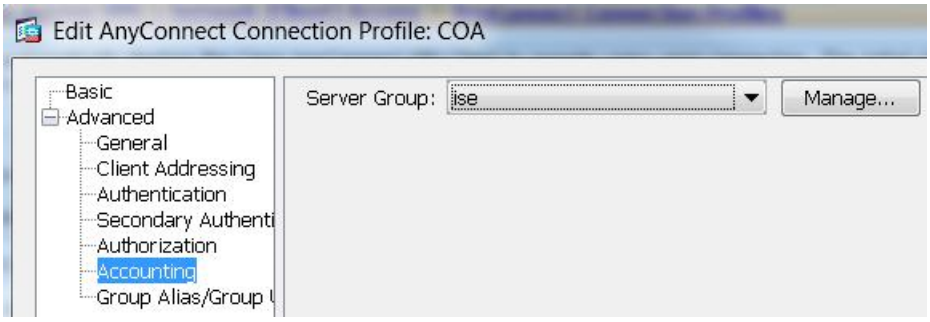
- 客户端地址池 (Client Address Pools)：分配相应的 VPN IP 池

步骤 5：在“默认组策略”(Default Group Policy) 下。

- 组策略 (Group Policy)：选择相应的组策略
- 启用 SSL 或 IKEv2 协议，或同时启用两者
- DNS 服务器 (DNS Servers)：这些 DNS 服务器将被送往 AnyConnect 客户端。在此字段中输入将用于解析 ISE 服务器 IP 地址的 DNS 服务器



- 在“连接”(Connection) 配置文件中，展开“高级”(Advance) 选项，将“记帐”(Accounting) 配置为指向 ISE



- 选择**确定 (OK)** 和**应用 (Apply)** 以应用您的配置

配置用于安全状态重定向的 ACL

步骤 1：导航至**配置 (Configuration) →→防火墙 (Firewall) →→高级 (Advanced) →→ACL 管理器 (ACL Manager)**，选择**添加 ACL (Add ACL)**。

步骤 2：ACL 名称：输入 ACL 访问权限，让用户能以之预先进行安全评估，示例名称为“redirect”

步骤 3：高亮显示新创建的 ACL，添加 ACE 访问规则，并为客户端提供足够的访问权限以允许其修复不可信的系统。在示例中，规则 1 和 2 允许 NAC 发现我们的 ISE 服务器，规则 3 提供 AD/DNS，规则 4 和 5 提供对我们的 AV 和 Microsoft 补丁服务器的访问权限，规则 6 是允许重定向所有其他流量的允许 HTTP。

#	Enabled	Source	... ... Destination	... Service	Action	... ... Description
redirect						
1	☑	any	192.168.1.10	8905	Deny	swiss
2	☑	any	192.168.1.10	8905	Deny	swiss
3	☑	any	192.168.1.5	domain	Deny	DNS Server
4	☑	any	192.168.1.15	ip	Deny	AV Server
5	☑	any	192.168.1.20	ip	Deny	Microsoft Patch Server
6	☑	any	any	http	Permit	Allow for redirect

注意：ISE 还能够限制 ISE 发送的 dACL 的特定用户组访问权限。

使用 CLI 针对 CoA 配置 ASA

本节介绍可配置 CoA 的 ASA 的命令行界面。

步骤 1：创建 AAA 服务器组。

- ASA> en
  Password: *********
  ASA# conf t
  ASA(config)# aaa-server ISE protocol radius ASA(config-aaa-server-group)# interim-accounting-update ASA(config-aaa-server-group)# dynamic-authorization ASA(config-aaa-server-group)# aaa-server ISE host 192.168.4.10 ASA(config-aaa-server-host)# timeout 21 ASA(config-aaa-server-host)# key **********
  ASA(config-aaa-server-host)#
  exit ASA(config)#

步骤 2：创建“未知或非合规”状态所需的访问列表。修复客户端所需的任何方面都需要创建访问列表。在此使用案例中，我们将流量限制到 DNS、ISE、AV 服务器和 Microsoft Patch Management 的 AD。计算机通过安全评估后，此 ACL 将在 CoA 生效后被另一 DACL 所替代。在本文档中，我们将此 ACL 称为 **redirect**，并将在稍后配置 ISE 时调用此 ACL。

- ASA(config)# access-list redirect remark exclude ISE server
  ASA(config)# access-list redirect extended deny ip any4 host 192.168.4.10 (hostname/IP of ISE server)
  ASA(config)# access-list redirect remark exclude DNS server
  ASA(config)# access-list redirect extended deny ip any4 host 192.168.4.5 (hostname/IP of DNS server)
  ASA(config)# access-list redirect remark redirect all other traffic
  ASA(config)# access-list redirect permit ip any4 any4

步骤 3：创建隧道组并应用 VPN IP 地址池和 AAA 服务器组。

- ASA(config)# tunnel-group “CoA” type remote-access
  ASA(config)# tunnel-group “CoA” general-attributes
  ASA(config-tunnel-general)# address-pool **add in your “**IP pool address” ASA(config-tunnel-general)# authentication-server-group **add in your** “ISE server group name” ASA(config-tunnel-general)# accounting-server-group **add in your** “ISE server group name” ASA(config-tunnel-general)# default-group-policy **add in your** “Group Policy” ASA(config-tunnel-general)#exit
  ASA(config)# tunnel-group “COA” webvpn-attributes
  ASA(config-tunnel-webvpn)# group-alias “COA”
  enabled ASA(config-tunnel-webvpn)# exit
  ASA(config)# exit
  ASA# write
  memory

针对 CoA 配置 ISE

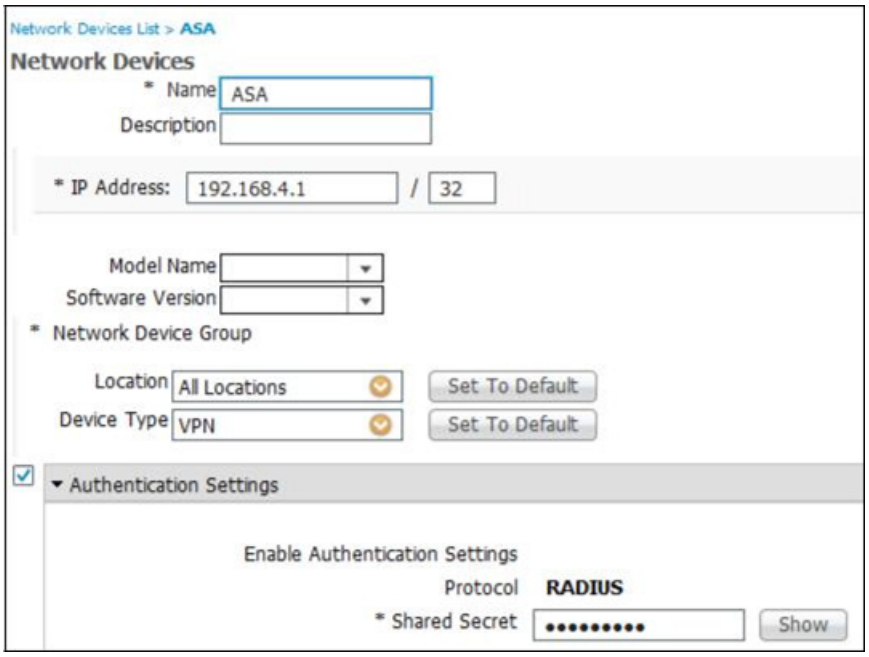
为 ASA 创建网络设备条目

我们需要登录我们的 ISE 控制台，导航至我们的网络设备并添加我们的 ASA。此配置允许 ISE 和 ASA 通过 RADIUS 进行通信。

步骤 1：导航至**管理员 (Administrator)→→网络资源 (Network Resources)→→网络设备 (Network Devices)**，选择**添加 (Add)**。

- **名称 (Name)**：添加 ASA 的名称
- **说明 (Description)**：可选择添加说明
- **IP 地址 (IP Address)**：添加 ASA 的 IP 地址
- 点击**身份验证设置 (Authentication Settings)** 下拉菜单
  - **共享密钥 (Shared Secret)**：输入与为 ASA 创建的相同的共享密钥。

步骤 2：选择**提交 (Submit)**。



为 ISE 安全状态配置策略

考虑到 ISE 已加入 Active Directory 域控制器，本文档将重点介绍要使 ISE 和 ASA 通过 RADIUS 进行通信以进行身份验证，需采取哪些步骤。

对于这一特定使用案例，我们将重点介绍如何创建策略以将 ISE NAC 代理安装在 Windows 7 系统上并为文件执行安全状态策略检查。

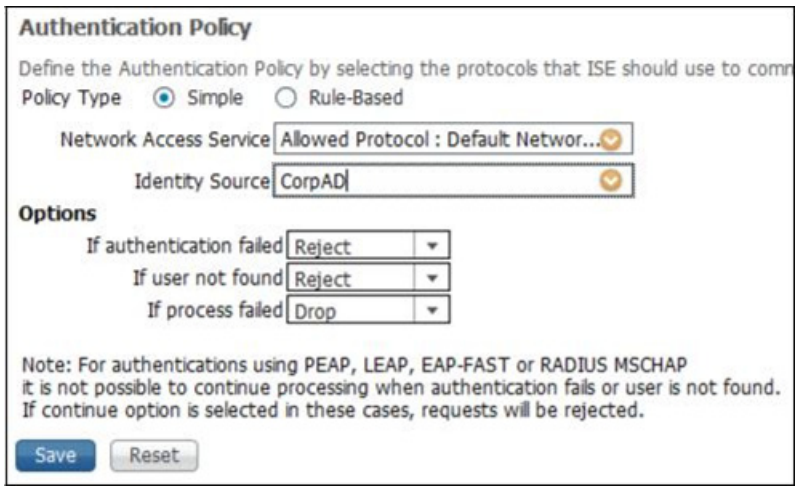
ASA 将把身份验证请求发送到 ISE，并利用此身份验证策略确定对用户进行身份验证应依据的身份源。在本例中，我们选择了 COA 身份源，这是我们的 Active Directory。

本节中，我们需要为不可信和可信设备创建授权条件，然后 ISE 将基于这些结果将策略推送到 ASA。在本使用案例中，如果 ISE 无法确定计算机的合规状态，它将被确定为未知设备，我们将应用一个策略以指示用户下载我们的 ISE NAC 代理。如果用户是合规的，我们将推送完全访问权限的 ISE 策略。

配置身份验证

步骤 1：导航至**策略 (Policy)→→身份验证 (Authentication)**。

- **策略类型 (Policy Type)**：选择“简单”(Simple) **或**“基于规则”(Rule Based)
- **网络访问服务 (Network Access Service)**：选择下拉列表并依次选择**允许的协议 (Allowed Protocols)→→默认网络访问 (Default Network Access)**
- **身份源 (Identity Source)**：选择您的 Active Directory 域（示例：Corp AD）
- 点击**保存 (Save)**



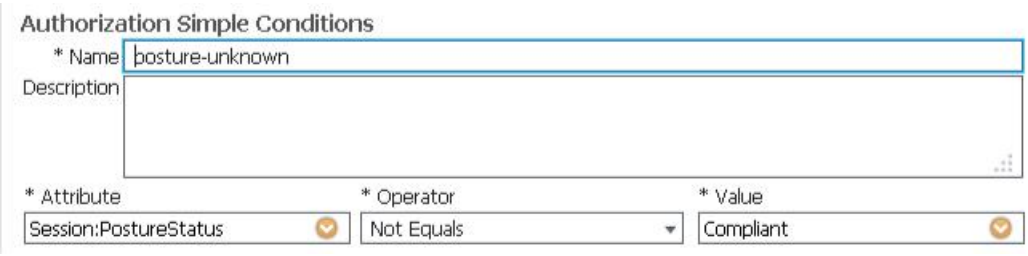
配置授权

创建 Posture-Unknown 条件

步骤 1 导航至**策略 (Policy)→→策略要素 (Policy Elements)→→条件 (Conditions)**。

步骤 2 依次选择**授权 (Authorization)→→简单条件 (Simple Condition)**，然后选择**添加 (Add)**。

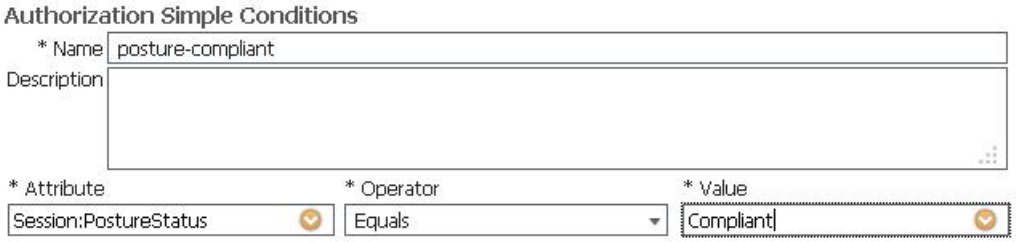
- **名称 (Name)**：提供一个名称（示例：posture-unknown）
- **说明 (Description)**：为策略提供说明
- **属性 (Attribute)：会话 (Session)→→安全状态 (Posture) | 运算符 (Operator)：不等于 (Not Equals) | 值 (Value)：合规 (Compliant)**
- 选择**提交 (Submit)**



创建 Posture-Compliant 条件

步骤 1 导航至**策略 (Policy)→→策略要素 (Policy Elements)→→条件 (Conditions)**。

- 依次选择**授权 (Authorization)→→简单条件 (Simple Condition)**，然后选择**添加 (Add)**。
  - **名称 (Name)**：提供一个名称（示例：posture-compliant）
  - **说明 (Description)**：为策略提供说明
  - **属性 (Attribute)：会话 (Session)→→安全状态 (Posture) | 运算符 (Operator)：等于 (Equal) | 值 (Value)：合规 (Compliant)**
  - 选择**提交 (Submit)**



创建用于 VPN 重定向的授权配置文件

此授权策略将调用我们在 ASA 上创建的 **redirect** ACL，并使用户能够安装 NAC 客户端。**redirect** ACL 可能也已用于提供对 AV 服务器或 WSUS 的有限访问权限。

程序：导航至**策略 (Policy)→→策略要素 (Policy Elements)→→结果 (Results)**

- 从左侧依次选择**授权 (Authorization)→→授权配置文件 (Authorization Profiles)**，然后选择**添加 (Add)**
  - **名称 (Name)**：Posture-Remediation
  - **说明 (Description)**：可选
  - **访问类型 (Access type)**：ACCESS_ACCEPT
  - 在“常见任务”(Common Tasks) 下，选中 **Web 重定向 (Web Redirection)**，然后从下拉列表中选择**客户端调配（安全状态）(Client Provisioning [Posture])**。在 ACL 旁边填写 **redirect**。（**redirect** 是我们在本文档的前一节中在 ASA 上创建的 ACL。ACL 框中的文本区分大小写，必须与 ASA ACL 上创建的内容相匹配）

注意：只有在 ASA 向终端提供的 DNS 无法解析 ISE 主机名的情况下，才需要采取以下步骤。

  - 在“高级属性设置”(Advanced Attributes Settings) 下，依次选择 **Cisco-VPN3000→→CVPN300/ASA/PIX7.x-Primary-DNS**。在值框中，提供能够解析 ISE 主机名的 DNS 服务器的 IP 地址。

使用上述信息（DNS IP 条目除外），应该会显示与下面显示类似的**属性详细信息 (Attributes Detail)**。

为合规用户创建动态访问控制列表 (dACL)

dACL 是一个被授权策略调用的访问控制列表。

程序：导航至**策略 (Policy)→→策略要素 (Policy Elements)→→结果 (Results)**

- 从左侧依次选择**授权 (Authorization)→→可下载 ACL (Downloadable ACLs)**，然后选择**添加 (Add)**
  - 名称 (Name)：输入一个名称（示例：**Posture-Compliant**）
  - 说明 (Description)：**返回的安全状态合规 (Posture status returned compliant)**
  - DACL 内容 (DACL Content)：**permit ip any any**
  - 选择**提交 (Submit)**

为合规用户创建授权策略

dACL 将被推送到已成功通过 ISE NAC 代理安全状态评估的 VPN 用户。

程序：导航至**策略 (Policy)→→策略要素 (Policy Elements)→→结果 (Results)**

- 从左侧依次选择**授权 (Authorization)→→授权配置文件 (Authorization Profiles)**，然后选择**添加 (Add)**
  - 名称 (Name)：**Posture-compliant**
  - 说明 (Description)：**用户合规 (User is compliant)**
  - 访问类型 (Access type)：**ACCESS_ACCEPT**
  - 在“常见任务”(Common Tasks) 下，启用 **DACL 名称 (DACL Name)** 并从下拉列表中选择 **Posture-Compliant**。
  - 选择**提交 (Submit)**

为未知/非合规安全状态创建授权策略

程序：导航至**策略 (Policy)→→授权 (Authorization)**

- 在最顶部规则上的“编辑”(Edit) 按钮的旁边，点击箭头**在上方插入新规则 (Insert New Rule Above)**
- 规则名称 (Rule Name)：**Posture-Remediation**
- Any：**Any**
- 条件 (Condition)：从库中选择现有条件，选择条件名称，然后导航至**简单条件 (Simple Conditions)→→posture-unknown**
- 权限 (Permissions)：**标准 (Standard)→→posture-remediation**
- 点击**完成 (Done)**，然后点击**保存 (Save)**

为合规安全状态创建授权策略

- 在最顶部规则上的“编辑”(Edit) 按钮的旁边，点击箭头**在下方插入新规则 (Insert New Rule Below)**
- 规则名称 (Rule Name)：**Posture-Compliant**
- Any：**Any**
- 条件 (Condition)：从库中选择现有条件，选择条件名称，然后导航至**简单条件 (Simple Conditions)→→ posture-compliant**
- 权限 (Permissions)：**标准 (Standard)→→posture-compliant**
- 点击**完成 (Done)**，然后点击**保存 (Save)**

配置用于部署的安全状态代理

ISE 有 2 种适用于 Windows 的代理，其中一个您可以下载到计算机上，另一个是一次性 Web 代理。ISE 也支持面向 MAC 的 NAC 代理。

本节介绍如何部署 ISE NAC 代理和配置基本的安全状态规则。第一步，您可以选择手动配置或让 ISE 自动下载 ISE NAC 代理和合规模块。合规模块包含最新的供应商更新，应定期添加到您的客户端调配策略中以确保适当的终端评估。

本例选择了“自动下载”(Automatic Download)，这可定期更新带有最新模块的 ISE。在本使用案例中，策略创建于基于最新客户端的 NAC 代理以及适用于 Windows 系统的合规模块（在本文撰写时提供）的基础之上。

配置客户端调配资源

程序：导航至**策略 (Policy)→→结果 (Results)**

- 依次选择**客户端调配 (Client Provisioning)→→资源 (Resources)**，然后选择**添加 (Add)**

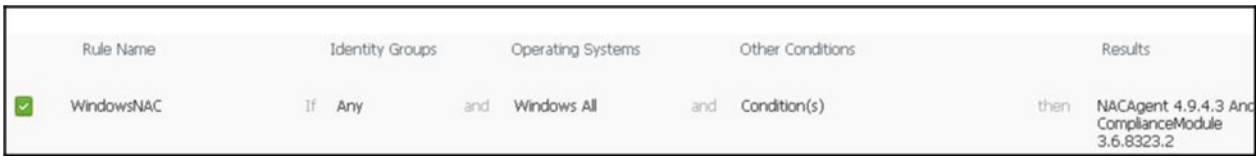
注意：选择**添加 (Add)** 后，系统会为您提供本地磁盘和思科站点这两个选择，请根据您的 ISE 环境模式选择相应的方式。如果您希望 ISE 自动下载，请导航至**管理 (Administration)→→设置 (Settings)→→客户端调配 (Client Provisioning)** 并在下拉列表中选择“启用自动下载”(Enable Automatic Download) 旁边的**启用 (Enable)**。

配置客户端调配策略

程序：导航至**策略 (Policy)→→客户端调配 (Client Provisioning)**

- 规则名称 (Rule Name)：输入一个名称（示例：**Windows-nac-download**）
- 身份组 (Identity Groups)：**Any**
- 操作系统 (Operating System)：选择 Windows 操作系统（本例中选择了 **Windows All**）
- 其他条件 (Other Conditions)：**N/A**
- 结果 (Results)：
  - 代理：**NACAgent 4.x**
  - 配置文件 (Profile)：**N/A**
  - 合规模块 (Compliance Module)：**ComplianceModule 3.x**
  - 所有其他字段均保留默认设置

- **保存 (Save)**

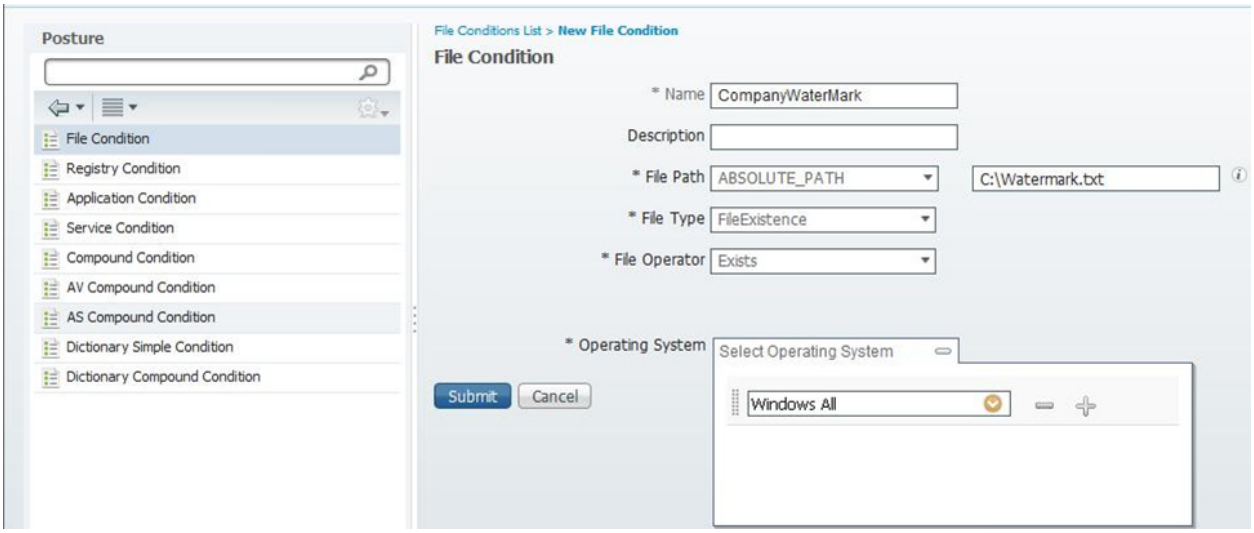


配置安全状态要求

安全状态要求定义为在允许扩展访问之前您要对计算机进行检查的方面。在本使用案例中，我们检查某个公司的水印。您还可以选择检查防病毒终端以及最新的定义是否已应用。

程序：导航至**策略 (Policy)→→策略要素 (Policy Elements)→→条件 (Conditions)**

- 从左侧树结构中依次选择**安全状态 (Posture)→→文件条件 (File Condition)**，然后选择**添加 (Add)**
  - 名称 (Name)：**CompanyWaterMark**
  - 文件路径 (File Path)：Absolute_Path，C:\Watermark.txt
  - 文件类型 (File Type)：FileExistence
  - 文件运算符 (File Operator)：存在 (Exists)
  - 操作系统 (Operating System)：Windows All



创建安全状态要求

现在安全状态条件已配置完毕，我们需要将其指定为尝试获取公司网络访问权限的终端需要进行的安全状态检查。在本使用案例中，我们将通知用户其计算机不合规，方法是通过 NAC 代理发送一条信息称缺失文件要求检查已开始，然后将文件 Watermark.txt 重新添加到相应的目录。

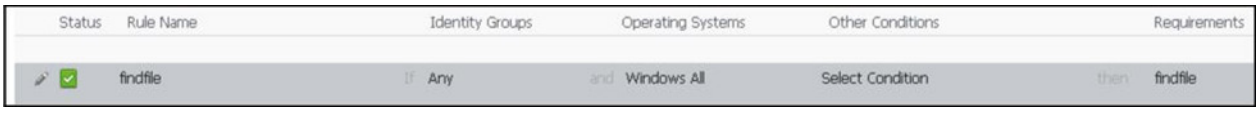
- **程序**：导航至**策略 (Policy)→→策略要素 (Policy Elements)→→结果 (Results)**
- 从左侧树结构中依次选择**安全状态 (Posture)→→要求 (Requirements)**，然后选择“编辑”(Edit) 旁边的下拉列表并选择**插入新要求 (Insert new Requirement)**
  - 名称 (Name)：**Findfile**
  - 操作系统 (Operating System)：**Windows All**
  - 条件 (Condition)：**用户定义 (User Defined) 文件条件 (File Condition) CompanyWaterMark**
  - 修复操作 (Remediation Actions)：**仅信息文本 (Message Text Only)**
    - 通知用户的信息 (Message informing the User)：您缺失 **C:\Watermark.txt** 文件，请重新添加该文件 (You’re missing **C:\Watermark.txt** please add back the file)
- 点击**完成 (Done)**，然后点击**保存 (Save)**

创建要应用于所有 Windows 终端的安全状态策略

本节我们将利用条件和要求构建一个安全状态策略，ISE NAC 代理将使用该策略在网络连接期间进行评估。

程序：导航至**策略 (Policy)→→安全状态 (Posture)**

- 名称 (Name)：**Findfile**
- 身份组 (Identity Groups)：**Any**
- 操作系统 (Operating System)：**Windows All**
- 其他条件 (Other Condition)：<留空>
- 要求 (Requirements)：**findfile**
- 点击**完成 (Done)**，然后点击**保存 (Save)**



连接 VPN 客户端并监控 ASA 和 ISE 日志

针对 CoA 配置好 ISE 和 ASA 并且配置好安全状态策略以检查 c:\ 目录中的 Watermark.txt 后，现在是时候通过 VPN 连接远程终端了。在本示例中，终端是一台未将 Watermark.txt 添加到 c:\ 目录的 Windows 7 计算机。NAC 将向 ISE 报告终端的状态，ISE 将限制访问权限，并告知用户终端不合规。用户将需要将 Watermark.txt 添加到 c:\ 目录才会变为合规。

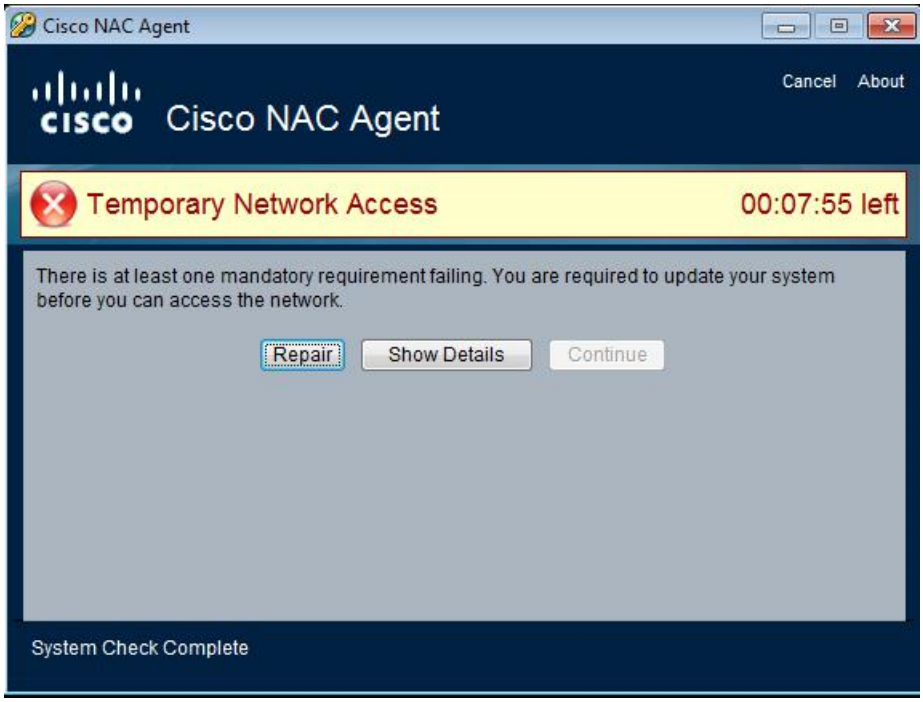
我们将在 ASA CLI 和 ISE 授权变更 (CoA) 前后监控终端的状态。

将非合规终端连接到 ASA 头端

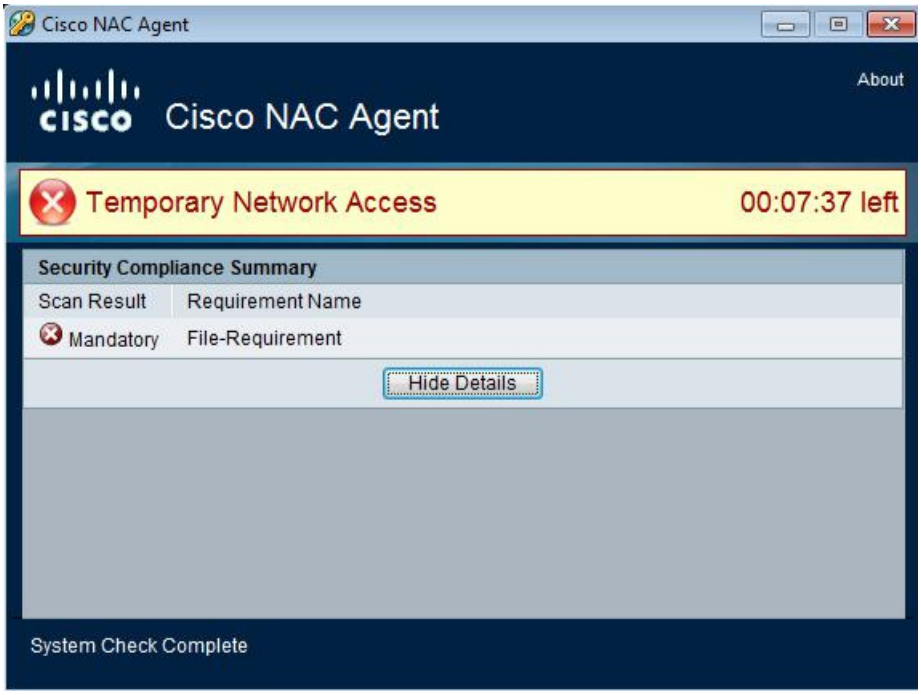
步骤 1　连接到 ASA 头端。

在您的客户端 PC 上启动 AnyConnect VPN 代理并连接到已针对 CoA 配置好的 ASA。

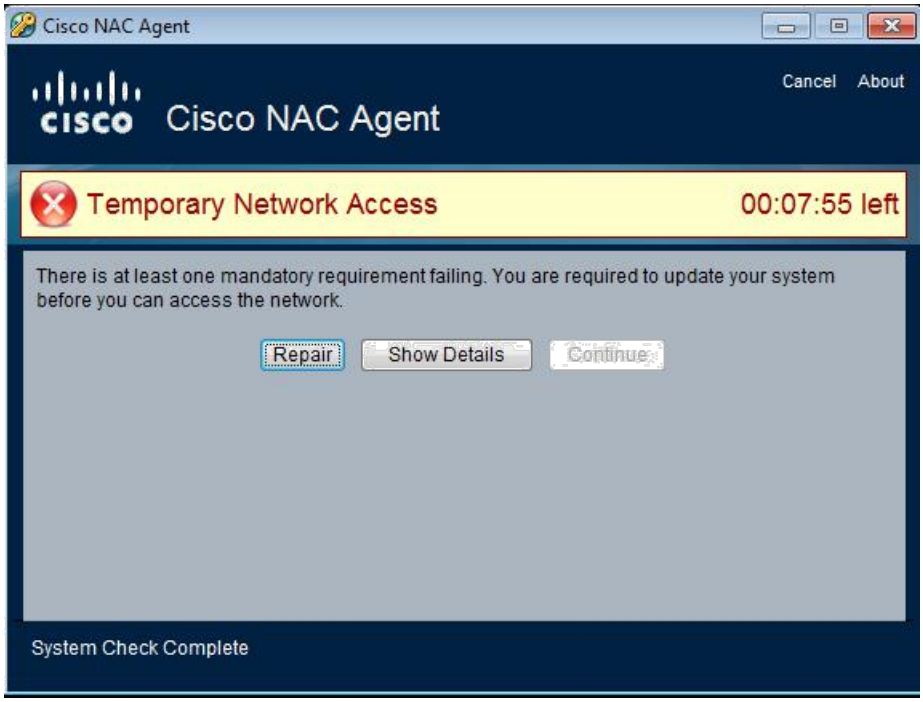
NAC 代理会弹出一则通知，显示设备不合规。



步骤 2　　点击详细信息会通知用户不合规的原因。在本例中，我们在 c:\ 目录中缺少 Watermark.txt（文件要求）。



步骤 3　点击“隐藏详细信息”(Hide Details)，然后点击“修复”(Repair) 按钮。安全状态策略创建后，系统会在策略中定义一条信息以通知用户将 Watermark.txt 添加到 c:\ 目录。



查看 ASA CLI

终端处于非合规状态时，ISE 将调用 ASA 上的 redirect ACL。在 ASA 中启用 CLI 提示，运行 **sh vpn-sessiondb detail anyconnect**。您会发现 ISE 已向下方所示的终端分配一个会话 ID。

```
COA# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : paul                   Index        : 12
Assigned IP  : 192.168.5.100          Public IP    :         .177
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
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     : 1065060                Bytes Rx     : 347025
Pkts Tx      : 2297                   Pkts Rx      : 2277
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : COA_GroupPol           Tunnel Group : COA
Login Time   : 10:37:40 EDT Thu Jun 12 2014
Duration     : 0h:01m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a804010000c0005399bb34
Security Grp : none

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

ISE 为该终端分配了配置的 redirect ACL（本指南在前面已介绍过如何配置）。如果 NAC 代理修复计时器到期，则该终端只有在将 Watermark.txt 添加到 c:\ 目录或隔离后才会收到一个新的 dACL。

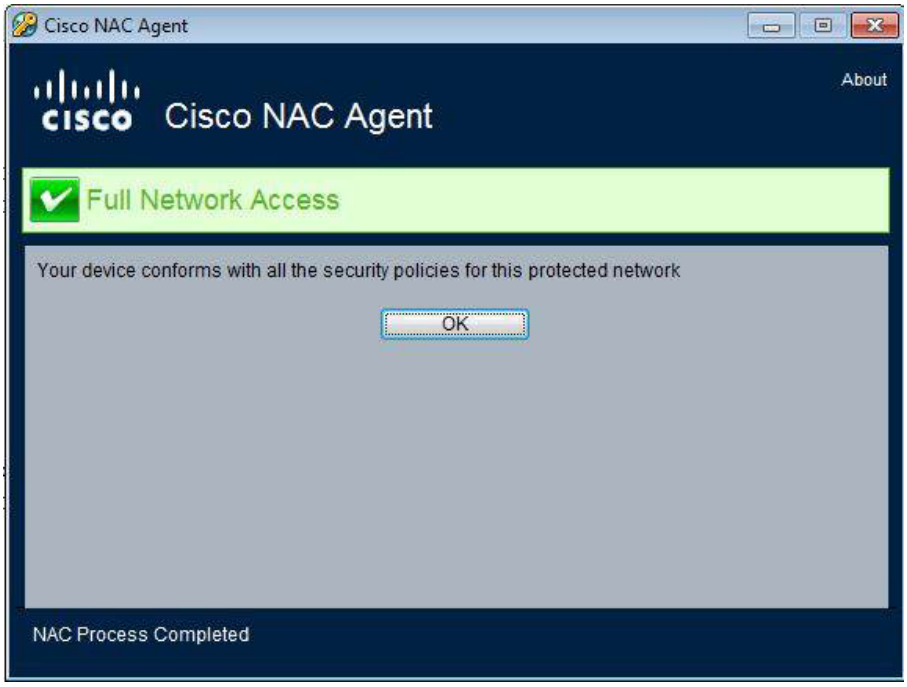
```
ISE Posture:
  Redirect URL : https://FCS-ISE.cert.loco:8443/guestportal/gateway?sessionId=c0a804010000c
0005399bf7a&action=cpp
  Redirect ACL : redirect
```

将 Watermark.txt 添加到终端并重新扫描

步骤 1. 创建一个名为 Watermark.txt 的文件，将其保存在您的 c:\ 目录。

步骤 2. 将 watermark.txt 添加到 c:\ 目录后，从 NAC 代理中选择“重新扫描”(Re-Scan)。

NAC 将扫描 watermark.txt 文件，并向用户提供完全网络访问权限。



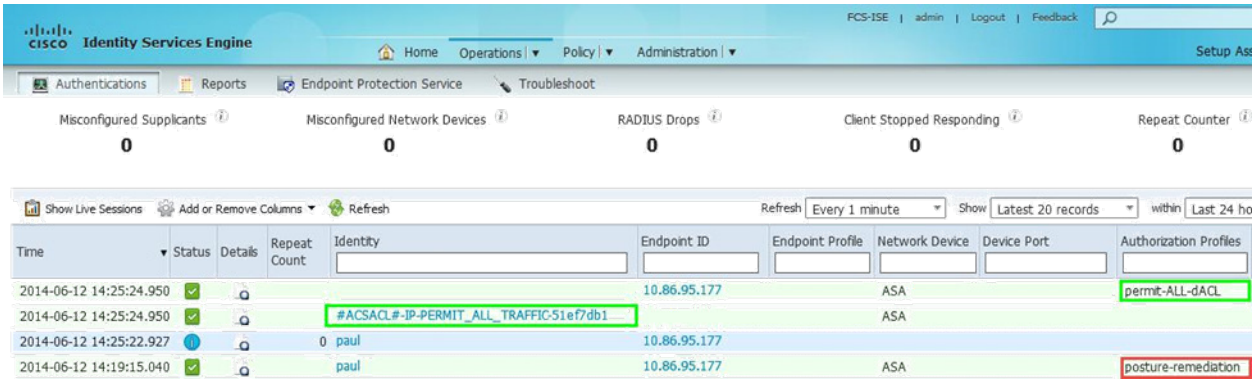
查看 ASA CLI 和 ISE 日志

现在终端合规后，ISE 会将 permit ip 为 any any 的 dACL 推送到 ASA 上。在 ASA 中启用 CLI 提示，运行 **sh vpn-sessiondb detail anyconnect**。您会发现 ISE 已向下方所示的终端分配新的 dACL。

```
DTLS-Tunnel:
  Tunnel ID    : 16.3
  Assigned IP  : 192.168.5.100          Public IP    :          .177
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: DTLSv1.0               UDP Src Port : 64243
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.05152
  Bytes Tx     : 89887                  Bytes Rx     : 64615
  Pkts Tx      : 318                    Pkts Rx      : 473
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

查看 ISE 操作日志

程序：导航至**操作 (Operations)→→身份验证 (Authentications)**，您应能看到终端从非合规状态 (posture-remediation) 变成安全状态合规状态 (permit-ALL-dACL)



参考资料

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#pgfId-42231

http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/release/notes/asarn92.html