与ISE版本1.3配置示例的AnyConnect 4.0集成

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[拓扑和流](#)
[Configure](#)
[WLC](#)
[ISE](#)
[步骤1.添加WLC](#)
[步骤2.配置VPN配置文件](#)
[步骤3.配置NAM配置文件](#)
[步骤4.安装应用程序](#)
[步骤5.安装VPN/NAM配置文件](#)
[步骤6.配置状态](#)
[步骤7.配置AnyConnect](#)
[步骤8.客户端设置规则](#)
[步骤9.授权配置文件](#)
[步骤10.授权规则](#)
[Verify](#)
[Troubleshoot](#)
[Related Information](#)

Introduction

本文在允许您配置几个AnyConnect安全移动性客户端模块和自动地设置他们到终端的思科身份服务引擎(ISE)版本1.3描述新的功能。本文提交如何配置在ISE的VPN、网络接入管理器(NAM)和状态模块和推进他们对集群用户。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- ISE配置、认证和授权
- 无线局域网控制器(WLCs)的配置
- 基本的VPN和802.1x知识
- VPN和NAM配置文件的配置用AnyConnect配置文件编辑器

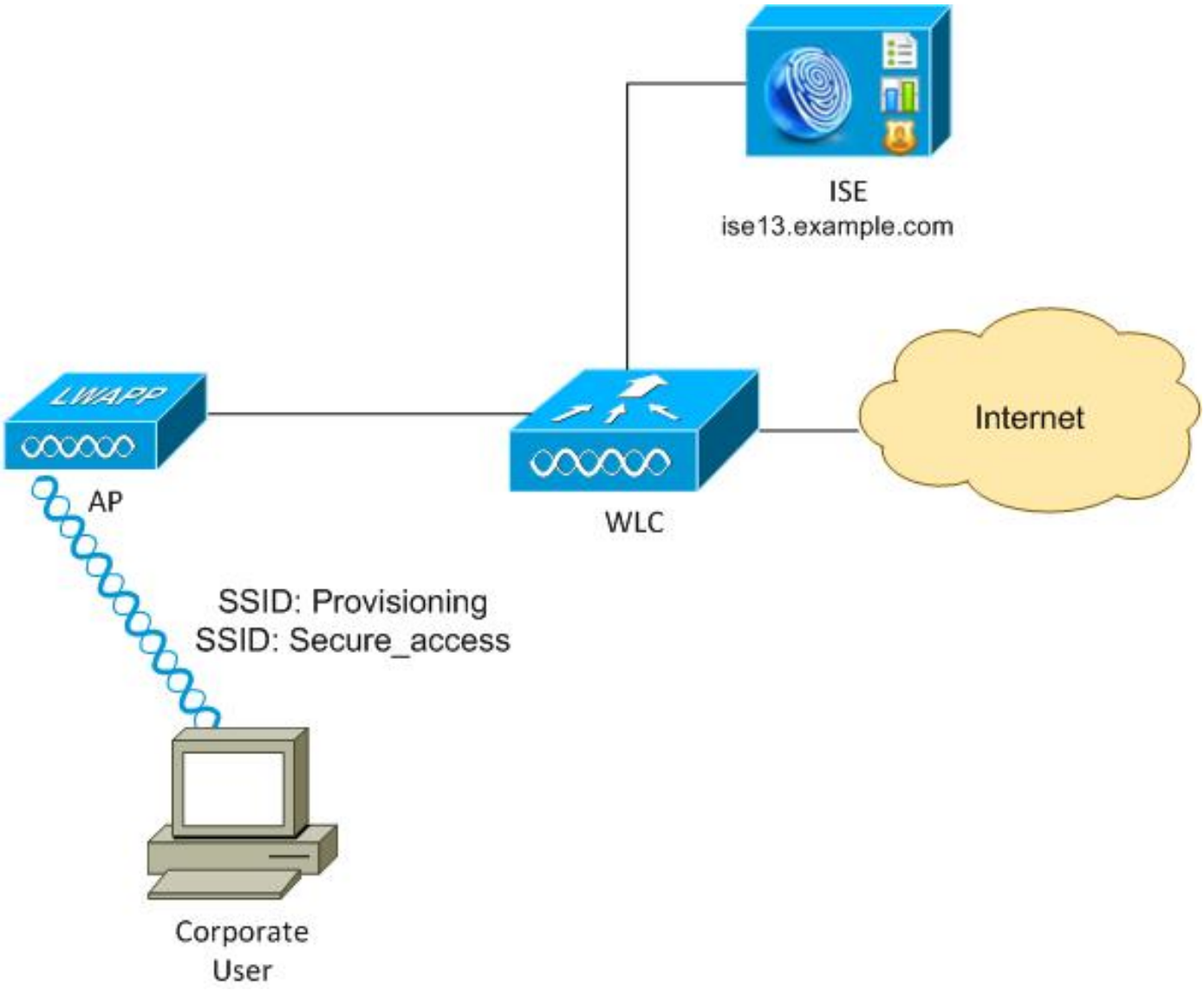
Components Used

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco WLC版本7.6和以上
- Cisco ISE软件，版本1.3和以上

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

拓扑和流



这是流：

步骤1.集群用户acceses服务集标识(SSID) ：设置。进行802.1x认证与可扩充验证协议保护的EAP (EAP-PEAP)。**设置**授权规则在ISE遇到，并且用户为AnyConnect设置重定向(通过客户端设置Protal)。如果AnyConnect在机器没有被发现，安装所有被配置的模块(VPN， NAM，状态)。与该配置文件一起，每个模块的配置被推进。

Step 2.一旦安装AnyConnect，用户必须重新启动PC。在重新启动， AnyConnect运行，并且后正确的SSID根据被配置的NAM配置文件(Secure_access)自动地使用。使用EAP-PEAP (为例，可扩充验证可能也使用传输层安全(EAP-TLS))。同时，状态模块检查位置是否是兼容的(检查**c:\test.txt文**

件的存在)。

第 3 步：如果位置状态状态未知(从状态模块的没有报告)，为设置仍然重定向，因为**未知**Authz规则在ISE遇到。一旦位置是兼容的， ISE发送授权(CoA)的更改到无线局域网控制器，触发再验证。第二个认证出现，并且**兼容**规则在ISE被击中，将提供用户全部存取给网络。

结果，用户配置有AnyConnect VPN、NAM和允许对网络的统一的访问的状态模块。 相似的功能在可适应的安全工具(ASA)上可以使用VPN访问。目前， ISE能为与一非常粒状方法的任一种访问执行同样。

此功能对集群用户没有被限制，但是可能是最普通为该组用户配置它。

Configure

WLC

WLC配置有两Ssid ：

- 设置- [WPA + WPA2][Auth(802.1X)]。此SSID使用AnyConnect设置。
- Secure_access - [WPA + WPA2][Auth(802.1X)]。此SSID使用安全访问，在终端配置有为该SSID被配置的NAM模块后。

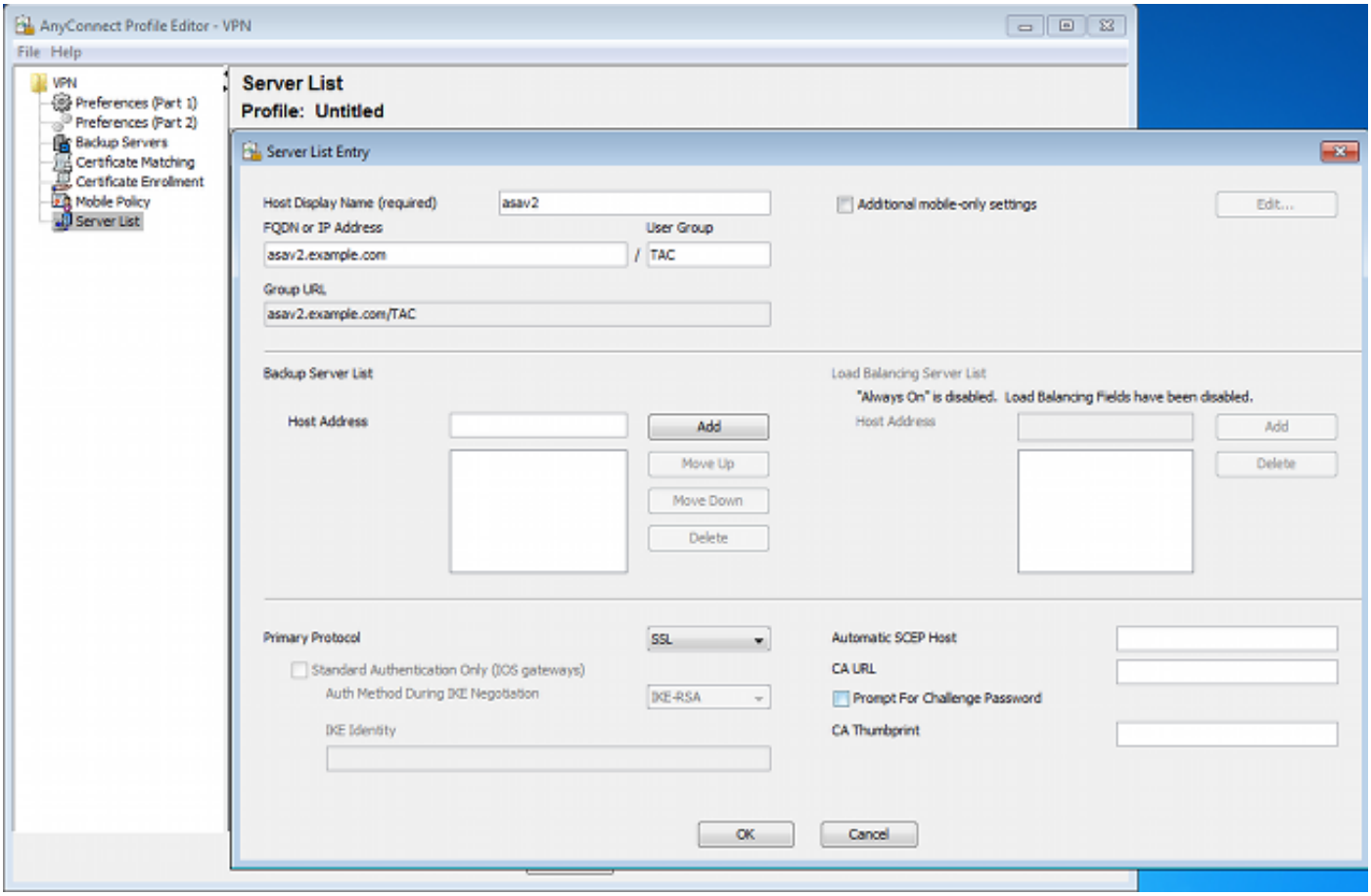
ISE

步骤1.添加WLC

添加WLC到在ISE的网络设备。

步骤2.配置VPN配置文件

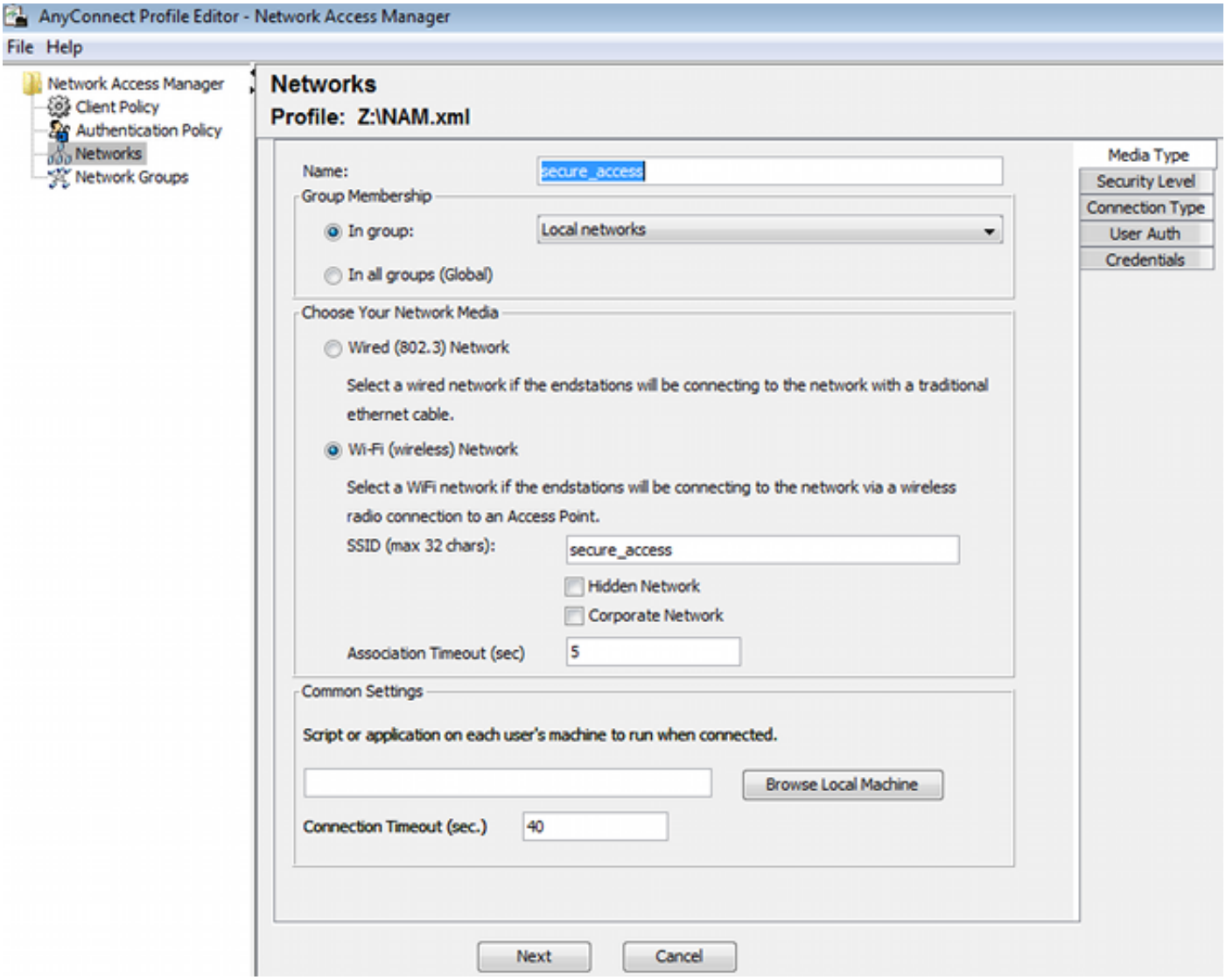
用VPN的AnyConnect配置文件编辑器配置VPN配置文件。



仅一个条目为VPN访问被添加了。只是对**VPN.xml的**XML文件**。**

步骤3.配置NAM配置文件

用NAM的AnyConnect配置文件编辑器配置NAM配置文件。



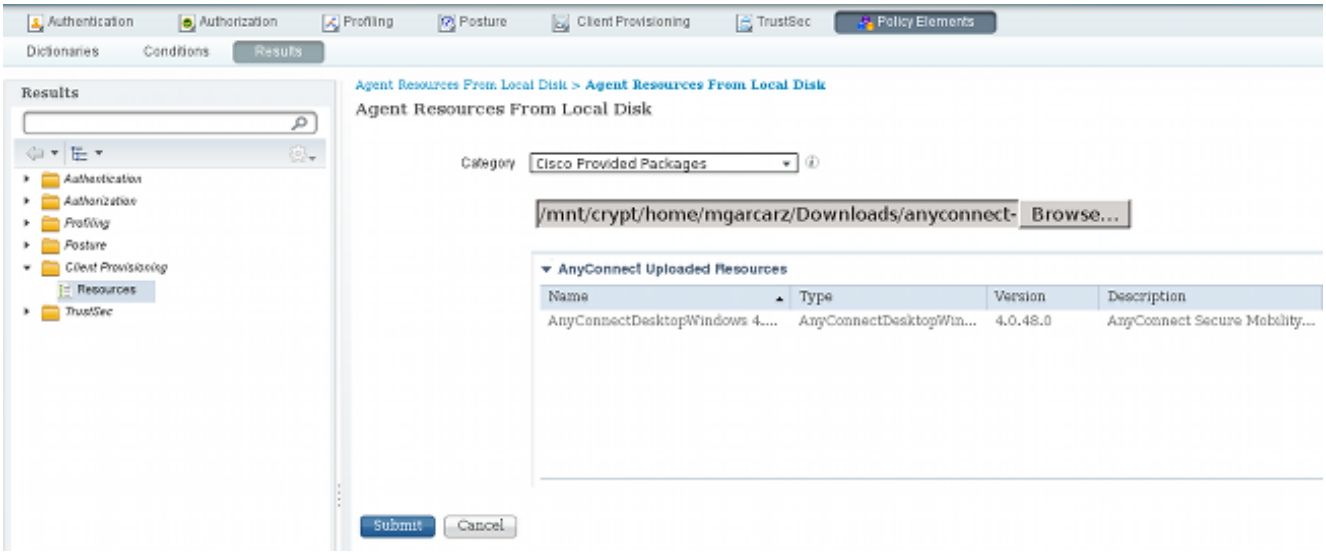
仅配置了一SSID ：**secure_access**。只是对**NAM.xml的**XML文件**。**

步骤4.安装应用程序

1. 从Cisco.com手工下载应用程序。

   anyconnect-win-4.0.00048-k9.pkganyconnect-win-compliance-3.6.9492.2.pkg

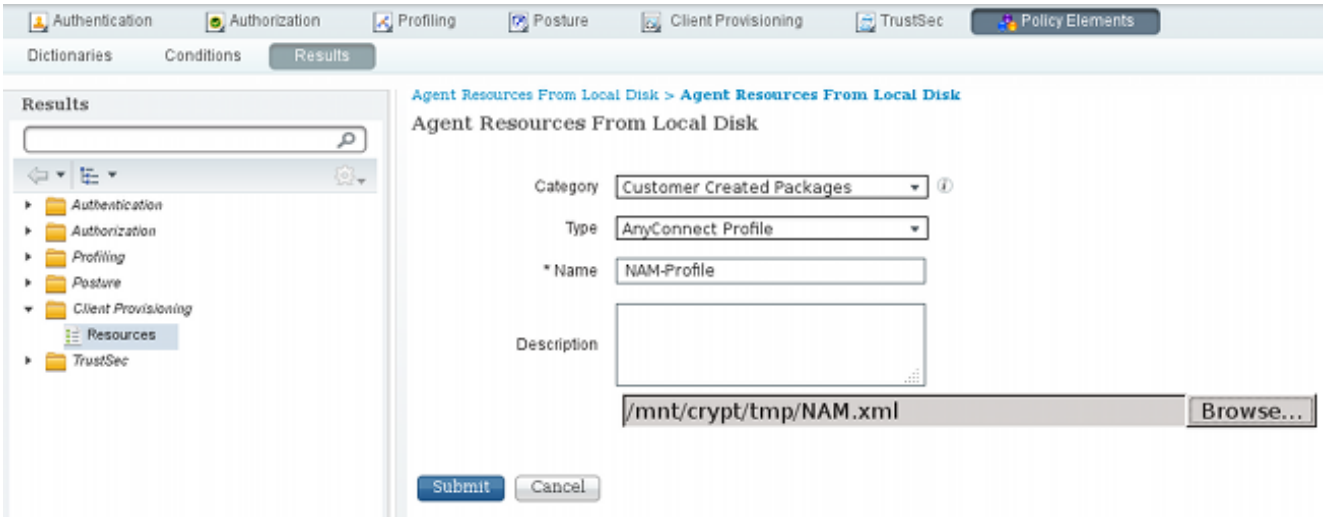
2. 在ISE，请连接对**策略>结果>客户端设置>资源**，并且从本地磁盘添加代理程序资源。
3. 选择Cisco提供了程序包并且选择**anyconnect-win-4.0.00048-k9.pkg** ：



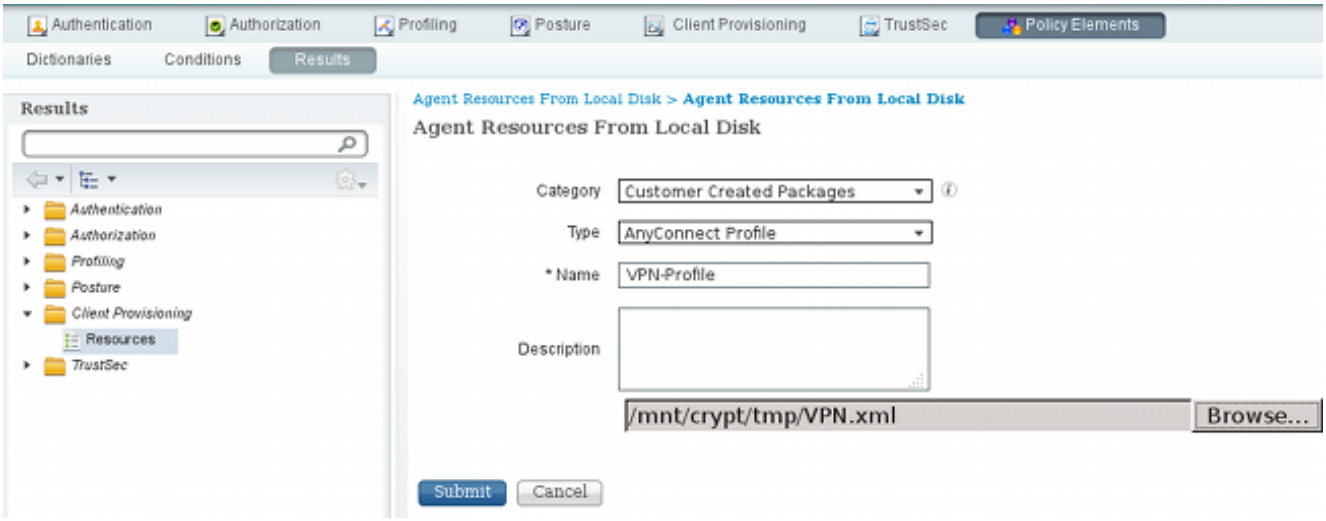
4. 重复标准模块的第4步。

步骤5.安装VPN/NAM配置文件

1. 连接对**策略>结果>客户端设置>资源**，并且从本地磁盘添加代理程序资源。
2. 选择用户被创建的程序包和类型**AnyConnect配置文件**。选择以前被创建的NAM配置文件(XML文件)：



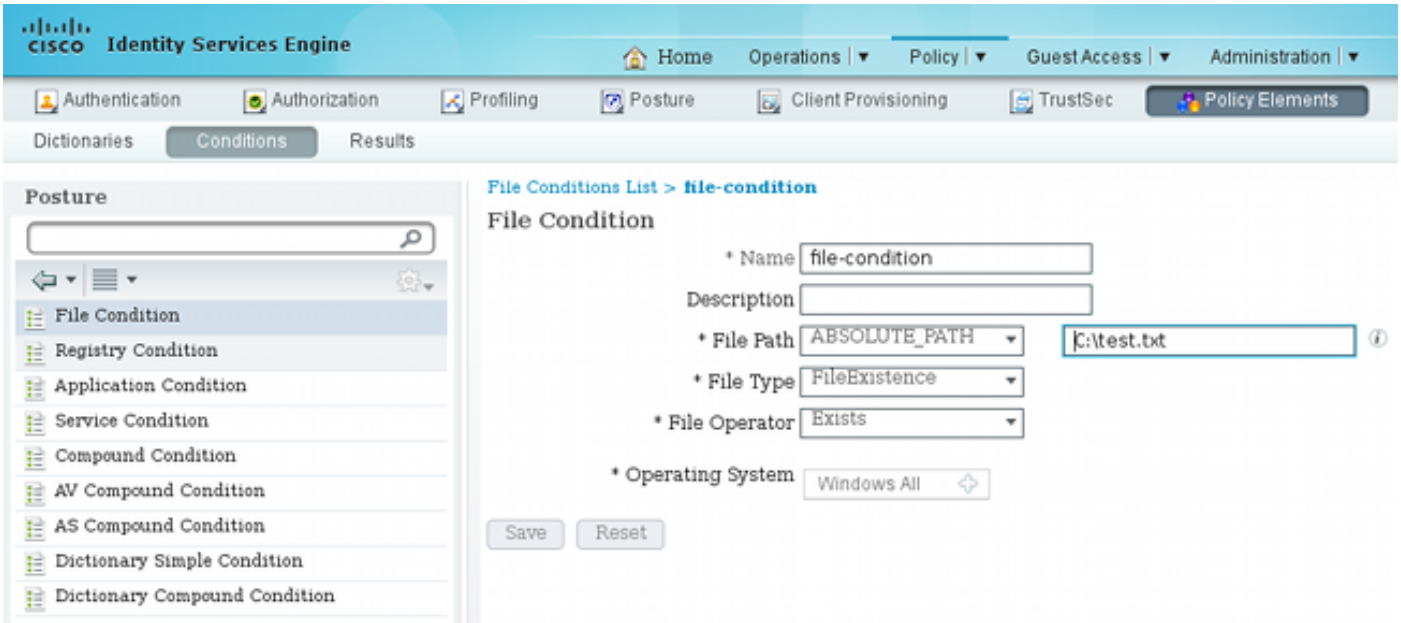
3. 重复VPN配置文件的相似的步骤：



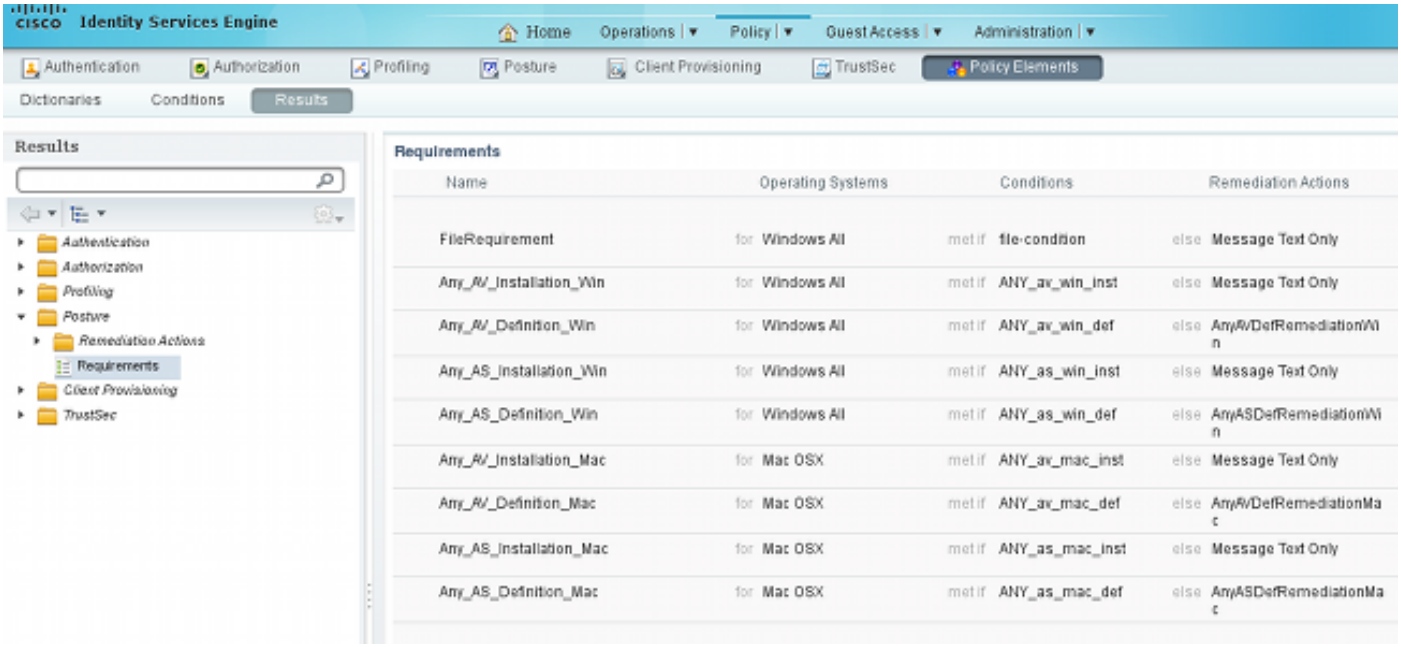
步骤6.配置状态

NAM和VPN配置文件必须配置有外部AnyConnect配置文件编辑器和被导入到ISE。但是状态在ISE充分配置。

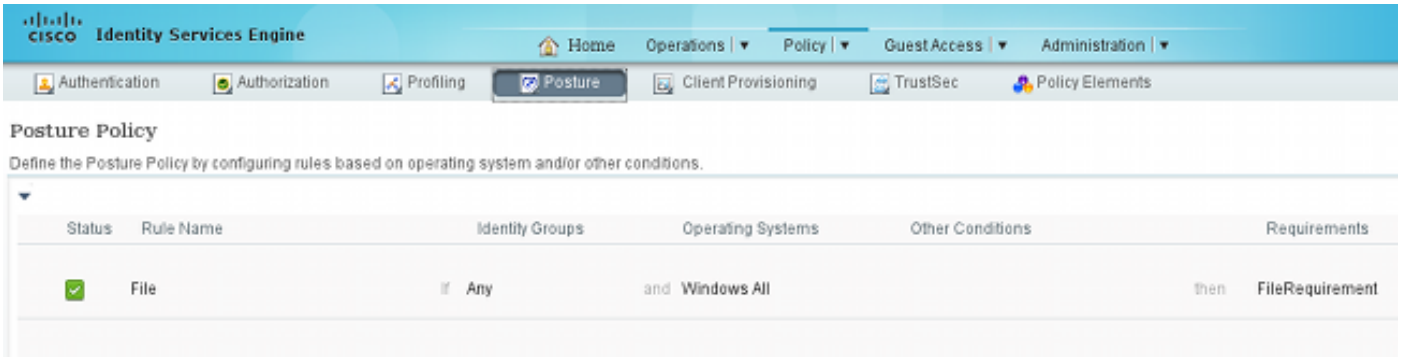
连接对**策略>情况>状态>文件Condition.You**能看到文件存在的一个单纯条件被创建了。您必须有文件为了是兼容的与状态模块验证的策略：



此情况使用需求：



并且需求用于状态策略微软视窗系统：

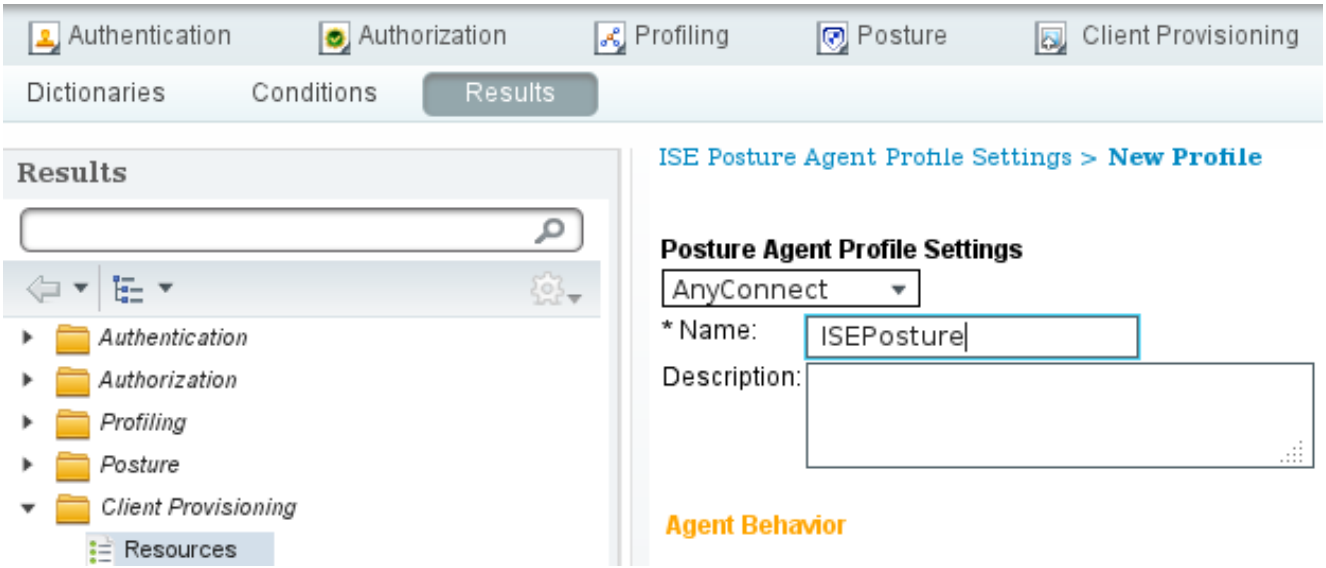


关于状态配置的更多信息，请参见[在Cisco ISE配置指南的状态服务]。

一旦状态策略准备好，是时间添加状态代理配置。

1. 连接对**策略>结果>客户端设置>资源**并且添加网络准入控制(NAC)代理程序或AnyConnect代理程序状态配置文件。

2. 选择AnyConnect (从ISE版本1.3的一个新的状态模块使用了而不是老NAC代理程序) ：



3. 从状态协议部分，请勿忘记添加*为了允许代理程序连接到所有服务器。

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

4. 如果服务器名规则字段空出， ISE不保存设置并且报告此错误：

```
Server name rules: valid value is required
```

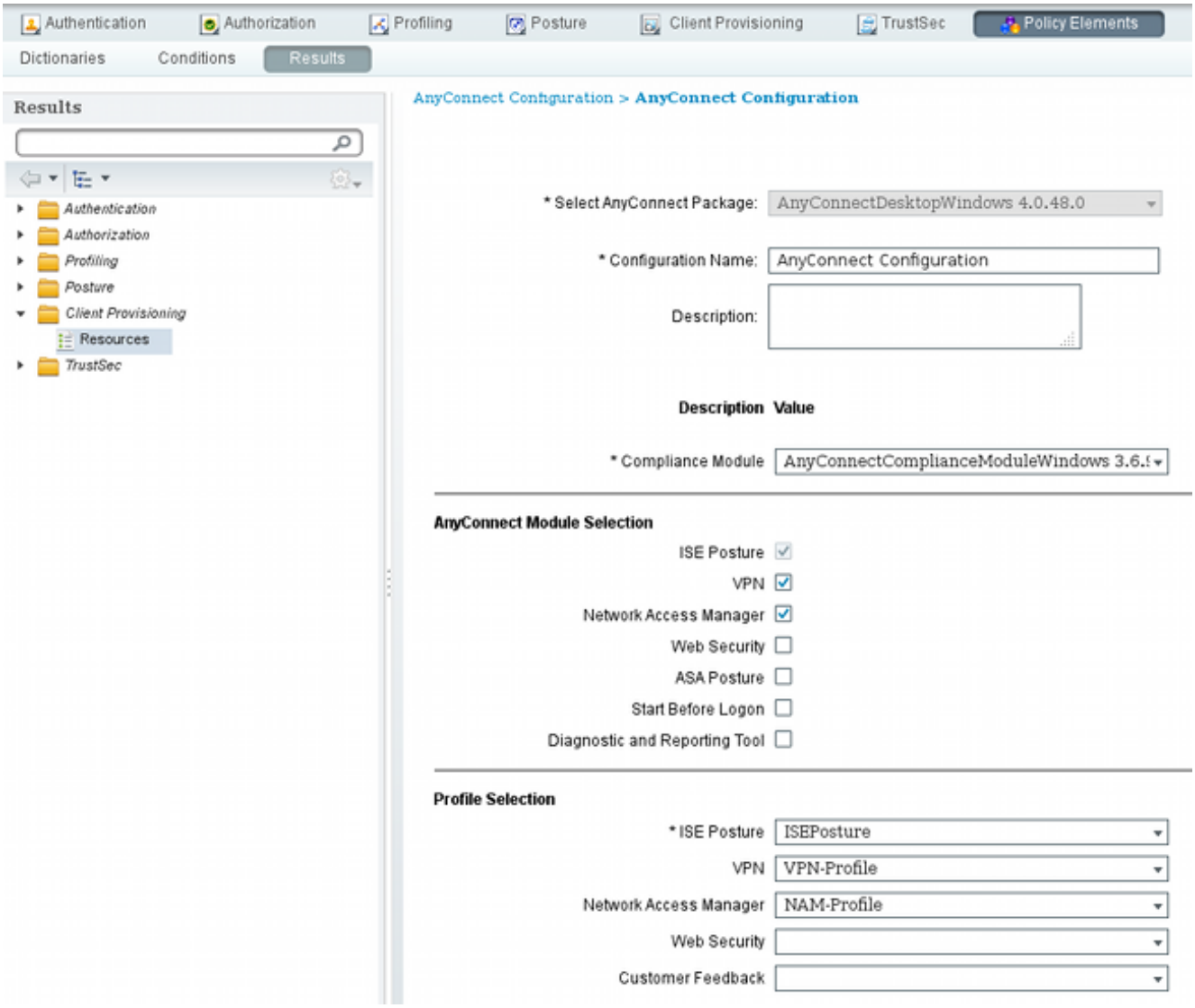
步骤7.配置AnyConnect

在此阶段，和所有模块(VPN、NAM和状态)的配置文件配置配置了所有应用程序(AnyConnect)。是时间在一起地粘合它。

1. 连接对**策略>结果>客户端设置>资源**，并且添加AnyConnect配置。

2. 配置名字并且选择标准模块和全部必需AnyConnect模块(VPN、NAM和状态)。

3. 在配置文件选择，请选择为每个模块配置的前配置文件。



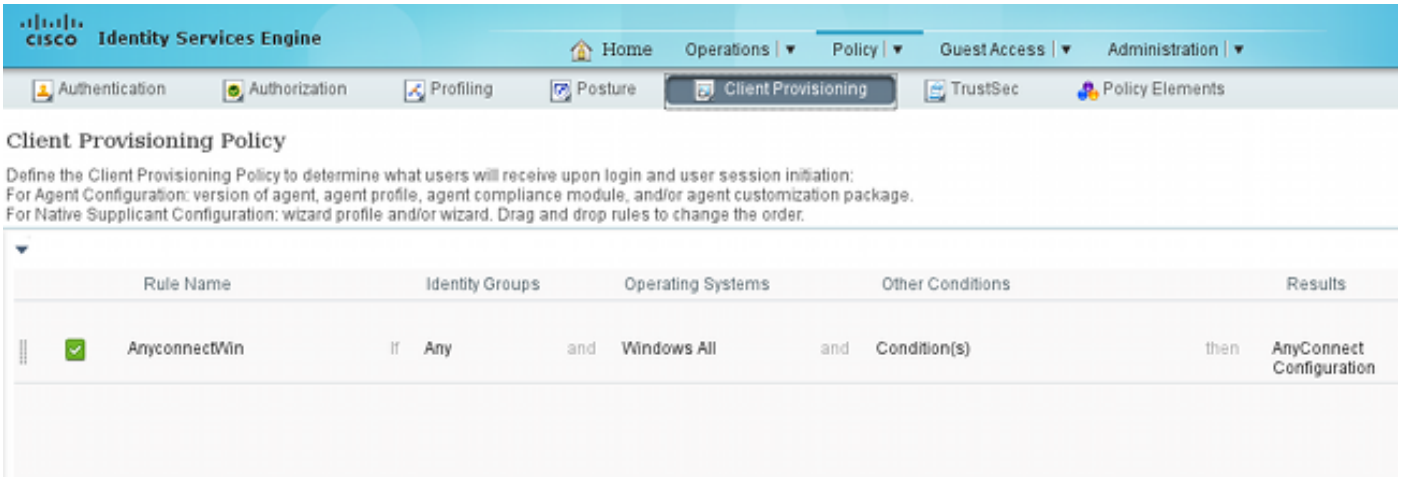
4. VPN模块对于其他模块是必需作用corrrectly。即使VPN模块没有为安装选择，在客户端上将被推进并且安装。如果不要使用VPN，有配置隐藏VPN模块的用户界面VPN的一个特殊配置文件的可能性。应该添加这些线路到**VPN.xml文件：**

```
 <ClientInitialization>
<ServiceDisable>true</ServiceDisable>
</ClientInitialization>
```

5. 也安装这种配置文件，当您使用**从**iso程序包时(anyconnect-win-3.1.06073-pre-deploy-k9.iso)**的Setup.exe。**然后， VPN的VPNDisable_ServiceProfile.xml**配置文件**与配置一起安装，禁用VPN模块的用户界面。

步骤8.客户端设置规则

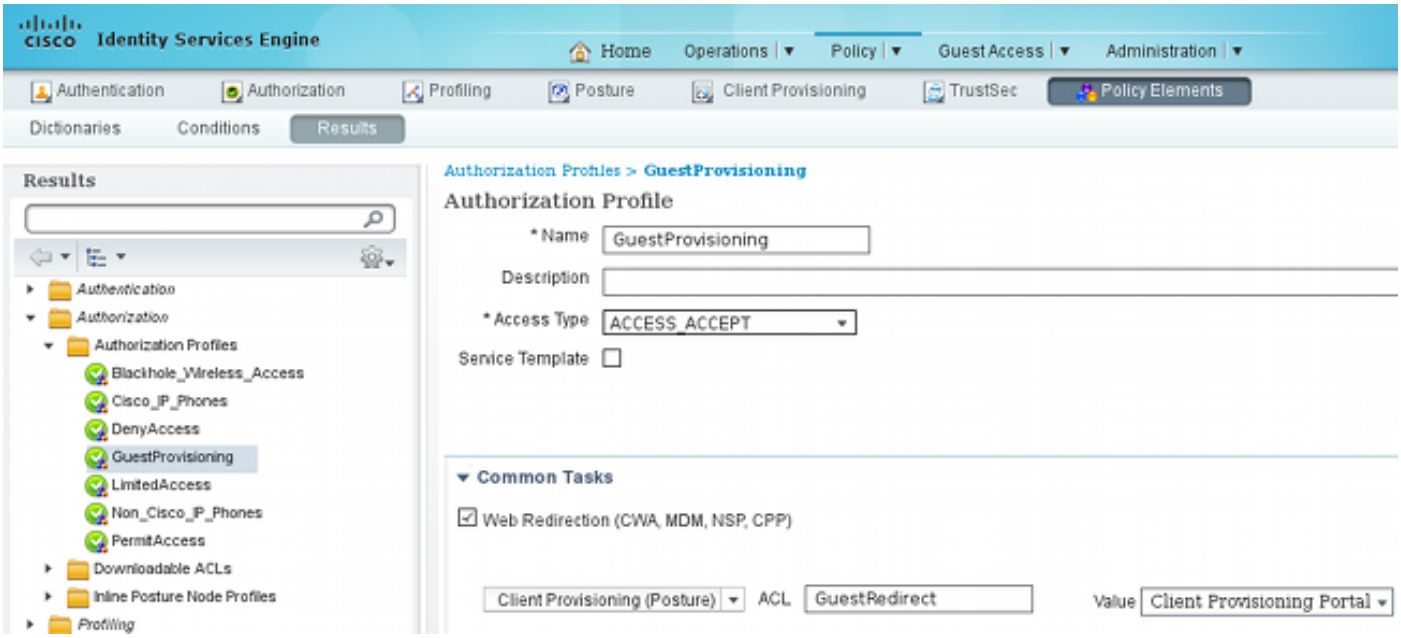
客户端设置规则应该参考在创建的AnyConnect配置第7步：



客户端设置规则决定哪个应用程序将被推进给客户端。仅一个规则必要这里与指向在创建的配置第7.步的结果。这样，为客户端设置重定向的所有微软视窗终端以所有模块和配置文件将使用AnyConnect配置。

步骤9.授权配置文件

客户端的授权配置文件供应需要被创建。使用默认客户端设置的门户：



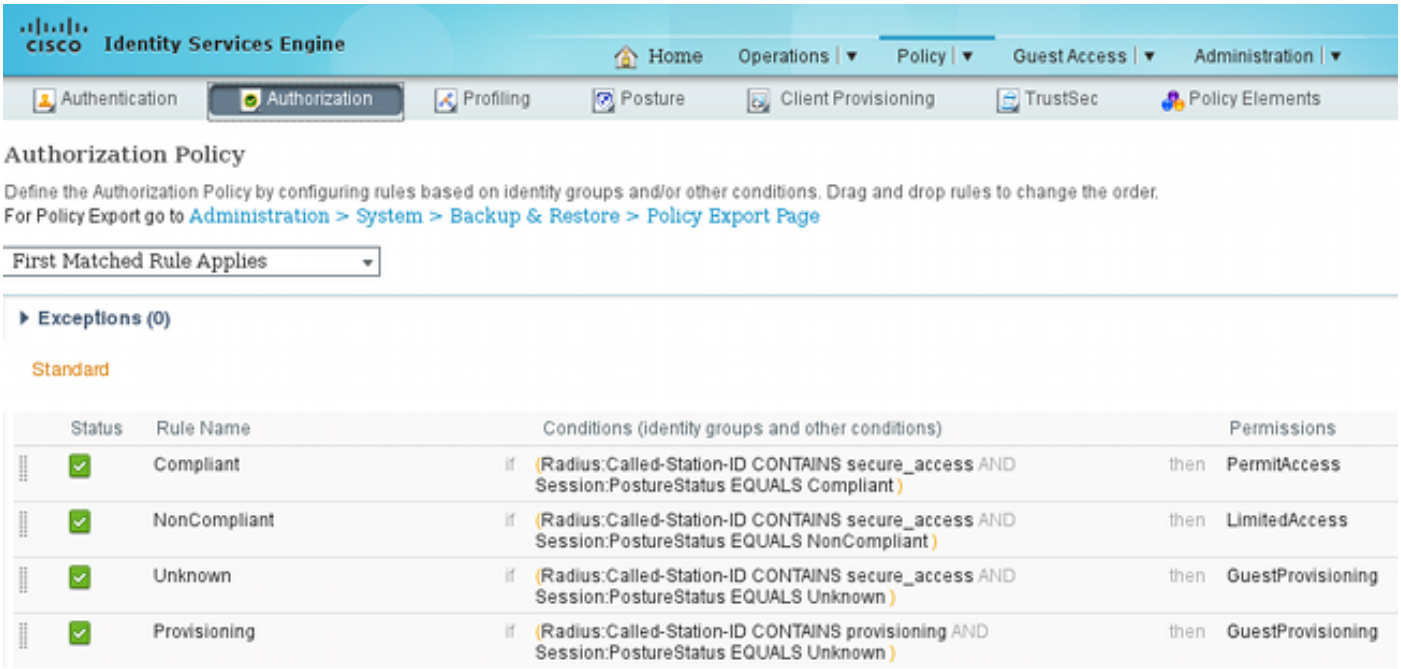
此配置文件迫使用户为设置重定向到默认客户端设置的门户。此门户评估客户端Provisiong策略(在创建的规则第8)步。授权配置文件是授权规则的结果在配置的第10.步。

GuestRedirect访问控制表(ACL)是在WLC定义的ACL的名字。此ACL决定应该重定向哪数据流到ISE。欲知更多信息，请参见与交换机和身份服务引擎配置示例的中央Web认证。

也有提供有限的网络访问的另一个授权配置文件(DACL)为固执的用户(告诉LimitedAccess)。

步骤10.授权规则

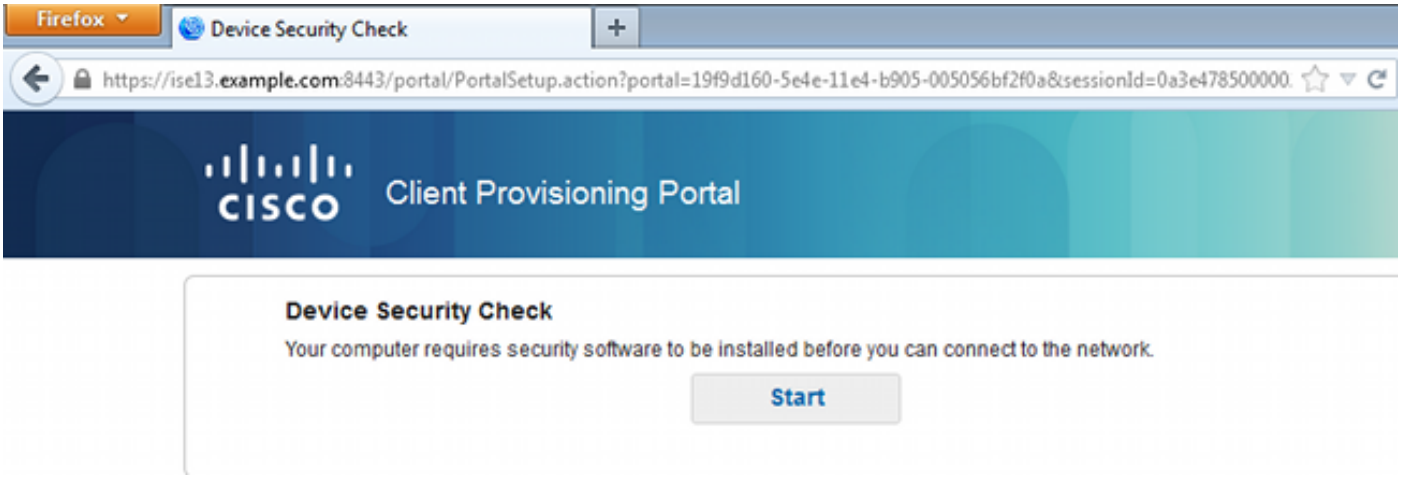
所有那些被结合到四个授权规则：



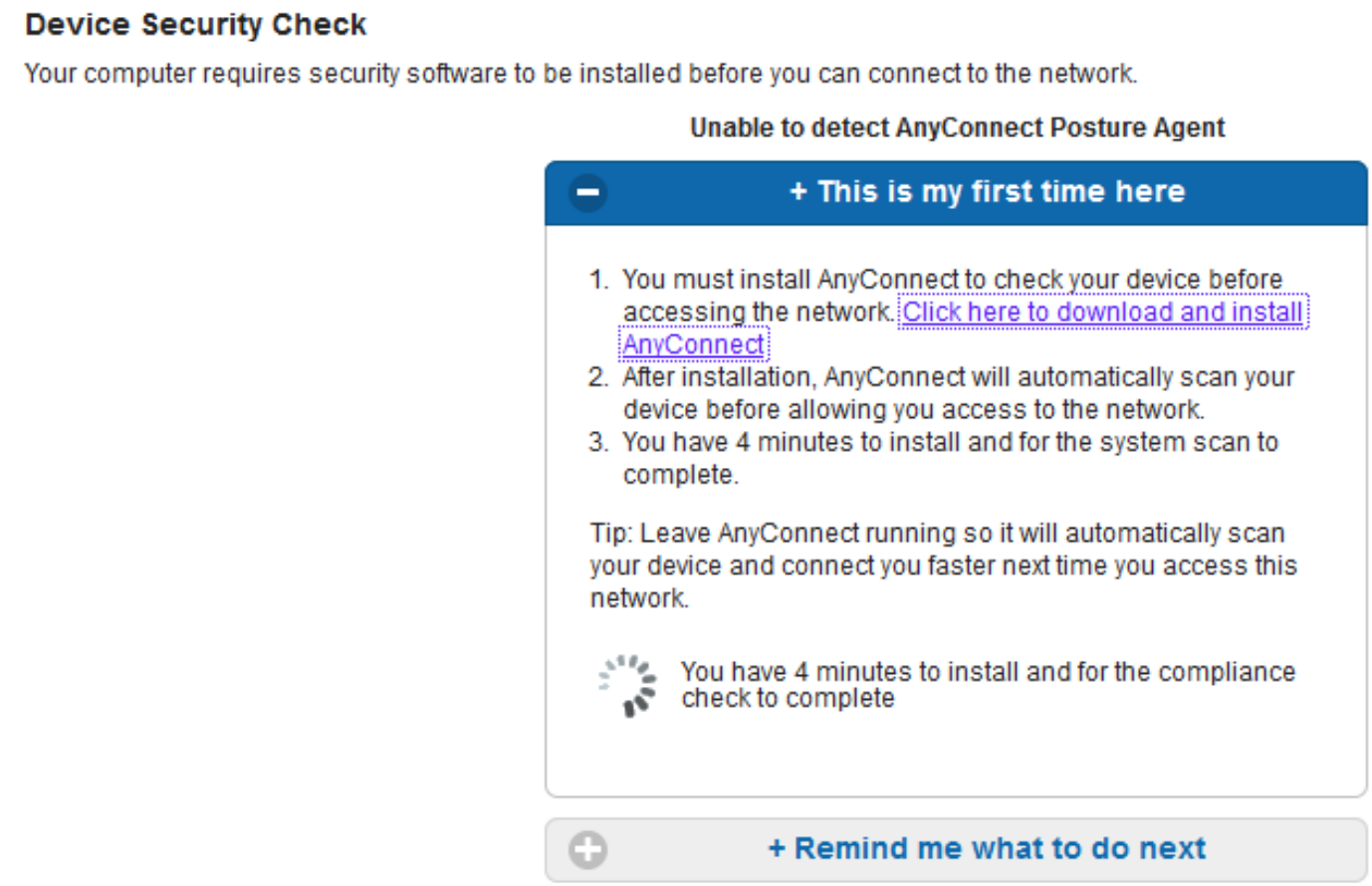
首先您连接到设置SSID和为设置重定向对默认客户端设置的门户(规则已命名Provisioning)。一旦连接到**Secure_access** SSID，为设置仍然重定向，如果从状态模块的报告没有由ISE (规则已命名Unknown)收到。一旦终端是完全适应的，授予全部存取(兼容的规则名称)。如果终端报告如固执，限制了网络访问(规则已命名NonCompliant)。

Verify

您与设置SSID产生关联，设法访问所有网页和重定向到客户端设置的门户：

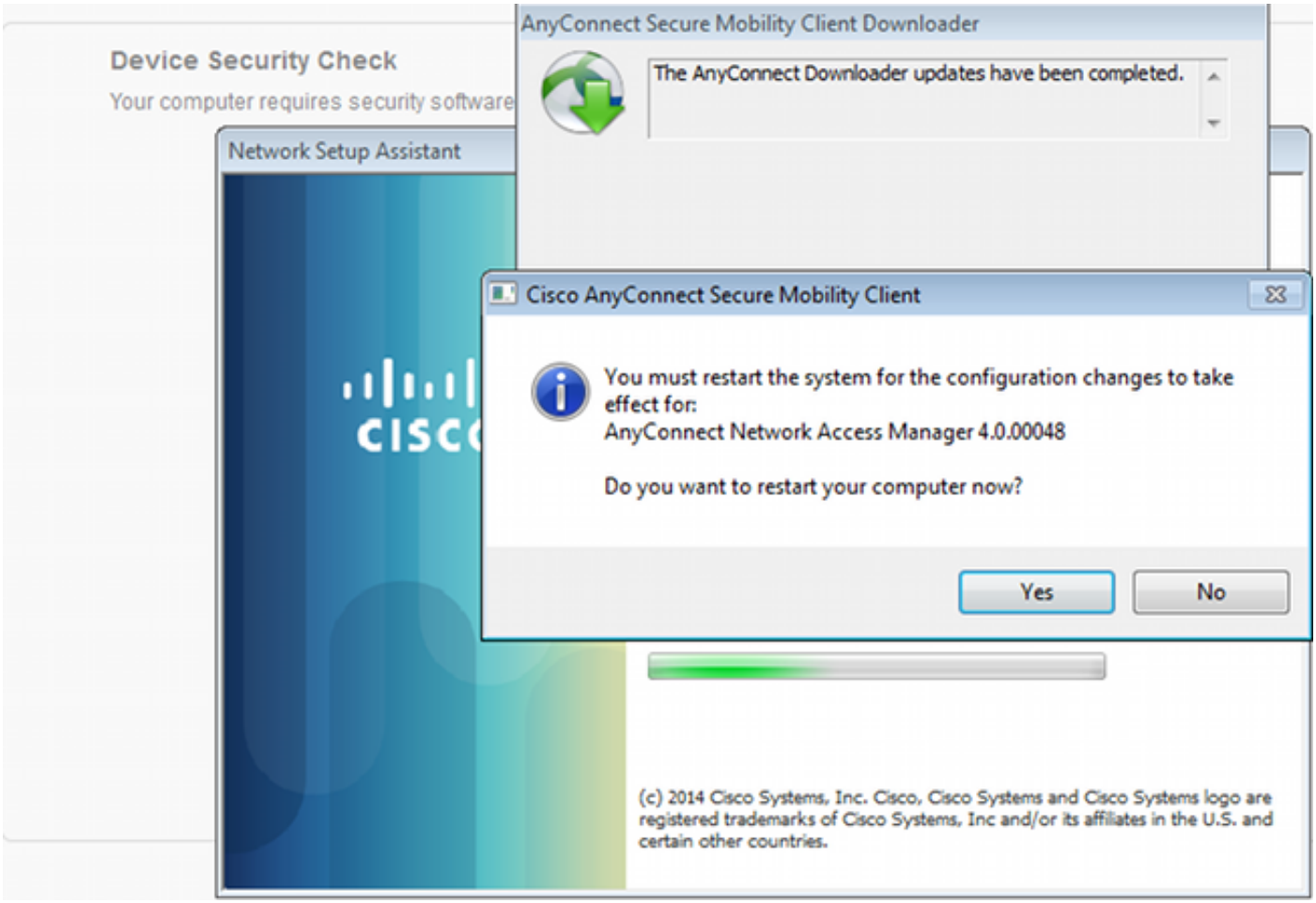


因为没有发现AnyConnect，您请求安装它：

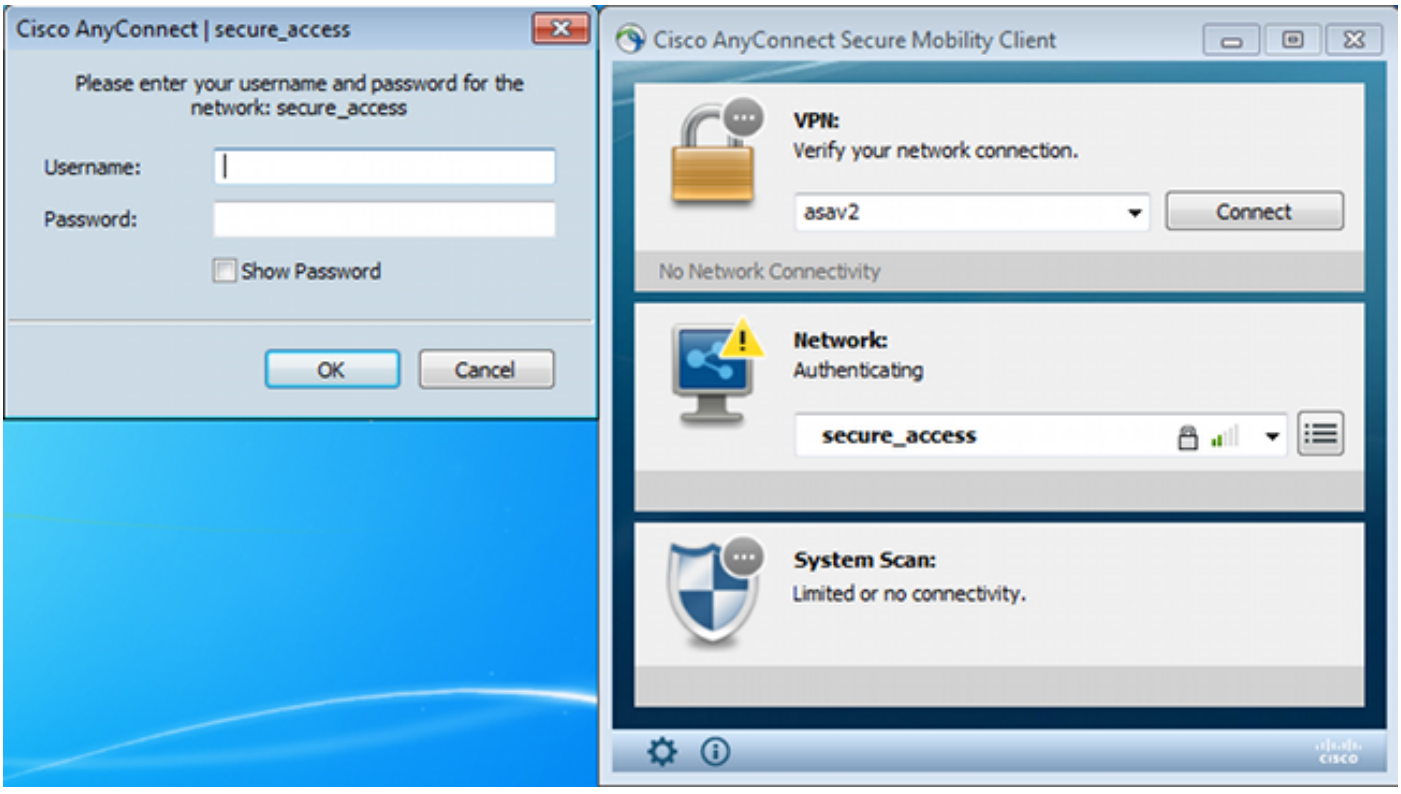


一个小的应用程序告诉了网络建立助理，负责整个安装过程，下载。注意它跟版本1.2的网络建立助理不同。

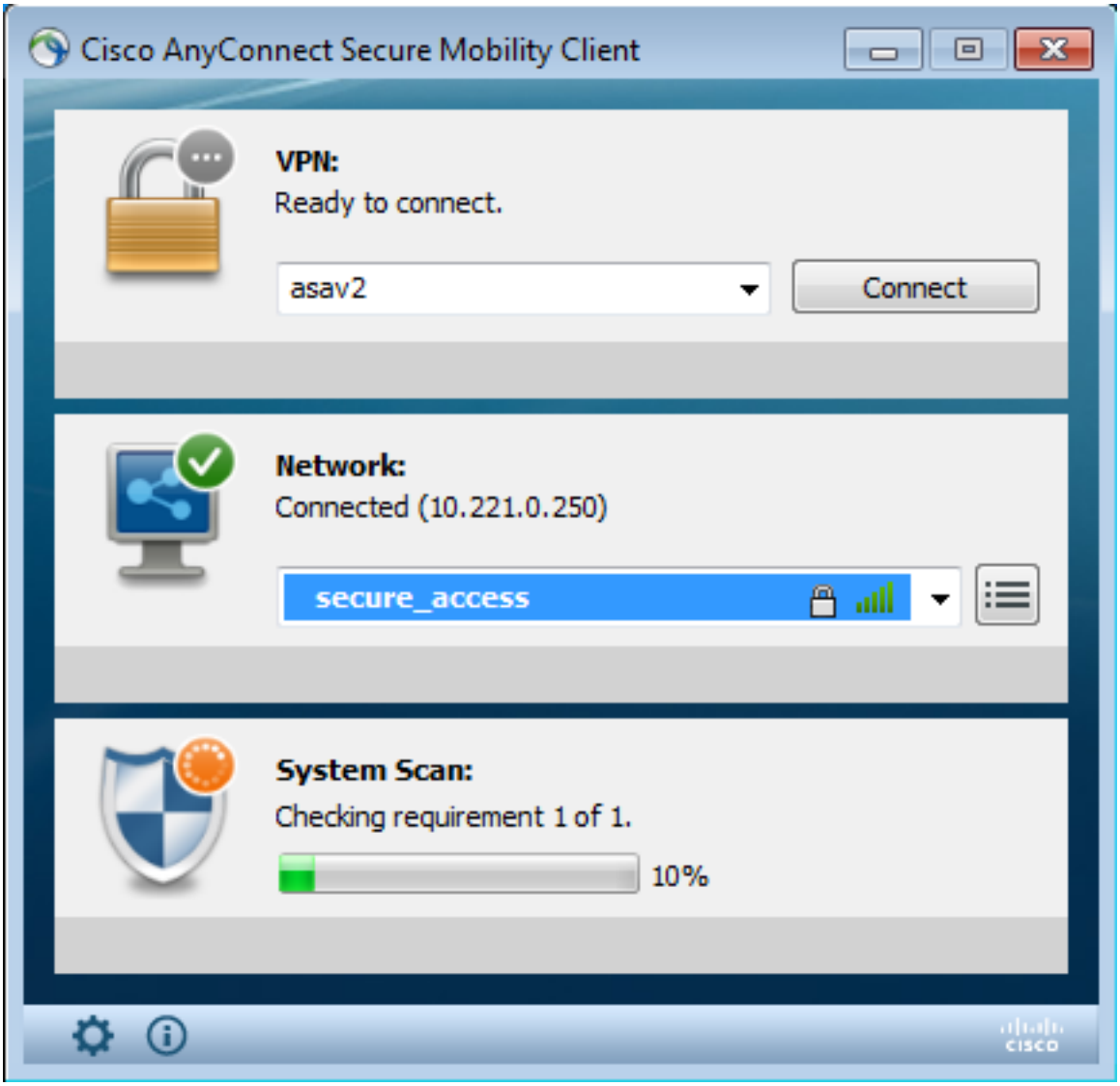
安装所有模块(VPN、NAM和状态)并且被配置。您必须重新启动您的PC ：



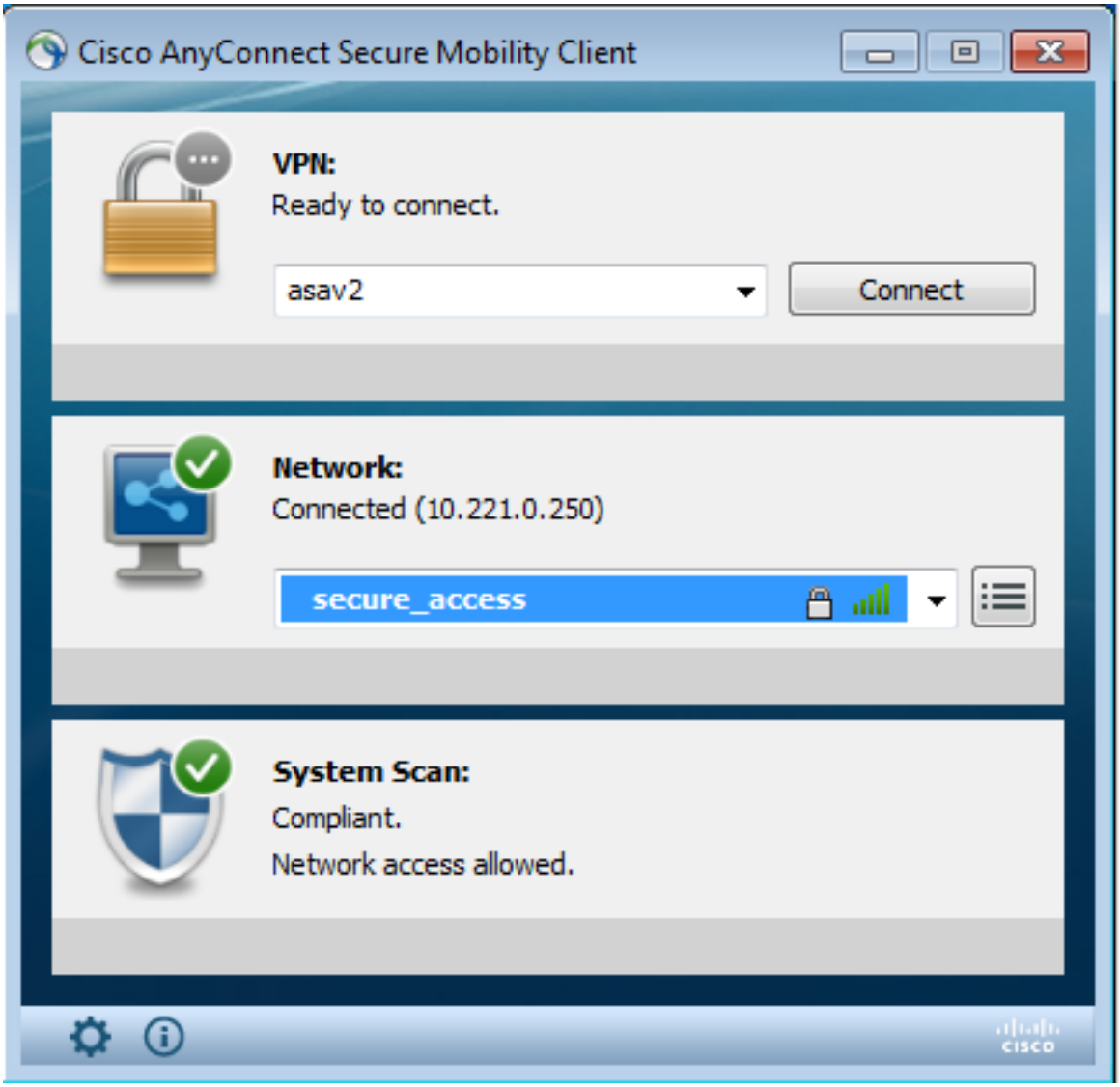
在重新启动 ， AnyConnect自动地被执行，并且后NAM设法与secure_access SSID产生关联(根据被配置的配置文件)。注意正确地安装VPN配置文件(asav2 VPN的条目) ：



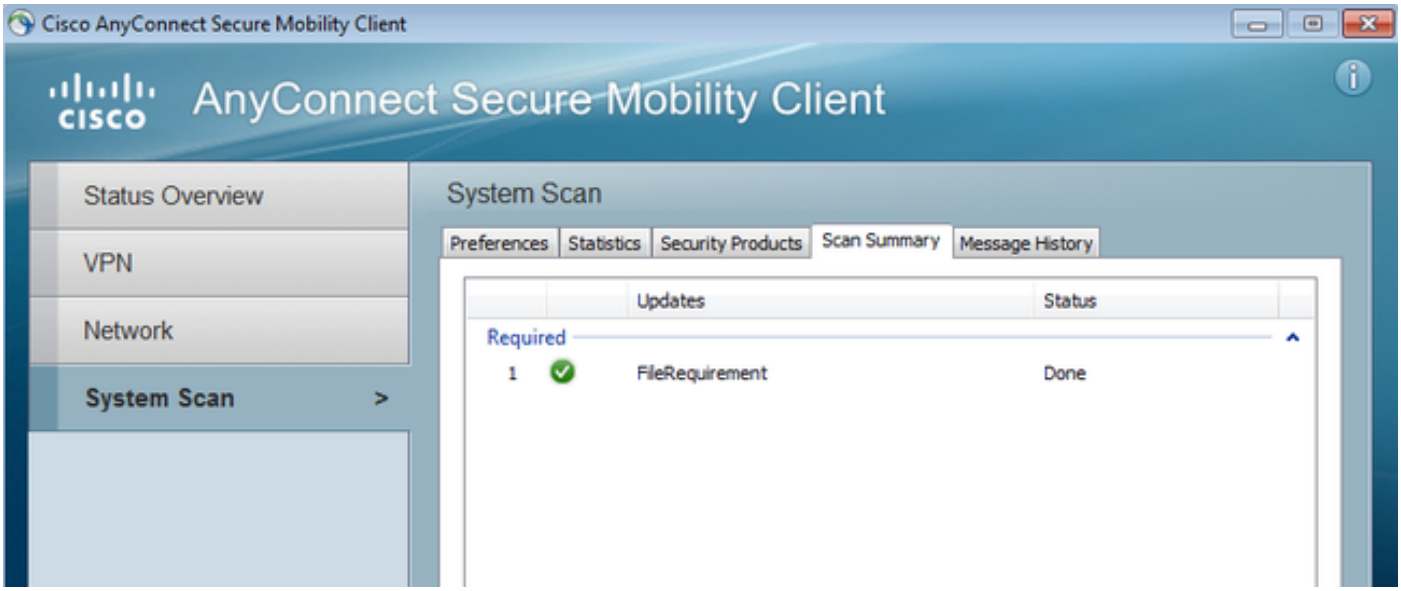
在认证以后 ， AnyConnect下载更新并且摆验证进行的规则姿势 ：



在此阶段，也许仍然有限享用(您遇到在ISE的未知授权规则)。一旦位置是兼容的，那由状态模块报告：



详细资料可以也被验证(FileRequirement是满足的) ：

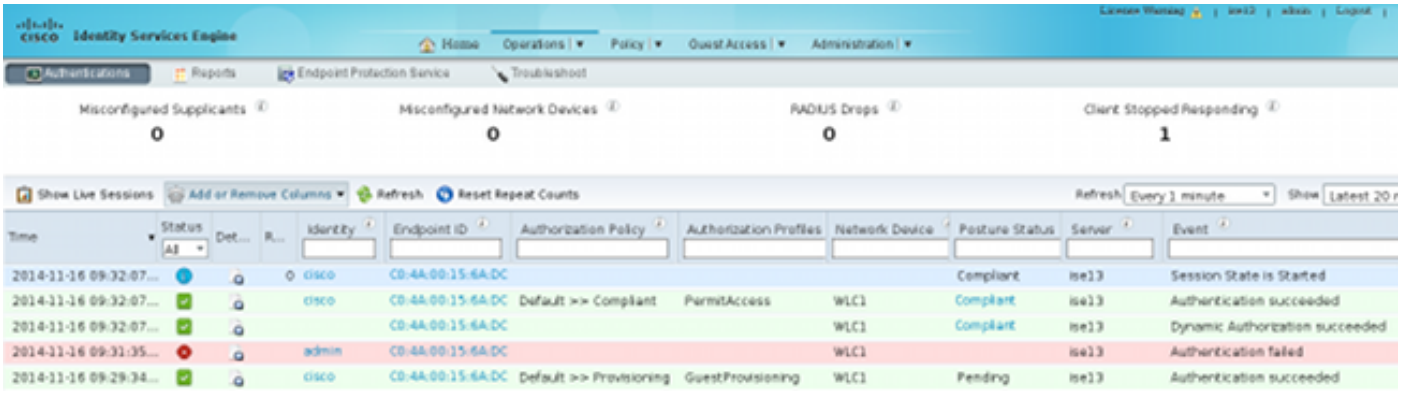


消息历史记录显示详细步骤：

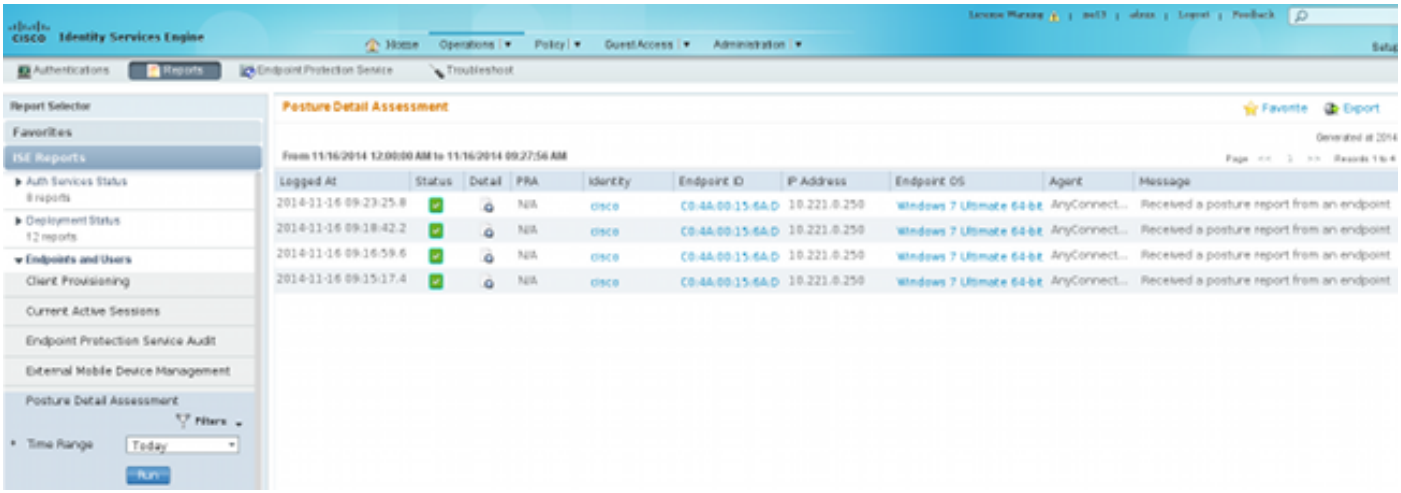
```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

```
9:18:38 AM Checking for customization updates...
9:18:38 AM Performing any required updates...
9:18:38 AM The AnyConnect Downloader updates have been completed.
9:18:38 AM Update complete.
9:18:38 AM Scanning system ...
9:18:40 AM Checking requirement 1 of 1.
9:18:40 AM Updating network settings ...
9:18:48 AM Compliant.
```

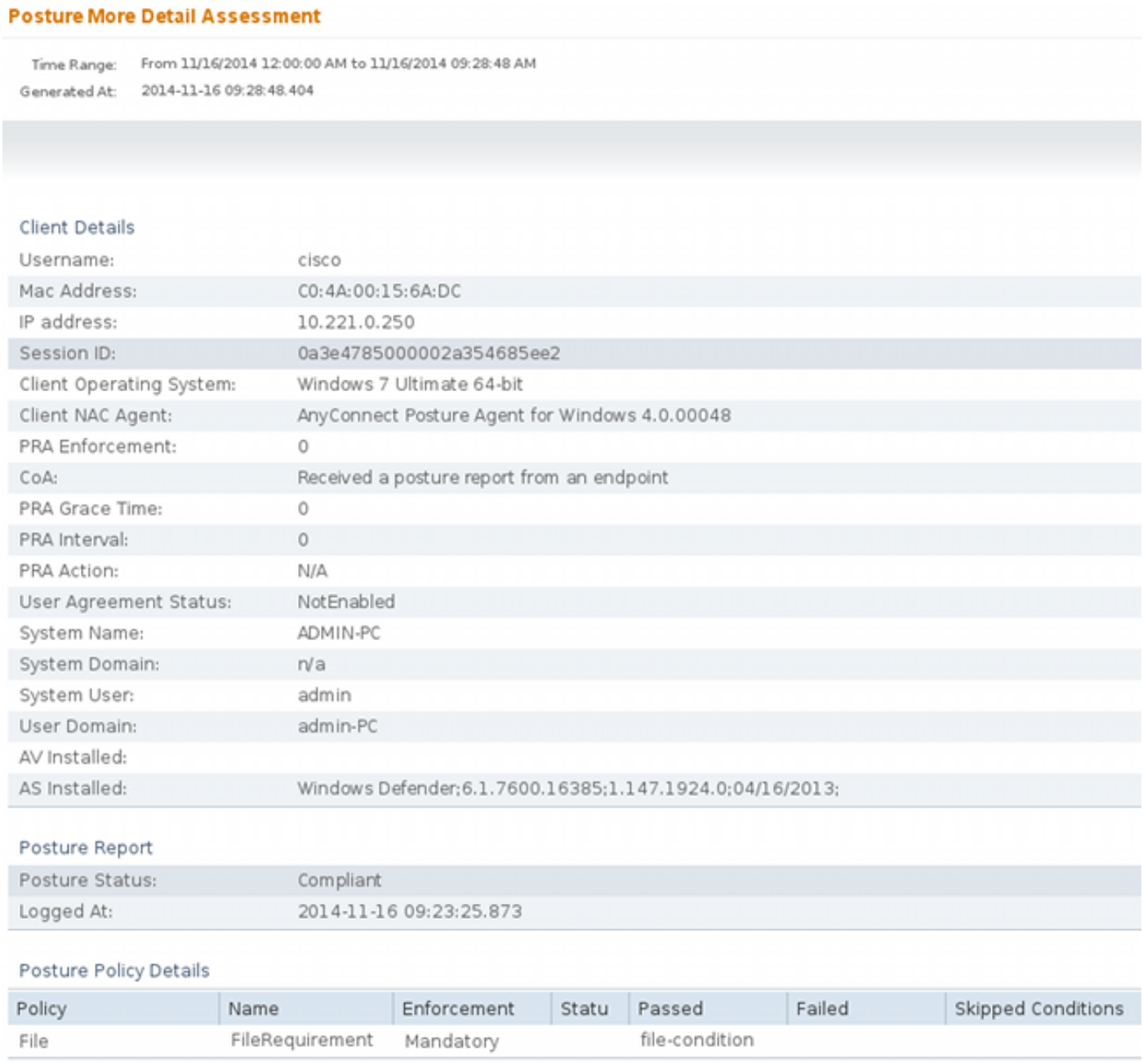
成功的报告被发送到ISE，触发授权的更改。第二个认证遇到兼容规则，并且准许充分的网络访问。如果状态报告在ISE被发送，当仍然联合到设置的SSID，这些日志被看到：



状态报告指示：



详细资料报表显示是满足的FileRequirement ：



Posture More Detail Assessment

Time Range: From 11/16/2014 12:00:00 AM to 11/16/2014 09:28:48 AM
Generated At: 2014-11-16 09:28:48.404

Client Details

Username:	cisco
Mac Address:	C0:4A:00:15:6A:DC
IP address:	10.221.0.250
Session ID:	0a3e4785000002a354685ee2
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.0.00048
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-PC
System Domain:	n/a
System User:	admin
User Domain:	admin-PC
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.147.1924.0;04/16/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2014-11-16 09:23:25.873

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
File	FileRequirement	Mandatory		file-condition		

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- [在Cisco ISE配置指南的状态服务]
- [Cisco ISE 1.3管理员指南]
- [Technical Support & Documentation - Cisco Systems]