在思科ISE配置指南的状态服务

目录

简介

本文描述状态服务、客户端供应、状态策略创建和访问策略配置思科身份服务引擎的(ISE)。终端两个有线的客户端(连接对Cisco交换机)和无线客户端的评估结果(连接对Cisco无线控制器)讨论。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎(ISE)
- Cisco IOS软件交换机配置
- Cisco无线LAN控制器(WLC)配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE版本1.1.3
- Cisco Catalyst 3560系列交换版本15.0(2) SE2
- Cisco 2504系列WLC版本7.4.100.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

ISE状态服务

状态服务工作流包括三个主要配置部分：

- 客户端供应
- 状态策略
- 授权策略

客户端供应

为了执行状态评估和确定终端的标准状态，设置终端用代理程序是必要的。网络准入控制(NAC)代理程序可以是不变的，藉以代理程序安装并且是每次自动地装载的用户登录。或者，美洲台代理程序可以是临时的，藉以一个基于Web的代理程序动态地下载对每个新会话的终端然后删除，在状态评估进程后。美洲台代理程序也实现修正并且提供可选Acceptable Use Policy (AUP)给最终用户。

所以，其中一在工作流的第一步是检索代理程序文件从Cisco网站和创建确定的策略哪些代理程序和配置文件下载对终端，根据属性例如用户标识和客户端OS类型。

状态策略

状态策略定义了套终端的需求能是视为的兼容的根据文件在线状态、注册表项、进程、应用程序、Windows和抗病毒(AV) /anti间谍软件(AS)检查和规则。状态策略应用对终端根据定义的条件例如用户标识和客户端OS类型。终端的标准(状态)状况可以是：

- 未知：数据未收集为了确定状态状态。
- 固执：状态评估执行，并且一个或更多需求失败。
- 兼容：终端与所有强制需求是兼容的。

状态需求根据可配置套一个或更多情况。单纯条件包括单个评估检查。复合条件是一个或更多单纯条件的一个逻辑组。每个需求关联与帮助终端满足要求的一修正操作，例如AV签名更新。

授权策略

授权策略定义了将传送的级别网络访问和可选服务对根据状态状态的终端。视为不兼容与状态策略的终端可能或者被检疫，直到终端变得兼容;例如，一项典型的授权策略可能限制仅客户网络访问摆姿势和修正资源。如果由代理程序或最终用户的修正是成功的，则授权策略能准许对用户的特许网络访问。策略经常强制执行与可下载的访问控制列表(dACLs)或动态VLAN分配。在本例中配置示例，dACLs使用终端访问实施。

状态示例工作流

在此配置示例，不变(美洲台代理程序)和临时(Web代理程序)代理程序文件中下载对ISE，并且要求域用户下载美洲台代理程序和来宾用户下载Web代理程序的客户端提供的策略定义。

在状态评估前策略和需求配置，授权策略更新应用授权配置文件对被标记如固执的域用户和访客。以此配置限制访问摆姿势和修正资源定义的新的授权配置文件。作为兼容和来宾用户被标记的员工允许正常网络访问。一旦客户端供应服务验证，状态需求配置为了检查抗病毒安装、病毒定义更新和Windows关键更新。

> **Note**:在您尝试配置状态前，请验证在这些的所有项目终端和ISE清单。

终端清单

1. ISE完全合格的域名(FQDN)一定是可解决由端点设备。
2. 验证终端浏览器配置如显示此处：

   Firefox或镀铬物：在浏览器必须启用Java插件。**Internet Explorer** ：在浏览器设置必须启用ActiveX。**Internet Explorer 10** ：**导入自签名证书**：如果使用一自签名证书ISE，请运行管理员模式的Internet Explorer 10为了安装这些证书。**兼容模式**：在Internet Explorer 10设置必须更改兼容模式为了允许美洲台代理程序下载。为了更改此设置，用鼠标右键单击蓝色柱状图在Internet Explorer 10屏幕顶部和选择**命令柱状图**。导航对**Tools>兼容性视图**设置，并且添加ISE IP或FQDN到站点列表。
   启用Activex控件：思科ISE安装思科美洲台代理程序和Web代理程序用Activex控件。默认情况下在Internet Explorer 10，选项提示输入Activex控件禁用。采取这些步骤为了启用此选项：导航对**工具> Internet选项**。导航对**安全选项卡**，并且点击**互联网**和**自定义级别**。在Activex控件和插件部分，请启用**自动提示输入Activex控件**。
3. 如果防火墙存在本地在客户端或沿网络路径对ISE，您必须打开ISE美洲台通信的这些端口：

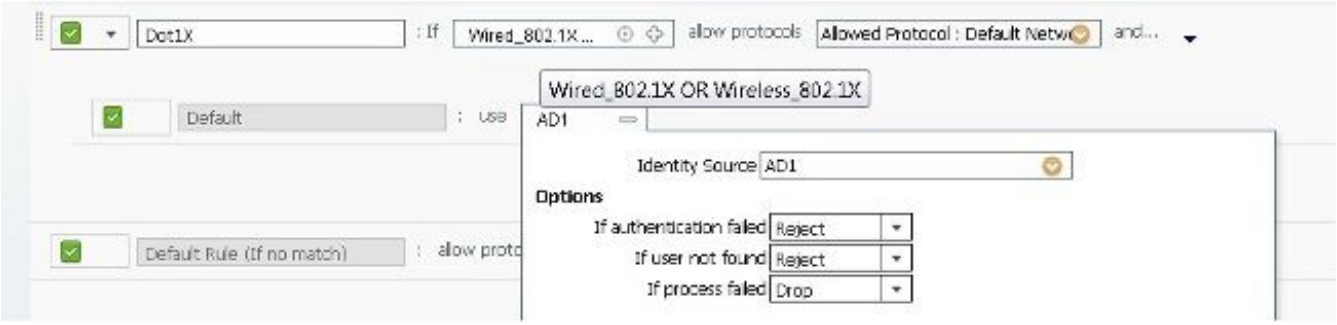
UDP/TCP 8905 ：使用美洲台代理程序和ISE (瑞士端口)之间的状态通信。UDP/TCP 8909 ：使用客户端供应。TCP 8443 ：使用访客和状态发现。**Note**:ISE不再使用传统端口TCP 8906。

4. 如果客户端安排一个代理服务器配置，请修改代理设置为了屏蔽ISE的IP地址。疏忽执行如此中断为中央Web验证(CWA)和客户端供应要求的通信。

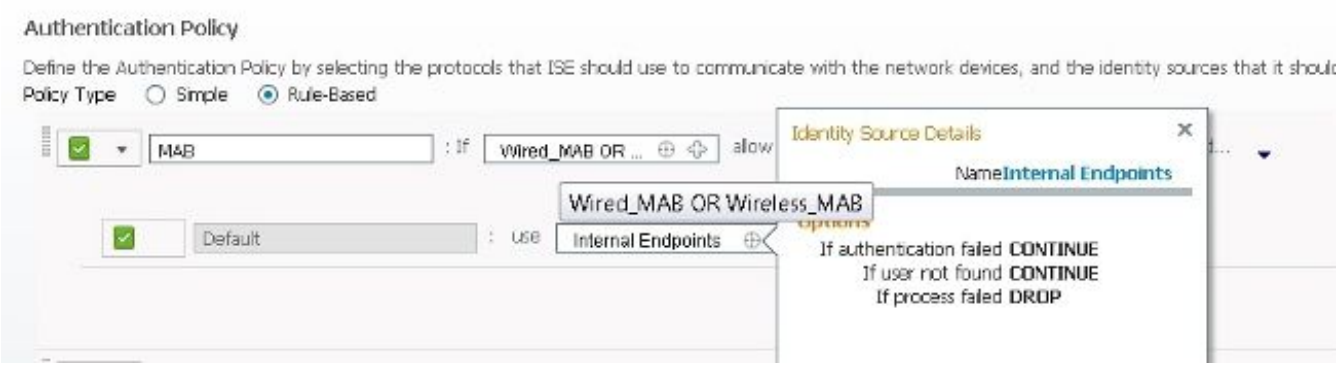
ISE清单

- 导航对**Administration >外部标识来源>活动目录**，并且验证ISE加入对激活目录(AD)域。
- 点击**组**选项卡，并且验证域用户用户组被添加到AD配置。
- 导航到**Administration >网络资源>网络设备**，并且验证交换机和WLC定义作为网络访问设备(纳季)。
- 在**策略>验证下**，请保证dot1x，并且MAC验证旁路(MAB)规则配置如描述此处：

  有线的Dot1x认证和无线客户端派遣到AD标识存储。



有线的MAB认证和无线设备发送对内部终端;**如果用户没找到继续，**请务必检查选项。



配置ISE

ISE配置概述

此示例ISE配置包括这些步骤：

1. 配置并且部署客户端供应服务。
2. 配置授权策略。
3. 配置状态策略。

4. 配置Windows服务器更新服务(WSUS)修正。

配置并且部署客户端供应服务

1. 验证ISE代理配置。

   导航给**管理>System >设置>代理**。如果代理为互联网访问要求，请完成服务器和端口详细资料。
2. 下载预先构建状态检查AV/AS和Microsoft Windows.

   导航对**管理>System >设置>状态>更新**。因为更新未下载，在底下右边的窗格的更新信息应该是空的。配置以下值：

   单击**更新当前**，并且确认更新可能采取一些时间完成的警告。

   Note:如果ISE不访问互联网访问，脱机状态更新可以在Cisco.com的下载。
3. (可选)请配置代理程序行为的一般设置。

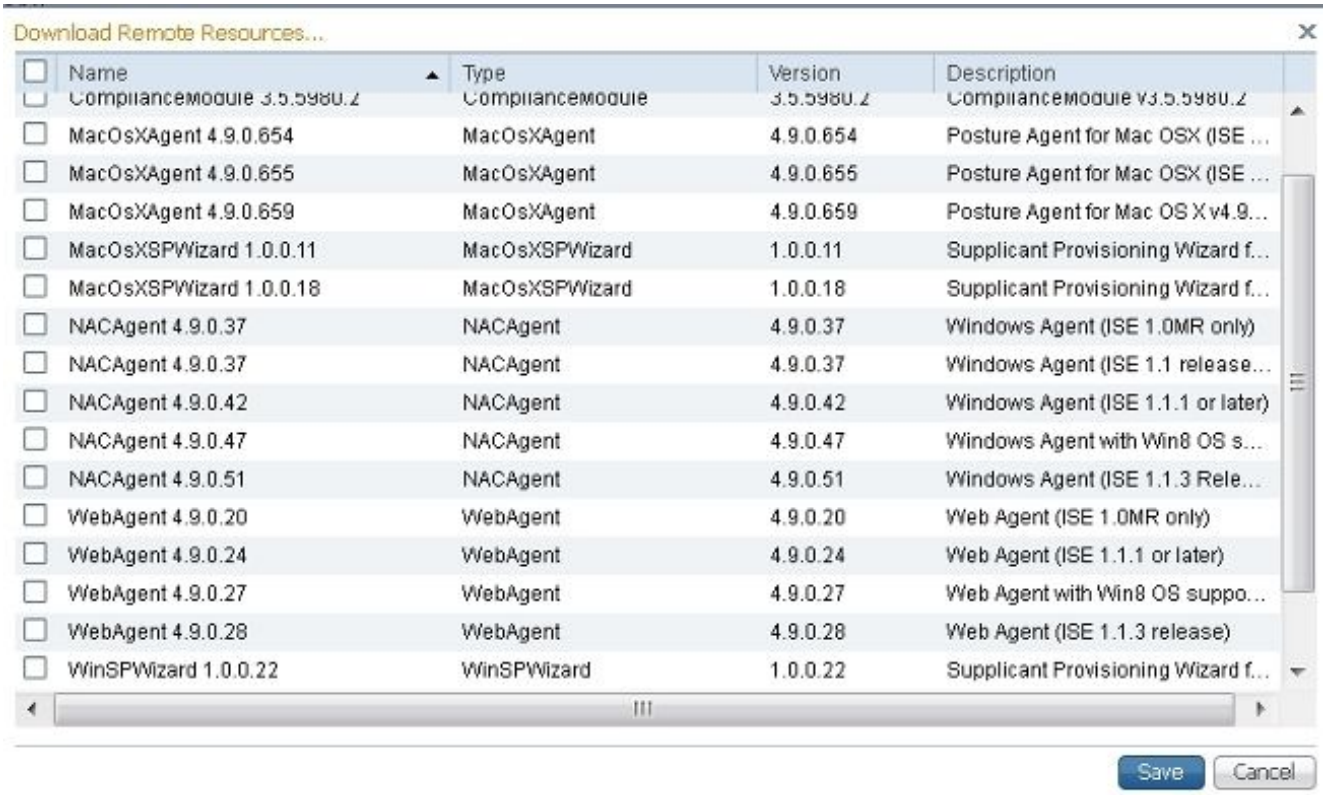
   选择**管理>System >设置>状态>General设置**，并且查看修正计时器、网络转换迪莱和默认状态状态的默认值。设置修正计时器为8分钟。**在**复选框以后检查(enable (event))**自动地接近的洛金成功屏幕**和set time对5秒如显示此处：

   Click **Save**.
   Note:通过代理程序配置文件覆盖分配的值这些全局设置。默认状态状态定义了不安排一个美洲台代理程序安装的客户端的状态。如果没有使用客户端供应，此值可以设置到固执。
4. 设置位置和策略下载客户端供应更新。

   点击**管理>System >设置>**从左边窗格的**客户端供应**，并且验证这些默认值设置：

5. 下载代理程序文件。

   导航对**策略>Policy元素>结果**，展开**客户端供应**文件夹，并且选择**资源**。从右边的窗格，请点击**从思科站点的Add>代理程序资源**从下拉列表。弹出窗口显示远程资源：



最少，请选择当前美洲台代理程序、Web代理程序和法规遵从性模块(AV/AS支持模块)从列表，并且点击**"Save"**。客户端供应文件类型是：

美洲台代理程序：Windows客户端PC。的不变状态代理程序**Mac OS X代理程序**：Mac OS X客户端PC机的不变状态代理程序**Web代理程序**：仅Windows PC。的临时状态代理程序**法规遵从性模块**：提供更新给当前AV/AS供应商支持为美洲台代理程序和Mac OS X代理程序的OPSWAT模块。不可适用对Web代理程序。**配置文件**：美洲台代理程序和Mac OS X代理程序的代理配置文件。在客户端PC机的本地更新已安装XML文件不可适用对Web代理程序。请等待，直到文件下载到ISE设备。

6. (可选)请创建您的客户端的一美洲台代理配置配置文件。

   从右边的窗格，请单击**添加**，然后选择**ISE**从下拉列表的**状态代理程序配置文件**。修改配置文件为了满足部署要求。

   只有当其他值没有定义，合并选项更新当前代理程序配置文件参数。覆盖选项更新参数值是否明确地定义。对于可配置美洲台代理程序参数完整列表，参考思科身份服务引擎用户指南，版本1.1.x。
7. 定义域用户和来宾用户的客户端提供的策略。

   导航对**策略>客户端供应**。如此表所述，增加两个新的客户端供应规则。在所有规则条目右边单击Action按钮为了插入或复制规则。

   Note:如果多个版本同样文件类型(美洲台代理程序Web代理程序法规遵从性模块)下载到客户端供应信息库，请选择多数当前版本联机，当您配置规则时。点击**"Save"，当完成。**
8. 配置Web验证门户为了下载状态代理程序如定义由客户端提供的策略。

   导航对**Administration > Web门户Management>设置**，展开**访客**文件夹，选择多**PORTAL配置**，并且选择**DefaultGuestPortal**。在**操作**选项卡下，请使选项为了允许来宾用户下载代理程序

和对自己注册。

定义赛弗注册访客角色和赛弗注册时间配置文件如显示此处。访客自己服务是让用户创建帐户，不用赞助商干预的可选配置。此示例使自己服务为了简化访客注册过程。

(可选)设置来宾用户的AUP如显示此处：

点击**"Save"**，当完成。

配置客户端供应的授权策略并且摆姿势

授权策略设置将授权的访问和服务种类对终端根据他们的属性例如标识、访问方法和遵照状态策略。在本例中的授权策略保证不是兼容的状态的终端被检疫;即终端授权满足的有限访问设置代理软件和到修正失败的需求。仅状态兼容终端授权特许网络访问。

1. (可选)。定义限制终端的网络访问不是兼容的状态的dACL。

   导航对**策略>Policy元素>结果**，展开**授权**文件夹，并且选择**可下载的ACLs**。单击从右边的窗格**添加**在DACL管理下，并且输入新的dACL的这些值。

   这是示例状态dACL。因为ISE 1.1.x当前不支持ACL语法验证，查看准确性的dACL条目。

   单击**提交**，当完成。
2. 定义802.1Xauthenticated/NAC代理程序用户的一新的授权配置文件名为**Posture_Remediation**。配置文件有效利用端口访问控制的新的dACL，并且URL重定向流量重定向的ACL。

   导航对**策略>Policy元素>结果>授权**，并且选择**授权配置文件**。单击从右边的窗格**添加**，并且输入授权配置文件的这些值：

   这些产生的属性详细信息应该出现在页底端：

   访问类型= ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   cisco ：cisco-av-pair=url-redirect-acl=ACL-状态重定向
   cisco ：cisco-av-pair=url-redirect = https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cpp单击**提交**为了应用您的更改。

   Note:在交换机或WLC必须配置ACL-POSTURE-REDIRECT ACL本地。ACL名义上被参考

ISE授权策略。对于交换机重定向ACL， permit条目确定应该重定向什么流量到ISE，而，在WLC， permit条目定义了不应该重定向什么流量。

3. 定义Web验证的/Web代理程序用户的一新的授权配置文件名为**CWA_Posture_Remediation**。配置文件有效利用端口访问控制的新的dACL，并且URL重定向流量重定向的ACL。

   导航对**策略>Policy元素>结果>授权**，并且选择**授权配置文件**。单击从右边的窗格**添加**，并且输入授权配置文件的这些值：

   这些产生的属性详细信息应该出现在页底端：

   访问类型= ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   cisco ：cisco-av-pair=url-redirect-acl=ACL-状态重定向
   cisco ：cisco-av-pair=url-redirect
   =https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cwa单击**提交**为了应用您的更改。

   Note:两配置文件之间的差异是URL重定向cisco-av-pair属性。需要验证的用户重定向到CWA的访客门户。一旦验证，用户自动地重定向对CPP当必要时。通过802.1X验证的用户重定向直接地对CPP。

4. 更新授权策略为了支持状态标准。

   导航对**策略>授权**。更新与这些值的现有授权策略。请使用选择器在规则条目结束时为了插入或复制规则：

   点击**"Save"**为了应用您的更改。

   Note:此授权配置文件应用对有线和无线用户用户访问。WLC不考虑到dACL。交换机仅支持dACL功能。对于无线，重定向ACL是否决所有流量的足够除了纠正服务器和ISE状态。

配置AV状态策略

此示例显示如何定义一项AV策略以这些状态情况：

- 摆域用户的策略姿势能有ClamWin AV安装的和当前。
- 摆来宾用户的策略姿势能安装ClamWin AV，如果没有抗病毒安装。

1. 定义验证ClamWin AV安装在终端的AV状态情况。此检查用于状态需求应用对员工。

   导航对**策略>Policy元素>情况**，展开**状态**文件夹，并且选择**AV复合条件**。单击从右边的窗格菜单**添加**。如果AV产品没出现在**供应商**字段下，状态更新未下载或下载未完成。输入这些值：

   单击**提交**在页底端。

2. 定义验证ClamWin AV签名版本在终端的AV状态情况。此检查用于状态需求应用对员工。

   从左边窗格的挑选**AV复合条件**，和单击从右边的窗格菜单**添加**。输入这些值：

单击**提交**在页底端。

3. 定义验证所有支持的AV安装在终端的AV状态情况。此检查将使用状态需求应用对来宾用户。

   从左边窗格的挑选**AV复合条件**，和单击从右边的窗格菜单**添加**。输入这些值：

   单击**提交**在页底端。

4. 定义安装在终端的ClamWin AV的状态修正操作。

   导航对**策略>Policy元素>结果**，并且展开**状态**文件夹。展开**修正操作**内容。选择**林克修正**，并且单击从右边的窗格菜单**添加**。输入这些值：

   单击 **submit**。

   Note:*REM服务器IP*代表ClamWin安装存在您的纠正服务器的IP地址。在本例中的可执行文件在纠正服务器被前置。为了使工作的修正，请保证ClamWin更新服务器IP在以前已配置的dACL和重定向ACL包括。

5. 定义更新在终端的ClamWin AV的状态修正操作。

   选择从左边窗格的**AV/AS修正**，并且单击从右边的窗格菜单**添加**。输入这些值：

   单击 **submit**。

6. 定义将应用给员工和来宾用户的状态需求。

   选择从**策略>Policy元素>结果>状态的需求**。输入这些条目到表。请使用选择器在规则条目结束时为了插入或复制规则：

   点击**"Save"，**当完成。

   Note:如果一个预先配置的情况不显示在情况下列表，请验证适当的OS为情况选择以及需求规定。是相同的或是为在情况选择列表的规则显示选择的OS的一子集仅的情况。

7. 配置状态在雇员计算机的策略为了保证ClamWin AV安装和当前有Windows的7，并且所有支持的AV安装和在来宾用户计算机的当前。

   导航对**策略>状态**，并且创建与在此表里提供的值的新的策略规则。为了指定状态需求如必须，可选或者审计，请在需求名称右边单击图标，并且从下拉列表选择选项。

   点击**"Save"**为了应用您的更改。

配置WSUS修正

此示例显示如何保证有Windows的7所有雇员计算机有安装的最新的关键补丁程序。Windows服务器更新服务(WSUS)内部地管理。

1. 定义检查并且安装最新的Windows 7补丁程序的状态修正操作。

   导航对**策略>Policy元素>结果**，并且展开**状态**文件夹。展开**修正操作**内容。选择**Windows服务器更新修正**，并且单击从右边的窗格菜单**添加**。输入这些值，并且单击**提交**：

Note:如果要使用思科规则为了验证Windows更新，请创造您的状态条件，并且定义您的在步骤2.的条件。

2. 定义将应用给员工的状态需求。

   导航对**策略>Policy元素>结果>状态**，并且选择**需求**。输入这些条目到表。请使用选择器在规则条目结束时为了插入或复制规则：

   Note:您能找到情况**pr_WSUSRule**在**思科下定义情况>正常复合条件**。(这是选择的一个假的规则，因为Step1设置严重级别将验证的Windows更新。)

3. 配置状态策略为了保证有Windows的7雇员计算机有最新的关键Windows 7补丁程序。

   导航对**策略>状态**，并且创建与值的新的策略规则在此表里：

   点击**"Save"**为了应用您的更改。

采样交换机配置

此部分提供交换机配置的摘要。供仅参考使用并且不应该复制或粘贴到生产型交换机。

全局Radius和Dot1x配置

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
ip radius source-interface Vlan (x)
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-acce ss-req
radius-server attribute 25 access-request include
radius-server host <ISE IP> key <pre shared key>
radius-server vsa send accounting
radius-server vsa send authentication
```

在波尔特将应用的默认ACL

```
ip access-list extended permitany
permit ip any any
```

Enable (event) Radius授权崔凡吉莱

```
aaa server radius dynamic-author
client <ISE IP> server-key <pre share d key>
```

Enable (event)网域名称转址和记录日志

```
Ip device tracking
```

```
Epm logging
Ip http server
Ip http secure server
```

重定向ACL

```
ip access-list extended ACL-POSTURE-REDIRECT
deny udp any eq bootpc any eq bootps
deny udp any any eq domain
deny udp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8909
deny udp any host <ISE IP> eq 8909
deny tcp any host <ISE IP> eq 8443
deny ip any host <REM SERVER IP>
deny ip any host 192.230.240.8           (one of the ip of CLAMwin database virus Definitions)
permit ip any any
```

Note:端点设备的IP地址一定是可及的从Switch Virtual Interface (SVI)为了重定向能工作。

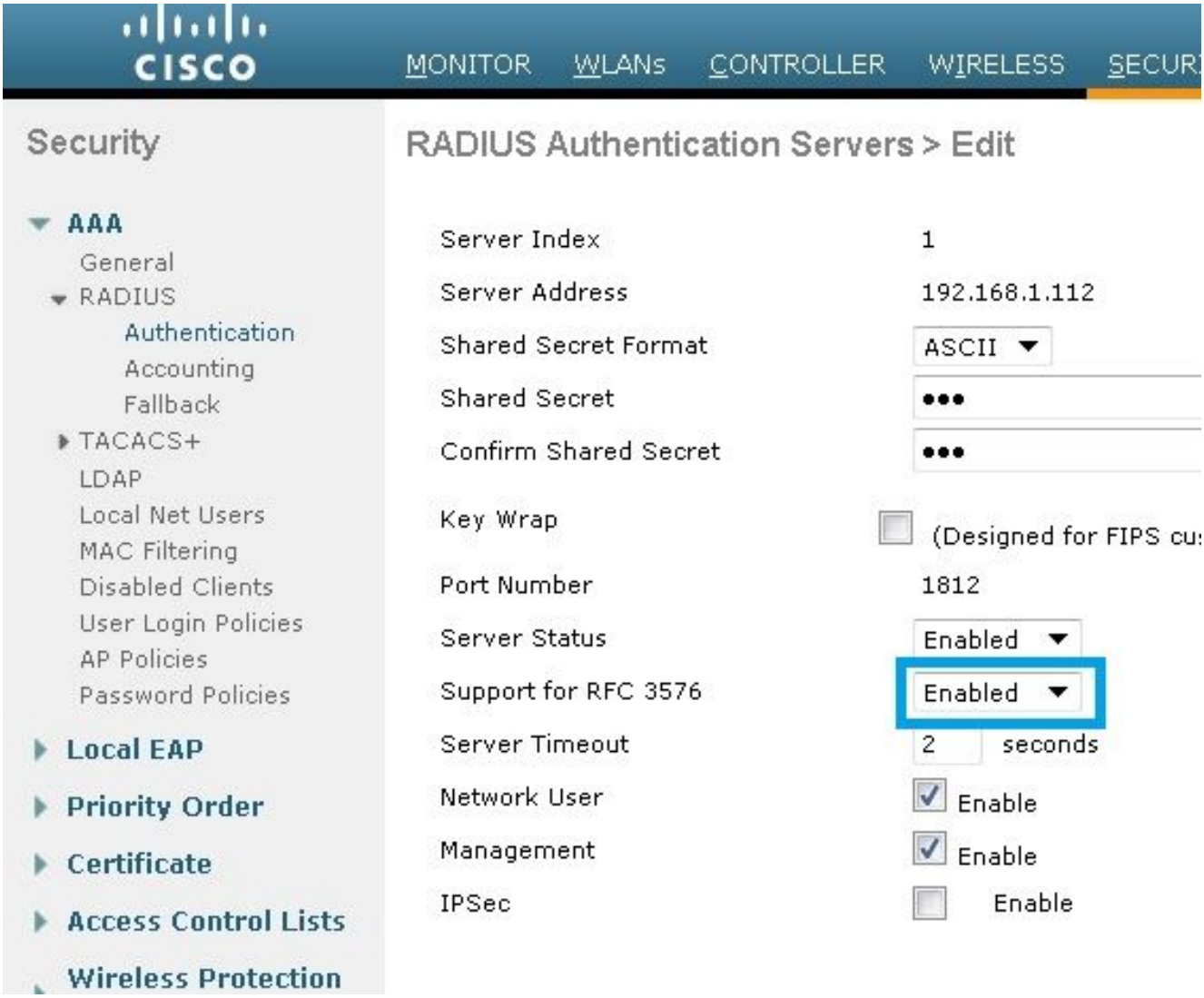
交换端口配置

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier
than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

示例WLC配置

全局配置

1. 保证RADIUS服务器有(CoA)启用的RFC3576;默认情况下它启用。



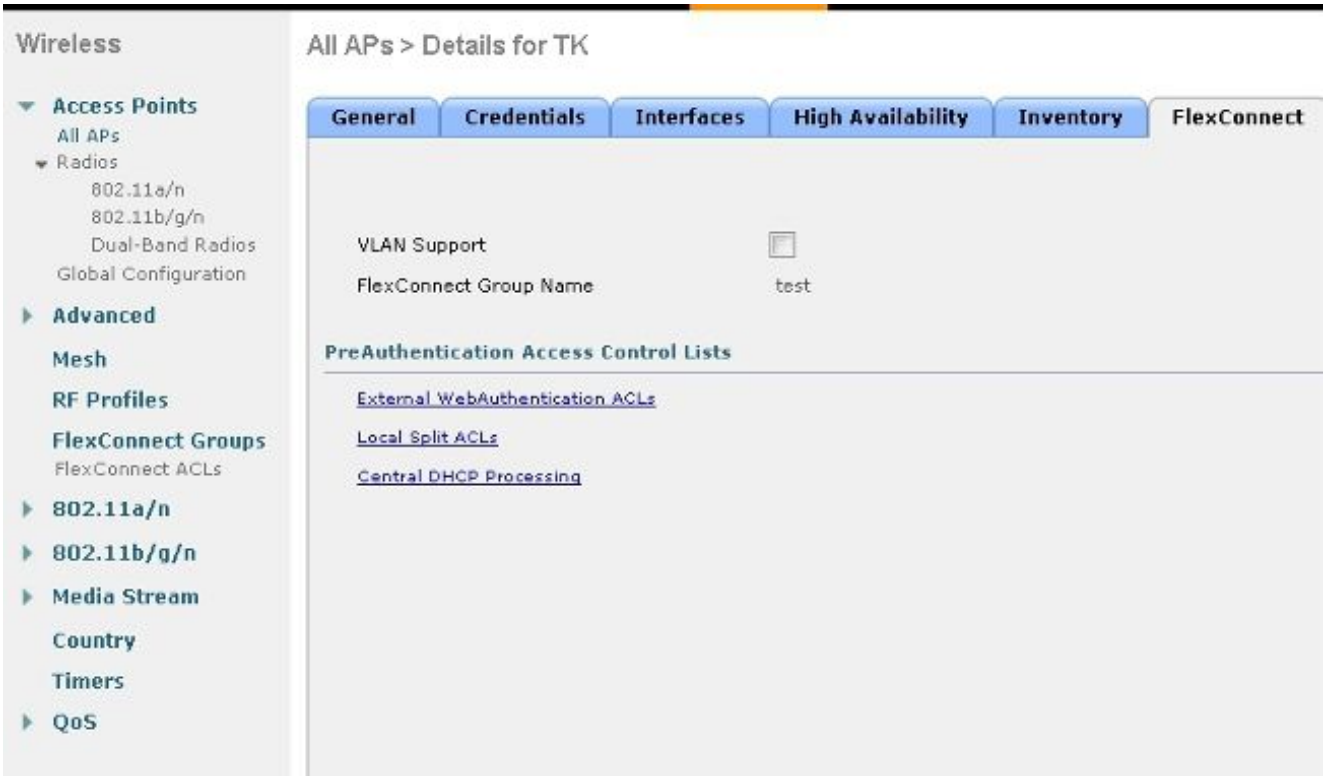
2. 导航对**安全>访问控制列表**，创建在WLC的ACL并且称它'ACL-POSTURE-REDIRECT'。

15和16用于此示例ClamWin 192.230.240.8包含数据库定义文件的AV更新。

对于与本地交换的FlexConnect，您必须创建FlexConnect ACL，并且应用它对WebPolicy ACL。ACL有名称和在WLC的ACL一样并且有同样属性。

1. 点击**FlexConnect ACL**。

2. 点击**外部WebAuthentication ACL**。



3. 添加WebPolicy ACL。

4. 单击 **Apply**。

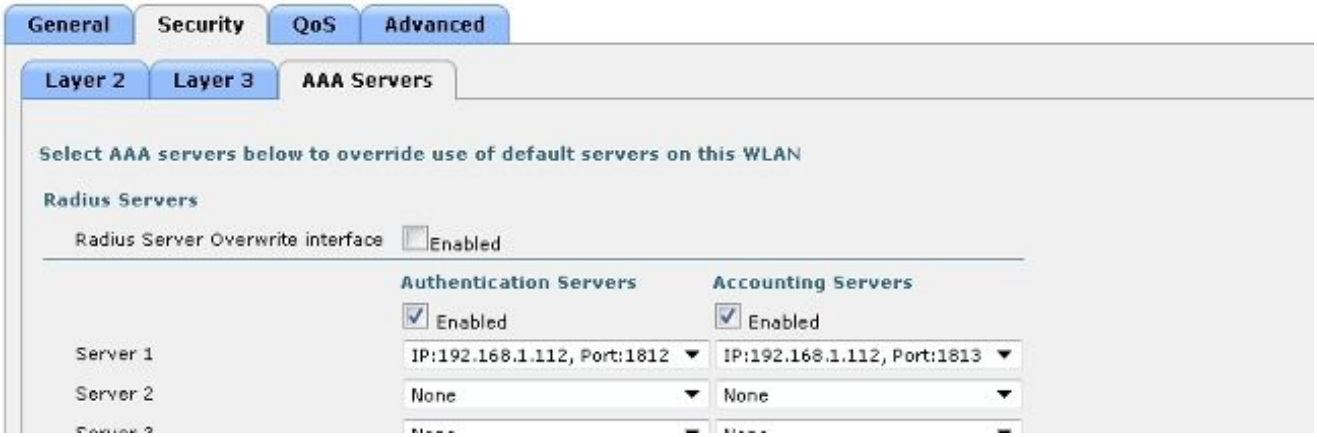
雇员SSID配置

创建一新的雇员服务集标识(SSID)或修改当前一个。

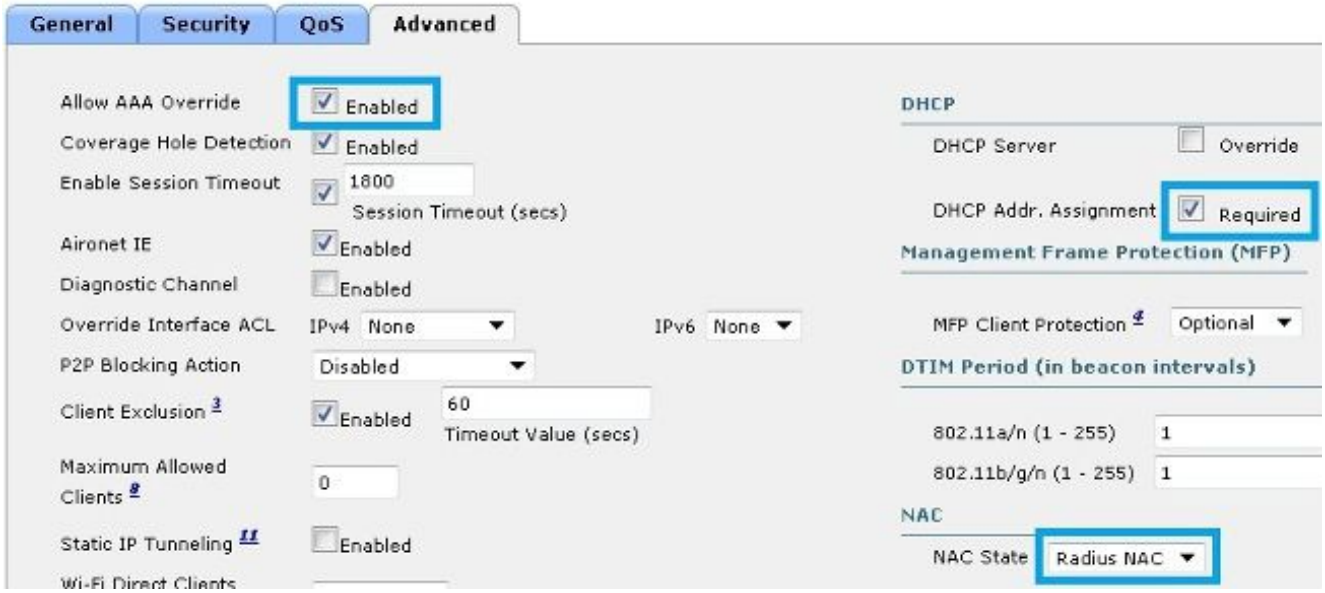
1. 在**WLAN**选项卡，请单击**创建新**或点击一现有WLAN。

2. 点击**安全选项卡**，点击**Layer2**选项卡，然后设置适当的安全。这是WPA的配置与dot1x的。

3. 点击**AAA服务器**选项卡，并且检查(enable (event)) ISE作为RADIUS服务器验证和核算。



4. 点击**高级选项卡。**，检查(enable (event))**允许AAA覆盖**和**DHCP地址。分配**复选框，和设置**美洲台状态**为Radius美洲台。



访客SSID配置

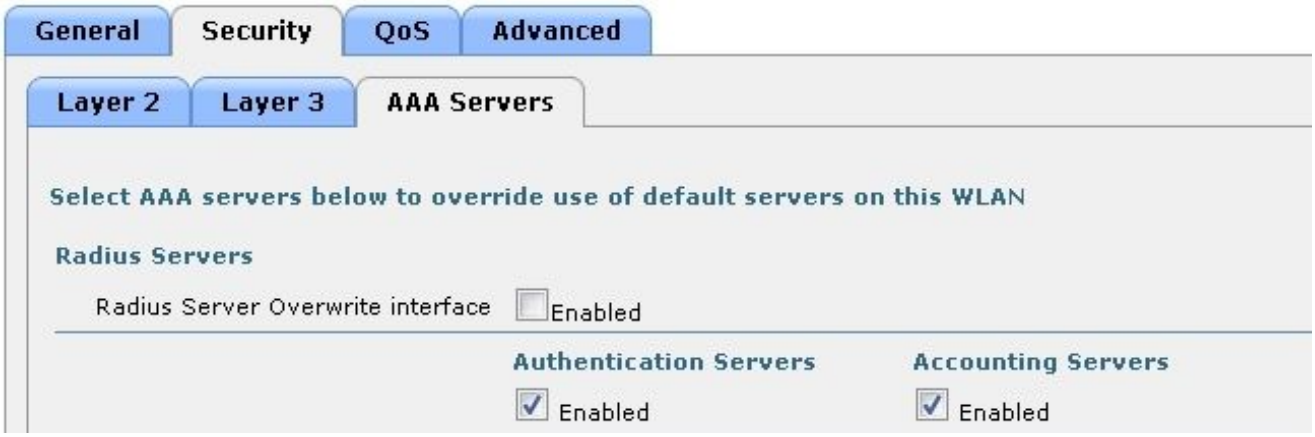
创建与访客SSID的一新的WLAN或修改一当前一个。

1. 在**WLAN**选项卡，请单击**创建新**或点击一现有WLAN。

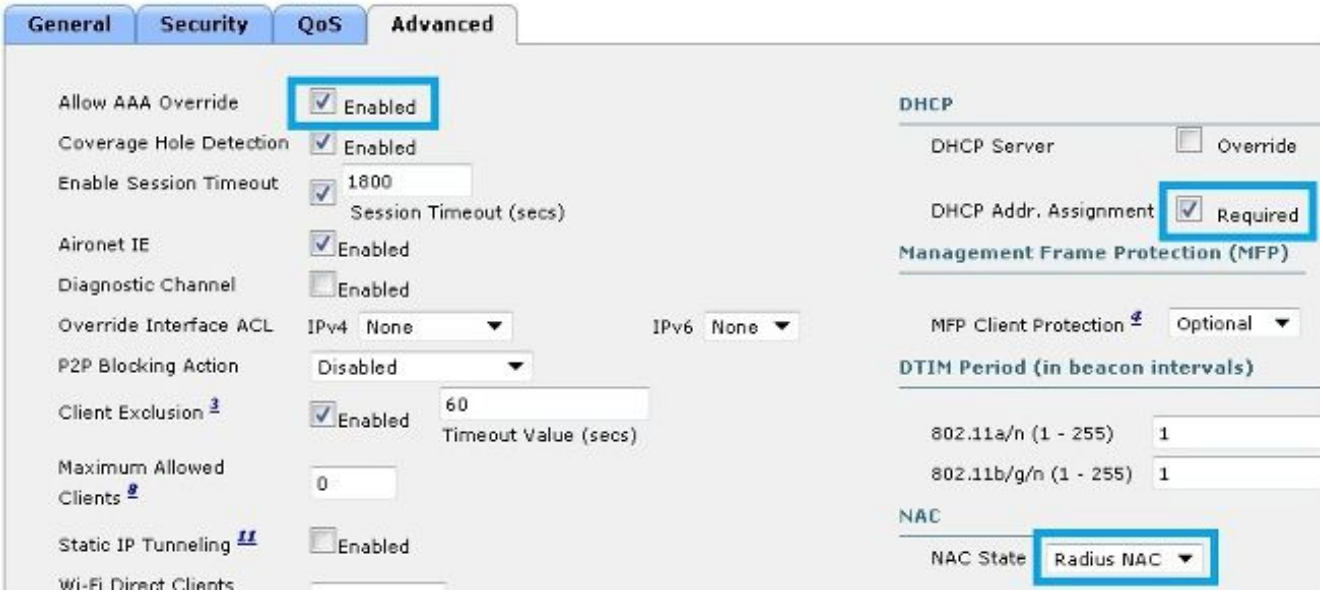
2. 点击**安全选项卡**，点击**Layer2**选项卡，然后检查(enable (event))**过滤**复选框。的**MAC**

3. 点击**第3层**选项卡，并且保证所有选项禁用。

4. 点击**AAA服务器**选项卡，并且检查(enable (event)) ISE作为认证服务器和记帐服务器。



5. 点击**高级选项卡。**，检查(enable (event))**允许AAA覆盖**和**DHCP地址。分配**复选框，和设置**美洲台状态**为Radius美洲台。

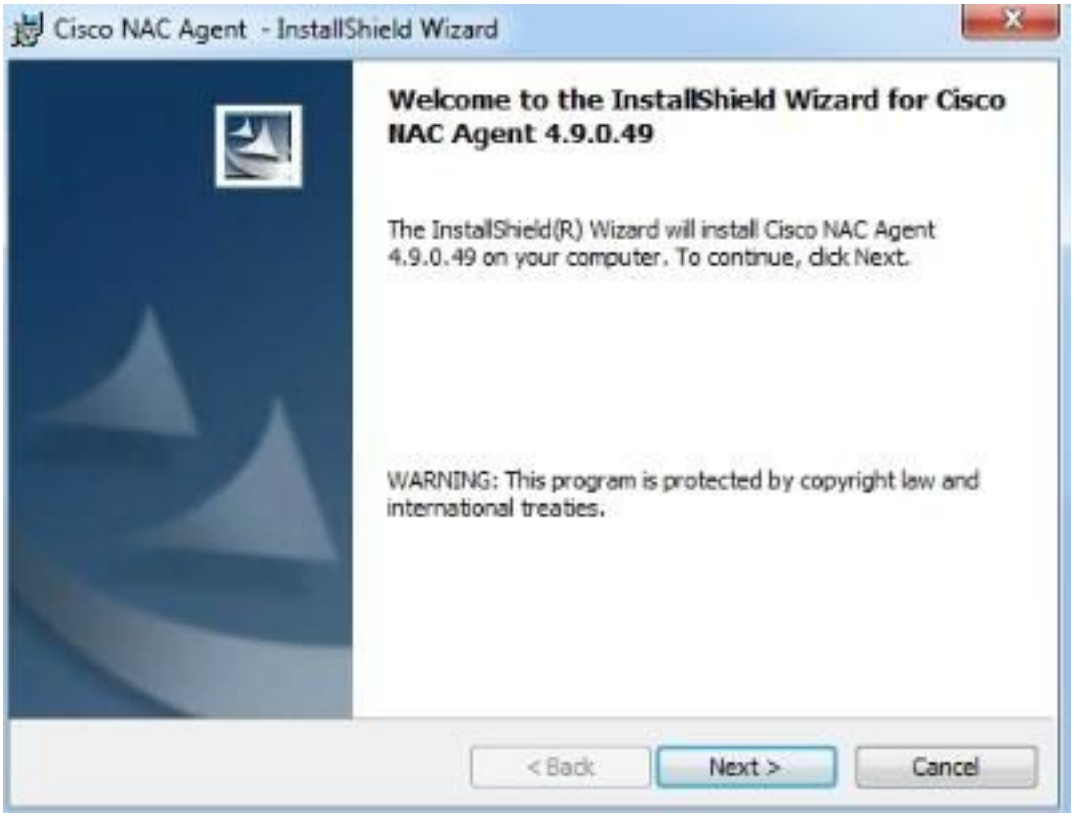


雇员Dot1x状态(美洲台代理程序)

一旦客户端连接对以前配置的WLAN这是状态的步骤从客户端方面。

1. 配置您的无线PEAP MSCHAP的V2 SSID (员工)或有线网络，并且连接域用户用户组的一个AD用户。
2. 打开浏览器，并且设法导航到站点。重定向提示符显示。
3. 单击**单击安装代理程序**。

4. 单击 **Next**。

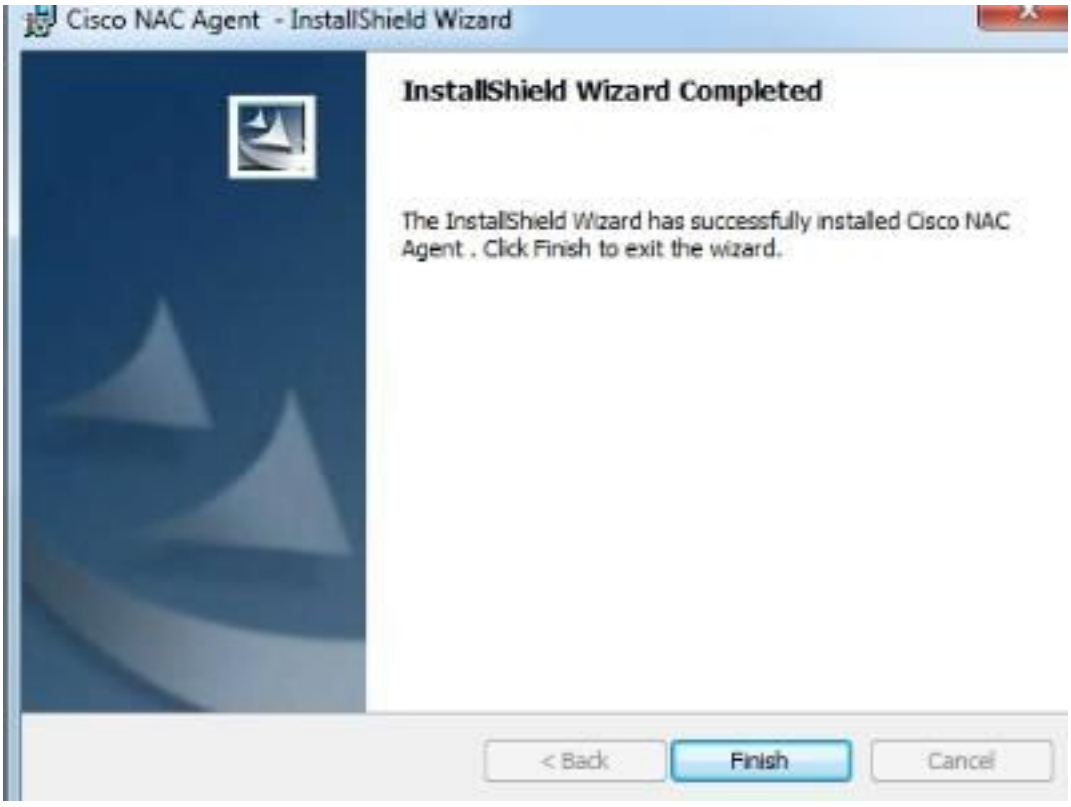


5. 点击**我接受许可证协议的条件**，并且**其次**单击。

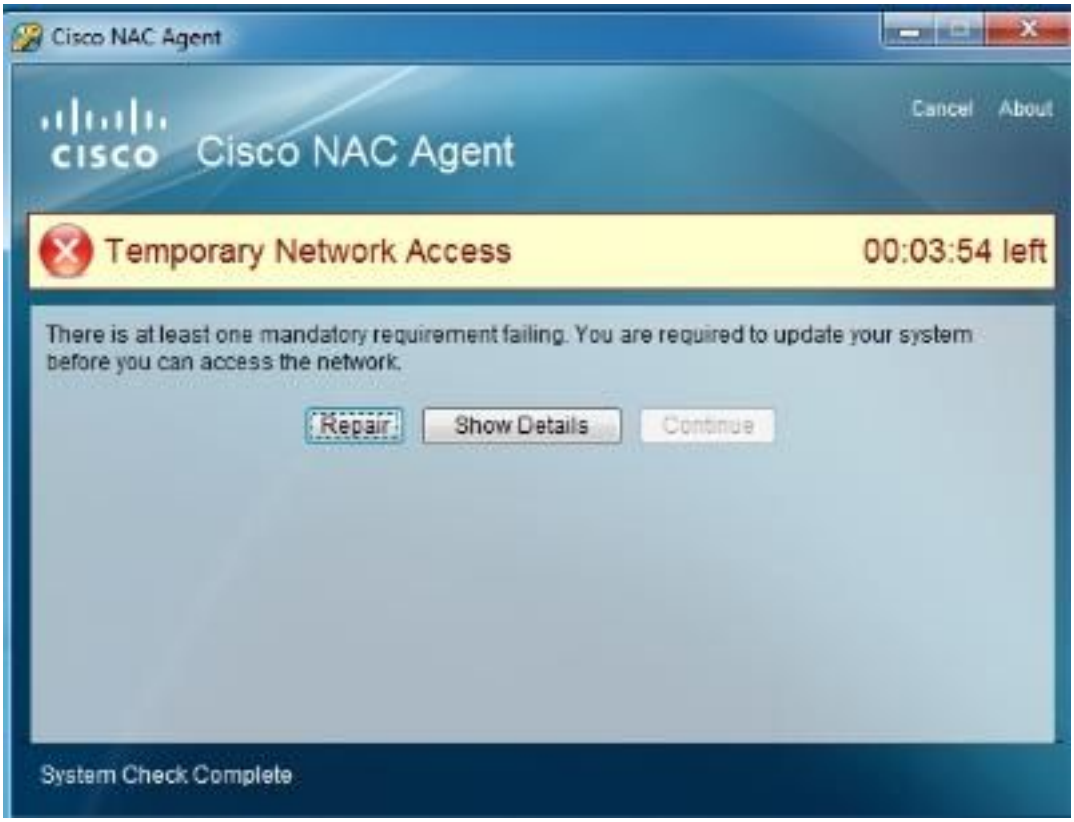
6. 点击**完整**，并且**其次**单击。

7. 单击 **Install**。

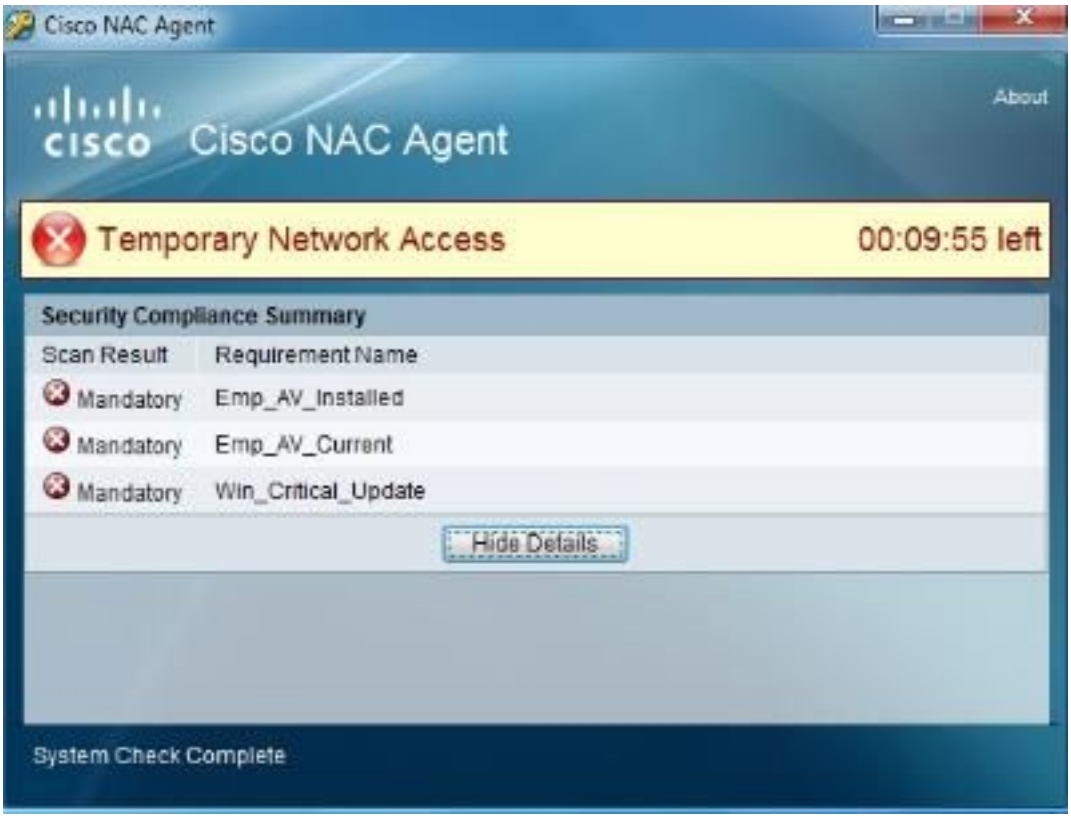
8. 选择**芬通社**。



9. 一旦安装完成，美洲台代理程序冒出。单击**显示详细信息**。



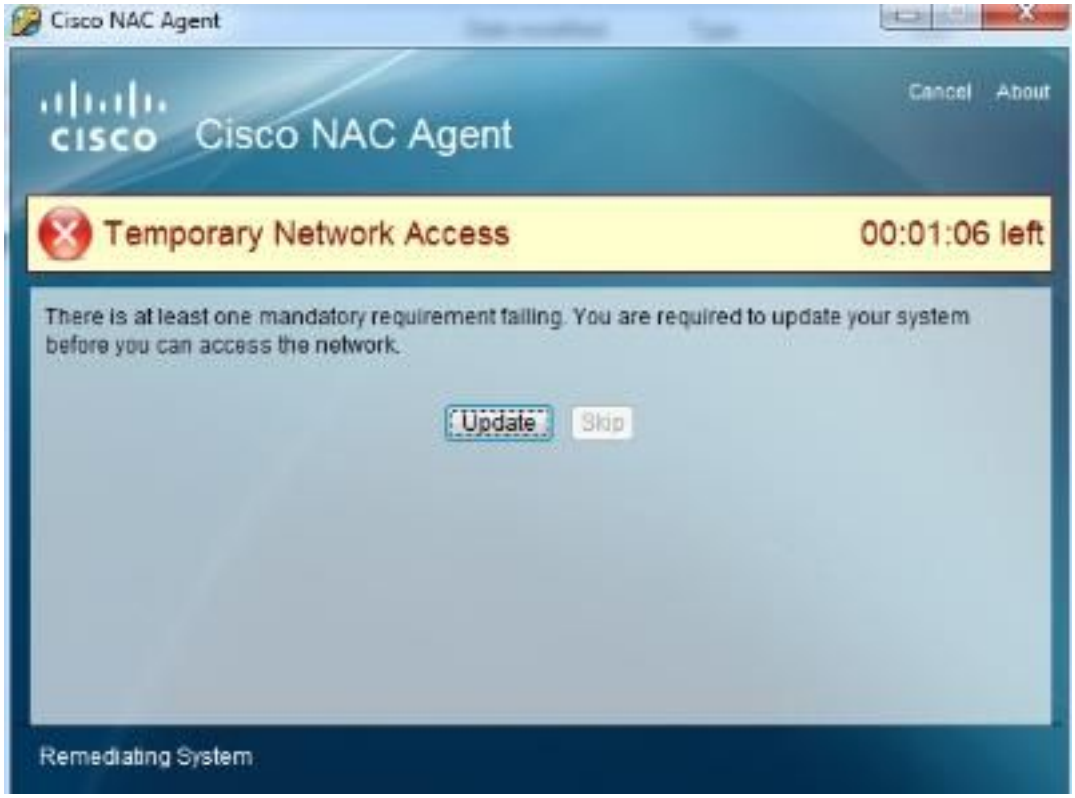
输出显示ClamWin没有安装和没有更新。一些Windows关键更新没有安装。



10. 单击**去林克**为了安装抗病毒从纠正服务器。

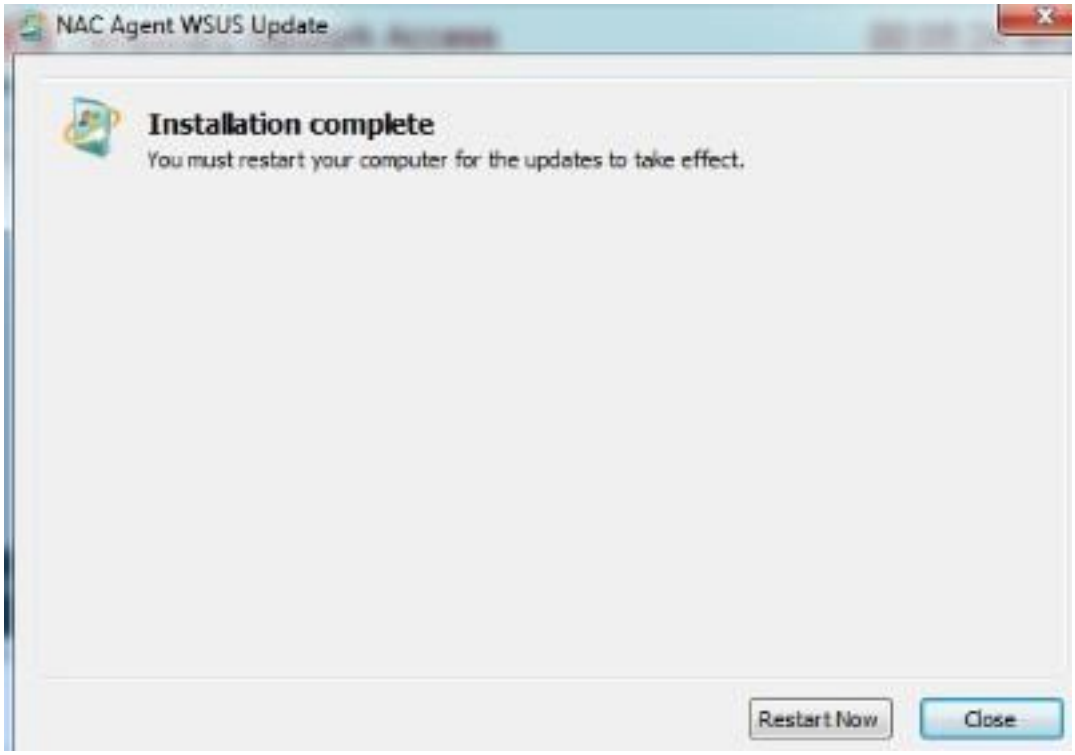
11. 点击**运行**，并且继续进行ClamWin AV安装。

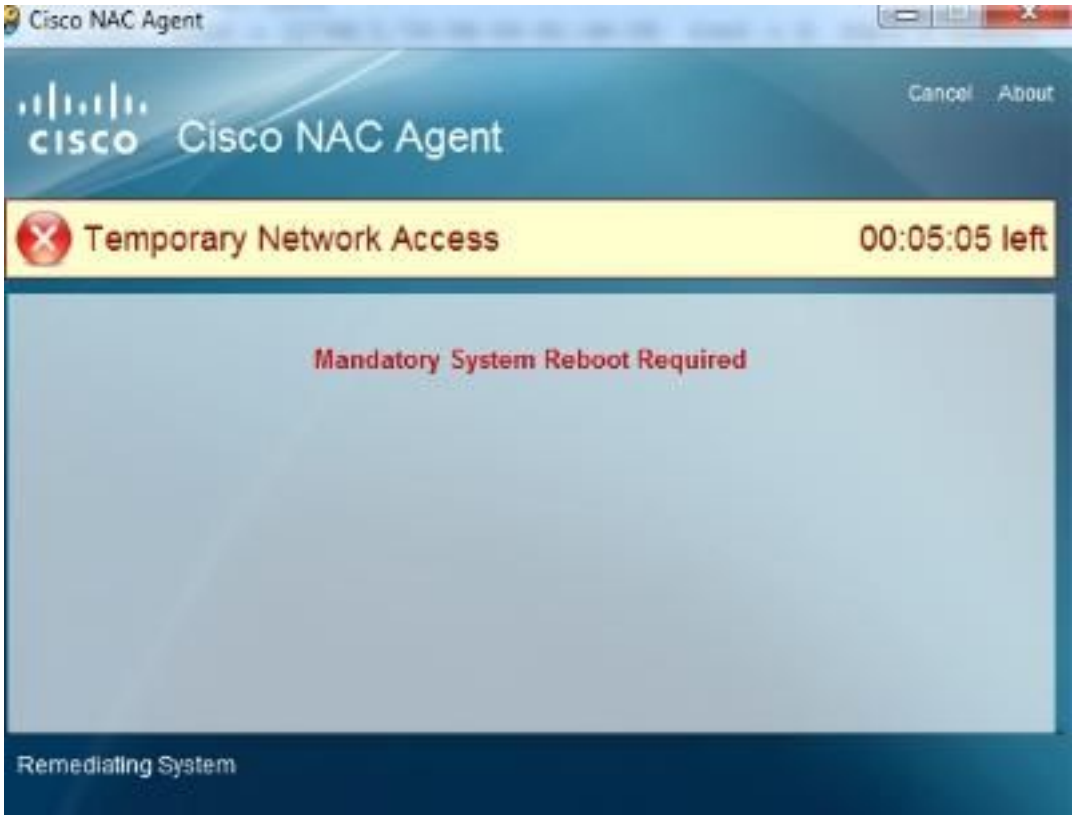
12. 在抗病毒安装后，美洲台代理程序提示输入更新。点击**更新**为了获得最新的病毒定义文件。当提交同样屏幕第二次时，再请单击**更新**为了安装Windows更新。



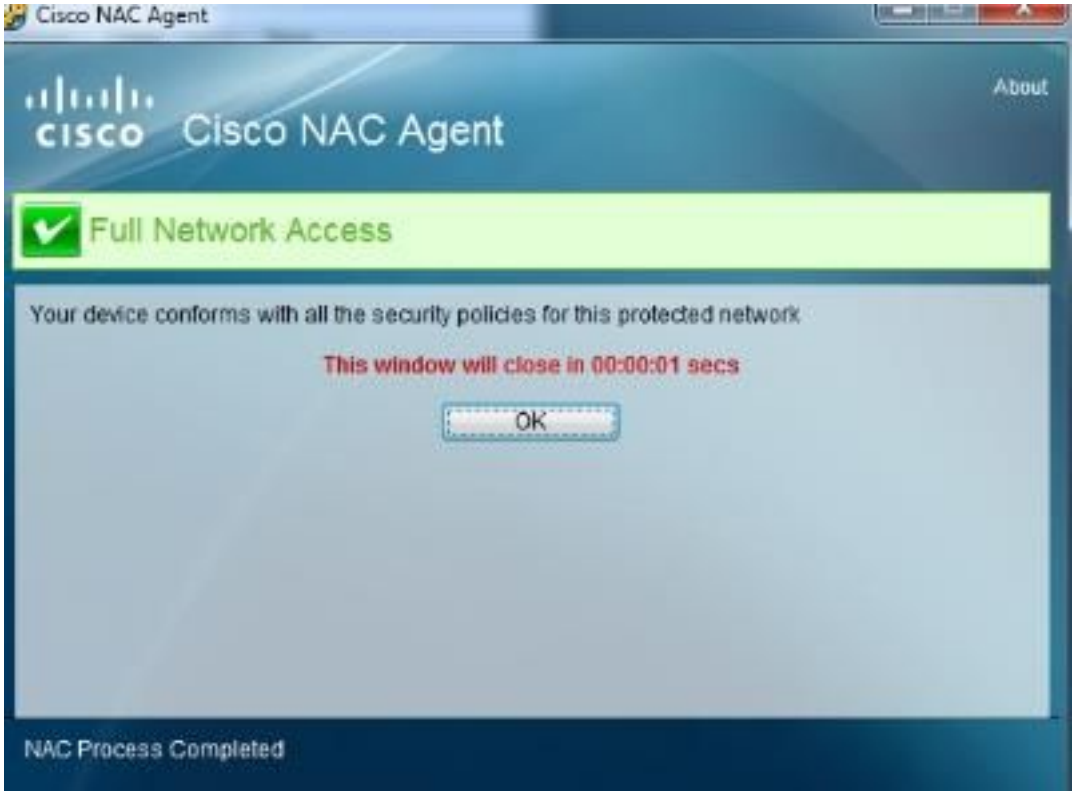
美洲台代理程序与您的WSUS联系为了检查和安装最新的关键更新。

13. **当前**单击**重新启动**为了完成更新。





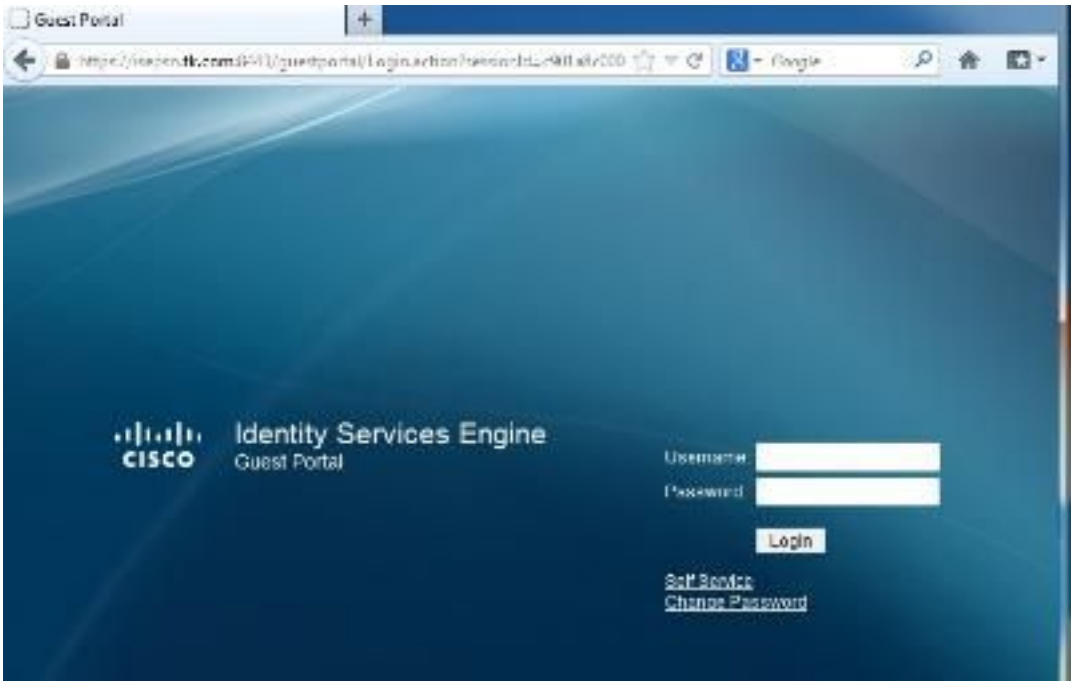
14. 在重新启动，系统是兼容的后。



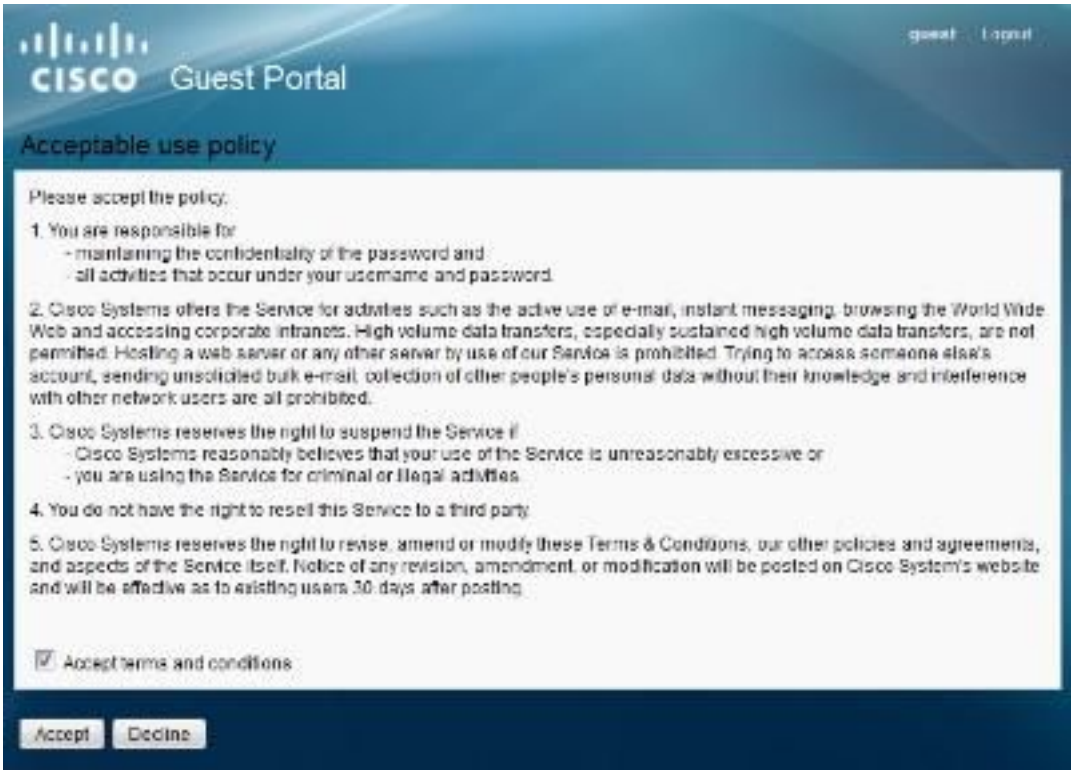
访客CWA状态(美洲台Web代理程序)

这是用户执行的步骤，一旦他们连接对与启用的状态的访客SSID。

1. 连接对您的访客SSID或者请勿配置在您的有线网络的dot1x。
2. 打开浏览器，并且设法导航到站点。
3. 浏览器重定向到访客门户。
4. 点击**赛弗注册**，并且继续进行验证。



5. 单击**接受**为了接受AUP。

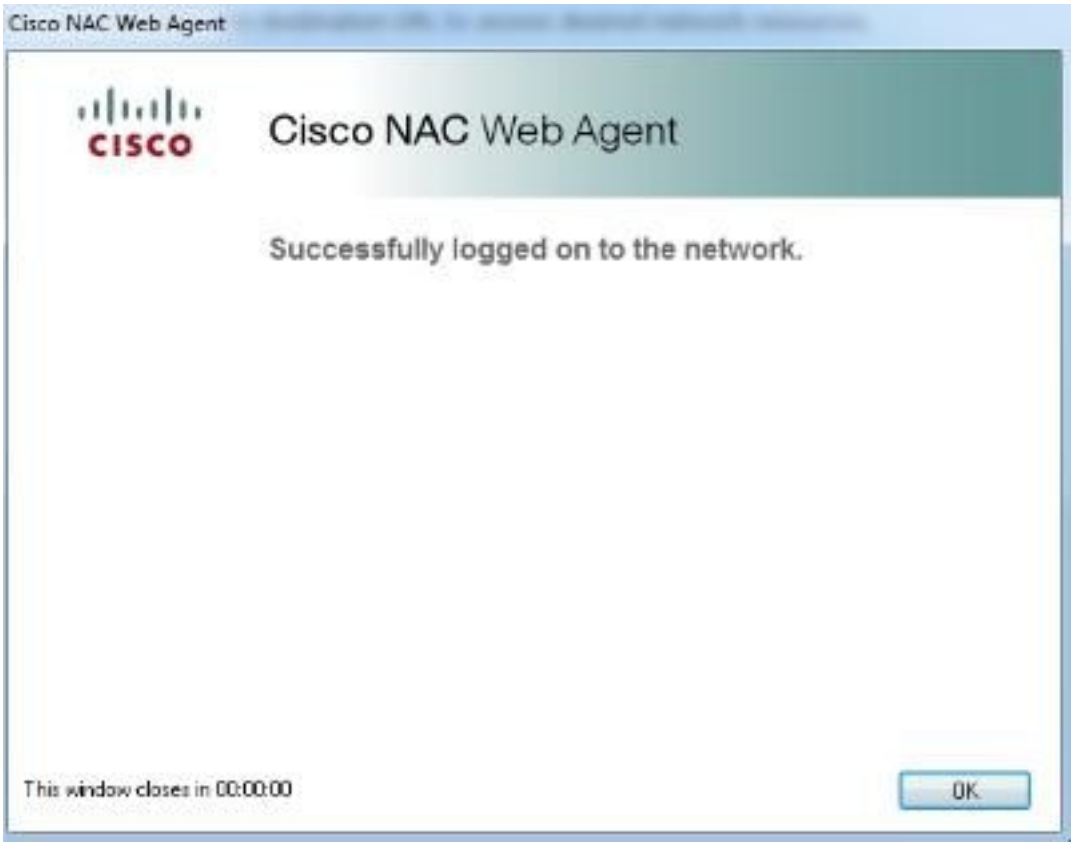


6. 选择**单击安装代理程序**。

7. 单击**点击此处对修正。**

8. 点击**运行**，并且继续进行抗病毒安装。

当前发现PC兼容的。



9. 检查ISE认证登录顺序验证动态授权成功，并且您匹配授权配置文件与兼容状态涉及。

常见问题

除客户端供应之外的部署选项

参考的思科身份服务引擎用户指南，版本1.1x ：设置的客户端机器用思科美洲台代理程序MSI安装程序。

美洲台代理程序的发现号主机

美洲台代理程序到达正确的ISE策略决定端(PDP)用不同的方式，根据是否发现主机定义：

1. 如果发现主机没有定义：美洲台代理程序发送在端口80的HTTP请求到网关;必须重定向此流量到状态发现链路(CPP)为了发现能适当地工作。
2. 如果发现主机定义：美洲台代理程序发送在端口80的HTTP请求到主机;必须重定向此流量到状态发现链路(CPP)为了发现能适当地工作。如果有与重定向的一问题，美洲台代理程序设法直接地与在端口定义的发现主机联系8905;状态验证没有保证，因为会话信息可能不取得到在那PDP，除非节点组定义，并且PDP在同一组内。
3. 如果发现主机不可能被到达，美洲台代理程序落回到方法1，如此设法用默认网关接触。

选择发现号主机，一个应该考虑到，从美洲台代理程序的最初的流量往发现号主机应该是可视对PDP。因此，好选择能是：PDP地址，在相同子网的不存在的主机作为PDP节点。

雇员浏览器配置与代理

1. 如果不使用客户端供应，并且雇员PCs配置与代理，没有更改的需要，因为状态发现信息包在端口80被发送并且绕过代理设置。
2. 如果使用客户端供应服务，请做这些变动对交换机配置和对WLC为了拦截在代理(此处8080的定义的端口的HTTP数据流在本例中)，如果代理不是在端口80。

    - 在端口8080的代理配置交换机的：

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab

switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
```

```
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

- 代理配置WLC。默认情况下， WLC截住HTTP请求用目的地TCP端口80仅。如果要拦截在端口8080的其他HTTP数据流必须通过命令行界面(CLI)配置此命令：

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

Note:交换机允许在一个端口的重定向。所以，如果指定交换机重定向的另一个端口，状态发现发生故障，并且状态流量发送到在NACAgentCFG.xml定义的发现主机(美洲台代理程序配置文件)。

dACL和重定向ACL

重定向ACL对于客户端供应、中央Web验证和状态发现号是必需的。然而， dACL用于为了限制网络访问和仅应用对不改道的流量。

为了解决此情况，您能：

1. 定义仅重定向ACL，并且重定向您要丢弃的所有流量(如执行在示例)。
2. 定义较不限制式的重定向ACL，并且应用过滤流量没有重定向的dACL。
3. 定义重定向ACL，并且应用限制网络访问的VLAN。因为VLAN流量可以由一意识到应用程序的防火墙，过滤这是最好的方法。

美洲台代理程序不冒出

1. 检查ISE实际验证，并且验证验证匹配您的状态授权配置文件。
2. 从客户端PC，请打开cmd。键入**nslookup**，并且验证您能解决ISE PDP主机名。
3. 从您的客户端浏览器，请键入**https:// ISE***主机名*：**8905/auth/discovery**，和确保您接收ISE FQDN作为答复。

如果所有这些步骤是成功的，并且，如果您的交换机或WLC配置遵守本文，您的以下步骤应该是：

- 请使用Wireshark为了开始在PC的一个捕获。
- 重新启动美洲台Agent服务。
- 收集思科日志包装工。
- 找出在美洲台代理程序目录的NACAgentCFG.xml。

一旦采集了数据包捕获、美洲台代理程序日志、NACAgentCFG配置文件和Windows事件查看器日

志，请与Cisco TAC联系。

无法访问修正的WSUS

如果使用WSUS 3.0 SP2，并且美洲台代理程序无法访问WSUS Windows更新，请验证您安排WSUS最新的补丁程序安装。此补丁程序对于Windows客户端是必需为了浏览从WSUS的更新。

验证您能访问此文件：**http://** *ip wsus* **/selfupdate/iuident.cab**。

参考Windows服务器更新服务3.0 SP2分步指南其他信息。

请勿有内部托管型WSUS

当您配置您的状态修正规则时，您能仍然使用Windows更新服务器。

客户端必须允许访问这些站点，因此不能重定向这些URL ：

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com
- http://stats.microsoft.com
- https://stats.microsoft.com

在ISE Live日志看到的没有失败的认证

您也许被诱惑创建授权策略规则在一个固执的客户端的情况的触发为了限制访问。然而，您看不到认证尝试发生故障，直到修正计时器超时，特别是当您使用Web代理程序。实际上，代理程序注意不顺从并且启动修正计时器。

ISE通知状态是失败，只有当修正计时器超时时或用户点击**取消**。所以，它是良好的做法提供允许修正对所有客户端的默认访问，但是阻塞访问其他表。

验证

一些验证程序在前面的部分包括。

故障排除

一些故障排除程序在前面的部分包括。