无线BYOD用身份服务引擎

目录

简介

思科身份服务引擎(ISE)是思科的下一代策略服务器该提供认证和授权基础设施对思科TrustSec解决方案。它也提供其他两关键服务：

- 第一服务将提供方式描出根据属性思科从多种信息源的ISE接收自动地的端点设备设备类型。此服务(呼叫Profiler)提供等同的功能给什么思科用Cisco NAC Profiler设备以前提供。
- 另一重要服务思科ISE提供是扫描终端标准;例如， AV/AS软件安装和其定义文件正确性(叫作状态)。思科以前仅提供此确切的状态功能Cisco NAC设备。

思科ISE提供一个等同的级别功能，并且用802.1X认证机制集成。

用无线局域网控制器集成的思科ISE (WLCs)能提供描出移动设备机制例如苹果公司iDevices (IP电话、iPad和iPod)，机器人根据智能电话和其他。对于802.1X用户，思科ISE能提供同样水平服务例如描出和摆扫描姿势。在思科ISE的访客服务可能也集成与思科WLC通过重定向对思科ISE的Web认证请求验证的。

本文引入Bring的无线解决方案您自己的设备(BYOD)，例如提供根据已知终端和用户策略的被区分的访问。本文不提供BYOD完整的解决方案，然而服务展示动态访问一简单用例。使用ISE赞助商门户，其他配置示例包括，特权用户能赞助设置的无线访客访问一访客。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有软件版本的7.2.103 Cisco无线LAN控制器2504或2106
- Catalyst 3560 – 8端口
- WLC 2504
- 身份服务引擎1.0MR (VMware服务器镜像版本)
- Windows 2008服务器(VMware镜像) — 512M， 20GB磁盘Active DirectoryDNSDHCP证书服务

拓扑

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

无线局域网控制器RADIUS美洲台和CoA概述

此设置使WLC寻找来自ISE RADIUS服务器的网域名称转址AV对。附加对与启用的RADIUS美洲台设置的一个接口的这仅在WLAN。当网域名称转址的Cisco AV对接收时，客户端被放到POSTURE_REQD状态。这基本上是相同的象WEBAUTH_REQD状态内部地控制器的。

当ISE RADIUS服务器视为时客户端是Posture_Compliant，它发出CoA ReAuth。Session_ID用于配合它。使用此新建的AuthC (再验证)它不发送URLRedirec AV对。由于没有URL重定向AV对，WLC知道客户端不需要其中任一更加长的状态。

如果RADIUS美洲台设置没有启用， WLC忽略URL重定向VSA'S。

CoaReAuth ：这启用与RFC 3576设置。ReAuth功能被添加了到以前支持的现有CoA命令。

RADIUS美洲台设置从此功能是互相排斥，虽然要求为了CoA能工作。

PRE状态ACL ：当客户端在POSTURE_REQ状态时， WLC的默认行为是阻塞除了DHCP/DNS的所有流量。(它在url-redirect-acl AV对呼叫)的PRE状态ACL应用给客户端，并且什么允许ACL是什么客户端能到达。

PRE验证ACL与VLAN覆盖：是与访问VLAN不同7.0MR1不支持的检疫或AuthC VLAN。如果设置从策略服务器的VLAN，它将是整个会话的VLAN。VLAN更改在第一AuthZ以后不是需要的。

无线局域网控制器RADIUS美洲台和CoA功能流

当客户端验证对后端服务器和美洲台状态验证时，消息的下面的图提供详细信息交换。

1. 使用dot1x验证，客户端验证。
2. RADIUS访问接受运载包括允许IP地址和端口的端口的80重定向的URL和PRE验证ACL，或者检疫VLAN。
3. 客户端将重定向对在访问提供的URL接受，并且放到新状态，直到状态验证完成。客户端在此状态与ISE服务器谈并且验证在ISE美洲台服务器配置的策略。
4. 在客户端的美洲台代理程序启动状态验证(对端口80)的流量：代理程序发送HTTP发现请求到控制器重定向对在访问提供的URL接受的端口80。ISE知道尝试的客户端到达并且响应直接地给客户端。客户端得知ISE服务器IP的这样，并且从现在起，客户端直接地与ISE服务器谈。
5. 因为ACL配置允许此流量， WLC允许此流量。在VLAN覆盖的情况下，流量桥接，以便到达ISE服务器。
6. 一旦ISE客户端完成评估，与reauth服务的一RADIUS CoA Req发送对WLC。这启动客户端的再验证(通过发送EAP-START)。一旦再验证成功， ISE发送访问接受与新的ACL (若有)和没有URL重定向或者访问VLAN。
7. WLC有CoA Req的支持和断开Req根据RFC 3576。WLC需要根据RFC 5176支持再验证服务的CoA Req。
8. 而不是可下载的ACLs，预先配置的ACL在WLC使用。ISE服务器发送ACL名称，在控制器已经配置。
9. 此设计应该为VLAN和ACL案件工作。在VLAN覆盖的情况下，我们重定向端口80重定向并且

允许(流量的网桥)其余在检疫VLAN的。对于ACL，在访问接收的PRE验证ACL接受应用。此图提供此功能流的一视觉表示：

描出概述的ISE

不管他们的设备类型，思科ISE仿形铣床服务在您的网络提供在发现，查找和确定所有附加的终端的功能的功能，为了保证和维护对您的企业网络的适当的访问。它主要收集属性或一套所有终端属性在您的网络的并且根据他们的配置文件分类他们。

仿形铣床包括这些组件：

- 传感器包含一定数量的探测器。探测器通过查询网络访问设备获取网络信息包，并且转发从终端收集到分析器的属性和他们的属性值。
- 分析器评估终端使用匹配属性和他们的属性值收集的已配置的策略和标识组，分类终端给指定的组并且存储与匹配的配置文件的终端在思科ISE数据库。

对于移动设备检测，它是推荐使用这些探测器的组合适当的设备标识：

- RADIUS (呼叫站点Id) ：提供MAC地址(OUI)
- DHCP (主机名) ：主机名-默认主机名能包括设备类型;例如：jsmithipad
- DNS (反向IP查找) ：FQDN -默认主机名能包括设备类型
- HTTP (用户代理) ：在特定移动设备设备类型的详细信息

在本例中iPad的，仿形铣床捕获从用户代理属性的Web浏览器信息，以及从请求消息的其他HTTP属性，并且添加他们到终端属性列表。

创建内部标识用户

MS激活目录(AD)没有为简单要求proof-of-concept。ISE可以使用作为唯一的标识存储，包括区分访问和精细的策略控制的用户访问。

在版本ISE 1.0，使用AD集成， ISE在授权策略能使用AD组。如果ISE使用内部用户存储(没有AD集成)，组不可能用于策略与设备标识组(在ISE将解决的已确定bug一道1.1)。所以，只有个人用户可以被区分，例如员工或承包商，当使用除设备标识组之外。

完成这些步骤：

1. 打开浏览器窗口对https://ISEip地址。
2. 导航对**Administration >身份管理>标识。**
3. 选择**用户**，然后单击**添加**(网络访问用户)。输入这些用户值并且分配到雇员组：名称：员工密码：
4. 单击 **submit**。名称：承包商密码：
5. 确认两个帐户创建。

添加无线局域网控制器到ISE

启动RADIUS请求对ISE的所有设备必须有在ISE的一个定义。这些网络设备根据他们的IP地址定义。ISE网络设备定义能指定因而允许定义的IP地址范围代表多个实际设备。

在什么之外为RADIUS通信要求， ISE网络设备定义包含其他ISE/device通信的设置，例如SNMP和

SSH。

网络设备定义的另一个重要方面适当地分组设备，以便分组的这在网络访问策略可以被有效利用。

在此练习，为您的实验室要求的设备定义配置。

完成这些步骤：

1. 从ISE请去**Administration >网络资源>网络设备**。
2. 从网络设备，请单击**添加**。输入IP地址，屏蔽检查验证设置，然后输入“cisco’共享机密的。
3. 保存WLC条目，并且确认在列表的控制器。

配置无线验证的ISE

ISE需要为验证802.1x无线客户端配置和使用活动目录作为标识存储。

完成这些步骤：

1. 从ISE请导航对**策略>验证**。
2. 单击展开Dot1x > Wired_802.1X (-)。
3. 点击**从库的**齿轮图标添加**条件**。
4. 从下拉式情况的选择，请选择**复合条件> Wireless_802.1X**。
5. 设置Express情况对**或**。
6. 展开以后允许协议选项，并且接受默认内部用户(默认)。
7. 留下一切别的东西在默认。点击**“Save”**完成步骤。

引导无线局域网控制器

连接对网络的WLC

Cisco2500无线局域网控制器部署指南也是可用的在Cisco 2500系列无线控制器部署指南。

配置使用启动向导的控制器

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
```

```
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

邻居交换机配置

控制器连接到相邻交换机的(快速以太网1)以太网端口。邻居交换机端口配置作为802.1Q中继并且允许在中继的所有VLAN。本地VLAN 10允许将连接的WLC的管理接口。

802.1Q交换机端口配置如下：

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

添加认证服务器(ISE)到WLC

ISE需要被添加到WLC为了启用802.1X和CoA功能无线终端的。

完成这些步骤：

1. 打开浏览器，然后连接对莢WLC (使用安全HTTP) > https://wlc。
2. 导航对**Security > Authentication >New**。
3. 输入这些值：服务器 IP 地址:10.10.10.70 (检查分配)共享密钥:ciscoRFC 3576的(CoA)支持：已启用(默认)一切别的东西：默认
4. 单击**应用**继续。
5. 选择**新建的RADIUS认为的> Add**。
6. 输入这些值：服务器 IP 地址:10.10.10.70共享密钥:cisco一切别的东西：默认
7. 单击**运用**，然后保存WLC的配置。

创建WLC雇员动态接口

完成这些步骤为了添加WLC的一个新的动态接口和映射它对员工VLAN ：

1. 从WLC，请导航对**Controller>接口**。然后单击 **New**。
2. 从WLC，请导航对**Controller>接口**。输入以下：接口名称：员工VLAN id ：11
3. 进入以下雇员接口的：端口号:1VLAN标识符：11IP 地址：10.10.11.5网络屏蔽：255.255.255.0网关：10.10.11.1DHCP ：10.10.10.10
4. 确认新的雇员动态接口创建。

创建WLC访客动态接口

完成这些步骤为了添加WLC的一个新的动态接口和映射它对访客VLAN ：

1. 从WLC，请导航对**Controller>接口**。然后单击 **New**。
2. 从WLC，请导航对**Controller>接口**。输入以下：接口名称：访客VLAN id ：12
3. 为访客接口进入这些：端口号:1VLAN标识符：12IP 地址：10.10.12.5网络屏蔽：255.255.255.0网关：10.10.12.1DHCP ：10.10.10.10
4. 确认访客接口被添加了。

添加802.1x WLAN

从WLC最初的启动，也许已经有创建的默认WLAN。如果那样，请修改它或创建一新的WLAN支持无线802.1X验证如指南所示。

完成这些步骤：

1. 从WLC，请导航对**WLAN >创建新**。
2. 对于WLAN，请输入以下：配置文件名称：pod1xSSID ：同样
3. 对于WLAN设置> General选项，请使用以下：收音策略：所有接口/组：管理一切别的东西：默认
4. 对于WLAN > Security选项卡> Layer2，设置以下：Layer2 Security:WPA+WPA2WPA2策略/加密：已启用/AES验证锁上Mgmt ：802.1X
5. 对于WLAN > Security选项卡>AAA服务器，设置以下：无线电服务器覆盖接口：已禁用验证/记帐服务器：已启用服务器 1：10.10.10.70
6. 对于WLAN >Advanced选项卡，设置以下：允许AAA覆盖：已启用美洲台状态：Radius美洲台(选择)
7. 回到WLAN > General选项>enable WLAN (复选框)。

测验WLC动态接口

您需要做有效雇员和访客接口的一次快速检查。请使用所有设备联合到WLAN，然后更改WLAN接口分配。

1. 从WLC，请导航对**WLAN > WLAN**。单击编辑在更早的练习创建的您的安全SSID。
2. 更改接口/接口组给**员工**，然后单击**应用**。
3. 若被设定适当地，设备收到从员工VLAN (10.10.11.0/24)的一个IP地址。此示例显示获得一个新的IP地址的IOS设备。
4. 一旦上一个接口被确认了，请更改WLAN接口分配给**访客**，然后单击**应用**。
5. 若被设定适当地，设备收到从访客VLAN (10.10.12.0/24)的一个IP地址。此示例显示获得一个新的IP地址的IOS设备。
6. **重要信息：**更改接口分配回到原始管理。
7. 单击**运用**并且保存WLC的配置。

iOS的(IP电话/iPad)无线验证

关联对WLC通过一已验证SSID内部用户(或集成的， AD用户)使用一个IOS设备例如IP电话、iPad或者iPod。跳到这些步骤，如果不可适用。

1. 在IOS设备上，请去WLAN设置。启用WIFI，然后选择在前面部分创建的802.1X启用的SSID。
2. 提供此信息为了连接：用户名：员工(内部–员工)或承包商(内部–承包商)密码：
3. 单击接受ISE证书。
4. 确认IOS设备从管理(VLAN10)接口获得IP地址。
5. 在WLC >监视器>客户端，请验证终端信息包括使用，陈述和EAP类型。
6. 同样地，客户端信息可以由ISE >监视器>验证页提供。
7. 点击**Details图标**为了操练下来对会话的详细信息的会话。

添加状态重定向ACL到WLC

状态重定向ACL在WLC配置， ISE将使用限制状态的客户端。有效地和在最低ACL允许ISE之间的流量。若需要可选规则在此ACL可以增加。

1. 导航到**WLC > Security >访问控制列出>访问控制列表**。单击 **New**。
2. 为ACL提供一名称(ACL-POSTURE-REDIRECT)。
3. 单击**添加**新的ACL的**新规则**。设置以下值为ACL顺序#1。单击**应用，**当完成。来源：任一目的地：IP地址10.10.10.70， 255.255.255.255协议：任一操作：Permit
4. 确认顺序被添加了。
5. 单击 **Add New Rule**。设置以下值为ACL顺序#2。单击**应用，**当完成。来源：IP地址10.10.10.70， 255.255.255.255目的地：任一协议：任一操作：Permit
6. 确认顺序被添加了。
7. 设置以下值为ACL顺序#3。单击**应用，**当完成。来源：任一目的地：任一协议：UDP源端口：DNS目的端口：任一操作：Permit
8. 确认顺序被添加了。
9. 单击 **Add New Rule**。设置以下值为ACL顺序#4。单击**应用，**当完成。来源：任一目的地：任一协议：UDP源端口：任一目的端口：DNS操作：Permit
10. 确认顺序被添加了。
11. 保存当前WLC配置。

启用描出在ISE的探测器

ISE需要配置作为探测器有效描出终端。默认情况下，这些选项禁用。此部分显示如何配置ISE是探测器。

1. 从ISE管理，请导航对**管理>System >部署**。
2. 选择**ISE**。单击**编辑ISE主机**。
3. 从Edit节点页，请选择配置文件配置并且配置以下：DHCP ：已启用，所有(或默认)DHCPSPAN ：已启用，所有(或默认)HTTP ：已启用，所有(或默认)RADIUS ：已启用，N/ADNS:已启用， N/A
4. 重新关联设备(IP电话/iPads/Droids/Mac等等)。
5. 确认ISE终端标识。导航对**Administration >身份管理>标识**。点击终端列出什么被描出了。**注意：** 初始描出是从RADIUS探测器。

Enable (event) ISE设备的配置文件策略

箱外， ISE提供多种终端配置文件库。完成这些步骤为了启用设备的配置文件：

1. 从ISE，请导航对**策略>描出**。
2. 从左窗格，请展开**描出策略**。
3. 点击**苹果公司设备>苹果公司iPad**，并且设置以下：启用的策略：已启用创建匹配标识组：选定
4. 点击**苹果公司设备>苹果公司IP电话**，设置以下：启用的策略：已启用创建匹配标识组：选定
5. 点击**机器人**，设置以下：启用的策略：已启用创建匹配标识组：选定

ISE状态发现号重定向的授权配置文件

完成这些步骤为了配置授权策略状态重定向允许将重定向的新的设备对适当发现和描出的ISE ：

1. 从ISE，请导航对**策略>Policy元素>结果**。
2. 展开**授权**。点击**授权配置文件**(左窗格)并且单击**添加**。
3. 创建与以下的授权配置文件：名称：Posture_Remediation访问类型：Access_Accept常用工具：状态发现号，启用状态发现号， ACL ACL-POSTURE-REDIRECT
4. 单击**提交**完成此任务。
5. 确认新的授权配置文件被添加。

创建ISE员工的授权配置文件

添加员工的一授权配置文件允许ISE授权和允许与已分配属性的访问。雇员VLAN11在这种情况下分配。

完成这些步骤：

1. 从ISE，请导航对**策略>结果**。展开**授权**，然后点击**授权配置文件**并且单击**添加**。
2. 进入以下雇员授权配置文件的：名称：Employee_Wireless普通的任务：VLAN，启用VLAN，sub值11
3. 单击**提交**完成此任务。
4. 确认新的雇员授权配置文件创建。

创建ISE承包商的授权配置文件

添加承包商的一授权配置文件允许ISE授权和允许与已分配属性的访问。承包商VLAN 12在这种情况下分配。

完成这些步骤：

1. 从ISE，请导航对**策略>结果**。展开**授权**，然后点击**授权配置文件**并且单击**添加**。
2. 进入以下雇员授权配置文件的：名称：Employee_Wireless普通的任务：VLAN，启用VLAN，sub值12
3. 单击**提交**完成此任务。
4. 确认承包商授权配置文件创建。

描出设备的状态的/授权策略

一点信息知道关于新设备，当首先来在网络上时，管理员将创建相应的策略允许在允许访问前将识别的未知终端。在此练习，授权策略将创建，以便新设备将重定向对状态评估的ISE (对于移动设备agentless，因此只描出是相关的);终端将重定向对ISE俘虏门户和已确定。

完成这些步骤：

1. 从ISE，请导航对**策略>授权**。
2. 有Profiled思科IP电话的一项策略。这是箱外。编辑此作为状态策略。
3. 输入此策略的以下值：规则名称：Posture_Remediation标识组：任一其他情况>创建新：(先进的)会话> PostureStatusPostureStatus >等于：未知
4. 设置以下权限的：权限>英文虎报：Posture_Remediation
5. 单击 **Save**。**注意：** 二者择一海关政策元素可以是创建的添加易用。

测试状态修正策略

对简单演示可执行显示ISE适当地描出根据状态策略的新设备。

1. 从ISE，请导航对**Administration >身份管理>标识**。
2. 点击**终端**。关联并且连接设备(在本例中的一个IP电话)。
3. 刷新终端列表。观察什么信息给。
4. 从端点设备，请浏览对：URL ：http://www (或10.10.10.10)设备重定向。接受所有提示输入证书。
5. 在移动设备完全重定向后，从ISE刷新终端再列出。观察什么更改。上一个终端(例如，苹果公司设备)应该更改到“苹果公司iPhone'etc。原因是HTTP探测器有效得到用户代理信息，作为进程重定向一部分到俘虏门户。

被区分的访问的授权策略

在成功的测试状态授权，继续建立策略支持员工和承包商的被区分的访问用已知设备和对用户角色后的另外VLAN分配特定(在此方案、员工和承包商)。

完成这些步骤：

1. 导航对**ISE >Policy >授权**。
2. 添加/插入在状态修正策略/线路上的一新规则。
3. 输入此策略的以下值：规则名称：员工标识组(请展开) ：终端标识组终端标识组：描出描出：机器人、苹果公司iPad或者苹果公司IP电话
4. 为了指定附加设备类型，请点击+并且添加更多设备(若需要) ：终端标识组：描出描出：机器人、苹果公司iPad或者苹果公司IP电话
5. 指定此策略的以下权限的值：其他情况(请展开) ：创造新的条件(Advanced选项)情况>表达式(从列表) ：InternalUser >名称InternalUser >名称：员工
6. 添加兼容状态的会话的一个条件：权限> Profiles>英文虎报：Employee_Wireless
7. 单击 **Save**。确认策略适当地被添加了。
8. 通过添加承包商策略继续。在本文中，上一个策略被复制为了加快进程(或，您能为良好的做法手工配置)。从雇员策略>操作，请点击**下面重复项**。
9. 编辑此策略的(备份)以下字段：规则名称：承包商其他情况> InternalUser >名称：承包商权限：Contractor_Wireless
10. 单击 **Save**。确认上一个备份(或新建的策略)适当地配置。

11. 为了预览策略，请点击策略在**扫视**。策略一览查看统一的提供汇总和容易发现策略。

测试CoA被区分的访问的

当为区分访问和策略准备的授权配置文件，是时间测试。有单个获取的WLAN，员工将分配员工VLAN，并且承包商将是为承包商VLAN。苹果公司IP电话/iPad用于以下的示例。

完成这些步骤：

1. 连接对获取的WLAN (POD1x)用移动设备并且请使用这些凭证：用户名：员工密码：
2. 点击**加入**。确认员工是分配的VLAN 11 (员工VLAN)。
3. 单击**忘记此网络**。确认通过单击**忘记**。
4. (如果同样用于上一个步骤)，请去WLC并且取消现有客户端连接。导航对**监视器>客户端> MAC地址**，然后点击**删除**。
5. 另一个可靠方法清除上次客户端会话将禁用/enable (event) WLAN。去**WLC > WLAN > WLAN**，然后点击WLAN编辑。不选定**已启用>应用**(禁用)。检查方框**已启用>应用**(重新启用)。
6. 去上一步移动设备。再连接对与这些凭证的同样WLAN ：用户名：承包商密码：
7. 点击**加入**。确认承包商用户是分配的VLAN 12 (承包商/访客VLAN)。
8. 您能查看在**ISE >监视器>授权的**ISE实时日志视图。您应该看到个人用户(员工，承包商)获得被区分的授权配置文件(Employee_WirelessvsContractor_Wireless)用不同的VLAN。

WLC访客WLAN

完成这些步骤为了添加访客WLAN允许访客访问ISE赞助商访客门户：

1. 从WLC，请导航对**新建的WLAN > WLAN >Add**。
2. 进入以下新的访客WLAN的：配置文件名称：pod1guestSSID ：pod1guest
3. 单击 **Apply**。
4. 进入以下在访客WLAN > General选项下：状态：已禁用接口/接口组：访客
5. 导航对访客**WLAN > Security > Layer2**并且输入以下：第 2 层安全：无
6. 导航对访客**WLAN > Security >第3层**选项卡并且输入以下：第3层安全：无Web策略：已启用Web策略sub值：验证预先身份验证ACL ：ACL-POSTURE-REDIRECTWeb认证类型：外部(请重定向到外部服务器)URL ：https://10.10.10.70:8443/guestportal/Login.action
7. 单击 **Apply**。
8. 确保**保存WLC配置**。

测试访客WLAN和访客门户

现在，您能测试访客WLAN的配置。它应该重定向访客到ISE访客门户。

完成这些步骤：

1. 从一个IOS设备例如IP电话，请导航对**wi-fi网络>enable**。然后，请选择Pod访客网络。
2. 您的IOS设备应该显示从访客VLAN (10.10.12.0/24)的一个有效IP地址。
3. 打开Safari浏览器并且连接对：URL ：http://10.10.10.10Web验证重定向出现。
4. 请单击**继续，**直到您到达在ISE访客入口页面。下张示例屏幕画面显示在访客门户洛金的

IOS设备。这确认WLAN和ISE访客的正确设置门户是活跃的。

ISE无线赞助了访客访问

ISE可以配置允许访客将被赞助。在这种情况下您将配置ISE访客策略允许赞助访客访问的内部或AD域(如果集成)用户。您也将配置ISE允许赞助商查看访客密码(可选)，是有用对此实验室。

完成这些步骤：

1. 添加雇员用户到SponsorAllAccount组。有不同的方式执行此：去直接地组或者编辑用户并且分配组。对于此示例，请导航给**Administration >身份管理> Groups >用户标识组**。然后，请点击**SponsorAllAccount**并且添加雇员用户。
2. 导航给**Administration >访客Management>赞助商组**。
3. 单击**编辑**，然后选择**SponsorAllAccounts**。
4. 选择授权级别并且设置以下：查看访客密码：是
5. 点击**"Save"**为了完成此任务。

赞助的访客

以前，您配置适合的访客策略和组允许AD域用户赞助临时访客。其次，您将访问门户的赞助商并且创建一临时访客访问。

完成这些步骤：

1. 从浏览器，请导航对这些URL之一：http:// <ise ip>:8080/sponsorportal/**或**https:// <ise ip>:8443/sponsorportal/。然后，与以下的登录：用户名：aduser (活动目录)，员工(内部用户)密码：
2. 从赞助商页，请单击**创建单个来宾用户用户帐号**。
3. 对于一临时访客，请添加以下：名字:需要的(例如，山姆)姓氏:需要的(例如， Jones)组角色：访客时间配置文件：DefaultOneHour时间区域：其中任一/默认
4. 单击 **submit**。
5. 访客帐户根据您的上一个条目创建。注意密码是可视(从上一个练习)与哈希***相对。
6. 打开此窗口显示访客的用户名和密码。您将使用他们测试访客门户洛金(其次)。

测试访客门户访问

当新的访客帐户创建由AD用户/赞助商，是时间测试访客门户和访问。

完成这些步骤：

1. 在首选的设备(在这种情况下苹果公司iOS/iPad)上，请连接对荚访客SSID并且检查IP地址/connectivity。
2. 请使用浏览器并且尝试导航到http://www。您重定向对访客门户登录页。
3. 使用访客帐户的洛金创建在上一个练习。如果成功，可接受的使用规定页出版。
4. 检查**接受条款和条件**，然后单击**接受**。原始URL完成，并且终端是允许的访问作为访客。

身份验证配置

为了与ISE的安全通信，确定通信是否是涉及的验证或为ISE管理。例如，对于配置使用ISE Web UI， X.509证书和证书信任一系列需要配置启用非对称加密。

完成这些步骤：

1. 从您的有线的已连接PC，请打开浏览器窗口对https://AD/certsrv。**注意：** 请使用安全HTTP。**注意：** 用Mozilla Firefox或MS Internet Explorer为了访问ISE。
2. 登陆作为administrator/Cisco123。
3. 单击 **Download a CA certificate, certificate chain, or CRL**。
4. 点击**下载CA证书**并且保存它(请注释保存位置)。
5. 打开浏览器窗口对https:// <Pod-ISE>。
6. 去**管理>System >证书>证书权限证书**。
7. 选择**认证机关证书**操作并且浏览对以前下载的CA cert。
8. 选择**客户端的托拉斯有EAP-TLS的**，然后提交。
9. 确认CA是被添加的委托作为根CA。
10. 从浏览器，请去**管理>System >证书>证书权限证书**。
11. 单击**添加**，然后**生成证书签名请求**。
12. 提交这些值：证书主题：CN=ise.corp.rf-demo.com密钥长度：2048
13. ISE提示符CSR是可用的在CSR页。单击 **Ok**。
14. 选择从ISE CSR页的CSR并且点击**出口**。
15. 保存文件到所有位置(例如，下载等等)
16. 文件将保存作为*.pem。
17. 寻找CSR文件并且编辑与任一Notepad/Wordpad/TextEdit。
18. 复制内容(挑选all>复制)。
19. 打开浏览器窗口对https:// <Pod-AD>/certsrv。
20. 点击**请求证书**。
21. 单击以提交**高级证书申请**。
22. 在保存的请求字段粘贴CSR内容。
23. 选择**Web服务器**作为认证模板，然后单击**提交**。
24. 选择**编码的DER**，然后点击**下载证书**。
25. 保存文件到已知位置(例如，下载)
26. 去**管理>System >证书>证书权限证书**。
27. 点击**Add>捆绑CA证书**。
28. 浏览对以前下载的CA证书。
29. 选择**协议EAP**和**管理接口**，然后单击**提交**。
30. 确认CA是被添加的委托作为根CA。

Windows 2008年激活目录集中

ISE能直接地与激活目录(AD)联络用户/计算机验证的或获取的验证信息用户属性。为了通信与AD，必须“加入ISE’到AD域。在此练习您将加入ISE对AD域，并且确认AD通信正确地工作。

完成这些步骤：

1. 为了加入ISE对AD域，从ISE去**Administration >身份管理>外部标识来源**。
2. 从左窗格(外部标识来源)，请选择**活动目录**。
3. 在右边，请选择**Connection选项**并且输入以下：域名：corp.rf-demo.com标识存储名称：AD1
4. 点击**测试连接**。输入AD用户名(aduser/Cisco123)，然后点击OK键。

5. 确认测试状态显示**成功的测验**。
6. 选择显示详细日志并且对排除故障观察有用的详细信息。单击 **OK** 继续。
7. 点击**保存配置**。
8. 点击**加入**。输入AD用户(administrator/Cisco123)，然后点击OK键。
9. 确认加入操作状态显示**成功**，然后点击OK键继续。服务器连接状态显示**已连接**。如果此在任何时间状态变化，测试连接将帮助排除故障与AD操作的问题。

添加活动目录组

当AD组被添加时，更加粒状的控制允许对ISE策略。例如， AD组可以由功能角色区分，例如雇员或承包小组，不用体验的相关bug在上一个ISE策略对用户仅被限制的1.0练习。

在此实验室，使用域用户和仅雇员组。

完成这些步骤：

1. 从ISE，去**Administration >身份管理>外部标识来源**。
2. 选择**活动目录> Groups**选项卡。
3. 点击**+Add**，然后**选择组从目录**。
4. 在继续采取的行动窗口(请选择目录组)，请接受域的(公司RFdemo.com)默认并且过滤(*)。然后，请点击RetrieveGroups。
5. 选择**域用户**和**雇员**组的方框。完成后单击 **OK**。
6. 确认组被添加了到列表。

添加标识来源顺序

默认情况下， ISE设置使用内部用户验证存储。如果AD被添加，顺序优先级顺序可以创建包括ISE将使用检查验证的AD。

完成这些步骤：

1. 从ISE，请导航对**Administration >身份管理>标识来源顺序**。
2. 点击**+Add**为了添加一个新的顺序。
3. 输入新名字：**AD_Internal**。添加所有可用的来源到选定字段。然后，请重新命令，当需要，以便AD1被搬到列表的顶部。单击 **submit**。
4. 确认顺序被添加了到列表。

ISE无线赞助了与集成AD的访客访问

ISE可以配置允许将赞助的访客与策略为了允许AD域用户赞助访客访问。

完成这些步骤：

1. 从ISE，请导航对**Administration >访客Management>设置**。
2. 展开**赞助商**，并且点击**验证来源**。然后，请选择**AD_Internal，**标识存储顺序。
3. 确认AD_Internal，标识存储顺序。单击 **Save**。
4. 导航对**Administration >访客Management>赞助商组策略**。

5. 插入在第一个规则上的新的策略(请点击从权利的**操作**图标)。
6. 对于新的赞助商组策略，请创建以下：规则名称：域用户标识组：任一其他情况：(请创建新的/Advanced) > AD1AD1 ：外部组AD1外部组>等于> corp.rf-demo.com/Users/Domain用户
7. 在赞助商组中，设置以下：赞助商组：SponsorAllAccounts
8. 导航给**Administration >访客Management>赞助商组**。
9. 选择编辑> **SponsorAllAccounts**。
10. 选择授权级别并且设置以下：查看访客密码：是

配置在交换机的SPAN

配置SPAN - ISE mgt/探测器接口是L2在WLC管理接口附近。交换机可以配置到SPAN和其他接口，例如雇员和访客接口VLAN。

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

参考：苹果公司MAC OS X的无线验证

WLC的关联通过一已验证SSID作为一个内部用户(或集成的， AD用户)使用苹果公司Mac OS X无线笔记本电脑。跳过，如果不可适用。

1. 在Mac，请去WLAN设置。启用WIFI，然后选择并且连接对802.1X启用的Pod在上一个练习创建的SSID。
2. 提供以下信息连接：用户名：aduser (如果曾经AD)，员工(内部–员工)，内部的承包商(–承包商)密码：802.1X ：自动TLS证书：无此时，笔记本电脑也许不连接。另外， ISE能投掷一个失败的事件如下：`Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain`
3. 去设置**系统首选>网络>机场>的802.1X**并且设置新的Pod SSID/WPA配置文件验证如下：TLS ：已禁用PEAP ：已启用TTL ：已禁用EAP-FAST ：已禁用
4. 点击OK键继续和允许将保存的设置。
5. 在网络屏幕，请选择适当的SSID + 802.1X WPA配置文件并且点击**连接**。
6. 系统也许为用户名和密码提示。输入AD用户和密码()，然后点击OK键。客户端应该通过与有效IP地址的PEAP显示**已连接**。

参考：Microsoft Windows XP的无线验证

WLC的关联通过一已验证SSID作为一个内部用户(或集成的， AD用户)使用Windows XP无线笔记本电脑。跳过，如果不可适用。

完成这些步骤：

1. 在笔记本电脑，请去WLAN设置。启用WIFI并且连接对802.1X启用的Pod在上一个练习创建的SSID。
2. 访问WIFI接口的网络属性。
3. 导航对**Wireless Networks选项**。选择荚SSID网络属性> Authentication选项> EAP type= Protected EAP (PEAP)。
4. 点击EAP属性。
5. 设置以下：验证服务器证书：已禁用认证方法：获取的密码(EAP-MSCHAP v2)

6. 点击OK键在所有windows的完成此配置任务。
7. Windows XP客户端提示输入用户名和密码。在本例中，它是。
8. 确认网络连通性， IP寻址(v4)。

参考：Microsoft Windows的7无线验证

WLC的关联通过一已验证SSID作为一个内部用户(或集成的， AD用户)使用Windows 7无线笔记本电脑。

1. 在笔记本电脑，请去WLAN设置。启用WIFI并且连接对802.1X启用的Pod在上一个练习创建的SSID。
2. 访问无线管理器并且编辑新的Pod无线配置文件。
3. 设置以下：认证方法：PEAP切记我的凭证… ：已禁用验证服务器证书(高级设置) ：已禁用认证方法(副词。设置) ：EAP-MSCHAP v2请自动地请使用我的Windows登录… ：已禁用

相关信息

- 技术支持和文档 - Cisco Systems