FlexConnect部署指南的无线BYOD

目录

简介

移动设备更加计算上变为强大和受欢迎在消费者中。数百万这些设备被出售给有高速的消费者wi-fi，因此用户能通信和协作。消费者当前习惯这些移动设备带领进入他们的寿命的生产率增强和寻求带领他们的个人经验进入工作区。这在工作场所创建带来的功能需要您自己的设备(BYOD)解决方案。

本文为BYOD解决方案提供分组部署。员工连接对与新的iPad的一公司服务集标识(SSID)并且重新定向到赛弗注册门户。思科身份服务引擎(ISE)利用公司激活目录(AD)验证用户并且与强制执行使用扩展验证传输层安全的请求方配置文件一起下载与一嵌入式iPad MAC地址和用户名的一证书对iPad，(EAP-TLS)作为dot1x连接的一个方法。基于在ISE的授权策略，用户能然后连接使用dot1x和获得访问合适资源。

在Cisco无线LAN控制器软件版本的ISE功能早于7.2.110.0不支持通过FlexConnect接入点的本地交换客户端(AP)联合。发布7.2.110.0支持FlexConnect的AP这些ISE功能本地交换和在中央验证的客户端的。此外，请发布7.2.110.0集成与ISE 1.1.1提供(但是没有被限制对)无线的这些BYOD解决方案功能：

- 设备描出和状态
- 设备已注册和请求方设置
- Onboarding个人设备(提供iOS或机器人设备)

Note:虽然支持，其它设备，例如PC或Mac无线膝上型计算机和工作站，在此指南没有包括。

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：

- 思科Catalyst交换
- Cisco无线LAN (WLAN)控制器
- Cisco WLAN控制器(WLC)软件版本7.2.110.0和以后
- 在FlexConnect模式的802.11n AP
- Cisco ISE软件版本1.1.1和以上
- 与Certificate Authority (CA)的Windows 2008 AD
- DHCP 服务器
- 域名系统 (DNS) 服务器
- 网络时间协议 (NTP)
- 无线客户端笔记本电脑、智能手机和片剂(苹果公司iOS、机器人、Windows和Mac)

Note:Cisco无线LAN控制器和轻量级接入点的参考的版本注释重要信息的版本的7.2.110.0关于此软件版本。Cisco.com站点的洛金新版本笔记的，在您装载和测试软件前。

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。

拓扑

一最小网络设置，如此图表所显示要求为了正确实现和测试这些功能：

对于此仿真，您需要与FlexConnect AP，一本地/远程站点有本地DHCP的， DNS、WLC和ISE的网络。FlexConnect AP连接到中继为了测试与多个VLAN的本地交换。

设备已注册和请求方设置

必须注册设备，以便其本地请求方能已配置为dot1x验证。凭正确的验证策略，用户重定向对guest页和已验证由雇员凭证。用户看到设备已注册页，请求他们的设备信息。设备提供的流程然后开始。如果操作系统(OS)不为设置支持，用户重定向到资产注册门户为了标记MAC验证旁路(MAB)访问的设备。如果支持OS，登记进程开始并且配置设备的本地请求方dot1x验证的。

资产注册门户

资产注册门户是允许员工通过验证和注册过程启动onboarding终端ISE平台的元素。

管理员能删除从终端身份页的资产。每名员工能编辑，删除和列入黑名单他们注册的资产。列入黑名单的终端分配到黑名单标识组，并且授权策略由列入黑名单的终端创建为了防止网络访问。

赛弗注册门户

在中央Web验证(CWA)流，员工重定向到给他们输入他们的凭证，验证和输入特定的资产特定他们希望注册的门户。此门户呼叫设置门户的赛弗并且类似于设备已注册门户。它允许员工进入MAC地址以及终端的一有意义的escription。

验证和供应

一旦员工选择赛弗注册门户，他们挑战提供一套有效雇员凭证为了继续到供应相位。在成功认证以后，终端可以设置到终端数据库，并且证书为终端生成。在页的一条链路允许员工下载请求方试验向导(SPW)。

> **Note**:参考FlexConnect功能一览表Cisco条款为了查看BYOD的最新的FlexConnect功能一览表。

设置iOS的(IP电话/iPad/iPod)

对于EAP-TLS配置， ISE按照苹果公司通过空气(OTA)登记进程：

- 在成功认证以后，评估引擎评估客户端供应策略，导致请求方配置文件。
- 如果请求方配置文件是为EAP-TLS设置， OTA进程确定ISE是否是未知CA自已签署的或签字的使用。如果其中一个条件是真的，用户询问下载ISE或CA证书，在登记进程能开始前。
- 对于其他EAP方法， ISE推送最终配置文件在成功认证。

设置机器人的

由于安全考虑，必须从机器人市场站点下载机器人代理程序，并且不可能从ISE设置。思科上传向导的版本候选版本到机器人市场通过思科机器人市场发行商帐户。

这是机器人提供的流程：

1. 思科使用软件开发工具(SDK)为了创建有.apk分机的机器人包。
2. 思科上传包到机器人市场。
3. 用户配置在客户端供应的策略与适当的参数。
4. 在设备的注册以后，当dot1x验证发生故障时，最终用户重定向对客户端供应服务。
5. 供应入口页面提供重定向用户到机器人市场门户他们能下载SPW的一个按钮。
6. 思科SPW启动并且执行请求方的供应： SPW发现ISE并且下载从ISE的配置文件。SPW创建cert/密钥对EAP-TLS的。SPW做简单认证登记协议(SCEP)代理请求呼叫对ISE并且获得证书。SPW应用无线配置文件。如果配置文件顺利地，应用SPW触发再验证。SPW退出。

双重SSID无线BYOD赛弗注册

这是双重SSID无线BYOD赛弗注册的进程：

1. 访客SSID的用户关联。
2. 用户打开浏览器和重定向到ISE CWA访客门户。
3. 用户在访客门户输入一个雇员用户名和密码。
4. ISE根据事实验证用户，和，他们是员工而不是访客，重定向用户对guest页雇员的设备已注册。
5. MAC地址在设备已注册被事前填充guest页为DeviceId。用户输入说明并且如果必须接受Acceptable Use Policy (AUP)。
6. 用户选择**接受**并且开始下载和安装SPW。
7. 该用户设备的请求方与所有证书一起设置。
8. CoA发生，并且设备重新关联对公司SSID (公司)并且验证与EAP-TLS (或其他授权方法在使用中该请求方的)。

单个SSID无线BYOD赛弗注册

在此方案中， Protected Extensible Authentication Protocol (PEAP)有公司接入的(公司)单个SSID该支持和EAP-TLS。没有访客SSID。

这是单个SSID无线BYOD赛弗注册的进程：

1. 公司的用户关联。
2. 用户输入雇员用户名和密码到PEAP验证的请求方。
3. ISE根据PEAP方法验证用户，并且，提供授权策略接受与重定向对guest页雇员的设备已注册。
4. 用户打开浏览器和重定向对guest页雇员的设备已注册。
5. MAC地址在设备已注册被事前填充guest页为DeviceId。用户输入说明并且接受AUP。
6. 用户选择**接受**并且开始下载和安装SPW。
7. 该用户设备的请求方与所有证书一起设置。
8. CoA发生，并且设备重新关联对公司SSID并且验证与EAP-TLS。

功能配置

完成这些步骤为了开始配置：

1. 对于此指南，请保证WLC版本是7.2.110.0或以后。

2. 导航对**Security>RADIUS >验证**，并且添加RADIUS服务器到WLC。

3. 添加ISE 1.1.1到WLC ：

   输入共享塞克雷。设置RFC 3576的支持对**已启用**。

4. 添加ISE服务器和RADIUS记帐服务器一样。

5. 创建WLC PRE验证ACL使用在后ISE的策略。导航到**WLC** > Security **>访问控制列出> FlexConnect ACL**，并且创建名为**ACL-REDIRECT的**新的FlexConnect ACL (在本例中)。

6. 在请求方设置期间，在ACL规则，请允许到/从ISE的所有流量，并且允许客户端的流量。

   第一个规则(顺序1) ：

   对其中**任一的**集合来源。设置IP (ISE地址)/网络屏蔽**255.255.255.255**。设置操作**允许**。

   为第二规则(顺序2)，设置来源IP (ISE地址)/对其中**任一的**掩码255.255.255.255和操作**允许**。

7. 创建名为Flex1的一新的FlexConnect组(在本例中) ：

   导航对**FlexConnect组> WebPolicies**选项卡。在WebPolicy ACL字段下，请单击**添加**，并且选择**ACL-REDIRECT**或以前创建的FlexConnect ACL。确认它填充**WebPolicy访问控制列表**字段。

8. 单击**运用**并且**保存配置**。

WLAN 配置

完成这些步骤为了配置WLAN ：

1. 创建双重SSID示例的一开放WLAN SSID ：

   输入WLAN名称：**DemoCWA** (在本例中)。选择状态的**已启用**选项。

2. 导航对**安全选项卡> Layer2**选项卡，并且设置这些属性：

   第 2 层安全：**无**MAC过滤：**已启用**(方框被检查)快速转换：**已禁用**(方框没有被检查)

3. 去**AAA服务器**选项卡，并且设置这些属性：

   验证和帐户服务器：**已启用**服务器 1：*<ISE IP地址>*

4. 从**AAA服务器**选项卡移下来。在验证web-auth用户的优先级指令下，请确保**RADIUS**使用验证，并且没有使用其他。

5. 去**高级选项卡。**，并且设置这些属性：

   允许AAA覆盖：**已启用**美洲台状态：**Radius美洲台**
   Note:RADIUS网络准入控制(NAC)，当FlexConnect AP在断开模式时，不支持。因此，如果FlexConnect AP在独立模式并且丢失对WLC的连接，所有客户端被断开，并且SSID不再通告。
6. 移下来在高级选项卡。和集FlexConnect本地交换对**已启用**。

7. 单击**运用**并且**保存配置**。

8. 创建802.1X WLAN SSID名为**Demo1x** (在本例中)单个和双重SSID方案的。

9. 导航对**安全选项卡> Layer2**选项卡，并且设置这些属性：

   第 2 层安全：**WPA+WPA2**快速转换：**已禁用**(方框没有被检查)认证密钥管理：802.lX ：**Enable (event)**

10. 去**高级选项卡。**，并且设置这些属性：

    允许AAA覆盖：**已启用**美洲台状态：**Radius美洲台**

11. 移下来在**高级选项卡。**和集FlexConnect本地交换对**已启用**。

12. 单击**运用**并且**保存配置**。

13. 确认两个新的WLAN创建。

FlexConnect AP配置

完成这些步骤为了配置FlexConnect AP ：

1. 导航到**WLC >无线**，并且点击目标FlexConnect AP。

2. 点击**FlexConnect**选项卡。

3. 启用VLAN支持(方框被检查)，设置本征VLAN ID，并且点击**VLAN映射**。

4. 设置VLAN ID对**21** (在本例中)本地交换的SSID的。

5. 单击**运用**并且**保存配置**。

ISE配置

完成这些步骤为了配置ISE ：

1. 登陆到ISE服务器：< *https://ise* >。

2. 导航对**Administration >身份管理>外部标识来源**。

3. 点击**活动目录**。

4. 在Connection选项：

   添加**corp.rf-demo.com**域名(在本例中)，并且更改标识存储名称默认对**AD1**。点击**保存配置**。点击**加入**，并且提供要求的AD管理员帐户用户名和密码加入。状态一定绿色。Enable (event)**连接对：**(方框被检查)。

5. 执行一基本连接测验对AD与一个当前域用户。

6. 如果对AD的连接是成功的，对话确认密码正确。

7. 导航对**Administration >身份管理>外部标识来源**：

   点击**证书验证配置文件**。单击为新证书验证配置文件(CAP)**添加**。

8. 输入**CertAuth**名称(在本例中) CAP的;对于首席用户名X509属性，请选择**公用名称**;然后，请单击**提交**。

9. 确认新的CAP被添加。

10. 导航对**Administration >身份管理>标识来源顺序**，并且单击**添加**。

11. 给予顺序**TestSequence**名称(在本例中)。

12. 移下来对**证书基于验证**：

    启用**选择证书验证配置文件**(方框被检查)。选择**CertAuth** (或及早创建的另一CAP配置文件)。

13. 移下来对**验证搜索列表**：

    移动从联机的AD1向选定。点击上按钮为了迁移AD1向最优先考虑的事。

14. 单击**提交**为了保存。

15. 确认新的标识来源顺序被添加。

16. 请使用AD为了验证门户我的设备。导航对**ISE > Administration >身份管理>标识来源顺序**，并且编辑**MyDevices_Portal_Sequence**。

17. 添加**AD1**到选定列表，并且点击上按钮为了迁移AD1向最优先考虑的事。

18. Click **Save**.

19. 确认MyDevices_Portal_Sequence的标识存储顺序包含**AD1**。

20. 重复步骤16-19为了添加Guest_Portal_Sequence的AD1，并且点击**"Save"**。

21. 确认Guest_Portal_Sequence包含**AD1**。

22. 为了添加WLC到网络接入设备(WLC)，导航到**Administration >网络资源>网络设备**，和单击**添加**。

23. 添加WLC名称， IP地址，子网掩码，等等。

24. 移下来对验证设置，并且输入共享塞克雷。这必须匹配WLC RADIUS的共享机密。

25. 单击 **submit**。

26. 导航对**ISE** >Policy >Policy**元素>结果**。

27. 展开**结果**和**授权**，点击**授权配置文件**，并且单击为新配置文件**添加**。

28. 给此配置文件这些值：

    名称：**CWA**

    Enable (event) Web验证(方框被检查) ：

    Web验证：**集中化**ACL ：**ACL-REDIRECT** (这必须匹配WLC PRE验证ACL名称。)重定向：**默认**

29. 单击**提交**，并且确认CWA授权配置文件被添加了。

30. 单击**添加**为了创建一新的授权配置文件。

31. 给此配置文件这些值：

    名称：**提供**

    Enable (event) Web验证(方框被检查) ：

    Web认证值：**请求方设置**

    ACL ：**ACL-REDIRECT** (这必须匹配WLC PRE验证ACL名称。)

32. 单击**提交**，并且确认提供授权配置文件被添加了。

33. 移下来在结果，展开**客户端供应**，并且点击**资源**。

34. 选择**本地请求方配置文件**。

35. 给予配置文件**WirelessSP**名称(在本例中)。

36. 输入这些值：

    连接类型：**无线**SSID ：**Demo1x** (此值是从WLC 802.1x WLAN配置)允许协议：**TLS**密钥大小：**1024**

37. 单击 **submit**。

38. Click **Save**.

39. 确认新配置文件被添加了。

40. 导航对**策略>客户端供应**。

41. 输入IOS设备供应规则的这些值：

    规则名称：**iOS**标识组：**任一**

    操作系统：**Mac iOS全部**

    结果：**WirelessSP** (这是及早创建的本地请求方配置文件)

导航对**结果>向导配置文件**(下拉列表) > **WirelessSP**。

42. 确认iOS供应配置文件被添加了。

43. 在第一个规则的右边，请找出操作下拉列表，并且选择以上**重复项下面**()。

44. 更改新规则的名称到**机器人**。

45. 更换操作系统到**机器人**。

46. 保持不变其他值。

47. 点击**“Save”** (左下屏幕)。

48. 导航对**ISE** >Policy >**验证**。

49. 修改情况包括Wireless_MAB，并且展开**Wired_MAB**。

50. 点击**条件名**下拉列表。

51. 选择**字典>复合条件**。

52. 选择**Wireless_MAB**。

53. 在规则右边，请选择箭头展开。

54. 选择从下拉列表的这些值：

    标识来源：**TestSequence** (这是及早创建的值)如果验证失败：**拒绝**如果用户没找到：**继续**如果进程失败：**丢弃**

55. 去**Dot1x**规则，并且更改这些值：

    条件：**Wireless_802.1X**

    标识来源：**TestSequence**

56. Click **Save**.

57. 导航对**ISE** >Policy >**授权**。

58. 默认规则(例如黑色列表默认，被描出和默认)已经配置从安装;前两个可以忽略;默认规则编辑的以后。

59. 在第二个规则(被描出的思科IP电话)右边，请单击下箭头在旁边编辑，并且选择**下面插入新规则**。

    一个新的标准的规则#增加。

60. 更改从标准的规则的规则名称#对**OpenCWA**。此规则开始在开放WLAN (双重SSID)的注册过程走向访客网络为了安排设备设置的用户的。

61. 点击加号(+)情况的，并且单击**选择从库的现有情况**。

62. 选择**复合条件> Wireless_MAB**。

63. 在AuthZ配置文件，请点击加号(+)，并且选择**英文虎报**。

64. 选择标准**CWA** (这是及早创建的授权配置文件)。

65. 确认规则增加与正确条件和授权。

66. 点击**完成**(在规则的右边)。

67. 在同一个规则右边，请单击下箭头在旁边编辑，并且选择**下面插入新规则**。

68. 更改从标准的规则的规则名称#对**PEAPrule** (在本例中)。此规则是为PEAP (也用于单个SSID方案)检查802.1X的验证没有传输层安全(TLS)，并且该网络请求方设置启动与以前创建的提供授权配置文件。

69. 更改情况对**Wireless_802.1X**。

70. 在情况的右边单击齿轮图标，并且选择**添加属性/值**。这是'和'情况，没有'或'情况。

71. 找出并且选择**网络访问**。

72. 选择**AuthenticationMethod**，并且输入这些值：

    AuthenticationMethod ：**等于**

挑选**MSCHAPV2**。

这是规则的示例;请务必确认情况是和。

73. 在AuthZ配置文件，选择**英文虎报>提供**(这是及早创建的授权配置文件)。

74. 点击**完成**。

75. 在PEAPrule右边，请单击下箭头在旁边编辑，并且选择**下面插入新规则**。

76. 更改从标准的规则的规则名称#对**AllowRule** (在本例中)。此规则将用于为了允许对注册的设备的访问有安装的证书的。

77. 在情况下，请选择**复合条件**。

78. 选择**Wireless_802.1X**。

79. 添加并且归因于。

80. 在情况的右边单击齿轮图标，并且选择**添加属性/值**。

81. 找出并且选择**Radius**。

82. 选择呼叫站点**ID[31]**。

83. 选择**等于**。

84. 去**证书**，并且点击右箭头。

85. 选择**附属的替代方案名称**。

86. 对于AuthZ配置文件，请选择**英文虎报**。

87. 选择**Permit访问**。

88. 点击**完成**。

这是规则的示例：

89. 找出默认规则为了更改PermitAccess到DenyAccess。

90. 单击**编辑**为了编辑默认规则。

91. 去PermitAccess现有AuthZ配置文件。

92. 选择**英文虎报**。

93. 选择**DenyAccess**。

94. 确认默认规则有DenyAccess，如果没有找到匹配。

95. 点击**完成**。

这是为此测验要求的主要规则的示例;他们为单个SSID或双重SSID方案是可适用的。

96. Click **Save**.

97. 导航对**ISE > Administration >**System **>证书**为了配置有SCEP配置文件的ISE服务器。

98. 在证书操作，请点击**SCEP CA配置文件**。

99. 单击 **Add**。

100. 输入此配置文件的这些值：

名称：**mySCEP** (在本例中)URL ：**https:// <*ca-server*> /CertSrv/mscep/** (请检查您的CA服务器配置正确地址。)

101. 点击**测验连接**为了测试SCEP连接的连接。

102. 此答复显示服务器连通性是成功的。

103. 单击 **submit**。

104. 服务器回应CA配置文件顺利地创建。

105. 确认SCEP CA配置文件被添加。

用户体验-设置的iOS

双重SSID

此部分包括双重SSID并且描述如何连接对访客将设置和如何连接到802.1x WLAN。

完成这些步骤为了设置在双重SSID方案的iOS ：

1. 在IOS设备上，请去**wi-fi网络**，并且选择**DemoCWA** (在WLC的配置的开放WLAN)。

2. 打开在IOS设备的Safari浏览器，并且访问可及的URL (例如，内部/外部网络服务器)。ISE重定向您到门户。单击 **Continue**。

3. 您重定向到登录的访客门户。

4. 洛金用AD用户帐户和密码。安装CA配置文件，当提示。

5. 点击CA服务器的**安装**信任证书。

6. 一旦配置文件完全安装，请点击**完成**。

7. 返回到浏览器，并且点击**寄存器**。记录下来包含设备的MAC地址的设备ID。

8. 点击**安装**为了安装已验证配置文件。

9. **当前**单击**安装**。

10. 在进程完成后， WirelessSP配置文件确认配置文件安装。点击**完成**。

11. 去**wi-fi网络**，并且更改网络对**Demo1x**。您的设备当前连接并且使用TLS。

12. 在ISE，请导航对**操作>认证**。事件显示设备连接对开放访客网络，通过与设置的请求方的注册过程和在注册以后允许permit访问的进程。

13. 导航对**ISE > Administration >身份管理>** Groups **>终端标识Groups> RegisteredDevices**。MAC地址被添加了到数据库。

单个SSID

此部分包括单个SSID并且描述如何连接直接地到802.1x WLAN，为PEAP验证提供AD用户名/密码，通过访客帐户设置和重新连接与TLS。

完成这些步骤为了设置在单个SSID方案的iOS ：

1. 如果使用同一个IOS设备，请从注册的设备删除终端。

2. 在IOS设备上，请导航对**设置>常规>配置文件**。删除在本例中安装的配置文件。

3. 点击**删除**为了删除上一个配置文件。

4. 连接直接地对802.1x用存在的(清除)设备或用一个新的IOS设备。

5. 连接对**Dot1x**，输入用户名和密码，并且点击**加入**。

6. 请重复从ISE配置部分的步骤90和，直到适当的配置文件完全安装。

7. 导航对**ISE >操作>认证**为了监控进程。此示例显示连接直接地对802.1X WLAN的客户端，当设置，断开，并且重新连接对与使用的同样WLAN TLS。

8. 导航对**WLC >监视器> [Client MAC]**。在客户端详细信息，请注意客户端是在运转状态，其数据交换设置为本地，并且验证是中央的。这是可靠对于连接对FlexConnect AP的客户端。

用户体验-设置的机器人

双重SSID

此部分包括双重SSID并且描述如何连接对访客将设置和如何连接到802.1x WLAN。

机器人设备的连接进程非常类似于那为IOS设备(单个或双重SSID)。然而，一重要差异是机器人设备要求对互联网的访问为了访问谷歌市场(当前谷歌作用)和下载请求方代理程序。

完成这些步骤为了设置一个机器人设备(例如在本例中的三星星系)在双重SSID方案：

1. 在机器人设备中，请使用得wi-fi为了连接到**DemoCWA**和打开访客WLAN。

2. 接受所有证书为了连接到ISE。

3. 在访客门户输入用户名和密码为了登陆。

4. 点击**寄存器**。设备尝试到达互联网为了访问谷歌市场。增加所有另外的规则到PRE验证ACL(例如ACL-REDIRECT)在控制器为了允许到互联网。

5. 谷歌列出被建立的Cisco网络作为一机器人App。单击 **Install**。

6. 签到对谷歌，并且点击**安装**。

7. 单击 **Ok**。

8. 在机器人设备上，请查找已安装**思科SPW** app，并且打开它。

9. 确保您仍然登陆到从您的机器人设备的访客门户。

10. 点击**开始**为了开始wi-fi设置助理。

11. 思科SPW开始安装证书。

12. 当提示，设置证件存储设备的一个密码。

13. 思科SPW返回与验证名称，包含用户密钥和用户证书。点击**确定**以确认。

14. 思科SPW继续并且提示输入另一验证名称，包含CA证书。输入命名**iseca** (在本例中)，然后点击OK键继续为了。

15. 机器人设备当前连接。

门户我的设备

我的设备门户允许用户以前列入黑名单在设备丢失或窃取的事件的注册的设备。若需要它也允许用户延长服役。

完成这些步骤为了列入黑名单设备：

1. 为了登陆到我的设备门户，请打开浏览器，连接对https://ise-server:8443/mydevices (请注释端口号8443)，并且登陆与AD帐户。

2. 找出设备在设备ID下，并且单击**丢失？**为了启动列入黑名单设备。

3. 当ISE提示警告时，请点击**是**为了继续。

4. ISE确认设备被标记作为**丢失**。

5. 所有尝试连接到网络用注册的设备当前以前阻塞，即使有安装的有效证书。这是发生故障验证一个列入黑名单的设备的示例：

6. 管理员能导航到**ISE > Administration >身份管理>** Groups，点击**终端标识Groups>黑名单**，并且看到设备列入黑名单。

完成这些步骤为了复原一个列入黑名单的设备：

1. 从我的设备门户，请单击为该设备**复原**。

2. 当ISE提示警告时，请点击**是**为了继续。

3. ISE确认设备顺利地被复原了。连接被复原的设备对网络为了测试设备当前将允许。

参考-证书

ISE不仅要求一个有效CA根证明，而且需要CA签字的有效证书。

完成这些步骤为了添加，绑定和导入新建的委托CA证书：

1. 导航对**ISE > Administration >**System **>证书**，点击**本地证书**，并且单击**添加**。

2. 选择**生成证书签名请求**(CSR)。

3. 输入证书主题**CN=<ISE-SERVER***主机名.FQDN*>。对于其他字段，您能使用您的CA设置或值要求的默认。单击 **submit**。

4. ISE验证CSR生成。

5. 为了访问CSR，请点击**证书签名请求**操作。

6. 选择最近创建的CSR，然后点击**出口**。

7. ISE导出CSR到.pem文件。点击**保存文件**，然后点击OK键为了保存文件到本地设备。

8. 寻找并且打开有文本编辑的ISE证书文件。

9. 复制证书的整个内容。

10. 连接对CA服务器和登录与管理员帐户。服务器是Microsoft 2008 CA在 https://10.10.10.10/certsrv (在本例中)。

11. 点击**请求证书**。

12. 点击**先进的证书请求**。

13. 点击第二个选项为了**提交证书请求通过使用base-64-encoded CMC或…**。

14. 粘贴内容从ISE证书文件(.pem)到保存的请求字段，保证认证模板是**Web服务器**，并且单击**提交**。

15. 点击**下载证书**。

16. 保存certnew.cer文件;它使用的以后为了绑定与ISE。

17. 从ISE**证书**，请导航对**本地证书**，并且点击**Add>捆绑CA证书**。

18. 浏览对保存到在上一步的本地设备的证书，启用**EAP**和**管理接口**协议(方框被检查)，并且单击**提交**。ISE可能采取几分钟或更多为了重新启动服务。

19. 返回到CA的着陆页(https://CA/certsrv/)，和点击**下载CA证书、证书链或者CRL**。

20. 单击**下载 CA 证书**。

21. **保存**文件到本地设备。

22. 使用联机ISE的服务器，请去**证书**，并且单击**认证机关证书**。

23. 单击 **Import**。

24. 为CA证书浏览，启用**客户端验证的托拉斯**(方框被检查)，并且单击**提交**。

25. 确认新的委托CA证书被添加。

相关信息

- 思科身份服务引擎硬件安装指南，版本1.0.4
- Cisco 2000 系列无线局域网控制器
- Cisco 4400 系列无线局域网控制器
- Cisco Aironet 3500系列
- 弹性7500无线支线控制器部署指南
- 带来您自己的设备- Unified设备验证和一致访问经验
- 无线BYOD用身份服务引擎
- 技术支持和文档 - Cisco Systems