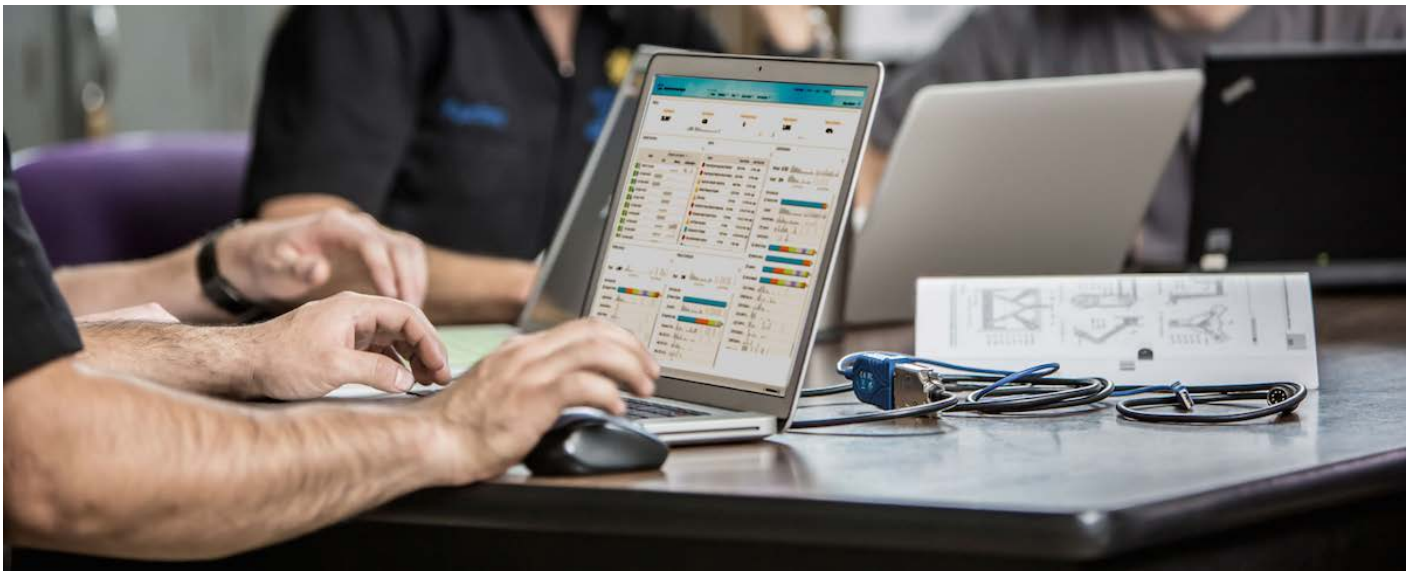


ISE 快速安装指南

安全访问操作指南系列

作者：Jason Kunst

日期：2015 年 5 月

目录

关于本指南

本指南介绍了通过思科无线控制器配置思科身份服务引擎 (ISE) 来提供访客接入的快速过程。使用本指南中的步骤，您只需大约两个小时即可为用户完成访客接入设置。

本指南基于 ISE 1.3 创建，同时也支持 ISE 1.4。

本指南支持两种类型的门户：

- 热点访客的访客接入门户
- 具有凭证的访客的访客接入门户

使用本指南

本指南包含两个部分，介绍使用 ISE 和思科无线控制器 (WLC) 安装和配置无线访客接入所需的活动。

- **第 1 部分 - 安装和配置思科无线控制器 (WLC)** - 第 1 部分介绍在开始执行**第 2 部分**中列出的任务之前必须完成的安装预设置和配置活动。

- **第 2 部分 - 在 VMware 上安装和配置身份服务引擎 (ISE)** - 第 2 部分介绍在 VMware 服务器上安装和配置 ISE 软件以及使用 WLC 配置访客服务的过程。

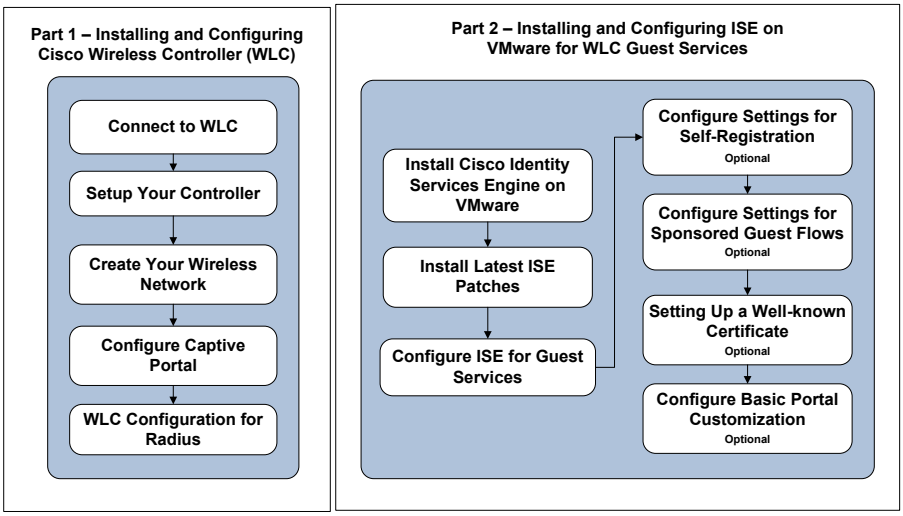


图 1. ISE 快速安装和配置过程以及使用 WLC 配置访客服务的过程

要求

- VMware ESX (i) 4.x 或更高版本
- 作为 SNS-3415 设备运行的虚拟机 - 请参阅 VMware 设备规范的表 2
- 具有最新补丁的思科身份服务引擎 1.3 或 1.4 版本
    - 存在已知问题 (CSCus55690)。此问题应该会在 1.3 Patch 3 和 1.4 Patch 1 中得到解决。思科强烈建议您在获得这些补丁后立即进行安装。

- **注**：如果设备本应被清除而未被清除，则设备不会被从终端数据库中删除并且会获得访问权限。

- 运行 7.6.x 或 8.x 的物理思科无线控制器 (WLC)

注：本指南仅适用于新安装，如果不是新安装，请对控制器执行出厂重置。有关重置控制器的步骤，请参阅控制器相关文档。

访客接入

当公司外部人员尝试使用公司网络访问互联网或网络上的资源和服务时，您可以通过各种访客门户为其提供网络访问权限。访客通常代表授权访客、承包商、客户，或者需要访问网络的其他临时用户。

本指南支持两种类型的访客接入门户：

- 热点访客的访客接入门户
- 具有凭证的访客的访客接入门户

热点访客的访客接入门户

热点访客的访客接入门户是指配置为提供网络访问权限而不要求访客提供用于连接的用户名和密码的访客门户。此类型的访客接入可消除管理每个单独访客帐户所需的开销。当访客连接到网络时，系统会将其重定向至 ISE 热点访客门户，访客必须在该门户接受可接受的使用策略 (AUP) 才能获得网络访问权限并最终访问互联网。

具有凭证的访客的访客接入门户

具有凭证的访客的访客接入门户提供网络访问权限，但是要求访客具有用户名和密码才能获得访问权限。访客可以为自己创建用于登录访客门户的帐户。此门户还可与发起人所创建的凭证结合使用。例如，发起人可以是员工或前台接待人员。当访客连接到网络时，系统会将其重定向至允许其使用通过自注册创建或由发起人提供的凭证进行登录的门户。在访客登录后，可能会要求其接受可接受的使用策略 (AUP) 才能获得网络访问权限并最终访问互联网。您也可以使用所发起的要求用户具有由发起人创建的凭证的访客门户设置访问权限。

有关访客门户和功能的详细信息，请参阅思科访客接入。

下载思科 ISE 软件

使用 ISE 软件下载链接下载最新的思科 ISE 软件和 ISE 补丁。下载时间将因网络的速度而异。

软件下载

点击思科 ISE 下载软件访问思科 ISE 软件下载页面，其中可下载的文件如下所示：

- ISE 1.3 或 1.4 的 ISE VM OVA 文件：虚拟 SNS-3415
  - 例如：ISE-1.3.0.876-virtual-SNS3415-2.ova
- ISE 1.3 或 1.4 的最新补丁文件
  - 例如：ise-patchbundle-1.3.0.876-Auto1-125229.x86_64.tar.gz

注：当下载 ISE 补丁 (tar.gz) 时，某些 Web 浏览器（如 OSX Safari）要求在安装补丁时维护存档结构。为此，请使用 Firefox 或 Google Chrome 浏览器。

您可以点击以下链接，查看有关下载思科 ISE 软件的视频：

- ISE 简介以及思科 ISE 软件下载方法

规划

在开始安装和配置 ISE 和 WLC 之前，我们建议您花一些时间收集稍后安装和配置 ISE 及 WLC 过程中将会用到的信息。我们已创建可用于帮助组织和记录服务器信息的检查表。请在安装和配置过程中根据需要参阅此检查表。

注：在安装 ISE 之前并且您正在记录**预设置检查表**信息时，请确保您有权访问以下服务。如果这些服务不可用，则安装过程可能会失败。

- DNS
- NTP 和默认网关

在 **ESX** 和 **NTP 主机**上验证时间是否正确。主机时间必须同步才能使服务和证书正常工作。

预设置检查表

编号	服务	描述	在此处记录信息
1	WLC 系统名称	• 在 WLC 上配置的控制器系统的名称 • *例如：WLC*	WLC 系统名称：_____
2	无线控制器 IP、子网掩码和网关	• WLC 的网络信息	无线控制器 IP：_____ 子网掩码：_____ 网关：_____
3	DHCP 服务器 IP	• 网络中的 DHCP 服务器 • 在 WLC 上配置	DHCP 服务器 IP：_____
4	访客 SSID	• 访客要访问的网络名称 • 在 WLC 上配置 • *例如：yourcompany-guest*	访客 SSID：_____
5	访客 VLAN（可选） 如果访客使用的网络与管理网络是同一网络，则无需选择此项	• 用于访客的 VLAN • 在 WLC 上配置 • *例如：50*	访客 VLAN：_____
6	访客网络 IP 地址、子网掩码和网关	• 控制器需要在访客网络上具有一个 IP 地址，以便与访客进行通信 • 在 WLC 上配置	访客网络 IP：_____ 子网掩码：_____ 网关：_____
7	DNS 服务器 IP	• 网络中的 DNS 服务器 • 在 ISE 上配置	DNS 服务器 IP：_____

8	NTP 服务器 IP	• 网络中的 NTP 服务器 • 在 ISE 上配置	NTP 服务器 IP：_____
9	ISE IP、子网掩码和网关	• ISE 的网络信息 • 在 ISE 上配置	ISE IP：_____ 子网掩码：_____ 网关：_____
10	ISE 主机名	• ISE 服务器的名称 • 在 ISE 上配置 • *例如：yourdomain.com*	ISE 主机名：_____
11	Management Network VLAN	• ISE 和 WLC 在 ESX (i) 主机上要连接到的网络 • 在 WLC 和 ESX(i) 主机上配置 • *例如：100*	管理 网络 VLAN：_____
12	共享密钥	• 这是在 ISE 和 WLC 之间通信时共享的密码，其目的是保护 RADIUS 通道的安全 • 在 WLC 和 ISE 上配置	共享密钥：_____

配置WLC 的基础知识

有多种方法可以配置思科无线局域网控制器。在本指南中，我们将使用 WLAN 快速设置。有关 WLAN 快速设置和 WLC 配置的详细信息，请选择以下链接之一：

- WLAN 快速设置视频
- 思科 WLAN 版本说明

连接到 WLC

在连接所有组件以配置思科无线访客服务之前，您需要先在笔记本电脑（计算机）和 WLC 之间建立通信。在笔记本电脑和 WLC 之间建立初始通信后，即可完成硬件设置和软件安装程序。

设置控制器

要连接到 WLC，请执行以下步骤：

步骤 1 将**管理员笔记本连接至 WLC 上的端口 2**，如图 1 所示。

图 2. 笔记本电脑 - WLC 连接

笔记本电脑应从子网 192.168.1.0/24 获取 IP 地址。

步骤 2 打开浏览器，然后在地址栏中输入 **https://192.168.1.1** 以访问 WLC 管理员用户界面。

系统将显示 WLC 管理员用户界面，如图 2 所示。

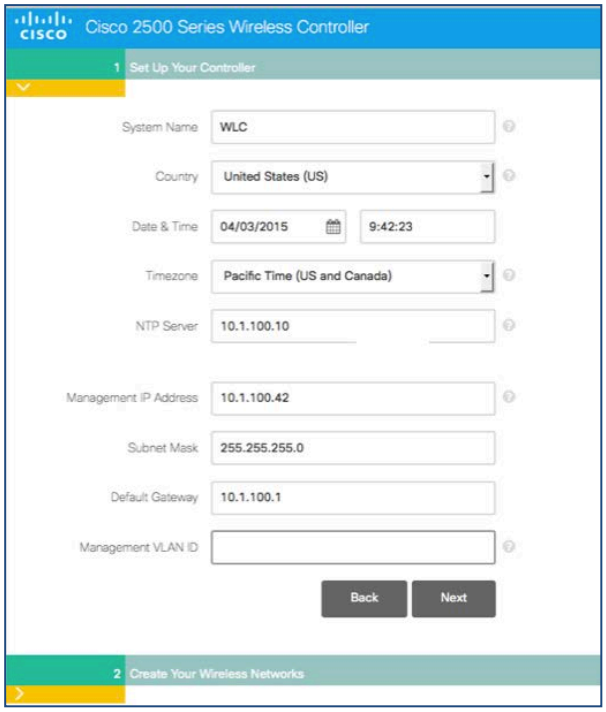


图 3. WLC - Set Up Your Controller 选项卡

步骤 3 输入用于管理控制器的凭证。请参阅您在**规划**一节中完成的**预设置检查表**。

表 1. 无线局域网控制器向导

字段	描述
System Name	WLC 系统名称 预设置检查表项目编号 - 1
Country	您当前所在国家/地区位置
Date & Time	您的当前日期和时间
Timezone	从下拉菜单中选择时区
NTP Server	NTP 服务器的 IP 地址 预设置检查表项目编号 - 8
Management IP Address	用于管理无线控制器的 IP 地址 预设置检查表项目编号 - 2
Subnet Mask	WLC 的子网掩码 预设置检查表项目编号 - 2

字段	描述
Default Gateway	WLC 的默认网关 预设置检查表项目编号 - 2
Management Network VLAN	管理网络 VLAN 预设置检查表项目编号 - 11

步骤 4 点击 **Next** 继续操作。

接下来，需要创建无线网络。

创建无线网络

步骤 1 点击 **X** 以取消选中 **Employee Network**。

注：本指南不会介绍为员工（内部用户）设置无线 dot1x 网络的相关内容。

步骤 2 点击 **Guess Network** 旁边的复选标记，如图 3 所示：

图 4. WLC - Create Your Wireless Network 选项卡

表 2. Create Your Wireless Networks 选项卡字段

字段	描述
Network Name	访客的无线网络 (SSID) 预设置检查表项目编号 - 4
Security	从下拉菜单中所列的选项中选择安全类型 “Web Consent”
VLAN	从下拉菜单中所列的选项中选择 VLAN “New VLAN”
VLAN IP Address	访客网络的 IP 地址 预设置检查表项目编号 - 6
VLAN Subnet Mask	VLAN 子网掩码的 IP 地址 预设置检查表项目编号 - 6
VLAN Default Gateway	默认网关的 IP 地址 预设置检查表项目编号 - 6
VLAN ID（可选）	VLAN 的 ID（可选，如果使用管理网络，则无需选择此项） 预设置检查表项目编号 - 5
DHCP Server Address	DHCP 服务器的 IP 地址 预设置检查表项目编号 - 3

步骤 3 从规划阶段输入**所需信息**。

步骤 4 点击 **Next** 继续操作。

系统会显示确认屏幕，其中包含一条消息，询问您是否要应用 WLC 确认更改，并通知您在点击 **OK** 后系统将重新启动，如图 5 所示。

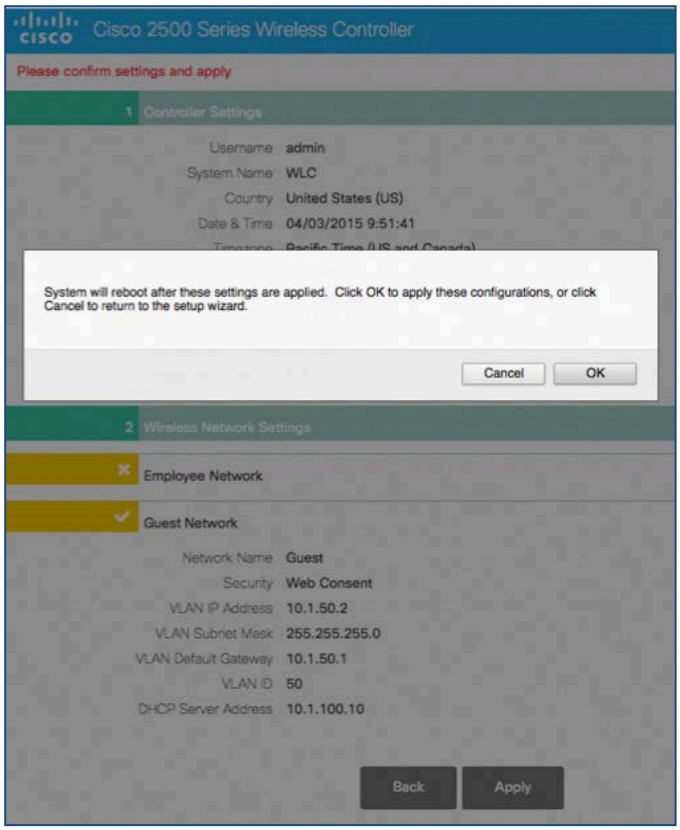


图 5. WLC - 创建无线网络确认屏幕

强制门户绕行配置

多个 Web 浏览器均支持思科身份服务引擎软件。为了将控制器用于思科 ISE 访客接入和 Apple 的 Safari Web 浏览器，您需要先完成强制门户绕行配置过程，然后才能安装和配置 ISE 访客服务。

要配置强制门户绕行，请执行以下步骤。

步骤 1 使用诸如 Putty 等 SSH 客户端连接到无线控制器 IP 地址。
步骤 2 登录到**控制器** CLI。
步骤 3 输入以下命令：

```
config network web-auth captive-bypass enable
```

控制器重新启动。

步骤 4 重新登录到 CLI 并使用以下命令显示状态：

```
show network summary
```

步骤 5 在最后一页上找到以下行。

提示：轻触两下空格键会转至最后一页。

```
Web Auth Captive-Bypass    ................... Enable
```

步骤 6 关闭 SSH 会话，然后使用 Web 浏览器再次连接到 WLC。

有关使用强制门户绕行的详细信息，请参阅适用于特定代码版本的配置强制绕行。

拓扑示例

为更好地说明本文档中所列的方案和配置，请查看以下拓扑示例。

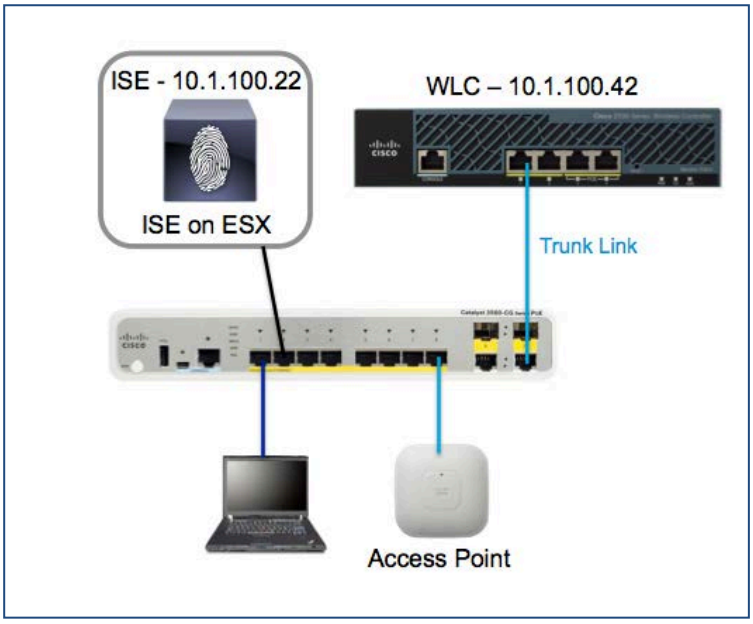


图 6. 拓扑示例

拓扑示例中的思科 3560G 交换机（图 6）可与所有组件进行基本连接。为访问 VLAN 100，交换机上的所有端口都将进行配置。但是，**端口 10** 需要配置为中继端口。

有关交换机配置的详细信息，请参阅附录 A。

注：WLC 重新启动后，管理功能随即在 VLAN 100（例如 10.1.100.42）上处于激活状态，并不再通过旧 IP 地址进行响应。

步骤 1 将管理员笔记本电脑与 WLC 上的**端口 2** 断开连接，并改为将其连接到交换机上的**端口 1**。

步骤 2 将 WLC 上的**端口 1** 连接到交换机上的中继端口。

您应该能够使用交换机访问 WLC。（例如：https://10.1.100.42）。

为 RADIUS 配置 WLC

下一节中将说明为与 ISE 协作，如何在 WLC 上配置必要的安全设置。通过 RADIUS NAC，ISE 可以发送授权变更 (COA) 请求，表明用户现已经过身份验证并能够访问网络。实际上，ISE 借此能够随时更改客户端的状态，而无需新的会话。能够让客户端从重定向到 ISE 以进行门户身份验证的状态进行切换，然后经过身份验证后，将该客户端的状态改为允许访问网络（例如互联网）。

在 WLC 上配置 RADIUS 身份验证服务器

要配置 RADIUS 身份验证服务器，请执行以下步骤：

步骤 1 登录到无线局域网控制器 (WLC) 服务器 GUI 上。
步骤 2 从左侧菜单中选择 **Security > AAA > RADIUS > Authentication**，如图 7 所示。

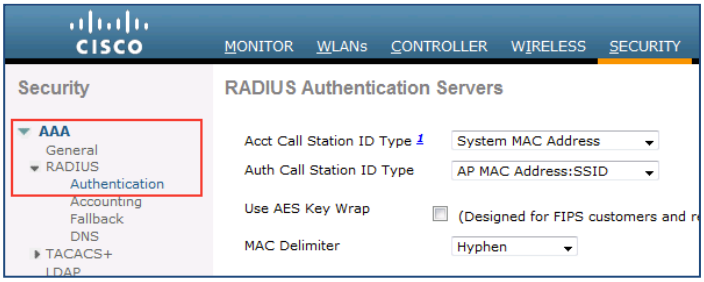


图 7. Radius 身份验证服务器

步骤 3 点击 **New**。

系统将显示 RADIUS Authentication Server 屏幕，如图 8 所示。

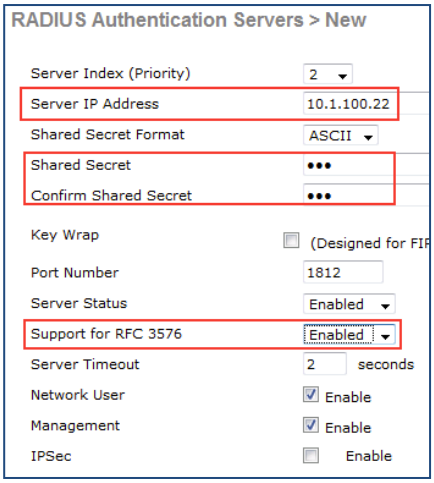


图 8. Radius 身份验证服务器 - 编辑

步骤 4 输入 **ISE IP Address** 和 **Shared Secret**。
步骤 5 启用 Support for **RFC 3576**。

步骤 6 点击 **Apply**。

在 WLC 上配置 RADIUS 记帐服务器

要配置 RADIUS 记帐服务器，请执行以下步骤：

步骤 1 登录到无线局域网控制器 (WLC) 服务器 GUI 上。
步骤 2 从左侧菜单中选择 **Security** > **AAA** > **RADIUS** > **Accounting**，如图 9 所示。

图 9. RADIUS 记帐服务器

步骤 3 点击 **New**。

系统将显示 RADIUS 记帐服务器屏幕，如图 10 所示。

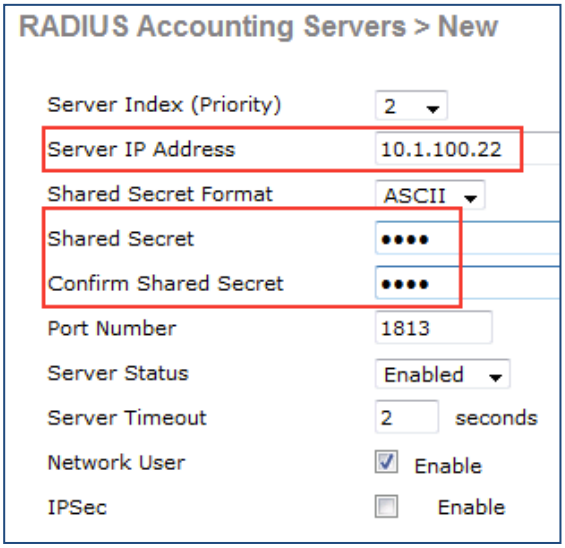


图 10. RADIUS 记帐服务器 - 编辑

步骤 4 输入 **ISE IP Address** 和 **Shared Secret**。
步骤 5 点击 **Apply**。

将 WLC 配置更改为使用集中式 Web 身份验证 (CWA)

要将 WLC 配置更改为使用 CWA，请执行以下步骤。

步骤 1 选择 **WLAN**。
步骤 2 选择 **Guest SSID**。

图 11. WLAN

步骤 3 选择 **Security** 选项卡。

步骤 4 点击 **Layer 2** 选项卡。

系统将显示 Layer 2 Security 选项卡选项，如图 12 所示。

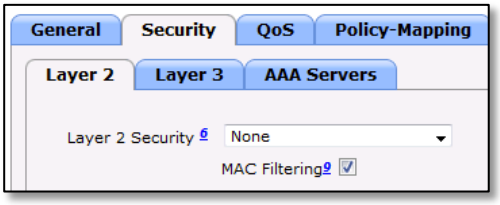


图 12. 第 2 层安全性

步骤 5 对于 Layer 2 Security，选择 **None**。

步骤 6 启用 **MAC Filtering**。

步骤 7 点击 **Layer 3** 选项卡。

系统将显示 Layer 3 Security 选项卡选项，如图 13 所示。

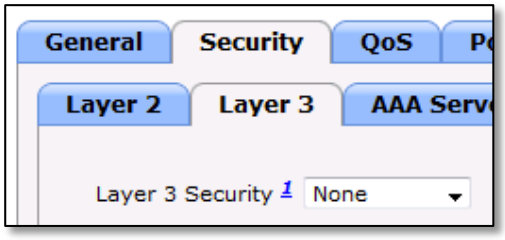


图 13. 第 3 层安全性

步骤 8 选择 **None**。

步骤 9 选择 **AAA Servers**。

系统将显示 AAA Servers 选项，如图 14 所示。

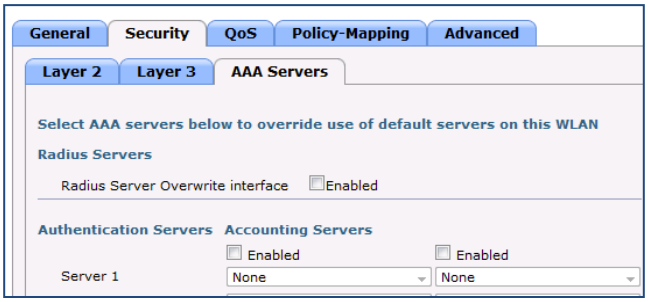


图 14. AAA 服务器安全性

步骤 10 针对 **Authentication and Accounting** 选择并启用 Server 1 标签下的 ISE 服务器 IP，如图 15 所示。

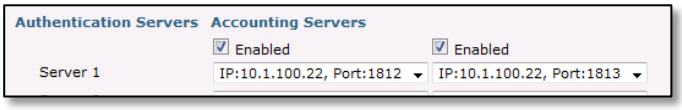


图 15. AAA 服务器安全性

步骤 11 点击 **Advanced** 选项卡。

步骤 12 系统将显示 Advanced 选项卡选项，如图 16 所示。

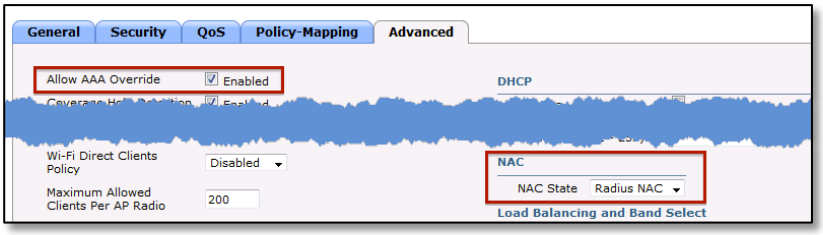


图 16. Advance 选项卡选项

步骤 13 启用 **Allow AAA Override**。

步骤 14 在 **NAC State** 下，使用下拉菜单选择 **RADIUS NAC**。

步骤 15 点击 **Apply**。

配置用于访客重定向的 ACL 并允许访问

本节介绍如何在 WLC 上配置 ACL。目标是配置允许访客客户端访问访客服务的 ACL。

配置 ACL 以将访客设备重定向至 ISE 访客门户

步骤 1 转至 WLC GUI 并选择 **Security > Access Control Lists > Access Control Lists**。

系统将显示 Access Control Lists 页面，如图 17 所示。此页面列出 WLC 上配置的 ACL。通过此页面还可编辑或删除任何 ACL。

图 17. 访问控制列表

步骤 2 点击 **New** 按钮以创建新 ACL。
步骤 3 输入 **GUESTREDIRECT** 作为名称，如图 18 所示。
步骤 4 点击 **Edit**，以便为 ACL 创建规则。

图 18. 访问控制列表

步骤 5 点击 **Apply** 按钮。

系统将显示 **Access Control Lists** 编辑页面，如图 19 所示。

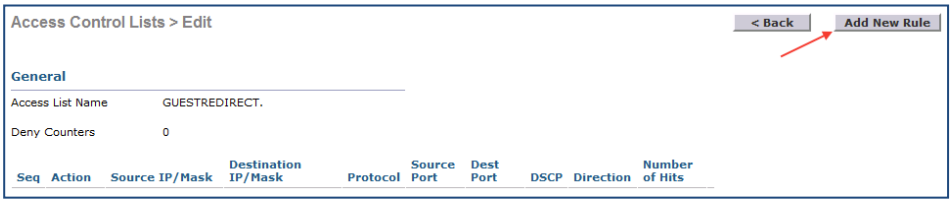
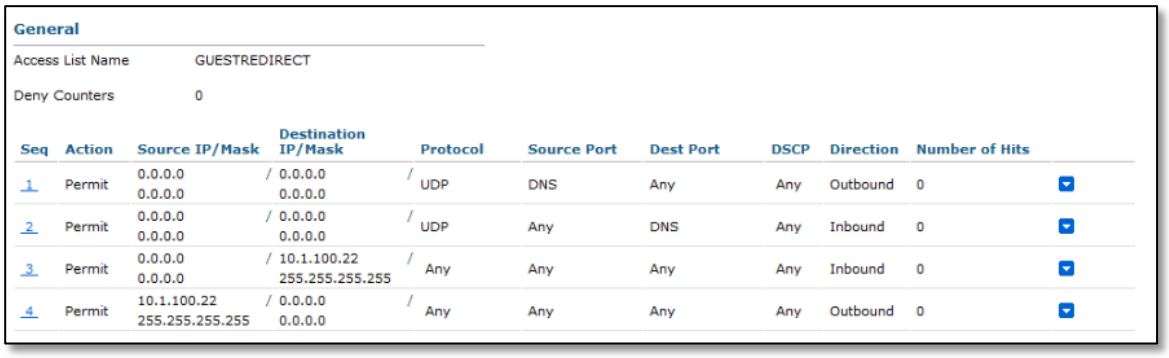


图 19. Access Control Lists 编辑页面

步骤 6 点击 **Add New Rule** 按钮。
步骤 7 系统将显示 **Access Control Lists > Rules** 页面。
步骤 8 配置规则，如图 20 所示。

注：10.1.100.22 是 ISE 的 IP 地址（使用 ISE IP 地址）。



General

Access List Name GUESTREDIRECT

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0

图 20. ACL 规则条目

配置 ACL 以在身份验证后允许访客访问互联网

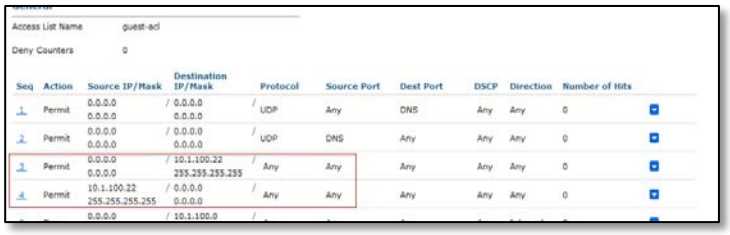
步骤 1 WLC 向导在设置时创建了一个 ACL，称为 **guest-acl**。

步骤 2 点击 **guest-acl** ACL。

步骤 3 在 **Sequence 2** 之后添加以下两个新规则。请务必依序添加。

- 允许任何条目**访问源 ISE IP**
- 允许任何条目**访问目标 ISE IP**

图 21 显示 **Sequence 2** 之后添加的两个新规则。



Access List Name guest-acl

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

图 21. 新规则条目

注：10.1.100.22 是 ISE 服务器的 IP 地址。针对新规则，请使用 ISE IP 地址。

至此“使用带有 WLC 的思科身份服务引擎处理访客服务”过程的第一部分 - 安装和配置思科无线控制器 (WLC) 已经完成。

在 VMware 上安装和配置 (ISE)

在本指南的此部分中，我们讨论在 VMware 服务器上安装和配置 ISE 软件所涉及的任务。

图 7 显示本指南的此部分中介绍的工作流程任务。此工作流程中介绍的活动表示使用 ISE 成功部署访客服务必须完成的任务。

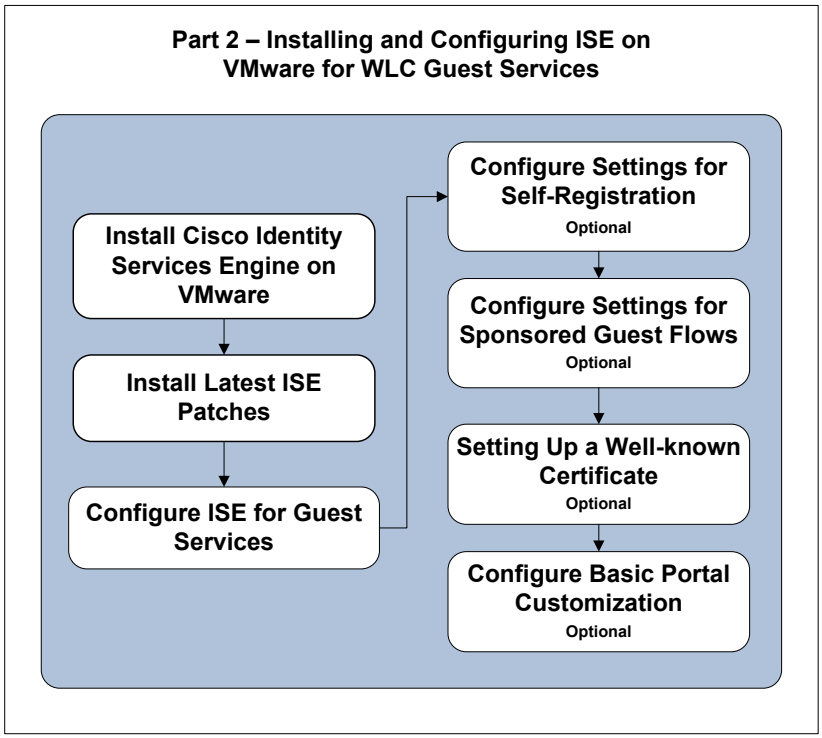


图 22. 在 VMware 上安装和配置 (ISE)

在虚拟机上安装思科 ISE

您可以使用 OVA 模板在虚拟机上安装和部署思科 ISE 软件。您之前已从 Cisco.com 下载了 OVA 模板。

将 ISE OVA 作为虚拟机进行部署

要使用 ESX(i) 5.x 在 ESX(i) 环境中部署 ISE OVA，请执行以下步骤。

步骤 1 打开 **VMware vSphere Client**。
步骤 2 登录到 **VMware host**。
步骤 3 从 VMware vSphere Client 中选择 **File > Deploy OVF Template**。
步骤 4 点击 **Browse** 以选择 OVA 模板，然后点击 **Next**。
步骤 5 确认 OVF Template Details 页面中的详细信息，然后点击 **Next**。
步骤 6 在 Name and Location 页面中输入虚拟机的名称以唯一识别该虚拟机，然后点击 **Next**。
步骤 7 选择 **data store** 以托管 OVA。
步骤 8 点击 Disk Format 页面中的 **Thick Provision** 单选按钮，然后点击 **Next**。

思科 ISE 版本 1.3 同时支持详细和精简调配。但是，我们建议您选择详细调配以实现更好的性能。如果选择精简调配，那么诸如升级、备份和恢复以及调试日志记录等需要更多磁盘空间的操作在初始磁盘扩展期间可能会受影响。

注：如果系统要求您选择 Lazy 或 Eager Zero，请选择 Lazy。

步骤 9 验证 Ready to Complete 页面中的信息。
步骤 10 选中 **Power on after deployment** 复选框。
步骤 11 点击 **Finish**。

运行 ISE 设置

在本节中，您使用 vSphere 控制台命令行界面 (CLI) 设置 ISE 虚拟机。当安装过程完成时，虚拟机自动重新启动。当虚拟机重新启动时，您将看到系统提示。

步骤 1 在系统提示符下，输入 **setup**，然后按下 **Enter** 键。

系统将显示安装向导并引导您完成初始配置。

步骤 2 使用在本文档的“预设置规划”一节中收集的信息回答来自安装向导的提问。

下面的示例显示 **setup** 命令的示例输出。

```
localhost login: setup
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address[]: 10.1.100.22
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.100.1
Enter default DNS domain[]: yourdomain.com
```

```
Enter primary nameserver[]: 172.16.168.183
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC] :
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
```

有关安装的更多详细信息，请参考管理指南的在 VMware 系统上安装思科 ISE 软件一节。

安装 ISE 补丁

将 ISE 虚拟机设置为启动并正常运行后，请使用以下说明安装最新的补丁来给系统打补丁。

步骤 1 登录到 **ISE Admin UI** (http://iseapaddress)。
步骤 2 导航至 **Administration > System > Maintenance > Patch Management > Install**。
步骤 3 点击 **Browse**，然后选择已从 Cisco.com 下载的补丁。
步骤 4 点击 **Install** 安装补丁。

在主要管理节点中安装补丁后，思科 ISE 将您注销，您必须等待几分钟，然后才能再次登录。

注：在补丁安装进行过程中，**Show Node Status** 是 Patch Management 页面上可访问的唯一功能。

步骤 5 导航至 **Administration** > **System** > **Maintenance** > **Patch Management** 以返回到 Patch Installation 页面。

有关 ISE 补丁的详细信息，请参考《ISE 1.3 管理指南》的安装软件补丁一节。

为访客接入配置 ISE

将无线控制器 (WLC) 配置为网络接入设备 (NAD)

步骤 1 登录到 **ISE Admin UI**。
步骤 2 导航至 **Administration > Network Resources > Network Devices**。
步骤 3 选择 **Add**，如图 23 所示。

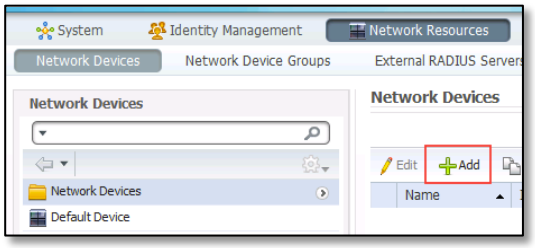


图 23. ISE 网络设备 - 添加设备

系统将显示 Network Devices 编辑页面，如图 24 所示。

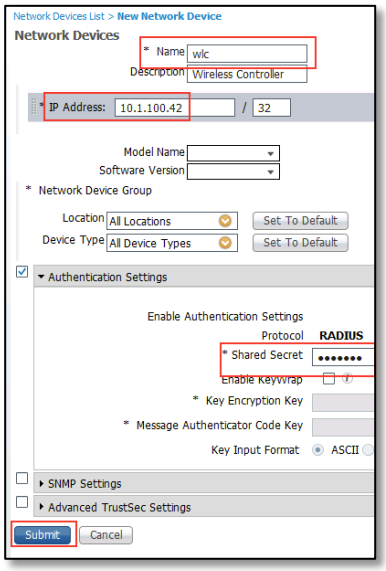


图 24. 网络设备

步骤 4 输入**设备名称**。
步骤 5 输入**设备 IP 地址**。
步骤 6 启用 **Authentication Settings**。
步骤 7 输入 **Shared Secret**（预检查表项目编号 - 12）。
步骤 8 点击 **Submit**。

身份验证策略设置

通过身份验证策略，您可以静态定义允许的协议以及思科 ISE 应该用于通信的身份源或身份源序列。默认情况下，思科 ISE 为访客接入提供预配置的适用身份验证策略。

查看默认身份验证策略

要查看预配置默认身份验证策略，请执行以下步骤。

步骤 1 登录到 **ISE Admin UI**。
步骤 2 导航至 Policy > Authentication。

系统将显示 Default Authentication Policy 页面，如图 25 所示。

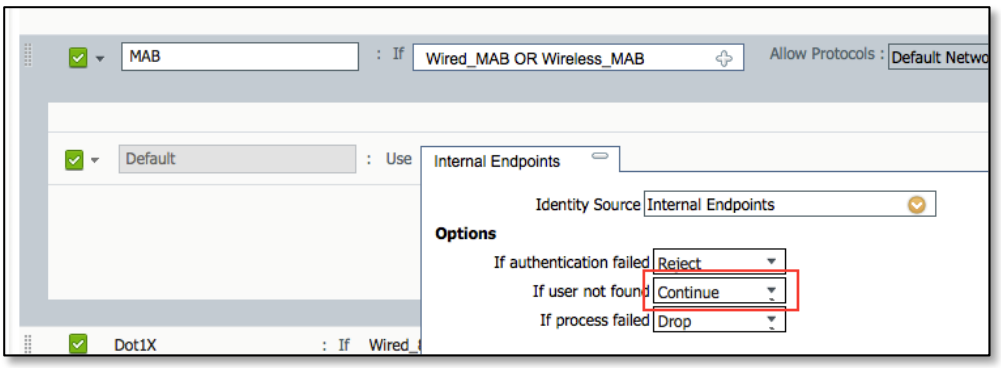


图 25. 默认身份验证策略

在默认身份验证策略中，未知内部终端的 **MAB** 设置为 **Continue**，这使访客终端（未知）能够继续进行身份验证并获得授权重定向到访客门户。

创建授权配置文件以将访客终端重定向到 ISE

当终端首先访问网络时，需要重定向到访客门户进行身份验证。处理该重定向需要授权配置文件。

步骤 1 导航至 **Policy** > **Policy Elements** > **Results**。
步骤 2 展开 **Authorization** 并点击 **Authorization Profiles**。
步骤 3 点击 **Add**。
步骤 4 输入以下信息：

- **Name**：Guest Redirect。
- 选中 **Web Redirection** 并选择**重定向类型**：Hotspot 或 Centralized Web Authentication（用于 Self-Registration 或 Sponsored Guest Flows）。
- **ACL**：ACL 区分大小写，并且必须与 WLC 中配置的名称相匹配。按照**“配置用于访客重定向的 ACL 并允许访问”**一节中的配置使用 **GUESTREDIRECT**。
- **Value**：选择相应的默认门户（Hotspot、Self-Registration 或 Sponsored）。

步骤 5 点击 **Submit**。

用于重定向的热点配置文件示例

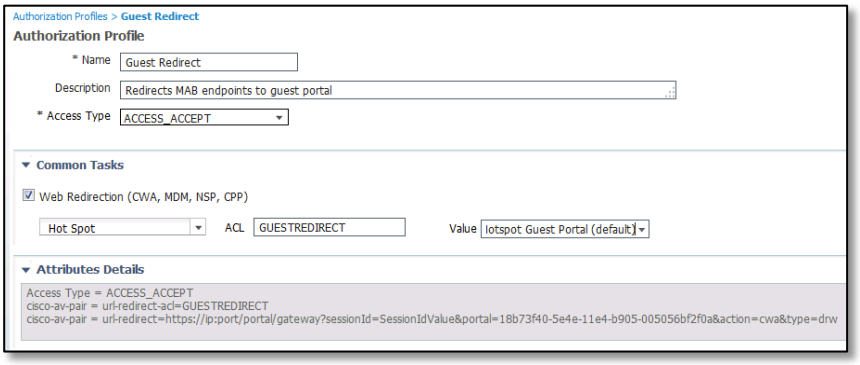


图 26. 授权配置文件 - 用于重定向的热点配置文件

凭证式重定向示例

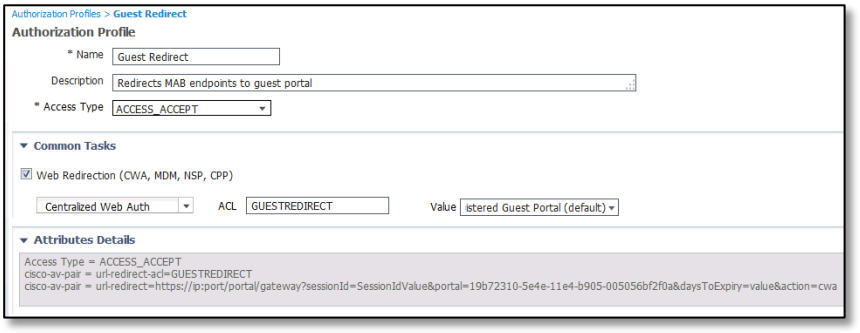


图 27. 授权配置文件 -- 凭证式重定向

创建授权配置文件以允许访问

在本节中，将会创建一个新授权配置文件，以在用户/设备进行身份验证后允许网络访问。

要创建授权配置文件以允许访问，请执行以下步骤。

步骤 1 导航至 **Policy** > **Policy Elements** > **Results**。
步骤 2 展开 **Authorization** 并点击 **Authorization Profiles**。
步骤 3 点击 **Add**。

系统将显示 New Authorization Profile 屏幕，如图 28 所示。

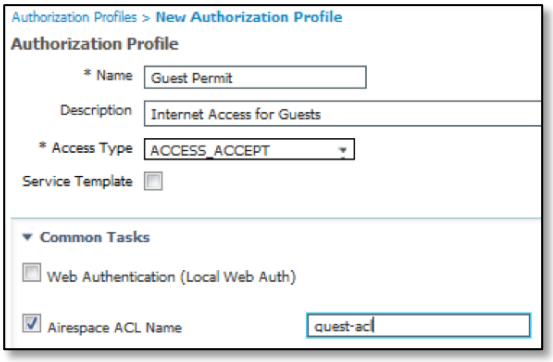


图 28. 新建授权配置文件

步骤 4 输入以下信息，如图所示：

- **Name**：Guest Permit
- **Description**：Internet Access for Guests
- 选中 **Airespace ACL Name** 并输入 **guest-acl**

注：ACL 区分大小写，并且必须与 WLC 中的定义**完全**匹配。此 ACL 是先前在“**配置用于访客重定向的 ACL 并允许访问**”一节中创建的。

步骤 5 点击 **Submit**。

为访客接入创建授权策略

创建必要的授权规则，促使重定向到访客门户。通过创建授权策略，还可以在设备或用户进行身份验证后根据终端组实现快速访问。

步骤 1 导航至 **Policy** > **Authorization**。
步骤 2 在 **Default** 规则行上点击 **Edit 旁边的箭头**。
步骤 3 插入 **New Rule Above**。
步骤 4 添加两个新规则以匹配您已设置的规则，如图 29 所示。

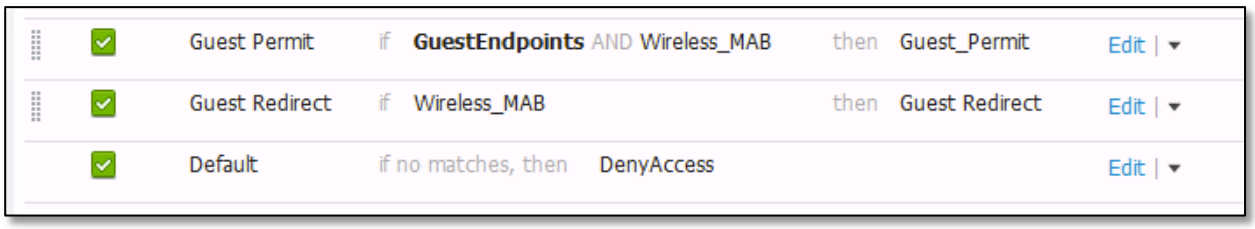


图 29. 授权策略 - 添加新规则

步骤 5 将第一个规则创建为重定向规则。
步骤 6 命名该规则：**Guest Redirect**。
步骤 7 选择 If **Wireless_MAB**。
步骤 8 选择 Authorization Profile **Standard** > **Guest Redirect**。
步骤 9 点击 **Done**。

步骤 10 在 **Guest Permit Rule** 上方插入其他规则。
步骤 11 命名该规则：**Guest Permit**。
步骤 12 选择 If **GuestEndpoint** and **Wireless_MAB**。
步骤 13 选择 **GuestPermit** 配置文件。
步骤 14 点击 **Done**。
步骤 15 点击 **Save**。

任何门户类型的配置流程都将显示一个页面，其中用户接受 AUP（热点）或登录到凭证门户。在任一流程中接受 AUP 之后，系统会将设备注册到 **GuestEndpoints** 中，并在 30 天内允许访问该设备而不再次进行重定向。30 天后，将从 **GuestEndpoints** 组中清除该设备，然后流程重复执行。

您刚完成的步骤是使门户启动并正常运行的必需步骤。

如果您使用热点门户进行访客接入，则可以跳至“**设置已知证书**”一节。

如果您使用自注册或赞助的门户，则需要另行配置。请继续执行下一节“**配置自注册和赞助的访客所需的设置**”。

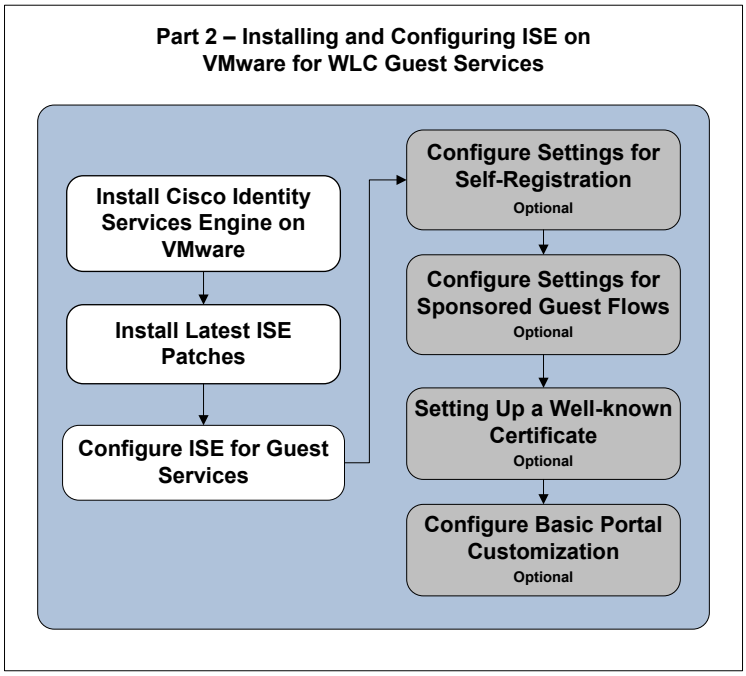


图 30. 第 2 部分：在 VMware 上为 WLC 访客服务安装和配置 ISE

配置自注册和赞助的访客流所需的最低设置（可选）

配置访客位置和时区

需要这些设置来支持自注册和赞助的访客流。您有必要设置访客接入网络所通过的位置，以便访客或发起人可以在帐户将要激活时轻松选择时区。如果没有配置位置，则帐户将不会在正确的时间激活。

为易于使用，如果仅有一个位置配置为在门户和发起人组中使用，则不会为访客和发起人提供用于选择位置的选项。

以 PST 时间进行的部署可以使用内置于系统中的 San Jose 位置，然后跳至**“配置赞助的访客流所需的设置”一节**。

您将无法更改默认的 San Jose 位置的名称。您无需删除该名称，因为如果不选择使用它，则其不会显示。

有关位置和 SSID 的详细信息，请点击此处访问本指南的对应小节。

要配置访客位置和时区，请执行以下步骤。

步骤 1 导航至 **Guest Access > Settings**。
步骤 2 展开 **Guest Locations and SSIDs**。
步骤 3 系统将显示 **The Guest Locations and SSIDs** 页面，如图 31 所示。

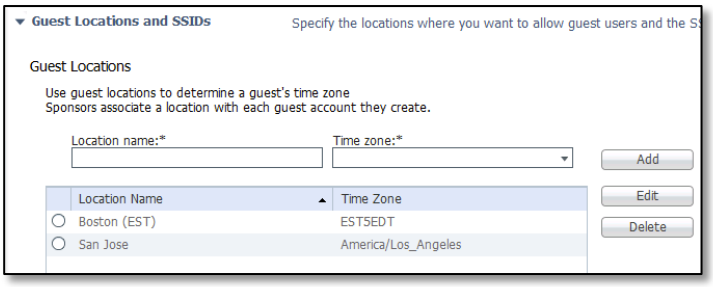


图 31.

步骤 4 在 **Location Name 和 Time zone** 中输入**位置名称和时区**。例如：使用 EST5EDT 的 Boston (EST)。

注：请保留 San Jose 位置。

步骤 5 点击 **Add**。
步骤 6 点击 **Save**。

配置门户以使用位置

您必须配置门户以使用此新添加的位置。

注：如果您同意使用 San Jose（PST 时间）作为默认值，则可以跳过本节。

步骤 1 导航至 **Guest Access > Configure > Guest Portals**。
步骤 2 选择您使用的门户（**Self-Registration 或 Sponsored Guest Portal**）。

步骤 3 折叠 **Portal Settings 和 Login page settings**。
步骤 4 在 Page Settings 下的 **Location** 中：添加已创建的位置，如图 32 所示。
步骤 5 点击 **Add**。
步骤 6 点击 **Submit**。

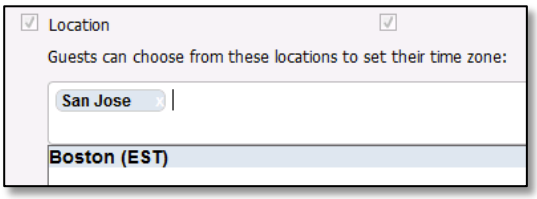


图 32. 访客门户 - 位置

配置赞助的访客流所需的设置（可选）

需要以下步骤来支持赞助的访客。如果您使用的只是 Self-Registration 门户，则设置完成后可以跳过此过程并移至“**设置已知证书**”一节。

设置发起人组

通过创建内部帐户或将 ISE 配置为与 Active Directory 集成，可以设置发起人。如果您与 Active Directory 集成，请跳过“**从 Active Directory 使用发起人帐户**”一节。

要创建内部帐户，请执行以下步骤。

步骤 1 导航至 **Administration > Identity Management > Identities > Users**。
步骤 2 点击 **Add**。
步骤 3 在 **Sponsor** 中填写发起人的信息。
步骤 4 在 **User Groups** 下选择 **ALL_ACCOUNTS**（默认）。
步骤 5 点击 **Submit**。
步骤 6 跳至“**配置发起人组的位置**”一节。

从 Active Directory 使用发起人帐户

仅在将访客接入系统与发起人组所在的 Active Directory 服务器集成的情况下，才需要查看下面两节。如果计划使用 ISE 上创建的发起人帐号（在上一节中完成），并且不希望将其与 AD 相结合，则可以向下跳至**配置发起人组的位置**。

有关详细信息，请参阅《ISE 配置指南》中的以 Active Directory 作为外部身份源。

要从 Active Directory 创建发起人帐户，请执行以下步骤。

步骤 1 导航至 **Administration > Identity Management > External Identity Sources**。
步骤 2 选择 **Active Directory**。
步骤 3 点击 **Add**，如图 33 所示。

图 33. 身份管理 - 外部身份源

步骤 4 输入 Join Point 的**名称**。
步骤 5 输入 **AD 域**。
步骤 6 点击 **Submit**。

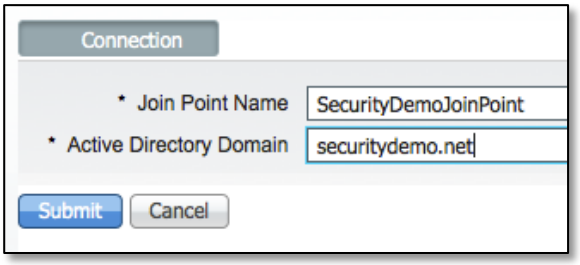


图 34. Active Directory

步骤 7 点击 **Groups** 选项卡。

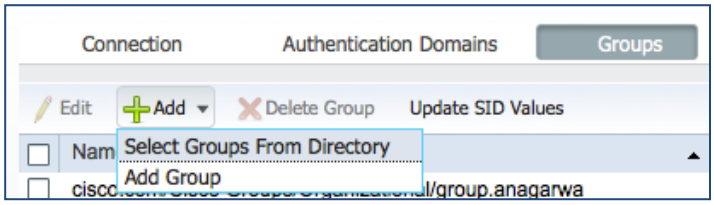


图 35. Groups 选项卡

步骤 8 点击 **Add**，Select **Groups from Directory**。
步骤 9 在选择组后，点击页面底部的 **OK**。
步骤 10 点击页面底部的 **Save**。

在 All_Accounts 中设置 Active Directory 发起人组

以下步骤显示如何将包含发起人或员工的组与发起人组相关联。在本示例中，我们使用的是域用户。

步骤 1 导航至 **Guest Access > Configure**。
步骤 2 点击 **Sponsor Groups > ALL_ACCOUNTS**。

系统将显示 Sponsor Group 页面，如图 36 所示。

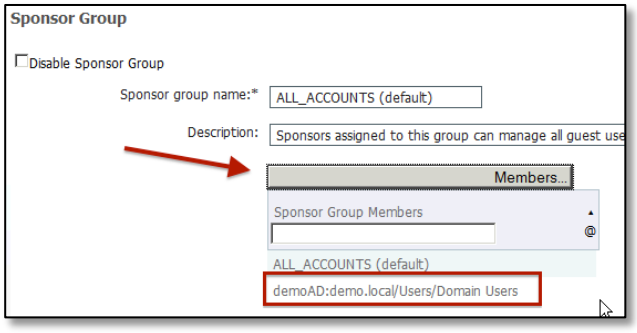


图 36. Sponsor Group 页面

步骤 3 点击 **Member** 并将域用户转移到 **Selected User Groups** 区域，如图 37 所示。

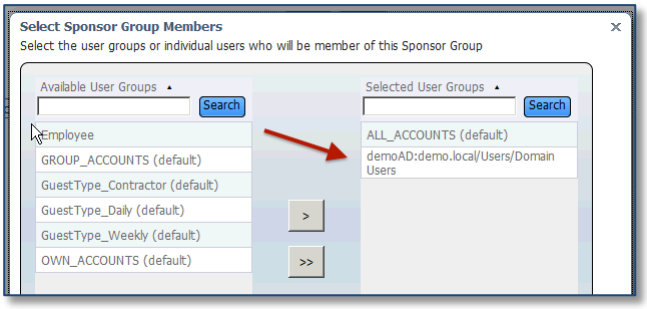


图 37. 所选用户组

步骤 4 点击 **OK**。

配置发起人组的位置

务必配置正确的位置，以便在发起人创建访客帐户时使用。如果您同意使用 San Jose 位置，则可以跳过本节。否则，请添加新位置。

步骤 1 从 **Select the locations that guests will be visiting** 部分中选择您希望访客使用的位置，如图 38 所示。
步骤 2 删除不需要的位置。

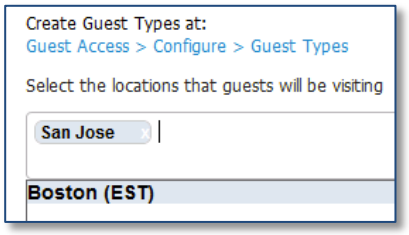


图 38. Select the locations that guests will be visiting 窗格

步骤 3 滚动到页面顶部，然后点击 **Save**。
步骤 4 点击 **Close**。

设置基于 ISE 发起人门户 FQDN 的访问

通过发起人门户，发起人可以为访客、访问者、承包商、顾问或客户创建临时帐户，以执行 HTTP 或 HTTPS 登录来获得网络访问权限。网络可以是公司网络，或者访问权限可以提供对互联网的访问。

通过 ISE 管理 UI 访问发起人门户而不进行任何特殊配置有两种方法。

- **Manage Accounts 按钮 -** 这为管理员保留
- **门户测试 URL -** 此 URL 可以发送到发起人，以便其能够轻松使用站点书签 -（默认）

建议为发起人提供轻松的发起人门户 URL。示例如下：http://sponsorportal.yourcompany.com

要设置 ISE 发起人门户，请执行以下步骤。

步骤 1 导航至 **Guest Access** > **Configure** > **Sponsor Portals**。
步骤 2 点击 **default Sponsor portal**，系统将显示 Portal Settings 窗格，如图 39 所示。
步骤 3 在 **Portal Settings** 下找到 **Fully Qualified Domain Name (FQDN)** 部分并输入“sponsorportal.yourcompany.com”。

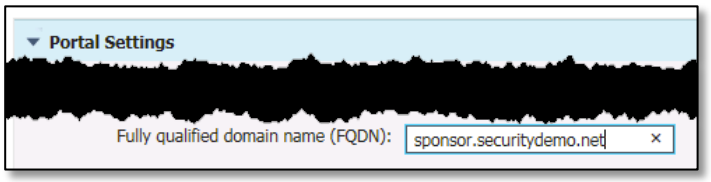


图 39. 门户设置

步骤 4 滚动到页面顶部并点击 **Save**。

现在，您需要更新 **DNS**，以确保此 **FQDN** 解析为 ISE IP 地址。通过使用将 sponsorportal.yourcompany.com 指向 yourise.yourcompany.com 的 CNAME 别名，可以实现此目的。

有关详细信息，请参阅《ISE 1.3 门户用户指南》的支持访客一节。

设置已知证书（可选）

本节中的信息使用 ISE 1.3 开发而成。版本 1.4 的“设置已知证书”工作流程可能略有不同。

无需执行下一节的操作，即可使系统启动并正常运行，以便进行访客接入。它是可选步骤，但强烈推荐执行该步骤。要确保用户在通过其 Web 浏览器连接到访客、发起人或管理员门户时不必接受无效的证书，您应该对 ISE 服务器使用已由已知证书颁发机构签名的证书。

如果您想要暂时跳过本节，则可以在完成最低设置时继续转至**后续内容**一节。

SSL.com 是完全支持本指南中推荐的证书类型的已知供应商，但是存在其他可能适用的提供商。

注：每位证书提供商都可能引用具有不同名称的证书类型。它通常帮助致电公司或使用其在线 Web 聊天来说明 SAN 字段需要的信息。告诉它们您正在 SAN 字段中查找包含通配符和 FQDN 的证书，其中 FQDN 包含在 CN= 字段中。

有关通配证书和一般证书的详细信息，请参考以下文档：

- ISE 管理员指南 - 思科 ISE 中的通配证书支持
- 移动包条款 - 当 SSL 证书通配时
- Aaron Woland 网络世界博客 - 通配证书以及如何用于 ISE

下一过程中所列的步骤显示从 SSL.com（从属于 Comodo）使用 SAN 中的通配符设置统一通信证书 (UCC) 的示例。

创建证书签名请求并将 CSR 提交给证书颁发机构

步骤 1 导航至 **Administration > System > Certificates > Certificate Signing Requests**。

步骤 2 输入用于生成 **CSR** 的**值**，如图 40 所示。

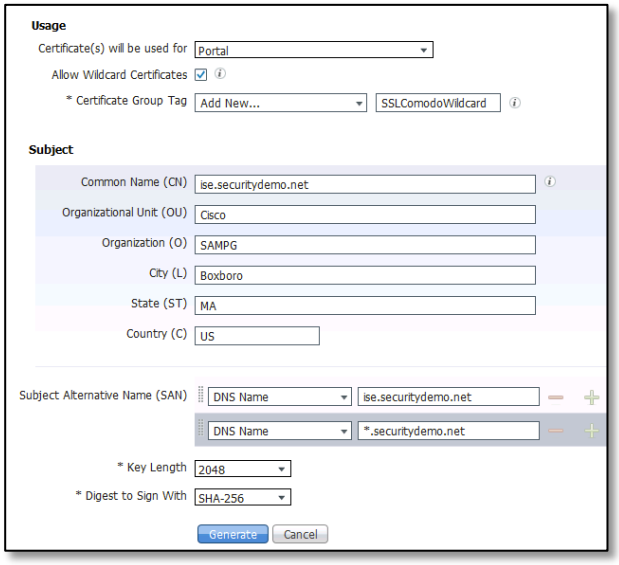


图 40. 证书签名请求

Usage

- Certificate(s) will be used for：**Portal**
- Allow Wildcard Certificates：**已选中**
- Certificate Group Tag：**Add New -** 为其提供名称：例如 SSLComodoWildcard

Subject

- Common name：**yourdomain.com**
- 根据组织将该主题的其他部分替换为相应的信息
- Subject Alternative Name (SAN)=
  SAN DNS Name 1 = yourise.yourcompany.com
  SAN DNS Name 2 = *.yourcompany.com
- 将最后两个字段保留为默认值

步骤 3 点击 **Generate** 生成 CSR。系统将生成 CSR，如图 41 所示。

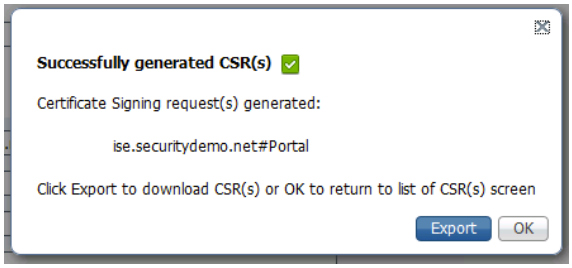


图 41. 已成功生成 CSR

步骤 4 点击 **Export** 保存文件。

步骤 5 在文本编辑器中打开**文件**。

步骤 6 从“---- BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST----”**复制所有文本**。

步骤 7 将 **CSR** 的内容粘贴到所选 CA 的证书请求中。

图 41 显示 SSL.com 门户。

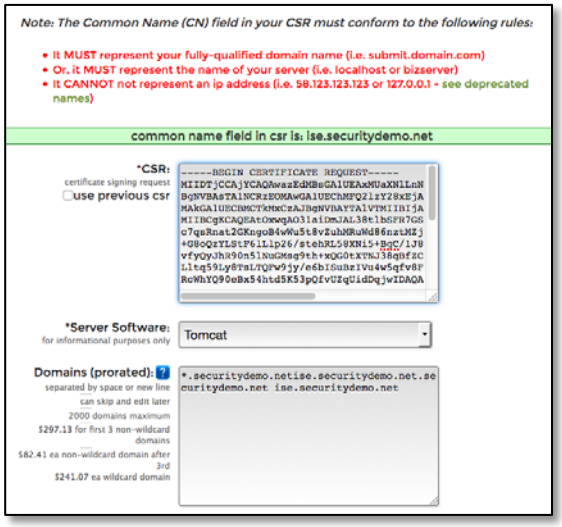


图 42. SSL.com 门户

步骤 8 下载**签名证书**。

注：某些 CA 可能会将签名证书通过电子邮件发送给您。生成的下载或电子邮件附件通常采用 zip 文件形式，其中包含必须添加到思科 ISE 受信任证书库的 CA 新签名证书和公共签名证书。将数字签名证书、根 CA 证书和其他中间 CA 证书（如果适用）保存到运行客户端浏览器（在后续部分中将导入）的本地系统中。

将证书导入到受信任证书库

在本节中，将会导入必要的证书，以使客户端和服务器通信能够受信任。除服务器证书以外，ISE 在通信时还会向客户端提供根证书和中间证书（如果需要）。

注：并非所有运营商都具有要求安装的中间证书。中间证书来自从属 CA。此示例使用的是从属于 Comodo 的 SSL.com。Comodo 从属于 AddTrust 根 CA。因此，示例导入的是根证书以及两个从属证书。

要导入全部三个证书，请执行以下步骤。

步骤 1 导航至 **Administration > System > Certificates > Trusted Certificates**。
步骤 2 点击 **Import**。

- 根 CA：AddTrustExternalCARoot.crt
- 从属 CA：SSLcomDVCA_2.crt
- 从属 CA：USERTrustRSAAddTrustCA.crt

步骤 3 系统将显示 Import a new Certificate into the Certificate Store 窗格，如图 43 所示。

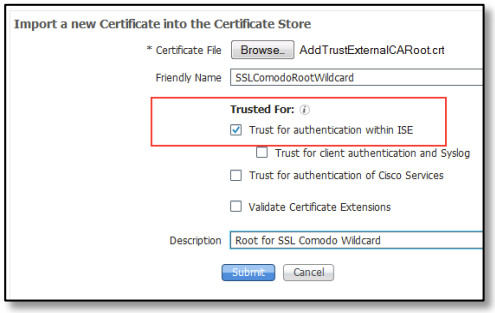


图 43. Import a new Certificate into the Certificate Store 窗格

步骤 4 使用以下步骤（**4 至 9**）导入下列证书：

- **根 CA**：AddTrustExternalCARoot.crt
- **从属 CA**：SSLcomDVCA_2.crt
- **从属 CA**：USERTrustRSAAddTrustCA.crt

步骤 5 点击 **Browse** 选择**根 CA 证书**。
步骤 6 在 **Friendly Name** 中输入友好的名称。
步骤 7 选择 CA **返回的根证书**。
步骤 8 点击 **Trusted for** 标签下的 Trust for Authentication within ISE 复选框。
步骤 9 输入**描述**。
步骤 10 点击 **Submit**。

将 CA 签名的证书绑定到签名请求

现在，您已收到 CA 返回的数字签名证书并导入 CA 证书，下一步是从 ISE 将由 CA 签名的证书绑定到 CSR，从而将证书与用于生成 CSR 的私钥配对。

步骤 1 导航至 **Administration > System > Certificates > Certificate Signing Requests**。
步骤 2 选择**签名请求的对应条目**。
步骤 3 点击 **Bind Certificate**，如图 44 所示。

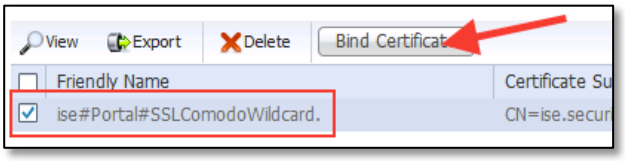


图 44. 绑定证书

步骤 4 点击 **Browse** 选择 CA 签名的证书。
步骤 5 为证书指定 **Friendly Name**。
步骤 6 选中 **Allow Wildcard Certificates** 复选框以绑定证书，该证书在 **Subject Alternative Name** 中的 **Subject** 或 **DNS** 中的任何 **CN** 内都包含通配符，即星号 (*)。
步骤 7 系统将自动配置其他选项。
步骤 8 点击 **Submit** 以绑定 CA 签名的证书，如图 45 所示。

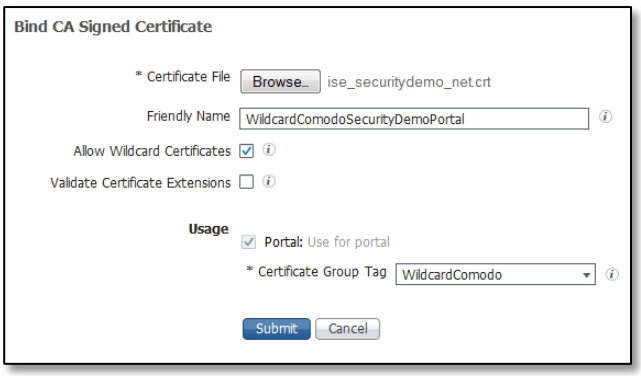


图 45. 绑定已签名的证书

将证书编辑用于管理员门户和 EAP 身份验证

此步骤是可选的。如果您想要在访问 ISE 管理员门户时也使用已知证书，从而获得更好的用户体验（不会要求用户安装或信任自签名证书）或未来扩展到 dot1x 客户端，请遵循以下步骤。执行绑定操作后，需要返回并编辑证书以更新其用途。

要编辑证书，以便用于管理员门户和 EAP 身份验证，请执行以下步骤。

步骤 1 导航至 **Administration > System > Certificates > System Certificates**。

步骤 2 编辑**最近导入的证书：**SSLComodoWizard，如图 46 所示。

图 46. System Certificate 窗格

步骤 3 通过选中 **EAP Authentication 和 Admin** 的复选框来编辑用途选项，如图 47 所示。

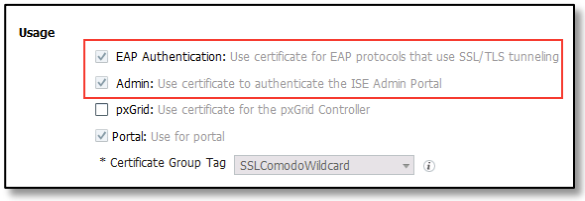


图 47. Usage 窗格

步骤 4 点击 **Submit**。

ISE 系统将重新启动。

您已完成使用已知证书设置 ISE 的过程。

有关处理证书的详细信息，请参考《ISE 1.3 管理指南》的管理证书一节。

将门户设置为使用已知证书

现在，您已设置已知证书，需要将其分配给访客门户，从而在与访客设备通信时使用。进行此更改会影响您已设置的所有其他门户。如果您使用的是发起人门户，则此操作还会更新门户，因此无需在该门户上进行更改。

步骤 1 登录到 **ISE 管理员门户**。

步骤 2 导航至 **Guest Access > Configure > Guest Portals**。

步骤 3 点击您使用的默认访客门户：**Hotspot**、**Self-Registered** 或 **Sponsored**。

步骤 4 选择当处理 **Portal Settings** 窗格下的下拉菜单中的已知证书时，在步骤中设置的 **Certificate group tag**，如图 48 所示。

图 48. Portal Settings 窗格

步骤 5 滚动到**页面顶部**并点击 **Save**。

步骤 6 当系统询问“**Do you want to change the certificate for all the portals on the same port?**”时，按 **OK** 继续操作。

步骤 7 点击页面顶部的 **Close**。

配置基本门户定制（可选）

无需执行下一节的操作，即可使系统启动并正常运行，以便进行访客接入。此操作是可选步骤，有助于用户熟悉新访客门户的基本定制选项。

要定制访客门户，请执行以下步骤。

步骤 1 点击 Guest **Access → Configure → Guest Portals**。

步骤 2 点击您使用的门户（**Hotspot、Self-Registered 或 Sponsored**）以编辑该门户。

处于活动状态的门户显示为具有**绿色圆圈的复选标记**，如图 49 所示。

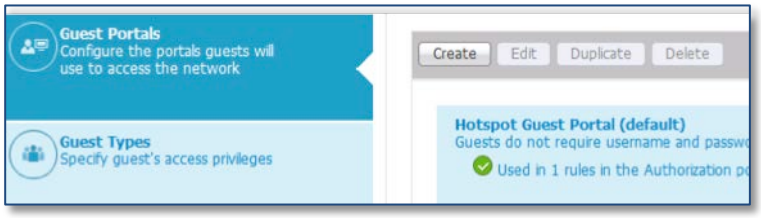


图 49. Hotspot Guest Portal

步骤 3 点击页面顶部的 **Page Customization** 部分，如图 50 所示。

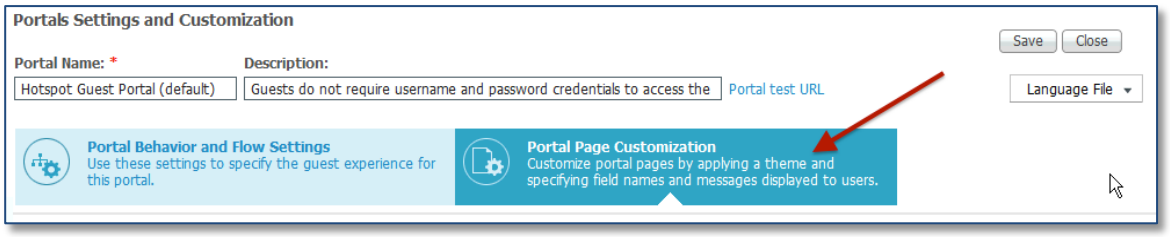


图 50. Portals Settings and Customization 页面

ISE 1.3 为您提供直接内置于产品的基本定制功能。通过定制，还可更轻松地实时查看您所做的更改。本文档不会详细介绍所有这些项目，但是您可以从页面顶部开始查看，因为在此处可以更改诸如徽标、横幅和正文等组成部分。您还可以选择一些内置颜色主题。

步骤 4 要更改门户的主题颜色，请使用内置 **Portal Theme** 或使用 **Tweaks** 修改颜色，如图 51 所示。

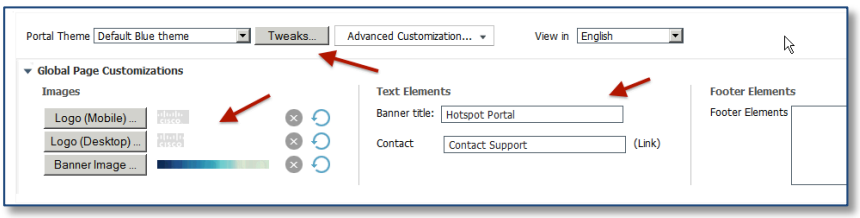


图 51. 页面定制选项

步骤 5 您可以上传用于门户的**徽标**和**横幅**。

在此主要部分下，您不但可以调整整体外观和风格，还可以进入各个页面。根据门户设置和门户类型，在页面左侧会显示不同的选项。可以在页面上的不同区域中调整文本。

此外还有微缩预览功能，用于显示您对门户的更改。

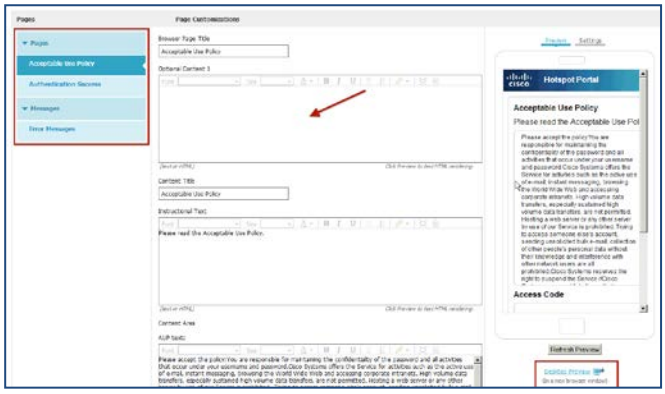


图 52. 门户定制 - 微缩预览

步骤 6 完成一些基本定制后，通过点击微缩预览右下方的选项，查看 **desktop preview**（与页面顶部的门户测试 URL 相同）。

注：您也可以通过使用页面顶部的**门户测试 URL**（而不使用实际客户端）来测试用户将执行的完整流程。

步骤 7 关闭桌面预览浏览器窗口。

步骤 8 点击页面顶部的 **Save**。如图 53 所示。

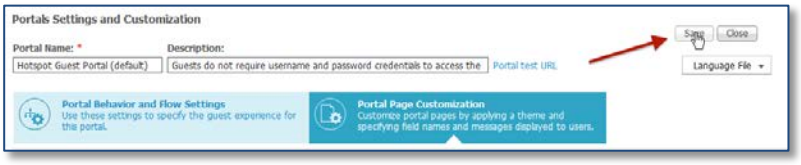


图 53. 保存门户页面定制

有关访客定制的详细信息，请参考管理员指南的定制最终用户 Web 门户一节。

至此，使用 ISE 1.3 安装思科无线访客接入的过程已完成！

后续内容

有关其他配置选项，请参阅位于 http://www.cisco.com/go/ise 的思科 ISE 文档。

附录 A - 交换机配置

以下是交换机配置文件的示例。

```
hostname 3560CG
!
vlan 50
 name GUEST
!
vlan 100
 name Mgmt
!
interface GigabitEthernet0/1
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/7
 switchport access vlan 90
 switchport mode access
!
interface GigabitEthernet0/8
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/9
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan50
 ip address 10.1.50.1 255.255.255.0
 ip helper-address 10.1.100.10
!
interface Vlan100
 ip address 10.1.100.1 255.255.25
```