

Cisco ISE 1.3 v1.1 – Guest Access Management

Last Updated: 14-04-2015

关于此演示

这个篇章将帮助你演示几个 Cisco 访客接入解决方案，应用在 Cisco Identity Service Engine 的无线技术连接，并包括以下几个特定的情景.

- 使用无线热点接入访客网络
- 自行注册访客网络接入，需要主办方 SMS 和邮件访客证书说明的批准
- 主办访客网络接入，需要 SMS 和邮件访客证书说明
- 使用大量引入特征来展现 ISE 中的多个访客账户

表格内容

情景 1: 使用热点访客网络接入

- 接入网络热点
- 演示 ISE 中的基础热点流程

情景 2: 使用主办批准，自行注册访客接入

- 清楚设备
- 自行注册设备
- 关闭访客注册批准
- 批注访客注册请求
- 接入访客网络
- 演示 ISE 中的自行注册访客流程

情景 3: 主办批准的访客接入

- 清除设备
- 创建访客账户
- 在 ISE 中演示主办访客流程
- 在 Bulk 中创建访客账户

演示要求

下面的表格列出了预设置演示的要求

Table 1. 演示要求

必须的	可选的
建议终点路径 <ul style="list-style-type: none"> 819W router, registered and configured for dCloud 主控制工作站 <ul style="list-style-type: none"> 使用 AnyConnect 手提电脑 用户设备 <ul style="list-style-type: none"> Tablets 智能手机 手提电脑 	支持终点路径/AP <ul style="list-style-type: none"> 路由器, 注册并配置的 dCloud Cisco Aironet Series Access Point (3000, 2700, 2000 or 1000 series)

备注: 如果你登录一个手提电脑, 那就需要两个手提电脑。一个用来通过 RDP 接入 dCloud Workstations1 来展示 ISE UI 和其他演示特征。另一个手提电脑将用来演示接入在这个演示中的热点或者访客网络

演示设置

所有接入组件所需要的信息位于你激活的演示的拓扑和服务器菜单

拓扑菜单: 点击拓扑中的任意服务器, 挑出一个窗口, 含有可选择的服务器操作



服务器菜单: 点击任何服务器名字边上的  或者  按钮, 来显示可选择的服务器操作和凭证

Table 2. 演示服务器和证书

设备	IP Address	Access Method	Username	Password
Prime Infrastructure	198.18.133.65	Workstation1 Browser	admin	C1sco12345
vWLC	Private: 198.19.11.10	Workstation1 Browser	Session Owner	Session ID
	Public: See Session Details	Local Browser		
Workstation1	198.18.133.36	WebRDP or AnyConnect	administrator	C1sco12345
Exchange Server	198.18.133.2	WebRDP or AnyConnect	administrator	C1sco12345
AD1	198.18.133.1	WebRDP or AnyConnect	administrator	C1sco12345
Portals	198.18.133.110	Putty	linuxuser	C1sco12345
ISE	198.18.133.27	Workstation1 Browser	admin	C1sco12345

Table 3. 可利用的 Portals

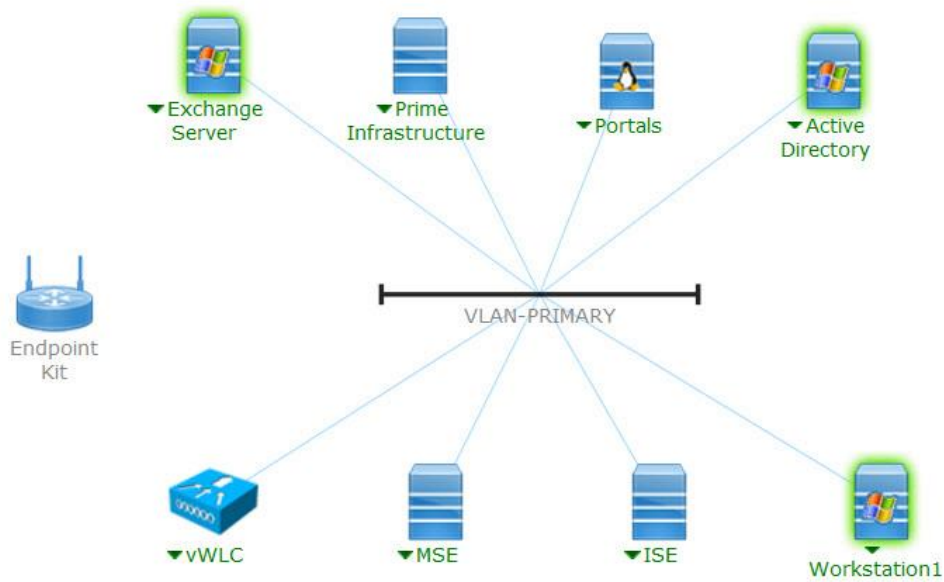
Scenario / Vertical	Main Portal URL	Sponsor Portal URL
Default / dCloud	N/A	http://sponsor.dcloud.cisco.com
Healthcare	http://health.dcloud.cisco.com	http://sponsor-health.dcloud.cisco.com
Education	http://edu.dcloud.cisco.com	http://sponsor-edu.dcloud.cisco.com
Federal	http://federal.dcloud.cisco.com	http://sponsor-fed.dcloud.cisco.com
Corporate	http://corp.dcloud.cisco.com	http://sponsor-corp.dcloud.cisco.com

Table 4. 登陆的信息以及访问的权限

Scenario / Vertical	Username	Password	Access Level
Healthcare	doctor	C1sco12345	Tier 1 - Full Access
Healthcare	nurse	C1sco12345	Tier 2 - Limited Access
Education	dean	C1sco12345	Tier 1 - Full Access
Education	professor	C1sco12345	Tier 2 - Limited Access
Federal	captain	C1sco12345	Tier 1 - Full Access
Federal	officer	C1sco12345	Tier 2 - Limited Access
Corporate	manager	C1sco12345	Tier 1 - Full Access
Corporate	employee	C1sco12345	Tier 2 - Limited Access
N/A	itadmin	C1sco12345	Full demo access

演示拓扑

这个演示是在一个完全虚拟的环境下运行的。很多组件是使用行政级别账户来完全设置的。行政账户细节被包括在相关的篇章步骤中。

Figure 1. 演示拓扑结构

演示准备

演示前

我们强烈推荐你至少回顾此流程一次，在给听众做演示前。这将使你能熟悉文件和演示的结构

准备是做客户演讲的成功关键

以下步骤罗列了你的演示和你的演示环境的设置

为了演示需求条款以及完全接入后台演示组件，终点 AP 必须被设置为连接并在你的激活演示部分操作。使用一个终点路径（由你提供）使这个过程简单并容易，在初设置以后。

如果你没有使用一个终点路径，你的每个演示接入点每次都需注册，因为 WLC IP 地址是唯一的。

预约演示

1. 浏览 dcloud.cisco.com 来接入 dCloud UI 并使用你的 Cisco.com 证书登录
2. 登录并设置你的终点路径，如果这是你第一次使用你的 dCloud 路径[如何操作]
3. 预约一个演示[如何操作]
4. 从你的演示地址测试你的带宽，在操作任何一个演示篇章之前[如何操作]
5. Verify your demonstration has a status of under on the page in the dCloud UI.


验证你的演示有一个激活（Active）状态，在 dCloud UI 的 My Demonstrations 的 My Dashboard 网页

- 大约需要 15 分钟的时间来激活你的演示

连接到 WORKSTATION1

6. 使用以下操作之一连接到 Workstation1
 - 使用 webRDP [如何操作] 或者
 - 使用 Cisco AnyConnect（强烈推荐）[如何操作]
 - 通过 Anyconnect 连接到演示后，使用你的本地 RDP 客户来连接至 Workstations，位置在 198.18.133.36。登录（管理者/Cisco12345）。
 - 打开 Workstation1 的 Firefox。你的主页设置在 <http://topo.dcloud.cisco.com>，将允许你浏览拓扑和链接到后台演示组件。点击浏览模式的 home 按钮，如果你需要回到拓扑屏幕。

配置终端设备

7. 在 Workstation1，确保你的 Country 是激活的，在 Cisco Wireless Controller（WLC）的演示中[如何操作 

备注：WLC 这个演示的登录需要阶段特定证书（session specific credentials）。username 是你的 dcloud username，password 是你的会议 session ID。你可以从你的激活演示的会议细节部分获得这个信息。


备注：如果你的用户名含有无效字符，例如@，你的登录将失败。已提供“dcloud”一类的用户姓名，如果需要的话还可以用做独特的 Session ID 作为密码。

Figure 2. 登录 WLC1 证书

Session Details	
Demo Configuration	
Session ID:	64960
End Time :	11/14/2014 00:15:00
Owner:	arobotti
Last Modified:	10/27/2014
VPN Available:	true
Endpoint Routers:	AR-819W

password

username

8. 你的 3000, 27000, 2000, 或者 1000 Series AP 条款 [如何操作 

备注：如果使用终点路径，这一步只需要完成一次。当使用这些演示时强烈推荐这个步骤。没有终点路径，AP 必须使用新的演示 WLC IP 地址再做规划，当你每次计划一个新的演示时。

9. 在 FlexConnect 模式中设置你的 AP
- WLC 点击 Wireless，在顶部
 - 点击你的 AP

Figure 3. 终点路径 AP 显示在 WLC 的无线项

MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
All APs								
Current Filter		None		[Change Filter] [Clear Filter]				
Number of APs		1						
AP Name	IP Address(Ipv4/Ipv6)	AP Model						
AP501c.bfa3.077a	174.97.231.254	AP802H-AGN-A-K9						

- 点击 General 项
- 确保 AP 模式设置在 FlexConnect，点击 Apply


Figure 4. AP 模式-FlexConnect


All APs > Details for AP501c.bfa3.077a

General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
General			Versions			
AP Name	AP501c.bfa3.077a		Primary Software Version	8.0.100.0		
Location	default location		Backup Software Version	0.0.0.0		
AP MAC Address	50:1c:bf:a3:07:7a		Predownload Status	None		
Base Radio MAC	74:26:ac:77:7c:60		Predownloaded Version	None		
Admin Status	Disable ▾		Predownload Next Retry Time	NA		
AP Mode	FlexConnect ▾		Predownload Retry Count	NA		
AP Sub Mode	None ▾		Boot Version	12.4.25.1		
Operational Status	REG		IOS Version	15.3(3)JA\$		
Port Number	1		Mini IOS Version	0.0.0.0		
Venue Group	Unspecified ▾		IP Config			
Venue Type	Unspecified ▾		DHCP Ipv4 Address	10.66.108.164		
Venue Name			Static IP (Ipv4/Ipv6)	<input type="checkbox"/>		
Language			Time Statistics			
GPS Location			UP Time	0 d, 03 h 08 m 19 s		
GPS Present	No		Controller Associated Time	0 d, 03 h 05 m 34 s		
			Controller Association Latency	0 d, 00 h 02 m 44 s		
Hardware Reset			Set to Factory Defaults			
Perform a hardware reset on this AP			Clear configuration on this AP and reset it to factory defaults			
<input type="button" value="Reset AP Now"/>			<input type="button" value="Clear All Config"/>			
			<input type="button" value="Clear Config Except Static IP"/>			



备注：如果你的 AP 没有被设置在 FlexConnect 模式，你将看不到播放任何的 SSIDs，即使你成功注册到控制器！

确认演示是否准备好

10. 确认你的 AP 是可操作的。[如何操作 

- 你现在完成通过 AP 连接工作站 1 的操作。[如何操作 

11. 基于你演示的位置，你需要完成额外的演示准备

- 在 Cisco Office 地址完成额外的演示准备[如何操作 
- 在 Customer Site 完成额外的演示准备[如何操作 



这个演示在 4 个纵向（公共卫生，教育，联邦政府和公司）明确地设计了很多为客户设立的端口，以及默认的 dcloud 带宽端口。如果你为客户运行此演示的 4 个纵向之一，并希望利用客户设计端口进入这个演示，请参见 Cisco ISE 端口管理 [Americas] 演示指南。在 ISE UI 的 3 个简单改变中，你可以使用为客户设计的端口运行以下演示章节。在进一步使用时，请确认使用 Cisco ISE 端口管理演示指南定制你的演示。如果你不希望改变默认 dCloud 带宽端口，请继续以下第一章节。

Scenario 1. 热点接入访客网络接入

在这个章节中，机构只需要给访客接入网络，并不希望访客在 BYOD 在线，授权访客接入或者自定义访客接入进行更复杂的步骤。例如，一个咖啡店或者酒店只想给访客提供热点网络接入，但不希望访客进入注册流程。在这个章节，你将使用一个终端设备连接一个热点无线网络，并演示这个设备有网络连接，并能连接到主要的 Table 3 中罗列的纵向端口页。

演示步骤

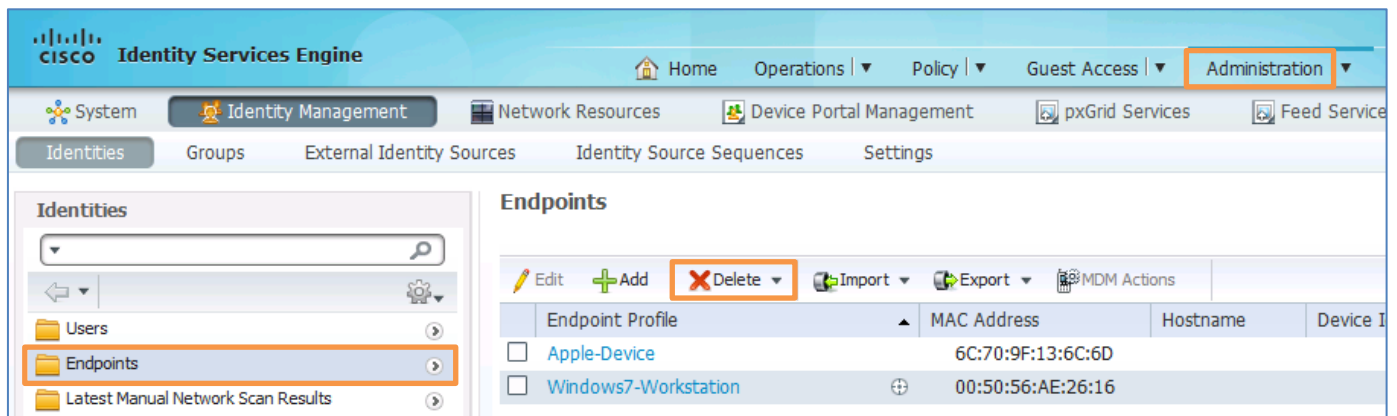
连接网络热点

1. 清除在演示中使用的每个个人设备的设置。如果设备设置没有被清除，你可能不会被重导至访客端口或者其他需要的页面
 - a. 清除 Web Cache [如何操作 
 - b. 清除 Personal Device Settings [如何操作 

备注：运行步骤 2-10 如果你已经完成 Cisco ISE 1.3 设备登录和管理 [Americas] 演示指南。如果你没有完成那个章节，直接跳到步骤 11.

2. 从 Workstation1 打开 Firefox，并在 <https://ise.dcloud.cisco.com> 登录 ISE。你可以键入地址，或者登录 ISE 通过点击 ISE 图标在拓扑主页，或者登录 ISE 书签在书签工具栏。登录 (admin/C1sco12345)。
 - 手动在地址栏输入 URL.
 - 在拓扑工具栏点击 ISE 图标.
 - 访问收藏栏的 ISE 链接.
3. 移动你的鼠标至 administration。在身份管理，点击 Identities。
4. 点击左手边的 Endpoints
5. 选择所有的终点，并点击 Delete，然后 Delete Selected。 选择 Yes 当被问到你是否想删除终点时。

Figure 5. Deleting an Endpoint from ISE 从 ISE 删除一个终点



6. 登录 <http://wlcl.dcloud.cisco.com> 页，从 Workstation1 接入 WLC。你可以用几种不同的方法做这一步：
 - 在地址栏手工键入地址
 - 在书签工具栏点击 WLC1 的书签
 - 点击浏览模式的主页键，回到拓扑图，然后点击 vWLC。

- a. 登录 vWLC，使用同样的你在演示准备步骤 7 获得的设备制定证书
- b. 点击 MONITOR，然后点击左手边的 Clients
- c. 你应该可以看见已经加入热点的任一客户。移到右边，移动鼠标到下拉箭头直到其展开，然后点击 Remove

Figure 6. 从 WLC 删除一个客户

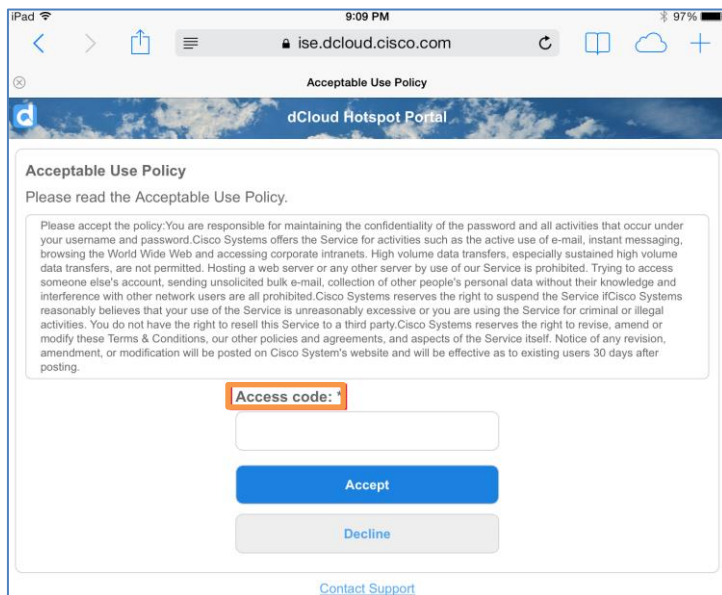


7. 连接用户设备至开放无线 SSID **dCloud-Hotspot**。
8. 打开用户设备的支持的，已内置的网络浏览器，并且使用 HTTP 来浏览任何一个网页。

备注：确认当打开浏览器时，你可使用 HTTP 连接一个页面。如果你使用 HTTPS 连接一个页面，你将不会被重导至热点端口。这是因为在现在的 WLC 的号码中有一个缺陷，不能操作 HTTPS 重导。

9. 如果跳出安全窗口，点击 Continue。你将被重导至 dcloud 热点端口，在那里将呈现一个可接受的使用策略（AUP），并提示需要接入代码

Figure 7. dCloud 热点端口



备注：在 ISE 需要一个热点接入代码完全是一个随机设置。一些结构希望提供完全的不需要输入代码的开放式网络热点接入，而有一些更倾向于需要一个接入代码来保障基础安全。ISE 是很有弹性的，并且可以根据客户需要来设置任一方式。

10. 输入 dcloud 作为 Access Code，点击 Accept。在接受 AUP 后，你的设备将被自动重导至 <http://www.cisco.com>。这演示了你的设备已连接网络-你不需要输入登录证书。

11. 参考 Table 3，找到你的章节（公共卫生，教育，联邦政府或者公司）的主要端口页面
12. 浏览表中列举的主要端口页面（例如 <http://health.dcloud.cisco.com>）
13. 演示用户现在接入了主要端口页面以及 General Resources，但未接入 Internal Resources 或者 My Registered Devices 页面。

Figure 8. 公共安全连接中心 - <http://health.dcloud.cisco.com>

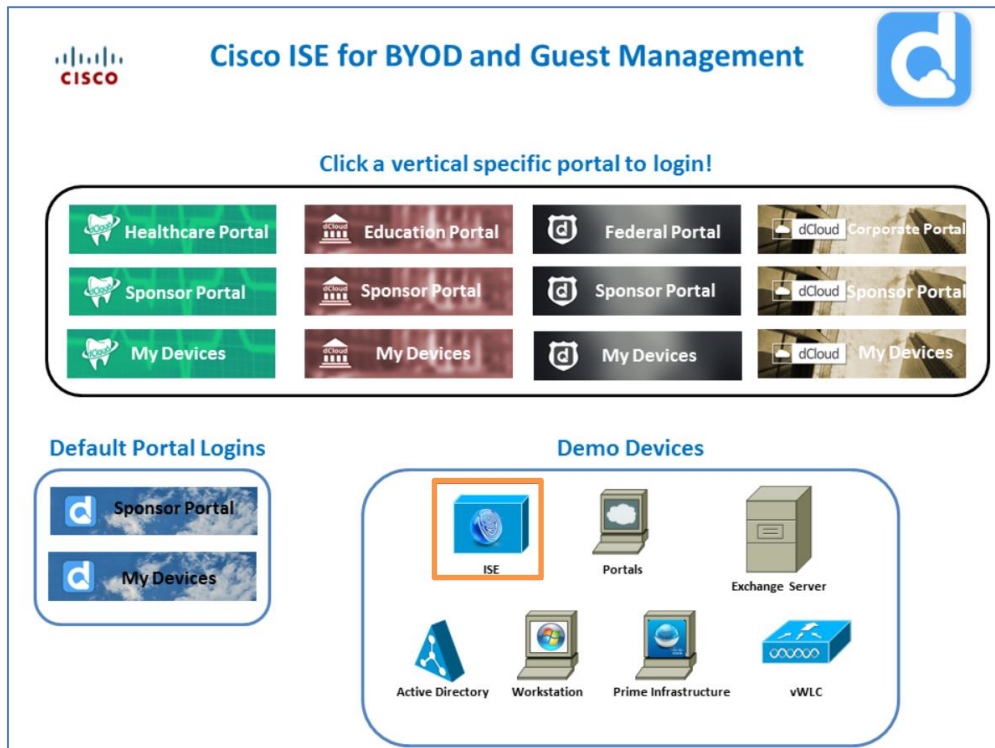


演示 ISE 中的基本热点流程

这个设备已经成功加入热点，并且已经连接网络。下一步，我们将简单的看一下 ISE UI，来演示如何 ISE 的基本内容：

- 设备的动态简介
 - 应用合适的授权文件；并且
 - 动态允许访客网络接入。
1. 在 Workstation1，在电脑上运行 Firefox，然后使用 admin/Cisco12345 和以下任意一个方法登陆 ISE，<https://ise.dcloud.cisco.com>
 - 手动在地址栏输入 URL
 - 在拓扑工具栏点击 ISE
 - 使用收藏夹里面的 ISE 收藏链接

Figure 9. 在 <http://topo.dcloud.cisco.com> 网址上演示拓扑主页



2. 在 Operations 菜单移动你的鼠标，点击 Authentications。在这个屏幕上，我们可以看到最近的身份验证和 ISE 的授权情况。

备注：在这个特殊的案例中，有一个 MacBook 加入热点。

当这个设备第一次加入 dCloud-Hotspot SSID，他使用 MAB (MAC 身份验证通道) 来完成身份验证，并且 ISE 回到 WLC 的 HOTSPOT_REDIRECT 文件。这告诉 WLC 来重导所有的用户网络通路至 dCloud Hotspot Portal。

ISE 正确地介绍了这个设备室 MacBook。（在该例中不会显示基于设备类型特征区分的访问）

在用户输入正确的连接代码及接受 AUP，ISE 输送回第二个文件叫 HOTSPOT_ACCESS。这个文件将在 WLC 预设置的 ACL 退回，至允许接入网络和基本端口。

Figure 10. 引入 MacBook 文件，并动态应用热点接入 ISE

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Post
2014-11-04 16:09:29.442	🟡	0	A8:86:DD:9F:0A:	A8:86:DD:9F:0A:14	OS_X_Mavericks...	Web_Authentication >..	Web_Authentication ...	HOTSPOT_REDIRECT	WLC1		GuestEndpoints	
2014-11-04 15:53:04.818	🟢	0	A8:86:DD:9F:0A:	A8:86:DD:9F:0A:14	OS_X_Mavericks...	Web_Authentication >..	Web_Authentication ...	HOTSPOT_ACCESS	WLC1		GuestEndpoints	
2014-11-04 15:22:30.917	🟢	0	A8:86:DD:9F:0A:	A8:86:DD:9F:0A:14	OS_X_Mavericks...	Web_Authentication >..	Web_Authentication ...	HOTSPOT_ACCESS	WLC1		GuestEndpoints	
2014-11-04 15:22:26.795	🟢	0		A8:86:DD:9F:0A:14					WLC1			
2014-11-04 15:18:52.772	🟢	0	A8:86:DD:9F:0A:	A8:86:DD:9F:0A:14		Web_Authentication >..	Web_Authentication ...	HOTSPOT_REDIRECT	WLC1			

Scenario 2. 通过 Sponsor Approval 使用 Self-Registered Guest Access with Sponsor Approval

在这个章节中，组织希望提供给拜访者有弹性的访客网络接入。组织希望给访客一定的弹性来注册他们自己的访客账户，并同时希望增加组织的安全性，通过再用户获得网络接入前，从主办方得到所需账户的批准。在这种类型中，一个用户能填写主办方需要的信息来获得他们移动设备商的访客账户，并且系统将发送一封邮件给主办方来要求批准。主办方然后能登录 ISE 主办方端口，并批准或者拒绝要求。如果主办方批准了账户请求，ISE 将创建用户账户，并发送一封邮件和 SMS 信息到访客用户告知其访客登录证书。然后访客能够使用他们的证书登录访客端口，并且接入网络以及主要的端口页面。

演示步骤

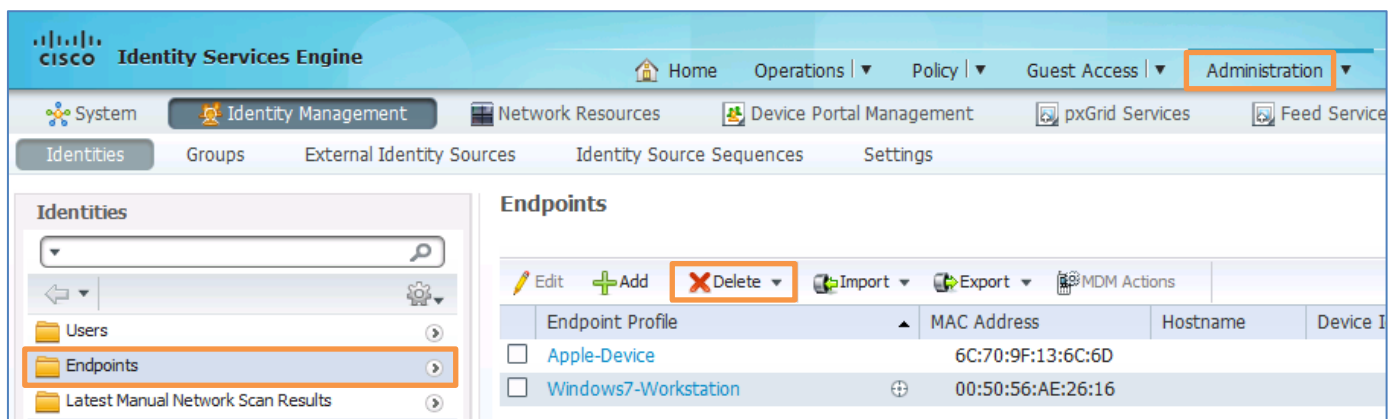
Cleanup devices 清除设备

备注：请务必根据以下指引仔细操作。因为我们已经回顾了其他流程，ISE 已经介绍了设备，身份验证，授权，以及加入到一个终点组。为了下一个流程的成功完成，我们将设备从 ISE 和 WLC 完全去除就非常重要，以及清除本地设备设置。若这些步骤失败，将导致在此演示中的结果未按照设计的生效。

在演示中，每个 personal device 的 Clear settings。如果设备设置没有清除，你将不能被重导至访客端口或者其他所需要的页面。

1. 清除 Web Cache. [如何操作 
2. 清除 Personal Device Settings. [如何操作 
3. 从 Workstation 打开浏览模式，登录至 <https://ise.dcloud.cisco.com>。你可以键入地址，或者接入 ISE，通过点击拓扑主页的 ISE 图标，或者通过接入 ISE 书签，在书签工具栏。登录 (admin/Cisco12345)。
4. 在 administration 页面中，在身份管理点击 Identities.
5. 点击左手边的 Endpoints
6. 选择你在热点章节使用的终点，点击 Delete，然后 Delete Selected。选择 Yes 如果被提问是否希望删除终点。

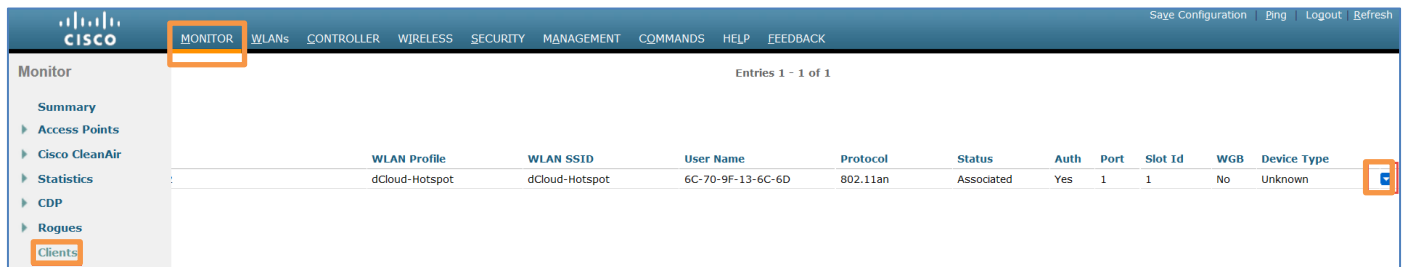
Figure 11. 从 ISE 删除一个终点



7. 从 Workstation 接入 WLC 登录页 <http://wlcl.dcloud.cisco.com>。你能够用几个不同的方法完成：
 - o 在地址栏手工输入地址
 - o 再书签栏点击 WLC1 的书签

- 点击浏览页的主页键，回到拓扑图表，点击 vWLC
8. 使用同样的 device specific credentials 登录 vWLC，你在演示准备第 7 步获得的。
 9. 点击 Monitor，然后 Clients，在左边
 10. 在连接热点前应该查看所有的客户。移到右边，浏览下拉箭头直到其展开，然后点击 Remove

Figure 12. 从 WLC 删除客户



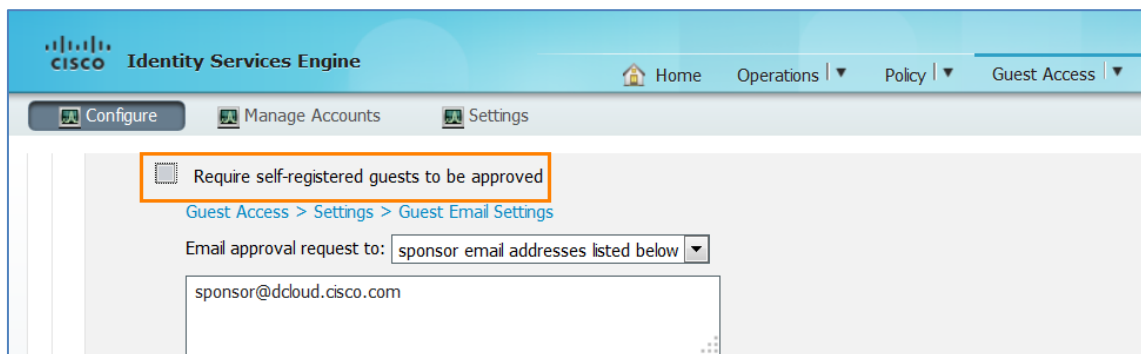
Self-Registering 的设备

备注：通过定义，主办方必须批准所有的自行注册访客账户。操作步骤 1-5，可以使主办方批准特点失效。再继续主办方批准激活，直接跳到第 6 步。

禁用 Sponsor Approval

1. 鼠标悬停在 Guest Access 点击 Configure。
2. 点击左边的 Guest Portals。
3. 下拉直到发现自行注册访客端口。点击名字编辑。
4. 在 Portal Behavior and Flow Settings 下，下拉至 Self-Registration Page Settings。
5. 将 Require self-registered guests to be approved 打钩框的钩去掉

Figure 13. 禁用 Guest Registration



6. 连接用户设备到开放的无线 SSID dCloud-Guest
7. 打开用户设备中可支持的内部网络浏览器，浏览任何网络页面。你将被重导至 dCloud 访客端口。

备注：确认当打开浏览器时，使用 HTTP 接入页面。如果使用 HTTPS，你将不能被重导至热点端口。这是因为在现有 WLC 代码中有一个缺陷，不能操作 HTTPS 重导。

8. 在按钮下点击 Don't have an account?

Figure 14. 访客端口登录页面

9. 填写访客账户所需的信息。请按照以下特定指引进行
- 邮箱地址必须是 `dcloud-guest@dcloud.cisco.com`
 - 电话必须是实际电话，当你希望访客证书通过 SMS 发送。请输入国家代码+区域码+电话号码，不能有间隔或破折号。例如：
15865551234
 - 点击 Register。

Figure 15. 访客 Self-Registration 页面

备注：访客证书将同时通过邮件以及 SMS 短消息的方式发送给访客用户。在真实情况下，访客用户将输入他们的真实邮箱地址。在这个演示情况下，我们无需发送邮件到任何一个域名。因此，为达到这个目的，在演示环境下设置了访客账户建立。一旦证书发送，我们将能登录访客邮箱账户通过 Microsoft Exchange OWA，来收到含有证书的邮件。如果一个邮箱地址输入，而不是 dcloud-guest@dcloud.cisco.com，你将不能收到访客证书邮件。如果电话号码没有用恰当的格式输入，你将不能收到 SMS。

10. 在提交访客注册请求后，登录页面显示一个提示，含有证书的一封邮件或者 SMS 信息已经送达，在主办者批准你的请求后。

Figure 16. 访客端口备注

The screenshot shows a mobile browser interface for the dCloud Guest Portal. At the top, the status bar indicates 'iPad', signal strength, '12:59 PM', and '41%' battery. The browser address bar shows 'ise.dcloud.cisco.com'. The page title is 'Sign On'. Below the title, there is a 'GUEST PORTAL' header with a logo. The main content area has a 'Sign On' heading and a welcome message: 'Welcome to the dCloud Guest Portal. Sign on with the username and password provided to you.' A prominent orange-bordered box contains the message: 'An email and SMS message containing your sign on credentials will be sent to you once your sponsor approves this request.' Below this, there are two input fields labeled 'Username:' and 'Password:'. A blue 'Sign On' button is positioned below the password field, and a link 'Don't have an account?' is at the bottom.

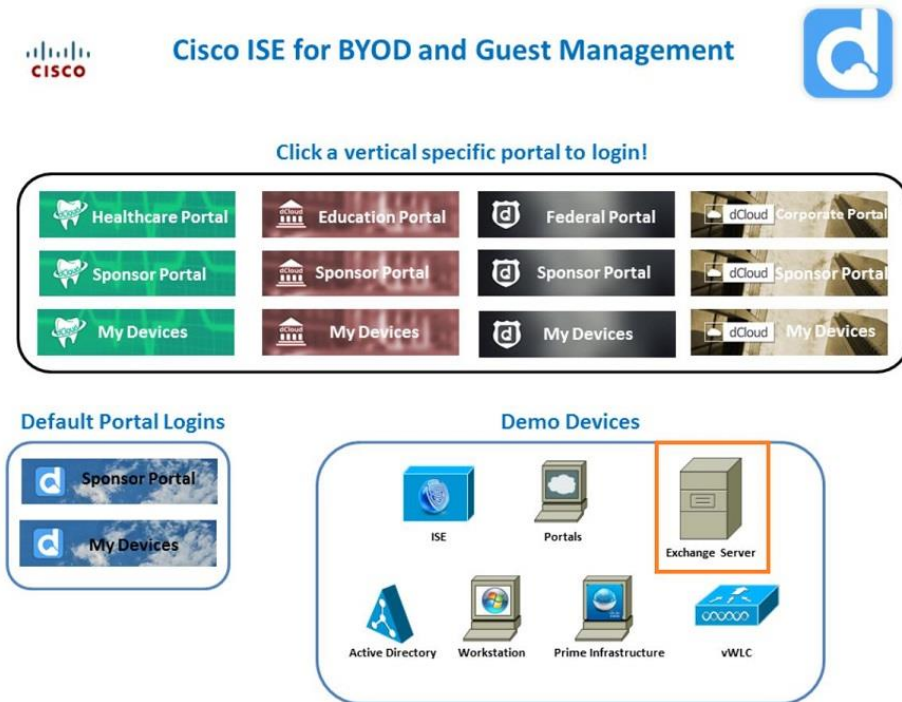
备注：你将不能收到 SMS 或者邮件知道主办者在下一步批准了访客注册请求。

批准访客注册请求

1. 在 Workstation1 打开浏览模式，点击 home 键浏览主页。
2. 在 Demo Devices 下，点击 Exchange Server 来打开在独立页面上的 Outlook Web App.

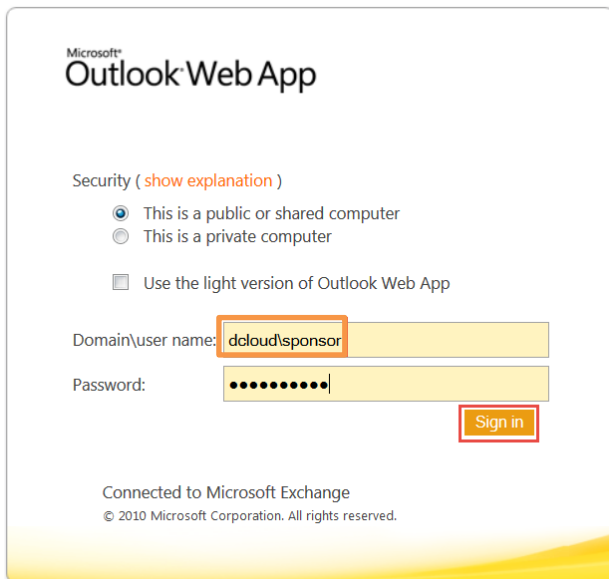
备注：显示 Outlook Web App 登录页面需要大约 10 秒钟。

Figure 17. 点击 Exchange Server 图标



3. 登录 Outlook Web App(dcloud\sponsor/Cisco12345)。

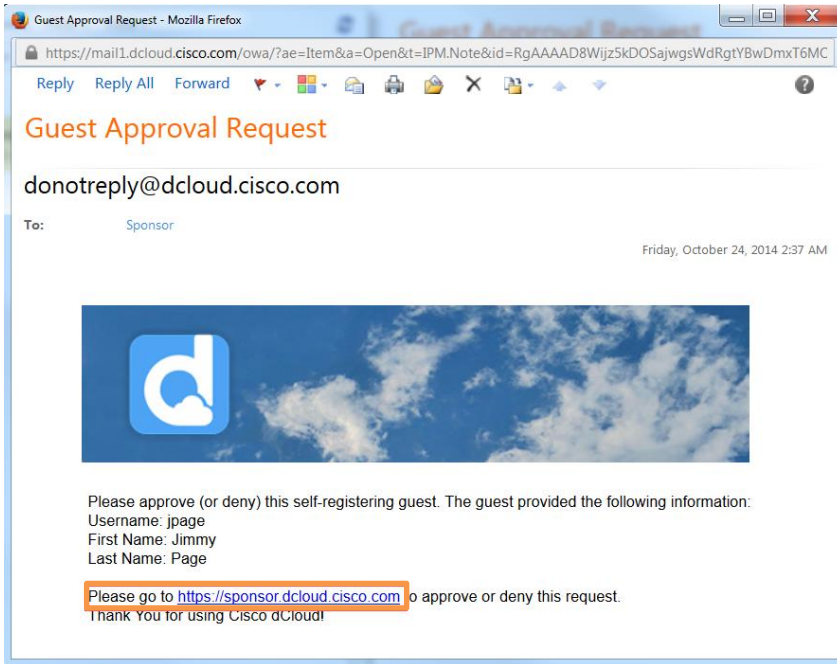
Figure 18. 更改 OWA Web 登录页面



4. 打开 Guest Approval Request 邮箱。点击链接 <https://sponsor.dcloud.cisco.com> 在邮件信息的底部来重导至 sponsor portal。

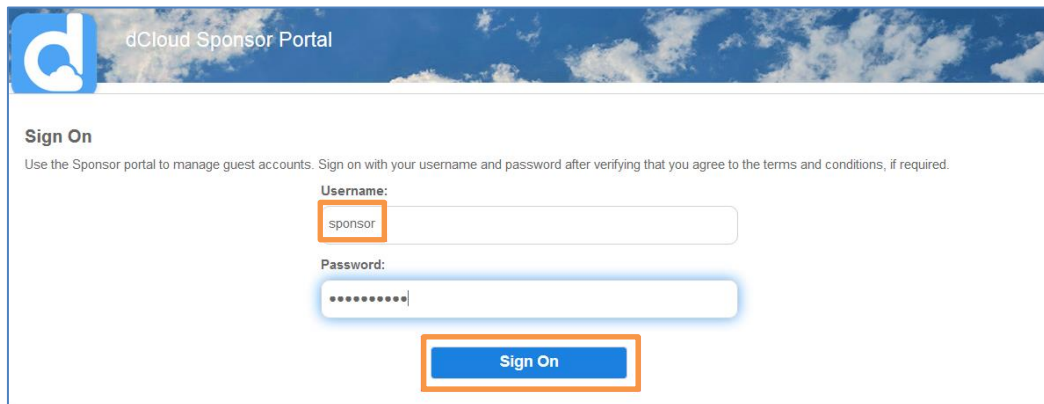
备注：如果你在开始浏览 Cisco ISE Portal Management [Americas] 演示指南前，针对一个特定的纵向定制你的演示，以上邮件的主办方端口 URL 将链接至一个特定纵向主办方端口，例如 <https://sponsor-health.dcloud.cisco.com> 或 <https://sponsor-edu.dcloud.cisco.com>

Figure 19. 在主办方邮箱中的访客批准邮件



5. 登录 Sponsor Portal (sponsor/C1sco12345)。

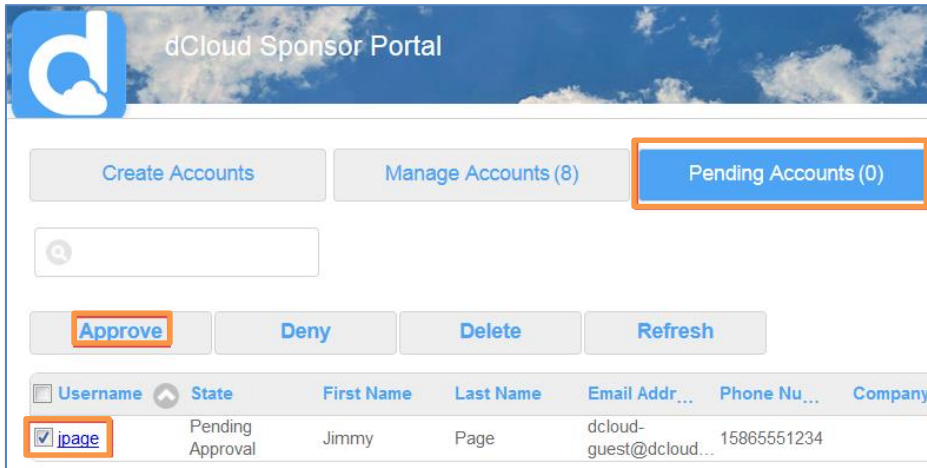
Figure 20. 主办方端口登录页面



6. 点击 Pending Accounts。选择你想要批准的访客人用户方框，点击 Approve。点击 OK 当被提问是否确定你想要批准选择的账户。

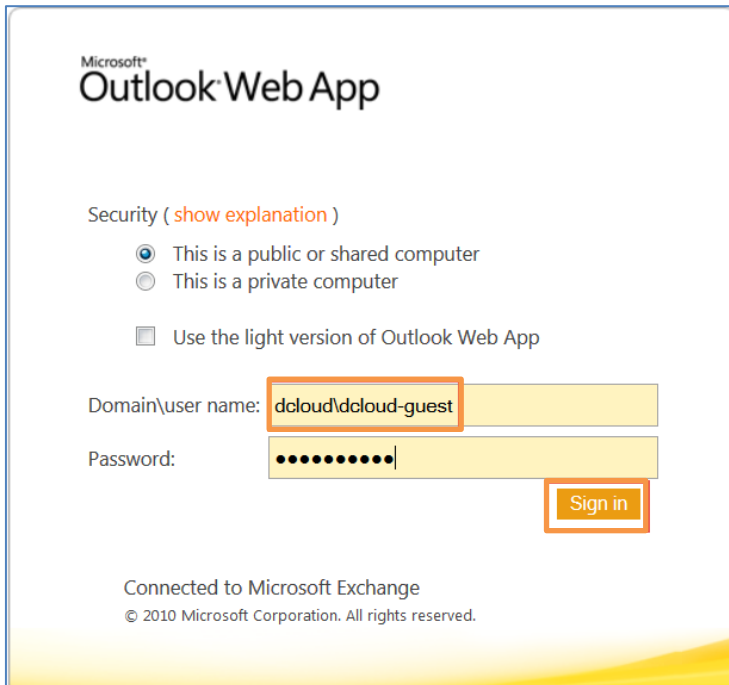
备注：一些用户在操作这个功能是会遇到出错。点击 OK 或者关闭出错窗口-可以忽略出错。

Figure 21. Sponsor portal 待定账户 (pending accounts)



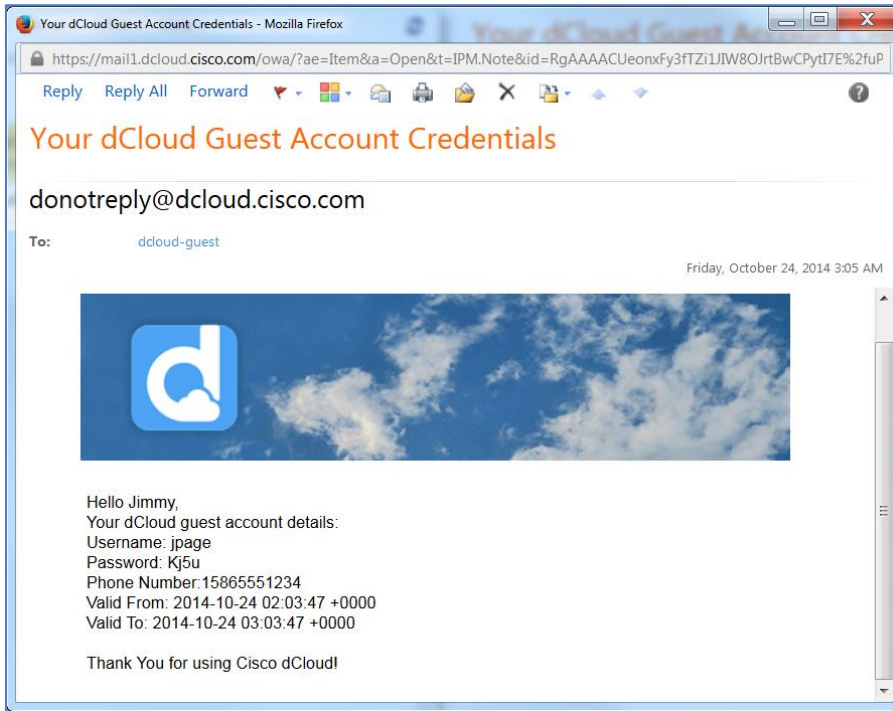
7. 你将受到一个有访客用户证书的 SMS 信息。收到 SMS 可能要花一分钟。另外，一封邮件被送到 dcloud-guest 用户账户。登录邮件，返回 Workstation1 并且退出主办方账户，通过点击右上角的 **sign out**。点击 Outlook Web Mail 的书签来回到登录页。登录 (dcloud\dcloud-guest/C1sco12345) 。

Figure 22. 更改 OWA Web 登录页面



8. 检查 **Inbox** 邮箱中含有访客证书的邮件。

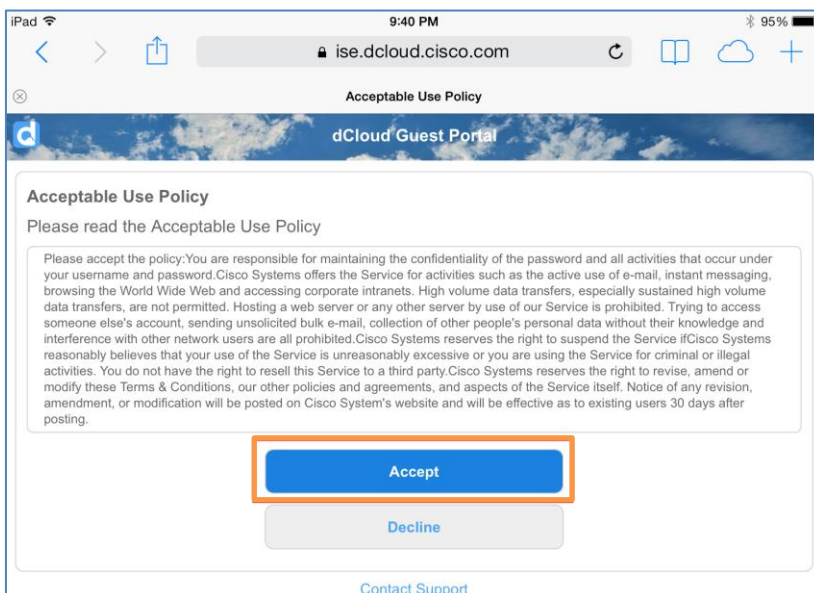
Figure 23. 含有批准证书的访客账户邮件



接入访客网络

1. 在用户设备商，使用你通过 SMS/邮件收到的证书登录访客端口
2. Click **Accept** to approve the Acceptable Use Policy (AUP), then **Continue**. The **Success** page indicates you have Internet access through the network. 点击 Accept 来批准 Acceptable Use Policy(AUP)，然后点击 Continue。Success 页面显示你已经通过网络接入了互联网。

Figure 24. Guest Portal AUP 访客端口 AUP



点击 www.cisco.com 链接来演示设备已经通过访客端口接入互联网。

参考 Table 2 以及发现你的部分的主要端口页面（公共卫生，教育，联邦政府或者公司）。浏览至表中的主端口页面。严书记用户现在接入了主要端口页面及通用资源，但没有接入内部资源或者注册设备链接。

Figure 25. 在 <http://health.dcloud.cisco.com> Healthcare Connections Center

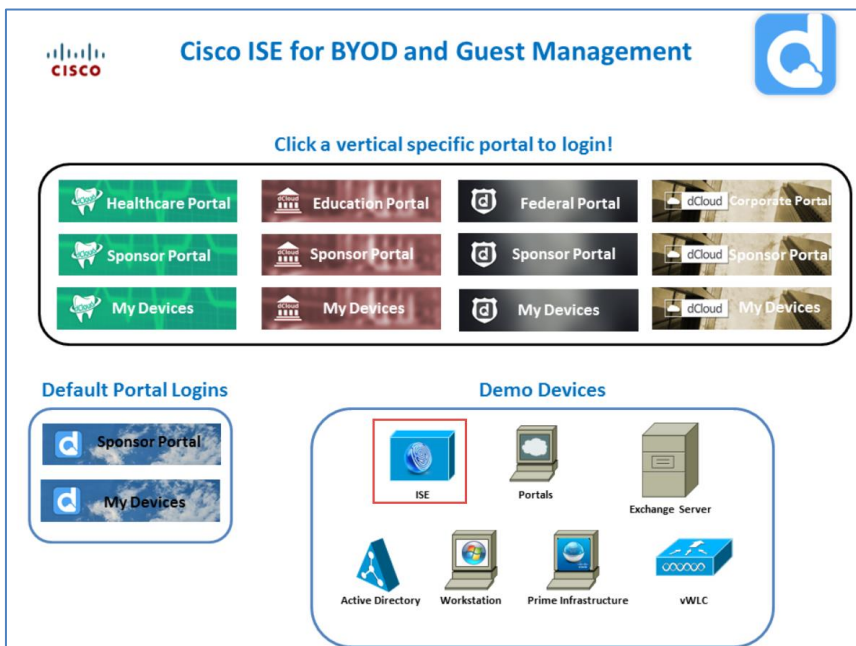


演示 ISE 中的自行注册访客流程

设备已经成功链接访客网络，并且已经有互联网连接。下一步，我们将简单地浏览 ISE UI，来演示 ISE 动态文件设备的基础，以及动态允许访客互联网接入，通过应用恰当的授权文件

1. 在 Workstation1，在电脑上运行浏览模式
2. 在拓扑图的 Demo Devices 部分，点击 ISE。这将带你进入 ISE 登录页面，在网址 <https://ise.dcloud.cisco.com>

Figure 26. 拓扑端口



3. 登录 ISE (admin/C1sco12345) .
4. 浏览 Operations 菜单，点击 Authentications。在这个屏幕，我们可以看见最近的 ISE 里的身份验证和授权

备注：在这个特殊的案例中，使用了 Apple iPad 来连接访客网络。

当设备第一次连接 dCloud-Guest SSID，他将使用 MAB (MAC authentication bypass)身份验证，以及 ISE 将 GUEST_REDIRECT 文件退回 WLC。这告诉 WLC 来重导 all user web traffic 至 dCloud Guest Portal。

然后，ISE 正确地引入了 Apple iPad 作为设备。在这个演示中，我们不会演示基于设备类型特征区别的介入。

在用户自行注册后，被主办方批准后，登录到访客端口，ISE 发送会第一个文件称作 GUEST_ACCESS。这个文件退回在 WLC 预设的 ACL，至允许接入互联网和基本端口。在以下的截图中，我们能够看见在被主办方批准的访客登录后，用户的“jpage”登录。

Figure 27. 动态访客接入应用

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2014-10-23 23:17:41.156			0	jpage	6C:70:9F:13:6C:6D	Apple-iPad			
2014-10-23 23:17:41.138				jpage	6C:70:9F:13:6C:6D	Apple-iPad	Web_Authentication >..	Web_Authentication ...	GUEST_ACCESS
2014-10-23 23:17:41.113					6C:70:9F:13:6C:6D				
2014-10-23 23:16:39.944				jpage	6C:70:9F:13:6C:6D				
2014-10-23 23:12:40.641					6C:70:9F:13:6C:6D 6C:70:9F:13:6C:6D	Apple-Device	Web_Authentication >..	Web_Authentication ...	GUEST_REDIRECT

Scenario 3. Sponsored Guest Access

在这个场景中，组织需要规定访客用户账户一些基本需要。访客用户账户能够为提前办公时间到达的访客设立，并能提供基本的无线网接入。在这个特殊的章节，组织希望有一个雇员提前授权访客用户一个访客账户，而不是自行注册。一个访客账户由授权者在授权端口创建，在计划到达时间之前，并且登陆证书同时通过 SMS 和邮件送达访客用户。当访客使用到达是，他们只需要简单地接入 dCloud-Guest SSID，登陆，以及获得访客接入网络。另外，ISE 授权端口允许大量引入用户账户。例如，在一个远程销售办公室，在一个大型销售聚会前夜，办公室行政人员可以授权 50 个新的到达办公室的来访者访客账户

备注：“访客接入”可以按照组织需要定义。在这个演示中，访客接入给访客者接入互联网和主要的端口页面。针对一些客户，访客接入只意味着互联网接入，或者可以接入互联网以及一些互联网资源。ISE 是有弹性的，可以根据你的客户需要设置。

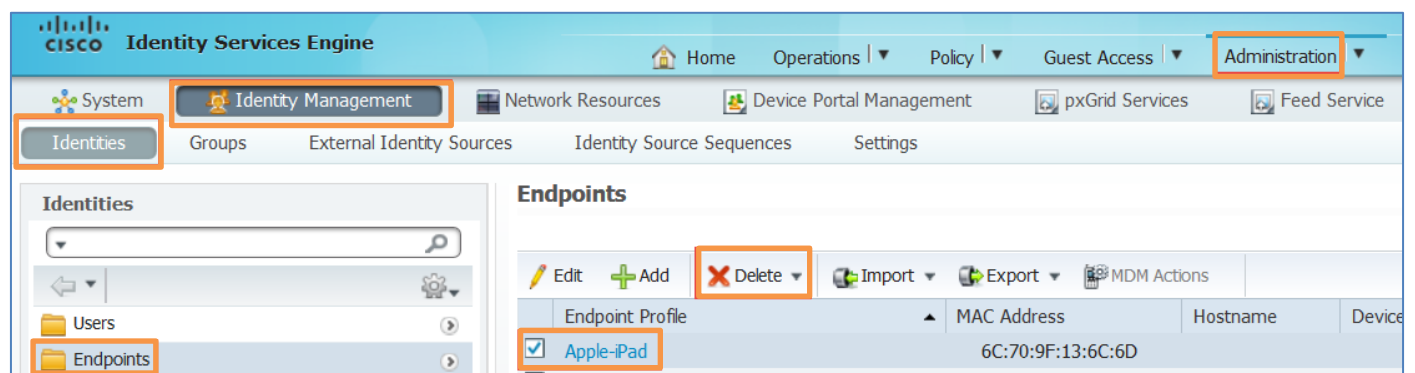
演示步骤

清除设备

备注：仔细跟随一下指引是必要的。因为我们已经回顾了其他流程，ISE 已经规定了设备，身份验证，授权，以及加入终点组。为了成功操作以下流程，我们从 ISE 和 WLC 完全去除设备是重要的，以及清除本地设备设置。这些步骤操作失败会导致设计的演示失败。

1. **Clear settings** 在演示中使用的每个 **personal device** 的设置。如果设备设置没有清除，你可能不会被重导至访客端口或者其他所需页面。
 - a. 清除 Web Cache [如何操作 
 - b. 清除 Personal Device Settings [如何操作 
2. 从 Workstation1 打开浏览模式，在 <https://ise.dcloud.cisco.com> 登录 ISE。你可以键入地址，或者通过点击拓扑主页 ISE 图标接入 ISE，或者在书签工具栏接入 ISE 书签。登录(admin/C1sco12345)。
3. 浏览 Administration。悬停在 Identity Management，点击 Identities。
4. 在左边的浏览栏点击 Endpoints
5. 选择你在热点部分使用的终点，点击 Delete，然后 Delete Selected。
6. 如果被提问是否想删除终点，点击 Yes

Figure 28. 从 ISE 删除终点



1. 从 Workstation1 接入 WLC，登录页面 <http://wlc1.dcloud.cisco.com>。你又一下几个不同的方法完成：
 - 在地址栏手工输入地址

- 在书签工具栏点击 WLC1 书签
 - 在浏览模式点击 home 键，回到拓扑图，点击 vWLC。
2. 使用相同的设备特定证书登录 vWLC，在演示准备部分的第 7 步获得的证书。
 3. 点击 MONITOR，然后点击左手边的 Clients，来浏览先前加入热点的任一客户。
 4. 将鼠标移动到右边下拉箭头知道展开，然后点击 Remove。

Figure 29. 从 WLC 删除客户

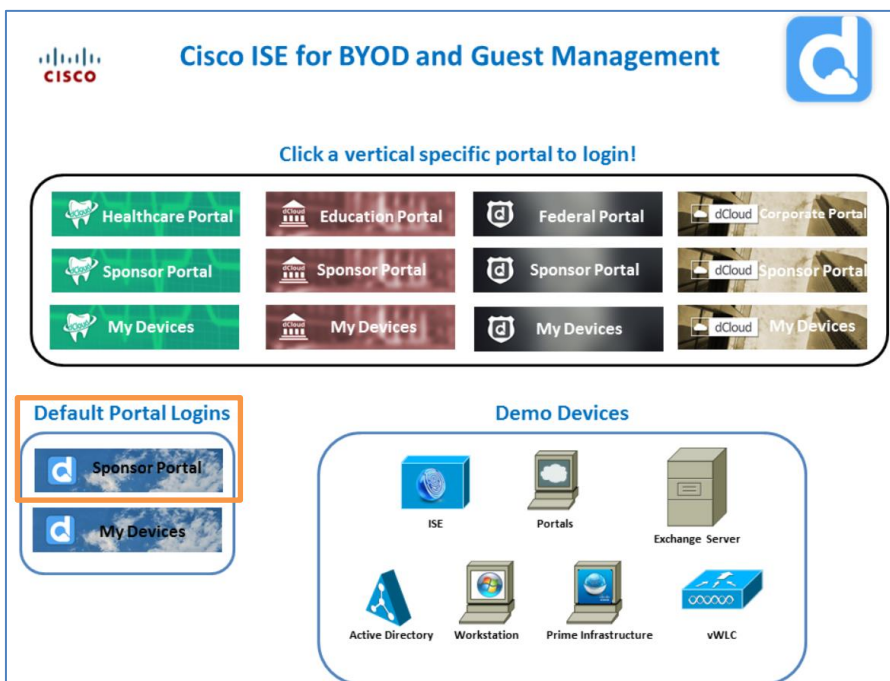


创建访客账号

1. 从 Workstation1 打开浏览模式，点击 Home 按钮
2. 在 Default Portal Login 部分，点击 Sponsor Portal，进入 Sponsor Portal 登录页面

备注：如果你在开始回顾 Cisco ISE Portal Management 演示指南[Americas]之前针对特定纵向定义你的演示，请在页面顶部 Click a vertical specific portal to login 部分点击针对你的纵向特定的主办方端口链接

Figure 30. 拓扑页面



3. 登录至 Sponsor Portal(sponsor /C1sco12345).

4. 在 **Creat Accounts** 表格，填写以下访客账户必须的信息：

- a. 邮箱地址必须是 dcloud-guest@dcloud.cisco.com
- b. 电话号码必须是你希望访客证书通过 **SMS** 能发送到的真实电话号码。请输入国家号码+区域号码+电话，无空格或者破折号。例如 15865551234.
- c. 完成后，点击 **Create** 来创建访客账户，并打开账户信息屏幕。

Figure 31. 从 sponsor portal 创建访客账户

d. 点击 **Notify**

Figure 32. 提醒访客成功创建账户

5. 在 **Notify** 栏，核对 **SMS** 和 **Email**。

6. 点击 **OK**，发送访客用户证书的 **SMS** 信息和邮件。收到信息需要一分钟。

Figure 33. Notify 弹出窗口

备注：在一个真实的环境中，主办方将输入一个真实的访客邮箱地址。在这个演示环境中，我们不能向任何域名发送邮件。因此，为了达到这个目的，在演示环境里设置了一个访客账户。

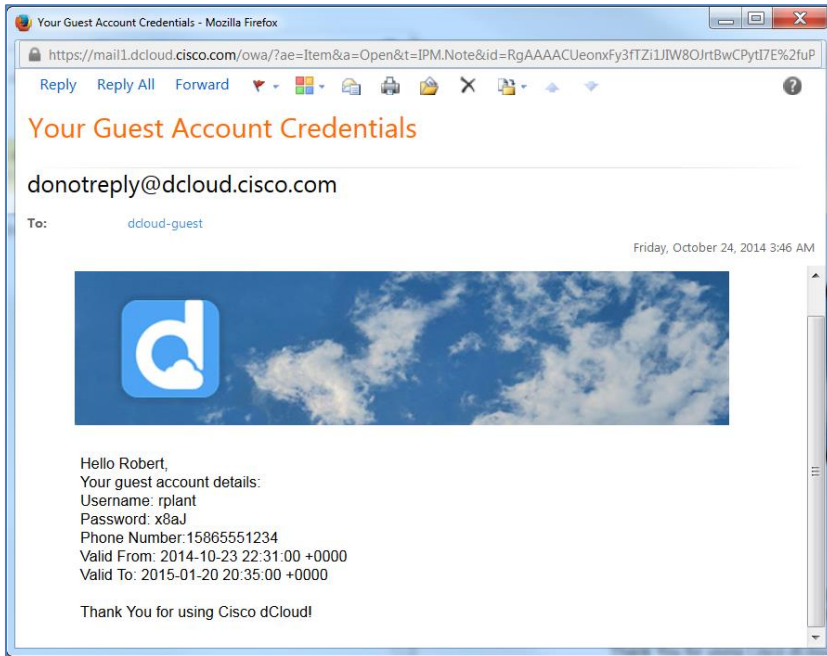
一旦证书被发送，我们将通过 Microsoft Exchange OWA 登录访客邮箱账户来确认含有证书的邮件。[如果邮件地址未输入 dcloud-guest@dcloud.cisco.com](mailto:dcloud-guest@dcloud.cisco.com)，你将不能收到访客证书邮件。如果电话号码未输入正确的格式，你将不能收到 SMS。

7. 为了收到邮件，点击 Outlook Web Mail 书签，并登录（dcloud\dcloud-guest/C1sco12345）。

Figure 34. 更改 OWA Web login page 登录页面

8. 检查邮箱中含有访客证书的邮件

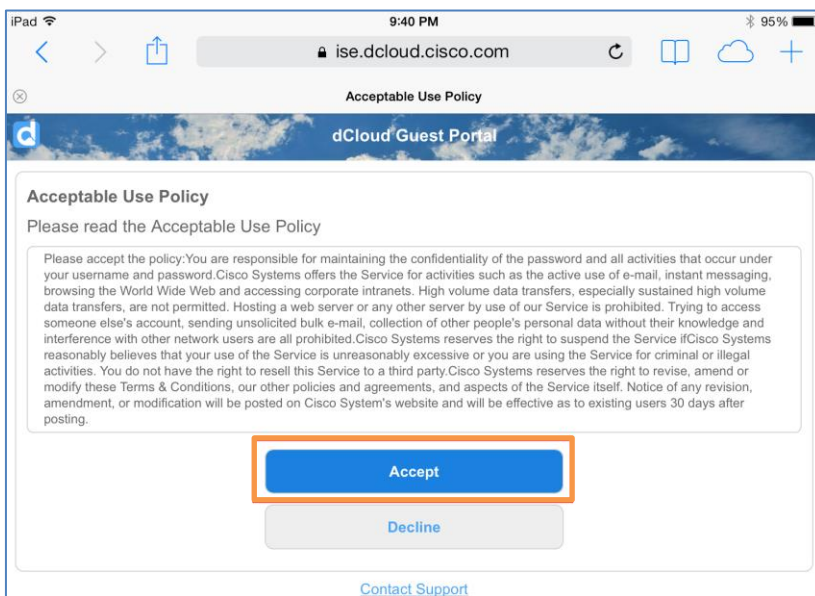
Figure 35. 含有证书的访客邮件批准,



9. 在用户设备商, 用 SMS/邮件收到的证书登录访客端口。

10. 点击 **Accept** 来批准 **Acceptable Use Policy(AUP)**, 然后点击 **Continue**。 **Success** 页面显示你已经通过网络登录互联网。

Figure 36. Guest Portal AUP 访客端口 AUP



11. 点击 www.cisco.com 的链接来演示设备已经通过访客端口登录互联网。

12. 根据 **Table 2**, 找到你的篇章的主要端口页 (公共卫生, 教育, 联邦政府或者公司)。浏览列表中的主要端口页面。演示用户已经介入主要端口页面以及通用资源, 但没有接入网络资源或者我的注册的设备链接。

Figure 37. 在 <http://health.dcloud.cisco.com> Healthcare Connections Center



演示 ISE 中的主办方访客流程

设备已经成功链接访客网络，并接入互联网。接下来，我们将回顾一下 ISE UI，来演示 ISE 动态设置设备，动态允许访客通过申请正确的授权文件来接入互联网的基本知识。

1. 在 Workstation1，在主机上运行浏览模式
2. 在拓扑图的 Demo Devices 部分，点击 ISE 并登录（admin/C1sco12345）。
3. 移动鼠标至 Operations 菜单，点击 Authentications。在这个屏幕上，你可以看见 ISE 中最近身份验证或者授权意图。

备注：在这个特殊的案例中，使用了 Apple iPad 来接入访客网络。当设备第一次连接 dCloud-guest SSID 时，使用了 MAB（MAC 身份验证通道）来做身份验证，并且 ISE 返还了 GUEST_REDIRECT 文件至 WLC。这告诉 WLC 来重导所有的网络通道至 dCloud Guest 端口。

很快 ISE 正确地将文件设置为 Apple iPad 设备。在这个演示中，我们将不显示设备差异引起的介入区别特征。

在用户使用主办方提供的账户登录访客端口后，ISE 发送回第二个文件较 GUEST_ACCESS。这个文件将退回 ACL 文件，这个文件再 WLC 被预设置，只被允许接入网络和基本端口。

在下面的截屏中，我们可以看到用户“rplant”在他的访客账户由主办方从授权端口创建后登录

Figure 38. 动态访客接入应用

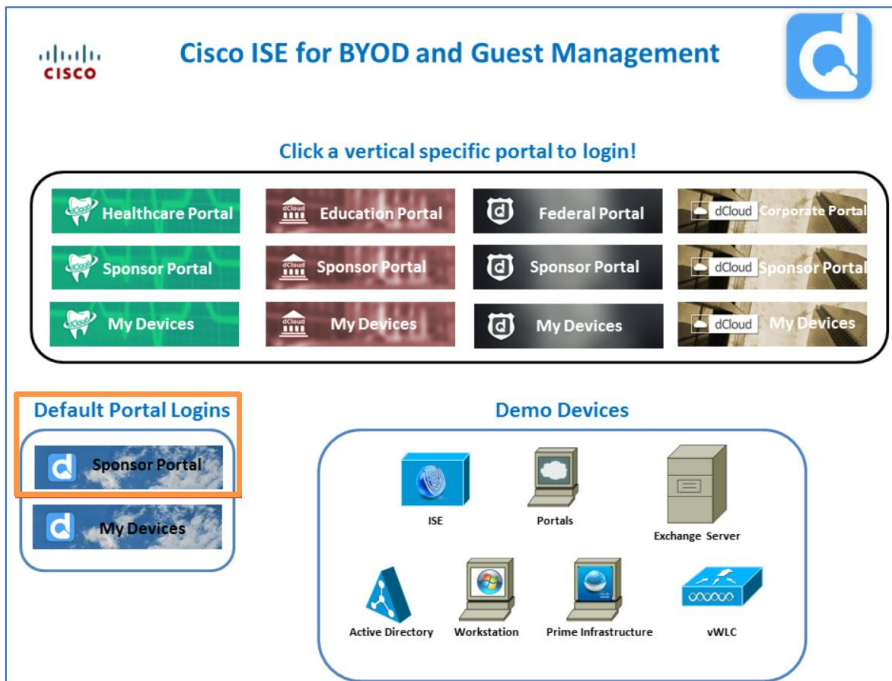
2014-10-24 03:33:53.449			0 rplant	6C:70:9F:13:6C:6D	Apple-iPad		
2014-10-24 03:33:53.436			rplant	6C:70:9F:13:6C:6D	Apple-iPad	Web_Authentication >..	Web_Authentication ... GUEST_ACCESS
2014-10-24 03:33:53.417				6C:70:9F:13:6C:6D			
2014-10-24 03:33:49.234			rplant	6C:70:9F:13:6C:6D			
2014-10-24 03:33:17.890				6C:70:9F:13:6C:6D 6C:70:9F:13:6C:6D		Web_Authentication >..	Web_Authentication ... GUEST_REDIRECT

创建大量访客账户

ISE 主办方端口能够同时提供很多访客账户，通过使用大量的引入特征。主办方可以从 ISE 主办方端口下载一个.csv 模板。这个.csv 模板有一列是针对特定的 ISE 需要的信息来创建不同的访客账户。使用这个模板，主办方可以填写所有的访客端口必须的信息，例如名，姓和电话号码。主办方然后引入.csv 文件至 ISE 主办方端口，并且 ISE 在电子表格中为所有的用户创建访客账户。在这个演示中，桌面上的 Workstation1 中有一个预先建立的.csv 文件，已经含有 8 个访客用户账户。

1. 从 Workstation1 打开浏览模式，或者通过点击 home 键浏览主页
2. 在 Default Portal Logins 部分点击 Sponsor Portal 来到 Sponsor Portal Login 页面

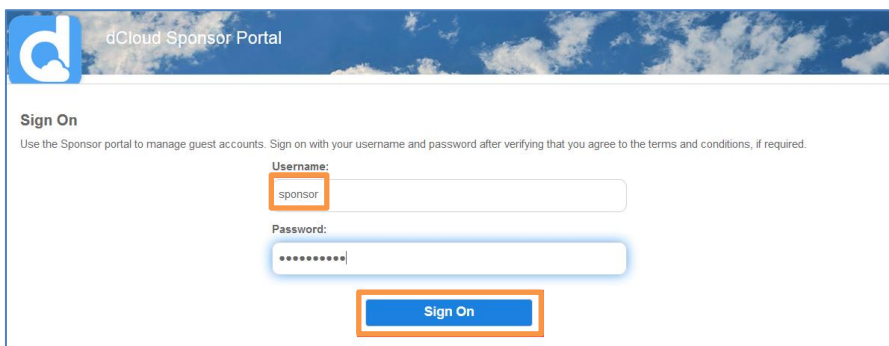
Figure 39. 拓扑页面



备注：如果你定制你的演示时针对一个特定的纵向，在开始 *Cisco ISE Portal Management [Americas]* 演示指引之前，请点击主办方端口特别针对你的页面顶部的纵向的链接，在 **Click a vertical specific portal to login** 部分

3. 使用主办方名字和密码 C1sco12345 登录 Sponsor Portal

Figure 40. 主办方端口登录页面



4. 在 Create Accounts 栏点击 Import 项
5. 点击 Browse，然后再桌面上选择 guest.csv 文件，点击 Open。
6. 点击主办方端口右下角的 Import

Figure 41. 创建大量账户

Create Accounts | Manage Accounts (1) | Pending Accounts (0) | Notices (0)

Guest type:
 Contractor (default)
 Maximum devices that can be connected: 5
 Maximum access duration: 365 days

Guest Information
 Known | Random | **Import**

Click to download the import template file.
[Download Template](#)

Select file: Maximum: 200

Language: English - English

Access Information
 Duration: 83 Days (Maximum: 365)
 From Date (yyyy-mm-dd) *: 2014-10-24 From Time *: 00:13
 To Date (yyyy-mm-dd) *: 2015-01-14 To Time *: 19:41

[Help](#)

7. 跳出对话框 “Account importing will be processed in the background”，点击左上角的 X

Figure 42. 关闭信息窗口

Create Accounts | Manage Accounts (9) | Pending Accounts (0) | Notices (1)

Guest type:
 Contractor (default)
 Maximum devices that can be connected: 5
 Maximum access duration: 365 days

Guest Information
 Known | Random

Click to download the import template file.
[Download Template](#)

Select file: Maximum: 200

Language: English - English

Access Information
 Duration: 83 Days (Maximum: 365)
 From Date (yyyy-mm-dd) *: 2014-10-24 From Time *: 00:13
 To Date (yyyy-mm-dd) *: 2015-01-14 To Time *: 19:41

Account importing will be processed in the background. Check Notices for status.

8. 点击 Notice 项。你将看到一个提示，8 个账户已经成功创建。

Figure 43. 创建引入账户

Create Accounts | Manage Accounts (9) | Pending Accounts (0) | **Notices (1)**

<input type="checkbox"/> Action Name	Number of Accounts	Status	Start	End
<input type="checkbox"/> Create Import Accounts	8	Success	2014-10-24T00:16:46.734Z	2014-10-24T00:16:47.909Z

9. 点击 **Create Import Accounts** 提示来显示提示。你将看到 8 个用户账户已经在 `guest.csv` 创建，含有每个用户的所有账户信息。点击 **Done** 返回主办方端口页面。

Figure 44. 成功引入大量访客账户

Account Information

Accounts imported successfully.
Accounts created: 8

Showing: 8

1. Username:dc1oud
Password:Hs8q
- Dee Cloud
dcloud-guest@dcloud.cisco.com
15551234567
2. Username:jlennon
Password:qs5m
- John Lennon
dcloud-guest@dcloud.cisco.com
15551234567
3. Username:pmccartney
Password:wPc9
- Paul McCartney
dcloud-guest@dcloud.cisco.com

10. 点击管理 **Manage Accounts** 键来查看添加的 8 个访客账户。以及先前创建的任何访客账户

Figure 45. 访客账户

User	State	First Name	Last Name	Email Ad...	Phone N...	Group Tag	Location	Sponsor	Guest Ty...	Expirati...	Time Left
bdylan	Created	Bob	Dylan	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M
dcloud	Created	Dee	Cloud	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M
eclapton	Created	Eric	Clapton	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M

备注：为了你的方便使用，Workstation1 部件已经安装 **Open Office Calc**。如果你愿意，你可以随机打开并编辑 `guest.csv` 文件来添加你自己的访客账户。



Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)