Cisco Prime IP Express的BYOD功能 — 白皮书

目录

简介

本白皮书介绍Cisco Prime IP Express(CPIPE)系统的BYOD功能和配置。Cisco Prime IP Express BYOD注册门户是一个易于处理的自助服务门户，用于注册和管理设备。它与Cisco Prime IP Express的DHCP、CDNS集成。详细记录了此系统所需的方法、架构和BYOD配置。使用本白皮书作为指南，您可以配置BYOD来注册和管理设备。

问题陈述

所有IP网络都面临一组常见问题。这与波士顿学院在开发其自动互联网登录系统之前面临的问题类似，例如：

- 为计算机提供由用户驱动的手动配置，使用正确的IP地址和网络设置。
- 在短时间内配置大量计算机
- 获取有关网络上配置的计算机的信息
- 控制对IP网络资源的访问
- 收集信息，帮助排除网络和安全事件故障

BYOD功能功能概述

您可以使用Cisco Prime IP Express系统的BYOD功能解决上述每个问题，因为它为员工提供全面的解决方案，以良好管理且安全的方式使用他们自己的支持IP的设备。它有效地消除了IT管理员在加入和跟踪个人和公司设备时面临的挑战。此功能的一些优势包括：

- 为设备提供由用户驱动的手动配置，其IP地址和网络设置正确。
- 在短时间内配置大量设备。
- 获取有关网络上配置的设备的信息。

当用户首次尝试连接BYOD设备时，Cisco Prime IP Express DHCP网络会自动将用户重定向到BYOD注册门户，因为用户必须使用其现有Active Directory凭证注册其设备。在注册期间，通过自动检测或手动输入来捕获有关用户设备的信息，如其MAC地址/DUID和其他元数据。此信息用于将用户映射到其设备并跟踪IP活动以进行审核和合规性。BYOD注册门户与Cisco Prime IP Express的DHCP集成。

用户视角：

BYOD功能为最终用户提供了激活设备和访问Cisco Prime IP Express(CPIPE)网络的简单流程。步骤如下：

- 将设备连接到网络
- 从浏览器请求http
- 系统会自动将您重定向到BYOD注册页面
- 注册页面填充设备详细信息并提示您输入用户凭证
- 提供凭证，例如用户名、密码
- 接受服务条款
- 点击注册按钮
- 等待几秒钟，设备将重新启动。

此过程通常只需大约三分钟。完成后，设备将激活，客户端将在DHCP服务器中创建。

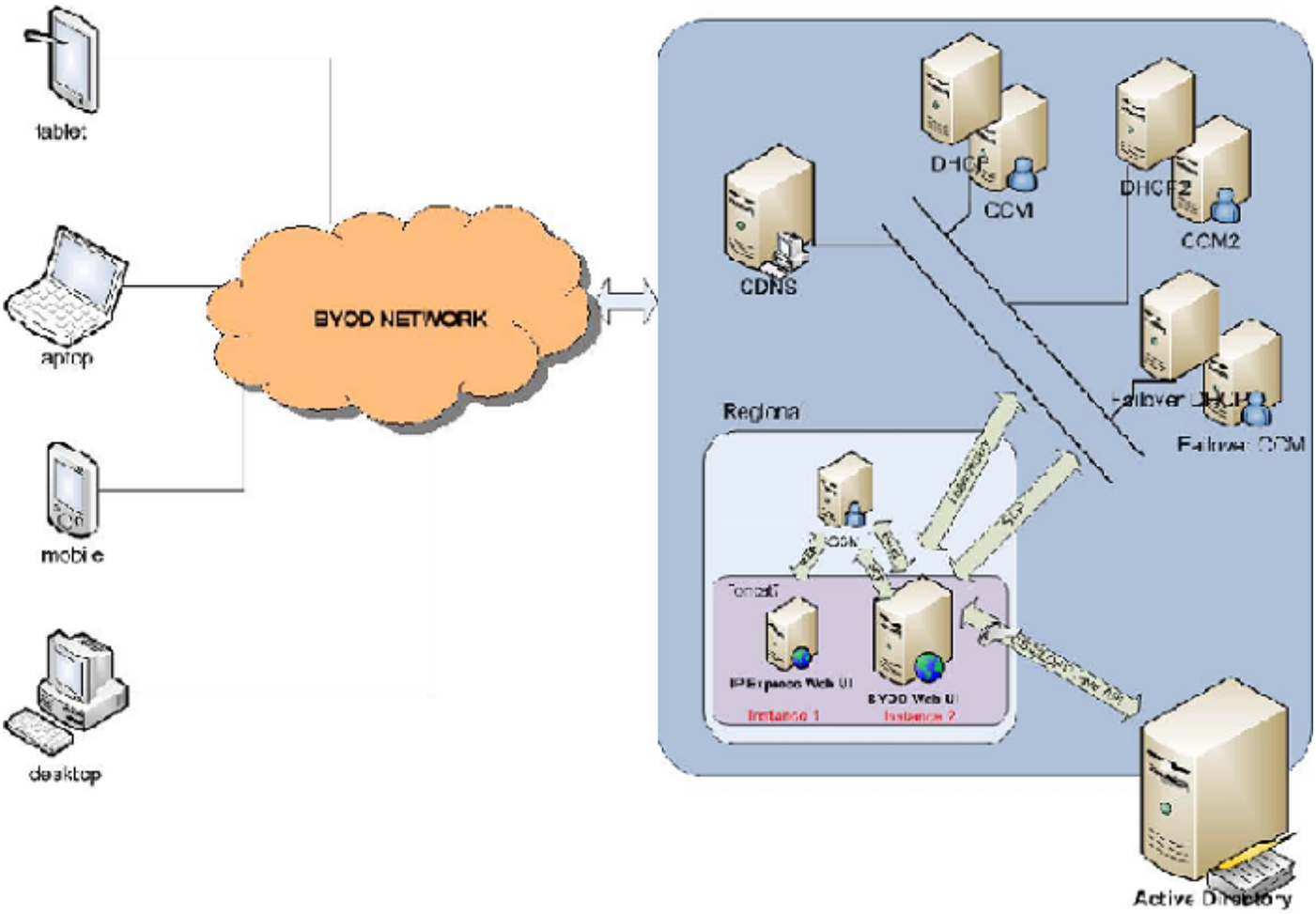
管理员的视角：

该系统是一个易于使用的自助服务Web门户，取代了许多耗时且容易出错的流程。这种自助服务系统的管理非常简单。

- 安装Cisco Prime IP Express Web服务器
- 配置BYOD（DHCP、CDNS服务器）
- 指导用户如何注册设备
- 指导用户如何使用用户登录页管理设备

功能架构

此功能的架构至少需要四个主要组件：本地DHCP服务器、CDNS服务器、区域服务器和Active Directory。在区域服务器中，新的tomcat实例运行以支持BYOD。标准CDNS服务器配置了带ACL列表的域重定向规则，可确保从特定地址范围的所有HTTP查询都解析为BYOD Web服务器地址。下图显示了功能架构图。



流程

下图描述了当用户/客户端将BYOD连接到网络时Web UI的流程。

- 当客户端将新设备连接到网络时，DHCPDISCOVER/SOLICIT数据包将发送到DHCP。
- DHCP提供临时IP并返回选项6(DHCPv4)或选项23(DHCPv6)（CDNS服务器地址）。
- 客户端向CDNS服务器发送DNS解析查询。
- CDNS域重定向规则为未注册的BYOD设备提供BYOD Web服务器IP，并重定向到设备注册页面。
- BYOD Web服务器从http报头数据获取客户端IP，并检查匹配的子网/前缀以查找客户端DHCP服务器地址。
- 如果找不到匹配的子网/前缀，则SCP请求会发送到区域CCM，以查找为此客户端提供服务的DHCP服务器，并更新BYOD内存中的子网/前缀信息。

- 将带地址的租用查询(根据RFC 4388(DHCPv4)和RFC 5007(DHCPv6))发送到相应的DHCP服务器，以获取客户端标识符（设备ID），并在设备注册页面中填入其他详细信息，如设备供应商、操作系统等。
- 客户端提供Active Directory凭证并提交登录表单。
- BYOD Web服务器根据Active Directory对凭证进行身份验证。
- 成功进行身份验证后，BYOD Web服务器将SCP请求发送到DHCP集群或故障转移对，以在DHCP客户端数据库中创建客户端条目（客户端类名、身份验证直到、设备类型、供应商、操作系统、MAC/DUID、用户名）。如果配置了LDAP，则仅在LDAP数据库中创建客户端。
- 最后，BYOD Web服务器将成功注册消息发送给客户端，其中包含其注册的所有设备的详细信息。
- 如果身份验证失败，BYOD Web服务器会以失败身份验证消息回复客户端。

BYOD配置

要构建支持BYOD功能的系统，您必须从开箱即用的设置中修改Cisco Prime IP Express配置，以启用服务器的一些高级功能。使用Cisco Prime IP Express区域服务器中的BYOD设置向导，您可以轻松完成此过程（BYOD配置设置）。

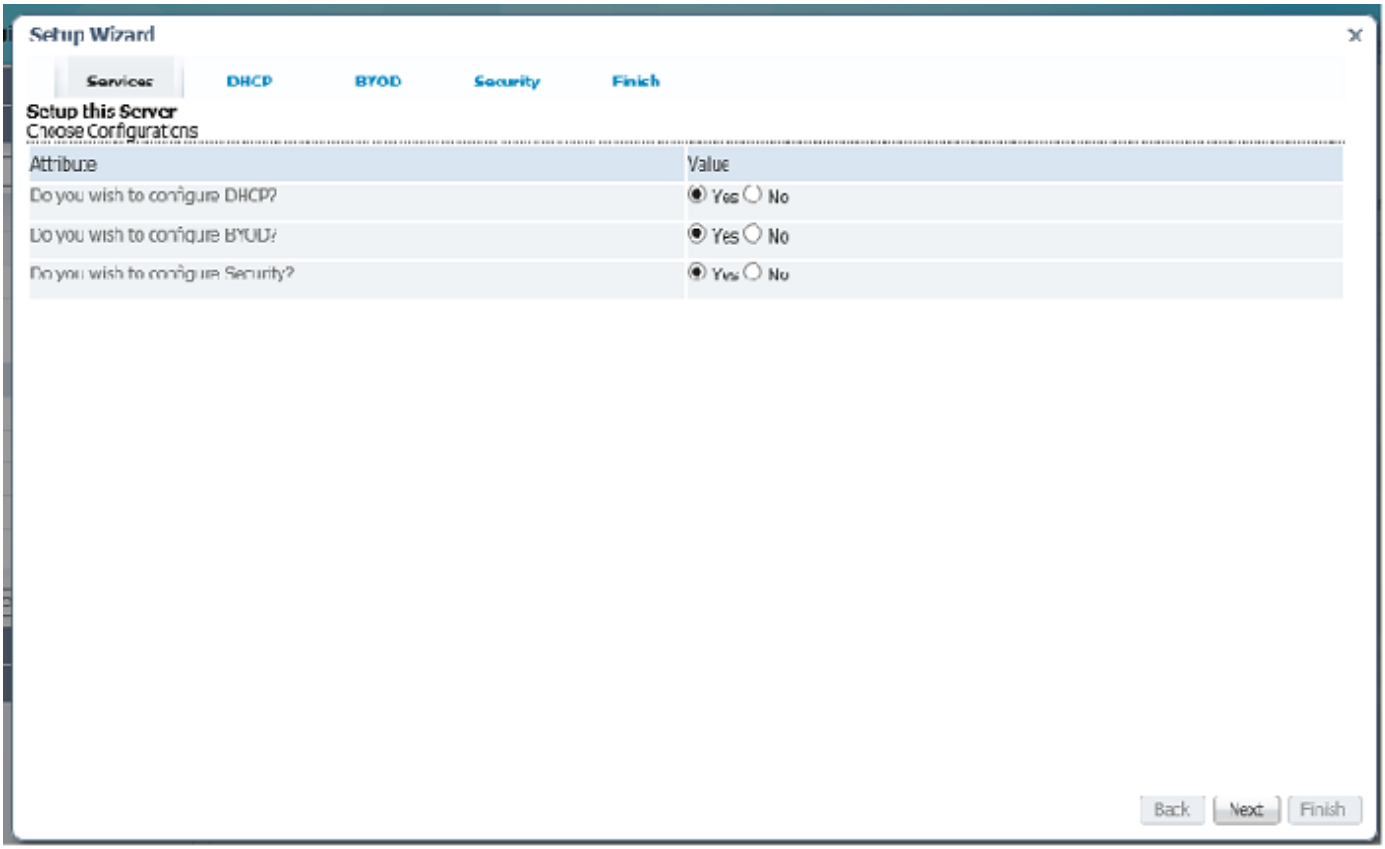
有关如何安装Cisco Prime IP Express的信息，请参阅《Cisco Prime IP Express安装指南》。

有关如何使用GUI的详细信息，请参阅快速入门指南和用户指南。

您可以在以下位置找到所有其他Cisco Prime IP Express生产文档：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-ip-express/tsd-products-support-series-home.html

BYOD设置向导

以下各节介绍Cisco Prime IP Express区域服务器中的BYOD设置向导工作流程。整个过程包括配置DHCP和CDNS服务器。对于简单设置，默认客户端用于未注册的BYOD设备，而用于复杂设置；使用client-class-lookup-id和client-lookup-expression。详细信息在用户文档/部署指南中提供。



DHCP 配置

要配置DHCP服务器，请完成以下步骤：

- 为故障转移选择值No。
- 为DHCPv4选择值Yes。
- 为DHCPv6选择值No，然后点击Next。
- “DHCPv4设置向导”页打开。
- 点击添加范围模板以创建范围。
- 在名称框中输入范围模板名称，然后点击添加DHCP范围模板按钮。
- 单击保存以保存范围模板，然后单击下一步以移动到下一页。
- 在Scope Name Expression文本框中输入(concat "byod-" subnet)。
- 在“范围表达式”文本框中输入(create-range first-addr last-addr)，然后点击保存以保存页面。单击 Next。
- 点击Add Subnet以创建子网。
- 在Address文本框中输入子网IP，例如10.76.206.0，然后点击Add Subnet按钮。
- 点击推送图标将子网推送到本地集群。
- 从Cluster or Failover下拉列表中，选择要向其推送子网的本地群集主机名。

- 从范围模板下拉列表中选择范围模板。
- 点击Push Subnet按钮。
- 单击“下一步”，转到“BYOD设置”页面。

BYOD配置

您可以使用BYOD Setup页面捕获CDNS服务器配置的详细信息，以创建域重定向规则（假设DNS）和未注册设备的租用时间。

1. 以下策略和客户端类在区域服务器中创建，并在设置向导页中进一步使用：BYOD策略名称：BYOD_未注册。添加DHCPv4 dhcp-lease-time选项(51)并设置DHCPv6 valid-lifetime和preferred-lifetime。为DHCPv4选择域名服务器选项6，为DHCPv6选择选项23。BYOD客户端类名：BYOD_Registered设置已排除的选择条件 — BYOD_Unregistered。BYOD客户端类名：BYOD_未注册。设置选择条件 — BYOD_Unregistered。设置策略 — BYOD_Unregistered。
2. 要配置BYOD，请执行以下步骤……从下拉列表中选择CDNS服务器。指定未注册客户端的时间，然后点击单击“下一步”，转到“策略”页。单击推送图标，从可用列表中选择本地群集主机名，然后使用返回箭头将其添加到目标群集，然后单击将数据推送到群集按钮。单击“关闭”按钮关闭“查看推送数据报告”。单击“下一步”移至“客户端类”页，然后单击“推送”图标，然后单击“将数据推送到集群”按钮。单击“关闭”按钮关闭“查看推送数据报告”，然后单击“下一步”转到“创建范围”页。在“值”下的文本框中指定百分比，以定义未注册客户端的IP范围。默认情况下，值为10。单击“下一步”转到“报告”页，此页显示分配给特定客户端的IP范围以及其他详细信息，如下图所示。单击“下一步”转到https配置页面。

区域服务器 — HTTPS配置

设置向导页面可用于Https配置；BYOD Web服务器需要这些详细信息。

要配置Https，请执行以下步骤：

- 使用“选择文件”按钮上传密钥库文件，并在“密钥库密码”文本框中输入密钥库密码，单击“上传”按钮，然后单击“下一步”以转到“重新加载服务器”页。

重新加载服务器

完成配置后，重新加载服务器页面可用于重新加载DHCP服务器、CDNS服务器和BYOD Web服务器。

为此，请执行以下步骤：

- 在“是”或“否”中指定值以重新启动BYOD Web服务器、CDNS Web服务器和DHCP Servers/Failover对，单击“重新加载服务器”按钮，然后单击“下一步”，“安全”页面打开。
- 从Value下拉列表中选择身份验证类型值Active Directory。
- 单击“保存并下一步”并移至“Active Directory页面”，然后单击“保存”。

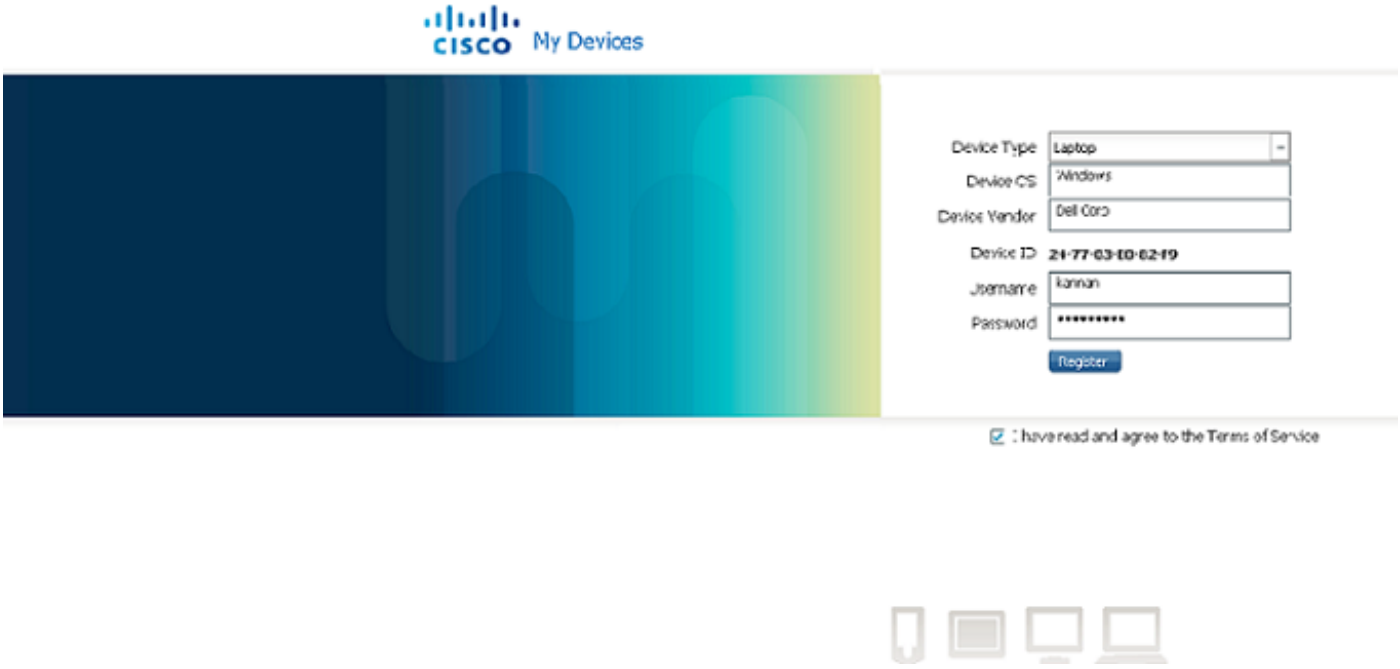
- 在各自的文本框中输入IP Address、Hostname和Port，例如IP=10.76.206.5、hostname= tmh2-chn-cnrent-AD1和port= 389，然后点击Add Address。
- 在域文本框中输入域名CPIPE.COM。
- 单击“下一步”，将打开“成功配置”页。单击完成完成配置设置过程。

设备注册页面

设备注册页面允许用户注册其设备。在本页中，预填了某些字段，如设备类型、设备操作系统、设备供应商和设备/ MAC ID，还允许用户编辑详细信息。但是，用户需要输入其凭证，例如：

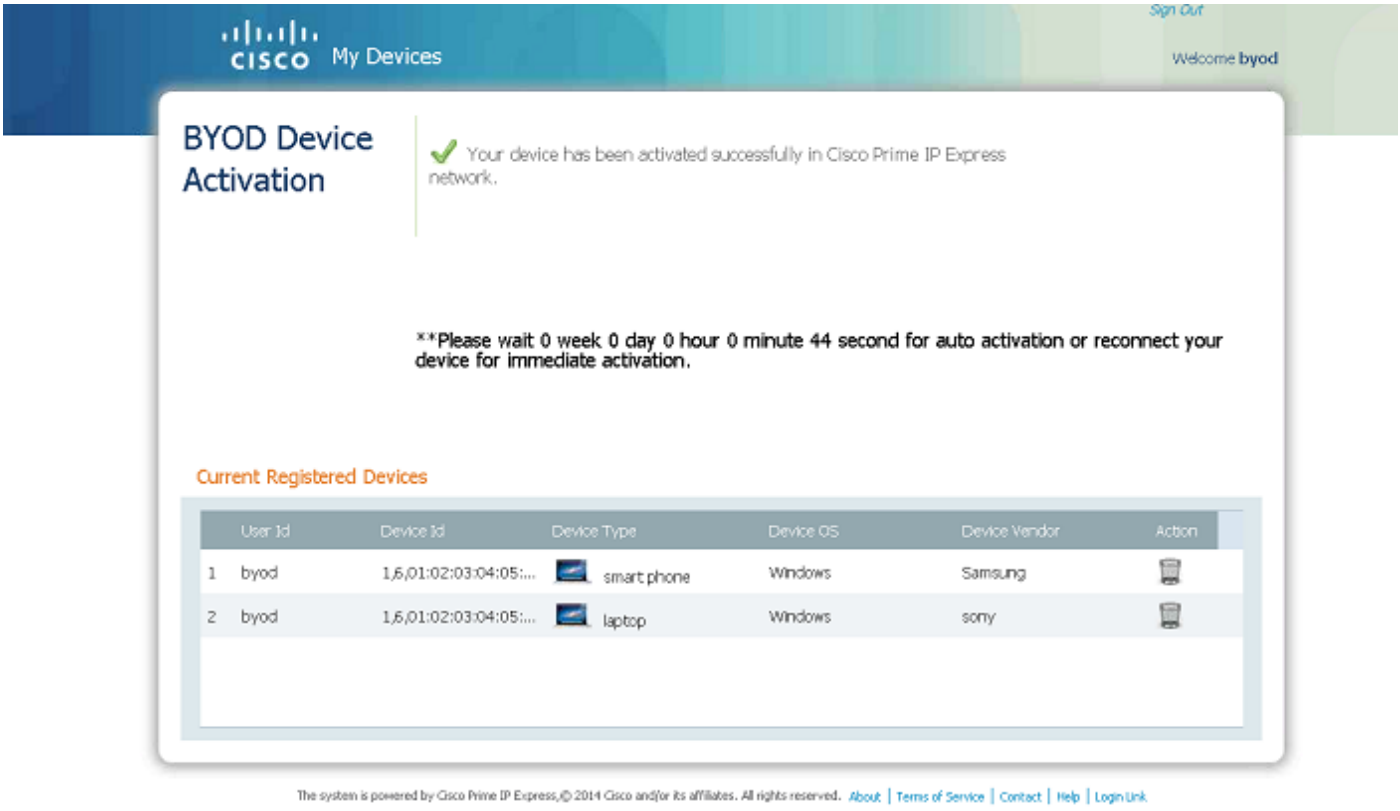
页面

- 用户名
- 密码
- 服务条款



激活成功页

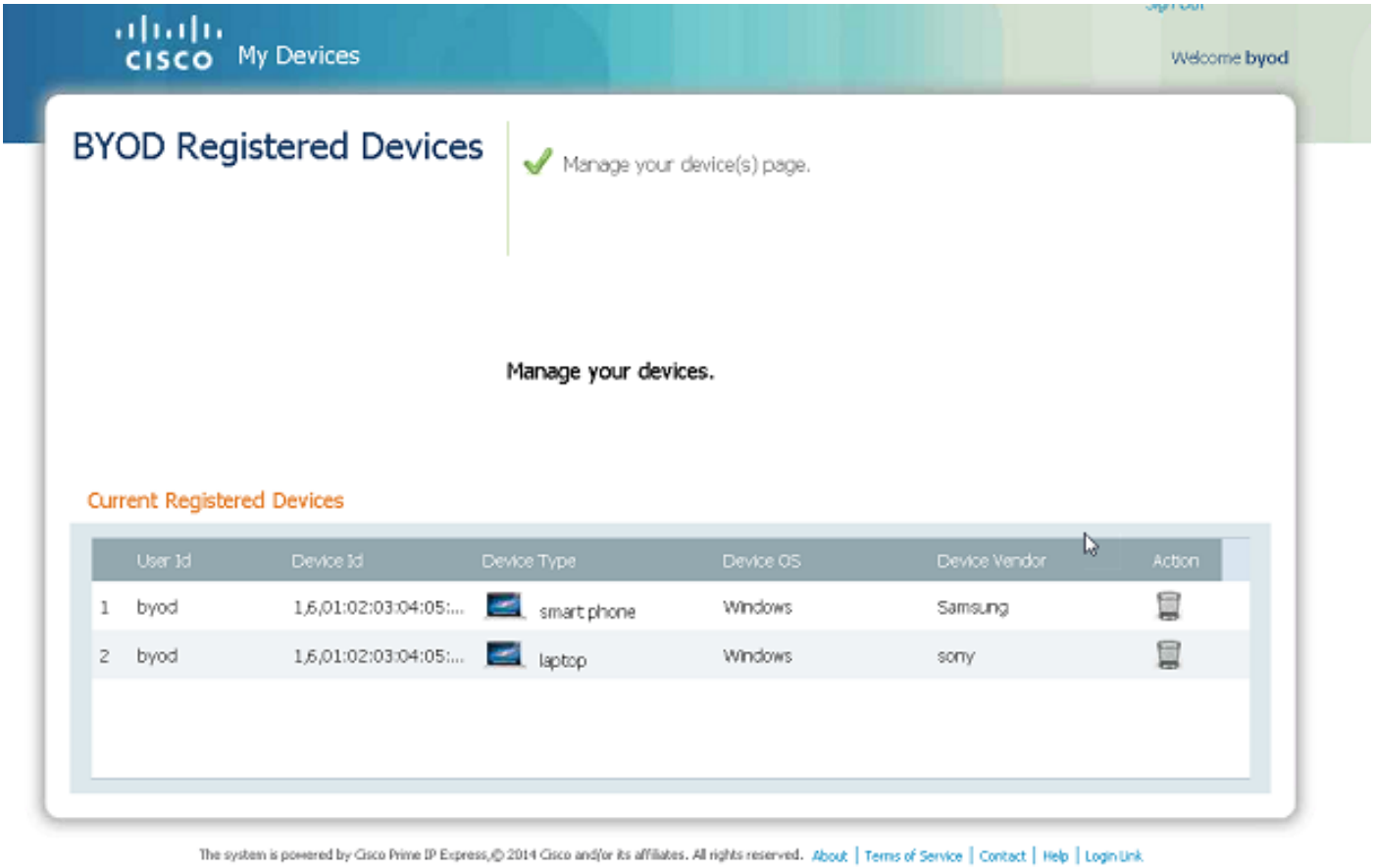
成功注册后，激活成功页显示包含自动激活和重新连接的租用时间的消息，如图所示。激活成功页还显示同一用户当前和以前注册的设备的列表。用户可以通过点击删除图标删除设备。



用于管理设备的用户登录页

用户登录页面允许用户删除其注册的设备。要登录到“用户登录”页面，用户需要提供其登录凭证，如用户名、密码，还需要接受服务条款。成功登录时，将打开BYOD注册设备页面。此页面用于管理已注册的设备，如删除设备。

- 用户名
- 密码
- 服务条款



查找表达式

查找表达式标识设备是现有设备还是未注册。它确定DHCP服务器的client-class-lookup-id属性的client-class，并且服务器在每个传入数据包上执行此表达式以确定数据包的客户端类。根据指定的表达式值，它返回一个字符串（数据包的客户端类名称，或指示客户端请求未考虑客户端类值的区别字符串）。查找表达式是为了确保每个客户端通过同一网络接收其适当的服务类别。

设置查找表达式

配置BYOD后，可通过以下步骤设置查找表达式：

- 单击专家进入专家模式。
- 打开“列表/添加DHCP客户端类”页，(导航：Design > DHCP Settings > Client Classes)
- 在左侧的“客户端类”窗格中创建或选择已创建的类。
- 在“编辑DHCP客户端类创建的客户端”页面的“创建新嵌入策略”下，在client-lookup-id和override-client-id中输入表达式，例如，在client-lookup-id文本框中输入(request option "relay-agent-info" "remote-id")，在override-client-id文本框中输入relay-agent-info "remote-id"。
- 点击 Save（保存），以保存设置。
- 打开“管理服务器”页(导航：操作>服务器>管理服务器)
- 在左侧的Manage Servers窗格中，点击Local DHCP Server（本地DHCP服务器）链接。
- 点击编辑本地DHCP服务器选项卡。

- 在client-class-lookup-id文本框中输入创建的客户端类名。
- 重新启动本地DHCP服务器以使这些更改生效。

LDAP客户端创建支持

当IP Express DHCP服务器启用LDAP客户端选项时，BYOD Web服务器启用“LDAP客户端创建”支持。

如果DHCP服务器在LDAP中启用了客户端查找，则BYOD在LDAP中创建客户端时需要区域服务器LDAP配置。

要在区域服务器中创建和配置LDAP客户端，请执行以下步骤：

- 单击专家进入专家模式。
- 打开“列表/添加LDAP远程服务器”页，(导航：Deploy > DHCP > LDAP)
- 点击左侧LDAP窗格中的添加LDAP图标，“添加DHCP LDAP服务器”窗口打开。
- 在名称和主机名文本框中输入LDAP名称和主机名，然后点击添加DHCP LDAP服务器。DHCP LDAP服务器在左侧的LDAP窗格中以给定名称添加。
- 点击左侧LDAP窗格中新添加的LDAP链接，“编辑LDAP远程服务器”(Edit LDAP Remote Server)页面打开，此页面名称和主机名将自动填充。
- 在相应的文本框中输入addr、端口值以及用户名和密码。
- 设置“enable” True的值。
- 设置启用“can-create”的值。
- 设置启用“can-query”的值。
- 设置启用“can-update”的值。
- 在查询下，输入“搜索路径”值。
- 在查询下，输入“搜索路径”值。
- 在Query下，保留“search-scope”的默认值SUBTREE
- 在创建设置(Create Settings)下，输入“dn-create-format”值
- 在“创建设置”下，输入“创建字典”值
- 在“创建设置”下，输入create-object-classes值
- 点击 Save（保存），以保存设置。
- 打开“管理服务器”页。(导航：操作>服务器>管理服务器)
- 在左侧的Manager Servers窗格中点击Local BYOD Web Server链接。

- 单击重新启动服务器图标重新启动本地BYOD Web服务器，使更改生效。

DHCP指纹

DHCP指纹是标识特定操作系统或设备类型的唯一标识符。

BYOD Web服务器读取“dhcp_fingerprints.conf”，并具有指纹(PRL)和操作系统说明的“HashMap”。

从DHCPv4租用查询应答中，BYOD Web服务器获取租用上用户定义的属性值并找到适当的操作系统（说明值）和操作系统编号。使用操作系统编号，它会找到适当的类定义，而类的说明会提供设备类型信息。

如果无法使用指纹文件识别操作系统供应商和设备类型，则使用http报头用户代理数据。模式匹配是对具有操作系统列表的主文件完成的。

要配置DHCP指纹，请执行以下步骤：

- 单击专家进入专家模式。
- 打开“列表/添加DHCP扩展”页，(导航：Deploy > DHCP > Extensions)
- 点击左侧Extensions窗格中的Add Extensions图标，Add DHCP Server Extension窗口打开。
- 在相应的文本框中输入扩展名"name"、"lang"、"file"和"entry"值。
- 点击Add DHCP Server Extension，然后点击Save以保存设置，添加新扩展。
- 点击左侧Add Extension窗格中的Extension链接，将打开Edit DHCP Extension页面。
- 单击右侧的“连接分机点”图标，“分机点”窗口打开，如图所示。
- 在“连接分机点”下，选择数据包解码后，然后单击“保存”，如图所示。
- 或者点击DHCP Extension Points选项卡，然后根据“post-packet-decode”选择Attach下拉列表。 此窗口也可用于取消连接连接的扩展。
- 打开“管理服务器”页面(导航：操作>服务器>管理服务器)
- 在左侧的Manager Servers窗格中，点击Local DHCP Server（本地DHCP服务器）链接。
- 单击重新启动服务器图标重新启动本地DHCP服务器以使更改生效。

注意：指纹应仅在本地服务器中配置。

主题配置

此页面允许BYOD管理员通过编辑主题属性（如特定颜色或颜色代码和徽标/背景图像）来编辑BYOD Web服务器页面的外观。

主题分为两种类型：非可定制默认思科主题和可定制主题。

要配置主题，请执行以下步骤：

- 单击专家进入专家模式。
- 打开“列表/添加自定义主题”页，(导航：部署> BYOD >主题)
- 单击左侧“主题”窗格中的“添加主题”图标，“添加自定义主题”窗口打开。
- 在相应的文本框中输入主题名称、背景颜色、登录页面标题字体颜色和页面标题字体颜色。
- 点击添加自定义主题(Add Custom Theme)，下一页将打开，其中包含您提供的详细信息。

注意：您可以使用此页上载背景图像、通用页标题图像、登录页徽标和通用页徽标。

- 单击“背景图像浏览”按钮，然后单击“上传”上传背景图像。
- 重复相同步骤，上传公共页眉图像、登录页日志和公共页徽标的图像。
- 点击 Save（保存），以保存设置。

内容页面

“内容”(Content)页面允许BYOD管理员配置特定于客户的消息，如注册/登录页消息、关于内容、服务条款、联系人和帮助。

当用户输入内容并提交或上传(.html)文件（表单）时。 它会为BYOD Web内容目录内的每个属性生成特定html文件，其中包含特定文件名，且内容链接指向特定html文件。

输入的内容放置在html段落标记之间，以确保内容以与输入内容相同的格式显示。

要配置内容页面，请执行以下步骤：

- 单击专家进入专家模式。
- 打开内容页面(导航：部署>BYOD >内容)
- 在各自的文本框中输入注册/登录页消息内容、关于内容、服务条款内容、联系内容和帮助内容的内容。
- 或者单击相应的浏览和加载按钮以导入内容。
- 点击 Save（保存），以保存设置。

词汇表

下面列出的列表描述了整个文档中使用的术语的缩写词。

自带设备：自带设备

广告：Active Directory

CPIPE:思科Prime IP Express

DHCP:动态主机配置协议

CDNS:缓存域名系统

ACL:访问控制列表

SCP:系统配置协议

CCM:中央配置管理器

RFC:请求命令

DUID:DHCP唯一标识符

LDAP:轻型目录访问协议