思科自带设备 (BYOD) CVD
版本 2.5

修订日期：2013 年 8 月 7 日

Cisco Validated Design

构建旨在解决业务问题的架构

作者简介

Zeb Hallock

Zeb Hallock，思科系统公司系统开发部技术营销工程师

Zeb Hallock 任职于思科的企业系统工程组，专门研究数字媒体系统。他也从事基于未来的协作系统的创建和开发，在该领域持有两项专利。他已在思科任职 10 年，致力于企业系统测试、基于 H.323 的视频会议的系统设计和测试，以及网络基础设施。他也是 Cisco Unified IP Contact Center Cisco Unified MeetingPlace 方面的研究专家。在加入思科之前，他曾担任局域网和 WAN 设计和实施方面的顾问。

John Johnston

John Johnston，思科系统公司系统开发部技术营销工程师

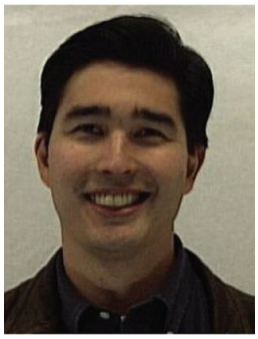
John Johnston 是思科系统开发部 (SDU) 的技术营销工程师。他已在思科任职 10 年，之前曾在思科高级服务组担任网络咨询工程师。在加入思科之前，他曾是 MCI 专业托管服务组的咨询工程师。在过去 15 年里， Johnston 一直致力于企业网的设计以及故障排除。在业余时间，他乐于处理基于微处理器的电子项目，包括无线环境传感器。 Johnston 持有 CCIE 认证 5232。他拥有北卡罗莱纳大学夏洛特校区的电气工程理学学士学位。

Fernando Macias

Fernando Macias，思科系统公司系统开发部解决方案架构师

Fernando Macias 是系统开发部 (SDU) 的解决方案架构师，专门研究企业市场分区的解决方案。 Fernando 已在思科任职超过 13 年，开发了包含视频、安全和内容交付产品在内的网络解决方案。 Fernando 也是思科高级服务团队的成员 （负责向大型企业公司提供网络设计支持），以及思科商业区域的系统工程师。在加入 SDU 之前， Fernando 专门研究云计算和安全，目标是引导公共部门客户了解云计算。

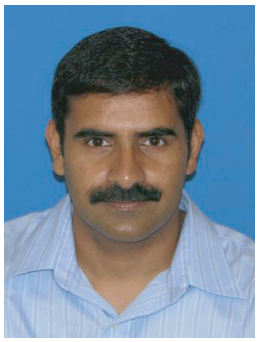
Fernando 不仅拥有技术管理和软件工程硕士学位，还拥有路由和交换方面的思科 CCIE 认证。



Roland Saville

Roland Saville，思科系统公司系统开发部技术主管

Roland Saville 是思科系统开发部 (SDU) 的技术主管，致力于为企业网部署制定最佳实践设计指南。他已在思科任职超过 15 年，曾担任系统工程师、咨询系统工程师、技术营销工程师和技术主管。在此期间，他专注于多种技术领域，包括将语音与视频集成到网络基础设施中、网络安全、无线局域网网络、 RFID 和能源管理。他也曾花时间研究零售市场分区。加入思科之前，他在雪佛龙公司担任了 8 年的通信分析师。 Saville 拥有爱达荷大学电气工程理学学士学位及圣塔克拉拉大学工商管理硕士学位。他曾与他人合著书籍 《Cisco TelePresence Fundamentals》（思科网真基础），并拥有 8 项美国 专利。



Srinivas Tenneti

Srinivas Tenneti，思科系统公司系统开发部技术营销工程师

Srinivas Tenneti 是思科系统开发部 (SDU) 技术营销工程师，负责 BYOD 项目安全组件的设计和架构。他已在思科任职 11 年有余，主要从事开发、系统测试及企业设计和架构工作。在过去 5 年里， Srinivas 研究 DMVPN 和 GETVPN 的设计和架构、分支架构、互联网边缘和用于 VPN 协议的 PKI 即服务。 Srinivas 与他人合著了书籍 *《PKI Uncovered: Certificate-Based Security Solutions for Next Generation Networks》*（PKI 揭秘：面向下一代网络的基于证书的安全解决方案）。

Mike Jessup

Mike Jessup，思科系统公司系统开发部技术主管工程师 / 架构师

Mike Jessup 于 1996 年加入思科，是思科系统开发部 (SDU) 的技术主管工程师 / 架构师。 Mike 主要从事 BYOD 系统架构和解决方案的确定和审批以及未来趋势等工作，并且与解决方案工程师合作，在思科验证设计中集成、验证和记录这些系统。 Mike 于 2011 年 11 月加入 SDU，之前曾在美国销售组织担任企业系统工程师，专门研究路由和交换、数据中心、应用优化和网络管理。自 1982 年直至加入思科， Mike 曾在多个信息系统公司和合作伙伴组织担任现场工程师和系统工程师职务。

Suyog Deshpande

Suyog Deshpande，思科系统公司系统开发部技术营销工程师

Suyog Deshpande 是思科系统公司系统开发部 (SDU) 的技术营销工程师，专门研究融合的有线和无线接入产品。 Suyog 已在思科任职 9 年，之前在无线网络业务部工作，那时他专门研究射频系统和融合接入产品。在加入思科之前， Suyog 担任过各种职务，涉及大规模无线网络的设计和部署，以及频谱智能和分析器产品的研究。

Tim Szigeti

Tim Szigeti，思科系统公司系统开发部技术主管

Tim Szigeti 是思科系统公司系统开发部技术主管，职责是针对 BYOD 解决方案设计网络架构。十多年来，他还专注于服务质量技术，在此期间他与他人合著了大量技术论文、设计指南以及 Cisco Press 书籍，包括 《End-to-End QoS Network Design》（端对端 QoS 网络设计）和《Cisco TelePresence Fundamentals》（思科网真基础）。 Szigeti 拥有 CCIE 认证 9794，以及不列颠哥伦比亚大学管理信息系统专业商业学士学位。

思科验证设计 (CVD) 计划简介

CVD 计划由一些经过设计、测试和记录的系统和解决方案组成，旨在提高客户部署的速度、可靠性和可预测性。如需更多信息，请访问 http://www.cisco.com/go/designzone。

思科自带设备 (BYOD) CVD 版本 2.5

第 1 部分

BYOD 设计概述

Cisco BYOD 解决方案组件

修订日期：2013 年 8 月 7 日

思科提供了全面的 BYOD 解决方案架构，该架构集合了整个网络的元素，为保护设备访问以及实现可视性和政策控制提供了统一方法。为了应对前文所述的诸多挑战， BYOD 实施不应视同于单个产品，而是应整合到一个智能网络。

下图显示了 Cisco BYOD 解决方案架构的高级示例。为了便于查看，我们将架构分为园区图和分支机构图来展示。以下部分详细说明了这些基础设施组件。

图 1-1　高级 BYOD 解决方案架构 - 园区视图

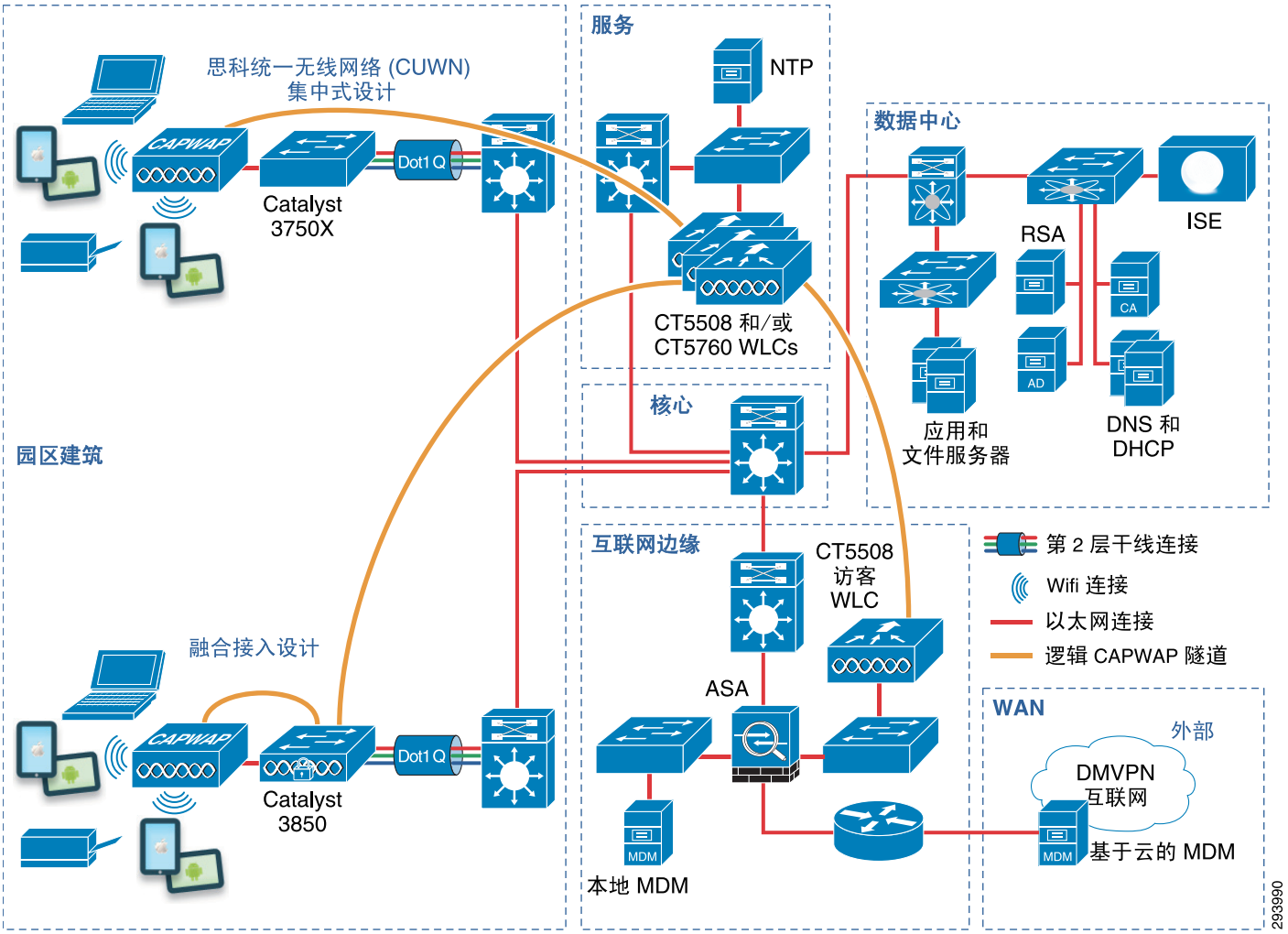
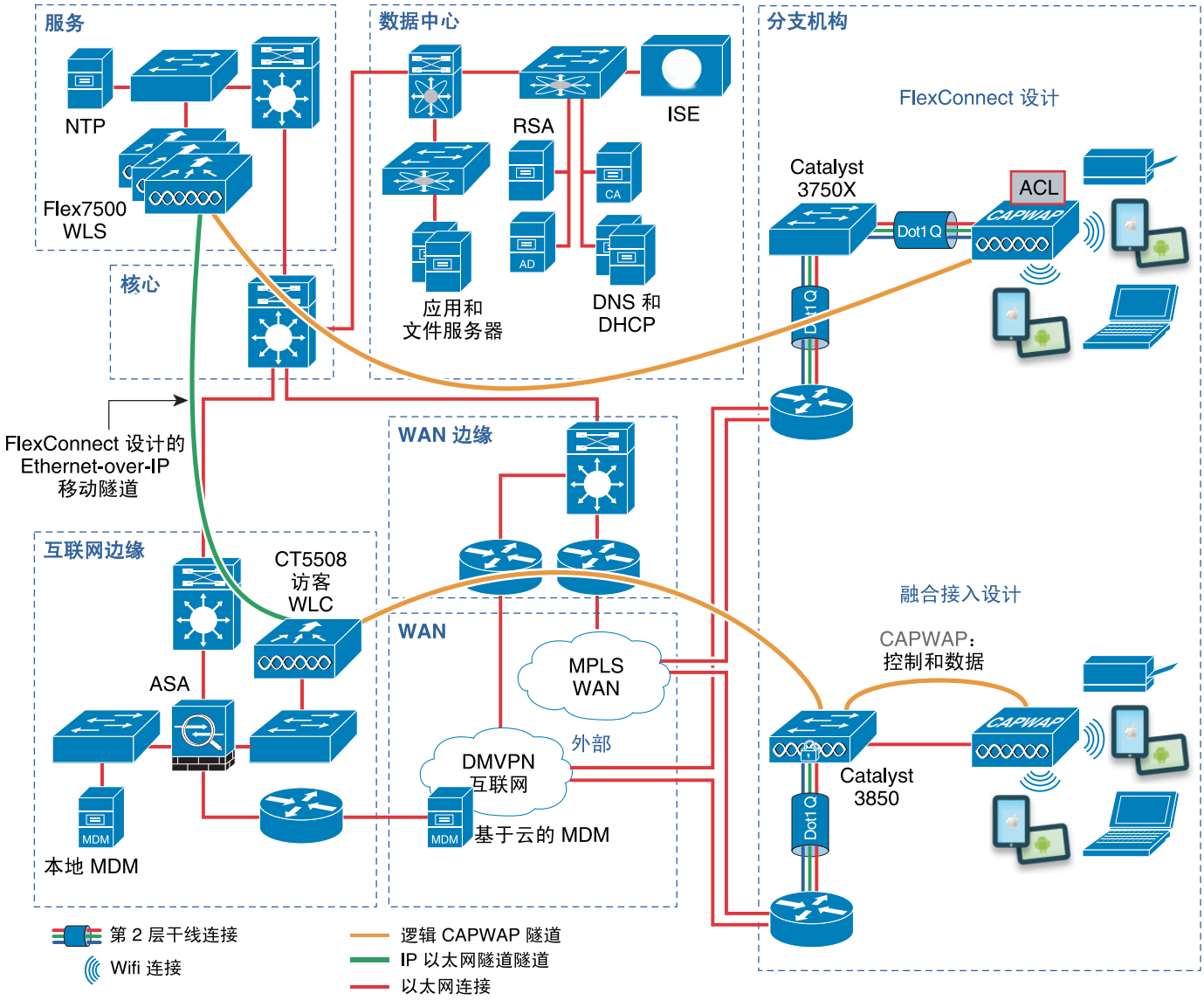


图 1-2　　高级 BYOD 分支机构解决方案架构 - 分支机构视图



思科接入点

思科接入点可为企业网络提供 WiFi 连接，并处理通过 802.1x 接入网络的身份验证请求。此外，分支机构位置处的思科接入点可以根据配置，将所有流量传输至园区或在本地交换流量。

思科无线控制器

思科无线局域网控制器 (WLC) 不但可用于自动化无线配置和管理功能，还可用于提供对 WLAN 的可视性和控制。 WLC 可以在提供集中接入点配置的同时，将同一接入策略和安全从有线网络核心扩展到无线边缘。 WLC 可与思科身份服务引擎 (ISE) 交互，实现对所有设备终端执行身份验证和授权策略。多个 WLC 可由 Cisco Prime 基础设施进行管理和监控。无线局域网控制器功能可以包含在独立设备中、集成到 Catalyst 交换机产品中，也可以虚拟运行于思科统一计算系统 (UCS) 中。集成控制器功能将在第 3 章，“BYOD 的园区网络和分支机构网络设计”的融合接入园区设计中讨论。

思科身份服务引擎

思科身份服务引擎 (ISE) 是 Cisco BYOD 解决方案架构的核心组件。它在一个通用平台上提供企业网络所需的必要服务，例如身份验证、授权和记帐 (AAA)、分析、状态和访客管理。 ISE 提供了一个统一策略平台，将组织安全策略与业务组成部分关联在一起。

ISE 还使用户能够按照 IT 部门定义的 BYOD 策略，通过自助注册门户负责设备自注册。通过发起人驱动的访客接入、设备分类、 BYOD 自注册和设备注册等功能，用户可以更灵活地将设备连入网络。

ISE 可与第三方移动设备管理器 (MDM) 集成，从而根据从 MDM 合规性规则获取的设备状态执行更精细的策略。

思科自适应安全设备

思科自适应安全设备 (ASA) 提供传统的边缘安全功能 （包括防火墙和入侵预防系统 (IPS)），同时还能为通过互联网的移动设备连接提供关键安全 VPN (AnyConnect) 终端 （包括家庭办公室、公共 WiFi 热点和 3G/4G 移动网络）。 ASA 提供的解决方案可满足公司拥有的设备和员工拥有的手提电脑、平板电脑或其他移动设备的连接和移动性要求。

Cisco AnyConnect 客户端

Cisco AnyConnect™ 客户端在受信任网络上提供 802.1x supplicant 客户端功能，并为通过非受信任网络（包括公共互联网、公共 WiFi 热点以及 3G/4G 移动网络）访问企业网络的设备提供 VPN 连接。部署和管理单个 supplicant 客户端不仅在操作上具有优势，而且为用户提供了共同的外观、感受和程序。

此外， AnyConnect 客户端还可用于以下目的：对 BYOD 设备进行设备状态评估、进行一定程度的策略实施、实施使用策略。

AnyConnect 客户端可以通过第三方 MDM 集中调配。这样不仅可以增强用户体验，还可以降低支持成本。用户可以通过配置 MDM 策略来管理有权使用 AnyConnect 的人员。

思科集成服务路由器

思科集成服务路由器 (ISR) （包括 ISR 2900 和 ISR 3900 系列）可为分支机构和家庭办公室提供 WAN 和局域网连接。局域网包括有线和无线接入。此外， ISR 具备直接连接到互联网和云服务、应用和网域网优化服务的能力，而且可以作为移动设备 VPN 连接的终端。

思科聚合服务路由器

思科聚合服务路由器 (ASR) 有多种配置，可在园区 WAN 边缘提供聚合 WAN 连接。此外， ASR 具备直接连接到互联网和云服务的能力，而且可以作为防火墙使用。 ASR 运行 Cisco IOS XE 软件，并提供灵活数据包匹配 (FPM) 及应用可视性与控制 (AVC)。

Cisco Catalyst 交换机

Cisco Catalyst® 交换机 （包括 Catalyst 3000、 Catalyst 4000 以及 Catalyst 6000 系列）可提供有线网络接入，并处理通过 802.1X 接入网络的身份验证请求。此外，该系列交换机在作为接入交换机部署时，可以为 VDI 工作站、 IP 电话和接入点等设备提供以太网供电 (PoE)。

思科融合接入交换机

Cisco Catalyst 3850 系列交换机可为设备提供融合的有线和无线网络接入。作为交换机， Catalyst 3850 可提供有线网络接入，并处理通过 802.1X 接入网络的身份验证请求。此外， Catalyst 3850 还包含集成在平台中的无线局域网控制器功能。作为无线控制器，它能够终止直接连接到 Catalyst 3850 交换机的接入点的无线流量，而不是将无线流量回传到集中式无线控制器中。这样可以针对无线流量提供更高的可扩展性，并提高交换机上无线流量的可视性。 Catalyst 3850 系列交换机与 Cisco ISE 交互，共同在整个设备终端执行身份验证和授权策略，从而为有线和无线设备提供单点策略实施。

当部署在分支机构位置的接入层时， Catalyst 3850 可配置为同时用作移动控制器 (MC) 和移动代理 (MA)，从而提供全面的无线控制器功能。当部署在大型园区时，Catalyst 3850 可配置为移动代理 (MA)，从而能够直接在交换机本身终止无线流量。为了提高可扩展性，可以将负责处理无线电资源管理 (RRM)、Cisco CleanAir、漫游功能和各种其他功能的移动控制器 (MC) 功能迁移到专用的 CT5760 或 CT5508 无线控制器。 Catalyst 3850 和 CT5760 无线控制器都运行 IOS XE 软件，可使 Cisco IOS 平台的丰富功能得到全面发挥。

Cisco Nexus 系列交换机

Cisco Nexus 交换机 （包括 Nexus 7000 和 5000 系列）在 CVD 中用作数据中心交换机。 Nexus 7000 交换机在园区核心、数据中心核心和聚合层之间提供 10GE 第 3 层连通性，并利用 VPC 为数据中心接入层 （所有服务器都连接到该层）的 Nexus 5000 交换机提供 10GE 第 2 层连通性。

Cisco Prime 基础设施

Cisco Prime 基础设施 (PI) 是思科激动人心的新产品，其目的是在实现无线和有线基础设施管理的同时，将来自多个组件的信息整合到一个位置。 Prime 基础设施不仅支持基础设施管理，还提供了一个用于发现网络访问者、所用设备、所在位置和访问时间的单一点。

Cisco Prime 基础设施 1.2 是 Cisco Prime 网络控制系统 1.1 (NCS) 的演进版本。它在改进 NCS 1.1 既有功能的同时提供了额外的基础设施和有线设备管理及配置功能。

Cisco Prime 基础设施可与其他多种组件交互，作为中央管理和监控门户。 Prime 基础设施直接与另外两种基于设备的思科产品 （思科移动服务引擎 (MSE) 和身份服务引擎 (ISE)）集成，以实现信息整合。 Prime 基础设施控制、配置并监控所有思科无线局域网控制器 (WLC)，通过扩展，还可以涵盖网络中的所有思科接入点 (AP)。Prime 基础设施还可配置和监控 Cisco Catalyst 交换机和思科路由器。

安全访问企业网络

新设备的自注册 （证书注册和配置文件调配）应该方便最终用户，而且只需最低限度的 IT 部门干预，对员工自有设备而言尤为如此。选择设备并不代表要放弃安全性。 IT 部门必须制定最低安全基准，所有设备必须符合此基准才能访问企业网络。此基准应包括 WiFi 安全性、 VPN 访问，以及用于预防恶意软件的附加软件。适当的设备身份验证对于确保新设备安全自注册、确保安全访问网络中的其他设备至关重要。因此，适当的设备身份验证可保护整个网络基础设施。

实施 BYOD 解决方案之前，需要考虑*谁*在访问网络、他们在使用*什么*设备，以及他们在*哪里*。用户可以从园区或分支机构位置启动调配流程。通过本设计，用户可以从任一位置调配和访问资源。过去，用户名 / 密码是大多数员工从有线工作站访问网络时所需的全部信息。通常情况下，收集和验证用户凭证会使用简单的服务器。随着组织在其网络中实施无线支持，用户除了需要具有用户名和密码，还要有一个唯一 SSID （无线网络名称）。

现在，数字证书和双因素身份验证为网络访问提供了更安全的方式。通常，最终用户必须下载客户端软件来请求证书和 / 或提供用于访问的安全令牌。将数字证书部署到客户端终端的挑战之一为：用户和终端可能需要直接访问公司的证书颁发机构 (CA) 服务器 （在通过验证可以访问公司网络后），以便手动安装客户端证书。此方法需要最终用户手动安装客户端证书，并确保其安装在本地终端的适当证书库中。

在基于非 PC 的设备中部署数字证书的流程有所不同，因为许多此类设备无法对创建 / 下载和安装数字客户端证书所需的所有特性和功能提供本地支持。随着用户移动性的增强，对访问网络的用户和设备进行身份验证已成为 BYOD 的一个重要方面。

证书注册和移动设备调配

将数字证书部署到终端设备需要一个可安全灵活地执行不同安全策略 （无论连接是从哪里发起）的网络基础设施。此解决方案的重点在于提供数字证书注册并进行调配，同时执行不同的权限级别。除 Windows 7 和 Mac OS X 以外，本设计指南还涵盖 Android™ 和 Apple® iOS™ 移动设备。

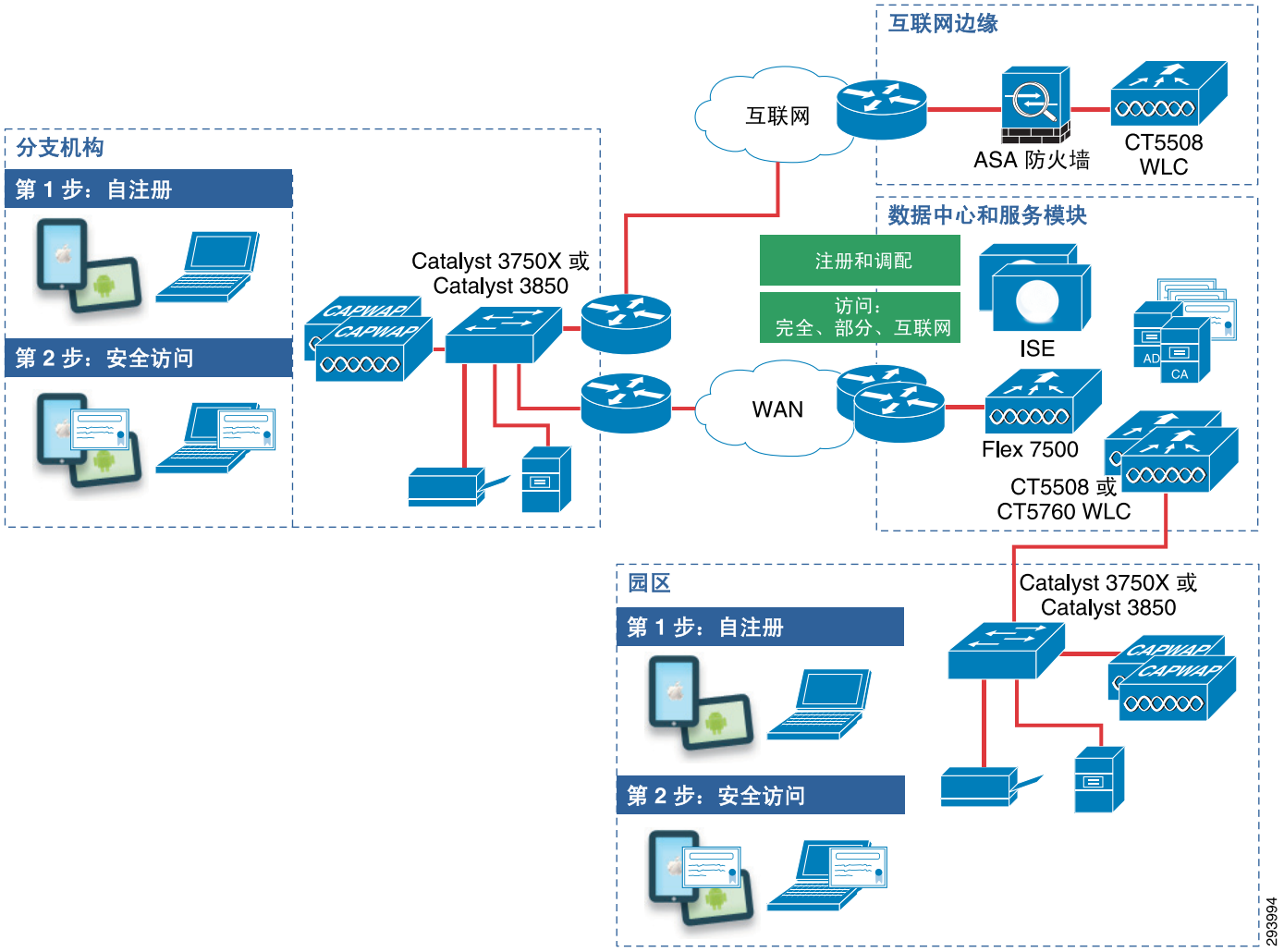
图 1-3 重点展示了移动设备连接到网络时，本解决方案要执行的常规步骤：

1. 一台新设备连接到称为 BYOD_Provisioning SSID 的调配 SSID。此 SSID（开放或通过 PEAP 确保安全）被配置为将用户重定向到访客注册门户。
2. 在用户正确通过身份验证后，便会开始进行证书注册和配置文件调配。
3. 调配服务获取有关移动设备的信息并调配配置文件，其中包含一个 WiFi 配置文件，该文件带有连接到名为 BYOD_Employee SSID 的安全 SSID 的参数。
4. 在后续连接中，设备使用 BYOD_Employee SSID，并根据不同的 ISE 授权规则被授予网络资源访问权限。

本设计指南还包括一个单 SSID 环境，其中使用同一 SSID 进行调配和安全访问。

未完成调配流程的员工设备只需连接到访客 SSID 或类似独享访客的 SSID ；该 SSID 可能配置为向访客或员工提供仅限互联网的访问权限或有限访问权限。

图 1-3　　注册和调配移动设备



BYOD 使用案例

修订日期：2013 年 8 月 7 日

组织的企业策略会规定内部 BYOD 解决方案所必须履行的网络访问要求。以下四个用例示例是组织可能实施的访问要求：

- 增强型权限 - 此用例为个人设备以及公司分发的设备提供网络访问权限。通过此用例，企业能够制定适当的策略来实现基于角色的细粒度应用访问，并扩展内部和外部安全框架。
- 有限权限 - 此用例可提供仅限于公司分发设备的访问权限。
- 高级权限 - 此综合用例也可以为个人和公司分发的设备提供网络访问权限。但是，通过与第三方移动设备管理器 (MDM) 集成，它可将设备的状态纳入网络访问控制决策。
- 基本权限 - 此用例是对传统无线访客访问权限的扩展。若企业策略不是为了使员工个人无线设备实现入网 / 注册，但仍提供仅互联网访问权限或部分网络访问权限，此用例可作为一种备选方法。

ISE 评估数字证书、 Active Directory 组成员身份、设备类型等，以此确定所要应用的网络访问权限级别。 ISE 提供灵活的工具集，用以识别设备并根据用户凭证和其他条件实施唯一的访问权限。

图 2-1 展示了本设计指南配置的各种权限级别。通过下列方法可实施这些访问权限级别：使用无线控制器或 Catalyst 交换机中的访问列表；将安全组标记 (SGT) 分配到设备流量；采用动态虚拟 LAN (VLAN) 分配。设计指南介绍了实施所需权限的各种方法。

图 2-1　　权限级别

	权限	访问
	完全访问	互联网和所有企业资源
	部分访问	互联网和部分企业应用
	仅互联网	仅互联网
	拒绝访问	明确拒绝网络访问

292593

增强型权限 - 个人和企业设备

此用例以有限权限用例为基础，通过注册数字证书和调配配置文件为入网个人设备提供基础设施。用例主要介绍如何根据身份验证和授权规则，为个人设备提供不同的访问权限级别。

对于已使用自助注册门户注册设备，且已收到根据其 Active Directory 组成员身份向其授予唯一访问权限的数字证书的员工：

- 完全访问 - 如果员工是 BYOD_Full_Access Active Directory 组成员。
- 部分权限 - 如果员工是 BYOD_Partial_Access Active Directory 组成员。
- 互联网权限 - 如果员工是 Domain Users Active Directory 组成员。

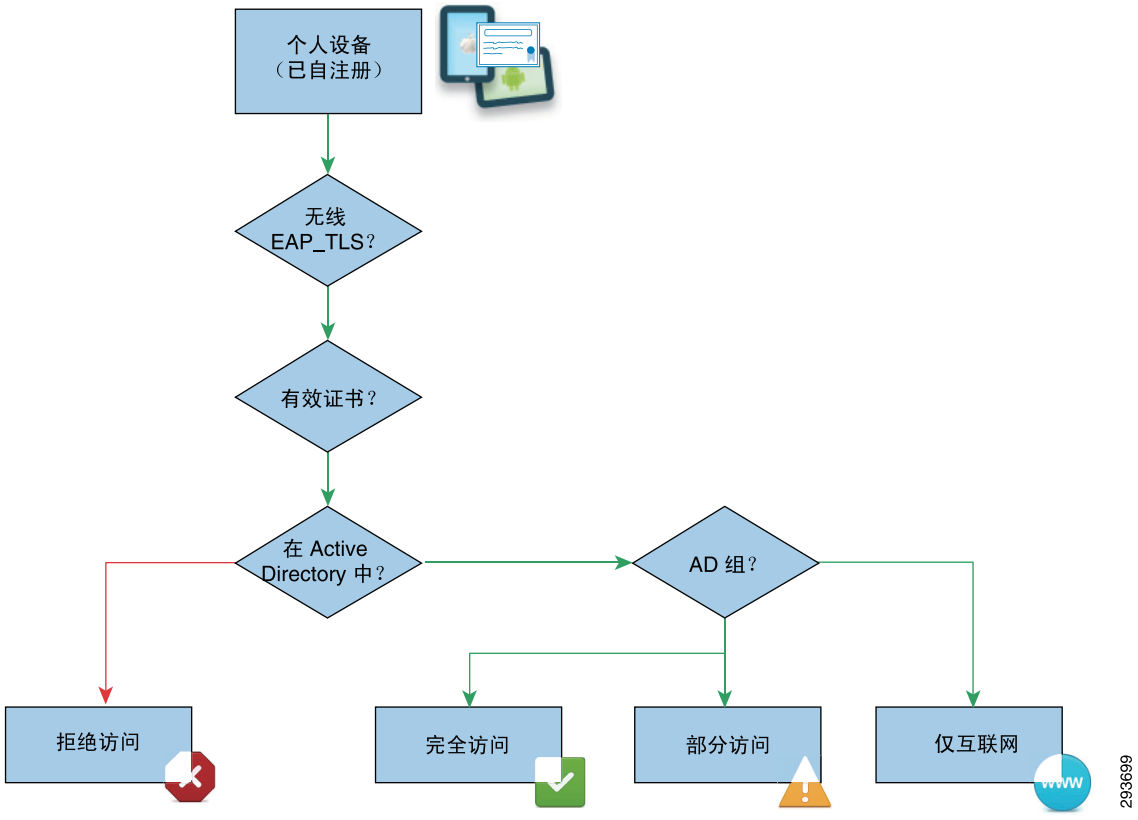
此用例向公司拥有的设备授予完全访问权限。

此外，用例还介绍了如何阻止个人拥有的设备（例如 Android 设备）访问网络。一些组织可能尚未准备好允许员工将个人设备连入网络，可能会阻止这些设备访问，直至他们满足企业或法律要求。 Cisco ISE 能够识别（分析）设备类型和阻止这些设备连入网络。例如，此用例涉及到 ISE 的设备分析功能，拒绝向 Android 设备授予访问权限。

作为 ACL 的备用方案，安全组标记可对园区无线用户和设备实施基于角色的策略。安全组标记采用免费技术提供实施策略和流量限制的可扩展方法，而且如果不需要 TCP/UDP 端口级别粒度化，会将 ACL 需求降至最低，在某些情况下甚至没有 ACL 需求。

图 2-2 重点展示了个人设备的连接流程。

图 2-2　　个人设备 BYOD 访问权限



此用例可以为组织提供一种接受其员工 BYOD 环境的有效方法，并提供网络资源差异化权限。

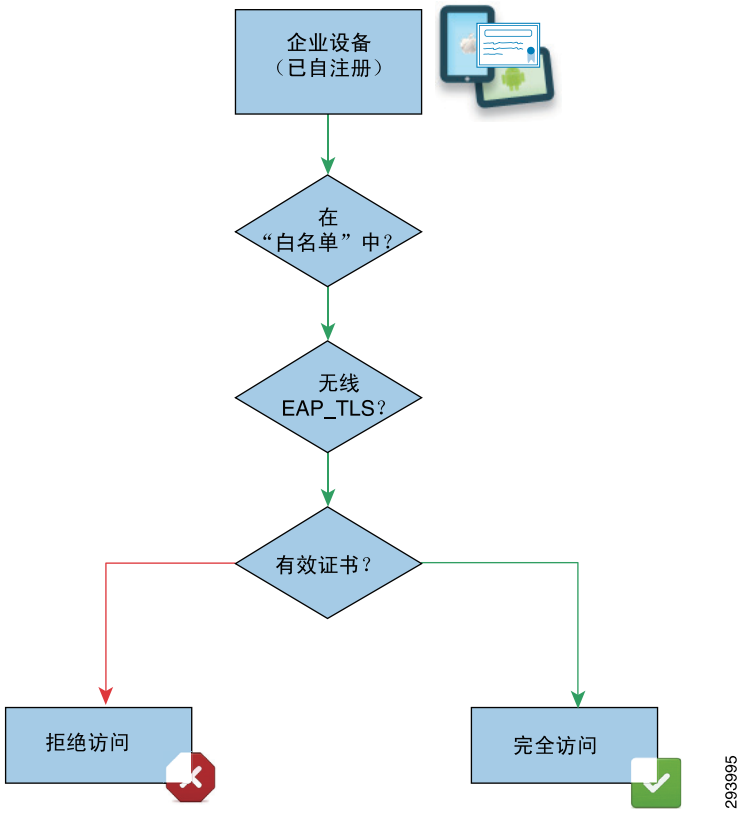
有限权限 - 公司设备

此用例适合满足下列条件的组织：决定实施更严格的策略，仅允许公司拥有或管理的设备访问网络，并拒绝向员工个人设备提供访问权限。

ISE 基于设备的证书和白名单身份组资格授权网络完全访问权限。此用例介绍白名单的使用，该名单是一系列在授权阶段评估并由 Cisco ISE 维护的企业设备。

图 2-3 展示了企业设备的连接流。

图 2-3　企业设备 BYOD 访问权限



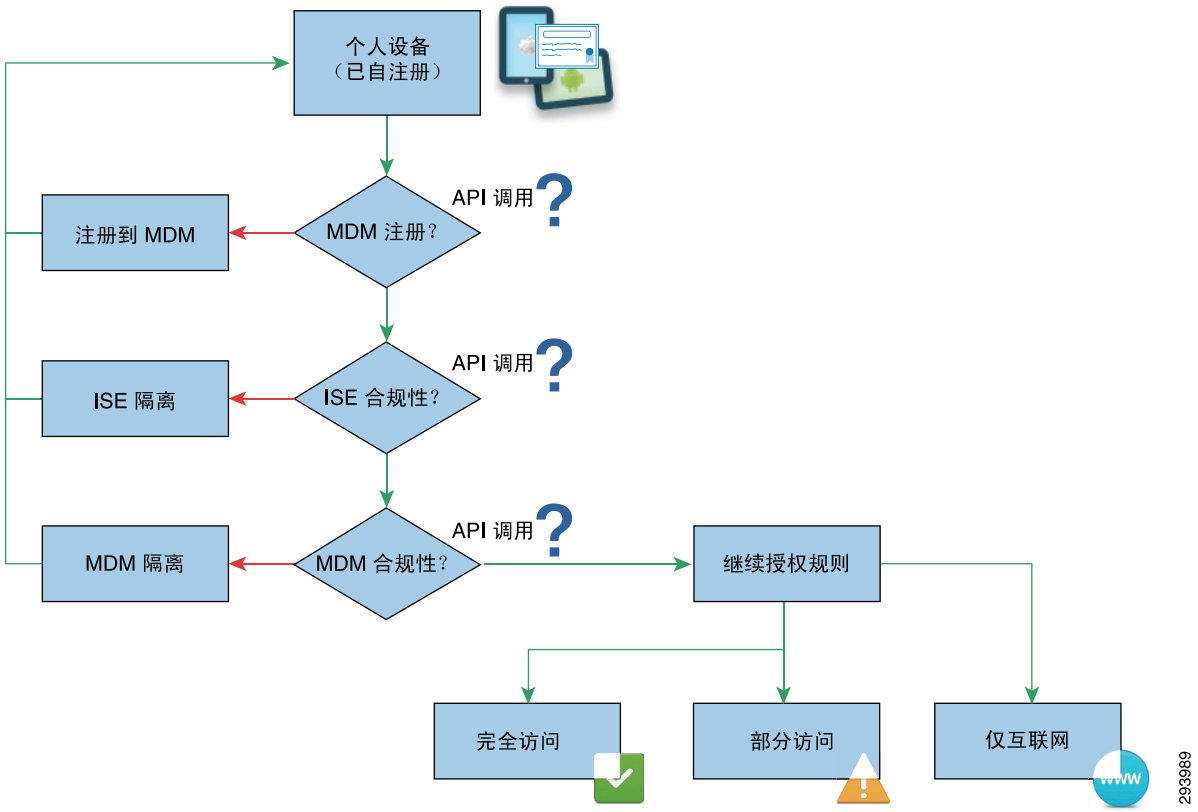
高级权限 - MDM 状态

此用例适合已购买移动设备管理器 (MDM) 来管理和保护移动终端的组织。MDM 不能实施网络访问控制策略时，它们将提供 ISE 不提供的唯一设备状态信息。通过将 ISE 策略与其他 MDM 信息相结合，可在移动终端上强制实施安全策略。

ISE 和第三方 MDM 之间的集成通过 REST API 实现，从而让 ISE 能够查询 MDM 以获得更多合规和状态属性。

图 2-4 展示了获得 MDM 合规信息和网络访问权限的连接流。

图 2-4　　MDM 合规性



基本权限 - 访客型

一些组织可能实施了一种业务策略，该策略不向入网无线员工个人设备提供访问权限，却为此类设备提供一些访问公司服务和互联网的权限。一些可能的原因包括：

- 组织不希望或无法在员工个人设备上部署数字证书。
- 员工可能不愿意让组织 “管理” 个人设备。
- 使用个人设备时，组织不愿意管理和维护单独的注册设备列表，或者管理用户的网络访问权限级别。

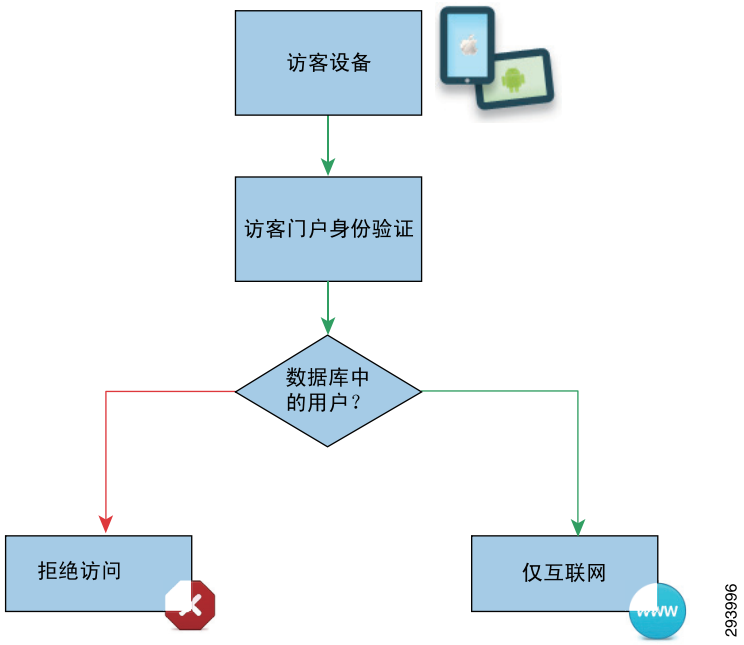
此用例设计的原则是，扩展传统访客无线访问，并为员工个人设备提供类似于访客的无线访问权限。设计指南主要介绍两种扩展访客无线访问权限的方法，以便员工个人设备能够访问访客网络：

- 允许员工自行调配访客凭证。
- 扩展访客网络身份验证 （网络身份验证），以便在对使用个人设备的访客和员工进行身份验证的同时使用 Microsoft Active Directory (AD) 数据库。

此外，设计指南还讨论了另一种方法，即为员工个人设备提供第二种访客型无线 SSID。

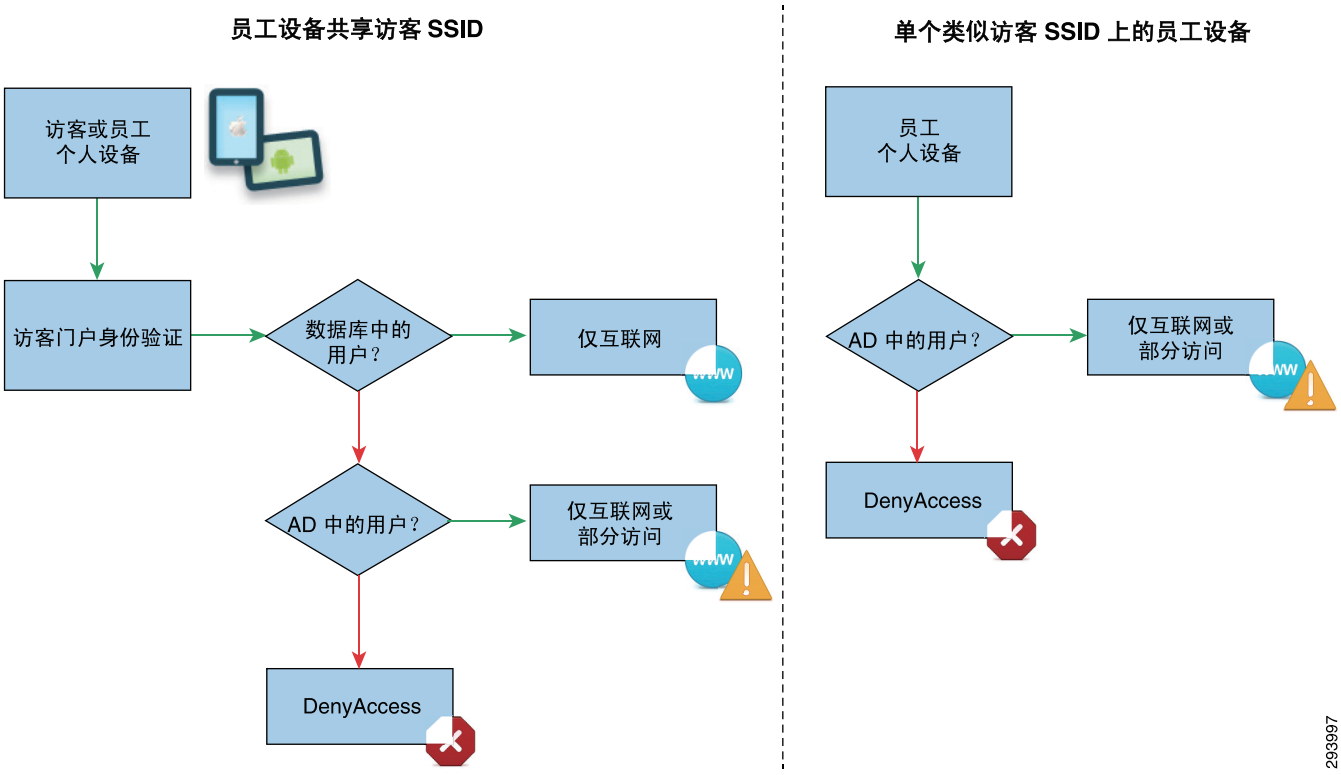
基本权限用例以传统无线访客访问为基础。图 2-5 展示的是对连接到访客无线网络的设备进行身份验证的常规方法。

图 2-5　　访客无线访问



本设计指南讨论了两种修改现有访客无线访问实施的方法，以便为员工个人设备提供基本访问权限，如图 2-6 中所示。

图 2-6　　基本权限



BYOD 的园区网络和分支机构网络设计

修订日期：2013 年 8 月 7 日

园区网络设计

正如分支机构网络设计，当且仅当实施一个设计合理的园区网络基础设施时，策略实施才有效。本节讨论园区 LAN 设计的高级关键设计要素。

本设计指南中讨论的两个园区 WLAN 设计分别是集中式接入 （本地模式）和融合接入设计。

集中式 （本地模式）无线设计

思科统一无线网络 (CUWN) 本地模式设计是指 WLAN 设计，这类设计的所有数据和控制流量从接入点回传至无线控制器，然后终止并放置在以太网网络中。这种设计也称为集中式无线设计或集中式无线叠加网络。大型园区常见的建议设计是将所有无线控制器放置到连接至园区核心的独立服务模块中。

此设计的潜在优势如下：

- 从园区网络的一个点对所有无线流量进行集中访问控制。
- 无线漫游的复杂性降低，因为无线控制器可以共享无线客户端更大的 IP 地址池。

此设计的潜在劣势如下：

- 无线控制器或连接至无线控制器的网络基础设施可能存在扩展瓶颈。这是因为，所有无线流量均回传至园区网络中部署无线控制器的一个中心点，然后在以太网网络上终止。但是请注意，这种问题可通过下列方法消除：部署更多集中式无线控制器；升级到更新的平台（例如 Cisco CT5760 无线控制器）；和 / 或将无线控制器移出楼宇分布模块。
- 无线流量的可视性降低，因为在穿越园区网络基础设施过程中，无线流量被封装到 CAPWAP 隧道中。

在本地模式设计中，连接到楼宇分布模块内部接入层交换机的接入点通过一个或多个集中式 WLAN 控制器进行配置和控制。在本设计指南中，我们使用一组专用于园区的 Cisco CT5508 无线控制器作为这类控制器，因为，它们为支持本地模式接入点提供比 Cisco Flex 7500 无线控制器更高的扩展能力。如前文所述，所有数据和控制流量从接入点回传至无线控制器，然后终止和放置在以太网网络中。园区基础设施内的访客无线流量被回传至园区 DMZ 网段中的专用 CT5508 访客锚点控制器。

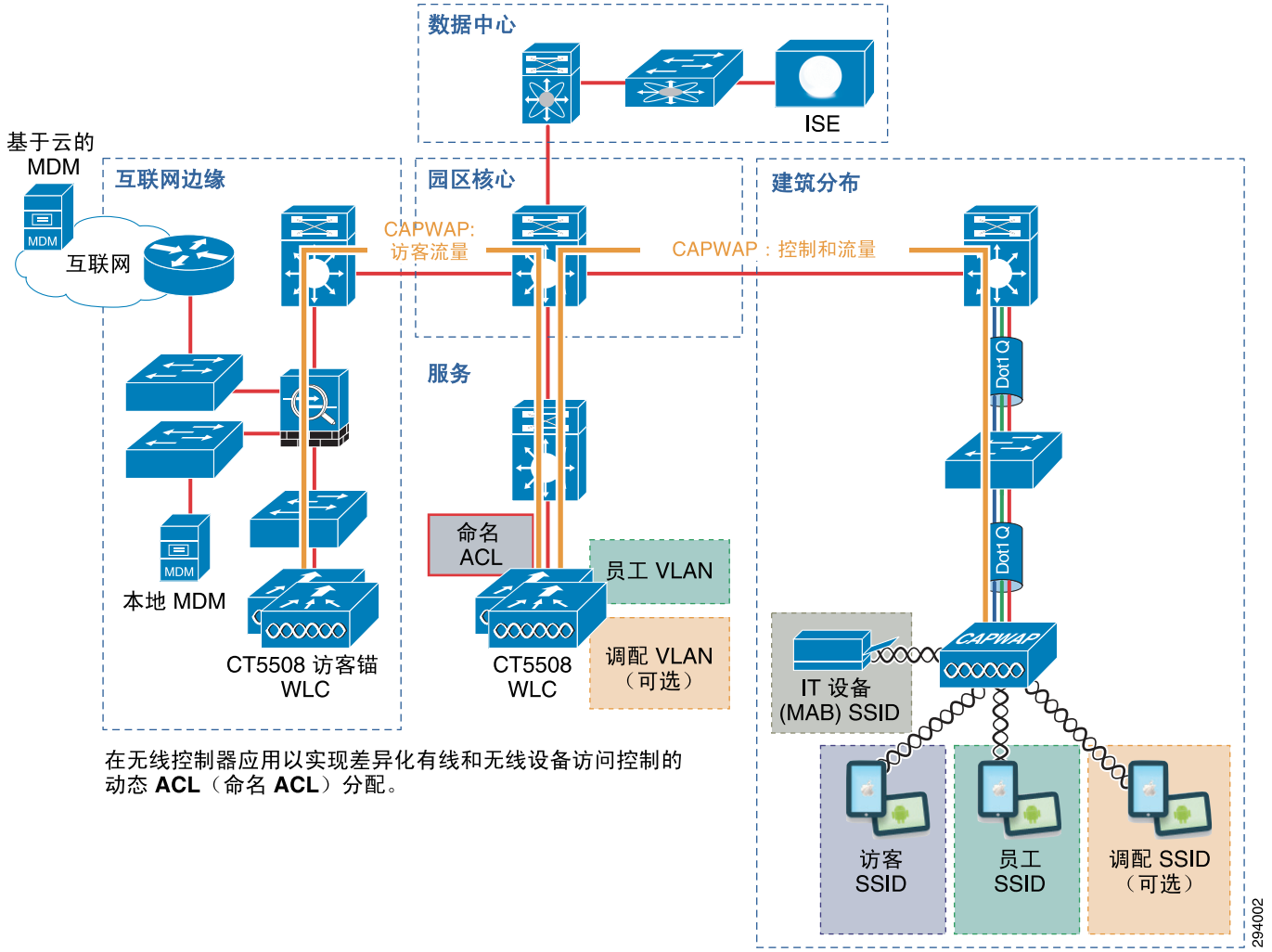
为了实施 BYOD 使用案例，我们研究了两种不用的为使用本地模式无线设计的园区提供差异化访问控制的方法。两种方法是：

- 对设备进行身份验证和授权之后应用适当的动态 ACL。
- 对设备进行身份验证和授权后，在设备上应用适当的安全组标记 (SGT)。

通过动态 ACL 实施访问控制时，设计指南选择的特定动态 ACL 为 Radius 指定的本地 ACL，也称为命名 ACL。而且，每个 CT5508 无线控制器上都必须配置这些命名 ACL。例如，我们会向已授予网络完全访问权限的个人设备静态分配与已授予部分权限的个人设备相同的 VLAN，但是会向每台设备应用不同的命名 ACL，从而授予不同的网络访问权限。

图 3-1 简要展示了如何在园区内实施使用命名 ACL 进行访问控制的集中式 （本地模式）无线 BYOD 设计。

图 3-1　　集中式 （本地模式）无线园区 BYOD 设计高级视图



在无线控制器应用以实现差异化有线和无线设备访问控制的动态 **ACL**（命名 **ACL**）分配。

通过安全组关联 (SGA) 实施访问控制时，必须在 Cisco ISE 中配置多个源和目标安全组标记 (SGT)。我们会向已授予网络完全访问权限的个人设备静态分配与已授予部分权限的个人设备相同的 VLAN，但是会向每台设备应用不同的 SGT，从而授予不同的网络访问权限。

安全组标记概述

在 BYOD CVD 的所有版本中，策略实施都是通过使用访问控制列表和 VLAN 完成的，以便在成功进行身份验证和授权之后根据需要限制用户流量。同时考虑应用 ACL 的设备数量以及为安全控制网络访问所需的持续维护因素，使用 ACL 可能会变成一项艰巨的管理负担。

BYOD v2.5 使用名为 TrustSec 的免费技术和安全组标记 (SGT)。安全组标记是一种简单的实施角色型策略的替代方法，而且，很少需要，在某些情况下甚至不需要 ACL，如果对 TCP/UDP 端口级别精确性没有要求。

安全组标记可作为园区无线用户和设备的 ACL 替代方法，在园区内，思科无线控制器集中部署在共享服务块中，并配置为在本地模式下运行。

ACL 复杂性和注意事项

到目前为止，实施流量限制和策略的方法包括：在无线控制器上使用各种命名 ACL、在多个路由和交换平台上使用静态和可下载 ACL 以及对分支机构中的 FlexConnect 无线流量使用 FlexACL。为配置和部署这些 ACL，需要结合使用通过 Telnet/SSH 的命令行 (CLI) 设备访问，或对静态配置的 ACL 使用的 Prime 基础设施等网络管理，同时使用思科身份服务引擎 (ISE) 集中定义可下载 ACL (DACL)，并将其推送至交换平台。

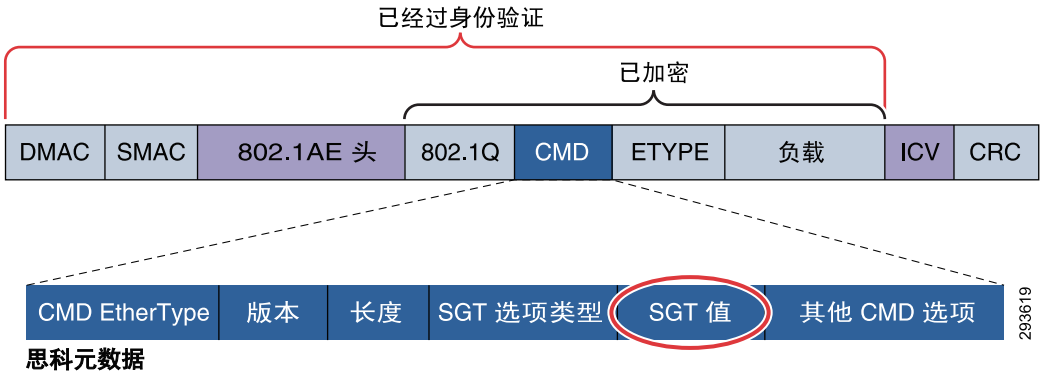
- 不同位置 （例如分支机构或区域机构）可能需要不同的 ACL，在这些位置可能需要对本地资源 （例如打印机、服务器等）实施用户权限。
- 企业策略变更可能会加剧 ACL 运营的复杂性。
- 安全漏洞风险会因潜在的设备错误配置而增加。
- 策略实施基于 IP 地址时， ACL 定义将变得更复杂。
- 平台功能 （例如处理器内存，可扩展性）或 TCAM 资源可能会受复杂 ACL 的影响。

通过实施思科安全组访问架构和使用安全组标记，Cisco TrustSec 为策略实施提供了可扩展的集中式模式。

安全组标记

安全组标记 （也称之为 SGT）支持通过将 IP 地址随机分配给由随意定义的 SGT 表示的封闭用户组对主机的 IP 地址进行抽象化。这些标记由 ISE 集中创建、托管和管理。安全组标记是在第 2 层帧的思科元数据字段中传输的 16 位值，如图 3-2 中所示。

图 3-2　　第 2 层 SGT 帧格式



安全组标记由管理员在 Cisco ISE 上定义，并由任意名称和 1 至 65,535 之间的十进制值表示，其中 0 为 “未知”保留。利用安全组标记，组织可以根据用户或设备在网络中的角色制定策略，从而为基于安全组标记，而不是 ACL 中 IP 地址的安全策略提供抽象层。

本 CVD 中的 SGT 部署方案

具体来讲， SGT 可作为增强型权限用例的策略实施方法，在这类用例中，园区无线用户 / 设备集中终止在以本地模式运行的无线控制器上，并被授予完整或部分网络访问权限。我们将定义不同类别的服务器，用户可能具有，也可能不具有这类服务器的访问权限。此外， CVD 还会定义一种通过使用无线控制器上的 ACL 只能访问互联网的类别，拒绝为其提供访问所有内部地址的权限。本 CVD 不探讨与 SGT 有关的 Catalyst 3850 和 CT-5760 等融合接入产品，因为，安全组标记和 SXP 当前不受支持。更多有关 SGT 和增强型用例的信息，我们将在随后讨论实际授权策略的各节中介绍。

在本 CVD 中，我们将详细阐述两种部署方案。第一个方案将使用安全组 ACL (SGACL) 在 Nexus 7000 数据中心交换机上实施策略，第二种方案将实施在配置为安全组防火墙 (SGFW) 的 Cisco ASA 上配置的策略。 SGACL 是在 Catalyst 交换平台上实施的基于角色的策略，它基于源和目标 SGT 值，明确给出允许或拒绝流量定义。同样，这些部署方案并不互相排斥，可以结合使用。图 3-3 和图 3-4 分别展示了第一种和第二种方案。

图 3-3　使用 SGACL 的策略实施

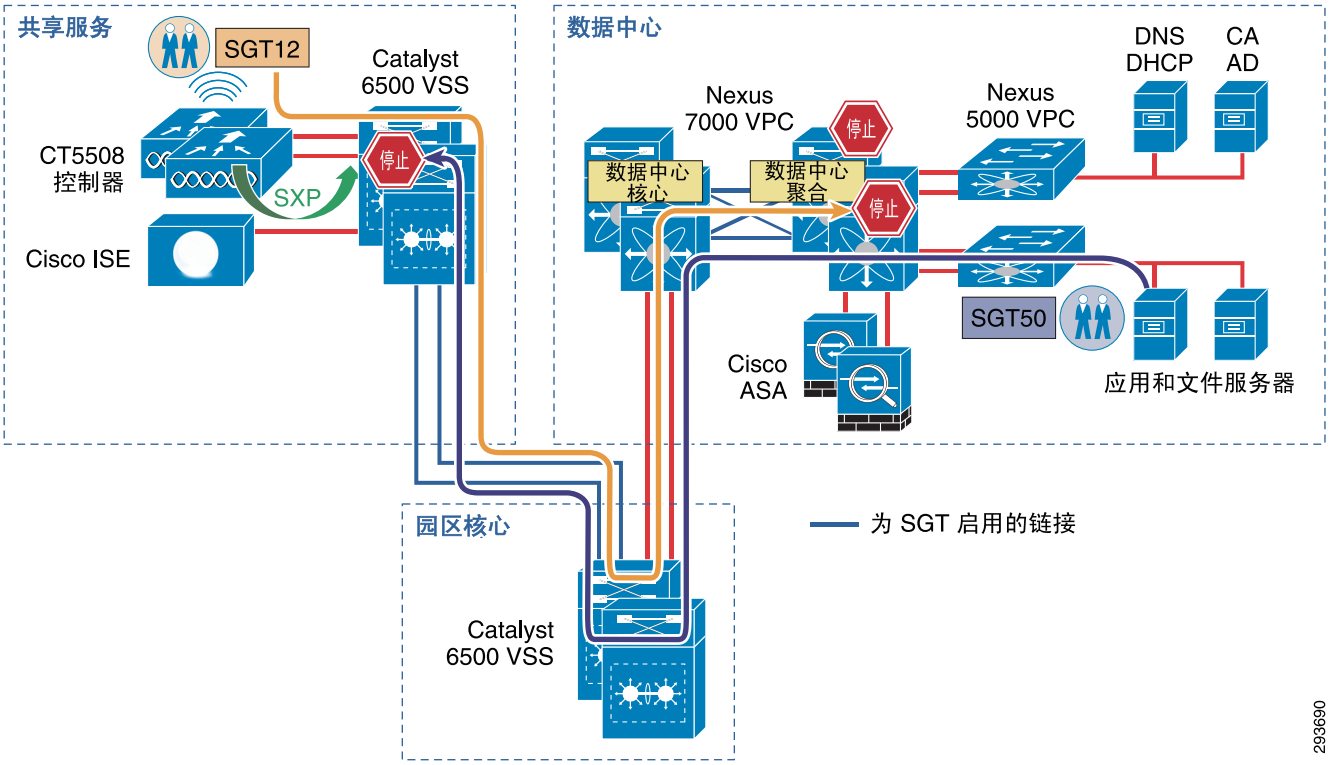
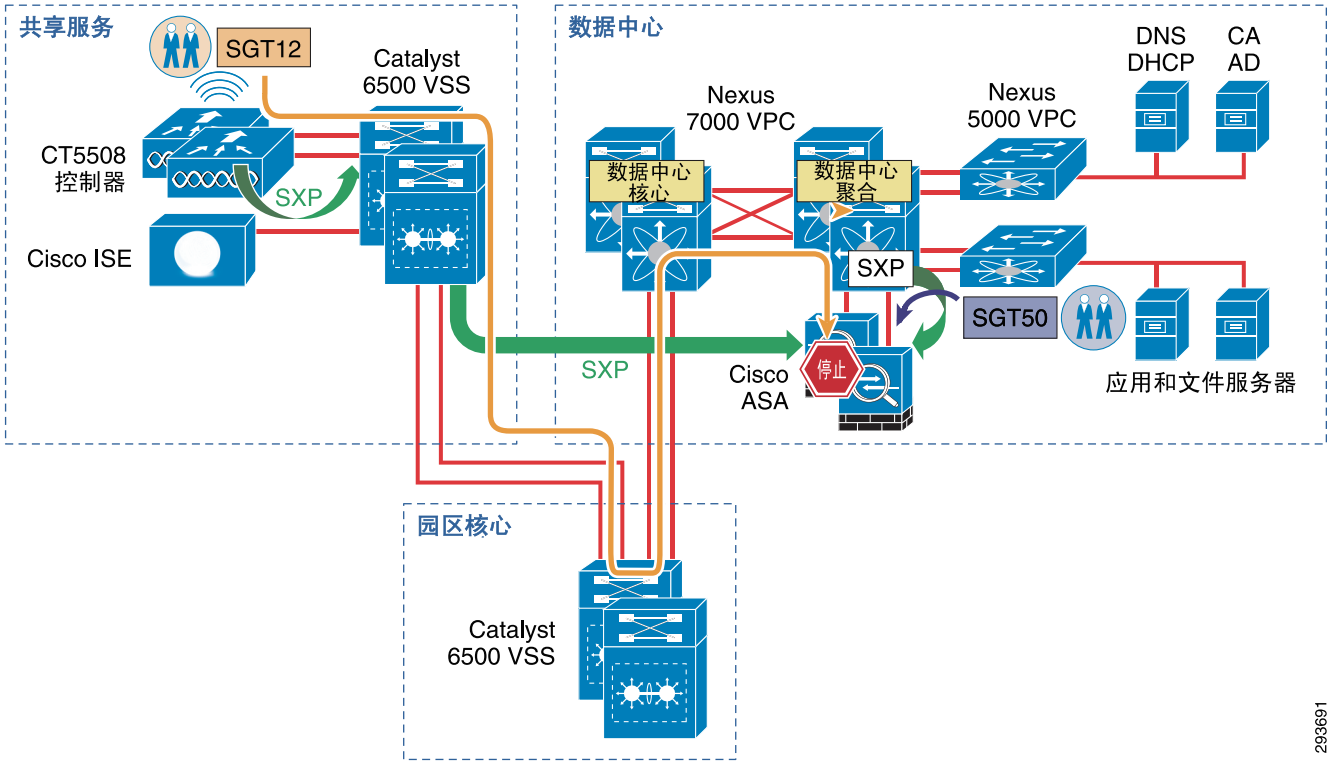


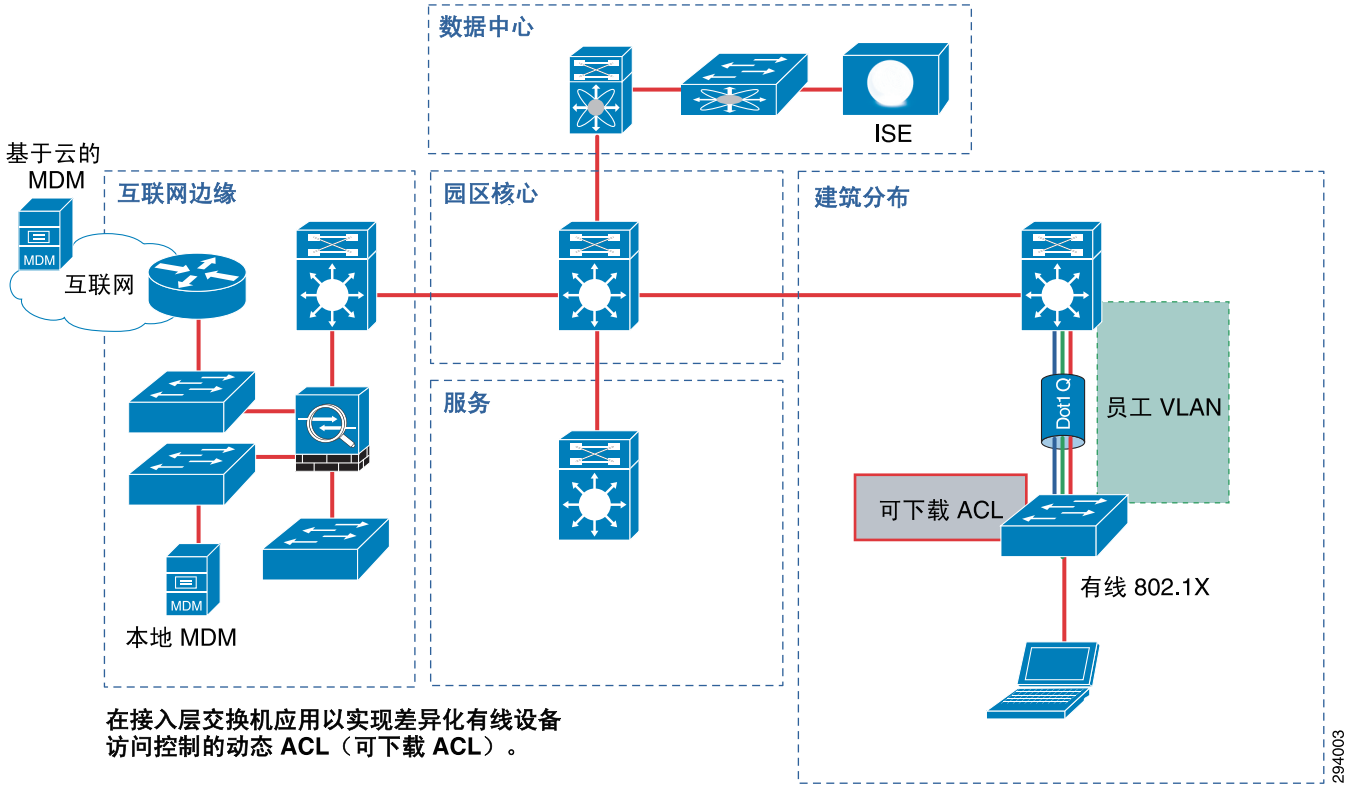
图 3-4　使用 SG-FW 的策略实施



园区有线设计

图 3-5 展示的是针对未实施融合接入 Catalyst 3850 系列交换机的园区的有线设计。换句话说，此有线设计适用于在楼宇分布模板的接入层实施 Catalyst 3750X 和 4500 系列等交换机，同时采用集中式（本地模式）无线设计的园区。

图 3-5　　非融合接入有线园区设计的高级视图



本指南假定 Catalyst 交换机在园区楼宇模块的接入层中部署为第 2 层设备。有线设备使用 802.1X 依照园区数据中心内的 ISE 服务器进行身份验证。在本设计中，有线设备均被静态分配到 Employee VLAN 这一个 VLAN。有线设备的差异化访问控制由应用至接入层交换机的 Radius 可下载 ACL 提供，而且，这些 ACL 将覆盖每个 Catalyst 交换机端口上预先配置的静态 ACL。

融合接入园区设计

融合接入园区 BYOD 设计重点介绍部署在大型园区的每个楼宇分布模块接入层中的多台 Catalyst 3850 系列交换机或交换机堆叠。交换机堆叠构成交换机对等组 (SPG)，其中的所有交换机都包含移动代理 (MA) 功能。SPG 内的漫游是通过 SPG 内各 MA 之间的全网状移动隧道处理的。大型园区内存在多个 SPG。

本设计指南假定 Catalyst 3850 系列交换机在园区内部署为第 2 层接入层交换机。每个园区楼宇分布模块中的第 3 层连接由 Catalyst 6500 分布式交换机提供。考虑到最小化生成树问题的园区设计最佳实践，我们假定 VLAN 未覆盖部署在不同配线间的多个 Catalyst 3850 系列交换机堆叠。在未来的设计指南中，我们将探讨 Catalyst 3850 系列交换机在分支机构内部署为第 3 层交换机的情况。

部署在园区集中式服务模块中的 Cisco CT5760 无线控制器具有移动控制器 (MC) 功能。连接到单个 MC 的多个 SPG 构成一个移动子域。大型园区内存在多个移动子域。移动子域内部 SPG 之间的漫游通过 Cisco CT5760 无线控制器完成。 CT5760 无线控制器还可以管理无线电资源管理 (RRM)、 WIP 等。

多个 Cisco CT5760 无线控制器构成移动组。因此，移动组也包括多个移动子域。移动子域之间的漫游通过移动组中的 Cisco CT5760 无线控制器完成。本设计指南中的设计假设存在一个移动组，因此仅覆盖一个移动域，并完全包含在大型园区内。

注意　Cisco CT5508 无线控制器还可以利用融合接入园区设计中的移动控制器 (MC) 功能。但是，CT5508 平台较旧，其整体吞吐量小于较新的 CT5760 平台。本版本的设计指南只讨论作为融合接入园区部署内移动控制器的 CT5760 无线控制器。未来版本可能会介绍部署方式相同的 CT5508 无线控制器。

园区楼宇分布模块中的接入点通过 Catalyst 3850 系列交换机中集成的无线控制器移动代理 (MA) 功能进行配置和控制。访客无线流量仍被回传至园区 DMZ 网段中的专用 CT5508 访客锚点控制器。使用融合接入园区设计时，配置流量 （也即来自尝试通过 ISE 联网的设备的流量）在 Catalyst 3850 系列交换机上本地终止。实施双 SSID 设计时，配置流量在独立的 VLAN 上终止。使用本设计，所有入网设备均在一个 VLAN 上终止。

注意　本指南仅讨论无线访客访问。有线访客访问可能会在本设计指南的未来修订版本中探讨。

此设计的潜在优势如下：

- 无线部署可扩展性提高，因为，无线流量在园区的每个接入层 Catalyst 3850 系列交换机上终止，而不是回传到一个或多个集中式无线控制器上。
- 无线流量的可视性增强，因为，无线流量在园区的每个接入层 Catalyst 3850 系列交换机上终止。

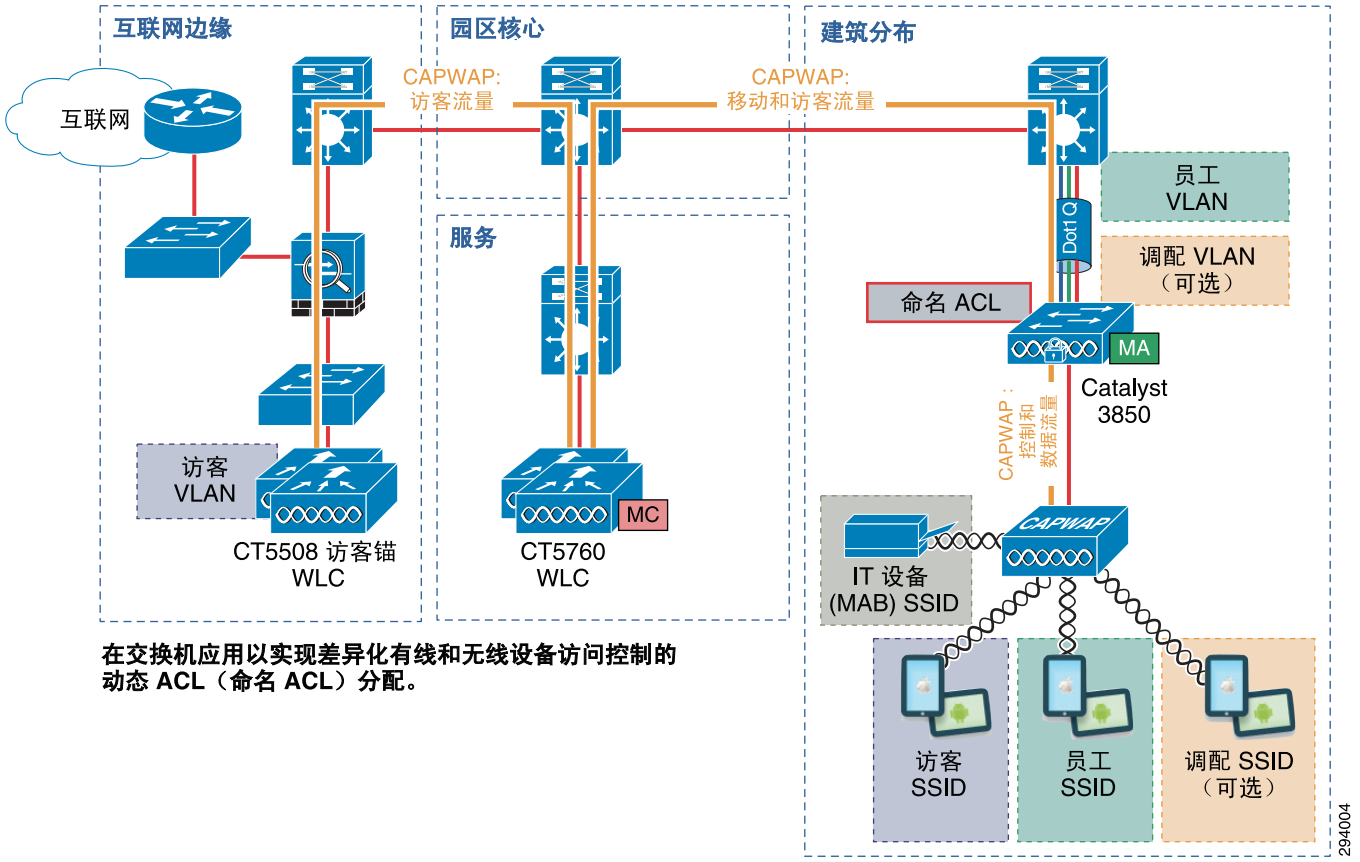
此设计的潜在劣势如下：

- 从园区网络的一个点对无线流量进行集中访问控制的效用降低。访问控制分摊到每个 Catalyst 3850 系列接入交换机上。但请注意，使用融合接入设计时，来自特定 WLAN 的流量仍然可以回传至集中式 CT5760 无线控制器并集中进行交换。这一点在园区迁移路径中有所阐述。
- 无线漫游变复杂的可能性更大，因为每个 Catalyst 3850 系列交换机都利用移动代理 (MA) 功能，这实际上意味着每个交换机都是一台无线控制器。

为了实施 BYOD 使用案例，本设计指南对使用融合接入设计的园区应用的方法是，对设备进行身份验证和授权，之后应用适当的命名 ACL。这种方法对有线设备和无线设备都适用。这些命名 ACL 必须在每个 Catalyst 3850 系列交换机上配置，并可提供差异化访问控制。例如，我们会向已授予网络完全访问权限的个人设备静态分配与已授予部分权限的个人设备相同的 VLAN，但是会向每台设备应用不同的命名 ACL，从而授予不同的网络访问权限。

图 3-6 展示的是简化的融合接入 BYOD 设计，此设计利用一个 Catalyst 3850 系列交换机作为园区中的移动代理 (MA)、一个 CT5760 无线控制器作为移动控制器 (MC)。

图 3-6　融合接入园区 BYOD 设计高级视图



在交换机应用以实现差异化有线和无线设备访问控制的动态 ACL（命名 ACL）分配。

注意　融合接入园区 BYOD 设计在本文中也被称之为外部控制器大型园区 BYOD 设计。本指南的未来版本可能会探讨小型园区和 / 或大型分支机构融合接入设计，在这类设计中，多个 Catalyst 3850 交换机堆叠将同时实施移动控制器 (MC) 和移动代理 (MA) 功能。在此类集成控制器小型园区 / 大型分支机构设计中，不需要外部 CT5760 无线控制器。

请注意，在本设计指南中，入网有线设备也被静态分配给与无线设备相同的 VLAN。因此，入网有线设备和无线设备将共享相同的 VLAN 以及相同的 IP 子网地址空间。客户可能因为各种问题（例如有关无线设备的附加安全合规性要求）而对有线和无线设备实施单独的子网。本版设计指南未对此进行探讨。动态分配的命名 ACL 为有线设备提供差异化网络访问权限。

假设所有园区交换机实施同一组 ACL 进行访问控制， Radius 可下载 ACL 也可以部署在园区内。在园区中实施可下载 ACL 的优点在于，访问控制项更改只需在 Cisco ISE 服务器中配置一次，而不必在所有园区 Catalyst 3850 系列交换机上配置。但是，使用这种方法还需要为园区和分支机构融合接入部署制定不同的 ISE 策略规则，假设命名 ACL 仍然部署在分支机构中。

如果需要在 ACL 中提供访问本地分支机构服务器的权限，在分支机构中实施可下载 ACL 会带来扩展问题。在这些情况下，每个分支机构都需要不同的可下载 ACL，因此，需要制定不同的 Cisco ISE 策略规则来标识每个分支机构的 ACL。所以，随着所部署分支机构数量的增加，这就演变成管理性不可扩展。

因此，本指南仅讨论融合接入分支机构设计和园区设计中使用命名 ACL 对入网设备进行访问控制的情况。由于两个设计均使用命名 ACL，因此，可对融合接入园区部署和分支机构部署使用相同的 Cisco ISE 策略规则，进而，可对融合接入设计使用一套策略规则，不论设备的位置如何。这将减少 Cisco ISE 策略的管理复杂性，但会增加操作的复杂性，因为需要在每个园区 Catalyst 3850 系列交换机上配置和维护 ACL。

注意　Cisco Prime 基础设施等管理应用可通过为融合接入 BYOD 分支机构设计和园区设计的命名 ACL 提供一个用于集中配置和部署的点，减轻 ACL 管理负担。

园区迁移路径

大型园区设计需要指出从传统 CUWN 集中式 （本地模式）无线叠加网络设计迁移至融合接入设计的方法。客户简单地将大型园区 “剪切”到融合接入设计的做法不可取。从传统 CUWN 集中式设计迁移至融合接入设计有很多可能的迁移路径。本节讨论其中一种可能的迁移路径。从初始叠加模式迁移的步骤如下：

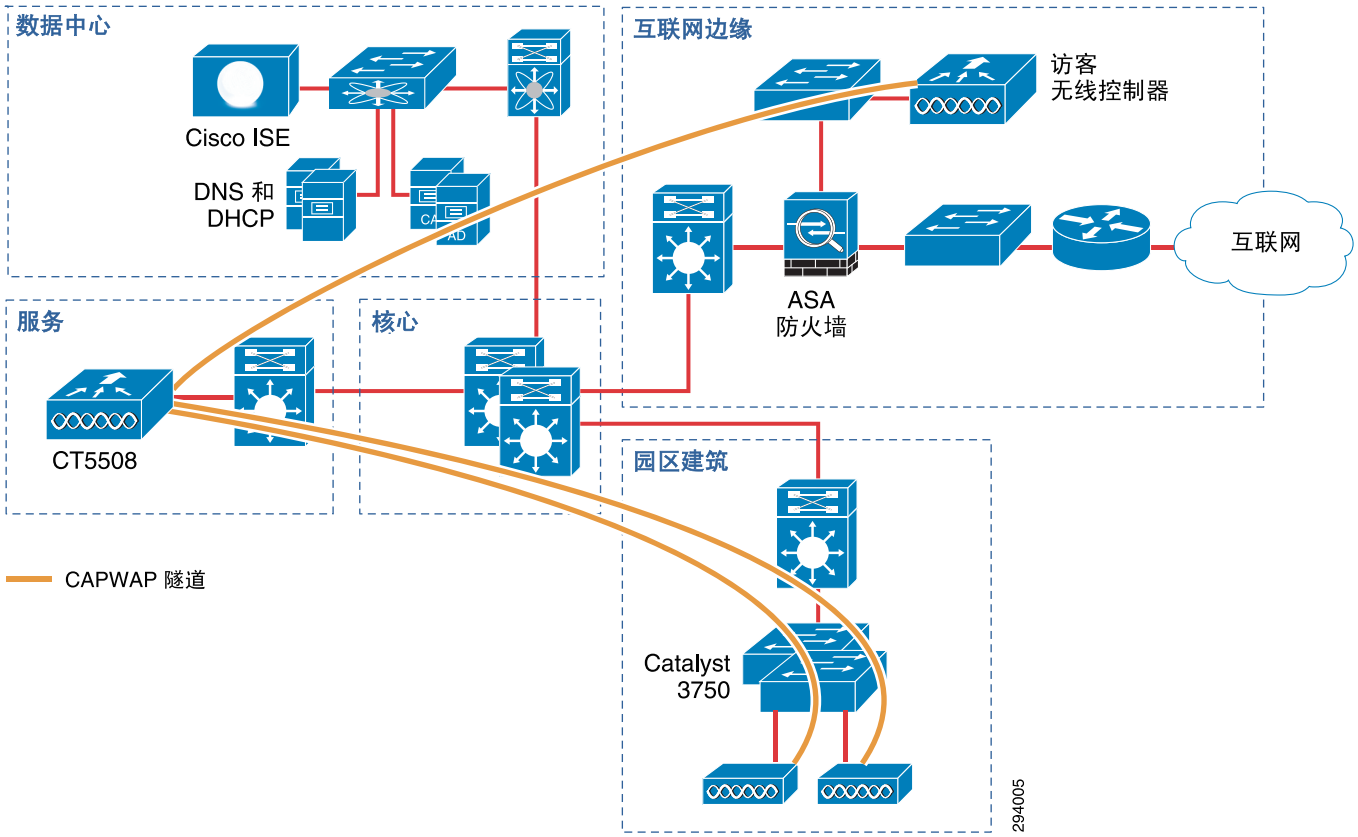
1. 仅本地 / 集中式模式
2. 融合接入和集中式混合模式
3. 完全融合接入

每一个步骤都将在下文中给出阐述。

初始叠加模式

图 3-7 展示了迁移路径中逻辑组件的初始状态 - 初始叠加模式。

图 3-7　迁移路径中的初始状态 - 初始叠加模式



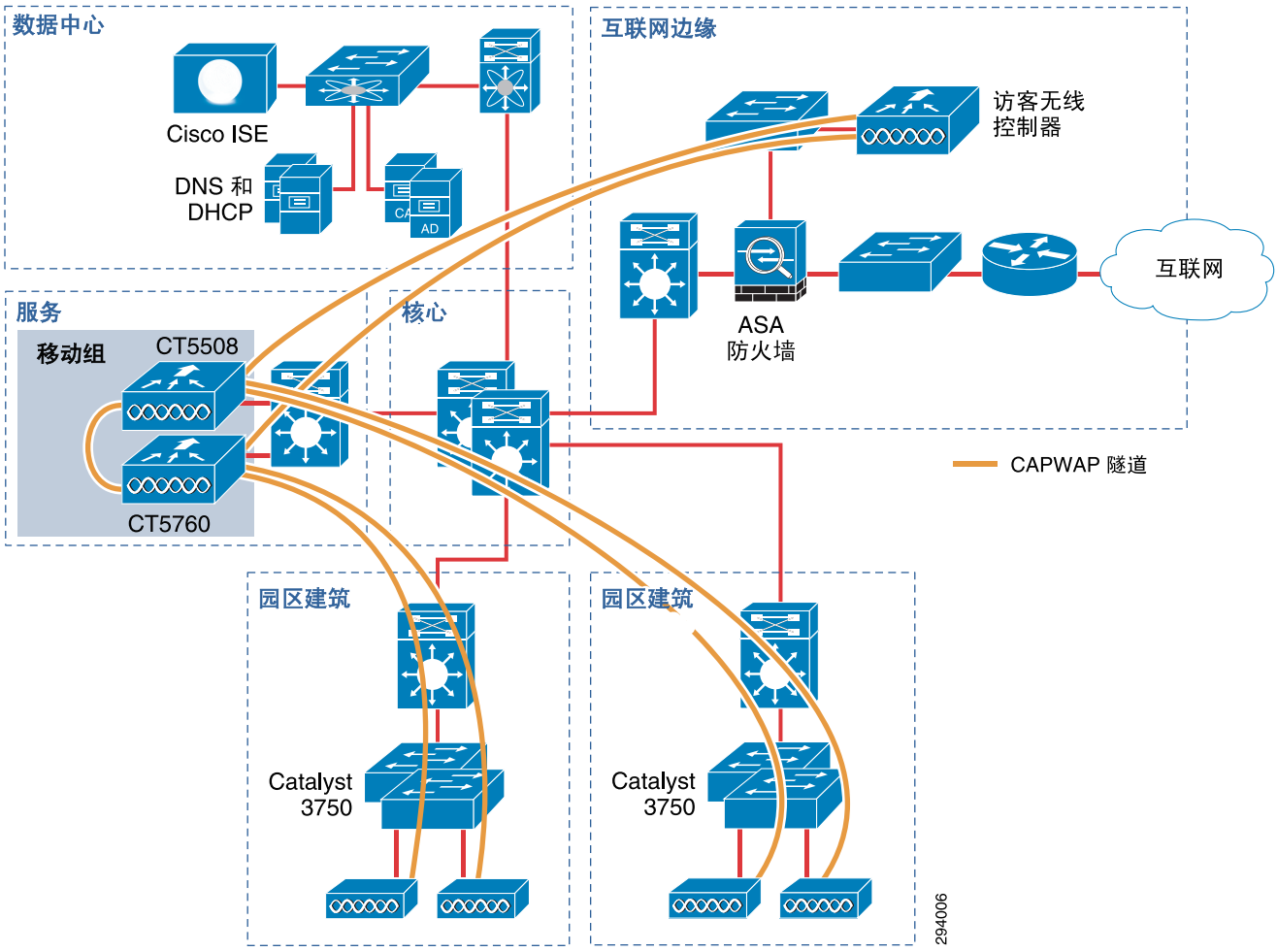
初始叠加模式包括接入点，这些接入点在本地模式下运行，并连接到园区内各个楼宇模块的接入层 Catalyst 3750-X 系列交换机上。接入点由位于园区服务模块中的 CT5508 无线控制器控制。CAPWAP 隧道从各个接入点延伸至 CT5508 无线控制器。位于互联网边缘模块内部 DMZ 分段中的第二个 CT5508 无线控制器用作专用无线访客锚点控制器。移动隧道（EoIP 或 CAPWAP，具体视软件版本而定）从园区（外部）CT5508 无线控制器延伸至访客（锚点）CT5508 无线控制器。

上文便是集中式（本地模式）无线设计中讨论的园区 BYOD 设计。

仅集中式模式 / 本地模式

图 3-8 展示了迁移路径第一步中的逻辑组件 - 仅集中式模式 / 本地模式。

图 3-8　　迁移路径第一步 - 仅集中式模式 / 本地模式



注意　请注意，术语 “本地模式” 与 CUWN 控制器结合使用，术语 “集中式模式” 与思科文档中的融合接入控制器结合使用。两个术语表示拥有用于无线流量的中央数据与控制层面的同一型号。换而言之，所有流量均回传至无线控制器，然后再放置到以太网网络上。

在迁移路径的这一阶段，客户只是增加了更多无线控制器容量。因为 CT5760 是较新的平台并具有更高的综合吞吐量，客户可能会通过将其添加到现有园区无线叠加设计，开始过渡到此平台。CT5760 支持最多 1,000 个接入点、最多 12,000 个客户端，每个无线控制器的吞吐量高达 60 Gbps。

注意　CT5760 的无线功能与具有最新软件版本部分功能的思科统一无线网络软件版本 7.0 大体相同。网络管理员必须确保 CT5670 具有所有必要的功能，然后才能将接入点从现有 CT5508 无线控制器迁移至 CT5760 无线控制器。有关支持功能列表，请参阅 《CT5760 控制器部署指南》：http://www.cisco.com/en/US/docs/wireless/technology/5760_deploy/CT5760_Controller_Deployment_Guide.html。

此时，假设楼宇模块配线间内的接入层交换机尚未达到更换周期。因此，在本地模式下运行的接入点仍连接到园区内各个楼宇模块的接入层 Catalyst 3750-X 系列交换机上。接入点由园区服务模块中的 CT5508 或 CT5760 无线控制器控制。这两者都属于同一移动组。 CAPWAP 隧道从各个接入点延伸至 CT5508 或 CT5760 无线控制器。 CT5508 和 CT5760 之间存在移动隧道。

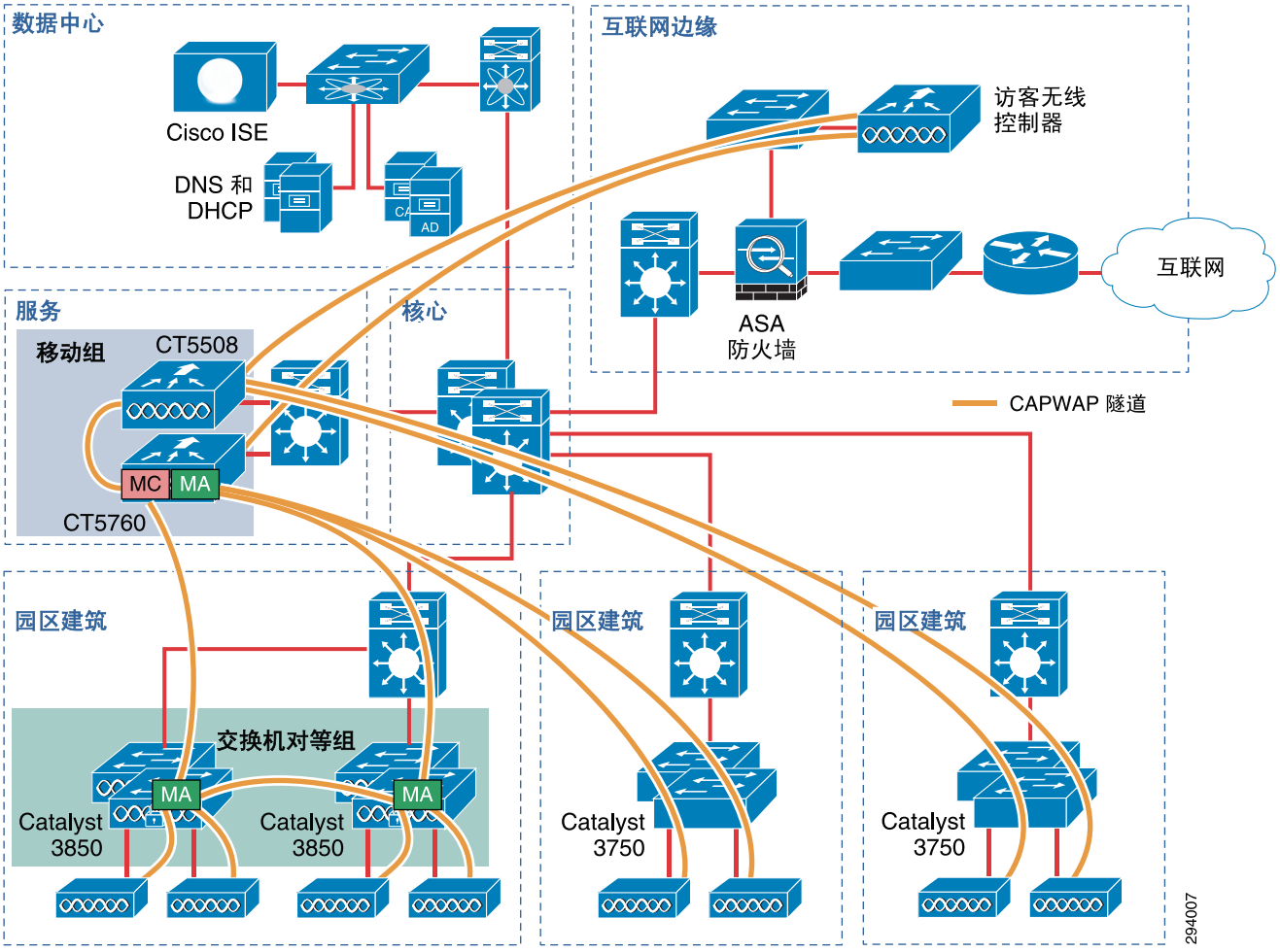
迁移至 CT5760 无线控制器最好在楼宇级别启动。换句话说，园区楼宇可以从现有 CT5508 无线控制器迁移到 CT5760 无线控制器 （可逐层迁移）。

要维持园区的无线网络，必须将现有 CT5508 无线控制器升级到 CUWN 软件版本 7.5。CUWN 软件版本 7.5 支持新移动隧道方法，此方法使用 CAPWAP 代替 EoIP，后者适用于 CT5760 无线控制器上运行的 IOS XE 3.2.2 软件。请注意，这包括升级专用于无线访客访问的 CT5508 无线控制器。移动隧道（本例中为 CAPWAP 通道）从外部 CT5508 和 CT5760 无线控制器延伸至锚点 CT5508 无线控制器。

融合接入和本地模式混合模式

图 3-9 展示了迁移路径第二步骤中的逻辑组件 - 融合接入和本地模式混合模式。

图 3-9　迁移路径的第二步 - 融合接入和本地模式混合模式



在迁移路径的这一阶段，假设楼宇模块配线间内的接入层交换机开始到达更换周期。在本情景中，客户选择了在楼宇模块的接入层部署 Catalyst 3850 系列交换机，并开始迁移至融合接入模式。同样，合理的迁移方法应是在楼宇级别启动。换句话说，可以将园区的一个楼宇从在集中模式下运行、连接到 Catalyst 3750-X 系列交换机并由 CT5760 控制的接入点迁移至在融合模式下运行、连接到 Catalyst 3850 系列交换机并由其控制的接入点 （可逐层迁移）。

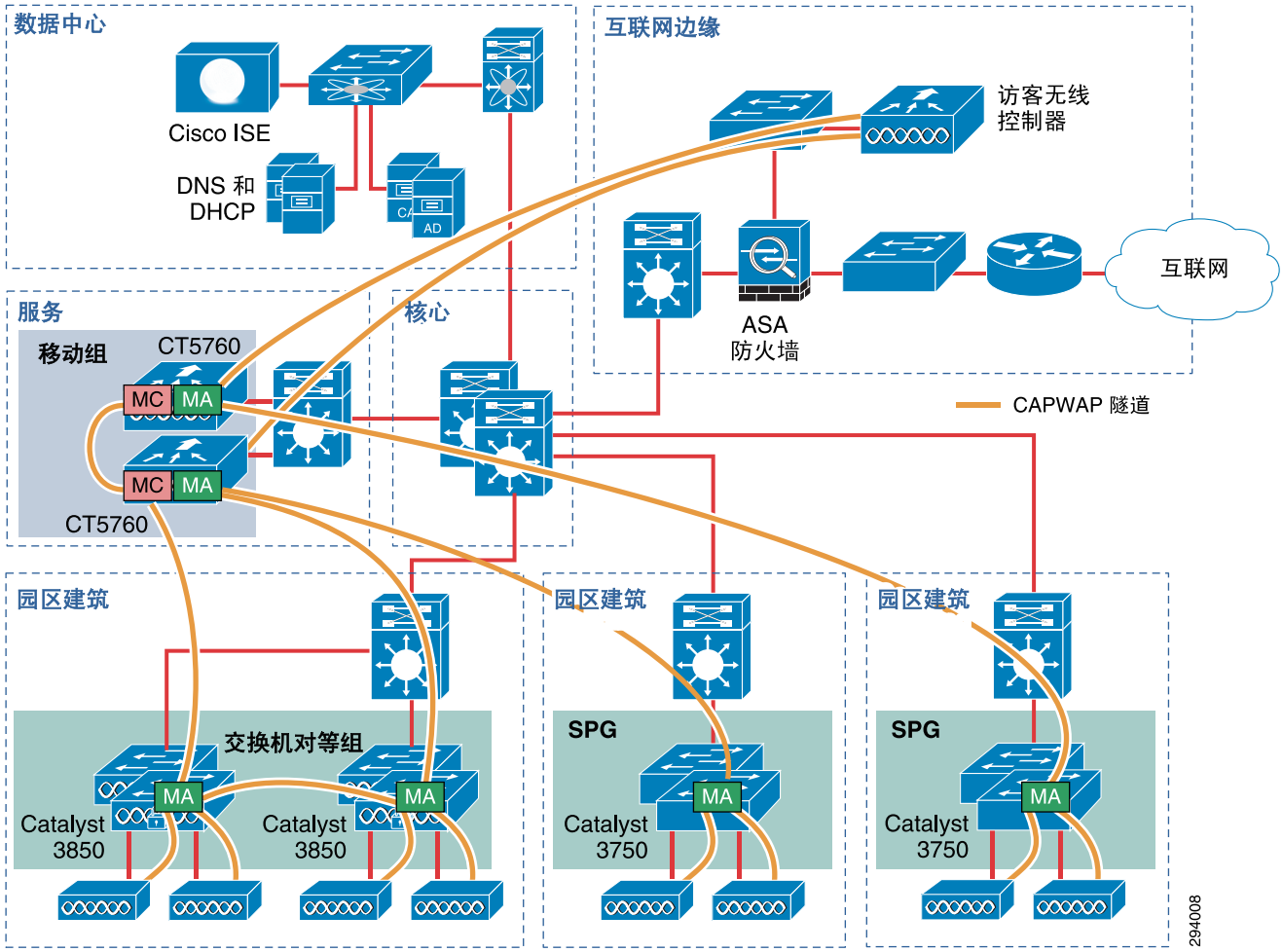
在此设计中，Catalyst 3850 系列交换机用作移动代理 (MA)，CT5760 无线控制器用作移动控制器 (MC)，并可能用作 Mobility Oracle (MO)。但是在楼层迁移过程中， CT5760 无线控制器仍在集中式模式中运行，因为接入点仍然连接到 Catalyst 3750-X 系列交换机。因此，此设计是集中式和融合接入 “混合”的设计。

CAPWAP 隧道从连接到 Catalyst 3750-X 系列交换机的各个接入点延伸至 CT5508 或 CT5760 无线控制器。 CAPWAP 隧道也可以从连接到 Catalyst 3850 系列交换机的各个接入点延伸至 Catalyst 3850 系列交换机。 CAPWAP 移动隧道从 Catalyst 3850 系列交换机内部的 MA 延伸至 CT5760 无线控制器内部的 MA。最后，CAPWAP 移动隧道在 Catalyst 3850 交换机（交换机对等体组 [SPG] 成员）内部的 MA 之间延伸。 SPG 卸载交换机组的移动流量，而且，交换机组内部会有大量移动流量。漫游在连接到属于同一 SPG 的 Catalyst 3850 系列交换机的接入点之间展开时， CT5760 内部的 MC 将不参与漫游。 SPG 可能涵盖楼宇一个楼层的一部分、整个楼层，有时候涵盖多个楼层。 CT5508 和 CT5760 之间也存在 CAPWAP 移动隧道。最后， CAPWAP 隧道移动从外部 CT5508 和 CT5760 折回无线访客接入的锚点。

完全融合接入

图 3-10 展示了迁移路径第三步的逻辑组件 - 完全融合接入模式。

图 3-10　　迁移路径的第三步 - 完全融合接入



本设计假设客户已停用在本地模式下运行的现有 CT5508 无线控制器，并迁移到使用 CT5670 无线控制器的融合接入设计。在迁移路径的这一阶段，假设楼宇模块配线间内的接入层交换机的更换周期已结束。在本情景中，客户选择了在楼宇模块的接入层只部署 Catalyst 3850 系列交换机，并完全迁移至融合接入模式。

注意　我们认识到一些客户可能永远无法完全迁移到完全融合接入模式，其他客户则可能需要几年的时间才能实现完全融合接入部署。

在此设计中，Catalyst 3850 系列交换机用作移动代理 (MA)，CT5760 无线控制器用作移动控制器 (MC)，并可能用作 Mobility Oracle (MO)。

CAPWAP 隧道从连接到 Catalyst 3850 系列交换机的各个接入点延伸至 Catalyst 3850 系列交换机。CAPWAP 移动隧道从 Catalyst 3850 系列交换机内部的 MA 延伸至 CT5760 无线控制器内部的 MA。CAPWAP 移动隧道在 Catalyst 3850 交换机（交换机对等体组 [SPG] 成员）内部的 MA 之间延伸。CAPWAP 移动隧道也可以在两个 CT5760 无线控制器之间延伸。最后，CAPWAP 移动隧道从外部 CT5760 无线控制器折回无线访客访问的锚点 CT5508。

注意　设计指南的此版本未验证子域之间的漫游 （例如，在充当 MC 的两个 CT5760 无线控制器之间的漫游）。

无线局域网控制器高可用性

随着越来越多的具有重要功能的设备移动到无线介质，无线网络的高可用性也随之变得越来越重要。实时音频、视频和文本通信依赖于企业无线网络，因此，零停机时间也将变成企业的普遍诉求。与有线网络中断一样，无线网络中断也能够产生巨大的负面影响。

在思科统一无线网络 (CUWN) 软件版本 7.3 及更高版本中，添加了拥有活动和热备份无线控制器的功能，可让接入点 (AP) 快速执行状态化切换 (SSO)。利用这项功能，所有接入点会话可状态化切换至配置与主 WLC 相同的热备份 WLC。所有独特的配置参数和特定于各个接入点的分组以及接入点组均被保留。 Flex-Connect 分组便是保留的配置，它可基于分支机构的位置将不同的限制和设置应用到一部分接入点。发生故障切换时，客户端关联将被取消。但是，接入点执行状态化切换之后，客户端应自动重新建立关联。

活动和备用 WLC 使用专用冗余接口每 100 毫秒发送一次 “保持连接”消息，同时也在两者之间发送配置、操作数据同步和角色协商信息。冗余接口是 WLC 之间通过以太网电缆直接连接的专用端口。 WiSM2 使用专用冗余 VLAN 代替冗余端口。保持连接消息丢失以及网络故障都会触发故障切换。活动和备用 WLC 共享相同的管理 IP 地址，但只有活动 WLC 处于运行状态，直至发生故障。

有关详细信息，请参阅 《WLC 高可用性部署指南》：
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bd3504.shtml。

注意 Cisco CT5760 无线控制器是基于 IOS XE 的控制器。 IOS XE 3.2.2 不支持接入点状态化切换 (AP SSO)。相反，由 CT5760 控制的接入点支持配置主用、二级以及三级无线控制器，以实现高可用性。具有无线控制器功能的 Catalyst 3850 系列交换机堆叠通过交换机堆叠本身可保证高可用性。这两个平台的高可用性不在本设计指南的讨论范围之内。本指南的未来版本将介绍 CT5760 和 Catalyst 3850 的高可用性。

分支机构广域网设计

很多分支机构网络管理员在部署 BYOD 解决方案之前会再次检查广域网 (WAN)。在特定情况下，访客网络能够将负荷提高至一定速率，不仅会消耗 WAN 带宽，还能够影响企业流量。有线网络的速度从 10 Mbps 提高到 1 Gbps，蜂窝网络也将 GPRS 的带宽从 30 kbps 增加至 LTE 带宽的 20 Mbps 左右，但传统分支机构 WAN 带宽在性能上未出现同样的提升。员工和客户希望企业网络的带宽、延迟以及抖动至少应达到家庭网络或蜂窝网络的水平。

此外，由于 WiFi 访问通常供企业用户免费使用，而且大多数手持设备将优先选择 WiFi 而不是蜂窝网络，因此，企业用户可能会继续使用访客或公司 SSID 访问互联网，甚至在 LTE 网络的速度更快时亦是如此。这就会迫使网络管理员寻找新的 WAN 传输机制 （例如城域以太网和 VPN-over-Cable）来满足用户期望。另一种方法是卸载分支机构的访客互联网流量，为公司流量保留 WAN 带宽。但是，从分支机构提供直接互联网访问应遵循公司安全策略。因此，WAN 上的负荷将增加。对分支机构 BYOD 服务没有新 WAN 要求时，应审查传输技术、接入速度和加密等问题。

分支机构 WAN 基础设施

本设计中的分支机构 WAN 基础设施将 Cisco ASR 1006s 作为前端路由器。两个 WAN 连接在这些设备终止；第一个路由器配置为服务提供商 MPLS 电路，第二个路由器配置互联网连接。这些前端路由器均放置在园区核心外部的 “WAN 边缘”块中。终止互联网连接的 ASR 也利用 IOS 基于区域的防火墙 (ZBFW)，而且允许朝向分支机构的通道流量。

在分支机构中，两种不同设计经过验证。第一种设计包括两个 Cisco 2921 ISR G2 路由器。这两个路由器中有一个终止 SP MPLS 电路，另一个则终止可专用于分支机构备份或用作公司流量替代路径的互联网连接。第二种设计由一个终止这两条电路的 Cisco 2921 ISR G2 路由器构成。

这两种部署模式都实施了 Cisco IOS 基于区域的防火墙 (ZBFW)，以保护分支机构到互联网的连接。禁止从分支机构到互联网的本地接入，尽管这种方法完全可行。出于此目的以及保护企业数据，设计实施了 DMVPN，而且，只允许隧道访问，以保护返回园区前端路由器的连接。数据中心访问权限便采用了这种处理。互联网访问通过公司防火墙 / 网关实现。另外，还利用 DMVPN 保护服务提供商 MPLS 电路中的流量。

有关 DMVPN、ZBFW 配置、QoS 以及 WAN 基础设施中其他组件的配置信息及设计指南不在本文档讨论范畴之内。

有关下一代企业 WAN (NGEW) 设计的详细参考信息，请参阅设计区文档：
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html。

更多 QoS 设计指南，请参阅 *《Medianet 设计指南》*：
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html。

分支机构 WAN 带宽要求

本指南介绍两种分支机构无线局域网设计，即 FlexConnect 和融合接入。在 FlexConnect 设计中，分支机构接入点由园区数据中心或服务模块中的无线 LAN 控制器进行管理。 CAPWAP 隧道在无线控制器和分支机构中的接入点之间建立。此 CAPWAP 隧道可控制流量，也可以在某些设计中控制入网过程中的数据流量。此流量通过 WAN 传输。即使设备可能会使用 FlexConnect 设计将流量本地终止在分支机构中的本地 VLAN 上，大部分流量将继续通过 WAN 流向企业数据中心。

在融合接入设计中，分支接入点由 Catalyst 3850 系列交换机的集成 WLAN 控制器功能管理。CAPWAP 隧道在 Catalyst 3850 系列交换机和分支机构中的接入点之间建立。此 CAPWAP 隧道可用于任何无线控制和数据流量。同样，即使设备可能会使用融合接入设计将流量本地终止在分支机构中的本地 VLAN 上，大部分流量将继续通过 WAN 流向企业数据中心。

因为本文档介绍的两个分支机构 WLAN 设计都使用一个中央 AAA 服务器（例如 Cisco ISE），随着入网员工托管设备的增多，身份验证和授权流量可能会增加。这些新的终端可能也会生成额外的新流量。此外，使用这两种分支机构无线 LAN 设计，访客互联网访问流量会回传至园区 DMZ 中的锚点控制器。这一切因素都可能会因 BYOD 部署而导致 WAN 线路上的负荷增加。

由于无法在部署 BYOD 之前确定流量的占用程度，因此预测额外的流量负荷非常困难。在特定情况下，无线访客流量很难被预测并且该流量可能会因本地事件的不同而出现很大的变化。合理的设计目标是在提供 BYOD 的每个分支机构实现至少 1.5 Mbps 的网络速度。头端 WAN 聚合线路的网络速度应视传统超用比 (OSR) 而定。这样可以为小型部署提供足量的带宽。大型分支机构可能需要额外带宽，尤其是访客用户可能希望使用高带宽应用 （例如视频流）。 WAN 架构必须足够灵活，以调整服务级别来满足需求。可支持额外带宽实现联网的子速率 MPLS 接入线路或专用 WAN 路由器可实现此目的。您还应考虑适用于每个分支机构的地址空间，因为 FlexConnect 和融合接入设计均支持从本地范围调用无线 DHCP 客户端。有关带宽管理技术 （例如速率限制）的更多信息，可参阅第 13 章， BYOD 访客无线接入。

加密要求

分支机构无线流量的本地终端是两种 BYOD 分支机构无线 LAN 设计的另一要素。此本地终端允许分支机构无线设备直接访问分支机构 LAN 中的资源，无需使 CAPWAP 隧道穿过集中式无线控制器。本地终端通过避免分支机构的发夹式流量折回园区中的无线控制器然后再折回分支机构服务器，减少了 WAN 所需传输的流量。其影响可减少 CAPWAP 隧道内的上游负荷和 CAPWAP 隧道外的下游负荷。将无线分支机构设备连接至同一分支机构内的服务器即可享受此优势。如果该流量流向数据中心，那么得益于其所具备的与有线流量等同的安全和性能级别，流向数据中心的流量仍然会经过 WAN （但在 CAPWAP 隧道外部）。根据应用的情况，流量可能无法进行加密，因此需要额外的 WAN 安全。如果分支机构使用宽带连接作为主用或备用路径，显然需要部署加密技术 （例如 DMVPN）。但是，虽然已使用 MPLS VPN 服务，企业仍然希望对流经外部的所有流量进行加密。

传输

使用 FlexConnect 和融合接入设计后，并非所有无线流量均可在本地终止。在本设计指南中，访客流量仍然会通过 CAPWAP 隧道传输到园区内的中央控制器。此外，使用 FlexConnect 设计后，根据实施的入网设计 （一个 SSID 与双 SSID）的情况，来自正在办理入网的设备的流量可能也会通过 CAPWAP 隧道传输到中央控制器。此流量可能会争用带宽，同时企业流量也会使用 WAN 链路 （但在 CAPWAP 隧道外部）。通过混合使用传统 QoS 服务和无线速率限制即可解决这些问题。在某些情况下，传输会确定合适的解决方案。

如果已部署第 2 层 MPLS 隧道，则可通过目标路由确定将 CAPWAP 流量传输至无线控制器所需连接的专用路径。这是将访客流量与流向园区的分支机构流量进行隔离的一种有效方法，因为带有本地终端的 FlexConnect 会将 CAPWAP 隧道外部的大部分企业流量直接送达目的地。如果没有较复杂的路由策略，我们很难管理从园区流向分支机构的返回流量，但通过仔细规划则可实现有效管理。

图 1-2 详细介绍了常见的 WAN 架构。

分支机构 LAN 网络设计

BYOD 的任何地点、任何设备要求意味着员工可以在园区或分支机构使用企业设备或个人设备。员工使用这些设备后， BYOD 架构的相关组件会对分支机构或园区内的这些设备执行相应的策略。只有当已经实施一个设计良好的园区网络基础设施时，策略实施才有效。此分支机构网络基础设施可分为 WAN 和 LAN 两部分。本节介绍分支机构 LAN 设计的关键设计要素。

当前思科接入点可以在思科统一无线网络 (CUWN) 架构中的一个实施模式下运行：

- 本地模式 （也称为集中式控制器设计）
- FlexConnect 模式

此外，最近思科将无线 LAN 控制器功能直接整合到了新一代接入层交换机 - Catalyst 3850。因此现在可提供第三种实施选择：

- 融合接入

FlexConnect 是一种主要适用于分支机构的无线设计，本节将对其作出详细介绍。在本设计指南中，本地模式是一种主要适用于园区的无线设计，园区网络设计将对其作出详细介绍。融合接入设计对分支机构和园区中的无线设计和有线设计都适用，因此本章中的两节均会对其作出详细介绍。

注意　可以将本地模式部署到大型分支机构，以调整分支机构内部部署的无线控制器的相关要求。在这种情况下，大型分支机构的 BYOD 设计类似于园区设计。

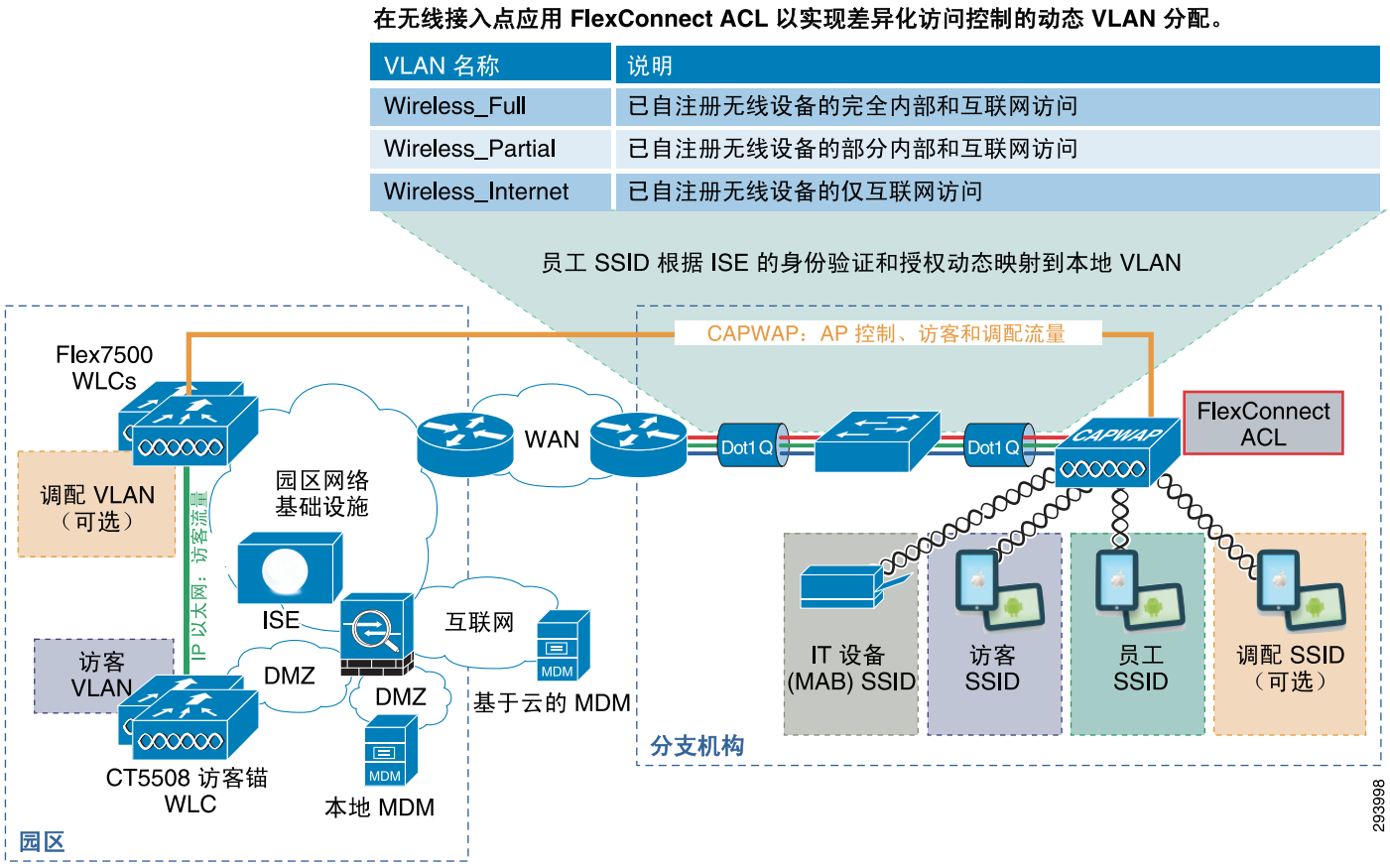
FlexConnect 无线设计

FlexConnect 是一种思科创新技术，可在部署 LAN 时提供更强大的灵活性。例如，无线 LAN 可配置为通过集中式 AAA 服务器对用户进行身份验证，但是，一旦用户经过验证，流量将在接入点的以太网接口进行本地交换。或者，流量也可以被回传并在无线控制器的以太网接口终止（如果需要）。FlexConnect 的本地交换功能可消除在必须访问分支机构的本地资源时，将数据流量一路回传至无线控制器的需要。这样会降低访问本地分支机构服务器上的应用的往返时间 (RTT) 延迟，提高应用的性能。同时，还可以减少访问资源时回传至分支机构本地的不必要发夹式流量。

您仍然可以通过一个或多个集中式无线局域网控制器配置和控制连接到分支机构接入层交换机的接入点。在本设计指南中，我们使用一组专用于分支机构的 Cisco Flex 7500 无线控制器作为这类控制器，因为它们为支持 FlexConnect 模式接入点提供比 Cisco CT5508 无线控制器更高的扩展性。另请注意：使用此设计后， WAN 中的访客无线流量被回传至位于园区 DMZ 网段中的专用 CT5508 访客锚点控制器。同时， WAN 中的配置流量 （也即来自尝试通过 ISE 入网的设备的流量）也可能会被回传至园区内的 Flex7500 无线控制器。

图 3-11 简要介绍如何在分支机构设计中实施 FlexConnect。

图 3-11　FlexConnect 无线分支机构设计高级视图



为了实施联网设备的 BYOD 使用案例，本设计指南对采用 FlexConnect 无线设计的分支机构应用的方法是，对设备进行身份验证和授权，然后将该设备连接到合适的 VLAN。每个接入点（或接入点组）和每个 VLAN 应用的静态配置的 FlexConnect ACL，均可提供针对无线设备的差异化访问控制。例如，将需要网络完全访问权限的个人设备连接到具有适当权限的 VLAN（其接入点上已配置 FlexConnect ACL）。已授予部分访问权限的个人设备会被连接到已配置不同 FlexConnect ACL 的不同 VLAN。

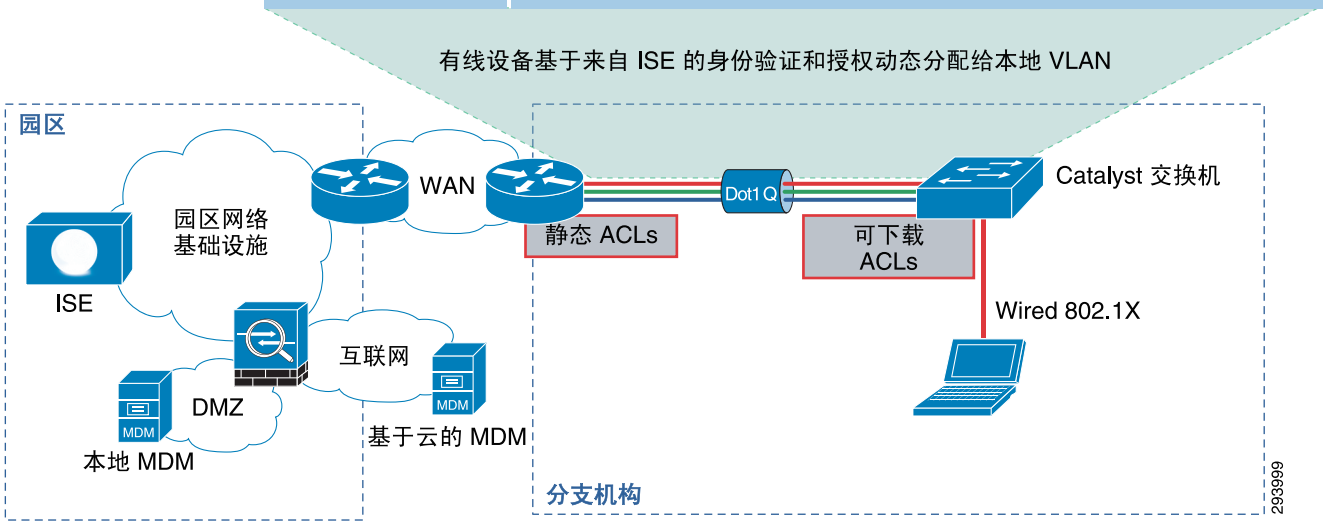
分支机构的有线设计

图 3-12 介绍的是针对未实施融合接入 Catalyst 3850 系列交换机的分支机构的有线设计。换句话说，此有线设计适用于实施 Catalyst 3750X 等交换机，并采用 FlexConnect 无线设计的分支机构。

图 3-12　非融合接入有线分支机构设计高级视图

动态 VLAN 分配和可下载的 ACL（后者覆盖默认静态 ACL）应用于有线交换机端口。
在分支机构路由器第 3 层子接口上配置的静态 ACL 提供了差异化的访问控制。

VLAN 名称	说明
Wireless_Full	已自注册无线设备的完全内部和互联网访问
Wireless_Partial	已自注册无线设备的部分内部和互联网访问
Wireless_Internet	已自注册无线设备的仅互联网访问

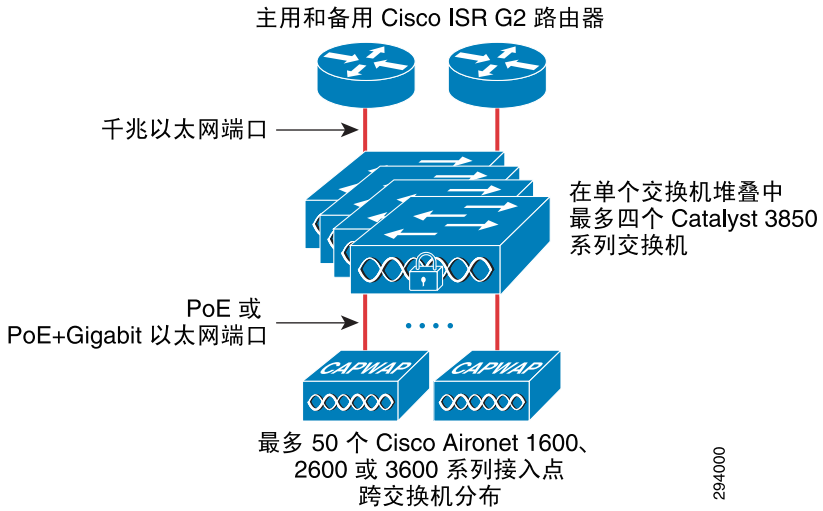


本指南假定将 Catalyst 交换机部署为分支机构内的第 2 层设备。使用 802.1X 执行有线设备是否能够通过园区数据中心内的 ISE 服务器的身份验证。同时，在本设计中，会根据有线设备的访问控制要求将这些有线设备动态分配到独立的 VLAN。 Catalyst 3750X 系列交换机应用的 Radius 可下载 ACL 将覆盖每个 Catalyst 交换机端口上预先配置的静态 ACL。有线设备的差异化访问控制由应用至 Cisco ISR G2 路由器第 3 层子接口的静态配置的 ACL 提供。

融合接入分支机构设计

融合接入分支机构 BYOD 设计假设在分支机构中部署一个 Catalyst 3850 系列交换机或交换机堆叠。因此设计仅适用于中小型分支机构。如图 3-13 所示。

图 3-13　　融合接入分支机构设计硬件



交换机堆叠中可至多部署 4 个 Catalyst 3850 系列交换机。每个交换机堆叠可至多支持 50 个接入点和 2000 个无线客户端。每台 Catalyst 3850 系列交换机可支持 （48 端口型号）至多 40 Gbps 的无线吞吐量。请注意，无线性能要求和物理距离限制通常决定了此设计可部署的无线接入点和客户端的实际数量。实施交换机堆叠后，应在交换机间部署接入点，以提高无线弹性。本设计指南假定将 Catalyst 3850 系列交换机部署为分支机构中的第 2 层交换机。分支机构中的第 3 层连接由 ISR 路由器提供，该路由器也用作分支机构的 WAN 连接点。未来的设计指南可能会将 Catalyst 3850 系列交换机部署为分支机构中的第 3 层交换机。

注意　在本文档中，融合接入分支机构 BYOD 设计也被称为集成控制器分支机构 BYOD 设计。

如前所述，思科已将无线 LAN 控制器功能直接整合到了 Catalyst 3850 系列交换机。这样，在必须访问分支机构的本地资源时，即可终止 Catalyst 3850 交换机上的无线流量，而不是将该流量回传至集中式无线控制器。与 FlexConnect 设计一样，融合接入设计可降低往返时间 (RTT) 延迟，提高应用的性能，同时还可以减少访问资源时回传至分支机构本地的不必要发夹式流量。

对于融合接入分支机构 BYOD 设计， Catalyst 3850 系列交换机堆叠将实施以下无线控制器功能：

- 移动代理 (MA) - 从接入点 (AP) 终止 CAPWAP 隧道，并维护无线客户端数据库。
- 移动控制器 (MC) - 管理子域内和子域之间的移动性、无线电资源管理 (RRM)、 WIPS 等。

由于仅存在一个交换机堆叠，因此只有一个交换机对等体组 (SPG)。移动组、移动子域和移动域完全包含在分支机构内。除用作无线访客流量的专用锚点控制器的 Cisco CT5508 无线控制器以外，园区无需使用其他集中式无线控制器。您仍然可以通过整合到 Catalyst 3850 系列交换机中的无线局域网控制器功能配置和控制分支机构中的接入点。访客无线流量仍被回传至园区 DMZ 网段中的专用 CT5508 访客锚点控制器。使用融合接入分支机构设计时，配置流量 （也即来自尝试通过 ISE 入网的设备的流量）在 Catalyst 3850 系列交换机上本地终止。实施双 SSID 设计时，配置流量在独立的 VLAN 上终止。使用本设计，所有入网设备均在一个 VLAN 上终止。

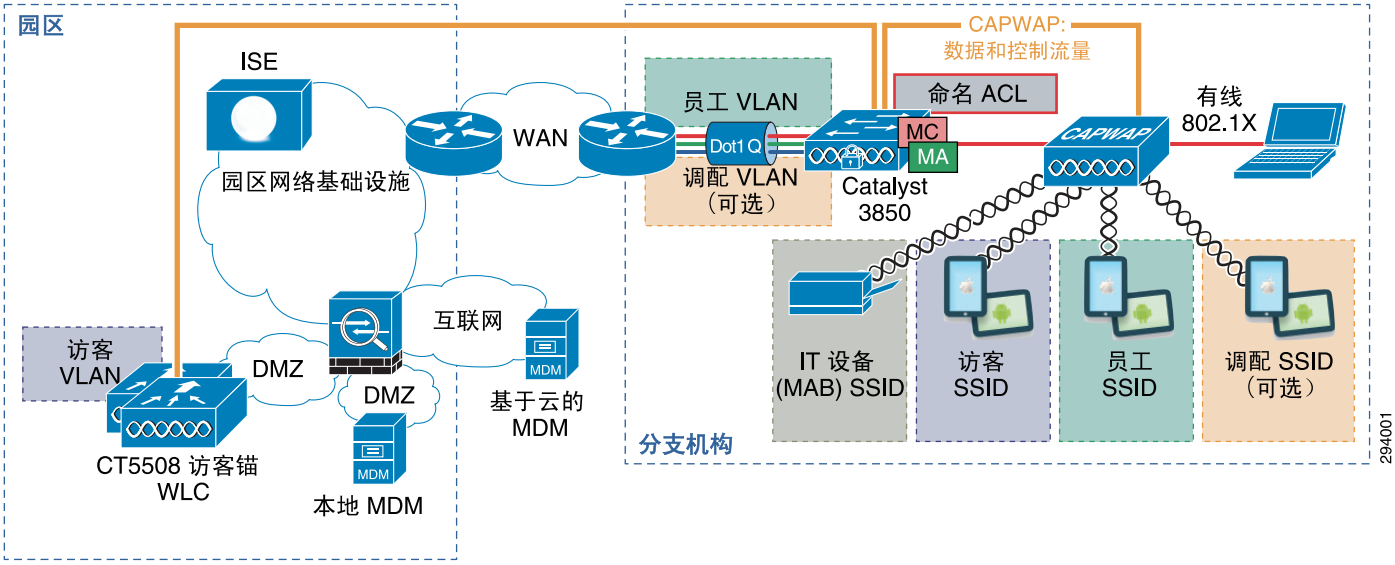
注意　请注意，部署融合接入无线设计 （将 Catalyst 3850 系列交换机用作移动控制器 (MC) 和移动代理 (MA)）时，用于无线访客接入的移动隧道是由 Catalyst 3850 交换机向 DMZ 中的访客锚点控制器发起的。因此，使用本设计，每个分支机构均会发起一个针对无线访客接入的移动隧道。对于 CT5508 无线控制器，移动域中的移动控制器最多为 72 台。因此，如果使用 CT5508 无线控制器，移动锚点隧道的最大数量限制为 71。由此，网络管理员可能需要部署额外的 CT5508 访客锚控制器。或者，网络管理员可以考虑为访客接入提供分支机构的直接互联网接入。本指南的未来版本可能会讨论此类设计。

为了实施 BYOD 使用案例，本设计指南对采用融合接入设计的分支机构应用的方法是，对设备进行身份验证和授权，然后应用适当的动态 ACL。这种方法对有线设备和无线设备都适用。特定动态 ACL 为 Radius 指定的本地 ACL，也称为命名 ACL。这些命名 ACL 必须在每个 Catalyst 3850 系列交换机上配置，并可提供差异化访问控制。例如，我们会向已授予网络完全访问权限的个人设备静态分配与已授予部分权限的个人设备相同的 VLAN，但是会向每台设备应用不同的命名 ACL，从而授予不同的网络访问权限。因为命名 ACL 是配置在特定分支机构的 Catalyst 3850 交换机上，所以单个 Cisco ISE 策略可以在多个分支机构实施。不过，每个分支机构的 ACL 内的访问控制条目 (ACE) 对分支机构的 IP 寻址来说可以是唯一的。这将减少 Cisco ISE 策略的管理复杂性，但会增加操作复杂性，因为需要在每个分支机构 Catalyst 3850 系列交换机上配置和维护 ACL。

图 3-14 简要介绍了如何在分支机构中实施融合接入 BYOD 设计。

图 3-14　融合接入分支机构 BYOD 设计高级视图

在交换机应用以实现差异化有线和无线设备访问控制的动态 ACL（命名 ACL）分配。



请注意，在本设计指南中，入网有线设备也被静态分配给与无线设备相同的 VLAN。因此，入网有线设备和无线设备将共享相同的 VLAN 以及相同的 IP 子网地址空间。客户可能因为各种问题（例如有关无线设备的附加安全合规性要求）而对有线和无线设备实施单独的子网。本版本的设计指南中将不探讨此问题。动态分配的命名 ACL 为有线设备提供差异化网络访问权限。

在 FlexConnect 和融合接入分支机构设计之间提供差异化访问权限的两种方法的原因在于，在 CUWN 软件版本 7.5 之前， FlexConnect 不允许向接入点动态分配 ACL，而是仅允许动态分配 VLAN。本设计指南中的 FlexConnect 无线设计沿用之前版本的设计指南，并继续要求对每个不同级别的访问控制提供单独的 VLAN。这样会增加分支机构网络配置管理中的管理负担。融合接入设计与园区无线设计更加一致，需要为多级访问控制提供单独的 VLAN。

面向 BYOD 的移动设备管理器

修订日期：2013 年 8 月 7 日

移动设备管理器 (MDM) 保护、监控并管理移动设备，包括公司拥有的设备和员工拥有的 BYOD 设备。 MDM 功能通常包括所有类型设备的策略与配置文件、数字证书、应用，以及数据和配置设置的空中 (OTA) 分发。 MDM 支持和管理的设备不仅包括智能手机和平板电脑等手持设备，还包括日益增多的手提电脑和桌面计算设备。

关键的 MDM 功能包括但不限于：

- PIN 实施 - 实施 PIN 锁定是阻止对设备进行未授权访问的第一步，也是最有效的一步；此外，强密码策略也可以通过 MDM 实施，减少暴力攻击的可能性。
- 越狱 /Root 权限破解检测 - 越狱 （在 Apple iOS 设备上）和 root 权限破解 （在 Android 设备上）是绕过设备管理并移除 SP 控制的两种方式。 MDM 可以检测到此类旁路并立即限制设备对网络或其他公司资产的访问。
- 数据加密 - 大多数设备在设备和文件级别都拥有内置加密功能。MDM 可确保只有支持数据加密并启用该功能的设备可以访问网络和公司数据。
- 数据擦除 - 丢失或被盗的设备可以由用户或管理员通过 MDM 执行完全或部分远程擦除。
- 数据丢失保护 (DLP) - 数据保护功能 （如 PIN 锁定、数据加密和远程数据擦除）可阻止未授权用户访问数据，而 DLP 会阻止授权用户对关键数据的误操作或恶意操作。
- 应用隧道 - 安全连接到公司网络通常是对移动设备的一项强制性要求。

Cisco ISE 1.2 与 MDM API 集成

虽然 Cisco ISE 提供了关键策略功能来支持 BYOD 解决方案，但它对设备状态的感知能力有限。例如， ISE 无法感知设备是否已经实施 PIN 锁定，设备是否已经越狱，或者设备是否正在加密数据等。另一方面， MDM 拥有此类设备状态感知，但其网络策略实施功能相当有限。

因此，为了让 ISE 和 MDM 优势互补，ISE 1.2 增加了对 MDM 集成 API 的支持，可以实现以下两项功能：

- 提取来自 MDM 服务器上的各种信息元素，以便制定包含设备详细信息和 / 或设备状态的粒度网络访问策略决策。
- 将管理活动通过 MDM 推送到受管设备 （例如远程擦除）。

截至本 CVD 发布之日， ISE 1.2 支持与以下第三方 MDM 供应商进行 MDM API 集成：

- AirWatch
- MobileIron

- Good Technology
- XenMobile
- SAP Afaria
- FiberLink Maas360

以下 MDM API 提取 / 推送功能在 ISE 1.2 中受支持且适用于所有第三方 MDM 系统：

- PIN 锁定检查
- 越狱检查
- 数据加密检查
- 设备增强信息检查
- 注册状态检查
- 合规状态检查
- 定期合规状态检查
- MDM 可达性检查
- （完全 / 部分）远程擦除
- 远程 PIN 锁定

MDM 部署选项和注意事项

MDM 解决方案主要有两种部署模式：

- 本地 - 在此模式下，MDM 软件安装在公司 DMZ 或数据中心中的服务器上，由企业 IT 员工支持和维护。
- 基于云 - 也称为 MDM 软件即服务 (SaaS) 模式，在此模式下，MDM 软件通过远程网络操作运营中心 (NOC) 的提供商托管、支持和维护；客户按月或年进行订用并获得通过互联网访问所有 MDM 硬件 / 软件的权利。

在部署 MDM 之前，企业必须制定关键决策，确定其 MDM 解决方案是本地 (on-prem) 还是基于云。此决策涉及多个业务和技术因素，包括以下几点：

- 成本 - 基于云的 MDM 解决方案通常比本地解决方案更具有成本效益；原因在于，它们无需在与专用 MDM 服务器相关的硬件、操作系统、数据库和网络方面花费不断增加的持续成本。还避免了 IT 员工为支持这些服务器而需要的所有其他培训。从云提供商的角度来说，因为这些固定基础设施成本已经投入，为企业用户供应量身定制的虚拟实例的边际成本将会很少，正因如此，其定价可能会颇具吸引力。
- 控制 - 本地模式为企业提供了最大程度的控制，这不仅包括对 MDM 解决方案的控制，还包括对与其集成的企业系统 （例如企业目录、证书颁发机构、电邮基础设施、内容存储库和管理系统，以下将对这些内容进行更详细的讨论）的控制。这是因为，本地模式无需对企业数据进行异地传输或存储。相反，基于云的服务需要放弃对整体解决方案进行一定程度的控制，因为机密信息、数据和文档需要传送到提供商，并且 （取决于服务的详细信息）也可能要异地存储。云提供商还可能在不遵守企业变更控制协议的情况下更新服务器上的软件。
- 安全 - 本地 MDM 模式通常被认为比基于云的模式更加安全；但是，这种安全级别上的感受差异可能正在缩小，尤其是考虑到仅 2012 年就有 140 亿美元的业务是通过 SaaS 安全执行的。最后，系统的安全在大体上不仅取决于部署的技术，还取决于保持硬件和软件适当更新和管理的可用流程。

- 知识产权 - 大多数 MDM 支持在其管理的设备上安全隔离企业数据；但是，这些系统通常需要通过 MDM 传递企业数据，才能空中传输到设备的安全且加密的部分。在基于云的模式中，此过程可能会带来额外的安全问题，因为此时，企业需要在设备管理以及知识产权和机密数据使用方面信任 MDM SaaS 提供商。
- 合规性 - 合规性可以规定金融、医疗以及政府 （和其他）组织的数据存储位置，以及存储方式。此类法规包括 PCI、HIPAA、HITECH、Sarbanes-Oxley 乃至美国爱国者法案。此类法规可能会阻止将敏感信息存储在云中，让组织不得不选择本地 MDM 模式。
- 可扩展性 - 基于云的模式比本地模式具有更好的可扩展性，因为无论小型还是大型部署 （或是介于中间的任何部署）它都可以适应，而且不会给用户带来任何基础设施成本的增加。相反，本地模式可能难以经济高效地进行小型部署。例如，一台可支持 100,000 台设备的 MDM 服务器被部署用于支持仅 100 台设备，这个成本就很不划算。此外，当设备数量增加时，本地模式所需的硬件和基础设施也将逐步增加。
- 部署速度 - 基于云的解决方案通常可以实现更快速的部署 （并且通常可以在订购当天启用），而本地解决方案的计划、安装和部署通常需要几个星期 （或更久）。
- 灵活性 - 基于云的 MDM 解决方案通常拥有对设备硬件和软件新版本的即日支持；而本地解决方案需要对 MDM 软件进行各个支持的新设备和软件的升级。
- 管理简便性 - 对于本地模式，IT 部门必须确保 MDM 拥有所有最新更新；在基于云的系统中，此责任属于提供商。

注意 思科并未倡导使用一种 MDM 部署模式，而不使用另一种模式；思科也不会推荐任何特定的第三方 MDM 解决方案。提及这些业务和技术注意事项仅仅是为了提醒您注意这诸多因素，对于 IT 架构师而言，在评估哪个 MDM 解决方案最能满足其特定业务需求时，这些可能会非常有帮助。

本地

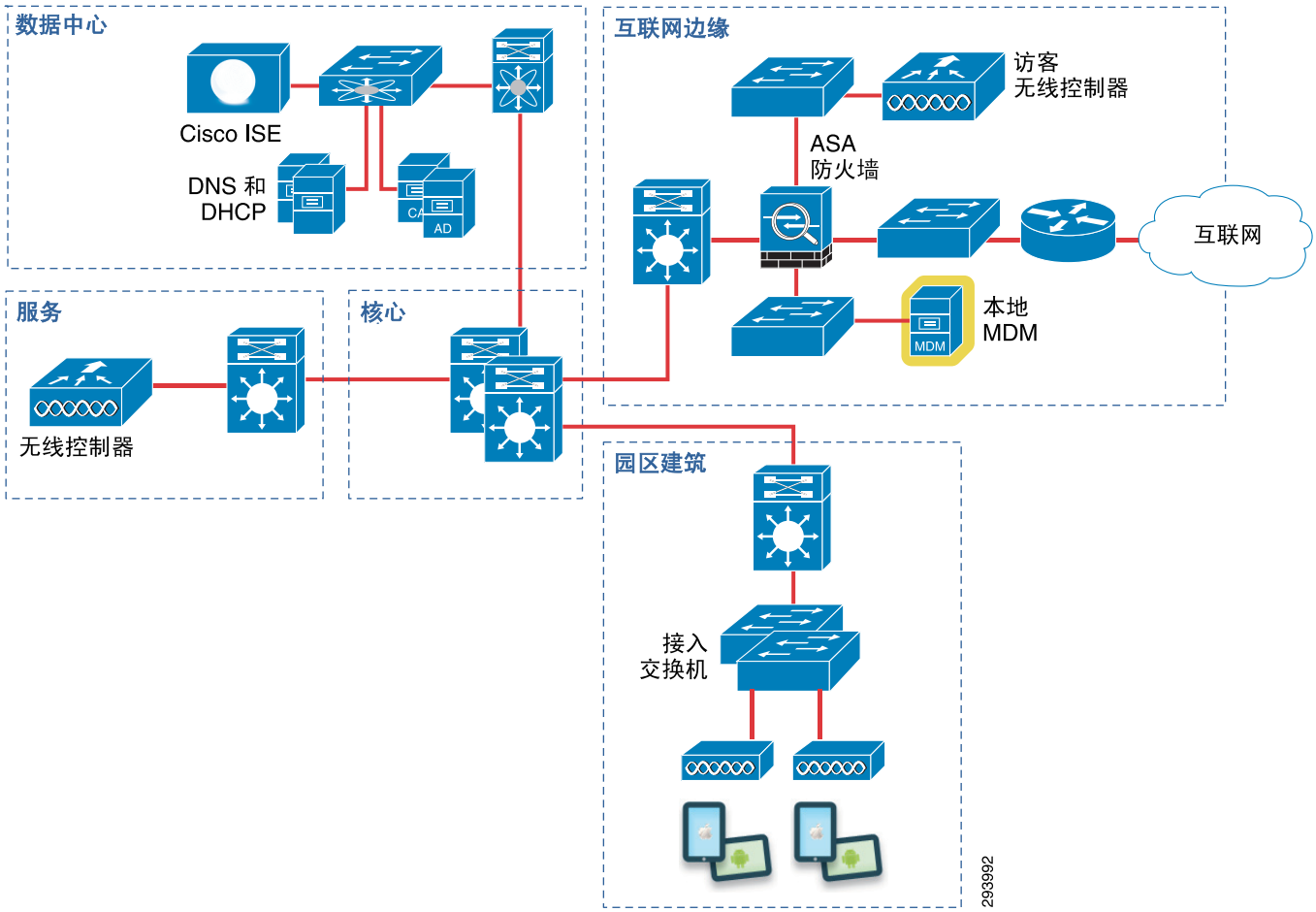
在本地 MDM 部署模式中， MDM 软件位于本地的一个 （或多个）专用服务器中，通常在互联网边缘或 DMZ 内。

此模式通常比较适合拥有高级技术专长 （例如能够配置、定期更新和管理此类服务器）的 IT 员工，或有较严格的安全 / 保密要求的企业 （可能会阻止基于云的服务管理其设备）。

本地模式还可为某些操作流程提供一些性能优势 （因为与基于云的服务相反，它与设备相对比较接近）。例如，如果网络访问策略包括 “MDM 可达性”检查，则此测试在本地 MDM 部署模式中的响应能力比在基于云的模式中要好。

对于使用本地 MDM 部署模式的园区 BYOD 网络，其网络拓扑如图 4-1 所示。

图 4-1　使用本地 MDM （在互联网边缘）的园区 BYOD 网络



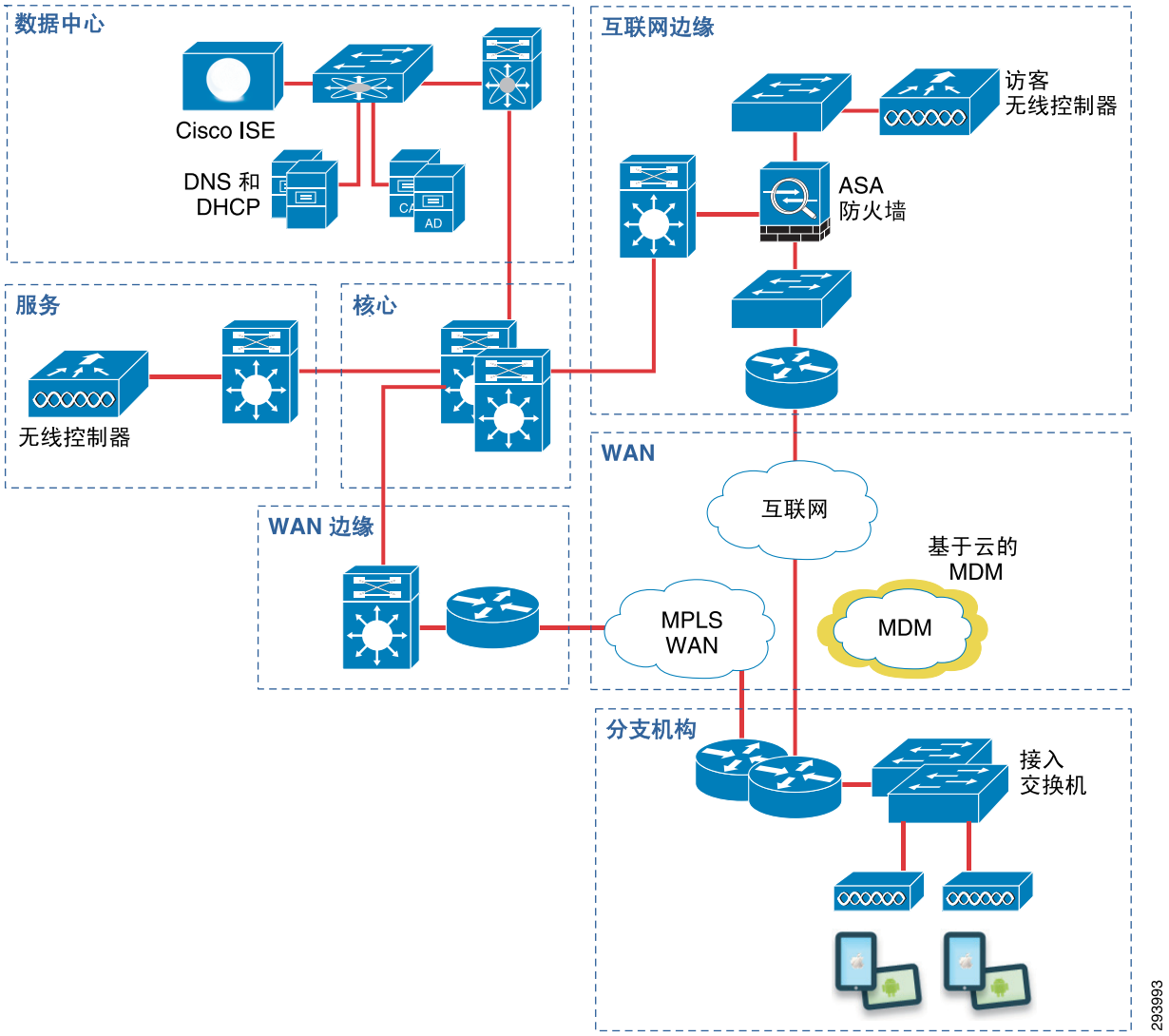
基于云

在基于云的 MDM 部署模式中，MDM 功能以 SaaS 的方式向客户提供：软件全部位于 MDM 供应商的云中，带有为每个客户提供的量身定制的虚拟实例。

从客户的角度来看，这种模式非常简便（因为他们现在不必配置、更新、维护和管理 MDM 软件）；但是，作为交换，他们放弃了对所有设备（以及设备中的某些数据）一定程度的控制，将这些控制交给了第三方 MDM SaaS 供应商，这可能会带来安全问题。因此，这种模式可能更适合于拥有一般 IT 技术专长且无特别安全要求的中小企业。

对于使用基于云的 MDM 部署模式的分支机构 BYOD 网络，其网络拓扑如图 4-2 所示。

图 4-2　使用基于云的 MDM 的分支机构 BYOD 网络



企业集成注意事项

除了本文档中详细介绍的企业网络与 MDM 的集成外，其他企业服务和资源对与 MDM 系统的集成也同样重要，包括：

- 企业目录服务
- 证书颁发机构 (CA) 以及公钥基础设施 (PKI)
- 电邮基础设施
- 内容存储库
- 管理系统

企业目录服务集成

MDM 可以利用企业目录服务（例如基于 LDAP 的目录、 Active Directory 等）有效组织和管理用户访问。管理员可以根据目录组成员身份将设备配置文件、应用和内容分配给用户。此外，有些 MDM 可以检测目录更改并自动更新设备策略。例如，如果在目录系统中停用某个用户，那么 MDM 可以取消基于设备的企业网络访问权限，并选择性地擦除设备。

企业证书颁发机构和公钥基础设施集成

MDM 可以利用证书颁发机构 （例如 Microsoft CA）或 SCEP 证书服务提供商 （例如 MSCEP 和 VeriSign）分配和验证证书，以便进行高级用户身份验证并保护对企业系统的访问。CA 集成可确保消息的完整性、真实性和保密性。其他 CA 集成可实现客户端身份验证、加密和消息签名。

此外， MDM 也可以与公钥基础设施 (PKI) 或第三方提供商集成，在无需用户干预的情况下配置证书并分发给设备。

电邮集成

企业电邮基础设施可以与 MDM 解决方案集成，以便提供与电邮管理相关的安全性、可视性和控制。这使得员工能够在其移动设备上访问企业电邮，而不影响安全性。不仅如此，此类集成还简化了移动电邮的管理 （例如空中配置电邮设置、阻止非受管设备接收电邮、实施设备加密等）。MDM 管理电邮的方法因 MDM 提供商而异，是一项具有竞争差异的功能。电邮策略信息无法通过 API 提供给 ISE。

内容存储库集成

通过将 MDM 系统与内容存储库集成，管理员一方面可以提供对公司文档的安全移动访问，一方面可以管理文档分发和访问权限 （包括能够查看、离线查看、通过电邮发送或打印文档）。这可以确保将正确的内容提供给正确的员工，而不影响通过加密连接分发给移动设备的文档本身的安全性。此外，文件和文档可以与公司文件系统和共享点同步，如此一来，文档的最新版本会在员工的移动设备上自动更新。为了确保安全，可以通过用户名、密码和证书对用户进行身份验证，然后再允许他们访问公司内容。此外，文档元数据 （包括作者、关键字、版本和创建或修改日期）可以按每个用户加以限制。

管理集成

MDM 系统可与企业管理系统集成，以强化对设备和控制台事件的日志记录、记录和报告。事件日志记录设置可以根据严重性级别配置，并能通过系统日志集成向外部系统发送特定级别。事件可能包括登录事件、失败登录尝试次数、系统设置和配置更改，以及配置文件、应用和内容更改等。此类管理系统集成可确保安全性以及法规和公司政策的合规性。

集成服务器

在本地部署模式中，这些企业系统与 MDM 的集成相对简单，因为其主要问题在于确保正确配置适当的协议，且路径内所有防火墙中的所需端口都已打开。但是，在基于云的部署模式中，此类集成需要从客户到 MDM 服务提供商和 / 或位于客户端 DMZ 中的专门 MDM 集成服务器 （或类似代理服务器）的安全传输协议 （例如通过 HTTPS）。

第 2 部分

配置基础设施

自带设备无线基础设施设计

修订日期：2013 年 8 月 7 日

思科无线 LAN 控制器 (WLC) 不但可用于将无线配置和管理功能自动化，还能提供对无线网络的可视性和控制。 WLC 能够与身份服务引擎交互，对各种不同的终端执行身份验证和授权策略。

在设计 WLAN 网络时，应该考虑以下几点：

- WLAN 的作用
- WLAN 的身份验证机制
- 网络中 WLAN 的数量

本设计指南在逻辑上将 WLAN 划分为不同的逻辑功能：设备调配和安全网络访问。这两个功能可由两个不同的 WLAN 分别提供，也可以合并到单个 WLAN。本设计指南既包括单 SSID 部署模式，也包括双 SSID 部署模式，同时适用于分支机构和园区位置。请注意，在本设计指南中，无线访客接入在另一个 WLAN 上实施。

选择单或双 SSID 配置时的部分考虑事项如下：

- 一些组织希望对自注册设备使用专用 SSID。
- 其他组织则将双 SSID 视为额外的管理负担。
- 增加一个 SSID 会增加通道开销。
- 启用太多 SSID 可能会降低无线性能。

组织的独特需求和偏好将影响部署的具体模式。 ISE 和 WLC 的配置都可以很容易地修改，从而支持单或双 SSID 部署。

园区 - 统一无线 LAN 设计

如第 3 章，“BYOD 的园区网络和分支机构网络设计”中的集中式 （本地模式）无线设计中所述，本设计指南讨论了两种适用于园区的无线 LAN 设计，即集中式设计 （本地模式）和融合接入设计。从园区无线基础设施连接的客户端由在本地模式 （中央交换）下配置的 CT5508 统一控制器专用集群提供服务，或由 Catalyst 3850 系列交换机 （提供移动代理 (MA) 功能）和 CT5760 无线控制器 （提供移动控制器功能）共同提供服务。本节讨论统一无线 LAN 设计，然后讨论融合接入。无线控制器配置适当的 SSID，以提供设备自注册和安全访问。此功能可通过单或双 SSID 来提供。

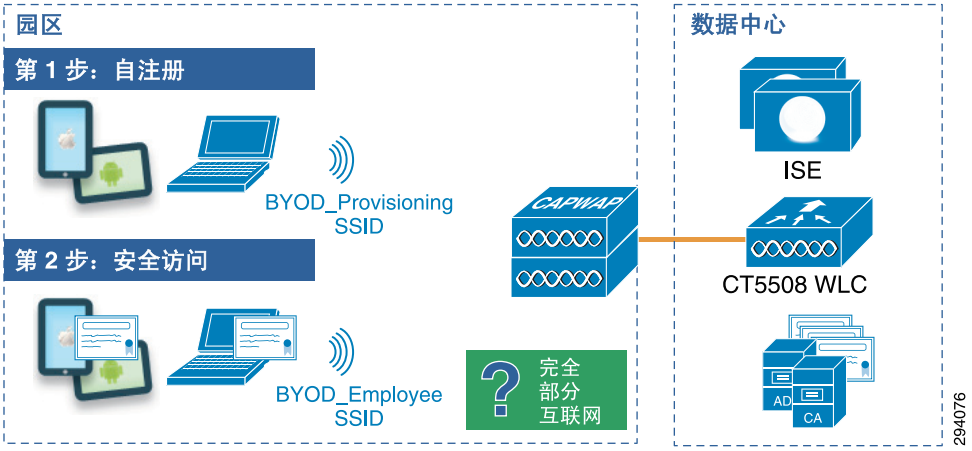
注意　CT5760 无线控制器也可以配置作为集中式（本地模式）无线控制器。如第 3 章，“BYOD 的园区网络和分支机构网络设计”的园区迁移路径中所述，这可能是从现有无线覆盖设计迁移到融合接入设计的必要步骤。

集中式园区 - 双 SSID 设计

此设计采用两个 SSID：一个提供注册 / 调配，另一个提供安全网络访问。在连接到 BYOD_Provisioning SSID 并完成注册和调配步骤后，用户连接到 BYOD_Employee SSID，该 SSID 通过安全 EAP-TLS 连接提供网络访问。

图 5-1 显示了适用于园区 AP 的双 SSID 设计。

图 5-1　　园区 - 双 SSID



在双 SSID 设计中，有一些额外的考虑事项：

- 调配 SSID 可以是开放形式，也可以采用密码保护形式。如果调配 SSID 是开放形式，则任何用户都可以连接到该 SSID；但如果它有密码保护，则仅允许具有凭证（如 AD 组成员身份）的用户连接到该 SSID。本设计指南中配置的调配 SSID 是开放形式，其唯一目的是提供自注册服务。
- 在调配设备后，假设用户将切换到第二个 SSID 以进行常规网络访问。为了防止用户一直与调配 SSID 保持连接，必须对调配 SSID 实施一个访问列表，该列表仅提供对 ISE、DHCP 和 DNS 的访问。 ACL_Provisioning_Redirect ACL 的详细信息如下所示。
- 本设计指南使用以下 SSID：BYOD_Provisioning 和 BYOD_Employee。

在表 5-1 中重点介绍了这两个 SSID 的属性。

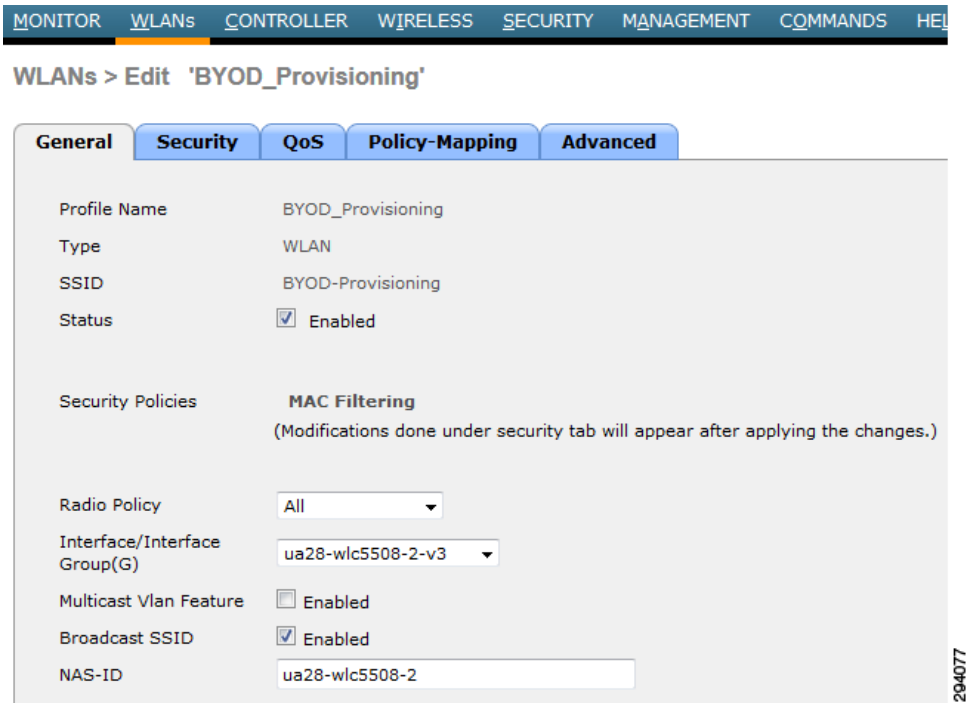
表 5-1　　WLAN 参数

属性	BYOD_Provisioning	BYOD_Employee
说明	仅用于设备调配	用于已完成自注册过程的员工
第 2 层安全	无 （对于开放式 SSID）	WPA+WPA2
MAC 过滤	已启用 （对于开放式 SSID）	已禁用
WPA+WPA2 参数	无	WPA2 策略、 AES、 802.1X
第 3 层安全	无	无
AAA 服务器	选择 ISE	选择 ISE
高级	AAA 覆盖已启用	AAA 覆盖已启用
高级	NAC 状态 - RADIUS NAC	NAC 状态 - RADIUS NAC
服务质量	尽力而为	白金级
AVC	无	已启用

要创建 WLAN，请点击 **WLANs > Create New > Go** 并提供 SSID 和配置文件详细信息。首先参阅图 5-2，其中重点显示了 BYOD_Provisioning SSID 的常规配置步骤。配置 BYOD_Employee WLAN 的步骤与之类似，但需要遵循表 5-1 中的设置。

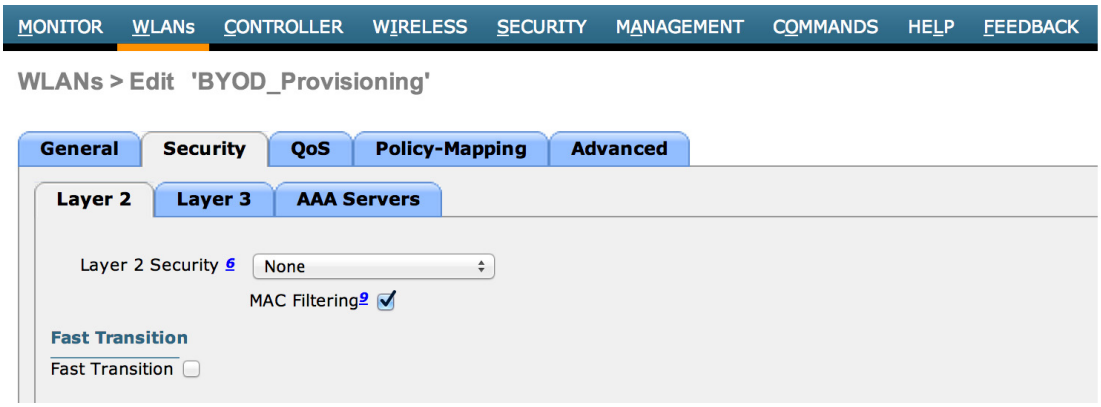
注意　在实施使用多个无线 LAN 控制器的自带设备解决方案时，必须保持各 WLAN ID 一致。ISE 使用 WLAN ID 来确定哪些 WLAN (SSID) 客户端用于连接到网络。确保每个 WLAN 在每个 WLC 上都有相同的 WLAN ID 对于正常运行和安全性至关重要。

图 5-2　　创建 BYOD_Provisioning SSID



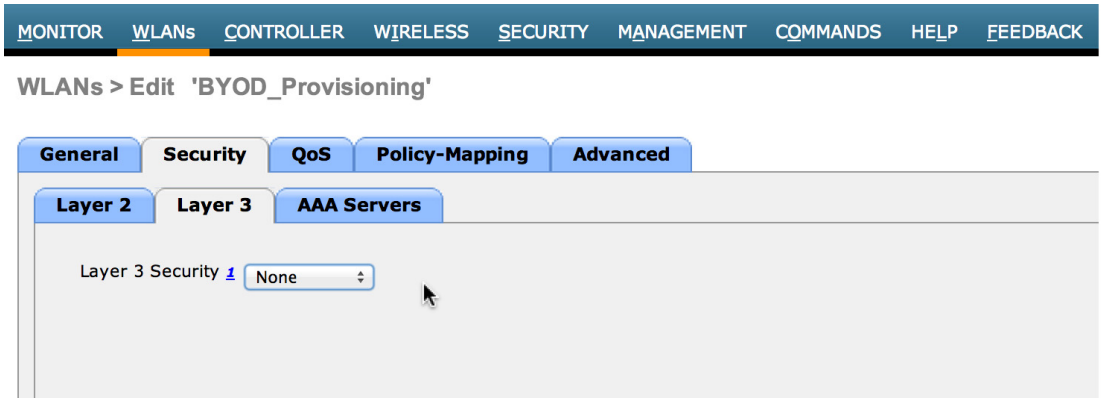
因为 BYOD_PROVISIONING 是开放式 SSID，所以第 2 层安全设置配置为 **None**。如果调配 SSID 必须采用密码保护形式，则必须将第 2 层安全设置配置为 WPA+WPA2 Enterprise。

图 5-3　　第 2 层安全设置



第 3 层安全被配置为 **None**，如图 5-4 中所示。

图 5-4　　第 3 层安全设置



安全设置中的主要配置是指定 RADIUS 服务器配置详细信息。图 5-5 显示了如何配置 ISE 的 IP 地址以进行身份验证和授权。

图 5-5　　AAA 安全设置

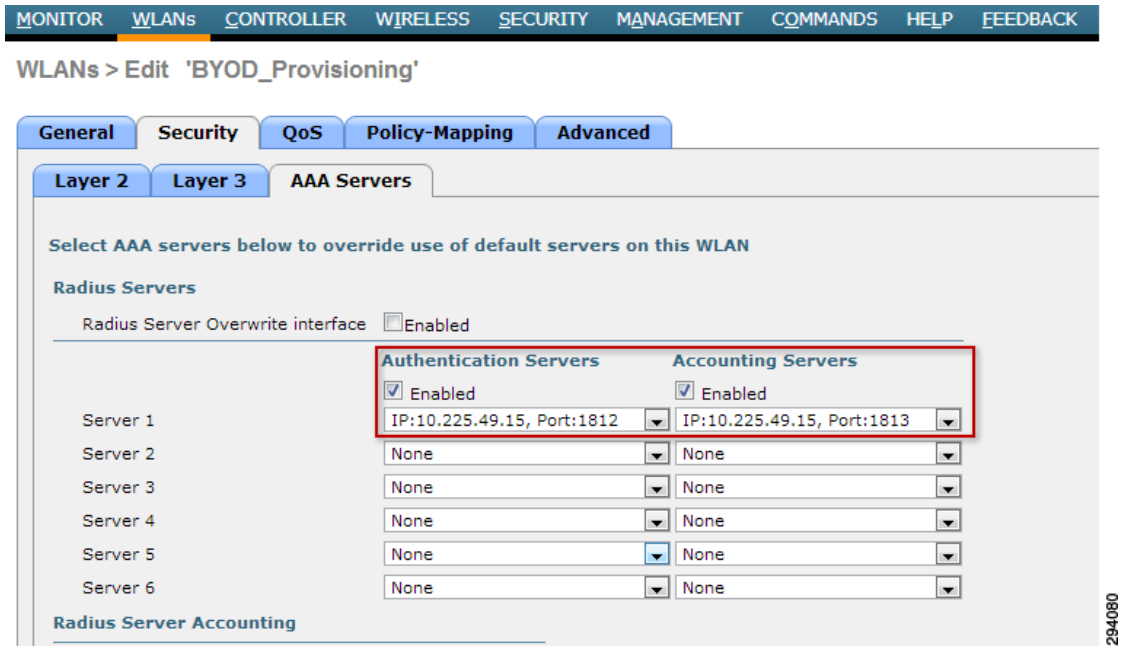
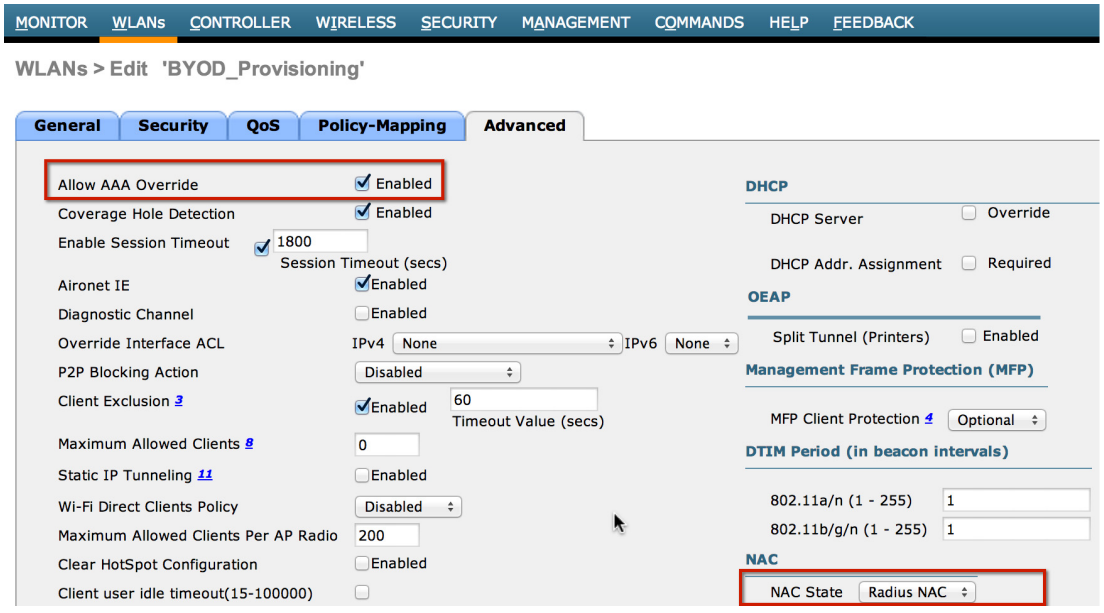


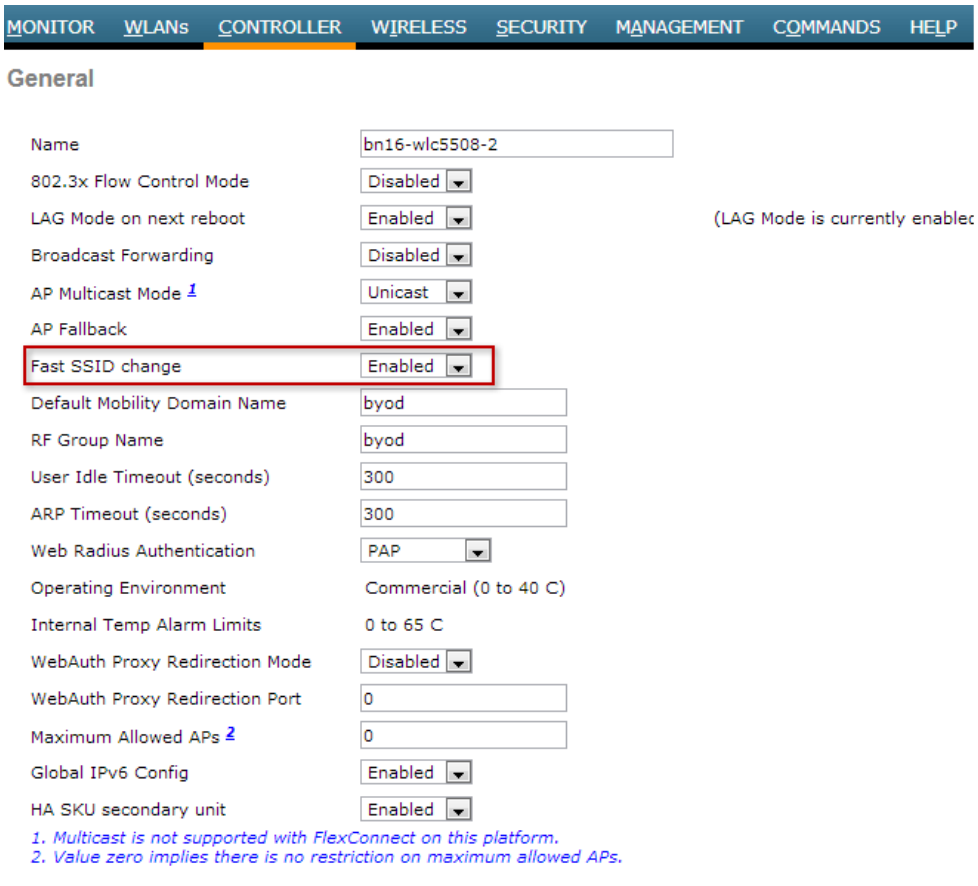
图 5-6 显示了高级设置，包括 AAA 覆盖和 NAC 状态。

图 5-6　　高级设置



当设备需要从一个 SSID 切换到另一个时，快速 SSID 更改功能非常有用。这适用于双 SSID 自带设备设计。当用户使用 BYOD_Provisioning 完成注册后，便会切换到 BYOD_Employee SSID。通过启用快速 SSID 更改功能，用户可立即切换到新 SSID 而不会感觉到任何延迟。要启用快速 SSID 更改，请点击 **Controller > General > Fast SSID change**，如图 5-7 中所示。

图 5-7　　快速 SSID 更改

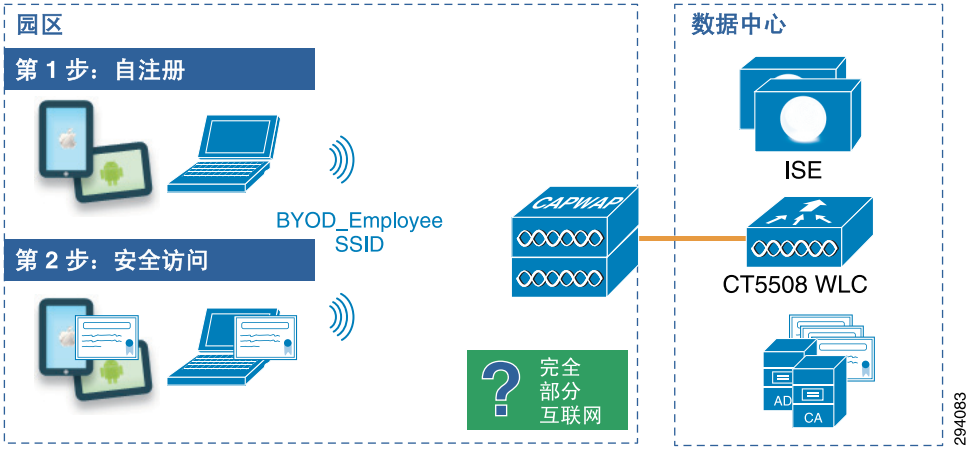


注意　第 6 章，“面向 BYOD 的身份服务引擎”中的授权策略和配置文件显示了用于双 SSID 调配和单 SSID 调配的 ACL 和授权配置文件。

集中式园区 - 单 SSID 设计

在单 SSID 设计中，自注册和安全网络访问使用的是同一 WLAN (BYOD_Employee)。图 5-8 显示了可以如何使用 5508 无线 LAN 控制器实施此设计。在本例中，控制器专用于管理园区中的 AP。

图 5-8　　园区 - 单 SSID



注意　第 6 章，“面向 BYOD 的身份服务引擎”中的授权策略和配置文件显示了用于双 SSID 调配和单 SSID 调配的 ACL 和授权配置文件。

集中式园区 - 使用 TrustSec 的策略实施

如第 3 章，“BYOD 的园区网络和分支机构网络设计”中的 ACL 复杂性和注意事项中所述，以前版本的 CVD 中使用在无线控制器上预配置的命名 ACL 来实施基于角色的策略，以实现对网络和数据中心资源的访问。本 CVD 引入了一项称为 TrustSec 的免费技术（即安全组访问 (SGA)），该技术通过使用安全组标记 (SGT) 来实施基于角色的策略，以此控制对数据中心资源的访问。本 CVD 讨论了如何通过在 ISE 中创建的网络设备定义而逐渐迁移到使用 SGT 来代替 ACL 或作为 ACL 的补充。

分支机构 - 统一无线 LAN 设计

FlexConnect 无线 LAN 设计

在本设计指南中，从分支机构位置连接的终端由 Flex 7500 无线 LAN 控制器或虚拟无线 LAN 控制器 (vWLC) 集群进行管理。 vWLC 是可在行业标准虚拟化基础设施上运行的软件，比较适合中小企业。

本节所述的配置参数同时适用于 vWLC 和 Flex 7500 控制器。

以下链接提供了有关如何使用 VMware 设置 vWLC 的更多信息：
http://www.cisco.com/en/US/customer/products/ps12723/products_tech_note09186a0080bd2d04.shtml。

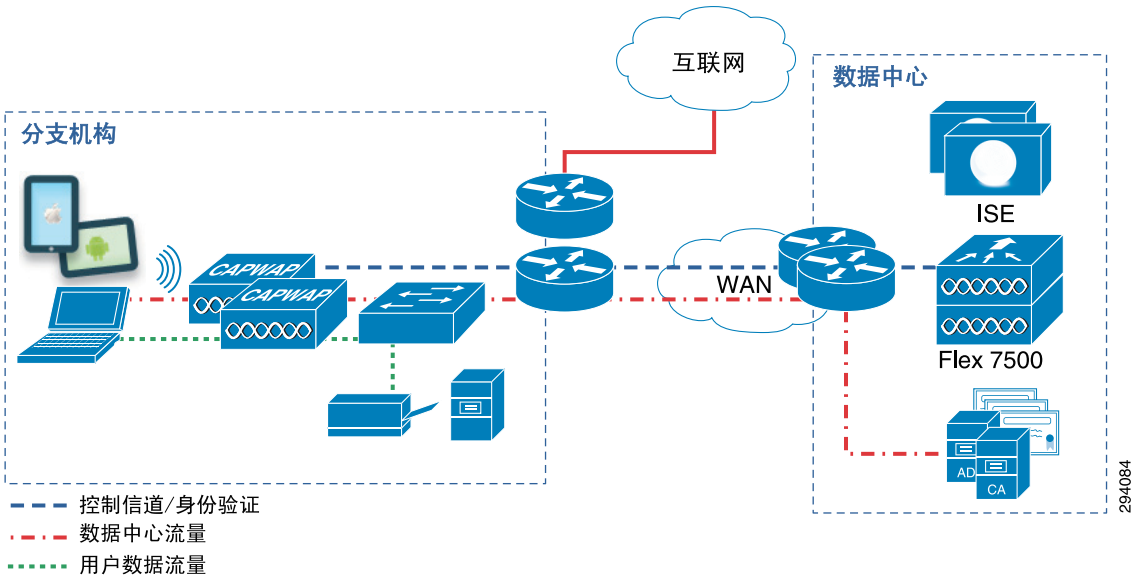
FlexConnect（以前称为混合远程边缘接入点或 H-REAP）是一款适合分支机构办公室和远程办公室部署的无线解决方案。通过该解决方案，客户可以从公司办公室通过广域网 (WAN) 链路配置和控制分支机构或远程办公室中的接入点，而无需在每个办公室中部署一个控制器。FlexConnect 接入点在与控制器失去连接时，可以在本地交换客户端数据流量并在本地执行客户端身份验证。

使用 FlexConnect 架构分配客户端数据流量具有一些优点：

- 无需在每个分支机构位置配备一个控制器。
- 在 WAN 链路发生故障期间能够在分支机构内提供移动弹性。
- 实现集中管理和故障排除。

图 5-9 中的 FlexConnect 架构显示了源自分支机构的不同通信流量。

图 5-9　　FlexConnect 架构



当终端与 FlexConnect 接入点相关联时，接入点会将所有身份验证消息发送到控制器，并根据 WLAN 配置，在本地交换数据包 （本地交换）或将数据包发送至控制器 （中央交换）。

对于数据包流量， WLAN 可采用以下任一模式：

- 中央交换 - 中央交换的 WLAN 通过隧道将无线用户流量和所有控制流量发送到集中式 WLC，由集中式 WLC 将用户流量映射到动态接口或 VLAN。
- 本地交换 - 在此模式中， FlexConnect 接入点通过在有线接口本地丢弃所有流量，实现本地交换数据包。无线用户流量通过 802.1Q 中继被映射到离散式 VLAN。

《Flex 7500 无线分支机构控制器部署指南》提供了更多详细信息：
http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml。

向用户提供差异化访问权限的关键策略是通过将用户动态分配给不同的 VLAN 来实现的。FlexConnect 的 AAA 覆盖功能根据从 ISE 返回的 RADIUS 属性向特定 VLAN 分配单独的客户端。

必须使用可由 ISE 服务器返回的所有可能的 VLAN 对接入点进行预配置。这包括作为授权的一部分而被 ISE 返回的 VLAN 分配。如果 AP 上不存在从 ISE 返回的 VLAN，客户端会恢复到为 WLAN 配置的默认 VLAN。

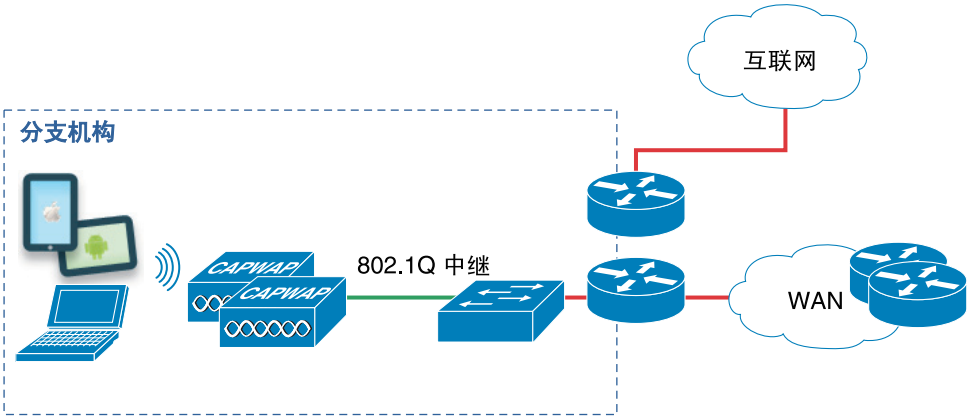
在本设计中，我们为 BYOD_Employee SSID 上的无线连接配置了三个 VLAN。表 5-2 列出了这些 VLAN 及其用途。

表 5-2　　VLAN 和用途

VLAN 编号	VLAN 名称	说明
10	Wireless_Full	分配给此 VLAN 的用户具有对园区和分支机构服务器的完全访问权限。
11	Wireless_Partial	分配给此 VLAN 的用户除具有互联网访问权限外，还有权访问其他园区和分支机构资源。
12	Wireless_Internet	分配给此 VLAN 的用户只能访问互联网。
18	AP_Mgmt_Flex	用户首先会被放入此本地 VLAN，直到授权策略确定了适当的 VLAN。

由于有不只一个 VLAN 配置用于本地交换，因此分支机构的 FlexConnect AP 必须连接到 802.1Q 中继链路。 AP 和上游交换机端口都需要配置为支持 802.1Q 中继。图 5-10 显示了连接到 FlexConnect AP 的接入层交换机的配置示例。

图 5-10　　中继配置



分支机构无线 IP 地址设计

一旦设备被动态分配给 VLAN，终端就必须从 DHCP 服务器获取 IP 地址。以下示例使用 **ip-helper address** 命令配置分支路由器的第 3 层子接口，使其指向一个 DHCP 服务器：

```
interface GigabitEthernet0/1
 description Trunk to branch bn22-3750x-1
 no ip address
 media-type sfp
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.200.10.2 255.255.255.0
 ip helper-address 10.230.1.61
```

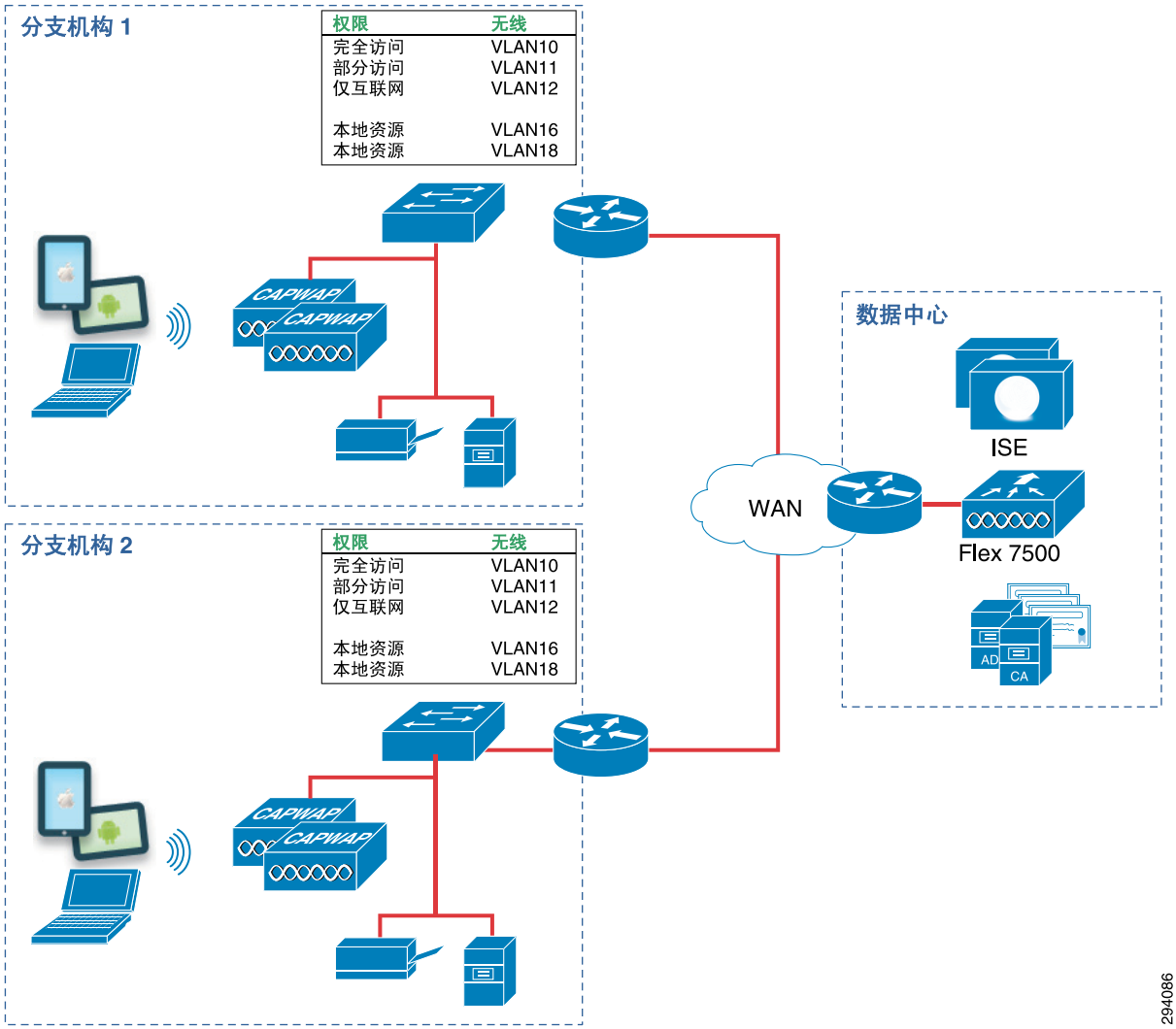
```
 standby 10 ip 10.200.10.1
 standby 10 priority 110
 standby 10 preempt
!
interface GigabitEthernet0/1.11
 encapsulation dot1Q 11
 ip address 10.200.11.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 11 ip 10.200.11.1
 standby 11 priority 110
 standby 11 preempt
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.200.12.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 12 ip 10.200.12.1
 standby 12 priority 110
 standby 12 preempt
```

图 5-11 中显示了两个分支机构利用数据中心资源的情况，并展示了以下要点：

- 在分支机构中，终端将根据其被授予的访问权限级别放置到不同的 VLAN。
- 来自分支机构的无线基础设施由单个 Flex 7500 控制器集群管理。
- 分配给 VLAN 10 的终端被授予对网络资源的完全访问权限，分配给 VLAN 11 的终端被授予对网络资源的部分访问权限，分配给 VLAN 12 的终端仅被授予互联网访问权限。

根据匹配的授权配置文件，用户将被分配给定义了预定义权限的特定 VLAN。

图 5-11　　在分支机构中使用的 VLAN

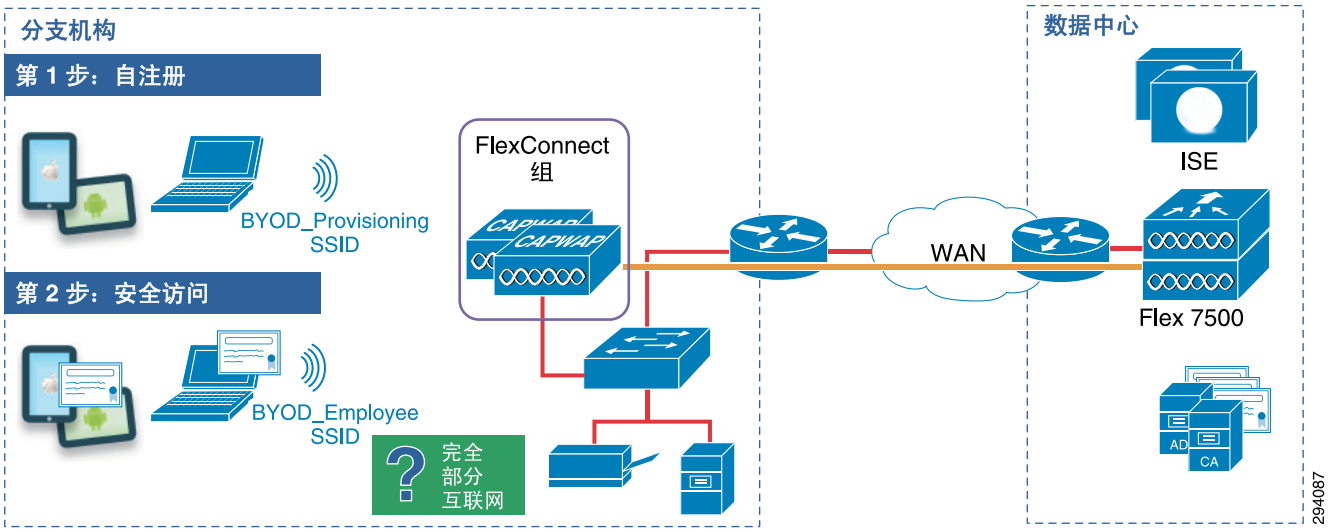


FlexConnect 分支机构 - 双 SSID 设计

在双 SSID 设计中，会配置两个 SSID：一个 SSID 提供注册 / 调配，另一个提供安全 EAP-TLS 访问。在连接到 BYOD_Provisioning SSID 并完成注册和调配步骤后，用户会连接到 BYOD_Employee SSID，由该 SSID 提供安全网络访问。

图 5-12 显示了适用于分支机构 AP 的双 SSID 设计。

图 5-12　　分支机构 - 双 SSID



在双 SSID 设计中，有一些额外的考虑事项：

- 调配 SSID 可以是开放形式或密码保护形式。如果调配 SSID 是开放形式，则任何用户都可以连接到该 SSID；但如果它有密码保护，则仅允许具有凭证（如 AD 组成员身份）的用户连接到该 SSID。
- 在调配设备后，用户通过 EAP-TLS 连接到 BYOD_Employee SSID 进行网络访问。为了防止用户一直与调配 SSID 保持连接，必须对调配 SSID 实施一个访问列表，该列表仅提供对 ISE、DHCP 和 DNS 的访问。此 SSID 的详细信息在“客户端推送”一节中讨论。

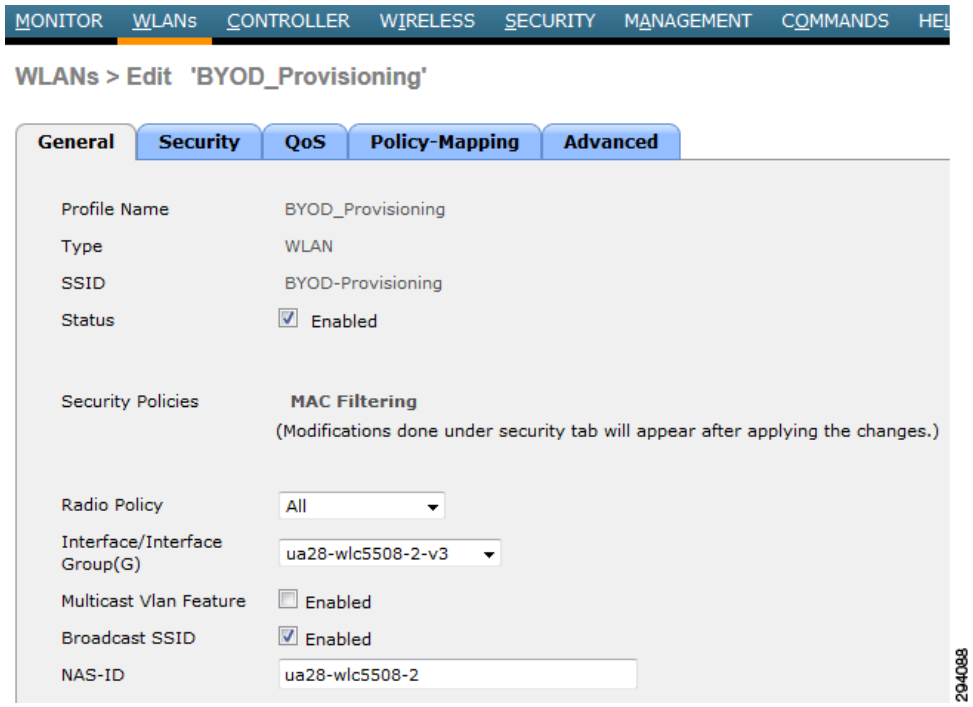
表 5-3 显示了在本设计指南中使用的 SSID 的 WLAN 参数。

表 5-3　　WLAN 参数

属性	BYOD_Provisioning	BYOD_Employee
说明	用于设备调配	用于已完成自注册过程的员工
第 2 层安全	无（对于开放式 SSID）	WPA+WPA2
MAC 过滤	已启用（对于开放式 SSID）	已禁用
WPA+WPA2 参数	无（对于开放式 SSID）	WPA2 策略、AES、802.1X
第 3 层安全	无	无
AAA 服务器	选择 ISE	选择 ISE
高级	AAA 覆盖已启用	AAA 覆盖已启用
高级	NAC 状态 - RADIUS NAC	NAC 状态 - RADIUS NAC
高级 - FlexConnect 本地交换	对中央交换调配禁用 对本地交换调配启用	已启用
服务质量	尽力而为	白金级
AVC	不适用	不适用

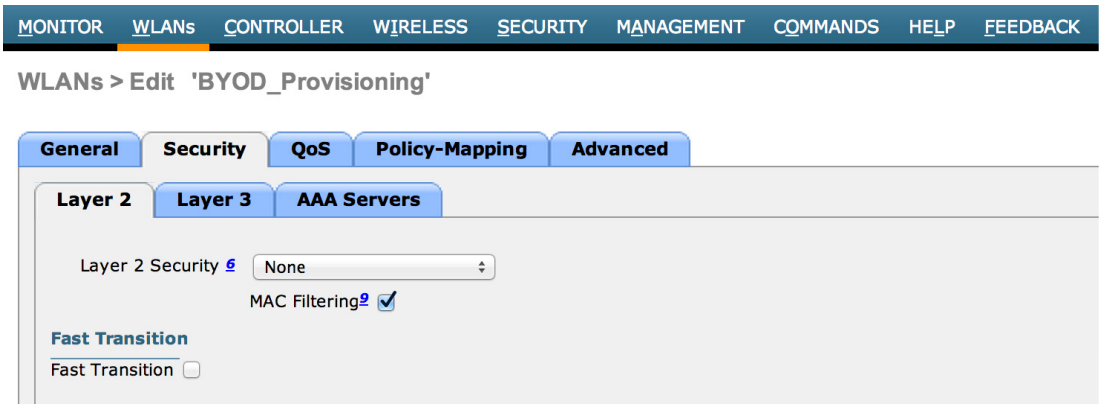
要创建 WLAN，请点击 **WLANs > Create New > Go** 并提供 SSID 和配置文件详细信息。图 5-13 显示了 BYOD_Provisioning SSID 的一般配置详细信息。

图 5-13　创建分支机构 BYOD_Provisioning SSID



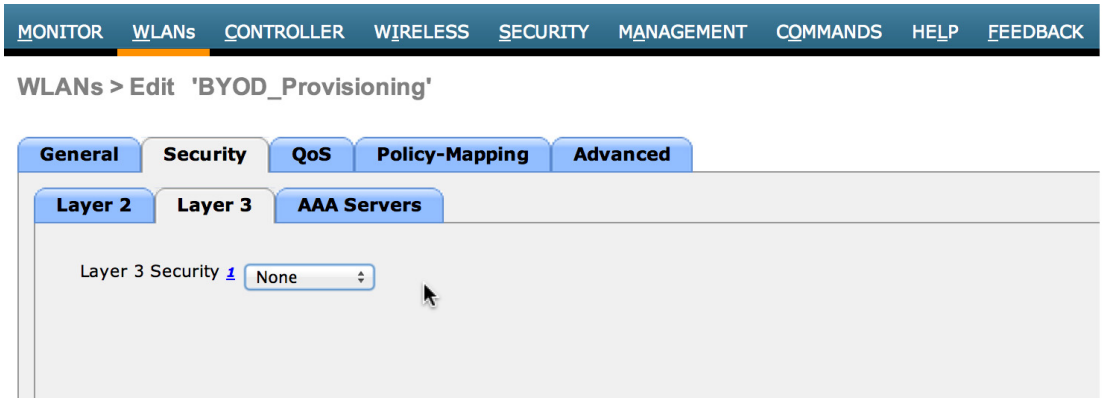
由于 BYOD_Provisioning 是开放式 SSID，第 2 层安全设置配置为 **None**。如果调配 SSID 必须采用密码保护形式，则第 2 层安全设置将被配置为 WPA+WPA2 Enterprise。

图 5-14　第 2 层安全设置



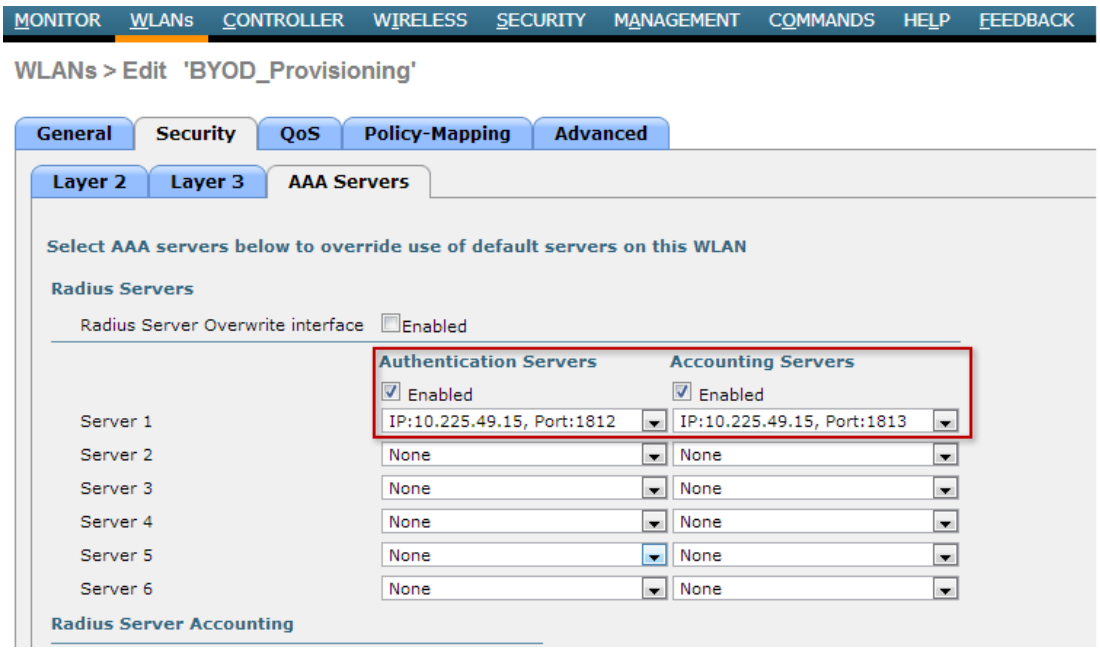
第 3 层安全被配置为 **None**，如图 5-15 中所示。

图 5-15　　第 3 层安全设置



在 **Security > AAA servers** 下，配置 RADIUS 服务器详细信息。图 5-16 显示了 ISE 中配置用于身份验证和授权的 IP 地址。

图 5-16　　AAA 安全设置



在双 SSID 部署中，可采用两种方式对调配流量进行导向：

- 从园区或数据中心 - 终端收到来自数据中心的 DHCP 作用域的一个 IP 地址，调配流量被导向经过分支机构与 Flex 7500 控制器之间的 CAPWAP 隧道。
- 在分支机构 - 终端收到来自分支机构的 DHCP 作用域的一个 IP 地址，调配流量使用交换和 WAN 基础设施来连接到数据中心资源。

双 SSID - 中央交换调配

图 5-17 显示了在使用中央交换调配的情况下，终端如何使用 CAPWAP 隧道与 ISE 和数据中心资源通信，以及所有流量如何通过隧道传回数据中心中的控制器。

图 5-17　　中央交换调配

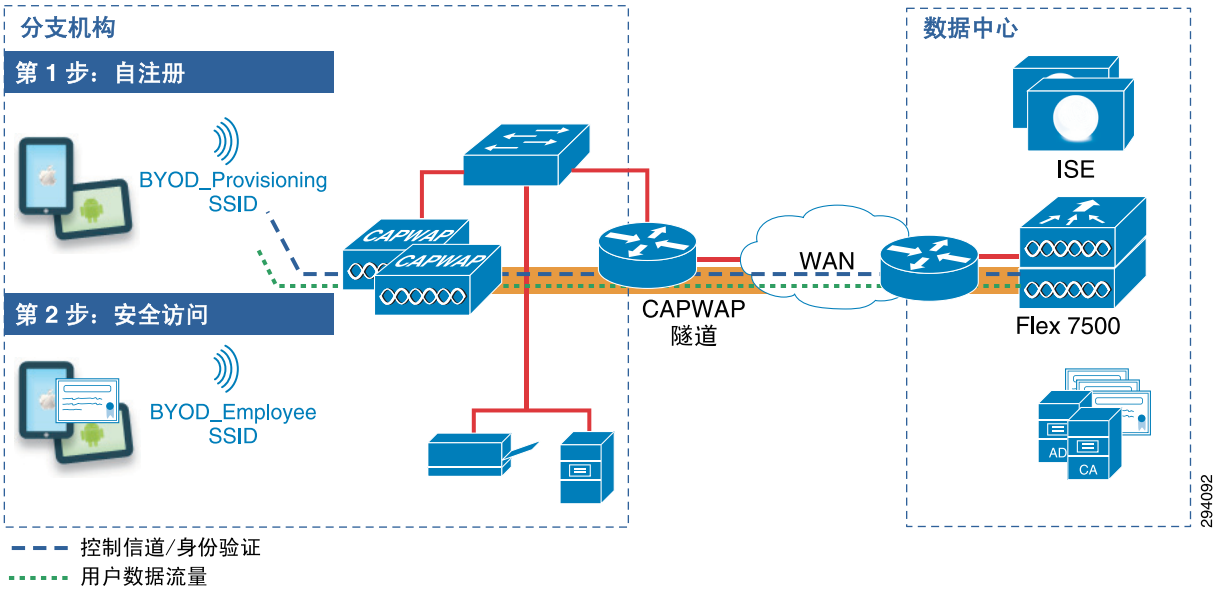
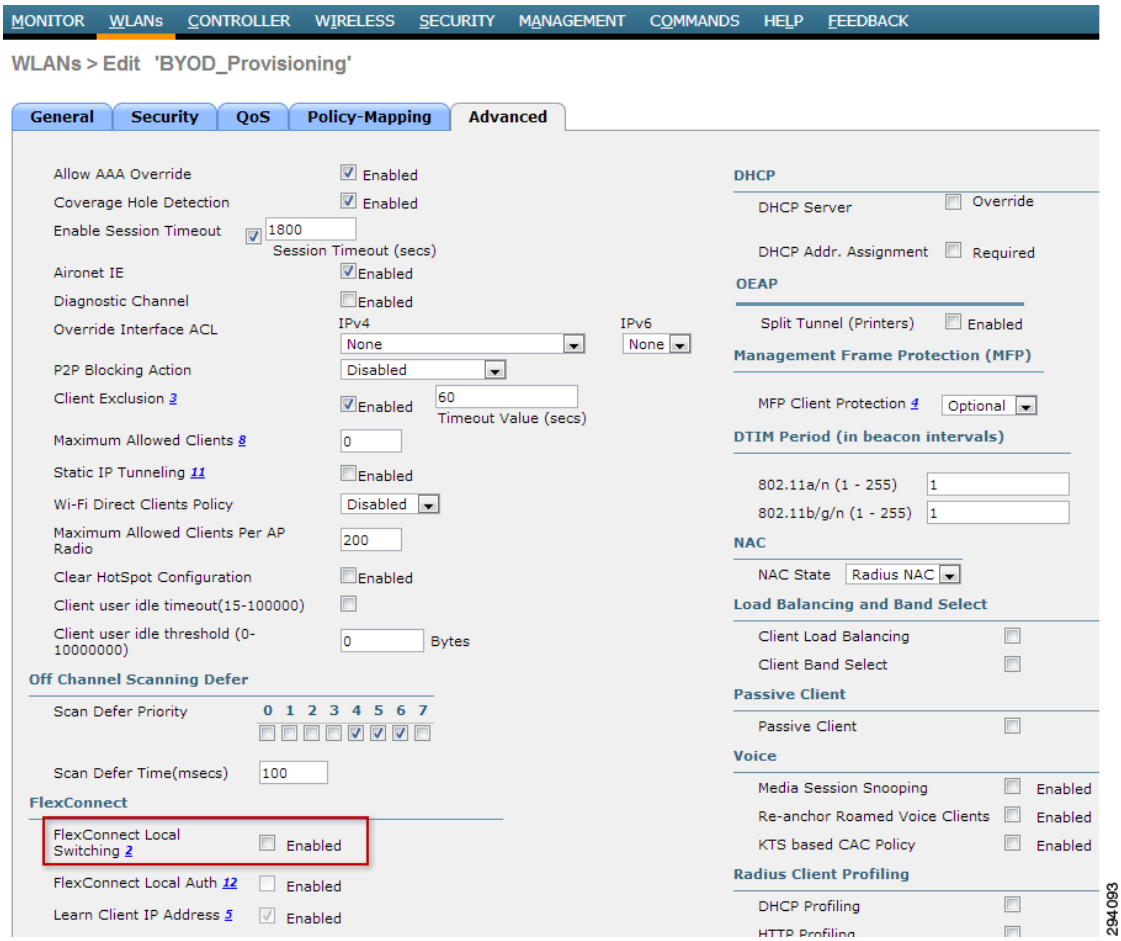


图 5-18 显示了 BYOD_Provisioning 的高级设置，包括 AAA 覆盖和 NAC 状态。对于中央交换调配， FlexConnect 本地交换设置处于禁用状态。

图 5-18　　中央交换调配的高级设置



注意　第 6 章，“面向 BYOD 的身份服务引擎”中的授权策略和配置文件显示了用于双 SSID 调配和单 SSID 调配的 ACL 和授权配置文件。

双 SSID - 本地交换调配

图 5-19 显示了采用本地交换模式的调配。用户数据流量被发送到交换机接口，终端依赖普通路由器 /WAN 基础设施来连接到 ISE 和其他网络资源。

图 5-19　　本地交换调配

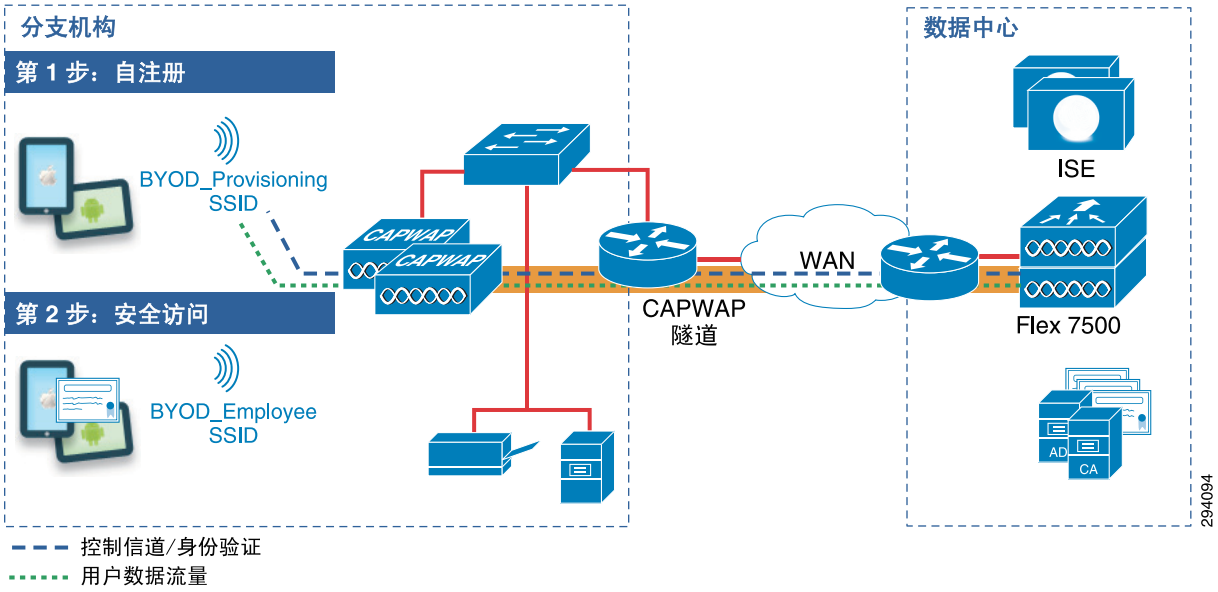
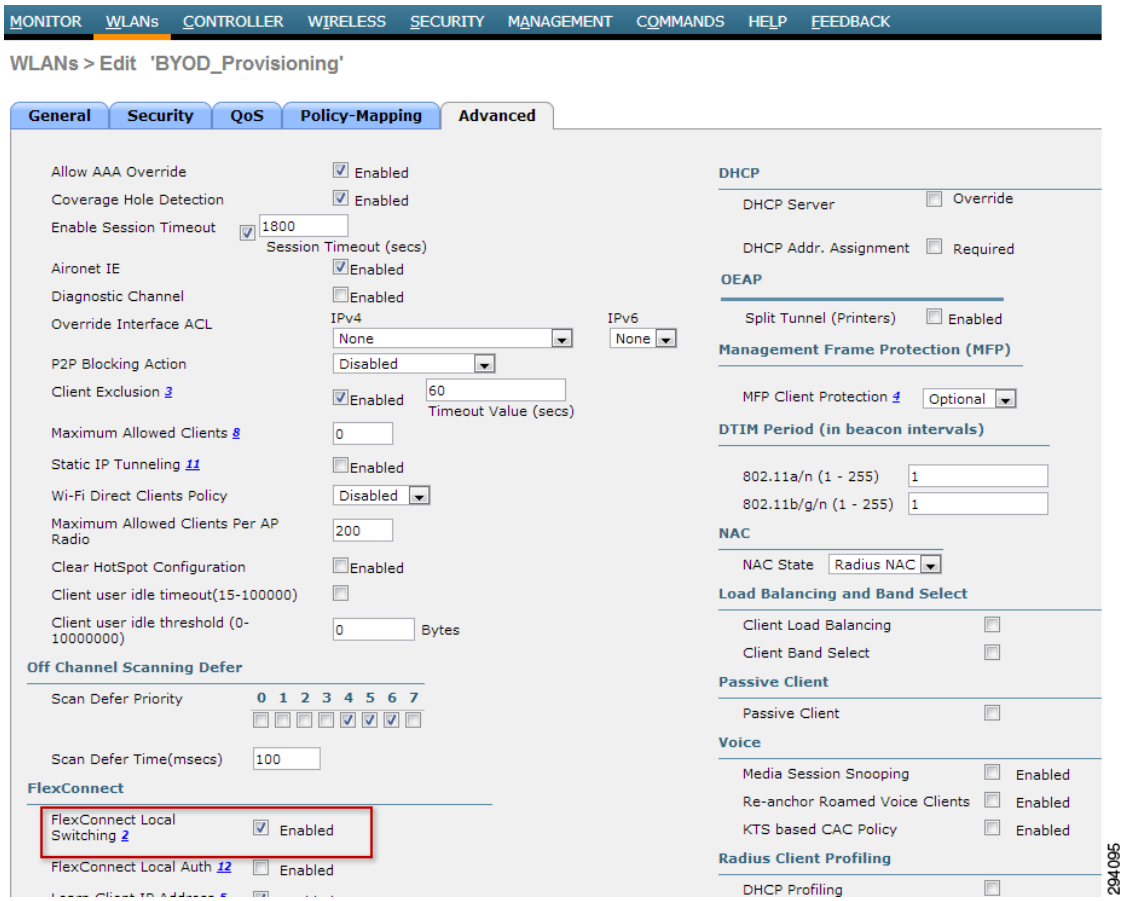


图 5-20 显示了 BYOD_Provisioning 的高级设置，包括 AAA 覆盖和 NAC 状态。对于本地交换调配， FlexConnect 本地交换处于启用状态。

图 5-20　　本地交换调配的高级设置



为了执行至自助注册门户的重定向，特定 FlexConnect 组的 Policies 选项卡下定义了一个 FlexConnect ACL，如图 5-21 中所示。

图 5-21　　FlexConnect 组的策略

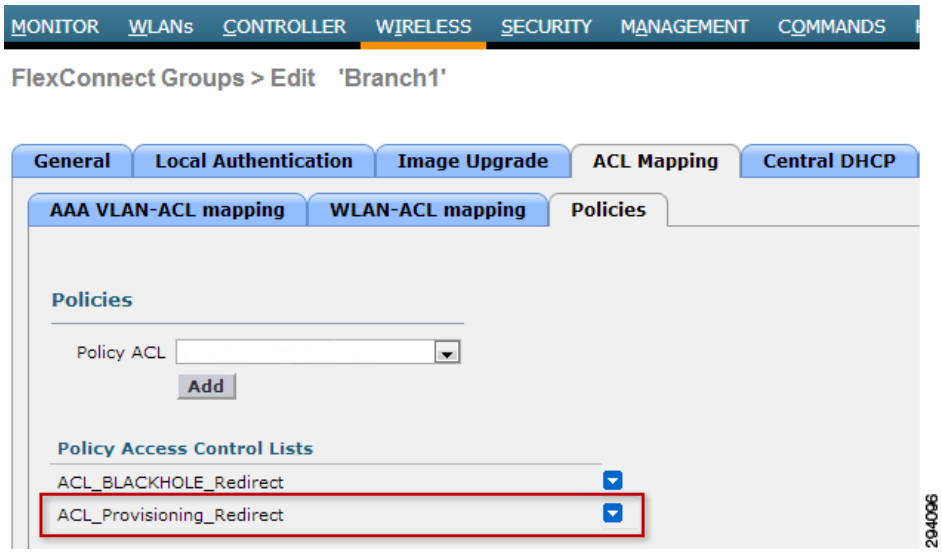
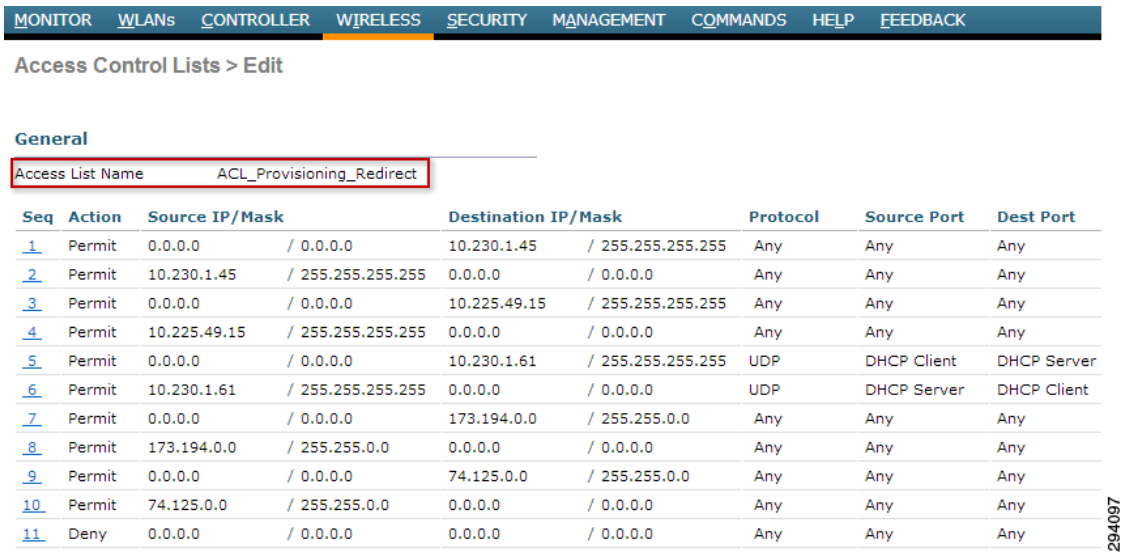


图 5-22 中所示的 ACL_Provisioning_Redirect FlexConnect ACL 允许访问 ISE、DNS 和 Google Play Store，同时拒绝所有其他流量。 Android 设备需要访问 Google Play 商店，以下载 SPW 包。

图 5-22　　ACL_Provisioning_Redirect FlexConnect ACL



Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
8	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
10	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

ACL_Provisioning_Redirect ACL 指定以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 对 Google Play 的访问。

注意　上面显示的 ACL 旨在提供网络管理员可用于在网络中部署的 ACL 的示例。Google 和 Apple App Store 的地址可能会更改，因此建议在部署 ACL 前验证这些地址的有效性。

注意　ACL_Provisioning_Redirect 必须重定向所有发送到 enroll.cisco.com 的流量。适用于 Android 设备的思科配置助手需要此重定向以发现 ISE 服务器的 IP 地址。

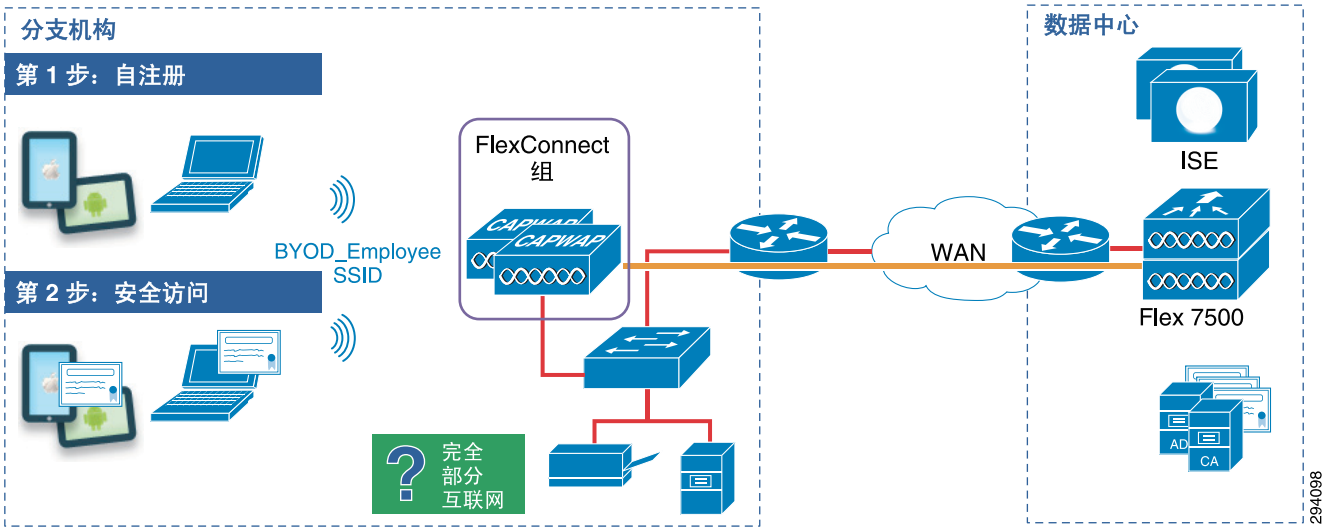
FlexConnect 分支机构 - 单 SSID 设计

在单 SSID 设计中，同一 WLAN 同时用于证书注册、调配 （自注册过程）和安全网络访问。部署单 SSID 解决方案时，应当考虑的部分注意事项有：

1. 由于身份验证方式为 PEAP，所以用户需要先输入 AD 凭证，注册过程才能开始。在 PEAP 协议中，服务器将其身份证书提供给最终用户。在本设计中， ISE 将其身份证书提供给终端。如果根证书在受信任提供商列表中不存在，某些终端可能拒绝该证书。在注册过程中，根 CA 证书会安装在终端上，但如果初始对话本身失败，则无法完成安装。因此，这会导致先有鸡还是先有蛋的问题。为了防止发生这种情况，必须由第三方信任的提供商 （如 VeriSign）签署 ISE 身份证书。
2. 如果不能满足上述要求，则最好部署双 SSID 设计。

图 5-23 显示了本设计如何使用 BYOD_Employee SSID，以及本设计如何通过 Flex 7500 控制器集群 （专用于管理分支机构中的 AP）得以实施。

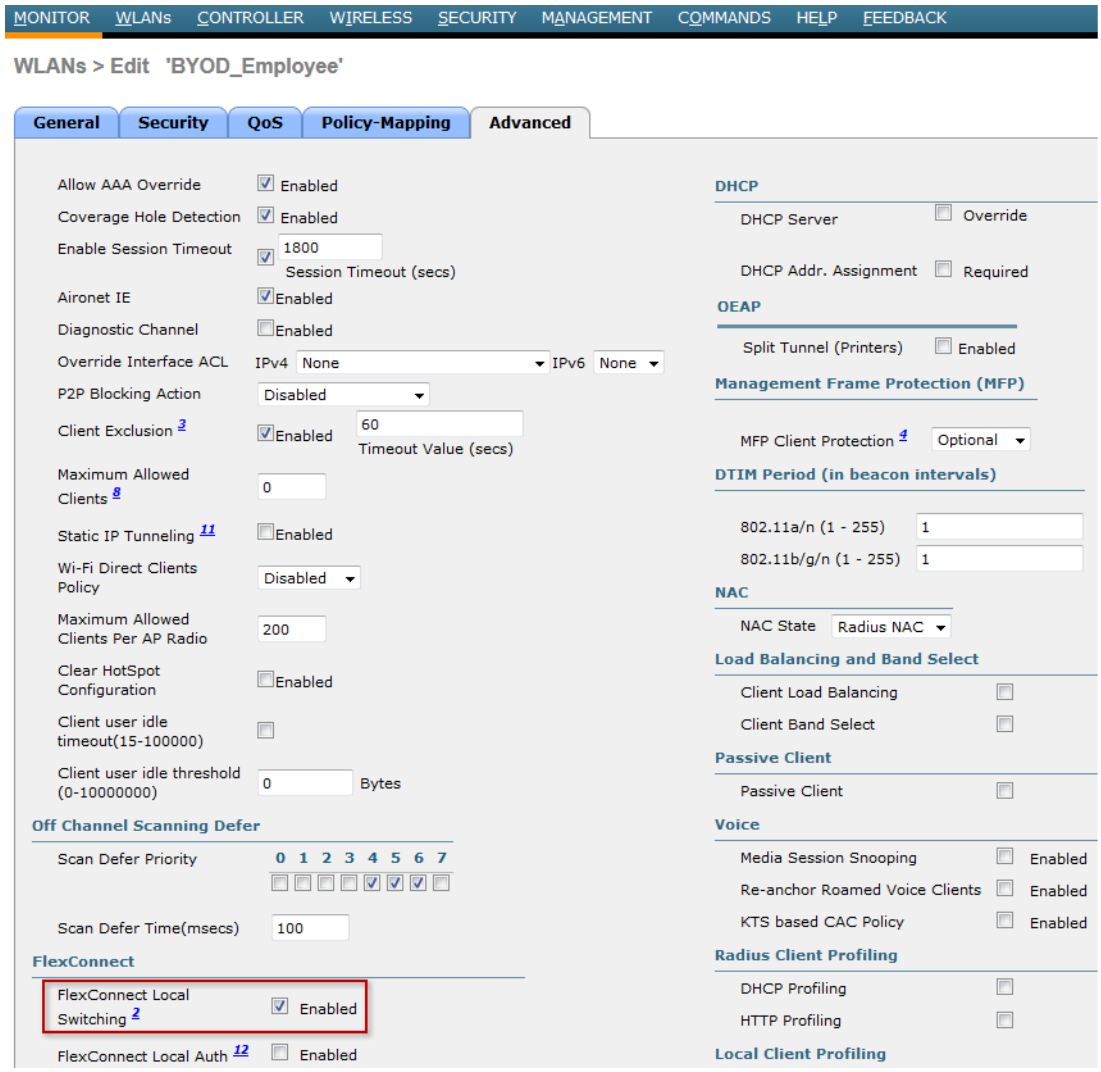
图 5-23　　分支机构 - 单 SSID



在此方案中， AP 与 Flex 7500 控制器相关联， FlexConnect 功能允许由单个 BYOD_Employee SSID 处理自注册和安全访问功能。

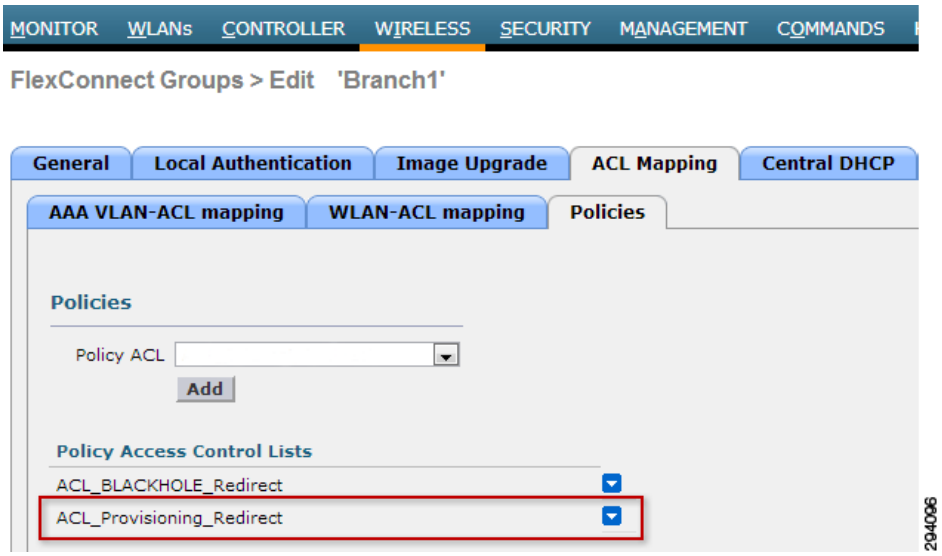
配置 BYOD_Employee WLAN 的步骤与之类似，但需要遵循表 5-3 中列出的参数。值得注意的是，在 BYOD_Employee WLAN 上启用了 FlexConnect 本地交换，如图 5-24 中的重点显示部分所示。

图 5-24　　FlexConnect 本地交换



为了执行至自助注册门户的重定向，在 Policies 选项卡下定义了一个 FlexConnect ACL，如图 5-25 中所示。

图 5-25　FlexConnect 组的策略

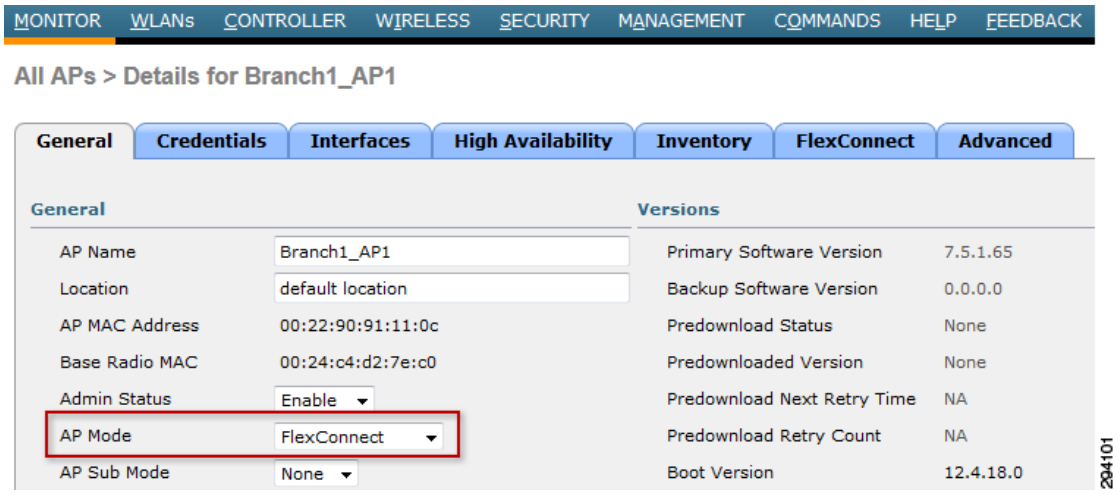


ACL_Provisioning_Redirect ACL 显示在上面的图 5-22 中。

FlexConnect 接入点配置

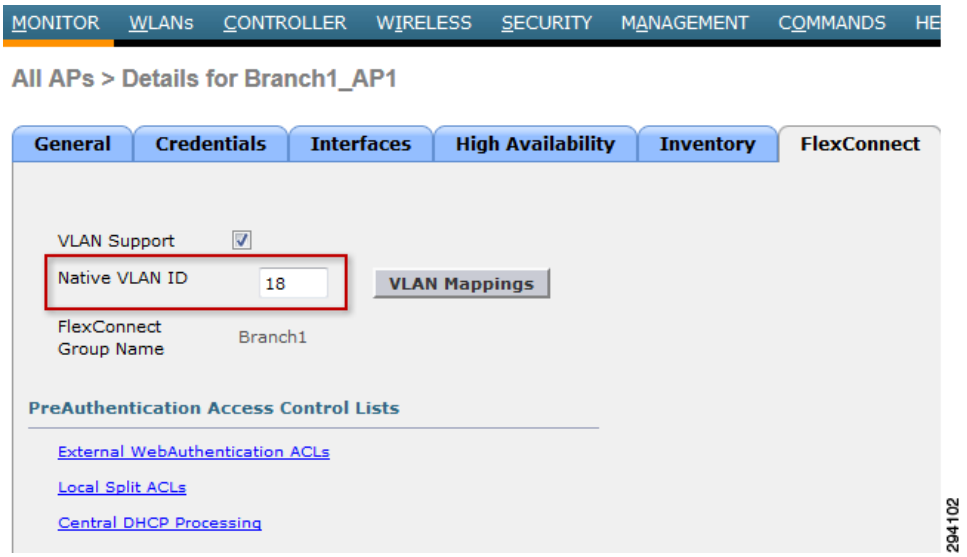
将 AP 模式更改为 FlexConnect，在 FlexConnect 模式下配置接入点。点击 **Wireless > Access Points**，然后选择适当的分支机构 AP。图 5-26 显示了 Branch1 中一个接入点的设置。

图 5-26　FlexConnect AP 模式



点击 **FlexConnect** 选项卡并为该分支机构指定本地 VLAN，如图 5-27 中所示。接入点依赖该本地 VLAN 进行 IP 连接。

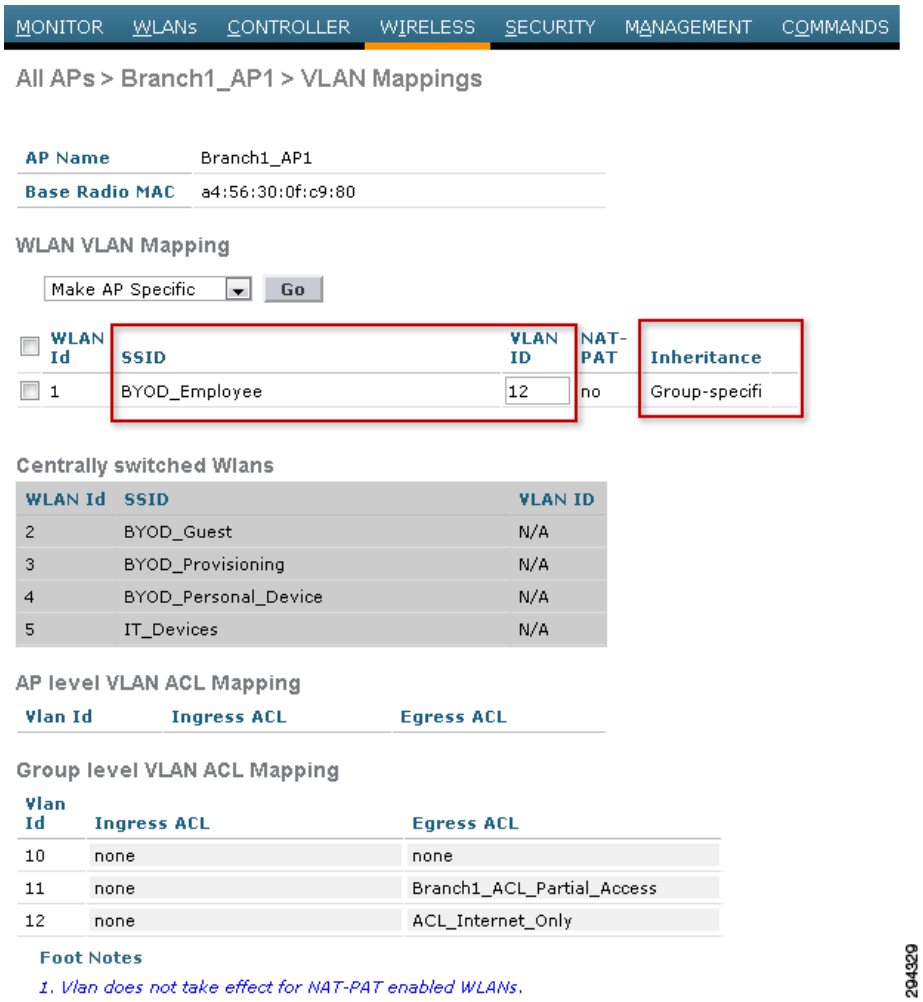
图 5-27　　本地 VLAN ID



定义要用于本地交换的 VLAN ID。在图 5-28 中，客户端在进行本地交换时从 VLAN 12（仅提供互联网访问）获取 IP 地址。当对 FlexConnect 功能使用 AAA 覆盖时，客户端会动态移动到其他 VLAN（具体取决于匹配的授权配置文件），并从定义的 VLAN 获取 IP 地址。

此配置可在 AP 级别配置，或者， AP 也可以从 FlexConnect 组继承设置。下一节将介绍 FlexConnect 组。

图 5-28　　BYOD_Employee VLAN ID



FlexConnect 组

通过 FlexConnect 组，可以方便地对共享同一配置设置的接入点进行分组。在对远程或分支机构位置的多个 FlexConnect 接入点进行分组时，此功能尤其有用。利用 FlexConnect 组，可以将配置参数一次性应用于所有接入点，而不必单独配置每个接入点。例如，只需将一个分支机构中的所有接入点添加到同一个 FlexConnect 组中，即可将 FlexConnect ACL 应用于跨所有这些接入点的一个特定 VLAN。

在本指南中，我们为每个分支机构定义了独自的 FlexConnect 组，如图 5-29 中所示。

图 5-29　　FlexConnect 组

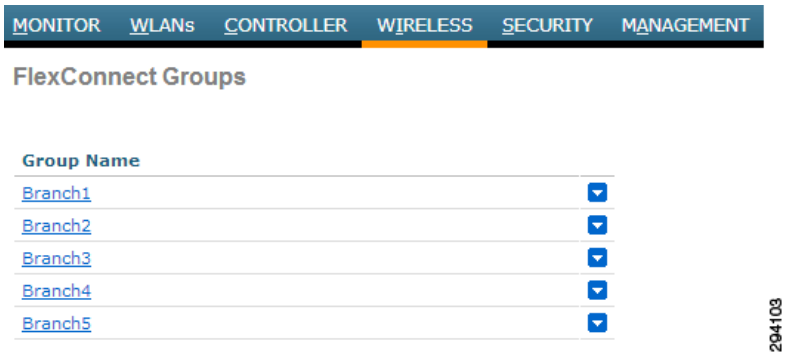
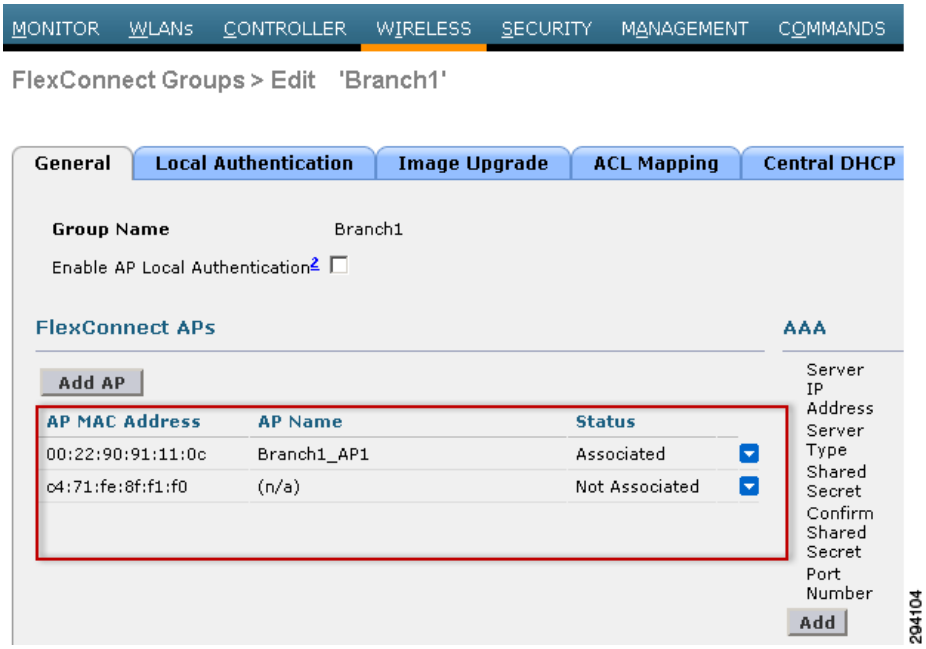


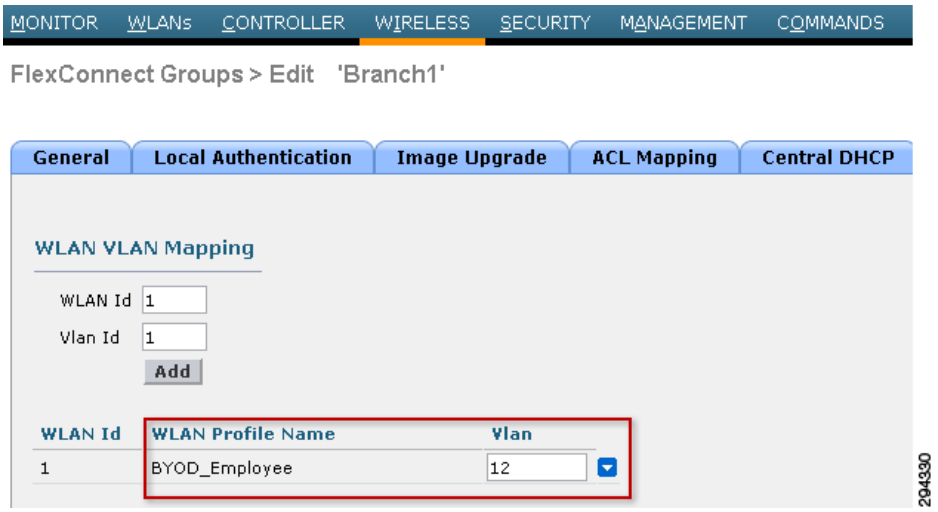
图 5-30 显示已添加到 Branch1 FlexConnect 组的接入点。

图 5-30　　Branch1 FlexConnect 组



用于本地交换的 VLAN ID 可以在 AP 级别定义，如图 5-28 中所示；也可以在 FlexConnect 组级别定义，如图 5-31 中所示。在本示例中，客户端在进行本地交换时从 VLAN 12（仅提供互联网访问）获取 IP 地址。当对 FlexConnect 功能使用 AAA 覆盖时，根据匹配的授权配置文件将客户端动态移动到一个不同的 VLAN，并且该客户端从定义的 VLAN 获取 IP 地址。

图 5-31　本地交换 VLAN - FlexConnect 组级别

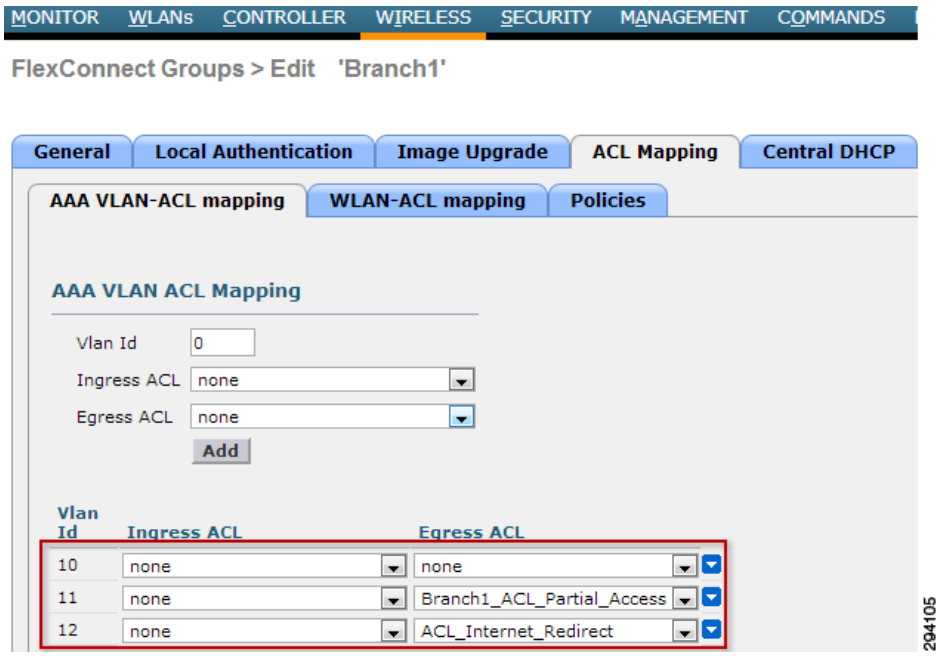


必须先对每个 VLAN 定义和分配 FlexConnect ACL， ISE 才能实施授权策略。通过点击 AAA VLAN-ACL mapping 选项卡，可以为每个 VLAN ID 实施 FlexConnect ACL。这里假设每个分支机构位置共享相同的 VLAN ID 号：

- VLAN 10 提供完全访问权限
- VLAN 11 提供部分访问权限
- VLAN 12 提供仅互联网访问权限

图 5-32 显示了不同的 FlexConnect ACL 如何映射到每个 VLAN。

图 5-32　VLAN-ACL 映射



在图 5-33 和图 5-34 中显示的 FlexConnect ACL 在第 10 章，“BYOD 增强型使用案例 - 个人和企业设备”中有更详细的说明。

图 5-33　Branch1_ACL_Partial_Access FlexConnect ACL

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name Branch1_ACL_Partial_Access

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
8	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any
10	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any
12	Permit	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any
14	Permit	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
15	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

294106

图 5-34　ACL_Internet_Only

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name ACL_Internet_Only

Deny Counters 0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
8	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
10	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
12	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

294107

FlexConnect VLAN 覆盖

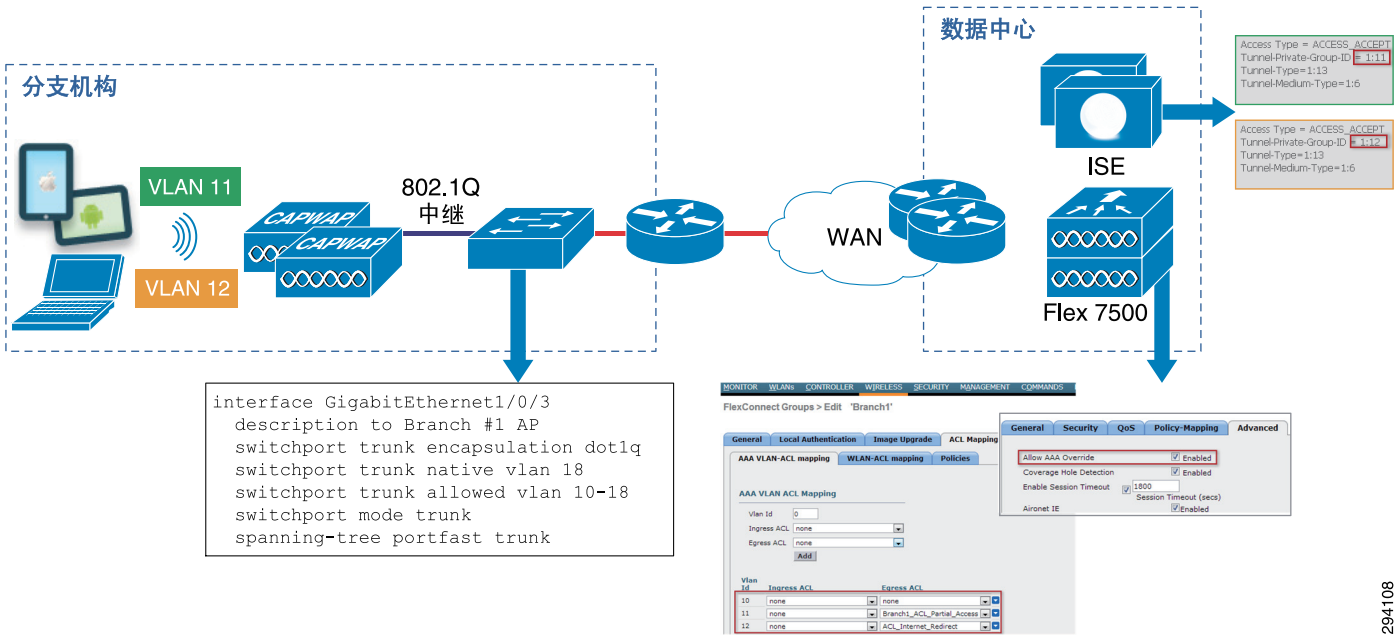
在当前 FlexConnect 架构中，WLAN 与 VLAN 之间有严格的映射，因此与 FlexConnect AP 上特定 WLAN 相关联的客户端必须符合与之有映射关系的 VLAN。此方法存在限制，因为要想继承不同的基于 VLAN 的策略，就必须将客户端关联到不同的 SSID。

WLC 从版本 7.2 开始，即支持针对本地交换配置单个 WLAN 上 VLAN 的 AAA 覆盖（动态 VLAN 分配）。要将终端动态分配到 VLAN，需要预先创建 VLAN ID，并对 FlexConnect 组中的相应 WLAN-VLAN 映射进行配置，如图 5-32 中所示。

图 5-35 显示了将终端动态分配到分支机构 VLAN 所需的不同配置设置，其中包括：

- 为本地交换模式配置的分支机构的 WLAN。
- Catalyst 交换机和接入点之间的 802.1Q 中继。
- 针对中继的本地 VLAN 和允许的 VLAN。
- ISE 授权配置文件定义了分配给终端的 VLAN。
- WLAN 在控制器上进行了配置，以允许 AAA 覆盖。
- 为 FlexConnect 组预定义了 VLAN 并定义了 VLAN-ACL 映射。

图 5-35　　FlexConnect VLAN 覆盖



园区 - 融合接入设计

融合的大型园区设计采用混合大型园区设计模式，如第 3 章，“BYOD 的园区网络和分支机构网络设计”的园区迁移路径中所述。一个混合大型园区设计包含多个 Catalyst 3850 交换机或交换机堆叠，它们部署在网络的接入层，在移动代理 (MA) 模式下运行。园区内的集中式思科 CT5760 控制器包含移动控制器 (MC) 功能。园区控制器内存在一个统一控制器 CT5508，后者与若干 CT5760 共同构成一个移动组。 AP 可以通过 Catalyst 3850 或 CT3750 交换机连接到 CT5760 或 CT5508 控制器。此外， CT5760 或 CT5508 可以用作园区互联网边缘的访客接入锚点。在本设计指南中， CT5508 被配置为访客控制器。

本设计指南假设大型园区融合接入设计符合下列条件：

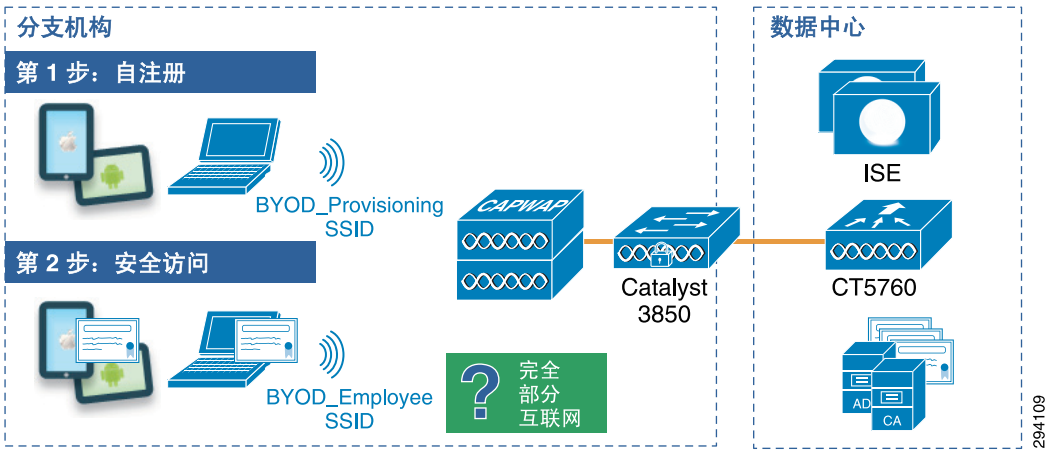
- 已注册的有线和无线设备将共享相同的 VLAN，因此也共享相同的 IP 子网寻址空间。客户可能因为问题 （例如有关无线设备的附加安全合规性要求）而对有线和无线设备实施单独的子网。本版设计指南未对此进行探讨。
- Catalyst 3850 系列交换机被部署为园区内的第 2 层接入交换机。第 3 层连接将由 Catalyst 6500 建筑分布层交换机提供。此外，为了符合园区最佳实践， VLAN 将被限制于单个配线间。换句话说， VLAN 不会扩展到各接入层交换机之间。未来的设计指南可能会解决 Catalyst 3850 系列交换机作为第 3 层交换机部署的问题，或解决 VLAN 跨多个接入层交换机扩展的问题。

园区融合接入 - 双 SSID 设计

在本设计中同样有两个 SSID：一个提供注册 / 调配，另一个提供安全网络访问。在连接到 BYOD_Provisioning SSID 并完成注册和调配步骤后，用户连接到 BYOD_Employee SSID，该 SSID 通过安全 EAP-TLS 连接提供网络访问。

图 5-36 显示了适用于园区 AP 的双 SSID 设计。

图 5-36　　园区 - 双 SSID



在融合接入双 SSID 设计中，有一些其他考虑事项：

- 调配 SSID 可以是开放形式，也可以采用密码保护形式。如果调配 SSID 是开放形式，则任何用户都可以连接到该 SSID ；但如果它有密码保护，则仅允许具有凭证 （如 AD 组成员身份）的用户连接到该 SSID。本设计指南中配置的调配 SSID 是开放形式，其唯一目的是提供自注册服务。

- 在调配设备后，假设用户将切换到第二个 SSID 以进行常规网络访问。为了防止用户一直与调配 SSID 保持连接，必须对调配 SSID 实施一个访问列表，该列表仅提供对 ISE、 DHCP 和 DNS 的访问。 ACL_Provisioning_Redirect ACL 的详细信息如下所示。
- 本设计指南使用以下 SSID：BYOD_Provisioning 和 BYOD_Employee。

在表 5-4 中重点介绍了这两个 SSID 的属性。

表 5-4　　WLAN 参数

属性	BYOD_Provisioning	BYOD_Employee
说明	仅用于设备调配	用于已完成自注册过程的员工
第 2 层安全	无 （对于开放式 SSID）	WPA+WPA2
MAC 过滤	已启用 （对于开放式 SSID）	已禁用
WPA+WPA2 参数	无	WPA2 策略、 AES、 802.1X
第 3 层安全	无	无
AAA 服务器	选择 ISE	选择 ISE
高级	AAA 覆盖已启用	AAA 覆盖已启用
高级	NAC 状态 - NAC	NAC 状态 - NAC

要在 CT5760 和 Catalyst 3850 上配置 WLAN BYOD_Provisioning SSID，请按以下步骤操作。BYOD_Provisioning SSID 上的安全性为 “NONE”，因为这是用来在网络上调配设备的调配 SSID。通过 FAST-SSID 功能，客户端可以在 ISE 正确调配 BYOD_Provisioning 后从该 SSID 切换到 BYOD_Employee SSID。

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
```

```
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD-Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

园区设计中的 Catalyst 3850 （充当移动代理 (MA)）和 CT5760 （充当移动控制器 (MC)）上都必须配置以上所示的示例。但请注意， VLAN 接口的 IP 寻址对于 MA 和 MC 来说是不同的，因为 MA 和 MC 部署在网络基础设施的不同部分。移动性作为本章中的单独主题在讨论 WLAN 配置之后进行说明。其他配置行必须添加到 MA 和 MC 来分别实现移动性。稍后将讨论这些内容。

BYOD_Provisioning SSID 没有第 2 层安全，因为这是用来在网络上调配设备的 SSID。相反，无线客户端使用 MAC 过滤（基本上是 MAB 的无线版本）向网络进行身份验证。在连接到网络时，URL 重定向和集中 Web 身份验证 (CWA) 策略从 ISE 下推到客户端。因此，在 BYOD_Provisioning SSID 上要求配置 MAC 过滤、 NAC 和 AAA 覆盖。

BYOD_Employee SSID 上的安全性采用 WPA2 和 AES 加密。请注意，这是融合接入平台（CT5760 或 Catalyst 3850）上 WLAN 的默认设置，因此并不显示在配置中。此 SSID 上要求配置 NAC 和 AAA 覆盖以支持将动态 ACL 分配给无线客户端。在本设计指南中，动态 ACL 是在 Catalyst 3850 交换机上本地配置的命名 ACL。

注意　管理级别命令 **show wlan name <*wlan 的名称*>** 可用于显示有关 Catalyst 3850 系列交换机或 CT5760 无线控制器上任何 WLAN 的配置的详细信息。其中包括不显示在配置中的任何默认设置。

即使在通过 BYOD_Provisioning SSID 进行自注册期间从 ISE 向无线客户端推送了 CWA 策略，仍必须在 Catalyst 3850 系列交换机上全局启用 HTTP 和 HTTPS 服务器功能。这是为了支持 Web 会话的 URL 从无线客户端重定向到 ISE 调配门户。RADIUS 服务器组配置重新指向 ISE，将其作为无线 （和有线）客户端身份验证和授权的 RADIUS 服务器。必须在 Catalyst 3850 系列交换机上全局启用强制网络门户旁路功能， Apple 设备才能成功地自注册。通过 fast-ssid-change 全局配置，客户端可以在 ISE 正确调配 BYOD_Provisioning 后从该 SSID 切换到 BYOD_Employee SSID。

对于充当 MC 的 CT5760 和充当 MA 的 Catalyst 3850 来说，无线移动配置命令是不同的。以下是一段 CT5760 无线控制器的全局移动配置代码示例。

```
!
interface Vlan47
 description MGMT VLAN
 ip address 10.225.47.2 255.255.255.0
 load-interval 30
!
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/Points to CT5508
wireless mobility group name byod
wireless management interface Vlan47
wireless rf-network byod
!
```

可以看到， CT5760 被配置为两个交换机对等组 (SPG) 的移动控制器 (MC)，在上述示例中这两个交换机对等组为 100 和 200。交换机对等组 100 包含一个充当 MA 的 Catalyst 3850 交换机。交换机对等组 200 包含两个充当 MA 的 Catalyst 3850 交换机。以下是一段 Catalyst 3850 无线控制器的全局移动配置代码示例。

```
interface Vlan47
 description MGMT VLAN
 ip address 10.225.61.5 255.255.255.0
 load-interval 30
!

wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / 5760 MC 的 IP 地址
```

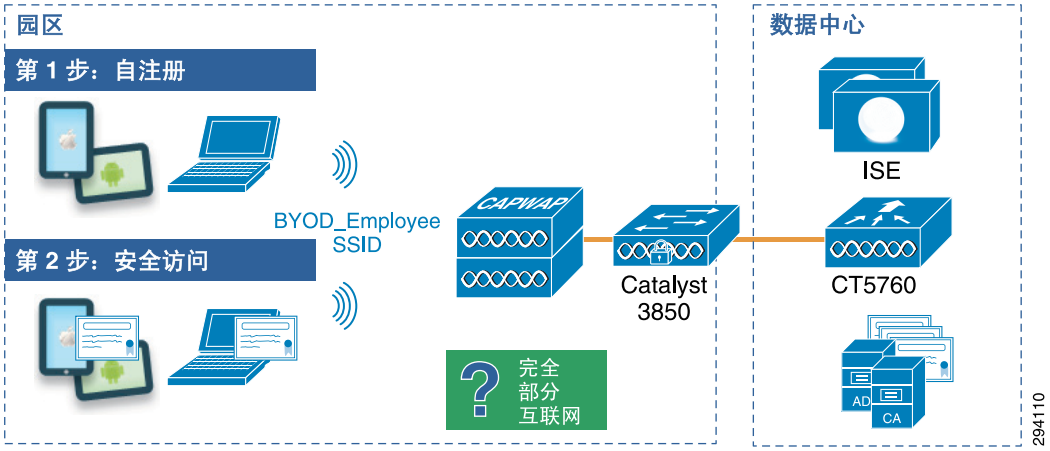
上述配置中所示的 Catalyst 3850 系列交换机的无线管理接口的相应 IP 地址是作为 SPG 200 的成员出现的。SPG 旨在扩展融合接入设计中的移动性。单个 SPG 内各 Catalyst 3850 系列交换机移动代理 (MA) 之间的漫游由交换机直接处理，而不涉及 CT5760 移动控制器 (MC)。这通过单个 SPG 内各 Catalyst 3850 系列交换机移动代理 (MA) 之间的全网状 CAPWAP 隧道来完成。两个 SPG 之间的各 Catalyst 3850 系列交换机移动代理 (MA) 之间的漫游由 CT5760 移动控制器 (MC) 处理。这通过每个 Catalyst 3850 系列交换机移动代理 (MA) 和 CT5760 移动控制器 (MC) 之间的 CAPWAP 隧道来完成。

如前所述，混合园区设计可能包括在本地模式下运行的 CT5508 无线控制器，以及融合接入基础设施。在从集中式无线重叠模式迁移到融合接入部署模式期间，这可能是必需的。为了支持在 CT5508 无线控制器和 CT5760 无线控制器之间的移动性，CT5508 无线控制器的 IP 地址作为无线移动组成员被添加到如上所示的 CT5760 的配置。

园区融合接入 - 单 SSID 设计

在单 SSID 设计中，自注册和安全网络访问使用的是同一 WLAN (BYOD_Employee)。图 5-37 显示了如何将 CT5760 用作 MC 并将 Catalyst 3850 用作 MA 来实施本设计。

图 5-37　　园区 - 单 SSID



单 SSID 融合园区设计的配置与双 SSID 设计几乎完全相同，只是前者无需使用 BYOD_Provisioning SSID。 CT5760 和 Catalyst 3850 上的配置代码片段如下所示。移动性将作为单独主题在讨论 WLAN 配置之后进行说明。

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
```

```
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
```

MC 和 MA 的移动配置都与前面所述的双 SSID 融合接入设计中相同。

园区融合接入 - 移动性

对于大型园区设计，了解移动性和漫游考虑事项很重要。

本设计的重点是在一个大型园区的接入层部署多个 Catalyst 3850 系列交换机或交换机堆叠。交换机堆叠构成交换机对等组 (SPG)，其中的所有交换机都包含移动代理 (MA) 功能。 SPG 内的漫游是通过 SPG 内各 MA 之间的全网状移动隧道处理的。大型园区内存在多个 SPG。 AP 必须直接连接到 MA，而不能通过中间交换机 （如 Catalyst 3750 交换机）来连接。

在园区中的集中式服务模块内部署的思科 CT5760 无线控制器包含移动控制器 (MC) 功能。连接到单个 MC 的多个 SPG 构成一个移动子域。大型园区内存在多个移动子域。移动子域内各 SPG 之间的漫游是通过思科 CT5760 和 / 或 CT5508 无线控制器来完成的。连接到 Catalyst 3850 交换机的各 AP 向 CT5760 MC 注册。 AP 还可以通过 Catalyst 3750 交换机连接到 CT5760。

多个 Cisco CT5760 和 / 或 CT5508 无线控制器构成一个移动组。因此，一个移动组也包括多个移动子域。各移动子域之间的漫游是通过移动组内的思科 CT5760 和 / 或 CT5508 无线控制器来完成的。在本设计中，单个移动组以及由此形成的单个移动域覆盖且完全包含在整个大型园区范围内。

对于同时包含 CUWN 本地模式和融合接入产品的混合模式，思科 CT5760 或 CT5508 还充当使用传统本地模式 （中央交换）无线连接来连接到 Catalyst 3750-X 系列交换机的接入点的无线控制器。

谨记以上考虑事项，其他的不用考虑太多。

默认情况下， Catalyst 3850 作为移动代理运行，且无需任何配置。 Catalyst 3850 还可以作为移动控制器运行。此模式是分支机构设计的一部分。

CT5760 无线控制器仅作为移动控制器运行。移动隧道应该设置在 CT5760 和 Catalyst 3850 之间，以便 Catalyst 3850 上连接的 AP 能够注册到 MC (CT5760)。 MC 的配置代码片段如下：

```
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
```

在每个充当 MA 的 Catalyst 3850 上，都需要下面的配置来建立与 CT5760 MC 或 5508 MC 的移动隧道。

```
wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / MC 的 IP 地址
```

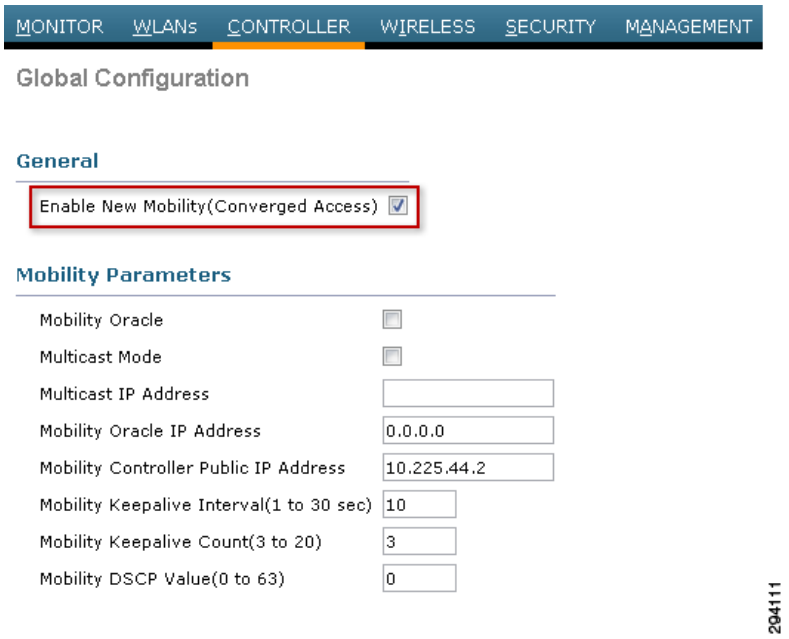
CT5508 和 CT5760 也可以构成一个移动组。CT5508 应该升级到 WLC 7.3.112 或 7.5 以上的版本，以支持融合接入和统一接入产品之间的移动性。CT5508 上支持 CT5760 和 CT5508 之间移动性的配置如下所示。本设计指南提供的指导适用于 CT5508 7.5 版。

```
wireless mobility controller/ 启用 MC 功能，默认在 CT5760 上已打开
wireless mobility group name byod/ 创建移动组 byod
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/ CT5508 的 IP 地址
```

注意　仅 WLC 版本 7.3.112 或 7.5 及更高版本支持融合接入产品和统一接入产品之间的移动性。请确保您拥有运行兼容代码的代码版本。本设计指南使用的是 7.5 版本。

为了支持融合接入和统一接入产品之间的移动性，应首先在 WLC 上启用新移动性，如图 5-38 中所示。

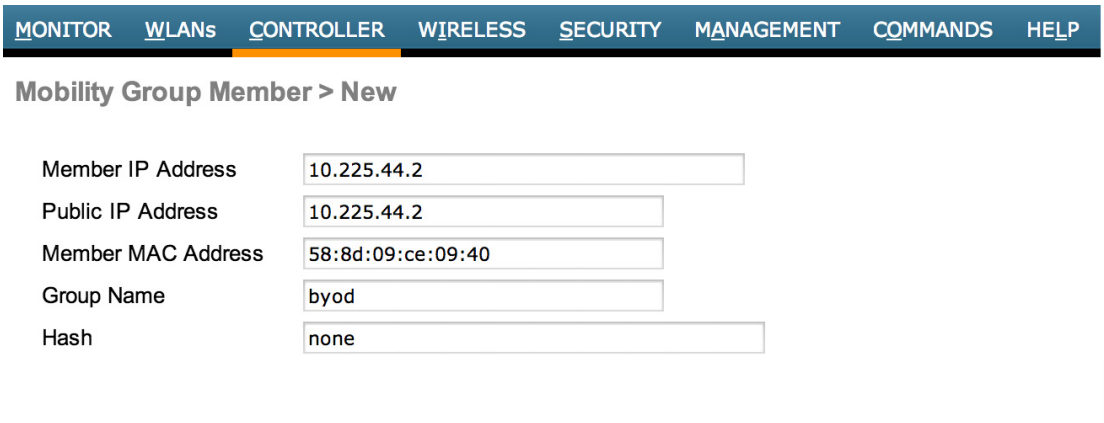
图 5-38　　启用新移动性



在启用新移动性并重新启动无线 LAN 控制器后，用于配置交换机对等组以及移动组的其他选项将被启用。要使 CT5760 和 CT5508 构成一个组并相互通信，需要进行如下的额外配置。

点击 **Mobility Management > Mobility Groups** 并点击 **New**，如图 5-39 中所示。

图 5-39　　创建新移动性组



以上成员 IP 地址应该是 CT5760 的 IP 地址，该地址支持移动消息传送及要在 CT5760 和 CT5508 之间建立的 CAPWAP 隧道。

部署大型园区 WLAN 基础设施时的其他设计考虑事项包括以下两个：

- 所有 Catalyst 3850 和 CT5760 上的 802.1X、 WLAN 和 VLAN 配置应相同。
- CT5760 和 CT5508 上的移动组名称应该相同。

分支机构 - 融合接入设计

采用融合接入设计时，可由同时充当移动代理 (MA) 和移动控制器 (MC) 的 Catalyst 3850 交换机来取代集中式 FlexConnect 无线控制器。访客无线接入仍使用相同的模式，其中访客流量自动锚定到位于园区互联网边缘内的专用访客锚点控制器。访客控制器既可以是采用 7.5 版本代码的 CT5508 控制器，也可以是 CT5760 融合无线 LAN 控制器。

集成控制器分支机构自带设备设计指南基于以下假设：

- 因此，入网有线设备和无线设备将共享相同的 VLAN 以及相同的 IP 子网寻址空间。对无线和有线客户端可以使用不同的 VLAN 和寻址空间，但本设计指南未对此进行讨论。
- Catalyst 3850 交换机部署为分支机构位置内的第 2 层交换机。分支机构内的第 3 层连接由 ISR 路由器提供，这些路由器也用作分支机构的 WAN 连接点。（未来的设计指南可能会讨论将 Catalyst 3850 部署为分支机构位置内第 3 层交换机的情形。）

分支机构融合接入 - 双 SSID 设计

在双 SSID 设计中，将为自注册设备配置具有 MAC 过滤功能（如 MAC 身份验证旁路）的专用开放式 SSID (BYOD_Provisioning)。该 SSID 将被静态映射到 Catalyst 3850 交换机上一个单独的调配 VLAN。图 5-40 显示了双 SSID 设计的分支机构融合接入。

图 5-40　　分支机构融合接入 - 双 SSID

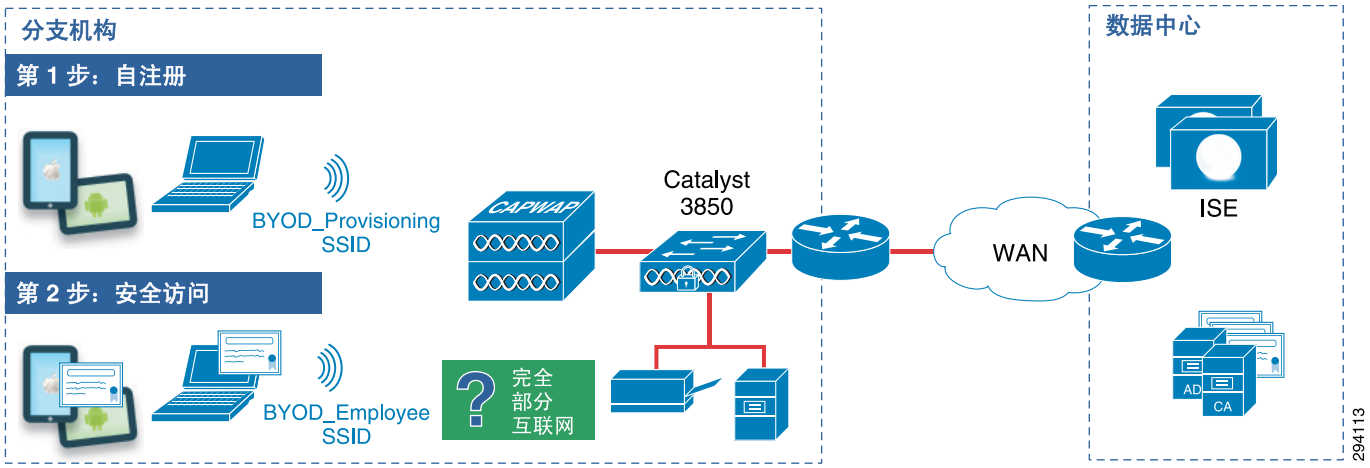


表 5-5 提供了使用双 SSID 自带设备自注册设计时分支机构内各 VLAN 的摘要。

表 5-5　　采用双 SSID 自带设备自注册设计时分支机构中的 VLAN

说明	VLAN	VLAN 名称
有线和无线企业接入。由 IT 管理的设备。具有完全、部分访问权限或仅具有互联网访问权限的由员工管理的设备。	12	BYOD_Employee
双 SSID 无线自注册的调配 VLAN。	13	BYOD_Provisioning
分支机构服务器的单独 VLAN。	16	Server
用于网络基础设施管理的专用 VLAN。	18	Management
用于穿越无线自动锚点隧道的隔离 VLAN。不中继到第 3 层路由器。	777	BYOD_Guest

以下配置代码片段提供了 Catalyst 3850 额外配置的一个示例，该额外配置用于支持使用 MAC 过滤的双 SSID 自带设备实施中无线设备的自注册。

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!

qos wireless-default-untrust
vtp domain bn
!
mac access-list extended MAC_ALLOW
 permit any any
```

```
!
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD_Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
!
```

以下配置代码片段是分支路由器配置的额外配置的部分示例，用于支持使用 MAC 过滤的双 SSID 自带设备实施中无线设备的自注册 （当 Catalyst 3850 系列交换机充当第 2 层交换机时）。

```
!
interface GigabitEthernet0/0
 description CONNECTION TO CATALYST 3850 SWITCH
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.13/ 调配 VLAN
 description CATALYST 3850 PROVISIONING VLAN
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61/ 将 DHCP 中继到 DHCP 服务器
 ip helper-address 10.225.42.15/ 将 DHCP 中继到 ISE 进行分析
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
```

分支机构融合接入 - 单 SSID 设计

在单 SSID 设计中，企业 SSID (BYOD_Employee) 通过非自注册设备的 PEAP 支持身份验证。在自注册完成后，企业 SSID 通过自注册设备的 EAP-TLS 支持身份验证。该企业 SSID 被静态映射到 Catalyst 3850 交换机上一个单独的企业 VLAN。图 5-41 显示了单 SSID 设计的分支机构融合接入。

图 5-41　　分支机构融合接入 - 单 SSID

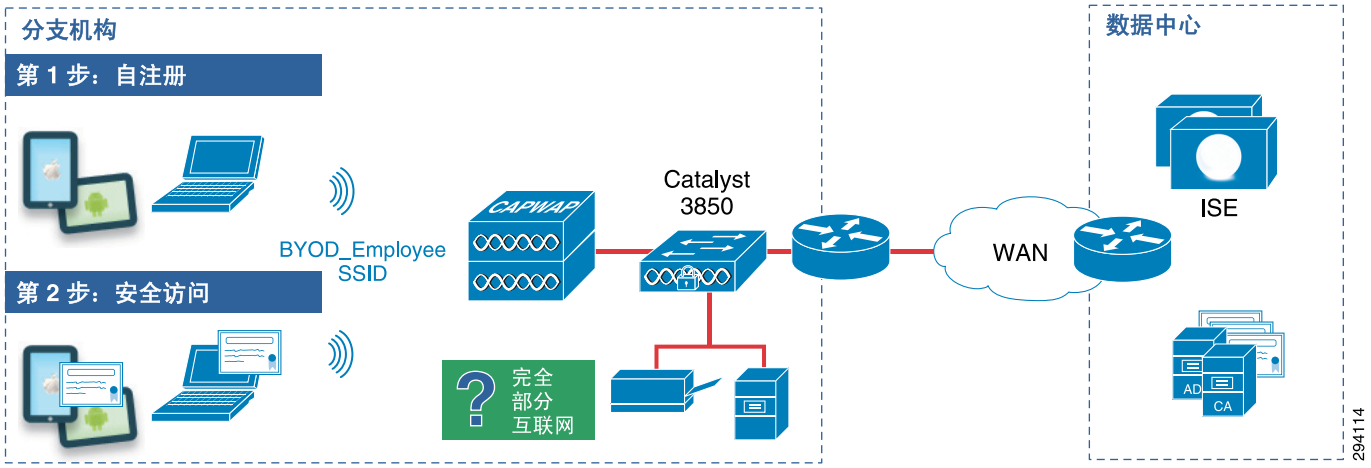


表 5-6 提供了使用单 SSID 自带设备自注册设计时分支机构内各 VLAN 的摘要。

表 5-6　　采用单 SSID 自带设备自注册设计时分支机构中的 VLAN

说明	VLAN	VLAN 名称
有线和无线企业接入。由 IT 管理的设备。具有完全、部分访问权限或仅具有互联网访问权限的由员工管理的设备。	12	BYOD_Employee
分支机构服务器的单独 VLAN。	16	Server
用于网络基础设施管理的专用 VLAN。	18	Management
用于穿越无线自动锚点隧道的隔离 VLAN。不中继到第 3 层路由器。	777	BYOD_Guest

以下配置显示了使用单 SSID 自注册模式时 Catalyst 3850 的部分相关配置。

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!
```

```
!
qos wireless-default-untrust
!
mac access-list extended MAC_ALLOW
 permit any any
!
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
!
?
```

面向 BYOD 的身份服务引擎

修订日期：2013 年 8 月 7 日

思科身份服务引擎 (ISE) 允许在整个有线和无线网络中实施集中配置策略，以帮助组织提供安全的统一接入。在 BYOD 模式中员工可以将个人设备安全地连接到网络，而 Cisco ISE 在此模式的实现过程中扮演着重要的角色。通过与第三方移动设备管理器 (MDM) 集成，还有更多设备状态可用于执行连接网络的权限。

Cisco ISE 提供了支持独立和分布式部署且高度可扩展的架构。本文所示的配置指南反映了带有多个节点的分布式架构。

对于小型 BYOD 部署，独立模式下可能会配置一个或两个 ISE 节点。根据 AAA 连接在接入层交换机和无线局域网控制器之间的配置方式，可以在冗余独立 ISE 节点间启用 AAA 工作流的活动 / 备份或负荷均衡。

对于较大型的 BYOD 部署，ISE 功能可以分布在多个节点上。分布式部署支持以下不同 ISE 角色：

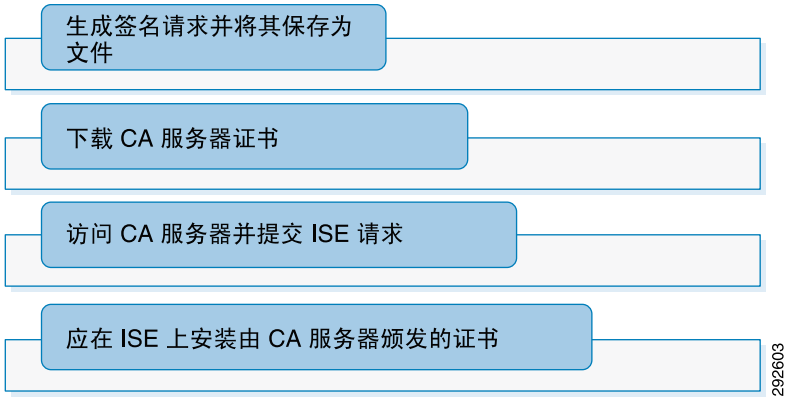
- 管理 - 管理节点处理所有系统级配置。在分布式部署中，可以有一个主要管理节点和一个次要管理节点。
- 监控 - 监控节点处理日志收集并提供监控和故障排除工具。在分布式部署中，可能有一个主要监控节点和一个次要监控节点。
- 策略服务 - 策略服务节点提供身份验证、授权、访客访问、客户端推送和分析服务。在分布式部署中，可能有多个策略服务节点。

若要对中型 BYOD 部署提供支持，可以在单个节点上部署管理和监控角色，而利用专用策略服务节点来处理 AAA 功能。对于大型 BYOD 部署，监控角色可以在提供集中日志记录功能的专用节点上实施。

ISE 的身份证书

ISE 需要由 CA 服务器签署的身份证书，才能获得终端、网关和服务器的信任。图 6-1 从较高层面说明了相关步骤。

图 6-1　　在 ISE 上部署身份证书的较高层面步骤



有关在 Cisco ISE 上安装数字证书的详细信息，请参阅 TrustSec 方法指南：http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf。

ISE 中的网络设备定义

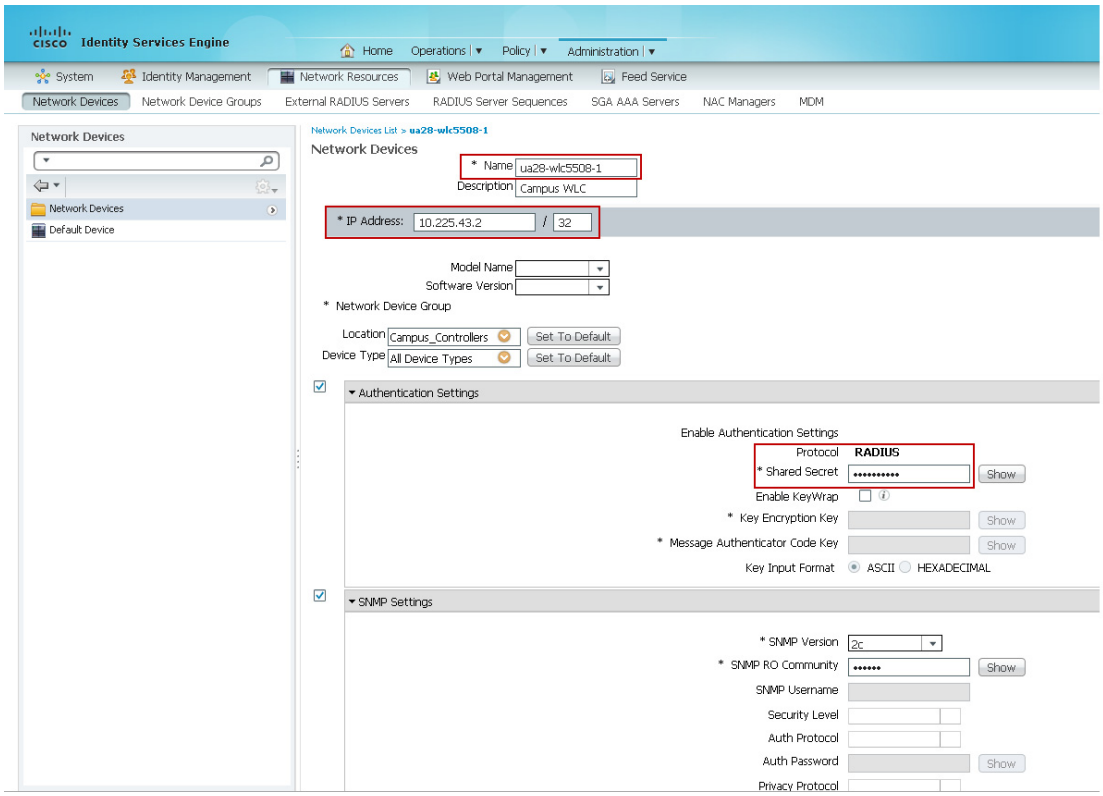
网络设备是用于尝试身份验证、授权和记帐 (AAA) 服务请求的 AAA 客户端，例如交换机、路由器等。网络设备定义支持思科身份服务引擎 (Cisco ISE) 与配置的网络设备进行交互。未定义的网络设备则无法接收来自 Cisco ISE 的 AAA 服务。

当用户 / 设备连接到网络基础设施 （例如为 802.1X 身份验证启用的无线控制器和交换机）时，网络设备充当客户端 Supplicant 客户端的 802.1X 身份验证器。为了让网络设备确定是否要授予访问权限，以及要为设备授权哪些服务，网络设备必须能够与作为验证服务器的 ISE 通信。若要实现此通信，必须使用有关该网络设备的信息以及用于对其进行验证的凭证配置 ISE。

若要使用此信息配置 ISE，请参阅图 6-2 和以下信息：

1. 在 ISE 中，转至 **Administration > Network Resources > Network Devices**，然后点击 **Add**。
2. 输入设备的主机名。
3. 输入网络设备的 IP 地址。这必须是用于从设备发送所有 Radius 通信的地址。
4. 如果之前已经自定义了网络设备位置或设备类型，请更改此位置或类型。
5. 配置 Radius 共享密码。必须与在网络设备上为 ISE 服务器配置的密码匹配。
6. 点击 SNMP Settings 旁的向下箭头并根据需要填写。

图 6-2　　ISE 中的网络设备配置

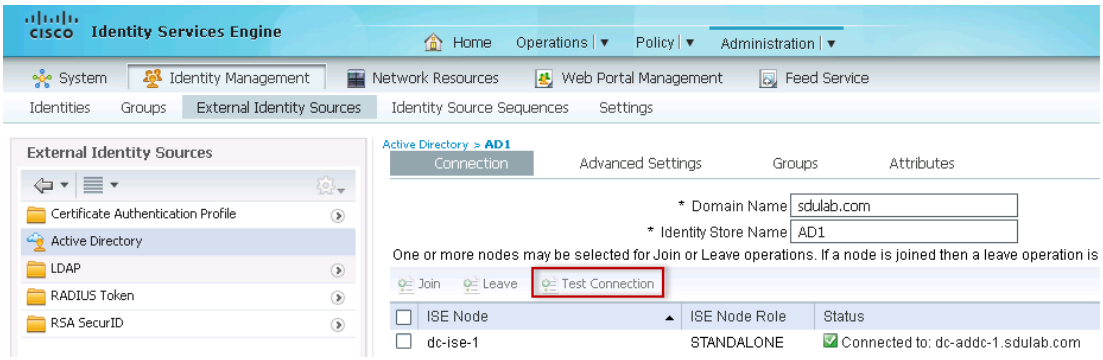


ISE 与 Active Directory 集成

虽然 ISE 可以出于身份验证目的维护内部用户列表，但大多数组织都依赖外部目录作为主要身份源。通过与 Microsoft Active Directory 集成，用户和组等对象在授权过程中变得至关重要，并且可以从单一来源访问。

若要与 Active Directory 集成，在 ISE 中，点击 **Administration > External Identity Sources > Active Directory** 并指定域名，如图 6-3 所示。若要验证 ISE 节点是否可以连接到 Active Directory 域，请点击 **Test Connection** 并使用 AD 用户名和密码进行身份验证，如图 6-3 所示。点击 **Join** 将 ISE 节点加入到 Active Directory。

图 6-3　　Active Directory 集成



注意　思科身份服务引擎用户指南提供了详细配置步骤：http://www.cisco.com/en/US/customer/docs/security/ise/1.2/user_guide/ise_user_guide.html。

访客和自助注册门户

Cisco ISE 服务器能够托管多个门户。BYOD 系统设计依靠访客门户提供无线访客接入，并且，出于调配目的，依靠将员工重定向到自助注册门户来进行设备自注册。第 13 章，“BYOD 访客无线接入”讨论了如何使用访客门户进行访客无线接入。默认 ISE 门户拥有标准思科品牌设计，可出于不同目的、按照单个策略进行自定义，以标识出独特的门户。

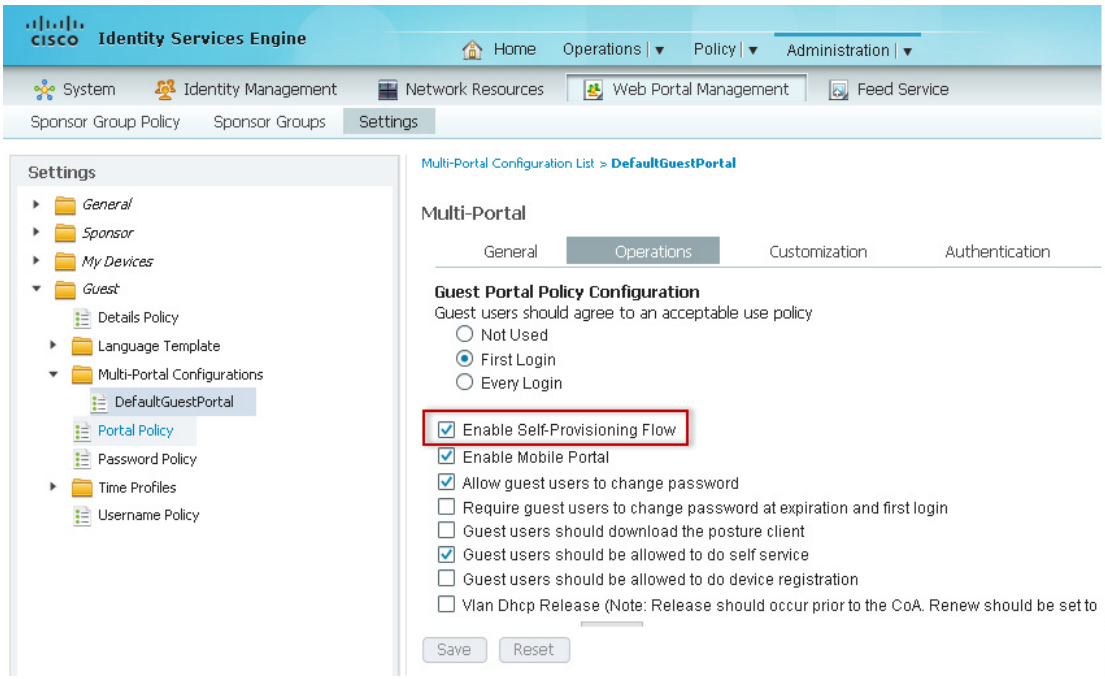
ISE 支持自助调配，允许员工注册自己的个人设备。在设备注册过程中， ISE 将使用其本地 Supplicant 客户端推送设备。

员工首次使用自己的个人设备进行工作和注册时， BYOD 系统会引导他们执行以下调配步骤：

1. 员工将设备连接到开放 SSID （两个 SSID 均为 BYOD_Provisioning SSID）。
2. 设备重定向至访客注册门户。
3. 员工输入凭证，而 ISE 针对 Active Directory 进行身份验证。
4. 如果设备尚未在网络中注册，会话将重定向到自助注册门户。
5. 系统会要求员工输入唯一的设备说明并完成设备注册。

要启用自助调配，请按照如下步骤配置这些门户：点击 **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**，如图 6-4 所示。

图 6-4　　门户设置 - Operations

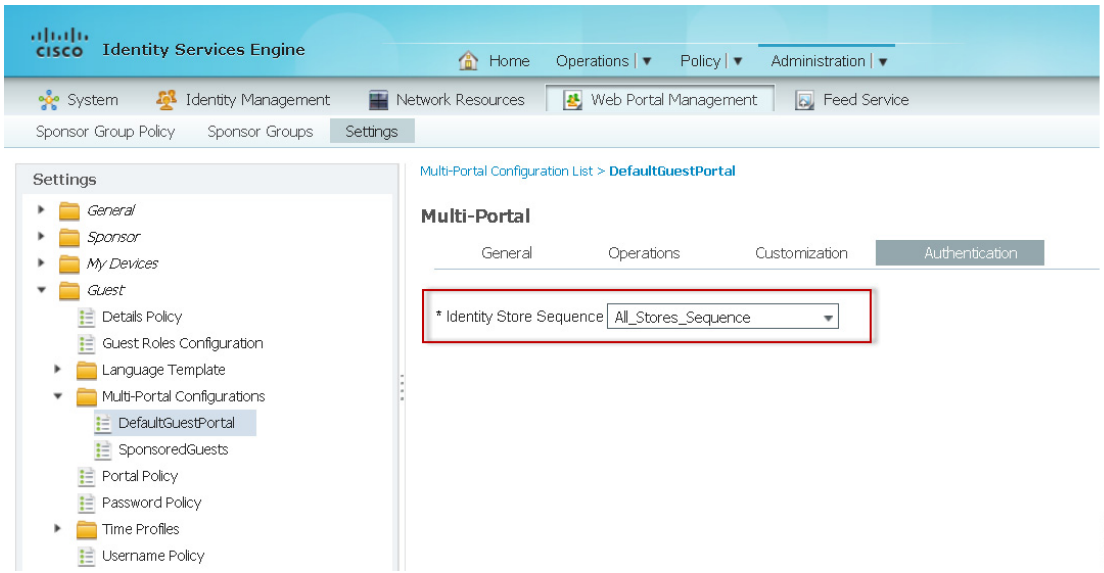


DefaultGuestPortal 是指用于自助注册的门户，或者在本文中称为自助注册门户。

若要指定门户对用户进行身份验证的方式，请选择特定门户中的 Authentication 选项卡，如图 6-5 所示，然后选择相应的选项：

- Guest - 门户验证存储在本地数据库中的访客用户帐户。
- Central WebAuth - 根据身份库序列中指定的数据库验证用户。
- Both - 首先根据本地访客数据库验证用户。如果未找到用户，则使用身份库序列中定义的其他数据库尝试身份验证。

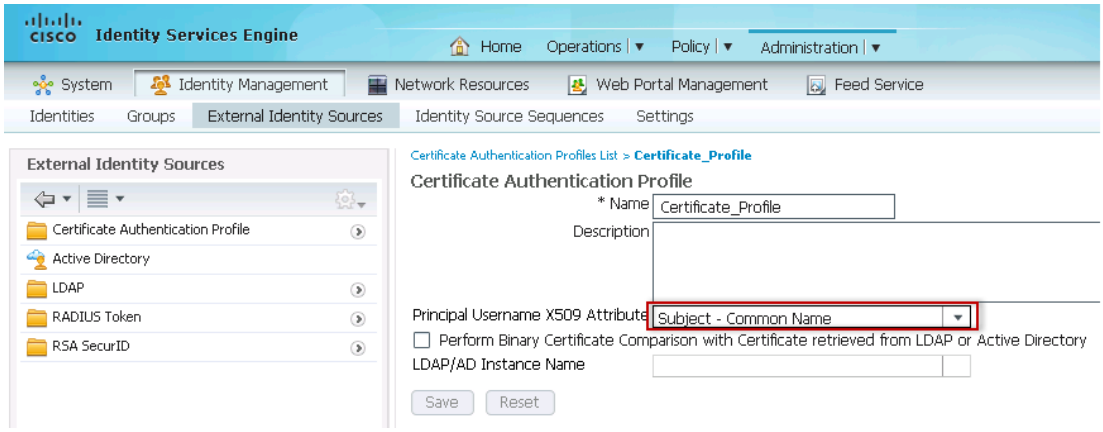
图 6-5　　身份验证门户设置



使用证书作为身份库的 ISE

若要将 ISE 配置为以证书作为身份库，选择 **Administration > External Identity Sources > Certificate Authentication Profile > Add**，并定义证书验证配置文件，如图 6-6 所示。

图 6-6　　证书验证配置文件

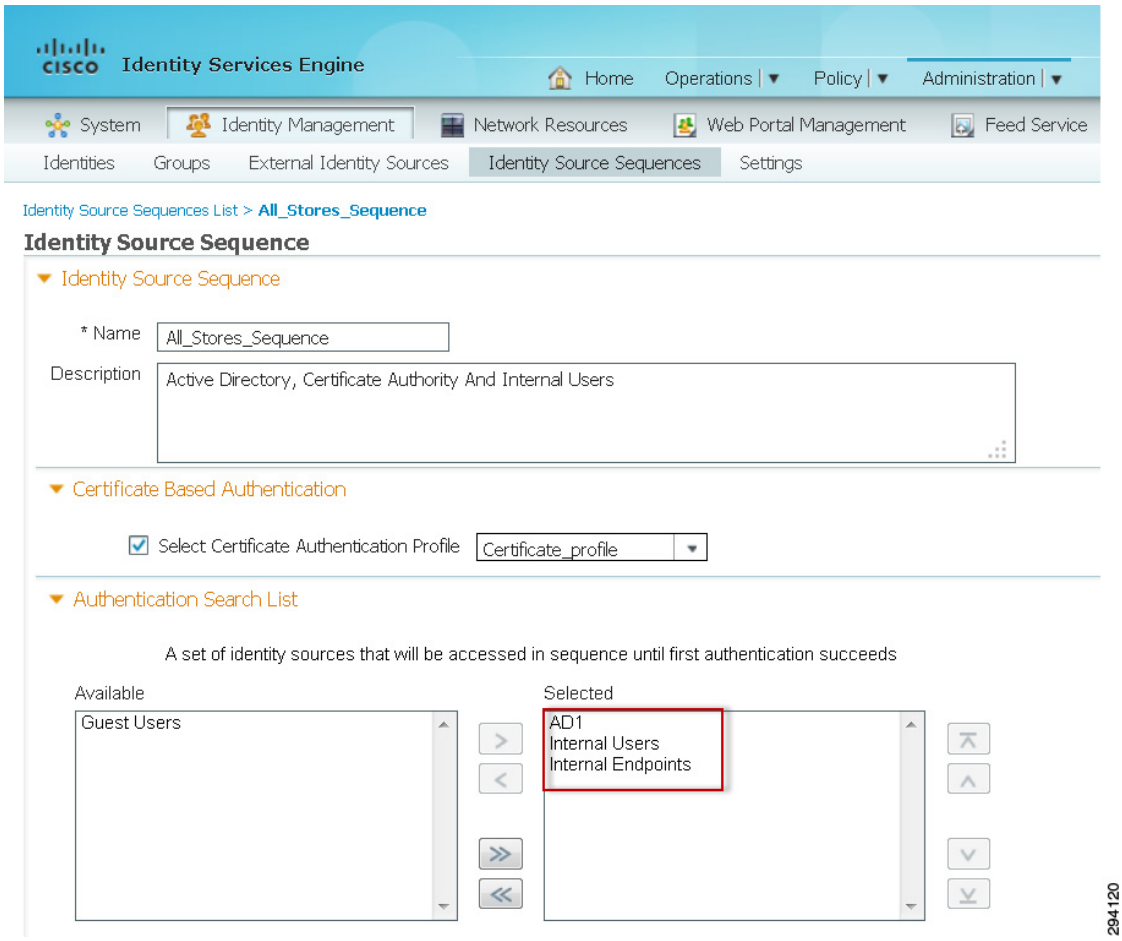


身份源序列

身份源序列用于定义 ISE 在不同数据库中查找用户凭证的顺序。这些数据库包括内部用户、Active Directory、 LDAP、 RSA 等。

若要添加新的身份源序列，点击 **Administration > Identity Source Sequences > Add**。图 6-7 中显示的配置新建了一个名为 All_Stores_Sequence 的身份源序列。它依赖于 Active Directory (AD1)、名为 “Certificate_profile ” 的证书配置文件和内部用户。

图 6-7　　身份源序列

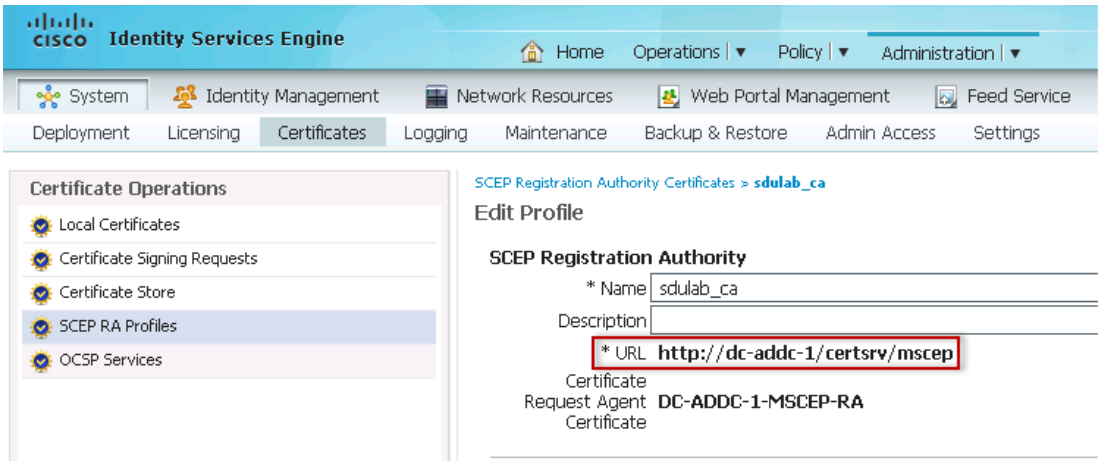


ISE 中的 SCEP 配置文件配置

在此设计中，ISE 作为简单证书注册协议 (SCEP) 代理服务器，因此，它允许移动客户端从 CA 服务器获取其数字证书。 ISE 的这一重要功能允许所有终端 （如 iOS、 Android、 Windows 和 MAC）通过 ISE 获得数字证书。此功能结合初次注册过程，显著简化了终端上数字证书的调配。

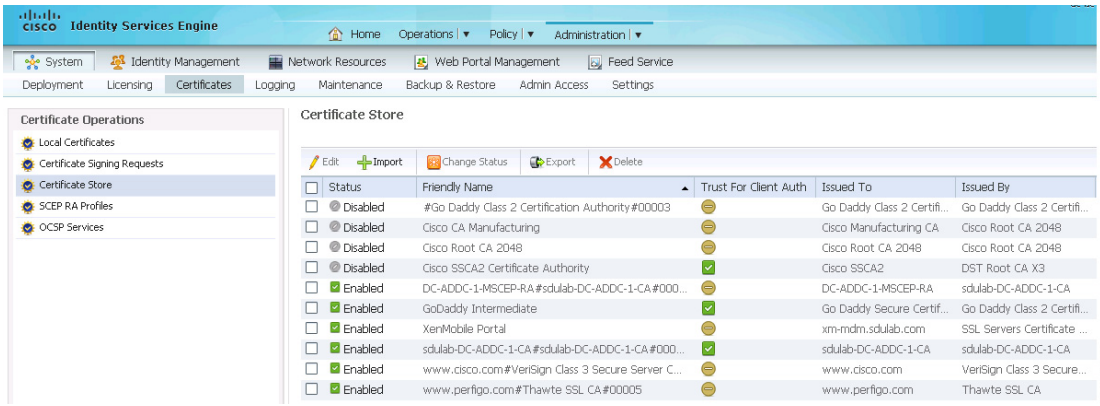
要在 ISE 中配置 SCEP 配置文件，请点击 **Administration > Certificates > SCEP RA Profiles > Add**。定义 SCEP 配置文件，如图 6-8 所示。

图 6-8　　SCEP 配置文件配置



配置成功后， ISE 下载 RA 证书和 CA 服务器的根 CA 证书，如图 6-9 所示。

图 6-9　　证书库



身份验证策略

身份验证策略用于定义由 ISE 用来与终端和用于身份验证的身份源通信的协议。 ISE 评估条件，并根据结果的真或假应用配置结果。身份验证策略包括：

- 允许的协议服务，例如 PEAP、 EAP-TLS 等
- 用于身份验证的身份源

与处理访问列表的方式类似，身份验证规则采取从上到下的处理顺序。如果满足第一个条件，则处理停止并使用分配的身份规则。

使用 “If、 then、 else”逻辑评估规则：

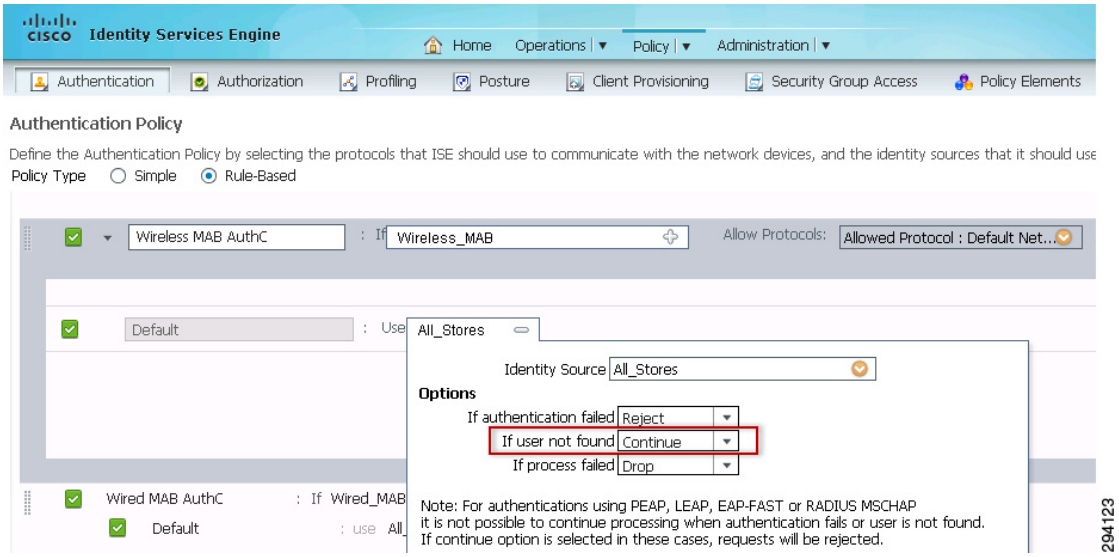
```
IF Wired_802.1X   Then
     Allow default protocols
Elseif   next condition
     Take action
Else
     Use Default Rule
```

在本文讨论的 BYOD 设计中，ISE 利用所有身份库验证了多个协议（如 MAB 和 dot1x）。身份库可以是 AD、Certificate_Profile、RSA、内部用户和内部终端。网络访问媒介可以是有线、无线或远程连接。网络设备可使用之前提到的任意媒介，使用不同的协议连接至 ISE。

MAC 身份验证旁路 (MAB) 协议用于验证未使用 dot1x 配置的设备。当新设备访问网络时，它通过 MAB 协议通信并使用自己的 MAC 地址作为其身份。在正常情况下，ISE 将验证 MAC 地址是否存在于任何身份库中；如果不存在，将拒绝该连接。但是，在此 BYOD 设计中，新设备出于自注册目的而使用 MAB 协议，不一定能够提前预知设备的 MAC 地址。

为了避免此问题，ISE 继续验证过程并将设备重定向到下一阶段，即使设备的 MAC 地址并不存在于任何身份库中。图 6-10 重点说明了此配置。

图 6-10　　MAB 的身份验证规则



在常规部署方案中，终端主要使用 dot1x 协议与 ISE 通信。ISE 使用 Active Directory 验证这些终端或通过数字证书进行验证。图 6-11 描述了不同的协议以及这些协议如何使用不同身份库进行身份验证。

图 6-11　　身份验证策略

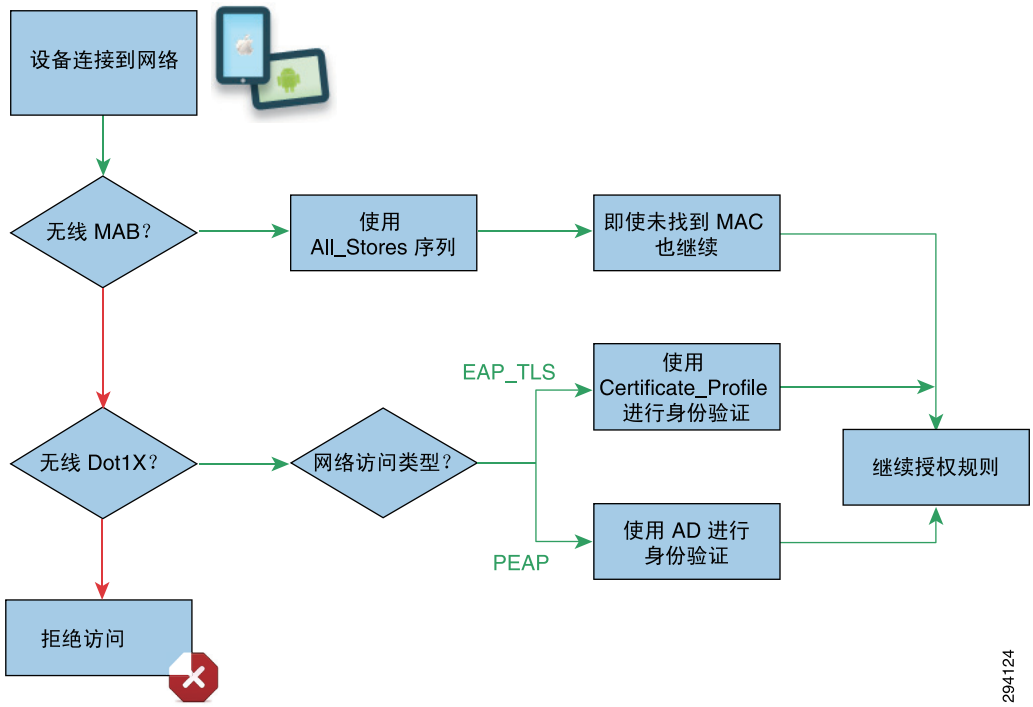


表 6-1 说明了这些规则在本设计指南中的实施方法。

表 6-1　　身份验证规则

规则名称	网络访问媒介	允许的协议	条件		身份库
Wireless MAB AuthC	无线 MAB	所有	默认		All_Stores
Wired MAB AuthC	有线 MAB	所有	默认		All_Stores
Wireless Dot1X AuthC	Wireless_8021X	所有	无线证书	EAP_TLS	Certificate_Profile
			无线密码	PEAP	All_Stores
Wired Dot1X AuthC	Wired_802.1X	所有	有线证书	EAP_TLS	Certificate_Profile
			有线密码	PEAP	All_Stores
Default					拒绝访问

无线身份验证策略

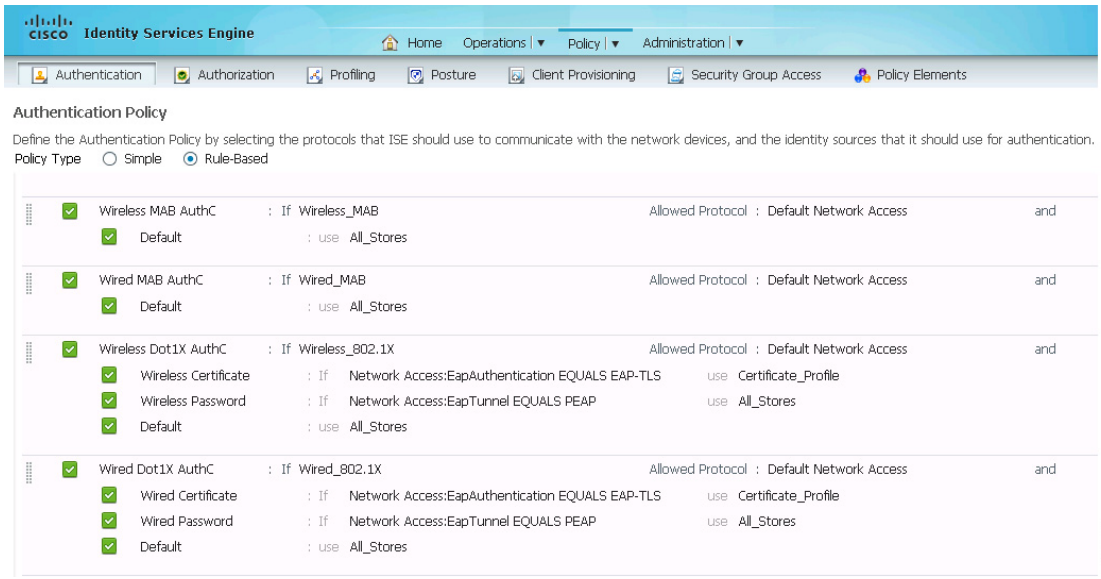
连接到无线网络时，终端设备可以使用 MAB 或 dot1x 协议。使用 MAB 的无线网络的身份验证策略在前面的章节中已经介绍。本节介绍使用 dot1x 协议的无线媒介的身份验证策略，如表 6-1 所示。

无线 Dot1x 身份验证是 wireless_dot1x 协议的规则名称。此规则匹配 wireless_dot1x 协议并有两个内部规则：

- 无线证书 - 当身份验证协议是 EAP_TLS 时匹配，并且使用身份库 Certificate_Profile 验证数字证书。
- 无线密码 - 在 PEAP 身份验证协议中匹配，并使用包含 Active Directory 的 All_Stores 身份库。

图 6-12 显示了这些规则在本设计指南中 ISE 上的配置方式。

图 6-12　　身份验证规则



客户端推送

对最终用户的设备类型进行分类时，Cisco ISE 会查看各种元素，包括操作系统版本、浏览器类型等。 ISE 对客户端机器分类后，如有必要，会使用客户端推送资源策略，确保客户端配置了合适的代理版本、最新合规性模块及正确的代理自定义包和配置文件。启用 DHCP 和 RADIUS 探测器中讨论了 ISE 分析服务。了解客户端推送策略和客户端推送资源之间的差异非常重要。客户端推送资源基本上是推送到终端设备并协助终端设备完成自注册流程的资源。客户端推送资源有两种类型：

- 可以在 ISE 上配置的本地配置文件，例如：iOS 配置文件。
- 必须从思科站点下载的软件调配向导。

另一方面，客户端推送策略可将终端设备与相应的客户端推送资源关联起来。因此，在配置客户端推送策略之前，必须将客户端推送资源添加到 ISE。本节将讨论 iOS、 Android、 Windows 和 Mac OS X 设备的客户端推送资源和客户端推送策略。

以下是在终端上进行客户端推送的注意事项：

- 根据不同的终端，将相应的软件调配向导 (SPW) 推送到设备。此向导配置终端上的 dot1x 设置，并配置终端以获取数字证书。
- 在某些终端 （例如 IOS 设备）中，不需要 SPW 包，因为 iOS 设备使用本地操作系统配置 dot1x 设置。
- 对于 Android 设备， SPW 包需要从 Google Play 商店下载。

客户端推送资源 - Apple iOS 和 Android

若要配置移动设备的客户端推送资源，点击 **Policy > Policy Elements > Results > Client Provisioning > Resources > Add Native Supplicant Profile**。图 6-13 显示了 Apple iOS 设备使用的无线 iOS TLS 配置文件的配置详细信息。此配置文件用于配置自注册后访问 BYOD_Employee SSID 所需的参数。

图 6-13　　无线 iOS TLS 配置文件

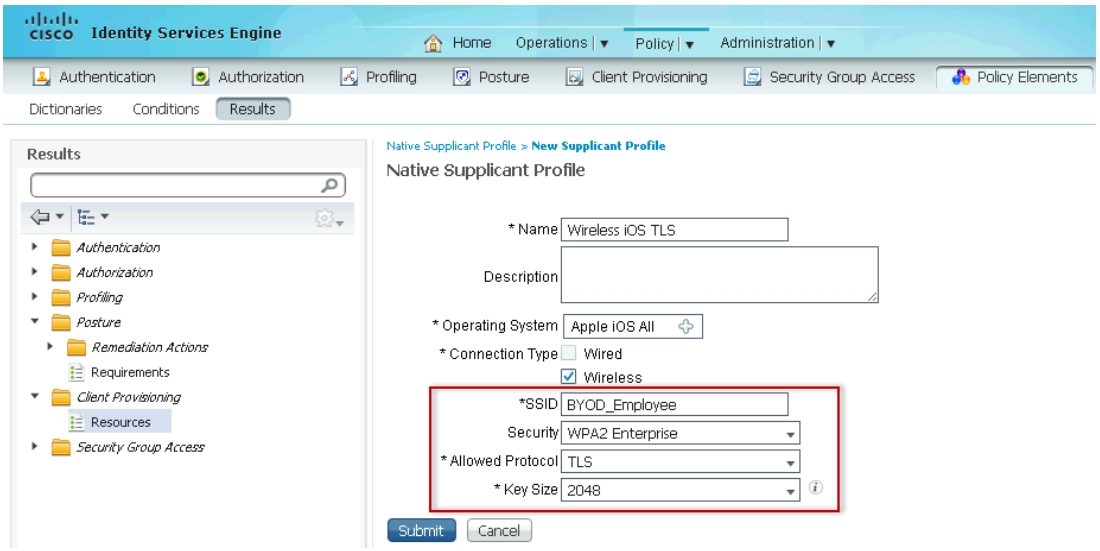
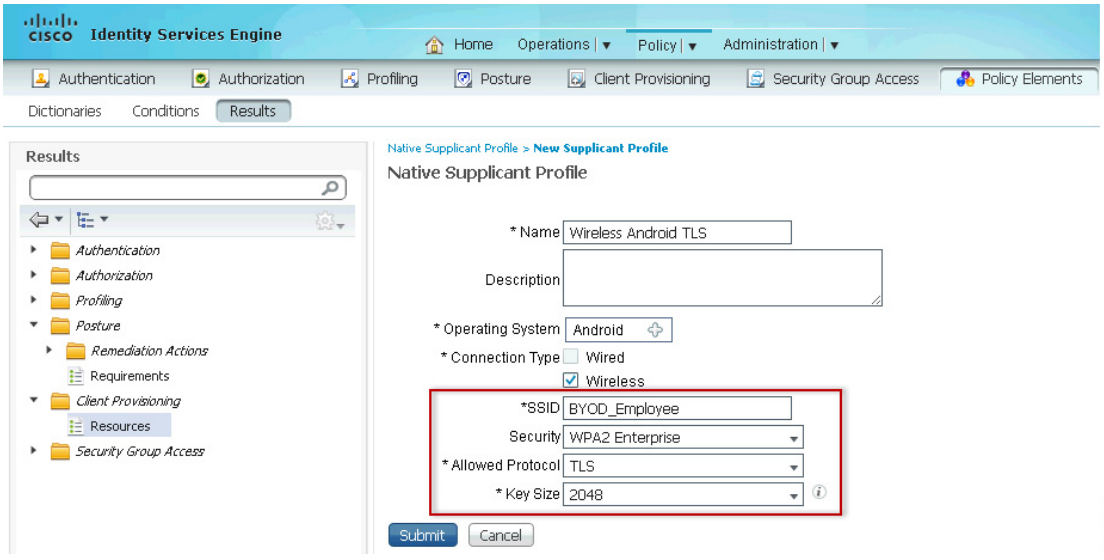


图 6-14 显示了 Android 设备使用的无线 Android TLS 配置文件的配置详细信息。

图 6-14　　无线 Android TLS

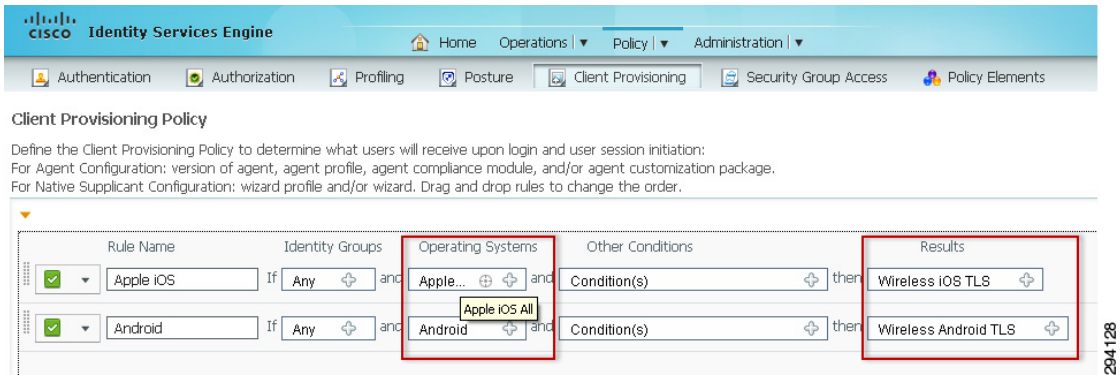


客户端推送策略 - Apple iOS 和 Android 设备

客户端推送策略确定哪些用户接收哪些版本的资源。在定义本地 Supplicant 客户端配置文件后，下一步是点击 **Policy > Client Provisioning**，在设备连接到网络时使用适当的配置文件。

图 6-15 中的配置用于确定设备上运行的操作系统并定义要分发的资源。在这种情况下，根据相应的操作系统分发先前定义的配置文件。

图 6-15　　客户端推送策略



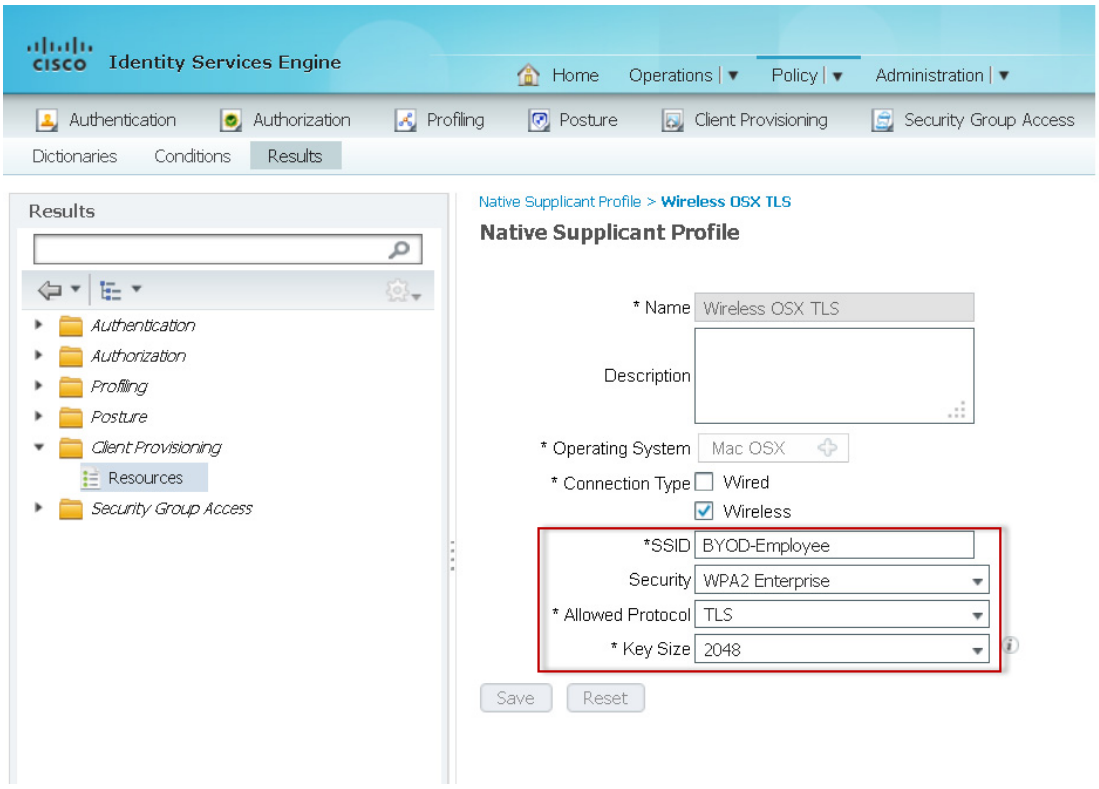
请务必注意，对于 Android 设备，用户也需要从 Google Play 商店下载软件，因为它不能由 ISE 分发。

客户端推送资源 - MAC OS

对于 Mac OS 工作站，需要使用以下项：

- 本地 Supplicant 客户端配置文件，用于确定应该在设备上调配哪种类型的配置，例如无线 SSID 名称。图 6-16 显示了 Mac OSX 设备的本地 Supplicant 客户端配置文件。

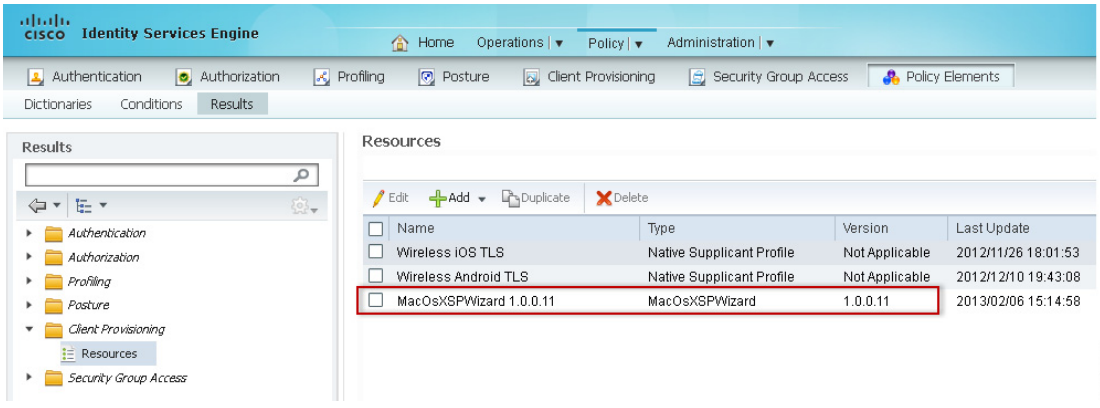
图 6-16　　Mac OSX 设备的本地 Supplicant 客户端配置文件



- 向导配置文件 - Supplicant 客户端推送向导配置文件是一种可从思科下载的软件代理。

若要定义客户端推送资源，请在思科站点上点击 **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > Agent Resources**，并选择 **MacOsXSPWizard**。图 6-17 显示了 MacOsXSPWizard 配置文件。

图 6-17　　Mac OsXSPWizard 配置文件



Mac OS 设备的客户端推送策略 - 无线

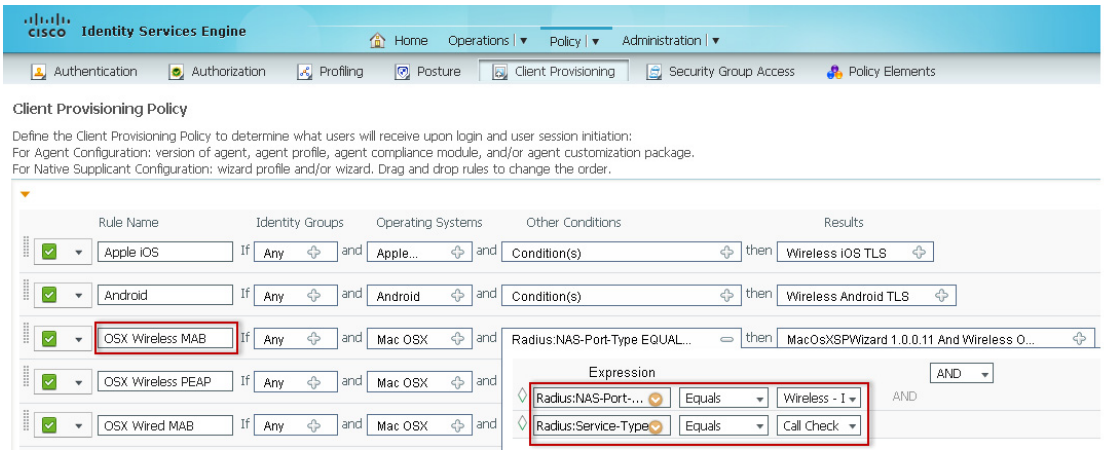
上一节讨论了调配 MAC OS 设备所需的资源。配置资源后，下一个步骤便是定义在什么条件下使用这些资源。在调配过程中，Mac OS X 设备可以使用 MAB 或 PEAP 协议。因此，必须配置不同的条件，使其与这两者之一匹配。

如果符合以下两个条件，则匹配 MAB 协议：

- Radius:NAS-Port-Type Equals Wireless—IEEE 802.11
- Radius:Service-Type Equals Call Check

图 6-18 显示了要在 MAB 协议中匹配的客户端推送策略。

图 6-18　　MAB 的客户端推送策略

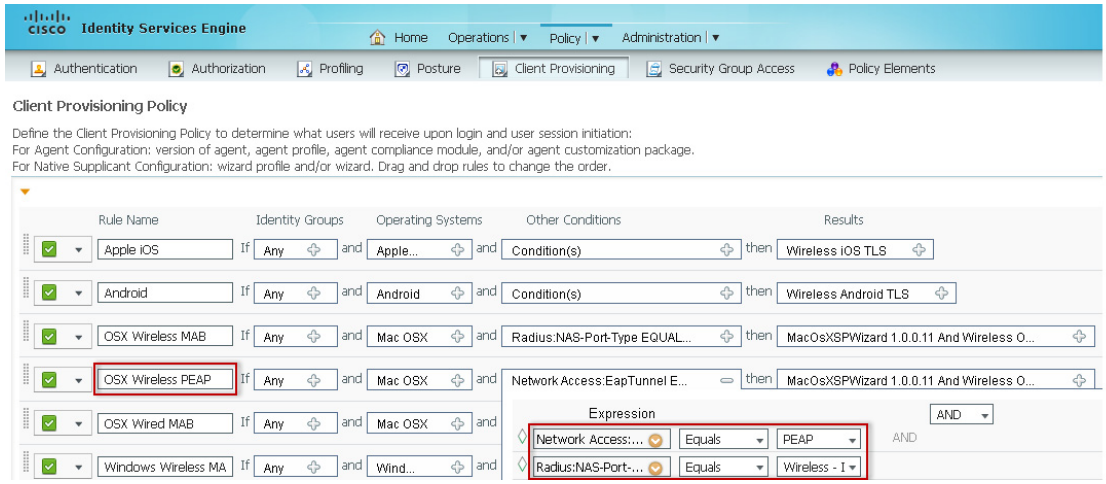


若要与使用 PEAP 协议的 Mac 设备匹配，需要满足以下条件：

- Radius:NAS-Port-Type Equals Wireless—IEEE 802.11
- Network Access:EapTunnel EQUALS PEAP

图 6-19 显示了要在使用 PEAP 协议的 MAC 设备上匹配的条件。

图 6-19　　PEAP 的客户端推送策略

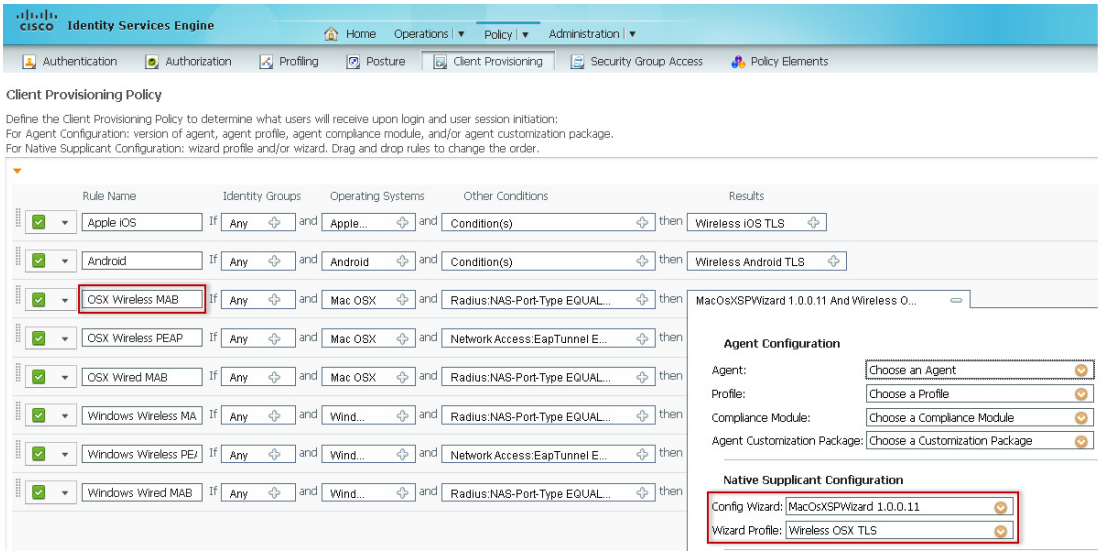


若要完成 MAC_OSX_Wireless 设备的客户端推送策略，必须定义如下内容：

- 操作系统必须选为 Mac OSX。
- 应使用与 MAB 或 PEAP 协议匹配的条件。
- 结果部分必须包含本地 Supplicant 客户端配置文件和适用于 Mac OS X 设备的 SPW。

完整策略如图 6-20 所示。

图 6-20　Mac OS X 的客户端推送策略



Windows 设备的客户端推送策略 - 无线 / 有线

定义 Windows 设备调配策略的配置步骤与 Mac OS X 或 IOS 设备的步骤非常类似，因此，这里不再重复相同的配置步骤。需要指出的唯一区别为，Windows 设备需要不同的 SPW 包。图 6-21 描述了使用 MAB 或 PEAP 的 Windows （有线或无线）设备的客户端推送策略。

图 6-21　Windows 的客户端推送策略

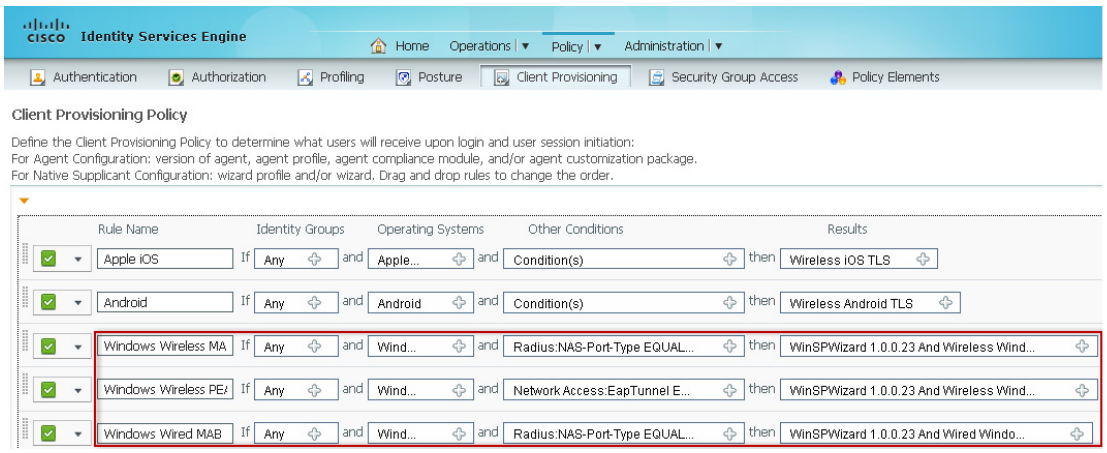
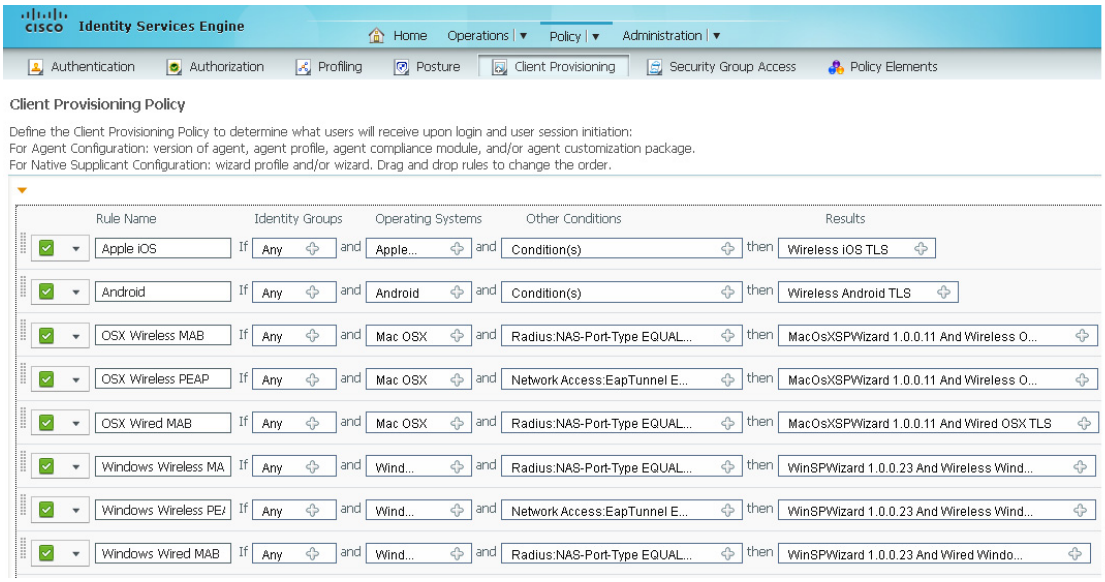


图 6-22 显示了测试过程中使用的完整客户端推送策略。

图 6-22　　完整客户端推送策略



分析

分析是一项关键服务，负责识别、查找和确定连接到网络的终端的功能，以拒绝或执行特定授权规则。其中两个主要分析功能包括：

- 收集器 - 用于从网络设备收集网络数据包并将属性值转发到分析器。
- 分析器 - 用于使用与属性匹配的已配置策略确定设备类型。

收集终端信息有两种主要方法：

- 作为收集器和分析器的 ISE。
- 从 7.3 版本开始， WLC 可以作为收集器，将所需属性发送至充当分析器的 ISE。

本地模式和 FlexConnect 模式中的接入点支持从运行 7.3 或更新版本的控制器执行客户端分析。表 6-2 显示了 WLC 和 ISE 分析之间的主要区别。

表 6-2　　ISE 与 WLC 分析支持

ISE	WLC
分析使用大量探测器，包括 RADIUS、DHCP、DHCP SPAN、 HTTP、 DNS 等	仅限基于 DHCP 和 HTTP 的分析
作为策略操作， ISE 支持多个不同属性	WLC 支持 VLAN、 ACL、会话超时、 QoS
分析规则可以通过用户定义属性进行自定义	只能使用默认分析规则

注意　本设计指南使用 ISE 的分析功能，并且未测试控制器客户端分析功能。

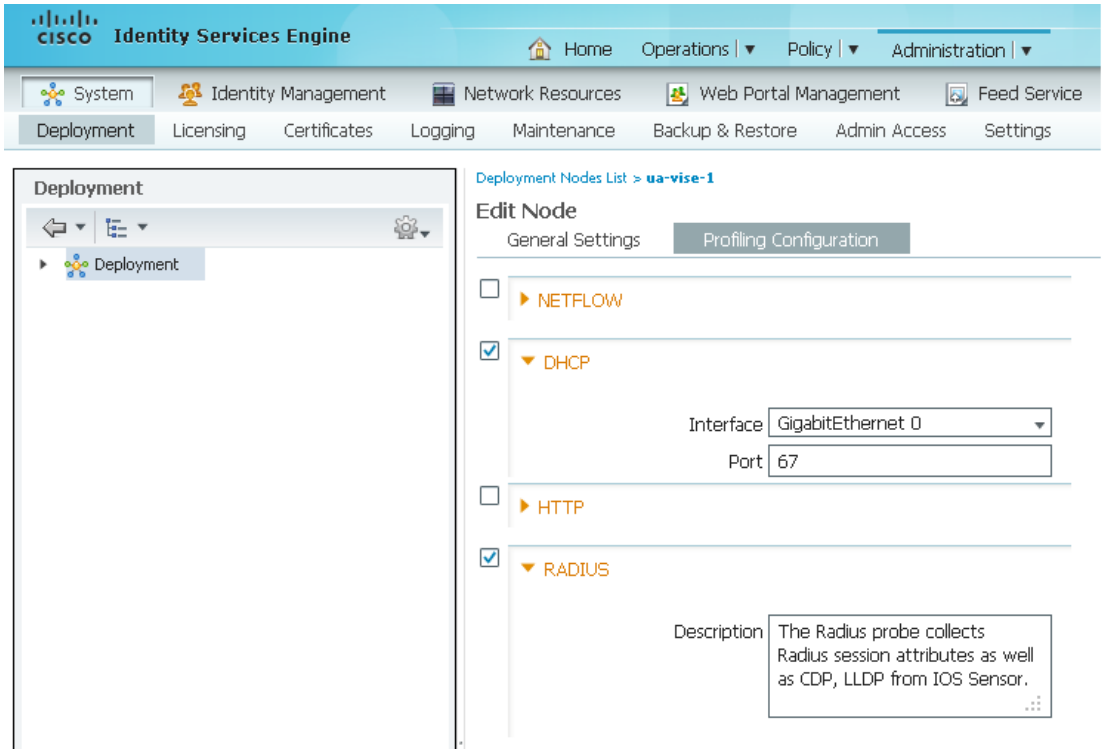
ISE 支持许多传感器，可捕获终端属性并根据其配置文件进行分类。传感器依赖于许多探测器，这些探测器通过查询网络接入设备捕获网络数据包。对终端进行配置后，可能会执行不同的身份验证和授权策略。根据设备配置文件使用不同策略的一些示例包括：

- 允许员工拥有的 iPad 访问网络，但仅用于 HTTP 流量。
- 如果连接到网络的 iOS 设备为公司拥有的设备，则享有网络的完全访问权限。
- 如果员工拥有的 iPad 已调配了数字证书，则享有网络的完全访问权限。
- 强制某些设备注册到其移动设备管理器。
- 拒绝任何 iPad 或 Android 设备的访问。

启用 DHCP 和 RADIUS 探测器

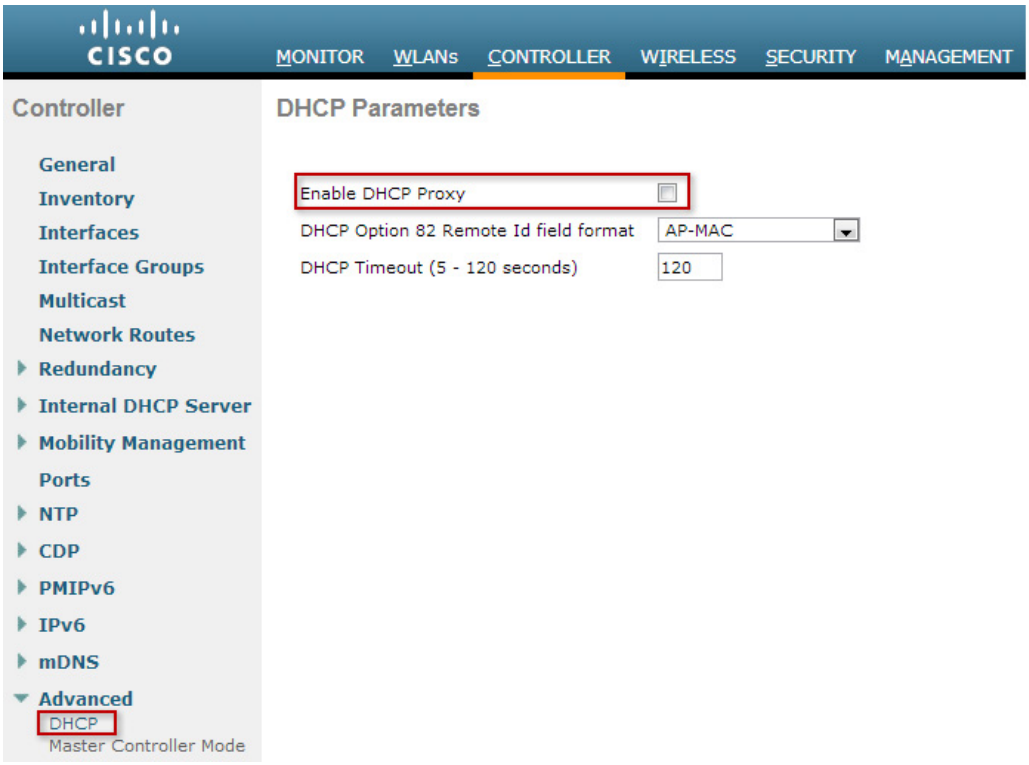
若要在 ISE 中启用分析，请点击 **Administration > System > Deployment**。点击 ISE 主机名并点击 **Profiling Configuration**。启用相应的探测器，以侦听从局域网交换机或无线局域网控制器转发的数据包，如图 6-23 所示。

图 6-23　　分析探测器



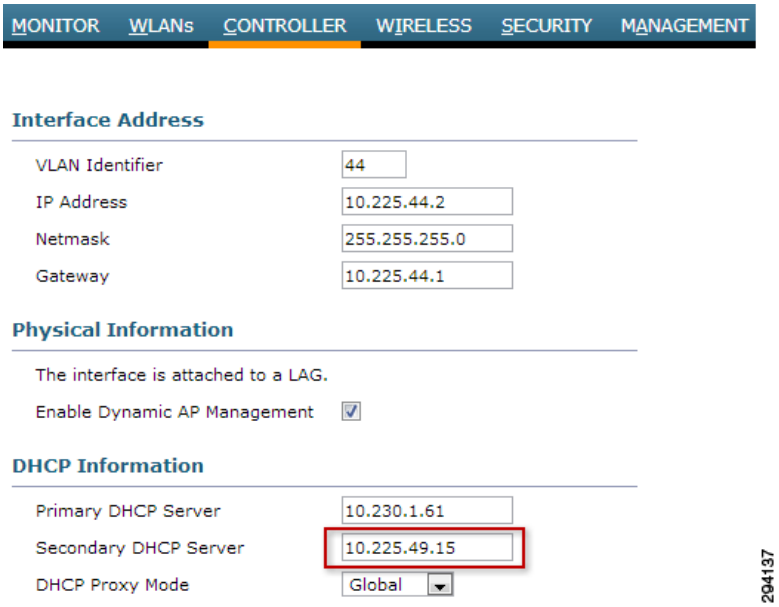
应该在 DHCP 桥接模式下配置无线局域网控制器，以将来自无线终端的 DHCP 数据包转发到 ISE。点击 **Controller > Advanced > DHCP** 并清除 Enable DHCP Proxy 复选框，如图 6-24 所示。

图 6-24　　禁用 DHCP 代理



通过点击 **Controller > Interfaces > Secondary DHCP**，将 ISE 的 IP 地址指定为 WLC 上的辅助 DHCP 服务器，如图 6-25 所示。

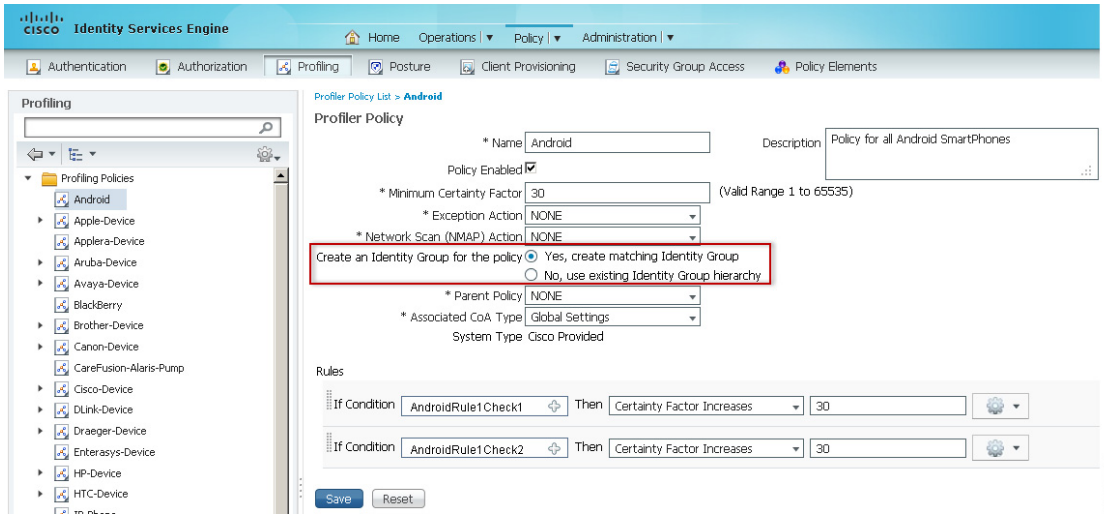
图 6-25　　辅助 DHCP 服务器



分析 Android 设备

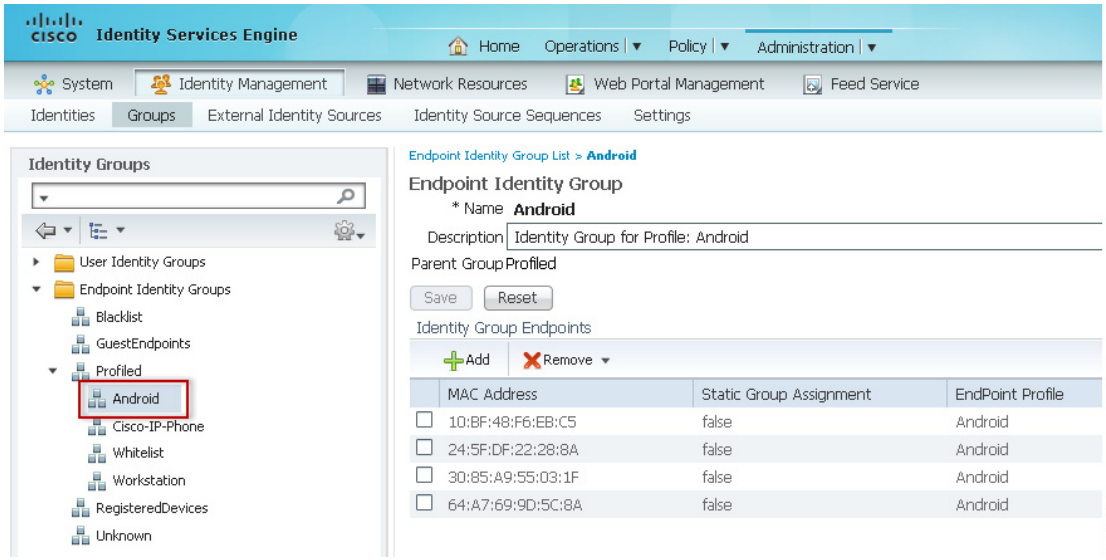
若要根据 Android 策略创建身份组，点击 **Policy > Profiling > Profiling Policies > Android** 并启用创建匹配身份组，如图 6-26 所示。

图 6-26　　Android 分析策略



Android 分析策略应该列在 Endpoint Identity Groups > Profiled 下。点击 **Administration > Identity Management > Groups**，查看由 ISE 分析的 Android 设备列表，如图 6-27 所示。

图 6-27　　Android 身份组



逻辑配置文件

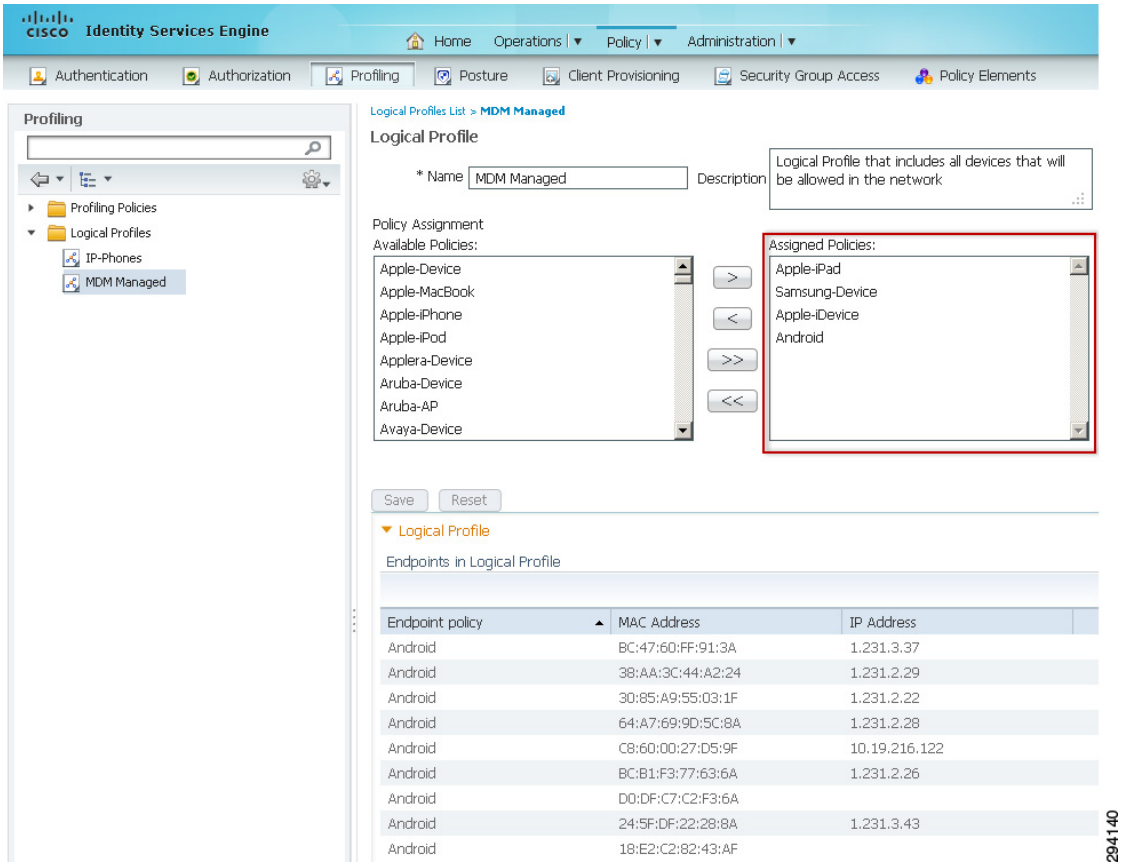
逻辑配置文件是对不同配置文件进行分组以创建配置文件整体类别的容器。逻辑配置文件为授权策略提供额外的灵活性，强化整体网络访问策略。

通过逻辑配置文件，授权规则中的单个条目可以包含多个配置文件。必须为每个设备类型创建匹配身份组，逻辑配置文件才会变为可用状态。

在本设计指南中，创建逻辑配置文件是为了对由 MDM 管理的移动设备进行分组。此配置文件将某些移动设备合并到可能从授权规则调用的单个逻辑配置文件中。

若要创建逻辑配置文件，请点击 **Policy > Profiling > Profiling > Logical Profiles**，如图 6-28 所示。

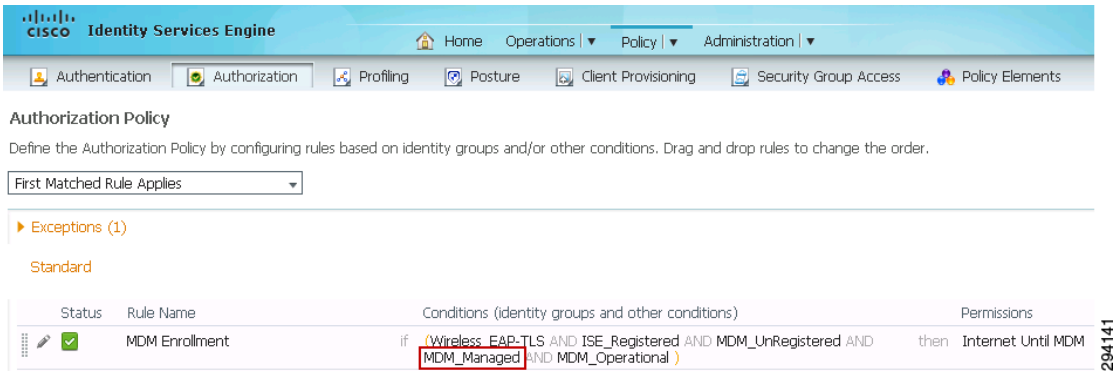
图 6-28　　MDM 托管逻辑配置文件



此逻辑配置文件可随时灵活添加新设备，无需修改授权规则。图 6-29 显示了如何使用 MDM 托管逻辑配置文件识别 MDM 支持的设备。

在本设计指南后面的部分对此与其他授权规则进行了更详细的说明。

图 6-29　　MDM 注册授权规则



授权策略和配置文件

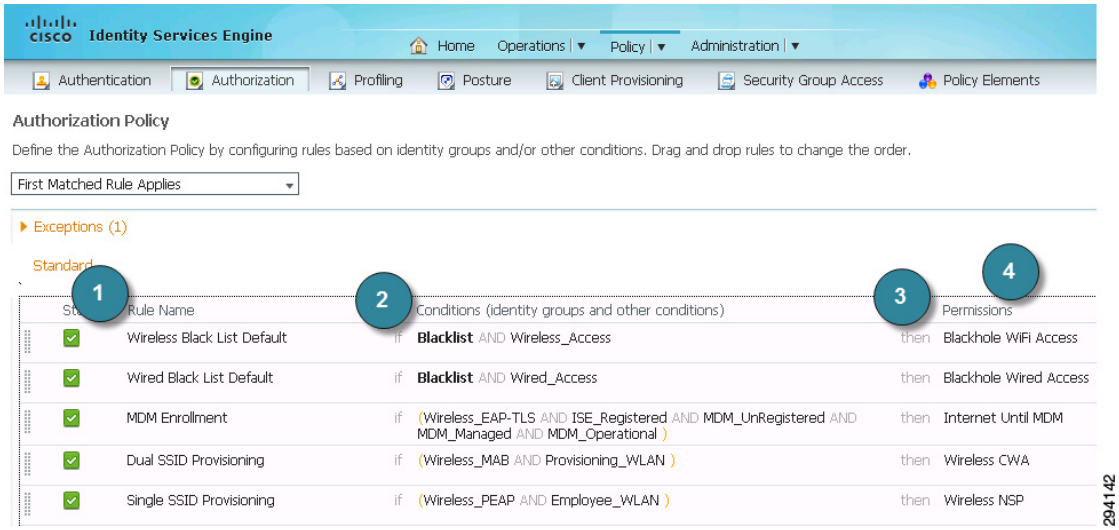
授权策略定义访问网络的整体安全策略。网络授权控制用户对网络及其资源的访问，以及每台设备可以使用此类资源在系统中执行什么操作。授权策略由多个规则组成。

授权规则由三个主要元素定义，如图 6-30 所示：

- 名称 (1)
- 条件 (2)
- 权限 (3)
- 授权配置文件 (4)

权限由授权配置文件执行 (4)。与身份验证规则类似，授权规则采用从上到下的处理顺序。如果满足第一个条件，则处理停止，且分配的权限规定要使用的授权配置文件。

图 6-30　　授权策略



授权配置文件

授权配置文件就像一个容器，其中的多个特定权限可允许访问一组网络服务。授权配置文件即是定义要授予的这组权限的地方，可能包括：

授权配置文件对授予用户或设备的特定权限进行分组，可能包括以下任务：

- 一个相关的 VLAN。
- 一个相关的可下载 ACL (DACL)。
- 无线局域网控制器属性，例如使用命名 ACL 或安全组标记进行策略实施。
- 使用字典中所含属性的高级设置。

除了标准 PermitAccess 和 DenyAccess 授权配置文件外，以下还列出了本设计指南中定义的部分配置文件：

- Wireless CWA - 此配置文件用于将无线设备重定向到使用 MAB 和双 SSID 的设备的注册门户。
- Wireless NSP - 此配置文件用于在无线用户使用 dot1x 或单 SSID 访问网络时，将其重定向到注册门户。
- Blackhole WiFi Access - 用于阻止对已报失设备的访问 （如需更多信息，请参阅第 14 章，“管理丢失或被盗设备”）。

本设计指南的其他章节还介绍了其他几种授权配置文件。

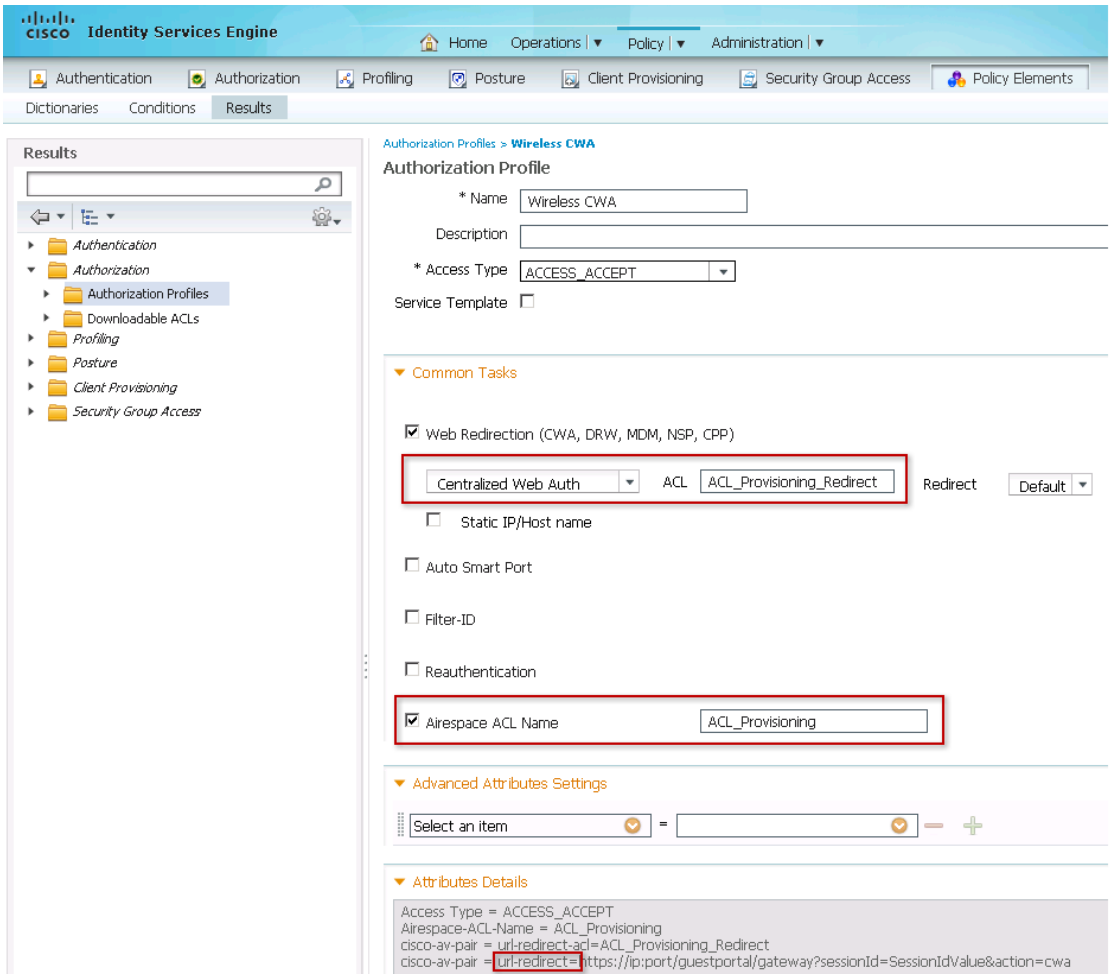
双 SSID 调配的无线 CWA 授权配置文件

此策略在双 SSID 配置中使用，在连接到网络时将无线设备重定向到自助注册门户。此授权配置文件通过触发 ACL_Provisioning_Redirect 访问列表限制访问，此列表已在无线局域网控制器中提前定义。

在实施双 SSID 时，调配 SSID 可以是开放的，也可以是使用 Active Directory 凭证进行密码保护的。在本设计指南中，调配 SSID 是开放的，并依赖于 MAC 身份验证旁路 (MAB) 授予网络访问权限。

若要配置此授权策略，点击 **Policy > Policy Elements > Results > Authorization Profiles**，如图 6-31 所示。

图 6-31　　无线 CWA 授权配置文件



为了强制设备转到自助注册门户，将使用唯一会话 ID 创建重定向 URL 并推送到设备：

https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

当用户启动 Web 浏览器时，设备会重定向到自助注册门户。为了阻止用户保持对调配 SSID 的连接，ACL_Provisioning_Redirect ACL 只允许对 Cisco ISE、DHCP 和域名系统 (DNS) 服务的访问。

无线 CWA 授权配置文件依赖于无线局域网控制器中预先定义的两个命名 ACL：

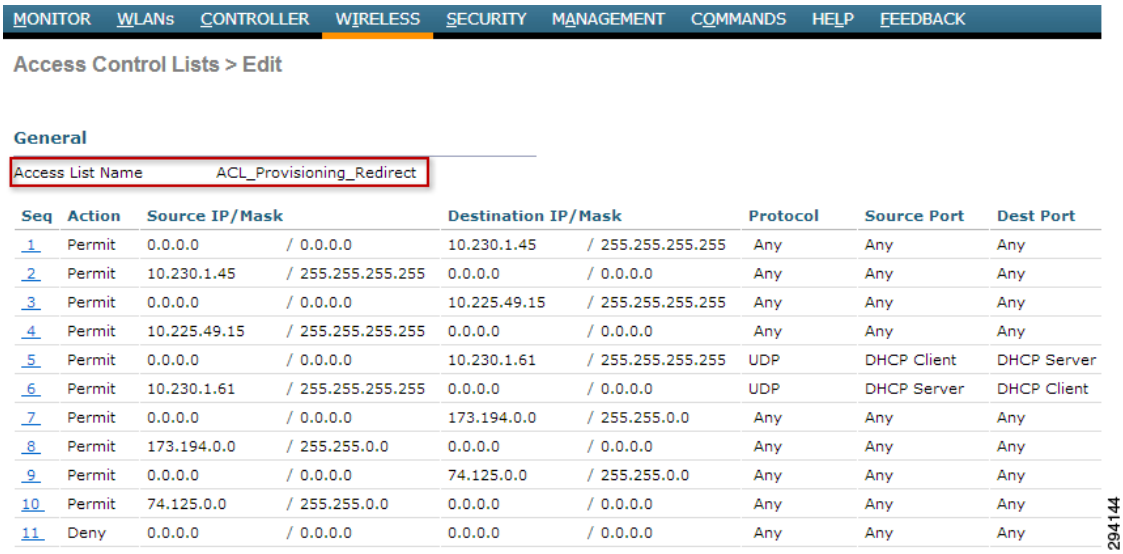
- ACL_Provisioning_Redirect - 应用于集中式网络身份验证设置。
- ACL_Provisioning - 通过 Radius: Airespace ACL-Name 属性值 (AV) 发送到无线控制器。

两个 ACL 在两个无线控制器间的行为稍有不同：

- 对于 CUWN 无线控制器（例如，CT5508 和 Flex 7500），ACL_Provisioning_Redirect 同时充当控制 Web 重定向的 ACL 和控制网络访问的 ACL。 ACL_Provisioning 仅作为一个额外的安全配置，并且在指定 URL 重定向时不会使用。对于 CUWN 无线控制器，图 6-32 所示的 ACL_Provisioning _Redirect ACL 可以与 ACL_Provisioning 相同。
- 对于基于 Cisco IOS XE 的无线控制器 （例如， CT5760 和 Catalyst 3850），ACL_Provisioning_Redirect 明确用作控制 Web 重定向的 ACL。ACL_Provisioning 用作控制无线客户端可以访问网络中哪些位置的 ACL。因此，指定 URL 重定向时，基于 IOS XE 的无线控制器会同时使用两个 ACL。

图 6-32 显示了 WLC 上 ACL_Provisioning_Redirect 的配置。这只是一个示例，因为每个组织都有独特的业务策略和安全要求。

图 6-32　　调配的 WLC 访问列表



ACL_Provisioning_Redirect ACL 指定以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 对 Google Play 的访问。

注意　Android 设备需要访问 Google Play 商店，以下载 SPW 包。修改 ACL 以允许终端下载 SPW。分析 DNS 服务器和设备之间的 DNS 事务是开发 ACL_Provisioning_Redirect 并对其进行故障排除的一种方法。

在 Catalyst 3850 或 CT5760 控制器上， ACL_Provisioning_Redirect 定义如下：

```
ip access-list extended ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 permit tcp any any eq www
 permit tcp any any eq 443
```

ACL_Provisioning_Redirect ACL 指定以下访问权限：

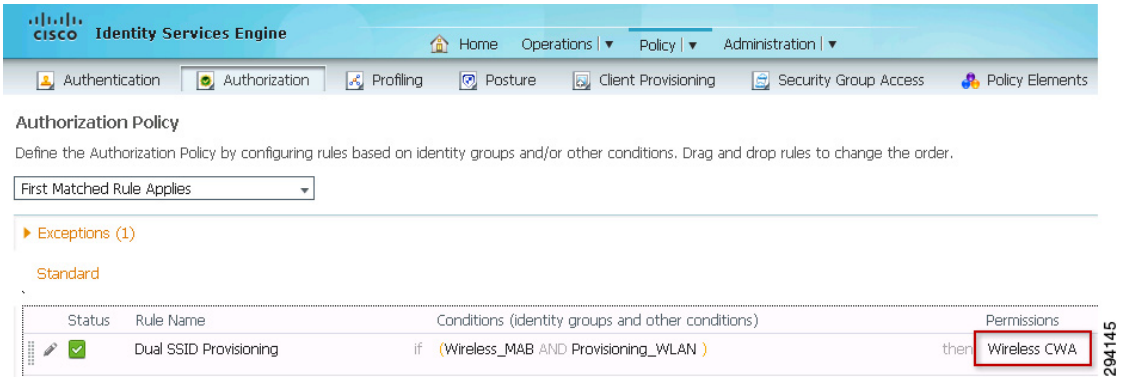
- 拒绝 （不重定向）以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 拒绝 （不重定向）以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 拒绝 （不重定向） DHCP 访问 （bootpc 和 bootps）。
- 允许 （重定向）对任何 Web 主机的 TCP 访问。

- 允许 （重定向）对任何安全 Web 主机的 TCP 访问。
- 拒绝 （不重定向）所有其他以互联网作为目标的访问。

双 SSID 调配授权规则

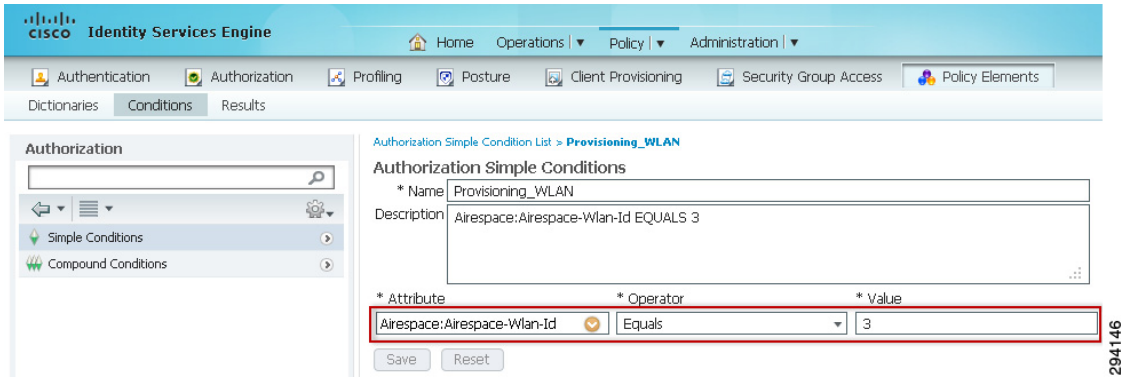
双 SSID 调配规则将无线 CWA 授权配置文件与将 MAB 设备授权到调配 SSID 的条件相关联，如图 6-33 所示。它包含两个条件：Wireless_MAB 和 Provisioning_WLAN。

图 6-33　双 SSID 授权规则



Wireless_MAB 条件是 ISE 中的预定义条件，而 Provisioning_WLAN 条件是在 **Policy > Conditions > Simple Conditions** 菜单中定义的条件，如图 6-34 所示。

图 6-34　Provisioning_WLAN 条件



在本 CVD 中，在测试期间，BYOD_Provisioning SSID 号定义为 3。当 SSID 号为 3 时，简单条件 Provisioning_WLAN 匹配。创建该条件是为了提高规则的可读性。

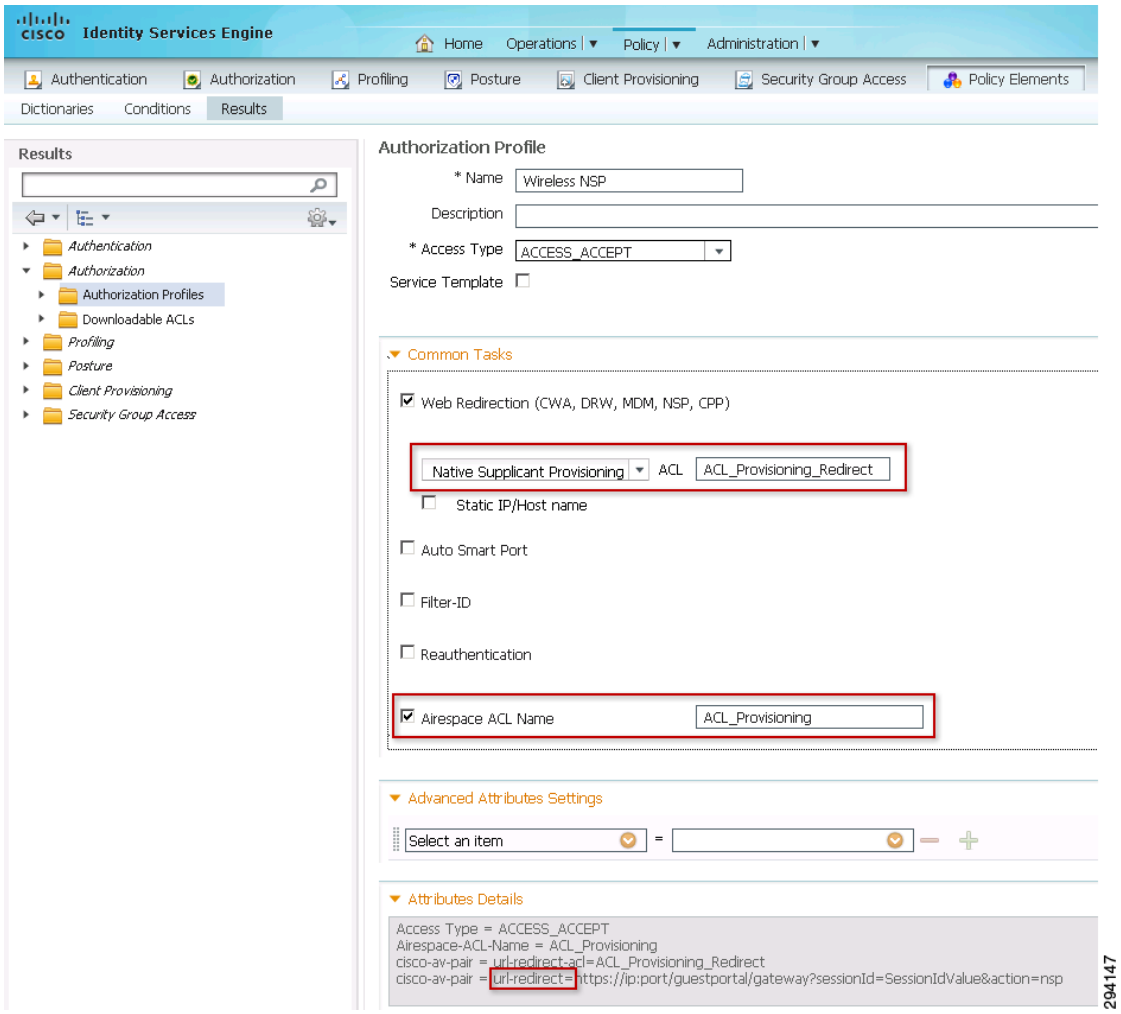
单 SSID 调配的无线 NSP 授权配置文件

通过将使用受支持个人设备的员工重定向到需要输入用户凭证的访客门户，无论设备类型是什么，本地 Supplicant 客户端流量都会启动。从这里，他们被重定向到自助调配门户，确认他们的设备信息。

无线 NSP 授权配置文件用于单 SSID 配置，以使用 PEAP 身份验证协议将设备重定向到访客门户。

若要配置此授权策略，点击 **Policy > Policy Elements > Results > Authorization Profiles**，如图 6-35 所示。

图 6-35　　无线 NSP 授权配置文件



无线 NSP 授权配置文件依赖于无线局域网控制器中预先定义的两个命名 ACL：

- ACL_Provisioning_Redirect - 应用于集中式网络身份验证设置。
- ACL_Provisioning - 通过 Radius: Airespace-ACL-Name 属性值 (AV) 发送到无线控制器。

两个 ACL 在两个无线控制器间的行为稍有不同：

- 对于 CUWN 无线控制器（例如，CT5508 和 Flex 7500），ACL_Provisioning_Redirect 同时充当控制 Web 重定向的 ACL 和控制网络访问的 ACL。 ACL_Provisioning 仅作为一个额外的安全配置，并且在指定 URL 重定向时不会使用。对于 CUWN 无线控制器，图 6-32 所示的 ACL_Provisioning _Redirect ACL 可以与 ACL_Provisioning 相同。
- 对于基于 Cisco IOS XE 的无线控制器 （例如， CT5760 和 Catalyst 3850），ACL_Provisioning_Redirect 明确用作控制 Web 重定向的 ACL。ACL_Provisioning 用作控制无线客户端可以访问网络中哪些位置的 ACL。因此，指定 URL 重定向时，基于 IOS XE 的无线控制器会同时使用两个 ACL。

单 SSID 调配授权规则

单 SSID 调配规则将无线 NSP 授权配置文件与对通过 PEAP 验证的无线设备进行授权的条件相关联。

为了强制设备转到自助注册门户，将使用唯一会话 ID 创建重定向 URL 并推送到设备：

https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp

当用户启动 Web 浏览器时，设备会重定向到自助注册门户。

图 6-36 显示了授权策略下定义的授权规则。此规则包括两个条件：Wireless_PEAP 和 Employee_WLAN。

图 6-36　　单 SSID 调配授权规则

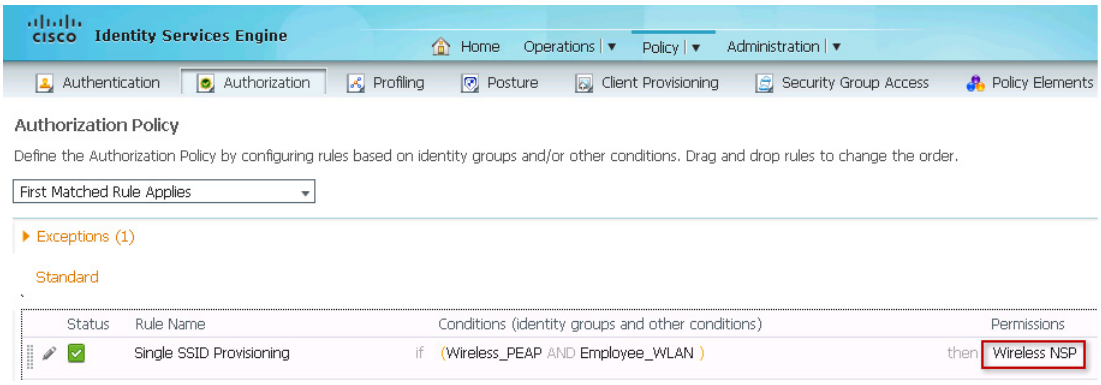
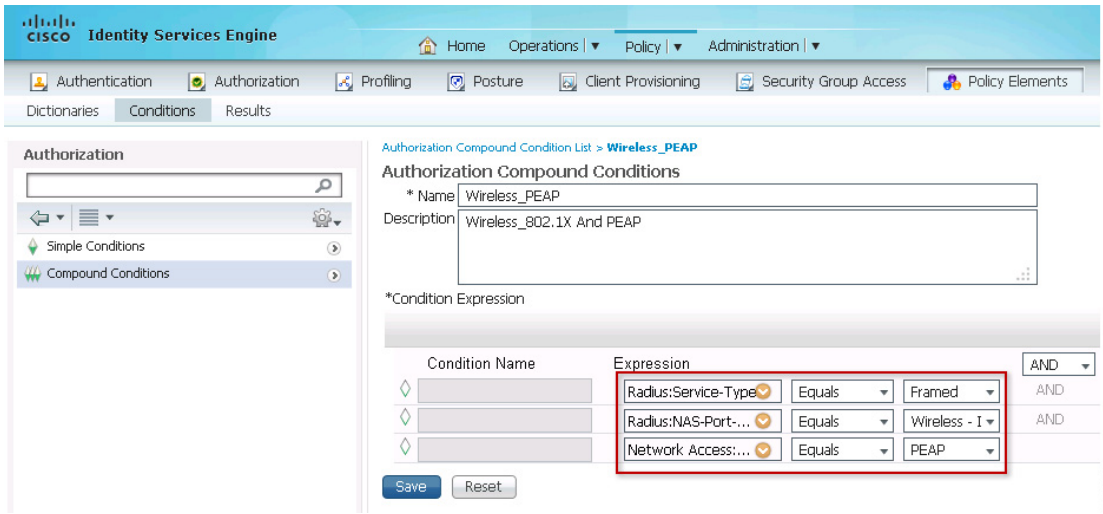


图 6-37 显示了 ISE 中的 Wireless_PEAP 复合条件，包括以下表达式：

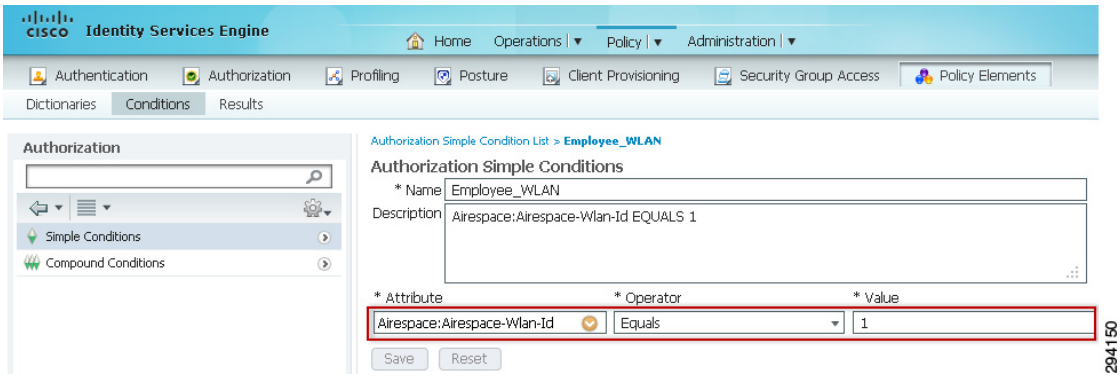
- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless—IEEE 802.11
- Network Access: EapTunnel Equals PEAP

图 6-37　　Wireless_PEAP 复合条件



在本 CVD 中，在测试期间， BYOD_Employee SSID 号定义为 1。当 SSID 号为 1 时，简单条件 Employee_WLAN 匹配。创建该条件是为了提高规则的可读性。

图 6-38　　Employee_WLAN 条件



证书颁发机构服务器

证书颁发机构服务器是分发数字证书的中心机构。在本解决方案中， Windows 2008 CA 服务器用作 CA 服务器。本节的重点是：

- 网络设备注册服务，即 Microsoft 的 SCEP 实施。
- 证书模板及其设计方法。

SCEP 的 NDES 服务器配置

网络设备注册服务 (NDES) 是 Microsoft 的 SCEP 实施，是使网络设备可以从 CA 注册 X.509 证书的通信协议。若要将数字 x.509 客户端证书分发和部署给用户，需要将 Microsoft 网络设备注册服务 (NDES) 与 Microsoft CA 服务器结合使用。有关如何实施 NDES 的详细信息，请参阅：http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx。

默认情况下， NDES 服务会配置为提供用于证书注册的一次性注册密码。 NDES 服务使用一次性密码通常是为了使网络和 IT 管理员能够为 IT 组织中的网络设备注册证书。但是，在本解决方案中，由于会使用 RSA SecurID 令牌验证远程终端，所以此功能被禁用。

禁用 NDES 服务器上的 “一次性密码”需要在以下注册表项中进行配置：Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword。

EnforcePassword 值数据设置为 “0”，以确保 NDES 不会请求密码。

注意　Windows Server 2003、 Microsoft 简单证书注册协议 (MSCEP) 要求在 CA 所在的同一台计算机上安装资源包附件。在 Windows Server 2008 中， MSCEP 支持已重命名为 NDES 并且是操作系统的一部分。 NDES 可以安装在与 CA 不同的计算机上 (http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx)。

IIS 的 NDES 扩展项使用注册表存储配置设置。所有设置存储在一个注册表项下：

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

注意　ISE 可能生成对 IIS 而言过长的 URL。为避免此问题，可能需要对默认 IIS 配置进行修改，使其允许更长的 URL。

以下命令应该使用管理员权限在命令行上运行：

```
%systemroot%\system32\inetsrv\appcmd.exe set config
  /section:system.webServer/security/requestFiltering
  /requestLimits.maxQueryString:"6044"
  /commit:apphost
```

证书模板

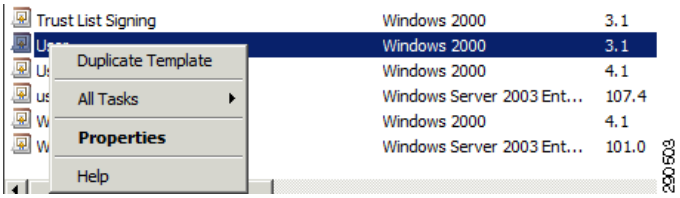
数字证书可以用于各种目的，例如服务器身份验证、安全电邮、文件系统加密和客户端身份验证。所以，为客户端颁发符合其用途的证书至关重要。例如， Web 服务器可能需要用于服务器身份验证的证书。同样，普通客户端需要主要可用于客户端身份验证的证书。因此，需要有证书模板，才便于根据用户的特定需求正确分发证书。在此解决方案中， Microsoft Windows 2008 CA 服务器中创建了安全模板，以便用户能够获得适当的证书。本节介绍在 Windows CA 服务器中设置证书模板的重要步骤以及用户需要执行的特定操作。

有关证书模板的详细信息，请参阅：
http://technet.microsoft.com/en-us/library/cc730826%28WS.10%29.aspx。

终端使用 SCEP 作为协议从 CA 服务器获取其数字证书。终端向 ISE 发送证书请求，ISE 将请求转发给 CA 服务器。ISE 被配置为 SCEP 代理，以处理这些请求， CA 服务器颁发证书后， ISE 将证书发送回客户端。“User”模板的属性会被使用。这是 Microsoft Server 2008 R2 CA 服务器部署中的默认模板。 Microsoft Server 2008 R2 中的默认模板不可编辑。因此，可以创建自定义模板，让管理员更灵活地定义证书选项。本节介绍如何创建本示例中名为 “user2”的自定义模板。

第一步是从预定义模板列表中创建复制模板。图 6-39 显示了如何创建复制模板。

图 6-39　　创建重复模板

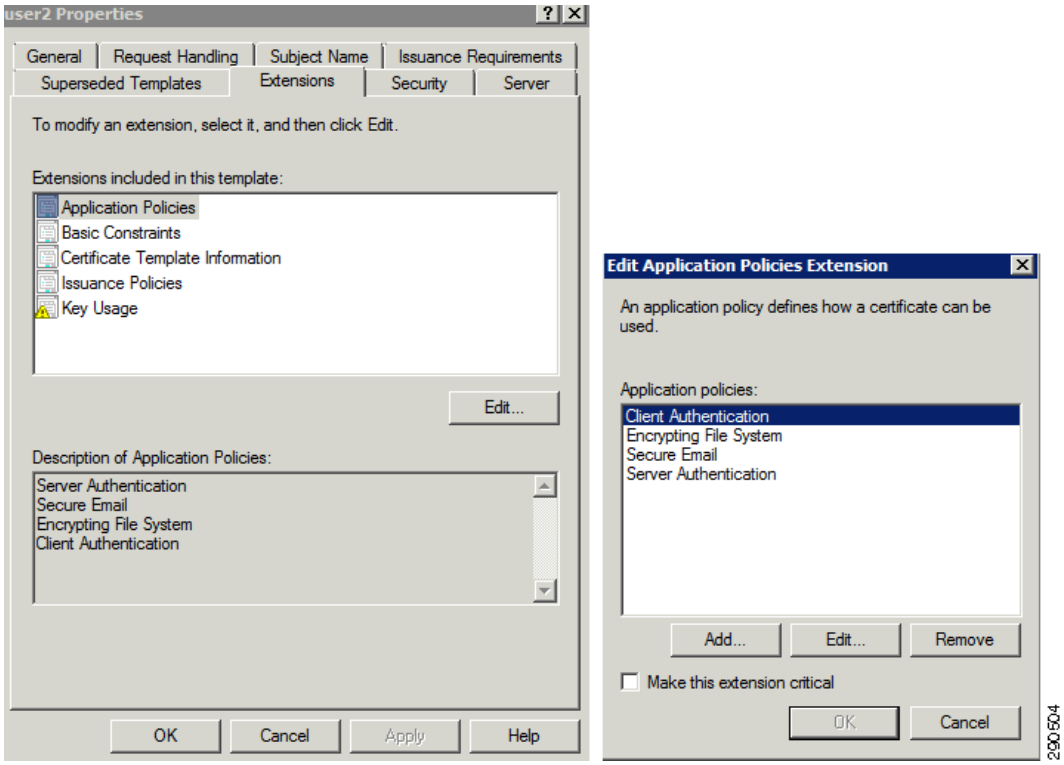


复制默认 “User”模板并重命名为 “user2”。然后，将 “user2”模板用于自动注册 AnyConnect VPN 客户端，客户端证书使用此新建模板。

下一步是配置由此 “user2”模板衍生的证书的扩展项。 EKU 扩展项和扩展的属性指定并限制证书的有效用途。扩展项是证书本身的一部分。它们由证书颁发者设置并且为只读。证书扩展属性是与能够在应用中设置的证书相关的值。若要获得关于扩展属性的详细信息，请参阅：
http://msdn.microsoft.com/en-us/library/aa380252%28v=vs.85%29.aspx。

图 6-40 介绍了如何配置证书的扩展属性。

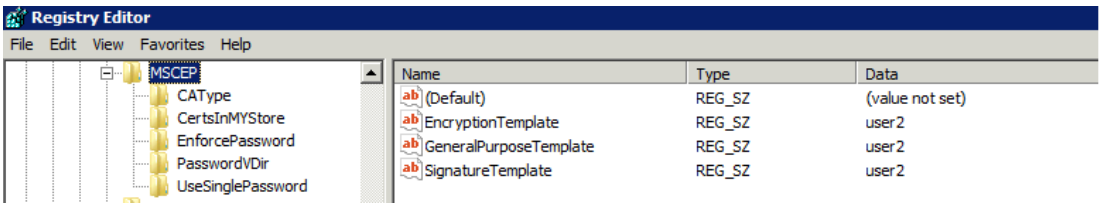
图 6-40　　配置证书的扩展属性



注意名为 “user2” 的模板。必须在注册表中设置此值，因为它对应于从 CA 服务器证书模板控制台中的 “User” 模板复制而来 “user2” 模板。

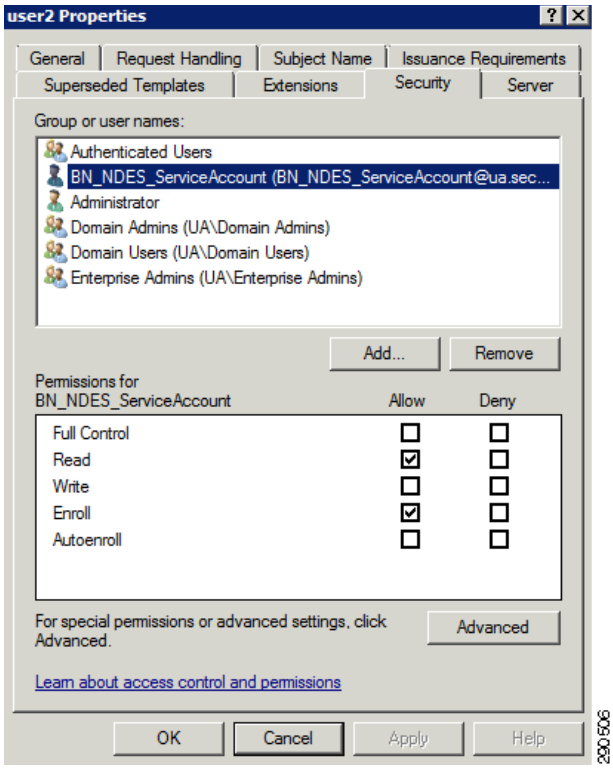
图 6-41 介绍了必须如何修改注册表设置，才能反映新创建的模板 “user2”。

图 6-41　　修改注册表



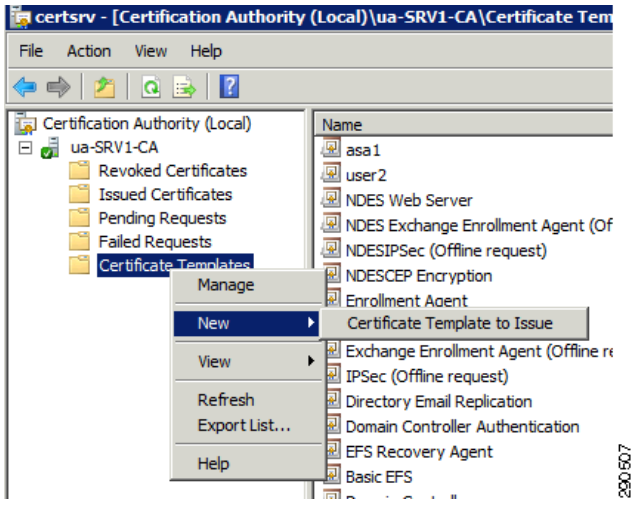
完成模板复制后，“user2” 模板中的 NDES_ServiceAccount 权限设置为 “读取和注册”。图 6-42 显示了为 “user2” 模板中的 NDES_ServiceAccount 设置的 “读取和注册” 权限。

图 6-42　　“读取和注册”权限



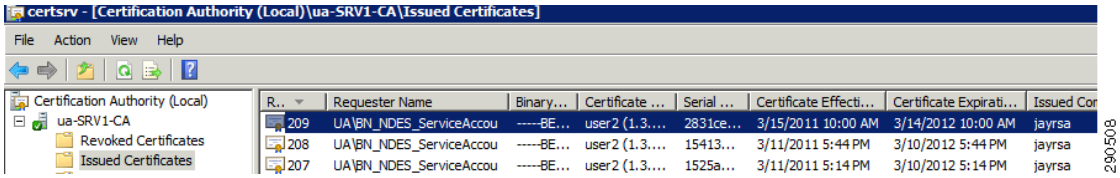
确保新创建的 “user2”模板可以通过 CA 颁发。右键点击 “user2”并选择新创建的 “User2 Certificate”，如图 6-43 所示。

图 6-43　　确保模板在 CA 中可用



现在，证书模板已经完全配置完毕，可供用户用于提交注册请求。图 6-44 显示了对用户“jayrsa”提交的 “user2”模板的成功注册请求。

图 6-44　　成功的注册请求



CA 服务器中出现一个成功的自动注册请求。请注意，请求方名称是为 “读取和注册” 权限配置的 NDES 服务帐户，而且 “user2” 证书模板已被选中。

自带设备有线基础设施设计

修订日期：2013 年 8 月 7 日

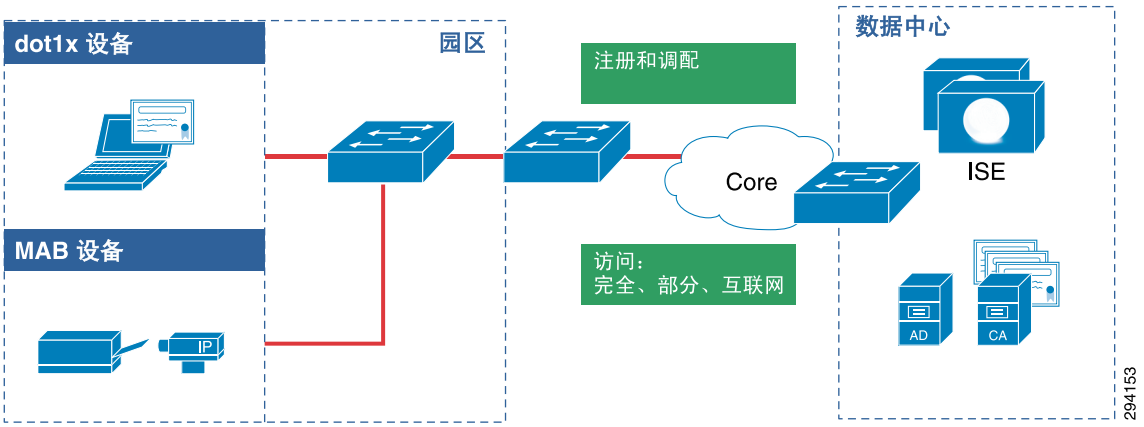
前面几节讨论了自带设备如何自注册到网络，以及如何使用无线介质为移动设备实施不同策略。本节讨论如何为有线设备设计和配置自注册和实施网络访问策略。这些设备可以位于园区位置，也可以位于分支机构位置。此外，使用融合接入层交换机或非融合接入层交换机均可以连接有线设备。本节讨论以下网络架构的设计和配置详细信息：

- 园区 （融合接入和非融合接入）
- 分支机构 （融合接入和非融合接入）

园区有线设计

在园区位置，有经过调配 / 注册过程的具有 802.1X 功能的客户端，还有打印机、摄像头等其他类型的设备 （这些设备不具备 802.1X 功能，只能提供其 MAC 地址作为其身份验证源）。这些设备也需要访问网络，此设计允许它们进行身份验证 / 授权并从 ISE 获取授权策略。图 7-1 显示了包括从园区的有线设备访问的端到端网络架构图：

图 7-1　　园区位置的有线设备的网络图



园区有线交换机的 VLAN 设计

在本文档所述的园区自带设备有线设计中，完全、部分或互联网等所有类型的 VLAN 分配是相同的。这意味着当访问端口的设备发生更改时，该端口的 VLAN 分配不会更改。例如，企业拥有的资产和个人设备将使用相同的 VLAN 编号。对于非融合接入交换机，策略实施由从 ISE 推送的 DACL 完成，而融合接入交换机中的策略实施通过使用命名 ACL （而不是 DACL）完成。要了解有关不同类型的 DACL 或命名 ACL 的详细信息，请参阅第 10 章，“BYOD 增强型使用案例 - 个人和企业设备”以下是接入层交换机的第二层接口的配置示例，该配置在集中式园区上或融合接入园区交换机上是相同的：

```
interface GigabitEthernet1/0/2
 switchport access vlan 42   !VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

园区有线基础设施的 IP 地址设计

在本设计指南中讨论的园区有线网络设计中，接入层交换机只执行第 2 层功能。聚合交换机执行第 3 层路由。以下是第 3 层聚合交换机的部分配置的示例：

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end

ua31-6500-1#
```

如上所见，使用 ip-helper address 命令对第 3 层接口进行配置，以帮助客户端获取 IP 地址。在本设计指南中， DHCP 服务器位于数据中心内。

园区中有线设备的策略实施

对于园区内的有线设备，策略实施主要通过 ACL 在接入层交换机上完成。使用两个不同的 ACL 组：

- 用于管理设备的 ACL - 这些 ACL 用于调配设备或管理设备 （如列入黑名单）。
- 主要用于实施策略的 ACL。

在园区非融合接入交换机中，策略实施是通过根据授权策略在 ISE 中定义 DACL 并将该 DACL 推送到接入层交换机上的端口来完成的。在融合接入交换机中，策略实施是通过 ISE 根据授权策略发送命名 ACL 来完成的。必须提前在融合接入 Catalyst 3850 交换机上配置命名 ACL。要获取有关本设计指南中使用的授权配置文件的详细信息，请参阅第 10 章，“BYOD 增强型使用案例 - 个人和企业设备”。

园区接入层交换机的 ACL 设计

本节讨论的 ACL 组用于在网络上调配设备、防止未经授权的访问和将设备加入黑名单。本节讨论的 ACL 既适用于融合接入层交换机，也适用于非融合接入层交换机。表 7-1 摘要显示了这些 ACL 及其用途。

表 7-1　　园区 ACL 和用途

ACL 名称	适用对象	用途
ACL-DEFAULT	接入层交换机	防止未经授权的访问通过交换机端口
ACL_Provisioning	ISE	允许终端访问完成自注册过程
ACL_Provisioning_Redirect	接入层交换机	重定向由访问网络的新设备发起的网络流量。此 ACL 是接入层交换机上存在的一个命名 ACL。
ACL_BLACKHOLE_Redirect	接入层交换机	重定向由黑名单中的设备发起的网络流量

ACL-Default - 此 ACL 在接入层交换机上配置并用作端口上的默认 ACL。其用途是防止未经授权的访问。在 802.1X 身份验证 / 授权方案中，在对设备进行身份验证和授权后，如果没有 DACL 应用于端口或者可下载的 ACL 的语法存在错误，则交换机会拒绝 ISE 发送的 DACL，而且 ACL-DEFAULT 保护在上述方案中的端口。在融合接入设计中，ACL 是在 Catalyst 3850 交换机上配置的命名 ACL。ISE 发送要在端口上应用的 ACL 的名称。同样，如果交换机拒绝 ISE 发送的命名 ACL， ACL-DEFAULT 会保护该端口。

园区接入层交换机上默认 ACL 的示例如下所示：

```
Extended IP access list ACL-DEFAULT
    10 permit udp any eq bootpc any eq bootps log (2604 matches)
    20 permit udp any host 10.230.1.45 eq domain
    30 permit icmp any any
    40 permit udp any any eq tftp
    50 deny ip any any log (40 matches)
```

从上述输出可以看出，ACL-DEFAULT 允许 DHCP、DNS、ICMP 和 TFTP 流量，而拒绝所有其他流量。

ACL_Provisioning_Redirect - 在自注册有线设备期间使用此 ACL。 ACL 用于重定向从客户端到任何位置的 HTTP 或 HTTPS 流量，这意味着当用户打开 Web 浏览器并尝试访问任意网站时，该流量会被重定向。如下所示的示例重定向用户发起的所有网络流量。但是，可以对此 ACL 进行修改以只允许将特定流量重定向至 ISE 门户。此设计的基本假设是所有设备都必须注册到 ISE，因此当未注册的设备访问网络时，它会被重定向至 ISE。

园区交换机上 ACL_Provisioning_Redirect ACL 的示例如下所示：

```
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (43 matches)
    30 deny ip any host 10.225.42.15 (27 matches)
    40 permit tcp any any eq www (30 matches)
    50 permit tcp any any eq 443 (240 matches)
```

ACL_BLACKHOLE_Redirect - 此 ACL 用于将已列入黑名单的设备重定向至 ISE 门户，以告知用户正在使用的设备已列入黑名单。此 ACL 类似于 ACL_Provisioning_Redirect ACL。

园区交换机上的 ACL_BLACKHOLE_Redirect 示例如下所示：

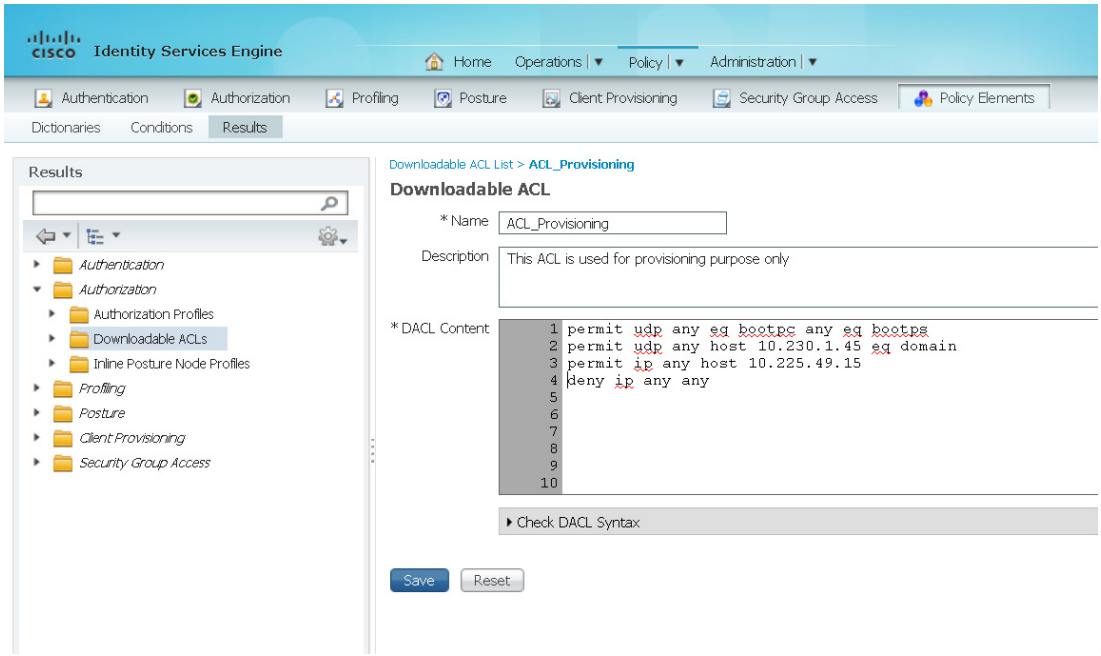
```
Extended IP access list ACL_BLACKHOLE_Redirect
    10 deny udp any eq bootpc any eq bootps
    20 deny udp any host 10.230.1.45 eq domain
    35 deny ip any host 10.225.49.15
    40 permit ip any any
```

注意　融合接入层交换机使用相同的 ACL_BLACKHOLE_Redirect 来重定向列入黑名单的有线设备。

调配 ACL

在自注册有线设备期间也使用此 ACL。此 DACL 是从 ISE 下载的，并限制只能访问 ISE、DNS 和 DHCP 服务器。此 ACL 在 ISE 上定义，如图 7-2 中所示。

图 7-2　　ACL_Provisioning



注意　ACL_Provisioning ACL 也用于融合接入层交换机。

园区交换机的 802.1X 和 AAA 配置

在本设计指南中， Cisco Catalyst 交换机用于为最终用户提供到网络的以太网连接。接入层交换机对客户端设备启用 802.1X 身份验证，并使用 RADIUS 协议与身份服务引擎进行交互。根据身份验证过程的结果，可能允许用户使用 VLAN 分配和可下载的访问控制列表 (DACL) 对网络进行有限制的访问或完全访问。下述灵活身份验证配置允许使用 802.1X 和 MAC 身份验证旁路 (MAB) 作为回退机制。灵活身份验证适用于不支持 802.1X 的设备 （如打印机）。

本节讨论在园区接入层交换机上启用 AAA 的配置详细信息，这些交换机可以是融合接入层交换机，也可以是非融合接入层交换机。

对园区交换机上的 AAA 配置接入交换机需要执行以下步骤：

步骤 1　启用身份验证、授权和记帐 （AAA）：

```
ACL(config)# aaa new-model
```

步骤 2　为 802.1X 创建一种身份验证方式 （默认对身份验证使用所有 RADIUS 服务器）：

```
ACL(config)# aaa authentication dot1x default group radius
```

步骤 3　为 802.1X 创建一种授权方法 （为策略实施启用 RADIUS）：

```
ACL(config)# aaa authorization network default group radius
```

步骤 4　为 802.1X 创建一种记账方法 （提供有关与 ISE 的会话的更多信息）：

```
ACL(config)# aaa accounting dot1x default start-stop group radius
```

为 RADIUS 配置接入交换机需要执行以下步骤：

步骤 1　将 ISE 服务器添加到 RADIUS 组：

```
ACL(config)# radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key
shared-secret
```

步骤 2　配置 ISE 服务器无响应时间 （总计 15 秒，即 3 次重试，每次超时为 5 秒）：

```
ACL(config)# radius-server dead-criteria time 5 tries 3
```

步骤 3　将交换机配置为发送特定于思科供应商的属性：

```
ACL(config)# radius-server vsa send accounting
ACL(config)# radius-server vsa send authentication
```

步骤 4　配置特定于思科供应商的属性：

```
ACL(config)# radius-server attribute 6 on-for-login-auth
ACL(config)# radius-server attribute 8 include-in-access-req
ACL(config)# radius-server attribute 25 access-request include
```

步骤 5　配置要用于提供 RADIUS 消息的 IP 地址：

```
ACL(config)# ip radius source-interface interface-name Vlan4093
```

为 802.1X 配置接入交换机需要执行以下步骤：

步骤 1　全局启用 802.1X （命令本身并不在交换机端口上启用身份验证）：

```
ACL(config)# dot1x system-auth-control
```

步骤 2　启用 IP 设备跟踪：

```
ACL(config)# ip device tracking
```

以下接口级命令对灵活身份验证启用 802.1X：

步骤 1　配置身份验证方式优先级 （dot1x 的优先级高于 MAB）：

```
ACL(config-if)# authentication priority dot1x mab
```

步骤 2　配置身份验证方式顺序 （dot1x 优先）：

```
ACL(config-if)# authentication order dot1x mab
```

步骤 3　启用灵活身份验证：

```
ACL(config-if)# authentication event fail action next-method
```

步骤 4　启用对物理端口上具有多个 MAC 地址的支持：

```
ACL(config-if)# authentication host-mode multi-auth
```

步骤 5　配置违例操作 （对可能未成功通过身份验证的其他设备限制访问）：

```
ACL(config-if)# authentication violation restrict
```

步骤 6　对 802.1X 启用端口：

```
ACL(config-if)# dot1x pae authenticator
```

步骤 7　对 MAB 启用端口：

```
ACL(config-if)# mab
```

步骤 8　配置计时器 （30 秒 (10x3)，直到回退到 MAB）：

```
ACL(config-if)# dot1x timeout tx-period 3
```

步骤 9　启用身份验证：

```
ACL(config-if)# authentication port-control auto
```

步骤 10　对端口启用 ACL-DEFAULT：

```
ACL(config-if)# ip access-group ACL-DEFAULT in
```

步骤 11　启用 http 和 https 服务器：

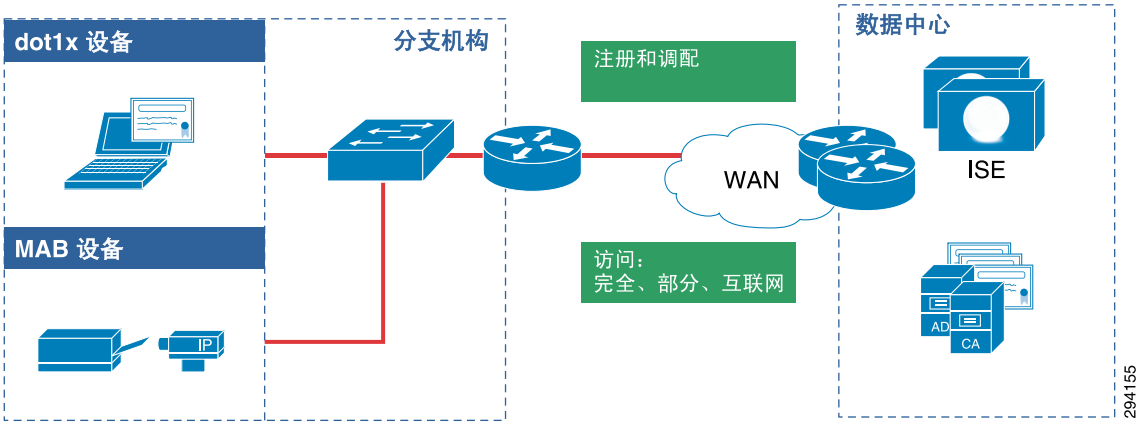
```
ACL (config)# ip http-server
ACL (config)# ip http secure-server
```

分支机构有线设计 - 非融合接入

在分支机构位置中，既有具备 802.1X 功能且经过调配 / 注册过程的客户端，也有不具备 802.1X 功能而只能提供其 MAC 地址作为身份验证源的其他设备类型，例如打印机、摄像头等。这些设备也需要访问网络，此设计允许它们进行身份验证 / 授权并从 ISE 获取其授权策略。本节讨论不部署融合接入 (Catalyst 3850) 交换机的分支机构的有线设计。本节讨论的分支机构有线设计与基于 FlexConnect 的无线分支机构设计配合使用。融合接入分支机构有线设计在分支机构有线设计 - 融合接入中讨论。

图 7-3 显示了包括从分支机构的有线设备访问的端到端网络架构图。

图 7-3　　分支机构位置的有线访问的网络图



分支机构位置的 VLAN 设计

对非融合接入分支机构位置的有线设备实施了四个 VLAN。表 7-2 列出了这些 VLAN 的名称及其用途。

表 7-2　　VLAN 及其用途

VLAN 名称	VLAN 编号	说明
Wired_Full	13	位于此 VLAN 中的设备具有对企业资源和分支机构本地服务器的完全访问权限。
Wired_Partial	14	位于此 VLAN 中的设备具有对资源的受限访问权限。
Wired_Internet	15	位于此 VLAN 中的设备只具有互联网访问权限。
Branch_Server	16	分支机构位置的本地服务器位于此 VLAN 中。

分支机构位置的 IP 地址分配

在本设计指南中讨论的非融合接入分支机构网络设计中，交换机只执行第 2 层功能，分支路由器执行第 3 层路由。因此，上述 VLAN 的所有第 3 层接口都在分支路由器上实施。以下是分支路由器的配置示例：

```
interface GigabitEthernet0/1.13
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
```

```
 ip helper-address 10.230.1.61
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
interface GigabitEthernet0/1.14
 encapsulation dot1Q 14
 ip address 10.200.14.2 255.255.255.0
 ip access-group Branch1_ACL_Partial_Access in
 ip helper-address 10.230.1.61
 standby 14 ip 10.200.14.1
 standby 14 priority 110
 standby 14 preempt
!
interface GigabitEthernet0/1.15
 encapsulation dot1Q 15
 ip address 10.200.15.2 255.255.255.0
 ip access-group ACL_Internet_Only in
 ip helper-address 10.230.1.61
 standby 15 ip 10.200.15.1
 standby 15 priority 110
 standby 15 preempt
!
interface GigabitEthernet0/1.16
 encapsulation dot1Q 16
 ip address 10.200.16.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 16 ip 10.200.16.1
 standby 16 priority 110
 standby 16 preempt
!
```

如上所见，使用 **ip-helper address** 命令对第 3 层接口进行配置，以帮助分支机构客户端获取 IP 地址。在本设计指南中， DHCP 服务器位于数据中心位置中。

分支机构中有线设备的策略实施

对于分支机构内的有线设备，策略实施主要通过 ACL 在接入层交换机上完成。使用两个不同的 ACL 组：

- 用于管理设备的 ACL - 这些 ACL 用于调配设备或管理设备 （如列入黑名单）。
- 主要用于实施策略的 ACL。

在设计分支机构的 ACL 时，应该考虑以下几点：

- 在网络中的每个分支路由器上配置静态 ACL。
- 配置 ISE 以将可下载的 ACL 推送到每个分支机构位置的接入层交换机。

表 7-3 列出了每种方法的优点和缺点。

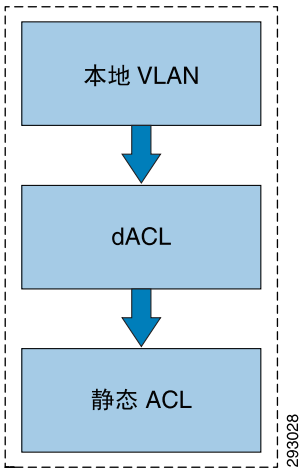
表 7-3　　ACL 策略实施

方法	优点	缺点
静态 ACL	根据分支机构的需要修改 ACL	难以单独管理每个分支机构策略
可下载的 ACL	集中访问控制	从管理角度看，为每个分支机构位置在 ISE 上创建一个单独的策略会使策略非常大。 例如，要管理 500 个不同的分支机构、 500 个 ACL、 500 个授权配置文件和 500 个授权策略规则，需要在 ISE 上定义。

上述每种方法都有优点和缺点。此设计指南重点讨论两种方法的组合。静态 ACL 是限制访问的主要方法。但是，静态 ACL 仅应用于路由器；要覆盖接入层交换机的每个端口上存在的 ACL（称为 “DEFAULT-ACL”），则从 ISE 下载一个 DACL （允许所有流量）。从 ISE 下载的此 DACL 允许流量从接入层交换机向上流到分支路由器。分支路由器预配置了用于限制访问的不同 ACL。这些 ACL 为用户提供完全、部分或互联网访问权限。

图 7-4 显示授权策略如何将 VLAN 信息和 DACL （允许所有流量）推送到接入层交换机上的端口，从而允许流量从接入层交换机到达对流量进行过滤的路由器。

图 7-4　　实施权限



分支机构位置的 ACL 设计

ACL 是实施策略所使用的主要方法，所以在分支机构位置中非常重要。在第二层交换机上定义的一些 ACL 用于调配用途，另一些则在分支路由器上定义。此外，一些 ACL 可能是从 ISE 下载的。

表 7-4 摘要显示了在分支机构位置的各种 ACL 及其用途。

表 7-4　　分支机构 ACL 和用途

ACL 名称	适用对象	用途
ACL_DEFAULT	交换机	防止未经授权的访问通过交换机端口
ACL_Provisioning_Redirect	交换机	重定向由访问网络的新设备发起的网络流量
ACL_Blackhole	交换机	重定向由黑名单中的设备发起的网络流量
ACL_Internet_Only	分支路由器	仅允许互联网流量
ACL_Provisioning	ISE	在调配过程中使用
ACL_Partial_Access	分支路由器	允许对特定资源具有部分访问权限

ACL_Default - 此 ACL 用作端口上的默认 ACL，用于防止未经授权的访问。在 802.1X 身份验证 / 授权方案中，在对设备进行身份验证和授权后，如果没有 DACL 应用于端口或者可下载的 ACL 的语法存在错误，则交换机会拒绝 ISE 发送的 DACL，而且 ACL_DEFAULT 保护在上述方案中的端口。默认 ACL 的示例如下所示：

```
bn22-3750x-1#show ip access-lists
Load for five secs: 13%/0%; one minute: 16%; five minutes: 16%
Time source is NTP, 16:24:50.872 EDT Wed Sep 19 2012

Extended IP access list ACL-DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any log
```

从上述输出可以看出，ACL_DEFAULT 允许 DHCP、DNS、ICMP 和 TFTP 流量，而拒绝所有其他流量。

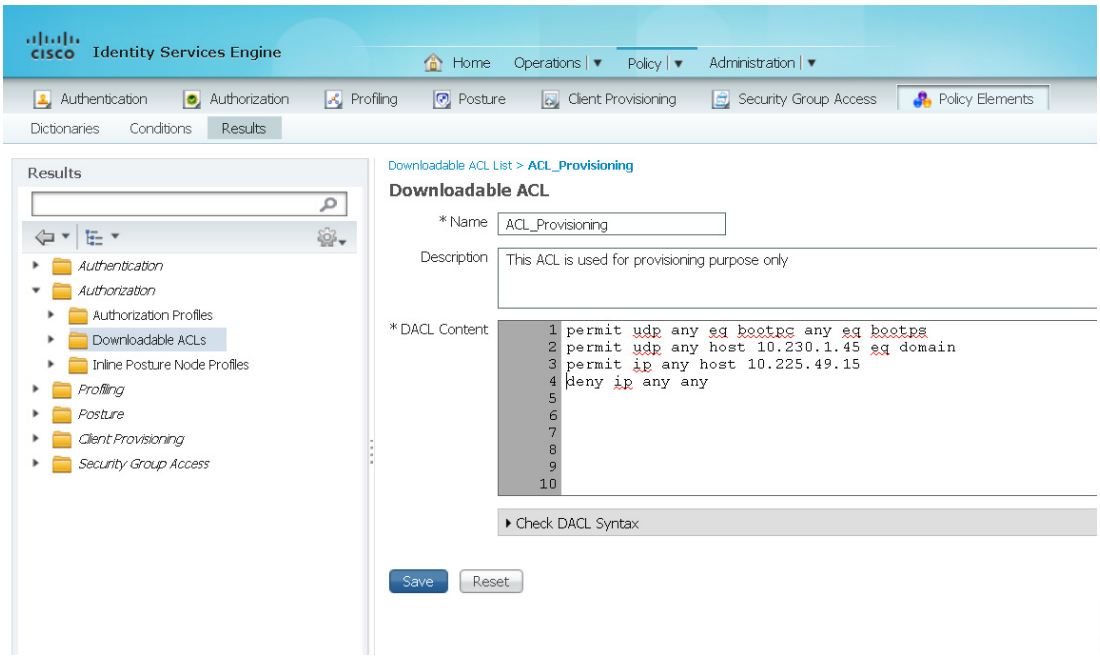
ACL_Provisioning_Redirect - 在自注册有线设备期间使用此 ACL。此 ACL 用于重定向从客户端到任何位置的 HTTP 或 HTTPS 流量，这意味着当用户打开 Web 浏览器并尝试访问任意网站时，该流量会被重定向。如下所示的示例重定向用户发起的所有网络流量。但是，可以对此 ACL 进行修改以只允许将特定流量重定向至 ISE 门户。此设计的基本假设是所有设备都必须注册到 ISE，因此当未注册的设备访问网络时，它会被重定向至 ISE。

```
uasl-3750x-1#show ip access-lists | begin ACL_Provisioning_Redirect
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (1865 matches)
    30 deny ip any host 10.225.42.15 (839 matches)
    40 deny ip any host 10.225.49.15 (1853 matches)
    50 permit tcp any any eq www (3728 matches)
    60 permit tcp any any eq 443 (4140 matches)
uasl-3750x-1#
```

调配 ACL

在自注册有线设备期间也使用此 ACL。此 DACL 是从 ISE 下载的，并限制只能访问 ISE、DNS 和 DHCP 服务器。此 ACL 在 ISE 上定义，如图 7-5 中所示。

图 7-5　　ACL_Provisioning



分支机构交换机的 802.1X 和 AAA 配置

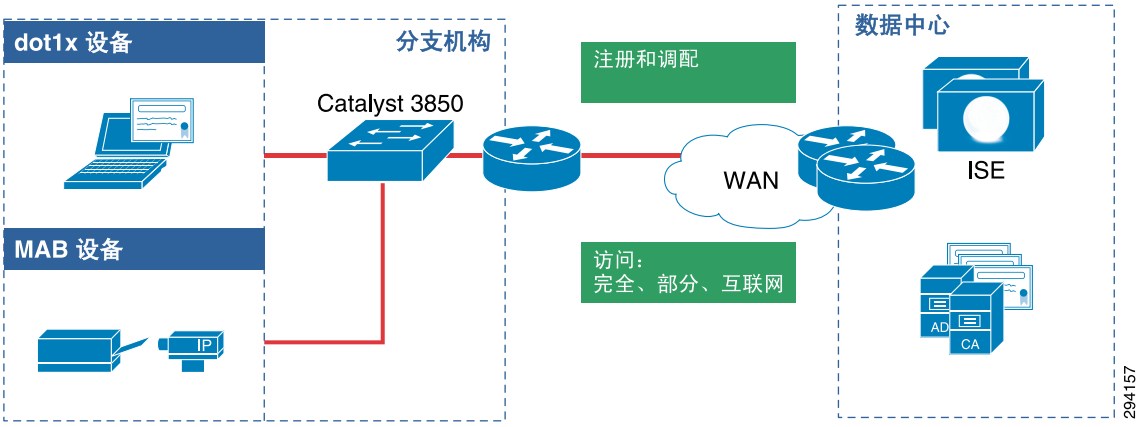
分支机构非融合接入交换机的 802.1X 和 AAA 的配置与园区交换机完全相同。请参阅园区交换机的 802.1X 和 AAA 配置了解详细信息。

分支机构有线设计 - 融合接入

在分支机构位置，有经过调配 / 注册过程的具有 802.1X 功能的客户端，还有打印机、摄像头等其他类型的设备（这些设备不具备 802.1X 功能，只能提供其 MAC 地址作为其身份验证源）。这些设备也需要访问网络，此设计允许它们进行身份验证 / 授权并从 ISE 获取其授权策略。本节讨论部署融合接入 (Catalyst 3850) 交换机的分支机构的有线设计。

图 7-6 显示了包括从分支机构的有线设备访问的端到端网络架构图：

图 7-6　　使用融合接入交换机的分支机构位置的有线设备的网络图



分支机构位置的 VLAN 设计

在本文档所述的分支机构自带设备有线设计中，完全、部分或互联网等所有类型的 VLAN 分配是相同的。这意味着当访问端口的设备发生更改时，该端口的 VLAN 分配不会更改。例如，企业拥有的资产和个人设备将使用相同的 VLAN 编号。融合接入交换机中的策略实施通过使用命名 ACL （而不是 DACL）完成。对每个设备应用不同的命名 ACL，从而授予不同的网络访问权限。因为命名 ACL 是配置在特定分支机构的 Catalyst 3850 交换机上，所以单个 Cisco ISE 策略可以在多个分支机构实施。不过，每个分支机构的 ACL 内的访问控制条目 (ACE) 对分支机构的 IP 寻址来说可以是唯一的。这会降低 Cisco ISE 策略的管理复杂性，虽然在每个分支机构 Catalyst 3850 系列交换机上配置和维护 ACL 会增加复杂性。

对融合接入分支机构位置的有线设备实施了三个 VLAN。表 7-5 列出了这些 VLAN 的名称及其用途。

表 7-5　　VLAN 及其用途 - 融合接入

VLAN 名称	VLAN 编号	说明
BYOD_Employee	10	此 VLAN 中的设备根据命名 ACL 而具有全部、部分或受限的访问权限。
BYOD_Provisioning	11	调配 VLAN。
Branch_Server	16	分支机构位置的本地服务器位于此 VLAN 中。

分支机构位置的 IP 地址分配

在本设计指南中讨论的融合接入分支机构网络设计中， Catalyst 3850 交换机只执行第 2 层功能。没有分支路由器，这一点与非融合接入的有线设计不同。以下是接入层交换机的第 2 层接口的配置示例，该配置在集中式园区上或融合接入园区交换机上是相同的：

```
interface GigabitEthernet1/0/2
 switchport access vlan 42   !VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
```

```
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

分支机构中的第 3 层连接由 ISR 路由器提供，这些路由器也用作分支机构的 WAN 连接点。以下是第 3 层路由器的部分配置的示例：

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end
```

如上所见，使用 **ip-helper address** 命令对第 3 层接口进行配置，以帮助分支机构客户端获取 IP 地址。

在使用融合接入交换机的分支机构中的策略实施

对于分支机构内的有线设备，策略实施主要通过 ACL 在接入层交换机上完成。使用两个不同的 ACL 组：

- 用于管理设备的 ACL - 这些 ACL 用于调配设备或管理设备 （如列入黑名单）。
- 主要用于实施策略的 ACL。

在融合接入交换机中，策略实施是通过 ISE 根据授权策略发送命名 ACL 来完成的。必须提前在融合接入 Catalyst 3850 交换机上配置命名 ACL。要获取有关本设计指南中使用的授权配置文件的详细信息，请参阅第 10 章，“BYOD 增强型使用案例 - 个人和企业设备”。

适用于融合接入交换机的分支机构的 ACL 设计

本节讨论两组 ACL，它们对于分支机构位置的融合接入层交换机都很重要：

- 用于调配的 ACL。
- 用于策略实施的 ACL。

表 7-6 摘要显示了融合接入分支机构有线分支机构设计中的各种 ACL 及其用途。

表 7-6　　分支机构 ACL 和用途

ACL 名称	适用对象	用途
ACL_DEFAULT	交换机	保护交换机端口
ACL_Blackhole	交换机	重定向由黑名单中的设备发起的网络流量
ACL_Internet_Only	交换机	仅允许互联网流量
ACL_Provisioning	ISE	在调配过程中使用
ACL_Partial_Access	交换机	允许对特定资源具有部分访问权限
ACL_Full_Access	交换机	对所有资源具有完全访问权限

ACL_Default - 此 ACL 用作端口上的默认 ACL，用于防止未经授权的访问。在融合接入设计中，这是通过命名 ACL 方式完成的。 ACL_DEFAULT 位于 Catalyst 3850 交换机上。

```
Extended IP access list ACL_DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any
```

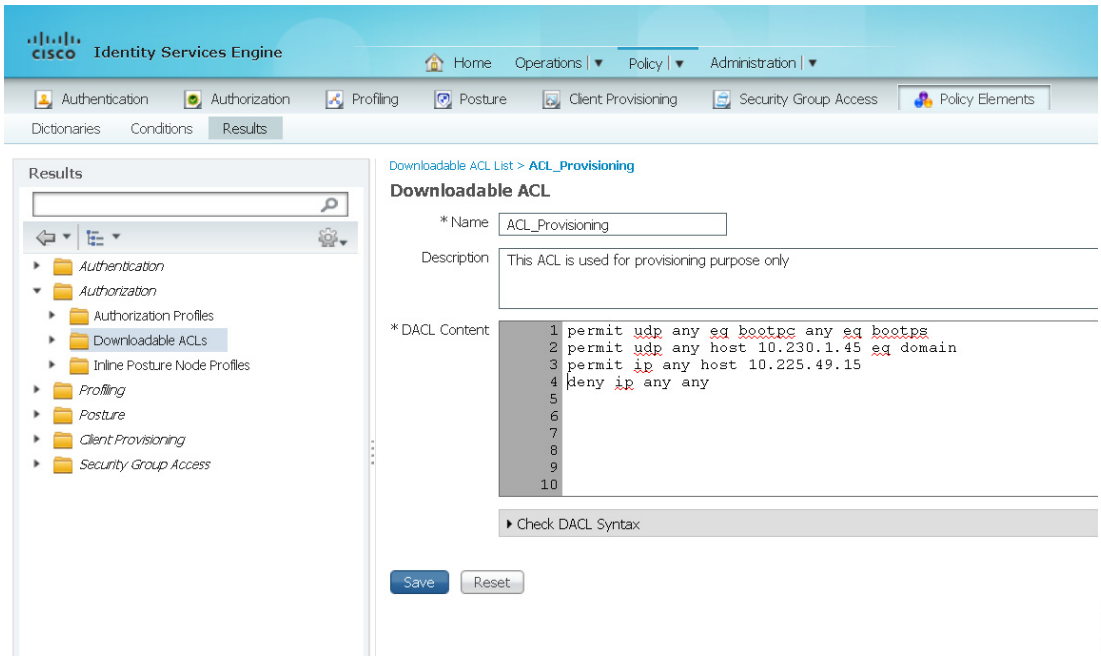
从上述输出可以看出， ACL_DEFAULT 允许 DHCP、 DNS、 ICMP 和 TFTP 流量，而拒绝所有其他流量。

ACL_Provisioning_Redirect - 在自注册有线设备期间使用此 ACL。此 ACL 用于重定向从客户端到任何位置的 HTTP 或 HTTPS 流量，这意味着当用户打开 Web 浏览器并尝试访问任意网站时，该流量会被重定向。如下所示的示例重定向用户发起的所有网络流量。但是，可以对此 ACL 进行修改以只允许将特定流量重定向至 ISE 门户。此设计的基本假设是所有设备都必须注册到 ISE，因此当未注册的设备访问网络时，它会被重定向至 ISE。

```
Extended IP access list ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit tcp any any eq www
 permit tcp any any eq 443
```

ACL_Provisioning - 在自注册有线设备期间也使用此 ACL。此 DACL 是从 ISE 下载的，并限制只能访问 ISE、 DNS 和 DHCP 服务器。此 ACL 在 ISE 上定义，如图 7-7 中所示。

图 7-7　　ACL_Provisioning



分支机构交换机的 802.1X 和 AAA 配置

分支机构交换机的 802.1X 和 AAA 的配置与园区交换机完全相同。请参阅园区交换机的 802.1X 和 AAA 配置。

分支机构或园区位置的 MAB 设备

本节讨论如何使用融合接入交换机或传统接入层交换机设计 MAB 设备的访问。MAB 设备可以存在于分支机构或园区位置。

MAB 设备通常指无法运行 802.1X 而只能提供其 MAC 地址进行身份验证的设备。请注意，自带设备在调配过程中也使用 MAB 协议。在调配过程中，自带设备被重定向至 ISE 访客门户以完成注册过程。MAB 设备无需注册，因此不需要重定向。对 MAB 设备的要求是对设备进行身份验证并应用授权策略。以下是对 MAB 设备需要执行的概要步骤：

1. 配置接入层交换机端口或 WLC 以支持 MAB 协议。
2. 将所有 MAB 设备的 MAC 地址列表作为一个身份组导入 ISE 中。
3. 配置有线和无线 MAB 设备的身份验证策略。在调配过程中，将使用此同一策略对自带设备进行身份验证。
4. 对有线和无线设备在 ISE 中配置授权策略规则。

当 MAB 设备连接时，接入层交换机使用设备的 MAC 作为身份验证源将身份验证请求发送至 ISE。示例如下所示。

```
Sep 25 11:09:50.741: %DOT1X-5-FAIL: Authentication failed for client (0050.568f.
1bb2) on Interface Gi1/0/10 AuditSessionID 0AC81304000000221292C2D59
Sep 25 11:09:50.741: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
 'dot1x' for client (0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC813
0400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-7-FAILOVER: 从客户端的 “dot1x” 发生故障切换
0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC81304000000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-5-START: 对客户端启动 “mab” (0050.568f.032b
) on Interface Gi1/0/10 AuditSessionID 0AC81304000000221292C2D59
```

在此设计中， MAB 设备的所有 MAC 地址都在名为 MAB_DEVICES 的内部身份组中，因此 ISE 会提前知晓此设备。要将新 MAC 地址添加到 MAB_DEVICES 身份组，请点击 **Administration > Groups > Endpoint Identity Groups**，如图 7-8 中所示。

图 7-8　　MAB_DEVICES 身份组

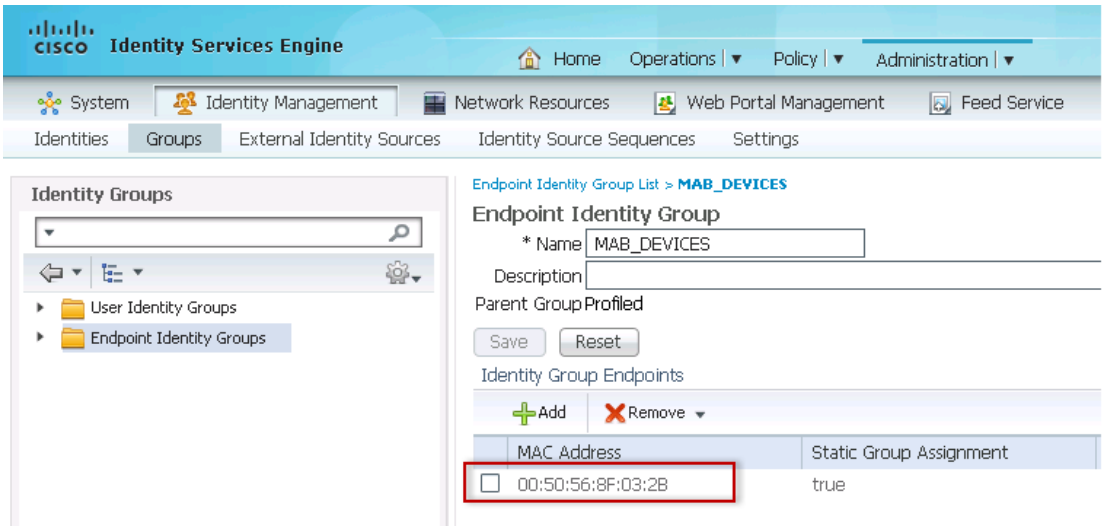
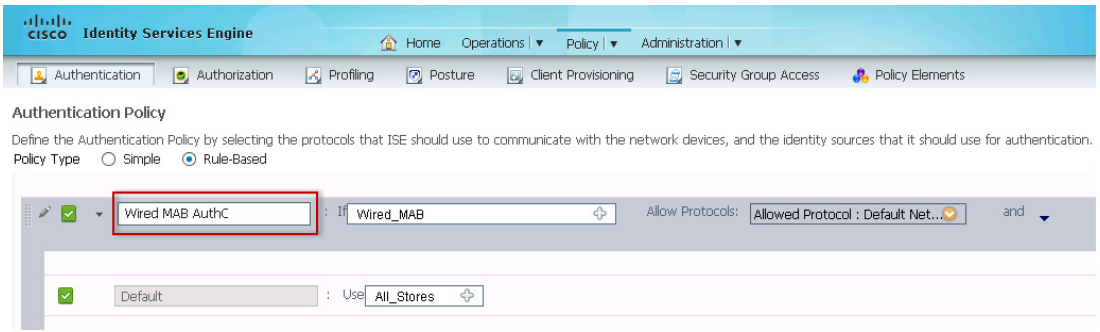


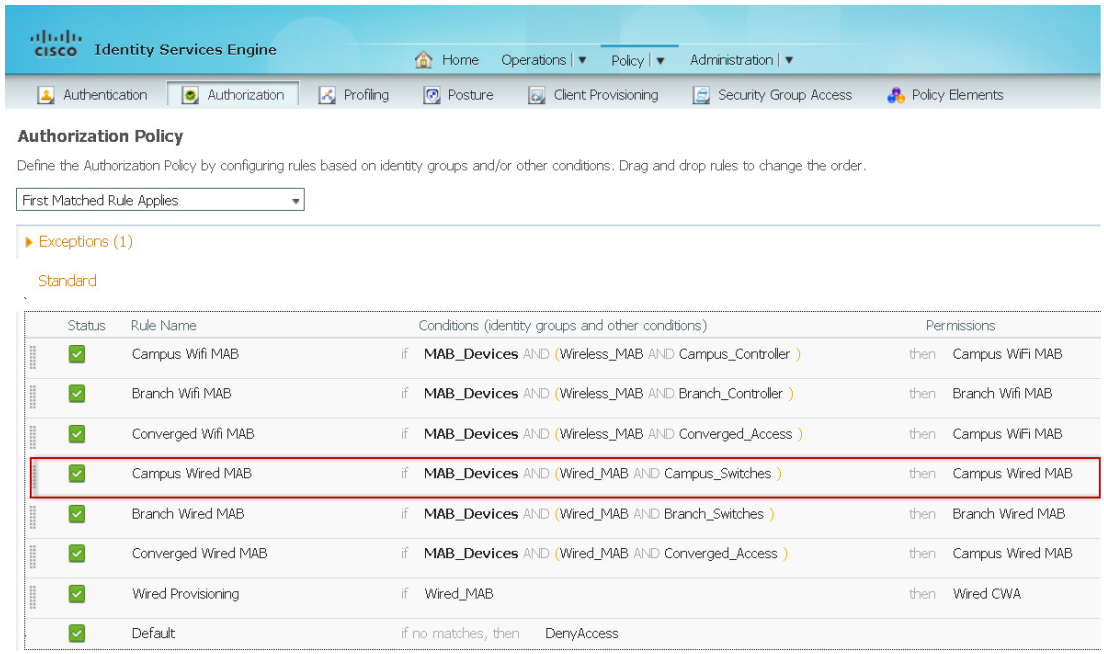
图 7-9 显示了在有线 MAB 设备的 ISE 上定义的身份验证策略。

图 7-9　　有线 MAB 身份验证



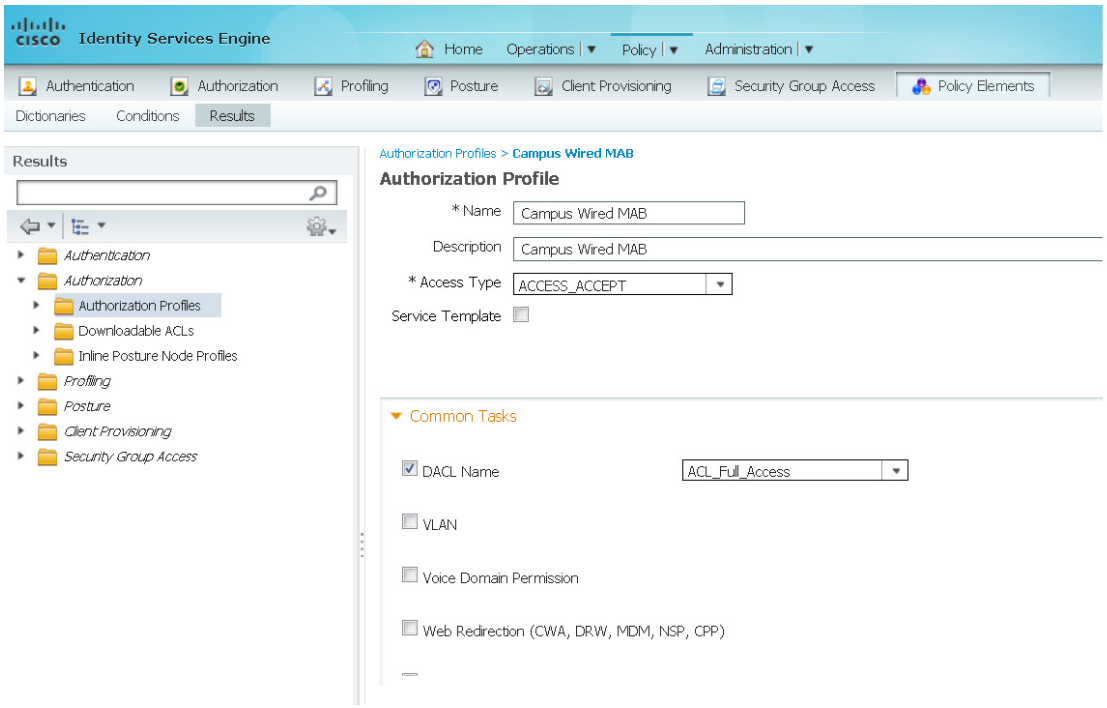
采用 FlexConnect 的分支机构设计中的 MAB 设备的授权策略与在园区位置中不同。在采用 FlexConnect 模式的身份验证设计中，每个设备都位于不同的 VLAN 中，但在具有融合接入的园区中或分支机构设计中并非如此。因此，对于分支机构位置与园区位置中的设备，分别在授权策略中定义不同的规则。图 7-10 显示了如何为园区设备定义策略规则。

图 7-10　　MAB 设备的授权策略



园区有线 MAB 是一个授权配置文件，该配置文件将适当的设置推入接入层交换机。图 7-11 显示了授权配置文件的详细信息。

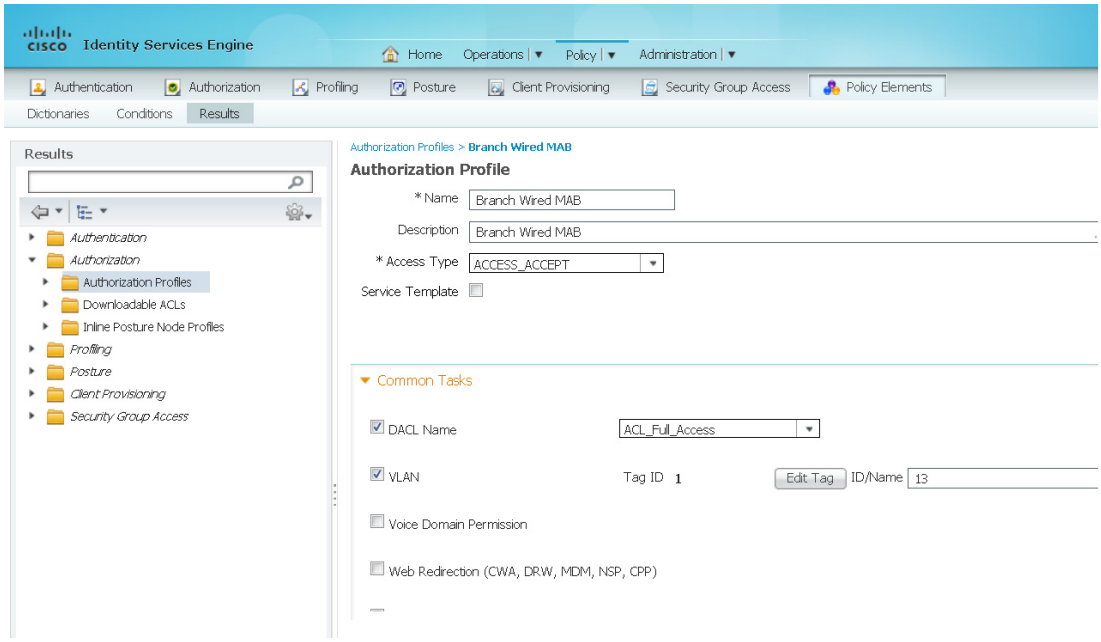
图 7-11　　园区有线 MAB 授权配置文件



园区有线 MAB 授权配置文件不推送 VLAN 信息，而是将一个 DACL 应用于端口。融合接入设计使用同一授权配置文件，如图 7-11 中所示。另请注意，在使用授权配置文件的融合接入设计中，DACL 同时用于园区和分支机构设计。

相反，对于具有 FlexConnect 的分支机构设计， Branch_Wired_MAB 授权配置文件将 VLAN 信息推送到有线交换机上的接入端口。图 7-12 显示了 Branch_Wired_MAB 配置文件配置。

图 7-12　　Branch_Wired_MAB 授权配置文件



融合接入分支机构设计也对 MAB 设备使用相同的授权配置文件，如图 7-12 中所示。

自带设备的安全组访问

修订日期：2013 年 8 月 7 日

以下小节介绍了此 CVD 中使用的基础设施，并概述了两种用于实施基于安全组标记的策略的部署方案。两种部署方案并不互相排斥，并能结合使用以满足企业的需求。此外，还提供了基础设施的详细配置信息。

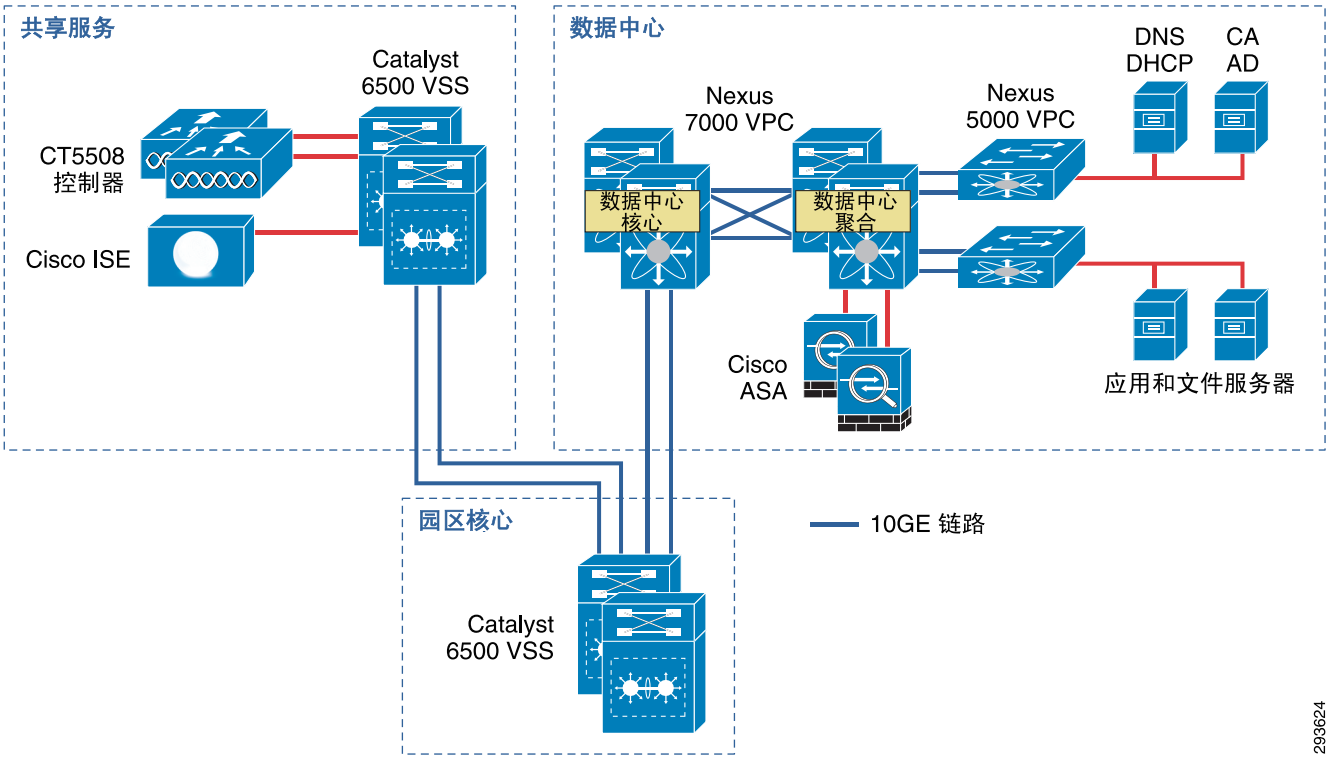
支持 SGA 的统一基础设施设计

如第 3 章，“BYOD 的园区网络和分支机构网络设计”中的本 CVD 中的 SGT 部署方案中所述，此 CVD 中考察了两种具体的基础设施部署方案。第一个用例使用在身份服务引擎上定义的 SGA 策略，产生的 SGACL 与 Catalyst 6500 和 Nexus 7000 基础设施进行动态交换。第二个用例也使用在身份服务引擎上定义的 SGA 策略，但通过配置在 ASA 上定义的安全组防火墙 (SG-FW) 策略实施该策略以提供对数据中心资源的安全访问。

在这两种方案中，通过针对本地模式配置的集中式 CUWN CT5508 控制器连接的园区无线用户 / 设备，可根据其授权角色和使用在这两种部署方案中实施的基于 SGT 的策略来访问数据中心资源。

图 8-1 描述了用于在 CVD 内进行 SGA 验证的基础设施。

图 8-1　　自带设备 v2.5 CVD 的 TrustSec 基础设施

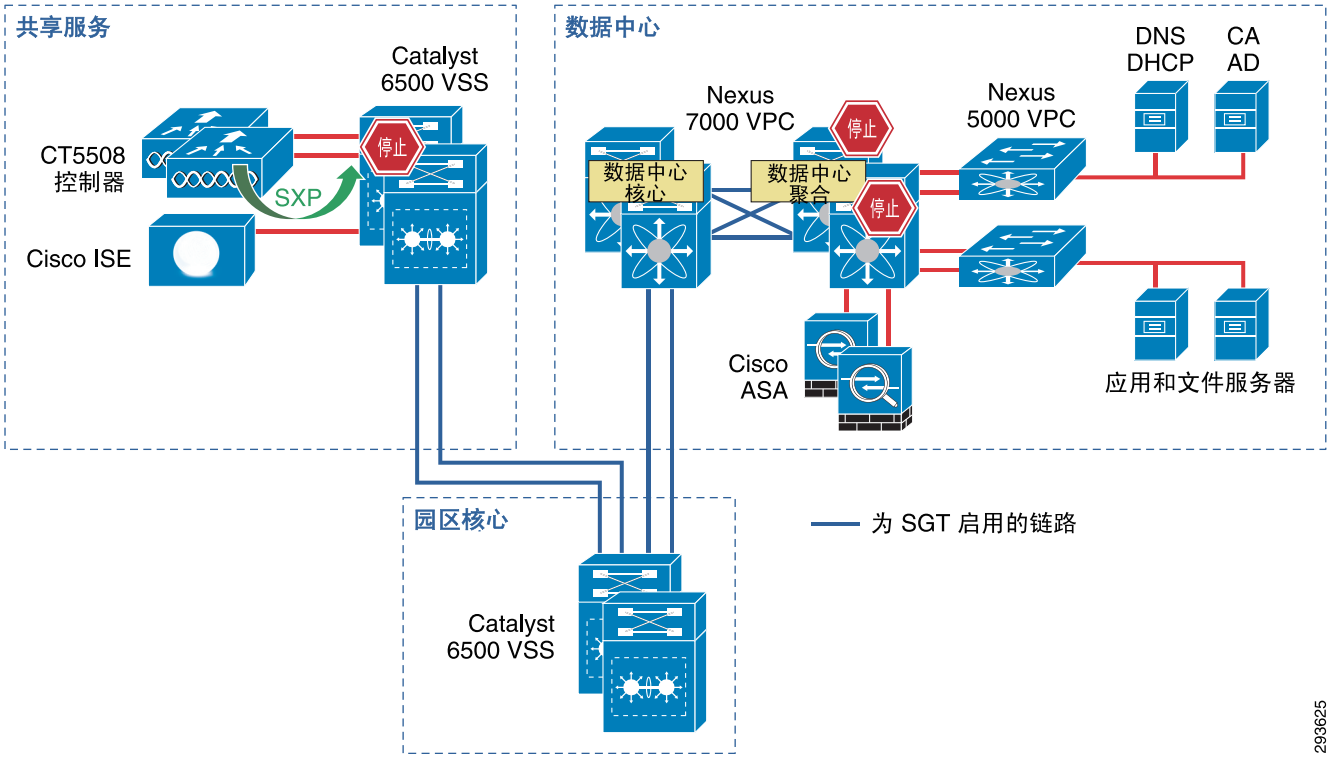


在图 8-1 中，共享服务中的 Catalyst 6500 VSS 与核心中的 Catalyst 6500 VSS 之间的链路以及到 Nexus 7000 的链路都是 10GE 链路。在 Catalyst 6500 上，具有 FourX 适配器的 WS-X6904 线路卡提供 10GE 接口，而 N7K-M108X2-12L 线路卡提供 Nexus 7000 接口。Nexus 7000 和 Nexus 5548 之间的链路以同样的方式连接到 N7K 上的 N7K-M108X2-12L 线路卡和 Nexus 5548 上的 10GE 端口。无线控制器、 ASA 防火墙、 ISE 和其他服务器的所有其他网络连接均为 1GE 链路。

方案 1 中 SGACL 的策略配置

对于部署方案 1，请参阅图 8-2。

图 8-2　　基础设施部署方案 1 SGT 实施



在部署方案 1 中，需要将安全组标记从共享服务 Catalyst 6500 VSS （在这里连接无线控制器）通过自带设备基础设施的核心转发到位于适当数据中心内的服务器。在图 8-2 中，以蓝色显示的链路将针对 SGT 转发进行配置，并针对 802.1ae MACsec 加密进行手动配置。如前所述，CT5508 无线控制器不支持在其 1GE 接口上进行本地标记，因此将按上图所示在控制器和共享服务 C6500 VSS 交换机之间定义安全组标记交换协议 (SXP) 连接。

在这第一种方案中，无线用户在成功经过身份验证和授权后将与特定角色相关联，同时，无线控制器将使用设备的 IP 地址和相应的 SGT 创建一个 IP 地址与 SGT 的映射。此映射将通过 SXP 告知无线控制器所连接的共享服务 Catalyst 6500。当无线用户流量流出共享服务 Catalyst 6500 时，将被标记上通过 SXP 从无线控制器获悉的相应 SGT。当此流量穿越支持 SGT 的核心时，此标记将以逐跳路由方式传播到 Nexus 7000，即各种服务器所在的数据中心的交换基础设施。

因为对位于 Nexus 数据中心基础设施中的服务器进行身份验证时不采用 802.1X，所以服务器 IP 地址与 SGT 的映射既可以在 Nexus 7000 数据中心聚合交换机上手动定义，也可以在 ISE 服务器上手动定义，后者随后会将该映射提供给 Nexus 7000。对于本 CVD 而言，这些映射已在 Nexus 7000 数据中心聚合交换机上手动定义。如第 3 章，“BYOD 的园区网络和分支机构网络设计”中的本 CVD 中的 SGT 部署方案中所述，还可以采用其他方法将流量与 Nexus 7000 平台上的特定 SGT 相关联。

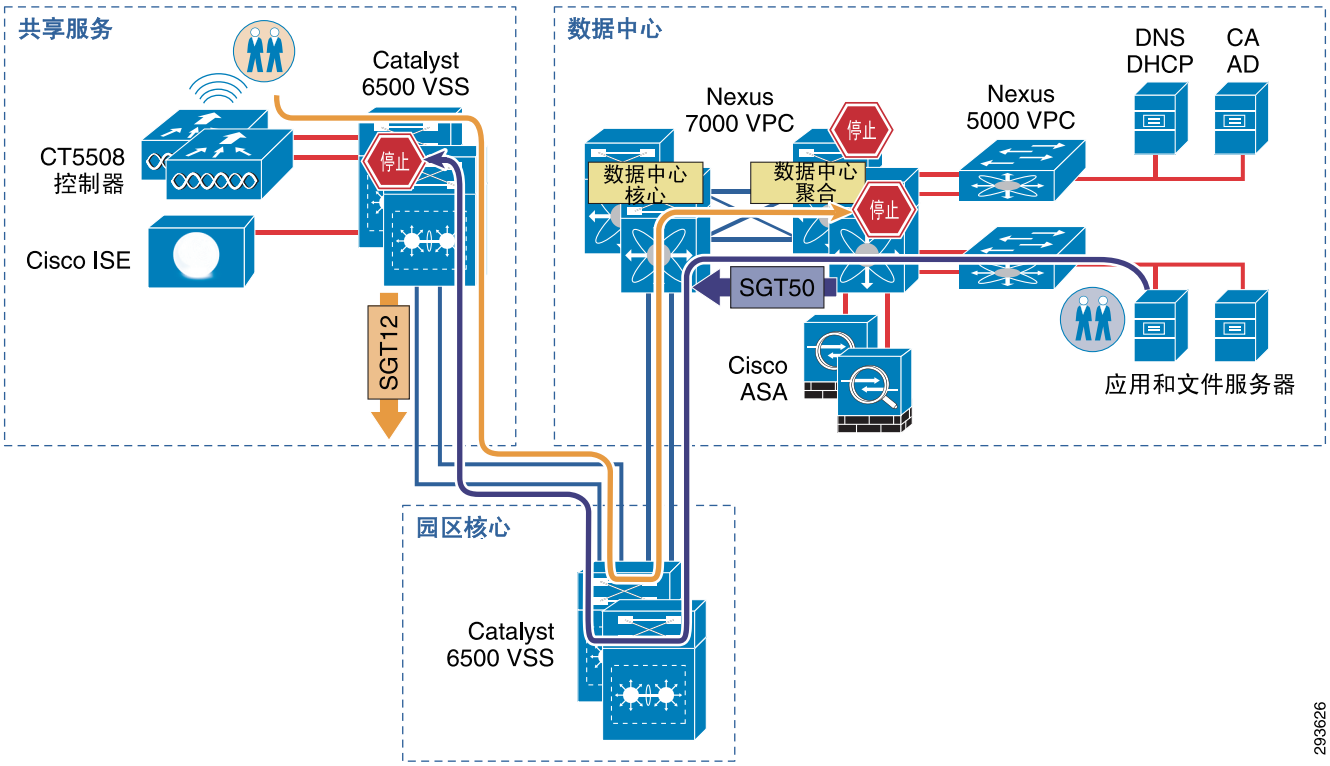
当带有标记的用户数据流量到达 Nexus 7000 数据中心交换机 （在该交换机上已创建服务器的手动 SGT 映射）时，流量将匹配在 ISE 上集中定义的 TrustSec 策略 (SGACL) 或在本地定义的策略 (SGT0) （如果目标未知），并根据情况进行转发或丢弃。

如前所述，所有的服务器 IP 与 SGT 映射都已在 Nexus 7000 聚合交换机上手动创建。当服务器连接到图 8-3 中所述的 Nexus 5548 交换机时，从 Nexus 5548 流出的流量不带有标记，因为尚未在其中创建映射。在此流量流经 Nexus 7000 聚合交换机后，将检查常驻 SGT 映射，并对从该聚合交换机出口流出的流量施加相应的 SGT。如果流量由与数据中心内某个与 SGT 相关联的服务器发起，则带有标记的流量会流出 Nexus 7000 数据中心交换机，穿越核心和共享服务基础设施并在通

往目标的每个跳跃路由上传播 SGT，该目标即与共享服务 6500 连接的无线控制器。在流量到达共享服务 6500 后，流量将与 TrustSec 策略 (SGACL) 进行匹配，然后根据具体情况确定是转发还是丢弃。

图 8-3 描述了将在统一接入基础设施的哪个位置实施 SGACL。

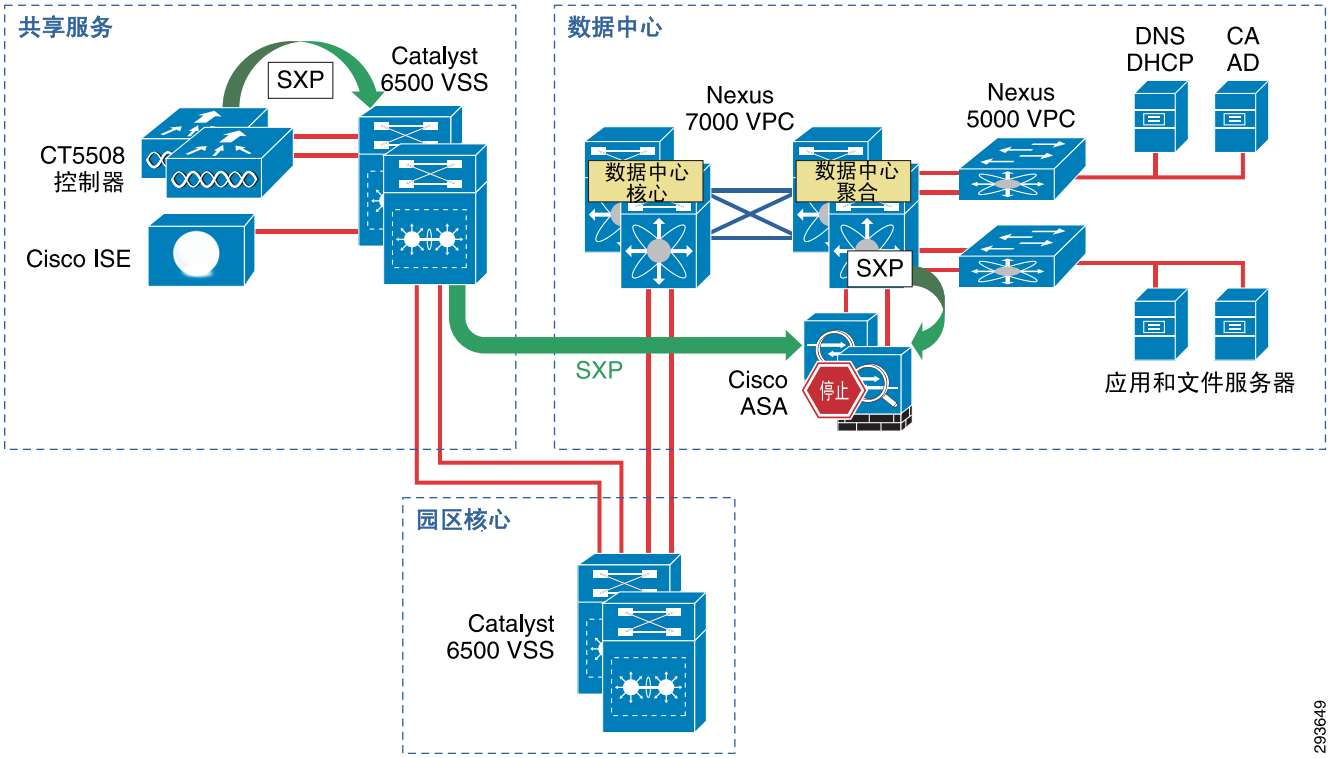
图 8-3　　部署方案 1 中的策略实施



方案 2 中的策略配置

对于部署方案 2 中使用的拓扑，请参阅图 8-4。

图 8-4　　部署方案 2 配置



部署方案 2 使用一种不同于 SGACL 的方法来实施 SGA 策略。在方案 2 中，运行版本 9.0 的 ASA 将用作安全组防火墙 (SG-FW)，保护数据中心资源免遭非法的外部访问。由于 ASA 当前不支持在其以太网接口上进行本地 SGT 标记，必须对其使用 SXP 以便从网络中已动态获悉或静态配置的其他区域获悉 IP/SGT 映射。

与在第一种部署方案中一样，无线用户在成功经过身份验证和授权后将与特定角色相关联，并会使用设备的 IP 地址和相应的 SGT 在无线控制器上创建 IP 地址与 SGT 的映射。安全组标记交换协议 (SXP) 用于将此映射告知无线控制器所连接的共享服务 Catalyst 6500。

然而，与方案 1 不同，此方案不需要启用共享服务 Catalyst 6500 VSS 和数据中心之间的 10GE 基础设施来支持安全组标记或 SGACL。相反，将使用 SXP 来将共享服务 Catalyst 6500 VSS 从无线控制器获悉的映射重新广告给 ASA 防火墙。

从无线控制器使用多跳 SXP 配置的主要原因是：对于网络中其他位置的单一广告，在共享服务中的 6500 VSS 交换机上集中管理所有的控制器 SXP 广告可以提供更简便的管理方式；完全可以在无线控制器和 ASA 防火墙之间创建 SXP 对等连接。唯一的其他注意事项是在本指南中使用的 WLC-5508 控制器以及 WiSM2 仅支持四个 SXP 连接，而 6500 的支持能力远超过此范围。

除了共享服务 6500 和 ASA 之间的 SXP 对等连接之外， Nexus 7000 聚合交换机还需要一个 SXP 对等连接来广告在这些交换机上配置的 SGT 映射。借助这些 SXP 广告， ASA 能够检查来自多个设备的流量并关联适当的标记来进行后续 SG-FW 策略实施，因为 ASA 的接口无法感知 TrustSec 且无法操作 SGT。

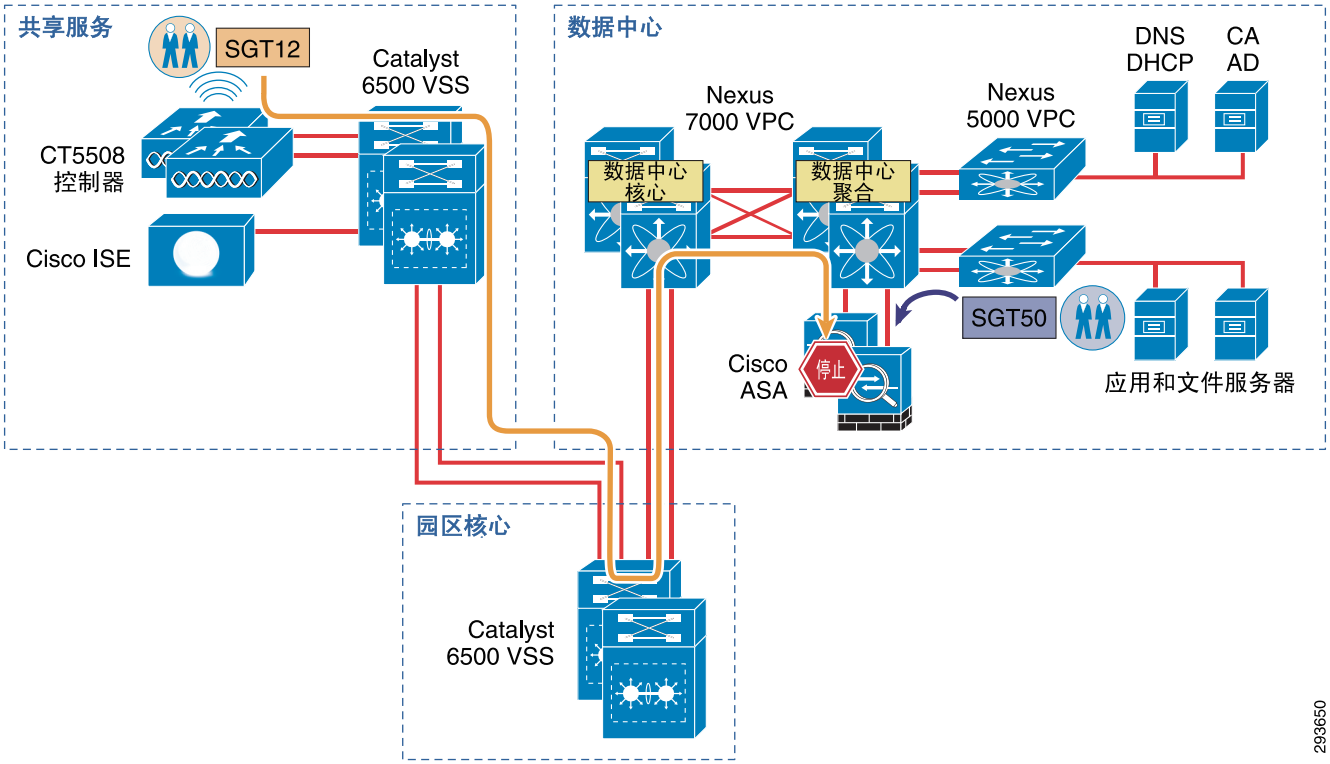
如前所述，必须对将用于实施 SG-FW 策略的 ASA 防火墙手动配置 SGT 策略，因为目前在 ASA 中不支持网络设备准入控制 (NDAC)，从而也无法从 ISE 动态获取这些策略。

当无线流量流出共享服务 Catalyst 6500 并到达数据中心时，这些流量将被取消标记并直通核心，进入数据中心交换基础设施并最终到达将实施适当 SG-FW 策略的 ASA 防火墙。

来自数据中心中某个服务器的流量在流出 Nexus 7000 聚合交换机出口时，同样会被取消标记并转发到将实施适用的 SG-FW 策略的 ASA 防火墙。

图 8-5 描述了在部署方案 2 中使用的基础设施和用于实施安全组策略的方法。

图 8-5　　使用 SXP 和 SG-FW 的 SGA 策略实施



TrustSec 摘要

有关特定平台的配置步骤的详细信息，请参阅 TrustSec 部分。

注意　**必须**安装 ISE 1.2 的补丁 1 以便网络设备和 ISE 之间的 NDAC（网络设备准入控制）正常运行。如果未安装补丁 1，则在配置了 CTS 手动模式时，网络设备将无法用 ISE 进行身份验证以获得 TrustSec 环境数据、PAC 文件和安全组策略；在配置了 CTS Dot1x 模式时，网络设备无法获得对对等 /TrustSec 链路进行身份验证所需的凭证。请参阅 ISE 1.2 版本说明，了解有关此**重要信息的**详细信息。

BYOD 的移动设备管理器集成

修订日期：2013 年 8 月 7 日

Cisco ISE 可以配置为通过基于 XML 的 API 与第三方移动设备管理器 (MDM) 产品集成。这样可根据移动设备状态制定网络决策，其中状态可能涉及到 PIN 锁、存储加密或注册状态。本版本的 Cisco ISE 支持 Apple 和 Android 设备。配置基础设施来支持此项功能包括，设置 ISE 使其向 MDM 发送 API 请求和配置 MDM 使其接受这些请求。第 4 章，“面向 BYOD 的移动设备管理器”中讨论了各种组件之间的通信问题。本节将概括介绍一些 MDM 配置，包括设备合规策略。您可以从如下地址的支持文档中查找详细的合作伙伴特定信息：http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html。

下文简要介绍了 MDM 架构通用拓扑。本节详细探讨的两种基本模式分别是内部模式和基于云的 SaaS 模式。这两种模式的组件相似，不过云模式还包括一个内部组件，以改善与企业集成的状况。

建立内部 MDM 的 IP 连接

通常，内部 MDM 驻留在 DMZ 中，或移动设备可以建立入站连接的位置。这样，设备在防火墙外部时， MDM 能够监控设备的状态。如果没有此访问权限，设备需要首先部署在网络中并进行查询，之后才能建立设备的状态合规。设备接入新网络时，不会自动更新服务器，因此查询需要企业手动启动。如果 MDM 驻留在数据中心内部，用户需要做一些调配才能接受来自互联网的入站 TCP 连接字。具体端口因 MDM 合作伙伴而异，有关详细信息请参见设计区的支持文档。

除接受来自设备的入站会话之外， MDM 需要建立指向推送服务器的出站连接。 MDM 使用推送服务定位设备，并将 MDM 策略的变更信息告知设备。 Apple 将此服务称之为 Apple 推送通知服务 (APNS)，并使用 Apple 签名证书验证 MDM 身份。 Google 则将此服务称之为 Google Cloud Messaging for Android (GCM)。这项服务取代了原来的 Cloud to Device Messaging Framework (C2DM)。 Apple 和 Android 均将推送服务融合至设备操作系统的 (OS) 中，使 MDM 服务器可与 MDM 客户端应用通信。Apple 设备还允许 MDM 借助适当的凭证与 OS MDM API 通信。这两项服务均要求最终用户创建相应的 Google 或 Apple 帐户。此帐户能够有效地将设备列表与用户绑定。

MDM 还可以托管以用户为中心的 “我的设备门户”，让用户可以登录 MDM 管理个人设备的一些信息。这一点与 ISE 提供的 “我的设备门户”类似，但两者又有严格区别，因为，前者的用途不同。用户可以从移动设备或其标准桌面进行连接。MDM Web 服务器可使用 ACL 进行配置，以限制特定源地址对 “我的设备门户”页面的访问。例如，可以阻止针对门户的互联网访问。对管理员网站同样也可以做类似配置。

默认情况下，MDM 也会接收端口 443 上的入站 HTTPS 会话来支持 ISE 使用的 API。与 MDM 位置相比， ISE 应部署在数据中心内。防火墙策略应设置为允许自 ISE 启动传向 MDM 服务器的 TCP 443 会话。 MDM 具有朝向出站防火墙的默认路由和朝向入站防火墙的更具体的 ISE 路由。

大多数 MDM 合作伙伴支持在可支持多个接口的虚拟机服务器进行内部部署。我们可以将 ISE 路由安排在专用链路上。DMZ 拓扑应符合现有的公司服务器策略。通常，利用 MDM 管理员可以借助 ACL 保护 API。在这种情况下， ACL 可以配置为允许 ISE、但拒绝所有其他连接。

ISE 支持外部连接使用代理。目前代理配置是一种全局配置。如果 ISE 需要使用馈送服务代理，那么它也会将 MDM 请求发送至该代理。这会导致 ISE 和内部 MDM 之间出现连接问题。在这种情况下，需要仔细审核代理配置，确保 ISE 可通过代理连接到 MDM。

为基于云的 MDM 建立 IP 连接

订用在线 MDM 服务可简化多个连接问题，尤其是移动设备和设备管理器之间的连接问题。由于在连接到公共互联网过程中，个人移动设备连接会占用大量时间，因此，选择此模式比传统企业内部模式更具优势。采用云模式时， Apple APNS 或 Google GCM 也能够得到简化。不过，企业仍然需要生成证书签名请求，并将此请求提供给 Apple，之后才能使用 APNS 服务。有关此问题的相关解释，请参见合作伙伴特定支持文档。然而，云部署具有一定优势的同时，在企业集成方面，特别是公司目录结构方面也面临着一些挑战。如果没有任何集成，则需要在 MDM 服务器上建立和维护独立专用的用户数据库。通常在云模式下，企业将创建一个驻留在 DMZ 中并用作代理保护 LDAP 绑定的小型集成服务器。有关此问题的相关解释，请参见合作伙伴特定支持文档。除了这一台额外的服务器外，企业内部模式中的任何其他组件在云模式中均可找到。

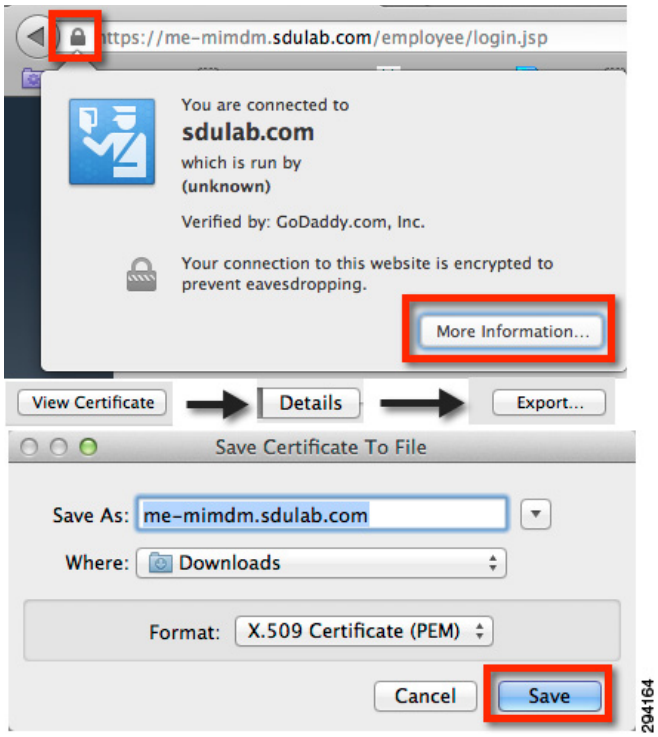
主要问题是 ISE 和基于云的 MDM 服务器之间的 HTTPS 连接（此连接从 ISE 引出）。企业防火墙应允许数据中心中的 ISE 服务器建立到 MDM 服务器的出站 HTTPS 连接。如果限制来自 ISE 等数据中心服务器的出站会话， MDM 合作伙伴可能会提供一系列目标子网。首先应将 MDM 服务器证书导入到本地 ISE 证书存储，这样 ISE 才会信任 MDM 服务器 （见下文说明）。 MDM 服务将提供 API 的 URL。在此站点上就应该导入此证书。此外，用户应能够在基于云的 MDM 服务器上建立指向 “我的设备门户”页面的出站 HTTPS 连接。这一点只有在用户不能访问互联网网站的环境中不能实现。如果使用 WCS 或 ScanSafe，则企业应确认 MDM 站点具有超过访问所需阈值的声誉得分，否则应手动将站点添加到允许的白名单。路由非常简单。 ISE 和用户设备将使用指向互联网的默认路由。会话可能会流经 NAT 边界，无需 NAT 修复。

此外，还必须为已隔离到 MDM 的移动客户端，以及 Apple 推送服务或 Google 云消息传送服务器提供连接。这样， MDM 可根据需要与设备通信，更新服务器上的设备状态信息。在某些情况下，移动客户端可能还需要访问 Google Play 和 Apple AppStore 下载所需的应用 （例如 MDM 移动客户端）。

配置 ISE 验证 MDM API

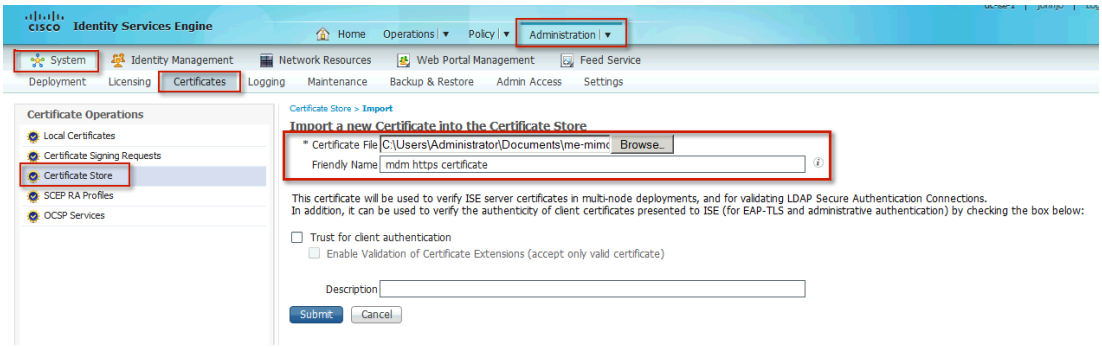
在配置 MDM 之前，ISE 必须信任 MDM 网站提供的 HTTPS 证书。在云或内部部署模式下，可通过安装 ISE 证书存储中的 MDM 的 HTTPS 证书获得信任。最简单的方法莫过于浏览 MDM 服务器，导出 HTTPS 证书，然后将其导入 ISE。图 9-1 展示了在 FireFox 中执行此操作的情况，但是，操作步骤可能与所有其他浏览器不同。

图 9-1　　导出 MDM 证书



证书保存到本地磁盘后，用户可将其导入到 ISE 的本地证书存储中。默认情况下，浏览器将使用基于证书所包含身份的名称（通常是该身份站点的 FQDN）保存证书文件。文件扩展名可能是众所周知的 MS-DOS 扩展名 .com，导致查找认证更加困难。尽管这样不会影响证书导入，但浏览硬盘驱动器上的文件可能会不太容易。在图 9-2 中展示的是将证书导入 ISE。

图 9-2　　将证书导入 ISE



如果 ISE 和 MDM 使用相同的 CA，则可能不需要导入 MDM SSL 证书。ISE 不维护大家所熟知的公共根证书系统列表，因此所有信任关系必须由管理员建立。安装 MDM SSL 证书是最简单的方法，此处介绍的目的是保证您安装成功。

创建 MDM API 用户帐户

除证书之外，ISE 还需要 MDM 用户帐户，以便访问 API。之前安装的证书允许 ISE 通过 HTTPS 连接 MDM，这将加密 ISE 和 MDM 之间的所有数据交换，包括 API 凭证。所有 MDM 合作伙伴均支持可授予 API 权限的本地用户帐户。一些供应商可能允许在 Active Directory 等外部数据存储上定义客户。如果 ISE 使用同一帐户访问 AD 或其他资源，并且集中开展计算机帐户管理，这一项功能便具有非常大的意义。在任何情况下，都应使用强密码保护 API 用户帐户。有关设置此帐户的具体指南，请参阅合作伙伴特定的支持文档或合作伙伴 MDM 管理员指南。

有两个帐户问题可能会有碍于 API 的正常使用：

- 不正确的用户名或密码组合
- 定义用户未获得 API 访问权限

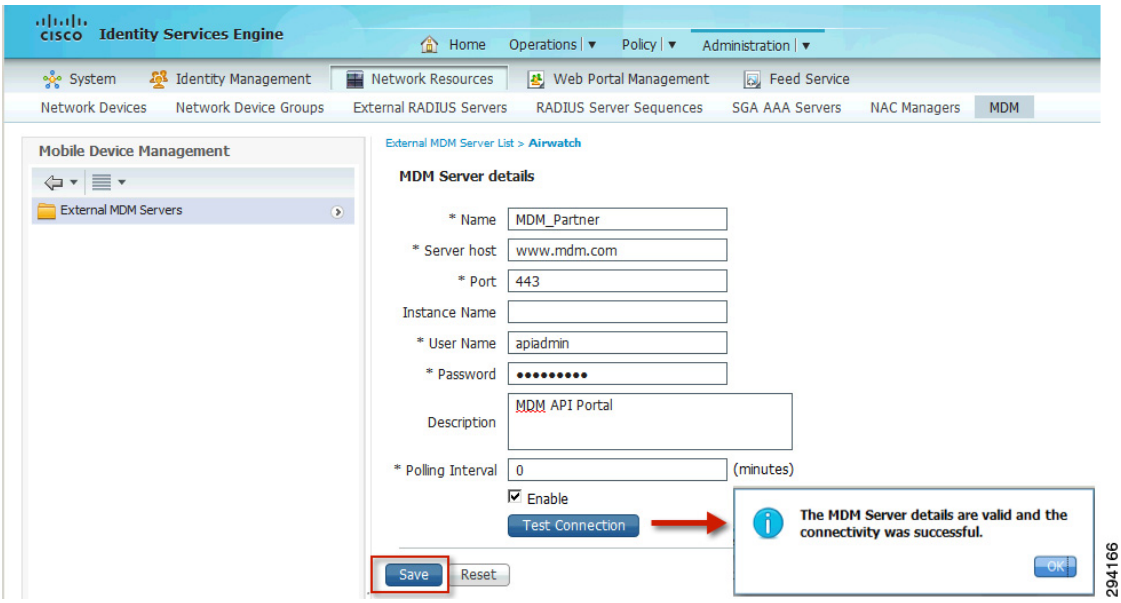
设置 MDM 连接

ISE 与 MDM 通信收集设备状况信息，或发出设备命令（例如公司擦除或锁定）。会话从 ISE 发起并流向 MDM 服务器。 MDM 服务器的 URL 通常与管理页面相同，并且是用于导出证书的网站。目录路径由系统自动处理，配置过程中将不予指定。实例用于订用云服务时比较常见的多租户部署。字段应为空，除非云提供商另有说明。 HTTPS 的端口通常是 TCP 443。通常，不能将 MDM 配置为侦听 API 用户的特定端口。任何更改都将影响管理员和用户门户页面。

轮询间隔规定了 ISE 多长时间查询 MDM 一次以获取设备状态变更信息。默认情况下，此间隔设置为 0 分钟，从而有效地禁用轮询。可启用轮询定期检查终端的 MDM 合规状态。如果发现设备不合规，且设备关联到网络，那么 ISE 会发出 CoA 强制设备重新进行身份验证。设备可能需要借助 MDM 修复，不过，这将取决于策略的配置情况。注意， MDM 合规性要求在 MDM 中配置，并且与 ISE 上配置的策略无关。即使 ISE 策略不考虑此字典属性，我们也可以设置轮询间隔，不过这种做法不可取。轮询的优势在于，如果用户的设备不满足 MDM 要求，他们将被迫重新授权该设备。轮询间隔时间越短， ISE 发现这种问题的可能性就越大。将间隔设置为一个较低的值之前，我们需要了解一些注意事项。 MDM 合规状态可能包括各种不特定于网络访问的情况。例如，设备管理员可能希望掌握使用企业设备的员工超过 80% 的数据计划的时间，以避免产生额外费用。在这种情况下，仅根据此属性阻止网络访问会加重 MDM 合规现象，违背设备管理员的初衷。此外， CoA 将中断用户 WiFi 会话，这可能会终止 VoIP 呼叫等实时应用。建议在充分理解 MDM 配置之前将轮询间隔保留为 0。如果设置轮询间隔，那么该间隔应与 MDM 上定义的设备签入时间相当。例如，如果 MDM 配置为这些设备每四小时报告一次状态，则 ISE 应设置为相同值，或不小于该值的一半。设备状态过度采样会给 MDM 服务器带来不必要的负荷，并导致移动设备的电池寿命缩短。

最后，“启用”复选框将在一台 MDM 服务器上设置为激活。我们可以保存多个配置，但是，一次只能有一个配置处于活动状态。图 9-3 展示了常规配置。

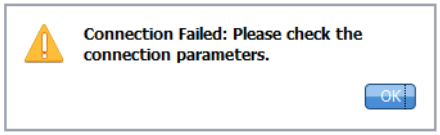
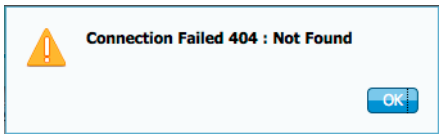
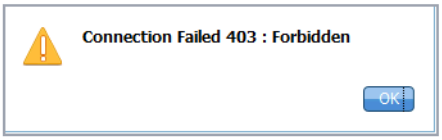
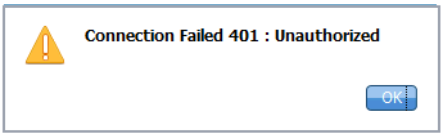
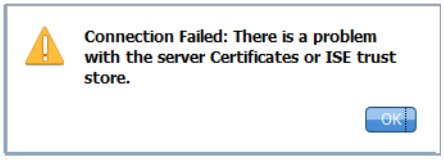
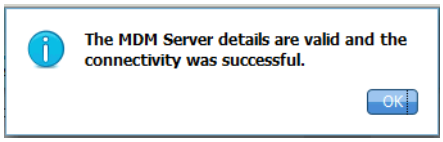
图 9-3　　MDM 服务器详细信息



验证 MDM 连接

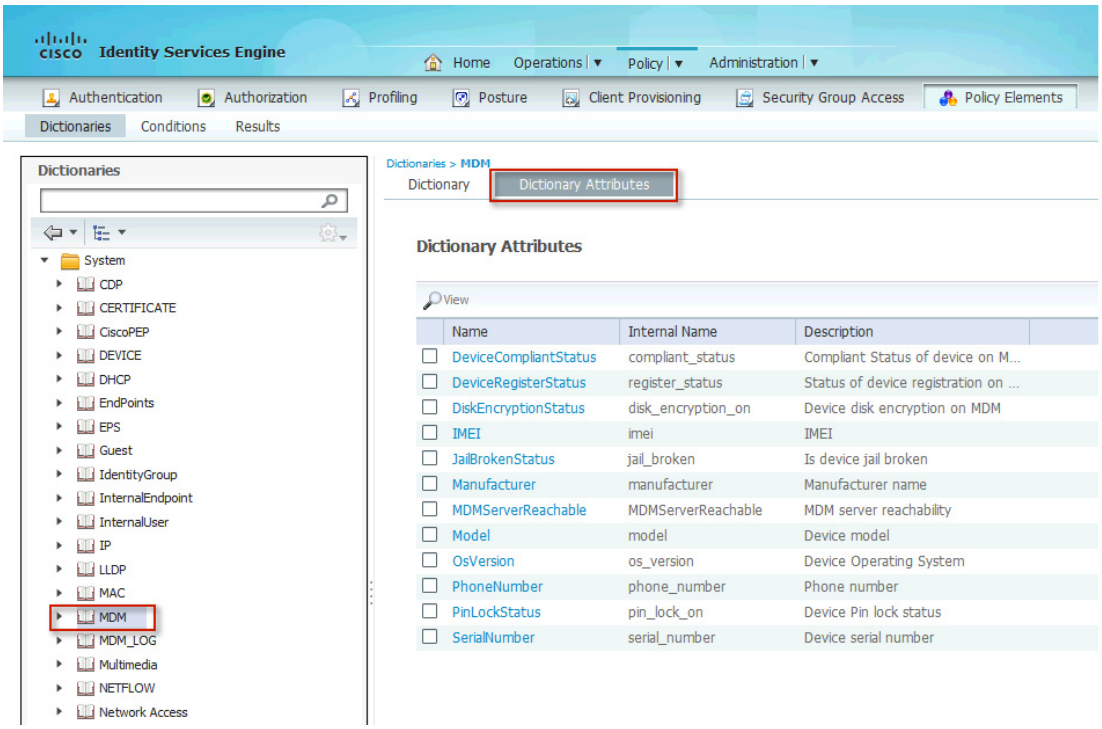
使用 “测试”按钮可建立到 MDM 的连接，并使用已配置的凭证尝试进行身份验证。执行此操作后保存设置。否则，“保存”按钮将验证设置。如果出错，可先取消选择 “MDM 启用”按钮，然后再保存。如果显示任何错误消息，管理员可参考表 9-1 查找改正设置的说明。要在之前已验证的服务器上重新运行测试，用户应取消选中 “启用”复选框、保存，然后重新选中此复选框。

表 9-1　　常见 MDM 连接错误代码

	ISE （驻留在数据中心）和 MDM （驻留在 DMZ 或云中）之间存在路由或防火墙问题。应检查防火墙配置，确认是否允许此方向的 HTTPS。
	产生 HTML 404 错误代码的最有可能的原因是不需要实例时配置了实例，或者配置了错误的实例。
	MDM 服务器上的用户帐户设置没有与其关联的正确角色。按如上所述，验证是否为 ISE 使用的帐户分配了 REST API MDM 角色。
	ISE 所使用帐户的用户名或密码不正确。另一个不太可能发生的情况是，输入的 URL 是有效的 MDM 站点，但与用来配置上述 MDM 帐户的站点不相同。这两种情况都会导致 MDM 服务器向 ISE 返回 HTML 代码 401。
	ISE 不信任 MDM 网站提供的证书。这意味着，未按照上文说明将证书导入至 ISE 存储，或者证书导入后过期。
	连接测试成功。管理员还应验证 MDM 字典是否已填充属性。

成功配置 MDM 后， ISE 策略字典中将包含创建策略所需的必要属性。用户可以通过点击**策略 > 字典 > 系统 > MDM** 验证字典，如图 9-4 中所示。

图 9-4　　字典属性



配置 MDM

除 ISE 必需的 API 用户帐户之外，还需要先在 MDM 上完成几项其他管理任务（例如，签署并安装 APNS 证书），ISE 才能通过 API 发出设备操作。合作伙伴特定支持文档详细介绍了最低要求。MDM 也可以配置为通过 LDAP 与公司目录结构集成。管理员应查阅 MDM 安装和管理指南，保证 MDM 系统达到完全正常的理想状态。

第 3 部分

BYOD 使用案例

BYOD 增强型使用案例 - 个人和企业设备

修订日期：2013 年 8 月 7 日

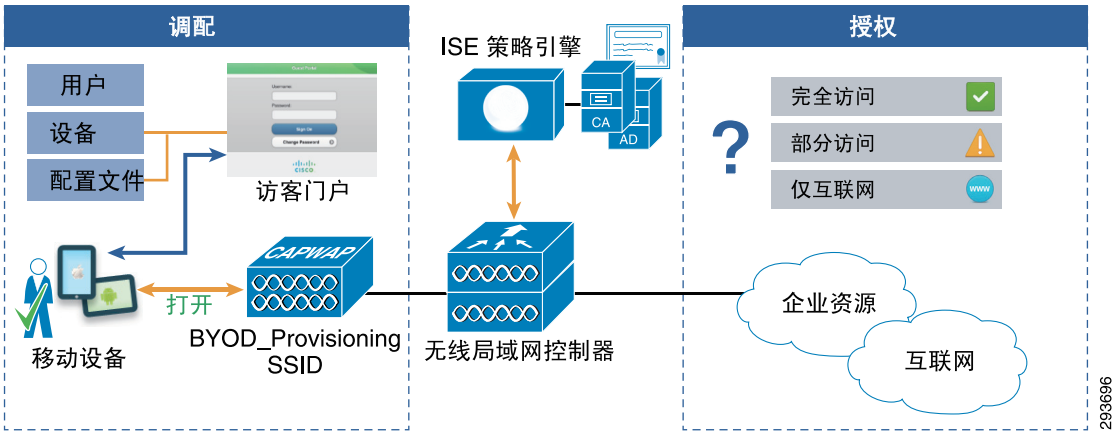
BYOD 增强型使用案例是 BYOD 有限使用案例的一个超集，涵盖了个人设备和企业设备。本章描述了针对个人设备访问部署 BYOD 的设计方案，以及每种方案的设计注意事项。还重点介绍了如何根据个人设备的类型拒绝该个人设备的访问。

BYOD 解决方案的主要目标之一是为员工提供一种简单方法，使其在无 IT 部门协助的情况下实现个人设备自注册。由于大部分员工的 BYOD 需求都可以通过简单的互联网接入或部分访问实现，因此员工只有在需要企业资源的完全访问权限时才需要 IT 部门的协助。

Cisco ISE 提供了不同的方法来定义安全策略，及确定每位员工有权访问的网络资源。然后，在整个网络基础设施中实施安全策略。 ISE 功能集非常灵活，可用于实施不同的业务策略。本章介绍了个人设备自注册的步骤，以及应用不同策略的方式。

图 10-1 显示了 ISE 分析和注册个人设备的方式，以及在该流程中发挥作用的不同网络组件（WLC、AD、CA）。ISE 会评估不同条件，以提供适当的授权和对网络资源的访问权限，包括数字证书、 Active Directory 组等。

图 10-1　　调配个人设备



注意　除非另有说明，否则本章所有图中的 “无线局域网控制器” 均指 Cisco Flex 7500、 CT5508 和 CT5760 无线控制器等独立设备，或集成在 Catalyst 3850 系列融合接入交换机中的无线局域网控制器功能。

图 10-2 显示了如何限制个人设备访问网络。设备连接后，无论用户是否通过身份验证，ISE 都会分析设备并执行 DenyAccess 授权规则。

图 10-2　　拒绝访问

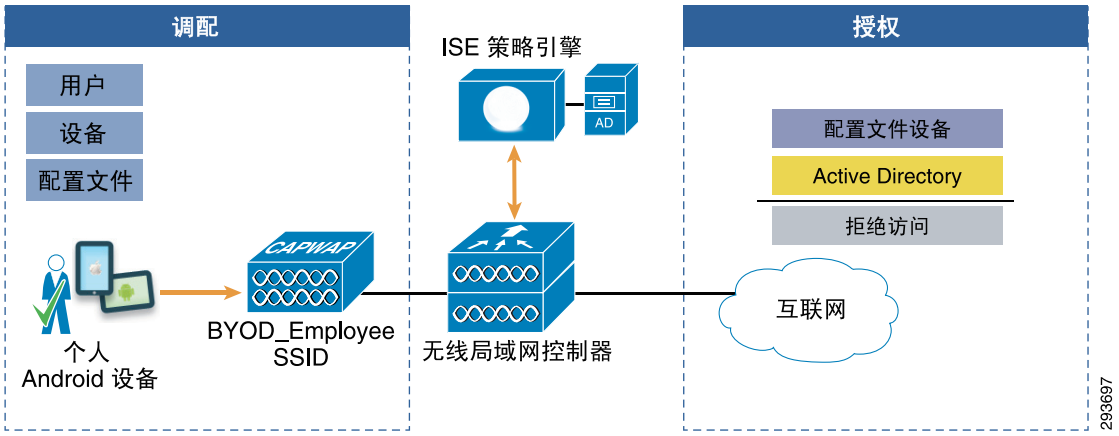


图 10-3 显示了本章中配置的不同权限级别。这些访问权限级别的实施使用了多种机制，包括无线局域网控制器 (WLC) 或 Catalyst 交换机中的访问控制列表 (ACL)、 WLC 中的安全组标记 (SGT) 分配，以及 Catalyst 交换机中的 VLAN 分配与接入点中的 FlexConnect ACL。

图 10-3　　个人设备的权限级别

	策略	访问
	完全访问	互联网和所有企业资源
	部分访问	互联网和部分企业应用
	仅互联网	仅互联网
	拒绝访问	明确拒绝网络访问

292642

Active Directory 组

Active Directory 组可以用作向用户授予不同访问权限的另一种方式。本章基于以下三个 AD 组：

- BYOD_Full_Access - 此组的成员被授予了网络资源的完全访问权限。
- BYOD_Partial_Access - 此组的成员被授予了网络资源的部分访问权限。通过此权限，用户可以访问互联网和企业应用子集，例如电邮、企业目录、差旅工具等。
- 域用户 - 所有用户都默认为此系统生成的组的成员。不是上述组中成员的员工会被授予访问互联网的权限。

此模式可轻松扩展为包括具有类似访问要求的其他用户组。创建新组和访问列表，以向承包商或合作伙伴授予访问权限就是一个很好的例子。

图 10-4 重点介绍了本章验证的不同访问策略，以及每种策略的不同要求和授予的权限。这些策略及其详细配置将在本章后文中介绍。

图 10-4　　访问策略和权限

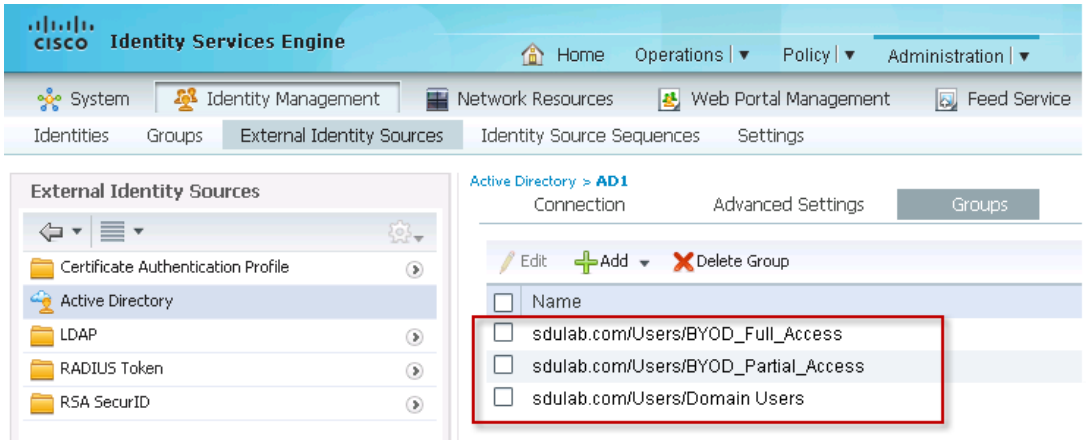
策略	位置	AD 组	配置文件	权限	
完全访问	园区/分支机构/SGT	BYOD_Full_Access		完全	✓
部分访问	园区/分支机构/SGT	BYOD_Partial_Access		部分	⚠
仅互联网	园区/分支机构/SGT	域用户		仅互联网	www
拒绝 Android 设备			Android	拒绝	✗

293698

注意　位置 SGT 指仅为执行 SGT 而指定的无线局域网控制器。

要配置可用于授权策略条件的 Active Directory 组，请点击 **Administration > Identity Management > External Identity Sources > Active Directory > Groups**，然后选中将用于策略条件和规则的组旁边的框。图 10-5 中包含了本设计指南中使用的组。

图 10-5　　Active Directory 组

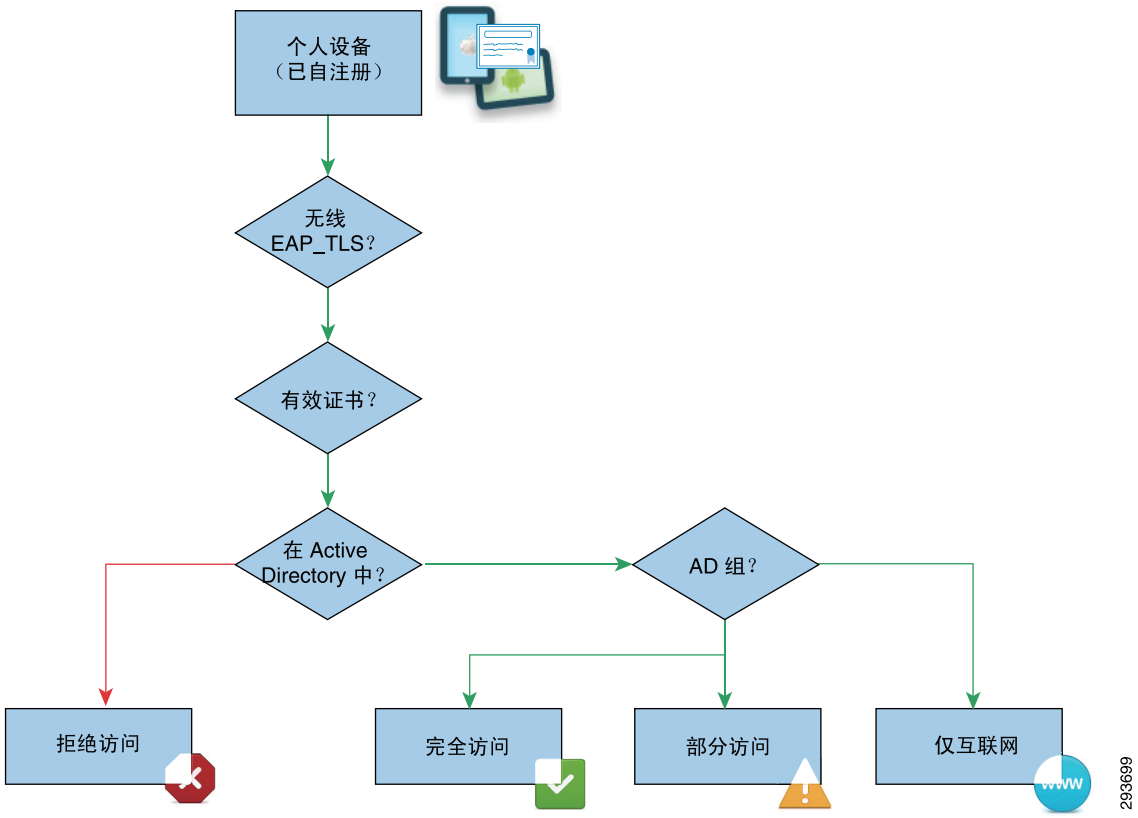


本章假定员工执行设备自注册后，将连接到 BYOD_Employee SSID。图 10-6 重点展示了个人设备的连接流程。

如果终端设备从无线 802.1X EAP-TLS SSID 连接，并拥有一份有效证书，则根据员工的 AD 组成员资格，员工可获得：

- 完全访问权限，前提为员工属于 BYOD_Full_Access 组。
- 部分访问权限，前提为员工属于 BYOD_Partial_Access 组。
- 互联网访问权限，前提为员工是有效的 Active Directory 成员 （域用户组）。

图 10-6　　个人设备 BYOD 访问



分发数字证书

由公钥加密算法支持的数字签名提供了一种验证设备和用户的方法。在公钥加密算法 （例如，RSA 加密系统）中，每个用户都有包含公钥和私钥的密钥对。这些密钥承担补充功能，并且通过其中一个密钥加密的任何内容可以通过另一个密钥解密。

数字签名通过发送方的私钥加密。必须验证签名，以确认发送方的身份。该操作由接收方完成，接收方可通过发送方的公钥解密签名。如果与数据一起发送的签名与针对数据应用公钥的结果相匹配，则会建立消息有效性。

此过程依赖于拥有发送方公钥副本的接收方，以及此密钥属于发送方 （而不是自称为发送方的某人）这一高度确定性。

在移动设备中部署数字证书需要独特的流程，因为许多此类设备无法与基于 PC 的传统设备一样对用于创建 / 下载和安装数字客户端证书的所有特性和功能提供本地支持。同时，一些终端无法在本地支持简单证书注册协议 (SCEP)。

例如，如果用户要使用 SCEP 在 Apple iOS 设备上安装数字客户端证书，则 IT 管理员需要使用 iPhone 配置实用程序手动创建配置文件，并通过电邮、 USB 或网页将配置文件分发到用户设备。

基于全功能 PC 的传统设备更易于充分利用众多服务 （如 Microsoft NDES）来提供证书注册。然而，随着市场中大量 Android 和 Apple iOS 设备的出现，我们无法断言这些设备可以与当前部署的众多企业服务进行本地互操作。

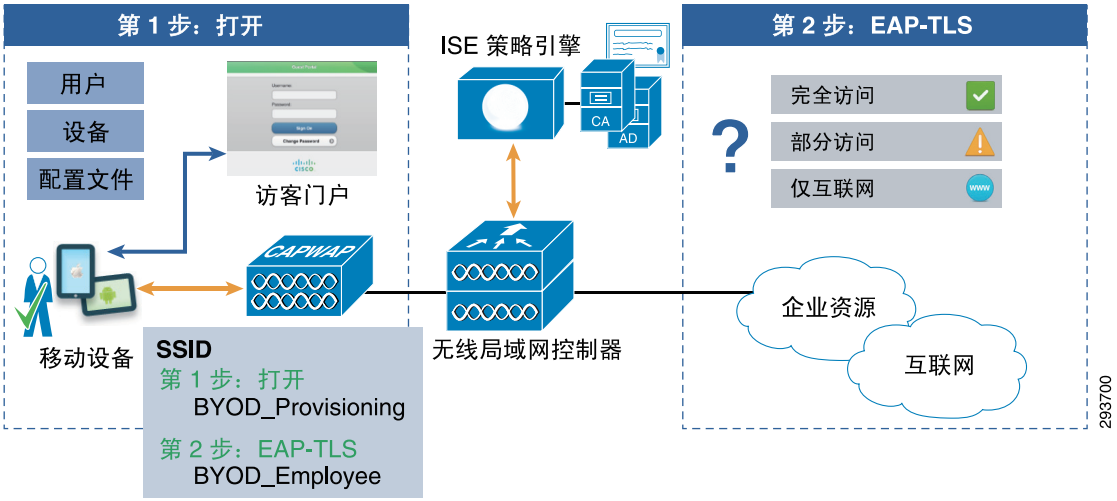
ISE 解决了这一问题，它使用 SCEP 代理功能 （允许终端通过 ISE 获取数字证书），将数字证书分发到终端。此外，此功能在初始注册过程中结合，避免了其他注册步骤。有关移动设备的下一节讨论了终端如何在注册过程中获取数字证书。

移动设备自注册

将数字证书部署到终端设备时，需要一个可安全灵活地实施不同安全策略的网络基础设施。图 10-7 重点展示了移动设备使用双 SSID 连接到网络时要遵循的常规步骤。

1. 一台新设备连接到调配 SSID。此 SSID （开放或通过 PEAP 确保安全）被配置为将用户重定向到访客注册门户。
2. 在用户正确通过身份验证后，便会开始进行证书注册和配置文件调配。
3. 调配服务请求来自移动设备用户的信息并调配配置文件，其中包含一个 WiFi 配置文件，该文件带有连接到安全员工 SSID 所需的参数。
4. 在后续连接中，设备使用员工 SSID，并根据不同的 ISE 授权规则被授予网络资源访问权限。

图 10-7　　注册和调配 - 双 SSID



自注册步骤也可以通过用于调配和安全访问的单 SSID 进行配置。移动设备连接后遵循的常规步骤相似，即将用户重定向到访客注册门户并使用数字证书和配置文件调配设备。

调配流程

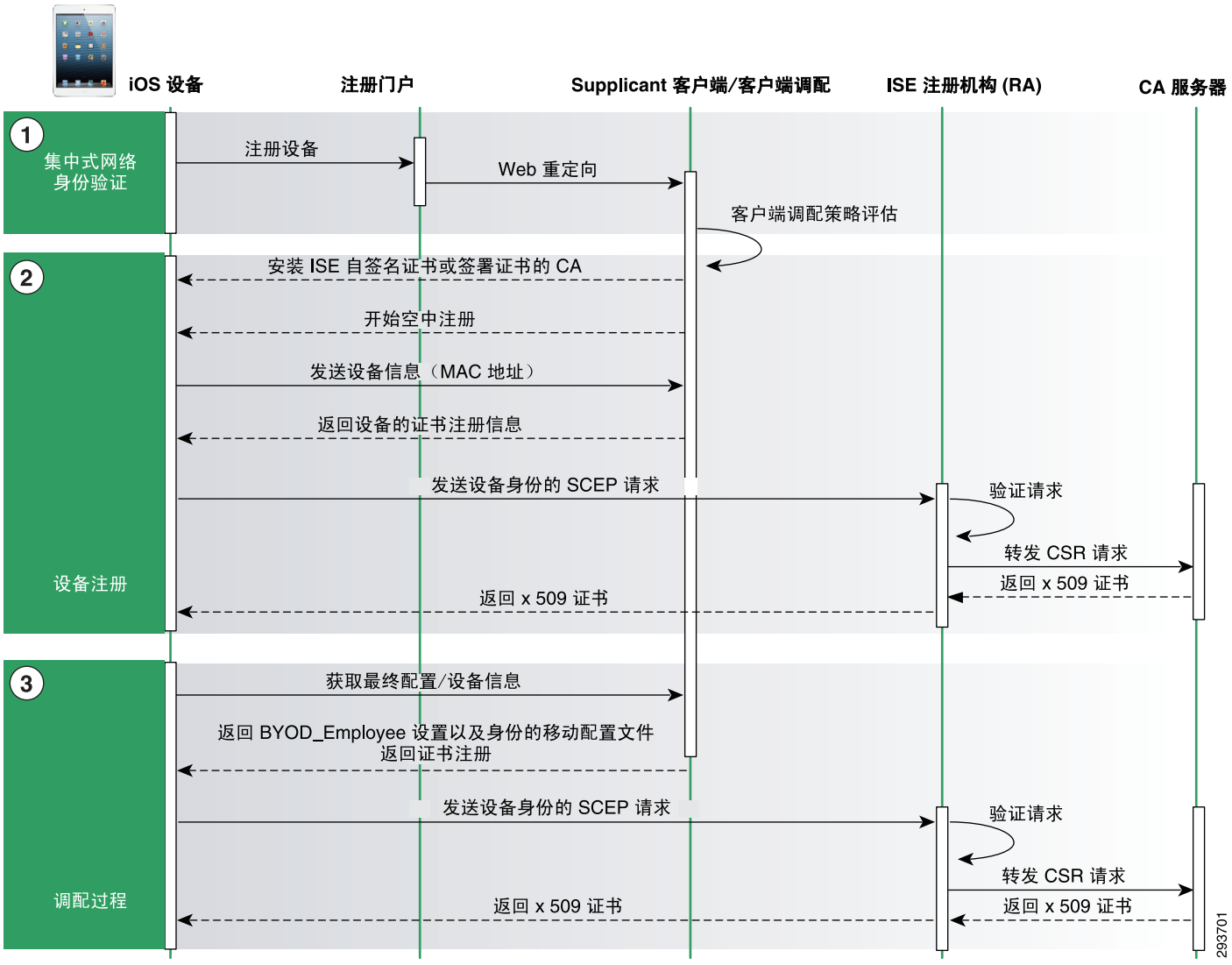
本节介绍了终端和访客注册门户之间的交互，以及注册数字证书和配置文件所需的步骤。Windows 和 Mac 设备的调配方式类似。

调配 Apple iOS 设备

调配 Apple iOS 设备时，将执行以下步骤：

1. 设备重定向至访客注册门户。
2. 在成功进行身份验证后，开始进行空中 (OTA) 注册。
3. 设备发送唯一标识符 （MAC 地址）和其他信息。
4. 证书注册信息发送到设备。
5. 向 ISE 提出 SCEP 请求， ISE 返回一份证书。
6. BYOD_Employee 的无线配置文件发送到设备。
7. 完成注册后，用户手动连接到 BYOD_Employee SSID。

图 10-8　　Apple iOS 设备调配流程



有关 IOS 设备空中注册和配置的详细信息，请查看 iPhone OS 企业部署指南：
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf。

调配 Android 设备

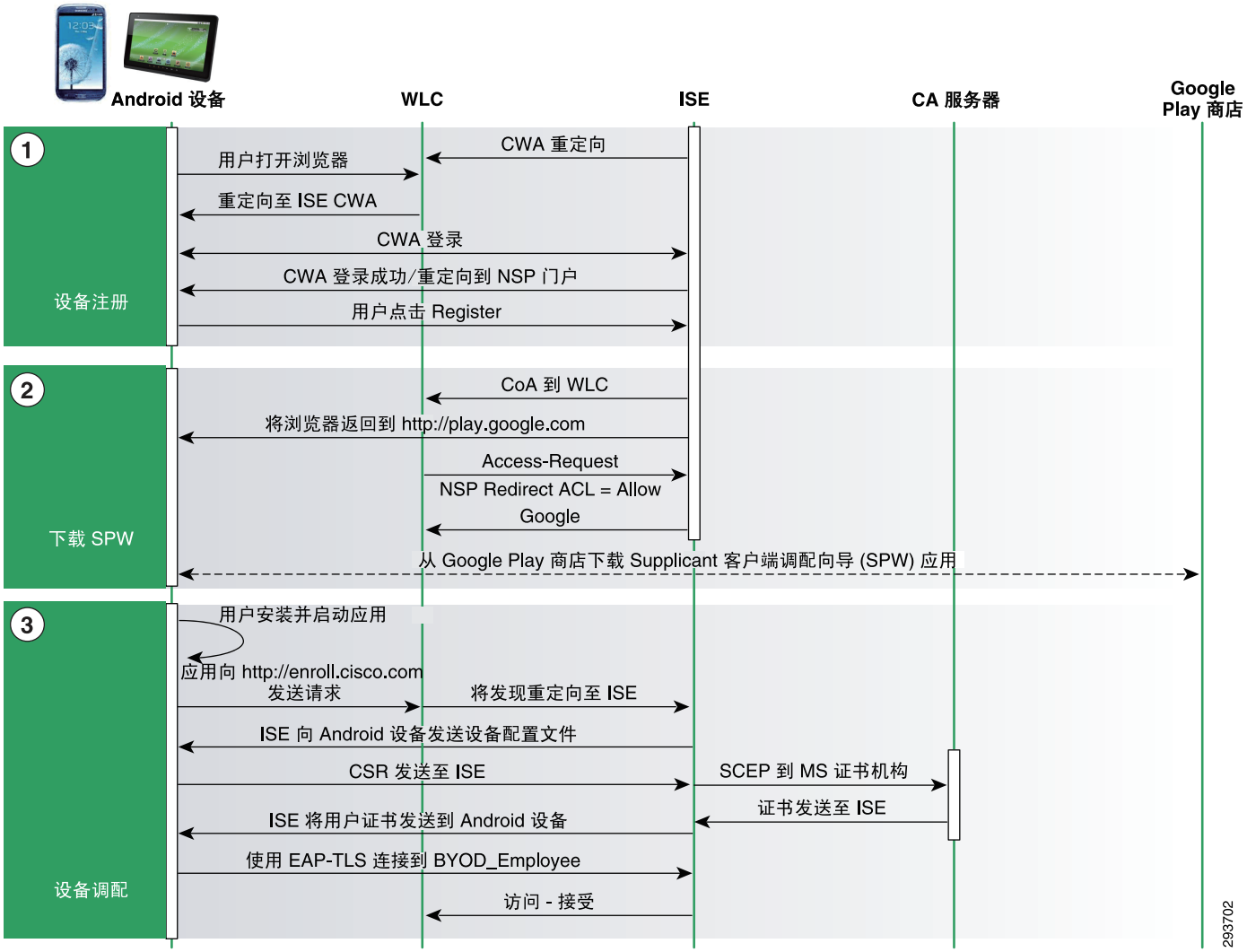
调配 Android 设备时，将执行以下步骤：

1. 设备重定向至访客注册门户。
2. 在成功进行身份验证后，自助注册门户页将用户重定向到 Google Play。
3. 用户安装 Supplicant 客户端推送向导 (SPW)。
4. 启动 SPW，以执行 Supplicant 客户端推送。 SPW 执行以下功能：
   a. 找到 ISE，并从 ISE 下载配置文件。
   b. 为 EAP TLS 创建证书 / 密钥对。
   c. 向 ISE 提出 SCEP 代理请求并获取证书。
   d. 应用无线配置文件，以允许连接到 BYOD_Employee SSID。
5. SPW 触发重新验证，并自动连接到 BYOD_Employee SSID。

注意　必须从 Google Play 下载 Android 代理，该代理并非由 ISE 调配。终端必须能够连接到互联网上的 Google Play。

注意　ACL_Provisioning_Redirect 必须重定向所有发送到 enroll.cisco.com 的流量。用于 Android 设备的思科配置助手需要通过此重定向找到 ISE 服务器。如图 10-9 中的第 3 步部分所示。如果在所有互联网流量（除 Google Play）都重定向到 ISE 后按照 CVD 中显示的指南操作，则无需考虑此问题。

图 10-9　　Android 设备调配流程



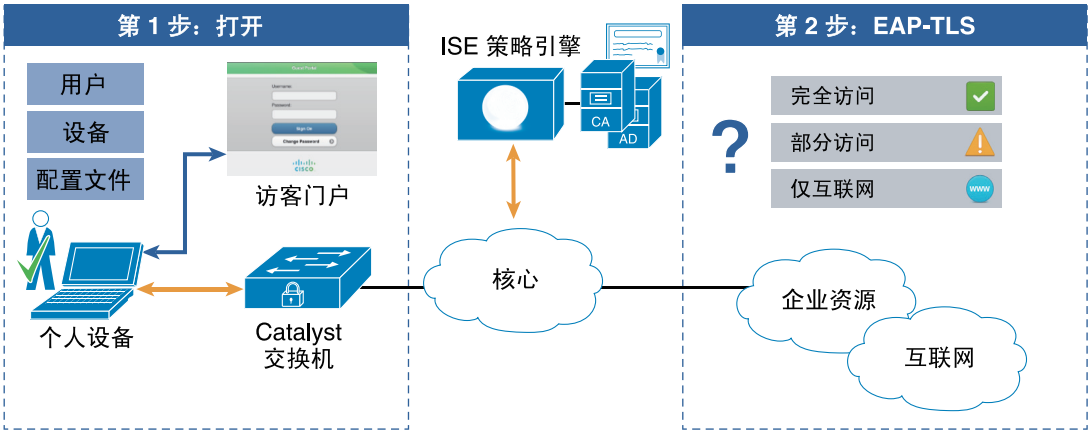
调配有线设备

BYOD 适用于有线设备和无线设备。有线设备的调配、注册、身份验证和授权方式与无线设备大致相同。以下是调配有线设备的一些优势：

- 证书调配可以在设备调配过程中完成，从而减轻了 IT 部门为在设备上调配证书而支持另一种模式的负担。
- 设备上的本地 Supplicant 客户端可以在调配过程中通过正确的协议配置。如果此步骤留给用户执行，则可能经常会导致错误配置和额外的 IT 部门管理开销。
- 为 IT 部门提供更简单的方法来清楚查看正在访问网络的人员，以及删除已丢失或被盗设备的网络访问权限的方法。

图 10-10 显示了用于部署有线设备的组件的高级概述。 ISE 使用多个构建块对设备进行身份验证和授权，如 AD 组成员资格、 EndPoints:BYODRegistration 属性和数字证书。本设计指南介绍了有关如何构建这些策略的示例。

图 10-10　　有线设备部署



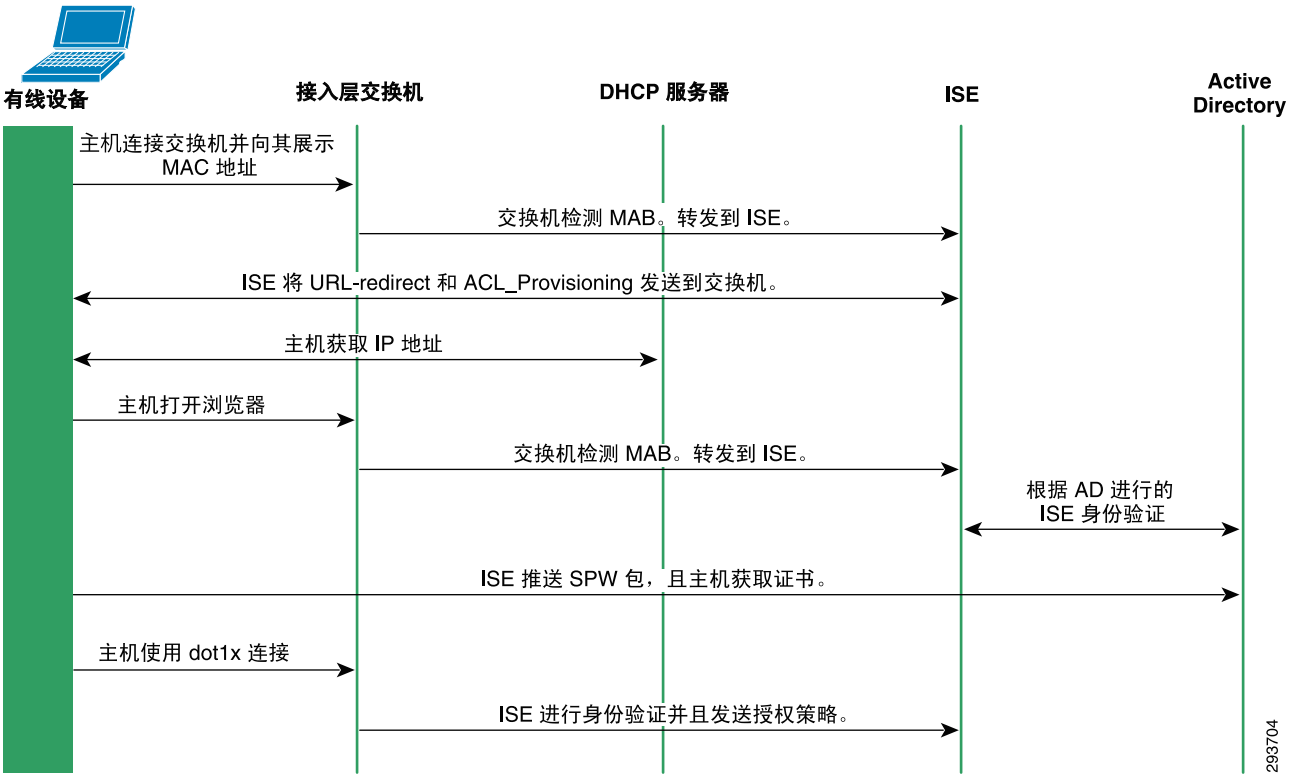
注意　除非另有说明，否则本章所有图中的“接入层交换机”均指 Catalyst 3750X 系列和 Catalyst 4500 系列等交换机，或 Catalyst 3850 系列融合接入交换机。

以下是有线设备连接到接入层交换机时出现的概要步骤：

1. 交换机必须检测到有线终端未针对 dot1x 配置，并且应使用 MAB 进行身份验证。
2. ACL_Provisioning_Redirect ACL 用于匹配网络流量。
3. URL 重定向必须指向 ISE 访客注册门户。
4. ACL_Provisioning ACL 必须在限制此状态下访问的端口下载。
5. 用户打开浏览器并尝试访问任何资源。
6. 交换机将用户重定向至 ISE 自助注册门户。
7. ISE 利用 AD 验证用户并推送 SPW 包。
8. SPW 包帮助用户注册并从 ISE 获取数字证书。
9. CoA 出现，并且用户使用获取的数字证书重新连接到网络。

图 10-11 列出了有线设备调配的流程。

图 10-11　　有线设备调配流程



密钥和证书存储

安全存储数字证书及其关联密钥的功能对每个设备都非常重要。存储的实施方式各不相同，具体取决于使用的操作系统或媒介。表 10-1 显示了本设计指南中测试的不同平台及其证书库。

表 10-1　　平台和证书库

设备	证书库	如何访问
Microsoft Windows	计算机证书库	使用 mmc.exe 实用程序的证书管理单元
Mac OS	设备证书库	使用密钥链访问应用
Apple iPad	设备证书库	Settings > General > Profile
Android	凭证存储	Settings > Location & Security

调配后，证书会具有以下属性 （可被 ISE 用于执行不同权限）：

主题通用名称 (CN)：
用于身份验证的用户身份

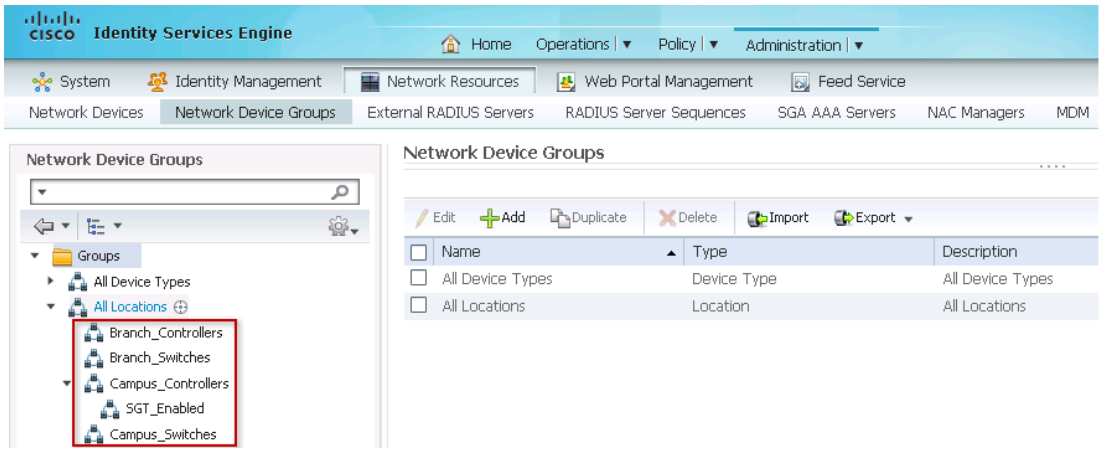
主题替代名称：
终端的 MAC 地址。

网络设备组

为了区分这些连接，ISE 依赖于网络设备组来根据 WLC 的位置或设备类型对 WLC 进行分组。这样，单个 ISE 就可以在不同设备组中实施策略。点击 **Administration > Network Resources > Network Device Groups** 来定义分支机构、园区和启用了 SGT 的控制器的位置。

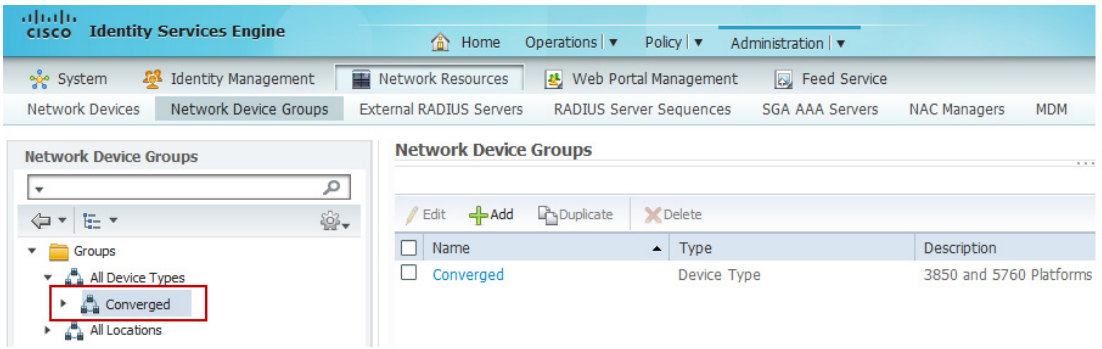
图 10-12 显示了授权策略中使用的不同位置。

图 10-12　　ISE 设备组 - 位置



同样，图 10-13 显示了名为 **Converged** 的设备类型，该类型可针对 Catalyst 3850 系列交换机和 CT5760 无线控制器创建，可用于授权策略中。

图 10-13　　ISE 设备组 - 设备类型

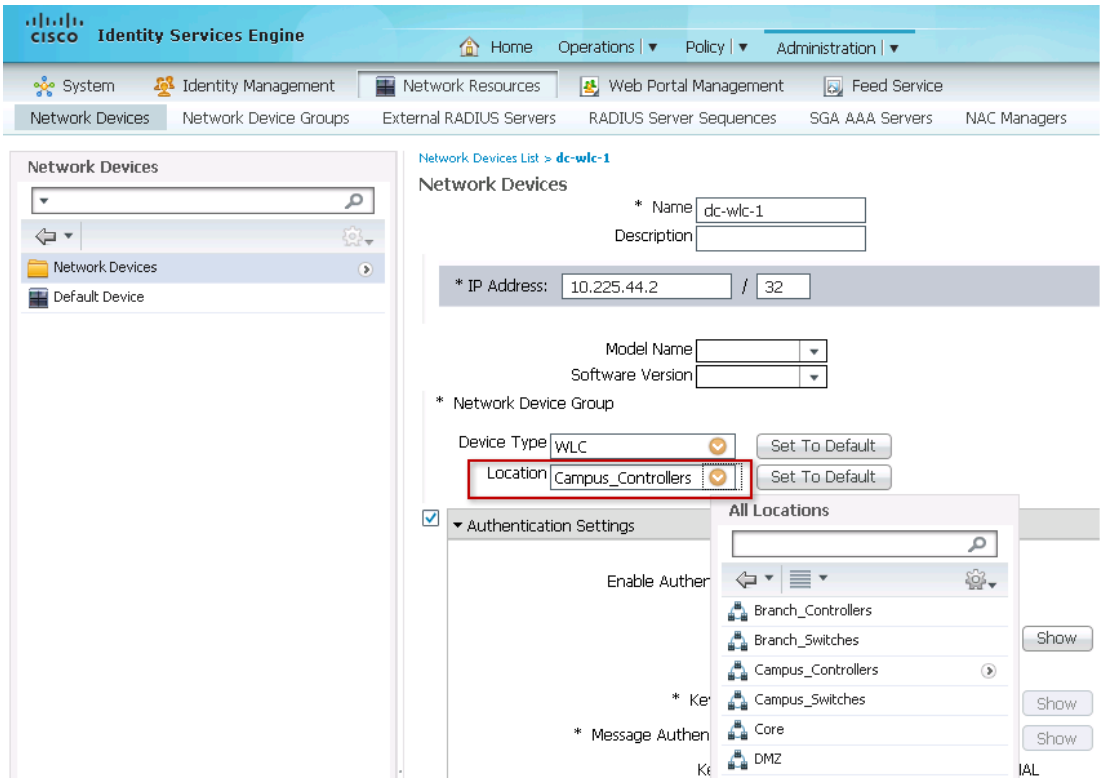


注意　融合接入设计使用设备类型而不是位置的原因之一为，本设计指南中融合接入分支机构和园区设计使用相同的授权策略规则。因此，从 Cisco ISE 的角度看，位置（园区与分支机构）与本设计指南中展示的融合接入设计不是特别相关。请注意，如果位置相关，则客户可以随时修改此处展示的设计，并选择分别为分支机构及园区融合接入设计部署授权策略。

每个无线局域网控制器（之前定义为网络设备）都需要添加到适当的设备组中，方式为点击 **Administration > Network Resources > Network Devices**，然后从下拉菜单中指定适当位置或设备类型。

图 10-14 显示了如何将 dc-wlc-1 无线局域网控制器加入 Campus_Controllers 网络设备组。

图 10-14　　ISE 网络设备 - 园区控制器



安全组访问的策略实施

在 BYOD 架构中实施 SGA 策略包含两个主要部分：

- 为终端和目标服务器定义标记。
- 定义并实施安全组 ACL 或安全组防火墙 (SG-FW) 策略。

在本设计中，安全组 ACL 可以在 Catalyst 和 Nexus 数据中心交换基础设施中或者在 ASA 防火墙中作为 SG-FW 策略实施。

安全组访问标记

安全组访问的基本理念是将设备或服务器的 IP 地址与安全组标记相关联，然后创建基于角色的策略，此类策略可根据这些源和目标 SGT 允许或拒绝流量。例如：标记有 SGT 10 的设备是否可以与标记有 SGT 40 的服务器通信？此流量会在实施点获得允许或被阻止。

使用此标记概念，为作为客户端访问网络的每种设备定义了唯一标记。如第 2 章，“BYOD 使用案例”中所述，个人和企业设备被授予了唯一权限，因此为每个使用案例定义了唯一标记。

表 10-2 介绍了如何将标记分配给不同设备。

表 10-2　　源标记

设备类型	标记
具有完全访问权限的企业设备	SGT 10
具有完全访问权限的个人设备	SGT 11
具有部分访问权限的个人设备	SGT 12

同样，目标服务器也需要与特定标记相关联。表 10-3 介绍了如何根据相应角色向服务器分配不同标记。

表 10-3　　目标标记

目标服务器	标记
开放式接入	SGT 40
企业服务器	SGT 50

安全组 ACL

在定义源标记和目标标记后，下一个逻辑步骤是定义出口策略矩阵，该矩阵可定义源标记和目标标记之间的策略实施。表 10-4 介绍了出口策略矩阵。

表 10-4　　出口策略矩阵

	设备类型	SGT 40	SGT 50
SGT 10	具有完全访问权限的企业设备	是	是
SGT 11	具有完全访问权限的个人设备	是	是
SGT 12	具有部分访问权限的个人设备	是	否

如表 10-4 中所示，被授予完全访问权限的企业或个人设备可连接到标记有 SGT 40 或 SGT 50 的服务器。类似的，具有部分访问权限的个人设备只能与标记有 SGT 40 的服务器连接。

SGACL 的实施取决于部署方案的类型。如果部署方案中 Nexus 为实施点，则会在 ISE 中定义 SGACL 并将其推送到 Nexus 交换机；然而，如果部署方案使用 ASA 作为实施点，那么将在 ASA 防火墙中手动配置基于 SGT 的访问规则。

SGT 授权策略

ISE 根据策略匹配和授权配置文件，将 SGT 标记分配到终端。采用 SGT 的集中式园区 （见本章后文）提供的信息涉及用于确定何时返回 ACL 和 SGT 的标准，该返回操作在根据 ISE 中定义的无线控制器网络设备类型进行成功授权后执行。

对于分配到服务器的目标标记，配置操作在数据中心交换机中手动完成，并且会根据部署方案进行实际实施。

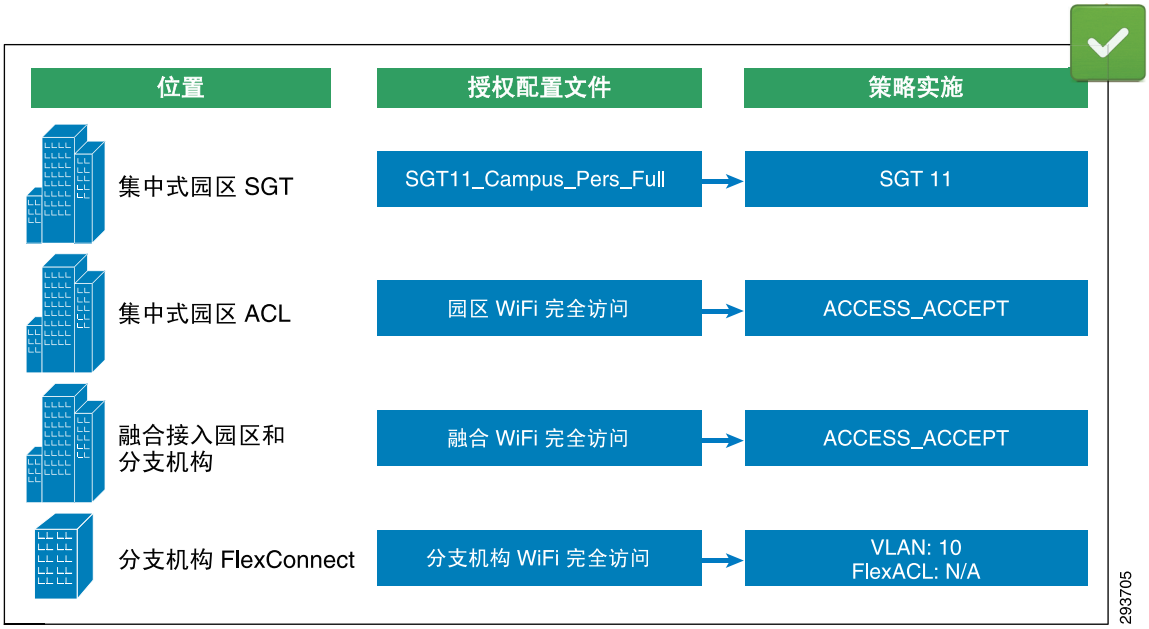
个人无线设备 - 完全访问权限

要向个人设备提供完全访问权限， Cisco ISE 会验证以下各项：

- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是 BYOD_Full_Access Active Directory 组的成员。

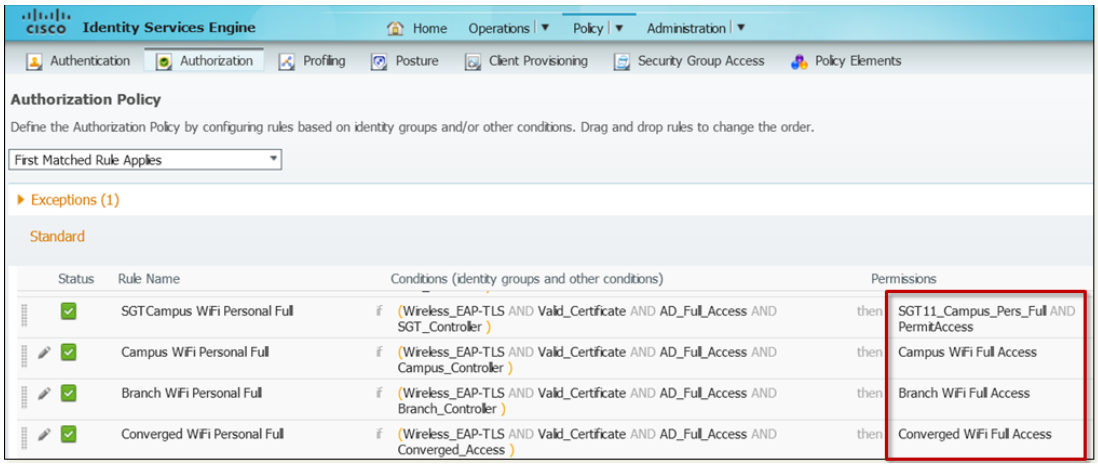
由于本设计指南中展示的无线设计依赖于 FlexConnect 分支机构、集中式控制器园区及融合接入园区和分支机构的不同 WLC，因此针对从每种设计发起的连接创建了唯一授权规则。在较高层面上，图 10-15 显示了如何针对从无线设计各异的不同位置发起的连接选择不同授权配置文件。每个授权配置文件会相应地实施一种唯一权限。

图 10-15　　完全访问权限实施



要在 ISE 中配置授权规则，请点击 **Policy > Authorization**。图 10-16 重点显示了向个人设备授予完全访问权限的授权策略。

图 10-16　　完全访问权限的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wireless_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包含的 MAC 地址匹配。（定义为简单条件）。
- 用户属于特定 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自无线控制器，该控制器是以下任一设备组的成员：Campus_Controller、SGT_Controller、 Branch_Controller 或 Converged_Access （定义为简单条件）。

注意　无线控制器是 Converged_Access 设备组的成员，它既可以是 Cisco CT5760 无线控制器等独立设备，也可以是具有集成无线控制器功能的交换机，如 Catalyst 3850。

简单和复合条件

为了提高授权策略的可读性，本设计定义了简单和复合授权条件，便于对不同条件进行分组。无需更改每条授权规则，即可重复使用和修改这些条件。

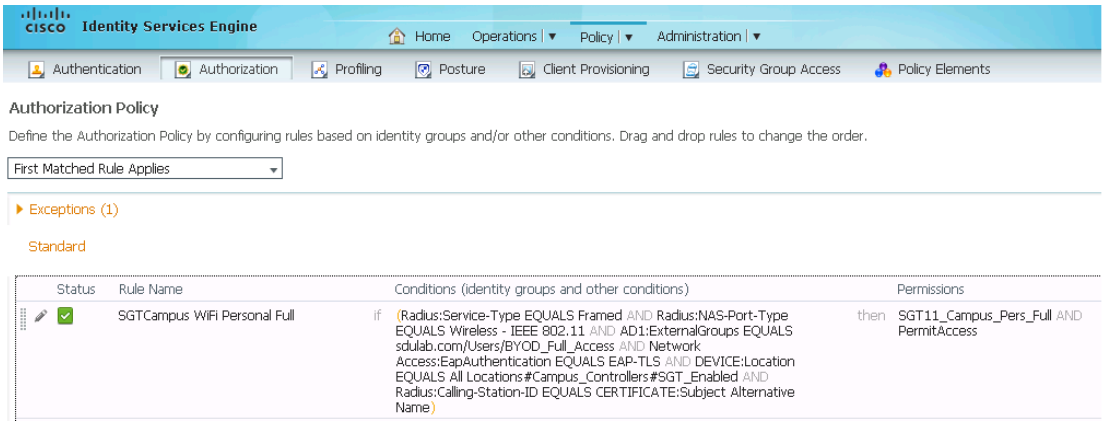
表 10-5 显示了授权规则中使用的条件：

表 10-5　　简单和复合条件

无线 EAP-TLS （复合）	
Wireless_EAP-TLS （请参阅图 10-18）	Radius:Service-Type Equals Framed AND Radius:NAS-Port-Type Equals Wireless - IEEE 802.11 AND Network Access:EapAuthentication Equals EAP-TLS
检查有效证书 （简单）	
Valid_Certificate （请参阅图 10-19）	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
Active Directory 组 （简单）	
AD_ Full_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Full_Access
AD_ Partial_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Partial_Access
AD_Domain_users	AD1:ExternalGroups EQUALS sdulab.com/Users/Domain User
WLC 位置或设备类型 （简单）	
SGT_Controller	DEVICE:Location EQUALS All Locations#Campus_Controllers#SGT_Enabled
Campus_Controller	DEVICE:Location EQUALS All Locations#Campus_Controllers
Branch_Controller	DEVICE:Location EQUALS All Locations#Branch_Controllers
Converged_Access	DEVICE:Device Type EQUALS All Device Types#Converged

为了说明采用简单 / 复合条件的价值，图 10-17 显示了未实施简单 / 复合条件情况下，阅读一条规则将增加多少时间和难度。

图 10-17　　无条件的授权规则



要定义新的复合条件，请点击 **Policy > Conditions > Authorization > Compound Conditions**。图 10-18 显示了 Wireless_EAP-TLS 条件如何将多个条件结合到一个条件中。

图 10-18　　Wireless_EAP-TLS 条件

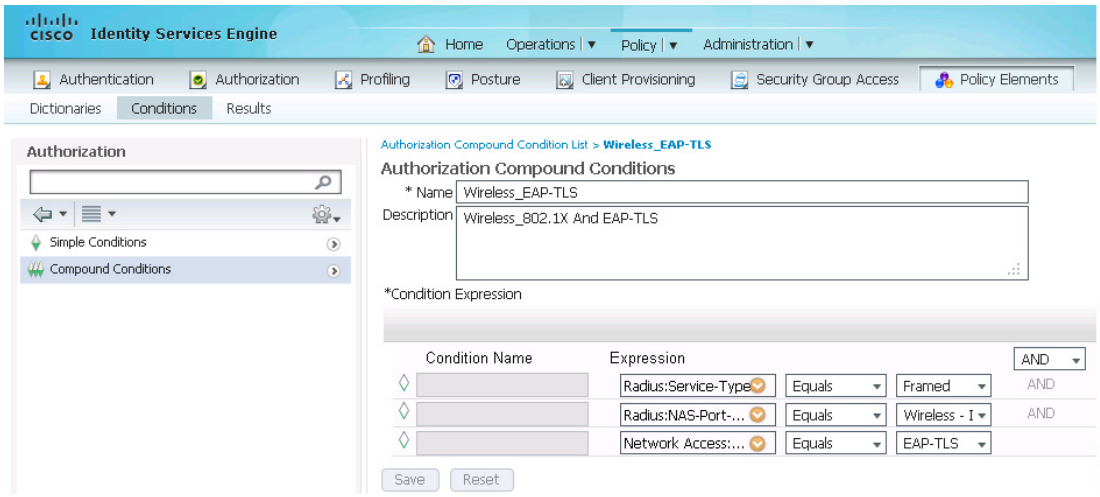


图 10-19 显示了 Valid_Certificate 简单条件。

图 10-19　　Valid_Certificate 条件

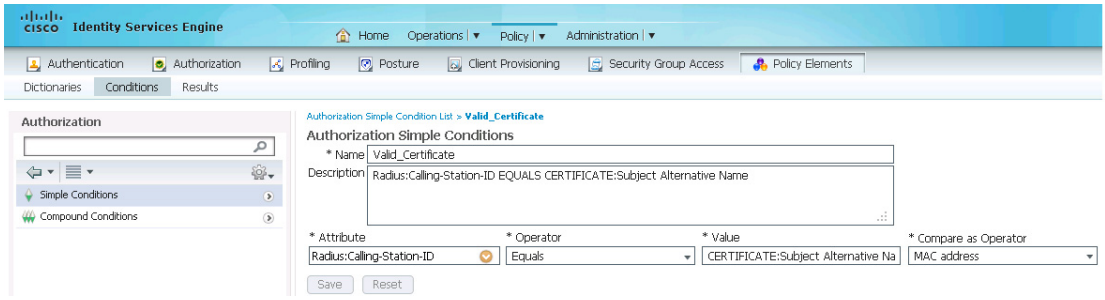


图 10-20 显示了 AD_Full_Access 简单条件。

图 10-20　　AD_Full_Access 条件

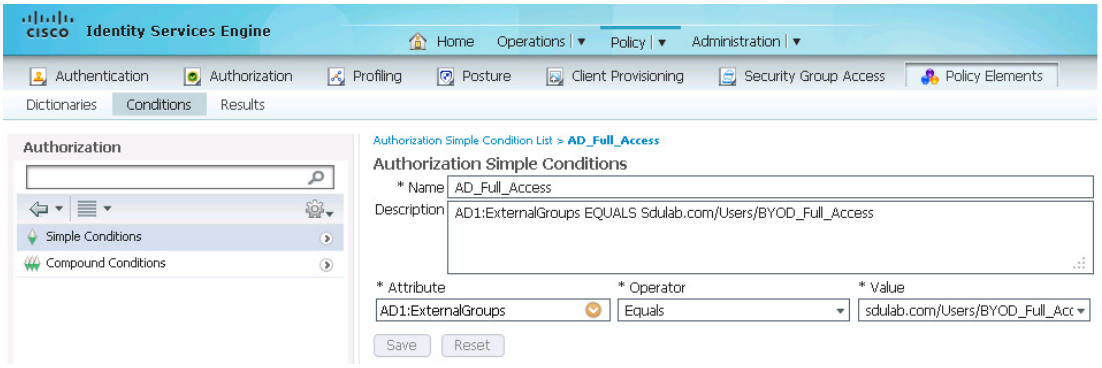


表 10-5 中提及的其他条件的定义方式与此类似。

权限

权限是授权策略匹配的结果，且授权可以具有不同的类型，如授权配置文件或标准结果。表 10-6 介绍了用于完全访问的权限。

表 10-6　　完全访问的权限

权限名称	权限类型	用途
SGT11_Campus_Pers_Full	标准结果	向 802.1X 无线设备分配 SGT，该设备从允许完全访问并且启用了 SGT 的控制器连接。
园区 WiFi 完全访问	授权配置文件	向从集中式园区控制器连接的 802.1X 无线设备提供完全访问权限。
分支机构 WiFi 完全访问	授权配置文件	向从 FlexConnect 分支机构控制器连接的 802.1X 无线设备推送 VLAN
融合 WiFi 完全访问	授权配置文件	向从融合接入控制器连接的 802.1X 无线设备提供完全访问权限。

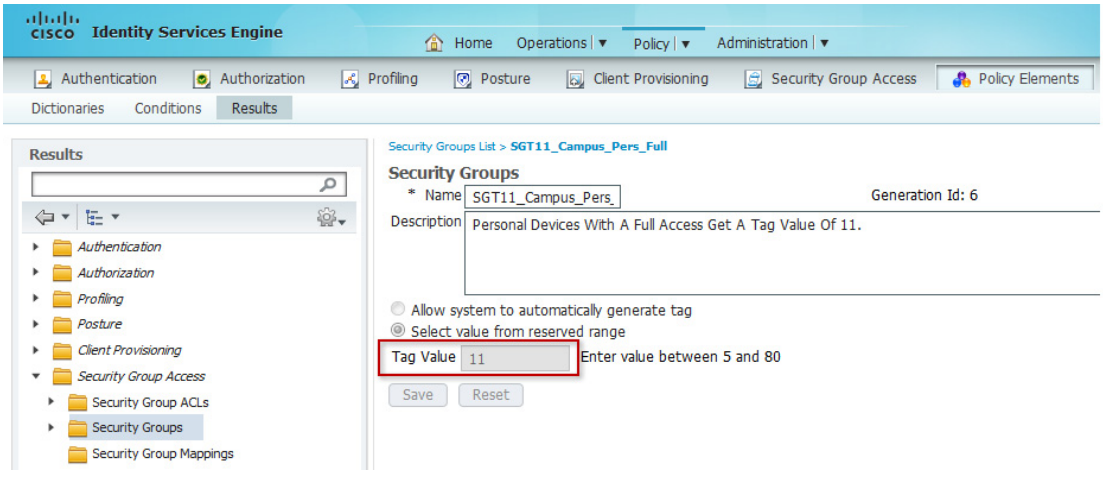
注意　在本设计指南中，融合接入基础设施是指使用 Catalyst 3850 系列交换机和 / 或 CT5760 无线控制器的分支机构或园区部署。

采用 SGT 的集中式园区

如安全组访问的策略实施中所述，拥有完全访问权限的个人设备会被分配 SGT 值 11。个人设备获取标记值 11 后，可以连接到数据中心中的所有服务器。

图 10-21 显示了 SGT11_Campus_Pers_Full 授权配置文件如何针对被授予完全访问权限的个人设备使用 SGT 11。

图 10-21　　SGT11_Campus_Pers_Full

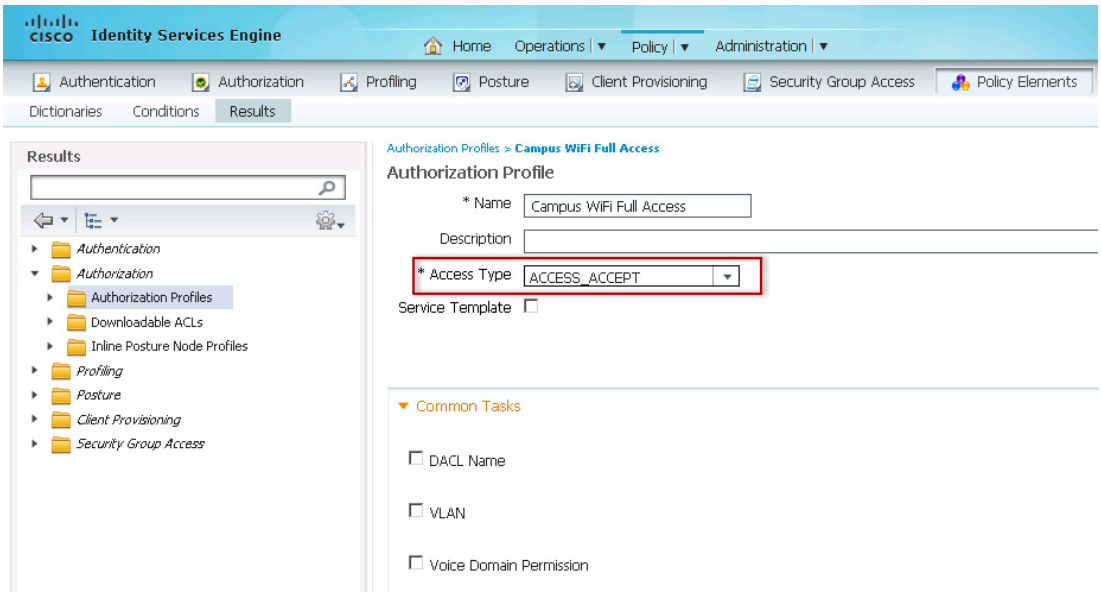


SGT 出口策略矩阵定义了 SGT11 的权限，即在园区采用 SGT 实施集中式控制器（本地模式）设计的情况下，允许其进行完全访问。请参阅安全组访问的策略实施，了解有关该矩阵的详细信息。

采用 ACL 的集中式园区

图 10-22 显示了园区 WiFi 完全访问授权配置文件如何使用 ACCESS_ACCEPT 访问类型来允许完全访问。

图 10-22　　园区 WiFi 完全访问

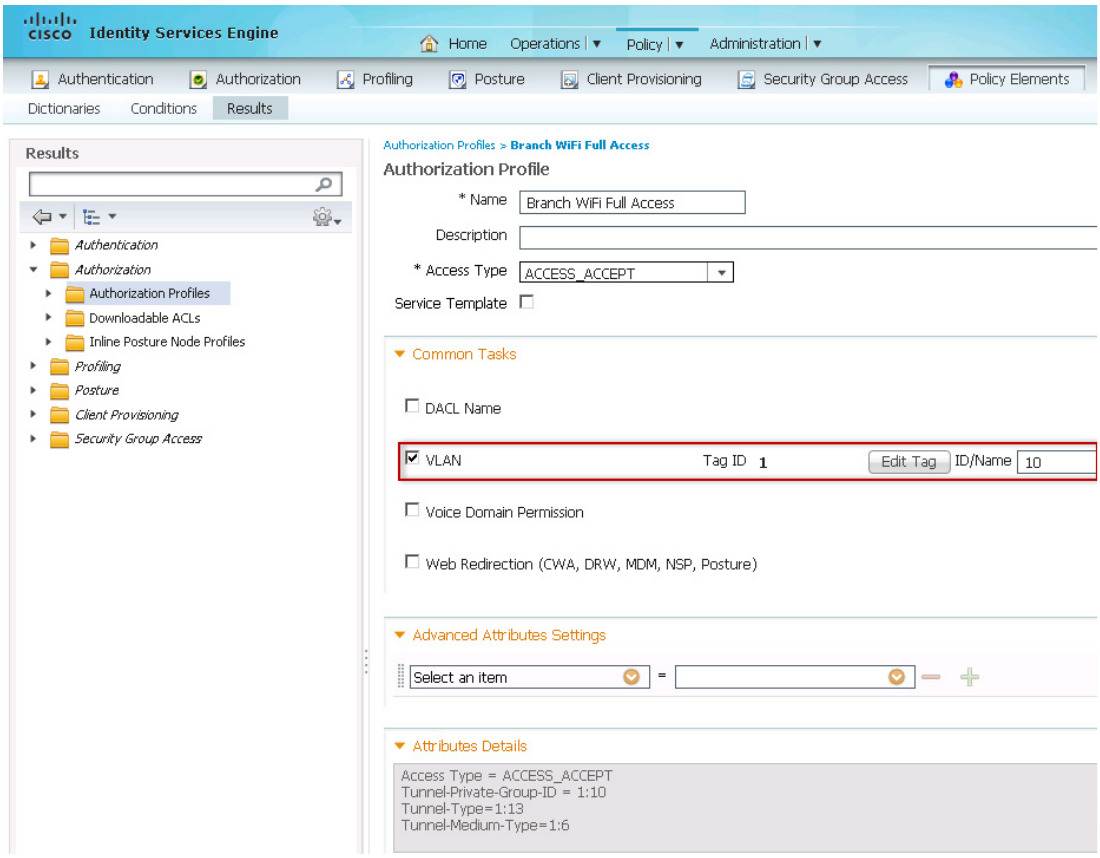


此授权配置文件允许完全访问，因此 ISE 无需指定用于访问控制的命名 ACL。

采用 FlexConnect 的分支机构

从动态实施 FlexConnect 的分支机构位置连接的终端会被分配到 VLAN 10，该 VLAN 已配置为提供完全访问权限。图 10-23 显示了分支机构 WiFi 完全访问授权配置文件。

图 10-23　　分支机构 WiFi 完全访问

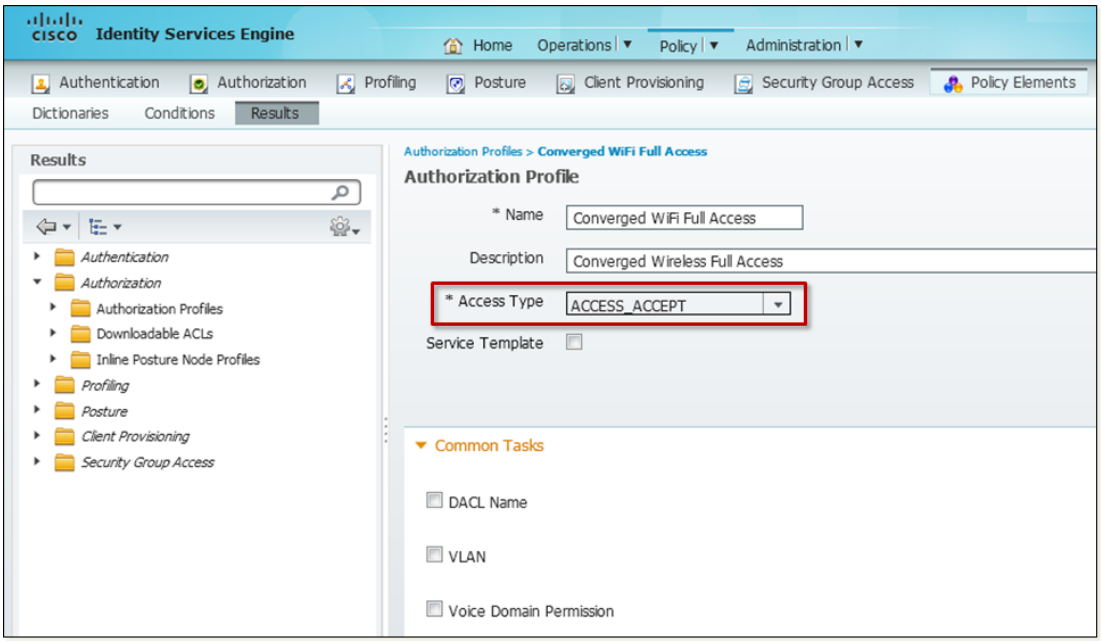


此授权配置文件允许完全访问，因此无需在接入点将用于访问控制的 FlexConnect ACL 与 VLAN 10 相关联。

融合接入分支机构或园区

图 10-24 显示了融合 WiFi 完全访问授权配置文件如何使用 ACCESS_ACCEPT 接入类型来允许完全访问。

图 10-24　　融合 WiFi 完全访问



同样，此授权配置文件允许完全访问，因此 ISE 无需指定用于访问控制的命名 ACL。

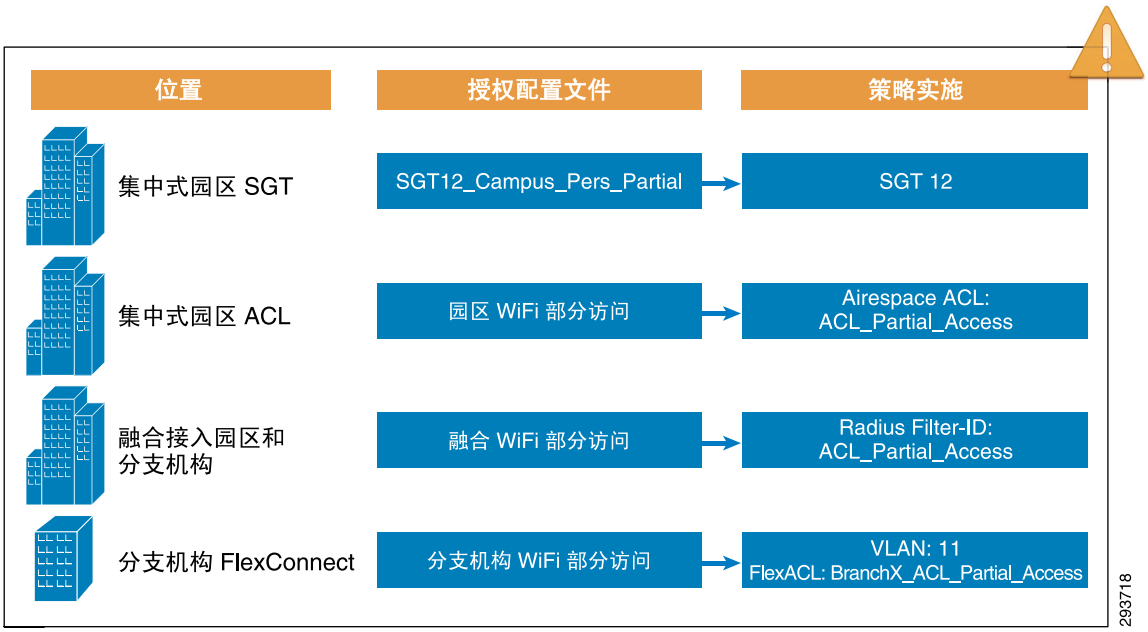
个人无线设备 - 部分访问权限

要向个人设备提供部分访问权限， Cisco ISE 会验证以下各项：

- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配 （在本例中，替代名称为终端的 MAC 地址）。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是 BYOD_Partial_Access Active Directory 组的成员。

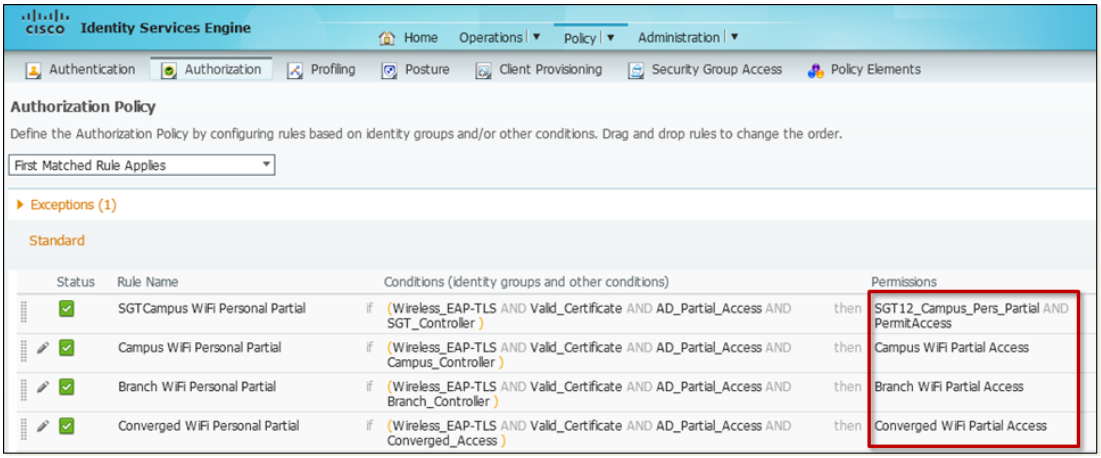
在较高层面上，图 10-25 显示了如何针对从无线设计各异的不同位置访问网络的设备选择不同授权配置文件。每个授权配置文件都会使用 VLAN、 SGT、动态 ACL、 FlexConnect ACL 等相应地实施一种唯一权限。

图 10-25　　部分访问权限实施



要在 ISE 中配置授权规则，请点击 **Policy > Authorization**。图 10-26 重点展示了向个人设备授予部分访问权限的授权策略。

图 10-26　　部分访问的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wireless_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包含的 MAC 地址匹配。（定义为简单条件）。
- 用户属于特定 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自无线控制器，该控制器是以下任一设备组的成员：Campus_Controller、SGT_Controller、 Branch_Controller 或 Converged_Access （定义为简单条件）。

简单和复合条件介绍了这些规则中使用的不同条件。

权限

权限是授权策略匹配的结果，且授权可以具有不同的类型，如授权配置文件或标准结果。表 10-7 介绍了用于部分访问的权限。

表 10-7　　用于无线部分访问的权限

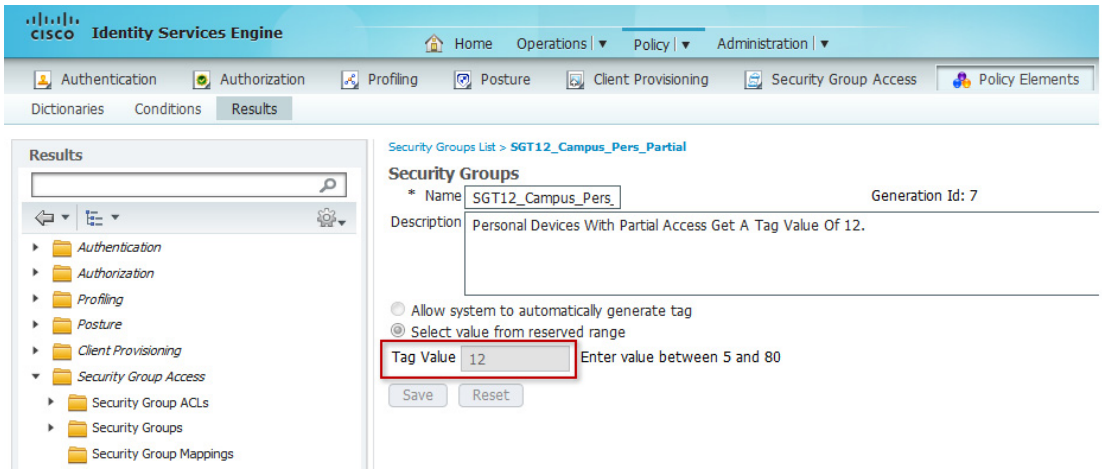
权限名称	权限类型	用途
SGT12_Campus_Pers_Partial	标准结果	向从启用了 SGT 的控制器连接的 802.1X 无线设备分配一个 SGT，该控制器可授予对数据中心中一些服务器的部分访问权限。
园区 WiFi 部分访问	授权配置文件	向从集中式园区控制器连接的 802.1X 无线设备推送命名 ACL。
分支机构 WiFi 部分访问	授权配置文件	向从 FlexConnect 分支机构控制器连接的 802.1X 无线设备推送 VLAN。
融合 WiFi 部分访问	授权配置文件	向 802.1X 无线设备推送命名 ACL，该设备从采用融合接入的园区或分支机构位置连接。

采用 SGT 的集中式园区

如安全组访问的策略实施中所述，拥有部分访问权限的个人设备会被分配 SGT 值 12。个人设备获取标记值 12 后，仅可以连接到数据中心中 SGT 值为 50 的那些服务器。

图 10-27 显示了如何配置 SGT12_Campus_Pers_Partial 授权配置文件，以向个人设备分配 SGT 12，从而允许部分访问。

图 10-27　　SGT12_Campus_Pers_Partial

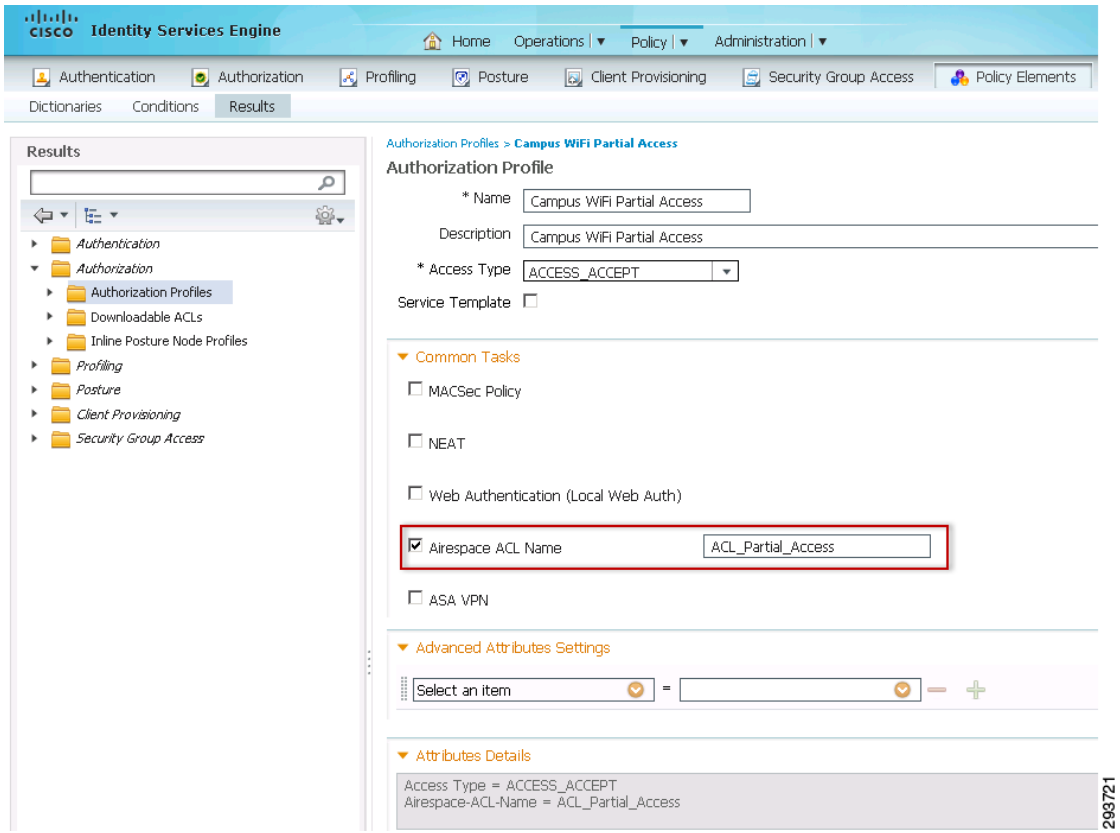


SGT 出口策略矩阵定义了 SGT12 的权限，即在园区采用 SGT 实施集中式控制器（本地模式）设计的情况下，允许其进行完全访问。请参阅安全组访问的策略实施，了解有关该矩阵的详细信息。

采用 ACL 的集中式园区

对于从实施集中式（本地模式）无线设计的园区位置连接的设备，园区 WiFi 部分访问授权配置文件依赖于 WLC 执行的 ACL_Partial_Access 访问列表。图 10-28 显示了授权配置文件。

图 10-28　　园区 WiFi 部分访问



思科无线局域网控制器支持命名 ACL，这意味着必须在控制器上提前配置 ACL，而不是直接从 ISE 下载使用。 ISE 会使用 RADIUS Airespace-ACL 名称属性值对，指示 WLC 应用 ACL_Partial_Access ACL。图 10-29 显示了此 ACL 的内容，如 CT5508 WLC 园区控制器中的定义所述。

图 10-29　　无线控制器上的 ACL_Partial_Access

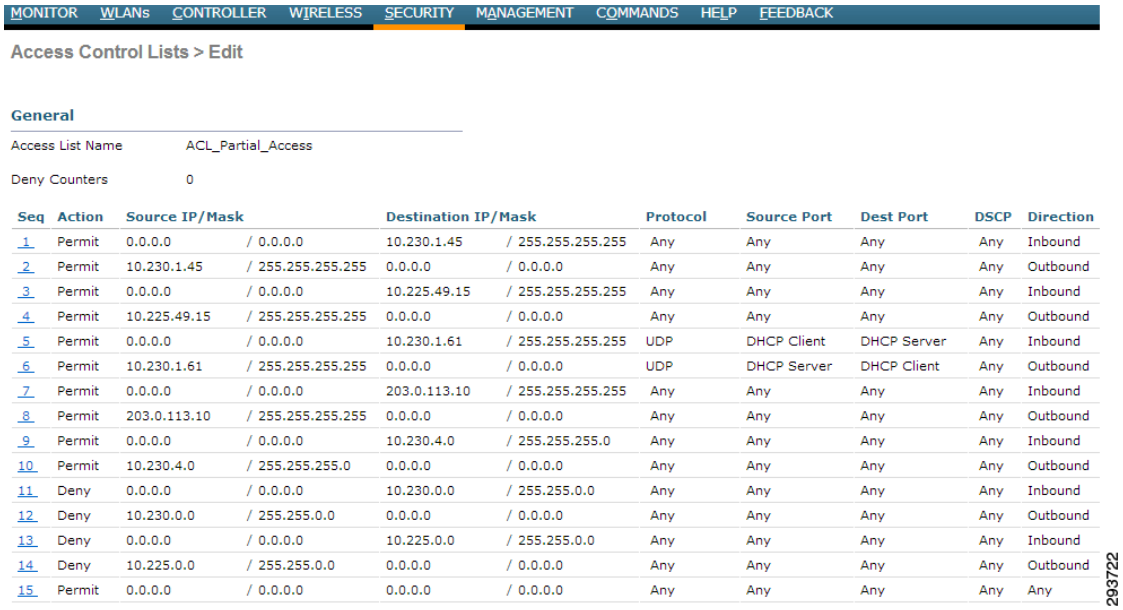


图 10-29 中显示的访问列表指定了以下访问：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 允许以 MDM 服务器 (203.0.113.10) 作为源 / 目标的 IP 访问。
- 允许以特定子网 (10.230.4.0 /24) 作为源 / 目标的 IP 访问。
- 拒绝以数据中心子网 (10.230.0.0 /16) 作为源 / 目标的 IP 访问。
- 拒绝以园区子网 (10.225.0.0 /16) 作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

注意　请注意，本章中 MDM 服务器的访问控制条目 (ACE) 包含在 ACL 中。本章中讨论的增强型访问使用案例未使用这些条目。第 11 章，“BYOD 高级用例 - 移动设备管理器集成”中讨论的高级访问使用案例使用了相同的授权策略规则和授权配置文件。

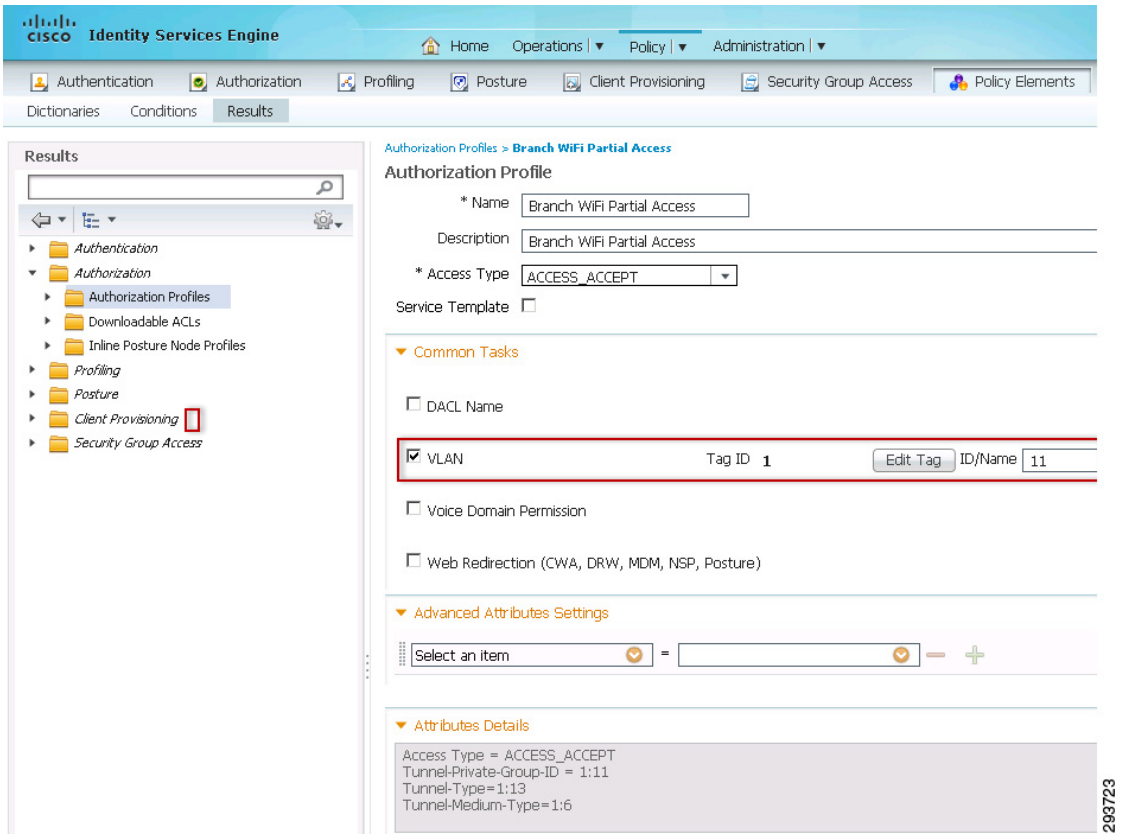
图 10-29 中显示的访问列表是用于执行假定性使用案例的一般示例，并不旨在用于每个组织。ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

注意　CT5508 WLC 最多支持 64 个 ACL，每个 ACL 最多有 64 行。

采用 FlexConnect 的分支机构

对于从实施 FlexConnect 无线设计的分支机构位置连接的设备，分支机构 WiFi 部分访问授权配置文件会将设备动态分配到 VLAN11，这是获取了部分访问权限的设备专用的 VLAN。图 10-30 显示了此授权配置文件。

图 10-30　　分支机构 WiFi 部分访问



在分支机构部署 ACL 的方式与在集中式 WLC 中使用 ACL 稍有不同。在本设计指南中，对于分支机构位置，Cisco 7500 Flex 无线控制器依赖于 FlexConnect ACL 来执行策略权限。FlexConnect ACL 在 WLC 上创建，并通过 AP 或 FlexConnect 组中定义的 VLAN 配置，同时使用针对动态或 AAA 覆盖 VLAN 的 VLAN ACL 映射。当授权策略匹配时，这些 FlexConnect ACL 会被推送到 AP。本设计指南依赖于 FlexConnect 组为每个 VLAN 实施 Flex ACL。步骤如下所示：

1. 为每个分支机构创建一个 FlexConnect ACL。
2. 为每个分支机构应用 FlexConnect 组中的 FlexConnect ACL。
3. 定义每个 VLAN 的 VLAN-ACL 映射。

在 FlexConnect 7500 控制器上，点击 **Security > Access Control Lists > FlexConnect ACLs**，并定义部分访问权限的 ACL 规则。图 10-31 显示了 Branch1_ACL_Partial_Access ACL，该 ACL 允许访问互联网和一些内部资源。

注意　每个分支机构可能需要一个唯一的 ACL，因为每个分支机构可能有各自的本地资源和唯一的 IP 地址空间。

图 10-31　　Branch1_ACL_Partial_Access

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name　Branch1_ACL_Partial_Access

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
8	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any
10	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any
12	Permit	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any
14	Permit	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
15	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

293724

上述 ACL 指定了以下访问权限：

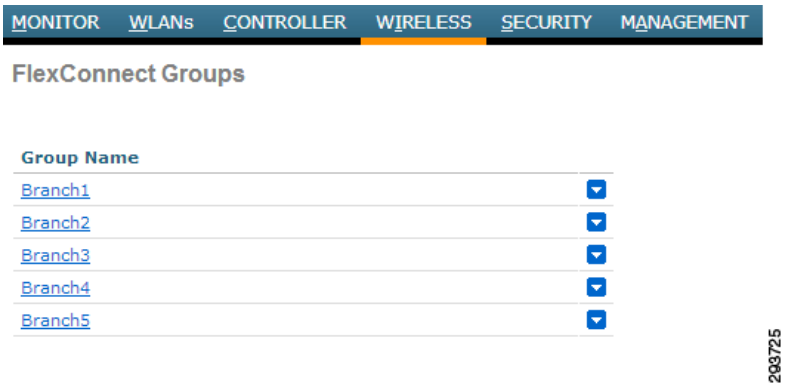
- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 允许以 MDM 服务器 (203.0.113.10) 作为源 / 目标的 IP 访问。
- 允许以特定子网 (10.230.4.0 /24) 作为源 / 目标的 IP 访问。可以添加类似的 ACL 条目，以允许访问 Branch1 子网 / 服务器。
- 拒绝以数据中心子网 (10.230.0.0 /16) 作为源 / 目标的 IP 访问。
- 拒绝以园区子网 (10.225.0.0 /16) 作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

注意　显示的访问列表是用于实施任意使用案例的一般示例，并不用于每个组织。ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

在本设计指南中，我们为每个分支机构定义了一个 FlexConnect 组，允许分支机构的多个 FlexConnect 访问点共享配置参数。

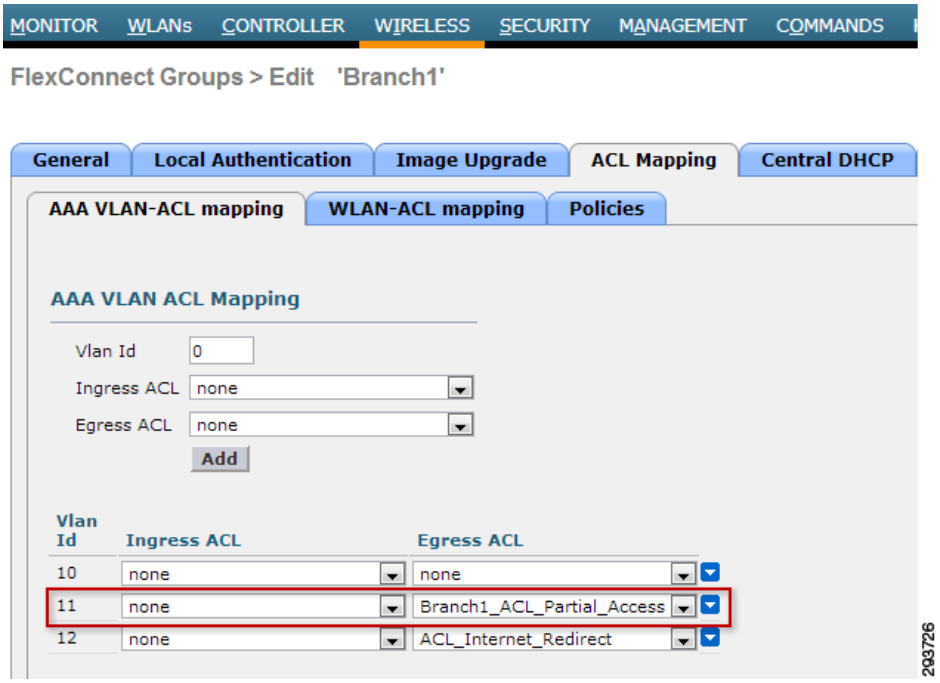
在 FlexConnect 7500 控制器上，点击 **Wireless > FlexConnect Groups**，并为特定分支机构位置选择 FlexConnect 组，如图 10-32 所示。

图 10-32　　FlexConnect 组



在图 10-33 中， Branch1 的 FlexConnect 组将 Branch1_ACL_Partial_Access ACL 应用于连接到 VLAN 11 的终端。

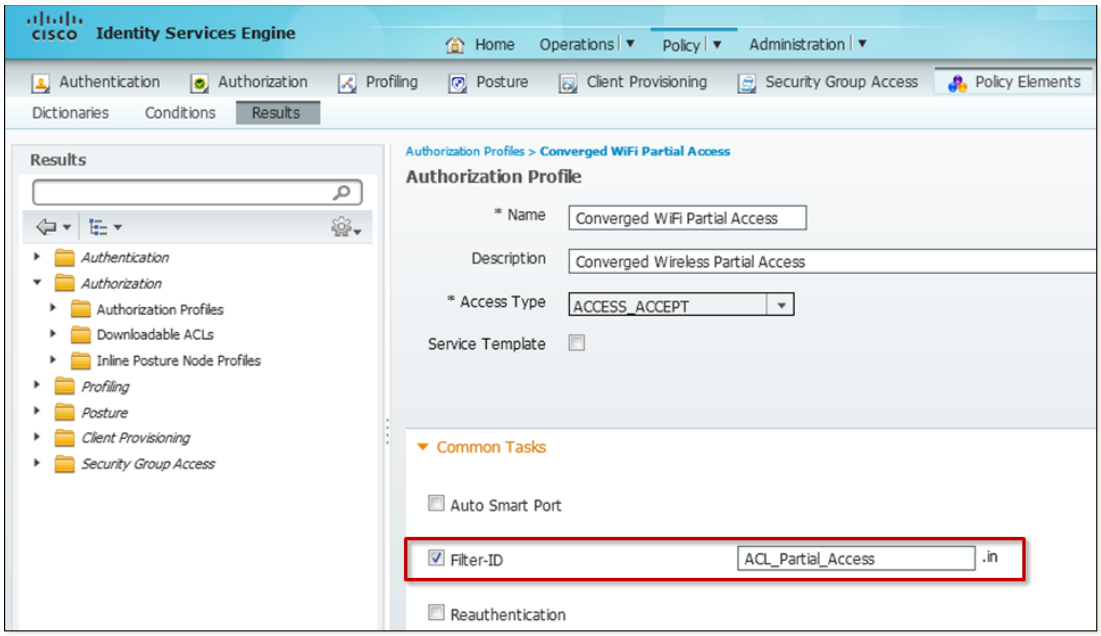
图 10-33　　Branch1 的 FlexConnect 组



融合接入分支机构或园区

对于从实施融合接入设计的园区或分支机构位置连接的设备，融合 WiFi 部分访问授权配置文件依赖于 Catalyst 3850 系列交换机执行的 ACL_Partial_Access 访问列表。图 10-34 显示了授权配置文件。

图 10-34　　融合 WiFi 部分访问



Cisco Catalyst 3850 系列交换机（以及 CT5760 无线控制器）支持命名 ACL 和可下载的 ACL。对于融合接入设计，将会实施命名 ACL，这意味着该 ACL 必须在 Catalyst 3850 交换机上进行配置，而不是直接从 ISE 下载使用。 ISE 会使用 RADIUS Filter-ID 属性值对，指示 WLC 应用 ACL_Partial_Access ACL。以下示例配置显示了此 ACL 的内容，如 Catalyst 3850 交换机中的定义所述。

```
!
ip access-list extended ACL_Partial_Access
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 203.0.113.10
 permit ip any 10.230.4.0 0.0.0.255
 permit ip any host 10.230.6.2
 permit ip any host 10.225.100.10
 deny   ip any 10.230.0.0 0.0.255.255
 deny   ip any 10.225.0.0 0.0.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
```

上述访问列表与图 29 中显示的访问列表相似，但是该列表配置在 Catalyst 交换机上，而不是无线控制器上。因此，访问列表的结构稍有不同。访问列表指定了以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 MDM 服务器 (203.0.113.10) 作为源 / 目标的 IP 访问。
- 允许以特定服务器 （10.230.6.2 和 10.225.100.10）作为源 / 目标的 IP 访问。
- 拒绝以数据中心子网 (10.230.0.0 /16) 作为源 / 目标的 IP 访问。
- 拒绝以园区子网 (10.225.0.0 /16) 作为源 / 目标的 IP 访问。
- 拒绝以分支机构子网 (10.200.0.0 /16) 作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

同样，本示例中所示的访问列表是一般性的，并不用于每个组织。 ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

注意　本指南介绍了使用 Radius:Airespace-ACL-Name AV 对，在 CT5508 和 Flex 7500 无线控制器等 CUWN 无线控制器平台上指定命名 ACL。但是，它介绍了使用 Radius:Filter-Id AV 对，在 CT5760 无线控制器和 Catalyst 3850 系列交换机等基于 Cisco IOS 的无线控制器平台上指定命名 ACL。对于无线设备，这只是为了强调一个事实：网络管理员可以在 BYOD 实施中使用传统 Airespace-ACL-Name AV 对或 Filter-Id AV 对的 Radius 标准方法。我们建议网络管理员将上述两种方法中的一种标准化，可能时在实际部署指定命名 ACL。

由于已针对来自采用融合接入基础设施的分支机构或园区的个人无线设备部分访问权限定义 ISE 策略规则，因此可以按需针对特定分支机构和园区自定义访问列表。如上所示的具体示例 ACL 与先前讨论的园区集中式 （本地模式）控制器设计中讨论的 ACL 一致。

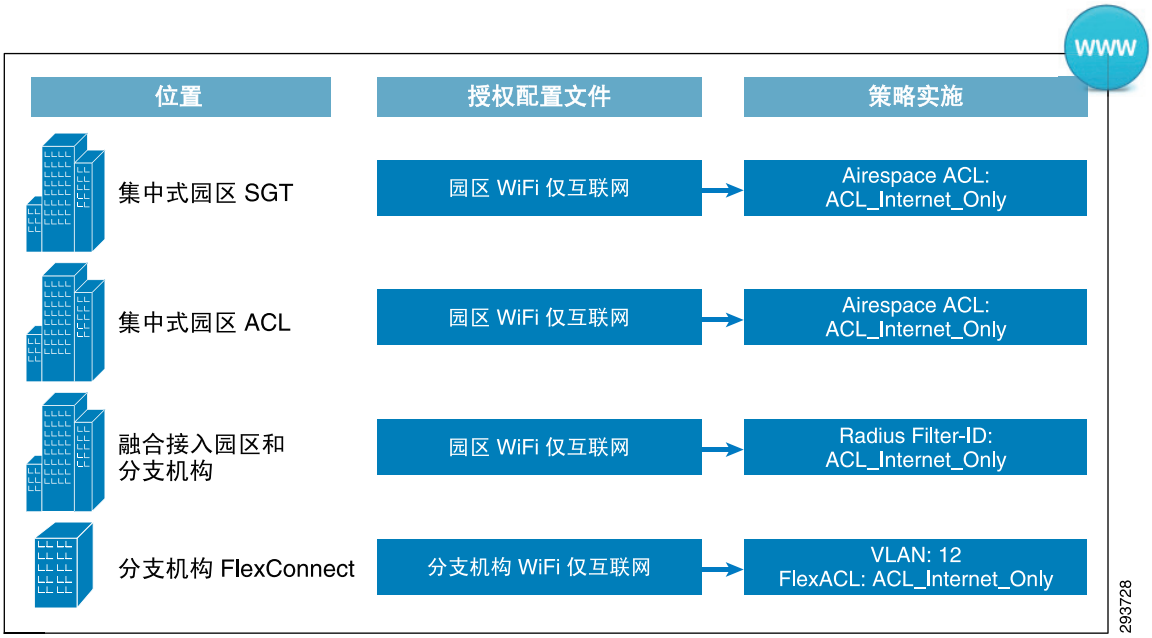
个人无线设备 - 仅互联网访问

要向个人设备提供仅互联网的访问， Cisco ISE 会验证以下各项：

- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配 （在本例中，替代名称为终端的 MAC 地址）。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是域用户 Active Directory 组的成员。

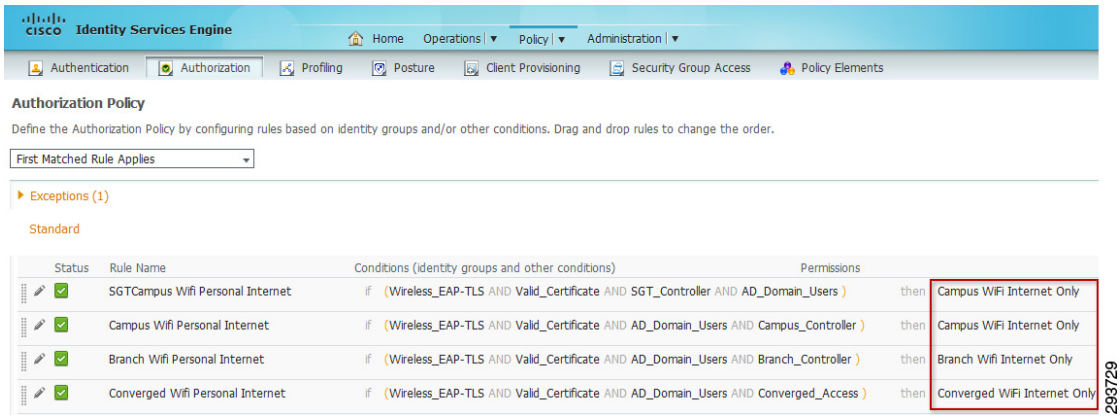
在较高层面上，图 10-35 显示了如何针对来自无线设计各异的不同位置的设备选择不同授权配置文件。每个授权配置文件会使用 VLAN、 SGT、命名 ACL、 FlexConnect ACL 等相应地实施一种唯一权限。

图 10-35　　仅互联网访问权限实施



要在 ISE 中配置授权规则，请点击 **Policy > Authorization**。图 10-36 重点展示了向个人设备授予仅互联网访问权限的授权策略。

图 10-36　　仅互联网访问的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wireless_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包括的 MAC 地址匹配（定义为简单条件）。
- 用户属于域用户 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自无线控制器，该控制器是以下任一设备组的成员：Campus_Controller、SGT_Controller、 Branch_Controller 或 Converged_Access （定义为简单条件）。

简单和复合条件介绍了这些规则中使用的不同条件。

权限

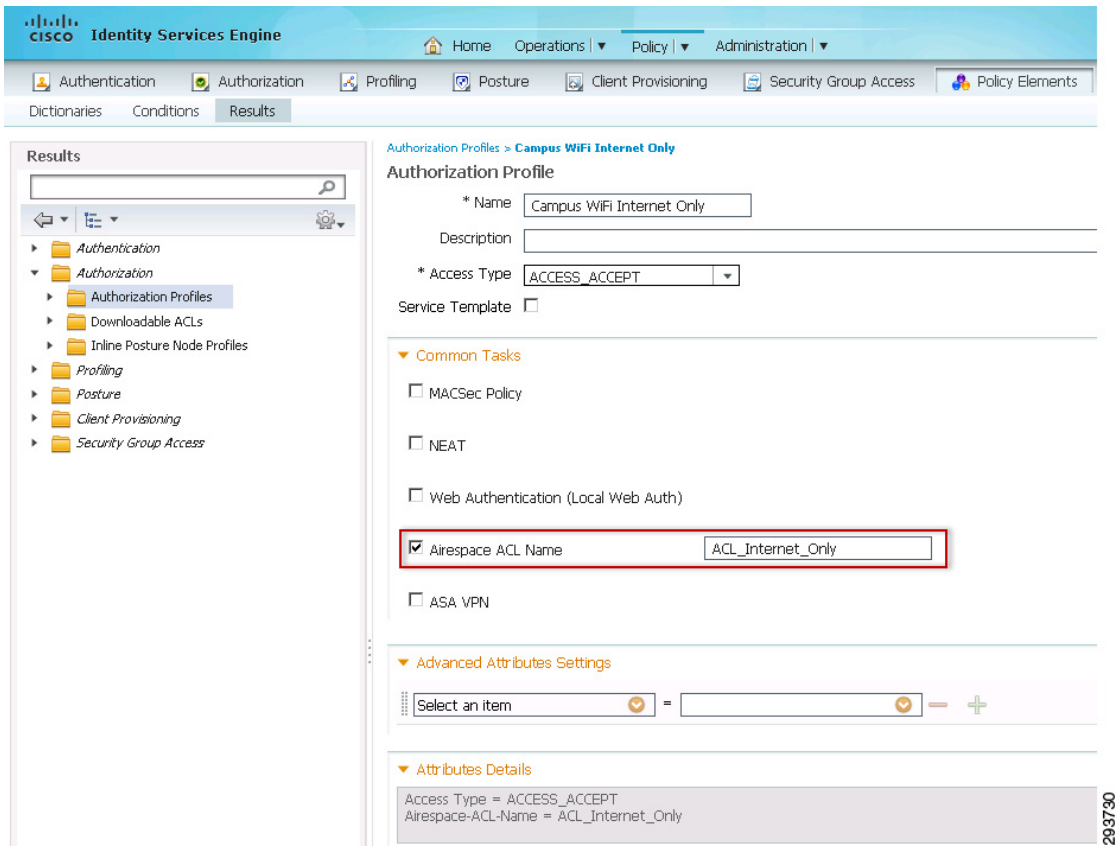
当授权策略规则中的所有条件都匹配时，规则会调用相应权限。在前面的部分中，权限结果既可以是授权配置文件 （非基于 SGT 的访问），也可以是标准结果 （基于 SGT 的访问）。但是，此部分中仅会使用授权配置文件，原因如下。

- 园区 WiFi 仅互联网适用于从 SGT_Enabled 控制器或从具有集中式 （本地模式）无线设计的园区连接的 802.1X 无线设备。园区控制器和 SGT_Enabled 控制器使用相同的授权配置文件。SGT 不用于标记仅互联网访问的流量，因为 SGT 依赖于源标记和目标标记，而互联网的目标标记未知。
- 分支机构无线仅互联网访问权限适用于从实施 Flexconnect 无线设计的分支机构位置连接的 802.1X 无线设备。
- 融合 WiFi 仅互联网适用于从实施融合接入基础设施设计的园区或分支机构位置连接的 802.1X 无线设备。

采用 SGT 或 ACL 的集中式园区

对于从实施集中式 （本地模式）无线设计的园区位置或从 SGT_Enabled 控制器连接的设备，园区 WiFi 仅互联网授权配置文件依赖于 WLC 执行的 ACL_Internet_Only 访问列表。图 10-37 显示了授权配置文件如何指示 WLC 应用 ACL。

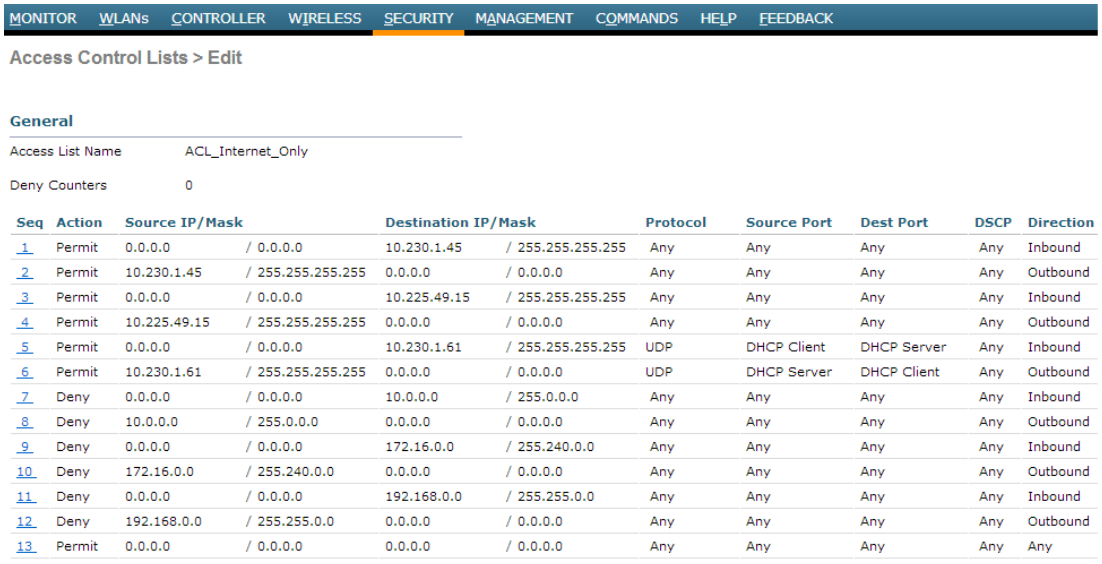
图 10-37　　园区 WiFi 仅互联网



思科无线局域网控制器支持命名 ACL，这意味着必须在控制器上提前配置 ACL，而不是直接从 ISE 下载使用。 ISE 会使用 RADIUS Airespace-ACL 名称属性值对，指示 WLC 应用 ACL_Internet_Only ACL。

图 10-38 显示了此 ACL 的内容，如 CT5508 WLC 园区控制器中的定义所述。

图 10-38　　ACL_Internet_Only



访问列表指定了以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 拒绝以内部网络地址空间（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

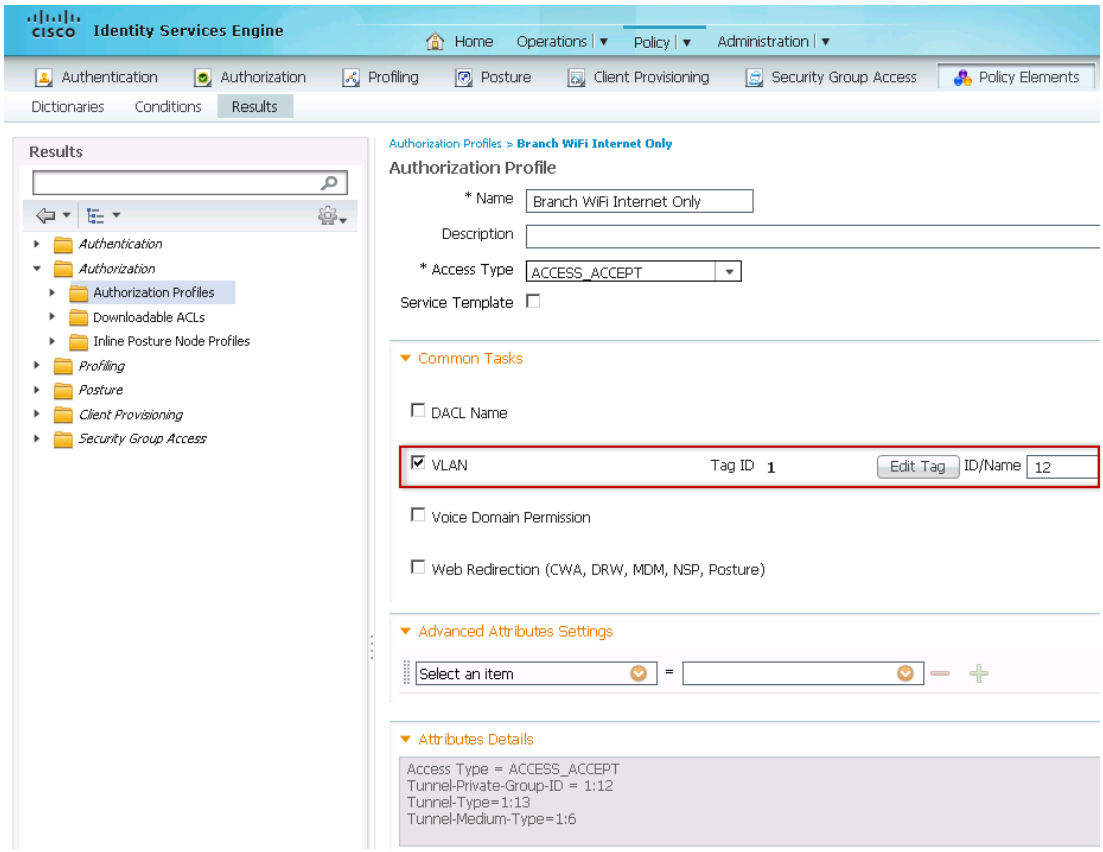
同样，访问列表是一般性的，并不用于每个组织。 ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

采用 FlexConnect 的分支机构

对于从实施 FlexConnect 无线设计的分支机构位置连接的设备，分支机构 WiFi 仅互联网授权配置文件会将设备动态分配到 VLAN12，这是获取了 Internet_Only 权限的设备专用的 VLAN。

图 10-39 显示了此授权配置文件。

图 10-39　　分支机构 WiFi 仅互联网



对于实施 FlexConnect 无线设计的分支机构位置，Cisco 7500 Flex 无线控制器依赖于 FlexConnect ACL 执行策略权限。 FlexConnect ACL 在 WLC 上创建，并通过 AP 或 FlexConnect 组中定义的 VLAN 配置，同时使用针对动态或 AAA 覆盖 VLAN 的 VLAN ACL 映射。当授权策略匹配时，这些 FlexConnect ACL 会被推送到 AP。

1. 为每个分支机构创建一个 FlexConnect ACL。
2. 为每个分支机构应用 FlexConnect 组中的 FlexConnect ACL。
3. 定义每个 VLAN 的 VLAN-ACL 映射。

在 FlexConnect 7500 控制器上，点击 **Security > Access Control Lists > FlexConnect ACLs**，并定义 Internet_Only 访问权限的 ACL 规则。图 10-40 显示了 Branch_ACL_Internet_Only ACL 的示例，该 ACL 仅允许访问互联网。此 ACL 在所有分支机构中都一样。

图 10-40　Branch_ACL_Internet_Only

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name　Branch_ACL_Internet_Only

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
8	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
10	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
12	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

293733

访问列表指定了以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 (10.230.1.61) 作为源 / 目标的 IP 访问。
- 拒绝以内部网络地址空间（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

该访问列表是一般性的，并不用于每个组织。ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

在本设计指南中，我们为每个分支机构定义了一个 FlexConnect 组，允许分支机构的多个 FlexConnect 访问点共享配置参数。

在 FlexConnect 7500 控制器上，点击 **Wireless > FlexConnect Groups**，并为特定分支机构位置选择 FlexConnect 组，如图 10-41 所示。

图 10-41　FlexConnect 组

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

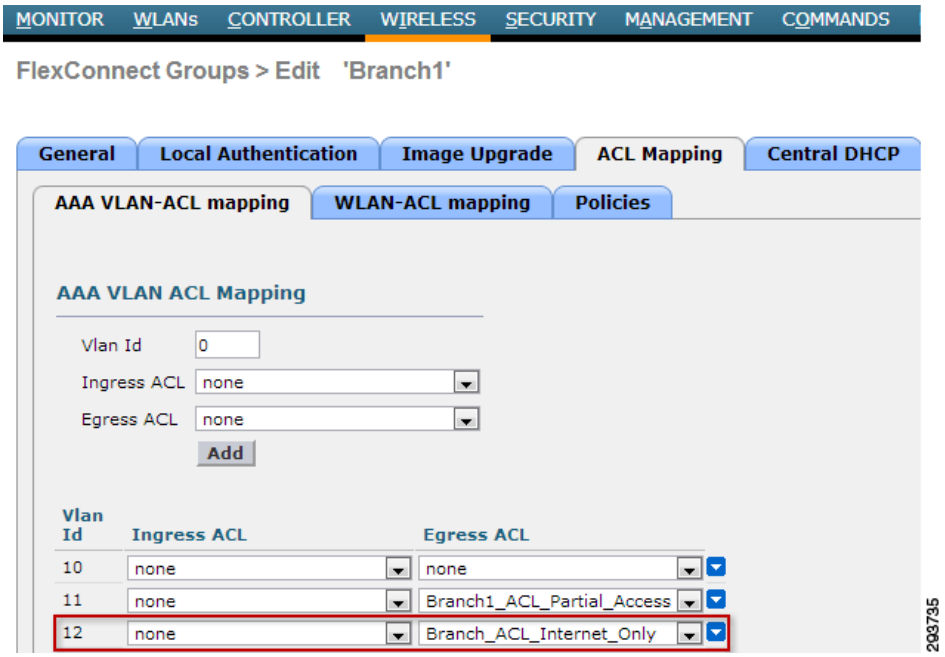
FlexConnect Groups

Group Name
Branch1
Branch2
Branch3
Branch4
Branch5

293734

在图 10-42 中， Branch1 的 FlexConnect 组将 Branch_ACL_Internet_Only ACL 应用于连接到 VLAN 12 的终端。

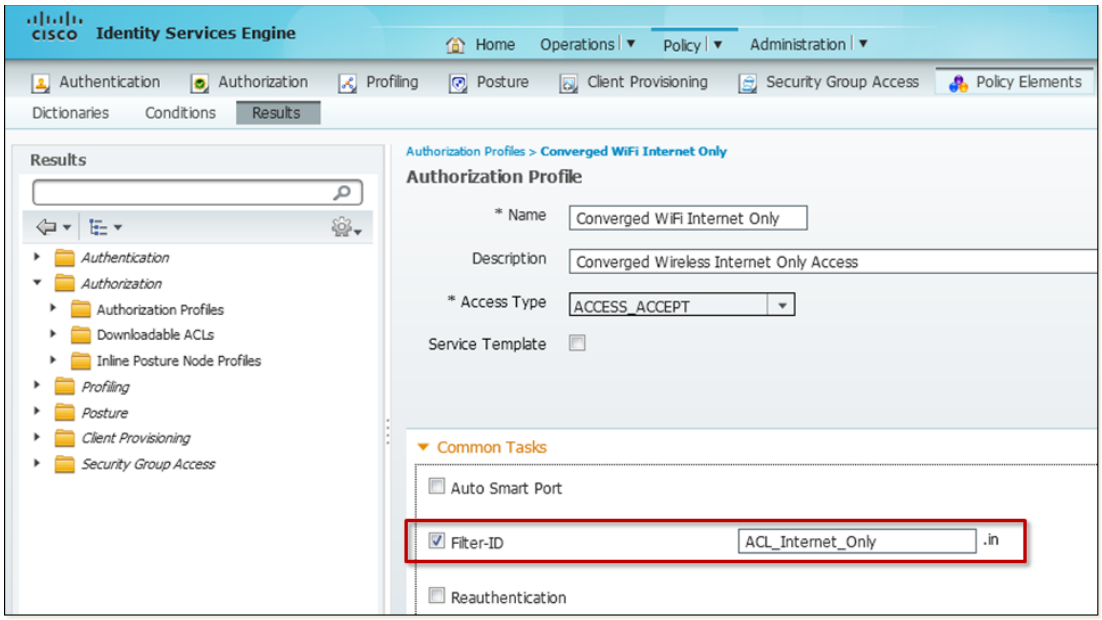
图 10-42　　Branch1 仅互联网访问的 FlexConnect 组



融合接入分支机构或园区

对于从实施融合接入设计的园区或分支机构位置连接的设备，融合 WiFi 仅互联网授权配置文件依赖于 Catalyst 3850 系列交换机执行的 ACL_Internet_Only 访问列表。图 10-43 显示了授权配置文件。

图 10-43　　融合 WiFi 仅互联网



Cisco Catalyst 3850 系列交换机 （以及 CT5760 无线控制器）支持命名 ACL 和可下载的 ACL。对于融合接入设计，将会实施命名 ACL，这意味着该 ACL 必须在 Catalyst 3850 交换机上进行配置，而不是直接从 ISE 下载使用。 ISE 会使用 RADIUS Filter-ID 属性值，指示 WLC 应用 ACL_Internet_Only ACL。以下示例配置显示了此 ACL 的内容，如 Catalyst 3850 交换机中的定义所述。

```
ip access-list extended ACL_Internet_Only
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.225.100.10
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
!
```

以上所示的访问列表与图 10-38 中显示的访问列表相似，但是该列表配置在 Catalyst 交换机上，而不是无线控制器上。因此，访问列表的结构稍有不同。但是，访问列表指定了以下访问权限：

- 允许 DHCP 访问 （bootpc 和 bootps）。
- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 拒绝以内部网络 IP 地址空间其他位置 （10.0.0.0 /8、 172.16.0.0 /12、 192.168.0.0 /16）作为源 / 目标的 IP 访问。
- 允许以所有其他地址 （互联网地址）作为目标的访问。

注意　上面显示的 MDM 具有私有 RFC1918 地址。在实际操作中， MDM 必须可从公共互联网访问，并且可能不需要 ACL 中的特定行条目。

同样，本示例中所示的访问列表是一般性的，并不用于每个组织。 ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

个人有线设备 - 完全访问权限

要向个人有线设备提供完全访问权限， Cisco ISE 会验证以下各项：

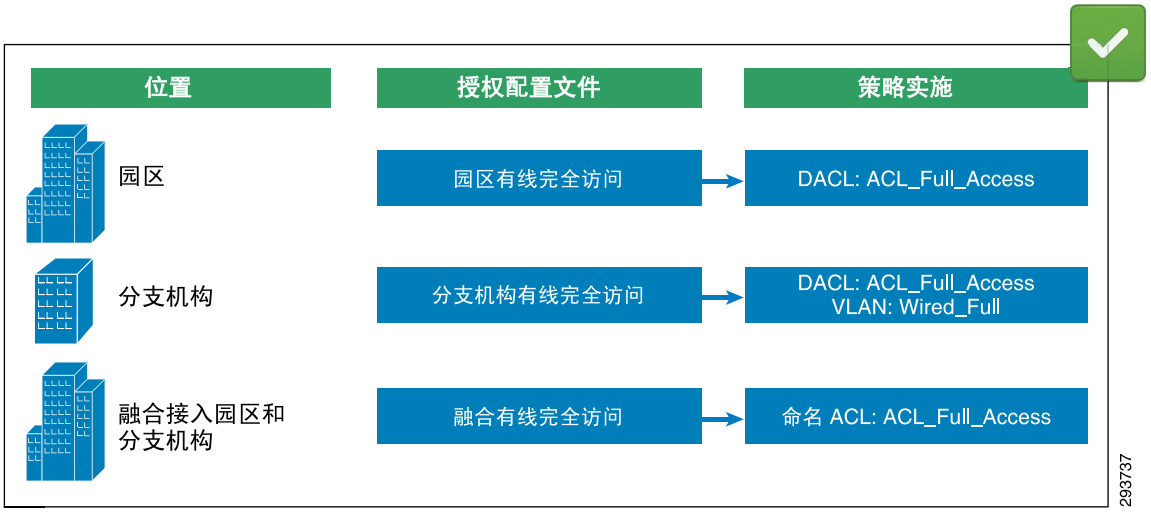
- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配 （在本例中，替代名称为终端的 MAC 地址）。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是 BYOD_Full_Access Active Directory 组的成员。

由于本设计指南中介绍的有线设计对融合接入园区和分支机构依赖于略不相同的访问控制机制，因此，对于未实施融合接入基础设施的园区和分支机构，会针对从每种设计发起的连接创建独特的授权规则。

注意　为了明确本设计指南，融合接入分支机构是指在分支机构网络的接入层部署 Catalyst 3850 系列交换机的设计。从有线角度看，未实施融合接入基础设施的分支机构是部署了 Catalyst 3750X 系列等其他 Catalyst 接入层交换机的分支机构。除非另有说明，否则这些在本设计指南中仅称为 “分支机构”。同样，融合接入园区是指在园区内建筑分布模块的接入层部署 Catalyst 3850 系列交换机的设计。从有线角度看，未实施融合接入基础设施的园区是部署了 Catalyst 3750X 系列等其他 Catalyst 接入层交换机的园区。除非另有说明，否则这些在本设计指南中仅称为 “园区”。这是为了尽量减少冗长语句的使用，例如，“未实施融合接入基础设施的分支机构”和 “未实施融合接入基础设施的园区”。

在较高层面上，图 10-44 显示了如何针对从基础设施设计各异的不同位置发起的连接选择不同授权配置文件。每个授权配置文件会使用 VLAN、动态 ACL （命名或可下载的 [DACL]）等相应地实施一种唯一权限。

图 10-44　　完全访问权限有线实施

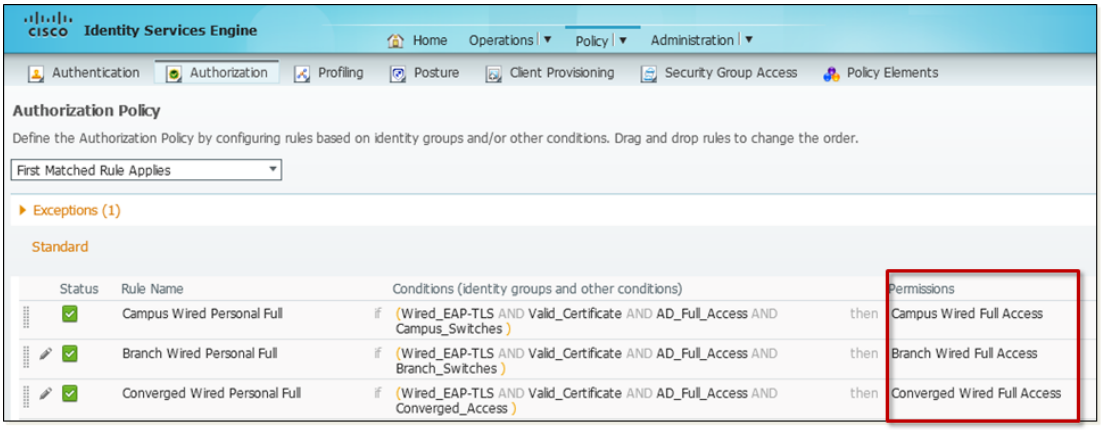


注意　本版设计指南未讨论安全组标记 (SGT) 的有线分配。因此，图 10-44 中没有通过 SGT 的有线策略实施。本指南的未来版本可能会介绍有线 SGT 分配。

为了区分这些连接， ISE 依赖于网络设备组来根据位置或设备类型对 Catalyst 交换机进行分组。这样，单个 ISE 就可以在不同设备组中实施策略。每个 Catalyst 交换机都需要添加到适当的设备组中，方式为点击 **Administration > Network Resources > Network Devices**，然后从下拉菜单中指定适当位置或设备类型。

图 10-45 显示了 ISE 中针对有线设备配置的授权配置文件的详细信息。

图 10-45　　有线完全访问的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wired_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包含的 MAC 地址匹配。（定义为简单条件）。
- 用户属于特定 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自 Catalyst 交换机，该交换机是以下任一设备组的成员： Campus_Switches、 Branch_Switches 或 Converged_Access （定义为简单条件）。

有线简单和复合条件

为了提高授权策略的可读性，本设计定义了简单和复合授权条件，便于对不同条件进行分组。无需更改每条授权规则，即可重复使用和修改这些条件。

表 10-8 显示了授权规则中使用的条件。

表 10-8　简单和复合条件

有线 EAP-TLS （复合）	
Wired_EAP-TLS	Radius:Service-Type Equals Framed Radius:NAS-Port-Type Equals Ethernet Network Access:EapAuthentication Equals EAP-TLS
检查有效证书 （简单）	
Valid_Certificate	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
Active Directory 组 （简单）	
AD_ Full_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Full_Access
AD_ Partial_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Partial_Access
AD_Domain_users	AD1:ExternalGroups EQUALS sdulab.com/Users/Domain User
WLC 位置或设备类型 （简单）	
Campus_Switches	DEVICE:Location EQUALS All Locations#Campus_Switches
Branch_Switches	DEVICE:Location EQUALS All Locations#Branch_Switches
Converged_Access	DEVICE:Device Type EQUALS All Device Types#Converged

权限

当授权策略规则中的所有条件都匹配时，规则会执行相应权限。权限可以是不同形式，如授权配置文件或标准结果。在本设计指南中，对于有线访问，授权策略用作策略规则匹配情况下的权限。表 10-9 介绍了用于有线用户完全访问的权限。

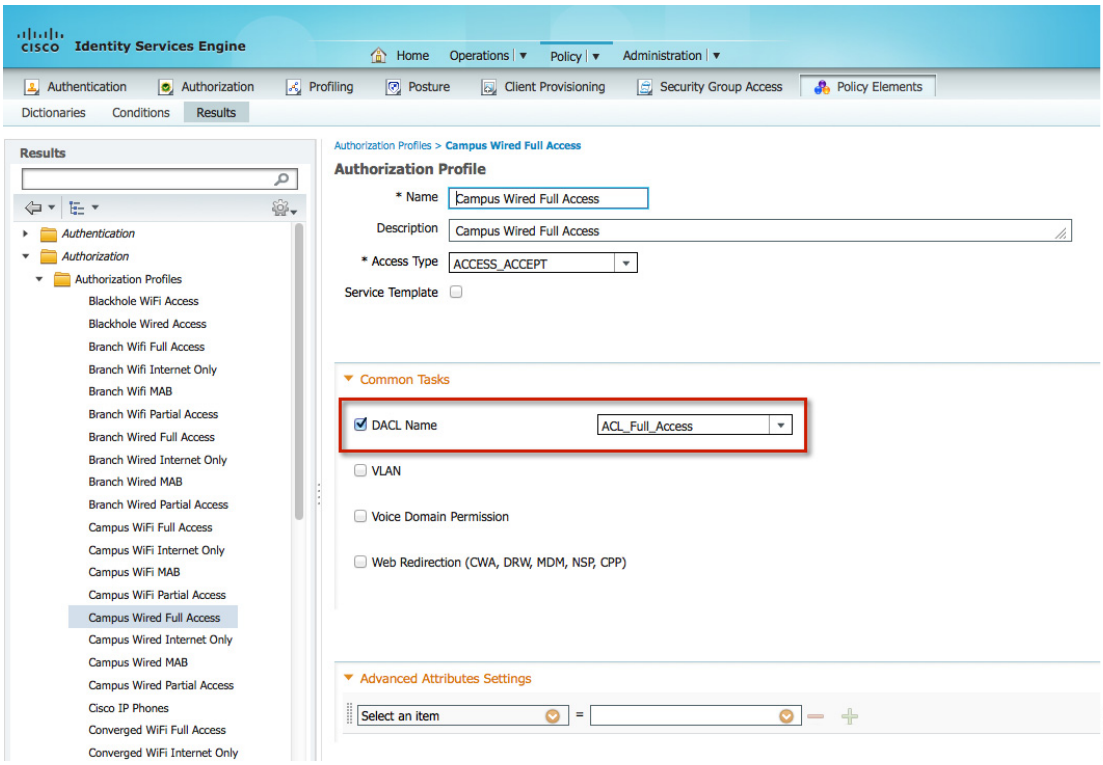
表 10-9　用于有线完全访问的权限

权限名称	权限类型	用途
园区有线完全访问	授权配置文件	向从园区位置连接的 802.1X 有线设备提供完全访问权限。
分支机构有线完全访问	授权配置文件	向从分支机构位置连接的 802.1X 无线设备推送 VLAN。
融合有线完全访问	授权配置文件	向 802.1X 有线设备推送命名 ACL，该设备从采用融合接入的园区或分支机构位置连接。

园区有线

图 10-46 显示了 ISE 中如何定义园区有线完全访问授权配置文件。

图 10-46　　园区有线完全访问授权配置文件

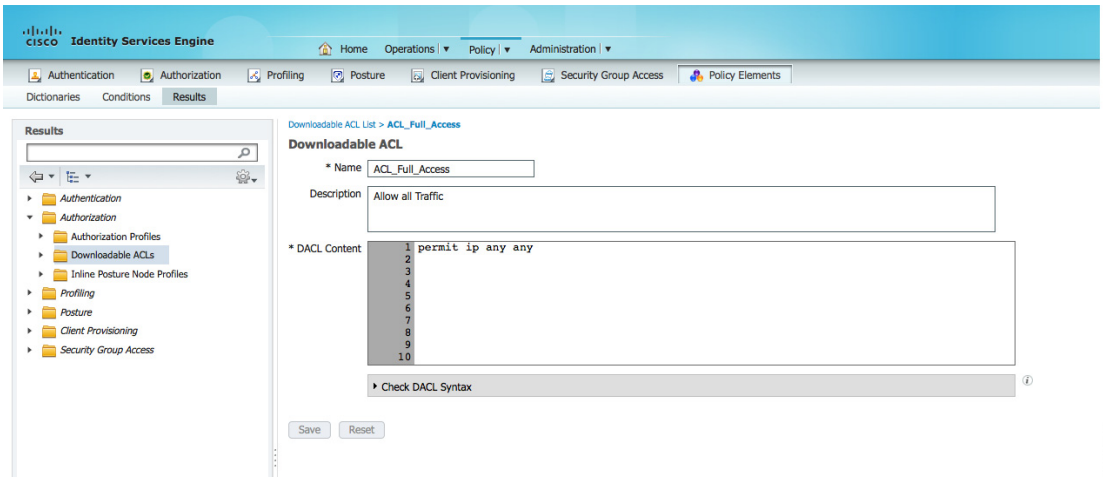


注意

Cisco Catalyst 交换机支持可下载的 ACL (DACL) 和命名 ACL。本设计指南介绍了两种 ACL 的使用，一种是实施非融合接入基础设施时用于有线设备访问控制的可下载的 ACL，另一种是实施融合接入基础设施时用于有线设备访问控制的命名 ACL。这是为了介绍基于 Cisco IOS 的平台可提供的访问控制功能的范围。如果客户需要，可以实现针对融合接入和非融合接入基础设施的相同有线策略实施，只需在两种设计中使用可下载的 ACL (DACL) 或命名 ACL 即可。可下载的 ACL 和命名 ACL 都既有优点，也有缺点，具体取决于它们在网络中的部署位置。

可下载的 ACL (DACL) 允许所有 IP 流量，会覆盖配置在交换机端口上的默认 ACL。如果由于某种原因，可下载的 ACL 未应用到交换机端口，则默认 ACL 会作为额外的预防措施。图 10-47 显示了 ISE 中必须配置的 DACL 定义：

图 10-47　　ISE 中向用户授予完全访问权限的 DACL 定义

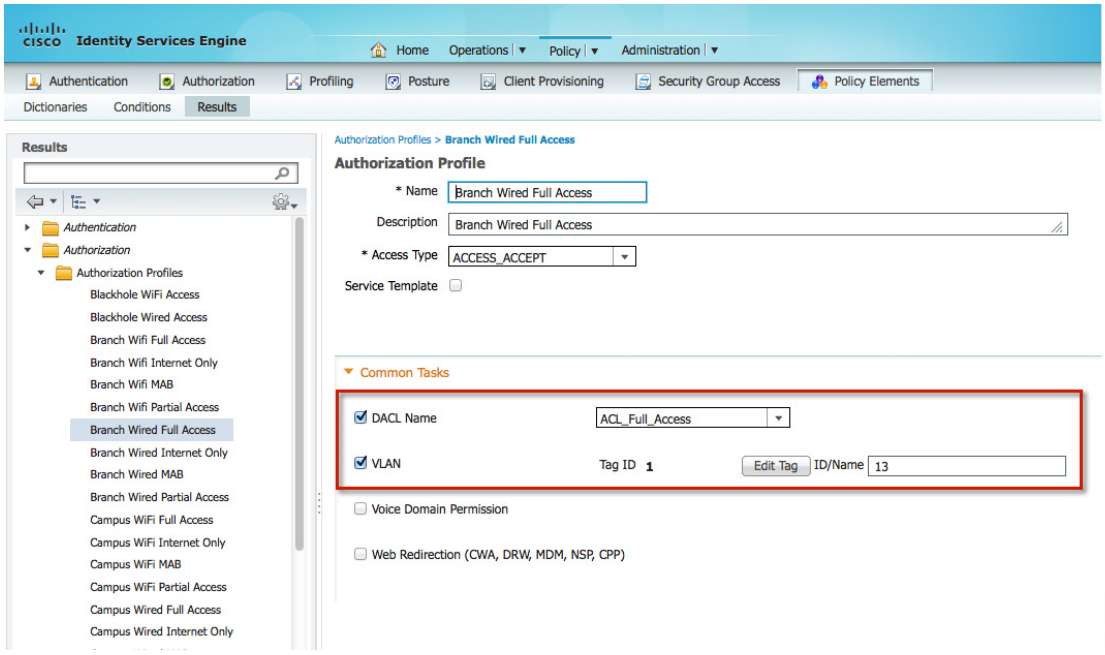


注意　ISE 1.2 能够检查 DACL 语法。应使用此功能，以尽量减少因语法错误未应用 DACL 的可能性。

分支机构有线

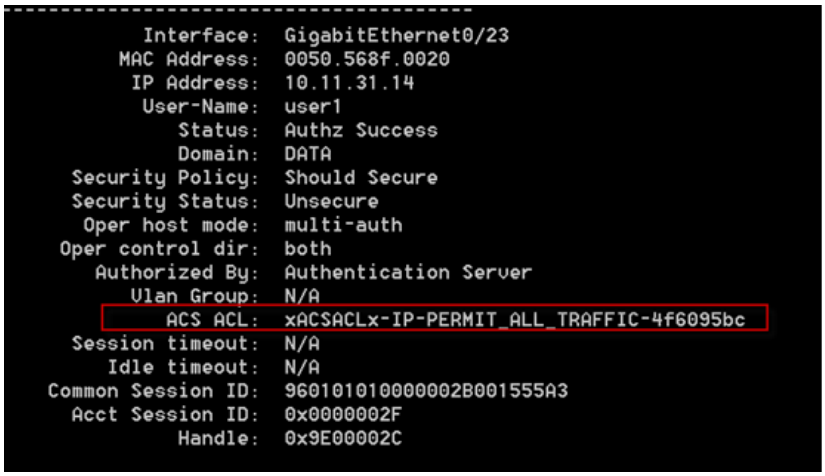
图 10-48 显示如何针对从未采用融合接入基础设施的分支机构连接的设备创建授权配置文件。授权配置文件会推送 VLAN 信息（在本示例中，为 VLAN 名称）和 ACL 信息。

图 10-48　　分支机构有线完全访问授权配置文件



此配置文件下载到 Catalyst 交换机后，终端会获得网络的完全访问权限。图 10-49 显示了使用开关命令 show authentication session interface Gi0/23 下载此配置文件后端口状态的示例。

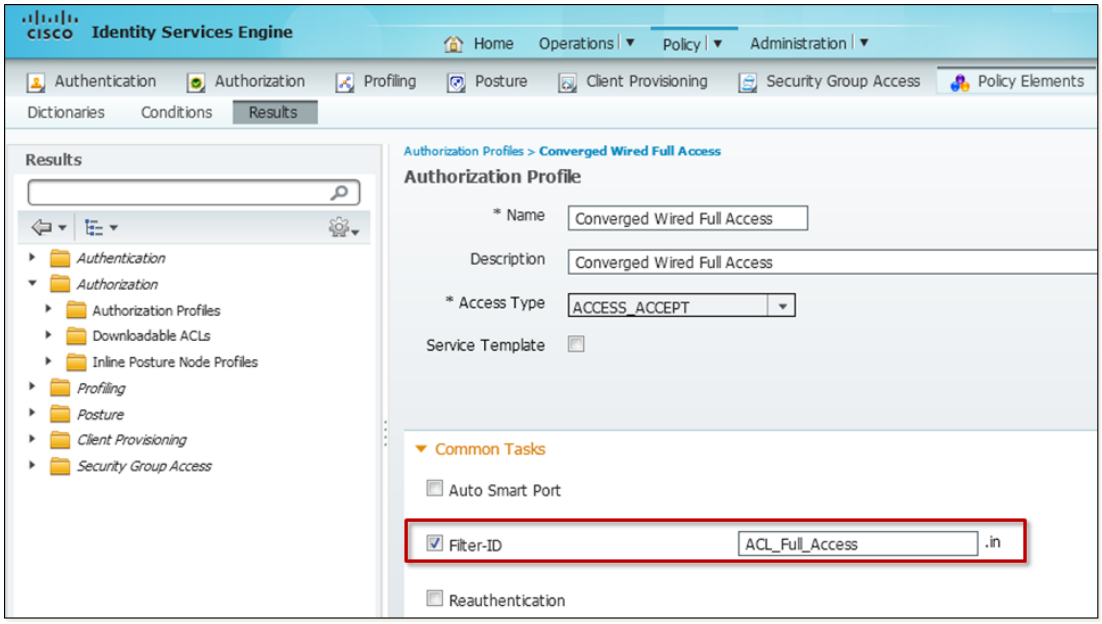
图 10-49　　Catalyst 交换机端口



融合接入分支机构或园区

图 10-50 显示了 ISE 中如何定义融合有线完全访问授权配置文件。

图 10-50　　融合有线完全访问授权配置文件



对于融合接入设计，将会实施命名 ACL，这意味着该 ACL 必须在 Catalyst 3850 交换机上进行配置，而不是直接从 ISE 下载使用。 ISE 会使用 RADIUS Filter-ID 属性值对，指示融合接入交换机应用 ACL_Full_Access ACL。以下示例配置显示了此 ACL 的内容，如 Catalyst 3850 交换机中的定义所述。

```
!
ip access-list extended ACL_Full_Access
 permit ip any any
!
```

此 ACL 用于覆盖交换机端口上配置的默认 ACL。如果交换机上未配置 ACL_Full_Access，则默认 ACL 会用作额外的预防措施。

个人有线设备 - 部分访问权限

除了互联网访问之外，部分访问权限还授予对企业资源的访问权限。如个人无线设备 - 部分访问权限所述，设备通过 ISE 的身份验证后，将会应用一个授权配置文件。对于有线设备，授权配置文件应用到接入层交换机。

要向个人有线设备提供部分访问权限， Cisco ISE 会验证以下各项：

- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配 （在本例中，替代名称为终端的 MAC 地址）。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是 AD_Partial_Access Active Directory 组的成员。

在较高层面上，图 10-51 显示了如何针对来自基础设施设计各异的不同位置的设备选择不同授权配置文件。每个授权配置文件会使用 VLAN、动态 ACL （命名或可下载的 [DACL]）等相应地实施一种唯一权限。

图 10-51　　有线部分访问权限实施

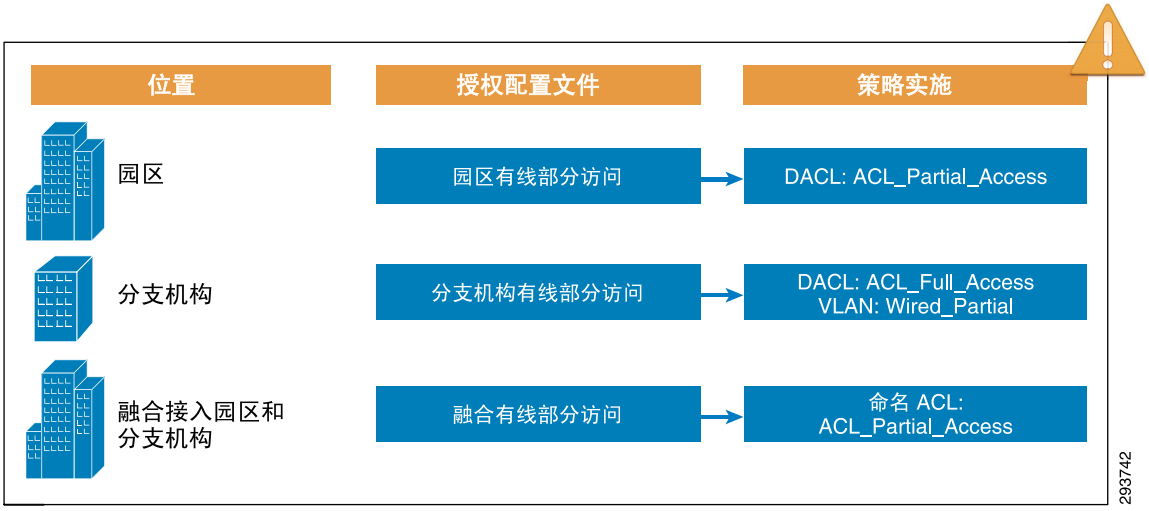
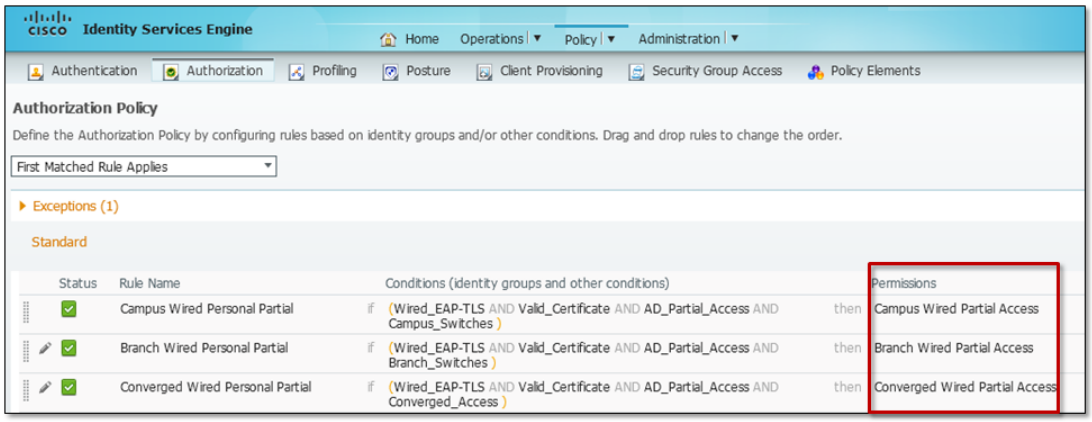


图 10-52 显示了 ISE 中针对有线设备配置的授权配置文件的详细信息。

图 10-52　有线部分访问的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wired_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包含的 MAC 地址匹配。（定义为简单条件）。
- 用户属于特定 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自 Catalyst 交换机，该交换机是以下任一设备组的成员：Campus_Switches、 Branch_Switches 或 Converged_Access （定义为简单条件）。

有线简单和复合条件介绍了这些规则中使用的不同条件。

权限

当授权策略规则中的所有条件都匹配时，规则会执行相应权限。权限可以是不同形式，如授权配置文件或标准结果。在本设计指南中，对于有线访问，授权策略用作策略规则匹配情况下的权限。表 10-10 介绍了用于有线用户部分访问的权限。

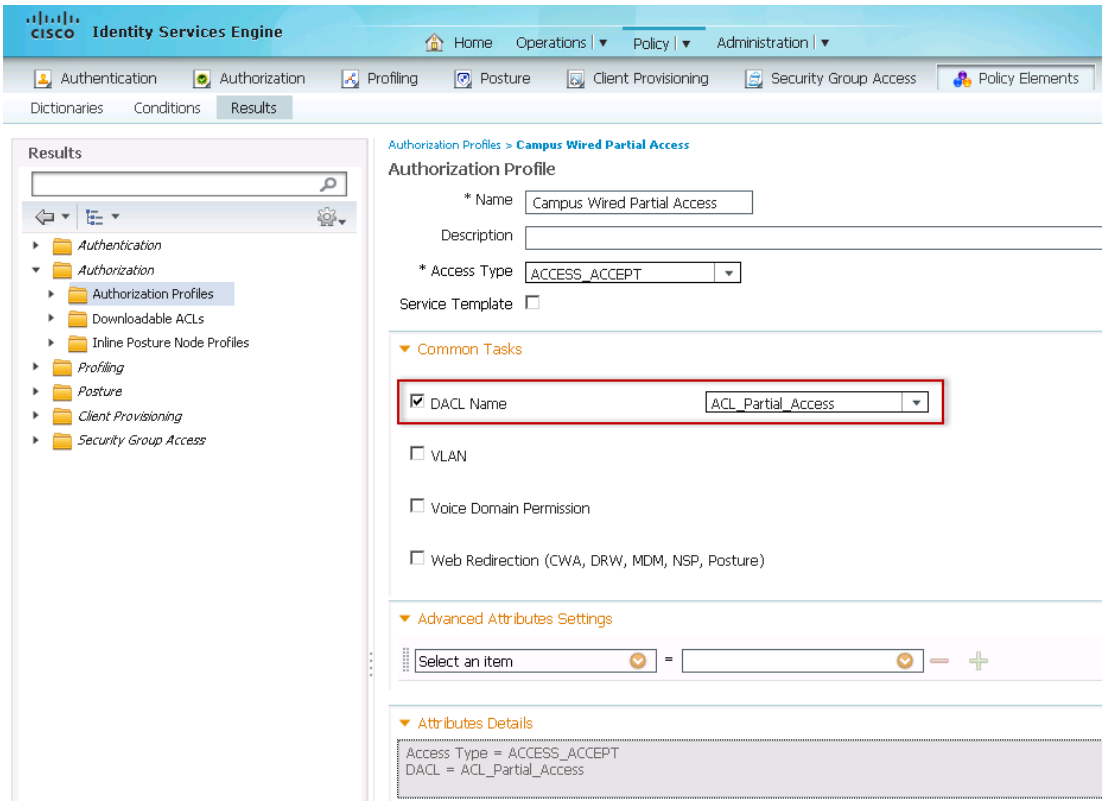
表 10-10　用于有线部分访问的权限

权限名称	权限类型	用途
园区有线部分访问	授权配置文件	向从园区位置连接的 802.1X 有线设备推送 DACL。
分支机构有线部分访问	授权配置文件	向从分支机构位置连接的 802.1X 无线设备推送 VLAN。
融合有线部分访问	授权配置文件	向 802.1X 有线设备推送命名 ACL，该设备从采用融合接入的园区或分支机构位置连接。

园区有线

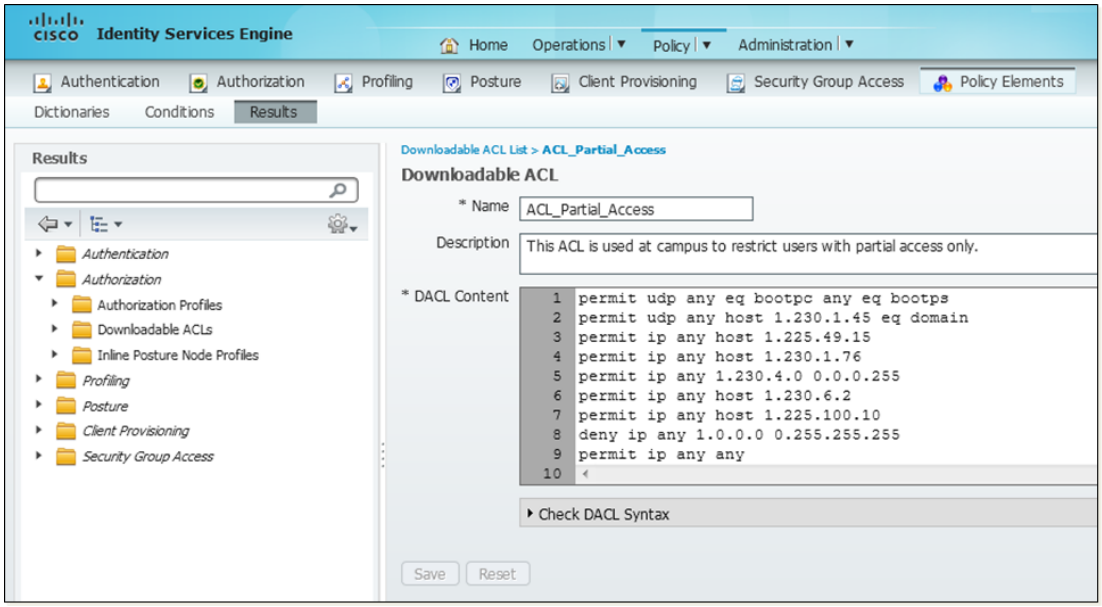
对于从园区位置连接的设备，园区有线部分访问授权使用由接入层交换机执行的名为 ACL_Partial_Access 的 DACL，如图 10-53 所示。

图 10-53　　园区有线部分访问



DACL 会覆盖交换机上配置的默认 ACL。图 10-54 显示了此 ACL 示例，该 ACL 在 ISE 中配置。

图 10-54　　ISE 中的 ACL_Partial_Access



上述 ACL 指定了以下访问权限：

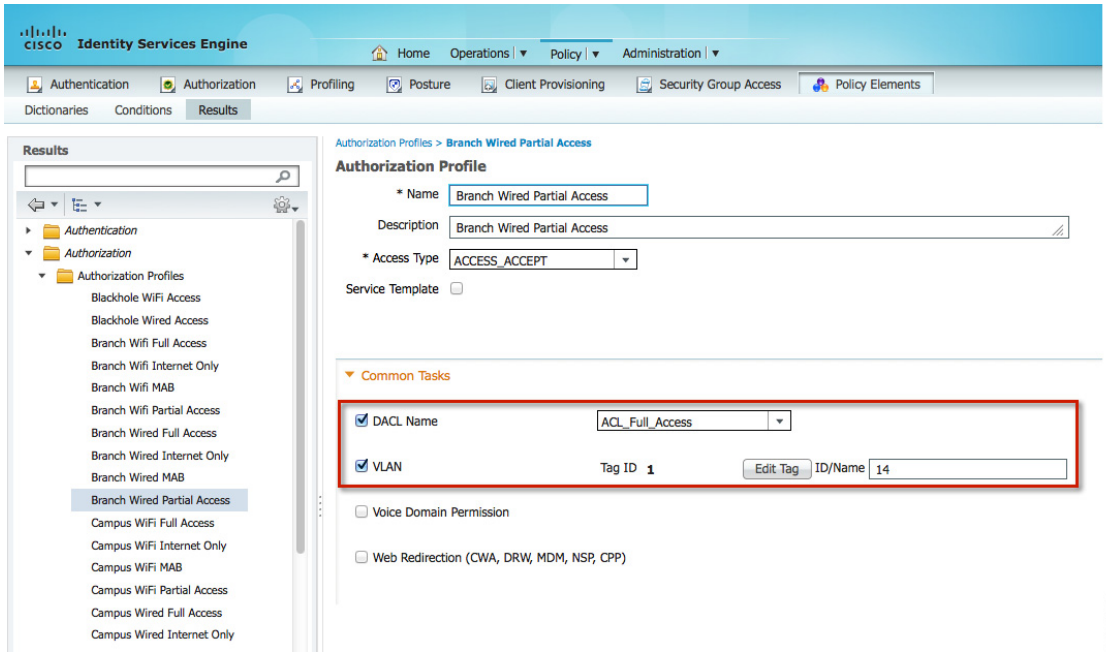
- 允许 DHCP 访问 （bootpc 和 bootps）。
- 允许 DNS 访问 DNS 服务器 (10.230.1.45)。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许以特定子网 (10.230.4.0 /24) 作为源 / 目标的 IP 访问。
- 允许以特定服务器 （10.230.6.2 和 10.225.100.10）作为源 / 目标的 IP 访问。
- 拒绝以内部网络地址空间（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

分支机构有线

对于从分支机构位置连接的设备，分支机构有线部分访问授权会将 VLAN 分配和可下载的 ACL 一起推送。

图 10-55 显示了 ISE 中配置的授权配置文件的详细信息。

图 10-55　　分支机构有线部分访问授权配置文件



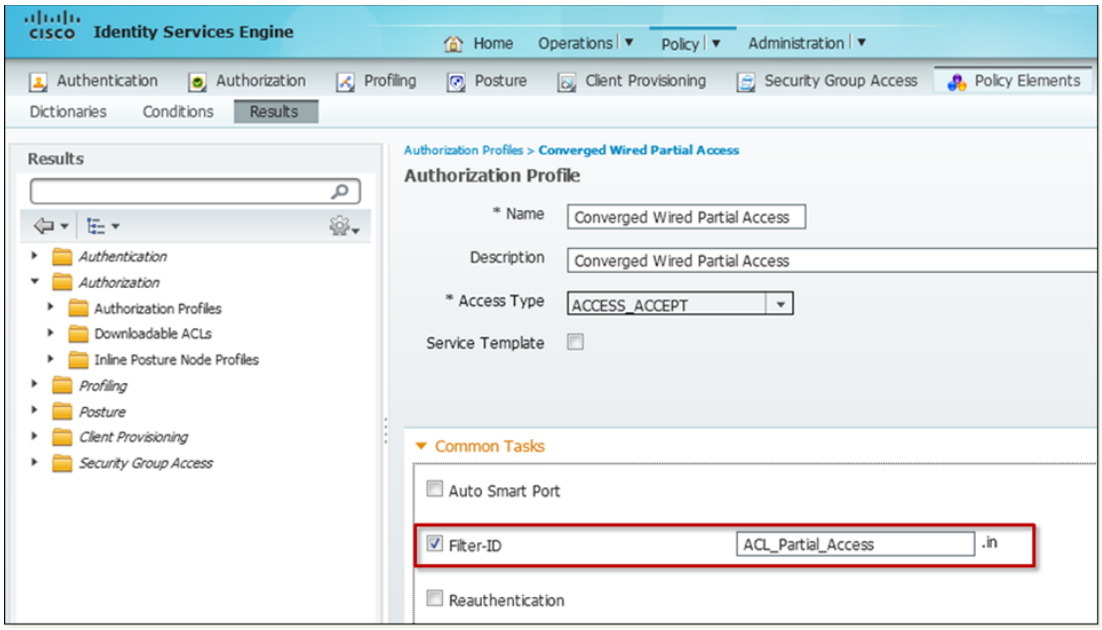
DACL 允许所有 IP 流量，因此主机发起的流量会到达应用了路由器 ACL 的分支路由器。

请参阅第 7 章，“自带设备有线基础设施设计”中的分支机构位置的 VLAN 设计，了解有关如何针对未实施融合接入基础设施的分支机构向 VLAN 14 分配提供完全访问权限的详细信息。

融合接入分支机构和园区

图 10-56 显示了 ISE 中如何定义融合有线部分访问授权配置文件。

图 10-56　　融合有线部分访问授权配置文件



对于融合接入设计，将会实施命名 ACL。ISE 会使用 RADIUS Filter-ID 属性值对，指示融合接入交换机应用 ACL_Partial_Access ACL。该 ACL 与个人无线设备 - 部分访问权限中针对融合接入基础设施讨论的 ACL 相同。对于有线设备， ACL 用于覆盖交换机端口上配置的默认 ACL。如果交换机上未配置 ACL_Partial_Access，则默认 ACL 会用作额外的预防措施。

个人有线设备 - 仅互联网访问

要向个人设备提供仅互联网的访问， Cisco ISE 会验证以下各项：

- 员工已通过访客注册门户完成自注册流程。
- 要唯一标识设备并防止欺骗， Calling-Station-ID 须与证书的主题替代名称相匹配 （在本例中，替代名称为终端的 MAC 地址）。
- 连接是使用 EAP-TLS 身份验证发起的。
- 用户是域用户 Active Directory 组的成员。

在较高层面上，图 10-57 显示了如何针对来自基础设施设计各异的不同位置的设备选择不同授权配置文件。每个授权配置文件会使用 VLAN、动态 ACL （命名或可下载的 [DACL]）等相应地实施一种唯一权限。

图 10-57　有线仅互联网访问权限实施

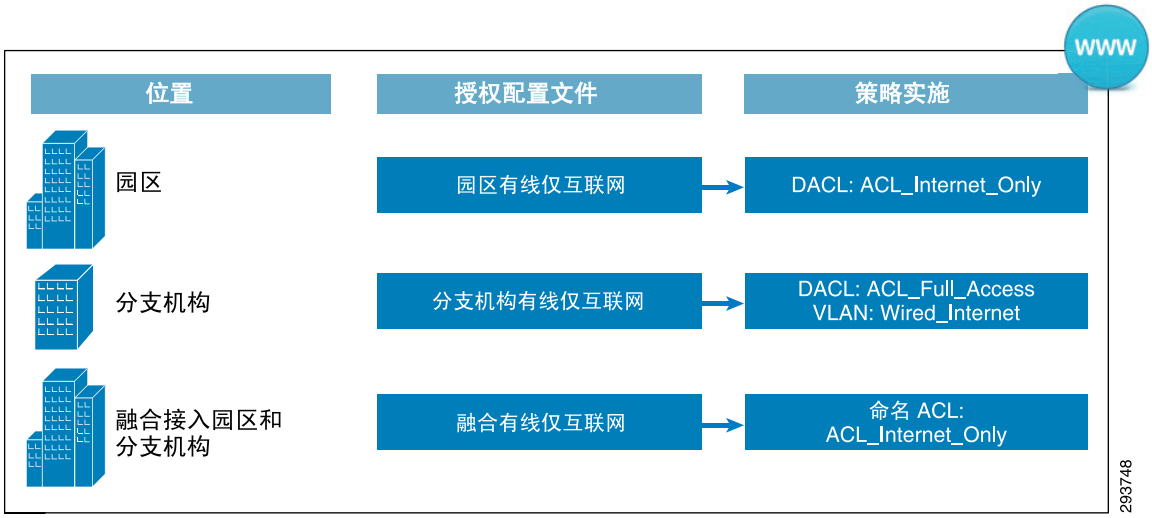
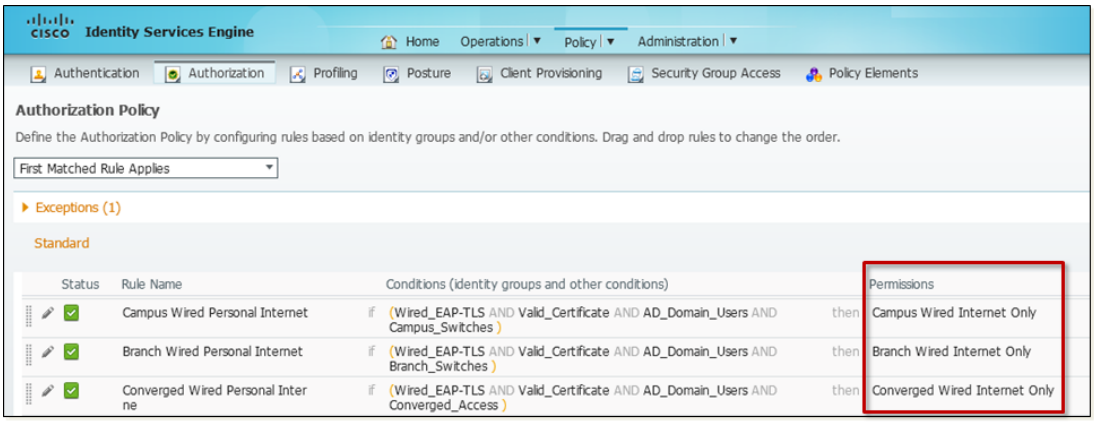


图 10-58 重点展示了向个人有线设备授予仅互联网访问权限的授权策略。

图 10-58　有线仅互联网访问的授权策略



详细查看规则时， ISE 会评估以下条件：

- Wired_EAP-TLS - 终端使用 EAP-TLS 连接 （定义为复合条件）。
- 终端具有一份有效证书。 Calling-Station-ID 与证书主题替代名称中包含的 MAC 地址匹配。（定义为简单条件）。
- 用户属于特定 Active Directory 组 （定义为简单条件）。
- Radius 身份验证源自 Catalyst 交换机，该交换机是以下任一设备组的成员：Campus_Switches、 Branch_Switches 或 Converged_Access （定义为简单条件）。

有线简单和复合条件介绍了这些规则中使用的不同条件。

权限

当授权策略规则中的所有条件都匹配时，规则会执行相应权限。权限可以是不同形式，如授权配置文件或标准结果。在本设计指南中，对于有线访问，授权策略用作策略规则匹配情况下的权限。表 10-11 介绍了用于互联网访问的权限。

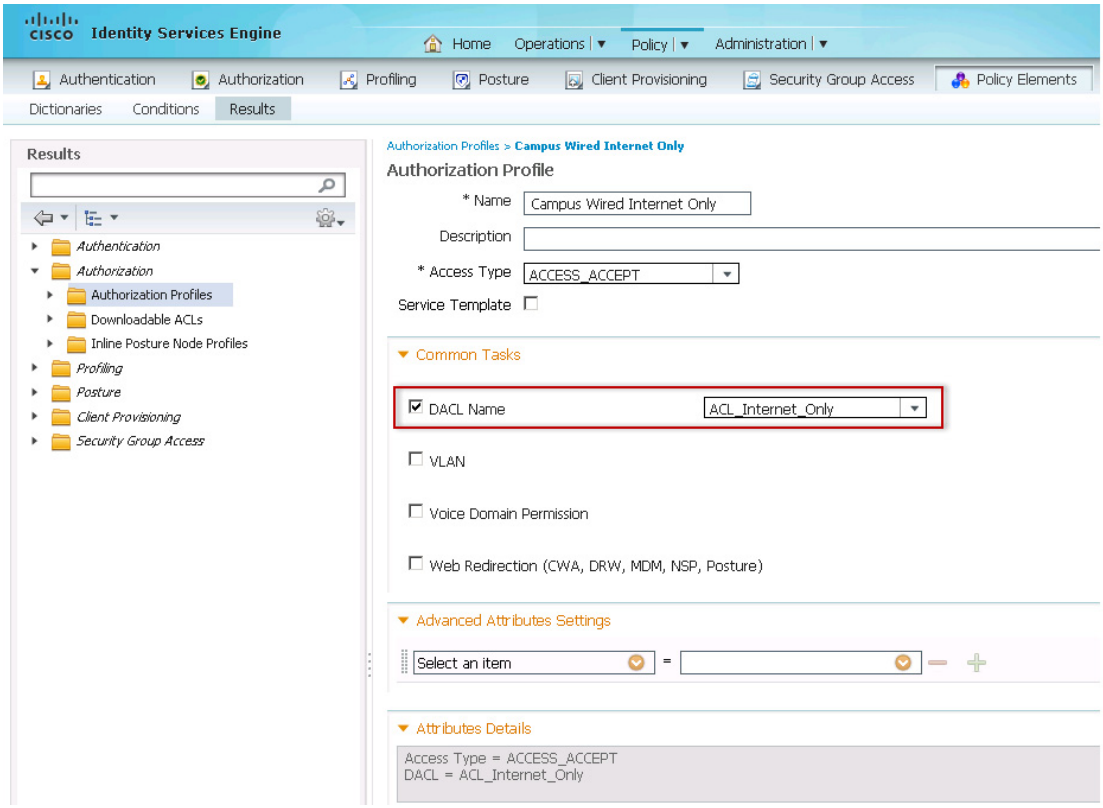
表 10-11　　用于有线互联网访问的权限

权限名称	权限类型	用途
园区有线仅互联网	授权配置文件	向从园区位置连接的 802.1X 有线设备推送 DACL。
分支机构有线仅互联网	授权配置文件	向从分支机构位置连接的 802.1X 无线设备推送 VLAN。
融合有线仅互联网	授权配置文件	向 802.1X 有线设备推送命名 ACL，该设备从采用融合接入的园区或分支机构位置连接

有线园区

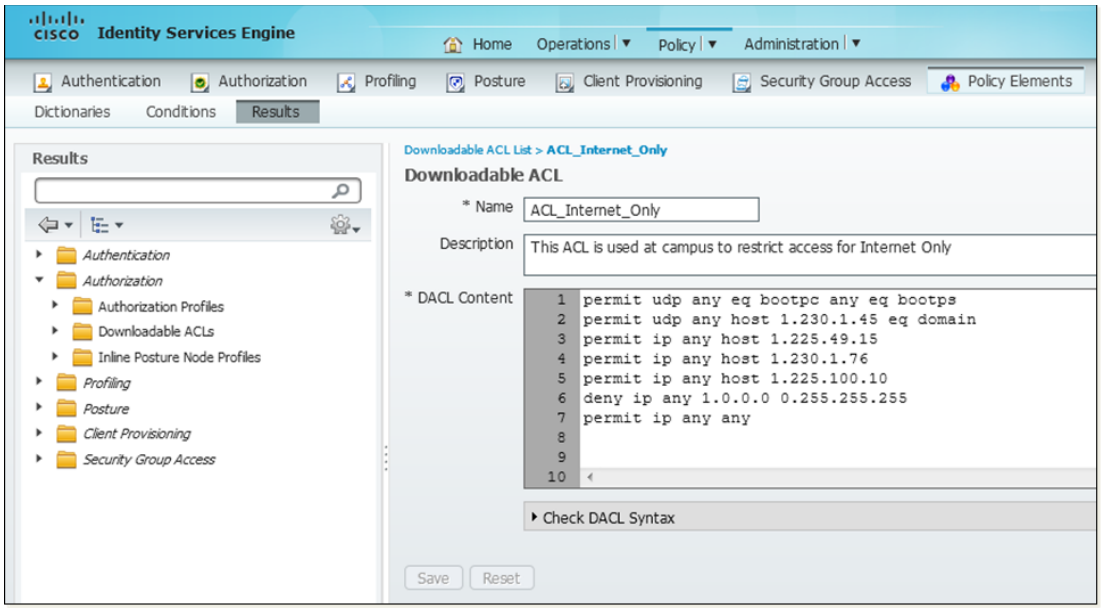
对于从园区位置连接的设备，园区有线仅互联网授权配置文件使用名为 ACL_Internet_Only 的 DACL，该 DACL 会被推送到接入层交换机端口。图 10-59 显示了授权配置文件。

图 10-59　　园区有线仅互联网授权配置文件



DACL 会覆盖交换机上配置的默认 ACL。图 10-60 显示了此 ACL 示例，该 ACL 在 ISE 中配置。

图 10-60　　ACL_Internet_Only DACL



访问列表指定了以下访问权限：

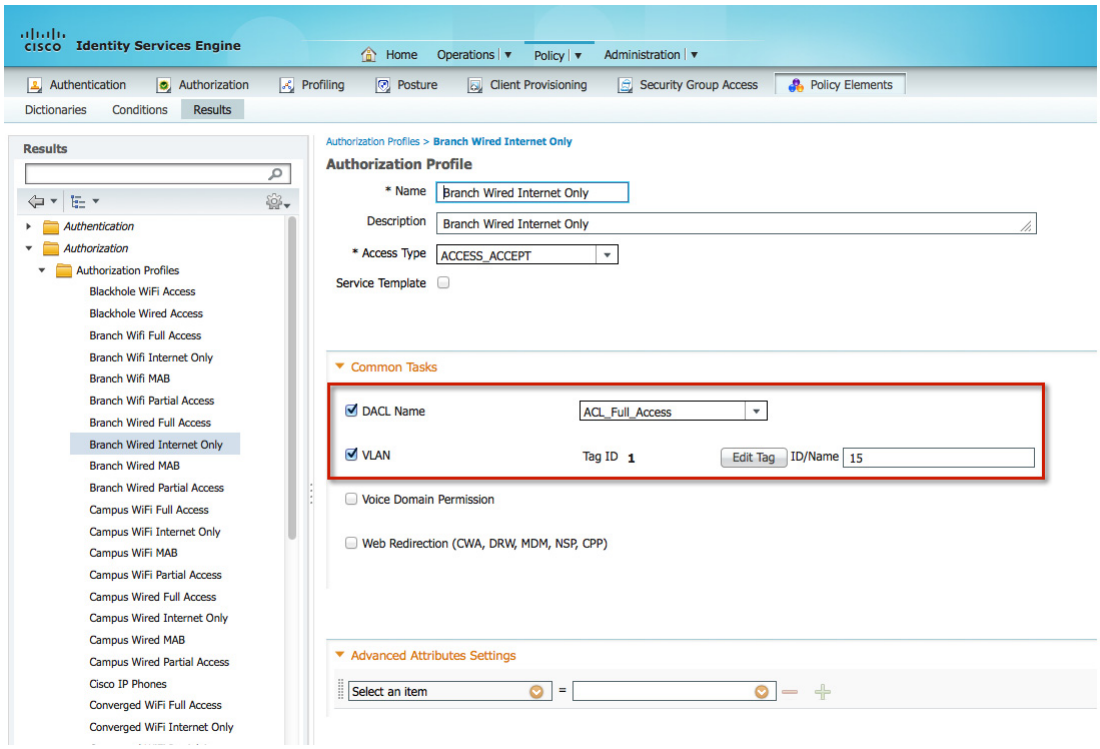
- 允许 DHCP 访问 （bootpc 和 bootps）。
- 允许 DNS 访问 DNS 服务器 （10.230.1.45）。
- 允许以 ISE 服务器 （10.225.49.15）作为源 / 目标的 IP 访问。
- 拒绝以内部网络地址空间（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

该访问列表是一般性的，并不用于每个组织。ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

分支机构有线

对于从分支机构位置连接的设备，分支机构有线仅互联网授权会将 VLAN 分配和可下载的 ACL 一起推送。图 10-61 介绍了分支机构有线 Internet_Only 授权配置文件，用于向从分支机构连接的个人设备授予 Internet_Only 访问权限。

图 10-61　　分支机构有线仅互联网授权配置文件



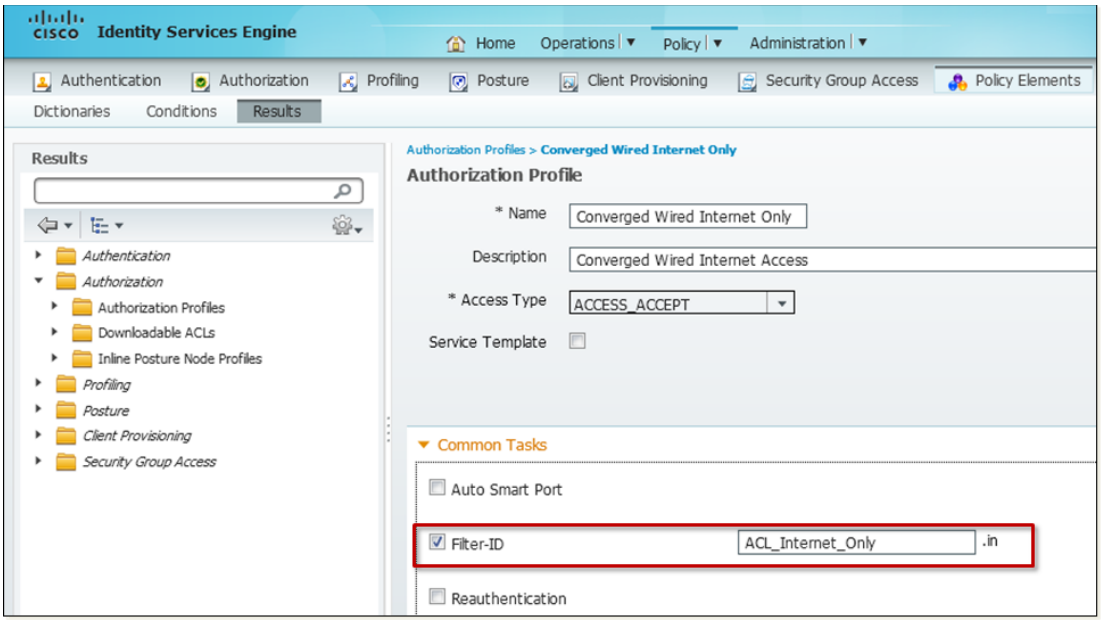
ACL_Full_Access DACL 会被推送到接入层交换机，以覆盖端口上的默认 ACL 并允许所有 IP 流量流至分支路由器。

请参阅第 7 章，“自带设备有线基础设施设计”中的分支机构位置的 VLAN 设计，了解有关如何针对未实施融合接入基础设施的分支机构向 VLAN 15 分配提供完全访问权限的详细信息。

融合接入分支机构和园区

图 10-62 显示了 ISE 中如何定义融合有线仅互联网授权配置文件。

图 10-62　　融合有线仅互联网授权配置文件



对于融合接入设计，将会实施命名 ACL。ISE 会使用 RADIUS Filter-ID 属性值对，指示融合接入交换机应用 ACL_Internet_Only ACL。该 ACL 与个人无线设备 - 仅互联网访问中针对融合接入基础设施讨论的 ACL 相同。对于有线设备， ACL 用于覆盖交换机端口上配置的默认 ACL。如果交换机上未配置 ACL_Internet_Only，则默认 ACL 会用作额外的预防措施。

Android 设备 - 拒绝访问

与之前使用案例中介绍的允许不同网络访问权限不同，本使用案例讨论如何拒绝某些 BYOD 设备连接到网络的访问权限。例如，一些组织可能决定采用更严格的 BYOD 环境，并仅向特定设备类型（例如， Android、 Apple iOS 等）授予访问权限。

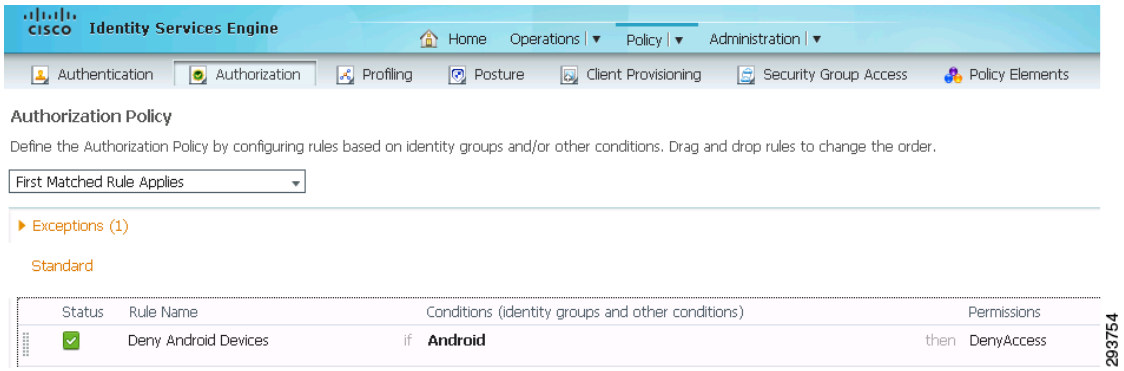
本示例侧重于根据 ISE 的分析功能拒绝 Android 设备访问。

要拒绝 Android 设备访问， Cisco ISE 会验证以下各项：

- 员工尝试连接到网络。
- ISE 分析器识别出设备类型。
- 如果设备类型为 Android，则拒绝其访问。

要在 ISE 中配置授权规则，请点击 **Policy > Authorization**。图 10-63 重点展示了拒绝 Android 设备访问的授权策略。

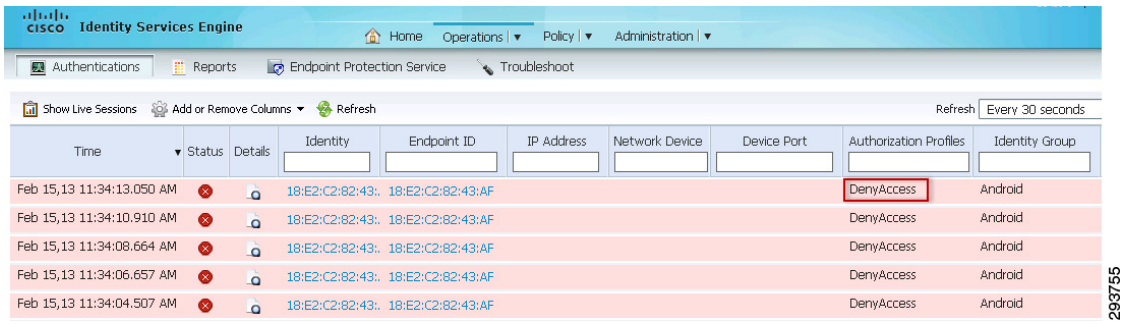
图 10-63　　拒绝 Android 设备



DenyAccess 授权配置文件用于执行权限并拒绝 Android 设备访问。 DenyAccess 配置文件是标准 ISE 配置文件，不能进行编辑。此保留配置文件不能进行编辑，但是可以在 **Policy > Results> Authorization Profiles** 下找到。

图 10-64 显示了 ISE 日志中的一个条目，强调了设备已分析为 Android 设备且已执行 DenyAccess 授权规则这一事实。

图 10-64　　DenyAccess

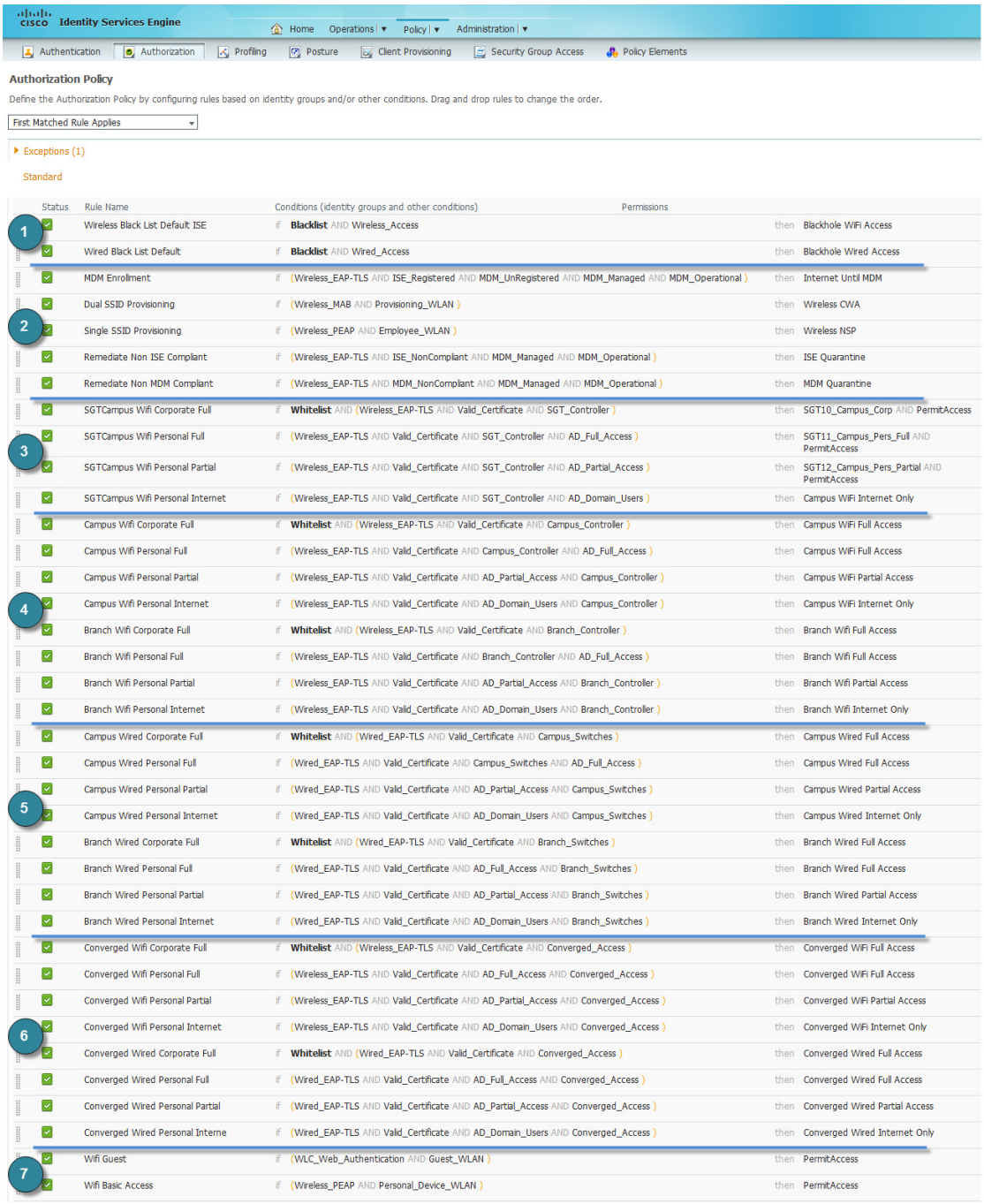


ISE 授权策略

为了提供参考，图 10-65 中显示了验证过程中使用的完整授权策略。该图重点显示了以下部分：

1. 用于将丢失或被盗的设备列入黑名单。
2. 自注册和 MDM 注册 / 修复 （高级使用案例需要）。
3. 从 SGT_Enabled 位置中的接入点连接的无线设备。
4. 从园区或分支机构位置中的接入点连接的无线设备。
5. 从园区或分支机构位置连接的有线设备。
6. 从融合位置连接的有线和无线设备。
7. 访客和基本访问。

图 10-65　　完整授权策略



第 11 章

BYOD 高级用例 - 移动设备管理器集成

修订日期：2013 年 8 月 7 日

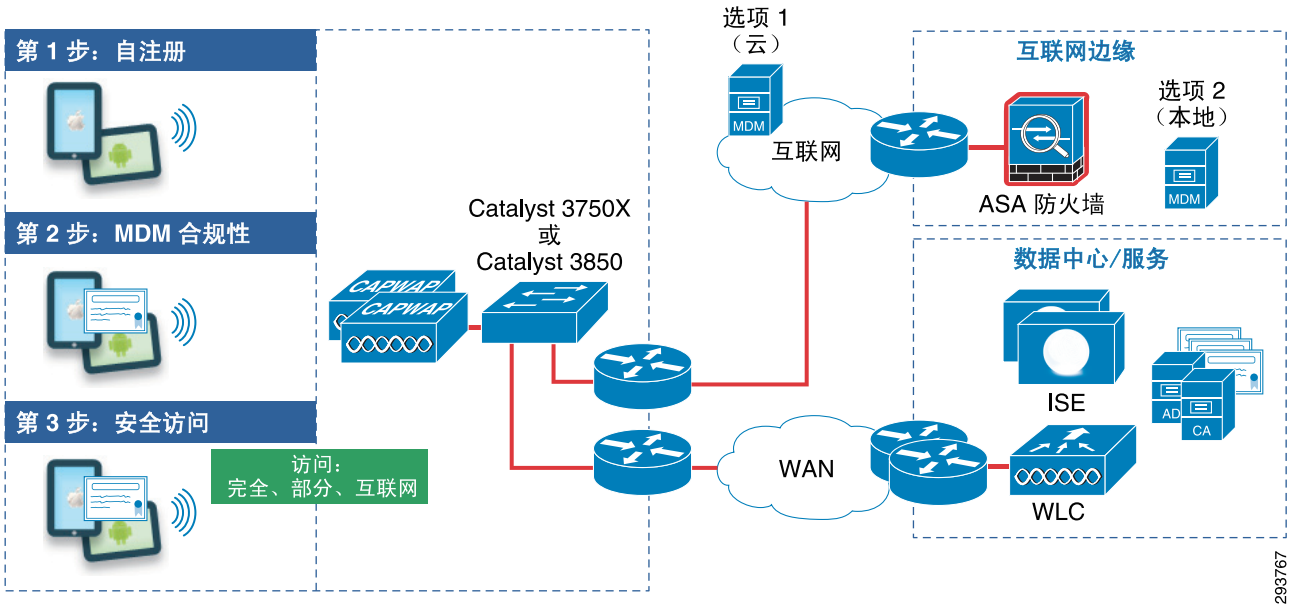
本章重点介绍通过与第三方移动设备管理器 (MDM) 集成获取更多设备状态信息。之前的章节侧重于入网的公司和个人设备以及提供差异化访问权限，本章则利用更详细的终端信息来实施授权策略。

MDM 服务器可保护、监视、管理并支持移动设备，确保移动应用使用安全，并对使用情况加以控制。网络是唯一可基于 VLAN 分配、 ACL （命名的或者可下载的 [DACL]）、 SGT、 FlexConnect ACL 等向终端提供粒度访问权限的实体。通过与第三方 MDM 服务器集成， Cisco ISE 可获得必要的设备属性，以便对这些终端实施更精细的网络访问。

图 11-1 展示了 MDM 与 Cisco ISE 之间的互通性。设备通过 ISE 入网后， ISE 将查询 MDM 获取更多终端信息。如果终端已经注册并符合 MDM 策略，可根据其他属性向设备授予访问权限，如前面各节所述。

请注意， MDM 服务器可部署在内部，也可以部署在云端。

图 11-1 MDM 互通性



检查设备合规性时，会按照下列步骤进行：

1. 用户连接到网络 SSID，并使用 ISE 引导完成注册和入网过程。
2. 使用适当的证书 / 配置文件入网后，用户可连接到安全的员工 SSID。
3. ISE 会向 MDM 服务器发出 API 调用。如果设备未注册 MDM，用户将看到相关页面，从中可转入 MDM 注册页面。
4. 注册 MDM 服务器完成后，用户将返回包含继续按钮的注册重定向页面。用户从该页面上选择继续选项后，ISE 会发出授权更改 (CoA)，迫使用户重新进行身份验证。API 现在应表明用户已注册 MDM。在授权流程持续期间， MDM API 结果将由 ISE 缓存。
5. ISE 使用特定 MAC 地址的 MDM 缓存信息验证设备的状态，包括 MDM 合规状态。如果设备不符合 MDM 策略，系统将再次通知用户，并要求用户遵守策略。
6. 设备符合策略后，系统将根据分配的权限授予用户相应的网络访问权限 （完整权限、部分权限或互联网权限）。
7. ISE 可定期轮询 MDM 服务器获得合规信息。

第 9 章，“BYOD 的移动设备管理器集成”更详细地介绍了如何配置 ISE 和 MDM 之间的集成。

支持的 MDM 功能

Cisco ISE 依靠 REST API 调用查询外部 MDM 服务器来获得更多终端信息。 ISE 和 MDM 之间的通信大多是单向的，由 ISE 向 MDM 发送不同的命令。这些命令其中一些查询设备信息 （型号、合规状态、序列号等），另一些则在设备上触发操作 （公司擦除、完全擦除、 PIN 锁等）。

以下是一些由 ISE 结合 MDM 服务器执行的功能：

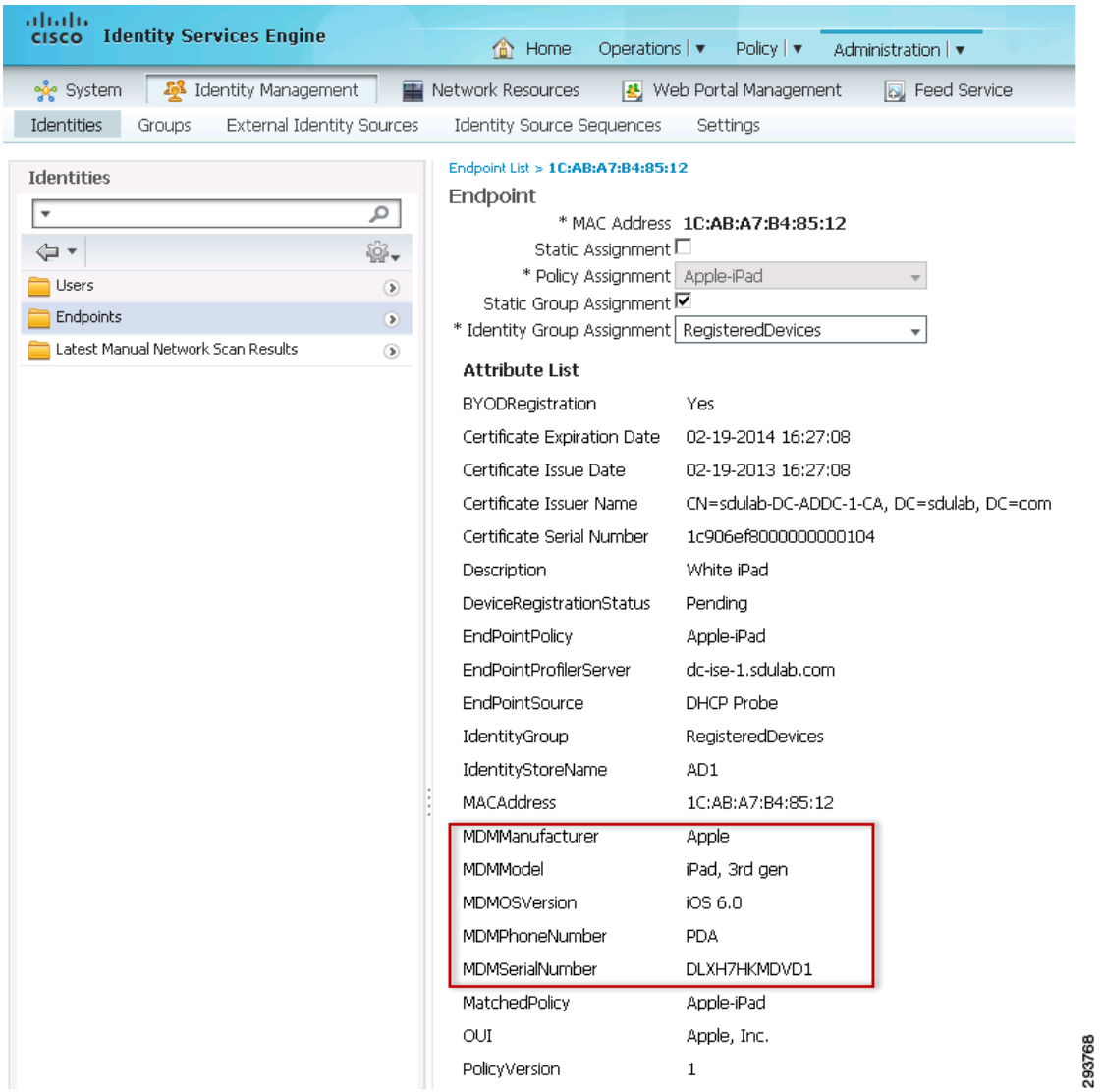
- 设备注册 - 连接到网络的未注册终端被重定向到 MDM 服务器托管的网页，以启动 MDM 注册流程。
- 设备补救 - Cisco ISE 向不合规终端强加强制网络门户。用户将被重定向至填写了通过 MDM API 获取的设备状态信息的 ISE 托管网页。此页面向用户做出提示，并指示达到合规状态所应执行的操作。
- 定期合规性检查 - Cisco ISE 定期轮询 MDM 服务器，以获取 MDM 不合规设备的列表。ISE 将判断此列表中是否有任何设备目前与网络关联，并对这些设备发出 CoA。
- 通过 MDM 服务器发出设备说明 - 通过 MDM 服务器可向用户的设备发出远程操作。

终端数据库利用从 MDM 服务器获得的更多信息 （无法使用 Cisco ISE 分析器收集）进行更新。可从 MDM 获取的设备属性包括以下各项：

- MDMManufacturer
- MDMModel
- MDMOSVersion
- MDMPHoneNumber
- MDMSerialNumber
- MDMIMEI

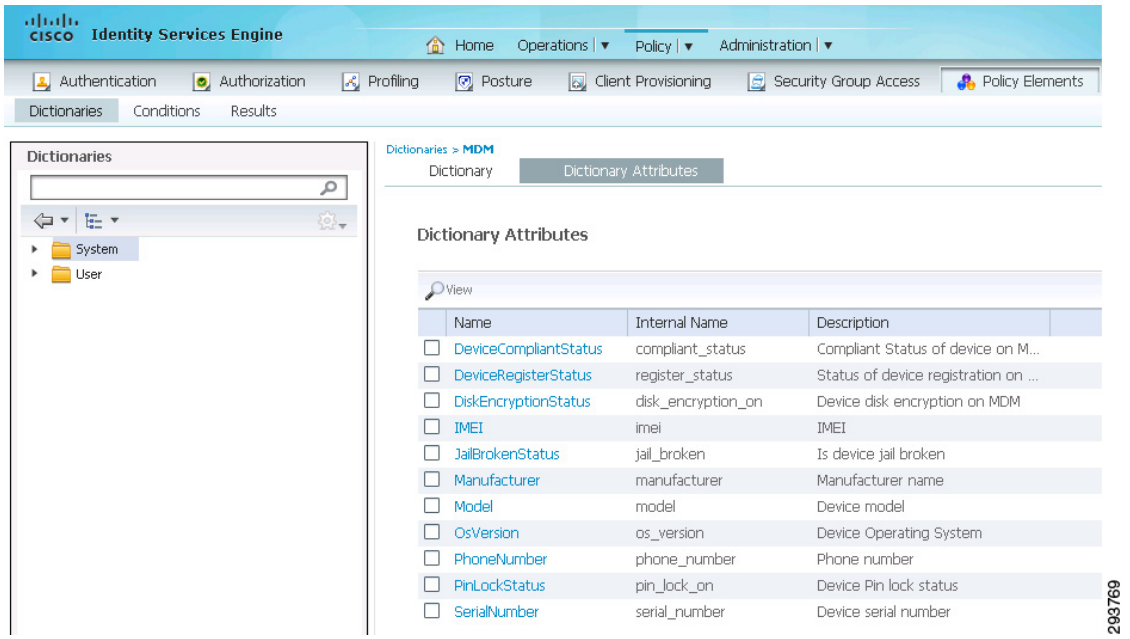
用户可通过依次点击 **Administration > Identity Management > Identities > Endpoints** 查看这些属性，如图 11-2 中所示。

图 11-2　　MDM 属性



通过与 MDM 服务器集成，Cisco ISE 能够根据其他 MDM 属性配置策略。在 **Policy > Dictionaries > MDM > Dictionary Attributes** 下可以查找字典属性，如图 11-3 中所示。

图 11-3　　字典属性



其中有些属性在本设计指南的许多授权规则中得到应用。

整合流程

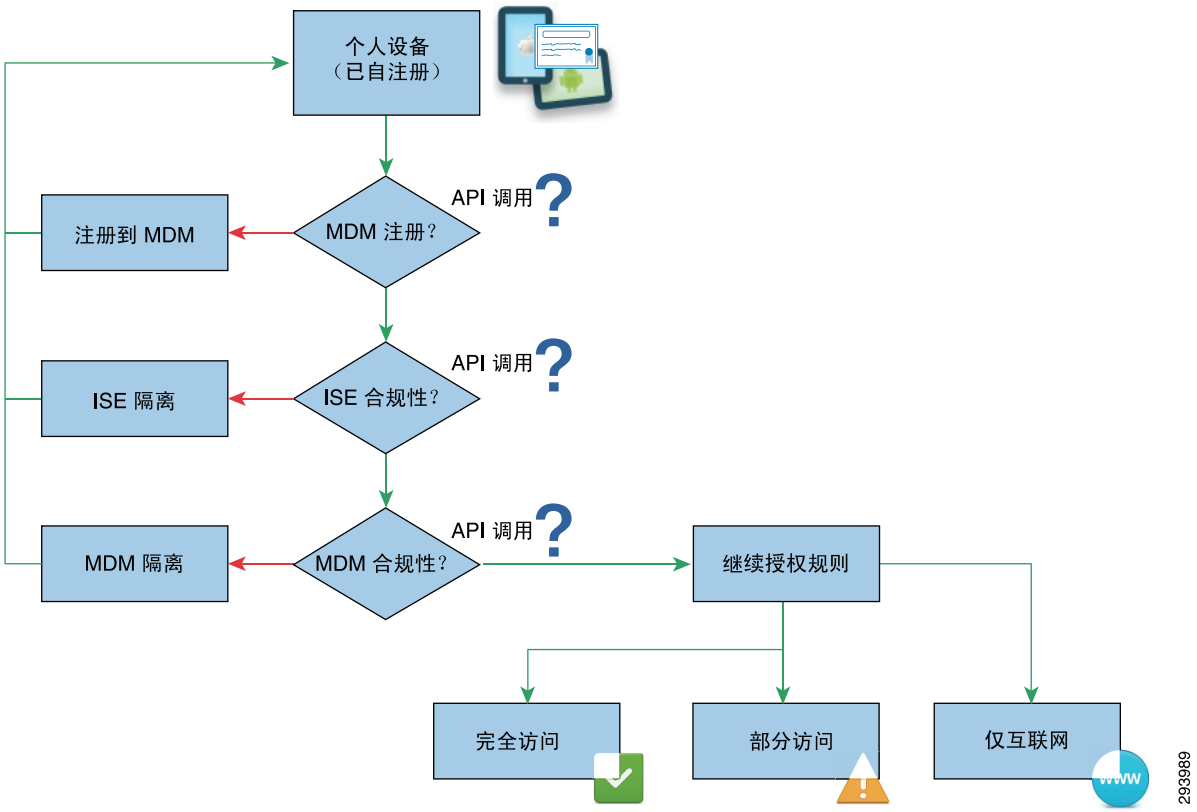
图 11-4 展示了 ISE 与 MDM 之间的整合流程：

1. 设备已入网，且用户连接到 BYOD_Employee SSID。
2. Cisco ISE 向 MDM 服务器发出 API 调用，以验证设备是否已经注册 MDM。
3. 如果设备未注册，且必须注册，则要求用户注册 MDM。这可能包括安装来自 Apple App Store 或 Google Play 的相关应用。
4. 在授予网络访问权限之前，ISE 强制执行某些设备属性。如果设备不兼容 ISE，则隔离该设备（如下文所述）。
5. 如果设备不符合 MDM 策略，则隔离该设备。

如果用户已入网，并符合 ISE 和 MDM 策略要求，则根据不同的规则授予适当权限。

注意　前面的章节已经介绍了如何向个人和公司设备授予完全访问、部分访问和仅互联网访问权限。

图 11-4　　MDM 合规性检查



ISE 合规性检查

设备注册 MDM 后， ISE 需要检查某些设备属性，才能授予网络访问权限。这可以作为一项额外检查，也可以作为验证某些设备属性的第一次机会。

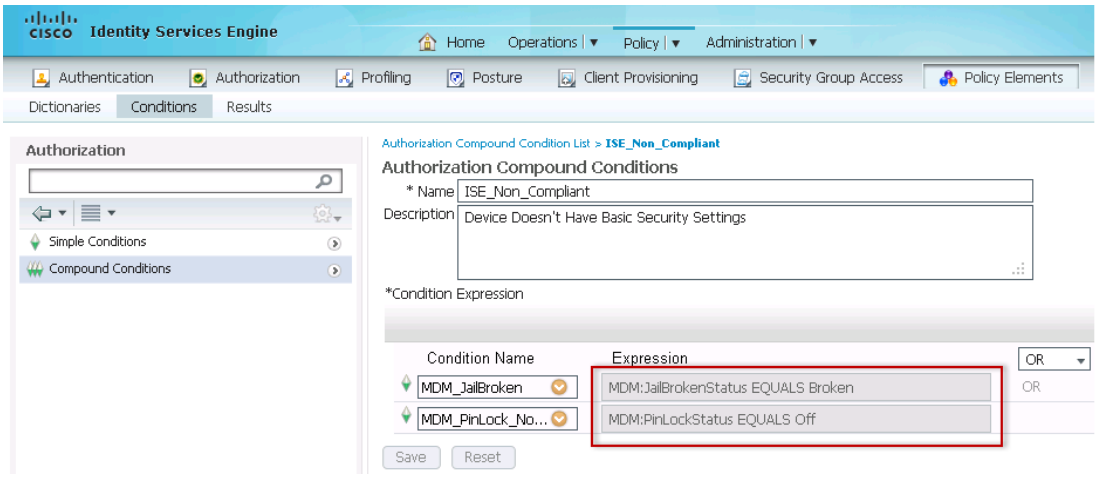
在本设计指南中，要获得网络访问权限，至少应验证两个设备属性：

- 已越狱或获得 root 权限的设备 - 不允许进入网络。
- PIN 锁实施 - 没有设备 PIN 锁的设备将被拒绝访问。

ISE 向 MDM 发出 *JailBrokenStatus* 和 *PinLockStatus* API 调用来验证这些属性。

ISE 会定义一个复合条件来检查这两个属性。要定义此复合条件，请点击 **Policy > Policy Elements > Conditions > Compound Conditions**，如图 11-5 中所示。

图 11-5　　ISE_Non_Compliant



可添加额外的字典属性满足每个组织的安全策略要求。

MDM 合规性检查

对于已入网并达到 ISE 合规性检查要求的设备， ISE 会向 MDM 发出一次额外的 API 调用，确保设备达到 MDM 规定的所有合规要求。

如果设备没有完全达到 MDM 的要求， ISE 将授予互联网访问权限，但拒绝提供访问所有内部资源的权限。用户尝试访问内部资源时， ISE 会将该会话重定向到一个门户，在该门户中会重点列出满足 MDM 合规性规则所需执行的操作。

ISE 会向 MDM 发出 DeviceCompliantStatus API 调用来验证合规情况。MDM 规定了导致设备违规的条件。

ISE 配置

在应用权限之前的 ISE 和 MDM 合规验证过程中，会用到多项 ISE 功能。这些功能包括逻辑配置文件、授权规则、 ACL 和旨在获得终端属性的 MDM API 调用。

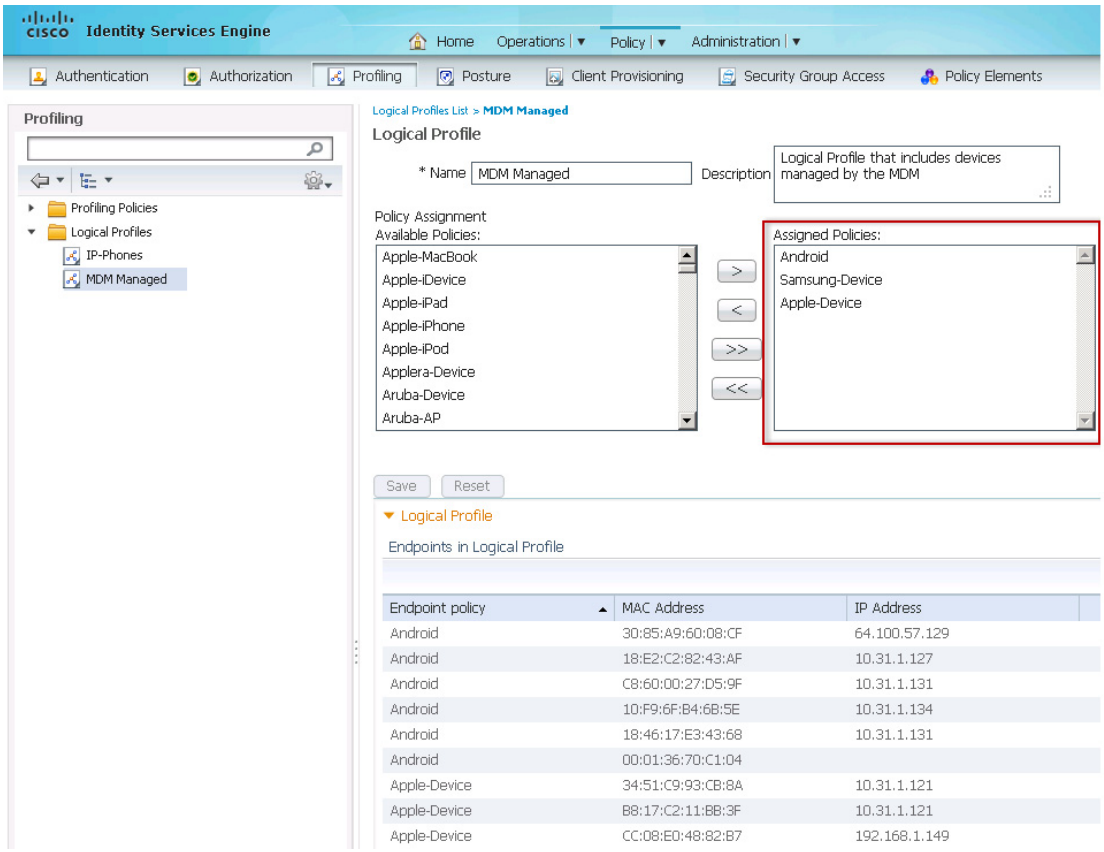
逻辑配置文件

Cisco ISE 中的分析服务能够识别连接网络的设备，进而根据设备类型授予终端适当的访问权限。通过收集终端属性，并根据终端配置文件对属性分组，可在特定类型的设备上实施独一无二的策略。

逻辑配置文件是共享某一共同属性的对象的虚拟容器。例如，全部由平板电脑或智能手机组成的一组设备便是一个逻辑配置文件。全部由 Android 或 Apple 设备组成的一组设备也是一个逻辑配置文件。就本设计指南而言，我们需要创建一个逻辑配置文件来包括由 MDM 管理的设备。这样，管理员可以动态添加或删除由 MDM 管理的设备。

图 11-6 展示了用于对 MDM 支持以及管理或许可的设备进行分组的 MDM 托管逻辑配置文件。此逻辑配置文件在定义 ISE 授权策略时使用，包括分析鉴定为 Android、三星和 Apple 设备的设备。要在 ISE 上配置此逻辑配置文件，请点击 **Policy > Profiling > Logical Profiles**。

图 11-6　　MDM 托管逻辑配置文件

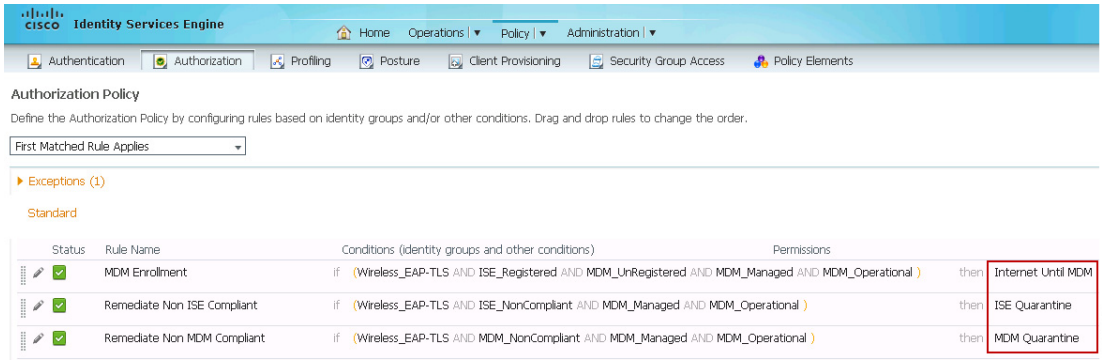


此逻辑配置文件能够轻松扩展，在无需修改 ISE 授权策略的情况下将其他受 MDM 支持和管理的设备纳入在内。

授权策略

图 11-7 展示了用于实施 MDM 和 ISE 合规的 ISE 授权规则。这些授权规则的执行时间在用户连入移动设备之后，在授予更多网络访问权限 （例如，完全、部分、互联网）之前。

图 11-7　　MDM 合规性授权规则



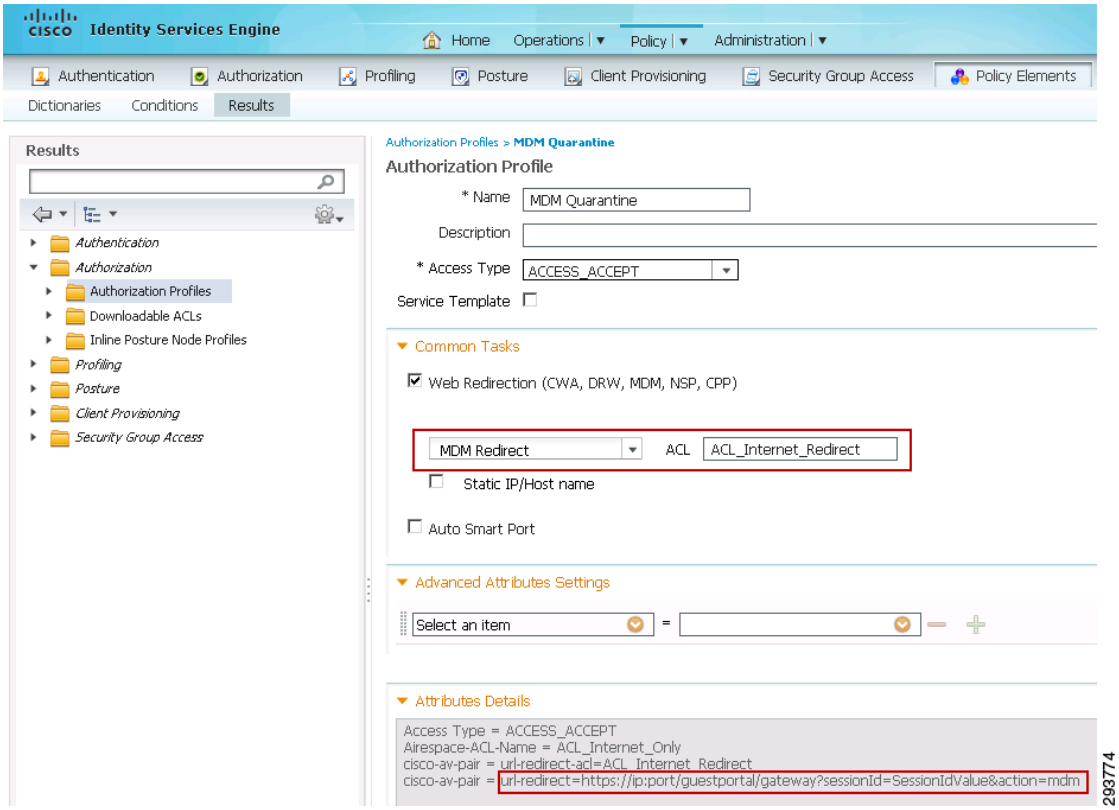
MDM 注册规则

满足以下条件时，匹配此规则：

- 终端通过无线 802.1X SSID 连接。
- 逻辑配置文件大小与 MDM 托管配置文件相同 - 设备由 MDM 托管和支持。
- 设备完成入网流程并注册 ISE。
- 设备**未**注册 MDM。

如果满足这些条件，则使用 *Internet Until MDM* 授权配置文件。此配置文件配置为将未注册设备重定向至图 11-8 中重点展示的 URL。

图 11-8　　Internet Until MDM

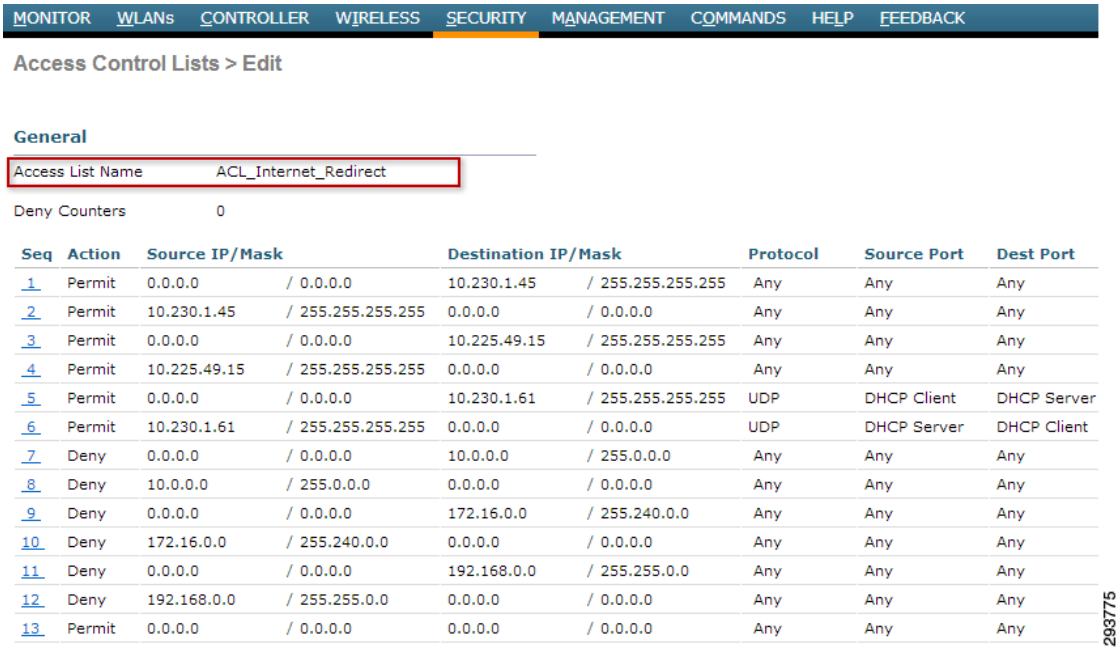


此授权配置文件依赖之前在无线局域网控制器中定义的两个命名 ACL，分别是：ACL_Internet_Redirect 和 ACL_Internet_Only。上图中显示的是将 ACL_Internet_Redirect 应用于“MDM 重定向”设置。在图 11-8 中，ACL_Internet_Only 通过 Radius:Airespace-ACL-Name 属性值 (AV) 对发送至无线控制器。两个 ACL 的行为在 CUWN 无线控制器 （例如 CT5508 和 Flex 7500）和基于 IOS XE 的控制器 （例如 CT5760 和 Catalyst 3850）之间稍有不同。

注意　在本文档中，无线局域网控制器是指独立设备（例如，Cisco CT5508、Flex 7500 或 CT5760 无线控制器），或者是指集成在 Catalyst 3850 系列交换机内部的无线控制器功能。

对于 CUWN 无线控制器， ACL_Internet_Redirect 同时充当控制网络重定向的 ACL 以及控制无线客户端可以访问网络中哪些内容的 ACL。 ACL_Internet_Only 仅用作额外的安全配置。当指定了 URL 重定向时， CUWN 无线控制器不使用此 ACL。对于 CUWN 无线控制器，图 11-9 中显示的 ACL_Internet_Redirect ACL 可以与前面章节讨论的 ACL_Internet_Only ACL 相同。

图 11-9　　ACL_Internet_Redirect



Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
8	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
10	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
12	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

ACL 指定以下访问权限：

- 允许以 DNS 服务器 （10.230.1.45）作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 （10.225.49.15）作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 （10.230.1.61）作为源 / 目标的 IP 访问。
- 拒绝以内部网络地址空间（10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16）作为源 / 目标的 IP 访问。
- 允许以所有其他子网 （互联网访问）作为源 / 目标的访问。

对于基于 Cisco IOS XE 的无线控制器，ACL_Internet_Redirect 严格用作控制网络重定向的 ACL。ACL_Internet_Only 用作控制无线客户端可以访问网络中哪些内容的 ACL。因此，指定 URL 重定向时，基于 IOS XE 的无线控制器会同时使用两个 ACL。示例 11-1 中展示的是适用于基于 Cisco IOS XE 的无线控制器的 ACL_Internet_Redirect ACL 示例。

示例 11-1　　适用于基于 IOS XE 的控制器的 Internet Redirect ACL

```
!
ip access-list extended ACL_Internet_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 172.16.0.0 0.15.255.255
 permit ip any 192.168.0.0 0.0.255.255
 deny   ip any any
!
```

上述 ACL 指定了以下访问权限：

- 拒绝 （不重定向） DHCP 访问 （bootpc 和 bootps）。
- 拒绝 （不重定向）以 DNS 服务器 （10.230.1.45）作为源 / 目标的 IP 访问。
- 拒绝 （不重定向）以 ISE 服务器 （10.225.49.15）作为源 / 目标的 IP 访问。
- 允许（重定向）以内部网络 IP 地址空间其他位置（10.0.0.0 /8、172.16.0.0 /12、192.168.0.0 /16）作为源 / 目标的 IP 访问。
- 拒绝 （不重定向）所有其他以互联网作为目标的访问。

示例 11-2 中展示的是适用于基于 Cisco IOS XE 的无线控制器的 ACL_Internet_Only ACL 示例。

示例 11-2　　适用于基于 IOS XE 的控制器的 Access ACL

```
!
ip access-list extended ACL_Internet_Only
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
!
```

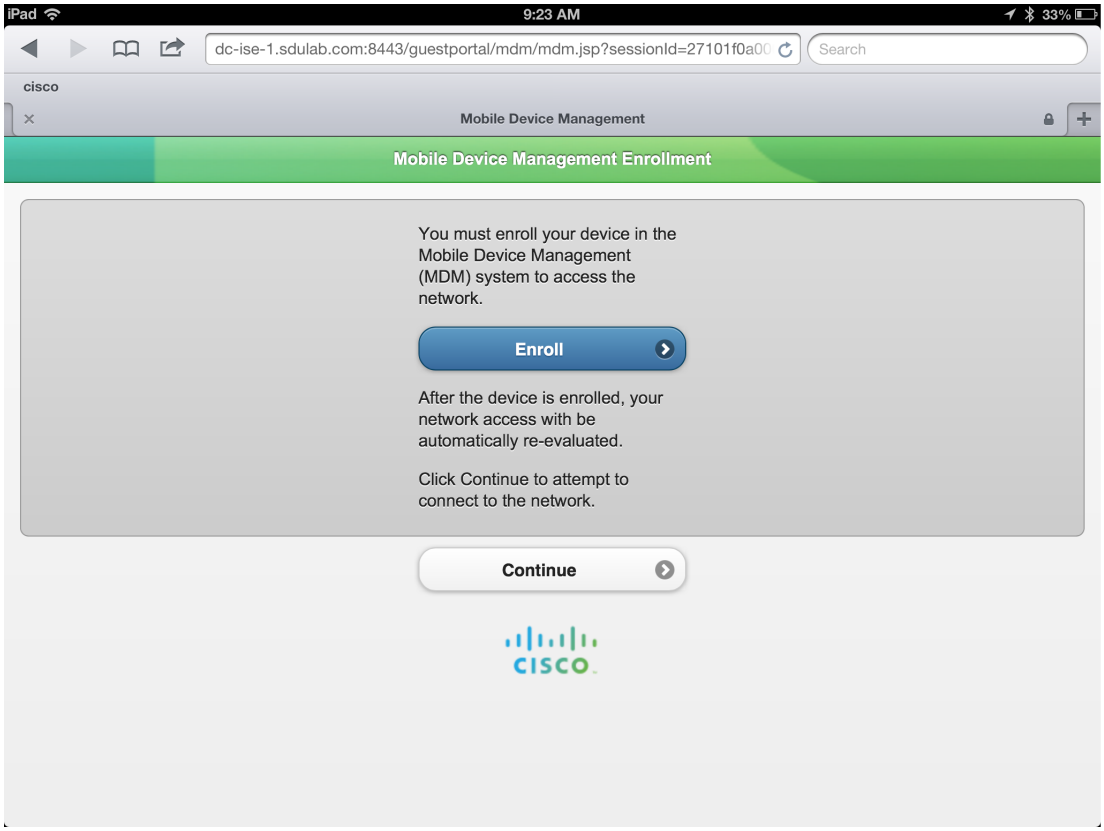
上述访问列表指定以下访问权限：

- 允许 DHCP 访问 （bootpc 和 bootps）。
- 允许以 DNS 服务器 （1.230.1.45）作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 （1.225.49.15）作为源 / 目标的 IP 访问。
- 拒绝以内部网络 IP 地址空间其他位置 （10.0.0.0 /8、 172.16.0.0 /12、 192.168.0.0 /16）作为源 / 目标的 IP 访问。
- 允许以所有其他地址 （互联网地址）作为目标的访问。

注意　示例 11-2 中显示的访问列表是通用列表，不一定适用于所有组织。 ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

用户首次尝试浏览内部资源时，会话将重定向至与图 11-10 中类似的页面，由其提供注册相应 MDM 的链接。

图 11-10　　注册 MDM

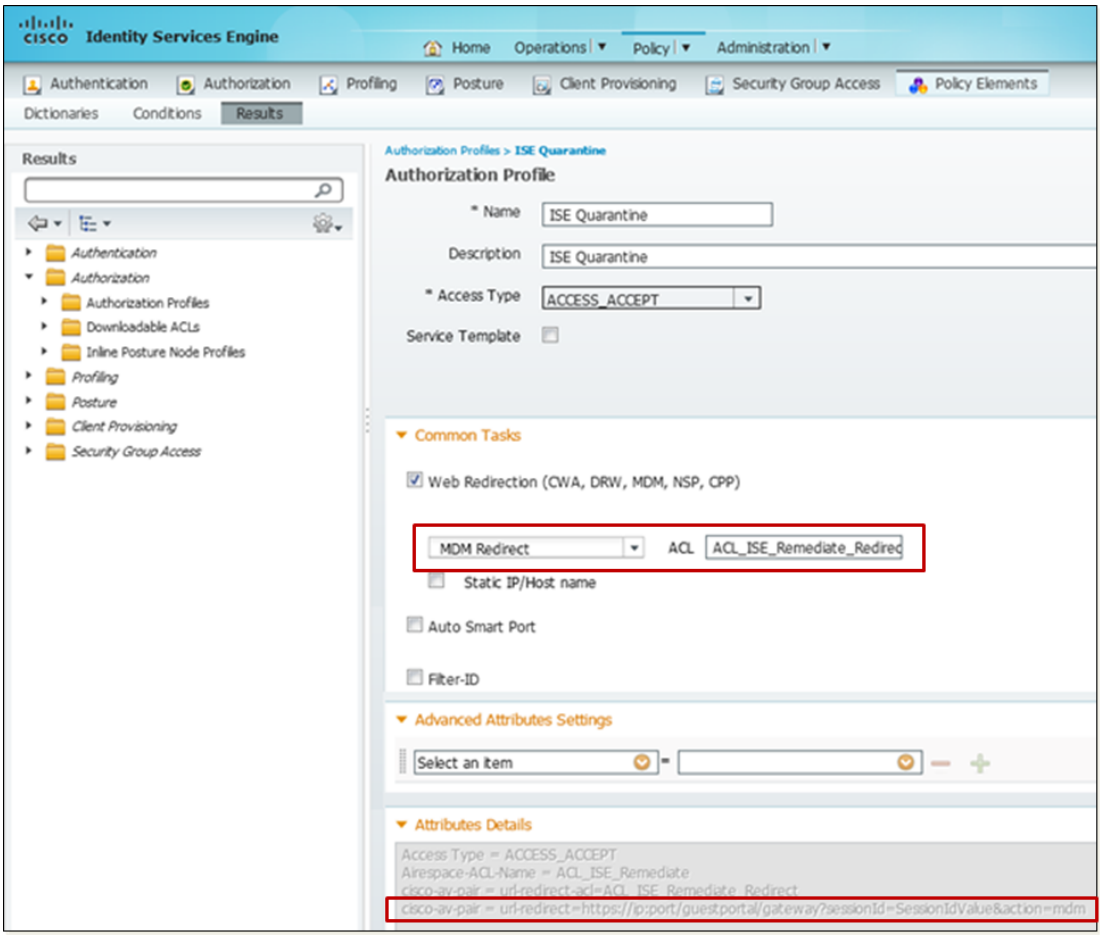


修复 ISE 不合规规则

满足以下条件时，匹配此规则：

- 使用 EAP-TLS 身份验证 （定义为复合条件，见下文）产生连接。
- 设备不符合 ISE 要求。 ISE_Non_Compliant 复合条件在图 11-5 中重点展示。
- 逻辑配置文件等于受 MDM 管理的设备 - 设备由 MDM 托管和支持，如图 11-6 中所示。
- 如果满足这些条件，则使用 ISE Quarantine 授权配置文件。此配置文件配置为将未注册设备重定向至图 11-11 中重点展示的 URL。

图 11-11　　ISE Quarantine 授权配置文件

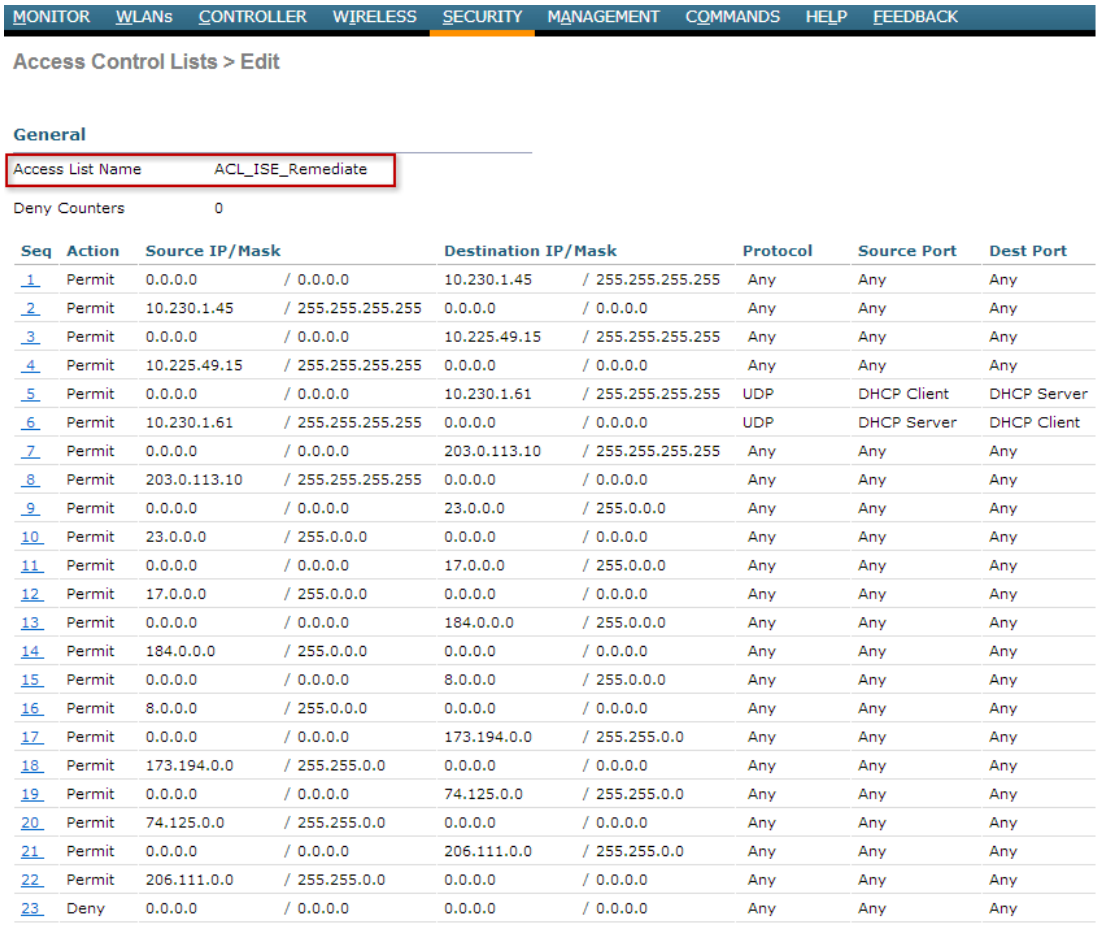


此授权配置文件依赖之前在无线局域网控制器中定义的两个命名 ACL，分别是：ACL_ISE_Remediate_Redirect 和 ACL_ISE_Remediate。图 11-11 中显示，ACL_ISE_Remediate_Redirect 正应用至 “MDM 重定向”设置。在图 11-11 中，ACL_ISE_Remediate 通过 Radius:Airespace-ACL-Name 属性值 (AV) 对发送至无线控制器。两个 ACL 的行为在 CUWN 无线控制器（例如 CT5508 和 Flex 7500）和基于 IOS XE 的控制器（例如 CT5760 和 Catalyst 3850）之间稍有不同。

对于 CUWN 无线控制器，ACL_ISE_Remediate_Redirect 同时充当控制网络重定向的 ACL 以及控制无线客户端可以访问网络中哪些内容的 ACL。 ACL_ISE_Remediate 仅作为一个额外的安全配置。当指定了 URL 重定向时， CUWN 无线控制器不使用此 ACL。

对于 CUWN 无线控制器，ACL_ISE_Remediate 和 ACL_ISE_Remediate_Redirect ACL 可以相同。图 11-12 中展示的是 ACL_ISE_Remediate ACL 示例。

图 11-12　ACL_ISE_Remediate



Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
8	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	23.0.0.0	/ 255.0.0.0	Any	Any	Any
10	Permit	23.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0	/ 0.0.0.0	17.0.0.0	/ 255.0.0.0	Any	Any	Any
12	Permit	17.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	184.0.0.0	/ 255.0.0.0	Any	Any	Any
14	Permit	184.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
15	Permit	0.0.0.0	/ 0.0.0.0	8.0.0.0	/ 255.0.0.0	Any	Any	Any
16	Permit	8.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
17	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
18	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
19	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
20	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
21	Permit	0.0.0.0	/ 0.0.0.0	206.111.0.0	/ 255.255.0.0	Any	Any	Any
22	Permit	206.111.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
23	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

ACL 指定以下访问权限：

- 允许以 DNS 服务器 （10.230.1.45）作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 （10.225.49.15）作为源 / 目标的 IP 访问。
- 允许以 DHCP 服务器 （10.230.1.61）作为源 / 目标的 IP 访问。
- 允许以 MDM 服务器 （203.0.113.10）作为源 / 目标的 IP 访问。
- 允许以 Apple 推送通知服务器 （23.0.0.0 /8 和 17.0.0.0 /8）作为目标的 IP 访问。
- 允许以 Google 云消息（184.0.0.0 /8、8.0.0.0 /8、173.194.0.0 /16、74.125.0.0 /16、206.111.0.0 /16）作为目标的 IP 访问。
- 拒绝进入 （重定向至）其他 IP 地址的 IP 访问。

对于基于 Cisco IOS XE 的无线控制器，ACL_Internet_Redirect 严格用作控制网络重定向的 ACL。ACL_Internet_Only 用作控制无线客户端可以访问网络中哪些内容的 ACL。因此，指定 URL 重定向时，基于 IOS XE 的无线控制器会同时使用两个 ACL。示例 11-3 中展示的是适用于基于 Cisco IOS XE 的无线控制器的 ACL_Internet_Redirect ACL 示例。

示例 11-3　　适用于 IOS XE 控制器的 Remediate Redirect ACL

```
!
ip access-list extended ACL_ISE_Remediate_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 1.230.1.45
 deny ip any host 1.225.49.15
 deny   ip any host 1.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any 23.0.0.0 0.255.255.255
 deny   ip any 17.0.0.0 0.255.255.255
 deny   ip any 184.0.0.0 0.255.255.255
 deny   ip any 8.0.0.0 0.255.255.255
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 deny   ip any host 1.225.100.10
 permit ip any any
!
```

上述 ACL 指定了以下访问权限：

- 拒绝 （不重定向） DHCP 流量。
- 拒绝 （不重定向）以 DNS 服务器 （1.230.1.45）作为源 / 目标的 IP 访问。
- 拒绝 （不重定向）以 ISE 服务器 （1.225.42.15）作为源 / 目标的 IP 访问。
- 拒绝（不重定向）以 MDM 服务器（主机 1.230.1.76 和子网 63.128.76.0 /24）作为源 / 目标的 IP 访问。
- 拒绝（不重定向）以 Apple 推送通知服务器（23.0.0.0 /8 和 17.0.0.0 /8）作为目标的 IP 访问。
- 拒绝（不重定向）以 Google 云消息（184.0.0.0 /8、8.0.0.0 /8、74.125.0.0 /16、173.194.0.0 /16、206.111.0.0 /16）作为目标的 IP 访问。
- 允许 （重定向）以所有其他 IP 地址作为目标的 IP 访问。

示例 11-4 中展示的是适用于基于 Cisco IOS XE 的无线控制器的 ACL_ISE_Remediate ACL 示例。

示例 11-4　　适用于 Cisco IOS XE 控制器的 Remediate Access ACL

```
!
ip access-list extended ACL_ISE_Remediate
 permit udp any eq bootpc any eq bootps
 permit ip any host 1.230.1.45
 permit ip any host 1.225.49.15
 permit ip any host 1.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any 23.0.0.0 0.255.255.255
 permit ip any 17.0.0.0 0.255.255.255
 permit ip any 184.0.0.0 0.255.255.255
 permit ip any 8.0.0.0 0.255.255.255
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
 deny   ip any any
!
```

上述访问列表指定以下访问权限：

- 允许 DHCP 流量。
- 允许以 DNS 服务器 （1.230.1.45）作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 （1.225.42.15）作为源 / 目标的 IP 访问。
- 拒绝以 MDM 服务器 （主机 1.230.1.76 和子网 63.128.76.0 /8）作为源 / 目标的 IP 访问。

- 允许以 Apple 推送通知服务器 （23.0.0.0 /8 和 17.0.0.0 /8）作为目标的 IP 访问。
- 允许以 Google 云消息（184.0.0.0 /8、8.0.0.0 /8、74.125.0.0 /16、173.194.0.0 /16、206.111.0.0 /16）作为目标的 IP 访问。
- 允许以所有其他 IP 地址作为目标的 IP 访问。

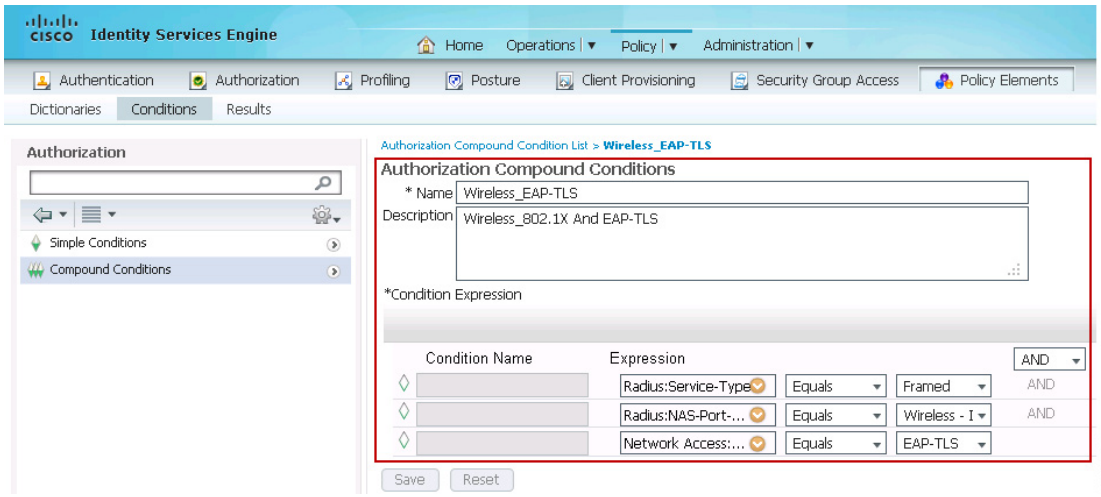
注意　示例 11-4 中显示的访问列表是通用列表，不一定适用于所有组织。 ACL 应更加具体，且仅允许在规定方向访问特定 IP 地址和协议。通常我们会尽可能详尽地描述 ACL，并将每一个条目深入定义到端口级别。

Wireless_EAP-TLS 复合条件检查以下情况：

- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless - IEEE 802.11
- Network Access:EapAuthentication Equals EAP-TLS

要定义此复合条件，请点击 **Policy > Conditions > Authorization > Compound Conditions**。图 11-13 显示了 Wireless_EAP-TLS 条件如何将多个条件结合到一个条件中。

图 11-13　Wireless_EAP-TLS 条件



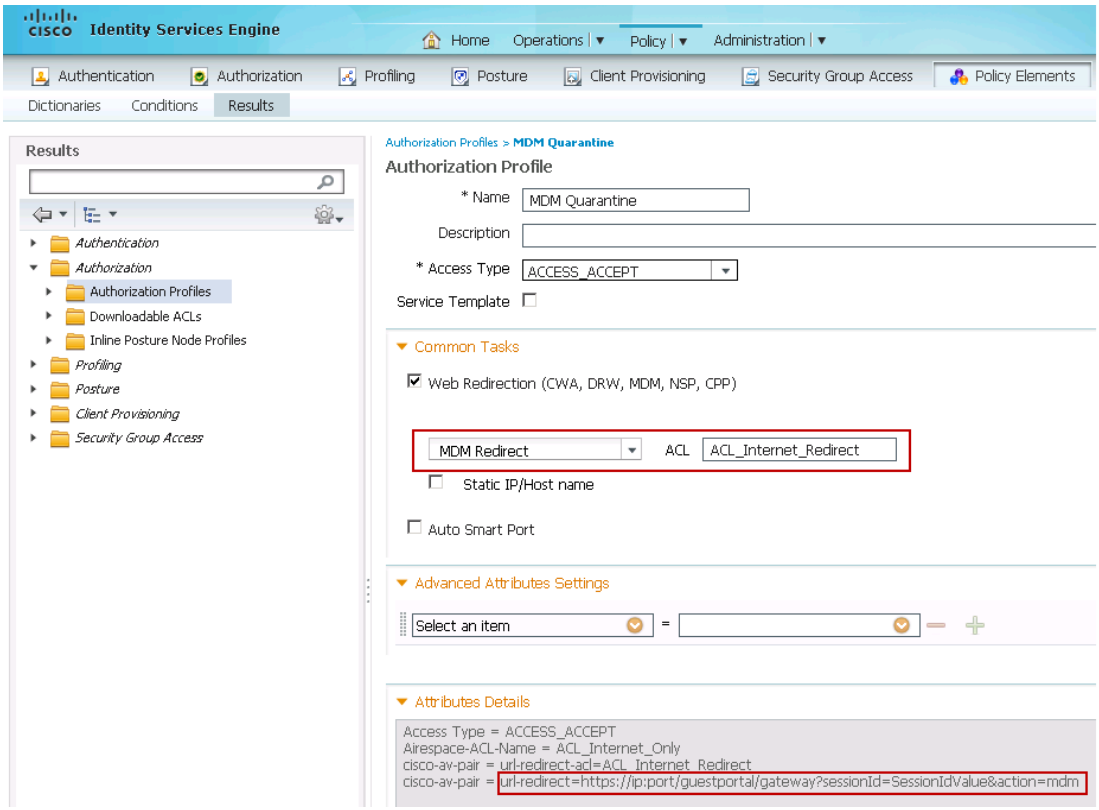
修复 MDM 不合规规则

满足以下条件时，匹配此规则：

- 使用 EAP-TLS 身份验证发起连接，如图 11-13 中重点展示的 Wireless_EAP-TLS 复合条件所定义的那样。
- 设备不符合 MDM 策略要求。ISE 向 MDM 发出 DeviceCompliantStatus API 调用，以获取此信息。
- 逻辑配置文件大小与 MDM 托管配置文件相同 - 设备由 MDM 托管和支持。

如果满足这些条件，则使用 MDM Quarantine 授权配置文件。此配置文件配置为将未注册设备重定向至图 11-14 中重点展示的 URL。

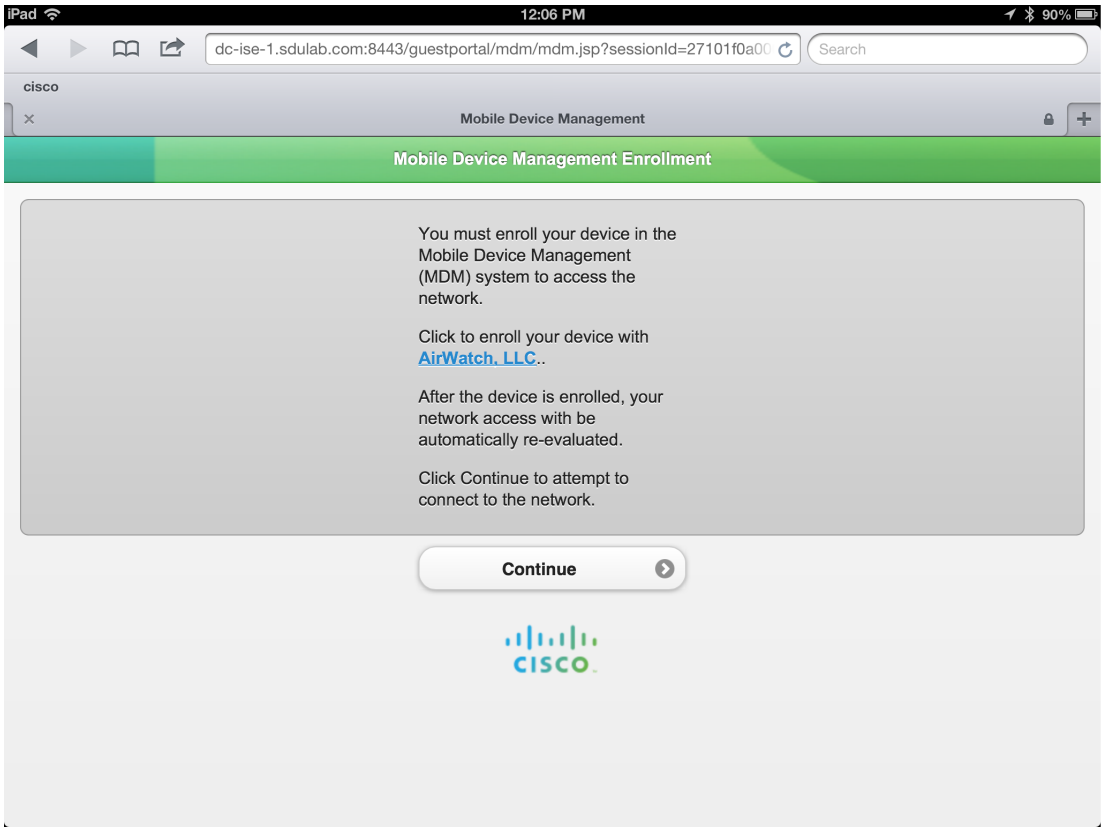
图 11-14　　MDM 隔离授权配置文件



授权配置文件依赖修复 ISE 不合规规则中之前讨论的两个命名 ACL，分别是：ACL_Internet_Redirect 和 ACL_Internet_Only。

用户尝试访问内部资源时，会话将重定向至与图 11-15 中类似的页面，表明设备为什么不符合 MDM 策略。

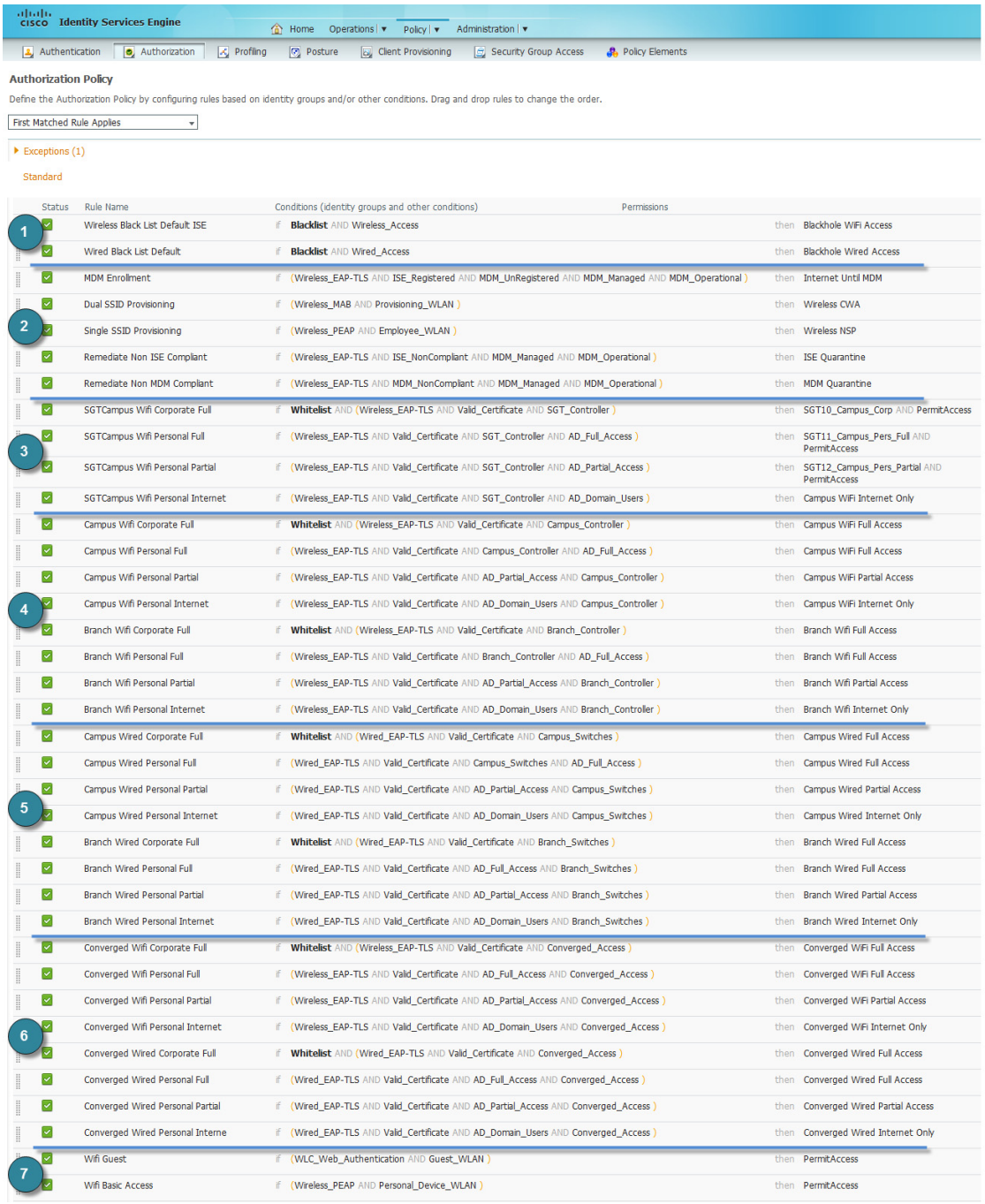
图 11-15　　MDM 隔离



为便于参考，测试过程中使用图 11-16 中显示的完整授权策略。该图重点显示了以下部分：

1. 用于将丢失或被盗的设备列入黑名单。
2. 入网和 MDM 注册 / 补救。
3. 从 SGT_Enabled 位置中的接入点连接的无线设备。
4. 从园区或分支机构位置中的接入点连接的无线设备。
5. 从园区或分支机构位置连接的有线设备。
6. 从融合位置连接的有线和无线设备。
7. 访客和基本访问。

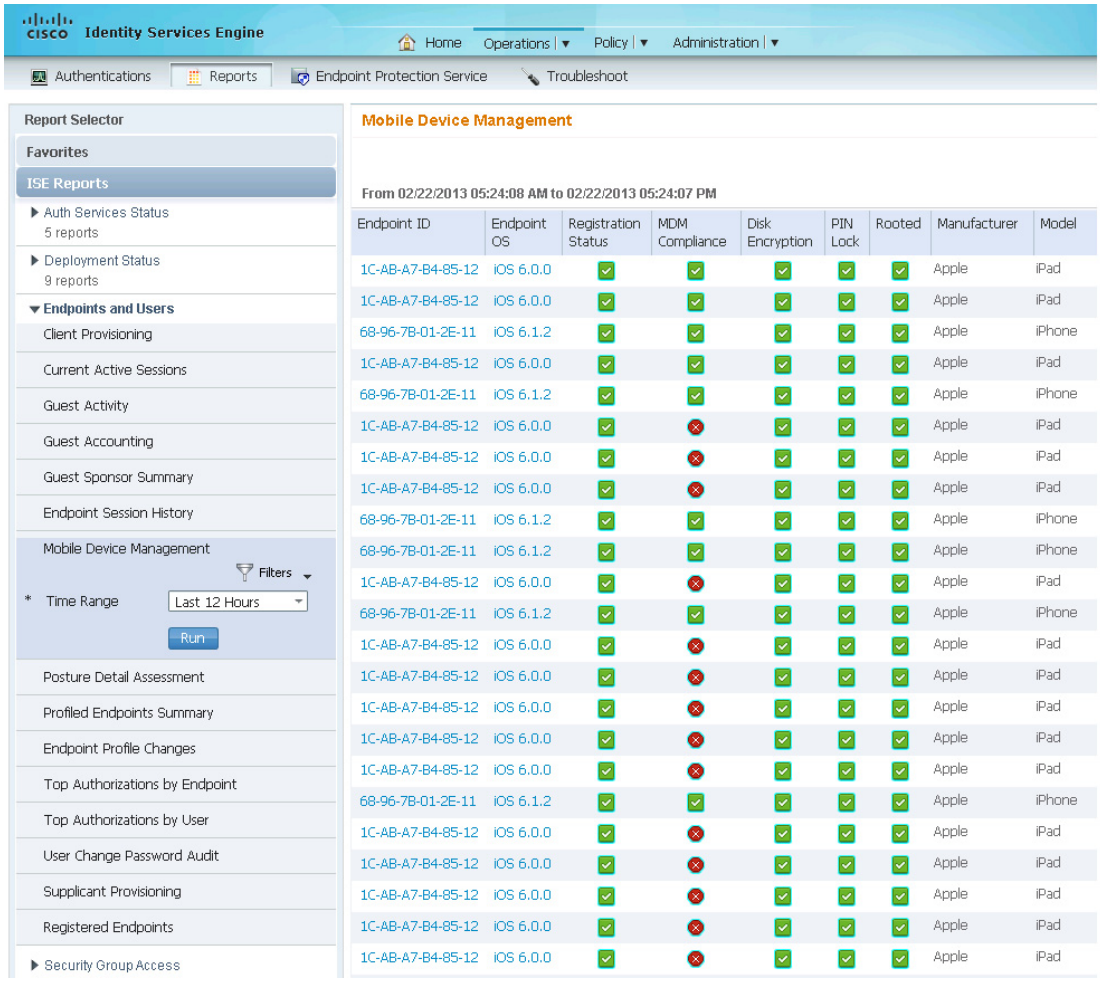
图 11-16　　完整授权策略



MDM 报告

Cisco ISE 提供用于审计、故障管理和故障排除的记录机制。有多个报告提供终端相关信息。在图 11-17 中，移动设备管理报告显示连接至 ISE 的终端和从 MDM 收集的若干属性。其他报告提供可用于报告和故障排除的其他信息。

图 11-17　　MDM 报告



BYOD 基本访问使用案例

修订日期：2013 年 8 月 7 日

本设计指南之前的章节对自注册员工个人设备进行了检查，以便提供完全、部分或仅互联网的访问。数字证书的使用能防止设备 MAC 地址欺骗，从而提供更高级别的身份验证安全。此外，自助注册访客门户和“我的设备”门户的使用，简化了员工个人设备的自注册和维护，从而降低了与提供 BYOD 服务相关联的 IT 运营成本。

尽管存在上述优势，但是部分组织可能仍然会决定采用不允许员工个人无线设备自注册，而仅为这些设备提供一部分公司服务和互联网访问权限的业务策略。这可能是由以下一种或多种原因造成的：

- 组织不希望或没有能力在员工个人设备上部署数字证书。
- 员工可能决定不接受组织对其个人设备的管理。
- 组织不希望按照行政管理方式管理和维护拥有完全网络访问权限的已注册企业设备和 BYOD 设备的单独列表。
- 组织可能希望简单地根据员工个人设备未知或不可信的安全状态将其限制在企业防火墙“之外”。

因此，下面的部分将针对不涉及员工无线设备自注册的设计方案展开讨论。这些设计的基本思路是扩展传统访客无线访问权限（在第 13 章，“BYOD 访客无线接入”中讨论），以及为员工个人设备提供类似访客的无线访问权限。

注意 本章的所有内容基于一个假设，即企业拥有的设备仍能自注册。为了防止员工个人设备获取企业网络的完全访问权限，仍必须使用白名单。

将访客无线访问权限扩展到员工个人设备

以下各节讨论扩展访客无线访问权限（在第 13 章，“BYOD 访客无线接入”中讨论），以便允许员工个人设备接入访客网络的两种方法：

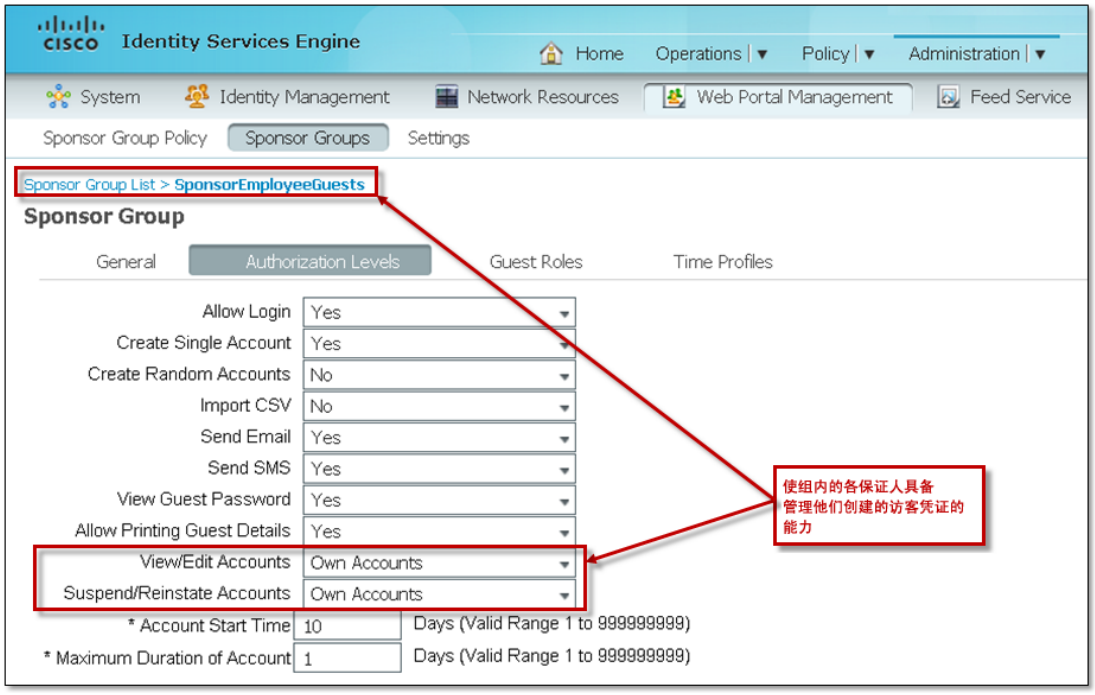
- 允许员工自行调配访客凭证。
- 扩展访客网络身份验证 (Web Auth)，以便在对使用个人设备的访客和员工进行身份验证时，也使用 Microsoft Active Directory (AD) 数据库。

允许员工自行调配访客凭证

第 13 章，“BYOD 访客无线接入”讨论了如何通过 Cisco ISE 保证人门户调配访客凭证。将访客无线访问权限扩展到员工个人设备的最基本形式就是允许员工将为自己保证为访客。然后，员工手动连接到开放的访客 SSID，在无线访客网络上使用个人设备。

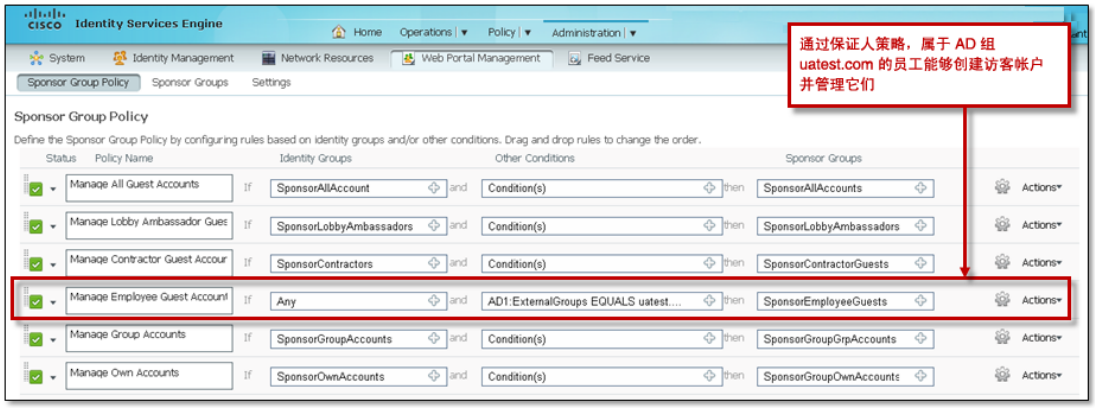
通过 Cisco ISE 保证人门户，保证人身份验证策略可根据特定 Microsoft AD 组内的成员而定。这在配置 Cisco ISE 保证人门户中进行了讨论，其中介绍了利用在 ISE 保证人组策略中使用 Microsoft AD 组的方法，来限制保证人对 Cisco ISE 服务器的访问。利用同样的方法，可通过向这些 Microsoft AD 组添加其他员工，使 ISE 保证人门户接受更大范围的访问。或者，可以创建一个新保证人组，允许单个员工配置访客凭证，但将他们限制为仅能修改已调配的凭证。示例如下图所示。

图 12-1　　允许员工创建自助访客凭证的 ISE 保证人组示例



通过 ISE 保证人组策略，可以将此 ISE 保证人组的成员限制为 Microsoft AD 组，如图 12-2 所示。

图 12-2　　允许员工创建自助访客凭证的 ISE 保证人组策略示例



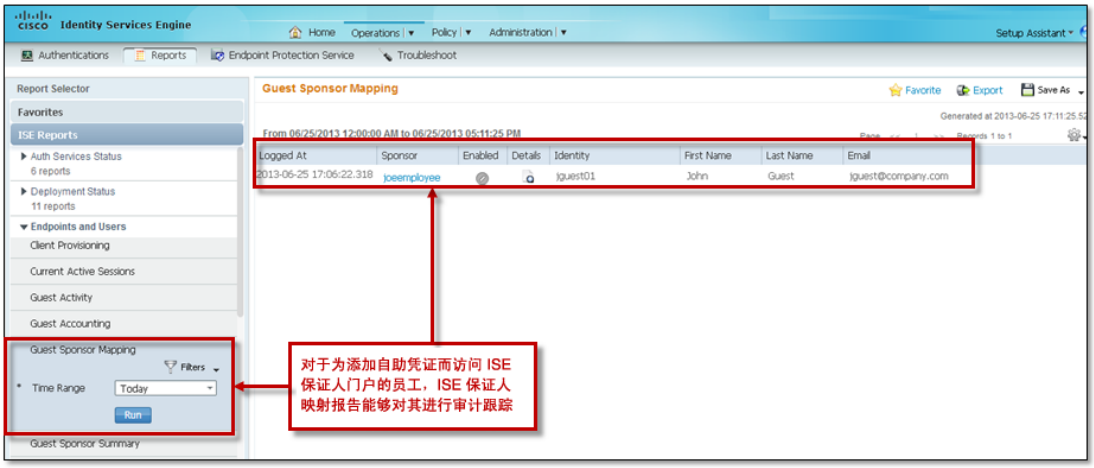
在本示例中，仅限既是 Microsoft Active Directory 域成员，又是 “用户 / 域用户”组成员的用户访问保证人组。示例的确切条件为以下形式：

```
AD1:ExternalGroups EQUALS uatest.com/Users/Domain Users
```

本示例中， Microsoft Active Directory 域为 “uatest.com”。请注意，必须将 Microsoft Active Directory 服务器配置为外部身份源，才能选择此选项。在本示例中， Microsoft Active Directory 服务器为 “AD1”。

此设计的一个优点是，通过有关员工在 ISE 保证人门户进行的身份验证的 ISE 报告，可以实现审计跟踪。员工成功创建访客凭证以及访客凭证创建成功时，都会显示 ISE 保证人映射报告。 ISE 保证人映射报告可以在不同的时间范围内运行 （从 30 分钟到最多 30 天），也可以在请求的自定义时间范围内运行。此报告可用于获取员工访问 ISE 保证人门户创建访客凭证的大致情况和频率。如图 12-3 中的示例所示。

图 12-3　　针对访问 ISE 保证人门户的员工的审计跟踪示例



请注意，这种允许员工为自己创建访客凭证的方法并不能阻止他们为访问组织的真正访客创建凭证。公司业务策略应规定真正的访客凭证仅能由保证人组的授权成员添加，如第 13 章，“BYOD 访客无线接入”中所述。下面一种设计方案通过去除员工为自己创建访客凭证的功能，完全消除了这一问题。

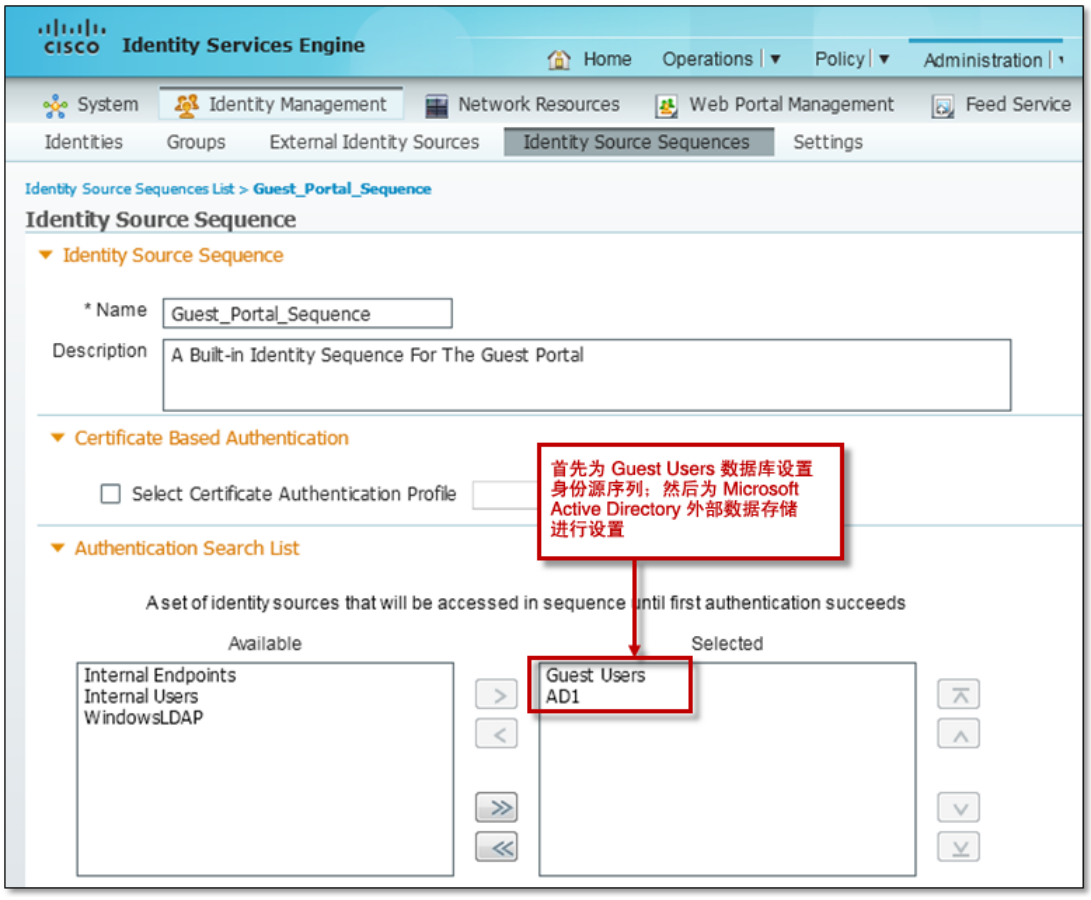
扩展网络身份验证，以便在对使用个人设备的员工进行身份验证时使用 Microsoft AD

前面的部分讨论了扩展访客无线访问权限以允许使用个人设备的员工接入访客网络的最基本方法。此方法仅仅是允许员工通过 Cisco ISE 保证人门户为自己配置访客凭证。虽然与其他方法（例如在访客无线控制器上使用共享保证人帐户添加凭证）相比，此方法具有若干优势，但它仍有一些缺陷。员工仍必须自行调配临时访客凭证。最后，除非使用公司业务策略，否则无法阻止员工为真正的访客提供保证。

要为员工个人设备提供接入访客无线网络的权限，另一种方法是，在执行网络身份验证 (Web Auth) 时，允许 ISE 服务器检查凭证的多个身份源。例如， ISE 服务器可以首先在其内部身份组（本地数据库）中检查访客凭证。如果未找到凭证，则检查 Microsoft AD 外部身份库，以查看访问访客网络的人员是否为员工 （而非访客）。

第 13 章，“BYOD 访客无线接入”中的 Cisco ISE 策略配置 中讨论了使用用户定义的名为 Guest_Portal_Sequence 的身份源序列，通过网络身份验证对访客访问权限进行身份验证。Guest_Portal_Sequence 仅使用内部用户身份源。通过将 Microsoft Active Directory (AD1) 外部身份源添加到该序列，可以很容易实现扩展，如图 12-4 所示。

图 12-4　　经扩展包括 AD 的 Guest_Portal_Access 身份源序列示例



现在，此配置可允许 Microsoft Active Directory 数据库中的员工在已进行网络身份验证并接受可接受使用政策 (AUP) 或最终用户协议 (EUA) 的情况下，通过其个人设备访问访客无线网络。

注意　此配置也允许员工通过公司拥有的设备访问访客无线网络，因为身份验证和授权决策仅基于 Microsoft Active Directory 用户 ID 和密码。在身份验证和授权决策中，不用考虑设备本身。

为员工个人设备部署类似访客的无线访问权限

前面的部分讨论了为使用个人设备的员工扩展无线访客网络访问权限的选项：一种是允许员工为自己配置访客凭证，另一种是扩展网络身份验证以便也检查存储员工凭证的 Microsoft AD 数据库。使用这些选项，员工个人设备可共享与访客设备相同的无线 SSID。员工个人设备也将共享与访客设备相同的 IP 子网寻址空间，因为它们会在 ASA 防火墙的同一 DMZ 网段终止。本质上，员工个人设备会被视为网络上的访客，这将会带来潜在的问题。

由于 IP 子网空间在访客设备和员工个人设备之间共享，所以可能会出现员工个人设备耗尽 IP 寻址空间的问题，并因而限制访客设备获取访客网络访问权限的能力，反之亦然。

ASA 防火墙访客 DMZ 接口入口策略可修改为允许从访客网络传入位于其他 DMZ 网段、专用于员工个人设备的公司网站服务器镜像的某些应用流。相关内容将在访问公司资源中进一步讨论。但是， ASA 防火墙策略将无法区分访客设备和员工个人设备，因为它们共享了同一 IP 子网地址空间。因此，要防止访客访问镜像 Web 服务器上的服务，镜像 Web 服务器本身的应用级别访问控制必不可少。同样， ASA 防火墙访客 DMZ 接口入口策略可修改为允许从虚拟客户端 （例如 Citrix 或 VMware 客户端）传入内部 Citrix 或 VMware 服务器的流量。如前所述， ASA 防火墙策略无法区分真正的访客设备和员工个人设备，因为它们共享了同一 IP 子网地址空间。要防止访客访问这些服务器， Citrix 或 VMware 服务器的应用级别访问控制必不可少。

由于访客 SSID 通常为开放形式且未加密，因此来自员工个人设备的流量将为明文形式，除非设备使用安全应用或某种对流量进行加密的 VPN 隧道。虽然只需要求使用 HTTPS 即可保证网络流量的安全，但并非员工个人设备中使用的所有应用都会加密。这样就留下了一些漏洞，安全运营人员必须将此考虑在内，尤其是对所有使用员工的公司登录名和密码进行身份验证的站点。如果企业内部数据会被员工个人设备通过访客无线网络访问，则应加密这些信息，以防窃听。允许员工设备启动 VPN 客户端以建立 IPsec VPN 会话 - 直接连接到 ASA 防火墙，或者向外连接到互联网并返回到其他公司 VPN 集中器 - 可能也是一种备选方案。另一个方案是为员工设备建立到 ASA 防火墙的 SSL VPN 隧道。这两个方案可能还需要按用户进行身份验证。

注意　思科的网络身份验证实施在重定向 Web 会话以及请求凭证时使用 HTTPS。

考虑到这些问题，在为访问访客网络的设备 （不论是真正的访客设备还是员工个人设备）授予访问权限时，安全运营人员可能会犹豫是否为其授予除互联网之外的访问权限。

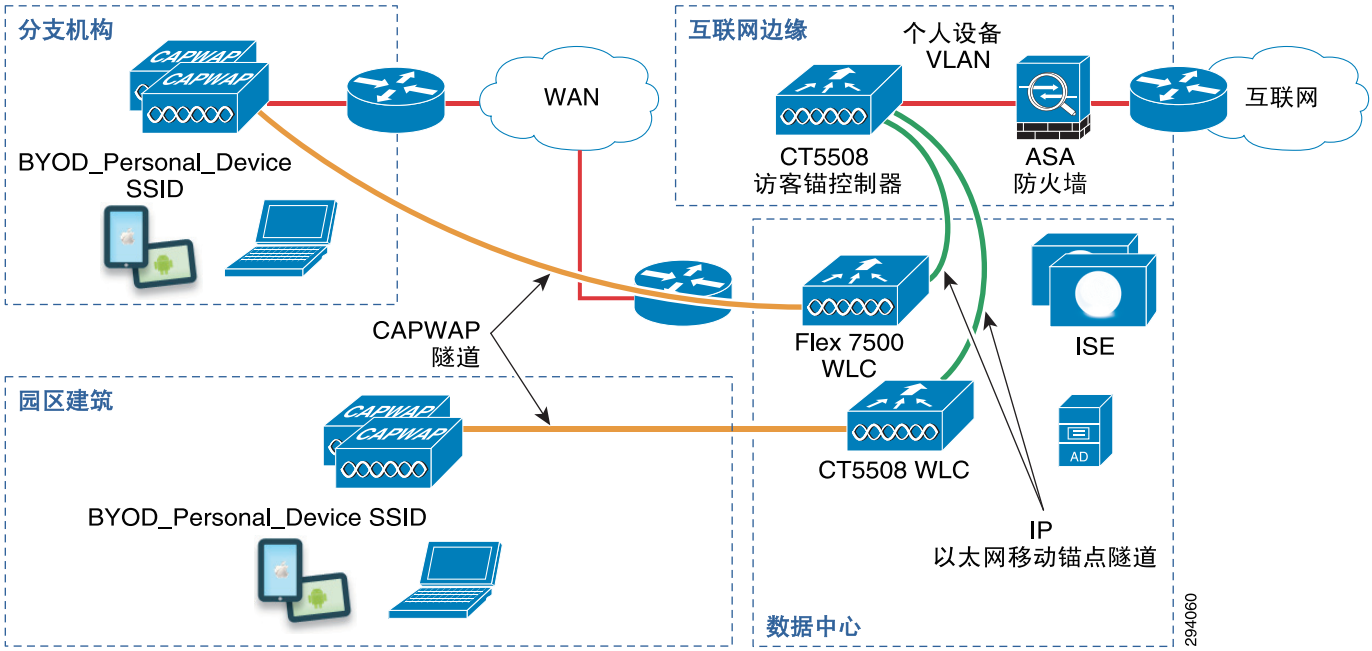
如第 13 章，“BYOD 访客无线接入”所述，本章使用了两组不同的术语。第一对术语是访客控制器和园区控制器。访客控制器是用于处理访客和员工个人设备流量的专用控制器。园区控制器专门用于处理内部流量。请注意，此处使用的术语 “园区控制器”有些笼统。本章中讨论的园区控制器可以指在园区位置内部署的独立无线控制器平台，也可以指在分支机构位置中部署的 Catalyst 3850 系列交换机中集成的无线控制器功能。

第二组术语是外部控制器和锚控制器。这两个术语会在用户从一个控制器漫游到另一个控制器时使用。用户关联的新控制器是外部控制器。此控制器将所有流量锚定到旧控制器，因此旧控制器称为锚控制器。本文档中使用了这些术语。

员工个人设备专用 SSID

本节讨论另一种方案，其中为员工个人设备调配了类似第二个访客的无线 SSID。此 SSID 以类似于无线访客 SSID 的方式，自动锚定到独立于 ASA 防火墙的另一个 DMZ 网段。图 12-5 中显示了使用 CUWN 基础设施实现此设计的示例。

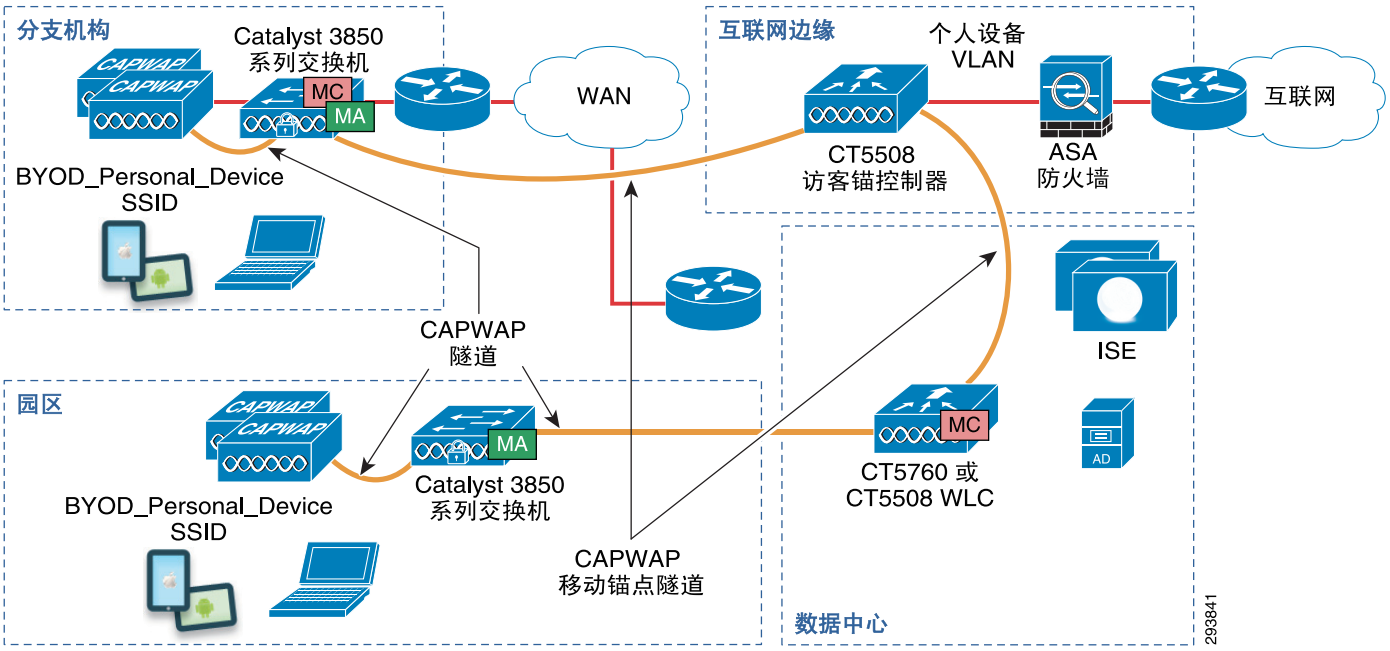
图 12-5　使用 CUWN 基础设施进行员工个人设备的类似访客无线接入



通过思科无线控制器的自动锚定移动功能，来自无线客户端的数据包经由内部无线控制器（称为外部控制器）与访客无线控制器（称为锚控制器）之间的移动隧道封装到访客无线控制器，以进行解封并传送到有线网络。

图 12-6 中显示了使用融合接入无线基础设施实现此设计的类似示例。

图 12-6　使用融合接入基础设施进行员工个人设备的类似访客无线接入



自动锚定移动功能也适用于融合接入基础设施。请注意，通过图 12-6 中显示的融合接入分支机构设计，分支机构中的 Catalyst 3850 交换机将同时执行移动代理 (MA) 和移动控制器 (MC) 功能。通过融合接入园区设计，Catalyst 3850 交换机仅执行 MA 功能。MC 功能由专用 CT5760 无线控制器执行。由于自动锚定隧道从融合接入设计中的 MC 发起，流量首先通过隧道从园区 Catalyst 3850 交换机传输到 CT5760 无线控制器，然后自动锚定到 DMZ 中的访客锚控制器。有关融合接入基础设施中的 MA 和 MC 功能的更多探讨，请参阅配置基础设施。

注意　在本版设计指南中，假设使用个人设备的员工需要手动关联到此 SSID。未来版本可能会研究其他使用 RADIUS 身份验证更改 (CoA) 功能或设备配置文件的方案。

为员工个人设备实施专用 SSID 的优势在于， SSID 无需配置为具有开放式接入，而且还可加密，这与本设计指南中讨论的访客 SSID 有所不同。相反，员工个人设备 SSID 可通过诸如 802.1X 身份验证和 WPA-2/AES 加密等机制保证安全，以防止员工个人设备遭到流量窃听。由于员工与 SSID 相关联，所以可以使用外部 Microsoft AD 身份源，通过 Cisco ISE 服务器对员工进行身份验证。

为员工个人设备实施专用 SSID 的另一个优点在于，可通过为每个 SSID 调配单独的 VLAN，将设备从访客设备中分离出来。可以部署单独的 DMZ 网段：或者作为独立于 ASA 防火墙的单独物理接口实施；或者作为独立于 ASA 防火墙单个物理接口的单独 VLAN 子接口实施。每个 DMZ 接口目前都具有独立的 IP 子网地址空间和独立的访问控制策略。这不仅扩展了为访客设备和员工个人设备部署的 IP 寻址空间，也消除了员工个人设备和访客设备相互造成对方可用 IP 地址耗尽的问题。访客 DMZ 可配置为仅允许访客设备接入互联网。员工个人可配置为允许访问互联网，以及访问位于另一个 DMZ 网段中的镜像 Web 服务器。通过修改 ASA 防火墙个人设备 DMZ 接口入口策略来允许从虚拟客户端（例如 Citrix 或 VMware 客户端）传入内部 Citrix 或 VMware 服务器的流量，还可以允许其他访问权限。访问权限还可以通过以下方式扩展：允许员工个人设备通过启动 VPN 客户端来建立 IPsec VPN 会话（直接连接到 ASA 防火墙；或者先外部连接到互联网，然后返回到其他公司 VPN 集中器）。另一种方案是为员工个人设备建立到 ASA 防火墙的 SSL VPN 隧道。

无线控制器配置

要部署这种为员工个人设备调配类似第二个访客的无线 SSID 的方案，则需要使用新 WLAN 为员工个人设备配置园区（外部）无线控制器和访客（锚）控制器。此 WLAN 具有与企业 WLAN 和访客 WLAN 不同的独特 SSID。

园区控制器配置

本节讨论针对园区控制器使用 CUWN 无线控制器或融合接入（基于 IOS XE）无线控制器时的配置。

CUWN 无线控制器配置

图 12-7 中显示了 CUWN 园区控制器配置的示例，其中，新 WLAN 称为 BYOD_Personal_Device WLAN。

图 12-7　　适用于员工个人设备 WLAN 的 CUWN 园区无线控制器配置示例

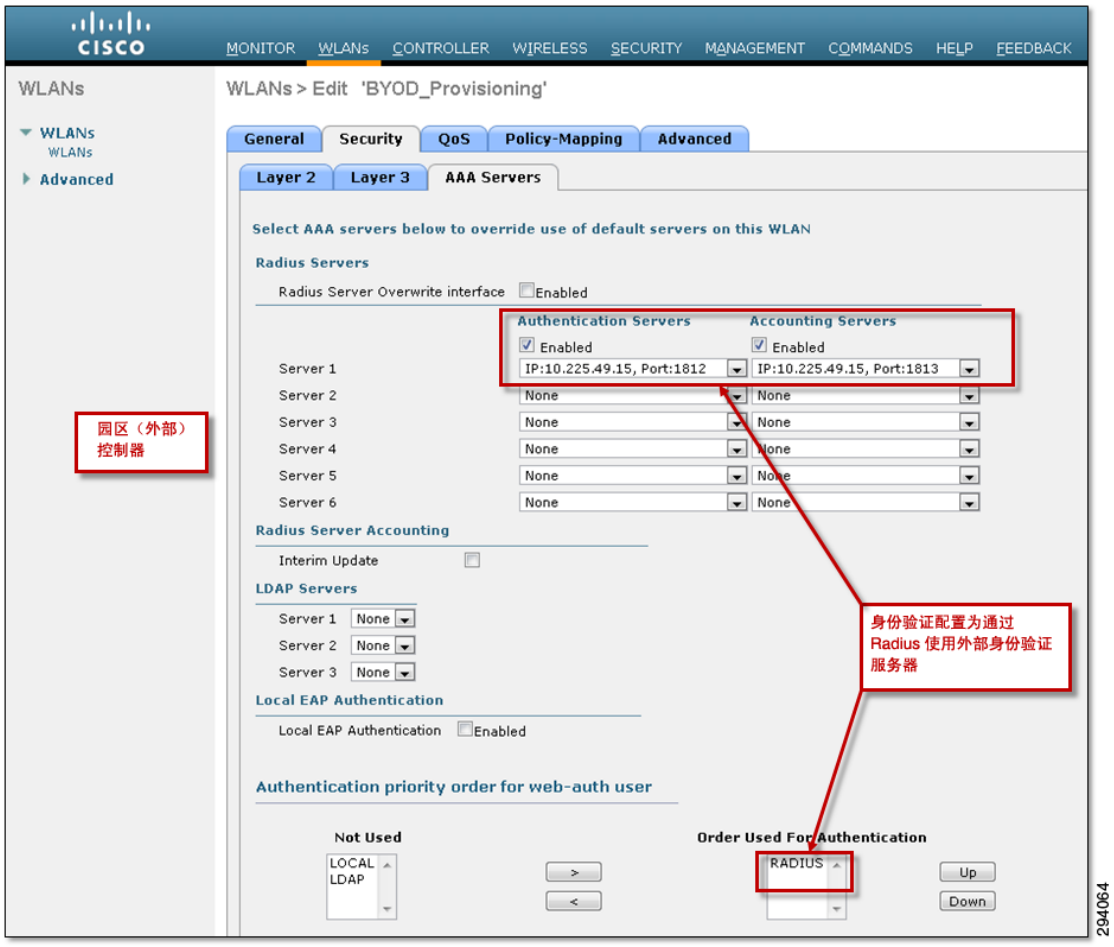
WLAN 配置为使用基于 AES 密码的 WPA2 安全设置，以及基于 802.1X 身份验证的密钥管理。接下来，需要使用指向访客（锚）控制器管理接口的移动锚点配置园区（外部）控制器上的 WLAN。如图 12-8 中的示例所示。请注意，在使用 FlexConnect 无线设计的分支机构情景中，为分支机构 AP 提供服务的控制器将作为分支机构个人设备 WLAN 的外部控制器。

图 12-8　　园区 CUWN 无线控制器上的移动锚点配置示例

请注意，园区控制器与访客控制器必须成为同一移动组的一部分，然后才能配置移动锚点。移动锚点会建立移动隧道，来自无线客户端的数据包将通过该移动隧道自动封装，然后从园区控制器发送至访客控制器进行解封并传送至有线网络。

网络管理员还必须配置员工个人设备 WLAN，以使用园区控制器中的 RADIUS 进行身份验证。如图 12-9 所示。

图 12-9　　通过 RADIUS 对园区控制器上的员工个人设备 WLAN 进行身份验证



由于此方案不涉及网络身份验证，因此不会发生 Web 会话重定向到访客门户，所以既不需要在配置访客控制器中配置网络身份验证，也无需任何预身份验证 ACL。员工个人设备连接到 SSID 时，园区控制器管理接口会向 Cisco ISE 服务器发起 RADIUS 会话，以进行身份验证和授权。成功进行了身份验证后，员工的个人设备将锚定到访客控制器。

融合接入 （基于 IOS XE）无线控制器配置

以下配置片段显示了基于 IOS XE 的无线控制器上的员工个人设备 WLAN 及部分 AAA 服务器配置。

```
!
aaa new-model
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
dot1x system-auth-control
!
```

```
ip http server
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 5 tries 3
radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key 7 1237161E060E5D56797F71
!                    / 以上行中的 Radius 服务器指向 ISE
!
wlan BYOD_Personal_Device 4 BYOD_Personal_Device/ 定义个人设备 WLAN 和 SSID
 client vlan Guest/ 静态分配给不可路由的 （隔离的） VLAN
 mobility anchor 10.225.50.35/ 创建到访客无线控制器的锚定隧道
 session-timeout 1800
 no shutdown    / 启用员工设备 WLAN
!
```

默认情况下会启用基于 AES 密码的 WPA2 安全设置，以及基于 802.1X 身份验证的密钥管理。因此，它们不会显示在配置中。管理级别的 **show wlan id <*wlan ID number*>** 命令可用于显示有关 WLAN 配置的其他详细信息，包括未在配置中显示的默认值。

必须在用作移动代理 (MA) 以及移动控制器 (MC) 的设备上配置员工设备 WLAN。因此，无论是将 Catalyst 3850 系列交换机部署为分支机构部署中的 MA 兼 MC、将 Catalyst 3850 系列交换机仅部署为园区部署中的 MA，还是将 CT5760 无线控制器部署为园区部署中的 MA 兼 MC，上述配置基本都是相同的。

上述配置中的访客客户端 VLAN 是 CT5760 无线控制器或 Catalyst 3850 系列交换机上隔离的 VLAN。它不中继到相邻的第 3 层设备。如果外部控制器和锚控制器之间的 CAPWAP 隧道中断，则会隔离所有访客设备。

以下配置片段显示了基于 IOS XE 的无线控制器上的移动组和移动组成员的配置。

```
!
wireless mobility group member ip 10.225.50.35 public-ip 10.225.50.35/ 访客控制器
wireless mobility group name byod/ 移动组名称
!
```

移动组名称和移动组对等点必须显示在作为移动控制器 (MC) 的设备上。因此，如果 Catalyst 3850 系列交换机已部署为分支机构部署中的 MA 兼 MC，则配置必须包括上述两行。如果仅将 Catalyst 3850 系列交换机部署为园区部署中的 MA，则其中将不包括移动组配置。而部署为园区内的 MA 兼 MC 的 CT5760 无线控制器将包含移动组配置。请注意，由于基于 IOS XE 的无线控制器仅支持新分层移动架构，因此无需通过配置来启用它。

注意　思科无线控制器目前支持两种不同的移动架构。旧移动架构依赖于无线控制器之间的 IP 以太网隧道。新移动架构也称为分层移动架构，它依赖于无线控制器之间的 CAPWAP 隧道。两种移动架构互不兼容。如果无线控制器之间需要移动功能 （包括自动锚定功能），则所有无线控制器必须运行新移动架构或旧移动架构。 Cisco 5508 和 WiSM2 无线控制器软件版本 7.3.112 以及 Cisco 5508、WiSM2 和 2504 无线控制器软件版本 7.5 支持新移动架构。IOS XE 软件版本为 3.2.0SE 和 3.2.2SE 的 Cisco 5760 无线控制器和 Catalyst 3850 系列交换机也都支持新移动架构。 7.4 版以及 7.3.112 以下版本的 CUWN 无线控制器仅支持旧移动架构。Cisco Flex 7500、8500 和 vWLC 不支持新移动架构。基于 IOS XE 的无线控制器不支持旧移动架构。因此，如果网络同时包含 Flex 7500 无线控制器和融合接入控制器，则必须使用 DMZ 部署一组独立的访客无线控制器，以便同时为本设计指南所探讨的访客无线设计中涉及的两种移动架构提供支持。

访客控制器配置

访客控制器是所有员工设备流量终结的点。在本版设计指南中，将仅讨论以 CT5508 CUWN 无线控制器作为访客控制器的情况。图 12-10 显示了员工个人设备 WLAN 的访客控制器配置示例。

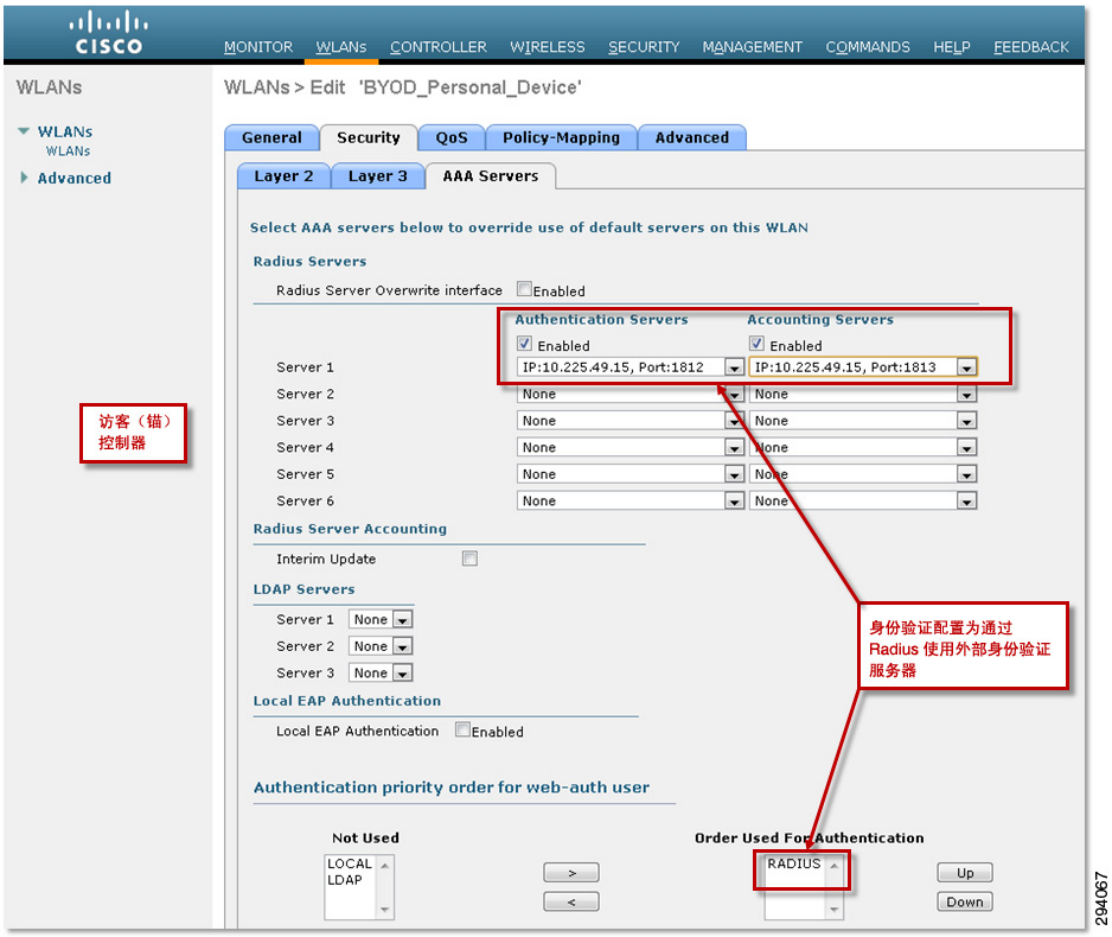
图 12-10　适用于员工个人设备 WLAN 的访客无线控制器配置示例

可以看到，访客控制器上的 WLAN 配置必须与园区控制器上的 WLAN 配置相匹配。访客控制器需要通过指向自身的移动锚点进行配置。如图 12-11 中的示例所示。

图 12-11　访客 CUWN 无线控制器上的移动锚点配置示例

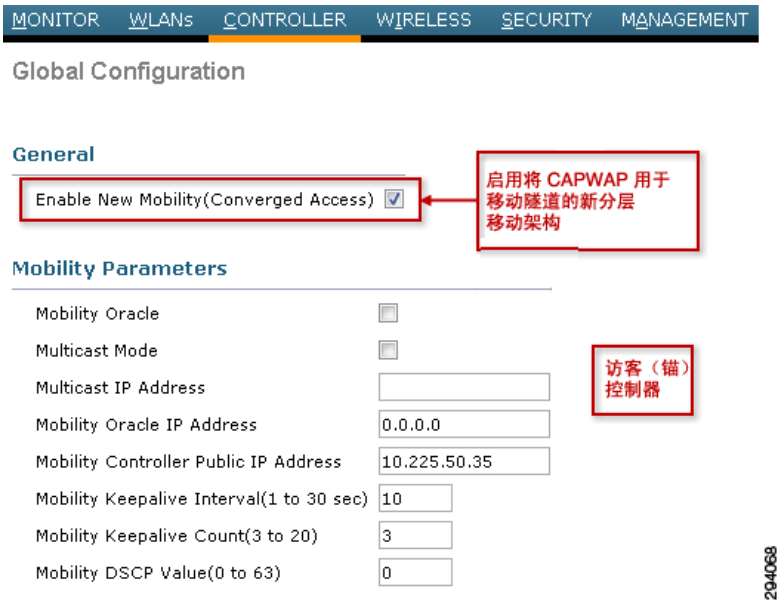
同样，此配置假设在配置移动锚点之前，园区控制器与访客控制器均配置为同一移动组的一部分。网络管理员还必须配置员工个人设备 WLAN，以使用访客控制器中的 RADIUS 进行身份验证。如图 12-12 所示。

图 12-12　通过 RADIUS 对访客控制器上的员工个人设备 WLAN 进行身份验证



最后，为支持新移动架构（也称为分层移动架构），网络管理员必须选中园区和访客控制器全局移动配置中的“启用分层架构”选项。如图 12-13 中的示例所示。

图 12-13　　启用分层移动架构

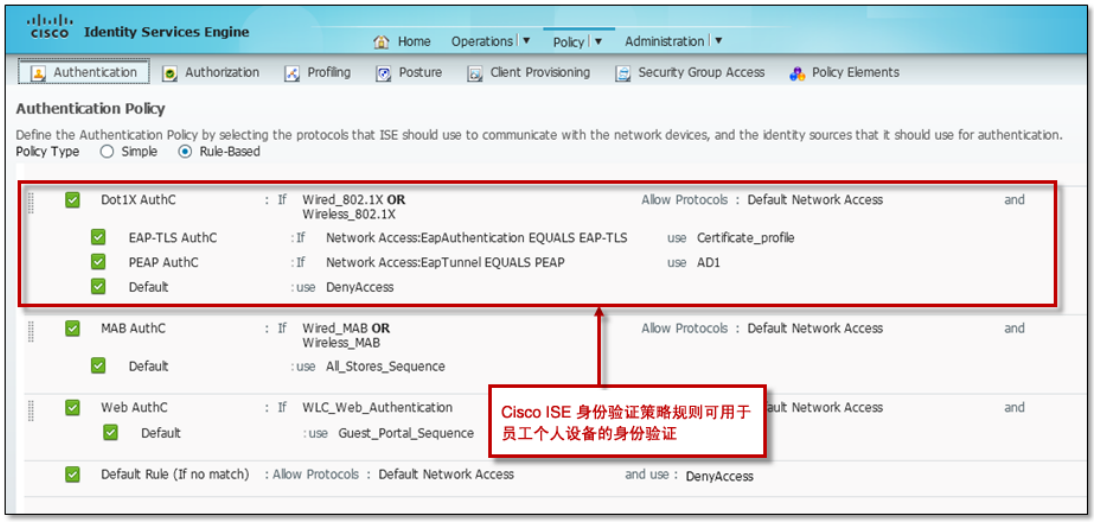


注意　由于 Flex 7500 无线控制器不支持新移动架构，对于将 Flex 7500 作为分支机构无线控制器的部署，可跳过此步骤。

Cisco ISE 策略配置

在受限访问使用案例中，现有身份验证规则用于为公司拥有的 （IT 管理的）设备的自注册提供支持，并对已自注册的公司拥有的设备进行身份验证。从 Cisco ISE 策略的角度来看，现有身份验证规则也适合在基本访问使用案例中用于为员工个人无线设备提供支持。该策略规则的示例如图 12-14 所示。

图 12-14　　允许员工个人无线设备接入的 Cisco ISE 身份验证策略示例



在此示例中，身份验证策略规则的逻辑格式如下：

```
IF (Wired_802.1X OR Wireless_802.1X)
    THEN (Allow Default Network Access AND
        IF Network Access:EapAuthentication EQUALS EAP-TLS USE Certificate_Profile
        IF Network Access:EapTunnel EQUALS PEAP USE AD1
        ELSE Default EQUALS DenyAccess)
```

Wired_802.1X 是一个系统生成的复合条件，在此处用于匹配交换机发出的基于 802.1X 的身份验证请求。它与以下两个标准 RADIUS 字典属性值 (AV) 对相匹配：

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Ethernet
```

Wireless_802.1X 是一个系统生成的复合条件，在此处用于匹配思科无线控制器发出的基于 802.1X 的身份验证请求。它与以下两个标准 RADIUS 字典属性值 (AV) 对相匹配：

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
```

Default Network Access 是一个系统生成的身份验证结果，允许将多种 EAP 协议用于身份验证。

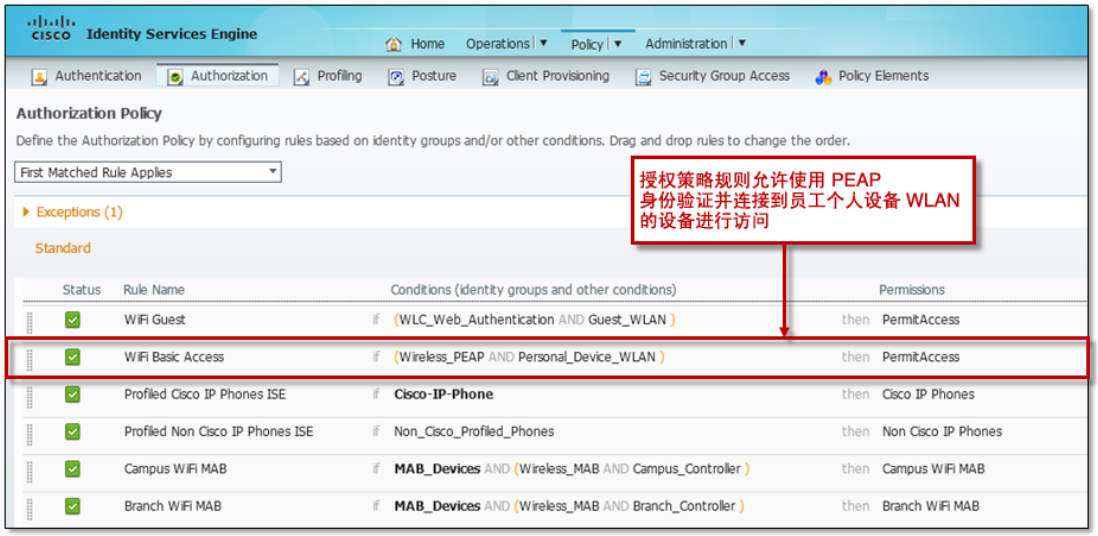
Certificate_Profile 是用户定义的证书身份验证配置文件，在 Cisco ISE 服务器的 “外部身份源” 部分配置。

AD1 对应 Microsoft Active Directory 身份库，通常用于在组织内部保存员工凭证。

对于基本访问使用案例，使用 PEAP 进行身份验证的员工个人无线设备会与第二个条件 - **IF Network Access:EapTunnel EQUALS PEAP USE AD1** - 匹配，这会导致这些设备进入授权阶段。请注意，上述示例适用于仅使用 PEAP 身份验证的员工个人设备。如果客户需要其他身份验证或 EAP 方法，则需要将其他条件添加到上述身份验证策略规则中。这些条件也可以使用 AD1 Microsoft Active Directory 身份库来验证员工用户凭证。或者，可以将默认条件从拒绝访问更改为同样使用 AD1 身份库。

从 Cisco ISE 策略的角度来看，需要添加一个额外的授权规则，以支持基本访问使用案例。此规则允许由员工个人设备 WLAN 对应的 SSID 向使用 PEAP 身份验证的设备发起的访问。该策略规则的示例如图 12-15 所示。

图 12-15　　允许员工个人无线设备访问的 Cisco ISE 授权策略示例



在此示例中，授权策略规则的逻辑格式如下：

```
IF (Wireless_PEAP AND Personal_Device_WLAN)
    THEN PermitAccess
```

Wireless_PEAP 是用户定义的复合授权条件，在此处用于匹配无线 PEAP 设备发出的身份验证请求。它与以下两个标准 RADIUS 字典属性值 (AV) 对相匹配，并附带一个指定使用 PEAP 的网络访问条件。

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
Network Access:EapTunnel EQUALS PEAP
```

Personal_Device_WLAN 是用户定义的简单授权条件，用于通过与员工个人设备 SSID 对应的 WLAN 接入网络的员工个人设备。它与 Airespace 字典中的以下 RADIUS AV 对相匹配：

```
Airespace-Wlan-Id - [1] EQUALS 4
```

Airespace-Wlan-Id 是与员工个人设备 SSID 对应的 WLAN 的标识号 (WLAN ID)。如图 12-16 所示。

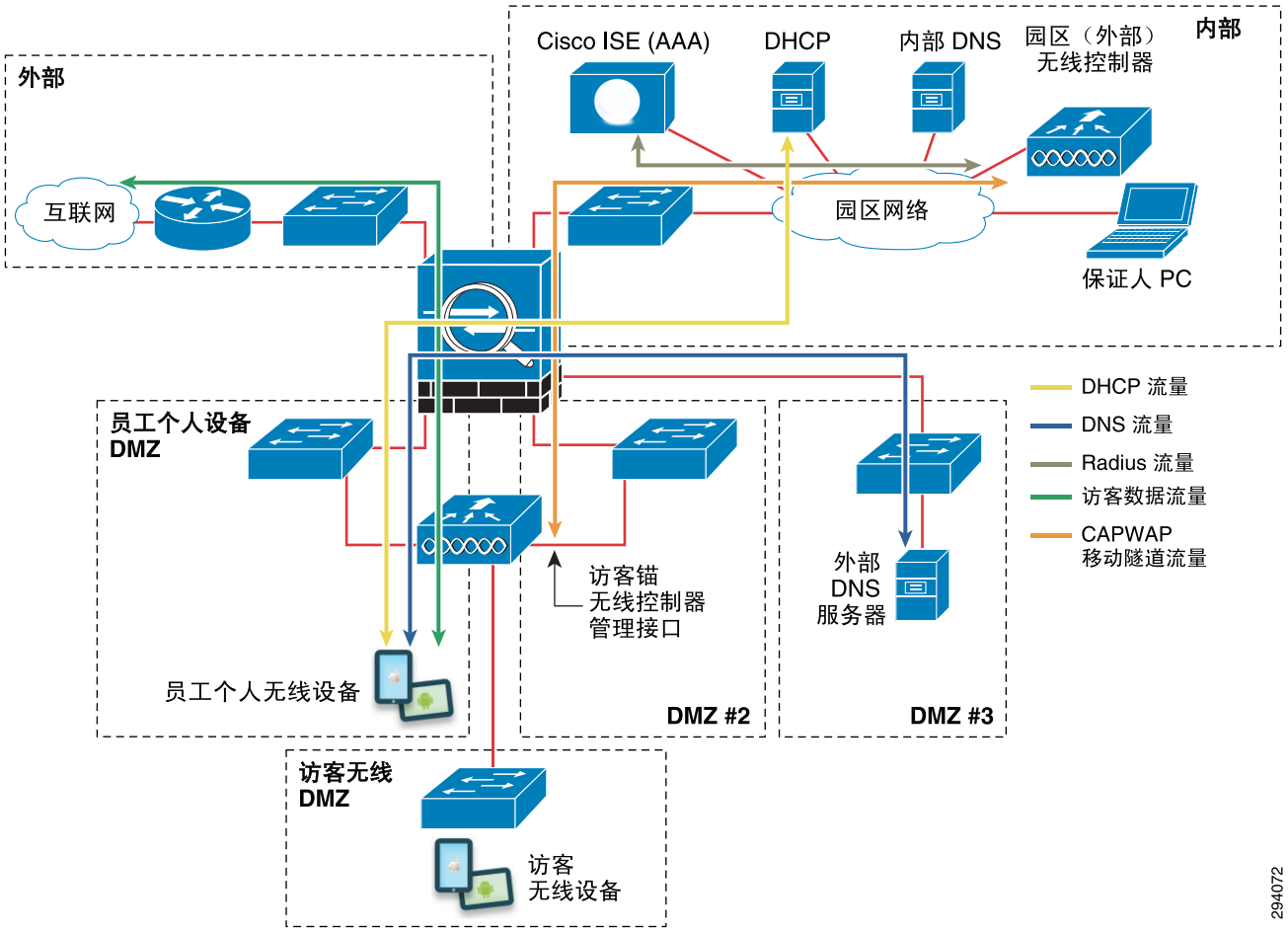
图 12-16　　显示员工个人设备 WLAN 和 SSID 的无线控制器 WLAN ID 示例

请注意，此 WLAN ID 在整个 BYOD 部署中必须保持一致。此规则允许 ISE 授权策略区分来自员工个人设备 SSID 的 802.1X 身份验证请求且仅允许访问。对于已有的 WLAN， WLAN ID 不可更改。要更改 WLAN ID，必须删除并重新创建 WLAN。

ASA 防火墙配置

图 12-17 显示需要通过 Cisco ASA 防火墙以支持此选项的流量的示例。

图 12-17　需要通过员工个人设备 Cisco ASA 防火墙的流量示例



园区（外部）无线控制器管理接口会向 Cisco ISE 服务器发起 RADIUS 会话，以进行身份验证和授权。因此，对于使用个人设备进行身份验证的员工，无需允许 RADIUS 会话通过 ASA 防火墙。如果使用较新的分层移动架构（如图 12-17 所示），则必须允许两个无线控制器的管理接口之间的 CAPWAP 自动锚定移动隧道（UDP 端口 5246 和 5247）通过 ASA 防火墙。如果使用较旧的移动隧道架构，则必须允许两个无线控制器的管理接口之间的 IP 以太网（IP 端口 97）自动锚定移动隧道，以及 WLAN 控制端口（UDP 端口 1666）通过 ASA 防火墙。

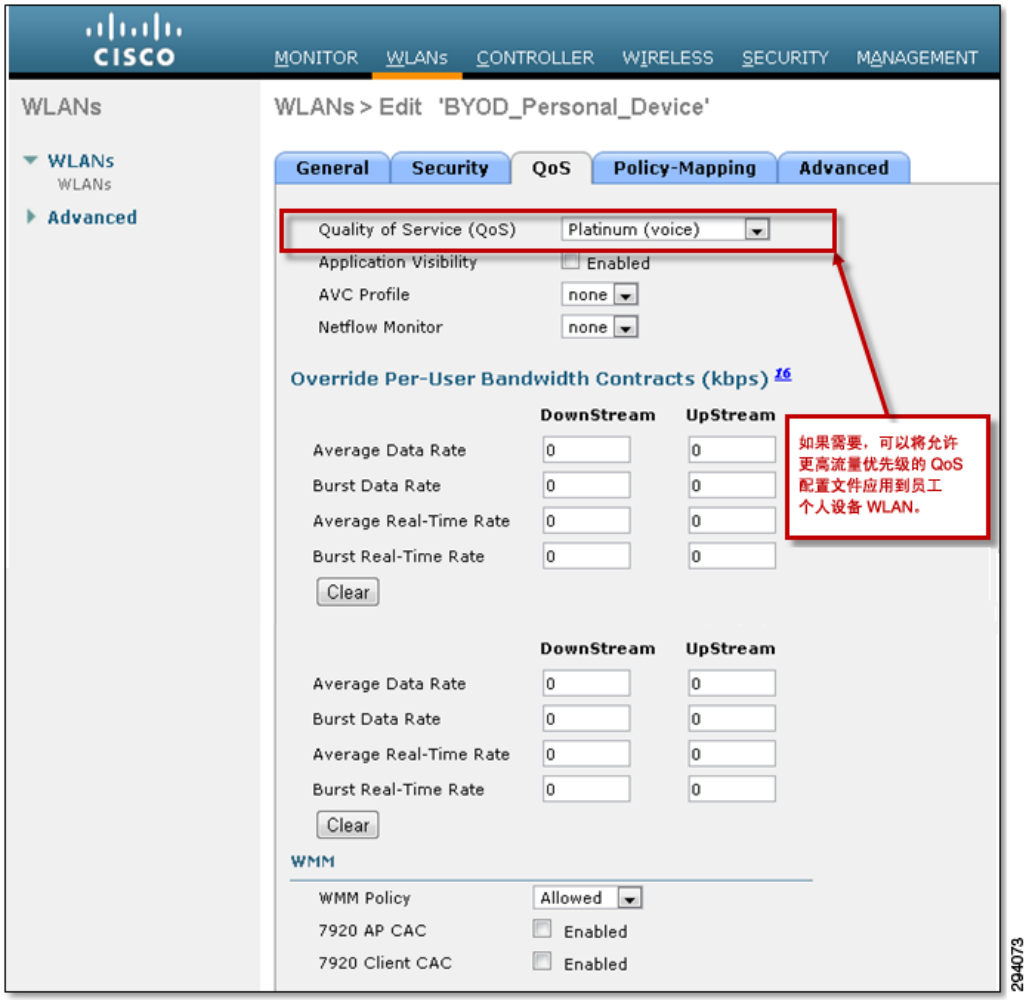
除了允许 DNS 和 DHCP（假设要部署内部 DHCP 服务器），还应该将 ASA 防火墙配置为阻止员工个人设备生成的所有其他流量进入内部网络。为了满足对公司资源的访问，可以打开更多端口，请参阅下节的具体论述，或参见表 13-2 中的汇总。

注意　为了满足访客无线接入需求，可能需要打开更多 ASA 防火墙端口，具体取决于第 13 章，“BYOD 访客无线接入”中讨论的部署模式。

差异化的服务质量处理

通过这种部署模式，可以对员工个人设备应用不同于访客无线设备的独立 QoS 策略。这是因为，员工个人无线设备会在无线访客设备的单独 WLAN 上终止。对于 CUWN 无线控制器，就软件版本 7.2 而言，QoS 通过配置文件方式应用到每个 WLAN，如图 12-18 所示。

图 12-18　　应用于 WLAN 的 QoS 配置文件示例



注意　基于 IOS XE 的无线控制器支持更广泛的 QoS 功能。但是，它们也能根据 CUWN 无线控制器的旧版配置文件模式，支持类似的每 WLAN QoS 功能。本版设计指南不讨论基于 IOS XE 的无线控制器上的 QoS。未来版本将深入讨论此主题。

如果要允许员工个人设备运行虚拟桌面客户端应用 （如 Citrix 客户端或 VMware 客户端），或者如果员工个人设备运行协作客户端 （如 Cisco Jabber），则可能需要采用这种配置。

注意　第 13 章，“BYOD 访客无线接入”讨论了每 SSID 和每用户速率限制。这些功能可以像用于访客设备那样用于员工个人设备。速率限制在园区 （外部）控制器上配置，而不是在访客 （锚）控制器上配置。

访问公司资源

由于员工设备是通过实际上位于公司防火墙之外的 DMZ 接口与网络相关联，因此它们无权访问位于防火墙内部的公司资源。这不仅完全可以接受，而且非常理想。员工设备仍可以接入公共互联网。这样，它们能够连接到基于云的资源，如 Cisco WebEx 或合作伙伴网站。这就为员工设备提供了某种级别的可用性，使其能够用作一种生产力工具。

公司可能希望在为员工设备提供其他资源的访问权限的同时，仍将这些设备限制在防火墙的访客侧，以维护安全性。有多种选项可以实现此目标，包括：

- 设置公司网站的镜像
- 允许 VPN 访问
- 允许虚拟桌面客户端访问

保护个人设备镜像站点的安全

为接入访客网络的员工个人设备提供服务的一种方式是，在另一个 DMZ 网段中设置公司网站的镜像，在本节中我们称之为员工设备安全区域 (EDSZ)。如果员工个人设备连接到访客无线网络，则只有在用户完成网络身份验证过程并接受可接受使用政策 (AUP) 或最终用户协议 (EUA) 之后，才能够访问网站。此网站不需要与内部网站精确匹配，但可以包含员工可在其个人设备上使用的相关内容，实现增效。此外，该网站可包含针对较小移动显示屏而优化的内容。举例来说，EDSZ 中可以提供的应用包括电邮入口、团队 wiki 页面或公司新闻站点。

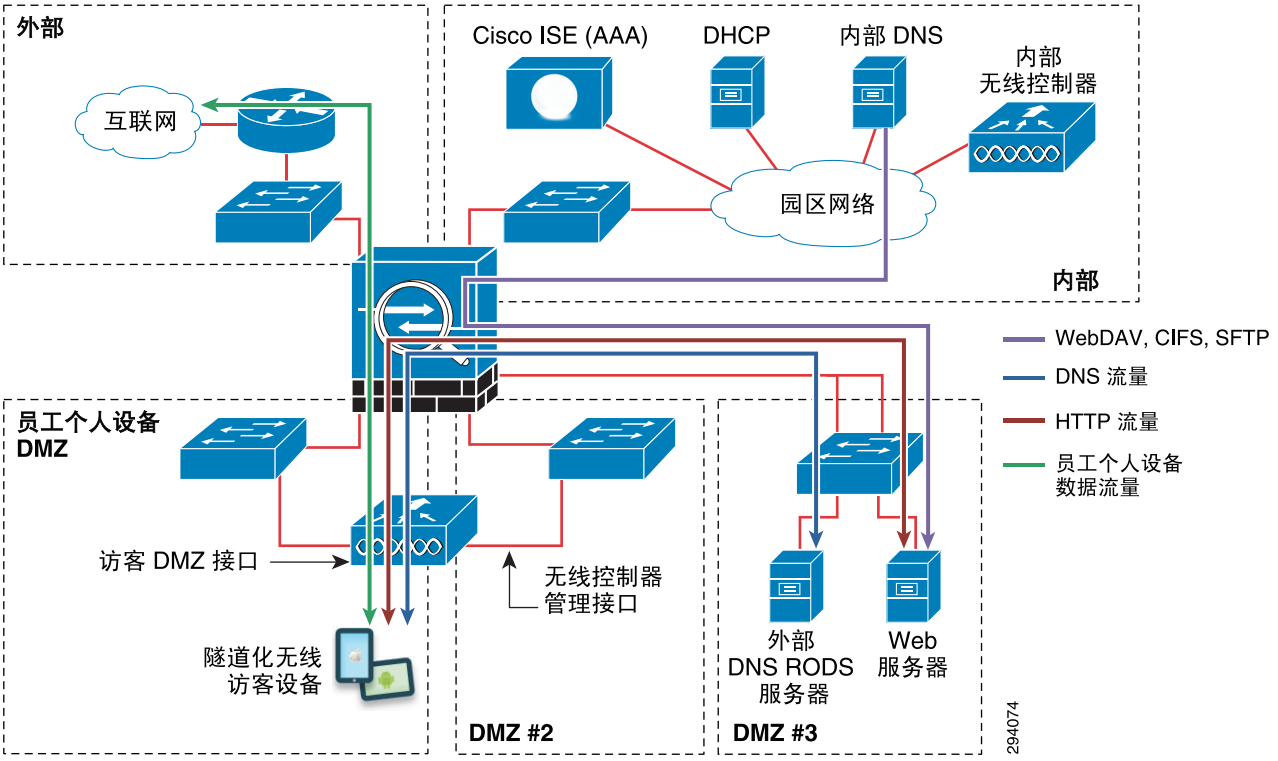
可使用以下几种方法设置安全网站。整体而言，此部署与典型 DMZ 网络服务非常相似，不同之处在于，服务器位于员工个人设备可以访问的子网中，而不是面向互联网的 DMZ 中。本节的目的不是为部署演示服务器、应用服务器和数据库服务器提供详细指导。站点管理员应该熟悉最适合其安全环境的方法。设置服务器时需要更进一步考虑的内容包括：

- 双附件 - 通常认为更安全。客户端 NIC 应实施防火墙服务，允许 TCP 80 端口或 443 端口上的入站连接。应仅允许客户端子网发起的会话请求到达服务器。不应允许服务器发起的会话请求到达客户端子网。如果员工设备无线网络已加密，某些组织可能愿意允许用户通过 HTTP 进行连接。
- 应使用后端 NIC 在服务器和数据存储或应用服务器之间移动内容。也可以允许对站点进行远程管理。虽然在通常情况下，会为独立于服务器到网络客户端网关的服务器到服务器通信设置专用且受保护的网关，但是单连接服务器也是可接受的。
- 内容交付 - 内容通常为静态或动态形式。静态内容可在夜间推送，也可以按需推送，以使网站保持最新。动态内容可以允许员工设备在站点发布信息。网站可以使用与外部数据存储同步的本地数据存储，或者具有指向应用服务器的安全通道。
- 用户身份验证 - 可使用一些方法来确保只有经过授权和身份验证的用户可以查看站点内容。使用 Microsoft Active Directory 或本地用户数据库是两种可行的方法。此外，也可以利用动态服务器网页 (ASP.NET) 来使用与 Microsoft Internet Information Server (IIS) 结合使用的登录控件，并提供单点登录 (SSO) 等更复杂的身份验证模式。本地数据库仅更易于设置，但需要较高的管理开销，通常仅适用于非常小的组织。
- 安全套接字 - 如果员工要发送敏感信息（例如其登录凭证），员工设备安全区域 (EDSZ) 内的网站应实施安全套接字层 (SSL) 或传输层安全 (TLS)。如果已通过无线加密实施 EDSZ，则可以在一定程度上缓解此要求。另一方面，如果员工设备驻留在传统访客网络中 （在这种网络中，无线数据包通常不受加密保护而且会与真实访客流量相混杂），则需要 SSL/TLS 网站。在员工将其公司凭证传递到镜像网站时，这一点尤为重要。
- Web 服务器软件 - 现有的 Web 服务器软件种类繁多。有关部署何种服务器的决定将影响到可用的安全功能。常见选择包括 Microsoft IIS、 Apple 和 Tomcat。维基百科提供了 Web 服务器软件的比较，对各种可用选项进行了说明

(http://en.wikipedia.org/wiki/Comparison_of_web_server_software)。此外，可以将站点托管于安全的云服务。此服务可能会受到 IP 地址限制或要求使用客户端证书。通过采取适当的安全防范措施，基于云的站点也能使移动员工访问某些日益踏上云之路的传统企业资源，例如薪资或福利。

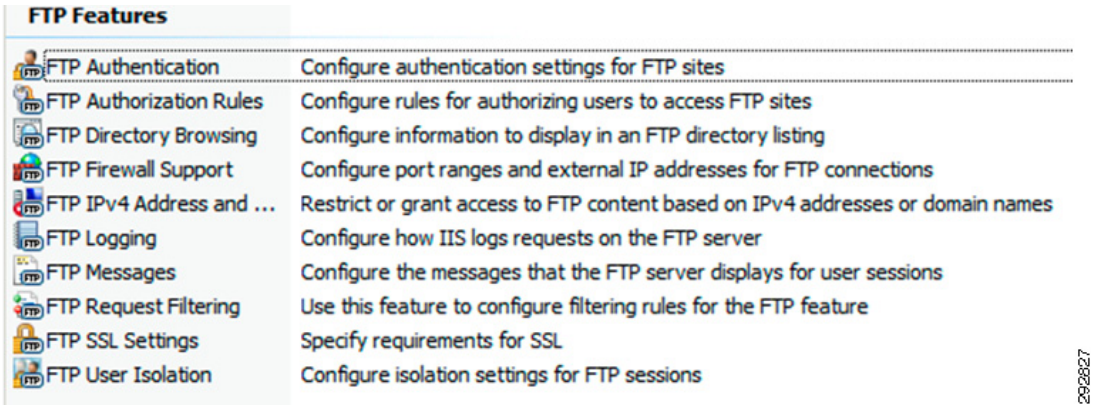
图 12-19 展示了一个简单场景，此场景将静态内容部署在一个专门面向使用个人设备的员工的 DMZ 中。使用 Microsoft IIS 7.0 以及特定于 DMZ 的其他网络服务（如 DNS 和只读目录服务 (RODS)）部署了 Windows 2008 服务器。用户由企业 Microsoft Active Directory 服务器进行身份验证。RODS 服务需要在同一服务器上安装 DNS。Web 服务器通常是一种专用设备。但在某些情况下，可能需要在同一服务器上运行 RODS 和 IIS，以便使用 Microsoft AD 简化基本身份验证。这比较适合需要支持少量至中等数量员工设备的环境。

图 12-19　　用于员工个人设备的镜像网站示例



将内容移动到安全服务器的方法有很多。一种方法是使用 FTP，但是，由于 FTP 并不安全，更好的方法是使用 SFTP 或基于 SSL 的 FTP (FTPS)。默认情况下，Microsoft IIS 未随附安全的 FTP 服务器。 Microsoft 支持 FTPS （而非 SFTP）。管理员必须从 Microsoft 网站（http://learn.iis.net/page.aspx/310/what-is-new-for-microsoft-and-ftp-in-iis-7/）复制安装包并将功能安装到其服务器。如果 FTP 已经在运行，则在安装 FTPS 服务器之前，管理员需要从服务管理器取消选择 FTP 功能。改进的 FTPS 服务器提供了标准 FTP 软件包不具备的其他工具，可用于管理对 FTP 站点的访问，如图 12-20 所示。

图 12-20　　FTPS 服务器中可用工具的示例



应禁用匿名身份验证，并且至少应启用基本身份验证。对于某些组织，可能有其他适合的选项。

管理员可以选择使用 Web 分布式创作和版本管理 （WebDAV）来代替 FTPS。由于许多操作系统都支持将连接安装到文件系统，因此此方法比 FTP 更为灵活。通过提供目录处理，Web 创作应用以及其他应用可以直接使用安全管道。WebDAV 基于 HTTP 或 HTTPS，并提供身份验证和加密数据的功能。如果员工直接位于访客 SSID 中，在发出密码后，应使用 WebDAV HTTPS。如果员工设备位于加密的 EDSZ 中，则应使用 WebDAV HTTPS 提供额外的加密层。RFC4918 的第 20 条详细说明了安全注意事项。

另一个类似于 WebDAV 的选项是 CIFS。此协议还允许在本地目录安装远程站点。这在 Microsoft 环境中很常见，而非 Windows 服务器可使用 Samba。Microsoft 的 Vista、Windows 7 和 Windows 8 下也支持 SMB2，它是 CIFS 的一个更新。还有其他多种方法可以提供与 Web 创作站点或应用服务器之间的安全路径。特定企业可能会利用与位于传统 DMZ 中的 Web 服务器相同的方法。

DNS 支持

员工设备需要访问 DNS 服务器。如果 EDSZ Web 服务器使用的是 RODS，那么 DNS 在目录服务器上就会已经处于可用状态。安装 RODS 会默认安装 DNS，除非管理员明确选择不安装。动态更新会受到保护，同时区域传输未被启用。如果 Web 服务器未使用 AD 进行员工身份验证，那么 DNS 将为一项独立的服务。

面向员工设备的 Outlook Web Access

电邮是一项可以提供给员工设备的基础服务。此过程可以通过将 Web 接口部署到邮件服务器（如适用于 Exchange 环境的 Outlook Web Access (OWA) 或 ActiveSync）来完成。有些企业可能已为需要在差旅中使用电邮的员工提供此项服务。在这种情况下，员工设备可以继续使用当前面向互联网的 OWA 服务器。

Microsoft 不支持 DMZ 区域中的 OWA 服务器。相反，OWA 服务器应该受防火墙保护。可以对端口 443 打开缺口。另一种方法是在 EDSZ 中安装 Apache 作为反向代理。 Microsoft 建议的方法是在客户端访问服务器 (CAS) 上运行 OWA，并通过 Microsoft 的互联网安全和加速 (ISA) 服务器将 CAS 发布到 EDSZ。这是一个完全成熟的部署，由于与其他方法相比，它具有一定的复杂性 （例如仅仅在 EDSZ DMZ 防火墙上打开指向企业 CAS HTTPS 的缺口），因此该方法可能不适用于为员工个人设备授予访问权限。

另一种选择是订用 Office365，这是 Microsoft 基于云的 Exchange 和 Office 环境。在这种情况下，员工可以使用公共互联网服务获取对其电邮或其他基于云的企业资源的访问权限。目前，还没有适合 Android 或 iOS 设备的本地 Office365 应用，除非用户使用基于 Windows 8 的移动设备，否则会被限制为 HTTPS 访问。此方法也允许通过 3G/4G 直接到云方式或外部方式访问相同资源。Microsoft 仅仅是多种基于云的企业电邮服务提供环境之一。

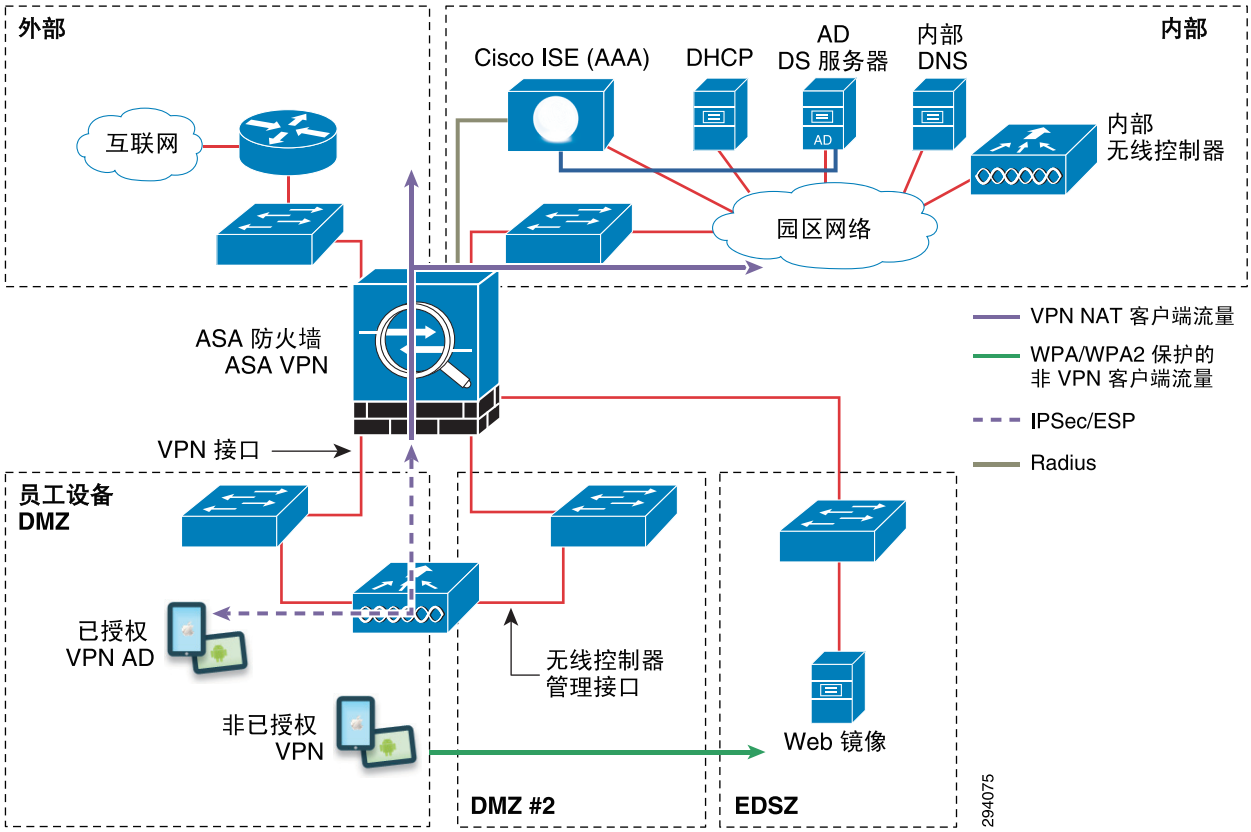
ActiveSync 支持

本文档的未来版本将讨论用于管理移动设备配置文件并为丢失或被盗的设备提供额外安全功能的移动设备管理器 (MDM)。某些 MDM 功能已从 Microsoft 获得许可，包括远程擦除、 PIN 锁定实施等。 ActiveSync 用于在 Microsoft Exchange 服务器和移动设备的电邮应用之间同步电邮、日历活动以及联系人。管理员可能会考虑为员工设备安全区域 (EDSZ) 中的设备提供 ActiveSync。如果配置正确且经过认证， ActiveSync 也可以提供前面提到的 MDM 安全功能。提供此支持的方法与 OWA 类似。可以将 EDSZ 中的防火墙策略设置为允许连接到可能会在 ISA 服务器上发布的 CAS 上的 ActiveSync。 ActiveSync 受 WebDAV 支持，并应在 HTTPS （TCP 端口 443）上使用。

VPN 客户端

将员工设备限制到访客或专用 EDSZ 的企业可能希望允许部分用户启动内置 VPN 客户端，以连接到网络的安全部分。可以采用两种方法。首先，设备可能已有权访问当前面向互联网的 VPN 集中器。在这种情况下，员工设备将通过公共互联网从访客网络连接，然后返回到 VPN 集中器所在的互联网 DMZ。如果员工设备流量与实际访客流量相混，则这可能是最佳方法。但是，如果将专用的安全 SSID 部署为受专用于员工个人设备的 ASA 防火墙保护，则该防火墙也可以为一些特权用户提供 VPN 访问权限。或者，专用 VPN 集中器可位于 EDSZ 中。在设备经过验证并加入安全无线域之后，这些用户将连接到 VPN 集中器，以获取其他安全访问权限。仅专用安全区域内的员工设备可以访问集中器。网络组件的一般布局如图 12-21 所示。

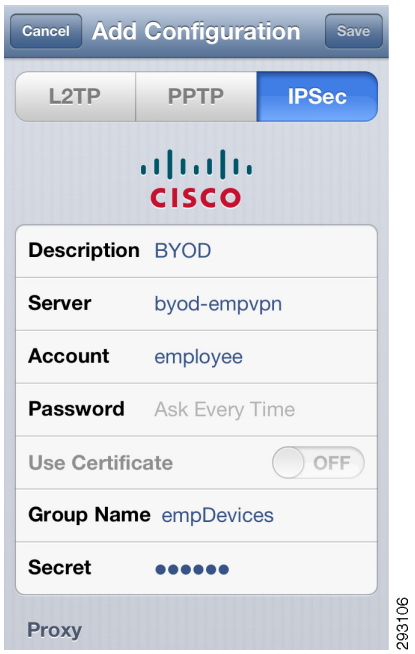
图 12-21　　员工区域 VPN 网络组件



Apple iOS 设备包括允许 ESP 隧道模式和 XAUTH 的内置 Cisco IPSec 客户端。 Apple 和 Android 设备都提供带有 IPsec 和预共享密钥 (PSK) 的 L2TP。可以将 ASA 设置为同时接受两种类型的 VPN 客户端。本讨论将侧重于在 Apple iOS 设备上发现的 Cisco VPN 客户端。

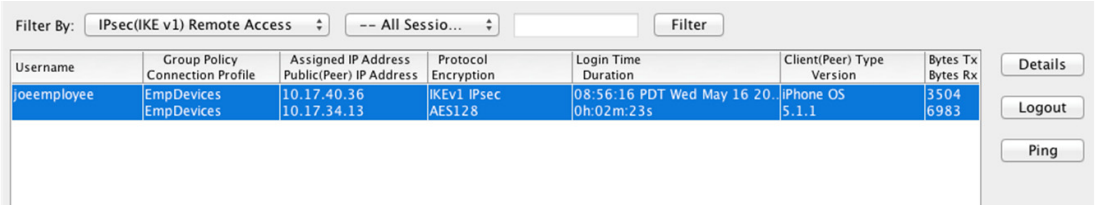
员工需要知道 VPN 集中器的名称、组和组密码，以配置 VPN 客户端。本文档的未来版本将说明如何在无用户干预的情况下将 VPN 配置推送到员工设备。也可以将证书推送到员工设备，以进一步保证对 VPN 集中器的安全访问。使用证书后，就无需再使用组和组密码。

图 12-22　　iOS VPN 客户端配置



用户连接到 VPN 集中器时，需要提供其 Microsoft AD 凭证。此信息通过 Cisco ASA 传递到 Cisco ISE 服务器，在那里可以进行策略决策。此决策可包括来自 Microsoft Active Directory 的属性，或者 Cisco ISE 可用于确定策略的任何其他参数。如果用户通过 Cisco ISE 进行了身份验证和授权，则 ASA 将完成 VPN 连接。一旦建立了连接， ASA 就可以对隧道应用更多安全性和访问限制，从而进一步控制员工设备可以访问的资源。 ASA 还可用于监控谁正在使用 VPN 门户，如图 12-23 所示。

图 12-23　　VPN 连接的 ASA 管理



ASA 提供了用于管理 VPN 连接的其他信息。

虚拟桌面客户端

另一个可用的部署模式是允许在员工设备上运行虚拟桌面。实际应用和关联数据仍在受保护的托管服务器上。一旦设备从网络断开，用户通常就无法再获得数据。企业可以控制哪些用户可以启动虚拟桌面，以及哪些应用可在该桌面使用。可以将 EDSZ 和托管服务器之间的防火墙配置为允许特定连接。

可以使用的方法多种多样。最简单的是，员工可使用 VNC 连接回他们的桌面或专用服务器。VNC 客户端可用于 iOS 和 Android 设备。对于一些不将可用性和可管理性视为要务的小型环境，这已经足够了。默认情况下，连接不会加密，这是一个问题。对于托管服务器上可用的应用，管理员可能缺乏必要的控制力。员工可能会冒风险连接到其桌面，并通过电邮或云文件共享服务

（如 Dropbox 和 Google Drive）将敏感数据发送到外部帐户。这仅为绕过 IT 策略的一种方法，应在允许远程桌面连接到员工部署的 VNC 服务器之前加以考虑。针对具有虚拟 VNC 桌面的员工设备的使用案例需要仔细审核。员工可能会坐在具有全键盘和鼠标的真实桌面设备之前，而不需要使用远程桌面。最佳的方法可能是阻止 TCP 端口 5900 穿过防火墙到达未知目的地。

思科提供了思科虚拟工作空间 (VXI) 智能解决方案，并与多家提供移动 iOS 和 Android 设备虚拟桌面的公司建立了合作，包括 VMware View、 Citrix 和 WYSE。员工设备上的虚拟桌面最适合由集中式 UCS 服务器保护并管理会话的 VXI 环境。通过为公司设备提供 VXI，扩展对员工设备的访问权限可能会提高工作效率。其实现方法是打开防火墙，允许连接到特定且已知的服务器。与 BYOD 相比，虚拟桌面因更低的 IT 成本而更具吸引力。由于对员工手提电脑的要求更低，添加平板电脑支持可使收益最大化。体积小、重量轻的 VDI 硬件设备取代了传统桌面，移动设备支持则将员工从条条框框中解脱了出来。使用虚拟桌面的平板电脑可以提供很多与员工手提电脑相同的功能，但其成本更低，能提供更强大的工具来应对丢失或被盗设备的问题，还能提供 VXI 固有的集中式数据安全。

最后， AnyConnect 可提供集成了 ASA 防火墙的集中式虚拟桌面。这是一个好的方法，因为安全性是系统的基础。 AnyConnect 桌面通过 SSL 连接到 ASA 防火墙。虚拟桌面的功能正在不断发展，本文档的下一版本将会进行更详细的介绍。

总结

这些类型的替代解决方案包括各种选项，可在不影响企业数据的情况下为员工提供计算资源。利用访客环境可以作为迁移路径的一部分，实现完全基于证书的 BYOD 解决方案。访客类型部署可以非常快速地设置，无需使用大量第三方设备，同时仍可满足允许员工使用个人设备以提高组织工作效率的基本需求。

第 4 部分

BYOD 操作和服务

BYOD 访客无线接入

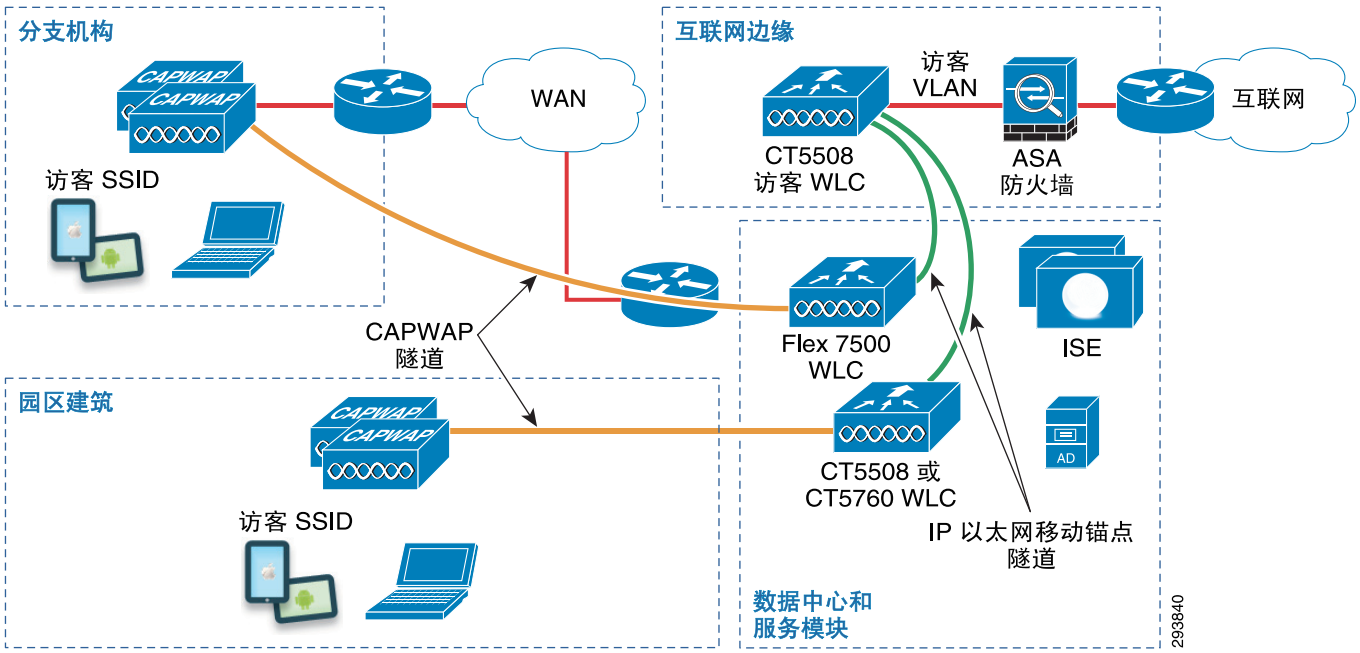
修订日期：2013 年 8 月 7 日

本章讨论无线访客设备的传统网络接入，并展现了在 BYOD 实施中部署访客无线设备的多种方式。还为第 12 章，“BYOD 基本访问使用案例”提供了背景信息，该章节讨论了如何扩展访客无线接入，使其支持员工个人无线设备。请注意，在本设计指南中，访客接入是指为由受访组织的代表授予保证的访客提供的临时互联网访问。

概述

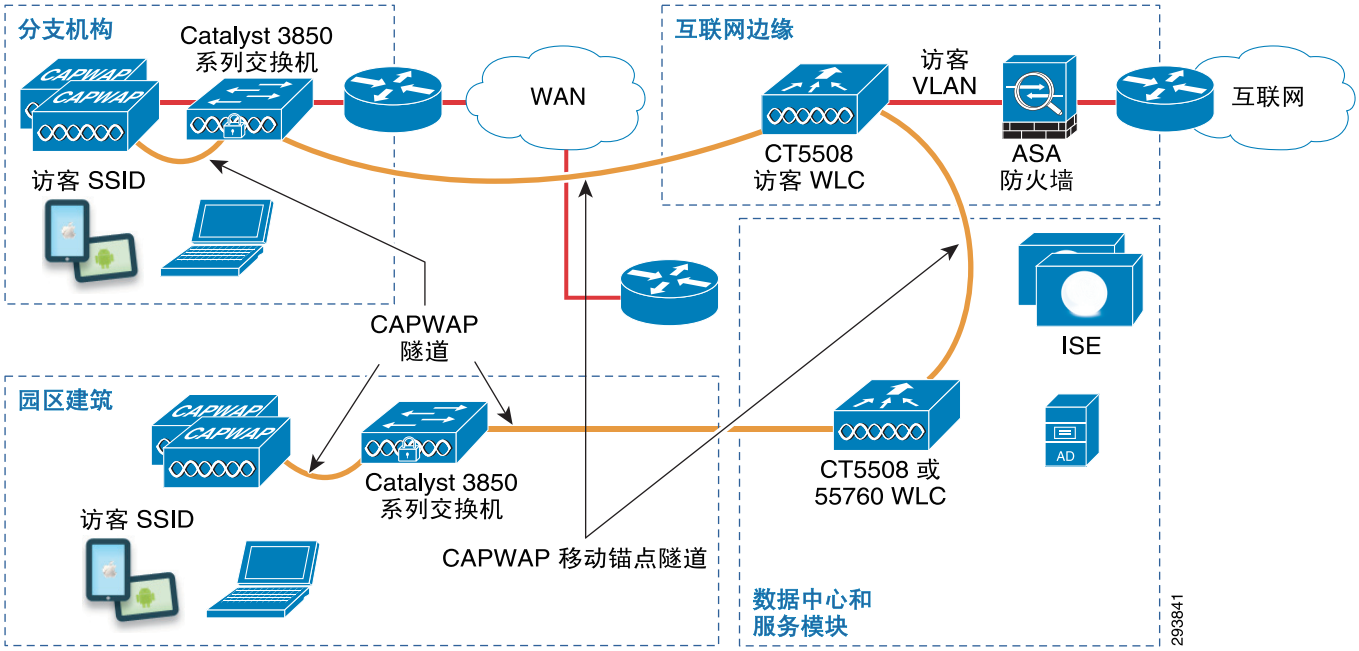
对于访客无线接入，思科建议您在互联网边缘模块中部署独立于 Cisco ASA 防火墙的 DMZ 网段的单独专用无线控制器。本设计示例使用思科统一无线网络 (CUWN) 基础设施，如图 13-1 所示。

图 13-1　使用 CUWN 基础设施的典型企业访客无线部署



本设计的一个类似示例使用融合接入基础设施，如图 13-2 所示。

图 13-2　使用融合接入基础设施的典型企业访客无线部署



可以部署多种访客接入选项。但是，本设计指南只讨论基于为不加密开放式接入配置的专用访客 SSID 的访客无线设计。这样做的原因通常在于，组织的 IT 部门通常不了解或不能控制访客无线设备的硬件或软件功能。因此，开放式接入是适用于所有无线设备的功能。

来自园区或分支机构位置的访客无线流量被配置为从内部无线控制器自动锚定（通过 IP 以太网或 CAPWAP 隧道化传输）到访客无线控制器。这样可以提供级别稍高的安全性，因为访客无线设备不在企业网络的“内部”终止。从客户的角度看，这通常是可取的，因为访客设备的安全状态无法确定。

注意　思科无线控制器目前支持两种不同的移动架构。旧移动架构依赖于无线控制器之间的 IP 以太网隧道。新移动架构也称为分层移动架构，它依赖于无线控制器之间的 CAPWAP 隧道。两种移动架构互不兼容。如果无线控制器之间需要移动功能（包括自动锚定功能），则所有无线控制器必须运行新移动架构或旧移动架构。 Cisco 5508 和 WiSM2 无线控制器软件版本 7.3.112 以及 Cisco 5508、WiSM2 和 2504 无线控制器软件版本 7.5 支持新移动架构。IOS XE 软件版本为 3.2.0SE 和 3.2.2SE 的 Cisco 5760 无线控制器和 Catalyst 3850 系列交换机也都支持新移动架构。 7.4 版以及 7.3.112 以下版本的 CUWN 无线控制器仅支持旧移动架构。Cisco Flex 7500、8500 和 vWLC 不支持新移动架构。基于 IOS XE 的无线控制器不支持旧移动架构。因此，如果网络同时包含 Flex 7500 无线控制器和融合接入控制器，则必须使用 DMZ 部署一组独立的访客无线控制器，以便同时为本设计指南所探讨的访客无线设计中涉及的两种移动架构提供支持。

本章使用了两组不同的术语。第一对术语是访客控制器和园区控制器。访客控制器是用于处理访客无线流量的专用控制器，而园区控制器专用于处理内部流量。请注意，此处使用的术语“园区控制器”有些笼统。本章中讨论的园区控制器可以指在园区位置内部署的一台或多台独立无线控制器平台，也可以指在分支机构位置中部署的一台或多台 Catalyst 3850 系列交换机中集成的无线控制器功能。

第二组术语是外部控制器和锚控制器。当用户从一个控制器漫游到另一个控制器时，将使用这两个术语。用户关联的新控制器是外部控制器，且此控制器将所有流量锚定到旧控制器，因此旧控制器称为锚控制器。

本设计指南章节主要从在整体 BYOD 部署中如何与网络基础设施以及与 AAA 服务的 Cisco ISE 服务器集成的角度讨论了无线访客接入。有关无线控制器支持访客接入的配置详细信息，请参阅思科企业移动 4.1 设计指南中的思科统一无线访客接入服务一章：http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html。

IP 寻址和 DNS

与其他设备一样，访客无线设备需要 IP 地址和域名解析 (DNS) 服务。本地 DHCP 服务器可以在支持访客无线接入的子网中部署。如果 ASA 防火墙在内部和访客无线 DMZ 接口之间执行 NAT，则此选项非常适合。在将访客 IP 寻址从企业网络的其他部分隔离方面，这可能是最安全的选项，但是它的成本有些高，并且更难以管理维护。实施配置有 DHCP 池的 ASA 防火墙来将 IP 地址直接发送回无线客户端后，此成本可以抵消。此选项的优势是访客 IP 寻址与企业网络的其余部分隔离，以及不必允许来自访客设备的 DHCP 通过 ASA 防火墙这一事实。缺点是需要管理 ASA 防火墙中访客无线设备的一个单独 IP 寻址池。

访客无线设备的 IP 寻址也可以通过企业网络内部的 DHCP 服务器提供。如果没有在内部和访客无线 DMZ 接口之间实施 NAT，则此选项非常适合。本章剩下的部分假定访客无线 DMZ 接口没有 NAT 功能。实施集中式 DHCP 服务器的优势是可对访客设备的 IP 寻址进行集中控制。缺点是 DHCP 必须获允许通过 ASA 防火墙才能传递到内部 DHCP 服务器。

可配置思科无线控制器，将无线客户端代理到内部 DHCP 服务器。这是无线控制器的通用部署模式。有了此配置， ASA 防火墙的 DMZ 接口需要允许来自与访客 WLAN 接口关联的无线控制器 IP 地址的入站 DHCP 数据包通过 ASA 防火墙。或者，可配置 ASA 防火墙，以将 DHCP 中继到内部 DHCP 服务器，而不是由访客无线控制器作为无线设备代理。有了此配置，访客无线客户端通过无线控制器直接发送 DHCP，然后由 ASA 防火墙的 DMZ 接口中继到内部 DHCP 服务器。注意，通过 Cisco ISE 服务器的终端设备 DHCP 分析可以通过将 DHCP 发现中继到内部 DHCP 服务器以及 ISE 分析服务器来完成。但是，可能不需要分析访客设备，因为它们只需要临时访问。

注意　网络管理员应该始终权衡启用 DHCP 服务器或 DHCP 中继功能带来的优势与在 ASA 防火墙上启用这些附加功能导致的增加风险，以确定适合组织的安全策略。

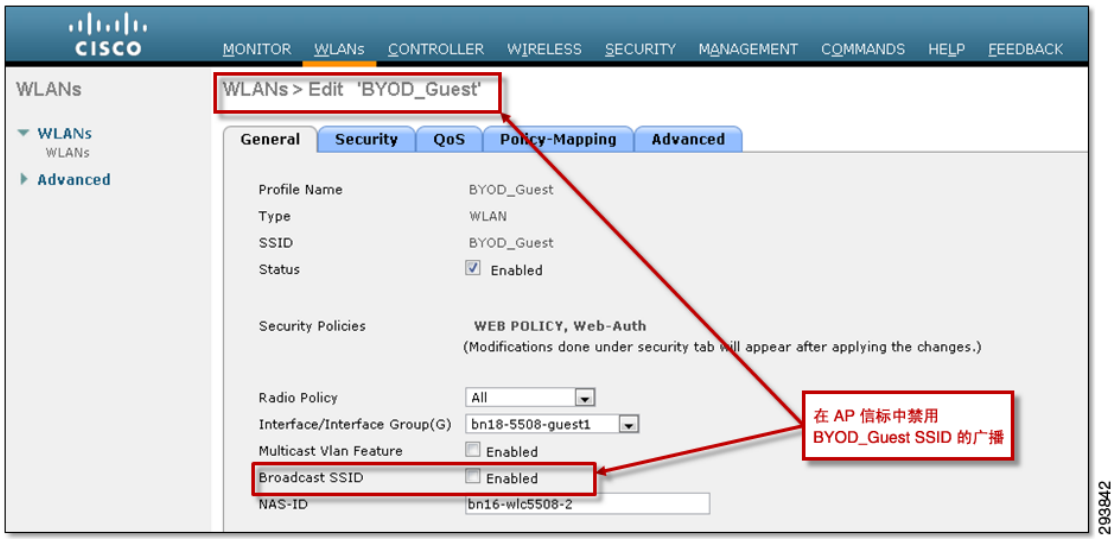
访客无线网络日益面临着 IP 地址耗尽的问题。这可能是将传统访客网络向员工个人设备开放导致的结果。也可能是在人口密集区域设立办公室带来的意外结果，在那些地方，公众连接到与组织访客 WLAN 相应的开放式 SSID，同时认为它在提供 “热点” 无线服务。随着消费者无线设备的持续激增，随着企业不断采用 BYOD 策略，此问题可能会越来越普遍。如果分支机构位置提供访客服务，需要的地址池会变得相当之大。

有多种方法可以帮助缓解 IP 地址耗尽问题。从安全角度来看，最佳解决方案是尝试调整接入点 (AP) 无线电，这样与访客 WLAN 相应的 SSID 以及组织的任何其他无线 SSID 在组织的物理边界之外将不可见。但是，在整个物理空间内维持足量无线覆盖的同时，这一点并不总是可行。

第二种方法是减少 DHCP 服务器上访客 WLAN 对应 IP 子网的租用时间。这不会阻止公众连接到与组织的访客 WLAN 对应的开放式 SSID。但是，当最终用户意识到他们没有访问任何内容所需的网络身份验证 (Web Auth) 凭证时，就可能会重新连接到另一个 SSID。如果 DHCP 租用时间减少，分配给这些设备的 IP 地址将能够更快地再次分配。缺点是 DHCP 有一些额外开销，还有，无线设备需要更快速地续订租期，这样会增加少量额外开销。

第三种方法通过不在 AP 信标中广播与访客 WLAN 对应的 SSID，将其隐藏。思科统一无线网络 (CUWN) 控制器可轻松实现此目标，方法是取消选中与访客 SSID 对应的 WLAN 的 Broadcast SSID 复选框，如图 13-3 所示。

图 13-3　　禁用 AP 信标中访客 WLAN 对应的 SSID 的广播



同样，以下配置示例仅显示禁用了 SSID 广播的融合接入 （基于 IOS XE）无线控制器中访客 SSID 的部分配置。

```
!
wlan BYOD_Guest 2 BYOD_Guest/ 访客 SSID 的配置
 no broadcast-ssid/ 禁用 AP 信标中 SSID 的广播
!
```

在阻止不必要的设备连接到与访客 WLAN 对应的开放式 SSID 方面，这绝不是一种万无一失的方法，因为它仍可以被其他方法发现。但是，该方法确实增大了查找和与其连接的难度，有可能减少不必要的设备数量和 DHCP 服务器颁发的 IP 地址数目。它的缺点是，访客在尝试连接到组织的访客无线网络时，必须手动键入 SSID 的名称。但是， SSID 的名称也可以包括在访问组织站点时或之前提供给访客的凭证内。

另一个选项是为访客无线网络调配一个更大的连续 IP 子网地址空间，只需更改现有访客 IP 地址空间的 IP 子网掩码即可。如果相邻 IP 地址空间可用且未使用，此选项非常适合。如果无法实现，可以在无线控制器上调配第二个访客 DMZ 接口，以增加可分配给访客 WLAN 中设备的 IP 地址空间。

增加可用 IP 地址池是确保访客不会因地址耗尽而阻止访问的最直接方法。值得注意的是，此方法不会阻止相邻无线客户端与错误的网络相关联。需要网络身份验证或其他方法控制对访客资源的访问。这也被视为审计访客用户实际数量和预计数量的一个较好措施。将通过访客门户的访客数量与从 DHCP 服务器租出去的地址数量相比较，是确定有多少无意无线客户端与网络相连接的一个好方法。如果租用地址的数量远远超出预计的访客数量，则可以将租用时间调低。

无线访客设备也需要名称转换服务 (DNS) 来到达互联网中的位置。此外，实施网络身份验证后，访客网络浏览器中的 URL 必须解析为 IP 地址。这是网络身份验证将会话重定向到访客门户以请求访客凭证时所必需的步骤。名称转换服务的提供方式为，允许访客设备到达 ASA 防火墙外另一个 DMZ 网段中部署的外部 DNS 服务器，或到达企业网络内部部署的内部 DNS 服务器。允许访客设备访问外部 DNS 服务器，其优势在于内部站点和服务可对访客设备隐藏。但是，如果无线访客网络扩展为包括员工个人设备（如第 12 章，“BYOD 基本访问使用案例”中所述），网络管理员需要确定外部 DNS 服务器是否仍然可以提供必要的名称转换服务。

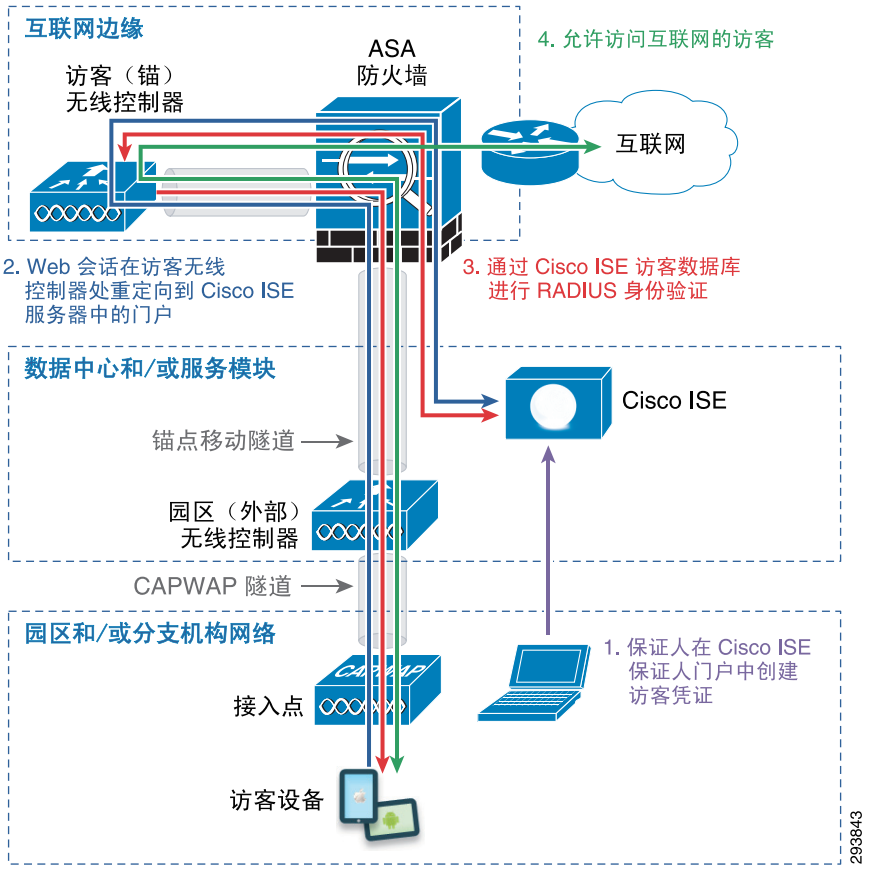
注意　从客户端到服务器的 DHCP 数据包使用 UDP 源端口 68 和目标端口 67。从服务器到客户端的 DHCP 数据包使用 UDP 源端口 67 和目标端口 68。 DNS 使用 UDP 端口 53。实施内部 DNS 和 DHCP 服务器时，必须允许这些端口通过防火墙。

身份验证和授权

大多数组织的 IT 部门选择先验证访客无线用户，然后再允许其接入互联网。访客用户在接入互联网之前阅读并同意可接受使用政策 (AUP) 或最终用户协议 (EUA) 时，通常会涉及这一步骤。由于组织的 IT 部门通常无法控制访客无线设备的硬件或软件功能，因此身份验证和授权决策通常仅基于访客的用户名和密码。换句话说，从 BYOD 的角度来看，在制定策略决策时可能不会考虑访客用于接入网络的设备。实施访客用户身份验证的一个典型方法（如图 13-4 所示）是通过访客用户的网络浏览器，这种方法称为网络身份验证或 Web 认证。要使用此身份验证方式，无线访客首先必须打开网络浏览器，并转到互联网上的某 URL。浏览器会话将重定向到一个 Web 门户，其中包含一个请求登录凭证的登录页面。身份验证成功后，访客用户可以访问互联网或重定向到其他网站。

访客接入情况主要取决于保证人（如门户管理员）访问门户以创建限时有效的临时访客凭证的能力。因此，下面的讨论也会涉及此功能。

图 13-4　　使用网络身份验证的访客无线接入



设计园区和分支机构位置的访客接入

在本文档中，园区和分支机构的网络访客接入设计实施非常相似。通常两者可以使用相同的配置步骤。部署访客接入解决方案包括配置多个组件，例如无线控制器 (WLC)、ASA 防火墙和 Cisco ISE。

WLC 配置

对于本文中显示的设计，访客网络会话的重定向和无线控制器的身份验证点被定向到 Cisco ISE 服务器。执行网络身份验证还有其他方法，但本指南不作讨论。访客客户端的网络会话被访客无线控制器重定向到 Cisco ISE 服务器中包含登录屏幕的门户。

注意　此选项有时称为集中式网络身份验证 (CWA)。

通过在中央位置放置网络身份验证登录页 （以及可选的 AUP 或 EUA），网络管理员可以为所有无线访客接入提供统一的登录页，无需将登录页下载到每个访客无线控制器。

如前面的概述所述，本设计建议部署两个不同的控制器：

- 处理所有内部无线流量的园区控制器。
- 仅处理访客流量的专用访客控制器。

这两个控制器之间会建立一个移动锚点隧道。本节讨论这两种控制器的配置详细信息。

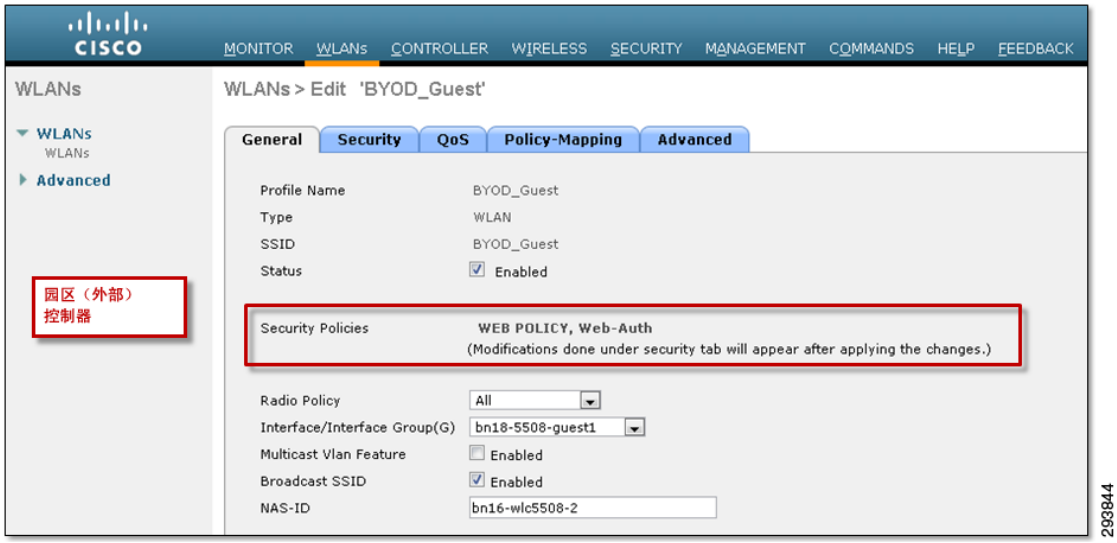
园区控制器

本节讨论使用 CUWN 无线控制器或融合接入 （基于 IOS XE）无线控制器时的园区控制器配置。

CUWN 无线控制器

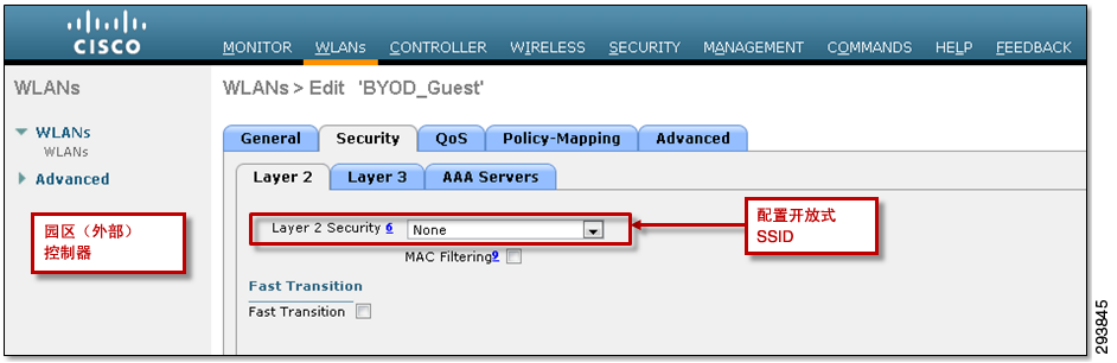
第一步是配置访客 SSID。图 13-5 显示了 BYOD_Guest SSID 的配置。注意，必须为网络身份验证配置身份验证。

图 13-5　园区控制器中的 BYOD_Guest SSID 详细信息



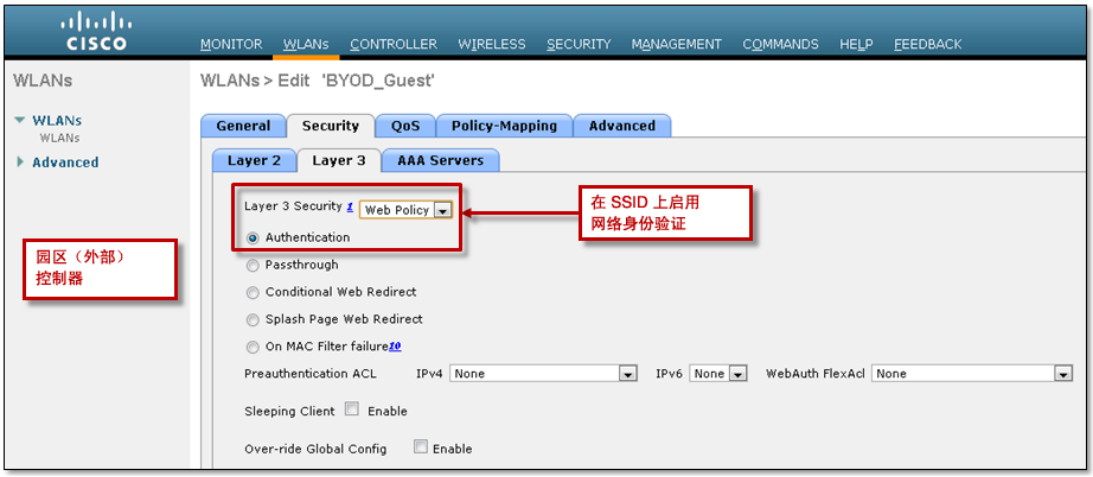
下一步是配置此 SSID 的第 2 层和第 3 层安全参数。图 13-6 显示了第 2 层安全参数。

图 13-6　BYOD_Guest 的第 2 层安全详细信息



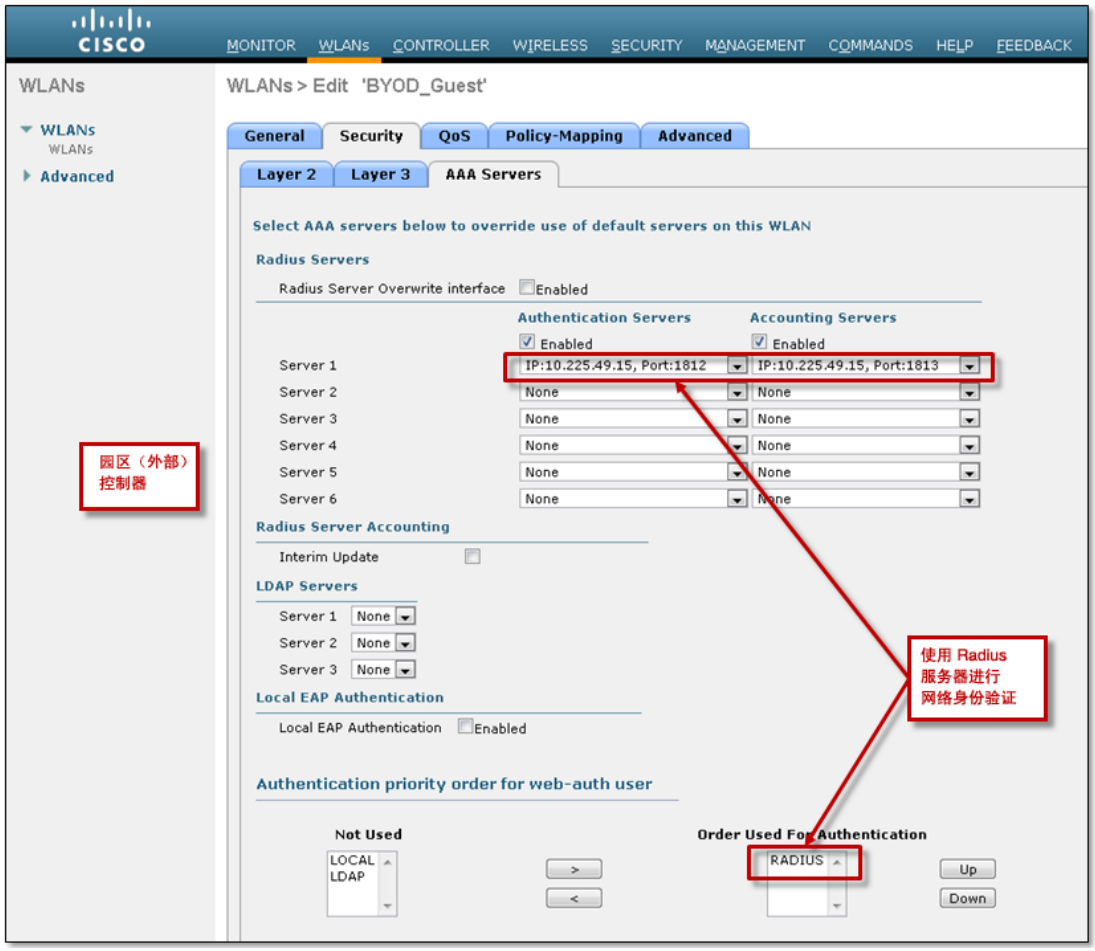
如前所述，第 2 层安全参数设置为 None，表示开放式 SSID。第 3 层安全参数如图 13-7 所示。

图 13-7　园区控制器中 BYOD_Guest WLAN 的第 3 层安全详细信息



第 3 层安全参数启用网络身份验证 (Web Auth)。下一步是配置 AAA 服务器参数，如图 13-8 所示。

图 13-8　园区控制器中 BYOD_Guest WLAN 的 AAA 服务器配置



配置 AAA 服务器参数，以便网络身份验证使用 Cisco ISE 服务器验证使用 Radius 的访客。

下一步是在园区和访客控制器之间配置移动隧道。必须先将访客控制器作为移动组成员添加到园区控制器。图 13-9 显示了此步骤的示例。

图 13-9　将访客控制器添加到移动组

注意　需要访客控制器管理接口的 MAC 地址和 IP 地址，才能将其添加为移动组成员。

最后，在指向访客控制器管理接口 IP 地址的 BYOD_Guest SSID 上创建移动锚点。如图 13-10 中的示例所示。

图 13-10　在园区控制器上配置移动锚点

为了支持新移动架构 （也称为分层移动架构），网络管理员必须选中园区无线控制器全局移动配置中的**启用分层架构**选项。如图 13-11 所示。

图 13-11　　启用园区控制器中的分层移动架构

注意　由于 Flex 7500 无线控制器不支持新移动架构，因此在将 Flex 7500 作为分支机构无线控制器实施时，可以跳过此步骤。

融合接入（基于 IOS XE）无线控制器

以下配置片段显示了融合接入（基于 IOS XE）无线控制器上的访客 WLAN 配置。

```
!
vlan 777          / 锚隧道出现故障时用于访客设备的隔离 VLAN
 name Guest
!
~
!
wlan BYOD_Guest 2 BYOD_Guest/ 园区控制器上的访客 WLAN、WLAN ID 和 SSID
 aaa-override
 client vlan Guest/ 静态分配给不可路由的（隔离的）VLAN
 mobility anchor 10.225.50.35/ 创建到访客无线控制器的 CAPWAP 锚定隧道
 no security wpa/ 第 2 层安全设置为 none（开放式 SSID）
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth/ 针对网络身份验证设置第 3 层安全
 session-timeout 1800
 no shutdown     / 启用访客 WLAN
!
```

注意，上述配置中的访客客户端 VLAN 是在 CT5760 无线控制器或 Catalyst 3850 系列交换机上隔离的 VLAN。它不中继到相邻的第 3 层设备。如果外部控制器和锚控制器之间的 CAPWAP 隧道中断，则会隔离所有访客设备。

必须在充当移动代理 (MA) 的设备和作为移动控制器 (MC) 的设备上配置访客 WLAN。有关 MA 和 MC 功能的详细信息，请参阅第 5 章，“自带设备无线基础设施设计”。因此，在大型园区内，如果融合接入基础设施包括配置为 MA 的 Catalyst 3850 交换机以及配置为 MC 的 CT5760 无线控制器，则必须在两台设备上配置访客 WLAN。在分支机构中，如果融合接入基础设施仅包括一台配置为 MA 兼 MC 的 Catalyst 3850 交换机，则访客 WLAN 的配置同样如上所述。

注意，无线移动配置将有所不同，具体取决于 Catalyst 3850 交换机是在大型园区内被配置为 MA 还是在分支机构内被配置为 MA 兼 MC。具体内容见第 5 章，“自带设备无线基础设施设计”。

为了支持访客接入，必须将访客无线控制器添加为 MC 中移动组的成员。以下部分配置显示了移动组及指向访客无线控制器的移动组成员的配置示例。

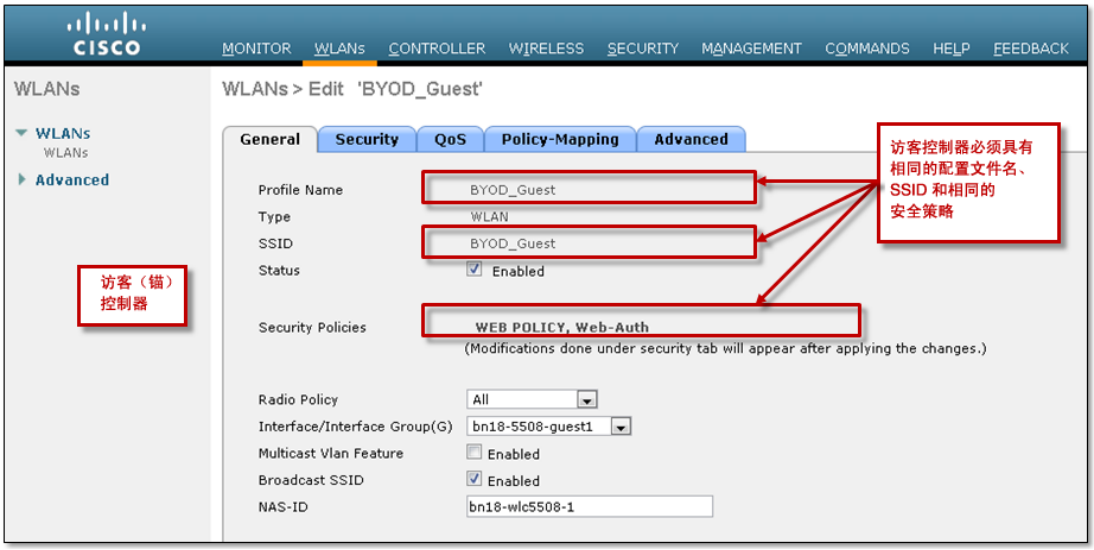
```
!
Wireless mobility controller/ 启用 MC 功能
wireless mobility group member ip 10.225.50.35 public-ip 10.225.50.35/ 访客控制器
wireless mobility group name byod/ 移动组名称
!
```

移动组名称和移动组对等点配置必须显示在作为移动代理 (MC) 的设备上。因此，如果 Catalyst 3850 系列交换机已部署为分支机构部署中的 MA 兼 MC，则配置必须包括类似的几行。如果仅将 Catalyst 3850 系列交换机部署为园区部署中的 MA，则其中将不包括移动组配置。而部署为园区内的 MA 兼 MC 的 CT5760 无线控制器将包含移动组配置。请注意，由于基于 IOS XE 的无线控制器仅支持新分层移动架构，因此无需配置来启用它。

访客控制器

访客控制器是所有访客无线流量终结的点。在本版设计指南中，将仅讨论以 CT5508 CUWN 无线控制器作为访客控制器的情况。如概述中所述，移动锚点隧道建立在访客控制器和园区控制器之间。访客控制器利用 ISE 验证源于园区或分支机构控制器的所有访客流量。第一步是定义名为 BYOD_Guest 的访客 SSID。此 SSID 的名称必须与园区控制器中定义的 BYOD_Guest 相同。图 13-12 显示了详细信息。

图 13-12　　访客控制器中的 BYOD_Guest 详细信息



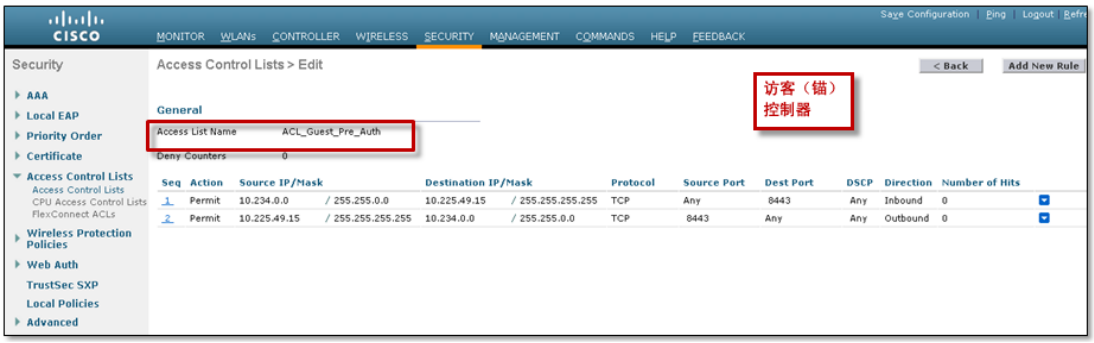
下一个重要的选项卡是 BYOD_Guest WLAN 的第 2 层安全详细信息，如图 13-13 所示。

图 13-13　访客控制器中 BYOD-Guest WLAN 的第 2 层安全详细信息

第 2 层安全设置为 None，表示开放式 SSID。必须为网络身份验证配置身份验证。两者都要与园区控制器的配置匹配。

使用远程 Cisco ISE 访客门户进行登录和可选的 AUP 或 EUA 时，网络身份验证预身份验证 ACL 是必要的。必须配置网络身份验证预身份验证 ACL，以允许所有与能分发给访客无线设备的访客无线子网关联的可能 IP 地址重定向至 Cisco ISE 访客门户的 TCP 端口 8443。网络身份验证预身份验证 ACL 的一个示例如图 13-14 所示。

图 13-14　通过网络身份验证的访客无线接入的预身份验证 ACL 示例



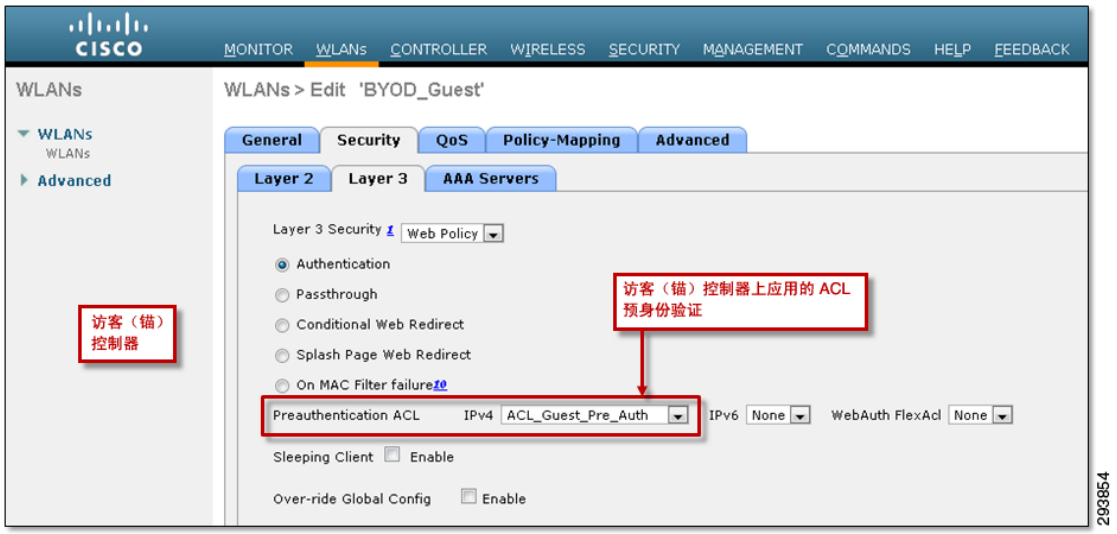
ACL 指定以下访问权限：

- 允许（不重定向）流量从 10.234.0.0/16 网络地址空间中的设备到达 ISE 服务器 (10.225.49.15) 的 TCP 端口 8443。

ACL 隐式拒绝 （重定向）其他所有到 ISE 访客门户的流量。指定将 ACL 降至访客无线控制器中的端口级别时，必须配置入站 （从无线访客设备到 Cisco ISE 服务器）和出站 （从 Cisco ISE 服务器到无线访客设备）规则。仅指定入站规则不会自动允许通过无线控制器的返回流量，就如同状态防火墙一样。此外，指定上述单一规则形式且方向为 “Any” 也不起作用。无线控制器不会反转返回流量的源和目标 IP 地址。

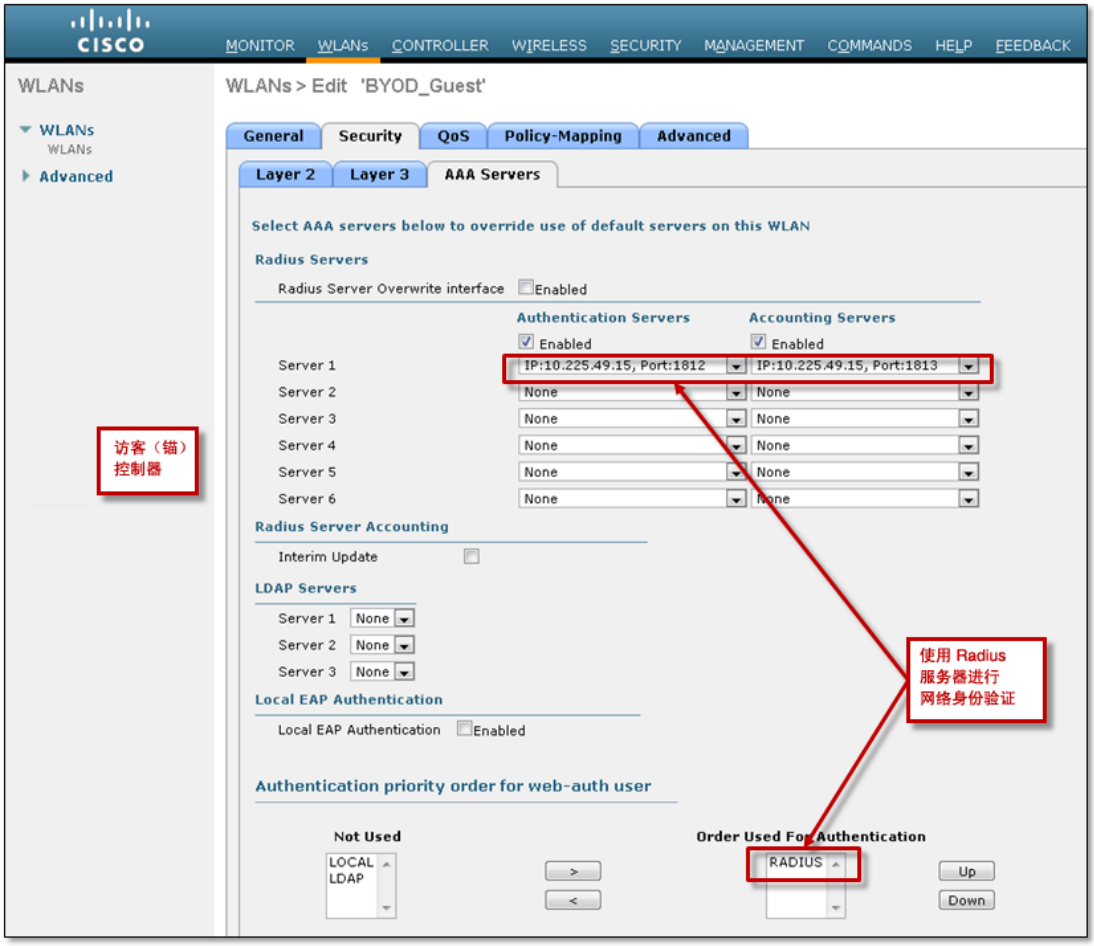
ACL 配置后，必须应用为网络身份验证预身份验证 ACL。此步骤在访客 WLAN 第 3 层安全策略中完成，如图 13-15 所示。

图 13-15　　将 ACL 作为网络身份验证预身份验证 ACL 应用



AAA 服务器配置详细信息如图 13-16 所示。

图 13-16　　访客控制器中 BYOD-Guest WLAN 的 AAA 服务器配置



配置 AAA 服务器参数，以便网络身份验证使用 Cisco ISE 服务器验证使用 Radius 的访客。

下一步是在访客和园区控制器之间配置锚定移动隧道。必须先将园区控制器作为移动组成员添加到访客控制器。如图 13-17 中的示例所示。

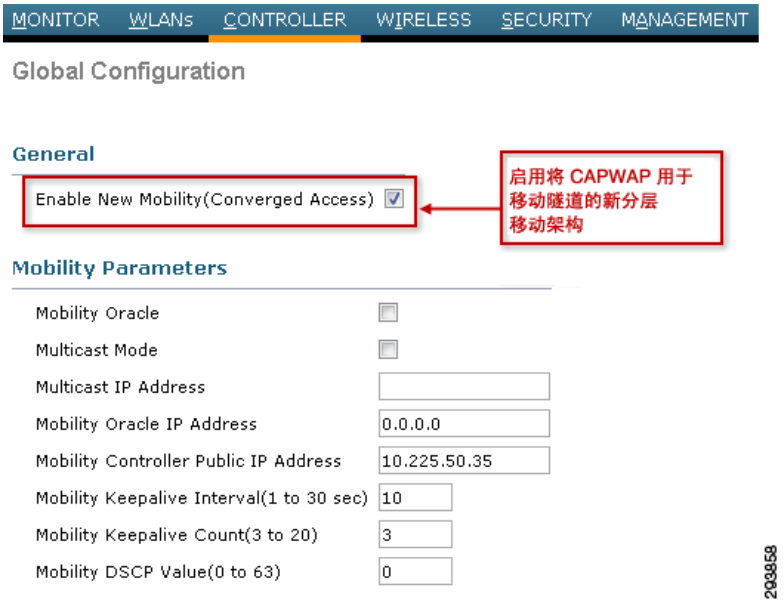
图 13-17　　将园区控制器添加到移动组

最后，在 BYOD_Guest SSID 中创建移动锚点。对于访客控制器，移动锚点指向自身管理接口的本地 IP 地址。这与指向访客控制器的园区控制器配置不同。如图 13-18 中的示例所示。

图 13-18　在访客控制器上配置移动锚点

为支持新移动架构（也称为分层移动架构），网络管理员必须选中无线控制器全局移动配置中的**启用分层架构**选项。如图 13-19 所示。

图 13-19　启用访客控制器中的分层移动架构



注意　由于 Flex 7500 无线控制器不支持新移动架构，因此，实施从 Flex 7500 外部控制器自动锚定无线设备的访客控制器时，可以跳过此步骤。

访客控制器利用外部服务器（即本设计中的 ISE）验证用户。因此，必须配置访客控制器，以将访客用户重定向至 ISE，如图 13-20 所示。

图 13-20　　重定向到外部服务器的配置

在图 13-20 中， **External Webauth URL** 设置如下：

https://guest.bntest.com:8443/guestportal/portals/SponsoredGuests/portal.jsp

服务器的名称（在上面的示例中为 **guest.bntest.com**）必须通过 DNS 解析为 ISE IP 地址，即本章各示例中的 10.225.49.15。

表 13-1 显示了本节屏幕截图和配置示例中使用的访客和园区控制器的 IP 地址信息。

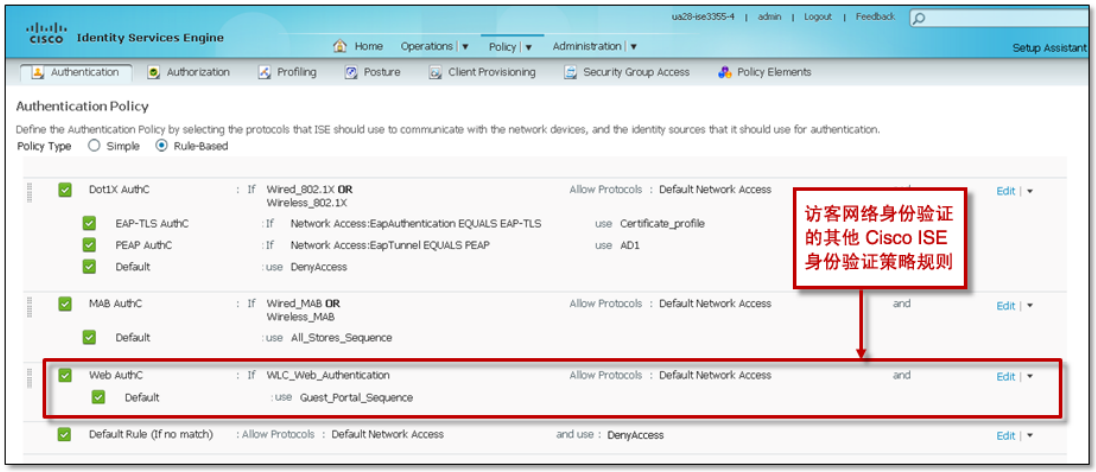
表 13-1　　园区 （外部）和访客 （锚）控制器的 IP 地址

设备	本地 IP 地址	远程 IP 地址
园区 CUWN 控制器	10.225.44.2	10.225.50.35
园区融合接入 （基于 IOS XE）控制器	10.225.47.2	10.225.50.35
访客控制器	10.225.50.35	1.225.44.2 和 10.225.47.2

Cisco ISE 策略配置

从 Cisco ISE 策略的角度，需要为访客身份验证添加另一个身份验证规则。此规则允许与访客 WLAN 对应的 SSID 发起无线控制器网络身份验证，以为无线访客接入使用单独的 Cisco ISE 用户身份序列。该策略规则的示例如图 13-21 所示。

图 13-21　　允许访客无线接入的 Cisco ISE 身份验证策略示例



示例身份验证策略规则的逻辑格式如下：

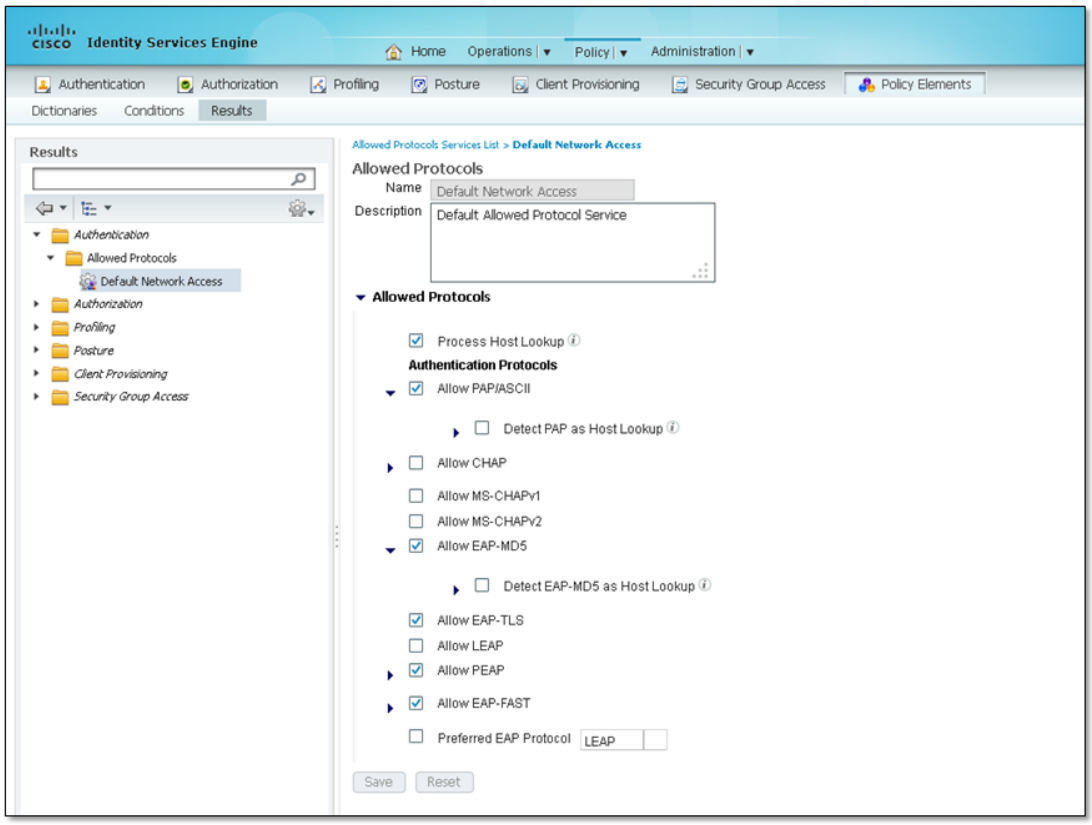
```
IF (WLC_Web_Authentication)
    THEN (Allow Default Network Access AND USE Guest_Portal_Sequence)
```

WLC_Web_Authentication 是一个系统生成的复合条件，在此处用于匹配来自思科无线局域网控制器的网络身份验证请求。它与以下两个标准 RADIUS 字典属性值 (AV) 对相匹配：

```
Service-Type - [6] EQUALS Login
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
```

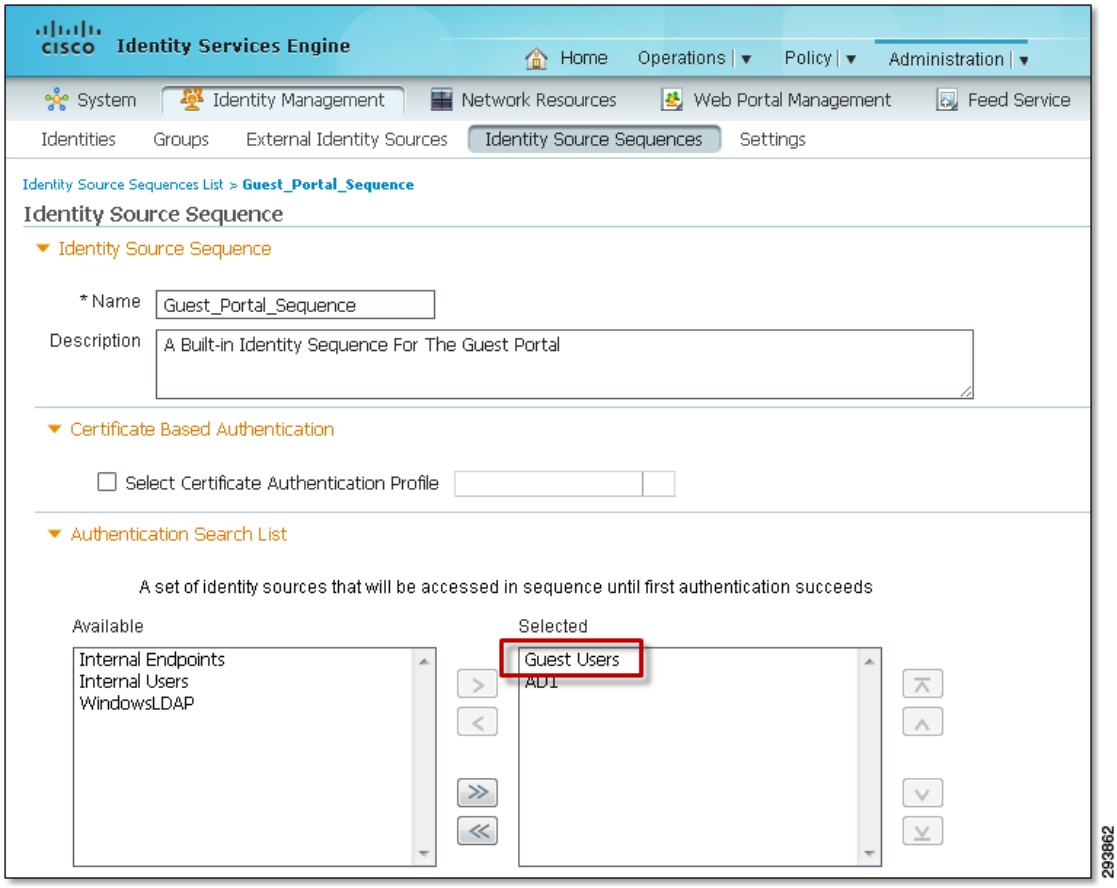
Default Network Access 是一个系统生成的身份验证结果，允许将多种协议用于网络身份验证。如图 13-22 中的示例所示。

图 13-22　Allowed Protocols 下 Default Network Access 的示例



Guest_Portal_Sequence 是一个用户定义的身份源序列。如图 13-23 中的示例所示。

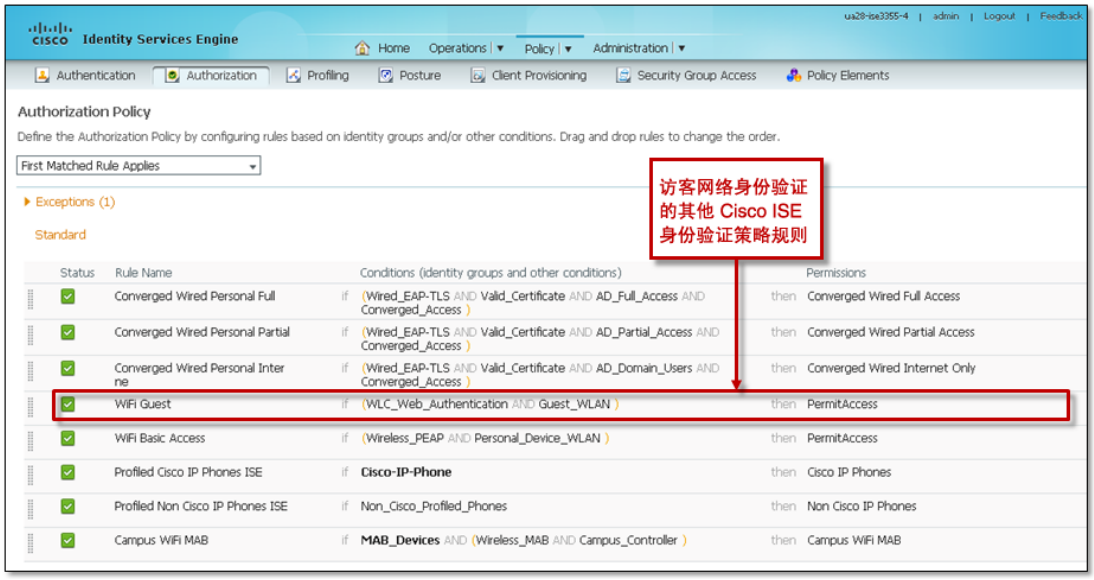
图 13-23　Guest_Portal_Access 身份源序列示例



上例中的 Guest_Portal_Sequence 使用 Guest Users 身份源作为主要源并使用 AD1 组作为下一个源。 Guest Users 是一个系统生成的身份源，是从 ISE 1.2 起增加的新功能。此身份源是访客凭证在通过 Cisco ISE 保证人门户配置时放置的位置，具体介绍见本章的后续部分。虽然当仅指定一个身份源时，身份源序列并非绝对必要，但是配置序列后，访客无线接入就能通过添加其他身份源轻松扩展为包括员工个人设备。

从 Cisco ISE 策略的角度，需要为访客用户添加另一个授权规则。此规则允许与访客 WLAN 对应的 SSID 发起的无线控制器网络身份验证访问。该策略规则的示例如图 13-24 所示。

图 13-24　　允许访客无线接入的 Cisco ISE 授权策略示例



示例授权策略规则的逻辑格式如下：

```
IF (WLC_Web_Authentication AND Guest_WLAN
    THEN Permit Access
```

WLC_Web_Authentication 在上文的身份验证策略中已进行了讨论。

Guest_WLAN 是一种用户定义的简单授权条件，用于通过与开放式访客 SSID 对应的 WLAN 进行网络身份验证然后接入互联网的访客。它与 Airespace 字典中的以下 RADIUS AV 对相匹配：

```
    Airespace-Wlan-Id - [1] EQUALS 2
```

Airespace-Wlan-Id 是与访客 SSID 对应的 WLAN 标识号 (WLAN ID)，如图 13-25 所示。

图 13-25　　示例访客无线控制器 WLAN ID

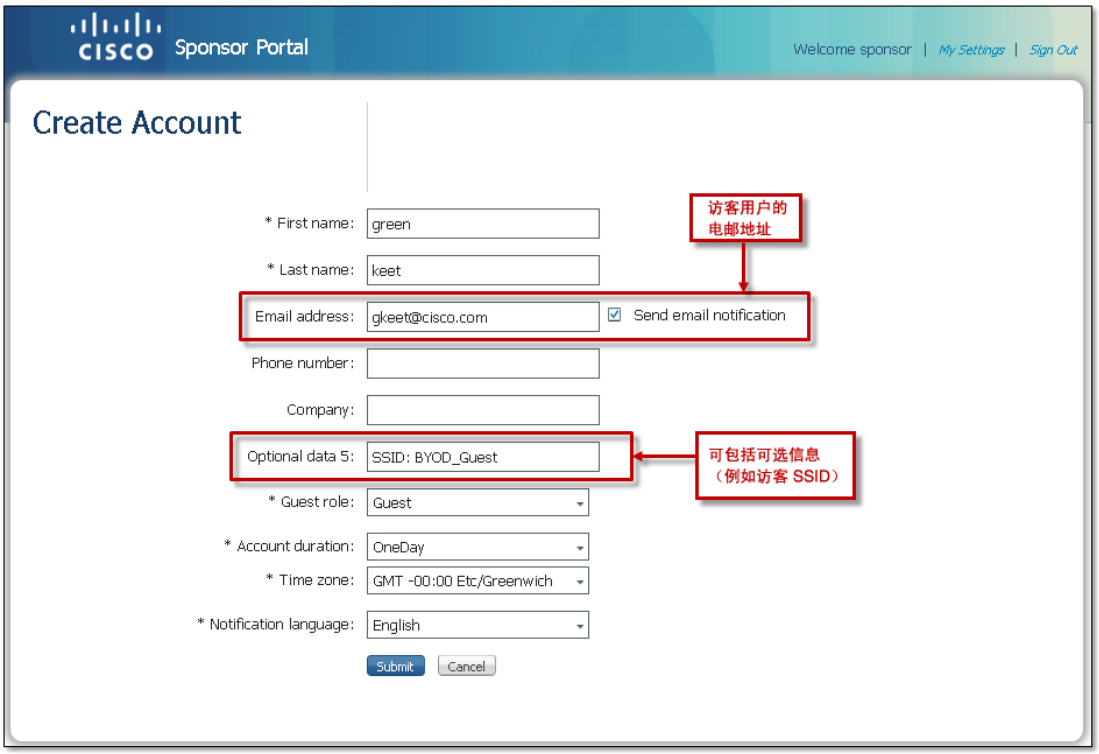
这允许 ISE 授权策略区分来自访客 WLAN 的 Web 身份验证请求并允许它们执行。

注意　可使用 Guest_WLAN 等简单条件为属性和值对分配描述性名称。这样，策略会更具可取性，也更易于提供支持。

Cisco ISE 保证人门户

Cisco ISE 保证人门户可通过以下地址访问：https://ISE_server:8443/sponsorportal/，其中 ISE_server 是 IP 地址或 Cisco ISE 服务器的名称。在 Cisco ISE 保证人门户中创建访客凭证的网页示例如图 13-26 所示。

图 13-26　在 Cisco ISE 保证人门户中创建访客凭证



其中可以包括访客公司名称、访客的电邮地址和电话号码以及用户定义的可选数据等信息。可选的数据可能包括访客需要连接的 WLAN SSID（如果 SSID 已隐藏），以及保证人的姓名、电话号码和所在部门。根据允许的时间配置文件，可以将凭证配置为在将来的某个日期和时间变为活动状态并在一段时间内保持活动状态。Cisco ISE 保证人门户还可以在访客凭证通过电邮或短信方式送达之前将其发送给访客。通过电邮发送凭证有助于确保访客提供有效的电邮地址。

访客凭证创建后，可以由保证人通过 Cisco ISE 保证人门户监控和管理，如图 13-27 所示。

图 13-27　从 Cisco ISE 保证人门户监控访客凭证

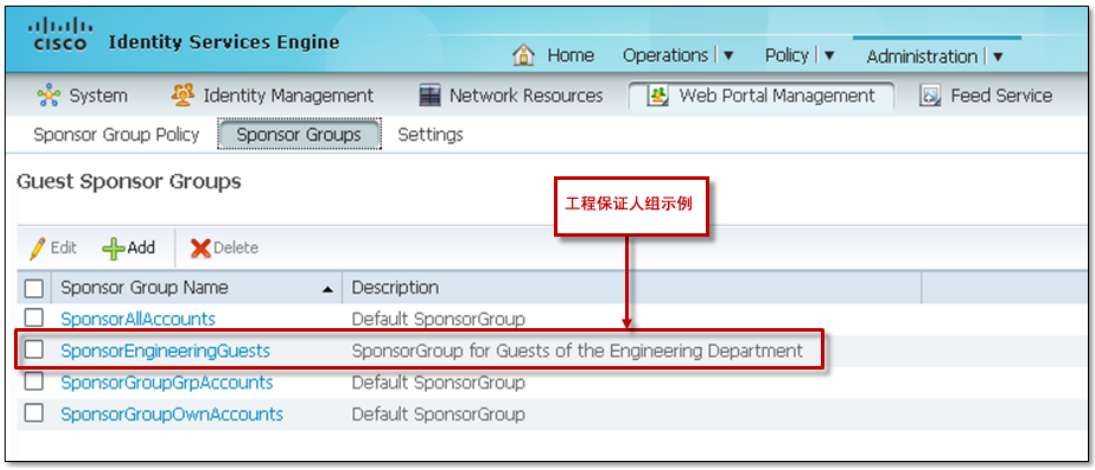
请注意，在图 13-27 中，用户名基于电邮地址，而不是仅基于访客的名字和姓氏。第 12 章，“BYOD 基本访问使用案例”也讨论了将访客无线访问权限扩展为允许员工个人设备。在访客用户名中使用电邮地址是区分可能具有相同名字和姓氏的访客和员工的一种方式。

配置 Cisco ISE 保证人门户

Cisco ISE 保证人门户的配置通过 Cisco ISE 服务器的 Web 门户管理部分完成。可以创建不同级别的保证人责任，包括只能查看和编辑自创的访客帐户的个人保证人，到可以查看和编辑特定组的访客帐户的组保证人，还有可以查看和编辑所有访客帐户的保证人。

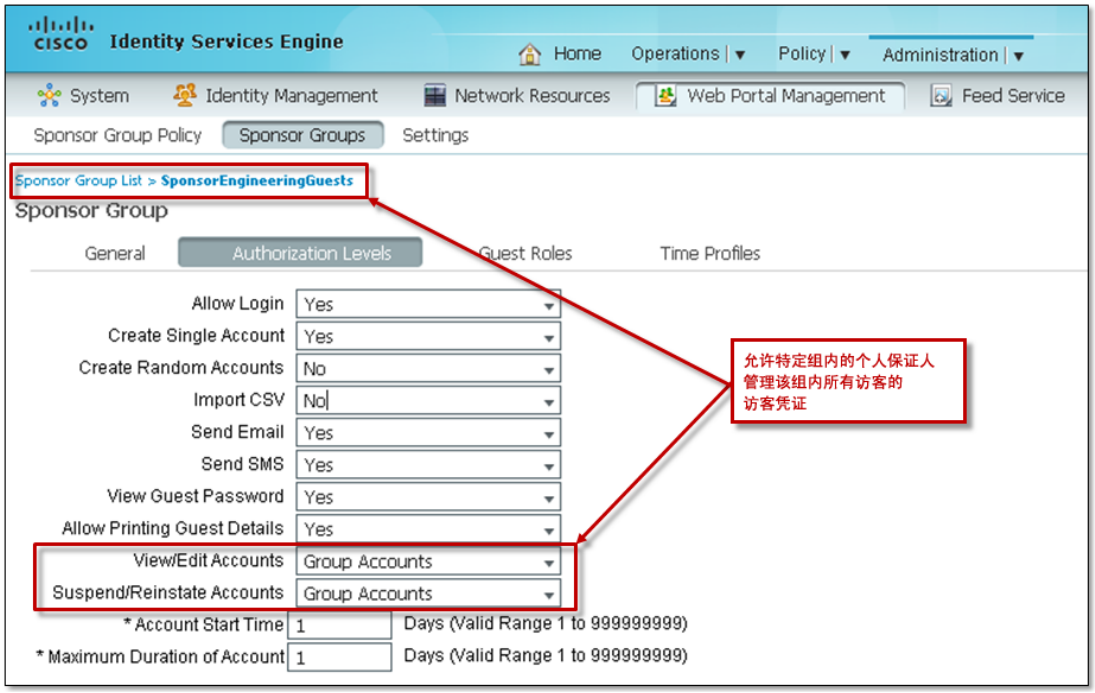
可以通过 Cisco ISE 服务器 Web Portal Management 部分下的 Sponsor Groups 选项卡创建多个保证人组，各组都包含各自的成员。图 13-28 显示了一个示例，其中为工程部保证的访客添加了一个单独的组。

图 13-28　多个 ISE 保证人组的示例



然后，可以通过双击特定保证人组并选择 **Authorization Levels** 选项卡为每个保证人组配置不同的授权参数，如图 13-29 所示。

图 13-29　　个人保证人组的授权级别示例



在此示例显示的配置中，保证人组的所有成员都可以查看、编辑、暂停和恢复由该保证人组的任何其他成员创建的访客凭证。但是，其他保证人组的成员不能修改为此组创建的访客凭证。

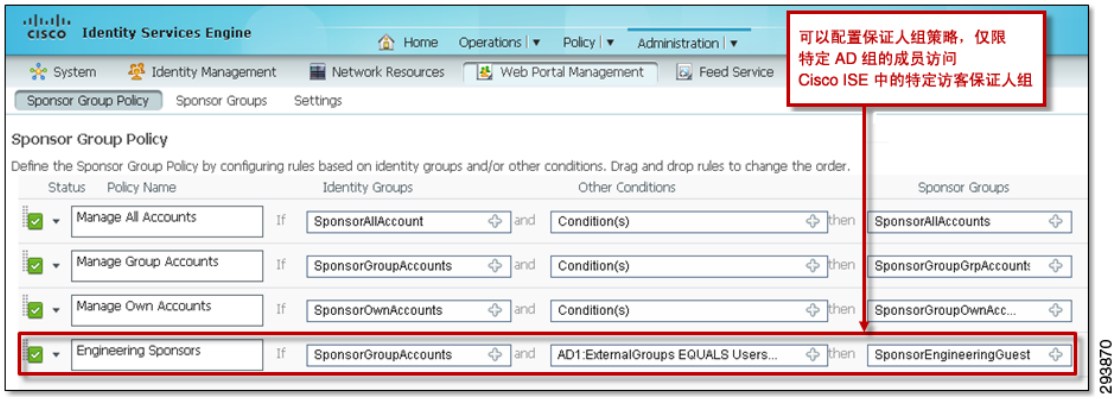
Guest Roles 选项卡用于选择用户身份组 （即访客凭证数据库），此保证人组成员创建的访客凭证便放置在其中。如图 13-30 中的示例所示。

图 13-30　　个人保证人组的访客角色示例

Time Profiles 选项卡允许网络管理员决定将哪个时间配置文件 （ISE 中的默认或预配置）应用到特定保证人组。

保证人组创建后， Sponsor Group Policy 选项卡可用于创建控制谁有权访问哪些保证人组的策略。更为常见的是，组织可能希望利用现有 Microsoft Active Directory 组区分不同的保证人。图 13-31 显示了此步骤的示例。

图 13-31　　保证人组成员的 Microsoft AD 示例



在本示例中，仅限既是 Microsoft Active Directory 域成员，又是 “Users/uatest.com” 组成员的用户访问保证人组。请注意，必须将 Microsoft Active Directory 服务器配置为外部身份源，才能选择此选项。在本示例中， Microsoft Active Directory 服务器为 “AD1”。

如果需要，通过严密控制拥有 ISE 保证人访问权限的 Microsoft AD 组成员，网络管理员可以将访客无线网络的使用限制为原始预期目的 （访客无线接入），而非员工个人设备。

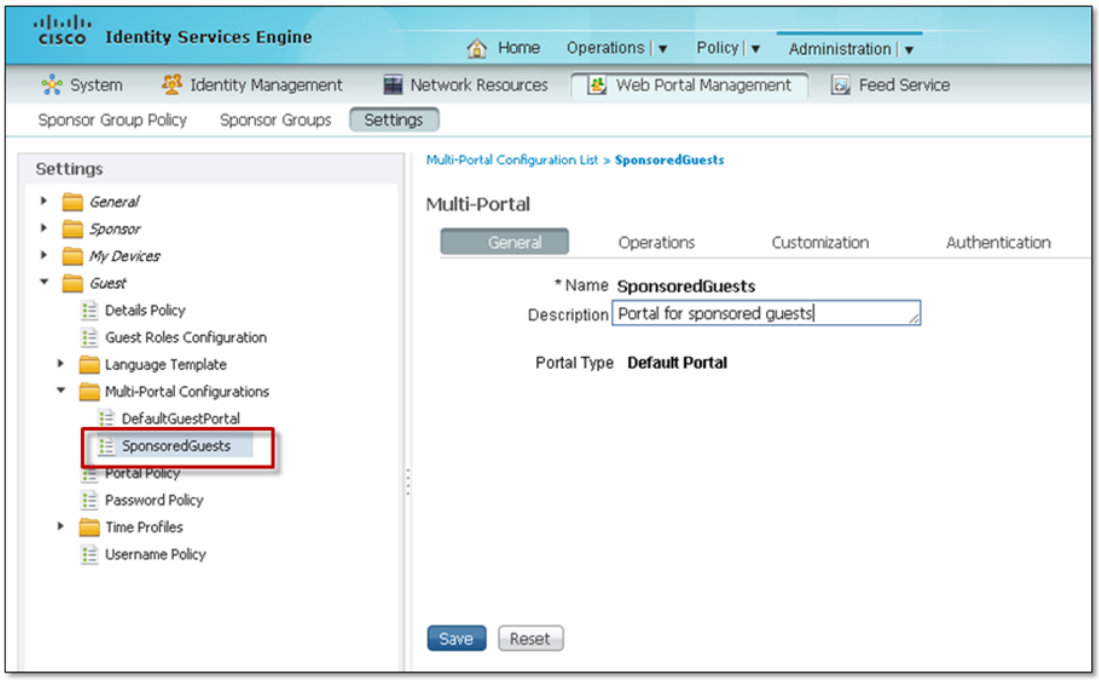
Cisco ISE 访客门户

如前所述， Cisco ISE 能够支持多个访客门户。 Cisco ISE 服务器拥有系统生成的 DefaultGuestPortal 配置。它允许网络管理员调配访客门户，目的是让员工或 IT 员工自注册公司拥有的设备或员工个人设备，如第 10 章，“BYOD 增强型使用案例 - 个人和企业设备”所述。

配置 Cisco ISE 访客门户

无线访客接入的另一个访客门户可以通过 Guest > Multi-Portal Configurations 定义。如图 13-32 中的示例所示。

图 13-32　　多门户 BYOD 部署示例



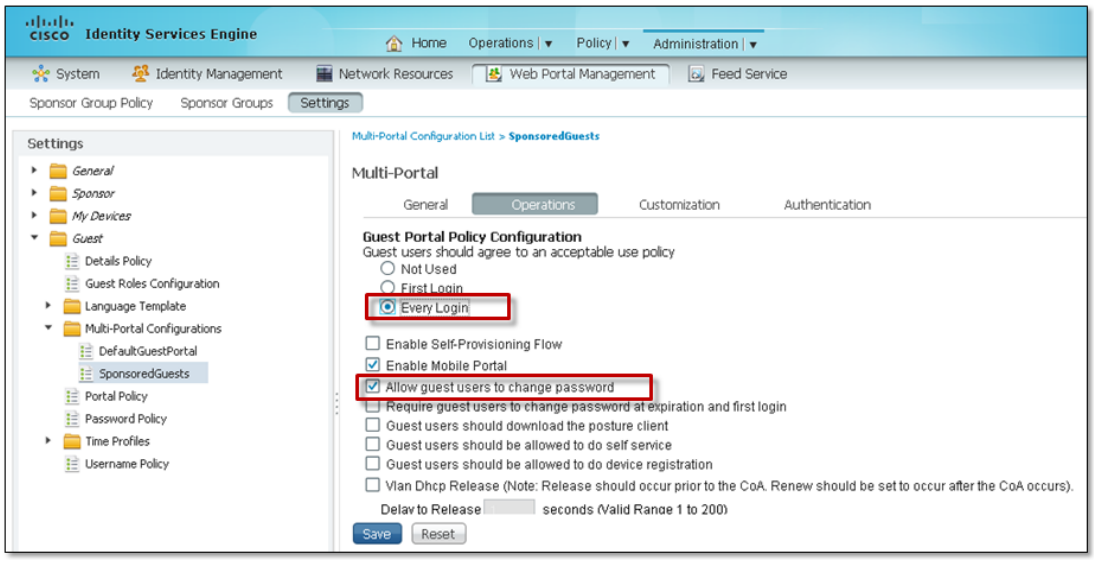
实施用户定义的访客门户时，需要在访客无线控制器 Web Auth Web Login Page 中配置 URL，如图 13-20 所示：

http://*ISE_server*:8443/guestportal/portals/*name_of_user-defined_portal*/portal.jsp

ISE_server 是 Cisco ISE 服务器的 IP 地址或名称。*Name_of_user-defined_portal* 是新用户定义访客门户的名称，在上例中为 SponsoredGuests。

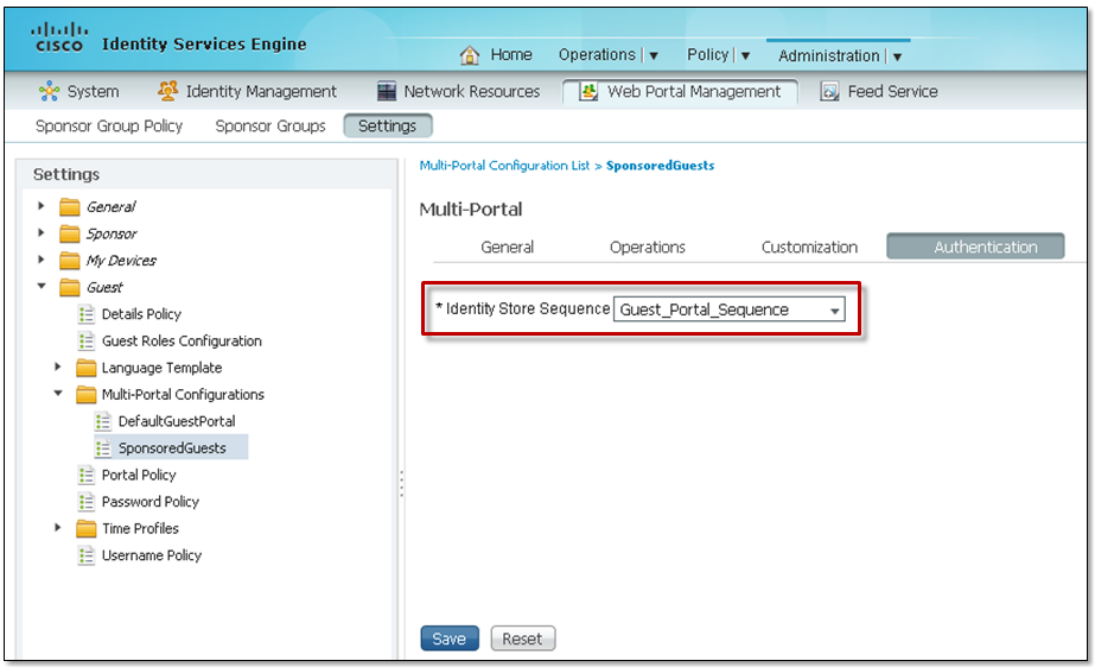
新访客门户定义后， Operations 选项卡可用于显示 “可接受使用政策”（也称为最终用户协议或 EUA），并控制访客可以还是必须更改保证人调配的密码。请注意， Operations 选项卡还可用于强制访客在从访客无线网络接入互联网之前将其设备注册到 Cisco ISE 服务器上。本设计指南假定，在制定允许对访客无线网络的访问决策时不考虑访客设备本身。因此，此使用案例不作讨论。图 13-33 显示了 Operations 选项卡的示例。

图 13-33　　Operations 选项卡示例



Authentication 选项卡确定哪个身份源序列用于访客凭证。如图 13-34 中的示例所示。

图 13-34　　用户定义的访客门户的身份验证设置示例

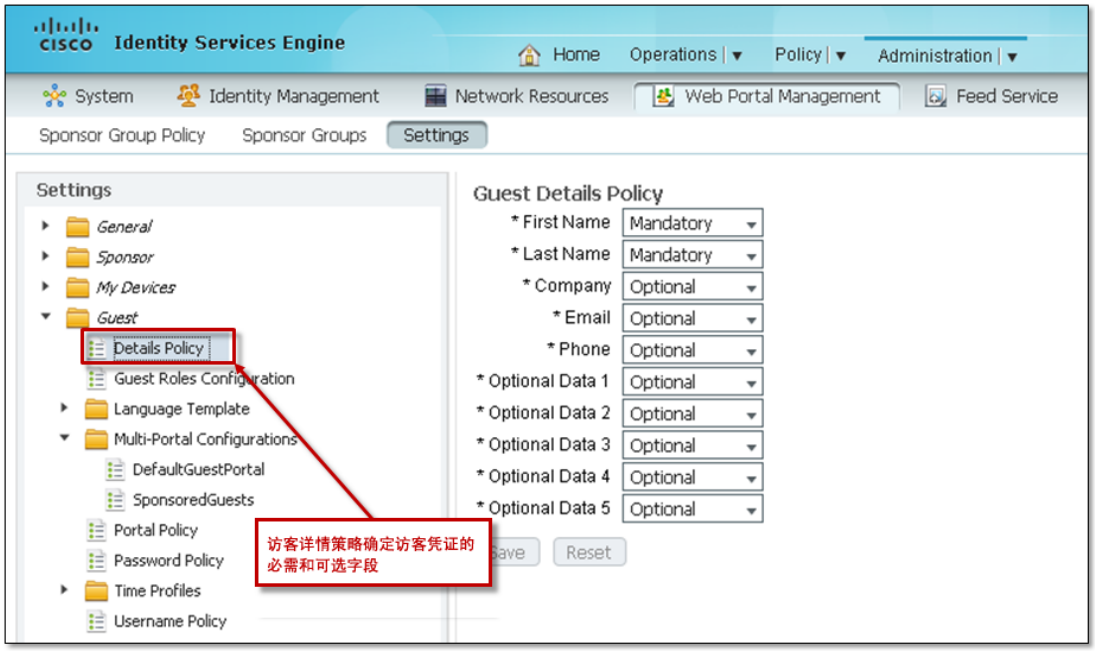


对于此示例，选择名为 **Guest_Portal_Sequence** 的身份源序列。仅部署无线访客接入时，此身份源序列才使用 **Guest Users**，如图 13-23 所示。这样，访客凭证便可以通过访客门户访问和 ISE 身份验证策略。此配置还允许访客接入轻松扩展为包括员工个人设备，只需增加 Microsoft Active Directory 身份库即可，如以下章节所述：第 12 章，“BYOD 基本访问使用案例”。

注意　Cisco ISE 身份验证日志可能会显示具有此配置的访客用户身份验证出现了两次，但只通过网络身份验证对访客进行了一次身份验证。

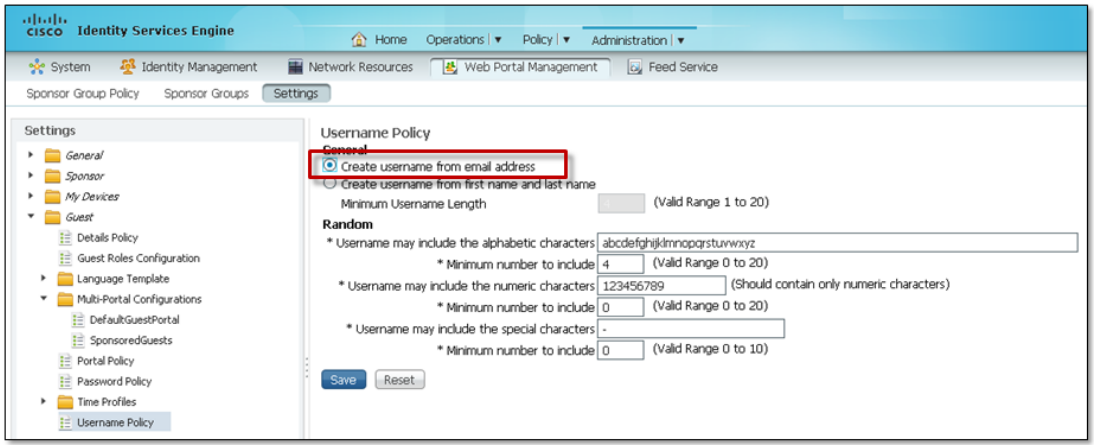
Guest Details Policy 用于配置其他全局访客参数，包括必需和可选参数。如图 13-35 中的示例所示。

图 13-35　Guest Details Policy 示例



Guest 文件夹下的其他网页控制其他全局访客配置参数，例如 Username Policy 和 Password Policy。在 Username Policy 中，可以选择根据其电邮地址选择访客用户名，如图 13-36 所示。

图 13-36　访客用户名策略示例

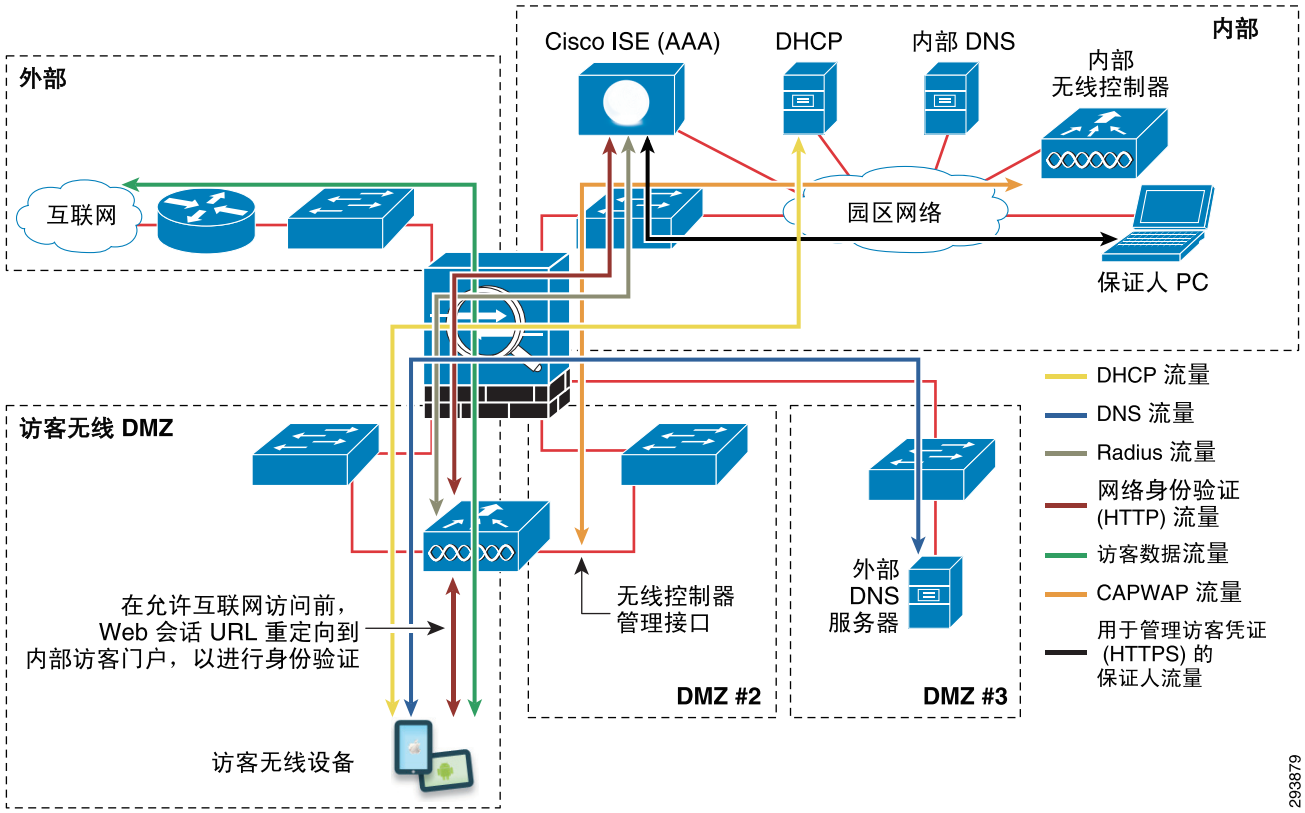


最后， Time Profiles 文件夹可用于为访客用户接入选择一个现有时间配置文件或创建自定义时间配置文件。时间配置文件由保证人在配置访客凭证时选择，用于控制访客用户何时能够接入网络以及接入时长。

ASA 防火墙配置

图 13-37 显示了需要通过 Cisco ASA 防火墙以支持本章所讨论的设计的流量示例。

图 13-37　　需要通过 Cisco ASA 防火墙的流量示例



本设计需要允许 RADIUS 会话通过访客无线控制器和 Cisco ISE 服务器之间的 ASA 防火墙。此外，本设计需要重定向并允许访客 Web 会话通过 ASA 防火墙到达思科 ISE 服务器所处的网络内部。默认情况下， Cisco ISE 为访客门户使用 TCP 端口 8443。使用较旧的移动架构时，还必须允许两个无线控制器管理接口之间的 IP 以太网（IP 端口 97）自动锚定移动隧道以及 WLAN 控制端口 （UDP 端口 1666）通过 ASA 防火墙。使用新分层移动架构时，必须允许两个无线控制器管理接口之间的 CAPWAP（用于控制的 UDP 端口 5246 和用于数据的 UDP 端口 5247）自动锚定移动隧道通过 ASA 防火墙。除了允许将 DNS、 DHCP （假设部署内部 DHCP 服务器）和 TCP 端口 8443 用于 HTTPS 重定向以外，应配置 ASA 防火墙，以阻止从访客无线设备生成的所有其他流量流入内部网络。

表 13-2 总结了需要允许通过 ASA 防火墙的相关端口。

表 13-2　　要允许通过 ASA 防火墙的端口

应用	传输协议	端口
IP 以太网		
（旧移动架构）	TCP/UDP	97
WLAN 控制		
（旧移动架构）	UDP	1666
ISE 访客门户	TCP	8443
DNS	UDP	53
BOOTPS (DHCP)	UDP	67
BOOTPC (DHCP)	UDP	68
CAWAP 控制信道 （新移动架构）	UDP	5246
CAPWAP 数据信道 （新移动架构）	UDP	5247

其他注意事项

实施 Apple iOS 或 Mac OS X Lion 等设备的访客无线接入时，网络管理员应该注意，这些设备已实施了自动检测强制网络门户是否存在的功能。它通过向 Apple 网站生成 HTTP 请求并查找响应执行此操作。如果收到重定向，则假设存在强制网络门户部署。此功能仅适用于拥有开放式接入的 SSID，与大多数访客无线网络一样。检测到强制网络门户部署时，iOS 或 Mac OS X Lion 设备会自动显示身份验证对话框窗口，无需最终用户启动网络浏览器。此功能通过弹出窗口执行网络身份验证，旨在简化不基于浏览器的应用接入互联网的过程，无需最终用户启动网络浏览器。许多基于 HTML 的移动应用不使用浏览器作为用户界面。这称为强制网络门户网络帮助 (CPNA)，实际是一种基于轻量级 HMTL 的用户界面。遗憾的是，该界面不能与 iOS 分析器管理器正确交互。其症状因 iOS 版本而异。在 iOS5 中，不取消 CPNA 的情况下，用户不能安装 WiFi 配置文件，因此会强制设备关闭调配 SSID。在 iOS6 中，用户会被自动转到配置文件管理器，但安装配置文件后，用户不会返回到 CPNA 以接收证书。在这两种情况下，CPNA 都不能成功自注册设备。

思科无线控制器已实施了绕过此功能的解决办法，允许 Apple iOS 或 Mac OS X Lion 设备在强制网络门户部署中运行，且使用 HTTPS 连接到带自签名证书的访客门户。对于 CUWN 无线控制器，网络管理员需要建立到访客无线控制器的 SSH 会话，并发出以下命令：

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

对于 IOS XE 无线控制器，网络管理员需要将以下命令添加到 CT5760 无线控制器或 Catalyst 3850 系列交换机的全局配置中：

```
captive-portal-bypass
```

此命令会使无线控制器应答 HTTP 请求，让 Windows 或 Mac OS X Lion 设备误以为没有强制网络门户部署。最终用户打开浏览器并尝试导航到任何站点时，会重定向到该门户，且系统会提示他们提供使用正常网络身份验证过程的凭证。请注意，在最终用户打开网络浏览器并继续正常的网络身份验证过程之前，不基于浏览器的应用不能接入网络。这包括基于 HTML 的应用，如 WebEx。

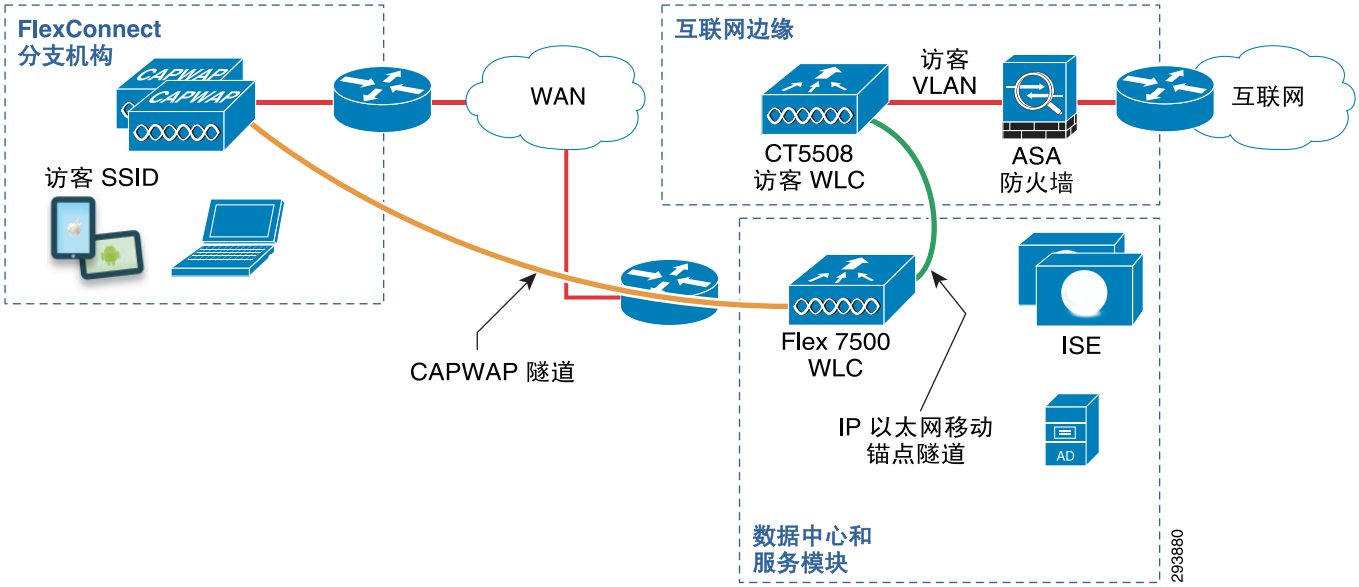
分支机构中的无线访客接入

分支机构网络经常提供无线访客服务。可以部署两个基本架构。第一个是集中模式，其中，所有分支机构无线访客流量通过 CAPWAP 隧道传递到位于园区内的中央控制器，即外部控制器。然后，无线访客流量会通过移动锚点隧道进一步传递到位于 DMZ 中的锚控制器。这是本设计指南中呈现的方式。

另一种方法是使用 FlexConnect 或融合接入基础设施，在本地将访客流量终止在分支机构中的安全分段。第二个方法的优势在于，访客流量不会消耗昂贵的企业 WAN 带宽。相反，访客流量隔离在分支机构中，并使用本地分支机构互联网路径。本指南的未来版本可能会探讨此选项。另外，还可以使用许多其他可能的 WAN 部署模式为访客用户提供互联网接入。介绍了各种网域网架构的一套白皮书可在以下位置获取：
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_white_papers_list.html。

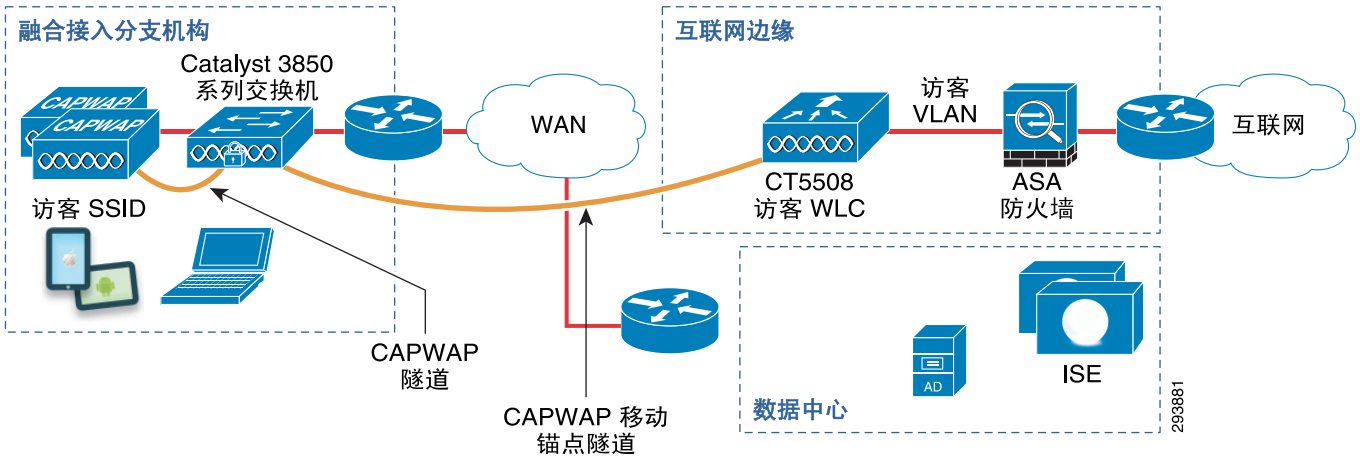
此处显示的指导遵守集中模式。对于 FlexConnect 无线设计，为分支机构位置服务并向分支机构 BYOD 设备提供自注册的 FlexConnect 无线控制器也用作外部控制器，将无线访客流量通过隧道传递到园区互联网边缘内的访客无线控制器中。图 13-38 显示了此模式所需的各种组件。

图 13-38　FlexConnect 分支机构中的访客无线接入



对于融合接入设计，作为分支机构位置无线控制器并向分支机构 BYOD 设备提供自注册的 Catalyst 3850 系列交换机也用作外部控制器，将无线访客流量通过隧道传递到园区互联网边缘内的访客无线控制器中。图 13-39 显示了此模式所需的各种组件。

图 13-39　融合接入分支机构中的访客无线接入



注意　请注意，部署融合接入无线设计（将 Catalyst 3850 系列交换机用作移动控制器 (MC) 和移动代理 (MA)）时，用于无线访客接入的移动隧道是由 Catalyst 3850 交换机向 DMZ 中的访客锚点控制器发起的。因此，每个分支机构将使用此设计发起无线访客接入的移动隧道。对于 CT5508 无线控制器，移动域中的移动控制器最多为 72 台。因此，如果使用 CT5508 无线控制器，移动锚点隧道的最大数量限制为 71。由此，网络管理员可能需要部署额外的 CT5508 访客锚控制器。或者，网络管理员可以查看提供的来自访客接入分支机构的直接互联网接入。本指南的未来版本可能会讨论此类设计。

由于为园区和分支机构无线接入部署了独立的无线控制器，因此，同一访客 SSID 可以在两个无线控制器上配置，但其特性（例如速率限制）不同。这是为分支机构和园区位置部署独立无线控制器的一个优势。

由于分支机构可用的 WAN 带宽有限，网络管理员经常需要将访客用户可以使用的带宽量限制为低于访客用户可在园区内使用的量。下一节讨论分支机构无线访客流量的速率限制。分支机构无线访客接入的大多数其他方面也是园区无线访客设计的必要部分。例如，分支机构无线访客可以继续使用访客门户的 Cisco ISE。逻辑上，分支机构访客流量的无线拓扑与园区访客流量的无线接入相同。主要区别在于访客 SSID 上的传输容量在较大程度上与在园区中不同，园区中物理路径通常由千兆以太网支持。

限制访客无线接入的速率

注意　本节仅适用于 CUWN 无线控制器平台。本指南的未来版本可能会将讨论扩展到融合接入（基于 IOS XE）无线控制器。

移动设备的广泛使用和对通用网络访问的预期引发了访客网络负荷的稳步增长。此解决方案提供了可用于管理这些负荷的速率限制工具。可以按每用户或每 SSID 以及上行和下行使用多种方式配置速率限制。

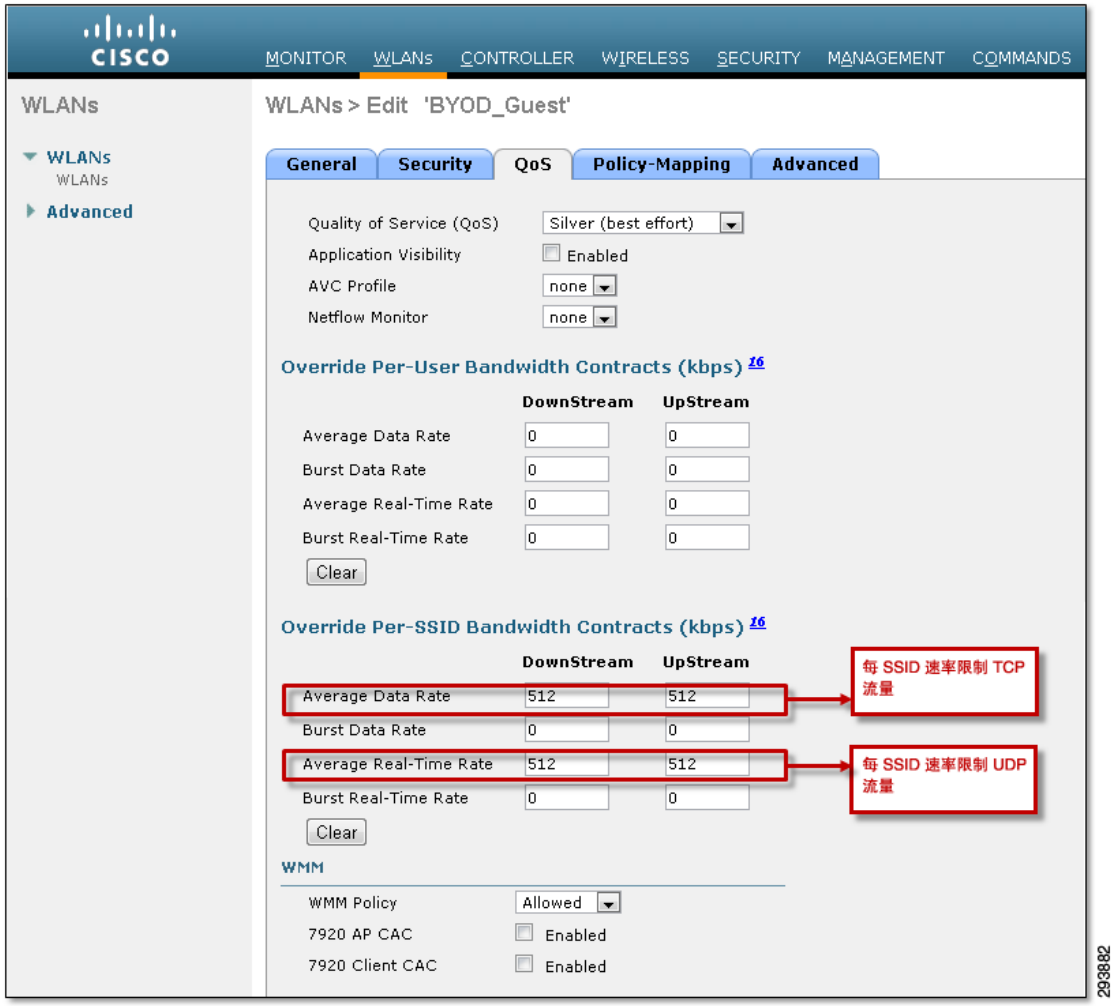
注意　由于速率限制是每 SSID、每接入点且每无线电的，因此每 SSID 速率限制实际上就是每 BSSID。但本设计指南将此称为每 SSID 速率限制。

每用户速率限制适用于每个特定无线设备。每 SSID 是由给定 SSID 中的所有设备共享的聚合速率。在这两种情况下，上行速率限制在无线电上发生。下行每 SSID 速率限制也在无线电上发生，而下行每用户速率限制在无线控制器上发生。

此上下文中的速率限制类似于策略管制。确定超过配置速率的数据包会被丢弃，不会进行测量或缓冲。策略器会实施令牌桶。令牌桶中以等于 CIR 的速度填充令牌。当令牌桶填满时，不会再增加额外的令牌。数据包传输时，令牌会从令牌桶中删除，并提供可用令牌。如果无可用令牌，数据包将被丢弃。令牌桶的大小用于确定突发速率。只要令牌可用，数据包便可以线速传输。为了保持配置的直观性，用户直接配置突发速率，而算法会确定相应的令牌桶大小。如果突发速率设置为 0，则使用默认令牌桶大小。图 13-40 显示了如何覆盖分配给 SSID 的 QoS 配置文件速率限制设置，以配置访客 SSID 速率限制的示例。

无线的一个独特特征就是并非所有传输都采用单一速率。信号强度和信噪比 (SNR) 会确定任何单个站点物理介质的实际速度。不同于速度固定为端口速率的有线网络，子网中每台主机的无线速率都可能不同，甚至会因为站点靠近或远离接入点而发生改变。有了无线速率限制，耗尽满的令牌桶所需的时间取决于无线客户端的访问速度，并不是固定的。关联在 54 Mbps 的站点耗尽令牌桶的速度快于 1 Mbps 的站点。如果使用每 SSID 速率限制，特定 AP 上的所有客户端共享一个令牌桶。如果使用每用户速率限制，则为每个站点分配一个唯一令牌桶。可以同时进行每客户端和每 SSID 速率限制。在这种情况下，令牌必须可用并且已从两个共享 SSID 令牌桶和每客户端令牌桶中移除，然后才能传输数据包。虽然这可以为尝试访问共享令牌的慢速用户提供更多公平性，但却增加了必须维护的状态信息量，从而提高了控制器上的处理要求。由于访客无线接入的许多部署都提供最优服务级别，额外的处理要求通常不值得。因此，此处仅显示每 SSID 调整。可能有业务案例证明可同时执行每用户和每 SSID 速率限制的其他方案。

图 13-40　　对访客 SSID 进行速率限制的示例配置



本设计指南中介绍的一种分支机构设计为企业无线客户端使用包含本地分支机构终端的 FlexConnect，为访客流量使用中央终端。企业批准的设备可能会将数据发送给中央数据中心内的服务器。或者，它们可能将数据发送到本地服务器。在需要访问本地服务器的地方，包含本地终端的 FlexConnect 可以消除通过 WAN 上的 CAPWAP 隧道向中央控制器传输数据的需要，从而节约 WAN 带宽。需要访问数据中心内的服务器时，本地终止的流量仍可通过 WAN 传输，但这些数据包不会在 CAPWAP 内传输。在这种情况下，可以应用常规 QoS 技术。因此，无线数据包与有线流量一起进行分类。企业有线和无线设备的常见分类适用于上行和下行两个方向。有了本文档中的设计，CAPWAP 隧道用于所有访客流量，即来自尚未自注册的个人设备的流量，以及无线控制流量（来自无线控制器和分支机构接入点的流量）。因此，在所有离开分支机构的 CAPWAP 流量中，大多数数据包可能属于访客用户。这有助于区分访客流量和企业流量。

图 13-40 中显示的示例配置允许数据速率和实时速率这两类速率。就此配置而言，数据是所有 TCP 流量，而实时是所有 UDP 流量。作为 QoS 的最佳实践，由于丢弃的数据包对流量的影响方式不同，建议阻止 UDP 和 TCP 直接相互竞争带宽。为每个协议提供不同的令牌桶可阻止 UDP 和 TCP 之间出现任何不需要的交互。

速率限制在外部控制器上配置。当园区和分支机构位置都提供访客接入时，将有两个外部控制器通过隧道传输到锚控制器。在每个外部控制器上配置的速率限制可能不同，并且对于该类用户来说是唯一的。通常，为园区访客服务的外部控制器比为分支机构访客用户服务的外部控制器拥有更高的带宽合同，因为相对于 WAN，园区可用带宽更高。

限制速率时还需要注意其他一些事项。由于 SSID 速率限制发生在无线电中，每个无线电会将 SSID 限制为配置的速率。这意味着，如果分支机构 A 和分支机构 B 是 BYOD_Guest SSID 的成员，每个分支机构都会限制访客流量，而不考虑相邻分支机构访客 SSID 上的当前负荷。但是，这意味着，如果访客 SSID 位于同一分支机构的两个无线电中，并且速率配置为 1 Mbps，则该分支机构 WAN 上的组合速率最高可达 2 Mbps。即使在单个 AP 中，如果访客 SSID 正在使用 2.4 GHz 无线电和 5 GHz 无线电，总带宽可能会是配置的访客速率限制的两倍。如前所述，速率限制功能的主要用途是保护无线电。因此，速率限制可能需要超订用要用于访客的 WAN 带宽。最小化超订用程度的一个可行方法是不在 5 GHz 无线电上启用访客 SSID。此外，参与此 SSID 的 AP 数应为提供足够覆盖范围所需的最小值。AP 组可用于管理哪些 AP 会参与其中。在所有分支机构位置限制单个 BYOD_Guest SSID 的速率可能导致不同分支机构出现不同的 WAN 速率，如图 13-41 所示。

图 13-41　　限制访客 SSID 的速率

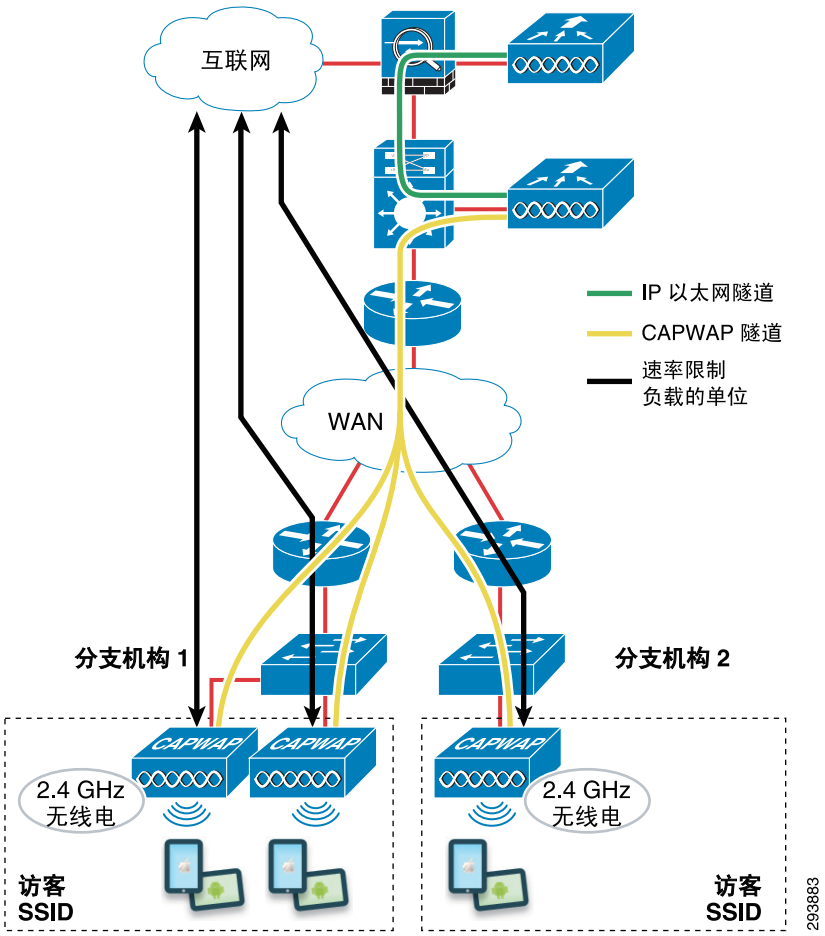


图 13-41 假设 BYOD_Guest SSID 的速率限制配置为 1 Mbps。在分支机构 1 中，本地 WAN 线路可能遇到多达 2 Mbps 的访客流量 （由于有两个 AP），而前端的 WAN 聚合线路可能遇到多达 3 Mbps 的访客负荷 （由于总共有三个 AP）。如果为访客流量使用单 SSID，则配置的速率应适合托管访客流量的最慢速分支机构。有一些可用选项可以更好地管理下文讨论的分支机构的访客负荷。

多个访客 SSID 和 AP 组

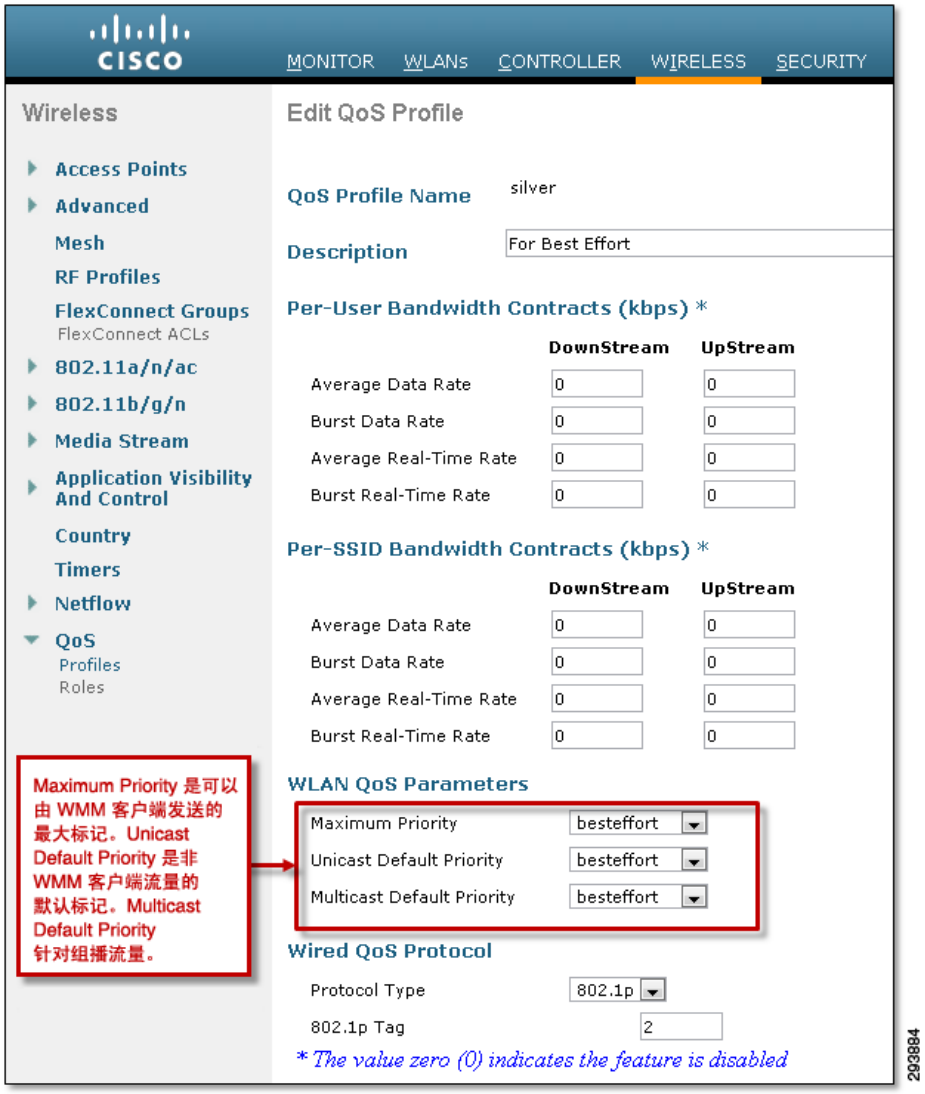
由于已按每 SSID 建立流量限制，并且，并非所有分支机构都有相同的带宽可供访客使用，管理员可能需要根据配置的速率限制建立多个访客 SSID。例如，可以将 GUEST_128 SSID 的速率限制为 128 Kb/s，而 GUEST_256 SSID 的速率可能是它的两倍。必须使用 AP 组确保两个 WLAN 并非在所有分支机构位置中都可用。如果大多数分支机构位置有一个以上 AP 可托管访客流量，则配置的速率限制将比最小化超订用的实际所需速率小。 AP 组可用于管理有多少个无线电会影响该位置的总访客负荷。多个访客 SSID 与 AP 组共同使用，可确保足量访客覆盖范围，无需过量 WAN 负荷。为分支机构 AP 创建信息性名称可简化 AP 组的创建。

AP 组在 “Flex 7500 无线分支机构控制器部署指南”中有详细介绍，该文章位于：http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml#ap-gr。

管理下行负荷

有了本文档中的 FlexConnect 设计， CAPWAP 隧道可用于所有访客流量，即来自尚未自注册的个人设备的流量，以及无线控制流量 （来自无线控制器和分支机构接入点的流量）。图 13-40 显示了一个示例，其中 Silver（最优）QoS 配置文件应用到了 BYOD_Guest SSID。QoS 配置文件用于设置封装在 CAPWAP 通道中的无线数据流量的 QoS 标记。请注意，CAPWAP 控制流量单独优先于 QoS 配置文件中的设置。图 13-42 显示了 Silver （最优） QoS 配置文件的默认设置示例。

图 13-42　　Silver （最优） QoS 配置文件的默认设置



QoS 配置文件可用于设置以下参数：

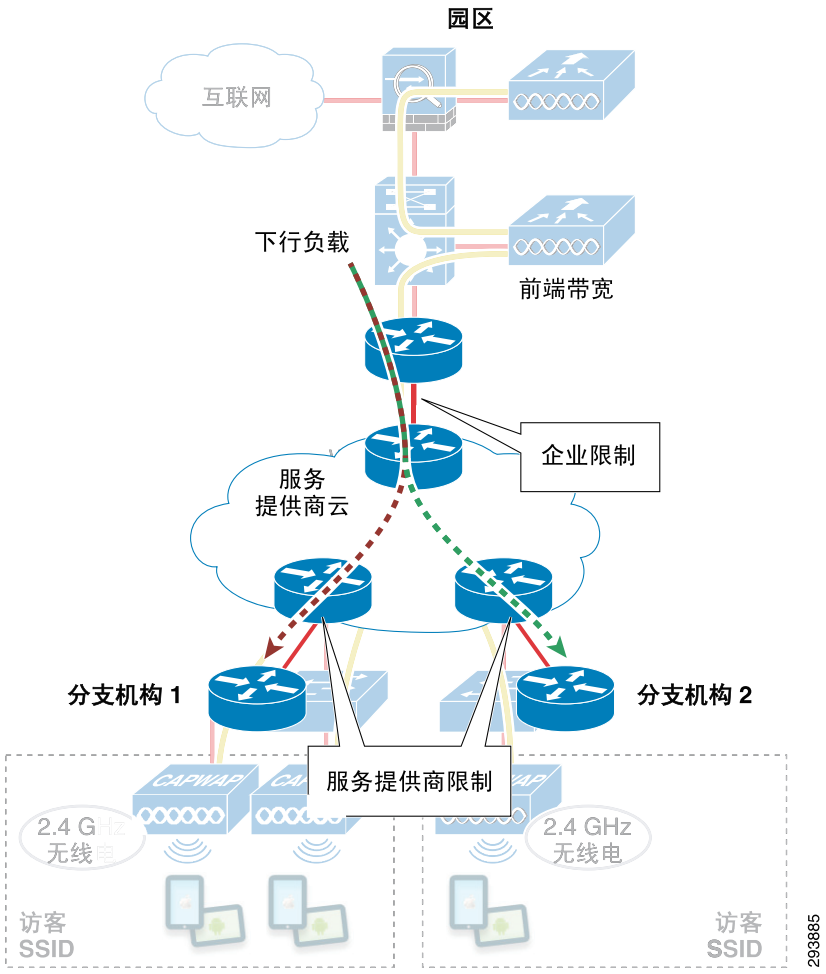
- Maximum Priority - 限制可以由支持 WiFi 多媒体 (WMM) 的无线客户端发送的最大 802.11 用户优先级标记。此参数的使用表示 SSID 被配置为支持 WMM。
- Unicast Default Priority - 设置从不支持 WMM 的无线客户端设备发送的流量的默认 802.11 用户优先级标记。
- Multicast Default Priority - 设置组播流量的默认 802.11 用户优先级标记。

然后，使用 802.11 用户优先级值设置在接入点和 CUWN 无线控制器之间的 CAPWAP 隧道内封装的流量的外部 DSCP 值。如上所示，默认用户优先级设置为最优，映射到 DSCP 0。因此在本例中，在所有传输到分支机构的 CAPWAP 流量中，大多数标记为 DSCP 0 的数据包很可能属于访客用户。这有助于区分访客流量和企业流量。

注意　网络管理员应该注意，Bronze QoS 配置文件的默认用户优先级设置为 Background。因此，如果网络管理员希望将访客流量设置为映射到 DSCP 8 （与 Scavenger 类的 CS1 对应）的较低 Background 用户优先级，可以通过将访客 SSID 分配到 Bronze QoS 配置文件来实现。网络管理员应考虑到组织的业务需求，以便确定应将访客流量考虑为 Best Effort 还是 Background。或者，网络管理员可以将 Silver QoS 配置文件的默认设置更改为 Background。但是，由于只有四个 QoS 配置文件可应用到 CUWN 无线控制器中配置的所有 SSID，因此，更改默认设置不一定是最佳解决方案。

在下行路径的两个位置，访客用户所带来的负荷可能影响企业流量。它们分别是网域网聚合路由器的出站接口以及与分支机构相邻的 PE 路由器上的出站接口。图 13-43 重点展示了下行方向中需要关注的区域。

图 13-43　　下行堵塞点



前面部分讨论的每 SSID 速率限制不会直接控制分支机构访客用户造成的 WAN 聚合前端上的负荷。访客负荷与托管访客 SSID 的分支机构 AP 总数乘以 WLAN 每 SSID 速率限制成比例。访客无线流量可能不同于其他 WAN 流量，因为它将在 CAPWAP 隧道中并使用默认 DSCP 设置进行标记。如果将相同的 QoS 配置文件应用到专用调配 SSID，来自员工自注册个人设备的部分流量也将使用同一方法标记。但是百分比很小。可以构建一个策略，使用默认 DSCP 值将 CAPWAP 数据包标记为 scavenger 类。这样便有将访客流量设置为低于默认企业流量优先级的效果。当 WAN

聚合线路的带宽开始饱和时，此策略将允许丢弃企业流量之前的无线访客流量。如果自注册流量也与访客流量一起被丢弃，则员工需要等待，直至 WAN 负荷降低，然后才能向网络中加入新设备。此过程的实施使用 WAN 聚合路由器出站线路上的传统 QoS 策略。有时，可以在分支机构上行链路上使用相同的方法，来管理分支机构 AP 数量不合理地超订用上行链路的情况。

由于存在访客流量，指向分支机构的服务提供商本地链路也可能会欠载。执行基于应用的流量控制后，每 SSID 速率限制确实可以限制有效访客带宽，从而帮助此方向的分支机构 WAN 链路。基于 TCP 的应用便是一个示例，该应用会管理流量，使丢弃最小化。即使下行方向的每 SSID 速率限制可在指向终端站的无线电中应用，客户端应用将节流以满足整个路径的可用速率。如果使用积极的策略器来执行约定的速率， SP PE 路由器上的最后一跳接口也会有助于应用限制。假设无线访客被重新标记为 scavenger，且已使用相应的 DSCP 到 EXP 映射，则 SP 策略器应该会不成比例地影响无线访客 TCP 应用。虽然访客互联网流量很少使用 UDP，它通常也会显示出与 TCP 相同的流量控制行为，即使协议自身不将反馈作为传输层的一部分实施。这是因为 UDP 通常是基于事务的。当 UDP 用于批量传输时，应用 （如 TFTP）会对数据块进行编号和确认。发射器不会发送数据块，直到接收器确认收到上一个数据块为止。如果数据块已丢弃，发射器将等待时间超时，然后再重新传输上一个数据块。基于 UDP 应用的流量控制有两个例外，是不使用 RTSP 监控已收数据的基于 UDP 的 IP 视频监控，以及 UDP 组播。两者都不是访客将在互联网上使用的典型应用。无论如何，每 SSID 速率限制是管理 SP PE 路由器上访客流量的有效方法。

管理丢失或被盗设备

修订日期：2013 年 8 月 7 日

当先前调配的设备丢失或被盗时，必须拒绝该设备的访问权限以防止对网络进行未经授权的访问。

对丢失或被盗设备的第一层防护是执行 PIN 锁定，该 PIN 是一个密码，用于解锁在短暂处于不活动状态 （通常是五到十秒）后自动锁定的设备。也可以采用更有效的方式，即在一定次数的密码尝试失败后清除移动设备上的所有数据，或执行有选择的擦除。可以结合使用 Cisco ISE 和移动设备管理器来实施此规则和其他规则。

Cisco ISE 可以通过多种方式来防止丢失或被盗设备连接到网络。员工可通过 “我的设备门户” 将设备标记为丢失并防止他人使用该设备进行未经授权的访问。此外，如果被标记为丢失的设备连接到网络， ISE 可能发出更改授权 (CoA) 以强制该终端断开网络。

管理员还可以将设备加入黑名单并强制该终端断开网络。此外，管理员还可以使用终端保护服务 (EPS) 隔离终端使其无法访问网络。

员工和管理在阻止丢失或被盗设备方面具有不同的能力：

员工：

从 “我的设备门户”：

- 报告设备丢失。
- 通过 MDM 实施 PIN 锁定。
- 通过 MDM 启动远程设备擦除。
- 恢复设备的访问能力，而无需重新注册设备。

注 已完全擦除的设备无法由 ISE 恢复，需要重新注册以恢复证书和 WiFi 配置文件。

管理员：

- 将终端添加到黑名单身份组。
- 如果终端已连接，则使用 “显示实时会话” 屏幕强制其断开网络。
- 通过 ISE 中的终端屏幕执行 PIN 锁定。
- 通过 ISE 中的终端屏幕启动远程设备擦除。
- 使用 ISE 的终端保护服务功能隔离终端 （员工无法恢复由管理员隔离的终端）。
- 撤销设备的数字证书。
- 禁用 RSA SecurID 令牌。

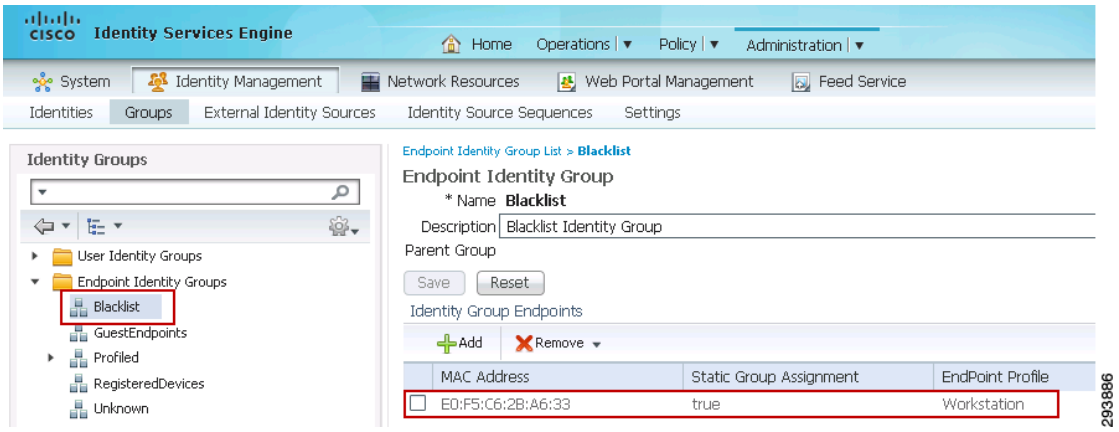
黑名单身份组

黑名单身份组由系统生成并由 ISE 维护以防止访问丢失或被盗的设备。在本设计指南中，使用两个授权配置文件对黑名单中的无线和有线设备执行权限：

- Blackhole WiFi Access
- Blackhole Wired Access

要显示黑名单身份组，请点击 **Administration > Identity Management > Groups > Endpoint Identity Groups**。图 14-1 显示了包含一个终端的空黑名单身份组。

图 14-1　　黑名单身份组

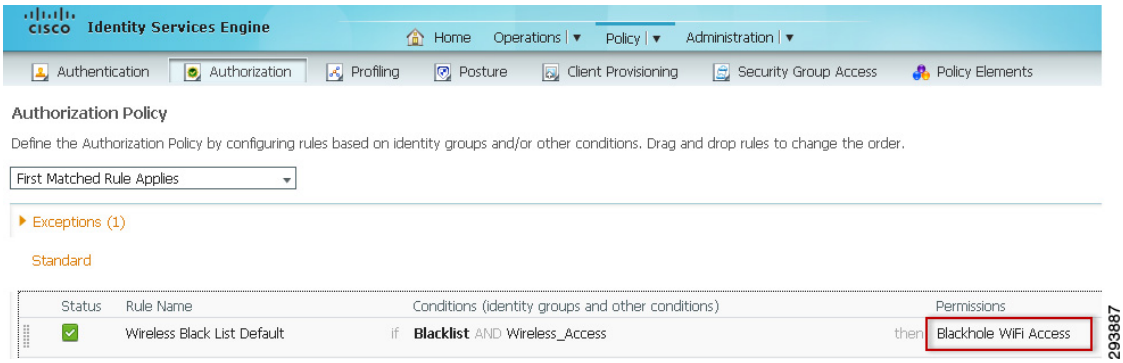


已列入黑名单的设备会分配给黑名单身份组。有线和无线设备都可以放入黑名单身份组中。授权配置文件用于定义对列入黑名单的设备授予的访问权限。已列入黑名单的设备的连接请求会被重定向到一个网页，该网页通知用户该设备已列入黑名单。

将无线设备列入黑名单

为了实施黑名单权限，在 **Policy > Authorization** 下定义了授权规则。图 14-2 显示了用于实施 Blackhole WiFi Access 权限的无线黑名单默认规则。

图 14-2　　无线黑名单默认授权规则

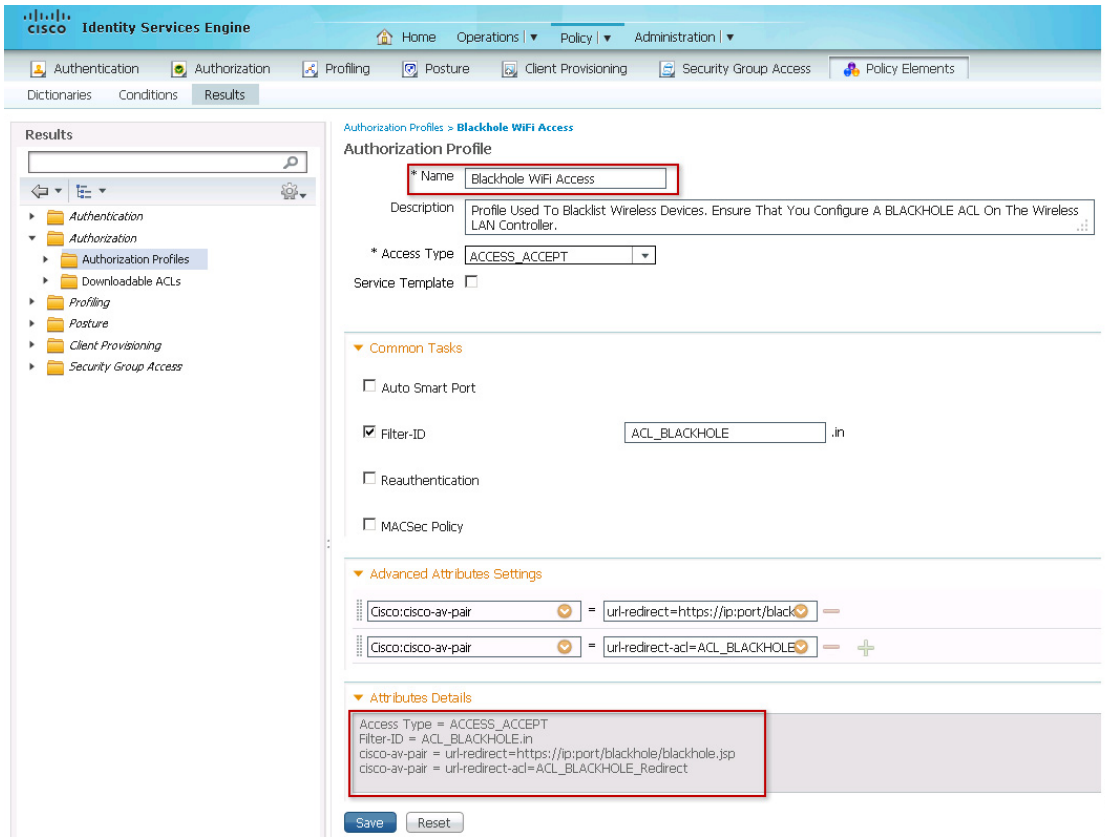


Blackhole WiFi Access 授权配置文件在 **Policy > Policy > Elements > Results > Authorization Profiles** 下配置，如图 14-3 中所示。访问类型被定义为 ACCESS_ACCEPT，且定义了下列 cisco-av-pair：

- cisco-av-pair：url-redirect=https://ip:port/blackhole/blackhole.jsp。当设备在黑名单身份组中时，用户被重定向到此页面。
- cisco-av-pair：url-redirect-acl=ACL_BLACKHOLE_Redirect。必须对无线 LAN 控制器配置一个名为 ACL_BLACKHOLE_Redirect 的 ACL，以便重定向能够在园区中正常工作且 FlexConnect ACL 在具有相同名称的分支机构中正常工作。

此授权配置文件只允许访问 ISE 的 “未经授权的网络访问”页面，以便告知用户该设备对网络的访问被拒绝。

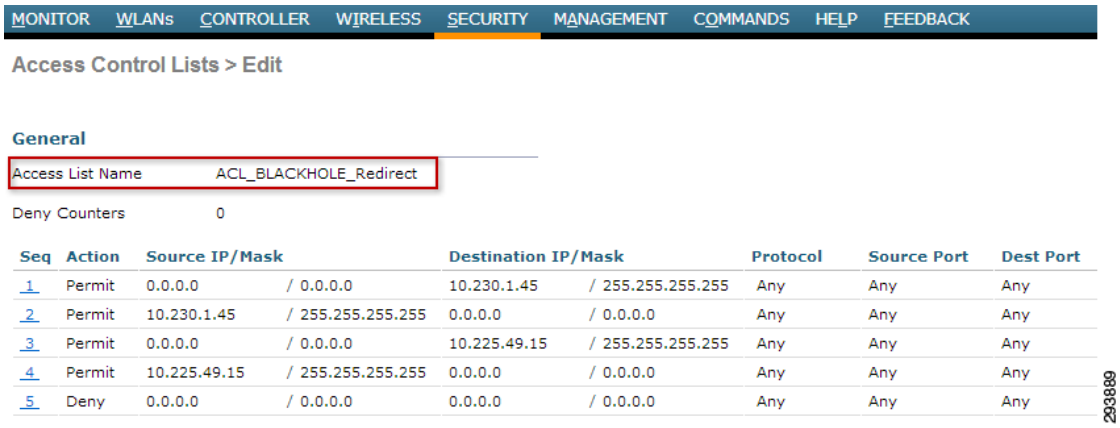
图 14-3　　Blackhole WiFi Access 授权配置文件



授权配置文件中两个 ACL 的行为在 CUWN 无线控制器 （如 CT5508 和 Flex 7500）和基于 IOS XE 的控制器 （如 CT5760 和 Catalyst 3850）中稍有不同。对于 CUWN 无线控制器，ACL_BLACKHOLE_Redirect 既充当用于控制网络重定向的 ACL，也充当用于控制哪个无线客户端获准访问网络的 ACL。

图 14-4 显示如何在 CUWN WLC 中定义 ACL_BLACKHOLE_Redirect 访问列表以只允许访问 ISE 和 DNS 服务器。通过授予对 DNS 和 ISE 的访问权限，终端能够访问在 ISE 上托管的 blackhole.jsp 网页。

图 14-4　ACL_BLACKHOLE_Redirect ACL



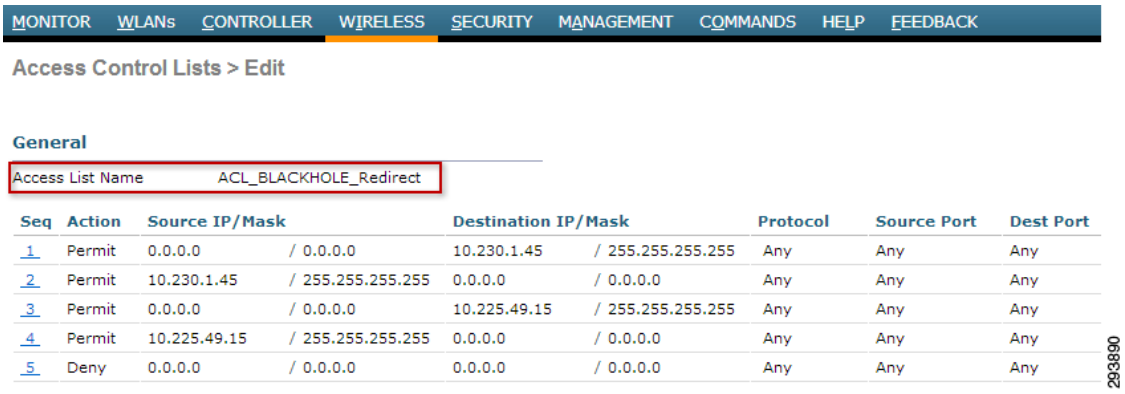
ACL 指定以下访问权限：

- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 拒绝以所有其他地址作为源 / 目标的访问。

注意　ACL_BLACKHOLE 只充当一个额外的安全配置。当指定了 URL 重定向时， CUWN 无线控制器不使用此 ACL。对于 CUWN 无线控制器， ACL_BLACKHOLE ACL 可以与 ACL_BLACKHOLE_Redirect ACL 相同。

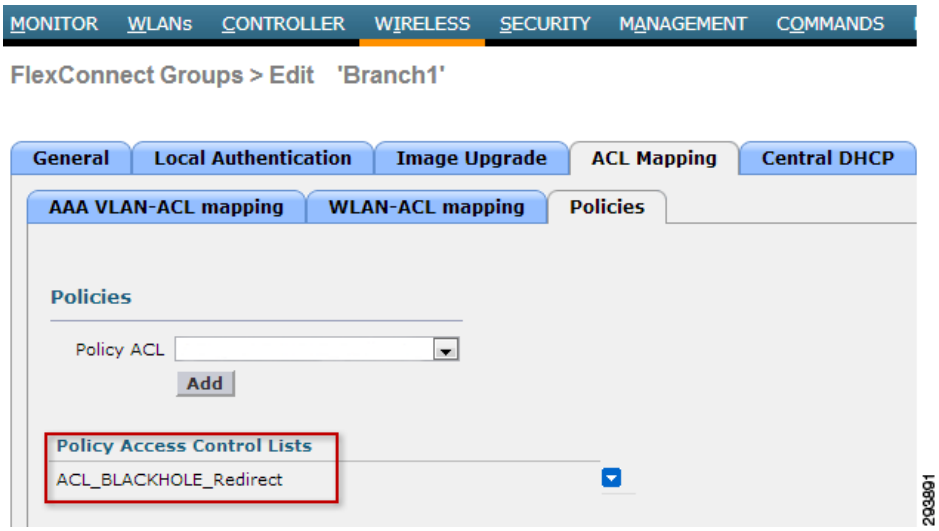
对于连接到分支机构的终端，定义一个类似的 FlexConnect ACL 并将其应用于 FlexConnect 组。图 14-5 显示了 ACL_BLACKHOLE_Redirect FlexConnect ACL。此 ACL 类似于如上所示的用于园区设备的 ACL，不同之处在于此 ACL 在 **Security > Access Control Lists > FlexConnect ACLs** 下定义。

图 14-5　ACL_BLACKHOLE_Redirect FlexConnect ACL



要应用来自分支机构的此 FlexConnect，请选择相应的 FlexConnect 组并点击 **Policies** 选项卡。添加 ACL_BLACKHOLE_Redirect ACL，如图 14-6 中所示。

图 14-6　　Branch1 的策略



在融合接入产品 （即 CT5760 无线控制器或 Catalyst 3850 系列交换机）上，必须配置 BLACKHOLE_ACL_Redirect 和 BLACKHOLE_ACL ACL。BLACKHOLE_ACL_Redirect ACL 的示例如下所示。

```
!
ip access-list extended ACL_BLACKHOLE_Redirect/ 重定向 ACL 的黑名单
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit ip any any
!
```

上述 ACL 指定了以下访问权限：

- 拒绝 DHCP 访问 （bootpc 和 bootps）。
- 拒绝以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 拒绝以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 允许 （重定向）所有其他 IP 访问。

以上 ACL 会将从任何源到任何目标的任何网络流量（HTTP 或 HTTPS）重定向到在 Cisco ISE 中列入黑名单的设备网页。

授权配置文件还将另一个由 Radius 指定的本地 ACL (BLACKHOLE_ACL) 应用于 WLAN 以控制网络访问。CT5760 和 Catalyst 3850 设计使用命名 ACL。ACL 的名称会通过 Airespace 字典中的 RADIUS Airespace-ACL-Name 属性值对从 ISE 发送到 Catalyst 3850 系列交换机或 CT5760 无线控制器。具体的示例格式如下：

```
Airespace-ACL-Name = ACL_BLACKHOLE
```

WLAN 访问控制 ACL (ACL_BLACKHOLE) 确定在 WLAN 上 Catalyst 3850 系列交换机或 CT5760 无线 LAN 控制器允许哪些流量。 BLACKHOLE_ACL ACL 的示例如下所示。

```
!
ip access-list extended ACL_BLACKHOLE/ 访问控制 ACL 黑名单
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
!
```

上述访问列表指定以下访问权限：

- 允许 DHCP 访问 （bootpc 和 bootps）。
- 允许以 DNS 服务器 (10.230.1.45) 作为源 / 目标的 IP 访问。
- 允许以 ISE 服务器 (10.225.49.15) 作为源 / 目标的 IP 访问。
- 隐式拒绝所有其他 IP 访问。

上面的 ACL 允许将来自任何源的流量重定向到在 Cisco ISE 中列入黑名单的设备网页。

一旦设备位于黑名单身份组中，该设备以后尝试连接到网络都将被拒绝。当用户在已列入黑名单的设备上打开一个 Web 浏览器时，会话会被重定向至图 14-7 中所示的页面。

图 14-7　　未经授权的网络访问

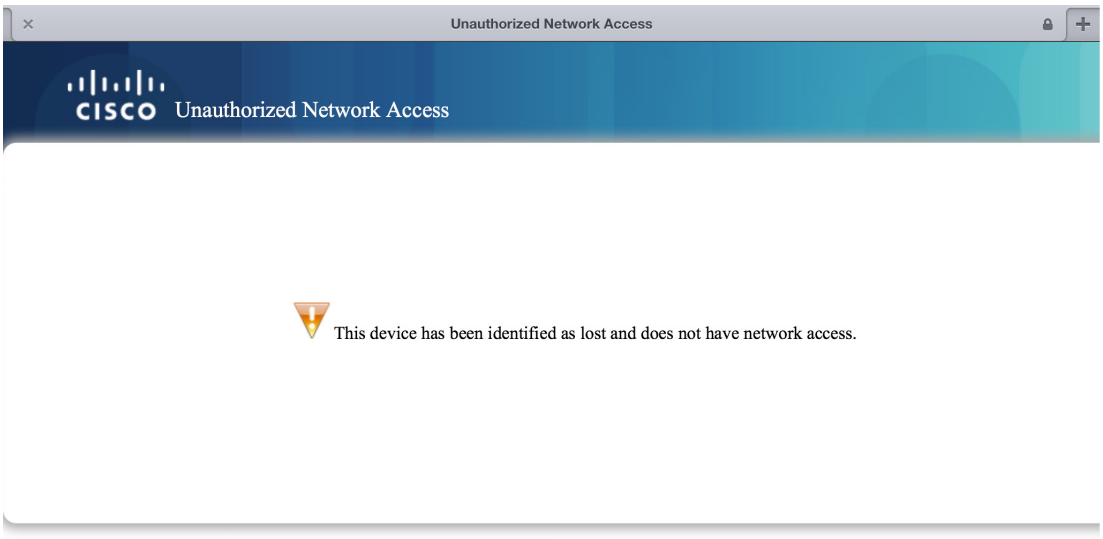
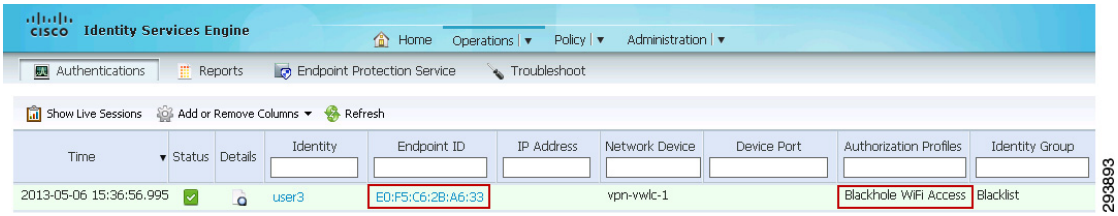


图 14-8 显示了已列入黑名单的设备如何尝试连接到网络以及如何应用 Blackhole WiFi Access 授权配置文件。

图 14-8　　黑名单身份组中的设备



黑名单有线设备

当有线设备列入黑名单时的用户体验与已列入黑名单的无线设备的体验类似。对于自带设备中通过融合接入产品和通过其他 Catalyst 交换机连接的设备，将自注册有线设备列入黑名单的 ISE 授权策略规则是相同的。如果设备已列入黑名单且用户尝试访问任何网页，该设备将重定向到门户，以告知用户该设备为丢失设备。以下步骤显示如何实现此行为：

步骤 1　创建仅允许访问 ISE 的 ACL_BLACKHOLE 可下载的 DACL。

步骤 2　在接入层交换机上创建一个名为 ACL_BLACKHOLE_Redirect 的 URL 重定向 ACL，它匹配所有的 HTTP 或 HTTPS 流量。

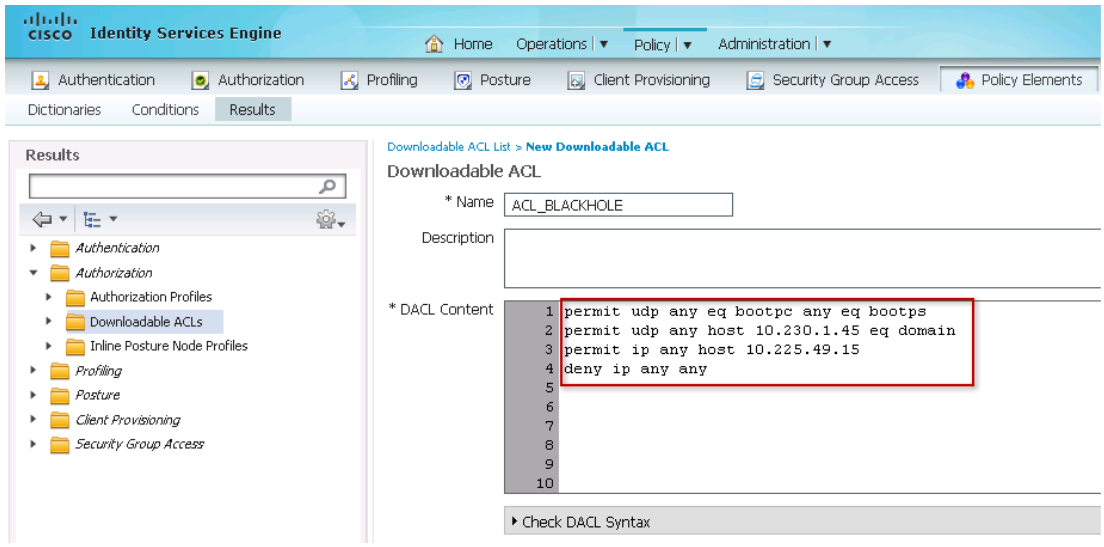
步骤 3　创建一个 Blackhole Wired Access 授权配置文件，用于将 DACL 和重定向链路推送到交换机。

步骤 4　在授权策略中定义一个新规则，该规则匹配已列入黑名单的设备并分配授权配置文件 Blackhole Wired Access 。

在 ISE 上创建一个可下载的 ACL

ACL_BLACKHOLE DACL 在 **Policy > Policy Elements > Results > Downloadable ACLs** 下创建，如图 14-9 中所示。

图 14-9　　ACL_BLACKHOLE DACL



上面的 ACL 允许将来自任何源的流量重定向到在 Cisco ISE 中列入黑名单的设备网页。

在交换机上创建 URL REDIRECT ACL

无论交换机是融合接入 Catalyst 3850 系列交换机还是 Catalyst 3750-X 系列交换机， URL 重定向 ACL 的配置都是相同的。有线交换机上 ACL_BLACKHOLE_Redirect ACL 的配置示例如下所示。

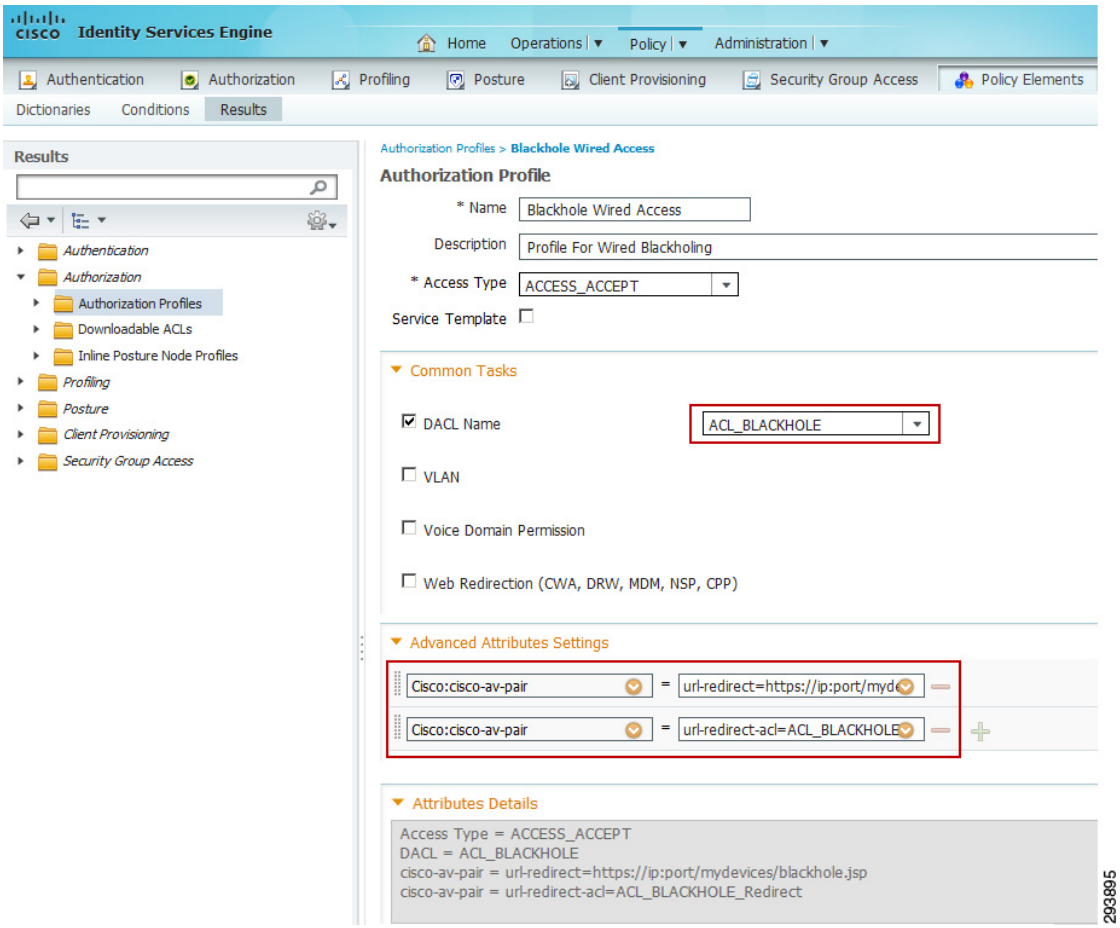
```
!
ip access-list extended ACL_BLACKHOLE_Redirect   / 重定向 ACL 黑名单
 udp any eq bootpc any eq bootps
 udp any host 10.230.1.45 eq domain
 ip any host 10.225.49.15
 permit ip any any
```

请注意，这就是上述用于 Catalyst 3850 系列交换机的黑名单无线设备的同一个 URL 重定向 ACL。请牢记，仅 Catalyst 3850 上需要 ACL， CT5760 无线控制器上并不需要，因为只有 Catalyst 3850 支持通过其交换机端口直接连接有线客户端。

配置授权配置文件

在 **Policy > Policy Elements > Results > Authorization Profiles** 下定义名为 Blackhole Wired Access 的授权配置文件，如图 14-10 中所示。

图 14-10　Blackhole Wired Access 授权配置文件



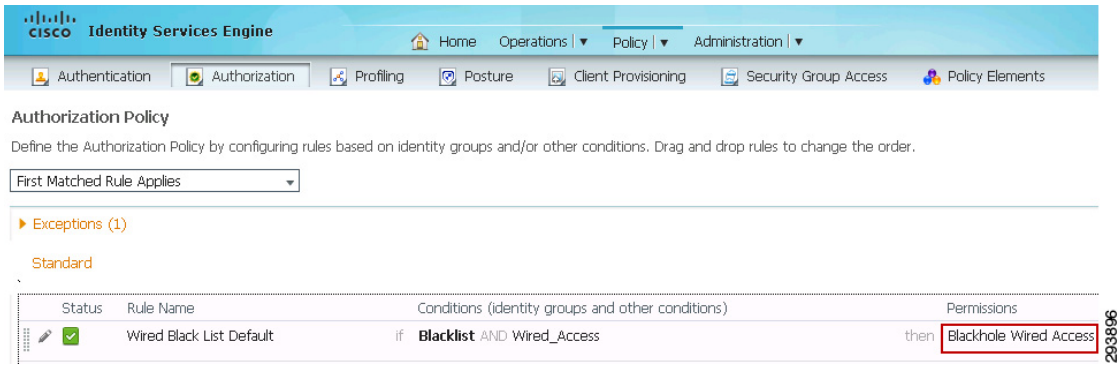
定义了下列 cisco-av-pair：

- cisco-av-pair：url-redirect=https://ip:port/mydevices/blackhole.jsp。当设备在黑名单身份组中时，用户被重定向到此页面。
- cisco-av-pair：url-redirect-acl=ACL_BLACKHOLE_Redirect。必须对接入层交换机定义一个名为 ACL_BLACKHOLE_Redirect 的 ACL，重定向才能正常工作。

在授权策略中创建一个规则

最后一个配置步骤是在授权策略中创建一个新规则，当该规则与列入黑名单的 dot1x 有线设备匹配时，它会使用在上面创建的 Blackhole Wired Access 授权配置文件。图 14-11 显示了该规则。

图 14-11　有线黑名单默认值



一旦定义了规则，将拒绝列入黑名单的有线设备访问网络。

员工的 “我的设备门户”

员工可以使用 “我的设备门户” 将设备标记为丢失，以防它们继续访问网络。该门户要求进行用户身份验证，并显示员工已添加或注册的设备。可以通过以下 URL 访问 “我的设备门户”：

https://<*ISE_IP_Address*>:8443/mydevices/

除了用于报告丢失或被盗设备，该门户还用于通过 MDM 集成执行 MDM 操作，例如要求 PIN 锁定和设备擦除。图 14-12 显示了 “我的设备门户” 页面。

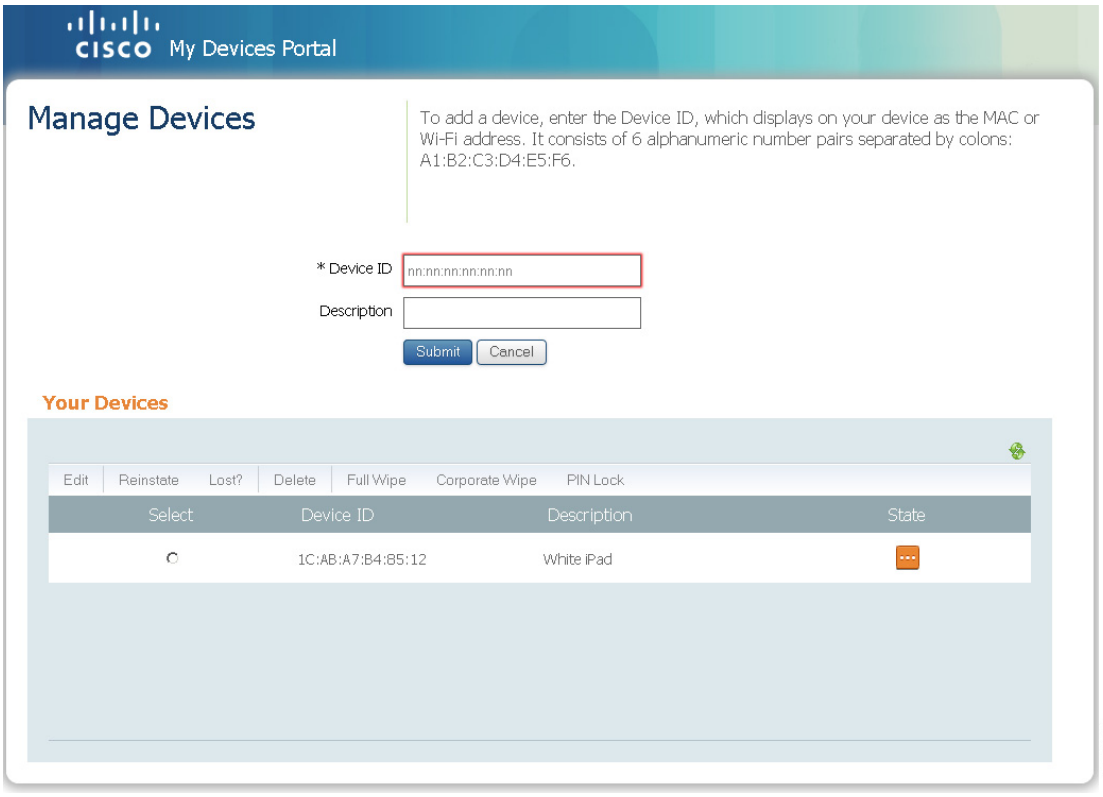
图 14-12　我的设备门户

该门户显示分配给员工的设备或以前使用自助注册门户注册的设备。

报告设备丢失

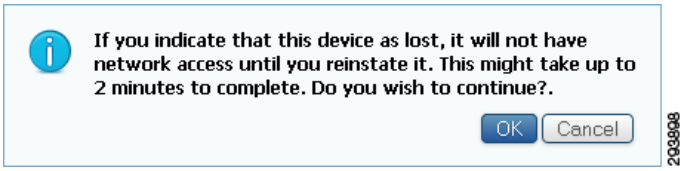
员工可以编辑设备的说明并报告设备丢失，如图 14-13 中所示。

图 14-13　　丢失的设备



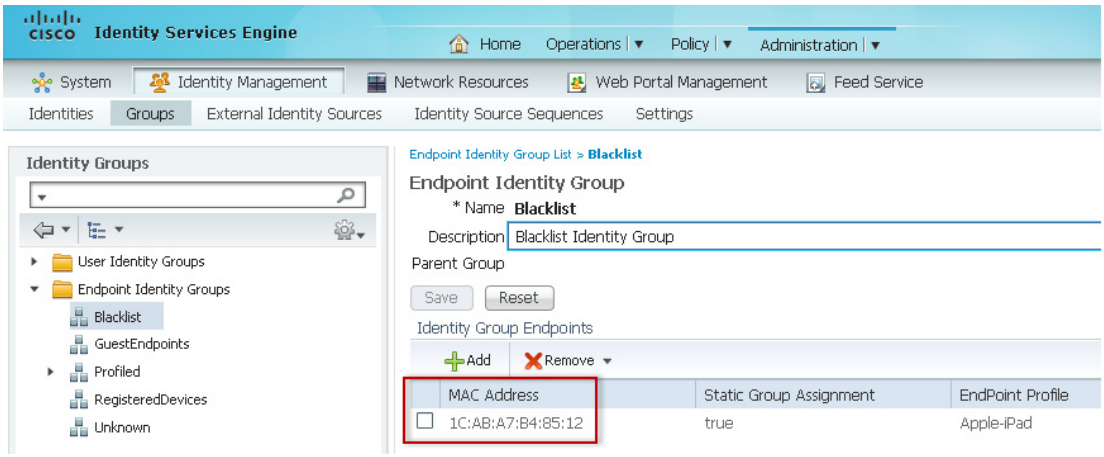
在将设备加入黑名单之前， ISE 显示如图 14-14 中所示的警告。

图 14-14　　黑名单警告



一旦设备被标记为丢失，该设备就被添加到黑名单身份组中。如果此时设备连接到网络， ISE 会发出授权更改 (CoA) 并强制设备断开网络。要验证设备是否已添加到黑名单身份组，请点击 **Administration > Identity Management > Groups > Endpoint Identity Groups** 并查看黑名单。图 14-15 显示 MAC 地址已添加到黑名单。

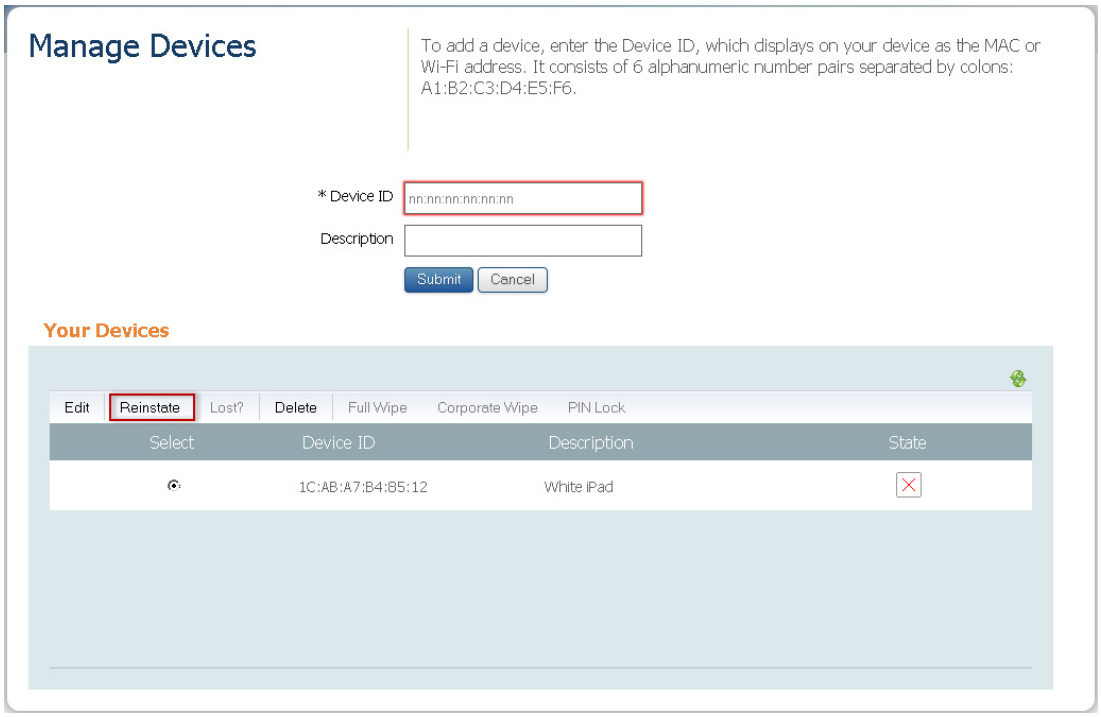
图 14-15　　黑名单身份组



恢复设备

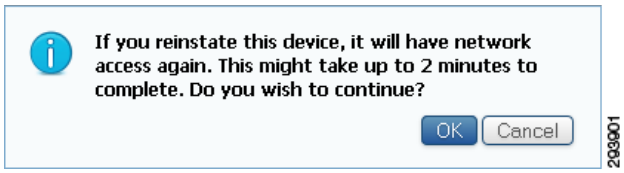
“我的设备门户”还使用户能够恢复已列入黑名单的设备，允许设备重新获得对网络的访问权限。图 14-16 显示了恢复 (Reinstate) 选项。

图 14-16　　恢复设备



在恢复设备之前， ISE 显示如图 14-17 中所示的警告。

图 14-17　　恢复警告



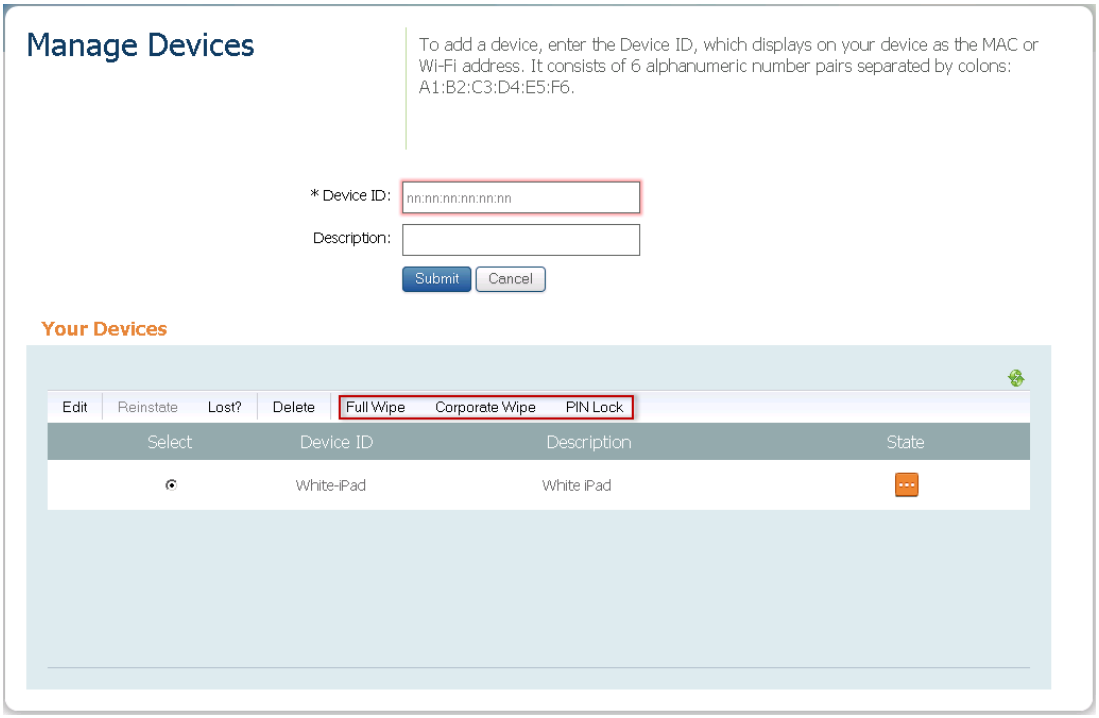
PIN 锁定和设备擦除

与 MDM 的集成使用户对设备具有更多的控制能力。使用 “我的设备门户”，员工能够：

- 启动企业擦除 - 删除在 MDM 策略中配置的设置和应用。
- 启动完全擦除 - 删除设备的所有信息 （出厂重置）。
- 实施 PIN 锁定 - 锁定设备。

图 14-18 显示了可从 “我的设备门户” 执行的 MDM 操作：

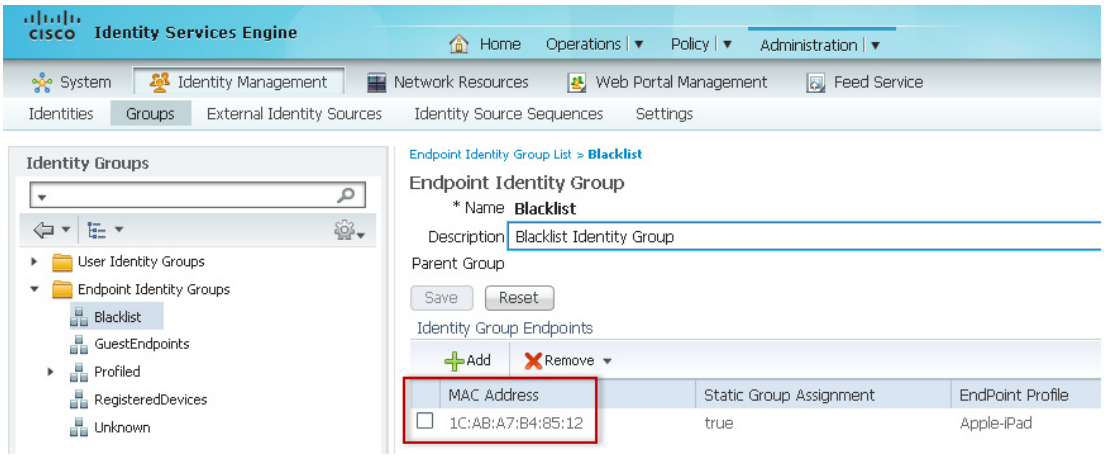
图 14-18　　从 “我的设备门户” 执行的 MDM 操作



管理员 - 将设备列入黑名单

管理员可以通过手动将设备添加到黑名单身份组来将其列入黑名单。点击 **Administration > Groups > Endpoint Identity Groups > Blacklist** 并添加要列入黑名单的设备的 MAC 地址。图 14-19 显示了已添加到身份组的 MAC 地址。

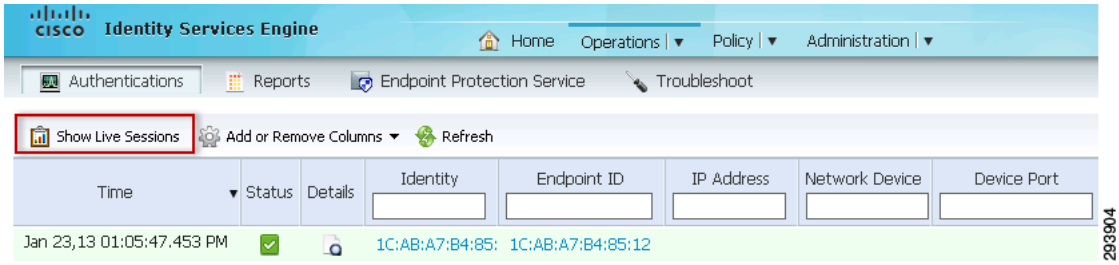
图 14-19　要列入黑名单的设备



请注意，通过将设备添加到黑名单身份组， ISE 可以防止以后连接到网络，但如果用户当前已连接到网络，则需要执行一个额外步骤来强制终端断开网络。

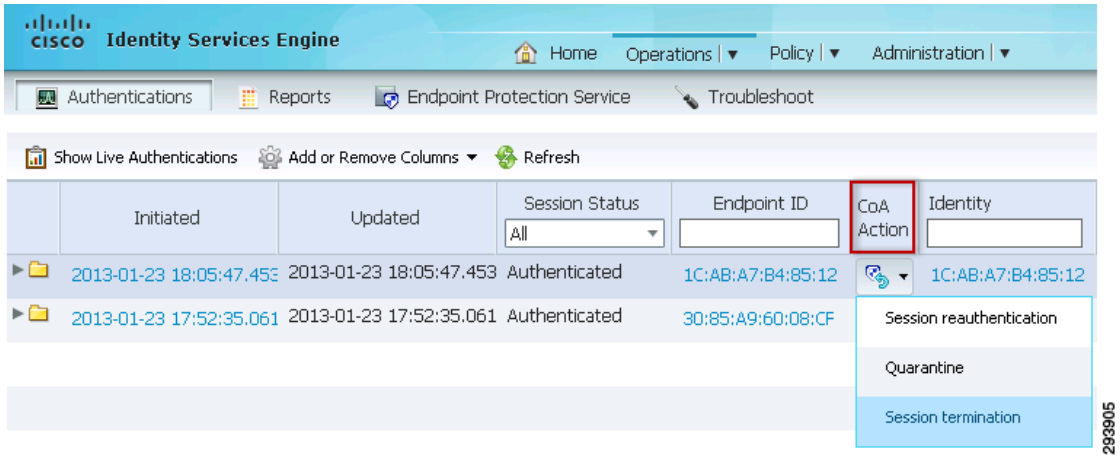
要强制设备断开网络，请点击 **Operations > Authentications > Show Live Sessions**，如图 14-20 中所示。

图 14-20　显示实时会话



要终止终端的会话，请从“CoA Action”菜单中选择“Session termination”，如图 14-21 中所示。

图 14-21　会话终止

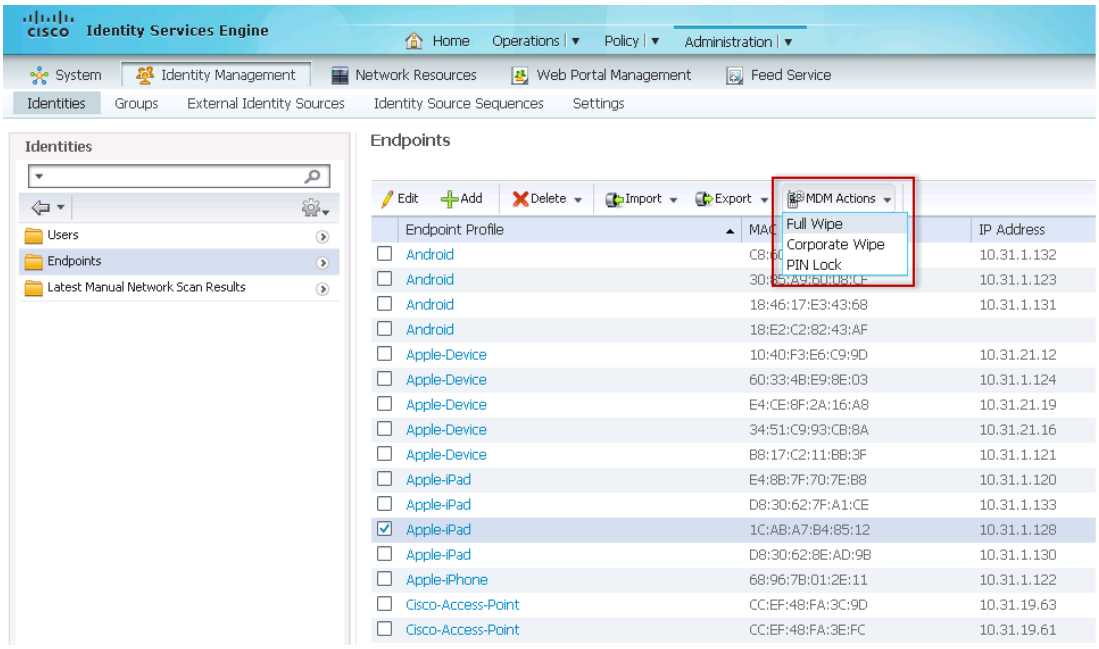


注意　员工可以选择使用 “我的设备门户” 来恢复由管理员列入黑名单的设备。

MDM 操作

管理员还可以选择在终端上执行 MDM 操作。要执行此操作，请点击 **Administration > Identities > Endpoints** 并选择适当的设备，如图 14-22 中所示。

图 14-22　　MDM 操作



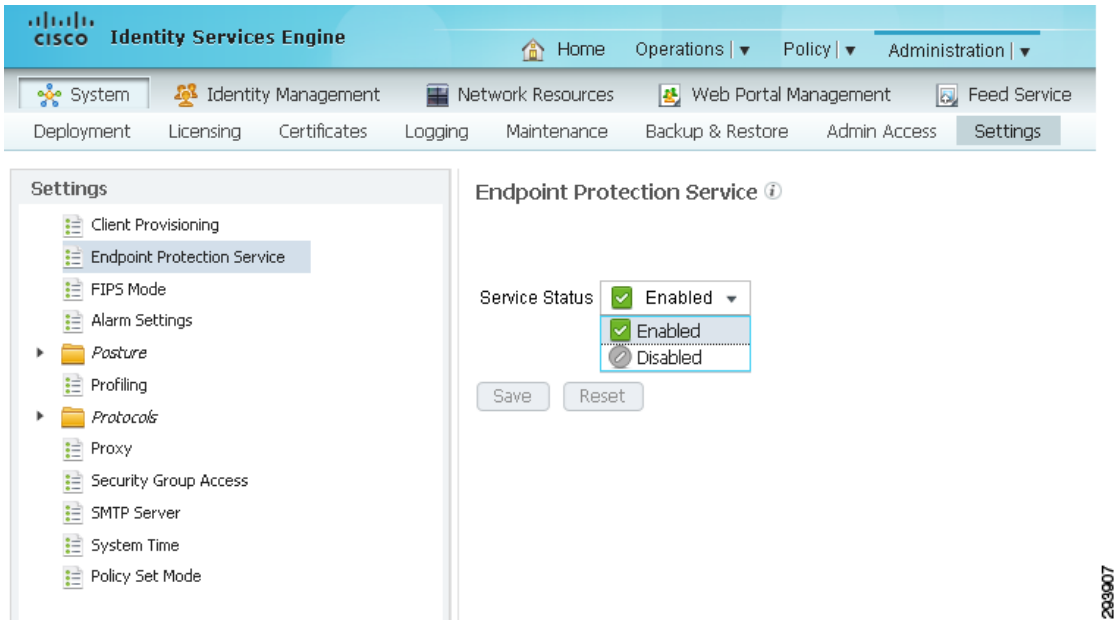
终端保护服务 (EPS)

终端保护服务是 ISE 提供的一项服务，用于扩展终端的监控和控制功能。 EPS 还监控和更改终端的授权状态。 EPS 可用于在不修改整体授权策略的情况下更改终端的授权状态。 EPS 允许管理员隔离设备 （即限制设备访问），以及取消隔离设备 （即允许完全访问网络以撤消隔离状态）。

注意　EPS 要求 ISE 高级许可证。

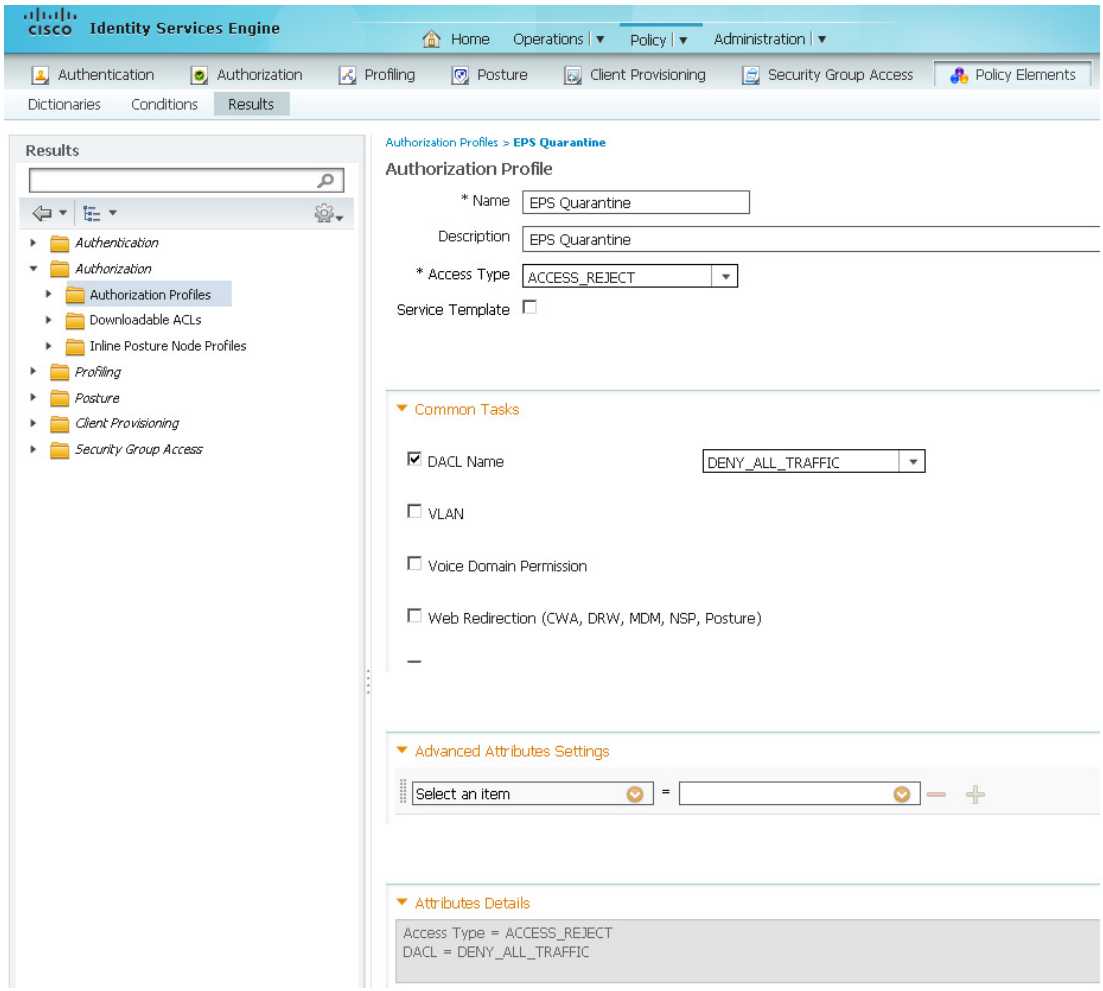
要启用 EPS，请点击 **Administration > System > Settings > Endpoint Protection Services** 并选择 **Enabled**，如图 14-23 中所示。

图 14-23　　启用 EPS



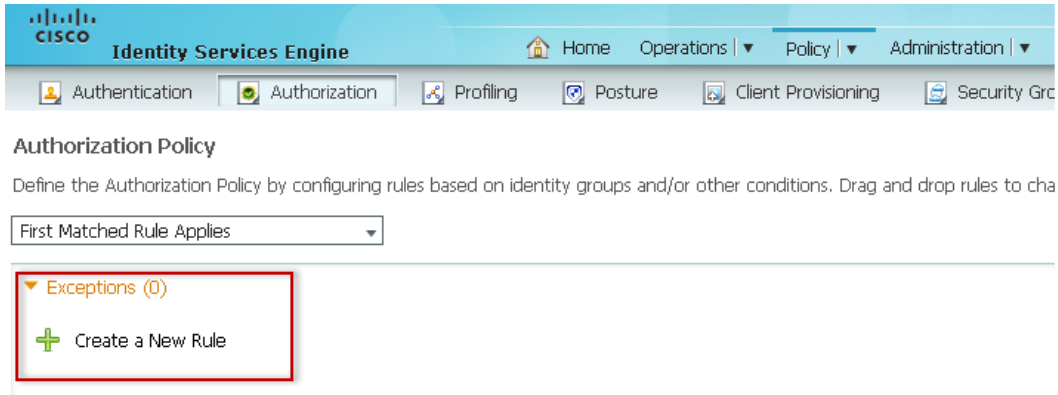
创建一个授权配置文件以定义对指定网络服务的权限。点击 **Policy > Policy Elements > Results > Authorization > Authorization Profiles** 并定义新的授权配置文件，如图 14-24 中所示。

图 14-24　　EPS_Quarantine 授权配置文件



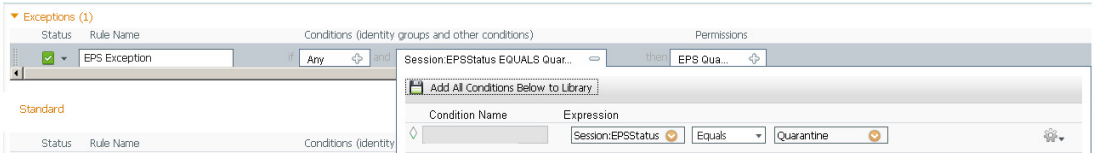
创建在处理标准策略之前要处理的 EPS 例外策略和规则。点击 **Policy > Authorization > Exceptions > Create a New Rule**，如图 14-25 中所示。

图 14-25　　EPS 例外策略



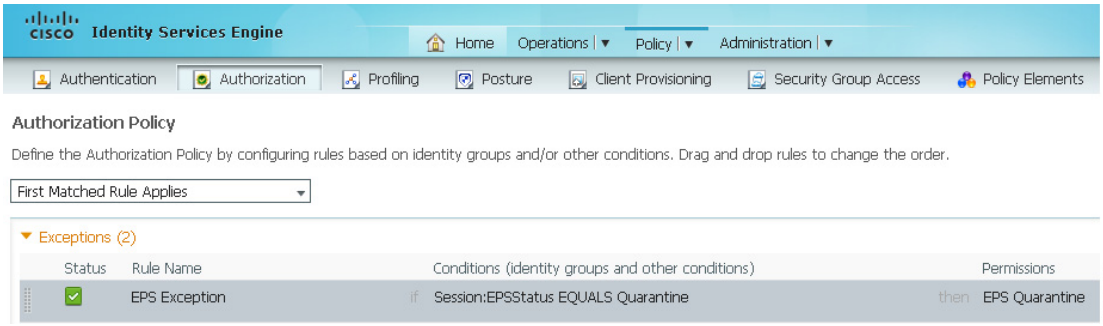
输入一个规则名称并在 Conditions 下创建一个新条件 (**Advanced Option**)。在 Expression 下，点击 **Select Attribute** 并选择 **EPSStatus Equals Quarantine**，如图 14-26 中所示。

图 14-26　　EPS 例外策略



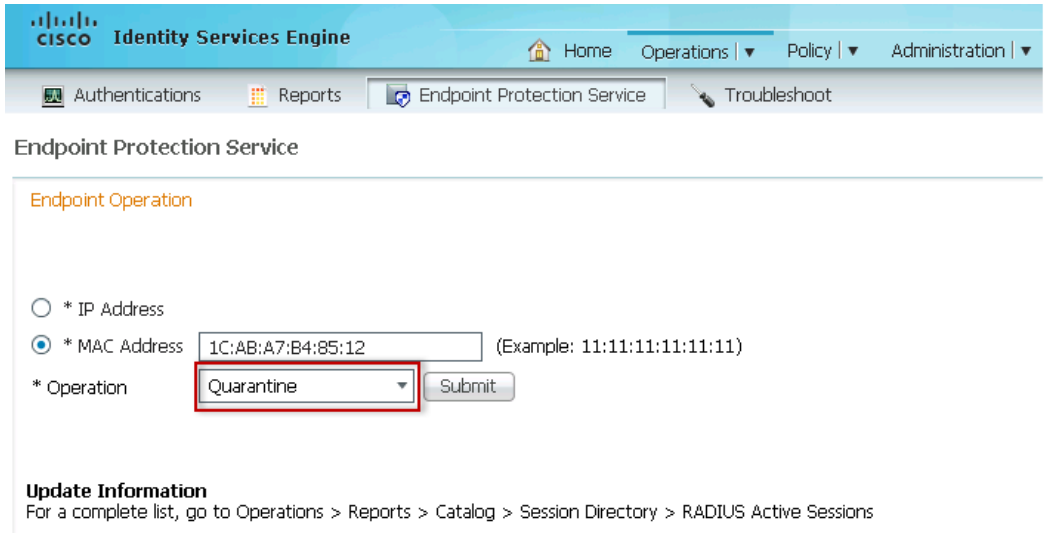
在 Permissions 下，选择先前定义的 **EPS_Quarantine** 授权配置文件。图 14-27 显示了完整的例外策略。

图 14-27　　EPS 隔离权限



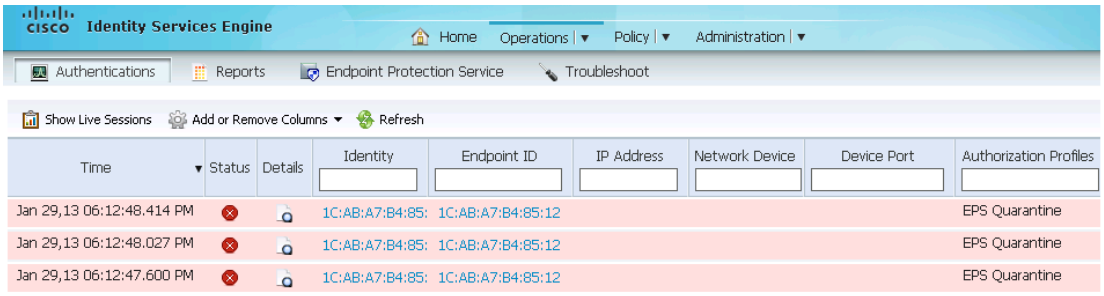
要隔离设备，请点击 **Operations > Endpoint Protection Service** 并输入要隔离的终端的 MAC 地址。在 Operation 下，选择 **Quarantine**，如图 14-28 中所示。

图 14-28　　EPS



当管理员点击 **Submit** 后，设备将被强制断开网络，而且将来的连接尝试也会被拒绝。图 14-29 显示了应用的 EPS_Quarantine 授权配置文件，以及设备如何被拒绝访问。

图 14-29　　隔离的终端

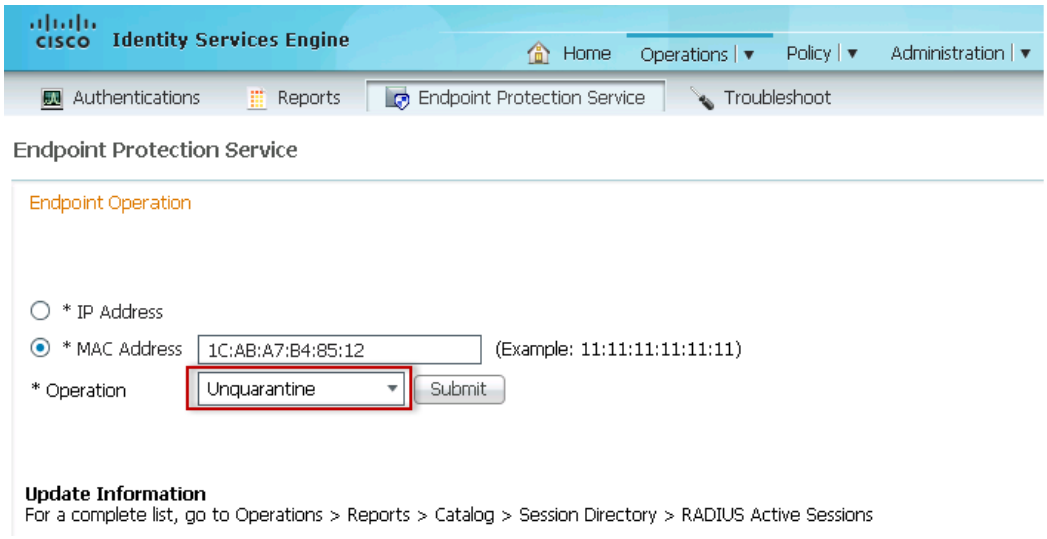


EPS 提供了一层额外的控制，以监控和更改终端的授权状态。

注意　因为 EPS 比列入黑名单的设备具有更高的优先级，员工无法选择恢复由管理员隔离的设备。

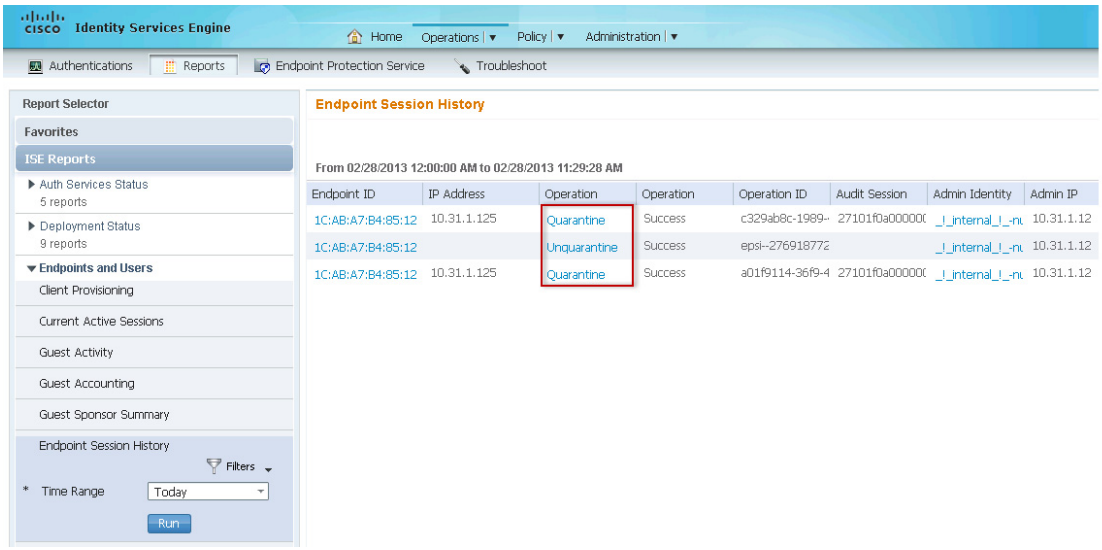
要隔离设备，请输入设备的 MAC 地址并从操作下拉菜单中选择 **Unquarantine**，如图 14-30 中所示。

图 14-30　　取消隔离设备



EPS 活动由 ISE 记录，并可通过点击 **Operations > Reports > Endpoints and Users > Endpoint Session History** 来查看。图 14-31 显示了一个包括终端信息的报告。

图 14-31　　EPS 日志

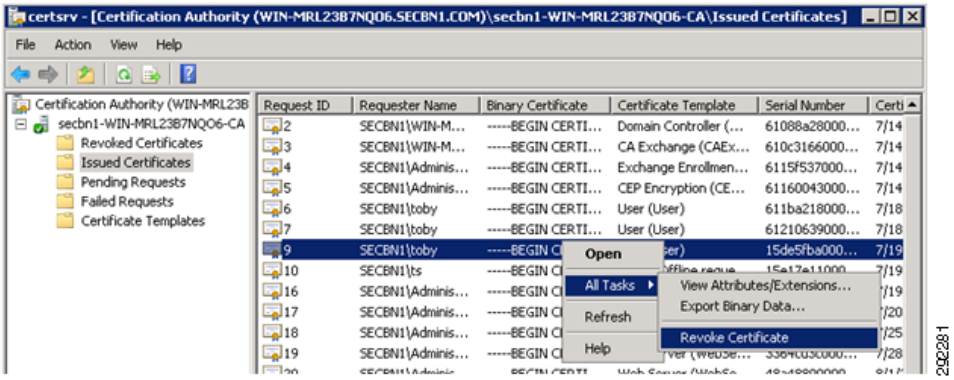


数字证书的吊销

管理员还可以选择吊销员工的由 CA 服务器颁发的数字证书，以防止将来未经授权的设备继续使用数字证书。 CA 服务器定期发布证书吊销列表 (CRL)。 ISE 被配置为根据 CRL 列表验证客户端提供的证书。如果存在匹配，则 ISE 拒绝客户端提供的数字证书。

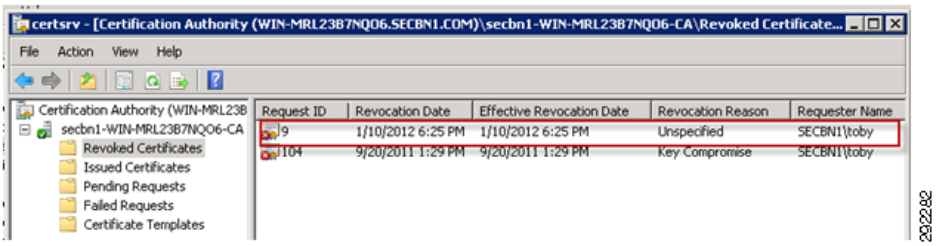
第一步是吊销 CA 服务器提供的数字证书。图 14-32 显示如何吊销用户名为 “toby” 的数字证书。

图 14-32　　吊销 CA 服务器上的数字证书



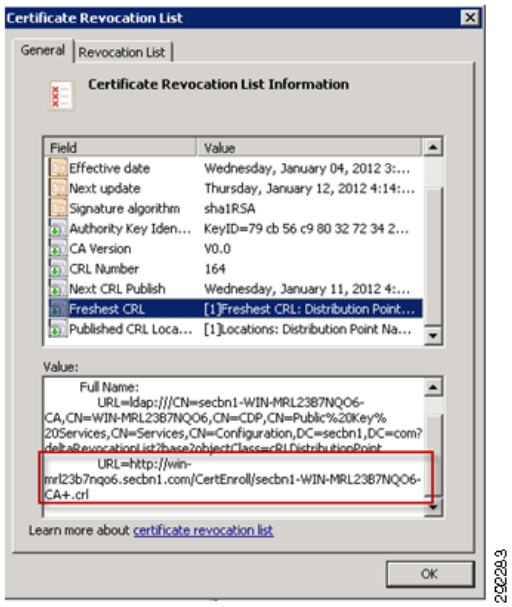
完成以上过程后，证书序列号将被添加到证书吊销列表 (CRL) 中。图 14-33 显示了 CRL 信息。

图 14-33　　证书吊销列表



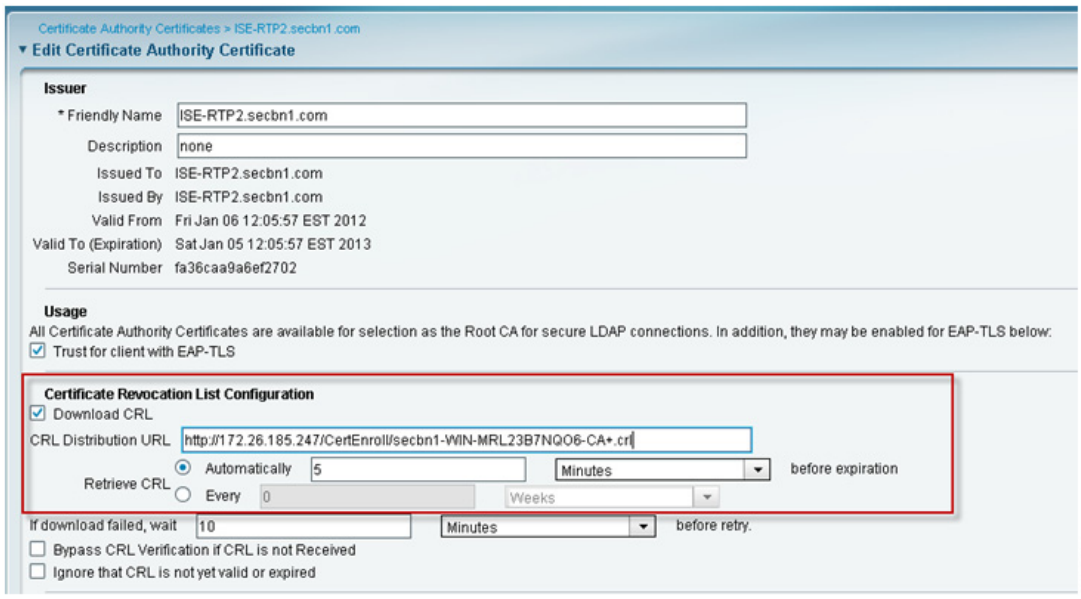
此信息由 CA 服务器定期发布。图 14-34 显示了 ISE 可下载列表的 CRL 的位置。

图 14-34　　CRL 分发点



下一步是用 CRL 分发位置配置 ISE，以便定期下载列表并将其与客户端提供的证书进行比较。点击 **Administration > Certificates > Certificate Authority Certificates** 并配置 CRL 值，如图 14-35 中所示。

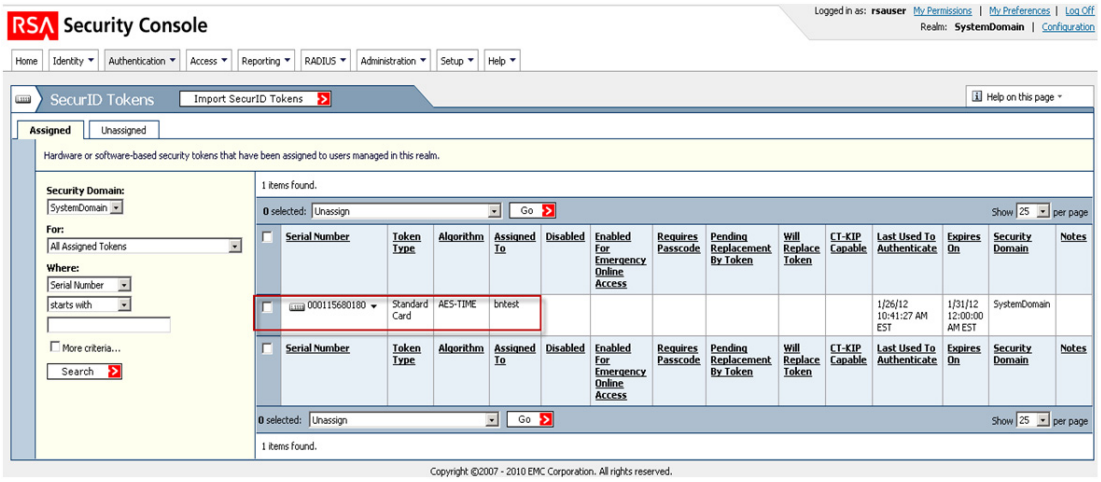
图 14-35　　ISE 上的 CRL 位置信息



禁用 RSA SecurID 令牌

当以前调配的设备丢失或被盗时，必须拒绝该设备的访问权限，以防止未经授权的网络访问。此外，必须在 RSA 服务器禁用远程用户的 RSA SecurID 令牌，使远程用户无法使用网络。图 14-36 显示了如何在 RSA 服务器上禁用 RSA SecurID 令牌。

图 14-36　　禁用 RSA SecurID 令牌



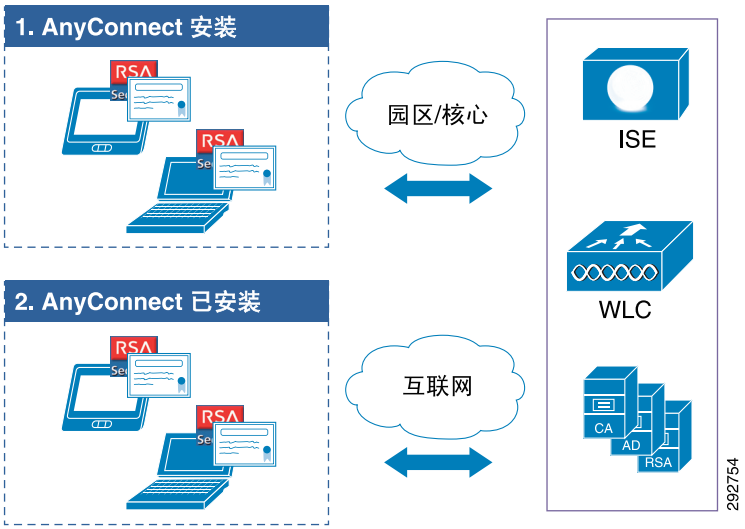
第 15 章

自带设备远程设备访问

修订日期：2013 年 8 月 7 日

自带设备设计应该能够适应各种尝试通过远程连接访问内部资源的设备。这些设备可以是工作站、平板电脑、智能手机，或者获准安全地连接到网络的任何其他设备。本设计使用 Cisco ASA 作为 VPN 网关来建立与远程终端的 SSL VPN 会话。 ASA 对用户的数字证书进行身份验证。然后，Cisco ISE 通过 RSA SecurID 令牌对用户进行身份验证。设备经过这两种身份验证才能访问网络。图 15-1 显示了远程设备访问所涉及的网络组件。

图 15-1　　远程设备网络组件



此设计基于以下假设来提供远程访问功能：

- 要远程连接到网络的设备必须是公司批准的设备。公司批准的设备是已经由 IT 组织调配了数字证书的设备。
- 设备必须在园区调配。调配过程包括：
  - 安装 AnyConnect 客户端
  - 配置 VPN 网关 IP 地址
  - 为用户设置一次性密码方案

  这些步骤必须先在园区位置完成，才能远程使用。此设计不允许对设备进行远程调配。
- 远程连接的设备需要经过双因素身份验证，这意味着用户应提供两种形式的凭证。

解决方案组件

提供远程客户端连接要用到以下组件：

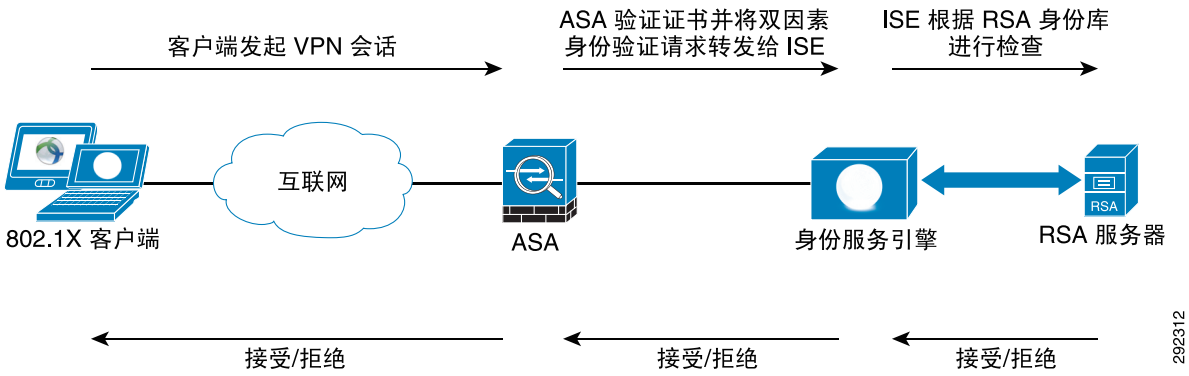
- 思科自适应安全设备 (ASA) - 作为 SSL VPN 集中器，用于终止 VPN 会话。
- Cisco AnyConnect - 用作在远程设备上安装的 VPN 客户端。
- 思科身份服务引擎 (ISE) - 作为外部身份源的中介，用于远程终端与 RSA 服务器之间的身份验证。令牌先从客户端转发到 ASA，然后从 ASA 转发到 ISE，继而从 ISE 转发到 RSA。
- RSA SecurID - 作为身份验证服务器，用于由客户端生成的令牌。

RSA SecurID

VPN 安全性的强度完全取决于在 VPN 连接的远程终端对用户 （和设备终端）进行身份验证的方法。基于静态密码的简单身份验证方式容易遭受密码 “破解” 攻击、窃听攻击甚至社会工程攻击。双因素身份验证由 “您知道的信息” 和 “您拥有的信息” 组成，是实现安全的公司网络远程访问的最低要求。有关详细信息，请参阅：
http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html。

本设计采用 RSA SecurID 身份验证服务器 7.1 和 RSA SecurID 硬件令牌来提供双因素身份验证。用户提供的密码是其秘密 PIN 和该时刻其令牌上实时显示的一次性密码 (OTP) 代码的组合。本设计除了采用 RSA SecurID （双因素身份验证），还部署和使用了 x.509 客户端数字证书。图 15-2 显示了 RSA 如何用于双因素身份验证。

图 15-2　　RSA 用于双因素身份验证

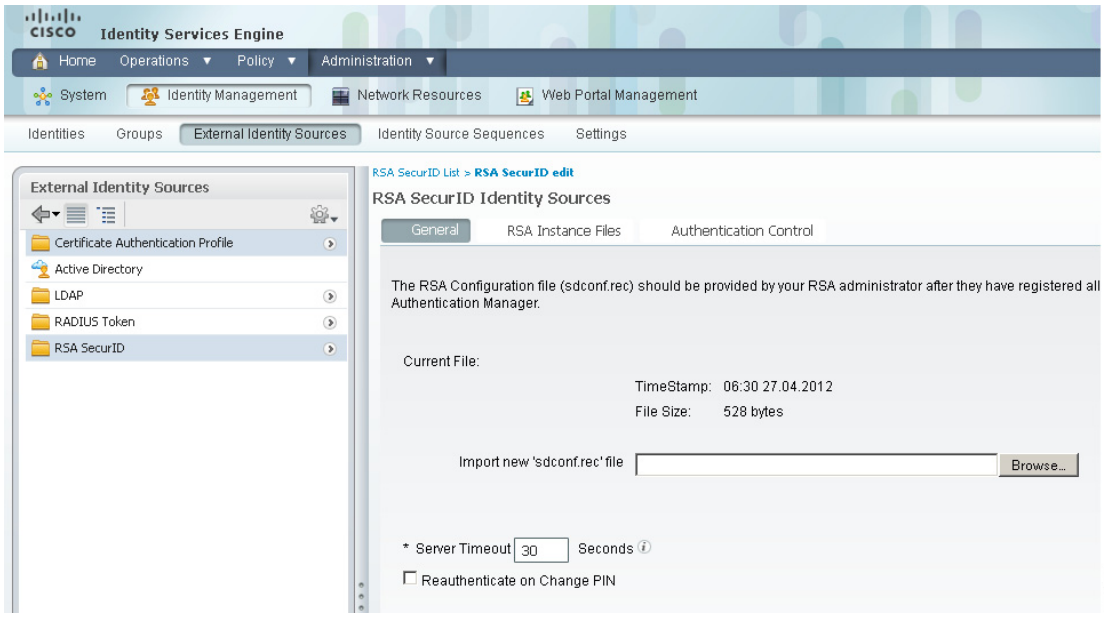


有关配置 RSA 安全身份验证管理器的信息，请参阅：
http://www.emc.com/security/rsa-securid.htm。

ISE 与 RSA 的集成

RSA 身份库主要用于对远程用户进行身份验证。远程用户首先需要使用其数字证书进行身份验证，然后必须使用 RSA SecurID 令牌提供一次性密码。要将 RSA 配置为身份库，请点击 **Administration > Identify Management > External Identity Sources > RSA SecurID > Add**，如图 15-3 中所示。

图 15-3　　RSA 服务器作为 ISE 的身份库



VPN 设计注意事项

本节讨论 ASA 在此设计中的主要作用，即终止 SSL VPN 连接。以下是实施 SSL VPN 时的部分设计考虑事项：

- 远程用户如何信任 VPN 网关？
- VPN 网关如何识别远程用户？
- 如何对不同类型的用户进行分组，以便提供不同类型的服务？
- 就特定客户端而言，需要哪种类型的移动客户端解决方案？
- 确定合适类型的 VPN 解决方案后，如何将移动客户端安装在远程设备上？
- 如何对 VPN 用户的策略设置进行集中？有时，远程用户可能无法轻松或方便地配置移动设备来获得 VPN 功能。

结合使用 Cisco ASA 和 Cisco AnyConnect 客户端可以解决上述注意事项。Cisco AnyConnect 客户端 3.0 用于满足有线用户、无线用户和远程用户的需要。 Cisco AnyConnect 安全移动客户端是下一代 VPN 客户端，它为远程用户提供与 Cisco 5500 系列自适应安全设备 (ASA) 的安全 IPsec (IKEv2) 或 SSL VPN 连接。 AnyConnect 可以为最终用户提供智能、无缝、随时随刻的连接体验，并为所有当今不断激增的托管和非托管移动设备提供移动安全保证。

Cisco AnyConnect 安全移动客户端在 AnyConnect 客户端软件包中集成了一些新模块：

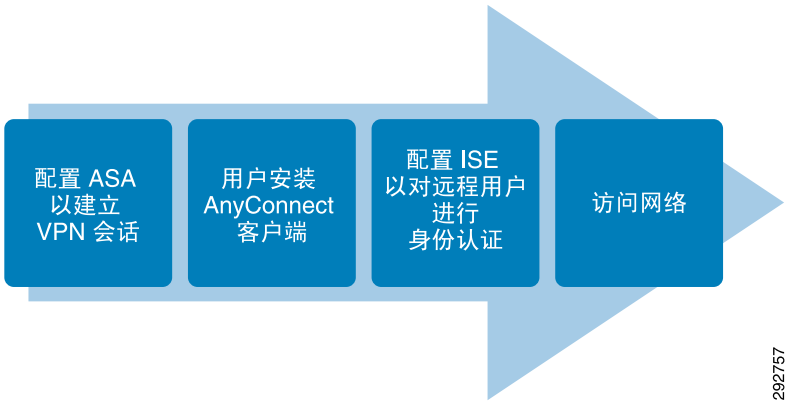
- 网络访问管理器 (NAM) - 以前称为思科安全服务客户端，此模块为有线和无线网络访问提供第 2 层设备管理和身份验证。
- 状态评估 - AnyConnect Posture 模块为 AnyConnect 安全移动客户端提供了一项功能，使其能够在与 ASA 建立远程访问连接之前识别主机中安装的操作系统、防病毒软件、反间谍软件和防火墙软件。根据此登录前评估，您可以控制哪些主机可获准与安全设备建立远程访问连接。 Host Scan 应用随状态评估模块提供，用于收集此类信息。
- 遥感勘测 - 将杀毒软件检测到的恶意内容来源的有关信息发送给 Cisco IronPort Web 安全设备 (WSA) 的 Web 过滤基础设施，后者将使用这些数据来提供更好的 URL 过滤规则。

- 网络安全 - 将 HTTP 和 HTTPS 流量路由至 ScanSafe Web 安全扫描代理服务器，以进行内容分析、恶意软件检测以及可接受使用策略管理。
- 诊断和报告工具 (DART) - 捕获系统日志和其他诊断信息的快照并在桌面上创建一个 .zip 文件，以便您可以轻松地将故障排除信息发送到 Cisco TAC。
- 在登录前启动 (SBL) - 通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接来连接到企业基础设施。

有关 Cisco AnyConnect 3.0 客户端的详细信息，请参阅：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac01intro.html。

图 15-4 显示了提供 VPN 连接的步骤。

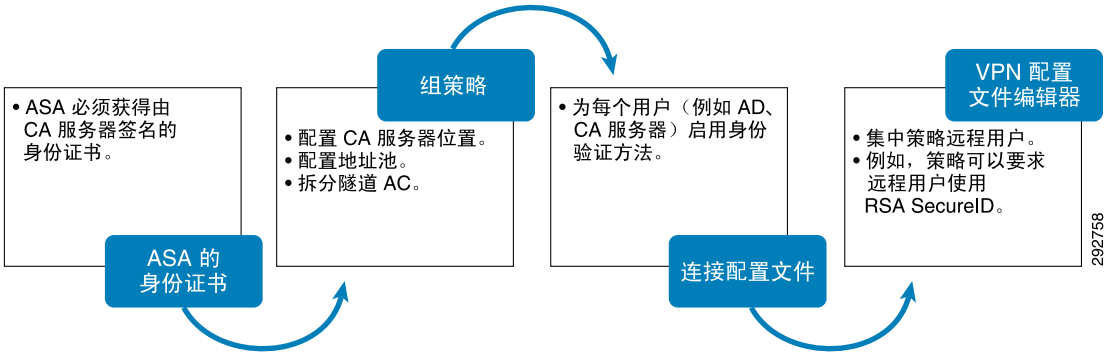
图 15-4　　提供 VPN 连接的概要步骤



ASA 配置

配置 ASA 涉及许多步骤。图 15-5 显示了配置 ASA 所需的概要步骤。

图 15-5　　配置 ASA

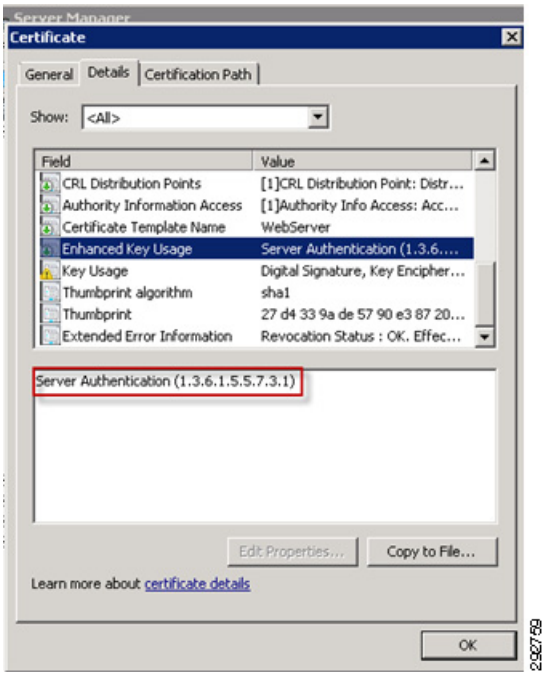


ASA 的身份证书

ASA 需要提供数字证书作为向客户端证明身份的凭证。远程客户端验证该数字证书，如果验证成功，则继续执行建立 VPN 连接的后续步骤。

ASA 提供的数字证书必须由受信任的第三方 （如 VeriSign）颁发，或者由受信任第三方签发的内部 CA 颁发。相反，如果 ASA 提供自签证书，则客户端无法验证该证书，因为签发机构 （自签证书的 ASA）不在客户端浏览器的受信任 CA 列表中。因此，为了获得更高的安全性，建议由受信任的第三方或受信任第三方签发的内部 CA 来颁发 ASA 的数字证书。当使用 Microsoft CA 作为内部 CA 时，请务必确认证书属性支持服务器身份验证。图 15-6 显示了可用于服务器身份验证的证书。证书应包含服务器身份验证的 EKU，如图 15-6 中所示。

图 15-6　　用于服务器身份验证的证书



ASA 可以通过使用 SCEP 或手动剪切并粘贴方法从 CA 服务器获取证书。要了解在 ASA 上部署证书的详细信息，请参阅：
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html。

下例显示了用于证书注册的 ASA 配置：

```
crypto ca trustpoint WIN2K-CA
 enrollment terminal
 subject-name CN=ASA-remote1
 serial-number
 ip-address 172.26.185.195
 keypair ssl
 no client-types
 crl configure
```

ASA 使用上述信任配置从 CA 服务器获取自己的身份证书。在此设计中，注册方法为终端。

以下命令显示了由 CA 服务器颁发给 ASA 的数字证书：

```
ASA-remote1(config)# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 1594b5d9000000000213
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=secbn1-WIN-MRL23B7NQO6-CA
    dc=secbn1
    dc=com
  Subject Name:
    cn=ASA-remote1
    hostname=ASA-remote1.secbn1.com
    ipaddress=172.26.185.195
    serialNumber=JMX1215L1KF
  CRL Distribution Points:
    [1]  ldap:///CN=secbn1-WIN-MRL23B7NQO6-CA,CN=WIN-MRL23B7NQO6,CN=CDP,CN=Publi
c%20Key%20Services,CN=Services,CN=Configuration,DC=secbn1,DC=com?certificateRevo
cationList?base?objectClass=cRLDistributionPoint
    [2]  http://win-mrl23b7nqo6.secbn1.com/CertEnroll/secbn1-WIN-MRL23B7NQO6-CA.
crl
  Validity Date:
    start date: 09:29:35 EST May 30 2012
    end   date: 09:29:35 EST May 30 2014
  Associated Trustpoints: WIN2K-CA
```

注意　客户端必须与证书中提供的 CRL 分发点建立了网络连接。

使用 ASA 信任点对远程用户进行身份验证

ASA 还需要一个信任点来对远程用户的身份证书进行身份验证。该信任点的配置如下：

```
crypto ca trustpoint Validate
 enrollment terminal
 crl configure
```

上例中的信任点 “Validate”用于复制根 CA 证书。要了解有关如何使用终端方法剪切并粘贴证书的更多信息，请参阅：
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html。

为不同类型的用户创建组

组策略是设计有效的用户访问机制的重要构建块。特定用户的需求可能有所不同。例如，一个用户可能希望使用域值 xyz.com 并使用 1.1.1.1 和 2.2.2.2 作为其 DNS 服务器。另一个用户可能有类似的需求，但同时还需要为其用户名配置一个代理服务器。如果您必须将所有这些属性关联到每个用户，配置可能会变得庞大而复杂。为了解决此问题，可以创建多个组，每个组都具有自己的个体属性集。这样，您只需将一个用户与一个组名相关联，而不必与大量属性相关联，从而最大限度地减少多用户情况下的配置复杂性。

默认情况下， Cisco ASA 创建 DftGrpPolicy 和其他组策略，它们继承大多数通用属性。对于每个组，只需显式配置非常特定的属性。

有关配置隧道组、组策略和用户的详细信息，请参阅：
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/vpngrp.html。

在本设计指南的组策略定义中，所需的主要属性有 vpn-tunnel-protocol、 split-tunnel-network-list 和地址池位置。此组策略的定义示例如下：

```
group-policy SSLClientPolicy internal     !This group policy is defined internally not
downloaded from radius.
group-policy SSLClientPolicy attributes
 wins-server value 10.1.6.100          !WINS server IP address
 dns-server value 10.1.6.100          !DNS server IP address
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split_ACL  !split_ACL prevents some local network traffic
from getting into VPN traffic.
default-domain value secbn1.com
 address-pools value testpool        !The IP address pool value.
```

连接配置文件配置

组策略定义组的属性，连接配置文件则指定特定于连接的属性。例如， AnyConnect 的一个连接配置文件指定属于此连接的用户是由 RADIUS 服务器进行身份验证还是在本地进行身份验证。连接配置文件还指向自己所属的组配置文件。如果在系统中未定义连接配置文件， ASA 会指向一个默认连接配置文件，但为了便于管理，最好定义一个特定组和若干连接配置文件。以下示例显示了 AnyConnect 连接配置文件的 ASA 配置：

```
tunnel-group SSLClientProfile type remote-access
tunnel-group SSLClientProfile general-attributes
 authentication-server-group ISE    !The remote sessions are authenticated with ISE.
default-group-policy SSLClientPolicy !The parent group policy used by this connection
profile.

tunnel-group SSLClientProfile webvpn-attributes
 authentication aaa certificate        !The remote users are authenticated by AAA and
Digital Certificate.
group-alias SSLVPNClient enable  !The remote users are presented with this alias name
during the session.
group-url https://172.26.185.195/SSLVPNClient enable
 group-url https://192.168.167.225/SSLVPNClient disable
!
```

上述配置步骤说明了如何使用 AnyConnect 配置 SSLVPN 会话。此配置也可以使用 ASDM 编辑器或其他管理工具来完成。有关使用其他工具进行配置的详细信息，请参阅以下网址上的 ASA 配置编辑器：
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_anyconnect.html#wp1090443。

在 ASA 上启用 AnyConnect VPN

在 ASA 上定义组策略和连接配置文件后，最后一步是在 ASA 上启用 AnyConnect VPN 功能。在启用 AnyConnect 之后，管理员还可以配置其他功能，如指向 AnyConnect 映像软件、 NAM 配置文件和 VPN 配置文件。以下示例显示了用于启用 AnyConnect 模块的配置命令：

```
webvpn
 enable outside
 anyconnect keep-installer installed !This forces the anyconnect to remain installed on
the endpoint device, after the session is terminated.
anyconnect modules none
```

调配 Windows 设备以远程连接到网络

要使获得公司批准的设备具备远程访问功能，用户必须在园区位置执行以下步骤：

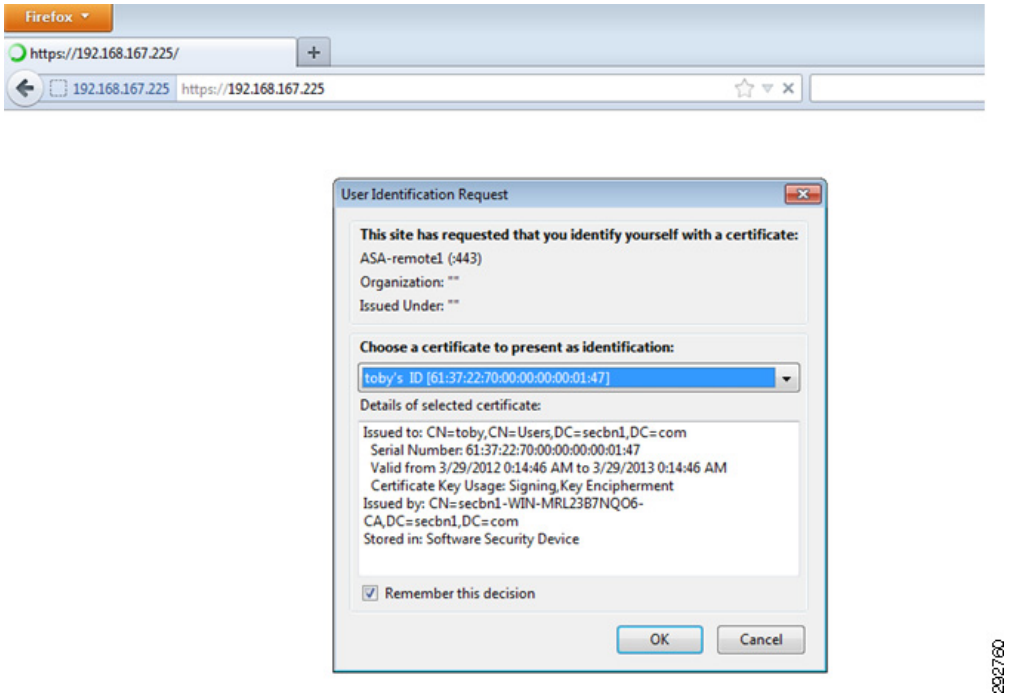
步骤 1　在远程设备上安装 RSA SecurID 应用，并在 IT 部门的支持下在该设备上调配软件。

步骤 2　假设在 AnyConnect 安装开始之前，工作站已成功完成注册和调配过程，也就是说工作站具有由 CA 服务器颁发的有效数字证书。

下述步骤适用于一次性安装。在安装完成后，用户将不再收到这些步骤的提示。

步骤 3　使用 Web 浏览器启动与 ASA VPN 网关 IP 地址的 SSL VPN 会话，如图 15-7 中所示。

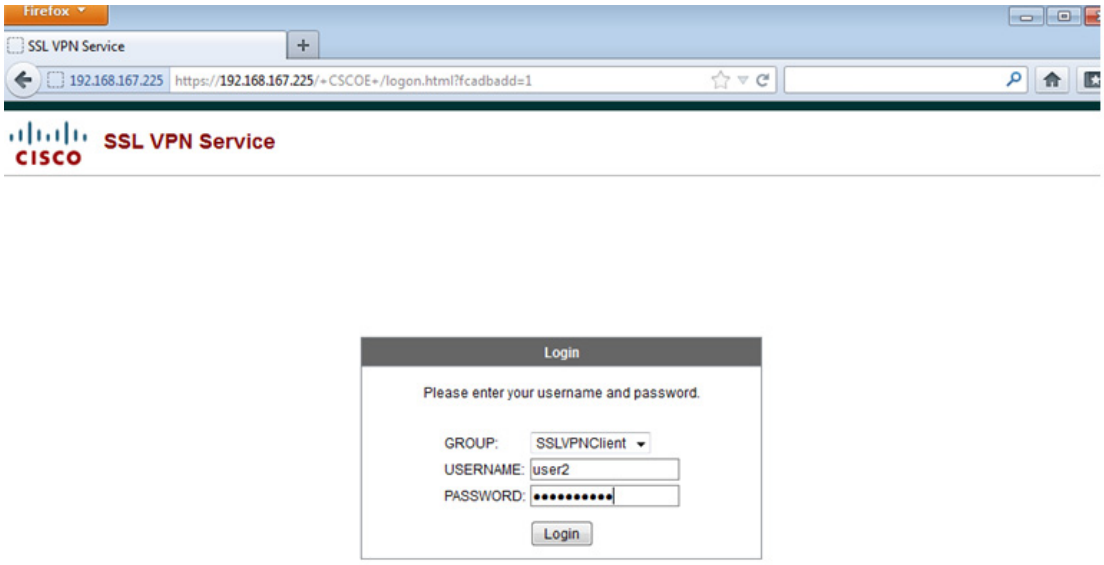
图 15-7　　与 ASA VPN 网关 IP 地址的 SSL VPN 会话



注意　ASA 远程终端提供的证书和 ASA 的身份证书必须由同一根 CA 服务器签发。

步骤 4　用户将看到登录屏幕，并需要选择他们所属的组。用户还需要选择组策略名称和有效的凭证，如图 15-8 中所示。

图 15-8　　选择组



步骤 5　用户凭证验证完毕后， Cisco AnyConnect 安装开始，如图 15-9 中所示。

图 15-9　　Cisco AnyConnect 安装

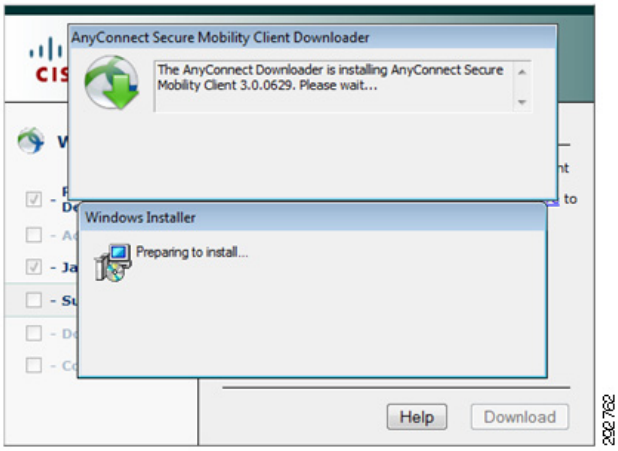
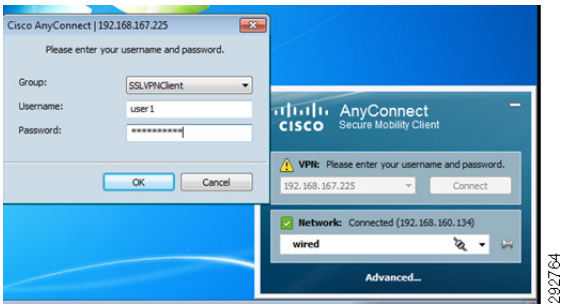


图 15-10 显示 Cisco AnyConnect 成功安装在工作站上：

图 15-10　　Cisco AnyConnect 成功安装

图 15-11 显示 Windows 工作站建立会话。

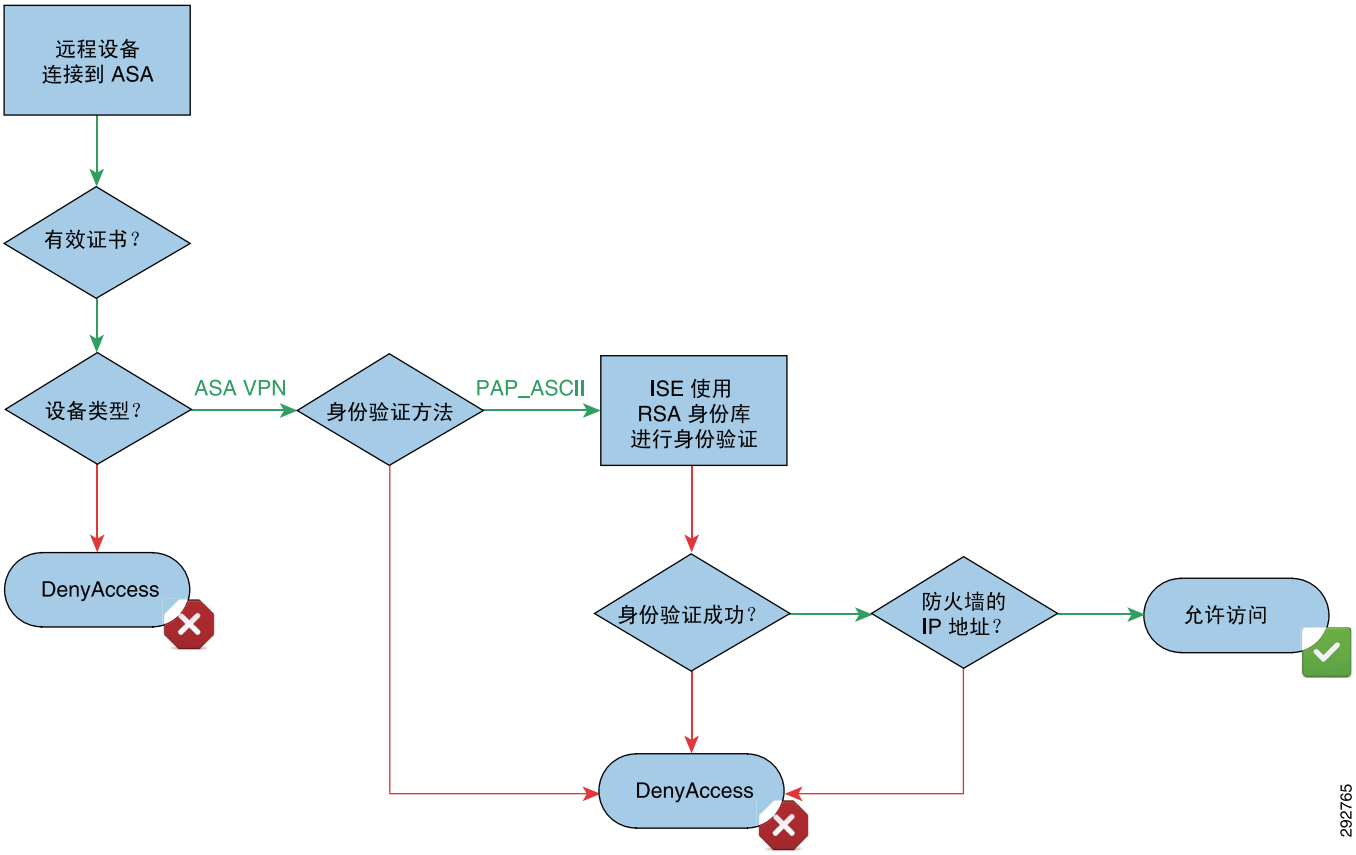
图 15-11　　AnyConnect 发起 VPN 连接



如“连接配置文件配置”部分所述，当远程员工连接到网络时， ISE 和 ASA 都会对设备进行身份验证。ASA 首先验证远程用户的数字证书。如果证书有效，则通过 RSA SecurID 令牌执行身份验证的下一步骤。如果两个身份验证均有效，则允许远程员工访问网络。

远程设备访问网络的逻辑流程图如图 15-12 所示。

图 15-12　　远程员工访问网络的逻辑流程图



验证所应用的 ISE 策略规则

如图 15-12 中所示， ISE 按照以下顺序验证远程用户：

1. 验证设备类型是否为 ASA VPN。这是为了确保只有配置为 VPN 类型的设备才能发起与 ISE 的通信。
2. 验证身份验证协议是否为 PAP_ASCII。 ASA 使用该协议将 RSA SecureID 令牌密码发送至 ISE， ISE 再将其发送到 RSA SecureID 服务器进行身份验证。
3. 在授权规则中， ISE 通过验证 ASA 的源 IP 地址来授权连接。在此设计中，远程 VPN 用户仅由 ASA 和 ISE 进行身份验证，并且不发生授权。图 15-13 和图 15-14 中具体显示了 ISE 中的身份验证和授权规则。

在图 15-13 中所示的 ISE 规则使用 RSA SecurID 身份库进行身份验证。

图 15-13　　身份验证规则

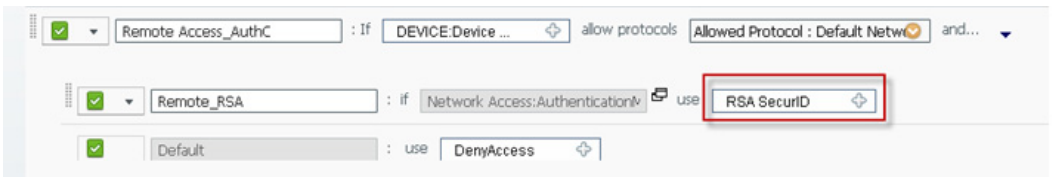
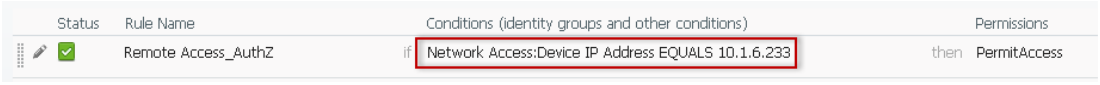


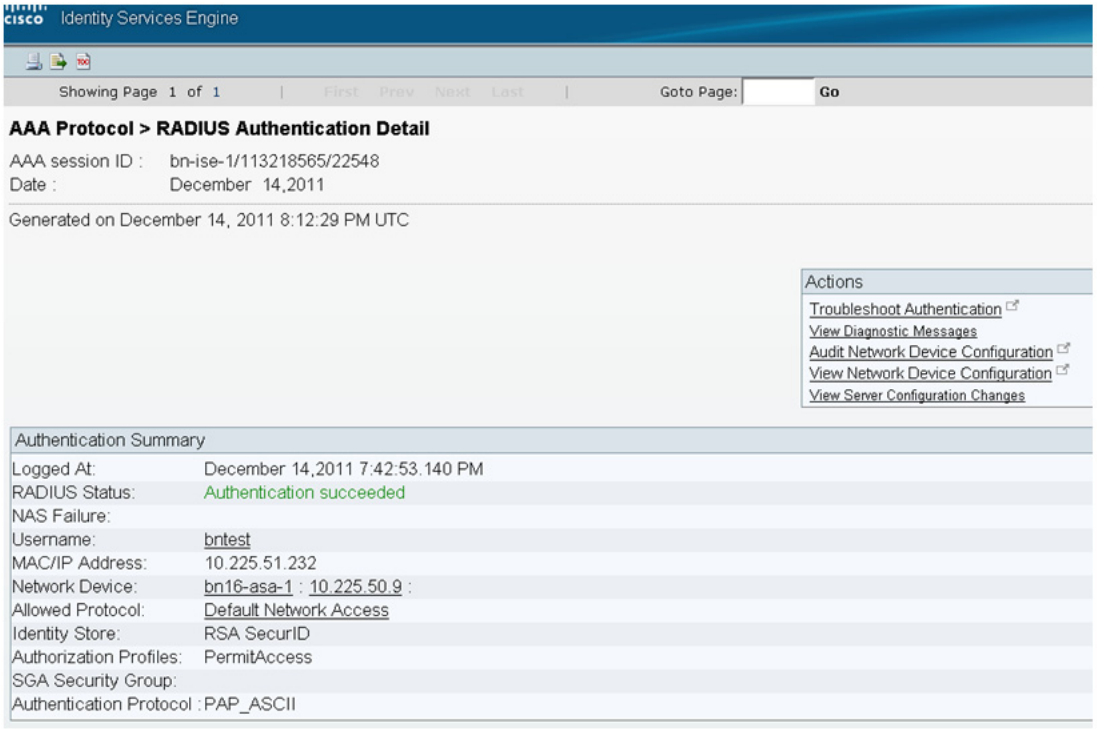
图 15-14 显示了 ISE 授权规则得到匹配的情况，因为远程设备已经连接，而且 Network Access: Device IP Address 与 ASA 防火墙的地址相匹配。

图 15-14　　授权规则



要验证哪些规则应用于 ISE 上，请点击 **Monitor > Authentication**，如图 15-15 中所示。

图 15-15　　ISE 上成功的远程员工身份验证的日志信息



调配 Apple iOS 设备以远程连接到网络

与工作站类似，在园区中调配的 Apple iOS 设备可以使用 Cisco AnyConnect 以远程方式建立与园区网络的 SSL VPN 连接。用户必须完成以下步骤，才能建立 SSL VPN 连接：

步骤 1　iOS 设备应已安装数字证书。图 15-16 显示了已完成调配的设备的示例。

图 15-16　已完成调配的设备

步骤 2　用户应从 Apple 的 App Store 安装 Cisco AnyConnect。

步骤 3　在 AnyConnect 上配置配置文件并选择已在设备中安装的证书（证书调配必须在发起远程 VPN 通信之前进行），如图 15-17 中所示。

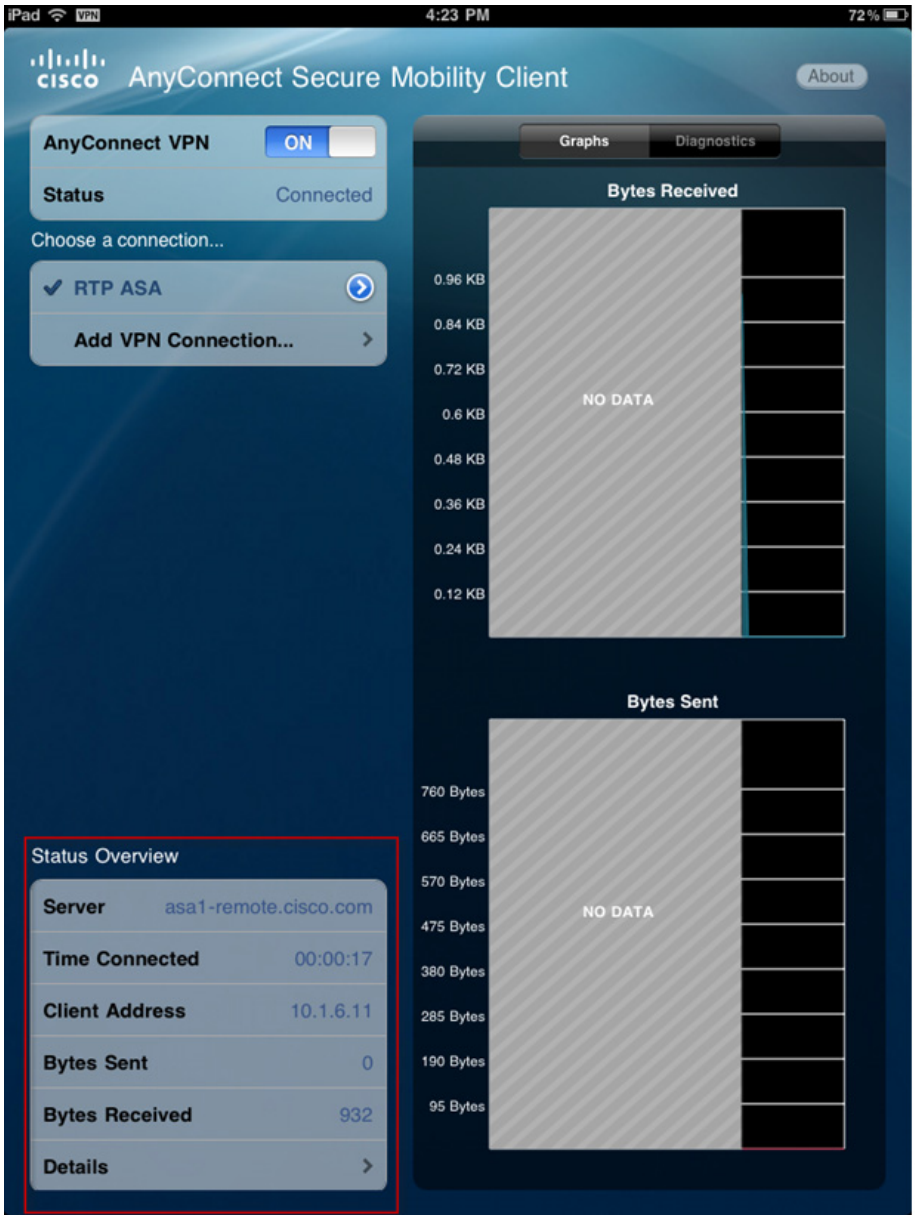
图 15-17　配置配置文件和选择证书

步骤 4　选择 VPN 组 （网络管理员必须告知用户所应选择的正确组），然后输入用户凭证。 ASA VPN 身份验证需要用户证书和用户凭证。因此必须输入用户凭证，如图 15-18 中所示。

图 15-18　　用户凭证

图 15-19 显示了一个成功连接的 SSL VPN 会话。

图 15-19　　成功连接的 SSL VPN 会话



BYOD 网络管理

修订日期：2013 年 8 月 7 日

BYOD 网络管理由以下三部分组成：

- Cisco Prime 基础设施概述 - 简要介绍 Cisco Prime 基础设施的基本功能。然后重点介绍 Prime 基础设施与 BYOD 直接相关的特定功能。
- BYOD 用户和设备跟踪 - 介绍使用来自多个组件并由 Cisco Prime 基础设施整合的信息来识别和跟踪网络上的最终用户和终端设备。
- 基于模板的 BYOD 配置 - 介绍使用 Cisco Prime 基础设施作为管理工具配置和维护思科无线局域网控制器 (WLC) 中的 BYOD 无线配置。

本文档不探讨 Prime 基础设施的基本实施，并假定 WLC 已经由 Prime 基础设施管理。有关 Prime 基础设施实施的详细信息，请参阅 《Prime 基础设施配置指南》：http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html。

重要缩略词和术语

表 16-1 缩略词和术语

关键术语	说明
Prime	Prime 在本文档中是指 Cisco Prime 基础设施。Cisco Prime 系列包含本文档未涉及的其他产品。
终端设备	也称为终端。兼指有线和无线设备，例如 Android 和 Apple 平板电脑和智能手机、有线 IP 电话，以及笔记本电脑。
最终用户	也称为用户。由一个或多个终端设备的 “用户名” 来识别。
WLC	也称为控制器。无线局域网控制器。
WLAN/SSID	WLAN （无线局域网）和 SSID 具有一对一关系，在本节可将其视为同一个事物。

Cisco Prime 基础设施概述

Cisco Prime 基础设施是思科新推出的一款产品，其目的是在实现无线和有线基础设施管理的同时，将来自多个组件的信息整合到一个位置。 Prime 基础设施不仅支持基础设施管理，还提供了一个用于发现网络访问者、所用设备、所在位置和访问时间的单一点。 Prime 基础设施的功能及其具备的其他组件不在本文档的讨论范围之内。 Cisco Prime 基础设施及支持组件简要介绍如下。

Cisco Prime 基础设施 1.2 是 Cisco Prime 网络控制系统 1.1 (NCS) 的演进版本，它在改进 NCS 1.1 既有功能的同时提供了额外的基础设施和有线设备管理及配置功能。

表 16-2　Cisco Prime 基础设施 1.2

Prime NCS 1.1	Prime 基础设施 1.2
• 无线网络管理 • 无线和有线监控与报告 • 基于模板的 WLC 配置 • 有线和无线环境的用户和设备跟踪	• 所有 NCS 1.1 功能 • 用户界面改善 • 基于模板的交换机和路由器配置 • 应用和媒体性能监控功能

Prime 基础设施和支持组件

Cisco Prime 基础设施可与其他多种组件交互，作为中央管理和监控门户。 Prime 基础设施直接与另外两种基于设备的思科产品 （思科移动服务引擎和身份服务引擎）集成，以实现信息整合。 Prime 基础设施控制、配置并监控所有思科无线局域网控制器 (WLC)，通过扩展，还可以涵盖网络中的所有思科接入点。 Prime 基础设施还可配置和监控 Cisco Catalyst 交换机和思科路由器。

图 16-1　Prime 基础设施组件交互摘要

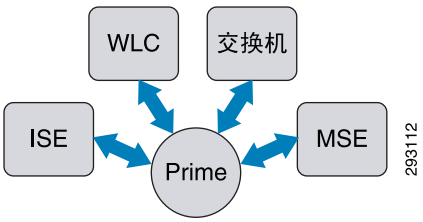


表 16-3　Prime 基础设施组件

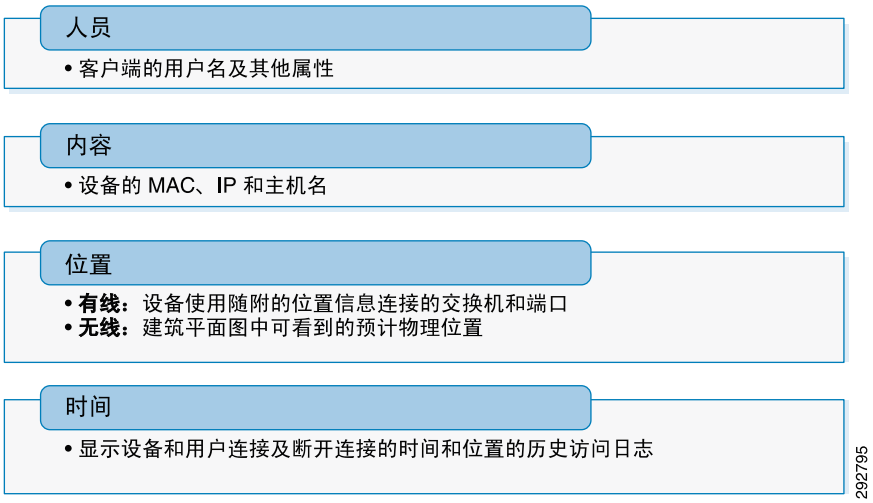
Prime 基础设施	Cisco Prime 基础设施是核心组件，负责将信息发送到其他四种组件，以及整合来自这些组件的信息。
ISE	思科身份服务引擎是 BYOD 的核心组件，用于用户和设备授权以及网络访问。 ISE 向 Prime 基础设施提供用户信息。
WLC	思科无线局域网控制器由 Prime 基础设施配置、控制和监控。 WLC 向 Prime 基础设施提供大量实时无线环境和客户端设备信息。
交换机 / 路由器	思科交换机和路由器由 Prime 基础设施配置、控制和监控。交换机 / 路由器向 Prime 基础设施提供有线设备信息，以便与无线设备信息整合。
MSE	思科移动服务引擎为 Prime 基础设施补充提供有关 Prime 基础设施所发现设备的当前和历史位置、使用情况以及其他信息。

有关 Cisco Prime 基础设施和 Cisco Prime 系列其他产品的详细信息，请访问：http://www.cisco.com/go/prime。

BYOD 用户和设备跟踪

掌握跟踪有线和无线网络上用户和设备的能力是了解网络访问者、所用设备、所在位置和访问时间的关键。

图 16-2　　人员、设备、位置以及时间摘要



通过掌握访问公司网络的人员、他们使用的设备以及连接位置，客户能够更好地了解：

- 网络上员工和设备的位置及其移动情况
- 可疑或未经授权的网络访问
- 丢失或失窃资产的位置，例如在大学校园环境中
- 网络中未知设备的位置
- 当前网络利用情况

添加有关用户和设备网络访问时间的历史记录能够：

- 持续记录用户和设备的网络访问时间及其具体位置
- 保留可搜索的用户和设备访问历史数据，便于跟踪和解决问题
- 保留端口使用情况历史数据

组件

Cisco Prime 基础设施是用户和设备跟踪的中心门户。 Prime 基础设施使用来自多个位置的信息生成一个针对当前及过去用户和设备网络访问的整合视图。图 16-3 和图 16-1 相结合展示了组件如何将用户和设备跟踪的人员、设备、位置以及时间要素涵盖在内。

图 16-3　　用户和设备跟踪的 Prime 基础设施组件交互摘要

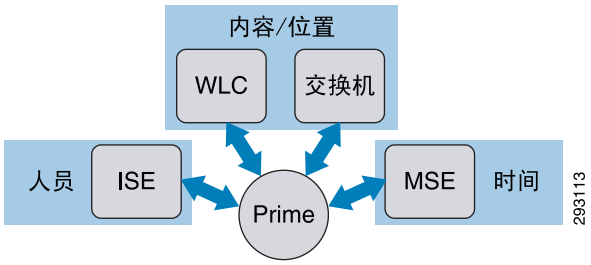


图 16-4 更详细地展示了 Prime 基础设施如何与架构的其余组件进行交互。下文列出了有线和无线用户的用户和设备跟踪所需的五个主要组件，以及每个组件的简要说明。

图 16-4　　Prime 基础设施与基础设施组件交互

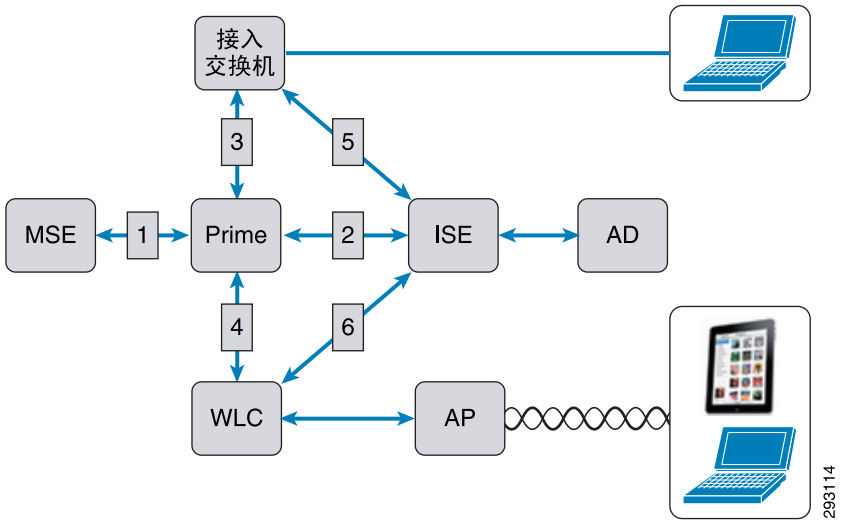


表 16-4　　Prime 基础设施与其他基础设施组件交互

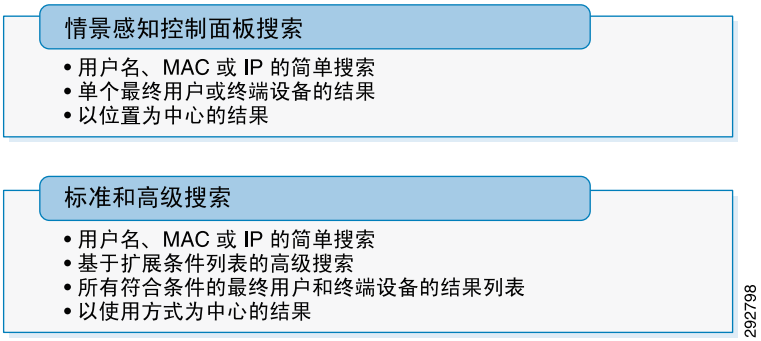
	组件	通信
1	Prime—MSE	Prime 接收移动设备的当前和历史位置信息
2	Prime—ISE	Prime 接收用户信息，包括用户名、设备 MAC 以及身份验证历史记录
3	Prime—交换机 / 路由器	Prime 接收有线设备信息，包括端口和 MAC。Prime 发送 / 接收组件配置。
4	Prime—WLC	Prime 接收无线用户信息和大量设备信息。 Prime 发送 / 接收组件配置。
5	交换机—ISE	RADIUS 身份验证
6	WLC—ISE	RADIUS 身份验证

为定位并跟踪用户和设备，Prime 基础设施将从所有这些来源提取信息，并主要根据公共 MAC 对信息进行整合。 Prime 基础设施以设备为重，因此将根据某一特定设备显示详细报告。此外，Prime 基础设施还能够显示特定用户访问网络使用过的所有设备，因此，能够跟踪某一特定用户使用过的多个无线和有线设备。

定位用户和设备

有两种显示用户和设备相关信息的基本方法。这两种方法都被视为 “搜索” 方法，尽管根据一系列过滤条件执行过滤和显示的功能远远超过大部分简单搜索方法的定义范畴。

图 16-5　　搜索类型



情景感知控制面板搜索

使用情景感知搜索可返回根据设备的当前 MAC、 IP 或最终用户的用户名过滤出的单个设备的信息。尽管此方法在搜索方式和显示内容上有所限制，但与标准搜索相比，其位置信息内容的确有细微的差别。

在图 16-6 中，情景感知控制面板上有一个名为 “位置辅助客户端故障排除” 的搜索框，这也是执行搜索的位置。搜索会即时解析设备的 MAC、 IP 或用户名，并仅显示该设备。

图 16-6　　情景感知控制面板

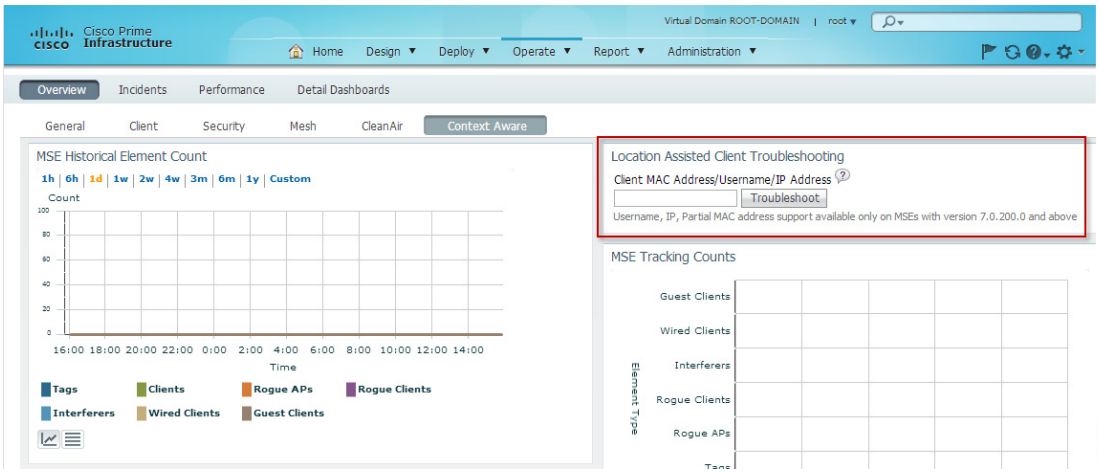
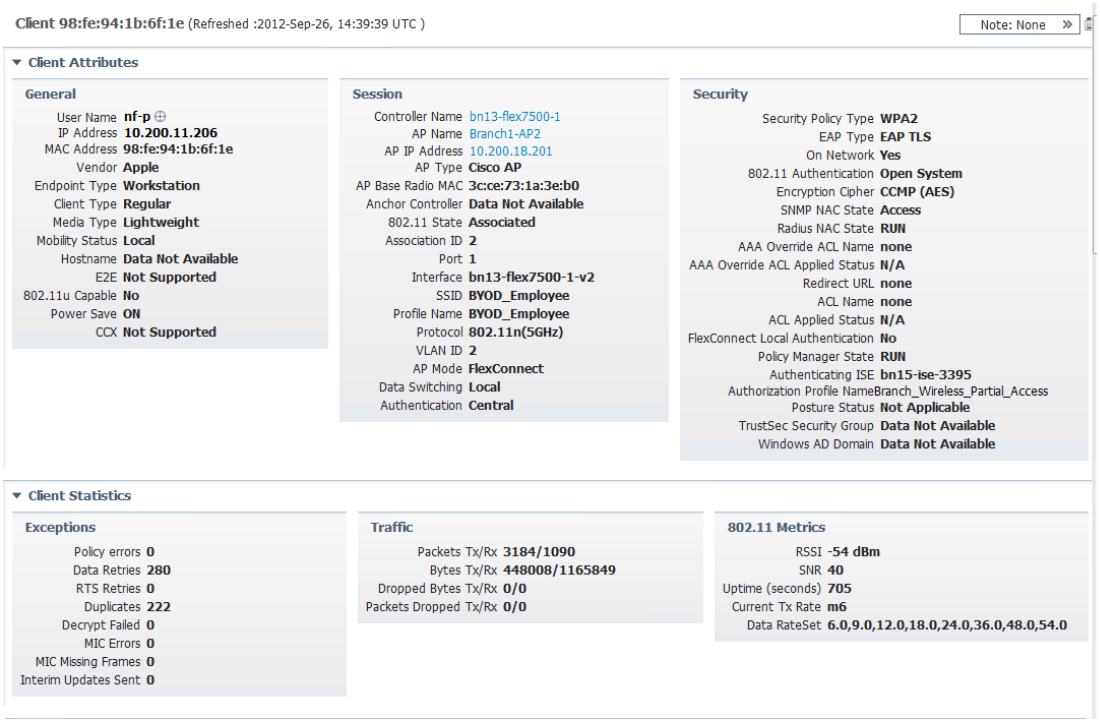


图 16-7 中显示的结果在两种搜索类型中都比较常见，结果中提供了许多有关设备及其最终用户（如果有）的最新信息。

图 16-7　　标准情景感知搜索结果

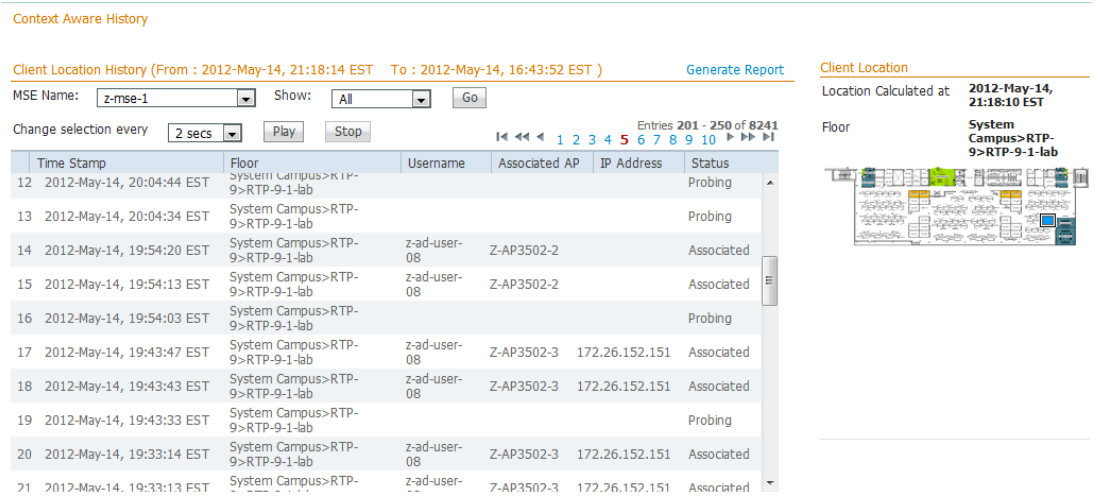


在搜索结果中，情景感知搜索特有的信息是基于位置的。标准和高级搜索可返回“关联历史记录”，其中包括位置，但使用的格式不相同。

从情景感知搜索结果中，您可以轻松得知设备在指定时间的准确位置，以及查看设备的移动记录。使用“播放”功能，可在地图上显示设备位置的更新状况，以直观的方式展示设备运动信息，而且，在实施正确的无线网络中，设备位置能够精确到几英尺之内。

图 16-8 展示了位置结果，其中蓝色方块表示设备在相邻楼层平面图上的当前位置。按“播放”可显示蓝色方块随设备在位置参照物中移动而移动。

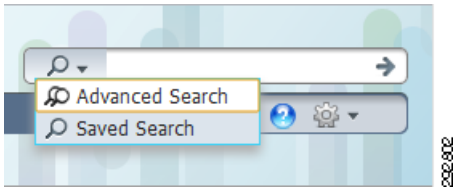
图 16-8　　情景感知搜索位置结果



标准和高级搜索

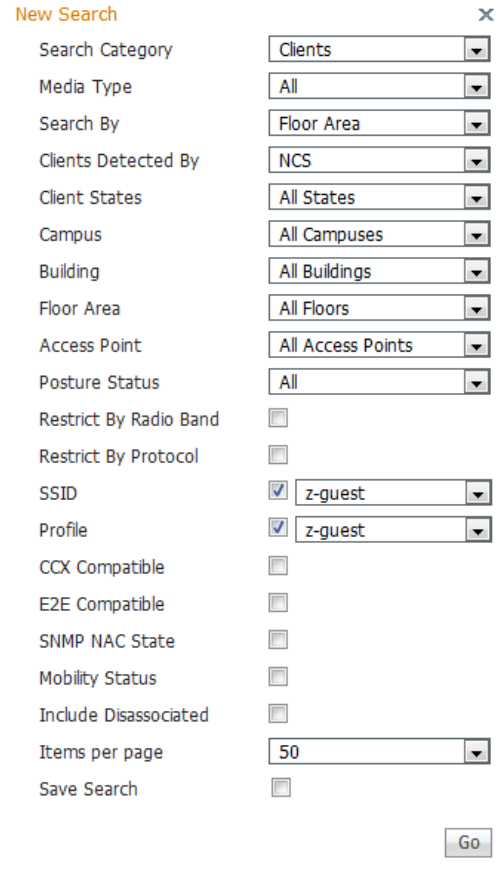
除使用情景感知控制面板搜索客户端或服务之外，还可以使用 Prime 基础设施任意页面右上角均显示的 “标准搜索” 和 “高级搜索” 来搜索客户端或设备。使用图 16-9 中显示的 “高级搜索” 选项可以开展更精细的搜索。标准和高级搜索返回的搜索结果主要与设备使用有关，但仍然包含位置信息。

图 16-9　　标准和高级搜索框



使用高级搜索可返回很多满足一组特定条件的最终用户或终端设备的相关结果，而不是只搜索某一特定用户或设备。可以使用的参数包括物理位置、用户类型、 SSID，甚至状态 / 身份验证状态。图 16-10 展示了可用的部分条件。

图 16-10　　高级搜索条件

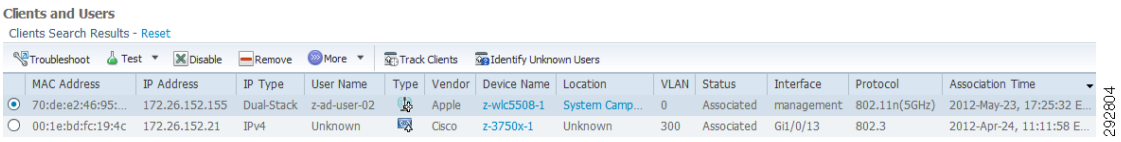


上面的表格是动态的，做出选择后表格会发生变化，也就是说，此图片仅显示了一部分 “客户端”类别可用的条件，在本示例中，“客户端”兼指终端设备和最终用户。

更多搜索条件和信息可参见 《Cisco Prime 基础设施配置指南》：http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html。

图 16-11 展示了搜索结果列表，其中包含有线用户和无线用户，除非过滤掉其中一个类型。本示例显示了两个设备，第一个是无线设备，第二个是有线设备。

图 16-11　　标准和高级搜索结果列表



仅搜索结果屏幕就提供了大量信息。而且，结果列可自定义，并可按照其中的任何列对结果列表排序。图 16-12 展示了可用列的列表。

图 16-12　　搜索结果列

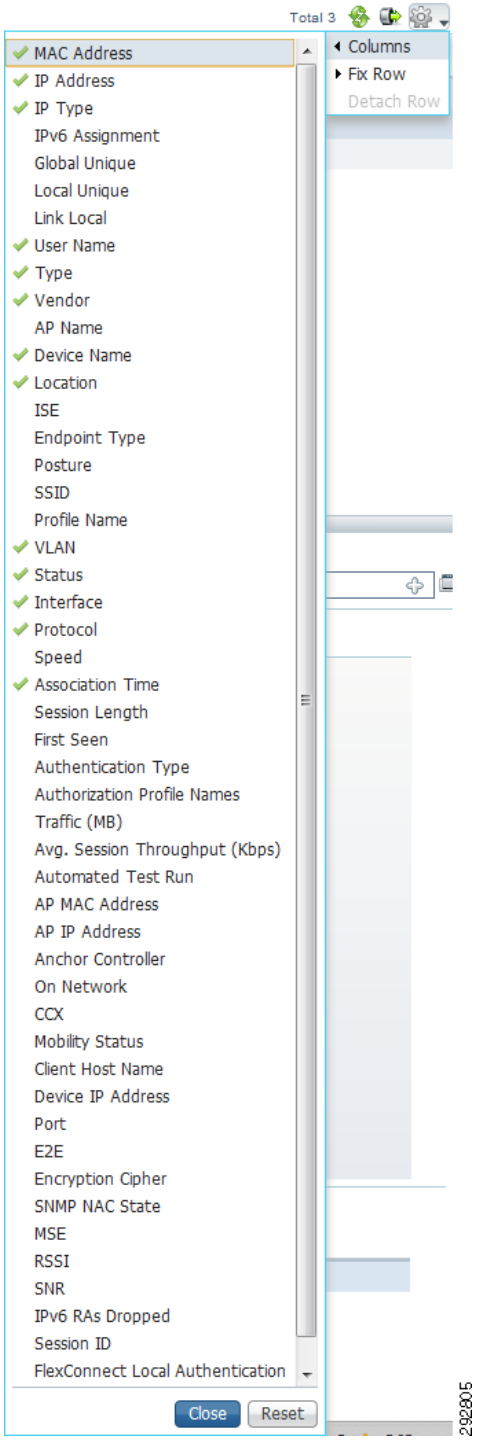


图 16-13 至图 16-18 展示的是针对从搜索列表中选择的各个设备的基本信息和扩展信息示例。图 16-13 展示的基本最终用户和终端设备信息和之前讨论的情景感知搜索相同。

图 16-13　　基本用户和设备详细信息

图 16-14 展示了关联时间、持续时间和位置，它们与情景感知搜索的位置历史记录相似，但并不相同。

图 16-14　　设备关联历史记录

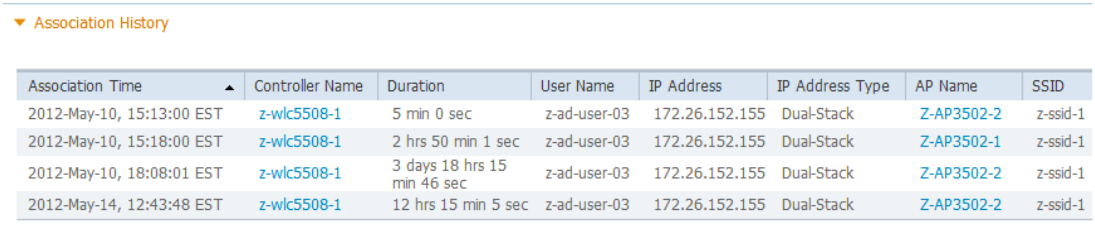


图 16-15 直接取自 ISE，展示了最近的身份验证成功和失败情况。

图 16-15　　设备身份验证历史记录

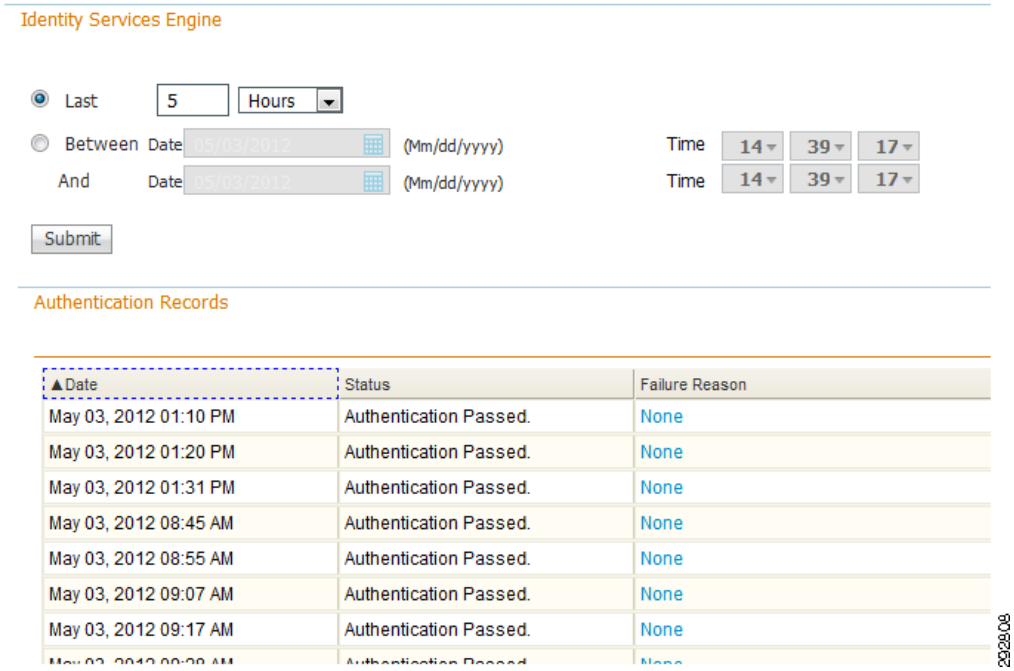


图 16-16 以图形方式展示了各个可更改时间段的信号质量。

图 16-16　　设备信号质量和使用情况历史记录

图 16-17 展示了设备的当前位置以及选定的任何其他信息。本示例仅选择了热图和 AP 位置，但还有很多其他项目可供显示，例如干扰设备和其他客户端。

图 16-17　　包含 AP 和客户端设备的平面图热图

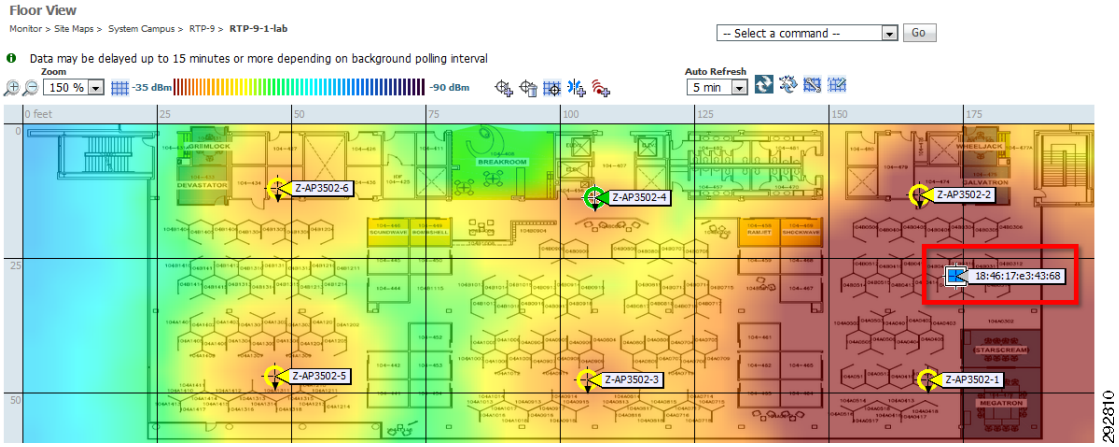
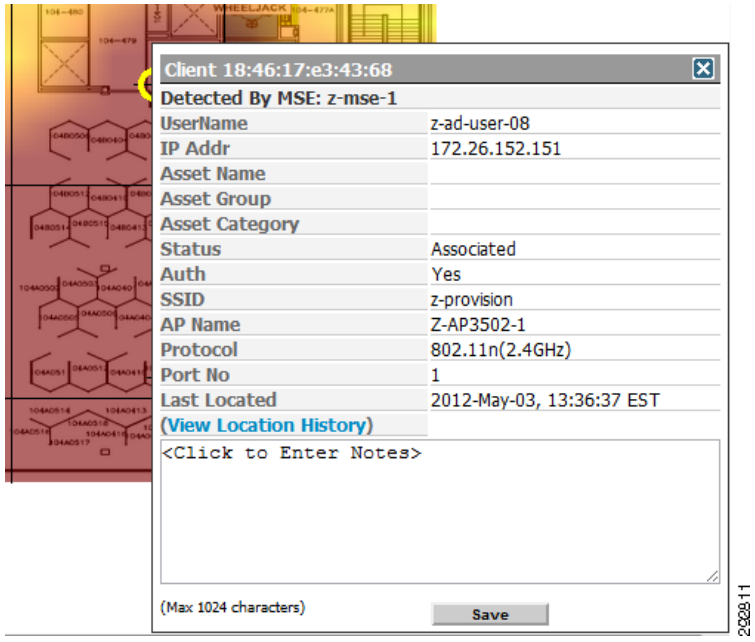


图 16-18 展示了热图上显示的任意设备的详细信息。

图 16-18　　从热图中弹出的设备详情



基于模板的 BYOD 配置

本节介绍如何使用 Cisco Prime 基础设施部署与维护思科无线局域网控制器 (WLC) 的配置，使其与本文探讨的 BYOD 配置匹配。

Cisco Prime 基础设施能够直接或通过使用模板控制思科无线局域网控制器 (WLC) 的配置。但是，一个模板不能配置整个控制器。模板细分为很多种，分别对应控制器的某一项功能。在控制器上实施的每一项小功能几乎都有可用的模板，而且模板的很多部分可在部署过程中修改，从而满足 WLC 中的独特设置。模板可针对所有 WLC 中的通用配置进行配置，并可在部分 WLC 或单个 WLC 上实施。

注意　每个 WLAN 只有一个 SSID，在理解本文内容时，为方便起见，可将这两个术语理解为同一事物：**WLAN = SSID**。

与单个配置 WLC 相比，基于模板的配置有很多优势：

- WLC 的配置一致
- 适合部署变化之需的多个模板
- 快速部署新组件或替换组件
- 具有快速回滚功能的配置变更试部署

WLC 的配置一致

通过基于 Web 的 WLC 管理界面配置多个 WLC 时，很容易造成配置不一致。不一致将对 WLAN 的功能、安全和性能产生深远的负面影响。

甚至配置顺序的不一致有时也会产生严重影响。例如，在不同控制器上以不同顺序配置多个 WLAN 将会导致 WLAN ID（标识每个 WLAN 的唯一整数）不一致。ISE 使用 WLAN ID 确定应对客户端作何处理。 WLAN ID 不一致会导致客户端连接到特定 SSID，但不能获得正确的访问权限，就像它们连接到了另外的 SSID。

不过此处有一点需要特别注意，Prime 基础设施可让控制器自动分配 WLAN ID。如果控制器的基本配置从一开始就不一致，例如某个 WLAN 在一个控制器上存在、在另一个控制器上却不存在，那么从 Prime 基础设施应用 WLAN ID 时， WLAN ID 的设置将出现不一致。配置时应仔细检查，确保所有控制器上的 WLAN ID 一致。

适合部署变化之需的多个模板

利用 WLC 的某些功能可能需要更改部署，具体取决于 WLC 的型号或它们在网络中的位置。如果 WLC 用于专用访客访问，某些功能的配置可能会与网络上的其他 WLC 有所不同，需要对模板做一些改动。

Prime 基础设施支持同一功能的多个模板，可根据 WLC 型号创建模板。模板可应用到所有 WLC 或应用时选择的各个 WLC 上。

快速部署新组件或替换组件

通过创建 WLC 配置模板，可利用最新模板快速配置新 WLC 和替换 WLC，从而缩短部署时间、消除因错误配置产生的错误。

具有快速回滚功能的配置变更试部署

可为特定功能创建多个模板这一项功能支持已更改的配置与当前配置在模板中共存。之后，新配置模板可在一个或多个 WLC 上进行测试，而且，出现问题时可以轻松回滚到之前的配置模板。

注意　缩略词 WLC （无线局域网控制器）在本文中应用普遍，展示的一些界面中使用的则是通用术语“控制器”。在本文中，“WLC”和 “控制器”指代同一个事物：**WLC = 控制器**。

模板创建与实施

在 Prime 基础设施中模板创建和实施非常简单，不过也需要注意几点。下文中的模板和配置特定于本文档中的 BYOD 解决方案，而且，它们不过是实施企业无线网络所需的众多设置和功能中的一小部分。

本节假设 WLC 已由 Prime 基础设施管理。有关 Prime 基础设施实施的详细信息，请参阅《Prime 基础设施配置指南》：
http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html。

模板创建

WLC 配置的模板创建可通过以下三种方式实现：

1. 直接在 Prime 基础设施中创建新模板。
2. 通过 Cisco Prime 基础设施配置一个 WLC，随后使用该配置创建模板。
3. 通过本地 WLC Web 接口配置一个 WLC，随后使用该配置创建模板。

下面的内容重点介绍第 2 种方法，即通过 Prime 基础设施配置一个 WLC，然后创建模板来配置其他 WLC 并更改原始 WLC。从逻辑上看，这种方法可能最合理，因为在已经配置 WLC 的情况下，此方法也将第 3 种方法融合在内。

对于那些希望同时了解 Prime 基础设施的界面与操作和 WLC，并且在今后使用单独的 WLC 来创建用于生产部署的配置和模板的人员，此方法也会很有吸引力。出于创建基本模板、进行功能试验以及介绍解决方案的目的，本文档中涉及的大多数功能可能会使用相对便宜的 Cisco 2504 以及基本许可证和单个接入点进行部署。 2504 用于 BYOD 解决方案所欠缺的两个主要功能是：作为 DMZ 访客 WLC 的功能和流量速率限制功能。这两个功能在第 13 章， BYOD 访客无线接入”中有所介绍。 BYOD 解决方案的所有其他特性和功能在此平台上均受支持。

由于 FlexConnect 环境的配置内容很广，所以并非列出的每一个步骤都针对初始配置。使用 Prime 基础设施界面而不是直接使用 WLC 界面会非常简单。本文介绍了 Prime 基础设施界面中的选项位置和功能方面的细微差异。

使用上文中的第 2 种方法 （通过 Prime 基础设施配置一个 WLC，随后使用该配置创建模板）应执行下列步骤。如果使用已经配置好的 WLC，请跳过第 1 步和第 3 步。

- 第 1 步 - 在新 WLC 上配置基本网络连接
- 第 2 步 - 将 WLC 作为托管设备添加到 Prime 基础设施
- 第 3 步 - 使用 Prime 基础设施直接配置 WLC
- 第 4 步 - 使用已配置的 WLC 创建模板
- 第 5 步 - 在一个或多个 WLC 上部署模板

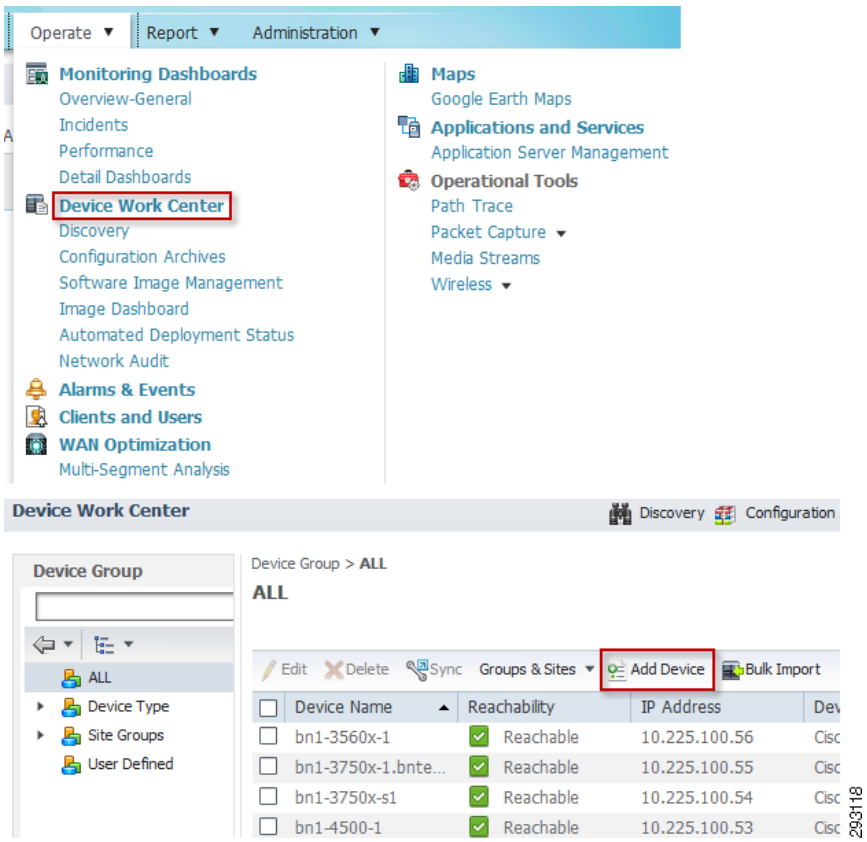
第 1 步 - 在新 WLC 上配置基本网络连接

此步骤应按照所要实施的 WLC 的相关文档来执行。有关所有 Cisco WLC 的文档，请访问 http://www.cisco.com/web/tsweb/redirects/mm/support/wireless.html。

第 2 步 - 将 WLC 作为托管设备添加到 Prime 基础设施

在 Prime 基础设施上，使用设备工作中心手动添加设备，如图 16-19 中所示。

图 16-19　　设备工作中心 - 添加设备



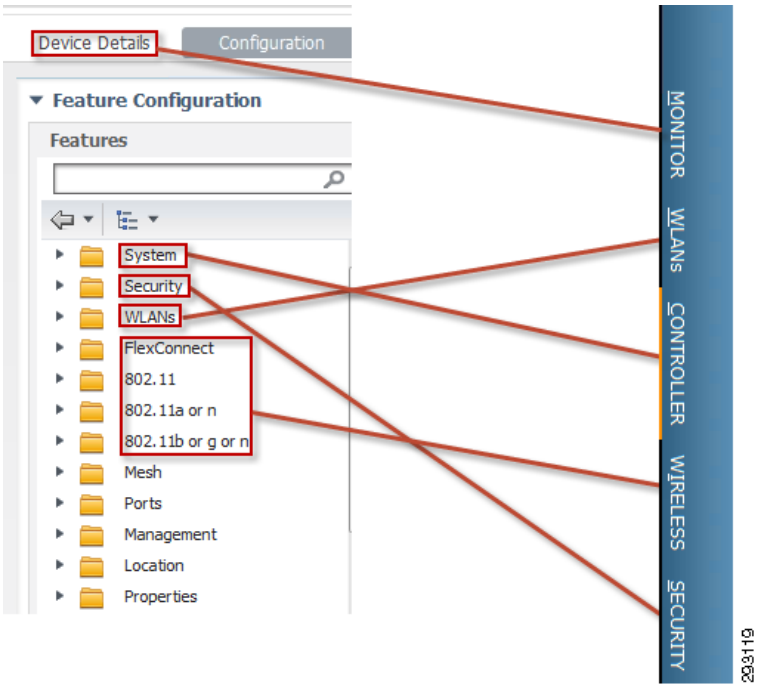
Prime 基础设施会在同步过程中确定 WLC 类型，因此无需指定 WLC 类型。或者，WLC 也可以通过发现过程添加 （未提供图示）。

WLC 添加成功后，会与 Prime 基础设施同步所有现有配置。此过程只需要几分钟的时间，且设备工作中心中的 “设备状态” 将显示 “托管”。 WLC 还将被放置到相应的设备类型文件夹中，此文件夹可在设备工作中心屏幕的左侧展开，如图 16-19 中所示。

第 3 步 - 使用 Prime 基础设施直接配置 WLC

现在，可通过选择 WLC，然后再选择下面部分中的 **Configuration** 选项卡，直接在设备工作中心中配置 WLC，操作与在 WLC 自己的 Web 接口上配置相似。这两个配置界面非常相似，但并非完全相同。图 16-20 展示了 WLC 界面主要类别如何映射到 Prime 基础设施类别。

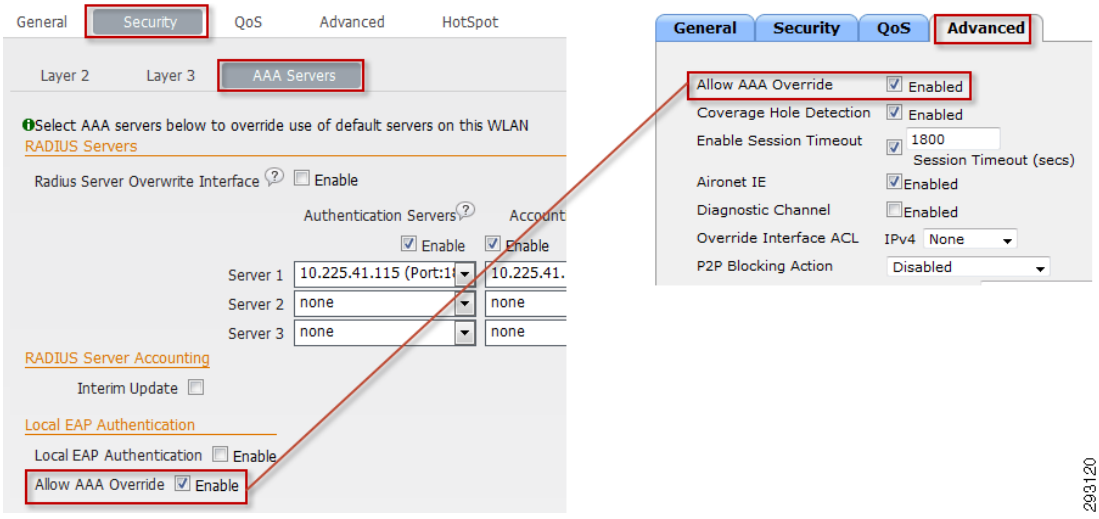
图 16-20　　WLC 界面类别映射到 Prime 基础设施类别



请注意，“AAA 覆盖”这项重要功能的位置不相同。

通过 WLC 界面配置时，“AAA 覆盖”功能位于 WLAN 设置的 **Advanced** 选项卡中。通过 Prime 基础设施配置时，这项功能则位于 WLAN 设置的 **Security** 选项卡中，如图 16-21 中所示。

图 16-21　　“AAA 覆盖”位于 WLAN 设置的 “高级”选项卡中

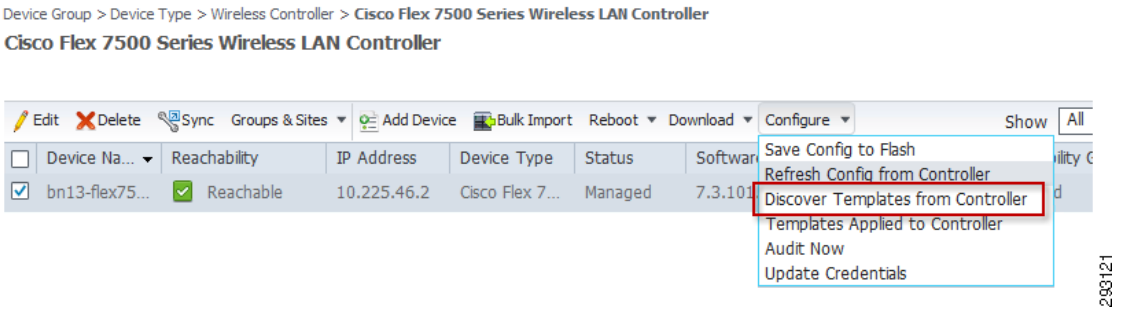


注意本节结尾的 WLAN ID 问题，因为它对 WLAN 的初始创建以及 WLAN 基于模板的部署都非常重要。

第 4 步 - 使用已配置的 WLC 创建模板

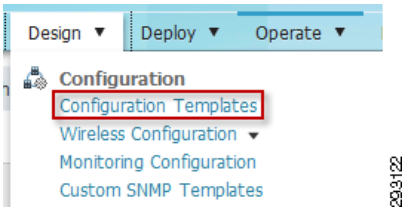
使用已配置的 WLC 创建模板非常简单。通过一个自动流程即可创建包含 WLC 中所有可用于创建模板的元素的模板。要执行此步骤，请访问**设备工作中心**中的设备，位置与上一步骤相同。选择已配置的 WLC，然后依次选择 **Configure**、 **Discover Templates from Controller**，如图 16-22 中所示。

图 16-22　　发现控制器中的模板



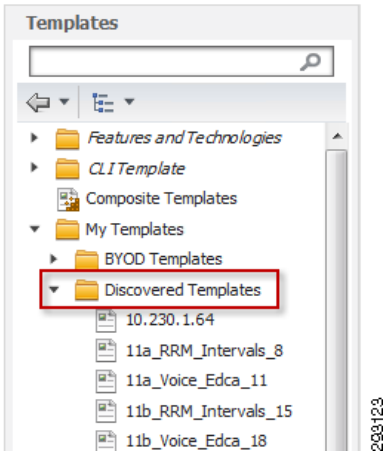
模板发现过程结束后，可从顶部菜单 **Design** 部分的 **Configuration Templates** 部分找到模板，如图 16-23 中所示。

图 16-23　　配置模板



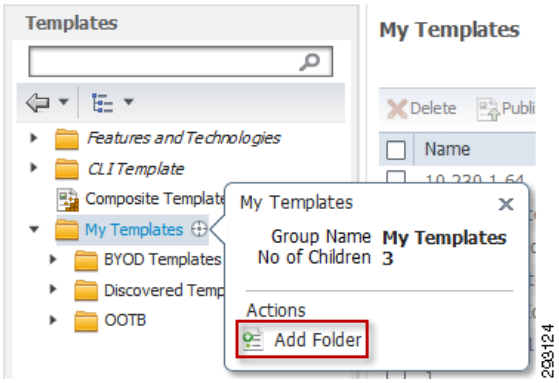
新发现的模板将显示在 **My Templates** 下的 **Discovered Templates** 中，如图 16-24 中所示。

图 16-24　　已发现模板



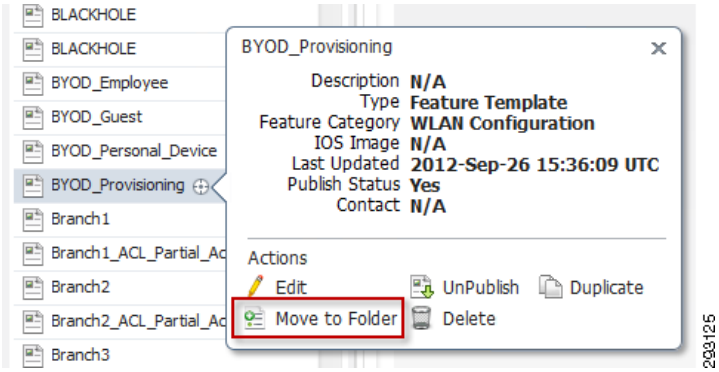
此部分包含很多模板，但真正需要的只有一小部分。在对模板进行任何自定义或部署之前，强烈建议将所需的模板整理到自定义文件夹中。首先创建一个新文件夹。将鼠标指针放到 **My Templates** 旁边，此时会弹出一个对话框。点击 **Add Folder**，如图 16-25 中所示。

图 16-25　　添加文件夹



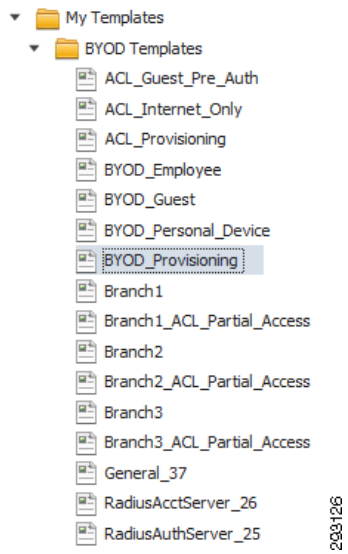
创建文件夹之后（在本例中是命名的 BYOD 模板），请逐一将指针放在每个所需模板旁边，点击 **Move to Folder**，然后将模板移动到新建文件夹，如图 16-26 中所示。

图 16-26　　移动模板



移动完成后，所有所需模板都将显示在新文件夹中，可供编辑和部署，如图 16-27 中所示。

图 16-27　　BYOD 模板



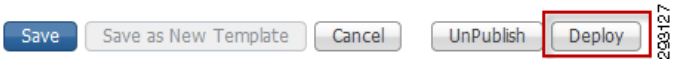
第 5 步 - 在一个或多个 WLC 上部署模板

部署没有独特设置的标准模板非常简单。部署需要独特配置的模板 （例如 FlexConnect 组）则涉及的内容较多。

FlexConnect 组有与之关联的特定接入点，而且每个 WLC 的接入点各不相同。简单的静态模板可能用途不大，而且部署必须支持自定义。以下模板部署是 FlexConnect 组部署，以最复杂的部署类型为例。

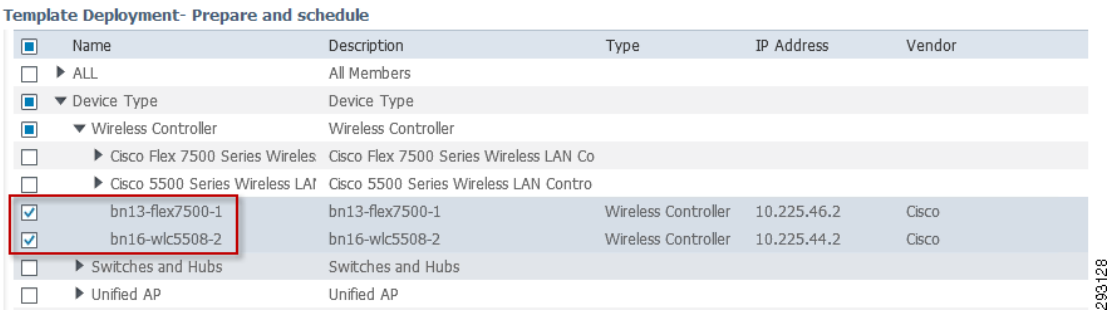
每个模板的底部是用于部署该模板的按钮 （如图 16-28 所示），点击此按钮将显示部署屏幕。

图 16-28　　部署按钮



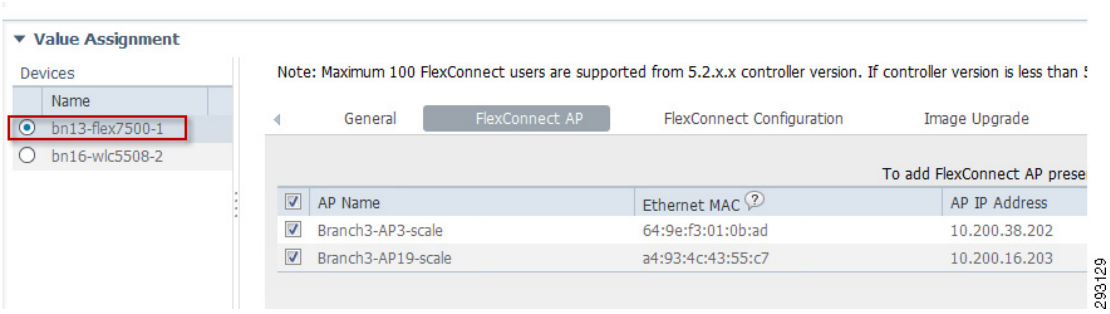
启动 FlexConnect 组模板后，必须选择目标 WLC。本示例选择了两个不同类型的 WLC，如图 16-29 中所示。

图 16-29　　部署屏幕



选择类型后，您会看到**值分配**屏幕，如图 16-30 中所示。在这一部分，您可以分别为每个 WLC 分配值和资源。在本示例中，可能需要分别为每个 WLC 的 FlexConnect 组添加接入点。通过点击屏幕最右侧的**添加接入点**（图片中未显示）可添加接入点，此操作将调出对 Prime 基础设施可见的所有接入点的列表。

图 16-30　　值分配



完成自定义后，可立即部署模板，也可以计划模板部署。

问题 1 - WLAN ID

ISE 使用 WLAN ID 确定连接到网络所使用的 SSID (WLAN) 客户端。此 ID 对每个控制器上的每个 WLAN 都是唯一的，因此，确保每个 WLAN 在每个控制器都有相同的 WLAN ID 对正常运行和安全至关重要。

对具有多个 WLC 的大型企业客户而言，要做到这一点可能是一项复杂的工作。请注意以下事项：

- Prime 基础设施无法设置 WLAN ID，而是让 WLC 分配 WLAN ID。
- WLC 的现有 WLAN ID 可增加至下一个可用整数。
- 直接使用 WLC Web 接口创建 WLAN 可选择 WLAN ID。
- WLAN 创建后， WLAN ID 无法更改。

下面的简单示例展示的便是这类问题：

- WLC A 未定义 WLAN。
- WLC B 有使用 WLAN ID 1 的 WLAN “Special-SSID”。

使用 Prime 基础设施创建名为 “Employee-SSID”、涵盖所有 WLC 的新 WLAN，会导致为 WLC A 分配 WLAN ID 1，并为 WLC B 分配 WLAN ID 2。

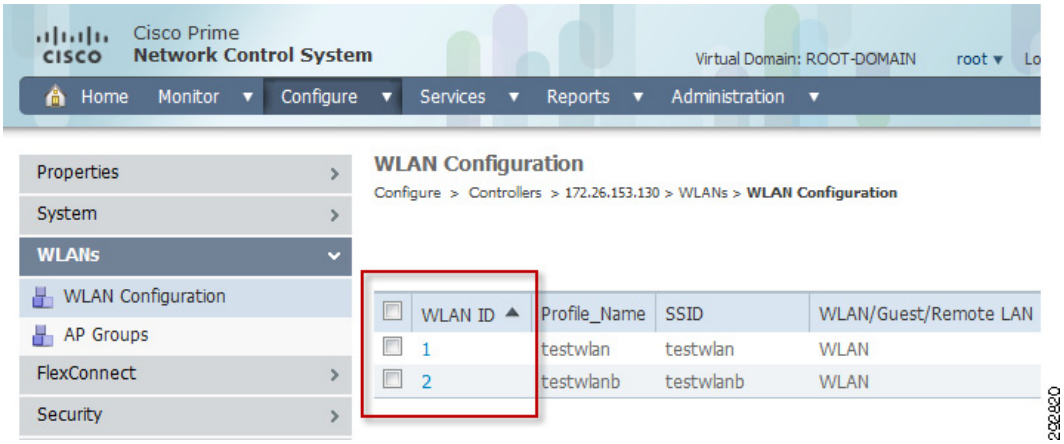
- WLC A
  - WLAN “Employee-SSID” WLAN ID 1
- WLC B
  - WLAN “Special-SSID” WLAN ID 1
  - WLAN “Employee-SSID” WLAN ID 2

为避免这种可能的严重不匹配，审核 WLAN 的现有 WLC 和针对 WLAN 配置准备 WLC 至关重要。仅使用 Prime 基础设施而不是 WLC 界面时，执行以下汇总的步骤（后文提供详细步骤）可避免 WLAN ID 不一致。

确保 WLAN ID 一致的详细步骤

1. 将所有 WLC 添加到 Prime 基础设施并同步其配置。
2. 使用 Prime 基础设施时，查看每个 WLC 上的 WLAN 确定现有的最大 WLAN ID，如图 16-31 中的示例所示。在本示例中，一个特殊的 WLC 上存在两个 WLAN。

图 16-31　　WLAN ID 列表



3. 创建已禁用虚拟 WLAN 模板并将其应用于 WLC，使其具有相同的最大 WLAN ID。

   如果虚拟 WLAN 是以“已禁用”状态创建，则彼此之间便不具有相关性。在本示例中，必须创建两个虚拟 WLAN 模板，并将其应用到任何没有 WLAN 的 WLC。

   作为创建虚拟 WLAN 的一种替代方法，也可以删除现有 WLAN，然后使用在 WLC 上直接手动设置的较大 WLAN ID 重新创建 WLAN。删除和重新创建是当前可用于更改 WLAN ID 的唯一方法。现有 WLAN 的 WLAN ID 无法更改。
4. 为 BYOD 配置创建新的 WLAN 模板并将其应用于所有 WLC。
5. 检查 WLC 以确保所有 WLC 上的 WLAN ID 分配一致。
6. 应用 WLAN 模板后，可根据需要删除虚拟 WLAN。

注意　在网络中添加新的 WLC 时，必须先对其应用虚拟 WLAN 模板，然后再应用 BYOD WLAN 模板。由于 WLAN ID 是按顺序分配的，因此必须始终按照相同的顺序应用 BYOD WLAN 模板。