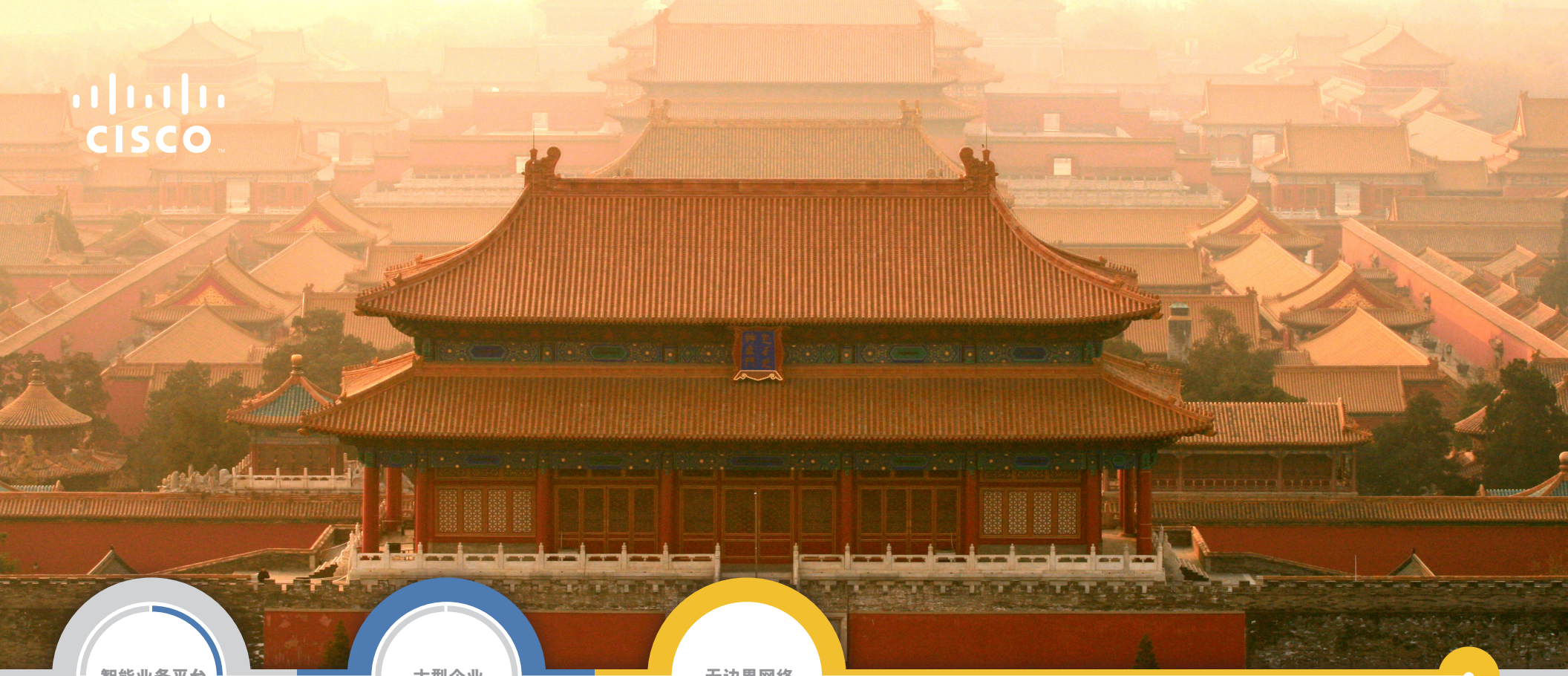


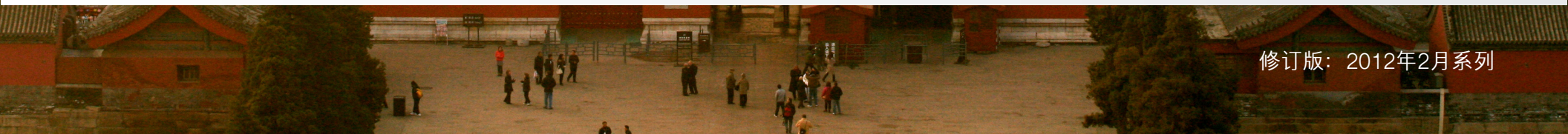
智能业务平台

大型企业

无边界网络

局域网与无线局域网 802.1 X 部署指南

智能业务平台



修订版：2012年2月系列

前言

本指南的目标受众

Cisco®智能业务平台(IBA)指南主要面向承担以下职务的人员：

- 需要实施解决方案时的标准规范的系统工程师
- 需要撰写思科IBA实施项目工作说明书的项目经理
- 需要销售新技术或撰写实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说，您也可以将思科IBA指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科将定期对IBA指南进行更新和修订。在开发新的思科IBA指南系列时，我们将会对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应当使用同一系列中的设计指南文档。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。我们以某系列指南发布时的年份和月份来对该系列命名，如下所示：

年　月 系列

例如，我们把于2011年8月发布的系列指南命名为“2011年8月系列”。

您可以在以下网址查看最新的IBA指南系列：

客户访问：http://www.cisco.com/go/cn/iba

合作伙伴访问：http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤，这些设备运行着Cisco IOS、Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系统命令的指定规则，您需要按照这些规则来输入命令。

在CLI中输入的命令如下所示：

```
configure terminal
```

为某个变量指定一个值的命令如下所示：

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示：

```
class-map [highest class name]
```

以交互示例形式显示的命令（如脚本和包含提示的命令）如下所示：

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入：

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

系统输出或设备配置文件中值得注意的部分以高亮方式显示，如下所示：

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

问题和评论

如需要了解更多有关思科IBA智能业务平台的信息，请访问

http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问

http://www.cisco.com/go/qpt

如果您希望在出现新评论时获得通知，我们可以发送RSS信息。

目录

本IBA指南的内容 1
关于IBA 1
关于本指南 1

简介 2
业务概述 2
技术概述 2

部署详解 4
部署身份服务引擎 4
支持了解局域网情况 10
支持了解无线网络情况 17
部署数字证书 22
启用802.1X认证 28
配置组策略对象 32
在Windows终端上部署AnyConnect 41
配置Mac工作站，以支持802.1X认证 45
监控 49

附录A：产品列表 56

本手册中的所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括但不限于适销性、适合特定用途和非侵权保证，或与交易过程、使用或贸易惯例相关的保证。在任何情况下，思科及其供应商对任何间接的、特殊的、继发的或偶然性的损害均不承担责任，包括但不限于由于使用或未能使用本手册所造成的利润损失或数据丢失或损害，即使思科或其供应商已被告知存在此类损害的可能性。这些设计如有更改，恕不另行通知。用户对于这些设计的使用负有全部责任。这些设计不属于思科、供应商或合作伙伴的技术建议或其它专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

文中使用的任何互联网协议（IP）地址均非真实地址。文中的任何举例、命令显示输出和图示仅供说明之用。在图示中使用任何真实IP 地址均属无意和巧合。

© 2012 思科系统公司。保留所有权利。

本IBA指南的内容

关于IBA

思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

思科IBA在一个综合解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能够实现无缝协作。IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足企业需求的解决方案，而不必担心技术复杂性方面的问题。

了解更多信息，请参阅《思科IBA使用入门》文档：
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

关于本指南

此附加部署指南包含以下章节：

- 业务概述——您的企业所面临的挑战。业务决策者可通过本章内容来了解介绍的解决方案与其企业运营的相关性。
- 技术概述——思科如何应对上述挑战。技术决策者可以利用此章节的内容了解解决方案的工作原理。
- 部署详情——解决方案的具体实施步骤介绍。系统工程师可以在这些步骤的指导下快速可靠地配置和启用解决方案。

本指南假定您已经阅读了本指南所依据的指南，如成功部署路线图中所示。

成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科IBA智能业务平台的信息，请访问：
http://www.cisco.com/go/cn/iba
如需要注册快速报价工具（QPT），请访问：
http://www.cisco.com/go/qpt

简介

业务概述

随着移动员工队伍日渐壮大，以及网络访问平台的多样化，企业纷纷想方设法来监控网络访问。企业不仅需要了解谁在访问其有线和无线网络，而且还要知道访问的时间和地点。此外，随着诸如智能手机和平板电脑等非传统设备的广泛采用，以及人们自带设备访问网络，企业需要知道有多少这样的设备正在联网。了解了这一信息，企业才能制定策略来防止非传统设备联网、仅限经批准的设备联网，或者使这些非传统设备更轻松地访问网络资源。

受到行业和法规遵从性（PCI、萨班斯一奥克斯利）的推动，企业需要能够报告谁在访问企业的信息、从哪里访问、以及使用哪类设备进行访问。诸如联邦信息处理标准（FIPS）和联邦信息安全管理法案（FISMA）等政府指令也要求各机构和实体与政府机构合作，跟踪此信息。在某些情况下，企业可以选择限制对于特定信息的访问，以遵守这些规定。

这一信息还可作为关键数据，用于生成高级安全策略。企业将此视作一项需要使用多种先进技术的艰巨任务，通常会因为不知道从何着手而延误了解决方案的实施。

本指南是部署基于身份的完整架构的第一步。未来的项目将阐述其它使用情况，侧重于提供执行、访客访问和机密性等功能的特性。

技术概述

思科身份服务引擎（ISE）是一种身份和访问控制策略平台，能够支持企业提高合规性、增强基础设施安全性和简化服务运营。思科ISE是Cisco TrustSec的一个核心组件。其架构使企业能够从网络、用户和设备收集实时的情景信息，通过将身份与诸如接入交换机、无线控制器和VPN网关等网元联系在一起，做出前瞻性策略决定。

这一部署使用思科ISE作为认证与记账服务器，为有线和无线网络以及使用RADIUS连接的远程接入VPN用户提供支持。思科ISE将作为现有活动目录（AD）服务的代理，为所有网络服务提供一个中央身份存储库。

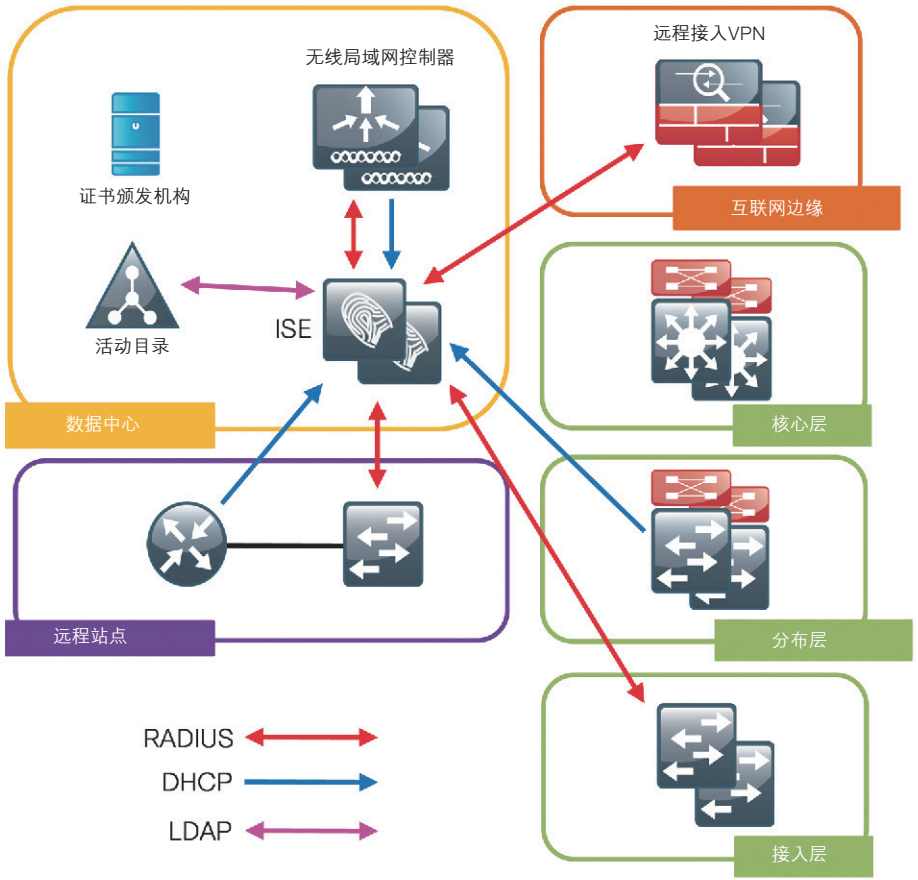
除了使用思科ISE进行认证，您还可以使用它对设备进行概况分析，以确定哪种设备类型可以访问网络。这项功能可通过基于特定特征，将网络流量与特定标准进行对比来完成。思科ISE当前包含多种探针，可支持动态主机配置协议（DHCP）、HTTP、RADIUS、域名系统（DNS）、简单网络管理协议（SNMP）陷阱和查询、以及Netflow。要分析流量，可将引擎部署为内置策略(inline policy)执行设备或者可将流量转发至引擎。例如，网络基础设施被配置为发送DHCP请求副本到思科ISE，以进行分析。之后该引擎将评估DHCP请求，根据请求中的数据识别设备。例如，引擎能够根据DHCP类标识符识别思科IP电话。

在局域网中，TrustSec有三种部署模式：监控模式、认证模式和执行模式。思科建议采用分阶段部署模式，由此可减少对网络访问的影响，同时逐步引入对网络的认证/授权。本指南将介绍在总部站点和远程站点部署监控模式，以及在数据中心集中部署思科ISE的情况。所使用的监控模式在总部站点和远程站点的接入层交换机上的IOS中部署了两个特性。第一个是MAC认证旁路（MAB），按MAC地址对交换机端口上的设备进行认证。监控模式会记录所连接的MAC地址并授权访问任意相连设备。第二个特性是802.1X开放模式，它允许交换机端口提供无限制的网络访问，即使未执行认证和授权也不受影响。这使得身份的部署不会影响现有连接。这种分阶段方法使我们能够为在未来转移到另一种模式（例如认证或执行模式）做好准备。在企业中，这些交换机配置将由思科局域网管理解决方案（LMS）4.1和全新Identity WorkCenter来管理。思科LMS通

过对身份部署执行网络就绪评估，为各种模式（监控、认证、执行）提供模板，并提供逐步向导来配置各种必要组件，从而简化了身份部署。

通过使用思科ISE作为支持无线802.1X认证和记账的RADIUS服务器，您可以将思科ISE集成到无线网络中。这项配置可在总部和远程站点网络中的每个无线局域网控制器（WLC）上完成。唯一例外的是用于访客访问的控制器。您也可以配置WLC，将DHCP请求转发至思科ISE，以对无线终端进行分析。

图1 – 思科ISE集成到思科IBA智能业务平台中



备 注

部署详情

此处描述的部署基于《面向大型企业的IBA智能业务平台一无边界网络局域网部署指南》中介绍的IP编址。本指南中使用的所有IP地址均为举例。您应使用适用于您架构的地址。

设备	IP地址	主机名
主用思科ISE	10.4.48.41	Ise-1.cisco.local
备用思科ISE	10.4.48.42	ise-2.cisco.local

流程

部署身份服务引擎

1. 设置初始主用引擎
2. 设置备用引擎
3. 配置证书信任列表
4. 配置思科ISE部署节点
5. 安装思科ISE许可证
6. 在思科ISE中配置网络设备
7. 配置思科ISE以使用活动目录
8. 禁用IP电话授权策略

程序1 设置初始主用引擎

步骤1：启动思科ISE，然后按照初始提示，输入setup（设置）。安装开始。

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost login: setup_
```

步骤2：输入主机名称、IP地址、子网掩码和引擎缺省路由。

Enter hostname[]: ise-1
Enter IP address[]: 10.4.48.41
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.48.1

步骤3：输入DNS信息。

Enter default DNS domain[]: cisco.local
Enter primary nameserver[]: 10.4.48.10
Add/Edit another nameserver? Y/N : n

步骤4：配置时间。

```
Enter primary NTP server[time.nist.gov]: ntp.cisco.local
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: PST8PDT
```

技术提示

时区缩写可在《思科身份服务引擎CLI参考指南》1.1版中找到：

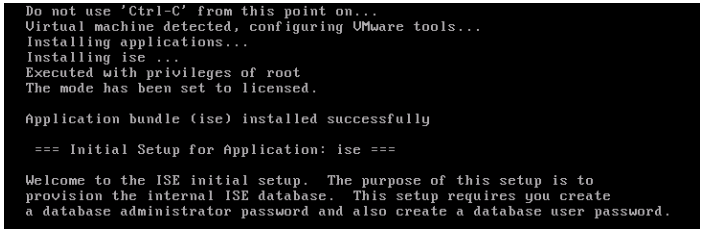
http://www.cisco.com/en/US/docs/security/ise/1.1/cli_ref_guide/ise_cli_app_a.html#wp1571855

步骤5：配置管理员帐户。

您必须配置一个管理员帐户，以访问CLI控制台。此帐户与用于访问GUI的帐户不同。

```
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

思科ISE完成安装并重启。此过程需要几分钟时间。您将需要在配置内部数据库期间输入一个新的数据库管理员密码和一个新的数据库用户密码。在安装过程中不要按Control-C，否则将会中止安装。



主用引擎现已安装。

程序2 设置备用引擎

设置备用引擎的步骤与设置主用引擎的步骤相同，唯一的区别就是针对引擎配置的IP地址和主机名称。要设置备用引擎，请按照程序1，使用备用引擎表中提供的值。

程序3 配置证书信任列表

这两款引擎使用公钥基础设施（PKI）来保护二者间的通信安全。最初，您在此部署中使用本地证书，并且必须在主用引擎和备用引擎之间配置一种信任关系。要完成此操作，您需要将本地证书从备用引擎导入主用引擎中。

步骤1：在您的浏览器中，连接到备用引擎的GUI，网址：http://ise-2.cisco.local

步骤2：在Administration（管理）> System（系统）中，选择Certificates（证书）。

步骤3：在Local Certificates（本地证书）窗口，选中备用引擎名称旁边的选项框，选择本地证书ise-2.cisco. local，然后点击Export（导出）。

步骤4：选择Export Certificate Only（仅导出证书），之后点击Export（导出）。

步骤5：当浏览器提示您保存文件到本地设备的某个位置时，选择要存放文件的位置，并加以说明。您将需要把这一文件导入到主用引擎中。

步骤6：在浏览器中，访问主用引擎的GUI，网址：http://ise-1.cisco.local。

步骤7：在Administration（管理）> System（系统）中，选择Certificates（证书）。

步骤8：在左侧的Certificate Operations（证书操作）窗格，点击Certificate Authority Certificates（证书颁发机构证书），然后点击Add（添加）。

步骤9：点击Certificate File（证书文件）字段旁边的Browse（浏览），找到从备用引擎导出的证书。该证书扩展名为.pem。

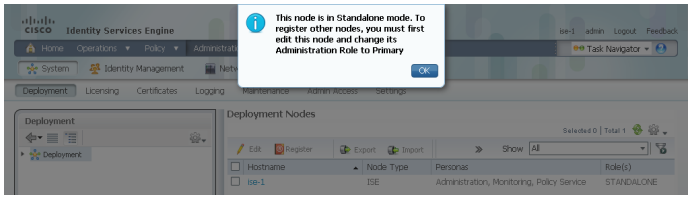
步骤10：点击Submit（提交）。

程序4　配置思科ISE部署节点

您可以配置思科ISE的各种功能在一个引擎上运行，或者在几个引擎间运行。这些功能包括管理、监视和策略服务等。在此示例安装中，您将部署一个主用引擎来执行所有三项功能，并部署一个备用引擎作为主用引擎的备份。

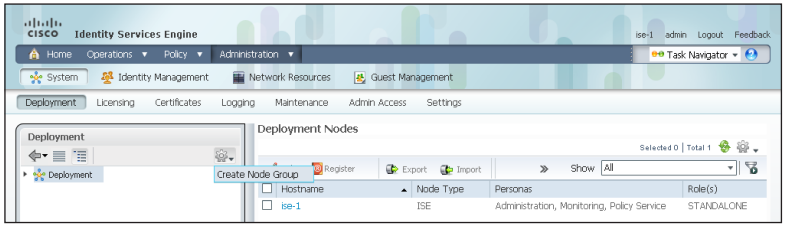
步骤1：连接至http://ise-1.cisco.local。

步骤2：在Administration（管理）菜单，选择System（系统），之后选择Deployment（部署）。出现一条消息，通知您此节点目前为独立节点。



步骤3：在Deployment（部署）窗格，点击齿轮图标，并选择Create Node Group（创建节点组）。

为了使这两个思科ISE设备能够共享策略和状态信息，它们必须位于一个节点组中。节点将使用IP组播来分发这一信息，因此它们需要能够通过IP组播进行通信。



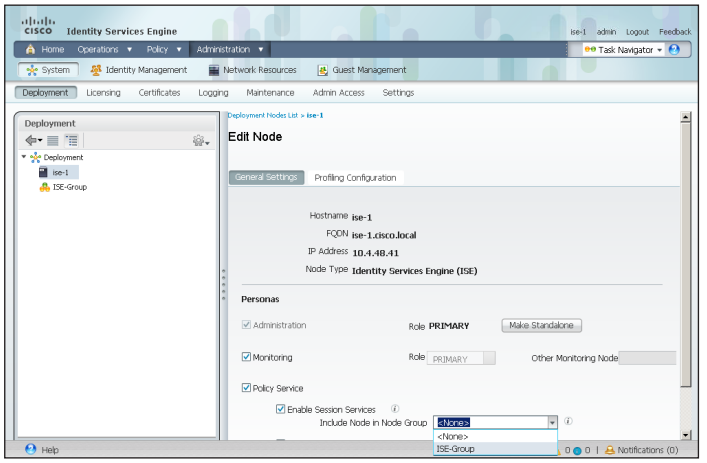
步骤4：配置节点组，节点组名称为ISE-Group，缺省组播地址为228.10.1.1.12。

步骤5：点击Submit（提交）。一个弹出窗口将显示该组已成功创建。点击OK（确定）。

步骤6：在左侧的Deployment（部署）窗格，展开Deployment（部署）。窗口中显示一个当前部署节点的列表。

步骤7：点击ise-1。通过此操作，您可以配置此部署节点。

步骤8：在General Settings（常规设置）选项卡下的Personas（角色）部分，点击Administration Role（管理角色）旁边的Make Primary（设为主用）。

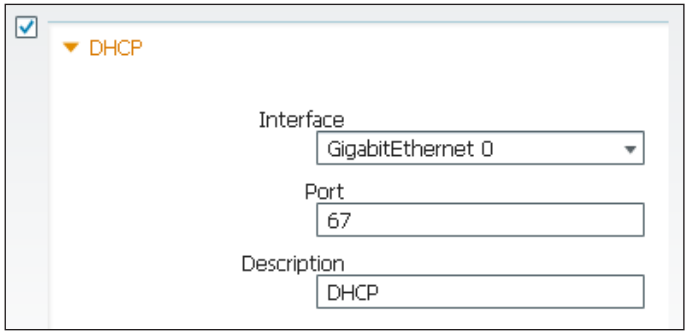


步骤9：从下拉菜单中选择ISE-Group节点组，将节点归入此节点组。

接下来，您将配置使用哪一方法来分析网络终端。

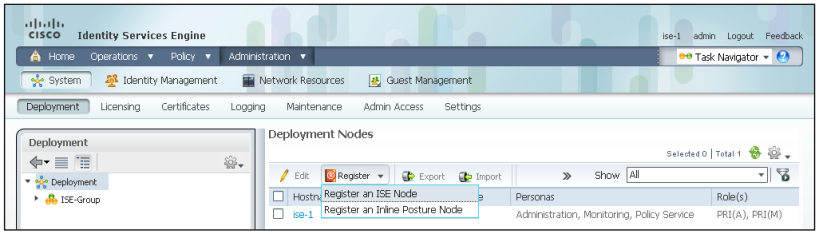
步骤10：点击Profiling Configuration（分析配置）选项卡。

步骤11：这一示例使用了DHCP和RADIUS。选中每一个旁边的选项框以启用这些方法，使用缺省参数，之后点击Save（保存）。



步骤12：在Edit Node（编辑节点）窗口，点击Deployment Nodes List（部署节点列表）。Deployment Nodes（部署节点）窗口打开。

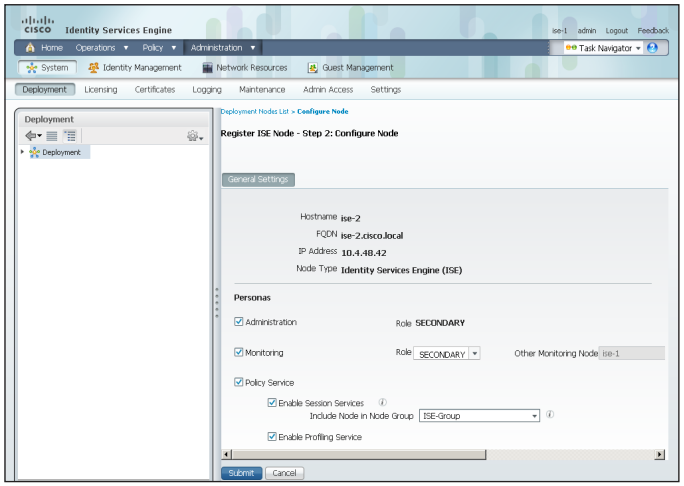
步骤13：点击Register（注册），之后选择Register an ISE Node（注册一个ISE节点）



步骤14：输入备用思科ISE的IP地址或主机名称，以及管理员帐户的凭证，点击Next（下一步）。

步骤15：配置ise-2作为组中的备用引擎，确保选中了所有选项框以启用所有角色，以及这一设备是备用引擎。从下拉菜单中选择节点组ISE-Group。

步骤16：点击Submit（提交）。节点进行注册，一个弹出窗口会显示流程是否成功。点击OK（确定）。



步骤17：在Deployment Nodes（部署节点）窗口，点击ise-2，点击Profiling Configuration（分析配置）选项卡，然后按您针对主用引擎所采用的方法配置DHCP和RADIUS选项。

步骤18：点击Save（保存）。

两个思科ISE装置现已配置为冗余对。

程序5 安装思科ISE许可证

思科ISE标配有针对基本和高级产品包的90天演示许可证。超过90天后，您需要获得思科的许可证。在冗余配置中，您只需在主用管理节点上安装许可证。

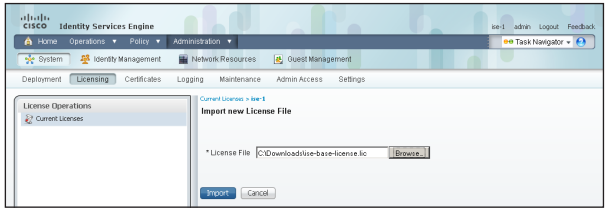
步骤1：将鼠标置于Administration（管理）之上，然后在菜单的System（系统）部分，选择Licensing（许可）。

注意，您在此只会看到一个节点，因为备用节点不需要许可证。

步骤2：点击思科ISE服务器的名称。此操作将允许您编辑许可证详情。

步骤3：在Licensed Services（许可的服务）下，点击Add Service（添加服务）。

步骤4：点击Browse（浏览），找到您的许可证文件，然后点击Import（导入）。



如果您要安装多个许可证，则每个许可证均需重复此过程。

技术提示

当安装Base（基本）许可证和Advanced（高级）许可证时，必须首先安装基本许可证。

程序6 在思科ISE中配置网络设备

配置思科ISE，以接受来自网络设备的认证请求。RADIUS需要共享密钥，以启用加密通信。每个将使用思科ISE进行认证的网络设备都需要拥有此密钥。

步骤1：将鼠标置于Administration（管理）之上，然后在菜单的Network Resources（网络资源）部分，选择Network Devices（网络设备）。

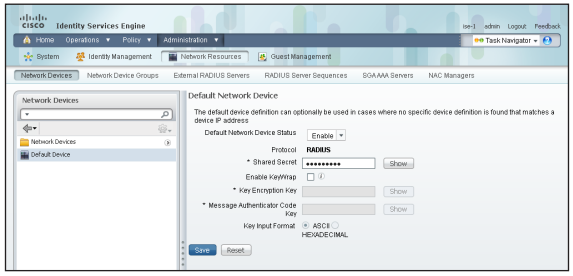
步骤2：在左侧窗格，点击Default Device（缺省设备）。

技术提示

每个网络设备可单独进行配置，或者可按位置、设备类型或IP地址范围进行分组。另一个选项是使用缺省设备来为未进行专门配置的设备配置参数。我们的所有网络设备必须使用相同的密钥，因此为了简单起见，我们将使用Default Device（缺省设备）。

步骤3：从下拉菜单中选择Enable（启用），启用Default Network Device Status（缺省网络设备状态）。

步骤4：输入RADIUS共享密钥，然后点击Save（保存）。



程序7　配置思科ISE以使用活动目录

思科ISE将使用现有的活动目录（AD）服务器作为外部认证服务器。首先，您必须配置外部认证服务器。

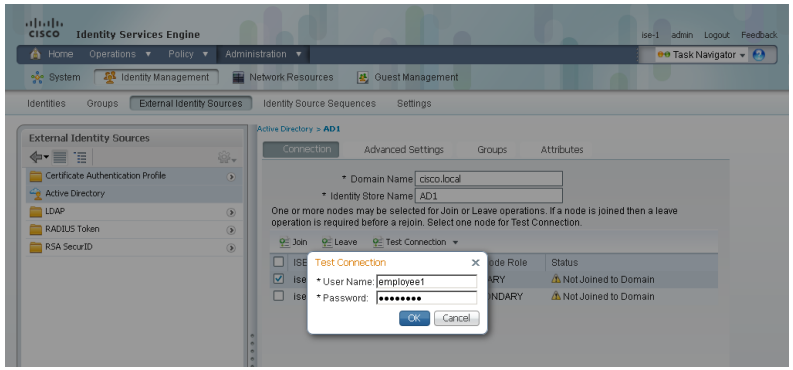
步骤1：将鼠标置于Administration（管理）之上，然后在菜单的Identity Management（身份管理）部分，选择External Identity Sources（外部身份源）。

步骤2：在左侧窗格，点击Active Directory（活动目录）。

步骤3：在Connection（连接）选项卡，输入AD域（例如“cisco.local”）和服务器的名称（例如“AD1”），配置到AD服务器的连接，之后点击Save Configuration（保存配置）。

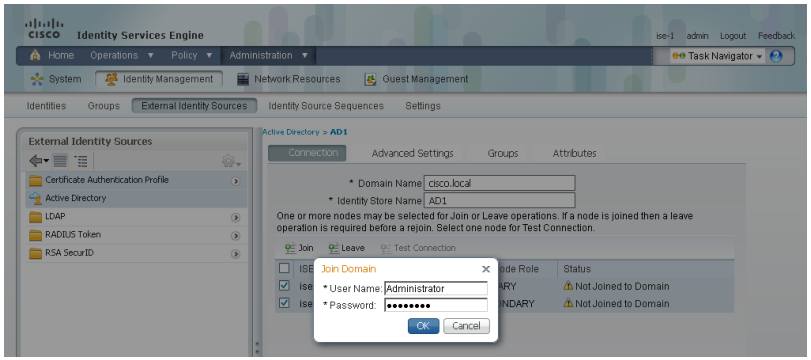
步骤4：选中节点旁边的选项框，然后点击Test Connection（测试连接），选择Basic Test（基础测试），验证这些设置。

步骤5：输入域用户的凭证，然后点击OK（确定）。



步骤6：选中每个节点旁边的选项框，然后点击Join（加入）。

步骤7：输入域管理员帐户的凭证。思科ISE现在被加入到AD域。

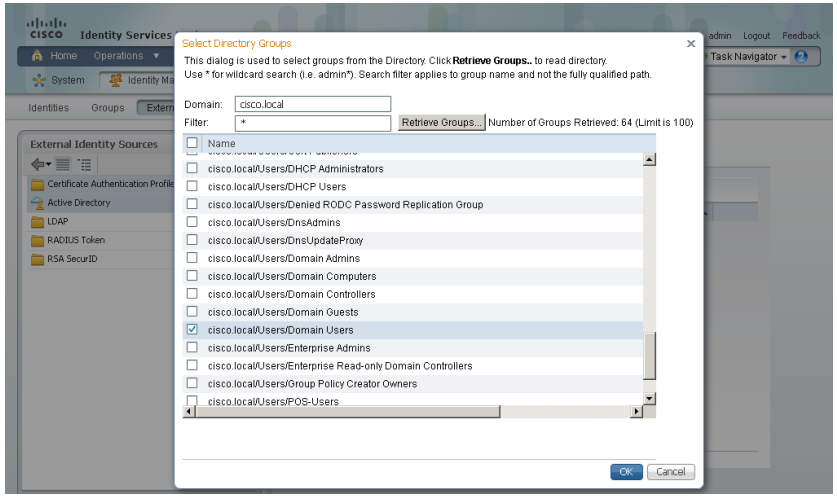


接下来，选择思科ISE将使用AD中的哪一个组进行认证。

步骤8：点击Groups（组）选项卡，点击Add（添加），然后点击Select Groups from Directory（从目录中选择组）。

步骤9：搜索您想添加的组。域字段已经填写。缺省过滤器是一个通配符，可列出所有组。点击Retrieve Groups（检索组），以获得您域中所有组的列表。

步骤10：选中您希望用于进行认证的组，然后点击OK（确定）。例如，对于此域中的所有用户，选择组<domain>/Users/Domain Users（<域>/用户/域用户）。



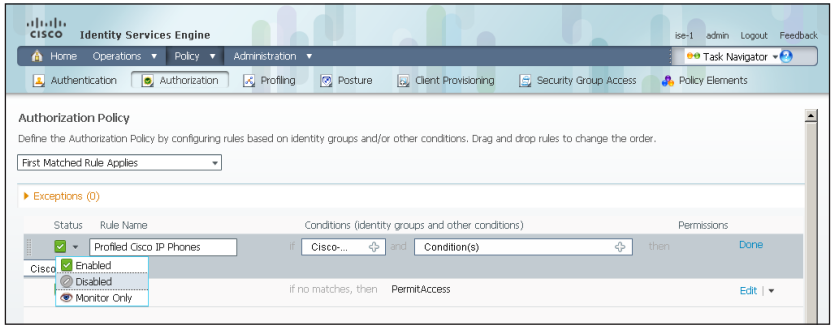
步骤11：点击Save Configuration（保存配置）。

程序8 禁用IP电话授权策略

针对已进行了分析的思科IP电话，系统提供有缺省策略。这一配置文件适用于电话连接的端口上的可下载访问列表。由于没有进行策略执行，此规则应禁用。

步骤1：在菜单栏，将鼠标置于Policy（策略）之上，然后点击Authorization（授权）。

步骤2：针对Profiled Cisco IP Phones（已分析思科IP电话）规则选择Edit（编辑），点击绿色对勾图标，选择Disabled（禁用），点击Done（完成），然后点击Save（保存）。



流程

支持了解局域网情况

1. 配置MAC认证旁路
2. 为有线用户配置802.1X
3. 在接入层启用RADIUS
4. 启用身份
5. 禁用端口安全计时器
6. 配置局域网配置文件

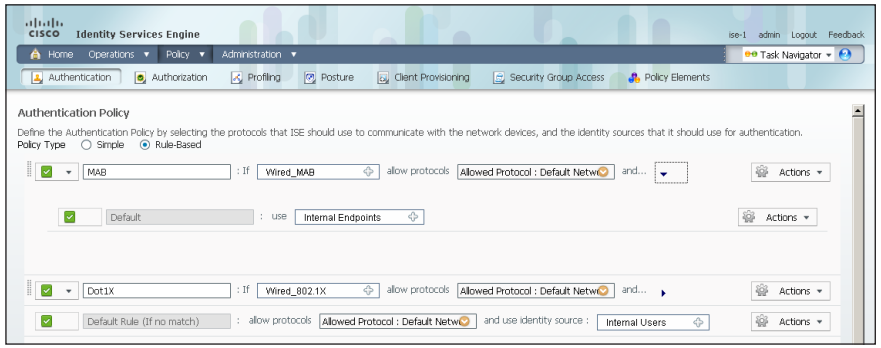
思科ISE现已针对身份进行了配置。下一步是使用Cisco LMS 4.1和Identity Workcenter来配置支持身份的交换机。

程序1 配置MAC认证旁路

MAC认证旁路使您可以在交换机上配置特定的计算机MAC地址，以绕过认证流程。对于Monitor Mode（监控模式），这是必要的，因为我们没有执行认证。MAB将被配置为允许任意MAC地址进行认证。

步骤1：将鼠标置于Policy（策略）之上，然后选择Authentication（认证）。Policy Type（策略类型）基于规则。
系统中有两项缺省规则，分别为MAB和Dot1X。

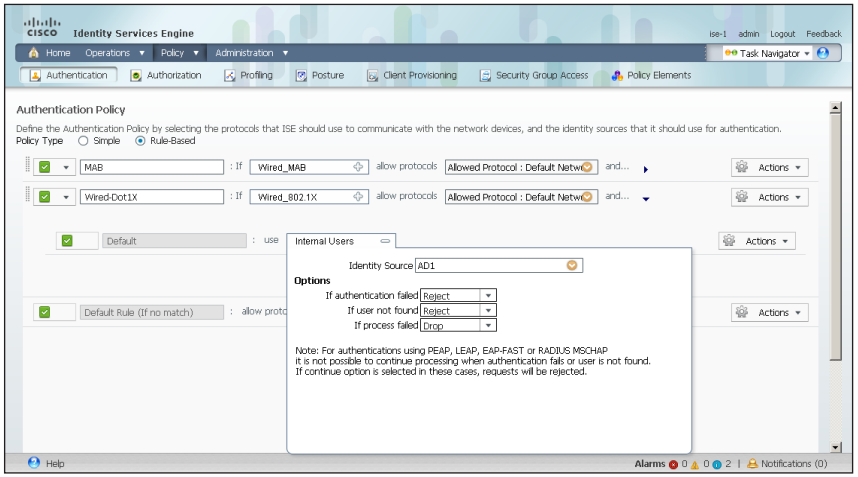
步骤2：使用缺省MAB策略。点击MAB规则“and…”右侧的黑色三角形。用于MAB规则的身份存储库出现。



接下来，更改用于分析的Internal User（内部用户）数据库上的选项。

步骤3：点击Internal Endpoints（内部终端）旁边的“+”符号。在本部署示例中，我们将允许所有终端进行认证。如果在数据库中没有找到MAC地址，您必须要绕过认证并继续。对于认证失败和未发现用户的情况，从下拉菜单中选择Continue（继续）。

步骤4：点击窗口中的任意位置继续，然后点击Save（保存）。



程序2 为有线用户配置802.1X

引擎上已经配置了Dot1X规则。在本部署示例中，尽管您目前不会采用802.1X请求者部署任何有线终端，但您仍应配置这一规则，为下一阶段的身份部署做好准备。

步骤1：将鼠标置于Policy（策略）之上，之后从菜单中选择Authentication（认证）。

步骤2：为了区分此规则与无线802.1X规则，将它重新命名为“Wired-Dot1X”。

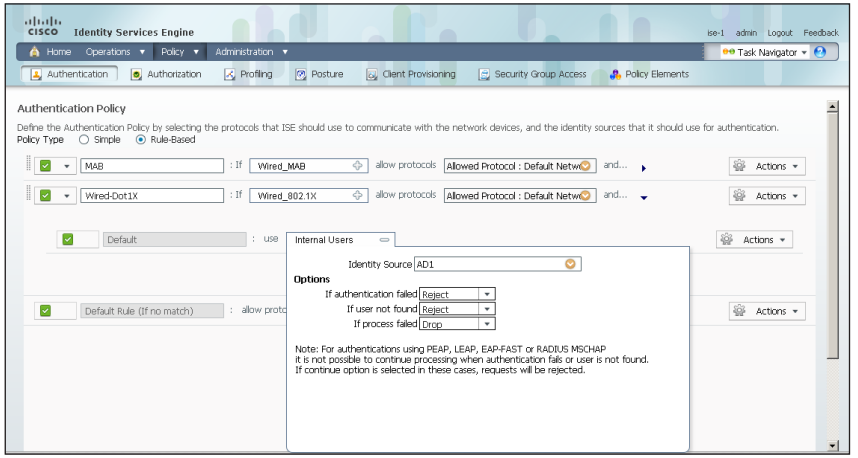
步骤3：点击Wired-Dot1X规则“and…”右侧的黑色三角形。用于此规则的身份存储库出现。

缺省身份存储库为内部用户数据库。针对802.1X，使用您之前定义的活动目录服务器。

步骤4：点击Internal Users（内部用户）旁边的“+”符号。通过此操作您可以编辑身份存储库和参数。

步骤5：从Identity Source（身份源）下拉列表中，选择先前定义的AD服务器AD1，针对这一身份源使用缺省选项，然后点击窗口中的任意位置继续。

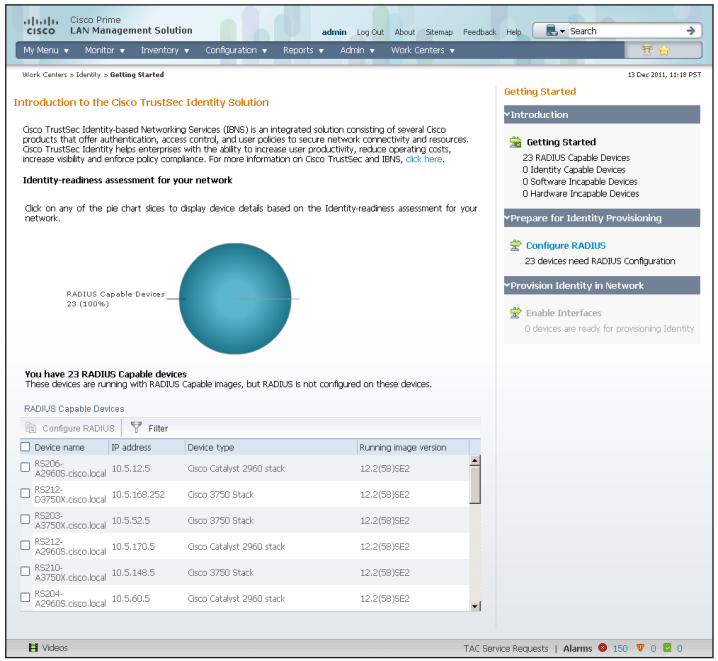
步骤6：点击Save（保存）。



程序3　在接入层启用RADIUS

步骤1：采用Web浏览器连接到思科LMS，例如：https://lms. cisco.local.

步骤2：将鼠标置于Workcenters之上，然后从Identity（身份）部分选择Getting Started（开始）。这将可显示该网络的Identity Readiness Assessment（身份就绪评估），从而检验软件版本是否支持身份特性，以及交换机是否能够运行RADIUS。



接下来，通过在交换机上启用RADIUS来配置身份。

步骤3：在支持RADIUS的设备表中，选择您希望启用RADIUS的交换机，然后点击Configure RADIUS（配置RADIUS）。

步骤4：选择RADIUS Group（RADIUS组）按钮，然后填写字段。输入ISE-Group作为RADIUS组名称，然后使用先前程序中所用的值作为Shared Key（共享密钥）。

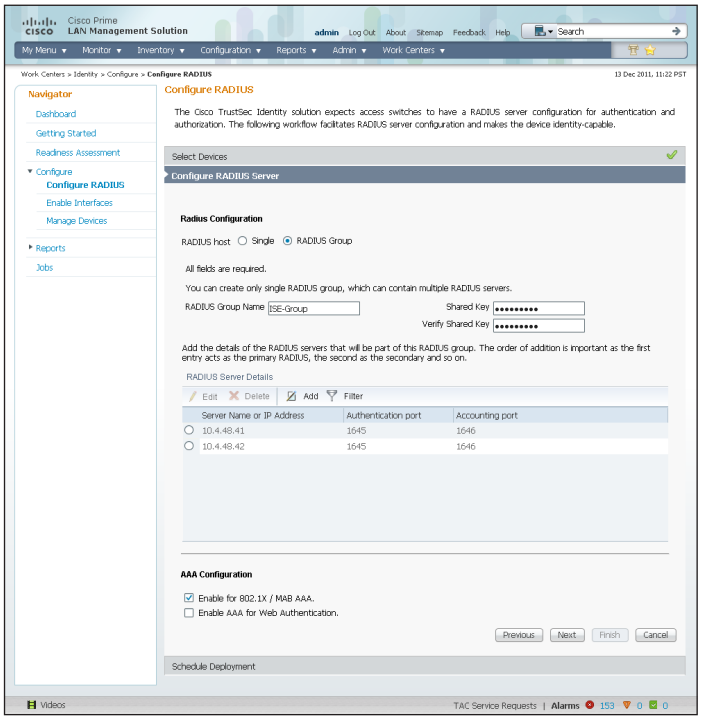
步骤5：在RADIUS Server Details（RADIUS服务器详情）部分，点击Add（添加）。

步骤6：在弹出窗口中，输入10.4.48.41作为RADIUS服务器IP地址，然后点击Save and add another（保存并添加另一个）。

步骤7：针对第二台RADIUS服务器输入10.4.48.42，然后点击Save（保存）。RADIUS服务器组已经配置完成。

步骤8：在AAA Configuration（AAA配置）部分，确保仅选择Enable for 802.1X / MAB AAA（针对802.1X / MAB AAA启用）。此时将出现一条警告信息，提示未配置用于Web认证的AAA。点击OK（确定）。

步骤9：点击Next（下一步），进行下一步。



技术提示

通过点击Preview CLI（预览CLI），您可以查看将被推送至交换机的CLI命令。

步骤10：输入任务描述，然后点击Finish（完成）以立即部署。

步骤11：当您收到关于添加AAA命令的警告时，点击Yes（是），然后在任务创建后生成的弹出窗口中点击OK（确定）。

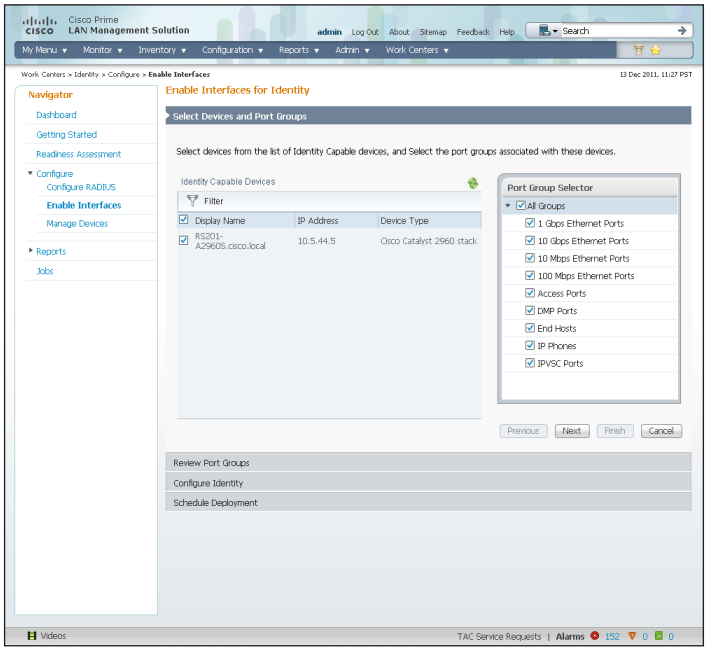
程序4　启用身份

身份配置会在交换机上启用监控模式。此操作会启用802.1X和MAC认证旁路（MAB），但不会启用认证策略。这将能够监控端口，而不会中断当前的网络活动。

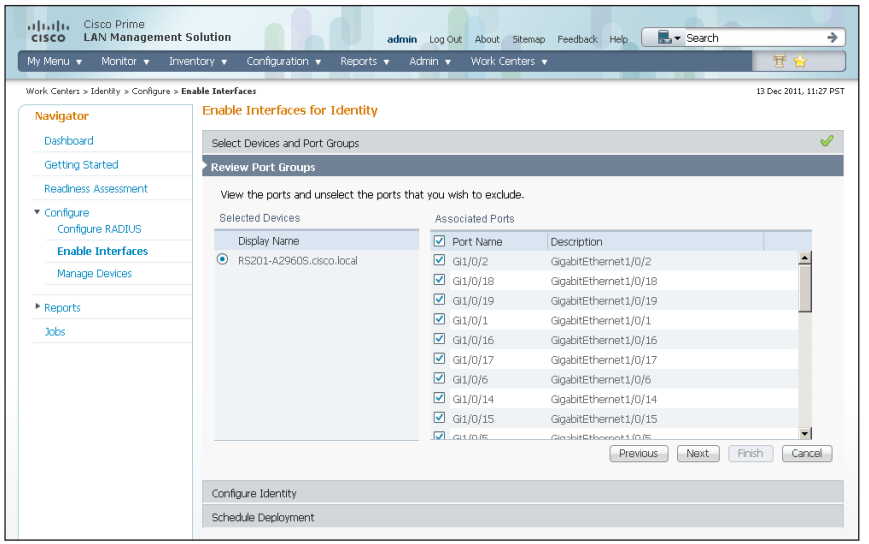
步骤1：将鼠标置于Work Centers（工作中心）上，然后在Identity（身份）部分选择Configure（配置）。

步骤2：在左侧的Navigator（导航器）窗格，点击Enable Interfaces（启用接口）。

步骤3：从列表中选择先前为RADIUS配置的交换机，并在端口组选择器中选择All Groups（所有组），然后点击Next（下一步）。



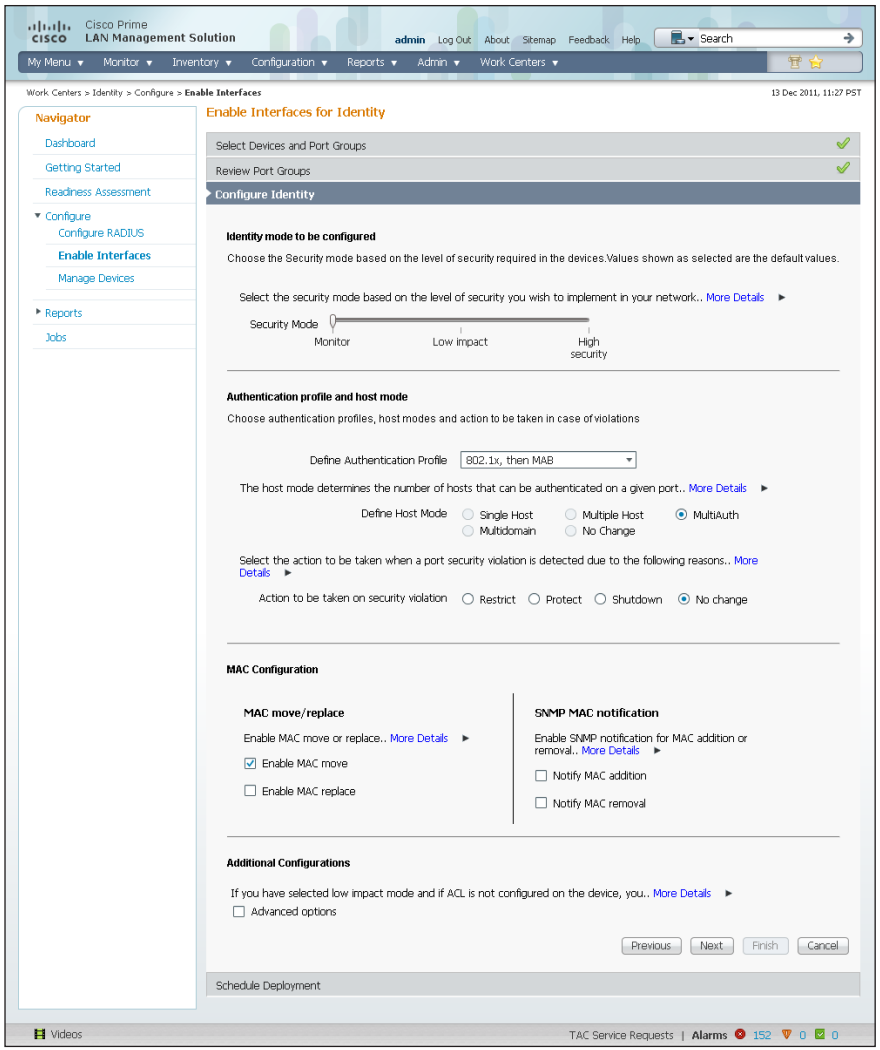
步骤4：选择您希望启用身份的端口旁边的复选框，然后点击Next（下一步）。



接下来，配置监控模式。

步骤5：将Security Mode（安全模式）滑块移到缺省的Monitor（监控）位置。

步骤6：在Authentication Profile（认证配置文件）部分，选择802.1X，然后在Define Authentication Profile（定义认证配置文件）滑块中选择MAB，确保在Define Host Mode（定义主机模式）部分选择MultiAuth，并针对在违反安全规定时要采取的Action（行动）选择No Change（无变更），然后在MAC Configuration（MAC配置）部分，确保仅选择Enable MAC Move（启用MAC移动）。



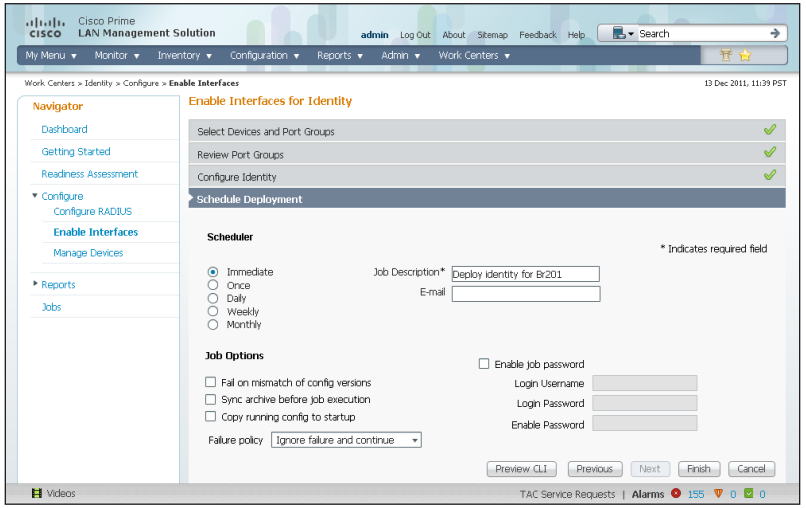
步骤7：点击Next（下一步）。身份配置完成。

接下来，您必须创建一项部署任务，以便将该配置交付给交换机。

步骤8：在Job Description（任务描述）字段中输入对部署任务的描述，然后点击Finish（完成）提交任务。点击OK（确定）。

技术提示

通过点击Preview CLI（预览CLI），您可以查看将被推送至交换机的CLI命令。



在前两个程序完成时，添加到交换机配置的全局命令如下：

```
aaa group server radius ISE-Group
 server 10.4.48.41
 server 10.4.48.42

aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa authorization configuration default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group

authentication mac-move permit
dot1x system-auth-control
```

```
radius-server host 10.4.48.41
radius-server host 10.4.48.42
radius-server key [key]
```

此程序完成时添加的接口命令如下:

```
interface [interface]
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

程序5　禁用端口安全计时器

当前的思科IBA智能业务平台设计结合使用了Port Security（端口安全）来提供一定水平的安全性，并防止非法设备连接。然而，802.1X也提供了这一功能，当在一个端口上同时启用这两项功能时，会出现冲突。因为端口安全性功能和802.1X都各有一组计时器，因此这种冲突在非活动计时器上表现得尤其明显。这一冲突会导致每当端口安全超时的时候，802.1X就会重新进行认证。为避免这种问题，需要禁用端口安全计时器。

步骤1：访问https://lms.cisco.local，连接到思科LMS服务器。

步骤2：将鼠标置于Configuration（配置）上，然后在Tools（工具）标题下选择NetConfig。此操作将打开Job Browser（任务浏览器）。

步骤3：点击Create（创建）。通过此操作，您可以配置新的任务。

步骤4：选择Port based（基于端口），然后点击Go（开始）。

步骤5：点击All Devices（所有设备）树旁边的“+”符号，选择您正在配置的交换机，然后点击Next（下一步）。

技术提示

在本例中，仅配置一个交换机，但您可以选择配置多个交换机来完成一个大型部署。Group Selector（组选择器）允许您按预定义的组或型号来选择交换机。

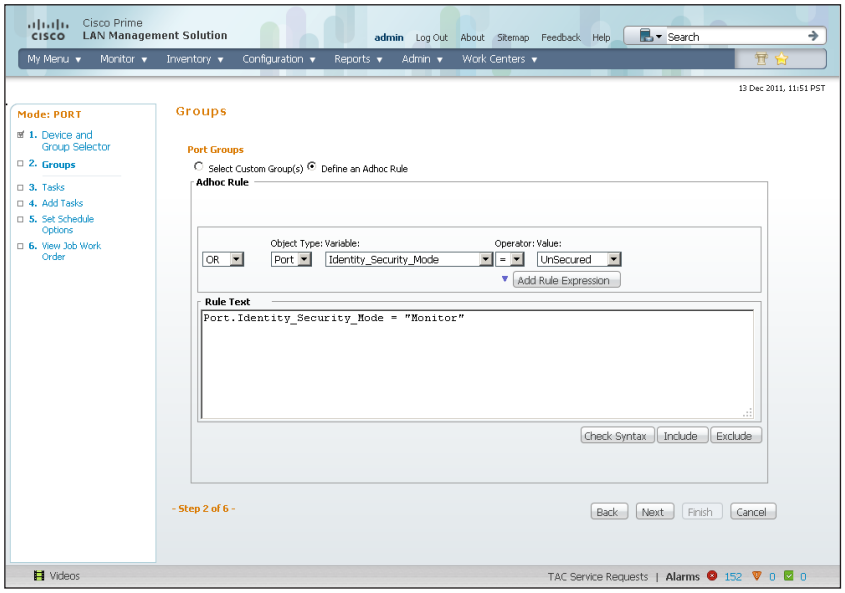
步骤6：选择Define an Ad-Hoc Rule（定义一个临时规则）。这将打开一个新屏幕。

步骤7：针对临时规则，对象类型选择Port（端口）。

步骤8：从Variable（变量）下拉菜单中，选择Identity_Security_Mode。

步骤9：Operator（运算符）选择“=”，Value（值）选择Monitor（监控）。

步骤10：点击Add Rule Expression（添加规则表达式），然后点击Next（下一步）。



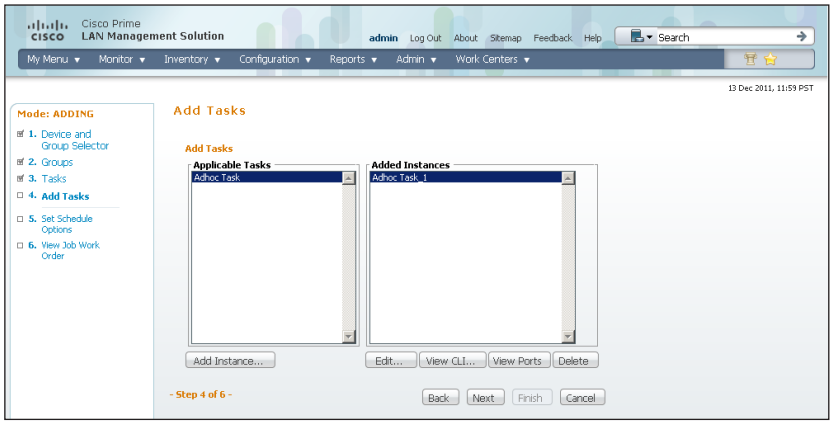
步骤11：在Task Selector（任务选择器）中，选择Adhoc Task（临时任务），然后点击Next（下一步）。

步骤12：点击Add Instance（添加实例），然后在新窗口中添加移除端口安排配置所必要的CLI命令。

```
no switchport port-security aging time
no switchport port-security aging type
no switchport port-security violation
```

步骤13：点击Applicable Devices（适用设备），选择将采用这一配置的交换机，点击Close（关闭），然后点击Save（保存）。

步骤14：在返回至Add Tasks（添加任务）窗口后，点击Next（下一步）。



步骤15：填写任务描述，然后点击Next（下一步），提交任务立即进行部署。

步骤16：点击Finish（完成），然后当您收到任务已成功提交的通知时点击OK。

程序6 配置局域网配置文件

思科ISE对终端进行概况分析的方式之一是检查从设备发出的DHCP请求。为了将这些请求转发至ISE，需要在主机网络的路由器接口上配置一个帮助地址。帮助地址采用广播数据包，并使之成为到指定地址的定向广播。

步骤1：连接到终端缺省路由器的控制台。

步骤2：在CLI，输入以下命令：

```
Router#ena
Router#conf terminal
Router(config)#interface [interface]
Router(config-if)#ip helper-address 10.4.48.41
Router(config-if)#ip helper-address 10.4.48.42
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
```

流程

支持了解无线网络情况

1. 为无线终端配置802.1X
2. 禁用思科ISE上的EAP-TLS
3. 添加ISE作为RADIUS认证服务器
4. 禁用原始RADIUS服务器
5. 添加ISE作为RADIUS记账服务器
6. 在WLC上添加备用DHCP服务器

要对无线客户端进行认证，您需要配置无线局域网控制器（WLC），以使用新的思科ISE服务器作为RADIUS服务器进行认证和记账。现有条目被禁用，以便如果移至思科ISE后出现任何问题，您可以快速恢复原始配置。此外，将WLC配置为采用思科ISE作为备用DHCP服务器，以便能够从来自这些客户端的DHCP请求中获得分析信息。

程序1 为无线终端配置802.1X

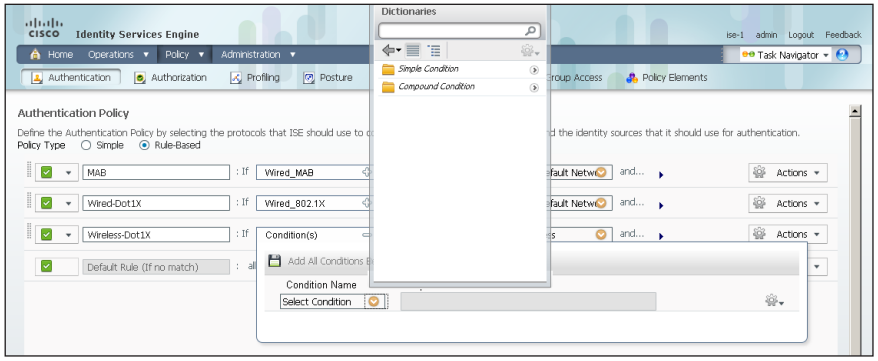
要区分认证日志中的无线用户，需要制定一条规则来确定无线用户进行认证的时间。

步骤1：转至Authentication Policy（认证策略）选项卡，将鼠标置于Policy（策略）之上，然后从菜单中选择Authentication（认证）。

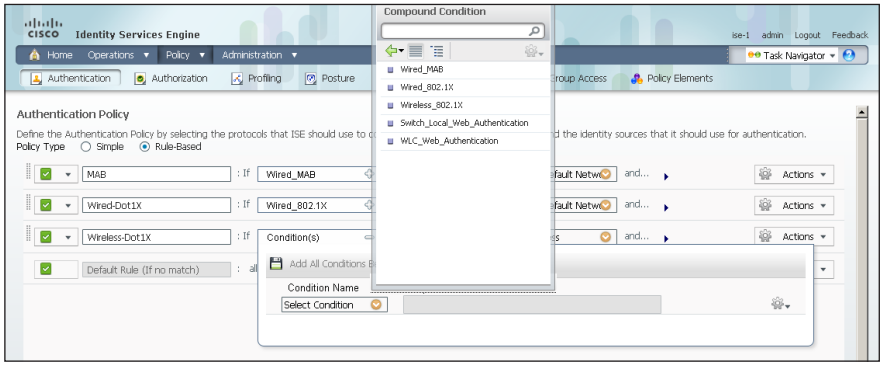
步骤2：点击用于Default Rule（缺省规则）的Actions（行动）按钮，并选择Insert new row above（在上面插入新行）。一个新规则“Standard Policy 1”创建完成。

步骤3：将“Standard Rule 1”重新命名为“Wireless-DotIX”。点击Condition(s)（条件）选项框中的“+”符号，并选择Select Existing Condition from Library（从库中选择现有条件）。

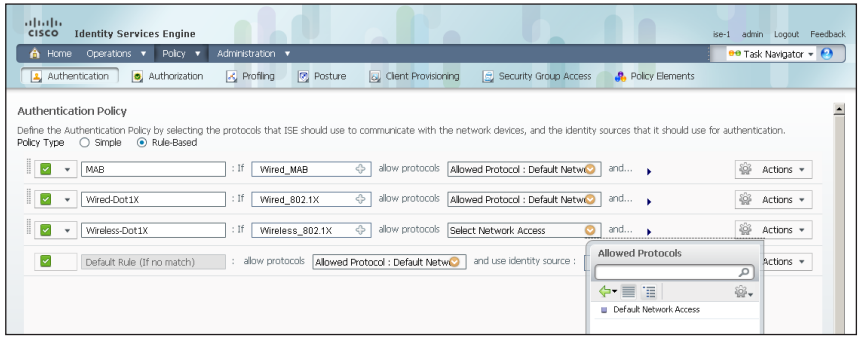
步骤4：在Select Condition（选择条件）下拉列表中，点击Compound Condition（复合条件）旁边的“>”符号。



步骤5：选择Wireless_802.1X，然后点击任意位置继续。



步骤6：点击Select Network Access（选择网络访问）下拉列表，点击Allowed Protocols（允许的协议）旁边的“>”符号，然后选择Default Network Access（缺省网络访问）。

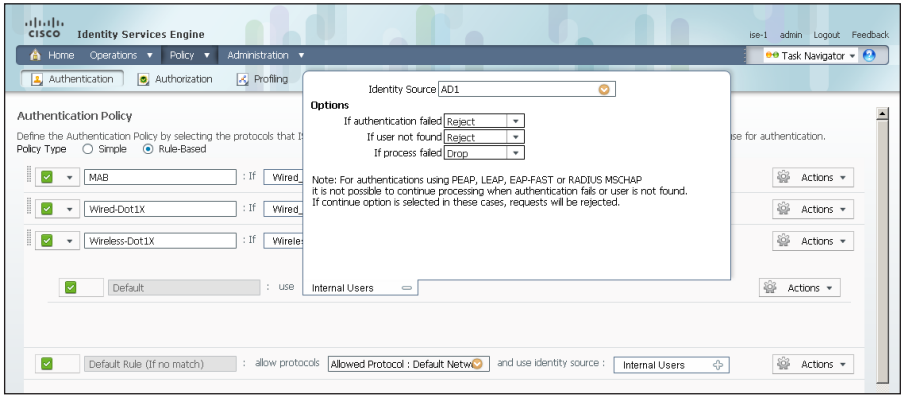


步骤7：点击Wireless-Dot1X规则“and…”右侧的黑色三角形。用于此规则的身份存储库出现。

步骤8：点击Set Identity Source（设定身份源）旁边的“+”符号。

步骤9：在Identity Source（身份源）下拉列表中，选择先前定义的AD服务器，如AD1。

步骤10：为这一身份源使用缺省选项，点击窗口中的任意位置继续，然后点击Save（保存）。



程序2　禁用思科ISE上的EAP-TLS

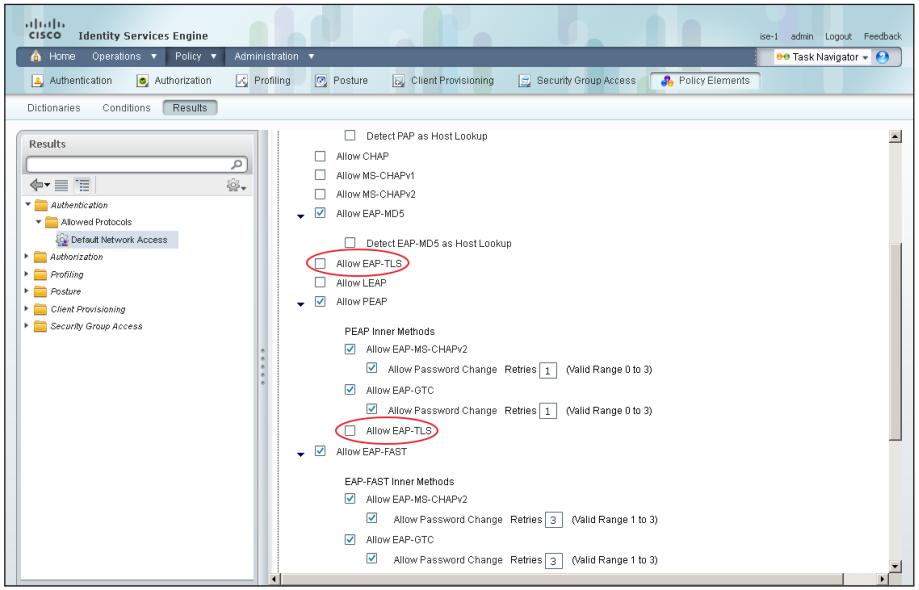
对于当前未采用数字证书的无线部署，您需要禁用EAP-TLS，以允许客户端登录。在本部署的以后阶段，您将部署数字证书。

步骤1：在菜单栏上，将鼠标置于Policy（策略）之上，然后在菜单的Policy Elements（策略元素）部分，选择Results（结果）。

步骤2：在左侧窗格，双击Authentication（认证）。此操作将展开选项。

步骤3：双击Allowed Protocols（允许的协议），然后选择Default Network Access（缺省网络访问）。

步骤4：取消选中全局Allow EAP-TLS（允许EAP-TLS）复选框，在PEAP设置下，取消选中Allow EAP-TLS（允许EAP-TLS）复选框，然后点击Save（保存）。



程序3　添加ISE作为RADIUS认证服务器

架构中的每一个无线局域网控制器（WLC）均需要执行这一程序，其中位于隔离区（DMZ）的访客WLC例外。

步骤1：访问https://wlc1.cisco.local，转至WLC控制台。

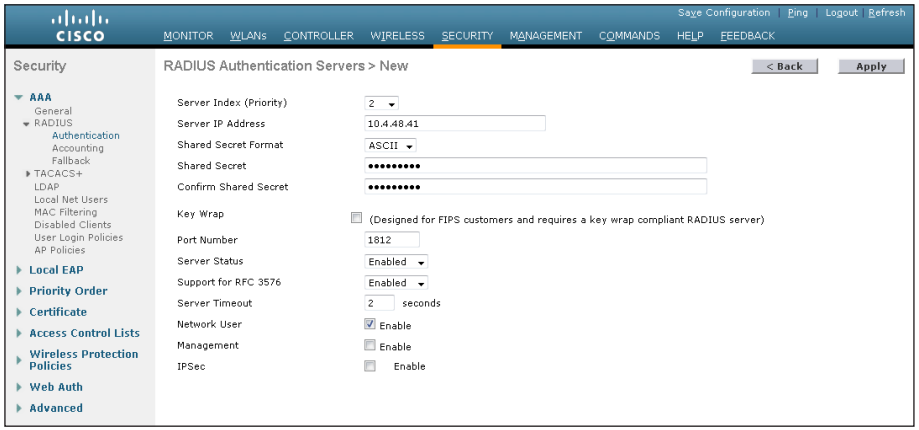
步骤2：在菜单栏，点击Security（安全性）。

步骤3：在左侧窗格中，点击RADIUS部分下的Authentication（认证）。

步骤4：点击New（新建）。一个新服务器被添加。

步骤5：输入“10.4.48.41”作为新服务器的IP地址，并输入您的RADIUS共享密钥。

步骤6：在Management（管理）旁边，取消选中Enable（启用）复选框，之后点击Apply（应用）。



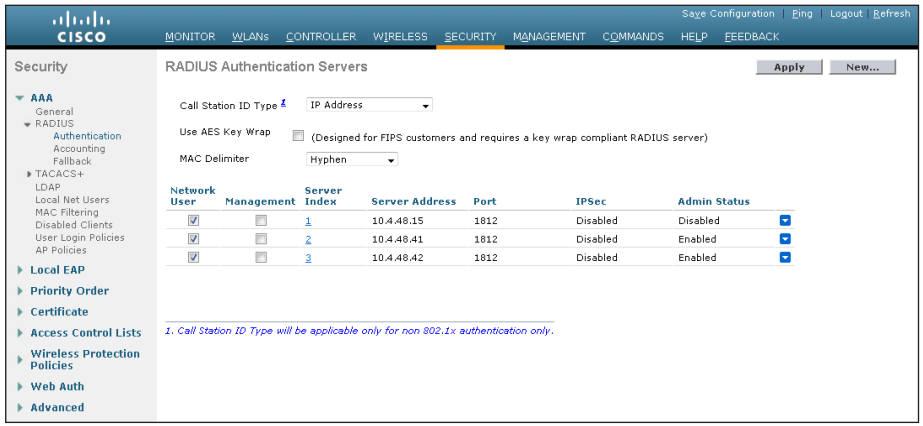
步骤7：重复步骤4到步骤6，将备用引擎10.4.48.42添加到WLC配置。

程序4 禁用原始RADIUS服务器

添加思科ISE作为RADIUS服务器后，禁用当前使用的RADIUS服务器。通过禁用服务器，而不是删除服务器，您可根据需要轻松切换回来。架构中的每一个无线局域网控制器（WLC）均需要执行这一程序，其中位于隔离区（DMZ）的访客WLC例外。

步骤1：在RADIUS Authentication Servers（RADIUS认证服务器）页面，点击原始RADIUS服务器的Server Index（服务器索引），然后针对Server Status（服务器状态）选择Disabled（禁用）。点击Apply（应用）。

步骤2：在RADIUS Authentication Servers（RADIUS认证服务器）屏幕，点击Apply（应用）。



程序5 添加ISE作为RADIUS记账服务器

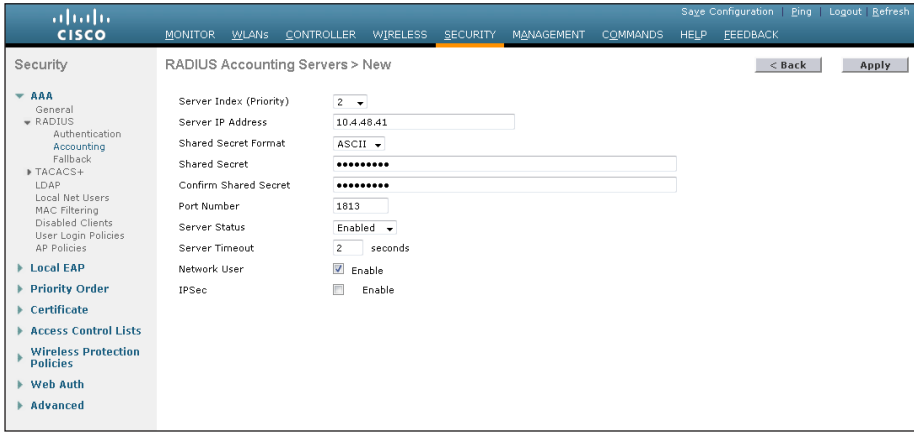
架构中的每一个无线局域网控制器（WLC）均需要执行这一程序，其中位于隔离区（DMZ）的访客WLC例外。

步骤1：在菜单栏，点击Security（安全性）。

步骤2：在左侧窗格中，点击RADIUS部分下的Accounting（记账）。

步骤3：点击New（新建）。一台新服务器被添加。

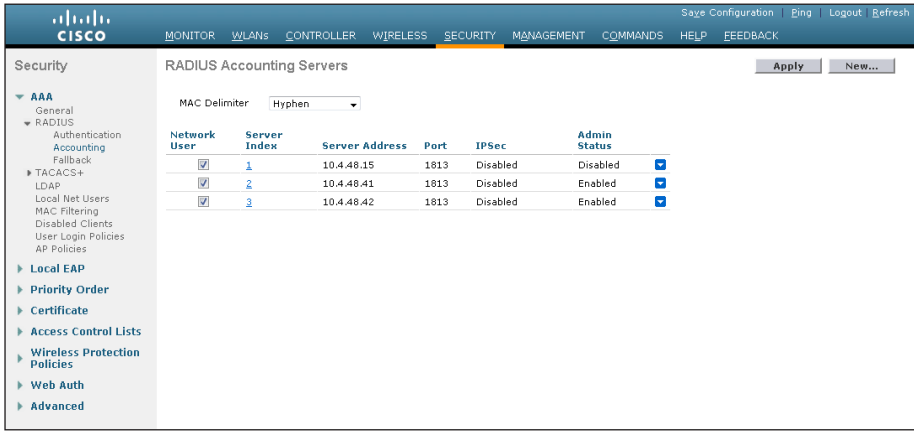
步骤4：输入“10.4.48.41”作为新服务器的IP地址，并输入您的RADIUS共享密钥，然后点击Apply（应用）。



步骤5：重复步骤4，将备用引擎10.4.48.42添加到WLC配置。

步骤6：在RADIUS Accounting Servers（RADIUS记账服务器）页面，点击原始RADIUS服务器的Server Index（服务器索引），然后针对Server Status（服务器状态）选择Disabled（禁用）。点击Apply（应用）。

步骤7：在RADIUS Accounting Servers（RADIUS记账服务器）屏幕，点击Apply（应用）。



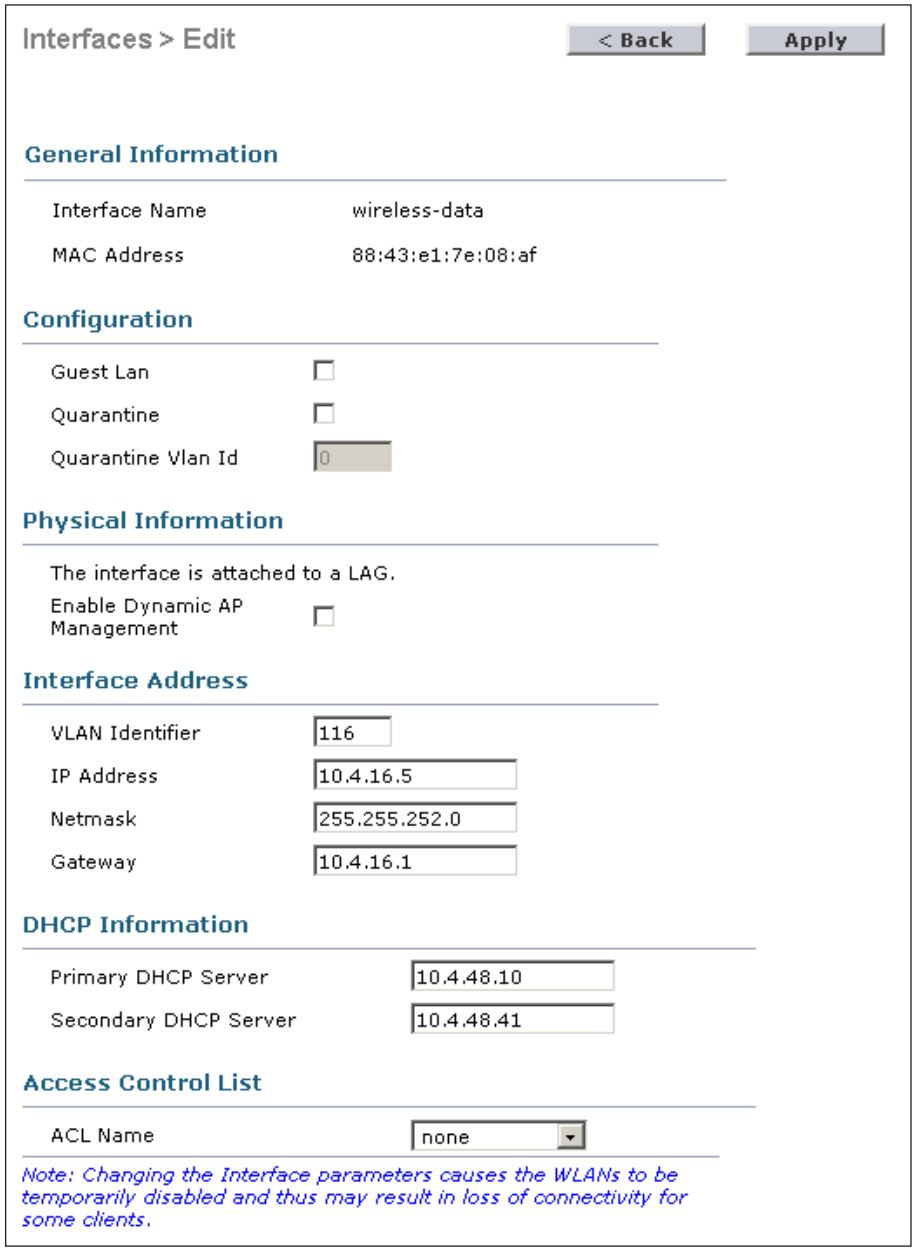
程序6　在WLC上添加备用DHCP服务器

您需要为WLC配置添加一台备用DHCP服务器，以发送DHCP请求到引擎，进行终端分析。

步骤1：在WLC上，转至Controller（控制器）> Interfaces（接口）。为您希望监控的客户端选择接口。

步骤2：在DHCP Information（DHCP信息）部分，添加思科ISE服务器作为备用DHCP服务器，然后点击Apply（应用）。

步骤3：当出现一条警告消息，提示需要禁用WLAN时，点击OK（确定）。



步骤4：点击Save Configuration（保存配置），然后点击OK（确定）。

目前，网络基础设施已启用，以便监控网络，进而确定连接设备的类型。另外，针对无线网络我们还启用了采用ISE的认证。这一部署阶段非常适合用来测试部署和监控网络访问。一些企业机构可能不需要实施下一阶段，可选择在此阶段停止。

流程

部署数字证书

1. 安装证书颁发机构
2. 为域安装可信的根证书
3. 在AD服务器中安装可信的根
4. 从CA中请求用于ISE的证书
5. 下载CA根证书
6. 颁发用于ISE的证书
7. 在ISE中安装可信的根证书
8. 在ISE中安装本地证书
9. 删除旧的证书和请求

在下一阶段部署中，您要配置基础设施，以支持将数字证书用于用户和计算机认证。在部署802.1X时使用数字证书是思科的一项最佳实践。在本部署示例中，您将向Microsoft Windows XP、Windows 7终端以及Apple Mac OS X设备部署数字证书。您将使用的证书颁发机构(CA)是嵌入至Windows Server 2008 Enterprise的一个组件，您要在现有活动目录(AD)服务器中将其启用。

程序1 安装证书颁发机构

步骤1：在AD服务器上安装企业根证书颁发机构。

技术提示

Microsoft Windows Server 2008 Active Directory证书服务逐步指南：
http://technet.microsoft.com/en-us/library/cc772393%28WS.10%29.aspx

程序2 为域安装可信的根证书

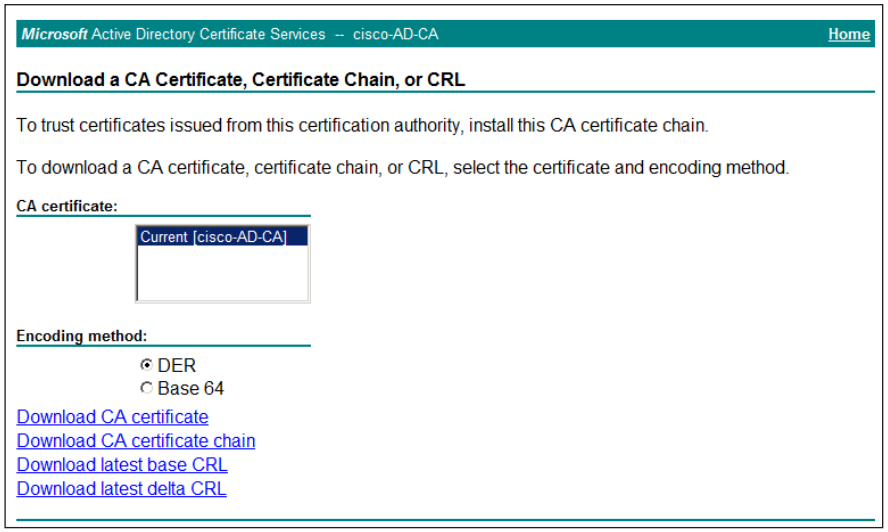
在AD控制器上安装可信的根证书并将其分发至客户端，以便来自CA服务器的证书成为可信的证书。

步骤1：在CA控制台中，启动Web浏览器，然后连接至证书颁发机构，https://ca.cisco.local/certsrv。

步骤2：点击Download a CA certificate, certificate chain, or CRL（下载CA证书、证书链或CRL）。

步骤3：确保选择当前证书，然后选择DER编码方法。

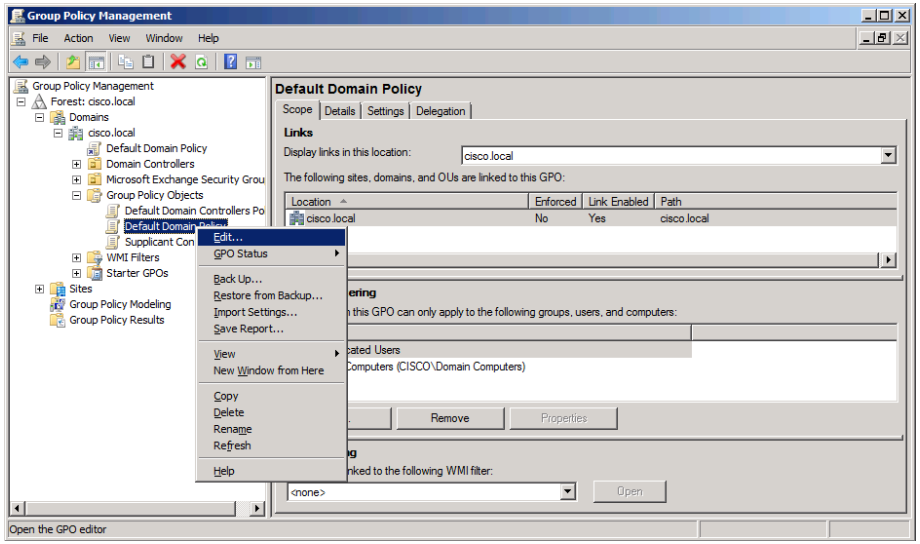
步骤4：点击Download CA Certificate（下载CA证书），然后在AD控制器中保存证书文件。



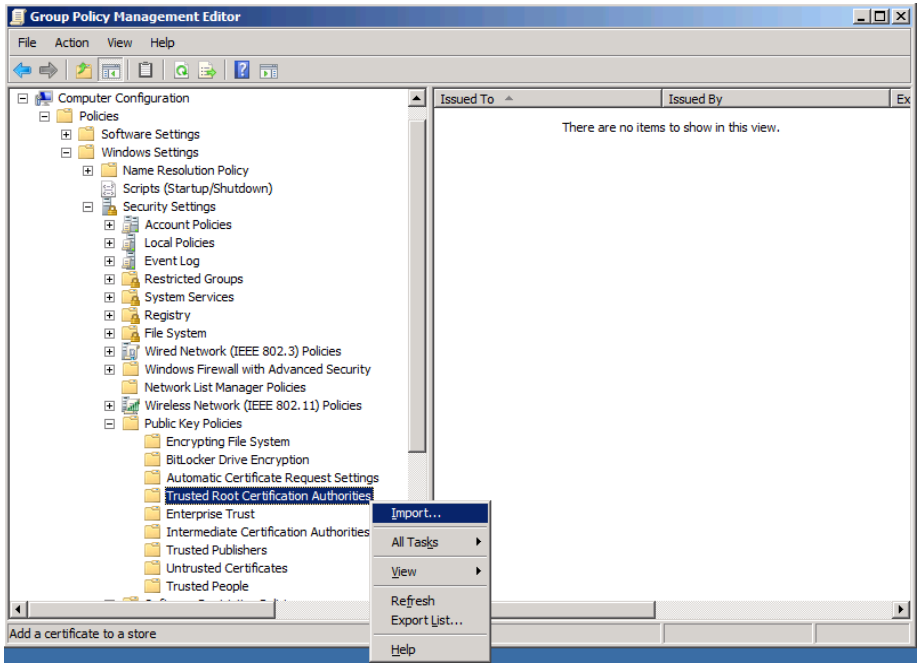
步骤5：在CA控制台中，转至Start（开始）> Administrative Tools（管理工具）> Group Policy Management（组策略管理）。

步骤6：依次展开Forest（目录林），Domain（域），local domain（本地域）和Group Policy Objects（组策略对象）。

步骤7：右键点击Default Domain Policy（缺省域策略），然后选择Edit（编辑）。

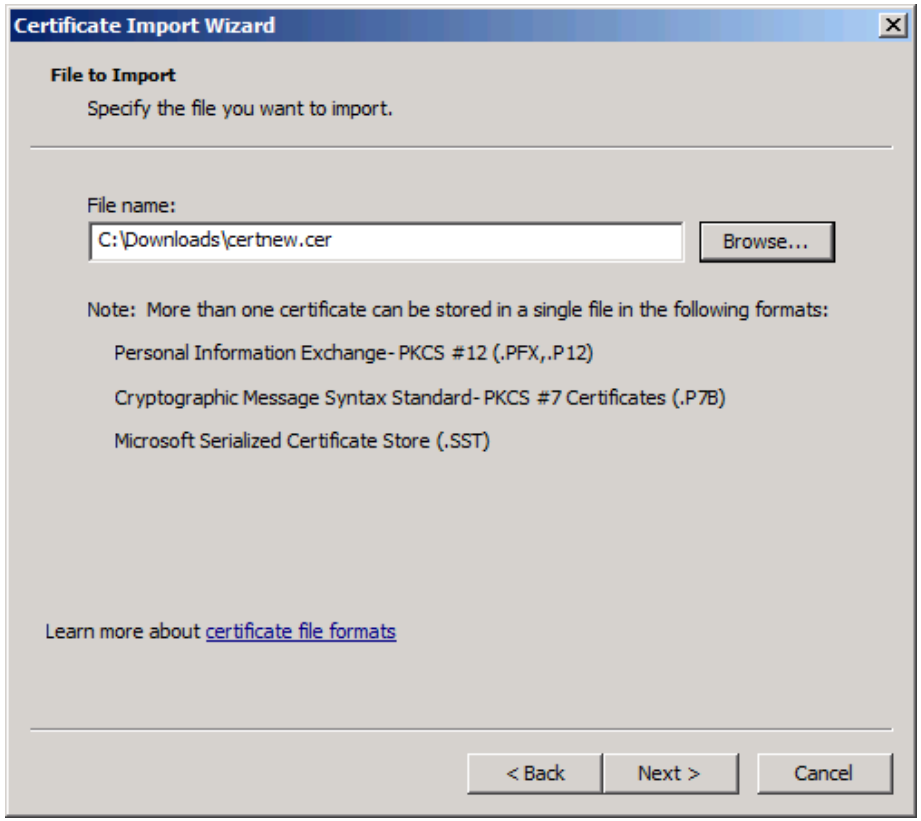


步骤8：转至Computer Configuration（计算机配置）> Policies（策略）> Windows Settings（Windows设置）> Security Settings（安全设置）> Public Key Policies（公钥策略），右键点击Trusted Root Certification Authorities（可信的根证书颁发机构），然后选择Import（导入）。Certificate Import Wizard（证书导入向导）将启动。



步骤9：点击Next（下一步）。

步骤10：点击Browse（浏览），找到在步骤4中保存的可信的根证书，然后点击Next（下一步）。



步骤11：将证书放入Trusted Root Certification Authorities（可信的根证书颁发机构）证书存储库，然后点击Next（下一步）。

步骤12：点击Finish（完成）。证书导入。

步骤13：点击OK（确定）。

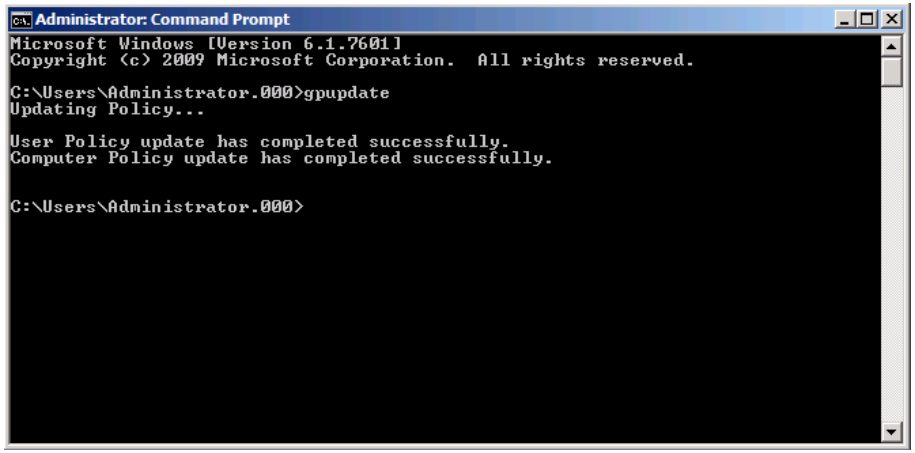
程序3　在AD服务器中安装可信的根

除了在AD服务器中安装用来分发至工作站的可信的根证书外，您还需要将其直接安装在AD服务器中。GPO更新将自动完成该步骤。在此程序中，您将立即运行该更新。

步骤1：在AD控制台中，转至Start（开始）>Run（运行）。

步骤2：键入cmd，然后按Enter打开命令窗口。

步骤3：键入gpupdate。组策略进行更新。



程序4　从CA请求用于ISE的证书

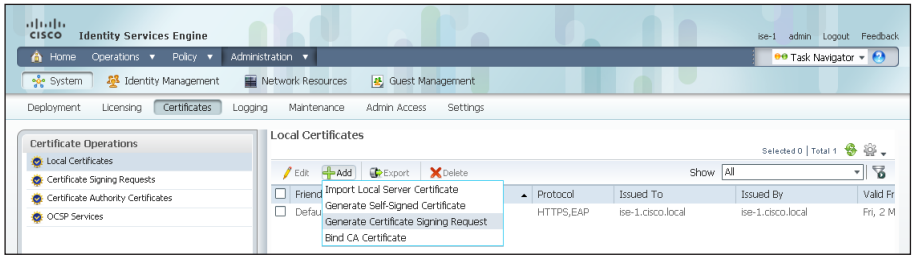
为了从CA获得证书，思科ISE需要生成一个签名请求，CA将使用它来生成证书。

步骤1：连接至https://ise-1.cisco.local.

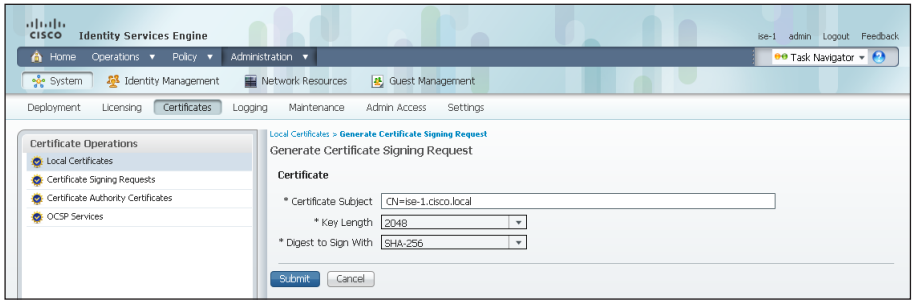
步骤2：将鼠标置于Administration（管理）之上，然后从菜单的System（系统）部分选择Certificates（证书）。

步骤3：在Certificate Operations（证书操作）下，选择Local Certificates（本地证书）。

步骤4：点击Add（添加），然后选择Generate Certificate Signing Request（生成证书签名请求）。

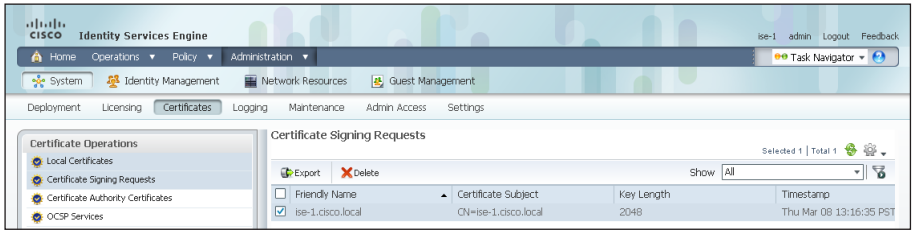


步骤5：在Certificate Subject（证书主题）字段中的“CN=”后，输入思科ISE服务器的完全合格域名(FQDN)，然后点击Submit（提交）。



步骤6：点击OK（确定）。这确认了证书已成功生成。

步骤7：点击Certificate Signing Requests（证书签名请求），选中新请求旁边的复选框，然后点击Export（导出）。



步骤8：将文件保存至您的本地计算机。您将使用该文件在CA中生成用于思科ISE的证书。

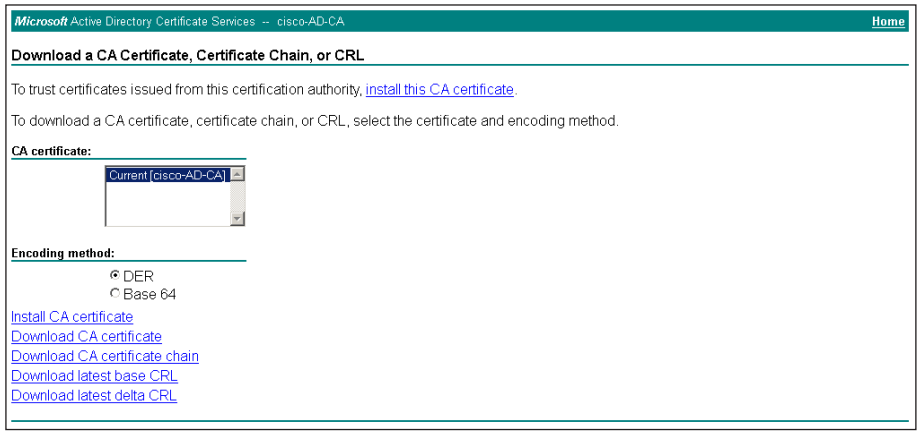
程序5 下载CA根证书

步骤1：转至https://ca.cisco.local/certsrv。

步骤2：点击Download a CA certificate, certificate chain, or CRL（下载CA证书、证书链或CRL）。

步骤3：确保选择当前证书，然后选择DER编码方法。

步骤4：点击Download CA Certificate（下载CA证书），然后在本地计算机中保存证书文件。



程序6 颁发用于ISE的证书

步骤1：点击Home（主页）。CA主页将显示。

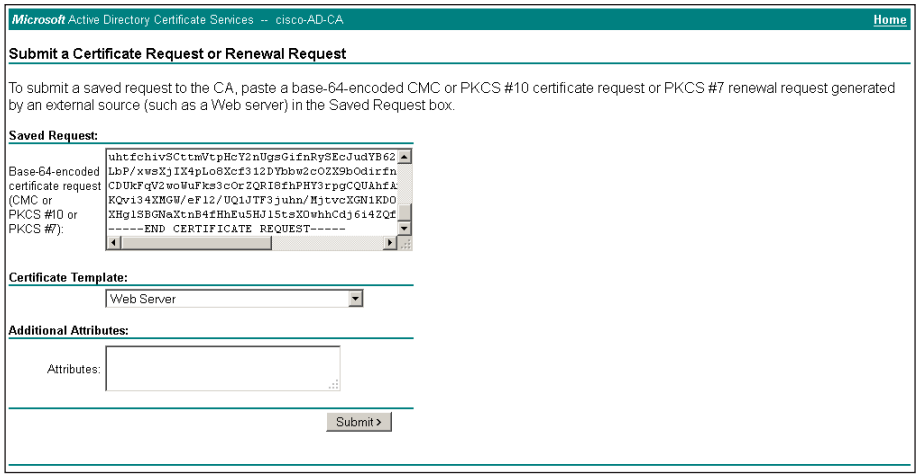
步骤2：点击Request a certificate（请求一个证书）。

步骤3：点击advanced certificate request（高级证书请求）。

步骤4：在Notepad等文本编辑器中，打开在程序4“从CA请求用于ISE的证书”中保存的证书文件。选中所有文本并将其复制到剪贴板。

步骤5：在浏览器打开的证书请求中，将该内容粘贴到Saved Request（已保存请求）部分中的文本框。

步骤6：在Certificate Template（证书模板）下拉列表中，选择Web Server（Web服务器），然后点击Submit（提交）。

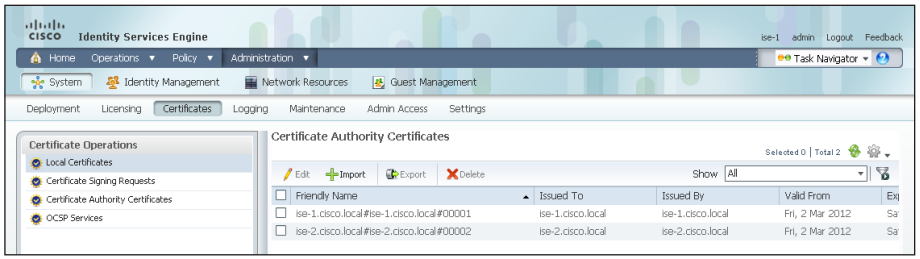


步骤7：选择DER encoded（DER已编码），然后点击Download certificate（下载证书）。证书将保存至您的本地计算机。

程序7　在ISE中安装可信的根证书

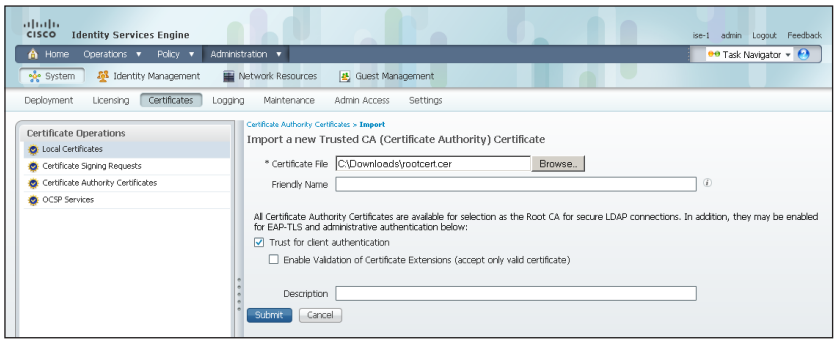
步骤1：在思科ISE界面中，将光标置于Administration（管理）上，然后从菜单的System（系统）部分中选择Certificates（证书）。

步骤2：点击Certificate Authority Certificates（证书颁发机构证书），然后点击Import（导入）。



步骤3：点击Browse（浏览），然后找到在程序5“下载CA根证书”中保存的根CA证书。

步骤4：选择Trust for client authentication（信任客户端认证），然后点击Submit（提交）。

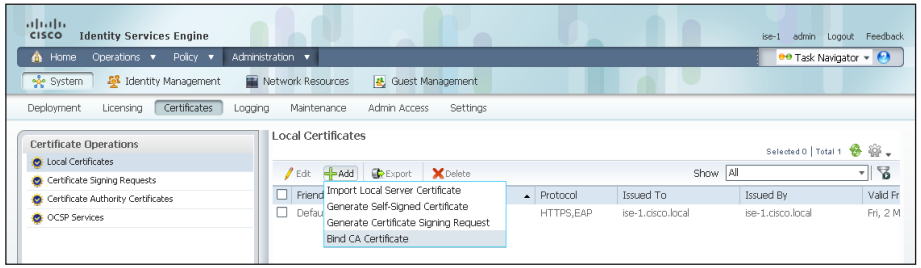


程序8　在ISE中安装本地证书

步骤1：在思科ISE界面中，将光标置于Administration（管理）上，然后从菜单的System（系统）部分中选择Certificates（证书）。

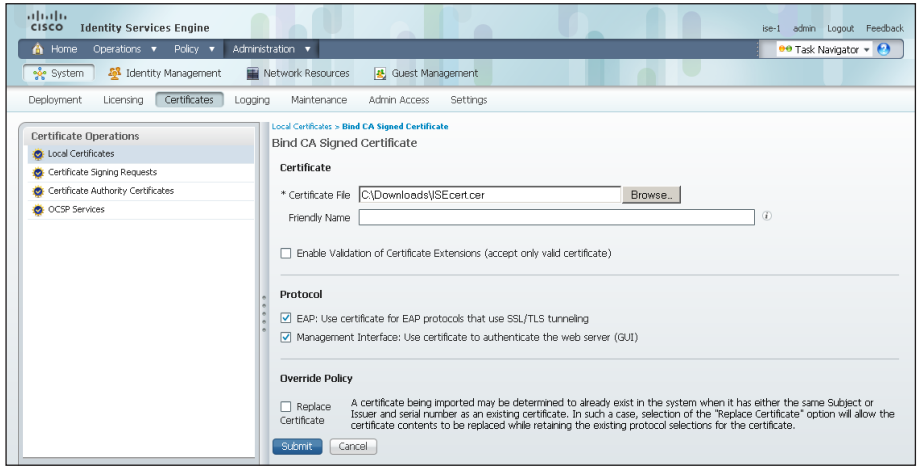
步骤2：点击Local Certificates（本地证书）。

步骤3：点击Add（添加），然后选择Bind CA Certificate（绑定CA证书）。



步骤4：点击Browse（浏览），找到在步骤1“颁发用于ISE的证书”中保存的证书。

步骤5：在Protocol（协议）部分中，同时选中EAP和Management Interface（管理接口）复选框。当您收到警告，提示选中Management Interface（管理接口）复选框将需要重启思科ISE设备时，点击OK（确定），然后点击Submit（提交）。



步骤6：当您收到警告提示思科ISE设备将重启时，点击OK（确定）。

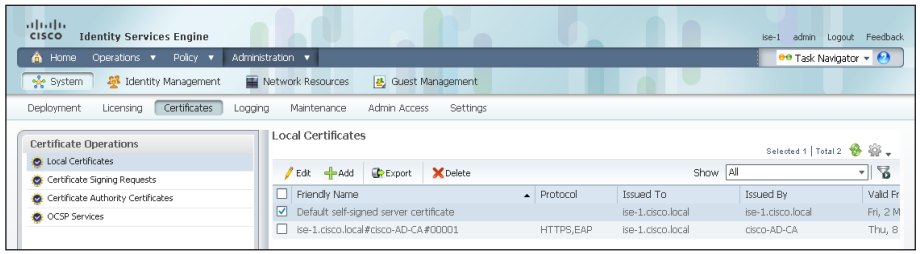
程序9　删除旧的证书和请求

既然您已经把本地证书导入至思科ISE，现在您需要删除旧的自签名证书和以前生成的证书签名请求。

步骤1：在思科ISE界面中，将光标置于Administration（管理）上，然后从System（系统）部分中选择Certificates（证书）。

步骤2：点击Local Certificates（本地证书）。

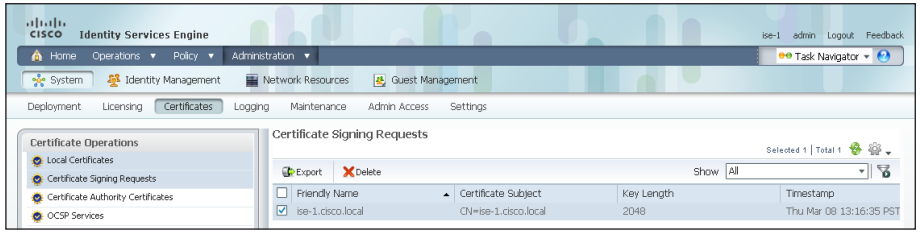
步骤3：选中自签名证书旁边的复选框。这是由思科ISE设备颁发的证书，而不是刚刚导入的由CA颁发的证书。



步骤4：点击Delete（删除），然后点击OK（确定）。

步骤5：点击Certificate Signing Requests（证书签名请求）。

步骤6：选中在程序4“从CA请求用于ISE的证书”中创建的Certificate Signing Request（证书签名请求）旁边的复选框。



步骤7：点击Delete（删除），然后点击OK（确定）。

流程

启用802.1X认证

1. 创建ISE策略
2. 启用证书
3. 启用EAP-TLS

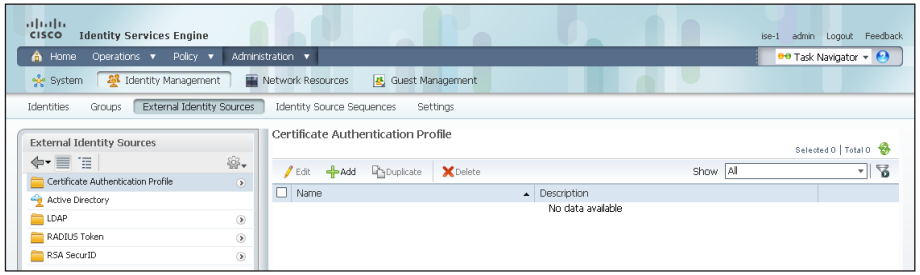
您将配置ISE策略，以支持使用数字证书对有线和无线用户进行802.1X认证。

程序1　创建ISE策略

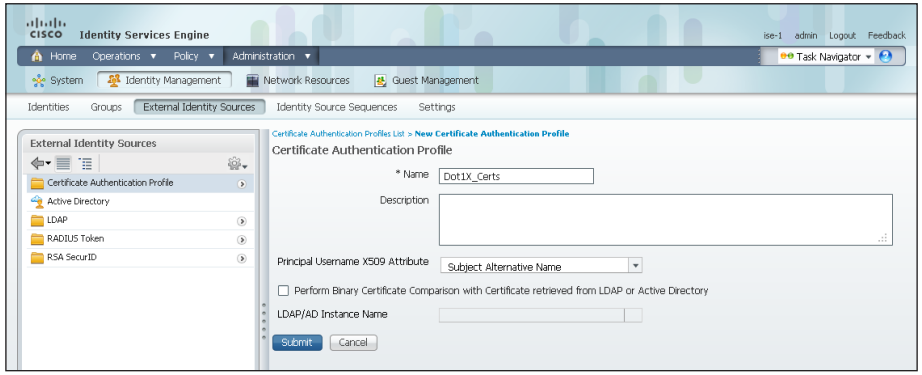
认证配置文件用于确定如何将证书用于认证。

步骤1：在Cisco ISE中，将光标置于Administration（管理）上，然后在Identity Management（身份管理）部分，选择External Identity Sources（外部身份源）。

步骤2：在左侧窗格中，点击Certificate Authentication Profile（证书认证配置文件），然后点击Add（添加）。



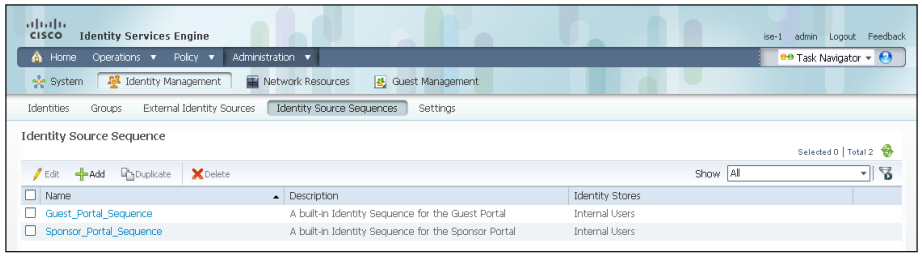
步骤3：为配置文件创建有意义的名称，然后从Principal Username X509 Attribute（主用户名X509属性）下拉列表中，选择Subject Alternative Name（主题备用名称）。



步骤4：点击Submit(提交)。

身份源序列允许将证书用作身份库，也允许在主用身份库不可用时将证书作为备用身份库。

步骤5：点击Identity Source Sequences（身份源序列），然后点击Add（添加）。

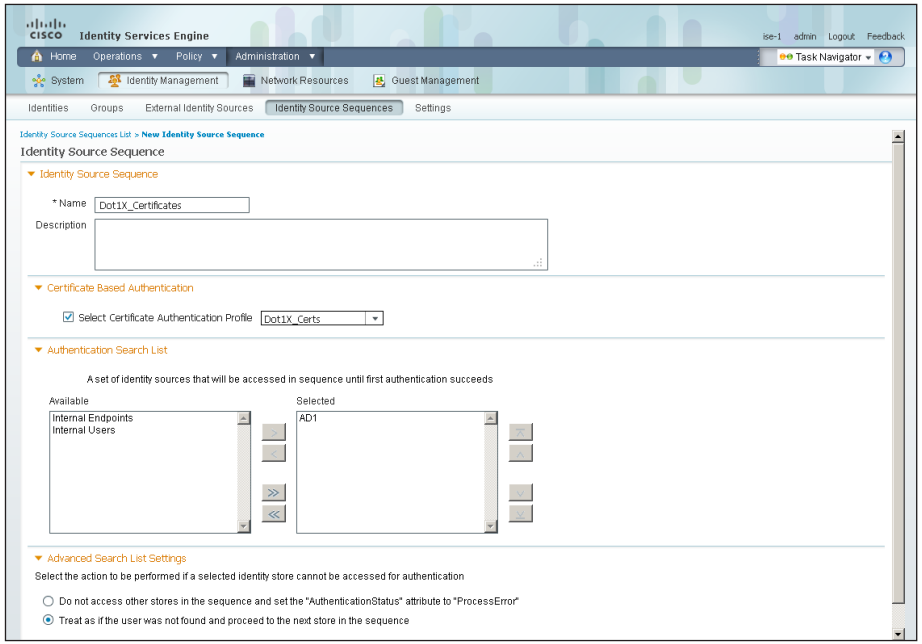


步骤6：为序列创建有意义的名称。

步骤7：在Certificate Based Authentication（基于证书的认证）部分，选择Select Certificate Authentication Profile（选择证书认证配置文件），然后选择先前创建的配置文件。

步骤8：在Authentication Search List（认证搜索列表）部分，从Available（可用）列表中双击AD服务器，将其移动至Selected（已选中）列表。

步骤9：在Advanced Search List Settings（高级搜索列表设置）部分，选择Treat as if the user was not found and proceed to the next store in the sequence（视为未找到用户并转至序列中的下一个存储库）



步骤10：点击Submit（提交）。

程序2　启用证书

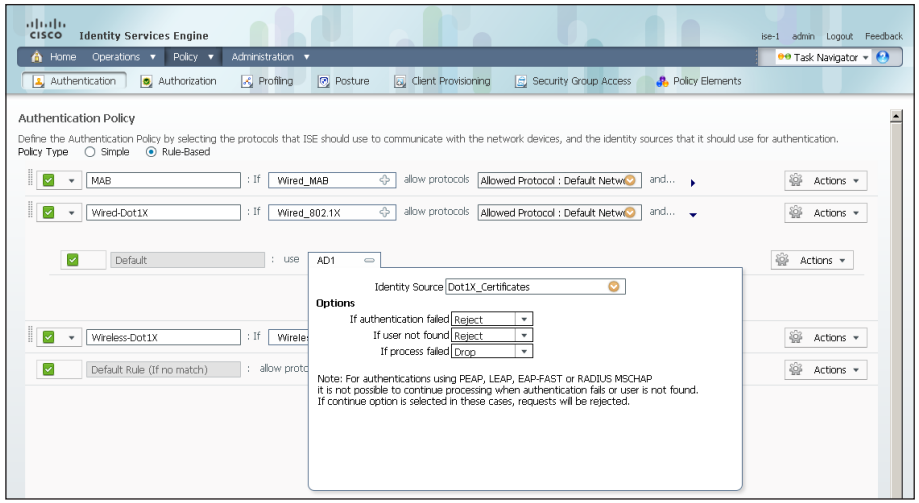
既然您已经创建了证书认证配置文件和用于数字证书的身份源序列，现在您需要为有线和无线用户启用802.1X认证策略。

步骤1：将鼠标置于Policy（策略）之上，然后从下拉菜单中选择Authentication（认证）。

步骤2：点击Wired-Dot1X规则“and…”右侧的黑色三角形。用于此规则的身份存储库出现。

步骤3：点击AD1身份存储库项旁边的“+”号。

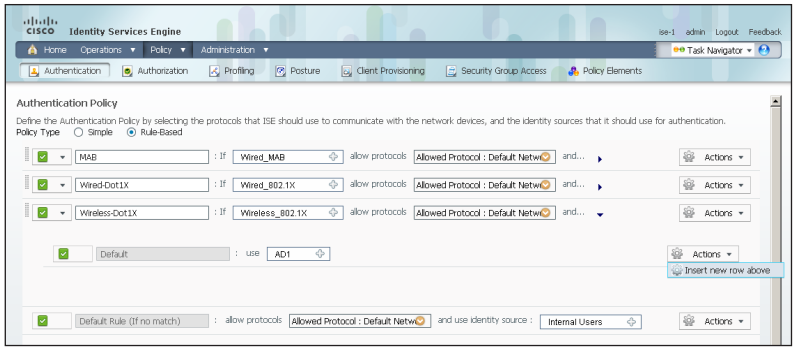
步骤4：在Identity Store（身份存储库）下拉列表中，选择在程序1“创建ISE策略”中创建的身份源序列，针对该身份源使用缺省选项，然后点击窗口中的任意位置继续。



对于无线用户，您应将认证策略修改为首先检查客户端是否使用了EAP-TLS，如果没有使用，则允许其采用PEAP等认证方法，将用户名和密码作为凭证。这使得未获得证书的用户也可以访问网络。一旦他们连接至网络，Windows客户端将向其推送证书，其他终端可以手动获取证书。

步骤5：点击Wireless-Dot1X规则的and...（和...）右侧的黑色三角。这将打开用于此规则的身份存储库。

步骤6：在Default（缺省）规则旁边的Actions（行动）下拉列表中，选择Insert new rule above（在上方插入新规则）。

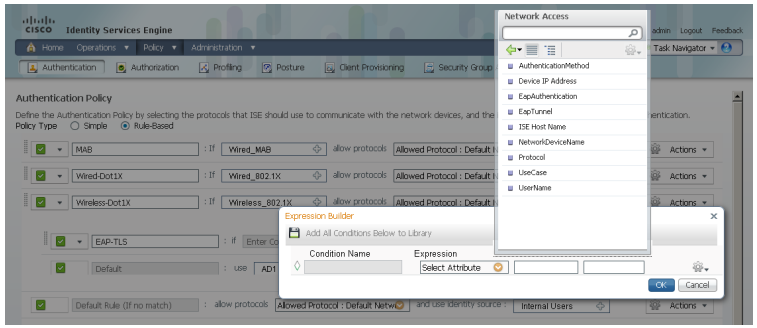


步骤7：为该规则输入名称，然后通过点击Enter Condition（输入条件）框旁边的符号打开表达式生成器。

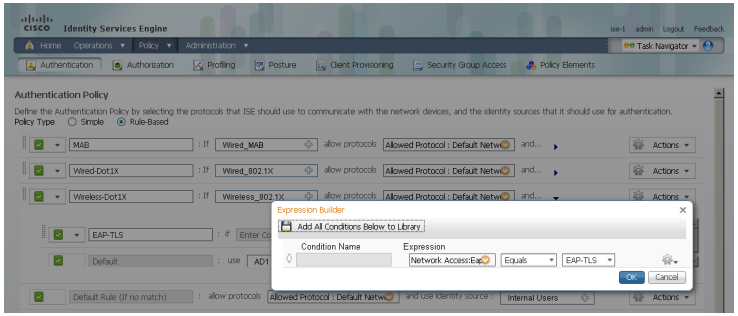
步骤8：点击Create New Condition(Advance Option)（创建新条件（高级选项））

步骤9：在Expression（表达式）下拉列表中，点击Select Attribute（选择属性）旁边的箭头。

步骤10：点击Network Access（网络访问）旁边的箭头，然后选择EapAuthentication。

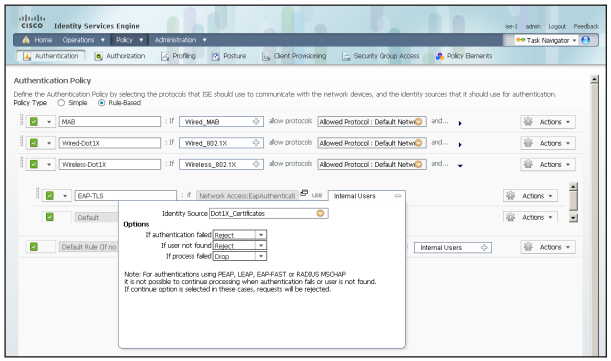


步骤11：在第二个下拉列表中，选择Equals（等于），在最后一个下拉列表中，选择EAP-TLS，然后点击OK（确定）。



步骤12：点击Internal Users（内部用户）旁边的“+”号。

步骤13：在Identity Store（身份存储库）下拉列表中，选择在程序1“创建ISE策略”中创建的身份源序列，针对该身份源使用缺省选项，然后点击窗口中的任意位置继续。



步骤14：点击Save（保存）。

程序3　启用EAP-TLS

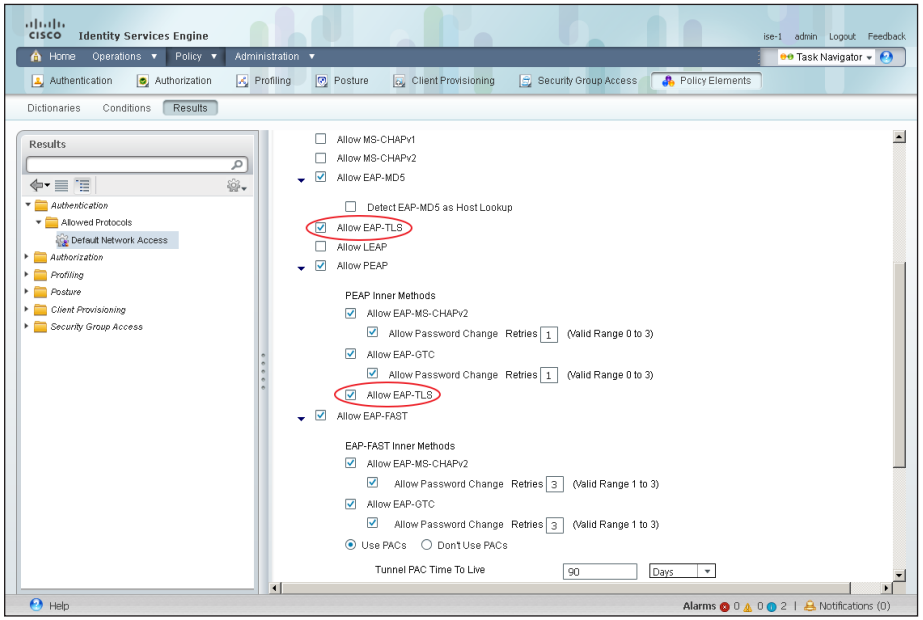
在上一节中，您禁用了EAP-TLS。既然您准备使用数字证书，现在您需要重新将其启用。

步骤1：在菜单栏上，将鼠标置于Policy（策略）之上，然后在Policy Elements（策略元素）部分，选择Results（结果）。

步骤2：在左侧窗格，双击Authentication（认证）。此操作将展开选项。

步骤3：双击Allowed Protocols（允许的协议），然后选择Default Network Access（缺省网络访问）。

步骤4：选择全局Allow EAP-TLS（允许EAP-TLS）复选框，在PEAP设置下，选择Allow EAP-TLS（允许EAP-TLS）复选框，然后点击Save（保存）。



流程

配置组策略对象

1. 创建工作站模板
2. 创建用户自动登入模板
3. 为有线终端配置GPO
4. 为无线终端配置GPO

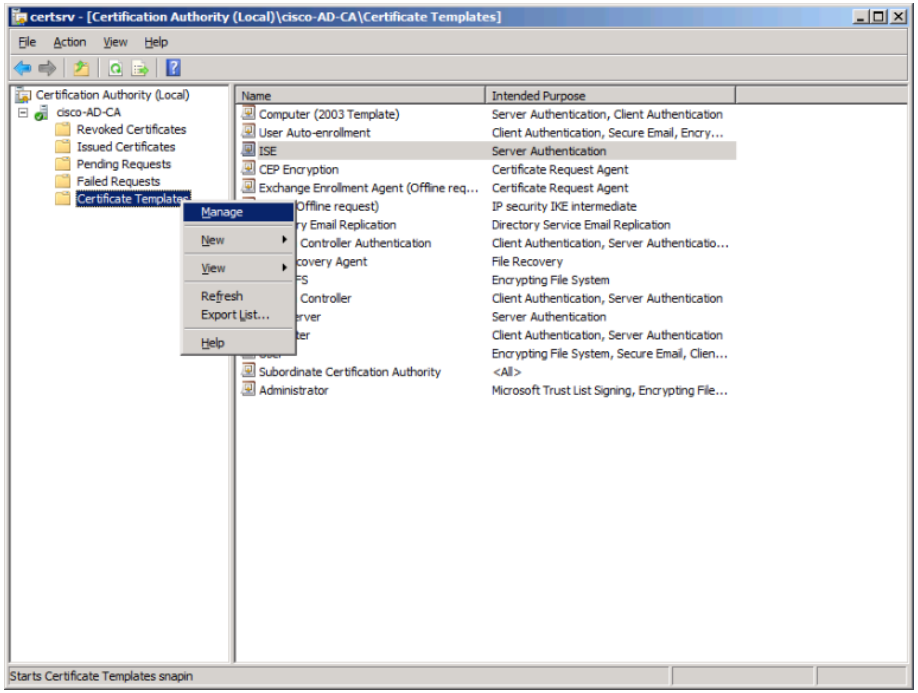
在本部署中，您将使用组策略对象(GPO)来分发证书，并为Windows XP和属于域成员的其他终端配置本机802.1X请求者。当计算机加入域，且用户证书部署到用户用来登录域的终端上以后，计算机证书将分发。本部署示例中的步骤介绍了如何编辑Default Domain Policy（缺省域策略），以便它可以应用至所有用户。如果需要，您也可以创建新的策略对象并将其应用至用户子集。

程序1　创建工作站模板

您需要在CA中创建一个证书模板，用于将计算机证书分发至加入活动目录(AD)域的工作站。

步骤1：在CA控制台中，转至Start（开始）> Administrative Tools（管理工具）> Certification Authority（证书颁发机构）。

步骤2：展开CA服务器，右键点击Certificate Templates（证书模板），然后选择Manage（管理）。Certificate Templates Console（证书模板控制台）打开。



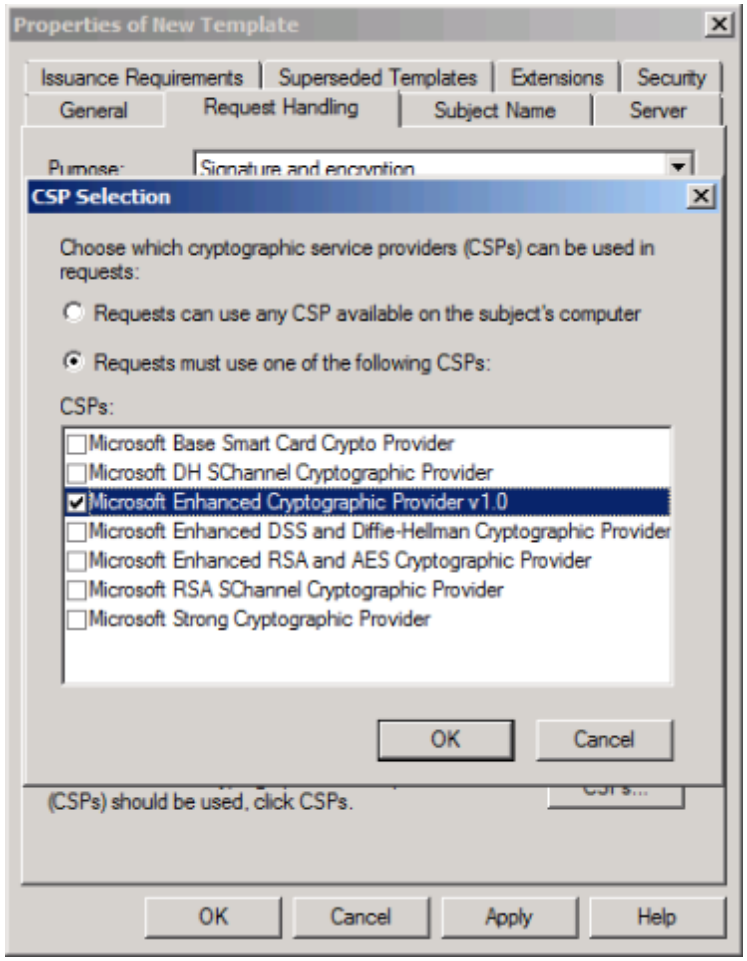
步骤3：右键点击Computer（计算机）模板，然后选择Duplicate Template（复制模板）。

步骤4：为实现兼容性，请确保选中Windows 2003 Server Enterprise。

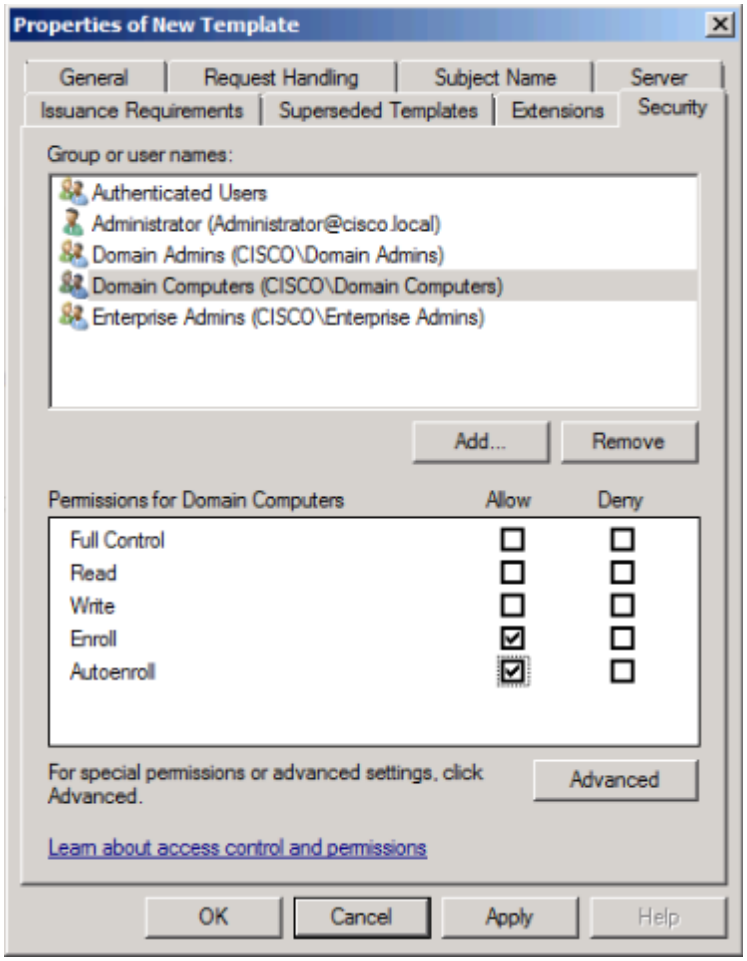
步骤5：在模板属性窗口中，点击General（常规）选项卡，然后提供模板名称。

步骤6：在Request Handling（请求处理）选项卡中，选择Allow private key to be exported（允许私钥导出），然后点击CSP。

步骤7：选择Requests must use one of the following CSPs（请求必须使用以下CSP之一）和Microsoft Enhanced Cryptographic Provider v1.0，然后点击OK（确定）。



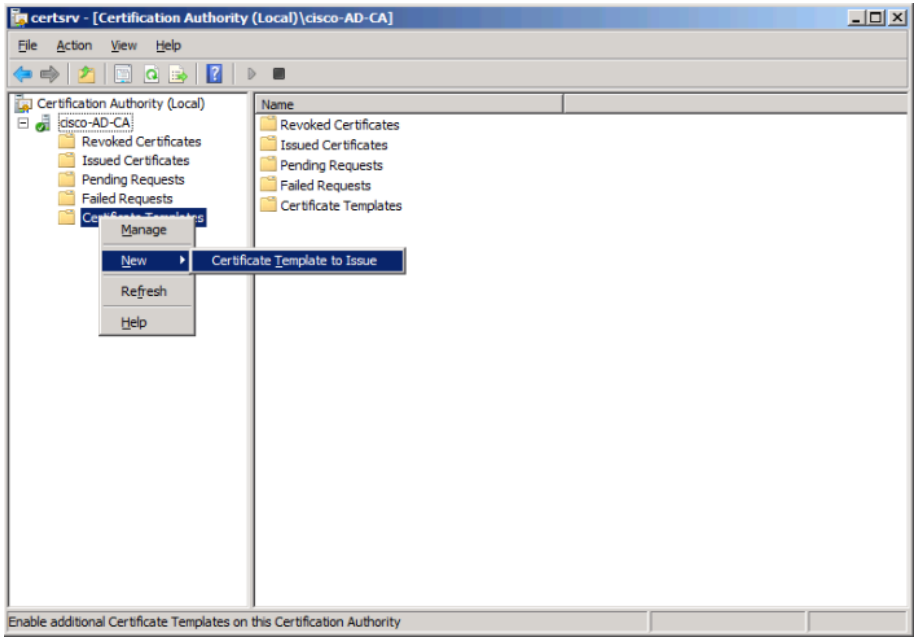
步骤8：在Security（安全性）选项卡中，点击Domain Computers（域计算机），然后确保针对Enroll（登入）和Autoenroll（自动登入）选择Allow（允许）。



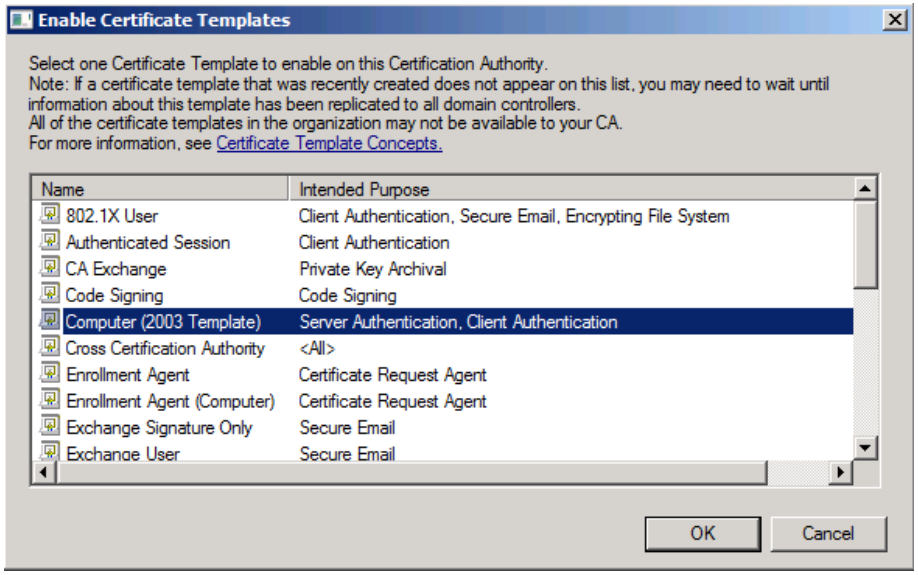
步骤9：其余选项卡使用缺省设置，然后点击OK（确定）。

步骤10：关闭Certificate Templates Console（证书模板控制台）。

步骤11：在Certificate Authority（证书颁发机构）控制台中，右键点击Certificate Templates（证书模板），然后选择New（新建）> Certificate Template to Issue（要颁发的证书模板）。



步骤12：选择先前定义的模板，然后点击OK（确定）。



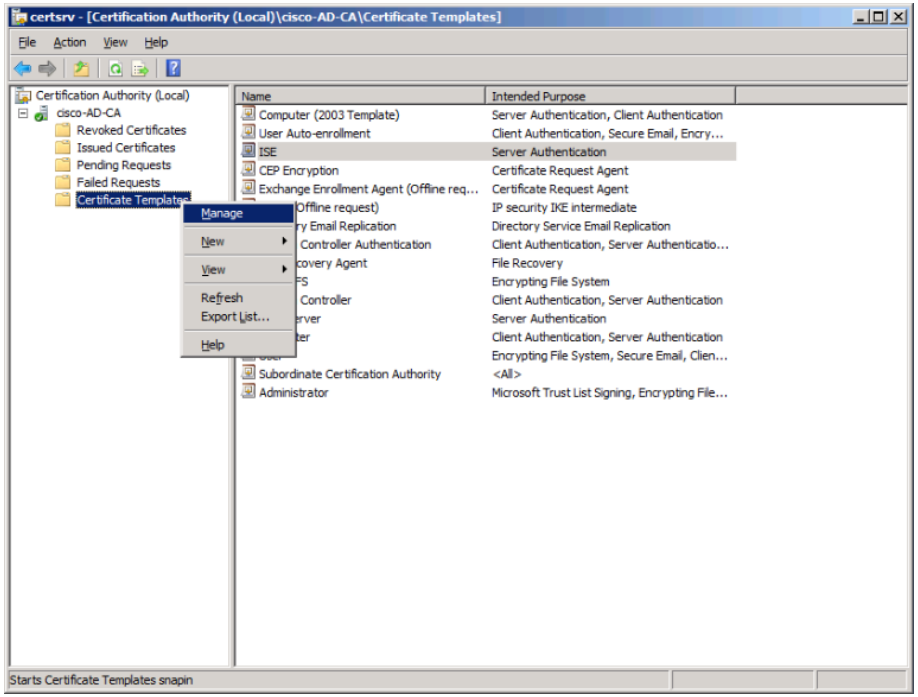
当计算机加入域或GPO策略刷新后（缺省期限为90分钟），计算机将收到计算机证书，以支持802.1X计算机认证。

程序2　创建用户自动登入模板

本部署可通过组策略对象(GPO)使域用户自动登入，在他们登录至域时获取证书。您需要为这些用户创建一个模板以便支持自动登入。

步骤1：在CA控制台中，转至Start（开始）> Administrative Tools（管理工具）> Certification Authority（证书颁发机构）。

步骤2：展开CA服务器，右键点击Certificate Templates（证书模板），然后选择Manage（管理）。Certificate Templates Console（证书模板控制台）打开。



步骤3：右键点击User（用户）模板，然后选择Duplicate Template（复制模板）。

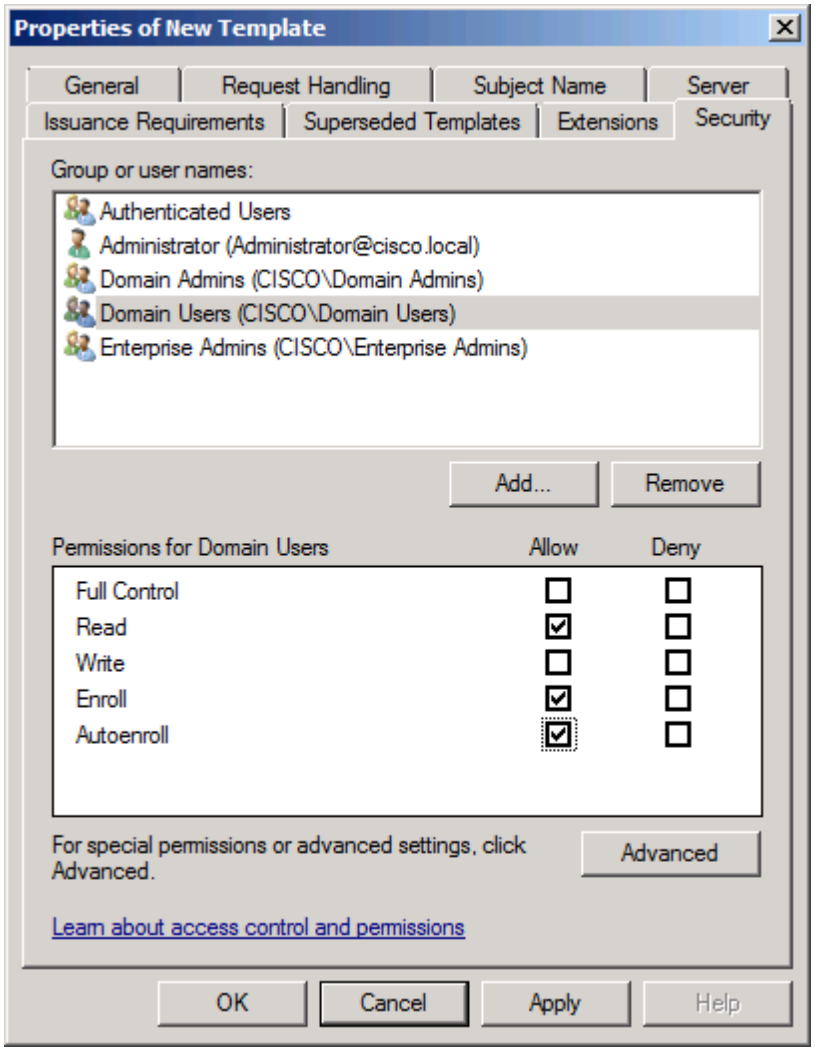
步骤4：为了与Windows XP兼容，请确保选中Windows 2003 Server Enterprise。

步骤5：在模板属性窗口中，点击General（常规）选项卡，然后提供模板名称。

步骤6：在Request Handling（请求处理）选项卡中，选择Allow private key to be exported（允许私钥导出），确保选中Enroll subject without requiring any user input（登入主题无需任何用户输入），然后点击CSP。

步骤7：选择Requests must use one of the following CSPs（请求必须使用以下CSP之一）和Microsoft Enhanced Cryptographic Provider v1.0，然后点击OK（确定）。

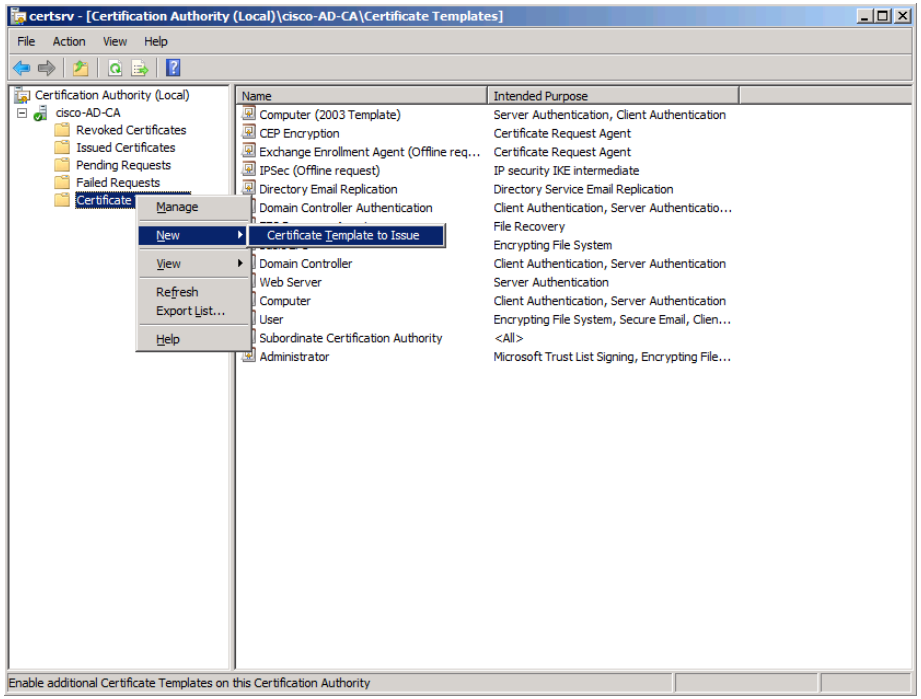
步骤8：在Security（安全性）选项卡中，点击Domain Users（域用户），然后确保针对Read（读取）、Enroll（登入）和Autoenroll（自动登入）选择Allow（允许）。



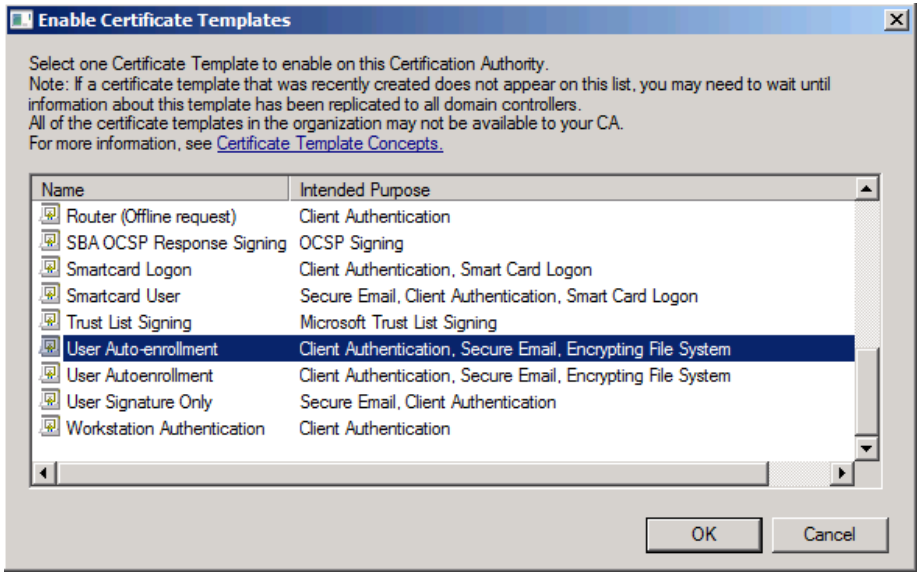
步骤9：其余选项卡使用缺省设置，然后点击OK（确定）。

步骤10：关闭Certificate Templates Console（证书模板控制台）。

步骤11：在Certificate Authority（证书颁发机构）控制台中，右键点击Certificate Templates（证书模板），然后选择New（新建）> Certificate Template to Issue（要颁发的证书模板）。



步骤12：选择先前定义的模板，然后点击OK（确定）。



当用户下一次登录域时或GPO策略刷新后，他将收到所推送的证书。如果用户登录至多个终端，则每个终端都要部署证书。

程序3　为有线终端配置GPO

本部署使用GPO为运行Windows XP SP3和更高版本的有线终端配置802.1X请求者。

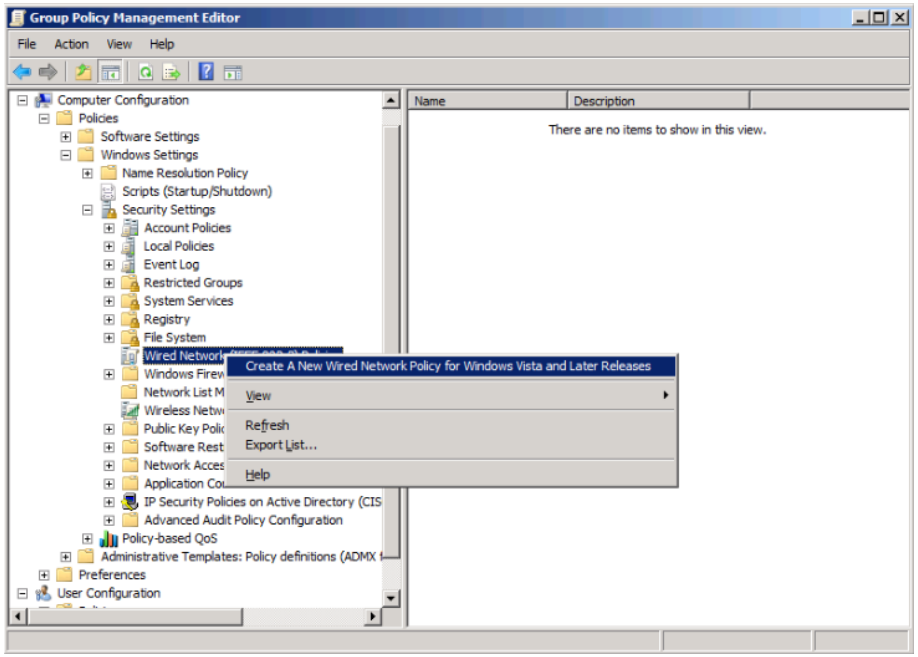
步骤1：在CA控制台中，转至Start（开始）> Administrative Tools（管理工具）> Group Policy Management（组策略管理）。

步骤2：依次展开Forest（目录林），Domain（域），local domain（本地域）和Group Policy Objects（组策略对象）。

步骤3：右键点击Default Domain Policy（缺省域策略）。Group Policy Management Editor（组策略管理编辑器）打开。

步骤4：在Group Policy Management Editor（组策略管理编辑器）中，转至Computer Configuration（计算机配置）> Policies（策略）> Windows Settings（Windows设置）> Security Settings（安全设置）。

步骤5：右键点击Wired Network (IEEE 802.3e) Policies（有线网络(IEEE 802.3e)策略），然后选择Create a New Wired Network Policy for Windows Vista and Later Releases（为Windows Vista和更新版本创建新的有线网络策略）。



步骤6：在General（常规）选项卡中，提供策略名称和描述，并确保选中Use Windows Wired Auto Config service for clients（为客户端使用Windows Wired Auto Config服务）。

步骤7：在Security（安全性）选项卡中，确保选中Enable of IEEE 802.1X authentication for network access（为网络接入启用IEEE 802.1X认证）。

步骤8：在Network authentication method（网络认证方法）下拉列表中，选择Microsoft: Smart Card or other certificate（Microsoft: Smart Card或其他证书）。

步骤9：在Authentication Mode（认证模式）下拉列表中，选择User or computer authentication（用户或计算机认证）。

步骤10：点击Properties（属性）。

步骤11：确保选中Use a certificate on this computer（在该计算机中使用证书）选项，并确保选中Use simple certificate selection（使用简单证书选择）和Validate server certificate（验证服务器证书）复选框。

步骤12：在Trusted Root Certification Authorities（可信的根证书颁发机构）列表中，选中CA根证书旁边的复选框。

步骤13：点击OK（确定），点击Apply（应用），然后再次点击OK（确定）。

程序4　为无线终端配置GPO

该部署使用GPO为运行Windows XP SP3和更高版本的无线终端配置802.1X请求者。

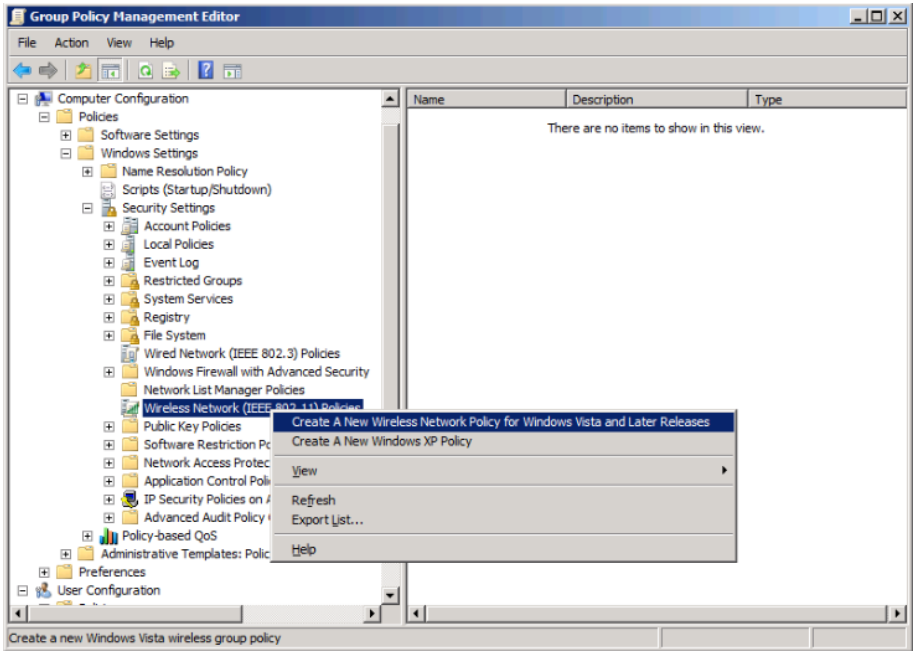
步骤1：在CA控制台中，转至Start（开始）> Administrative Tools（管理工具）> Group Policy Management（组策略管理）。

步骤2：依次展开Forest（目录林），Domain（域），local domain（本地域）和Group Policy Objects（组策略对象）。

步骤3：右键点击Default Domain Policy（缺省域策略）。Group Policy Management Editor（组策略管理编辑器）打开。

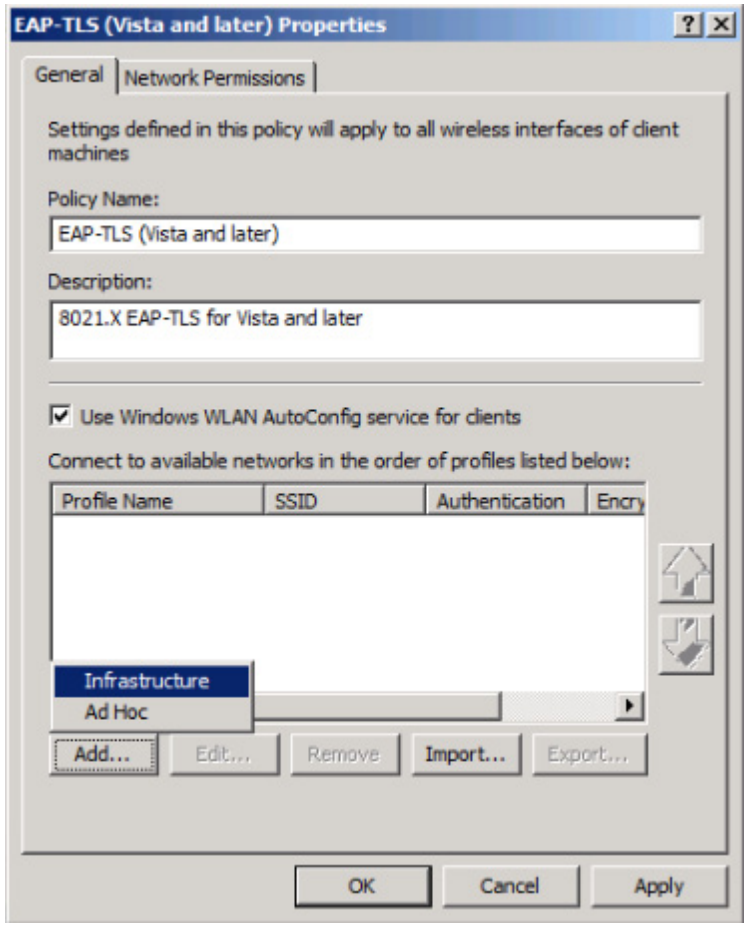
步骤4：在Group Policy Management Editor（组策略管理编辑器）中，转至Computer Configuration（计算机配置）> Policies（策略）> Windows Settings（Windows设置）> Security Settings（安全设置）。

步骤5：右键点击Wireless Network (IEEE 802.11) Policies（无线网络 (IEEE 802.11)策略），然后选择Create a New Wireless Network Policy for Windows Vista and Later Releases（为Windows Vista和更新版本创建新的无线网络策略）。



步骤6：在General（常规）选项卡中，输入策略名称和描述，并确保选中Use Windows WLAN AutoConfig service for clients（为客户端使用Windows WLAN AutoConfig服务）。

步骤7：点击Add（添加），然后选择Infrastructure（基础设施）。



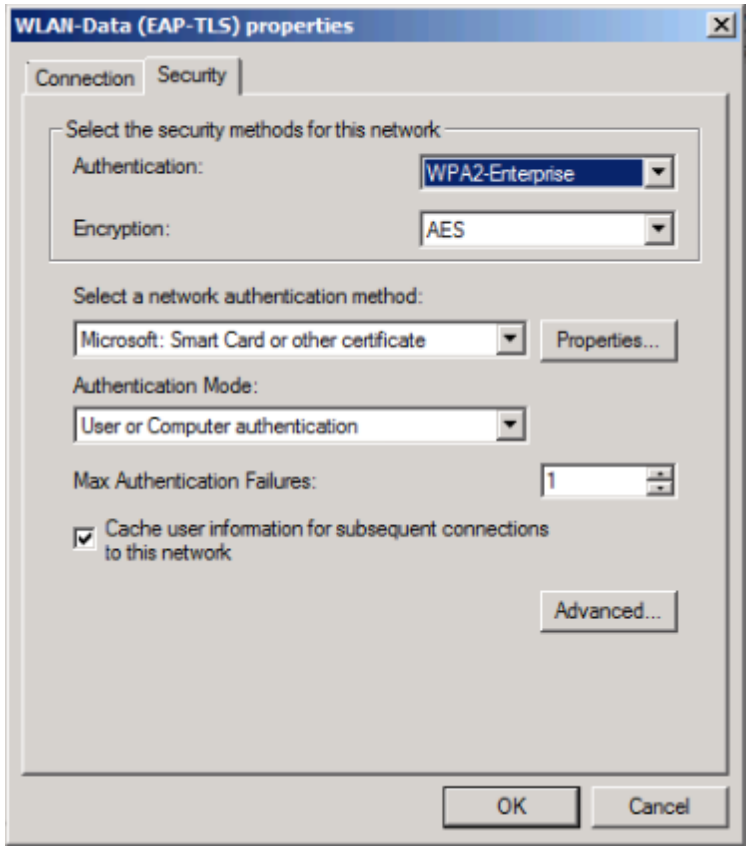
步骤8：为配置文件提供名称，输入无线网络的SSID名称，然后点击Add（添加）。

步骤9：点击Security（安全性）选项卡。

步骤10：在Authentication（认证）下拉列表中，选择WPA2-Enterprise，然后在Encryption（加密）下拉列表中，选择AES。

步骤11：在Select a network authentication method（选择网络认证方法）下拉列表中，选择Microsoft:Smart Card or other certificate（Microsoft:Smart Card或其他证书）。

步骤12：在Authentication Mode（认证模式）下拉列表中，选择User or computer authentication（用户或计算机认证）。



步骤13：点击Properties（属性）。

步骤14：确保选中Use a certificate on this computer（在此计算机上使用证书）选项，并确保选中Use simple certificate selection（使用简单证书选择）和Validate server certificate（验证服务器证书）复选框。

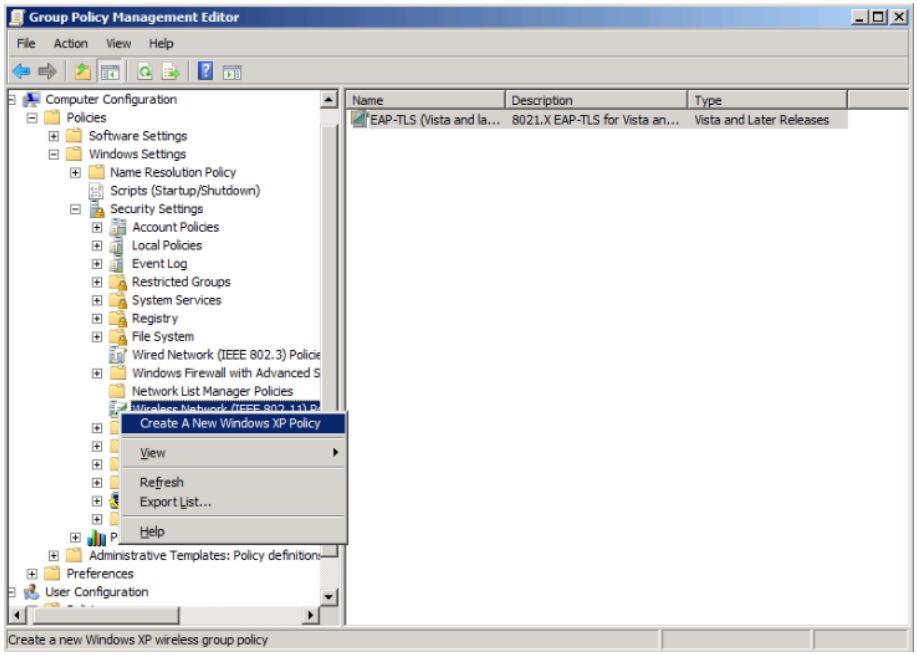
步骤15：在Trusted Root Certification Authorities（可信的根证书颁发机构）列表中，选中CA根证书旁边的复选框。

步骤16：点击OK（确定），然后再次点击OK（确定）。

步骤17：点击Apply（应用），然后点击OK（确定）。

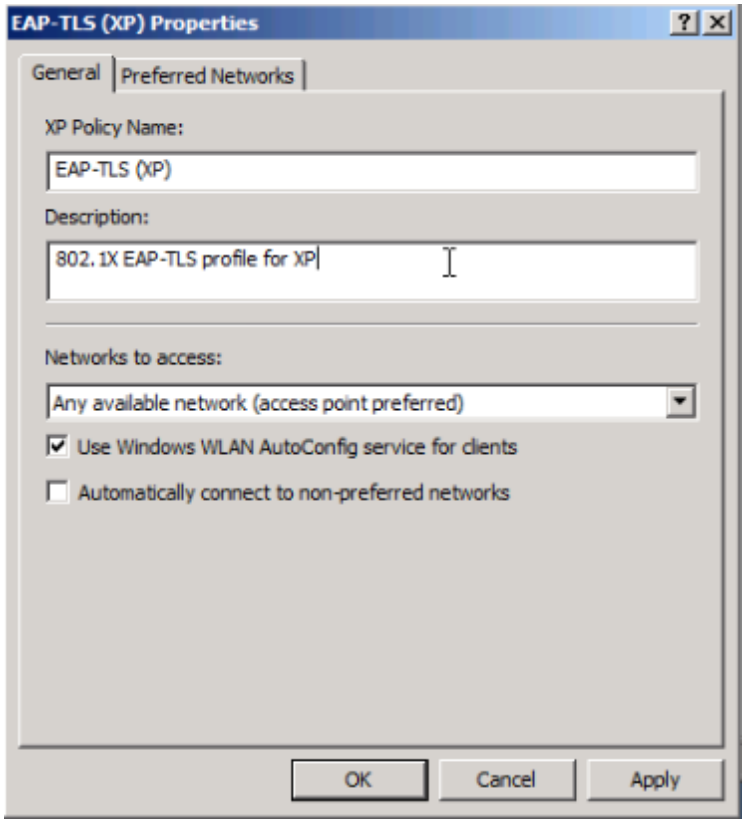
您还需要为Windows XP客户端创建策略。

步骤18：右键点击Wireless Network (IEEE 802.11) Policies（无线网络(IEEE 802.11)策略），然后选择Create a New Windows XP Policy（创建新的Windows XP策略）。



步骤19：在General（常规）选项卡中，提供策略名称和描述，并确保选中Use Windows WLAN AutoConfig service for clients（为客户端使用Windows WLAN AutoConfig服务）。

步骤20：在Networks to access（要访问的网络）列表中，选择Any available network (access point preferred)（任意可用网络（首选接入点））



步骤21：点击Preferred Networks（首选网络）选项卡。

步骤22：点击Add（添加），然后选择Infrastructure（基础设施）。

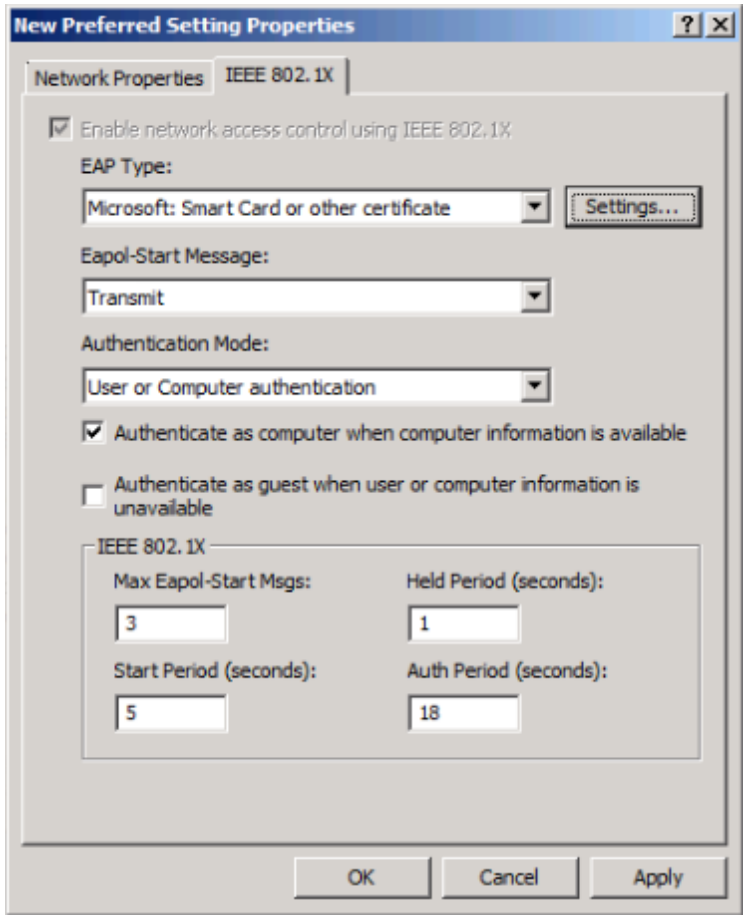
步骤23：输入网络的SSID并提供描述。

步骤24：针对Authentication（认证）选择WPA2，针对Encryption（加密）选择AES。

步骤25：点击IEEE 802.1X选项卡。

步骤26：在EAP type（EAP类型）列表中，选择Microsoft:Smart Card or other certificate（Microsoft:Smart Card或其他证书）。

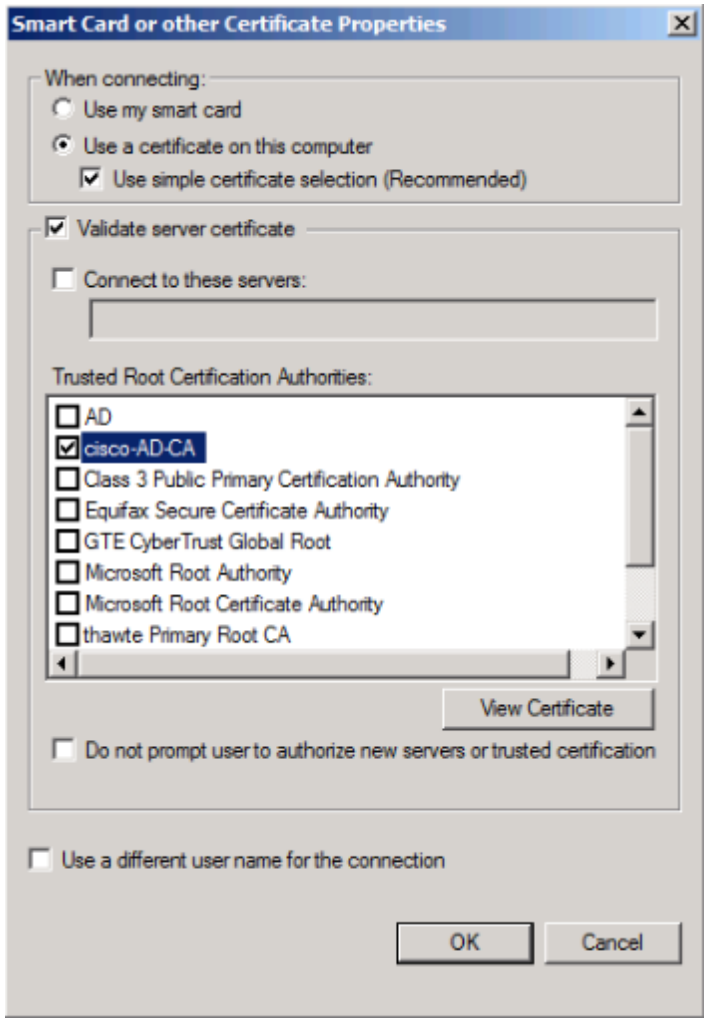
步骤27：在Authentication Mode（认证模式）列表中，选择User or Computer authentication（用户或计算机认证）。



步骤28：点击Settings（设置）。

步骤29：确保选中Use a certificate on this computer（在此计算机中使用证书）选项，并确保选中Use simple certificate selection（使用简单证书选择）和Validate server certificate（验证服务器证书）复选框。

步骤30：在Trusted Root Certification Authorities（可信的根证书颁发机构）列表中，选中CA根证书旁边的复选框。



步骤31：点击OK（确定）。

步骤32：点击Apply（应用），然后再点击OK（确定）。Profile Properties（配置文件属性）窗口显示。

步骤33：点击Apply（应用），然后再点击OK（确定）。

此时，所有运行Windows XP SP3和更新版本的终端在下一次登录域时或GPO策略刷新后，将拥有推送的802.1X请求者配置。

流程

在Windows终端上部署AnyConnect

1. 安装AnyConnect
2. 安装Profile Editor
3. 创建有线配置文件
4. 创建无线配置文件

在使用Network Access Manager模块的Windows终端中，Cisco AnyConnect Secure Mobility Client 3.0可以用作802.1X请求者。在本部署示例中，Network Access Manager通过采用数字证书的有线和无线配置文件进行配置。

程序1　安装AnyConnect

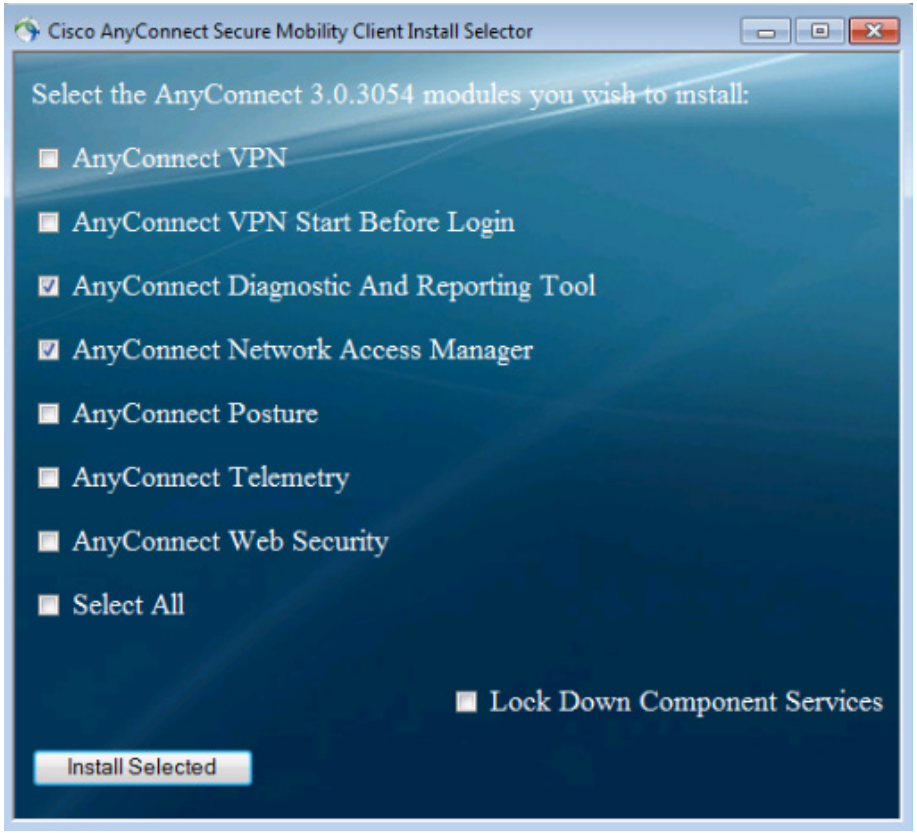
如欲将Cisco AnyConnect Secure Mobility Client 3.0用作Windows终端上的802.1X请求者，您需要从Cisco.com中下载最新版本和Profile Editor。该客户端作为ISO镜像分发，将需要刻录至磁盘，或通过提供该功能的实用程序作为磁盘镜像安装。为安装AnyConnect Secure Mobility客户端，您需要以管理员的身份登录。

读者提示

最新版本的Cisco AnyConnect Secure Mobility客户端和Profile Editor可从以下地址下载：
http://www.cisco.com/cisco/software/release.html?mdfid=283000185&flowid=17001&softwareid=282364313&release=3.0.5075&relind=AVAILABLE&rellifecycle=&reltype=latest

步骤1：通过在磁盘中启动Setup（设置）程序，启动AnyConnect Secure Mobility客户端的安装程序。

步骤2：选择AnyConnect Diagnostic and Reporting Tool（AnyConnect诊断和报告工具）和AnyConnect Network Access Manager，然后取消选中其他所有的复选框。



步骤3：点击Install Selected（安装已选择），验证已选择要安装的组件，然后点击OK（确定）。

步骤4：点击Accept（接受），接受许可协议。

步骤5：在安装完成后，点击OK（确定）。系统可能会要求您重新启动计算机。

程序2 安装Profile Editor

步骤1：找到以前下载的Profile Editor Installer（Profile Editor安装程序），然后双击它。安装流程开始。

安装需要Java Runtime Environment 1.6或更高版本。如果您还没有安装，系统将提示您进行安装。

步骤2：如果系统提示安装Java Runtime Environment 1.6或更高版本，请点击Next（下一步）。这样便可以完成安装。

步骤3：点击Next（下一步）。Profile Editor的安装将继续。

步骤4：点击Typical（典型），然后点击Install（安装）。

步骤5：点击Finish（完成）。安装完成。

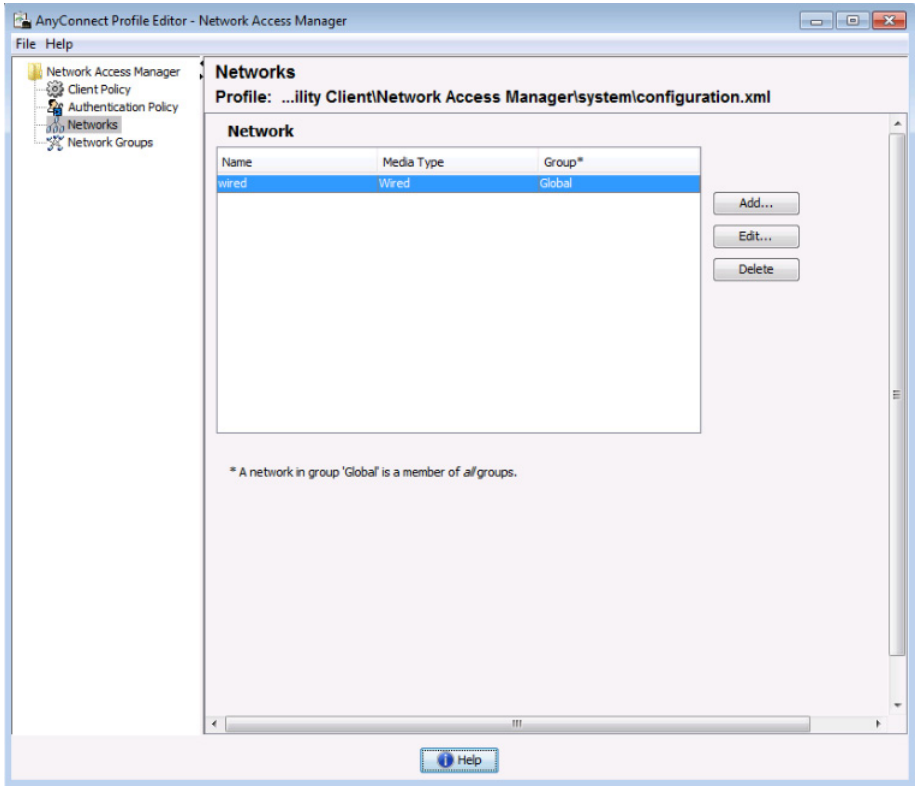
程序3 创建有线配置文件

步骤1：通过转至Start（开始）> All Programs（所有程序）> Cisco> Cisco AnyConnect Profiler Editor > Network Access Manager Profile Editor，启动Pfofile Editor。

步骤2：从File（文件）菜单中，选择Open（打开），并选择C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml。

步骤3：点击Networks（网络）。

步骤4：选择有线配置文件，然后点击Edit（编辑）。



步骤5：输入配置文件名称，然后点击Next（下一步）。

步骤6：选择Authenticating Network（验证网络），然后点击Next（下一步）。

步骤7：选择Machine and User Authentication（计算机和用户认证），然后点击Next（下一步）。

步骤8：选择EAP-TLS作为计算机认证方法，然后点击Next(下一步)。

步骤9：为计算机身份输入不受保护的身份模式。在本部署中，使用host.[domain]。

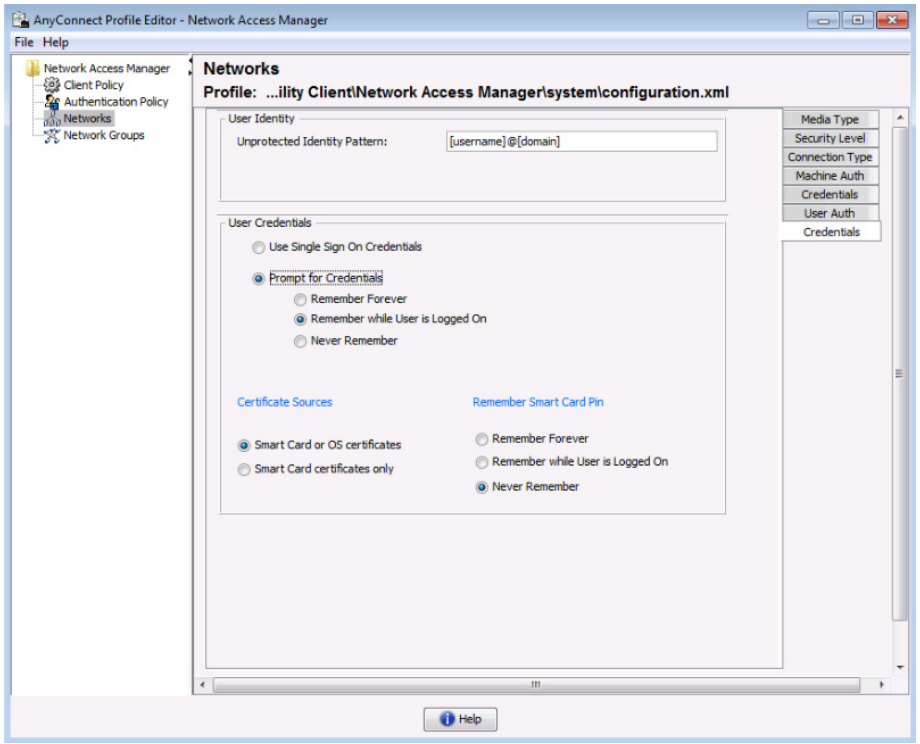
步骤10：点击Next（下一步）。

步骤11：选择EAP-TLS作为用户认证方法，然后点击Next(下一步)。

步骤12：为用户身份输入不受保护的身份模式。在本部署中，使用[username]@[domain]。

步骤13：在User Credentials（用户凭证）部分，选择Prompt for Credentials（凭证提示），然后选择Remember while User is Logged On（记住用户登录）。

步骤14：选择将Smart Card or OS certificates（Smart Card或OS证书）作为证书源，然后点击Done（完成）。

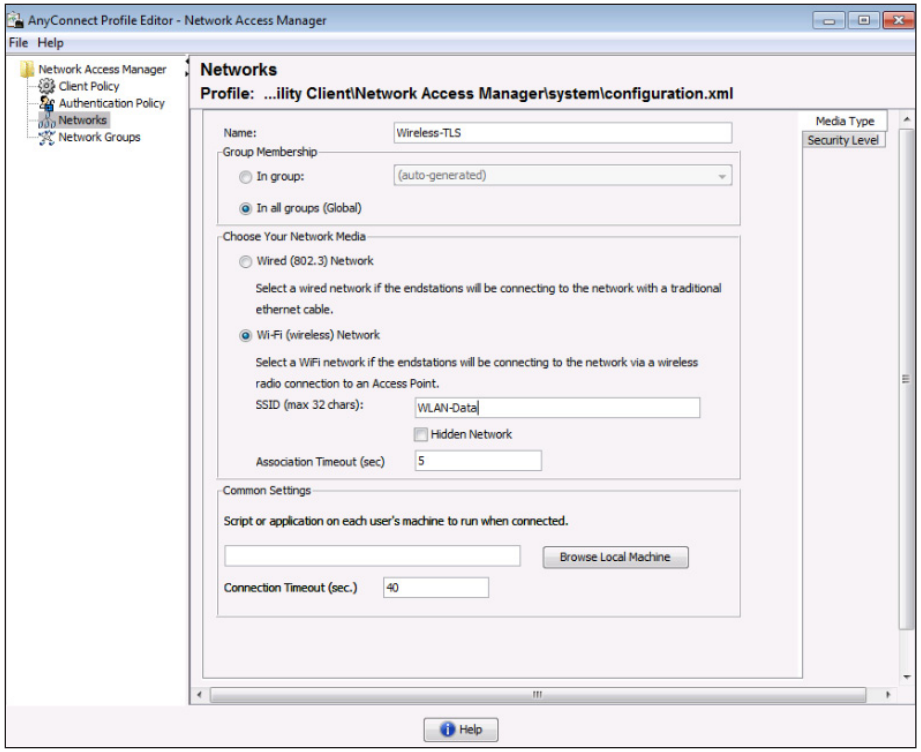


程序4　创建无线配置文件

步骤1：点击Add（添加）。这将创建一个新的无线配置文件。

步骤2：为该配置文件输入名称，然后在group membership（组成员关系）下选择In all groups (Global)（在所有组中（全局））。

步骤3：在Network Media（网络介质）部分，选择Wi-Fi (wireless) Network（Wi-Fi (无线)网络），输入无线网络的SSID，然后点击Next（下一步）。



步骤4：选中Authenticating Network（验证网络），选择WPA2 Enterprise (AES)作为关联模式，然后点击Next（下一步）。

步骤5：选择Machine and User Authentication（计算机和用户认证），然后点击Next（下一步）。

步骤6：选择EAP-TLS作为计算机认证方法，然后点击Next（下一步）。

步骤7：为计算机身份输入不受保护的身份模式。在本部署中，使用host.[domain]。

步骤8：点击Next（下一步）。

步骤9：选择EAP-TLS作为用户认证方法，然后点击Next(下一步)。

步骤10：为用户身份输入不受保护的身份模式。在本部署中，使用[username]@[domain]。

步骤11：在User Credentials（用户凭证）部分，选择Prompt for Credentials（凭证提示），然后选择Remember while User is Logged On（记住用户登录）。

步骤12：选择将Smart Card or OS certificates（Smart Card或OS证书）作为证书源，然后点击Done（完成）。

步骤13：从File（文件）菜单中，选择Save（保存）。这样将更新配置文件。

技术提示

如欲使用相同策略将Cisco AnyConnect Secure Mobility客户端部署至多个工作站，您可以创建一个定制安装包。您需要将安装盘中的所有文件复制到硬盘的文件夹中，例如C:\AnyConnect。然后，按照上述程序编辑配置文件。将文件(C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml)复制到C:\AnyConnect\Profiles\nam\configuration.xml。

将C:\AnyConnect的内容复制到某种可移动介质上，例如CD、DVD和USB驱动器等。

然后，您可以使用这一新的安装程序包，在工作站中运行安装。定制配置文件已加载，随时可用。

此时，所有Windows终端都已部署了证书，并可以使用802.1X认证。在无线网络中，任何不具有证书的设备都可以使用PEAP获取网络访问权限。

监控模式在有线网络中运行，因此未针对802.1X进行配置的终端仍可以通过MAC认证旁路(MAB)获得访问权限。

流程

配置Mac工作站，以支持802.1X认证

1. 在Mac OS X上安装根证书
2. 请求用户证书
3. 配置Mac OS X请求者

如果您拥有Apple Mac终端，您必须手动获取证书，并配置802.1X认证。本部署示例介绍了如何为Mac OS X 10.6执行该操作。

程序1　在Mac OS X上安装根证书

如欲在Mac OS X 10.6上安装可信的根证书，您需要从CA中手动请求证书，并将该证书安装在密钥链中。

步骤1：在Mac中，转至CA，网址：http://ca.cisco.local/certsrv。

步骤2：确保选择当前证书，然后选择DER编码方法。

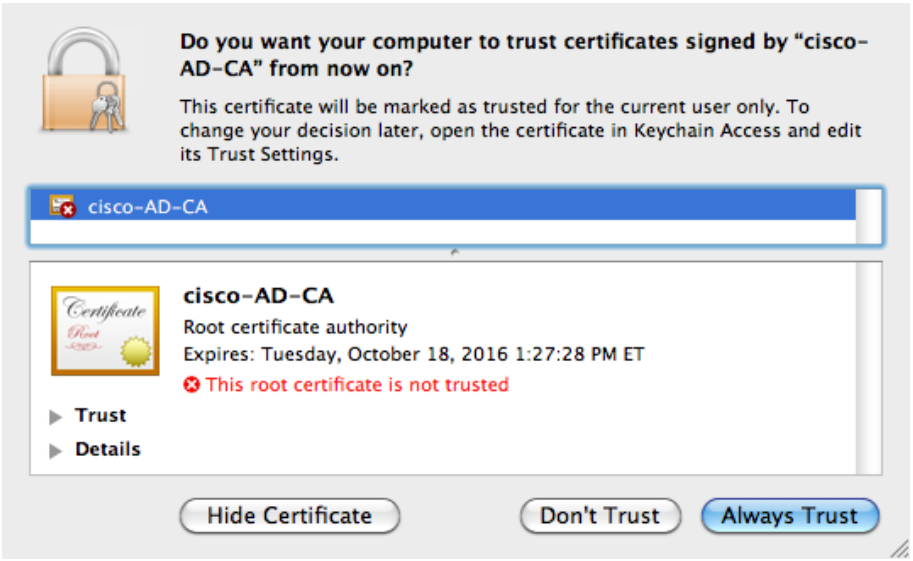
步骤3：点击Download CA Certificate（下载CA证书），然后保存证书文件。

步骤4：找到证书文件，然后双击。该操作将启动Keychain Access（密钥链访问）实用程序。

步骤5：点击Always Trust（始终信任）。

技术提示

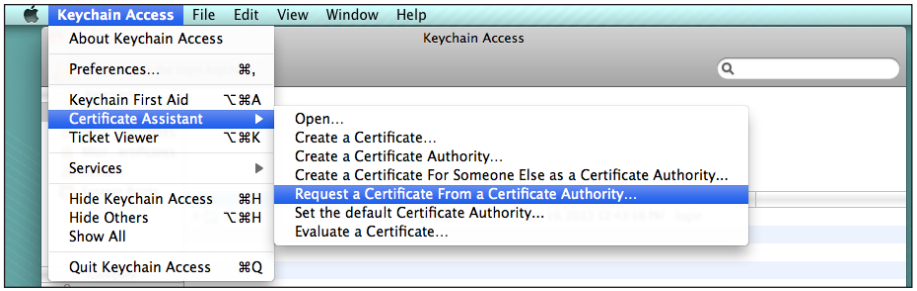
系统可能会要求您提供用户凭证，以便准许更改证书信任设置



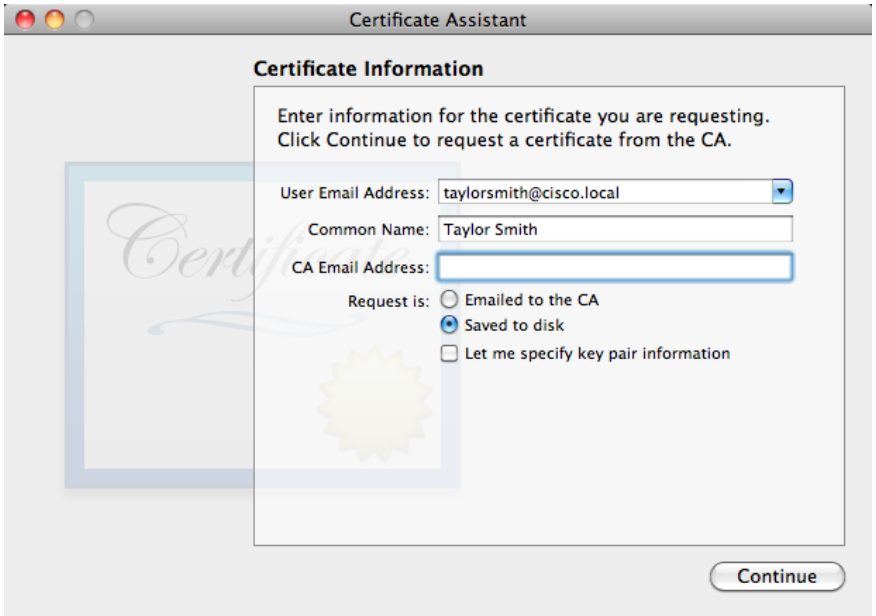
程序2 请求用户证书

下一步，您需要获取用于Mac的用户证书。为完成该步骤，您首先需要生成一个证书签名请求，然后从CA中请求证书。

步骤1：在Keychain Access实用程序中，从Keychain Access（密钥链访问）菜单中，选择Certificate Assistant（证书助理）> Request a Certificate from a Certificate Authority（从证书颁发机构请求一个证书）。



步骤2：在Certificate Assistant（证书助理）中，输入您的电子邮件地址和通用名称（通常为用户的姓和名），选择Saved to Disk（保存至磁盘），然后点击Continue（继续）。



步骤3：输入文件名和位置，然后点击Save（保存）。

步骤4：点击Done（完成）。

步骤5：在Mac中，转至http://ca.cisco.local/certsrv。当您针对CA进行认证时，请确保作为希望获取证书的用户进行认证。

技术提示

如果您在下载可信的根证书时仍保持浏览器窗口打开，请点击右上角的Home“主页”返回CA的主页面。

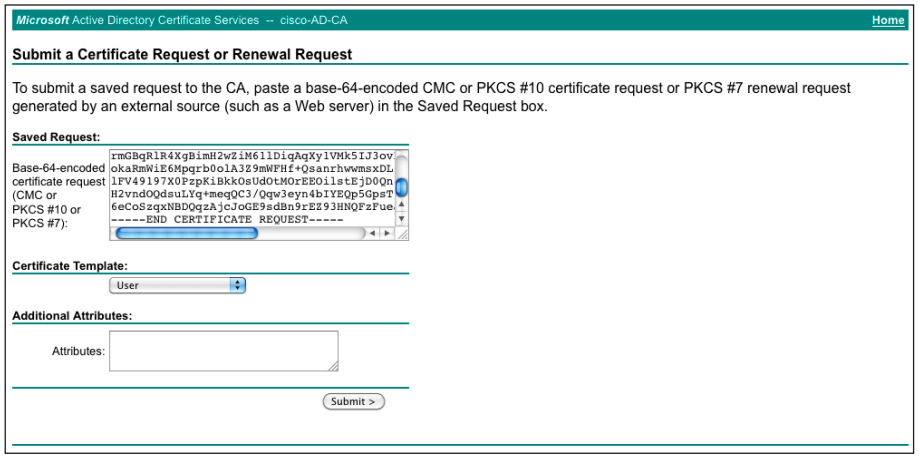
步骤6：点击Request a certificate（请求一个证书）。

步骤7：点击advanced certificate request（高级证书请求）。

步骤8：在TextEdit等文本编辑器中打开在步骤3中保存的认证请求文件，然后将其复制到剪贴板。

步骤9：在浏览器打开的证书请求中，将该内容粘贴到Saved Request（已保存请求）部分中的文本框。

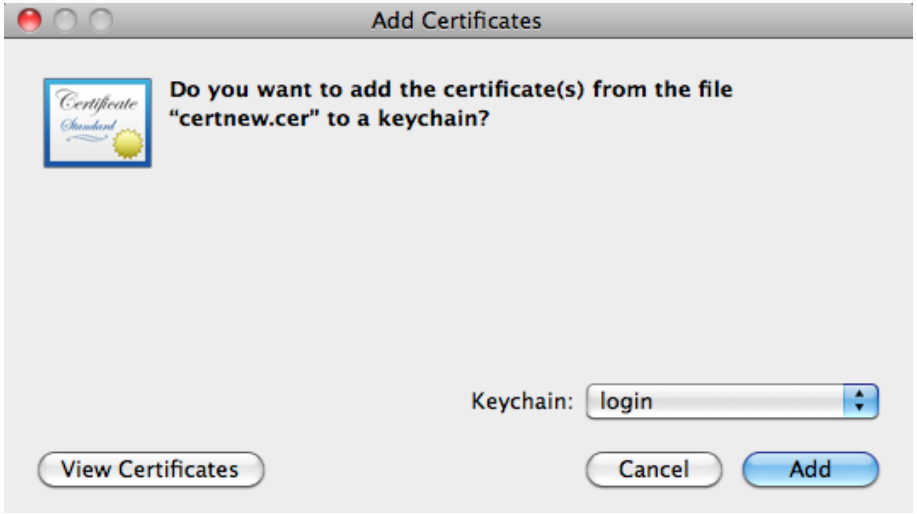
步骤10：在Certificate Template（证书模板）下拉列表中，选择User（用户），然后点击Submit（提交）。



步骤11：选择DER encoded（DER已编码），然后点击Download certificate（下载证书）。这样将保存证书。

步骤12：在Finder（查找器）中找到已保存的证书，然后双击将其导入至密钥链访问实用程序。

步骤13：在Keychain（密钥链）下拉列表中，选择login（登录），然后点击Add（添加）。



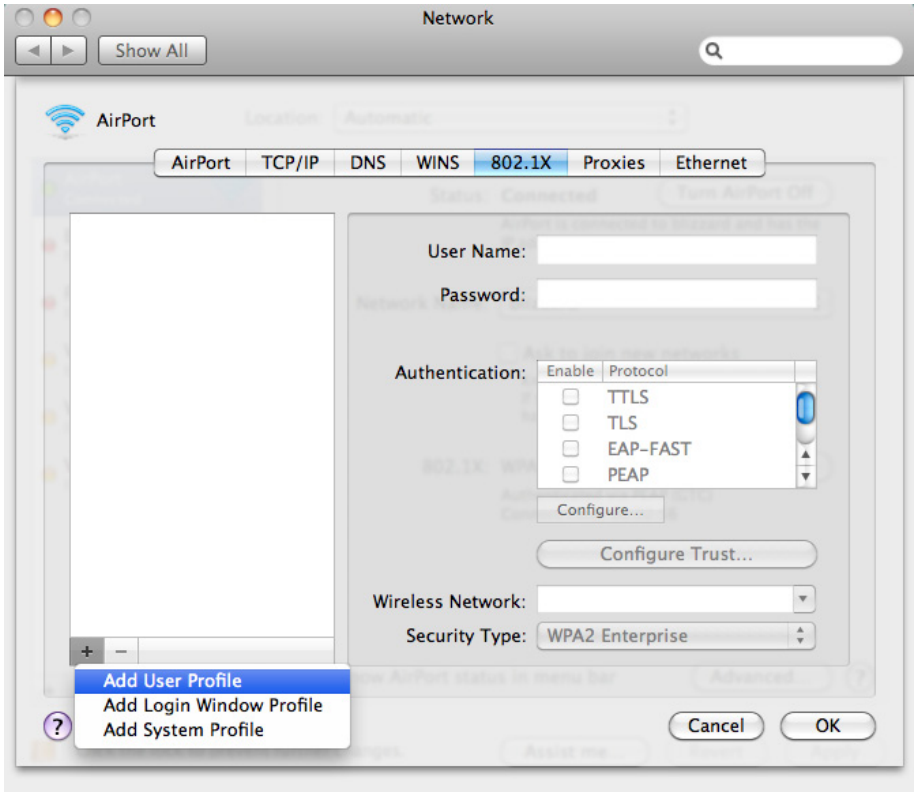
程序3 配置Mac OS X请求者

步骤1：在您的Mac上，启动System Preferences（系统偏好）。

步骤2：双击Network（网络）。

步骤3：点击Advanced（高级），然后点击802.1X选项卡。

步骤4：点击“+”号，并选择Add User Profile（添加用户配置文件）。

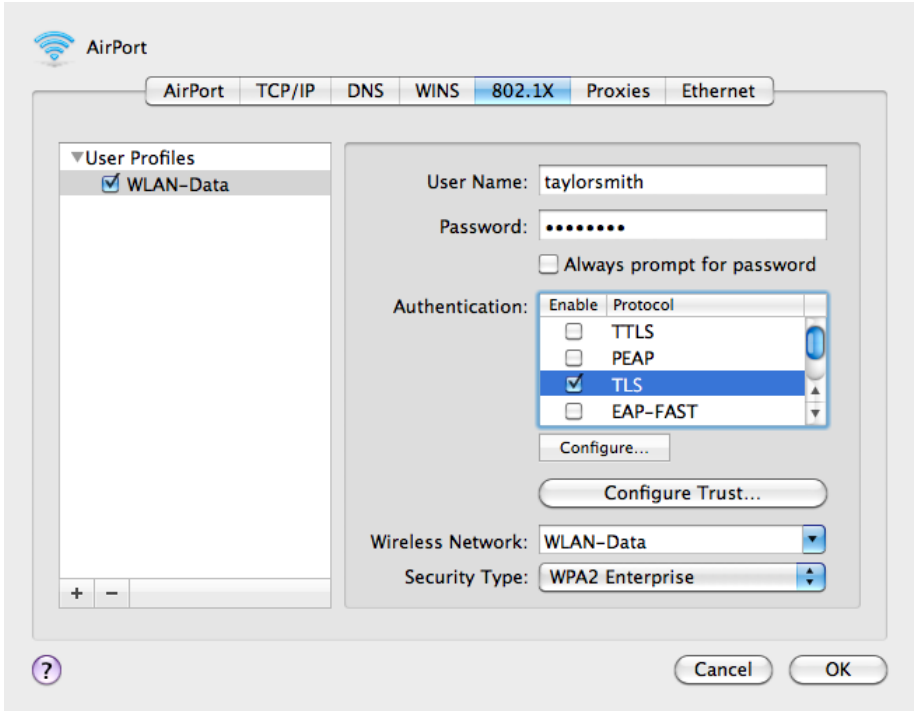


步骤5：为配置文件输入名称，然后输入用户名和密码。

步骤6：在Authentication（认证）部分，选择TLS，然后点击Configure（配置）。

步骤7：为该用户选择证书，然后点击Continue（继续）。

步骤8：对于无线连接，从列表中选择无线网络，然后针对Security Type（安全类型）选择WPA2 Enterprise。



步骤9：点击OK（确定），点击Apply（应用），然后退出System Preferences（系统偏好）。

针对所有Mac OS X终端重复此流程，以部署证书并启用802.1X认证。在无线网络中，任何不具有证书的设备都可以使用PEAP获取网络访问权限。监控模式在有线网络中运行，因此未针对802.1X进行配置的终端仍可以通过MAC认证旁路(MAB)获得访问权限。

流程

监控

1. 思科ISE仪表板
2. 配置身份组
3. 添加定制配置文件
4. 查看认证日志
5. 创建定制认证报告
6. 识别终端
7. 创建设备类型报告

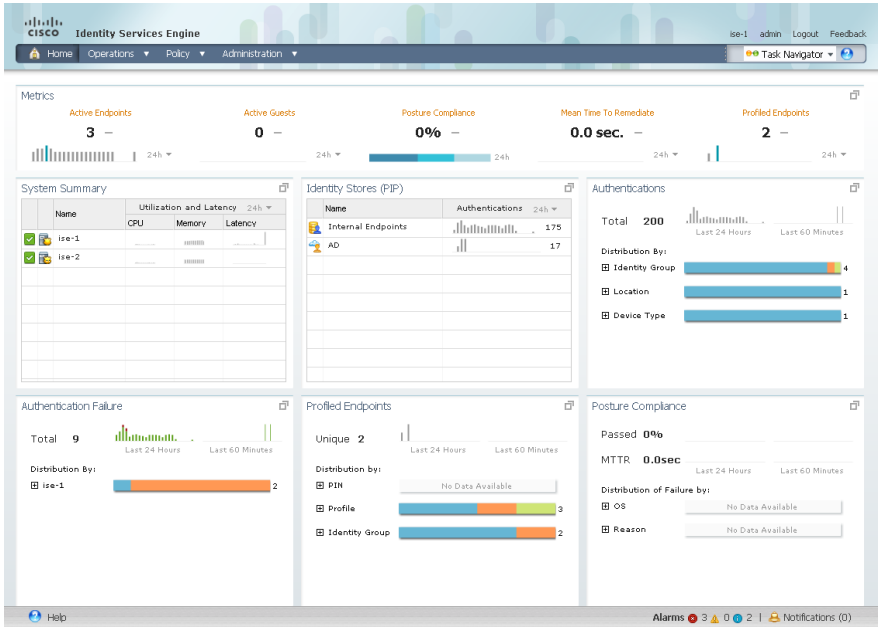
网络基础设施的配置已经完成。现在需要通过使用思科ISE的报告功能，回答有关网络访问的事件/时间/地点/人物的问题，以便更好地了解当前的网络活动。

思科ISE现在配置用于根据RADIUS和DHCP信息，对用户进行认证和对终端进行分析。思科ISE的报告功能使您可以确定哪类设备、何时、从哪里正在连接到您的网络。另外，您将了解到谁正在连接您的网络，以及使用的认证方法。

程序1　思科ISE仪表板

查看此信息的第一个位置是在思科ISE Home Dashboard（主仪表板）上。它总结了组中服务器的健康状况、如何对设备进行认证、以及对哪类设备进行了分析。

步骤1：在菜单栏，点击Home（主页）。各部分可通过点击右上角展开。



程序2 配置身份组

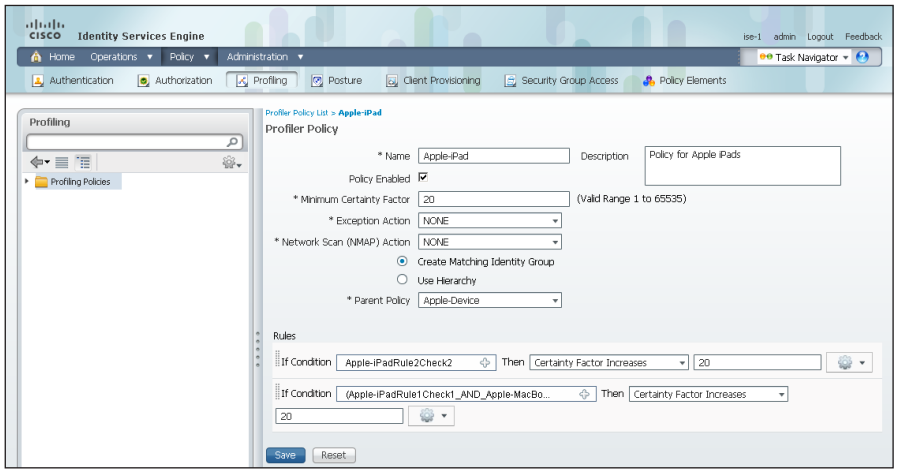
思科ISE拥有更多深入的报告选项，可提供关于连接至网络的设备的更详细信息。为帮助识别终端，您可以使用身份组来对已分析的终端进行分类，并生成报告。

以下示例介绍了如何对Apple iPad执行该操作。针对其它类型设备的程序与之类似。

步骤1：在菜单栏，将鼠标置于Policy（策略）之上，然后选择Profiling（分析）。

步骤2：点击Apple-iPad。这使您可以编辑该策略。

步骤3：选择Create Matching Identity Group（创建匹配身份组），然后点击Save（保存）。



您可以根据需求对其他终端类型重复这些步骤。您还可以查看用于分析终端的规则，以了解这一过程。在Apple iPad案例中，思科ISE使用了两个规则。一个基于DHCP信息，另一个基于HTTP。

程序3 添加定制配置文件

虽然有许多预定义的配置文件，您可能会发现您希望分析的设备不具备现成的配置文件。您可以利用该设备的独特特征创建新的配置文件。查看一些现有配置文件，了解可用于设备分析的选项和方法。

以下示例显示了如何使用从设备的DHCP请求中获取的信息为Cisco Cius创建配置文件。

步骤1：转至https://ise-1.cisco.local.

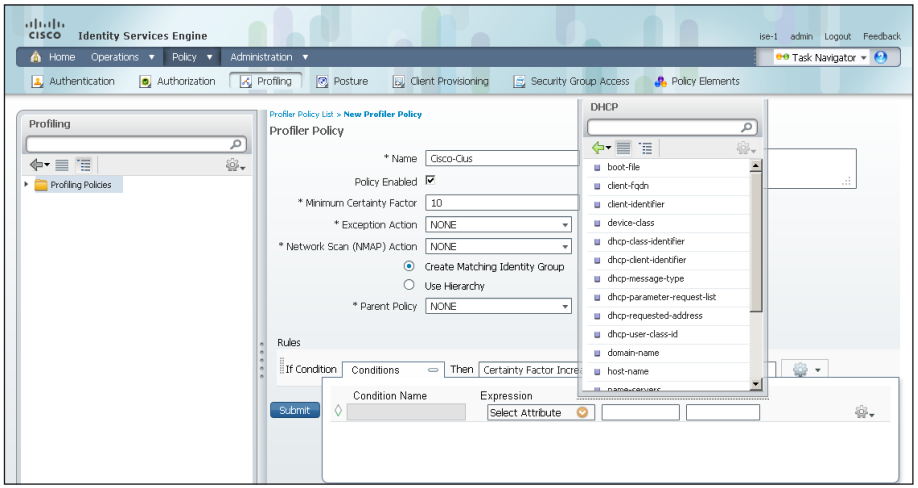
步骤2：将鼠标置于Policy（策略）上，然后从下拉菜单中，选择Profiling（分析）。

步骤3：点击Create（创建）。

步骤4：为该策略输入名称“Cisco-Cius”和描述。

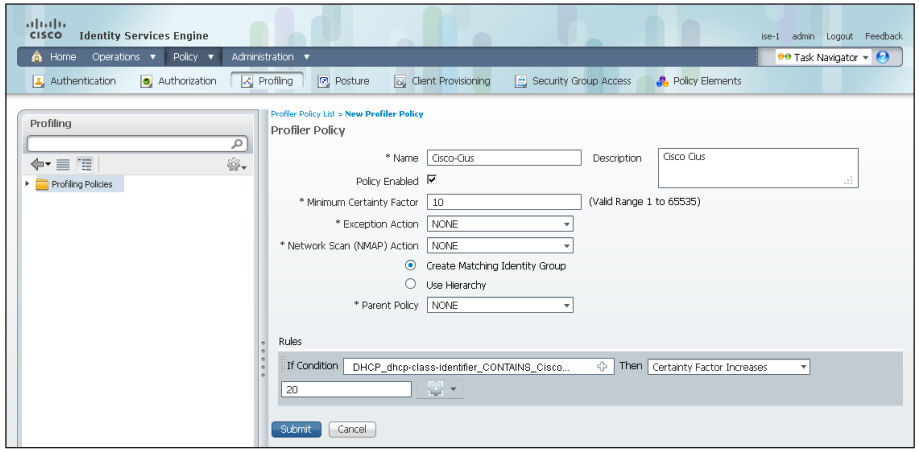
步骤5：在规则部分，点击Conditions（条件）旁边的“+”号，然后点击Create New Condition (Advance Option)（创建新条件（高级选项））。

步骤6：在Expression（表达式）下拉列表中，点击DHCP旁边的“>”号，然后选择dhcp-class-identifier。



步骤7：在第二个下拉列表中，选择CONTAINS（包含），然后在最后一个框中输入Cisco Cius。

步骤8：选择Certainty Factor Increases（确定因子增加），将值设为20，然后点击Submit（提交）。



程序4 查看认证日志

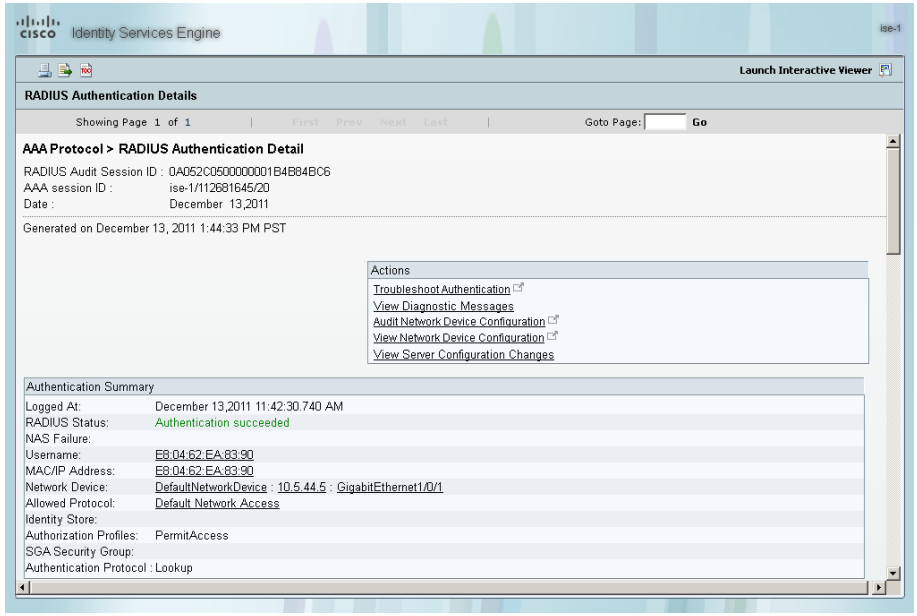
步骤1：在菜单栏，将鼠标置于Monitor（监控）之上，然后选择Authentications（认证）。认证日志显示。缺省选项是显示过去24小时内的最后20个记录。

对于通过MAB进行认证的设备，客户端的MAC地址作为用户名和终端列出。对于通过无线或VPN上的RADIUS进行认证的设备，将会显示用户名。

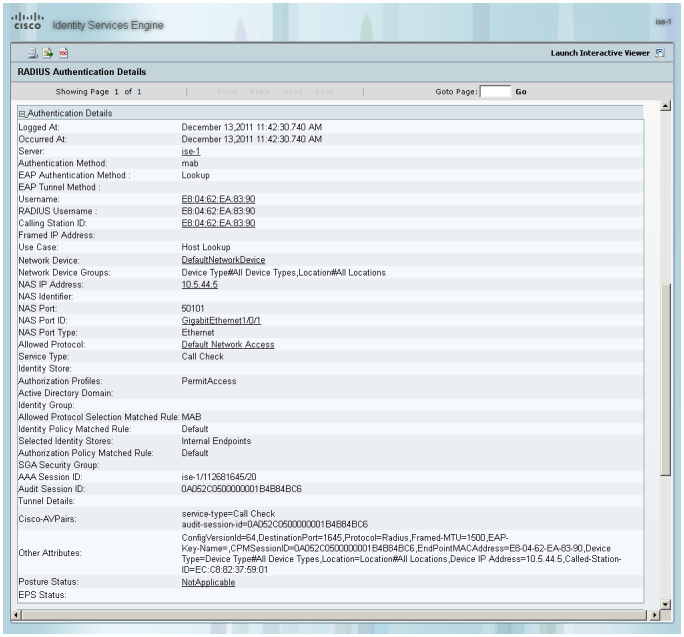
如果能够对设备进行分析，则会显示此信息。

步骤2：在MAB记录的详情列，点击“带有放大镜的页面”图标。此操作将会显示有关记录的详细认证信息。

在Authentication Summary（认证总结）部分，网络设备列出了终端连接的交换机的IP地址和端口。



在Authentication Details（认证详情）部分，您可以找到更多详情，例如Identity Group（身份组）和Identity Policy（身份策略）。



您还可以查看已采用RADIUS进行了认证的终端的类似数据。在这些记录中会显示用户名和所使用的EAP方法。

程序5 创建定制认证报告

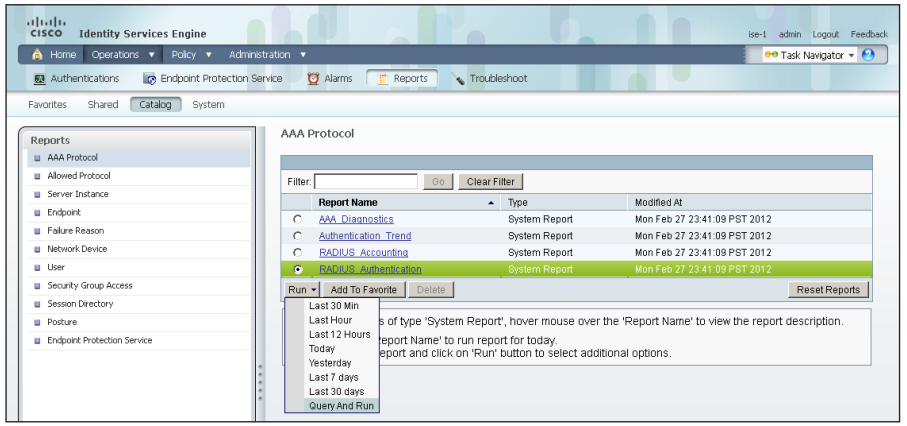
缺省认证日志视图仅限于显示最近的条目。要获得详细的报告，您需要创建一个定制报告。

步骤1：在菜单栏，将鼠标置于Monitor（监控）之上，然后在Reports（报告）部分，选择Catalog（目录）。

步骤2：在左侧窗格，选择AAA Protocol（AAA协议）。

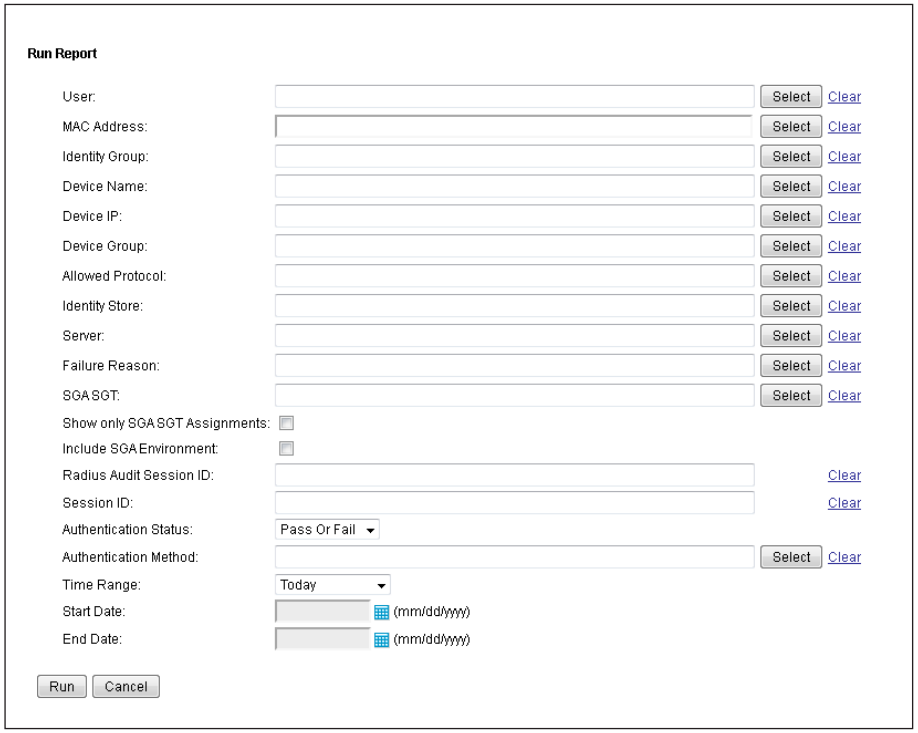
步骤3：选择RADIUS Authentication（RADIUS认证）。

步骤4：点击Run（运行）。用于生成缺省报告的不同时间范围将会显示。对于未列出的时间范围，选择Query and Run（查询并运行）。



步骤5：如果您选择Query and Run（查询并运行），所有参数可用于报告显示。选择参数后，点击Run（运行）生成报告。

图2 – RADIUS报告参数



程序6 识别终端

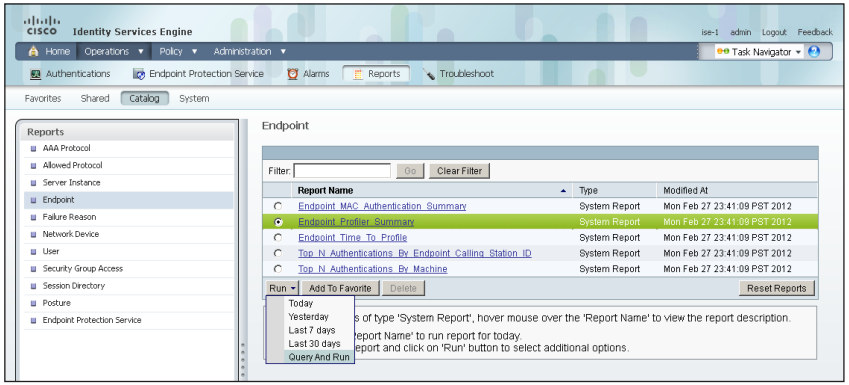
思科ISE可以使用从RADIUS和DHCP请求中收集到的信息，识别哪类设备正在连接网络。这有助于根据所使用的设备类型来确定网络安全策略。

步骤1：在菜单栏，将鼠标置于Monitor（监控）之上，然后在Reports（报告）部分，选择Catalog（目录）。

步骤2：在左侧窗格，选择Endpoint（终端）。这将显示可用的终端报告。

步骤3：选择Endpoint Profiler Summary（终端分析器总结），然后点击Run（运行）。

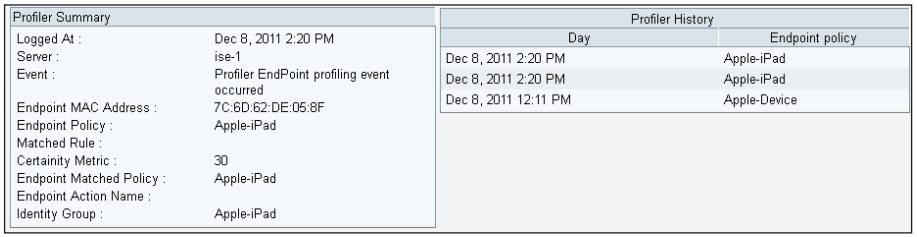
步骤4：选择所需的时间段，运行报告。



步骤5：当报告生成后，您可以通过点击放大镜图标，查看进行了已分析终端的详细信息。

总结部分中显示的详情包括MAC地址、终端策略和此终端的身份组。更多详细信息，如IP地址和网络访问设备等，在Endpoint Details（终端详情）部分提供。对于采用RADIUS进行了认证的无线和远程访问VPN终端，还将列出用户名。

图3 –终端配置文件总结



Profiler Summary	
Logged At :	Dec 8, 2011 2:20 PM
Server :	ise-1
Event :	Profiler EndPoint profiling event occurred
Endpoint MAC Address :	7C:6D:62:DE:05:8F
Endpoint Policy :	Apple-iPad
Matched Rule :	
Certainity Metric :	30
Endpoint Matched Policy :	Apple-iPad
Endpoint Action Name :	
Identity Group :	Apple-iPad

Profiler History	
Day	Endpoint policy
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 12:11 PM	Apple-Device

图4 –终端详情

Endpoint > Endpoint Profiler Detail

Generated on December 13, 2011 1:59:11 PM PST

Endpoint Session time : Not Applicable

Endpoint Details

Endpoint Static Assignment :
Endpoint Source :
Endpoint OUI : Apple, Inc
Endpoint Host Name :
Endpoint Subnet :
Endpoint NAD Address : 10.4.46.65
Endpoint VLAN :
Endpoint FQDN :
Endpoint Nameserver :
Endpoint Property : CPMSessionID=0a042e41000000494ee13838
StaticAssignment=false
NetworkDeviceGroups=Device Type#All Device Types
Location#All Locations
cisco-av-pair=audit-session-id=0a042e41000000494ee13838
Calling-Station-ID=7c-6d-62-de-05-8f
DestinationPort=1812
AcsSessionID=ise-1/112681645/7
giaddr=10.4.16.6
Device Type=Device Type#All Device Types
Service-Type=Framed
NAS-Identifier=WLC-2
TimeToProfile=25
LastNmapScanTime=0
dhcp-client-identifier=01:7c:6d:62:de:05:8f
StaticGroupAssignment=false
dhcp-requested-address=128.107.108.109
AuthenticationMethod=MSCHAPV2
EapAuthentication=EAP-MSCHAPv2
NetworkDeviceName=DefaultNetworkDevice
NAS-Port-Type=Wireless - IEEE 802.11
op=BOOTREQUEST
PostureAssessmentStatus=NotApplicable
IdentityGroupID=3e7f9a90-21db-11e1-aebd-005056a90008
Total Certainty Factor=30
User-Name=patjones
ciaddr=0.0.0.0
AuthenticationIdentityStore=AD1
dhcp-parameter-request-list=1
3
6
15
119
252
MatchedPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
DestinationIPAddress=10.4.48.41
NAS-Port=13
ADDomain=cisco.local
NmapScanCount=0
dhcp-message-type=DHCPDISCOVER
htype=Ethernet (10Mb)
EndPointMACAddress=7C-6D-62-DE-05-8F
ServiceSelectionMatchedRule=Wireless-Dot1X
PortalUser=
EndPointMatchedProfile=Apple-Device
RequestLatency=9
EapTunnel=PEAP
AuthState=Authenticated
Airespace-Wlan-Id=1
hlen=6
hops=2
host-name=SBA-iPad
FirstCollection=1323375086686
EndPointPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
SelectedAccessService=Default Network Access
secs=0
AuthorizationPolicyMatchedRule=Default
IdentityPolicyMatchedRule=Default
MessageCode=5200
DeviceRegistrationStatus=0
SelectedAuthorizationProfiles=PermitAccess
IdentityAccessRestricted=false
SelectedAuthenticationIdentityStores=AD1
flags=0x0000
chaddr=7c:6d:62:de:05:8f
yiaddr=0.0.0.0
Response={User-Name=patjones; State=ReauthSession:0a042e41000000494ee13838;
Class=CACS:0a042e41000000494ee13838:ise-1/112681645/7; Termination-Action=RADIUS-Request; MS-MPPE-
Send-Key=49:7c:f0:b6:89:6b:18:b0:d1:91:ca:89:44:25:3a:8f:fb:ef:65:7c:45:98:3d:59:1b:5f:a3:67:d4:d2:2e:f0;
MS-MPPE-
Recv-Key=c9:0b:04:f8:4e:9b:24:a8:9e:c1:5f:38:65:fc:e3:7d:eb:0a:5e:40:46:24:1b:aa:ee:0a:d7:4c:b4:fa:96:51; }
Location=Location#All Locations
PolicyVersion=1
Device IP Address=10.4.46.65
NmapSubnetScanID=0
Called-Station-ID=1c-17-d3-cb-48-50:WLAN-Data

程序7 创建设备类型报告

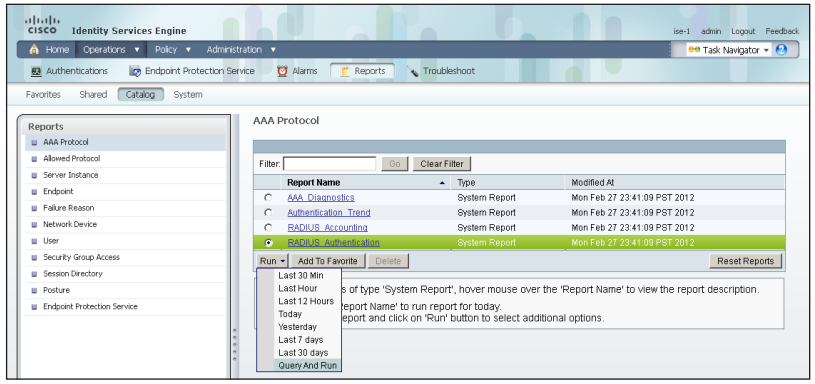
您可以根据之前配置的身份组来创建报告，以识别特定的设备。本示例将使用已经创建的组来识别Apple iPad。

步骤1：在菜单栏，将鼠标置于Monitor（监控）之上，然后在Reports（报告）部分，选择Catalog（目录）。

步骤2：在左侧窗格，点击AAA Protocol（AAA协议）。

步骤3：选择RADIUS Authentication（RADIUS认证）。

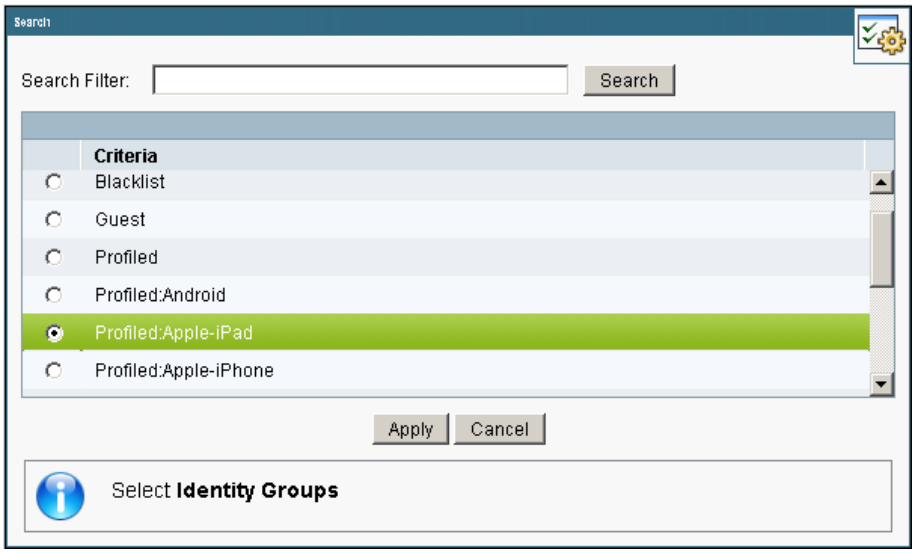
步骤4：点击Run（运行）并选择Query and Run（查询并运行）。



步骤5：针对您要查询的身份组，点击Identity Group（身份组）字段旁边的Select（选择）。搜索窗口将出现。

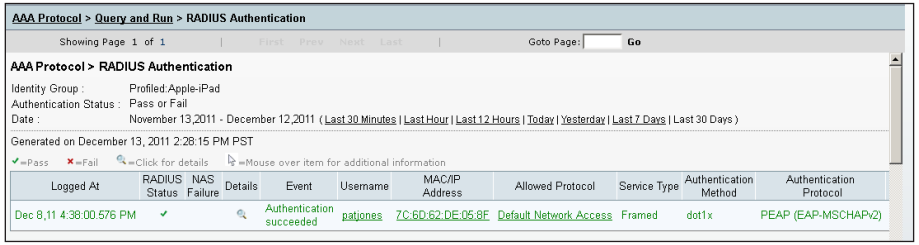
步骤6：保持搜索字段为空，点击Select（选择）搜索所有组。

步骤7：选择组Profiled:AppleiPad，然后点击Apply（应用）。



步骤8：为报告选择一个时间范围，然后点击Run（运行）。报告生成。

图5 –报告示例



附录A：产品列表

以下产品和软件版本已经过验证，可用于思科智能业务平台。

功能区域	产品	产品编号	软件版本
网络管理	思科身份服务引擎虚拟设备	ISE-VM-K9= L-ISE-BSE-2500= 思科身份服务引擎2500终端基本许可证 L-ISE-BSE-3500= 思科身份服务引擎3500终端基本许可证 L-ISE-BSE-5K= 思科身份服务引擎5000终端基本许可证 L-ISE-BSE-10K= 思科身份服务引擎10000终端基本许可证 L-ISE-ADV3Y-2500= 思科ISE 2500终端三年高级订阅许可证 L-ISE-ADV3Y-3500= 思科ISE 3500终端三年高级订阅许可证 L-ISE-ADV3Y-5K= 思科ISE 5000终端三年高级订阅许可证 L-ISE-ADV3Y-10K= 思科ISE 10000终端三年高级订阅许可证	1.1.0.665

功能区域	产品	产品编号	软件版本
网络管理	思科Prime LAN管理解决方案	LMS-4.1-100-K9 LMS 4.1，适用于设备数量高达100的网络 LMS-4.1-500-K9 LMS 4.1，适用于设备数量在100到500之间的网络 LMS-4.1-1K-K9 LMS 4.1，适用于设备数量在500到1000之间的网络 LMS-4.1-2.5K-K9 LMS 4.1，适用于设备数量在1000到2500之间的网络	4.1
用于PC、电话、接入点和其它设备的接入层	Catalyst 2960S 可堆叠以太网10/100/1000端口，带PoE+和堆叠模块	WS-C2960S-24PD-L Catalyst 2960S 24 GigE PoE+，2个10G SFP+ LAN Base WS-C2960S-48FPD-L Catalyst 2960S 48 GigE PoE+，2个10G SFP+ LAN Base WS-C2960S-24PS-L Catalyst 2960S 24 GigE PoE+、4个SFP LAN Base WS-C2960S-48FPS-L Catalyst 2960S 48 GigE PoE+、4个SFP LAN Base C2960S-STACK= Catalyst 2960S Flexstack堆叠模块	12.2(58)SE1

功能区域	产品	产品编号	软件版本
用于PC、电话、接入点和其它设备的接入层	Catalyst 3560X 以太网10/100/1000端口，带PoE+和上行链路模块	WS-C3560X-24P-S Catalyst 3750 24 10/100/1000T PoE +和IPB Image WS-C3560X-48PF-S Catalyst 3750 48 10/100/1000T全PoE +和IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP上行链路模块 C3KX-NM-10G Catalyst 3750X 10Gig SFP+上行链路模块	12.2(58)SE1
用于PC、电话、接入点和其它设备的接入层	Catalyst 3750X 可堆叠以太网10/100/1000端口，带PoE+和上行链路模块	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE +和IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T 全PoE +和IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP上行链路模块 C3KX-NM-10G Catalyst 3750X 10Gig SFP+上行链路模块	12.2(58)SE1
用于PC、电话、接入点和其它设备的接入层	Catalyst 4507R+E 双管理引擎 双电源	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE +和IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T 全PoE + 和IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP上行链路模块 C3KX-NM-10G Catalyst 3750X 10Gig SFP+上行链路模块	12.2(54)SG1

功能区域	产品	产品编号	软件版本
VPN（互联网边缘5K）	ASA 5510或ASA 5520或ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-K9 ASA5540-AIP40-K9	8.4.1
VPN（互联网边缘10K）	2个ASA 5520和500 SSL席位，或者2个ASA 5540和1000 SSL席位	ASA5520-SSL500-K9 ASA5540-SSL1000-K9	8.4.1
无线局域网	5508无线局域网控制器	AIR- CT5508-100-K9 5508无线局域网控制器，带100个无线接入点许可证	7.1.91.0

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

B-0000137-1 3/12