基本设置

管理门户

图 *1:* 思科 ***ISE*** 管理门户

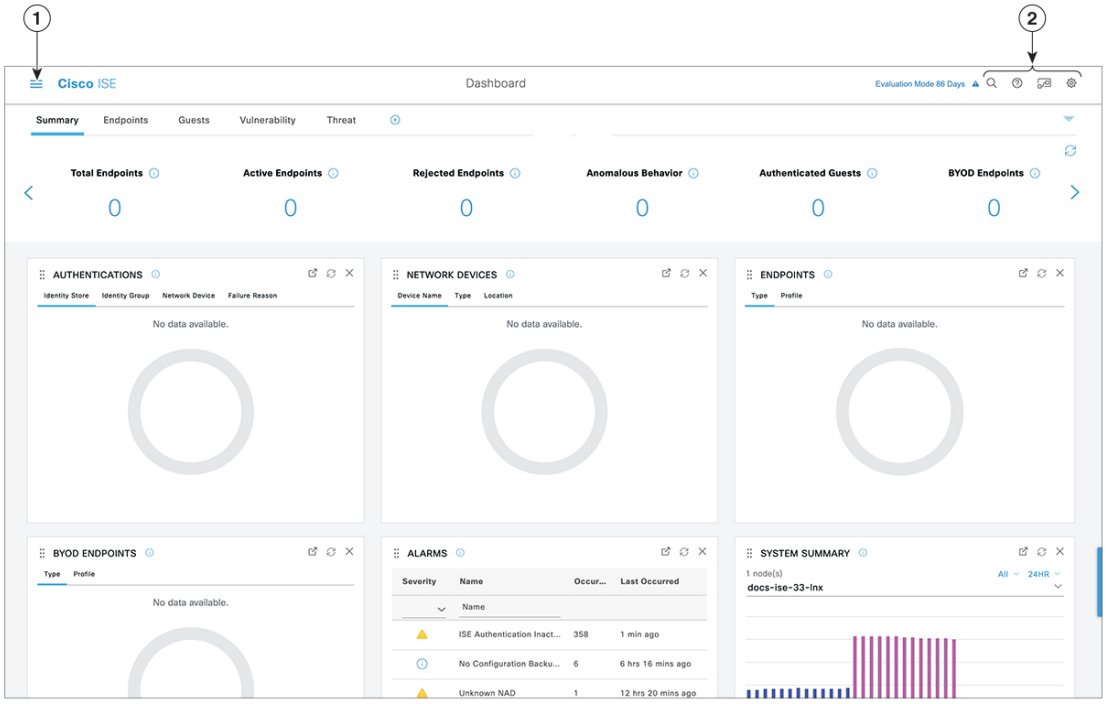
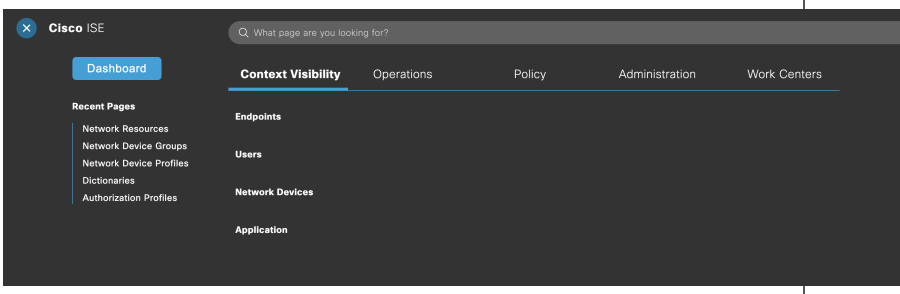


表 *1:* 思科 ***ISE*** 管理门户的组件

1	菜单图标	点击包含以下菜单的滑入式窗口的**菜单 (Menu)** 图标 (☰)。滑入式菜单窗口还包含一个搜索栏，您可以在其中找到所需的窗口。点击主页的**控制板 (Dashboard)**。 图 *2:* 思科 ***ISE*** 主菜单  • **情景可视性 (Context Visibility)**：情景可视性窗口显示有关终端、用户和网络访问设备 (NAD) 的信息。情景可视性信息按功能、应用、自带设备 (BYOD) 和其他类别进行细分，具体取决于您注册的许可证。情景可视性窗口使用中央数据库并从数据库表、缓存和缓冲区收集信息。因此，情景可视性 Dashlet 和列表中的内容会快速更新。情景可视性窗口由上方的 Dashlet 和底部的信息列表组成。通过修改列表中的列属性来过滤数据时，Dashlet 会刷新以显示修改的内容。 • **策略 (Policy)**：“策略”(Policy) 窗口包含用于管理身份验证、授权、分析、安全评估和客户端调配区域中的网络安全的工具。 • **管理 (Administration)**：“管理”(Administration) 窗口包含用于管理Cisco ISE 节点、许可证、证书、网络设备、用户、终端和访客服务的工具。

2	右上角菜单图标	

-

  使用此图标搜索终端并按配置文件、故障、身份库、位置、设备类型等显示其分布。

-

  点击此图标可查看交互式帮助 菜单，由此可访问多个资源。

-

  点击此图标可访问以下选项：

  - **PassiveID 设置 (PassiveID Setup)**：**PassiveID 设置 (PassiveID Setup)** 选项将启动 **PassiveID 设置 (PassiveID Setup)** 向导以使用 Active Directory 设置被动身份。配置服务器以从外部身份验证服务器收集用户身份和 IP 地址，并将经过身份验证的 IP 地址传送给相应的用户。

  - **可视性设置 (Visibility Setup)**：**可视性设置 (Visibility Setup)** 是一种价值证明 (PoV) 服务，它收集终端数据，例如应用、硬件资产、USB 状态、防火墙状态和 Windows 终端的总体合规性状态。然后，收集的数据将发送到Cisco ISE。当您启动 **ISE 可视性设置 (ISE Visibility Setup)** 向导时，可指定 IP 地址范围，以便对首选网段或一组终端运行终端发现。

    该 PoV 服务使用 Cisco Stealth Temporal 代理收集终端安全评估数据。Cisco ISE 会将 Cisco Stealth Temporal 代理推送到具有管理员帐户类型的运行 Windows 的计算机，该帐户会自动运行临时可执行文件以收集情景信息。然后，代理会自行删除。要体验 Cisco Stealth Temporal 代理的可选调试功能，请选中**终端日志记录 (Endpoint Logging)** 复选框（点击**菜单 (Menu)** 图标 (≡) 并选择**可视性设置 (Visibility Setup)** > **终端安全评估 (Posture)**），将调试日志保存在一个或多个终端中。您可以在以下任一位置查看日志：

    - C:\WINDOWS\syswow64\config\systemprofile\（64 位操作系统）
    - C:\WINDOWS\system32\config\systemprofile\（32 位操作系统）

  - **运行终端脚本 (Run Endpoint Scripts)**：选择此选项可在连接的终端上运行脚本，以执行符合组织要求的管理任务。这包括卸载过时软件、启动或终止进程或应用以及启用或禁用特定服务等任务。

-

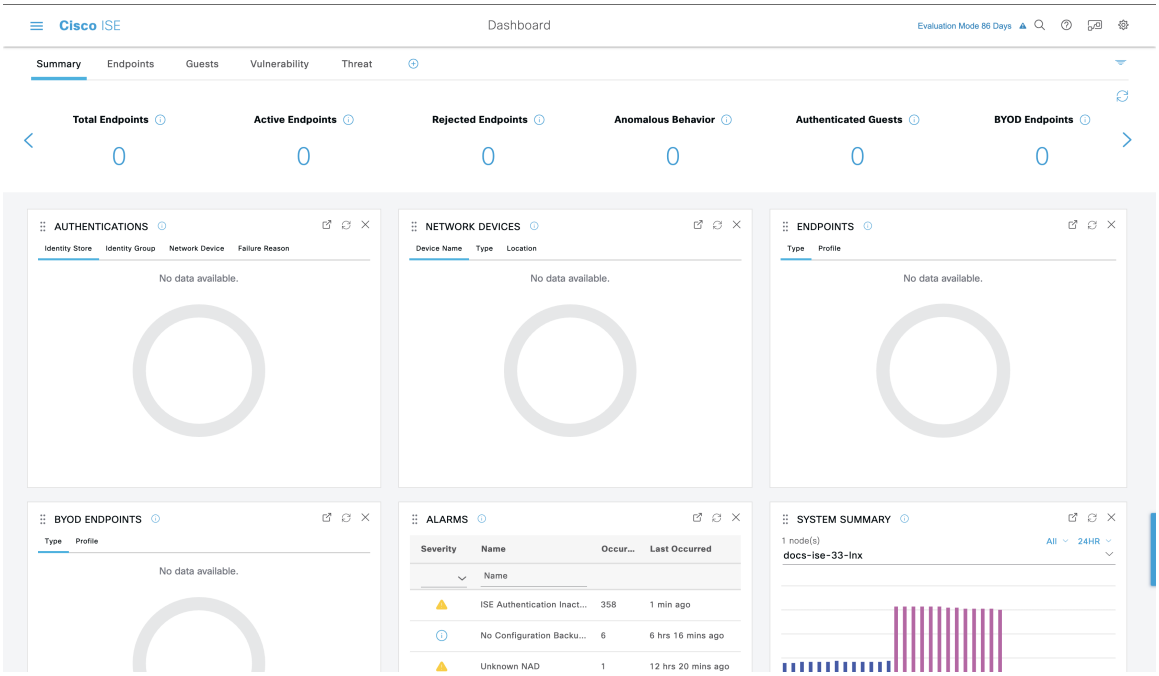
  点击此图标可查看系统活动的菜单，包括启动在线帮助和配置帐

		户设置。

思科 ISE 主页控制板

Cisco ISE 主页控制板显示对于有效地进行监控和故障排除很重要的综合性相关统计数据。控制板元素通常显示 24 小时内的活动。下图是Cisco ISE 控制板上提供的一些信息示例。仅可以在主策略管理节点 (PAN) 门户上查看Cisco ISE 控制板数据。

图 *3:* 思科 *ISE* 主页控制板



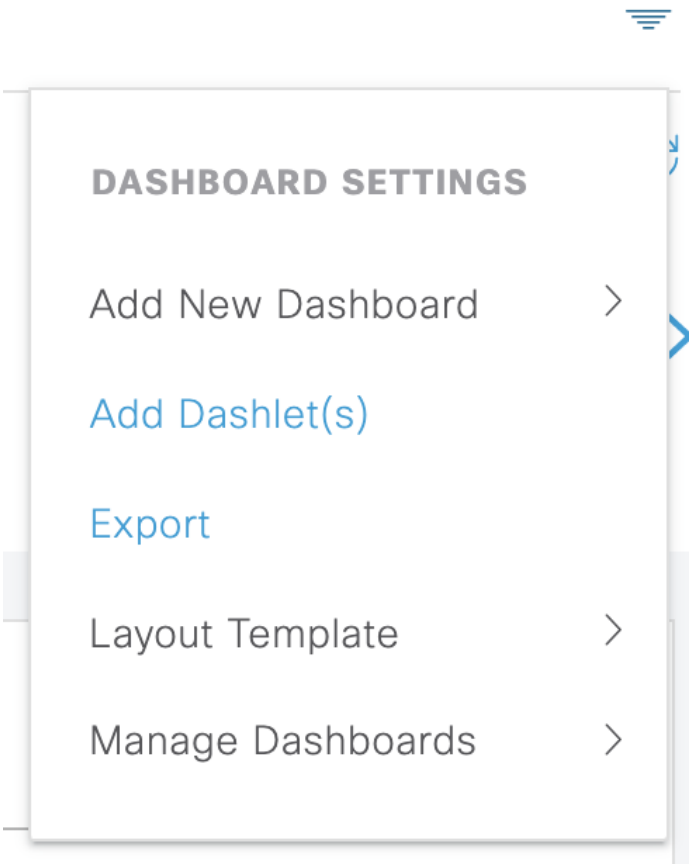
主页有五个显示Cisco ISE 数据的默认控制板。其中每个控制板都有多个预定义的 Dashlet。

- **摘要 (Summary)**：此控制板包含线性指标 Dashlet、饼形图 Dashlet 和列表 Dashlet。指标 Dashlet 不可配置。默认情况下，此控制板包含**状态 (Status)**、**终端 (Endpoints)**、**终端类别 (Endpoint Categories)** 和**网络设备 (Network Devices)** Dashlet。
- **终端 (Endpoints)**：默认情况下，此控制板包含**状态 (Status)**、**终端 (Endpoints)**、**终端类别 (Endpoint Categories)** 和**网络设备 (Network Devices)** Dashlet。
- **访客 (Guests)**：此控制板包含提供有关访客用户类型、登录失败和活动位置的信息的 Dashlet。
- **漏洞 (Vulnerability)**：此控制板显示漏洞服务器向Cisco ISE 报告的信息。
- **威胁 (Threat)**：此控制板显示威胁服务器向Cisco ISE 报告的信息。

配置主页控制面板

您可以点击页面右上角的**倒金字塔**图标来自定义主页控制板：

图 *4:* 自定义控制板



下拉列表中显示以下选项：

- **添加新控制板 (Add New Dashboard)** 可以让您添加新的控制板。在显示的字段中输入值，然后点击**应用 (Apply)**。
- **添加 Dashlet (Add Dashlet(s))** 会显示一个对话框，其中包含可用的 Dashlet 列表。点击 Dashlet 名称旁边的**添加 (Add)** 或**删除 (Remove)**，可从控制板添加或删除 Dashlet。
- **导出 (Export)** 会将选定的主页视图保存为 PDF。
- **布局模板 (Layout Template)** 会配置此视图中显示的列数。
- **管理控制板 (Manage Dashboards)** 包含两个选项：
  - **标记为默认控制板 (Mark As Default Dashboard)**：选择此选项可将当前控制板设为您选择主页时的默认视图。

- **重置所有控制板 (Reset All Dashboards)**：使用此选项可以重置所有控制板，并删除所有主页控制板上的配置。

情景可视性视图

“情景可视性”(Context Visibility) 页面的结构类似于主页，不同之处在于“情景可视性”(Context Visibility) 页面：

- 当您过滤显示数据时，保留当前环境（浏览器窗口）
- 可定制程度更高
- 侧重终端数据

您可以仅从主要管理节点 (PAN) 上查看情景可视性数据。

情景 (Context) 页面上的 Dashlet 显示有关终端和终端到 NAD 的连接信息。当前显示的信息取决于每个页面上的 Dashlet 下数据列表中的内容。每页根据选项卡名称显示终端数据视图。过滤数据时，列表和 Dashlet 都将更新。您可以点击圆形图的一个或多个部分，也可以过滤表中的行，或者任意组合这些操作来过滤数据。在您选择过滤器时，效果是可以叠加的，也称为级联过滤器，可让您深入查找想要的特定数据。您也可以点击列表中的终端，获得该终端的详细视图。

“情景可视性”(Context Visibility) 下有四个主视图：

- 终端 - 您可以根据设备类型、合规状态、身份验证类型、硬件清单等选择要显示哪些终端。有关其他信息，请参考硬件控制板 ， 第 12 页部分。

注释

我们建议在 NAD 上启用记账设置，以确保将记账开始和更新信息发送到思科 ISE。

仅当启用记账后，Cisco ISE 才能收集记账信息，如最新的 IP 地址、会话状态（已连接、已断开或已拒绝）、终端的非活动天数。这些信息显示在“实时日志/实时会话”(Live Logs/Live Session) 和“情景可视性”(Context Visibility) 页面中。在 NAD 上禁用记账时，“实时日志/实时会话”(Live Logs/Live Session) 和“情景可视性”(Context Visibility) 页面之间的记账信息可能缺失、不正确或不匹配。

注释 通过“可视性设置”(Visibility Setup) 向导，可以为终端发现添加 IP 地址范围列表。配置此向导后，Cisco ISE 会对终端进行身份验证，但未包含在配置的 IP 地址范围内的终端不会显示在“情景可视性”(Context Visibility) > “终端”(Endpoints) 选项卡和终端列表页面（在“工作中心”(Work Centers)> “网络访问”(Network Access)> “身份”(Identities)> “终端”(Endpoints)）中。

- 基于用户 (User-Based) - 显示来自用户身份源的用户信息。

  使用此视图时请注意以下几点：

  1. 如果用户名或密码属性发生任何更改，当身份验证状态发生变化时，将立即反映在此页面上。
  2. 如果在 Active Directory 中更改了除用户名以外的任何其他属性，则更新后的属性仅在重新身份验证后 24 小时后显示。
  3. 如果在 Active Directory 中更改用户名和其他属性，则更新后的更改将在重新身份验证后立即显示。

- 网络设备 (Network Devices) - 已连接终端的 NAD 列表。您可以点击 NAD 上的终端数量（最右列），以显示一个“情景可视性”(Context Visibility) 屏幕，其中列出按照该 NAD 过滤的所有设备。

  注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的网络设备会话状态摘要报告（“操作”[Operations]> “报告”[Reports] > “目录”[Catalog] > “网络设备”[Network Device] > “会话状态摘要”[Session Status Summary]）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。

- 应用 (Application) -“应用”(Application) 视图用于确定已安装指定应用的终端数量。结果以图形和表格格式显示。图形表示形式可帮助进行比较分析。例如，可以在表和条形图中找到使用 Google Chrome 软件的终端数量及其版本、供应商和类别（反网络钓鱼、浏览器等）。有关详细信息，请参阅应用控制板部分。

您可以在情景可视性 (Context Visibility) 下创建新视图，以创建自定义列表来进行其他过滤。此版本的自定义视图不支持 Dashlet。

在 Dashlet 中点击圆形图的一部分，打开新页面，其中包含在情景可视性 (Context Visibility) 模式下通过该 Dashlet 过滤的数据。在该新页面中，可以继续过滤所显示的数据，如在视图中过滤显示的数据，第 15 页中所述。

有关使用情景可视性查找终端数据的详细信息，请参阅以下使用 ISE 2.1 的Cisco YouTube 视频 https://www.youtube.com/watch?v=HvonGhrydfg。

相关主题

硬件控制板 ，第 12 页

情景可视性中的属性

为情景可视性提供属性的系统和服务有时对相同属性名称有不同值。几个示例如下所示：

操作系统

- *OperatingSystem* - 终端安全评估操作系统
- *operating-system* - NMAP 操作系统
- *operating-system-result* - 分析器整合操作系统

注释 在思科 ISE 中为终端启用多个探测时，“情景可视性”(Context Visibility) 页面中显示的终端操作系统数据可能存在一些差异。

门户名称

- *Portal.Name* - 打开设备注册时的访客门户名称
- *PortalName* - 未打开设备注册时的访客门户名称

门户用户

- *User-Name* - 来自 RADIUS 身份验证的用户名
- *GuestUserName* - 访客用户
- *PortalUser* - 门户用户

应用控制板

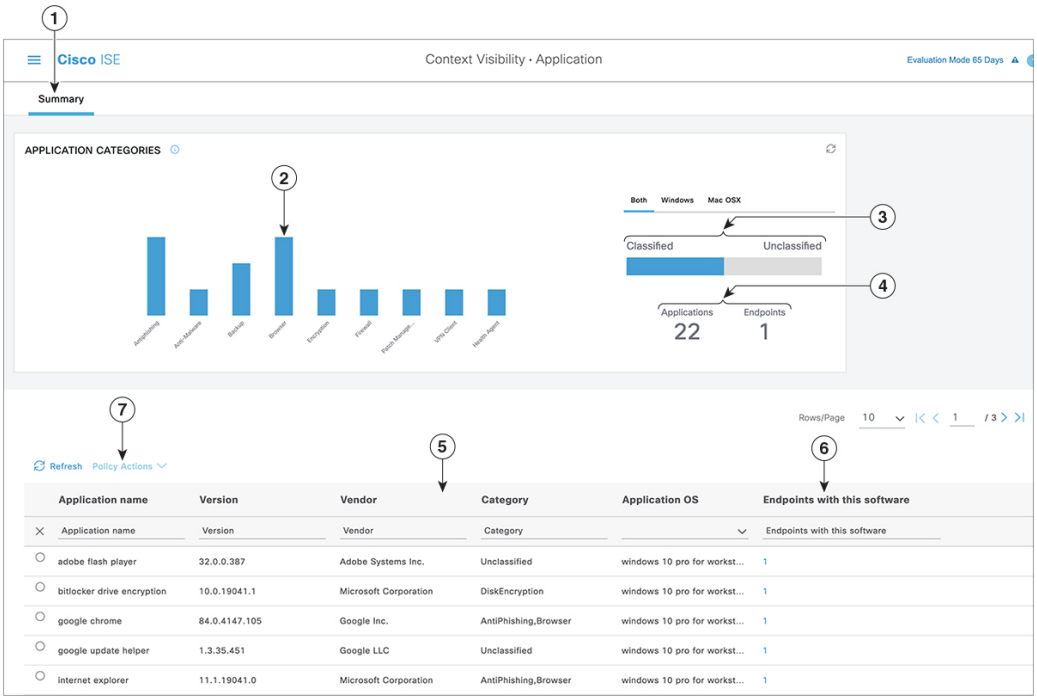


表 *2:* 应用控制板的说明

编号	说明
1	系统会默认选择**摘要 (Summary)** 选项卡。它显示**应用类别 (Application Categories)** Dashlet，其中包含条形图。应用分为 13 个类别：不属于这些类别的应用称为“未分类”应用。 可用类别包括防恶意软件、反钓鱼、备份、浏览器、防数据丢失、数据存储、加密、防火墙、即时消息程序、补丁管理、公共文件共享、虚拟机和 VPN 客户端。
2	每个条形对应一个类别。您可以将鼠标悬停在每个条形上，以查看与所选应用类别对应的应用和终端总数。
3	属于“分类”(Classified) 类别的应用和终端以蓝色显示。未分类的应用和终端显示为灰色。您可以将鼠标悬停在分类或未分类的类别条上，以查看属于该类别的应用和终端的总数。您可以点击**分类 (Classified)**，查看条形图和表 (5) 中的结果。当您点击**未分类 (Unclassified)** 时，条形图被禁用（灰显），结果显示在表 (5) 中。
4	系统根据所选过滤器显示应用和终端。您可以在点击不同的过滤器时查看浏览路径记录。您可以点击**清除所有过滤器 (Clear All Filters)**，删除所有过滤器。

<table>
<tr><th>编号</th><th>说明</th></tr>
<tr><td>5</td><td>当您点击多个条形时，表中会显示相应的分类应用和终端。例如，如果您选择“防恶意软件”(Antimalware) 和“补丁管理”(Patch Management) 类别，则显示以下结果。
<table>
<tr><th>应用名称</th><th>版本</th><th>供应商</th><th>类别</th><th>应用操作系统</th><th>有此软件的终端</th></tr>
<tr><td>网守</td><td>9.9.5</td><td>Apple Inc.</td><td>反恶意软件</td><td>windows 7 64 位、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>网守</td><td>10.9.5</td><td>Apple Inc.</td><td>反恶意软件</td><td>Windows 8 64 位、mac osx 10.10</td><td>3</td></tr>
<tr><td>软件更新</td><td>2.3</td><td>Apple Inc.</td><td>补丁管理</td><td>windows 7 64 位、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>点击表中有此软件的终端 (Endpoints With This Software) 列中的某个终端，查看终端详细信息，例如 Mac 地址、NAD IP 地址、NAD 端口 ID/SSID，IPv4 地址等。</td></tr>
<tr><td>7</td><td>您可以选择一个应用名称并从策略操作 (Policy Actions) 下拉列表中选择创建应用合规性 (Create App Compliance) 选项，以创建应用合规性条件和补救。</td></tr>
</table>

硬件控制板

“情景可视性”(Context Visibility) 下的“端点硬件”(Endpoint Hardware) 选项卡可以帮助您收集、分析和报告短时间内的终端硬件资产信息。可以收集信息，例如查找内存容量低的终端或查找终端的 BIOS 型号/版本。可以根据这些结果增加内存容量或升级 BIOS 版本。可以在计划购买资产之前评估要求。可以确保及时更换资源。可以收集此信息，而无需安装任何模块或与终端交互。总而言之，可以有效地管理资产生命周期。

在传出数据包通过以太网微处理器退出前，此 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **硬件 (Hardware)** 页面显示**制造商 (Manufacturers)** 和**终端利用率 (Endpoint Utilizations)** Dashlet。这些 Dashlet 反映基于所选过滤器的更改。**制造商 (Manufacturers)** Dashlet 显示装有 Windows 和 Mac OS 的终端的硬件资产详细信息。**终端利用率 (Endpoint Utilizations)** 面板显示终端的 CPU、内存和磁盘利用率。可以选择三个选项中的任何一个，以查看利用率百分比。

- CPU 使用率超过 n% 的设备。
- 内存使用率超过 n% 的设备。
- 磁盘使用率超过 n% 的设备。

注释 硬件资产数据需要 120 秒才能显示在 ISE GUI 中。将收集硬件资产数据以提供终端安全评估合规和不合规状态。

注释
- “硬件可视性”(Hardware Visibility) 页面中的快速过滤器至少需要 3 个字符才能生效。另一种使快速过滤器高效工作的方法是，在输入字符后点击其他列属性的过滤器。
- 一些列属性显示为灰色，这是因为此表仅用于根据与硬件相关的属性进行过滤。
- 操作系统过滤器仅适用于**制造商 (Manufacturers)** 图表。它与下面的表无关。

终端及其连接的外部设备的硬件属性以表格格式显示。系统将显示以下硬件属性：

- MAC 地址
- BIOS 制造商 (BIOS Manufacturer)
- BIOS 序列号 (BIOS Serial Number)
- BIOS 型号 (BIOS Model)
- 附加设备 (Attached Devices)
- CPU 名称
- CPU 速度 (GHz) (CPU Speed (GHz))
- CPU 利用率 (%) (CPU Usage (%))
- 核心数量
- 处理器数量 (Number of Processors)
- 内存 (GB) (Memory Size (GB))
- 内存使用率 (%) (Memory Usage (%))
- 内部磁盘总大小 (GB) (Total Internal Disk(s) Size (GB))
- 内部磁盘总可用大小 (GB) (Total Internal Disk(s) Free Size (GB))
- 内部磁盘总使用率 (%) (Total Internal Disk(s) Usage (%))
- 内部磁盘数 (Number of Internal Disks)
- NAD 端口 ID (NAD Port ID)
- 状态
- 网络设备名称
- 位置

- UDID
- IPv4 地址
- 用户名
- 主机名 (Hostname)
- 操作系统类型
- 异常行为
- 终端配置文件
- 说明
- 终端类型
- 身份组
- 注册日期
- 身份库
- 授权配置文件

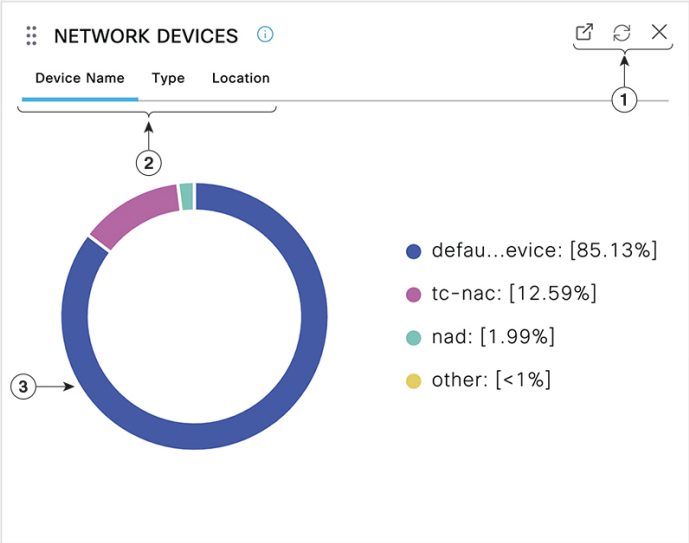
可以点击**已连接设备 (Attached Devices)** 列中与终端对应的编号，以查看当前连接到终端的 USB 设备的名称、类别、制造商、类型、产品 ID 和供应商 ID。

注释 Cisco ISE 会分析客户端系统的硬件属性，但对于某些硬件属性，Cisco ISE 不会进行分析。这些硬件属性可能不会显示在“硬件情景可视性”(Hardware Context Visibility) 页面中。

可以在以下位置控制硬件资产数据收集间隔 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)** 页面。默认间隔为 5 分钟。

Dashlet

下图是 Dashlet 的示例：



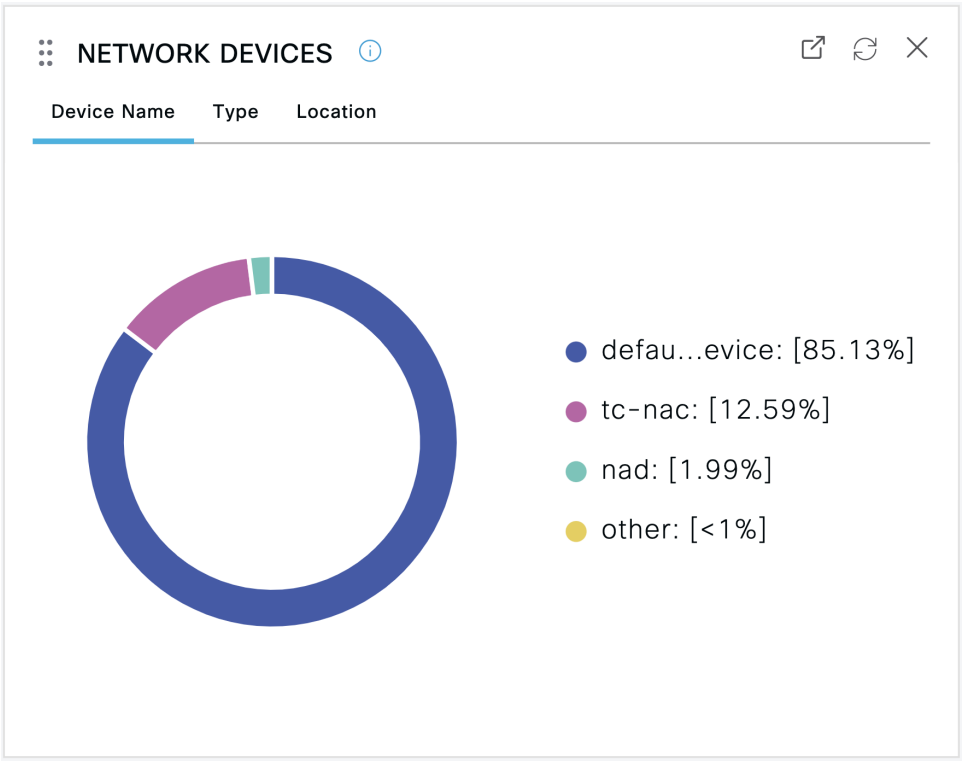
1. 打开新窗口图标表示可在新的浏览器窗口中打开此Dashlet。圆圈用于刷新。**X**用于删除此Dashlet，但仅在主页上可用。使用屏幕右上角的齿轮符号可删除情景可视性 (Context Visibility) 中的Dashlet。
2. 某些 Dashlet 具有不同类别的数据。点击类别以查看该数据集的饼形图。
3. 饼形图显示您已选择的数据。点击其中一个饼形区域将在情景可视性 (Context Visibility) 中打开新选项卡,其中包含基于该饼形区域过滤得到的数据。

在主页控制面板中点击该饼形图的一部分，将打开一个新的浏览器窗口，其中显示由您点击的饼形图部分过滤得到的数据。

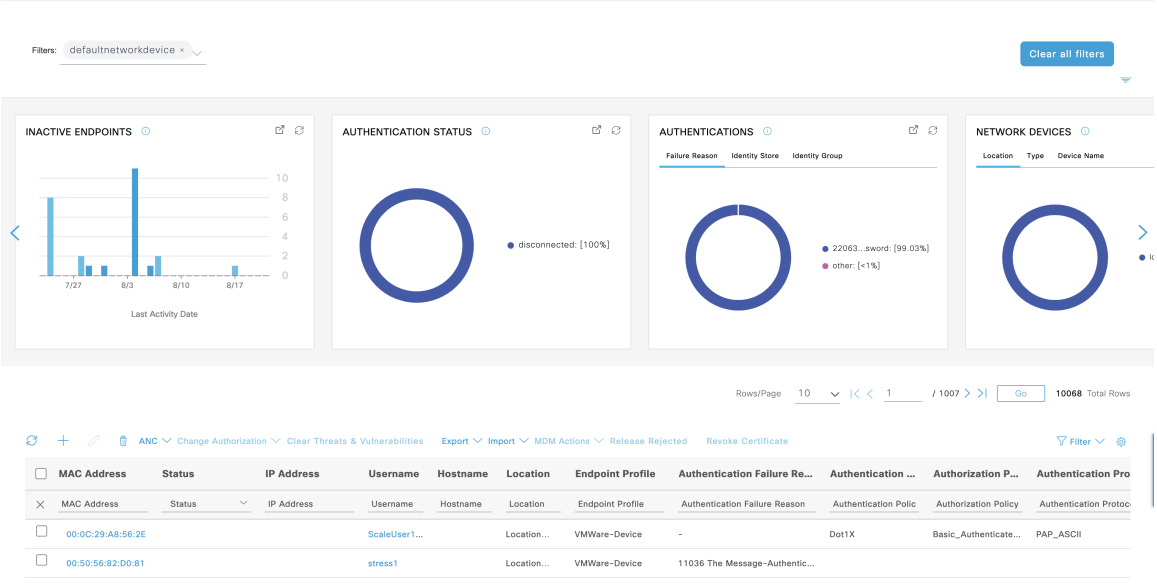
在情景视图 (Context Visibility) 中点击该饼形图的一部分将过滤显示数据，但不会更改情景；已过滤数据显示在同一浏览器窗口中。

在视图中过滤显示的数据

点击情景可视性 (Context Visibility) 页面上的任何 dashlet，可按您点击的项目过滤显示的数据，例如，饼图的一部分。



如果在**网络设备 (Network Devices)** Dashlet 中点击 **defau...evice**，系统会显示包含数据的新窗口，如下图所示：



通过点击饼图的更多部分进一步过滤数据。您还可以使用**过滤器 (Filter)** 下拉列表或数据列表右上角的齿轮图标来管理显示的数据。

您可以保存您的自定义过滤器。

创建自定义过滤器

可以创建和保存自定义过滤器，并修改预设过滤器中的筛选条件。自定义过滤器不保存在Cisco ISE数据库中。只能使用用于创建自定义过滤器的同一计算机和浏览器访问这些过滤器。

步骤 1 点击**显示 (Show)** 下拉列表，然后选择**高级过滤器 (Advanced Filter)**。

步骤 2 从 Filter 菜单中指定搜索属性，如字段、运算符和值。

步骤 3 点击 **+** 可添加更多条件。

步骤 4 点击**开始 (Go)** 可显示与指定属性匹配的条目。

步骤 5 点击**保存 (Save)** 图标可保存过滤器。

步骤 6 输入名称，然后点击**保存 (Save)**。过滤器现在显示在“显示”(Show) 下拉列表中。

使用高级过滤器按条件过滤数据

您可以使用高级过滤器根据指定的条件（例如 First Name = Mike and User Group = Employee）过滤信息。您可以指定不止一个条件。

步骤 1 点击**显示 (Show)** 下拉列表，然后选择**高级过滤器 (Advanced Filter)**。

步骤 2 从“过滤器”(Filter) 菜单指定搜索属性（例如字段、运算符和值）。

步骤 3 点击 **+** 可添加更多条件。

步骤 4 点击**开始 (Go)** 可显示与指定属性匹配的条目。

使用快速过滤器按字段属性过滤数据

通过快速过滤器，您可以输入列表页面中显示的任何字段属性的值，引用页面，并且仅列出与筛选条件相匹配的记录。

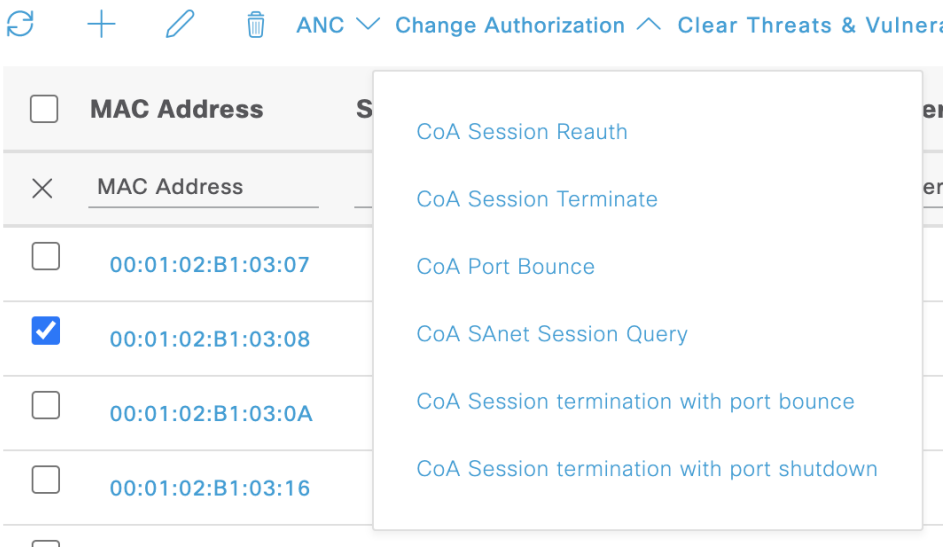
步骤 1 点击**显示 (Show)** 下拉列表并选择**快速过滤器 (Quick Filter)**。

步骤 2 在一个或多个属性字段中输入搜索条件，然后与指定属性相匹配的条目会自动显示。

视图列表中的终端操作

列表顶部的工具栏允许您对所选列表中的终端执行操作。并非每个列表的所有操作都已启用，某些操作取决于启用的功能。以下列表显示了必须在Cisco ISE 中启用后才能使用的两项终端操作。

- 已启用自适应网络控制 (ANC)，您可以选择列表中的终端，并分配或撤销网络访问。您也可以发出授权更改 (CoA)：



ANC（终端保护服务）需要在Cisco ISE 的**自适应网络服务 (Adaptive Network Service)** 窗口中启用。在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **端点保护服务 (Endpoint Protection Service)** > **自适应网络控制 (Adaptive Network Control)**\. 有关详细信息，请参阅在思科 ISE 中启用自适应网络控制。

- 如果已安装 MDM，您可以对选中的终端执行 MDM 操作。

思科 ISE 控制面板

Cisco ISE 控制板或主页（**主页 [Home]** > **摘要 [Summary]**）是您登录Cisco ISE 管理控制台之后显示的登录页面。此控制面板是一个集中管理控制台，由窗口顶部的仪表和下面的 Dashlet 组成。默认控制板为**摘要 (Summary)**、**终端 (Endpoints)**、**客户 (Guests)**、**漏洞 (Vulnerability)** 和**威胁 (Threat)**。有关其他信息，请查阅思科 ISE 主页控制板， 第 6 页部分。

注释 您应该仅在主 PAN 上查看控制板数据。

控制板的实时数据概要显示访问您的网络的设备和用户的状态以及系统的运行状况。

点击二级菜单栏中的齿轮图标，查看控制板设置的下拉列表。下表显示**控制板设置 (Dashboard Settings)** 菜单下可用选项的相关信息：

选项	说明
添加新控制面板 (Add New Dashboard)	您最多可以有 20 个控制板，包括 5 个默认控制板。

选项	说明
重新命名控制面板 (Rename Dashboard)	要重新命名控制面板（仅适用于自定义控制面板），请执行以下操作： **1.** 点击**重命名控制板 (Rename Dashboard)**。 **2.** 指定新名称。 **3.** 点击**应用 (Apply)**。
添加 Dashlet (Add Dashlet)	要将 Dashlet 添加到主页控制板，请执行以下操作： **1.** 点击**添加 Dashlet (Add Dashlet[s])**。 **2.** 在**添加 Dashlet (Add Dashlet[s])** 窗口中，点击要添加的 Dashlet 旁的**添加 (Add)**。 **3.** 点击**保存 (Save)**。 **注释** 您最多可以为每个控制板添加 9 个 Dashlet。

选项	说明
导出 (Export)	您可以将 Dashlet 数据导出为 PDF 或 CSV 文件。 为此： **1.** 从Cisco ISE 主页中选择相应的控制板，例如，“摘要”(Summary)。 **2.** 选择**控制面板设置 (Dashboard Settings)** > **导出 (Export)**。 **3.** 在**导出 (Export)** 对话框中，选择以下文件格式之一： • PDF 格式用于查看选定 Dashlet 的快照。 • CSV 格式用于下载 ZIP 文件形式的选定控制板数据。 **4.** 在 **Dashlet** 部分，选择所需的 Dashlet。 **5.** 点击**导出 (Export)**。 压缩文件中包含所选控制面板的单个面板CSV 文件。与 Dashlet 中的每个选项卡相关的数据在相应的 Dashlet CSV 文件中显示为单独的部分。 导出自定义控制板时，ZIP 文件将使用同一名称导出。例如，如果导出名为“MyDashboard”的自定义控制板，则导出的文件名为 MyDashboard.zip。
布局模板 (Layout Template)	您可以更改显示面板的模板布局。 要更改布局，请执行以下操作： **1.** 选择**控制面板设置 (Dashboard Settings)** > **布局模板 (Layout Template)**。 **2.** 从可用选项中选择所需的布局。

选项	说明
管理控制面板 (Manage Dashboards)	管理控制板 (Manage Dashboards) 菜单下提供以下选项： • “标记为默认控制板”(Mark as Default Dashboard)：使用该选项可将控制板设置为默认控制板（主页）。 • “重置所有控制板”(Reset all Dashboards)：使用该选项可将所有控制板还原为初始设置。

您可以点击相应自定义控制板旁的关闭 (**x**) 图标删除已创建的控制板。

注释 您不能重命名或删除默认控制面板。

所有 Dashlet 的右上角都有一个工具栏，包含以下选项：

- 分离 (Detach)：在单独的窗口中查看 Dashlet。
- 刷新 (Refresh)：刷新 Dashlet。
- 删除 (Remove)：从控制板中删除 Dashlet。

您可以使用 Dashlet 左上角的抓手图标拖放 Dashlet。

警报 Dashlet 中的快速过滤器 (Quick Filter in Alarms Dashlet)：可以根据严重性（如严重 (Critical)、警告 (Warning) 和信息 (Info)）过滤警报。“警报”（Alarms）Dashlet 位于主页上，包含具有“快速过滤器”(Quick Filter) 选项的过滤器下拉列表。

思科 ISE 国际化和本地化

Cisco ISE 国际化调整用户界面以适应受支持的语言。用户界面本地化采用区域特定组件和翻译文本。在 Windows、MAC OSX 和 Android 设备中，本地请求方调配向导可用于以下任何受支持的语言。

在Cisco ISE 中，国际化和本地化支持专注于支持（面向最终用户的门户中的）采用 UTF-8 编码的非英语文本以及管理门户中的选择性字段。

支持的语言

Cisco ISE 为以下语言和浏览器区域设置提供本地化和国际化支持。

表 *3:* 支持的语言和区域设置

语言	浏览器区域设置
中文（繁体）	zh-tw
中文（简体）	zh-cn
捷克语	cs-cz
荷兰语	nl-nl
英语	en
法语	fr-fr
德语	de-de
匈牙利语	hu-hu
意大利语	it-it
日语	ja-jp
韩语	ko-kr
波兰语	pl-pl
葡萄牙语（巴西）	pt-br
俄语	ru-ru
西班牙语	es-es

最终用户 Web 门户本地化

访客门户、发起人门户、我的设备门户和客户端调配门户会本地化为所有受支持的语言和区域设置。这包括文本、标签、消息、字段名称和按钮标签。如果客户端浏览器请求的区域设置未映射到Cisco ISE 中的模板，则门户会使用英语模板显示内容。

通过使用管理门户，您可以针对每种语言修改用于访客门户、发起人门户和我的设备门户的字段。您还可以添加其他语言。当前，您无法自定义客户端调配门户的这些字段。

您可以通过将 HTML 页面上传到Cisco ISE，进一步自定义访客门户。上传自定义页面时，您负责为部署提供相应的本地化支持。Cisco ISE 通过可以用作指南的样本 HTML 页面提供本地化支持示例。Cisco ISE 可以让您上传、存储和呈现自定义国际化 HTML 页面。

注释 NAC 和 MAC 代理安装程序及 WebAgent 页面未本地化。

支持 UTF-8 字符数据条目

向最终用户公开的Cisco ISE字段（通过Cisco客户端代理或请求方，或者发起人门户、访客门户、我的设备门户和客户端调配门户）支持所有语言的 UTF-8 字符集。UTF-8 是 Unicode 字符集的多字节字符编码，其中包括许多不同语言字符集，例如希伯来语、梵语和阿拉伯语。

字符集以 UTF-8 形式存储在管理配置数据库中，并且 UTF-8 字符集正确显示在报告和用户界面组件中。

UTF-8 凭证身份验证

网络访问身份验证支持 UTF-8 用户名和密码凭证。这包括来自访客和管理门户登录身份验证的 RADIUS、EAP、RADIUS 代理、RADIUS 令牌和 Web 身份验证。对用户名和密码的 UTF-8 支持适用于对照本地身份库及外部身份库进行的身份验证。

UTF-8 身份验证取决于用于网络登录的客户端请求方。某些 Windows 本地请求方不支持 UTF-8 凭证。

注释 RSA 不支持 UTF-8 用户，因此，使用 RSA 的 UTF-8 身份验证不受支持。兼容Cisco ISE 的 RSA 服务器也不支持 UTF-8。

UTF-8 策略和安全评估

Cisco ISE 中以属性值为条件的策略规则可以包含 UTF-8 文本。规则评估支持使用 UTF-8 属性值。此外，也可以通过管理门户使用 UTF-8 值配置条件。

终端安全评估要求根据 UTF-8 字符集修改为文件、应用和服务条件。

对发送至请求方的消息的 UTF-8 支持

RSA 提示符和消息使用 RADIUS 属性 REPLY-MESSAGE 转发到请求方，或者在 EAP 数据中。如果文本包含 UTF-8 数据，请求方将根据客户端的本地操作系统语言支持显示文本。某些 Windows 本地请求方不支持 UTF-8 凭证。

Cisco ISE 提示和消息可能与请求方运行所在的客户端操作系统的区域设置不同步。您必须调整最终用户请求方区域设置与Cisco ISE 支持的语言，使它们保持一致。

报告和警报 UTF-8 支持

对于Cisco ISE 中支持的语言，监控和故障排除报告和警报支持相关属性使用 UTF-8 值：支持以下活动：

- 查看实时身份验证。
- 查看详细的报告记录页面。
- 导出和保存报告。
- 查看Cisco ISE 控制板。

- 查看警报信息。
- 查看 tcpdump 数据。

门户中的 UTF-8 字符支持

Cisco ISE 字段中支持的字符集 (UTF-8) 比门户和最终用户消息中的本地化支持的字符集多得多。例如，尽管支持字符集本身，但是Cisco ISE不支持从右到左书写的语言（例如希伯来语或阿拉伯语）。

下表列出管理员和最终用户门户中支持 UTF-8 字符的字段，这些字符用于数据输入和查看，带有以下限制：

- Cisco ISE 不支持包含 UTF-8 字符的访客用户名和密码。
- Cisco ISE 不支持证书中的 UTF-8 字符。

表 *4:* 管理员门户 *UTF-8* 字符字段

管理员门户要素	UTF-8 字段
Network access user configuration	• User name 用户名可以由任意组合的大写和小写字母、数字、空格和特殊字符组成（`、%、^、;、:、[、{、|、}、]、\、‘、“、=、<、>、?、!和控制字符除外）。也不允许使用只包含空格的用户名。 • 名字 • Last name • e-mail
User list	• 所有过滤器字段 • User List 页面上显示的值 • 左侧导航快速视图上显示的值

管理员门户要素	UTF-8 字段
User password policy	密码可以由任意组合的大写和小写字母、数字和特殊字符组成（包括：“!”、“@”、“#”、“$”、“^”、“&”、“*”、“(”和“)”。密码字段接受任何字符，包括UTF-8字符，但不接受控制字符。 某些语言不支持大写或小写字母。如果用户密码策略要求用户输入含大写或小写字符的密码，并且如果用户的语言不支持这些字符，则用户无法设置密码。若要使用户密码字段支持 UTF-8 字符，在用户密码策略页面（**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **用户密码策略 (User Password Policy)**）中，必须取消选中以下选项： • 小写字母字符 • 大写字母字符 不能使用字典字词，其反序字符或用其他字符替换的字母。
Administrator list	• 所有过滤器字段 • Administrator List 页面上显示的值 • 左侧导航快速视图上显示的值
Admin login page	• User name
RSA	• 消息 • 提示符
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• 名称 (Name) • Remediation action > Message shown to Agent User • 要求列表显示

管理员门户要素	UTF-8 字段
Posture conditions	• File condition > File path • Application condition > Process name • Service condition > Service name • 条件列表显示
Guest and My Devices settings	• Sponsor > Language Template：所有支持的语言，所有字段 • Guest > Language Template：所有支持的语言，所有字段 • My Devices >Language Template：所有支持的语言，所有字段
System settings	• SMTP Server > Default e-mail address
Operations > Alarms > Rule	• Criteria > User • Notification > e-mail Notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions

管理员门户要素	UTF-8 字段
Attribute value in policy library conditions	• Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

用户界面外的 UTF-8 支持

本节包含在Cisco ISE 用户界面之外提供 UTF-8 支持的区域。

调试日志和 CLI 相关的 UTF-8 支持

某些调试日志中会显示属性值和安全评估条件详细信息，因此所有调试日志都应接受 UTF-8 值。您可以下载包含原始 UTF-8 数据的调试日志，使用支持 UTF-8 的查看器便能够查看这些数据。

ACS 迁移 UTF-8 支持

Cisco ISE 允许迁移 ACS UTF-8 配置对象和值。Cisco ISE UTF-8 语言可能不支持某些 UTF-8 对象的迁移，它可能会使用管理门户或报告方法，使迁移过程中提供的某些 UTF-8 数据变得无法读取。您必须将无法读取的 UTF-8 值（从 ACS 迁移）转换为 ASCII 文本。有关从 ACS 迁移到 ISE 的详细信息，请参阅适用于您的 ISE 版本的思科安全 ACS 到思科 ISE 迁移工具。

支持导入和导出 UTF-8 值

Admin 门户和发起人门户都支持纯文本与 .csv 文件，并且支持在导入用户帐户详细信息时使用 UTF-8 值。所提供的导出文件为 csv 文件。

REST 上的 UTF-8 支持

外部 REST 通信支持 UTF-8 值。这适用于Cisco ISE 用户界面上支持 UTF-8 的可配置项，管理员身份验证除外。REST 上的管理员身份验证要求使用 ASCII 文本凭证进行登录。

身份库授权数据的 UTF-8 支持

Cisco ISE 允许 Active Directory 和 LDAP 在授权策略中使用 UTF-8 数据进行策略处理。

MAC 地址标准化

ISE 支持对以下列任意格式输入的 MAC 地址进行标准化：

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

对于以下 ISE 窗口，可以提供完整 MAC 地址或部分 MAC 地址：

- Policy > Policy Sets
- Policy > Policy Elements > Conditions > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global Search
- Operations > Reports > Reports Filters
- Operations > Diagnostic Tools > General Tools > Endpoint Debug

对于以下 ISE 窗口，应提供完整的 MAC 地址（六个八位字节，用“:”或“-”或“.”分隔）：

- Operations) > Endpoint Protection Services Adaptive Network Control
- Operations > Troubleshooting > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting
- Operations > Troubleshooting > Diagnostic Tools > General Tools > Posture Troubleshooting
- Administration > Identities > Endpoints
- Administration) > System > Deployment
- Administration > Logging > Collection Filter

REST API 也支持完整 MAC 地址的标准化。

有效的八位字节仅包含 0-9、a-f 或 A-F。

思科 ISE 部署升级

通过Cisco ISE，可以从管理门户执行基于 GUI 的集中式升级。升级过程是相当简单的，升级进度和节点状态显示在屏幕上。有关升级前和升级后任务的列表，请参阅《思科身份服务引擎升级指南》。

“升级概述”(Upgrade Overview) 页面列出了部署中的所有节点、这些节点上启用的角色、所安装 ISE 的版本以及节点的状态（指示节点是处于活动状态还是非活动状态）。只有在节点处于活动状态时，才能开始升级。

管理员访问控制台

以下步骤说明了如何登录管理门户。

步骤 1 在浏览器地址栏中输入Cisco ISE URL（例如 https://<ise hostname or ip address>/admin/）。

步骤 2 输入在Cisco ISE 初始设置过程中指定和配置的用户名及区分大小写的密码。

步骤 3 点击**登录 (Login)** 或按 **Enter**。

如果您登录不成功，请在“登录”(Login) 页面点击**登录遇到问题？(Problem logging in?)** 链接并按照说明操作。

管理员登录浏览器支持

Cisco ISE 管理门户支持以下支持 HTTPS 的浏览器：

- Mozilla Firefox 79 及更低版本
- Mozilla Firefox ESR 60.9 及更低版本
- Google Chrome 84 及更低版本

ISE 社区资源

使用 Adblock Plus 时，ISE 页面无法完全加载

登录尝试失败后锁定管理员

如果在输入管理员用户 ID 的密码时错误次数足够多，则该帐户将在指定时间内暂停使用或被锁定（根据配置而定）。如果您选择锁定，则管理员门户会将您“封锁”在系统之外。Cisco ISE 在“服务器管理员登录”(Server Administrator Logins) 报告中添加一条日志，并吊销该管理员 ID 的凭证。您可以重置该管理员 ID 的密码，如《思科身份服务引擎安装指南》中的“重置因管理员锁定而禁用的密码”一节所述。禁用管理员帐户之前允许的失败尝试次数是可配置的，具体见《思科身份服务引擎管理员指南》中的 对思科 ISE 的管理访问一节。管理员用户帐户被锁定后，Cisco ISE 会向关联的管理员用户（如已配置）发送电子邮件。

任意超级管理员（包括 Active Directory 用户）均可启用被禁用的系统管理员状态。

在思科 ISE 中指定代理设置

如果现有网络拓扑要求您对Cisco ISE 使用代理来访问外部资源（例如可在其中查找客户端调配和安全评估相关资源的远程下载站点），则您可以使用管理门户指定代理属性。

代理设置会影响以下Cisco ISE 功能：

- 合作伙伴移动管理
- 终端分析器源服务更新
- 终端安全评估更新
- 终端安全评估代理资源下载
- CRL（证书吊销列表）下载
- 访客通知
- SMS 消息传输
- 社交媒体登录

Cisco ISE 代理配置支持代理服务器的基本身份验证。不支持 NT LAN Manager (NTLM) 身份验证。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **代理 (Proxy)**。

步骤 2 输入代理 IP 地址或 DNS 可解析主机名，并在**代理主机服务器：端口 (Proxy host server : port)** 中指定代理流量与 Cisco ISE 之间来回传播所通过的端口。

步骤 3 如果需要，请选中**必填密码 (Password required)** 复选框。

步骤 4 在**用户名 (User Name)** 和 **密码 (Password)** 字段中输入用于向代理服务器进行身份验证的用户名和密码。

步骤 5 在**用于这些主机和域的旁路代理 (Bypass proxy for these hosts and domain)** 中输入要绕行的主机或域的 IP 地址或地址范围。

步骤 6 点击**保存 (Save)**。

管理员门户使用的端口

管理员门户设置为使用 HTTP 80 端口和 HTTPS 443 端口，并且您无法更改这些设置。Cisco ISE 同时防止您分配任何最终用户门户使用相同的端口，这降低了管理员门户的风险。

启用外部 RESTful 服务 API

外部宁静的服务API根据HTTPS协议和其他方式和使用端口9060。

外部宁静的服务API支持基本身份验证。身份验证凭证加密并是请求报头的一部分。

您可以使用 REST 客户端（如 JAVA）、curl linux 命令、python 或任何其他客户端来调用外部 RESTful 服务 API 调用。

ESS管理员分配种类到用户执行操作使用外部宁静的服务API。在Cisco ISE 2.6 及更高版本中，ERS 用户可以是内部用户，也可以属于外部 AD。外部用户所属的 AD 组必须映射到 ERS 管理员组或 ERS 操作员组：

- 外部 RESTful 服务管理员 - 对所有 ERS API（GET、POST、DELETE、PUT）的完整访问权限。此用户可以创建、读取、更新和删除 ERS API 请求。
- 外部 RESTful 服务操作人员 - 只读权限（只能使用 GET 请求）。

注释 超级管理员用户可以访问所有 ERS API。

ERS 会话空闲超时为 60 秒。因此，如果在此期间发送了多个请求，则使用相同的会话，意味着相同的 CSRF。在空闲 60 秒后，它会重置并使用新的 CSRF。

默认情况下外部RESTful API服务未启用。如果您尝试调用API在启用之前呼叫的外部宁静的服务，您将收到错误响应。您必须启用Cisco ISE REST API对于Cisco ISE开发的应用REST API可以访问Cisco ISE。Cisco REST API使用HTTPS端口9060，默认情况下会关闭。Cisco ISE REST API在Cisco ISE管理员服务器上未启用，客户端应用程序从所有访客REST API请求的服务器将收到超时错误。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **ERS 设置 (ERS Settings)**。

步骤 2 对主管理节点选择**启用 ERS 进行读/写 (Enable ERS for Read/Write)**。

步骤 3 如果有任何辅助节点，请选择**为所有其他节点启用 ERS 进行读取 (Enable ERS for Read for All Other Nodes)**。

所有类型外部宁静的服务请求的主要ESS节点有效。辅助节点可以访问（GET请求）。

步骤 4 选择以下选项之一：

- 使用 CSRF 检查以增强安全性 (Use CSRF Check for Enhanced Security) - 如果启用此选项，ERS 客户端必须发送 GET 请求以从Cisco ISE 获取跨站请求伪造 (CSRF) 令牌，并将 CSRF 令牌包含在发送到Cisco ISE 的请求中。当收到来自 ERS 客户端的请求时，Cisco ISE 将验证 CSRF 令牌。Cisco ISE 仅在令牌有效时处理请求。此选项不适用于 ISE 2.3 之前的客户端。
- 对 ERS 请求禁用 CSRF (Disable CSRF for ERS Request) - 如果启用此选项，则不会执行 CSRF 验证。此选项可用于 ISE 2.3 之前的客户端。

步骤 5 点击**保存 (Save)**。

所有其它操作进行审核，并记录登录系统日志。外部宁静的服务API具有调试记录class，您可以从Cisco ISE GUI的调试日志记录的页面启用。

当您在Cisco ISE 中禁用外部 RESTful 服务时，端口 9060 保持开放，但不允许通过该端口进行通信。

相关主题

外部宁静的服务SDK，第 33 页

为 ERS API 启用外部 AD 访问

通过以下步骤，您可以为 ERS API 启用外部 AD 访问：

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 添加外部用户所属的 AD 组作为外部身份源。

请参阅将 Active Directory 用作外部身份源

步骤 3 从 AD 添加用户组。

请参阅添加用户

步骤 4 选择 **管理 (Administration)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)** > **身份验证方式 (Authentication Method)**。

步骤 5 从**身份源 (Identity Source)** 下拉列表选择 **AD：<加入点名称> (AD: <Join Point Name>)**。

步骤 6 选择**基于密码 (Password Based)** 或**基于客户端证书 (Client Certificate Based)** 的身份验证。

步骤 7 选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**。

步骤 8 将外部组作为成员用户添加到 ERS 管理员组或 ERS 操作员组。请转至 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)** > **ERS 管理员 (ERS Admin)ERS 操作员 (ERS Operators)**。

步骤 9 点击**添加 (Add)**。

步骤 10 选择该用户。

步骤 11 点击**保存 (Save)**。

ESS管理员分配种类到用户执行操作使用外部宁静的服务API。在Cisco ISE 2.6 及更高版本中，ERS 用户可以是内部用户，也可以属于外部 AD。外部用户所属的 AD 组必须映射到 ERS 管理员组或 ERS 操作员组：

- 外部 RESTful 服务管理员 - 对所有 ERS API（GET、POST、DELETE、PUT）的完整访问权限。此用户可以创建、读取、更新和删除 ERS API 请求。
- 外部 RESTful 服务操作人员 - 只读权限（只能使用 GET 请求）。

注释 超级管理员用户可以访问所有 ERS API。

外部宁静的服务SDK

您可以使用外部宁静的服务SDK开始迁移工具支持工具。您可以从以下URL访问外部宁静的服务SDK：https:// <ISE - ADMIN - NODE> ：9060/ers/sdk、外部宁静的服务SDK可以只通过外部宁静的服务管理员用户访问。

SDK包括以下组件

- 快速参考API文档
- 所有可用 API 操作的完整列表
- 架构文件可下载
- 在Java的示例应用程序可以下载
- curl 脚本格式的使用案例
- Python 脚本格式的使用案例
- 使用 Chrome Postman 的说明

指定系统时间和 NTP 服务器设置

Cisco ISE 允许最多配置三个网络时间协议 (NTP) 服务器。您可以使用 NTP 服务器维护正确时间和同步不同时区的时间。您还可以指定Cisco ISE 是否应仅使用经过身份验证的NTP 服务器，您可以为此目的输入一个或更多身份验证密钥。

Cisco建议将所有Cisco ISE 节点均设置为协调世界时 (UTC) 时区，特别是在您的思科 ISE 节点都安装于分布式部署中的情况下。此程序可确保无论时间戳如何，来自您的部署中各个节点的报告和日志始终同步。

对于 NTP 服务器，Cisco ISE 也支持公钥身份验证。NTPv4 使用对称密钥加密，但是也可根据公钥加密提供新的自动密钥方案。公钥加密通常被认为比对称密钥加密更安全，因为其安全性基于各个服务器生成的不会泄露的专用值。如果使用自动密钥，所有密钥分发和管理功能都将仅涉及公共值，可在很大程度上简化密钥分发和存储。

您可以在配置模式下从Cisco ISE CLI 将 NTP 服务器配置为使用自动密钥。我们建议您使用 IFF（敌我识别）识别方案，因为这种方案的使用最为广泛。

开始之前

您必须分配到了超级管理员角色或系统管理员角色。

如果您有一个主要和辅助Cisco ISE 节点，您必须登录辅助节点的用户界面并在您的部署中每个Cisco ISE 节点上逐一配置系统时间和 NTP 服务器。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **系统时间 (System Time)**。

步骤 2 输入您的 NTP 服务器的唯一 IP 地址 (IPv4/IPv6/FQDN)。

步骤 3 如果您想要限制Cisco ISE 仅使用经过身份验证的NTP 服务器保留系统和网络时间，请选中 **Only allow authenticated NTP servers** 复选框。

步骤 4 （可选）如果要使用私钥对 NTP 服务器进行身份验证，并且您指定的服务器中有任意服务器要求通过身份验证密钥进行身份验证，请点击 **NTP Authentication Keys**（NTP 身份验证密钥）选项卡并指定一个或更多身份验证密钥，如下所示：

a) 点击**添加 (Add)**。

b) 输入必要的**密钥 ID** 和**密钥值**。从下拉列表中选择 **HMAC**。Key ID 字段支持 1 至 65535 之间的数值，Key Value 字段支持最多 15 个字母数字字符。

c) 输入 NTP 服务器身份验证密钥后，请返回 NTP Server Configuration 选项卡。

步骤 5 （可选）如果要使用公共密钥身份验证对 NTP 服务器进行身份验证，请从命令行界面 (CLI) 配置 Cisco ISE 上的自动密钥。有关详细信息，请参阅对应于您的 ISE 版本的《思科身份识别服务引擎 CLI 参考指南》中的 **ntp server** 和 **crypto** 命令。

步骤 6 点击**保存 (Save)**。

更改系统时区

设置后，您便无法从管理门户编辑时区。要更改时区设置，必须在Cisco ISE CLI 中输入以下命令：

clock timezone *timezone*

有关 **clock timezone** 命令的详细信息，请参阅《思科身份服务引擎 CLI 参考指南》。

注释 Cisco ISE 在时区名称和输出缩写中使用 POSIX 式符号。因此，格林威治西部时区中有一个正号，东部时区中有一个负号。例如 TZ='Etc/GMT+4' 对应于标准时间 (UT) 后 4 小时。

注意 安装后，在Cisco ISE 设备上更改时区需要在该特定节点上重新启动 ISE 服务。因此，我们建议您在维护窗口内执行此类更改。此外，务必将单个 ISE 部署中的所有节点都配置为同一时区。如果 ISE 节点位于不同地理位置或时区中，则应在所有 ISE 节点上使用全球时区，例如 UTC。

配置 SMTP 服务器以支持通知

要更新 SMTP 服务器详细信息，请转至**管理 (Administration) > 系统 (System) > 设置 (Settings) > 代理 (Proxy) > SMTP 服务器 (SMTP server)**。配置简单邮件传输协议 (SMTP) 服务器，以执行以下操作：发送警报的电子邮件通知，使发起人向访客发送包含登录凭证和密码重置说明的电子邮件通知，使访客在自行成功注册后自动接收登录凭证以及访客帐户到期前要采取的操作。

警报通知的收件人可以是已启用**在电子邮件中包括系统警报 (Include system alarms in emails)** 选项的任何内部管理员用户。发送警报通知的发件人的邮件地址硬编码为 ise@<hostname>。

下表显示了分布式 ISE 环境中哪些节点会发送电子邮件。

电子邮件用途	发送电子邮件的节点
访客过期	主 PAN
alarms	活动 MnT
来自访客和发起人门户的发起人和访客通知	PSN
密码过期	主 PAN

以下字段用于配置 SMTP 服务器。

- **SMTP 服务器设置**
  - **SMTP 服务器 (SMTP Server)**：输入出站 SMTP 服务器的主机名。
  - **SMTP 端口 (SMTP Port)**：输入 SMTP 端口号。此端口必须打开才能连接到 SMTP 服务器。
  - **连接超时 (Connection Timeout)**：输入Cisco ISE 在开始新连接之前等待连接到 SMTP 服务器的最长时间。
- **加密设置 (Encryption Settings)**：选中“使用 TLS/SSL 加密”(Use TLS/SSL encryption) 以与安全 SMTP 服务器通信。如果使用 SSL，请将 SMTP 服务器的根证书添加到Cisco ISE 受信任证书。
- **身份验证设置 (Authentication Settings)**：授权可以是用户名和密码，也可以是 SSL。SSL 是默认设置。选中“使用密码身份验证”(Use Password Authentication) 以改为使用用户名和密码。

交互式帮助

交互式帮助为用户提供提示和分步指导，帮助用户轻松完成任务，从而有效地使用Cisco ISE。

默认情况下启用此功能。要启用或禁用此功能，请选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **交互式帮助 (Interactive Help)**，然后选中或取消选中**启用交互式帮助 (Enable Interactive Help)** 复选框。

启用安全解锁客户端机制

安全解锁客户端机制可在特定时间段内在Cisco ISE 命令行界面 (CLI) 上提供根外壳访问。一旦会话关闭或退出，根访问也会被撤销。

已使用同意令牌工具实施安全解锁客户端功能。同意令牌是一种统一的多因素身份验证方案，用于以可信的方式安全地授予对Cisco产品的特权访问权限，并且仅在客户和Cisco双方同意之后授予。

要在Cisco ISE CLI 上启用根外壳，请执行以下步骤：

步骤 1 在Cisco ISE CLI 中，输入 **permit rootaccess**：

```
ise/admin# permit rootaccess 1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出    输入 CLI 选项：
```

步骤 2 通过选择选项1生成同意令牌挑战：

```
1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出输入 CLI 选项：1 正在生成质
询..................................... 质询字符串（请仅复制星号行之间的所有内容）：
********************************************************************************
GLOX/gAAAQEBAAQAAAABAgAEAAAAAAMACImJxgubOhitBAAQiUwv+XeD3pnJ4HLnJy30MQUAEAAADhAGAANUUUHAAZUUVfQlQIAANUUUUACcJIDU2NGQ5NjgwMTEmZmEtOWI0ZS0wZjYtMTdlZDllMGQlM2UzNQ==
 ********************************************************************************* 启动 15 分钟后
台计时器 1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出     输入 CLI 选项：
```

步骤 3 将同意令牌质询发送至Cisco技术支持中心 (TAC)：

Cisco TAC 将使用您提供的同意令牌质询生成同意令牌响应。

步骤 4 选择选项 **2**，然后输入Cisco TAC 提供的同意令牌响应：

```
输入 CLI 选项：2 请准备就绪后输入响应.....................
[redacted]
 响应签名验证成功！授予外壳访问权限    sh-4.2# 是
```

注释 如果响应签名验证成功，则启用特权访问。

下一步做什么

要退出外壳模式，请运行 **exit** 命令：

```
sh-4.2# exit exit Root shell exited
```

您可以通过选择选项 **3** 查看根访问会话的历史记录：

```
1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出输入 CLI 选项：3
********************************** SN No : 1 ********************************** Challenge

3/WcjAAAQEBAAQAAAABAgAEAAAAAAMAM89hCTWWBAQwc9lyianffO4C5il+v8OQUAEAAADhAGAANUUUHAAZUUVfQlQIAANUUUUACcJIDU2NGQ5NjgwMTEmZmEtOWI0ZS0wZjYtMTdlZDllMGQlM2UzNQ==
```

```
 generated at 2019-06-12 15:40:01.000 ********************************** SN No : 2
**********************************
```

设置思科 ISE API 网关

Cisco ISE API 网关是一种 API 管理解决方案，它是通往多个Cisco ISE 服务 API 的单一入口点，改善了安全和流量管理。来自外部客户端的 API 请求将路由到Cisco ISE 上的 API 网关。这些请求会根据内部算法进一步转发到运行服务 API 的Cisco ISE 节点。

在Cisco ISE 版本 3.0 中，只有 MNT（监控）API 通过 API 网关路由。您可以选择要在其中启用 API 网关的Cisco ISE 节点。我们建议您在Cisco ISE 部署中的至少两个节点上运行 API 网关。

步骤 1 登录主策略管理节点。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **API 网关设置 (API Gateway Settings)**

步骤 3 在 **ISE API 网关节点列表 (ISE API Gateway Nodes List)** 区域中，选中要启用 API 网关的节点旁边的复选框。

步骤 4 点击**启用 (Enable)**。

故障排除

要排除与 API 网关相关的问题，请在**调试日志配置 (Debug Log Configuration)** 窗口中将以下组件的**日志级别 (Log Level)** 设置为**调试 (DEBUG)**。（要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**.）

- ise-kong
- kong

可从**下载日志 (Dowload Logs)** 窗口下载日志。（要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)**.) 您可以选择从**支持捆绑包 (Support Bundle)** 选项卡下载支持捆绑包，也可以从**调试日志 (Debug Logs)** 选项卡下载 kong 调试日志。

验证

如果您每次都能成功登录Cisco ISE 主策略管理节点 (PPAN)，则 API 网关设置将按预期工作。

FIPS 模式支持

ISE FIPS 140 模式将Cisco FIPS 对象模块加密模块初始化为 FIPS 140-2 模式。Cisco身份识别服务引擎使用嵌入式 FIPS 140-2 验证加密模块。有关FIPS 合规要求的详细信息，请参阅 FIPS 合规证明书。

启用 FIPS 模式时，Cisco ISE 管理员界面会在该页面右上角的节点名称左侧显示一个 FIPS 模式图标。

如果Cisco ISE 检测到使用了 FIPS 140-2 标准不支持的协议或证书，它会显示一条警告，其中包含不合规的协议或证书的名称，并且不会启用 FIPS 模式。确保只选择符合 FIPS 的协议并替换不符合 FIPS 的证书，然后再启用 FIPS 模式。

如果 FIPS 不支持证书中使用的加密方法，则必须重新颁发安装在Cisco ISE 中的证书。

打开 FIPS 模式时，以下功能会受影响：

- 基于安全套接字层 (SSL) 的轻量级目录访问协议 (LDAP)
- Cisco ISE 通过 RADIUS 共享密钥和密钥管理措施实现 FIPS 140-2 合规性。当启用 FIPS 模式时，使用不符合 FIPS 的算法的任何功能都将失败。

启用 FIPS 模式时：

- 对于 EAP-TLS、PEAP 和 EAP-FAST，将禁用所有不符合 FIPS 的密码套件
- 将在 SSH 中禁用所有不符合 FIPS 的密码套件
- 证书和私钥只能使用符合 FIPS 的散列和加密算法
- RSA 私钥必须为 2048 位或更高
- ECDSA 私钥必须为 224 位或更高
- ECDSA 服务器证书仅适用于 TLS 1.2
- 对于所有 ISE TLS 客户端，DHE 密码适用于 2048 位或更高的 DH 参数
- 不允许将 3DES 密码用于 ISE 服务器
- 不允许使用 SHA1 生成证书
- 不允许在客户端证书中使用 SHA1
- EAP-FAST 中的匿名 PAC 调配选项已禁用
- 本地 SSH 服务器将在 FIPS 模式下运行
- RADIUS 不支持以下协议：
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

启用 FIPS 模式后，部署中的所有节点将自动重新启动。Cisco ISE 通过先重新启动主 PAN、然后重新启动每个辅助节点（一次一个）来执行滚动重启。因此，建议您在更改配置之前计划停机时间。

提示 建议您在完成任何数据库迁移过程之前不要启用 FIPS 模式。

在思科 ISE 中启用 FIPS 模式

要启用 FIPS 模式，请执行以下操作：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **FIPS 模式 (FIPS Mode)**。

步骤 2 从 **FIPS 模式 (FIPS Mode)** 下拉列表中选择**已启用 (Enabled)** 选项。

步骤 3 点击**保存 (Save)**，然后重新启动计算器。

下一步做什么

启用 FIPS 模式之后，请启用并配置以下符合 FIPS 140-2 的功能：

- 生成自签证书，第 60 页
- 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 78 页
- 请参阅《》中的“网络设备定义设置”部分
- 在网络设备定义设置下配置 RADIUS 身份验证设置。

此外，可能要使用通用访问卡 (CAC) 功能启用管理员帐户授权。尽管严格而言，将 CAC 功能用于授权并不是一项 FIPS 140-2 要求，但它是一项众所周知的安全访问措施，用于在多种环境中提高 FIPS 140-2 合规性。

配置思科 ISE 以进行管理员 CAC 身份验证

开始之前

在开始配置前，请执行以下操作：

- 确保Cisco ISE 中的域名服务器 (DNS) 已针对 Active Directory 进行设置。
- 确保 Active Directory 用户和用户组成员已针对各管理员证书进行定义。

要确保Cisco ISE 可根据从浏览器提交的基于 CAC 的客户端证书对管理员进行身份验证和授权，请确保您已配置以下项目：

- 外部身份源（在下面的示例中为 Active Directory）
- 管理员所属的 Active Directory 中的用户组
- 如何在证书中查找用户身份
- Active Directory 用户组到Cisco ISE RBAC 权限映射

- 签发客户端证书的证书颁发机构（信任）证书
- 确定客户端证书是否已被 CA 吊销的方法

在登录Cisco ISE 时，您可以使用通用访问卡 (CAC) 对凭证进行身份验证。

步骤 1 在Cisco ISE 中配置 Active Directory 身份源并将所有Cisco ISE 节点加入 Active Directory。

步骤 2 根据指南配置证书身份验证配置文件。

请确保选择证书中包含 Principal Name X.509 Attribute 字段中的管理员用户名的属性。（对于 CAC 卡，卡上的签名证书通常用于查找 Active Directory 中的用户。Principal Name 可在此证书的“Subject Alternative Name”扩展中找到，确切的说是在名为“Other Name”的扩展的字段中。因此此处的属性选择应为“Subject Alternative Name - Other Name。”）

如果用户的 AD 记录包含用户的证书，并且您希望将从浏览器接收的证书与 AD 中的证书相比较，请选中 Binary Certificate Comparison 复选框，并选择之前指定的 Active Directory 实例名称。

步骤 3 启用 Active Directory 以进行基于密码的管理员身份验证。选择您之前连接并加入Cisco ISE 的 Active Directory 实例名称。

注释 在完成其他配置前，您必须使用基于密码的身份验证。接着，在此过程的最后一步，您可以将身份验证类型更改为基于客户端证书。

步骤 4 创建外部管理员组并将其映射到 Active Directory 组。选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**。创建外部系统管理员组。

步骤 5 配置管理员授权策略，将 RBAC 权限分配给外部管理员组。

注意 我们强烈建议您创建外部超级管理员组，将其映射到 Active Directory 组，并使用超级管理员权限（菜单访问和数据访问）配置管理员授权策略，并在该 Active Directory 组中至少创建一名用户。此映射确保基于客户端证书的身份验证启用后，至少一名外部管理员拥有超级管理员权限。此操作失败可能导致Cisco ISE 管理员被锁定，以致无法使用管理员门户中的关键功能。

步骤 6 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书存储区 (Certificate Store)**，将证书颁发机构证书导入Cisco ISE 证书信任存储区。

除非客户端证书信任链中的 CA 证书位于Cisco ISE 证书库中，否则Cisco ISE 不接受客户端证书。您必须将相应的 CA 证书导入到Cisco ISE 证书库中。

a) 点击**浏览 (Browse)** 以选择证书。
b) 选中“客户端身份验证的信任”(Trust for client authentication) 复选框。
c) 点击**提交 (Submit)**。

Cisco ISE 会提示您在导入证书后重启部署中的所有节点。您可以在导入所有证书后再重启。但是，在导入所有证书后，您必须重启Cisco ISE 才能继续。

步骤 7 配置证书颁发机构证书以验证吊销状态。

a) 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **OSCP 服务 (OSCP Services)**。
b) 输入 OSCP 服务器的名称、说明（可选）和服务器的 URL。

c) 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书存储区 (Certificate Store)**。
d) 对于对客户端证书签名的 CA 证书，指定如何执行该 CA 的吊销状态检查。从列表中选择一个 CA 证书并点击“编辑”(Edit)。在编辑页面中，选择 OCSP 和/或 CRL 验证。如果选择 OCSP，请选择用于该 CA 的 OCSP 服务。如果选择 CRL，请指定 CRL 分发 URL 和其他配置参数。

步骤 8 启用基于客户端证书的身份验证。选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

a) 在 Authentication Method 选项卡中选择基于客户端证书的身份验证类型。
b) 选择您之前配置的证书身份验证配置文件。
c) 选择 Active Directory 实例名称。
d) 点击**保存 (Save)**。

此时，您可以从基于密码的身份验证切换到基于客户端证书的身份验证。您之前配置的客户端身份验证配置文件决定了管理员证书的身份验证方式。使用外部身份源对管理员进行授权，此示例中的外部身份源为 Active Directory。

证书身份验证配置文件的 Principal Name 属性用于查找 Active Directory 中的管理员。

您现在已经完成了用于进行管理员 CAC 身份验证的Cisco ISE 配置。

支持的通用访问卡标准

Cisco ISE 支持使用通用访问卡 (CAC) 身份验证设备对自身进行身份验证的美国政府用户。CAC 是一种带电子芯片的身份识别卡，电子芯片包含一组标识特定员工身份的 X.509 客户端证书。通过 CAC 访问需要一个读卡器，您可将卡插入其中并输入 PIN。之后，卡中的证书会传输到 Windows 证书库，它们可供运行Cisco ISE 的本地浏览器等应用使用。

思科 ISE 中的通用访问卡操作

可以配置管理员门户，以便仅允许使用客户端证书向Cisco ISE 进行身份验证。不允许执行基于凭证的身份验证，例如提供用户 ID 和密码。在客户端证书身份验证中，您要插入通用访问卡 (CAC)，输入 PIN，然后在浏览器地址栏输入Cisco ISE Admin 门户 URL。浏览器将证书转发至Cisco ISE，Cisco ISE 进行身份验证并根据证书的内容向您授予登录会话权限。如果此进程执行成功，系统会向您显示Cisco ISE 监控和故障排除主页并提供相应的 RBAC 权限。

使用 Diffie-Hellman 算法保护 SSH 密钥交换

可以将Cisco ISE 配置为仅允许 Diffie-Hellman-Group14-SHA1 SSH 密钥交换。为此，必须从Cisco ISE 命令行界面 (CLI) 配置模式输入以下命令：

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

示例如下：

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

将思科 ISE 配置为发送安全系统日志

开始之前

要将Cisco ISE 配置为仅在Cisco ISE 节点之间和向监控节点发送受 TLS 保护的安全系统日志，您必须执行以下任务：

- 确保部署中的所有Cisco ISE 节点都配置具有相应的服务器证书。
- 确保默认网络访问身份验证策略不允许任何版本的 SSL 协议。
- 确保您部署的所有节点都注册到主 PAN。此外，确保部署中至少有一个节点已启用监控角色，从而用作安全系统日志接收器（TLS 服务器）。
- 检查支持的系统日志 RFC 标准。请参阅Cisco ISE 版本对应的《思科身份服务引擎网络组件兼容性》指南。

步骤 1 配置安全系统日志远程日志记录目标。

步骤 2 启用日志记录类别，以将可审核事件发送到安全系统日志远程日志记录目标。

步骤 3 禁用 TCP 系统日志和 UDP 系统日志收集器。仅应启用受 TLS 保护的系统日志收集器。

配置安全系统日志远程记录目标

Cisco ISE 系统日志由日志收集器收集和存储，用于各种用途。必须选择Cisco ISE 监控节点作为日志收集器，配置安全系统日志目标。

步骤 1 登录到管理员门户。

步骤 2 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 3 点击**添加 (Add)**。

步骤 4 输入安全系统日志服务器的名称。

步骤 5 从**目标类型 (Target Type)** 下拉列表中选择**安全系统日志 (Secure Syslog)**。

步骤 6 从**状态 (Status)** 下拉列表中选择**已启用 (Enabled)**。

步骤 7 在**主机/IP 地址 (Host/IP Address)** 字段中输入部署中Cisco ISE 监控节点的主机名或 IP 地址。

步骤 8 在**端口 (Port)** 字段中，输入 *6514* 作为端口号。安全系统日志接收器在 TCP 端口 6514 上进行侦听。

步骤 9 从**设备代码 (Facility Code)** 下拉列表中选择系统日志设备代码。默认值为 **LOCAL6**。

步骤 10 选中以下复选框以启用相应配置：

a) **包括此目标的警报 (Include Alarms For This Target)**

b) **符合 RFC 3164 (Comply to RFC 3164)**

c) 启用服务器身份检查 **(Enable Server Identity Check)**

步骤 11 选中服务器关闭时缓冲消息 **(Buffer Messages When Server is Down)** 复选框。如果选中此选项，Cisco ISE 会存储日志，如果安全系统日志接收器不可达，Cisco ISE 则会定期查看安全系统日志接收器，并在安全系统接收器出现时转发日志。

a) 在缓冲区大小 **(MB) (Buffer Size (MB))** 字段中输入缓冲区大小。

b) 要让Cisco ISE 定期检查安全系统日志接收器，请在重新连接时间（秒）**(Reconnect Time (Sec))** 字段中以秒为单位输入重新连接超时值。

步骤 12 在选择 **CA** 证书 **(Select CA Certificate)** 下拉列表中选择想要Cisco ISE 呈现给安全系统日志服务器的 CA 证书。

步骤 13 在配置安全系统日志时，确保不要选中忽略服务器证书验证 **(Ignore Server Certificate validation)** 复选框。

步骤 14 点击提交 **(Submit)**。

远程日志记录目标设置

下表介绍“远程日志记录目标”(Remote Logging Targets) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。要查看此处窗口，请点击菜单 **(Menu)** 图标 (☰)，然后选择管理 **(Administration)** > 系统 **(System)** > 日志记录 **(Logging)** > 远程日志记录目标 **(Remote Logging Targets)**。

表 *5:* 远程日志记录目标设置

字段名称	使用指南
名称 **(Name)**	输入新目标的名称。
目标类型 **(Target Type)**	选择目标类型。默认情况下设置为 UDP Syslog。
说明	输入新目标的简短说明。
IP 地址 **(IP Address)**	输入要存储日志的目标计算机的 IP 地址或主机名。 思科 ISE 支持 IPv4 和 IPv6 格式的日志记录。
端口 **(Port)**	输入目标计算机的端口号。
设备代码 **(Facility Code)**	选择要用于日志记录的系统日志设备代码。有效选项为 Local0 至 Local7。
最大长度 **(Maximum Length)**	输入远程日志目标消息的最大长度。有效选项为 200 至 1024 字节。

字段名称	使用指南
服务器关闭时缓冲消息 **(Buffer Message When Server is Down)**	如果希望Cisco ISE 在 TCP 系统日志目标和安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。Cisco ISE 会在连接恢复时重新尝试将消息发送到目标。连接恢复后，消息按从最旧到最新的顺序进行发送，并且缓冲消息始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
缓冲区大小 **(MB) (Buffer Size [MB])**	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。
重新连接超时（秒）**(Reconnect Timeout [Sec])**	输入时间（以秒为单位），提及在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
选择 **CA** 证书 **(Select CA Certificate)**	选择客户端证书。
忽略服务器证书验证 **(Ignore Server Certificate Validation)**	如果希望 ISE 忽略服务器证书身份验证并接受任何系统日志服务器，请选中此复选框。

相关主题

- 思科 ISE 日志记录机制
- 思科 ISE 系统日志
- 远程系统日志消息格式
- 思科 ISE 消息目录
- 集合过滤器
- 事件抑制绕行过滤器
- 配置远程系统日志收集位置
- 配置集合过滤器

启用日志记录类别以将可审核事件发送至安全系统日志目标

您必须为Cisco ISE 启用日志记录类别，才能将可审核的事件发送到安全系统日志目标。

步骤 1 登录到管理员门户。

步骤 2 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

步骤 3 点击**管理和操作审核 (Administrative and Operational Audit)** 日志记录类别旁的单选按钮，然后点击**编辑 (Edit)**。

步骤 4 从**日志严重性级别 (Log Severity Level)** 下拉列表中选择 WARN。

步骤 5 在**目标 (Targets)** 字段中，将之前创建的安全系统日志远程记录目标移动到**选定 (Selected)** 框。

步骤 6 点击**保存 (Save)**。

步骤 7 重复此程序以启用下列日志记录类别：

- **AAA 审核 (AAA Audit)**。

  请注意，INFO 是此类别的默认日志严重性级别，无法编辑。

- **终端安全评估和客户端调配审核**。

日志记录类别设置

下表介绍了**日志记录类别 (Logging Categories)** 窗口中的字段，可以使用此窗口配置日志严重性级别，并为要存储的所选类别的日志选择日志记录目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

表 *6:* 日志记录类别设置

字段名称	使用指南
名称 (Name)	显示日志记录类别的名称。
日志严重性级别 (Log Severity Level)	允许您从以下选项中选择诊断日志记录类别的严重性级别： • **严重 (FATAL)**：紧急情况。此选项意味着无法使用Cisco ISE，并且必须立即采取操作。 • **错误 (ERROR)**：此选项表示严重或错误情况。 • **警告 (WARN)**：此选项表示正常但值得注意的情况。这是默认情况。 • **信息 (INFO)**：此选项表示信息性消息。 • **调试 (DEBUG)**：此选项表示诊断错误消息。
本地日志记录 (Local Logging)	选中此复选框可为本地节点上的类别启用日志记录事件。
目标 (Targets)	允许使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 框之间转移目标来更改类别的目标。**可用 (Available)** 框包含本地（预定义）和外部（用户定义）的现有日志记录目标。初始为空的**所选 (Selected)** 框包含特定类别的选定目标。

相关主题

- 远程系统日志消息格式
- 思科 ISE 消息代码
- 配置远程系统日志收集位置
- 设置消息代码的严重性级别

禁用 TCP 系统日志和 UDP 系统日志收集器

为确保Cisco ISE 只在 ISE 节点间发送安全系统日志，必须禁用 TCP 和 UDP 系统日志收集器，并且只启用安全系统日志收集器。

注释 如果启用Cisco ISE 消息服务来向 MnT 节点传送 UDP 系统日志，则Cisco ISE 版本 2.6 及更高版本包括 TLS 保护的 UDP 系统日志。请参阅 经思科 ISE 消息服务传递的系统日志

步骤 1 登录到管理员门户。

步骤 2 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 3 点击 TCP 系统日志收集器旁的单选按钮。

步骤 4 点击**编辑 (Edit)**。

步骤 5 从**状态 (Status)** 下拉列表中选择**禁用 (Disabled)**。

步骤 6 点击**保存 (Save)**。

步骤 7 重复此过程，直到您禁用所有 TCP 或 UDP 系统日志收集器。

默认安全系统日志收集器

Cisco ISE 为 MnT 节点提供默认安全系统日志收集器。默认情况下，没有日志记录类别映射到这些默认的安全系统日志收集器。默认安全系统日志收集器的命名方式如下：

- 主 MnT 节点 - SecureSyslogCollector
- 辅助 MnT 节点 - SecureSyslogCollector2

可以在“远程日志记录目标”(Remote Logging Targets) 页面（“管理”(Administration) >“系统”(System)>“日志记录”(Logging)）上查看此信息。无法删除默认系统日志收集器，也无法更新默认系统日志收集器的以下字段：“名称”(Name)、“目标类型”(Target type)、“IP/主机地址”(IP/Host address) 和“端口”(Port)。

在Cisco ISE 全新安装过程中，系统中的“默认自签名服务器证书”将添加到信任存储区，并标记为“信任客户端身份验证和系统日志”(Trust for Client authentication and Syslog) 用法，从而可用于安全系统日志用法。在配置部署或更新证书时，必须将相关证书分配至安全系统日志目标。

在升级期间，如果有任何现有安全系统日志目标指向端口 6514 上的 MnT 节点，系统将保留相同的名称和配置，但升级后，无法删除这些系统日志目标，并且无法编辑以下字段：“名称”(Name)、“目标类型”(Target type)、“IP/主机地址”(IP/Host address) 和“端口”(Port)。如果在升级时不存在此类目标，则将创建类似于全新安装情景的默认安全系统日志目标，无需任何证书映射。可以将相关证书分配至这些系统日志目标。如果尝试将未映射至任何证书的安全系统日志目标映射至日志记录类别，则将显示以下消息：

```
请为 log_target_name 配置证书 (Please configure the certificate for log_target_name)
```

离线维护

如果维护时间段小于一小时，请使 ISE 节点离线并执行维护任务。当节点重新联机时，PAN 会自动同步维护期间发生的所有更改。如果更改未自动同步，可以手动将其与 PAN 同步。

如果维护时间段超过一小时，请在维护时注销节点，然后在将节点添加回部署时重新注册。

我们建议将维护安排在活动较少的时间段。

注释

1. 如果队列包含超过 1, 000,000 条消息或 ISE 节点离线超过 6 小时，则可能会出现数据复制问题。
2. 如果计划在主 MnT 节点上执行维护，我们建议在执行维护活动之前对 MnT 节点进行操作备份。

终端登录配置

此页面用于配置登录凭证，以便Cisco ISE 可以登录客户端。它用于：

- 终端脚本向导
- 无代理终端安全评估

为以下项配置登录凭证：

- **Windows 域用户 (Windows Domain User)**：用于通过 SSH 登录客户端的域凭证。您可以根据需要输入任意数量的 Windows 登录。如果配置了域用户，则会忽略本地用户配置。
- **Windows 本地用户 (Windows Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。
- **MAC 本地用户 (MAC Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。

思科 ISE 中的证书管理

证书是标识个人、服务器、公司或其他实体并将实体与公钥关联的电子文档。自签证书由证书创建者签名。证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。CA 签名的数字证书被视为行业标准而且更安全。

证书用于在网络中提供安全访问。Cisco ISE 使用证书进行节点间通信和与外部服务器（例如系统日志服务器、源服务器）及所有最终用户门户（访客、发起人和个人设备门户）进行通信。证书会标识连接终端的Cisco ISE 节点并且保护该终端和Cisco ISE 节点之间的通信。

您可以使用 Admin 门户为您的部署中的所有节点管理证书。

思科 ISE 提供安全访问所用的证书

Cisco身份服务引擎 (ISE) 依赖公钥基础设施 (PKI) 提供与终端和管理员之间的安全通信，以及多节点部署内Cisco ISE 节点之间的安全通信。PKI 依赖 X.509 数字证书传输用于消息加密和解密的公钥，并验证代表用户和设备的其他证书的真实性。Cisco ISE 提供管理员门户管理以下两类 X.509 证书：

- 这些证书是识别Cisco ISE 节点到客户端应用的服务器证书。每个Cisco ISE 节点都有自己的系统证书，每个证书及相应的私钥均存储在该节点上。
- 受信任证书 - 这些证书由证书颁发机构 (CA) 颁发，用于为从用户和设备接收的公钥建立信任。受信任证书库还包含由简单证书注册协议 (SCEP) 分发的证书，可将移动设备注册到企业网络中。在主管理节点 (PAN) 上管理受信任证书库中的证书，并且系统会自动将这些证书复制到 Cisco ISE 部署中的所有其他节点。

在分布式部署中，您只能将证书导入到 PAN 的证书信任列表 (CTL) 中。证书会被复制到辅助节点。

一般来说，为了确保Cisco ISE 中的证书身份验证功能不会受到证书驱动的验证功能中细微差别的影响，请为网络中部署的所有Cisco ISE 节点使用小写主机名。

证书使用

当您将证书添加或导入到Cisco ISE 中时，应指定证书的用途：

- Admin：用于节点间通信，以及对管理门户进行身份验证
- EAP：用于基于 TLS 的 EAP 身份验证
- RADIUS DTLS：用于 RADIUS DTLS 服务器身份验证
- Portal：用于与所有Cisco ISE 最终用户门户进行通信
- xGrid：用于与 pxGrid 控制器进行通信

您可以关联每个节点中的不同证书，以便与管理员门户 (Admin)、pxGrid 控制器 (pxGrid) 进行通信，以及进行基于 TLS 的 EAP 身份验证 (EAP)。但针对其中的每种用途，您只能关联每个节点中的一个证书。

由于部署中有多个策略服务节点 (PSN) 可以支持 Web 门户请求，所以Cisco ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时，您必须定义证书组标签并将其与您的部署中各个节点上的对应证书关联。您必须将此证书组标签与对应的最终用户门户关联（访客、发起人和个人设备门户）。此证书组标签是一种唯一标识符，帮助Cisco ISE 标识与这每一个门户通信时必须使用的证书。您可以从每个节点为每个门户指定一个证书。

注释 EAP-TLS 客户端证书应具有 KeyUsage=Key Agreement 和 ExtendedKeyUsage=Client Authentication 以用于以下密码：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS 客户端证书应具有 KeyUsage=Key Encipherment 和 ExtendedKeyUsage=Client Authentication 以用于以下密码：

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

思科 ISE 中的证书匹配

设置部署中的Cisco ISE 节点后，这两个节点将互相通信。系统将检查每个 ISE 节点的 FQDN，以确保其匹配（例如 ise1.cisco.com 和 ise2.cisco.com，如果使用通配符证书，则为 *.cisco.com）。此外，当外部机器向 ISE 服务器提供证书时，将根据 ISE 服务器中的证书对提供用于身份验证的外部证书进行检查（或匹配）。如果两个证书匹配，则身份验证成功。

对于 ，匹配操作将在 节点之间（如果有两个）或 与 pxGrid 之间执行。

Cisco ISE 按以下方式检查匹配的主题名称：

1. Cisco ISE 查看证书的主题别名 (SAN) 扩展。如果 SAN 包含一个或多个 DNS 名称，则其中必须有一个 DNS 名称与Cisco ISE 节点的 FQDN 相匹配。如果使用通配符证书，则通配符域名必须与 Cisco ISE 节点的 FQDN 中的域匹配。
2. 如果 SAN 中不包含 DNS 名称、或 SAN 完全缺失，则证书主题字段中的通用名称或通配符域必须与节点的 FQDN 匹配。
3. 如果未找到匹配项，则会拒绝该证书。

注释 导入到Cisco ISE 的 X.509 证书必须为隐私增强邮件 (PEM) 格式或可辩别编码规则 (DER) 格式。可导入包含证书链（即带有签署该系统证书的受信任证书序列的系统证书）的文件，但会受到某些限制。

X.509 证书的有效性

X.509 证书仅从特定日期开始有效。当系统证书到期时，取决于证书的Cisco ISE 功能会受到影响。当距离到期日还有 90 天时，Cisco ISE 会通知您系统证书即将到期。系统以多种方式显示此通知：

- 彩色到期状态图标显示在 System Certificates 页面。
- 到期消息显示在Cisco ISE 系统诊断报告中。
- 在距离到期日 90 天和 60 天时生成到期警报，在最后 30 天内，每天生成一次警报。

如果即将到期的证书为自签证书，您可以编辑证书，延长到期日。对于 CA 签名的证书，必须留出足够的时间，从 CA 获取替换证书。

在思科 ISE 中启用 PKI

公钥基础结构 (PKI) 是一种加密技术，用于实现安全通信和验证使用数字签名的用户的身份。

步骤 1 在每个部署节点上为启用 TLS 的身份验证协议（如 EAP-TLS）建立系统证书，以用于管理员门户身份验证、供浏览器和 REST 客户端访问Cisco ISE Web 门户，以及用于 pxGrid 控制器。

默认情况下，Cisco ISE 节点预先安装用于 EAP 身份验证、管理员门户、门户和 pxGrid 控制器的自签证书。在典型的企业环境中，此证书由受信任 CA 签名的服务器证书代替。

步骤 2 用与用户建立信任所需的 CA 证书以及向Cisco ISE 出示的设备证书填充受信任证书库。

要使用包含一个根CA证书以及一个或更多中间CA证书的证书链来验证用户或设备证书的真实性，请执行以下操作：

- 为根 CA 启用信任选项。

  从Cisco ISE GUI 中，选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **证书管理 (Certificate Management) 受信任证书 (Trusted certificates)** 在此窗口中，选择根 CA 证书，然后点击**编辑 (Edit)**。在**使用 (Usage)** 选项卡中，选择**信任范围 (Trusted For)** 部分中的复选框。

- 如果不想为根 CA 启用信任选项，请将整个 CA 证书链导入受信任证书存储区。

对于节点间通信，您必须使用验证属于Cisco ISE 部署中每个节点的管理员系统证书所需的信任证书填充受信任证书库。如果您想要使用默认自签证书进行节点间通信，则必须从每个Cisco ISE节点的“系统证书”(System Certificates)页面导出该证书并将其导入受信任证书库。如果您用 CA 签名的证书代替自签证书，只需用相应的根 CA 和中间 CA 证书填充受信任证书库。请注意，在完成此步骤之前，您无法在Cisco ISE 部署中注册节点。

当自带设备用户从一个位置移动到另一个位置时，如果您使用自签证书确保部署中客户端与PSN之间的安全通信，EAP-TLS 用户身份验证会失败。对于这种必须在某些 PSN 之间实现的身份验证请求，您必须通过外签 CA 证书或使用外部 CA 签名的通配符证书确保客户端与 PSN 之间的通信。

注释 在您从独立Cisco ISE 节点或PAN获取备份后，如果您更改您的部署中一个或更多节点上的证书配置，您必须再获得一个备份以恢复数据。否则，如果您尝试使用较旧的备份恢复数据，节点之间的通信可能会发生故障。

通配符证书

通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。例如，Certificate Subject中的CN值可以是一些通用主机名（例如aaa.ise.local），SAN字段会包含相同的通用主机名和通配符表示法（例如 DNS.1=aaa.ise.local 和 DNS.2=*.ise.local）。

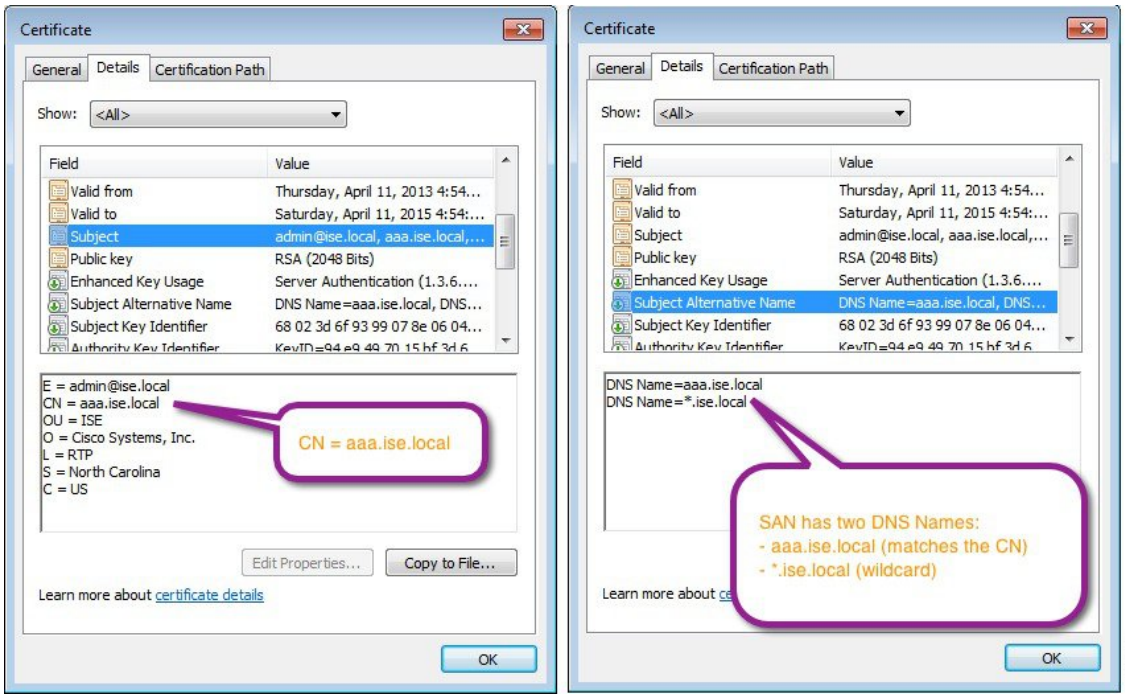
如果将某个通配符证书配置为使用 *.ise.local，可以使用同一证书来保护 DNS 名称以“.ise.local”结尾的任何其他主机，例如：。：

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

通配符证书用与普通证书一样的方式保护通信安全，并且使用相同的验证方法处理请求。

下图显示用于保护 Web 站点的一个通配符证书的示例。

图 *5:* 通配符证书示例



思科 ISE 中的通配符证书支持

Cisco ISE 支持通配符证书。在较低版本中，Cisco ISE 会验证为 HTTPS 启用的任何证书以确保 CN 字段与主机的完全限定域名 (FQDN) 完全一致。如果字段不一致，则证书无法用于 HTTPS 通信。

在较低版本中，Cisco ISE 使用该 CN 值来替换 url-redirect A-V 对字符串中的变量。此 CN 值还曾用于所有集中式 Web 身份验证 (CWA)、自行激活、安全评估重定向等。

Cisco ISE 使用 ISE 节点的主机名作为 CN。

适用于 HTTPS 和 EAP 通信的通配符证书

您可以在Cisco ISE 中将通配符服务器证书用于使用 SSL/TLS 隧道的 Admin（基于 Web 的服务）和 EAP 协议。通过使用通配符证书，不再需要为每个Cisco ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个Cisco ISE 节点分配唯一服务器证书的安全性低。

在向访客门户分配公共通配符证书并随根 CA 证书一起导入从属 CA 时，直到 ISE 服务重新启动后才会发送证书链。

注释 如果使用通配符证书，我们强烈建议您将域空间进行分区，以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，就可能导致严重的安全问题。

通配符证书在域名前使用星号 (*) 和一个句点。例如，证书的使用者名称的 CN 值是一般主机名称（例如 aaa.ise.local）,SAN 字段可以使用通配符，例如 *.ise.local。Cisco ISE 支持使用通配符证书，其中通配符 (*) 是所显示标识符最左侧的字符。例如，*.example.com 或 *.ind.example.com。Cisco ISE 不支持所显示的标识符中连通配符一起显示其他字符的证书。例如，abc*.example.com 或 a*b.example.com 或 *abc.example.com。

URL 重定向中的完全限定域名

当Cisco ISE 建立授权配置文件重定向时（用于集中 Web 身份验证、设备注册 Web 身份验证、本地请求方调配、移动设备管理和客户端调配与安全评估服务），所产生的 cisco-av-pair 包括一个类似于以下内容的字符串：

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

处理此请求时，Cisco ISE 会用实际值代替此字符串中的某些关键字。例如，Cisco ISE 会将 SessionIdValue 替换为该请求的实际会话 ID。对于 eth0 接口，Cisco ISE 将 URL 中的 IP 替换为Cisco ISE 节点的 FQDN。对于非 eth0 接口，Cisco ISE 使用 URL 中的 IP 地址。您可以为接口 eth1 至 eth3 分配主机别名（名称），然后在 URL 重定向期间，Cisco ISE 可以用其代替 IP 地址。

要实现此操作，您可以在配置模式下从 ISE CLI ISE /admin(config)# 提示符处使用 **ip host** 命令：

ip host *IP_address host-alias FQDN-string*

其中 IP_address 是网络接口的 IP 地址（eth1 或 eth2 或 eth3），host-alias 是您分配给网络接口的名称。FQDN-string 是网络接口的完全限定域名。使用此命令，您可以向网络接口分配主机别名或FQDN 字符串，或同时分配主机别名和 FQDN 字符串。

这是使用 **ip host** 命令的一个示例：ip host a.b.c.d sales sales.amerxyz.com

向非 eth0 接口分配主机别名之后，您必须在Cisco ISE 上使用 **application start ise** 命令重新启动应用服务。

使用此命令的 no 形式可删除主机别名与网络接口的关联。

no ip host *IP_address host-alias FQDN-string*

使用 **show running-config** 命令以查看主机别名定义。

如果您提供 FQDN 字符串，Cisco ISE 会使用 FQDN 替换 URL 中的 IP 地址。如果您仅提供主机别名，Cisco ISE 会将主机别名与所配置的 IP 域名组合以形成完整的 FQDN，并用 FQDN 替换 URL 中的 IP 地址。如果您不将网络接口映射至主机别名，则Cisco ISE 会使用 URL 中的网络接口的 IP 地址。

当您将非 eth0 接口用于客户端调配或本地请求方或访客流程时，您必须确保在策略服务节点证书的 SAN 字段中正确配置非 eth0 接口的 IP 地址或主机别名。

使用通配符证书的优势

- 节约成本。由第三方证书颁发机构签名的证书都很昂贵，尤其是当服务器数量增加的时候。在 Cisco ISE 部署中，可以在多个节点上使用通配符证书。

- 提高运营效率。通配符证书允许所有策略服务节点 (PSN) EAP 和 Web 服务共享同一证书。除了能显著节约成本之外，由于可以只创建证书一次，然后就可以将其应用于所有 PSN，所以还能简化证书管理。
- 降低身份验证错误。通配符证书可以解决 Apple iOS 设备常见的证书问题，即客户端将受信任证书存储于配置文件中，而不遵循信任签名 root 的 iOS Keychain。当 iOS 客户端首次与 PSN 通信时，它不会明确信任 PSN 证书，即使受信任证书颁发机构已为该证书签名。使用通配符证书，所有 PSN 上证书都将一样，所以用户只须接受一次该证书，接下来对不同 PSN 的身份验证就会继续进行，而不会报错或出现提示。
- 简化请求方配置。例如，启用 PEAP-MSCHAPv2 和服务器证书信任的 Microsoft Windows 请求方要求您指定要信任的各个服务器证书，否则当客户端使用不同的 PSN 进行连接时，系统会提示用户是否信任各个 PSN 证书。使用通配符证书，可以信任一个统一的服务器证书，而不需从每个 PSN 逐一信任各个证书。
- 通配符证书可以减少提示，增强无缝连接，从而提高用户体验。

使用通配符证书的缺点

以下是与通配符证书相关的一些安全问题：

- 失去可审核性和不可否认性
- 提高了私钥的泄露风险
- 不常见或管理员不了解

通常认为通配符证书没有每个 ISE 节点均拥有的唯一的服务器证书那么安全。但是，成本和运营因素比安全风险更重要。

ASA 等安全设备也支持通配符证书。

部署通配符证书时，一定要谨慎。例如，如果您使用 *.company.local 创建一个证书，而某个攻击者能够发现其私钥，则该攻击者就可以监听 company.local 域中的任意服务器。因此，最好给域空间分区以避免这类威胁。

要解决可能出现的这个问题和限制使用范围，也可以使用通配符证书保护您的组织的具体子域。在您想要指定通配符的通用名称子域部分添加一个星号 (*)。

例如，如果您为 *.ise.company.local 配置通配符证书，则可以将该证书用于保护 DNS 名称以“.ise.company.local”结尾的任意主机，例如：

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

通配符证书兼容性

通常在创建通配符证书时，会将通配符列为证书使用者的公用名 (CN)。Cisco ISE 支持这种类型的结构。但并不是所有的终端请求方都支持在证书使用者中使用通配符字符。

通过测试的所有 Microsoft 本机请求方（包括 Windows Mobile）不支持在证书使用者中使用通配符字符。

您可以使用另一个请求方，例如 Cisco AnyConnect 网络访问管理器 (NAM)，它可能允许在 Subject 字段中使用通配符字符。

您还可以使用特殊通配符证书（例如设计为与不兼容设备配合使用的 DigiCert 的 Wildcard Plus），方法是在证书的 Subject Alternative Name 中包含特定子域。

尽管 Microsoft 请求方限制似乎禁止使用通配符证书，但仍有其他方法创建通配符证书，允许它与通过测试的所有设备配合使用，从而实现安全访问，包括 Microsoft 本机请求方。

为此，您必须在 Subject Alterative Name (SAN) 字段中使用通配符字符，而不是在 Subject 中使用通配符字符。SAN 字段保留专为检查域名而设计的扩展名（DNS 名称）。有关详细信息，请参阅 RFC 6125 和 2128。

证书层次结构

在管理员门户中，您可以查看所有终端、系统和受信任证书的证书层次结构或证书信任链。证书层级包括证书、所有中间证书颁发机构 (CA) 证书和根证书。例如，当选择从管理员门户查看系统证书时，默认情况下会显示相应系统证书的详细消息。证书层级显示在该证书的顶部。点击层次结构中的任何证书可查看其详细信息。自签名证书没有任何层次结构或信任链。

在证书列表页面的“状态”(Status) 列中，您将会看到以下图标之一：

- 绿色图标 - 表示有效证书（有效信任链）
- 红色图标 - 表示存在错误（例如，信任证书缺失或过期）
- 黄色图标 - 警告证书即将到期并提示续订

系统证书

Cisco ISE 系统证书是向部署中的其他节点和客户端应用标识Cisco ISE 节点身份的服务器证书。系统证书的用途如下：

- 用于Cisco ISE 部署中的节点间通信。在 Usage 字段中为这些证书选择 Admin 选项。
- 由浏览器和连接到Cisco ISE Web 门户的 REST 客户端使用。在 Usage 字段中为这些证书选择 Portal 选项。
- 用于与 PEAP 和 EAP-FAST 组成外部 TLS 隧道。在 Usage 字段中选择 EAP 选项，以使用 EAP-TLS、PEAP 和 EAP-FAST 进行相互身份验证。
- 用于 RADIUS DTLS 服务器身份验证。
- 用于与 SAML 身份提供程序 (IdP) 进行通信。在“使用”(Usage) 字段中为这证书选择 SAML 选项。如果选择了 SAML 选项，则该证书不可用于其它服务。
- 用于与 pxGrid 控制器通信。在 Usage 字段中为这些证书选择 pxGrid 选项。

必须在Cisco ISE 部署中的每个节点上安装有效的系统证书。默认情况下，在安装期间，将在Cisco ISE 节点上创建两个自签证书和一个由内部Cisco ISE CA 签名的证书：

- 指定用于 EAP、管理员、门户和 RADIUS DTLS 的自签名服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 SAML IdP 之间安全通信的自签名 SAML 服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 pxGrid 客户端之间安全通信的内部Cisco ISE CA 签名的服务器证书（密钥长度为 4096，有效期为一年）。

设置部署并注册辅助节点时，指定用于 pxGrid 控制器的证书将自动替换为由主要节点的 CA 签名的证书。因此，所有 pxGrid 证书将属于同一 PKI 信任层次结构。

注释 当导出要导入其他节点的通配符系统证书（用于节点间通信）时，请确保导出证书和私钥，并指定加密密码。在导入过程中，将需要证书、私钥和加密密码。

注释 要确定对应于您的版本的支持密钥和密码信息，请查找适当版本的《思科身份识别服务引擎网络组件兼容性》指南。

为了提高安全性，建议您使用 CA 签名的证书替换自签证书。要获取 CA 签名的证书，您必须：

1. 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 78 页
2. 将根证书导入受信任证书库，第 72 页
3. 将 CA 签名的证书与 CSR 绑定，第 78 页

ISE 社区资源

步骤：实施 ISE 服务器端证书

思科身份识别服务引擎上的证书更新配置指南

查看系统证书

“系统证书”(System Certificate) 页面列出添加至Cisco ISE 的所有系统证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

系统显示“系统证书”(System Certificates) 页面，提供关于本地证书的以下信息：

- “友好名称”(Friendly Name) - 证书的名称。
- “使用者”(Used By) - 使用此证书的服务。
- “门户组标记”(Group Tag) - 仅适用于指定用于门户用途的证书。指定必须将哪个证书用于门户。
- “颁发给”(Issued To) - 证书使用者的通用名称。
- “颁发者”(Issued By) - 证书颁发者的通用名称。
- “生效日期”(Valid From) - 创建证书的日期，也称为开始时间证书属性。
- “到期日期”(Expiration Date) - 证书的到期日期，也称为截止时间证书属性。指示证书何时过期。到期日期有五个类别，每个类别有一个如下所述的关联图标：
  - 距到期还有 90 天以上（绿色图标）
  - 距到期还有 90 天或不足 90 天（蓝色图标）
  - 距到期还有 60 天或不足 60 天（黄色图标）
  - 距到期还有 30 天或不足 30 天（橙色图标）
  - 已到期（红色图标）

步骤 2 选择一个证书并选择 **查看 (View)** 以显示证书详细信息。

导入系统证书

可以从管理员门户为任意Cisco ISE 节点导入系统证书。

注释 在主 PAN 上更改管理员角色证书时会在所有其他节点上重新启动服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

开始之前

- 确保您在运行客户端浏览器的系统上拥有系统证书和私钥文件。
- 如果您导入的系统证书由外部 CA 签名，则将相关根 CA 或中间 CA 证书导入受信任证书存储区（**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任的证书 (Trusted Certificates)**）。
- 如果导入的系统证书中包含 CA 标志设置为 true 的基本约束扩展，请确保有密钥用法扩展并且设置了 keyEncipherment 位或 keyAgreement 位。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1

步骤 2 点击**导入 (Import)**。
此时将打开“导入服务器证书”(Import Server Certificate) 屏幕。

步骤 3 输入您要导入的证书的值。

步骤 4 点击**提交 (Submit)**。

系统证书导入设置

下表介绍可用于导入服务器证书的“导入系统证书”(Import System Certificate) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **导入 (Import)**。

表 *7:* 系统证书导入设置

字段名称	说明
选择节点 (Select Node)	（必填）选择您要导入系统证书的Cisco ISE 节点。
证书文件 (Certificate File)	（必填）点击**浏览 (Browse)**，从本地系统中选择证书文件。
私钥文件 (Private Key File)	（必填）点击 **浏览 (Browse)** 选择私钥文件。
密码 (Password)	（必填）输入密码以解密私钥文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
允许通配符证书 (Allow Wildcard Certificates)	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。 如果选中此复选框，Cisco ISE 会将此证书导入到部署中的所有其他节点。
验证证书扩展名 (Validate Certificate Extensions)	如果希望Cisco ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在，并且设置了 keyEncipherment 位和/或 keyAgreement 位。

字段名称	说明
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理员 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书 注释 在主 PAN 上更改管理员角色证书时会在所有其他节点上重新启动服务。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书 • **pxGrid**：用于确保pxGrid客户端和服务器之间的安全通信的客户端和服务器证书。 • **ISE 消息服务 (ISE Messaging Service)**：用于**经思科 ISE 消息传递的系统日志 (Syslog Over Cisco ISE Messaging)** 功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 56 页
查看系统证书，第 57 页
导入系统证书，第 58 页

生成自签证书

通过生成自签证书添加新的本地证书。Cisco建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署Cisco ISE，务必尽可能使用CA签名证书，确保生产网络中更统一地接受。

注释 如果正使用自签证书并且必须更改Cisco ISE 节点的主机名，则必须登录Cisco ISE 节点的管理员门户，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，Cisco ISE 将继续使用采用旧主机名的自签证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

自签证书设置

下表介绍“生成自签证书”(Generate Self Signed Certificate) 页面上的字段。您可以通过此页面为节点间通信、EAP-TLS 身份验证、Cisco ISE Web 门户创建系统证书以及与 pxGrid 控制器通信。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **生成自签名证书 (Generate Self Signed Certificate)**。

表 *8:* 自签证书设置

字段名称	使用指南
选择节点 (Select Node)	（必填）您要生成系统证书的节点。
公共名称 (CN) (Common Name [CN])	（如果您不指定 SAN，则此字段必填）默认情况下，Common Name 为您要生成自签证书的 ISE 节点的完全限定域名。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	与该证书关联的 IP 地址、DNS 名称或统一资源标识符 (URI)。
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。

字段名称	使用指南
密钥长度 (Key Length)	指定公共密钥的位大小。以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 **注释** 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果您计划获得公共 CA 签名的证书或将思科 ISE 部署为符合 FIPS 的策略管理系统，请选择 2048。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。
过期 TTL (Expiration TTL)	指定证书到期之前的天数。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
允许通配符证书 (Allow Wildcard Certificates)	如果要生成自签名通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。

字段名称	使用指南
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书。 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书。 • **pxGrid**：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务器证书。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 56 页
查看系统证书，第 57 页
生成自签证书，第 60 页

编辑系统证书

可以使用此页面编辑系统证书，续订自签证书。当编辑通配符证书时，更改将被复制到部署中的所有节点上。当删除通配符证书时，此通配符证书将从部署中的所有节点删除。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要编辑的证书旁边的复选框，然后点击**Edit**。

步骤 3 要续订自签证书，请选中**续签期限 (Renewal Period)** 复选框，然后输入以天、周、月或年为单位的到期 TTL。

步骤 4 点击**保存 (Save)** 保存更改。

如果选中**管理 (Admin)** 复选框，系统将重新启动Cisco ISE 节点上的应用服务器。此外，如果Cisco ISE 节点是部署中的 PAN，系统还将重新启动部署中所有其他节点上的应用服务器。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

注释 使用 Chrome 65 及更高版本启动 ISE 可能会导致 BYOD 门户或访客门户无法在浏览器中启动，即使 URL 已成功重定向也是如此。这是因 Google 引入的新安全功能所致，此功能要求所有证书具有“主题备用名称”(Subject Alternative Name) 字段。对于版本 ISE 2.4 及更高版本，必须填充“主题备用名称”(Subject Alternative Name) 字段。

要使用 Chrome 65 及更高版本启动，请执行以下步骤：

1。通过填充“主题备用名称”(Subject Alternative Name) 字段，从 ISE GUI 生成新的自签证书。必须同时填写 DNS 和 IP 地址。

2. ISE 服务此时会重新启动。

3. 在 Chrome 浏览器中重定向门户。

4. 在浏览器中，“查看证书”(View Certificate) > “详细信息”(Details) > 通过选择 base-64 编码来“Copy the certificate”(复制证书)。

5. 将证书安装到受信任路径。

6. 关闭 Chrome 浏览器，然后尝试重定向门户。

注释 在为操作系统 Win RS4 或 RS5 中的浏览器 Firefox 64 及更高版本配置无线 BYOD 设置时，可能无法添加证书例外。如果是全新安装 Firefox 64 及更高版本，此行为是预计行为，如果是从先前版本升级到 Firefox 64 及更高版本，则不会出现此行为。在这种情况下，可以通过以下步骤添加证书例外：

1. 针对 BYOD 流程单/双 PEAP 或 TLS 进行配置。

2. 通过 Windows ALL 选项配置 CP 策略。

3. 在最终客户端 Windows RS4/RS5 中连接 Dot1.x/MAB SSID。

4. 在 FF64 浏览器中键入 1.1.1.1 以重定向至访客/BYOD 门户。

5. 点击**添加例外 (Add Exception)** > **无法添加证书 (Unable to add certificate)**，然后继续执行流程。

变通方案是，需要导航至**选项 (Options)** > **隐私和设置 (Privacy & Settings)** > **查看证书 (View Certificates)** > **服务器 (Servers)** > **添加例外 (Add Exception)**

，手动为 Firefox 64 添加证书。

删除系统证书

您可以删除不再使用的系统证书。

可以一次从系统证书存储区中删除多个证书，但必须至少具有一个可用于管理员和 EAP 身份验证的证书。此外，无法删除用于管理员、EAP 身份验证、门户或 pxGrid 控制器的任何证书。但是，在禁用服务时可以删除 pxGrid 证书。

如果您选择删除通配符证书，则系统会从部署中的所有节点删除该证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中想要删除的证书旁边的复选框，然后点击**删除 (Delete)**。

系统将显示一条警告消息。

步骤 3 点击**是 (Yes)**，删除证书。

导出系统证书

您可以导出所选择的系统证书或某个证书及其关联的私钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要导出的证书旁的复选框，然后点击**导出 (Export)**。

步骤 3 选择是仅导出证书，还是导出证书及其关联的私钥。

提示 由于可能会暴露私钥值，我们不建议导出与证书关联的私钥。如果您必须导出私钥（例如，导出要导入其他节点以用于节点间通信的通配符系统证书时），请指定私钥加密密码。在将此证书导入另一Cisco ISE节点时，需要指定此密码以解密私钥。

步骤 4 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

步骤 5 点击**导出 (Export)** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以隐私强化邮件的格式进行存储。如果同时导出证书和私钥，则证书会导出为 .zip 文件，其中包含隐私强化邮件格式的证书和已加密的私钥文件。

受信任证书库

受信任证书库包括用于信任和简单证书注册协议 (SCEP) 的 X.509 证书。

受信任证书库中的证书在 PAN 上进行管理，并且复制至Cisco ISE 部署中的每个节点。Cisco ISE 支持通配符证书。

Cisco ISE 将受信任证书用于以下用途：

- 验证由终端和访问ISE-PIC管理员门户的Cisco ISE 管理员（使用基于证书的管理员身份验证）用于身份验证的客户端证书。
- 确保部署中Cisco ISE 节点之间的安全通信。受信任证书库必须包含与部署中每个节点上的系统证书建立信任所需的 CA 证书链。

- 如果将自签证书用于系统证书，则各个节点的自签证书必须放在 PAN 的受信任证书库中。
- 如果将自签证书用于系统证书，则 CA root 证书以及信任链中的任何中间证书都必须放在 PAN 的受信任证书库中。

- 实现安全的 LDAP 身份验证，在定义将通过 SSL 访问的 LDAP 身份源时，必须从证书存储区选择证书。
- 向准备使用个人设备门户在网络中进行注册的个人设备进行分配。Cisco ISE 在策略服务节点 (PSN) 上实施 SCEP 以支持个人设备注册。注册设备使用 SCEP 协议从 PSN 请求客户端证书。PSN 包含作为中介的注册机构 (RA)；RA 接收并验证来自注册设备的请求，然后将请求转发给颁发客户端证书的外部 CA 或内部Cisco ISE CA。CA 将证书发送回 RA，RA 再将其返回至设备。

  Cisco ISE 使用的每个SCEP CA 都通过 SCEP RA 配置文件定义。当创建 SCEP RA 配置文件时，系统将以下两个证书自动添加到受信任证书库：

  - CA 证书（自签证书）
  - RA 证书（证书请求代理证书），由 CA 签名。

  SCEP 协议要求 RA 将这两个证书提供给注册设备。通过将这两个证书放入受信任证书库，系统将其复制至所有 PSN 节点，以供这些节点上的 RA 使用。

注释 删除 SCEP RA 配置文件时，关联的 CA 链也会从受信任证书库中删除。但是，如果安全系统日志、LDAP 系统或信任证书引用相同的证书，则仅删除 SCEP 配置文件。

注释

- 导入到Cisco ISE 的 X.509 证书的格式必须为隐私增强邮件 (PEM) 或卓越编码规则 (DER)。可以根据特定限制，导入包含证书链的文件，也就是系统证书以及签名的受信任证书的序列。
- 在向访客门户分配公共通配符证书并随根 CA 证书一起导入子 CA 时，直到 ISE 服务重新启动后才会发送证书链

ISE 社区资源

在 ISE 2.0 中安装第三方 CA 证书

受信任证书库中的证书

受信任证书库中包含受信任的证书：生产证书、根证书、 和其他受信任的证书。根证书（Cisco根 CA）给生产（Cisco CA 生产）证书签名。默认情况下禁用这些证书。如果您在部署中将Cisco IP 电话作为终端，您应启用这两个证书，从而可以对用于电话的Cisco签名的客户端证书进行身份验证。

受信任证书库页面

下表介绍“受信任证书库页面”(Trusted Certificates Store) 窗口上的字段，您可以使用此页面查看添加到管理节点的证书。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

表 *9:* 证书库页面

字段名称	使用指南
友好名称 (Friendly Name)	显示证书的名称。
状态 (Status)	“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
信任范围 (Trusted for)	显示使用此证书的服务。
颁发给 (Issued To)	证书使用者的通用名称 (CN)。
颁发者 (Issued By)	证书颁发者的通用名称 (CN)。
生效日期 (Valid From)	“开始时间”证书属性。
到期日期 (Expiration Date)	“截止时间”证书属性。
到期状态 (Expiration Status)	提供有关证书到期状态的信息。此列显示五个图标和提示消息类别： • **绿色**：距到期还有 90 天以上 • **蓝色**：距到期还有 90 天或更短 • **黄色**：距到期还有 60 天或更短 • **橙色**：距到期还有 30 天或更短 • **红色**：已到期

相关主题

受信任证书库，第 65 页
查看受信任证书库证书，第 68 页
更改受信任证书库中的证书状态，第 69 页
在受信任的证书库中添加证书，第 69 页

受信任证书命名限制

CTL 中的受信任证书可以包含名称限制扩展。此扩展为证书链中后续证书的所有主题名称和主题替代名称的值定义命名空间。Cisco ISE 不检查根证书中指定的限制。

Cisco ISE 支持以下名称限制：

- 目录名称

  目录名称限制应该是主题/SAN 中目录名称的前缀。例如，

  - 正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：O=Cisco,CN=Salomon

  - 不正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：CN=Salomon,O=Cisco

- DNS
- 邮件
- URI（URI 限制必须以一个 URI 前缀开头，例如 http://、https://、ftp:// 或 ldap://）。

Cisco ISE 不支持以下名称限制：

- IP 地址
- 其他名称

当受信任证书包含不支持的限制并且验证的证书不包含相应字段时，系统会拒绝此证书，因为Cisco ISE 无法验证不支持的限制。

以下是受信任证书中名称限制的一个示例：

```
 X509v3 Name Constraints: critical Permitted: othername:<unsupported> email:.abcde.at
email:.abcde.be email:.abcde.bg email:.abcde.by DNS:.dir DirName: DC = dir, DC = emea
DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic DirName: C = BG, ST =
EMEA, L = BG, O = ABCDE Group, OU = Domestic DirName: C = BE, ST = EMEA, L = BN, O = ABCDE
 Group, OU = Domestic DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service
Z100 URI:.dir IP:172.23.0.171/255.255.255.255 Excluded: DNS:.dir URI:.dir
```

以下是与以上定义匹配的一个可接受客户端证书主题：

```
 Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1, CN=cwinwell
```

查看受信任证书库证书

“受信任证书”(Trusted Certificates) 页面列出所有已添加到Cisco ISE 的受信任证书。 要查看受信任的证书，您必须成为超级管理员或系统管理员。

要查看所有证书，请依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。系统将显示受信任证书页面，其中列出了所有受信任的证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

更改受信任证书库中的证书状态

必须启用证书状态，Cisco ISE 才能使用此证书建立信任。将证书导入受信任证书库时，将自动启用此证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 3 选中想要启用或禁用的证书旁边的复选框，然后点击 **编辑 (Edit)**。

步骤 4 更改状态。

步骤 5 点击**保存 (Save)**。

在受信任的证书库中添加证书

可以通过“证书存储区”(Certificate Store) 页面向Cisco ISE 添加 CA 证书。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保证书库证书位于运行您的浏览器的计算机文件系统上。证书必须是 PEM 或 DER 格式。
- 如果您计划将证书用于管理员或 EAP 身份验证，请确保在证书中定义基本限制并且确保 CA 标志设置为 true。

编辑受信任证书

在将证书添加到受信任证书库之后，可以通过使用编辑设置进行进一步编辑。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 选中要编辑的证书旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 根据需要修改可编辑字段。

步骤 4 点击**保存 (Save)** 以保存对证书库所做的更改。

编辑证书设置

下表介绍了“证书存储区编辑证书”(Certificate Store Edit Certificate) 窗口上的字段，可以使用此窗口编辑证书颁发机构 (CA) 证书属性。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管**

理 **(Administration)** > 系统 **(System)** > 证书 **(Certificates)** > 受信任证书 **(Trusted Certificates)** > 证书 **(Certificate)** > 编辑 **(Edit)**。

表 *10:* 证书库编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	
友好名称 (Friendly Name)	输入证书的友好名称。
状态 (Status)	选择“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
说明	输入可选的说明。
使用情况 (Usage)	
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您想要使用此证书验证服务器证书（从其他 ISE 节点或 LADP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅适用于选中“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框的情况）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。
证书状态验证 (Certificate Status Validation)	ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至 ISE 的证书吊销列表 (CRL) 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。
验证 OCSP 服务 (Validate Against OCSP Service)	选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。
如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)	如果 OCSP 无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致 ISE 拒绝当前评估的客户端或服务器证书。

字段名称	使用指南
OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)	选中此复选框供 ISE 在 OCSP 响应器无法访问时拒绝请求。
下载 CRL (Download CRL)	选中此复选框以使Cisco ISE 下载 CRL。
CRL 分类的 URL (CRL Distribution URL)	输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。
检索 (Retrieve CRL)	可以自动或定期下载 CRL。请配置下载时间间隔。
如果下载失败，请稍候 (If download failed, wait)	配置在Cisco ISE 再次尝试下载 CRL 之前等待的时间间隔。
如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)	选中此复选框，以使系统在收到CRL之前接受客户端请求。如果取消选中此复选框，Cisco ISE会拒绝使用选定CA签名的证书的所有客户端请求，直到收到 CRL 文件为止。
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	如果您希望Cisco ISE忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝EAP-TLS身份验证，请选中此复选框。 如果您希望Cisco ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查CRL文件，请取消选中此复选框。如果CRL尚未激活或已到期，Cisco ISE 会拒绝使用此 CA 签名的证书的所有身份验证。

相关主题

受信任证书库，第 65 页
编辑受信任证书，第 69 页

删除受信任证书

可以删除不再需要的受信任证书。不过，请确保不会删除 ISE 内部 CA（证书颁发机构）证书。ISE 内部 CA 证书只能在替换整个部署的 ISE 根证书链时删除。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 选中想要删除的证书旁边的复选框，然后点击**删除 (Delete)**。

系统将显示一条警告消息。如果已选择删除 ISE 内部 CA 证书，则点击：

- **删除 (Delete)** - 删除 ISE 内部 CA 证书。ISE 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。要允许终端再次接入网络，请将相同的 ISE 内部 CA 证书导入受信任证书存储区。
- **删除并撤销 (Delete & Revoke)** - 删除并撤销 ISE 内部 CA 证书。ISE 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。此操作无法撤销。必须替换整个部署的 ISE 根证书链。

步骤 3 点击**是 (Yes)**，删除证书。

从受信任证书库导出证书

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

注释 如果从内部CA导出证书，并计划使用该导出从备份恢复，则必须使用CLI命令 `application configure ise`。有关详细信息，请参阅导出思科 ISE CA 证书和密钥，第 105 页。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。

步骤 2

步骤 3 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

步骤 4 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

将根证书导入受信任证书库

导入根 CA 和中间 CA 证书时，您可以指定要为其使用受信任 CA 证书的服务。

开始之前

您必须具有来自已对 CSR 进行签名并返回数字签名 CA 证书的证书颁发机构的根证书和其他中间证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2

步骤 3 点击**导入 (Import)**。

步骤 4 在显示的**将新证书导入证书存储区 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)** 以选择您的 CA 签名和返回的根 CA 证书。

步骤 5 在**友好名称 (Friendly Name)** 中输入友好的名称。

如果没有输入**友好名称**，Cisco ISE 将使用 *common-name#issuer#nnnnn* 格式的名称填充此字段， 其中 *nnnnn* 是唯一编号。可以再次编辑证书来更改**友好名称**。

步骤 6 选中要为其使用此受信任证书的服务旁边的复选框。

步骤 7 （可选）在**说明** 字段中，输入此证书的说明。

步骤 8 点击**提交 (Submit)**。

下一步做什么

将中间 CA 证书导入到受信任证书库（如果适用）。

受信任证书导入设置

下表说明了“受信任证书导入”(Trusted Certificate Import) 窗口上的字段，可以使用此窗口将证书颁发机构 (CA) 证书添加到Cisco ISE。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**。

表 *11:* 受信任证书导入设置

字段名称	说明
证书文件 (Certificate File)	点击**浏览 (Browse)** 从运行浏览器的计算机选择证书文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果不指定名称，Cisco ISE 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您希望将此证书用于验证服务器证书（从其他 ISE 节点或 LDAP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。

字段名称	说明
验证证书扩展名 (Validate Certificate Extensions)	（仅适用于同时选中“信任客户端身份验证和系统日志”(Trust for client authentication and Syslog) 选项和“证书扩展上启用验证”(Enable Validation of Certificate Extensions) 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。
说明	输入可选的说明。

相关主题

受信任证书库，第 65 页
证书链导入，第 74 页
将根证书导入受信任证书库，第 72 页

证书链导入

您可以从单个文件导入多个证书，这个文件中包含从证书库接收的证书链。文件中的所有证书都必须为隐私增强邮件 (PEM) 格式，并且这些证书必须按照以下顺序排列：

- 文件中的最后一个证书必须是 CA 颁发的客户端证书或服务器证书。
- 前面的所有证书必须是根 CA 证书和所颁发证书的签名链中的所有中间 CA 证书。

导入证书链的过程分为两个步骤：

1. 在 Admin 门户中将证书链文件导入受信任证书库。此操作会将除最后一个证书之外的所有证书导入受信任证书库。
2. 使用绑定CA签名的证书操作导入证书链文件。此操作会将文件中的最后一个证书导入作为本地证书。

为思科 ISE 节点间通信安装受信任证书

当您设置部署时，在注册辅助节点之前，您必须使用适当CA证书填充PAN的证书信任列表(CTL)，这些证书用于验证辅助节点的管理员证书。对于不同的场景，填充 PAN 的 CTL 的程序也不同。

- 如果辅助节点使用 CA 签名的证书与管理门户通信，则您必须将辅助节点的 CA 签名证书、相关的中间证书（如果有）和根 CA 证书（属于签署辅助节点证书的 CA）导入到 PAN 的 CTL。
- 如果辅助节点使用自签证书与管理门户通信，则您可以将辅助节点的自签证书导入到 PAN 的 CTL。

注释

- 如果您更改了已注册辅助节点的管理员证书，则您必须获取适当 CA 证书（可用于验证辅助节点的管理员证书）并将其导入到 PAN 的 CTL。
- 当自带设备用户从一个位置移动到另一个位置时，如果您使用自签证书确保部署中客户端与PSN之间的安全通信，EAP-TLS用户身份验证会失败。对于这种必须在某些PSN之间实现的身份验证请求，您必须通过外签 CA 证书或使用外部 CA 签名的通配符证书确保客户端与 PSN 之间的通信。

确保由外部 CA 颁发的证书已经定义了基本约束且 CA 标记设置为 true。要为节点间通信安装 CA 签名证书：

步骤 1 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 78 页

步骤 2 将根证书导入受信任证书库，第 72 页

步骤 3 将 CA 签名的证书与 CSR 绑定，第 78 页

思科 ISE 中的默认受信任证书

Cisco ISE 中的受信任证书库（**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）包含默认可用的一些证书。这些证书会自动导入到库中，以满足安全要求。但是，并非必须使用所有这些证书。除非下表中另有说明，否则您可以使用您选择的证书，而不是已提供的证书。

表 12:

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
Baltimore CyberTrust Root CA	02 00 00 B9	在某些地区，此证书可用作 cisco.com 使用的 CA 链中的根 CA 证书。https://s3.amazonaws.com 上托管的 ISE 2.4 终端安全评估/CP 更新 XML 文件中也使用该证书。	版本 2.4 及更高版本。
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	此证书可用作 cisco.com 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	此证书可用作 cisco.com 和 perfigo.com 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	此证书用作 VeriSign Class 3 Secure Server CA-G3 的根 CA 证书。 在Cisco ISE 中配置 Profiler Feed Service 时，必须使用此证书。	版本 2.4 及更高版本。
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	这是一个中级 CA 证书，于 2020 年 2 月 7 日到期。您不需要更新此证书。 您可以按照以下任务删除证书。	版本 2.4 及更高版本。
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	连接到Cisco ISE 的某些Cisco设备可能使用此证书。默认情况下禁用此证书。	版本 2.4 和 2.6。
Cisco Manufacturing CA SHA2	02	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	连接到Cisco ISE 的某些Cisco设备可使用此证书。默认情况下禁用此证书。	版本 2.4 及更高版本。
Cisco Root CA M2	01	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Cisco服务的受信任证书。	版本 2.4 和 2.6。
QuoVadis Root CA 2	05 09	您必须在分析器、终端安全评估和客户端调配流中使用此证书。	版本 2.4 及更高版本。
Cisco ECC Root CA	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6。
Cisco Licensing Root CA	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco RXC-R2	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco ECC Root CA 2099	03	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。

从思科 ISE 删除默认受信任证书

- 请转至 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 查看您的所有受信任证书。
- 导出要删除的证书并保存，以便在需要时再次导入。

  点击要导出的证书对应的复选框，然后点击上方菜单栏上的**导出 (Export)**。密钥链将下载到您的系统。

- 删除证书。点击要删除的证书对应的复选框，然后点击上方菜单栏上的**删除 (Delete)**。如果任何 CA 链、安全系统日志或安全 LDAP 在使用该证书，则不允许删除它。
- 进行必要的配置更改，从 CA 链、安全系统日志和证书所属的系统日志中移除证书，然后再删除它。
- 删除证书后，检查相关服务（请参阅证书用途）是否如期运行。

证书签名请求

对于证书颁发机构 (CA)，要签发签名证书，您必须创建证书签名请求 (CSR) 并将其提交给 CA。

Certificate Signing Requests 页面会提供您已创建的证书签名请求 (CSR) 的列表。要从证书颁发机构 (CA) 获得签名，您必须导出 CSR，然后将证书发送至 CA。CA 给证书签名，然后返回证书。

您可以从 Admin 门户集中管理证书。您可以为您的部署中的所有节点创建 CSR 并导出这些 CSR。然后，您应该将这些 CSR 提交给 CA，从 CA 获取 CA 签名的证书，将 CA 返回的 root 和中间 CA 证书导入受信任证书库，并且将 CA 签名的证书与 CSR 绑定。

创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构

可以生成证书签名请求 (CSR)，为部署中的节点获取 CA 签名的证书。可以为部署中的选定节点或所有节点生成 CSR。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 输入用于生成 CSR 的值。有关每个字段的信息，请参阅证书签名请求设置。

步骤 3 点击**生成 (Generate)** 以生成 CSR。

系统将生成 CSR。

步骤 4 点击**导出 (Export)** 以在 Notepad 中打开 CSR。

步骤 5 复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的所有文本。

步骤 6 将 CSR 的内容粘贴到选定 CA 的证书请求中。

步骤 7 下载签名证书。

某些 CA 可能会将签名的证书通过邮件发送给您。签名的证书采用 ZIP 文件形式，其中包含必须添加到Cisco ISE 受信任证书存储区的 CA 新颁发证书和公共签名证书。将数字签名的 CA 证书、根 CA 证书和其他中间 CA 证书（如果适用）下载到运行客户端浏览器的本地系统中。

将 CA 签名的证书与 CSR 绑定

在具有由 AC 返回的数字签名证书之后，您必须将其绑定到证书签名请求 (CSR)。您可以从管理门户为部署中的所有节点执行绑定操作。

开始之前

- 您必须具有数字签名的证书，以及由 CA 返回的相关根和中间 CA 证书。
- 将相关的根和中间 CA 证书导入受信任证书存储区（**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

选择您正为其绑定 CSR 与 CA 签名的证书的节点旁边的复选框。

步骤 2 点击**绑定 (Bind)**。

步骤 3 点击**浏览 (Browse)** 选择 CA 签名的证书。

步骤 4 为证书指定“友好名称”(Friendly Name)。

步骤 5 如果您希望Cisco ISE 验证证书扩展，请选中**验证证书扩展 (Validate Certificate Extensions)** 复选框。

如果您启用**验证证书扩展 (Validate Certificate Extensions)** 选项，且您正在导入的证书包含 CA 标志设置为 ture 的基本约束扩展，则请确保存在密钥用法扩展，且已设置 keyEncipherment 位或 akeyAgreement 位。

注释 ISE 要求 EAP-TLS 客户端证书具有数字签名密钥使用扩展。

步骤 6 选中要为其将此证书用于“使用情况”(Usage) 区域的服务。

如果您在生成 CSR 时已启用“使用情况”(Usage) 选项，则此信息会自动填充。 如果您不想在绑定证书时指定用法，请取消选中“使用情况”(Usage) 选项。您可以稍后编辑证书并指定用法。

注释 在主 PAN 上更改管理员角色证书的证书将在所有其他节点上重新启动服务

在主 PAN 上更改管理员角色证书的证书将在所有其他节点上重新启动服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

步骤 7 点击**提交 (Submit)** 以绑定 CA 签名的证书。

如果您已选择将此证书用于Cisco ISE 节点间通信，则Cisco ISE 节点上的应用服务器会重新启动。

要在其他节点上绑定 CSR 与 CA 签名的证书，请重复此流程。

下一步做什么

将根证书导入受信任证书库 ， 第 72 页

导出证书签名请求

您可以使用此页面导出证书签名请求。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 选中想要导出的证书旁边的复选框，点击**导出 (Export)**。

步骤 3 点击**确定 (OK)**，将文件保存到正在运行客户端浏览器的文件系统中。

证书签名请求设置

通过Cisco ISE，只需一个请求即可从管理员门户为部署中的所有节点生成 CSR。此外，还可以选择为部署中的单个节点或多个两个节点生成 CSR。如果选择为单个节点生成 CSR，则 ISE 会自动在证书使用者的 CN= 字段中替换特定节点的完全限定域名 (FQDN)。如果选择在证书的“主体可选名称 (SAN)”(Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE 节点的 FQDN。如果选择为部署中的所有节点生成 CSR，请选中“允许通配符证书”(Allow Wildcard Certificates) 复选框，然后在 SAN 字段（“DNS 名称”(DNS name)）中输入通配符 FQDN 符号，例如，*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个Cisco ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个两个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个Cisco ISE 节点分配唯一服务器证书的安全性低。

下表列出 Certificate Signing Request (CSR) 页面中的字段，可以使用此页面生成可由证书颁发机构 (CA) 签名的 CSR。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书签名请求 (Certificate Signing Request)**。

表 *13:* 证书签名请求设置

字段	使用指南
证书将用于 **(Certificate(s) will be used for)**	

字段	使用指南
	选择即将对其使用证书的服务： **思科 ISE 身份证书** • **多用途 (Multi-Use)**：用于多种服务（管理员、EAP-TLS 身份验证、pxGrid 和门户）。多用途证书同时使用客户端和服务器密钥用法。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **管理 (Admin)** - 用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **EAP 身份验证 (EAP Authentication)**：用于服务器身份验证。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) **注释** EAP-TLS 客户端证书需要使用数字签名密钥。 • **RADIUS DTLS**：用于 RADIUS DTLS 服务器身份验证。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **ISE 消息服务 (ISE Messaging Service)**：用于“经Cisco ISE 消息传递的系统日志”功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **门户 (Portal)**：用于服务器身份验证（以确保与所有 ISE Web 门户之间的

字段	使用指南
	安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **pxGrid** - 同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 注释 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息： `source=local type=fatal message="unsupported certificate"` **思科 ISE 证书颁发机构颁发的证书**

字段	使用指南

	• **ISE 根 CA (ISE Root CA) -**（仅适用于内部 CA 服务）用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。
	• **ISE 中间 CA (ISE Intermediate CA)：**（仅适用于当 ISE 用作外部 PKI 的中间 CA 时的内部 CA 服务）用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成从属 CA 证书。签名 CA 的证书模板通常称为辅助证书颁发机构。此模板具有以下属性：
	  • **基本约束 (Basic Constraints)：**关键、是证书颁发机构
	  • **密钥使用 (Key Usage)：**证书签名、数字签名
	  • **扩展密钥使用 (Extended Key Usage)：**OCSP 签名 (1.3.6.1.5.5.7.3.9)
	• **更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)：**（仅适用于内部 CA 服务）用于更新整个部署的 ISE OCSP 响应方证书（不是证书签名请求）。出于安全原因，建议您每六个月更新一次 ISE OCSP 响应方证书。

允许通配符证书 (Allow Wildcard Certificates)	选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。
为这些节点生成 CSR (Generate CSRs for these Nodes)	选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成CSR，必须取消 Allow Wildcard Certificates 选项。
公共名称 (CN) (Common Name [CN])	默认情况下，公用名是您正为其生成 CSR 的 ISE 节点的 FQDN。$FQDN$ 表示 ISE 节点的 FQDN。当为部署中的多个节点生成 CSR 时，CSR 中的 Common Name 字段会替换为各个 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。

字段	使用指南
主体可选名称 (SAN) (Subject Alternative Name [SAN])	“IP 地址”(IP address)、“DNS 名称”(DNS name)、“统一资源标识符”(Uniform Resource Identifier, URI) 或与证书关联的“目录名称”(Directory Name)。 • **DNS 名称 (DNS name)**：如果选择“DNS 名称”(DNS name)，请输入 ISE 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项，请指定通配符符号（域名前的星号和句号）。例如：*.amer.example.com。 • **IP 地址 (IP address)**：将与证书关联的 ISE 节点的 IP 地址。 • **统一资源标识符 (Uniform Resource Identifier)**：您希望与证书关联的 URI。 • **目录名称 (Directory Name)**：根据 RFC 2253 定义的可区分名称 (DN) 的字符串表示。使用逗号 (,) 隔开多个 DN。对于“dnQualifier”RDN，避免使用逗号而是使用反斜杠“\”作为分隔符。例如，CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。
密钥长度 (Key Length)	指定公共密钥的位大小。 以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 **注释** 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果计划获取公共的 CA 签名证书，请选择 2048 或更大长度。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。

相关主题

证书签名请求，第 78 页
创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 78 页
将 CA 签名的证书与 CSR 绑定，第 78 页

设置供门户使用的证书

由于部署中有多个策略服务节点 (PSN) 可以支持 Web 门户请求，所以Cisco ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时，您必须定义证书组标签并将其与您的部署中各个节点上的对应证书关联。您必须将此证书组标签与对应的最终用户门户关联（访客、发起人和个人设备门户）。此证书组标签是一种唯一标识符，帮助Cisco ISE 标识与这每一个门户通信时必须使用的证书。您可以从每个节点为每个门户指定一个证书。

注释 思科 ISE 在 TCP 端口 8443（或者您为使用门户而配置的端口）上提供门户证书。

步骤 1 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 78 页。

您必须选择您已定义的证书组标签或为门户创建一个新证书组标签。例如 mydevicesportal。

步骤 2 将根证书导入受信任证书库，第 72 页。

步骤 3 将 CA 签名的证书与 CSR 绑定，第 78 页。

将默认门户证书组标签重新分配给 CA 签名的证书

默认情况下，所有Cisco ISE 门户使用自签证书。如果您要对门户使用 CA 签名的证书，您可以将默认门户证书组标签分配至 CA 签名的证书。您可以使用现有的 CA 签名证书或生成 CSR，并获取新的 CA 签名证书以供门户使用。您可以重新将任何门户组标签从一个证书分配到另一个证书。

注释 当您编辑现有的证书时，如果与证书关联的门户标签 (guest) 已被任意一个门户使用，则您无法将默认门户证书组标签或任何其他门户组标签重新分配到此证书。系统将列出使用“guest”门户标签的门户。

以下程序介绍了如何将默认门户证书组标签重新分配至 CA 签名的证书。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

将鼠标悬停在默认门户证书组标签旁边的i图标上，以查看使用此标签门户的列表。您还可以查看部署中具有已向其重新分配此标签的门户证书的 ISE 节点。

步骤 2 选中要用于门户的 CA 签名证书旁边的复选框，然后点击**编辑 (Edit)**。

请务必选择一个未被任何门户使用的 CA 签名证书。

步骤 3 在**使用情况 (Usage)** 区域，选中**门户 (Portal)** 复选框，然后选择“默认门户证书组标签”(Default Portal Certificate Group Tag)。

步骤 4 点击**保存 (Save)**。

系统将显示一条警告消息。

步骤 5 点击**是 (Yes)** 将默认门户证书组标签重新分配至 CA 签名的证书。

注册节点之前关联门户证书标签

如果您在注册新 ISE 节点之前对部署中的所有门户都使用“Default Portal Certificate Group”标签，请确保导入相关的 CA 签名证书，选择“Portal”作为服务，然后将“Default Portal Certificate Group”标签与此证书相关联。

向部署中添加新节点时，默认自签名证书与“Default Portal Certificate Group”标签相关联，并且门户配置为使用此标签。

注册新节点后，您无法更改 Certificate Group 标签关联。因此，在将节点注册到部署之前，您必须执行以下操作：

步骤 1 创建自签名证书，选择“Portal”作为服务，然后分配其他证书组标签（例如，tempportaltag）。

步骤 2 更改门户配置以使用新创建的证书组标签 (tempportaltag)。

步骤 3 编辑默认自签名证书并删除 Portal 角色。

此选项可删除与默认自签名证书的 Default Portal Certificate Group 标签关联。

步骤 4 执行以下操作之一：

选项	说明
生成 CSR	当生成 CSR 时： **1.** 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。 **2.** 将 CSR 发送到 CA 并获取签名证书。 **3.** 导入已将您的证书签入到受信任证书库中的 CA 的根证书和任何其他中间证书。 **4.** 将 CA 签名证书与 CSR 绑定。
导入私钥和 CA 签名证书	当导入 CA 签名证书时： **1.** 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。 **2.** 导入已将您的证书签入到受信任证书库中的 CA 的根证书和任何其他中间证书。

选项	说明
编辑现有 CA 签名证书。	当编辑现有 CA 签名证书时： 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。

步骤 5 将 ISE 节点注册到部署
部署中的门户配置会配置到“Default Portal Certificate Group”标签，并且门户配置为在新节点上使用与“Default Portal Certificate Group”标签关联的 CA 签名证书。

用户和终端证书续订

默认情况下，Cisco ISE 拒绝来自证书已过期设备的请求。但是，您可以更改此默认行为并配置 ISE 以满足这些请求并提示用户更新证书。

如果选择允许用户更新证书，Cisco建议您配置一个授权策略规则，检查在进一步处理请求之前证书是否已续签。处理来自证书过期设备的请求可能导致潜在的安全威胁。因此，必须配置正确的授权配置文件和规则来确保贵公司的安全不受影响。

在证书到期前或到期后，有些设备支持证书续订。但是在 Windows 设备上，您只能在证书到期前续订证书。Apple iOS、Mac OSX 和 Android 设备支持在证书到期前或到期后，进行证书续订。

策略条件中用于证书续订的字典属性

Cisco ISE 证书字典包含在策略条件中用于允许用户续订证书的以下属性：

- Days to Expiry：此属性规定证书有效的天数。您可以使用此属性创建可用于授权策略的条件。此属性可采用 0 至 15 之间的值。值 0 表示证书已过期。值 1 表示证书不到 1 天就要到期。
- Is Expired：此布尔属性表示证书是否已到期。如果想要只允许在证书接近到期时而不是在证书已到期之后续订证书，请在授权策略条件中使用此属性。

证书续订的授权策略条件

您可以使用授权策略中的CertRenewalRequired简单条件（默认情况下可用）以确保在Cisco ISE进一步处理请求之前更新证书（已到期或即将到期）。

用于续订证书的 CWA 重定向

如果用户证书在证书到期前已被吊销，则Cisco ISE会检查CA发布的CRL并拒绝身份验证请求。如果被撤消的证书已过期，则CA不得在其CRL中发布此证书。在此场景中，Cisco ISE可更新被撤消的证书。要避免此问题，在更新证书之前，请确保请求重新定向到集中式 Web 身份验证 (CWA) 以进行完整的身份验证。必须创建授权配置文件才能重定向用户以进行 CWA。

将思科 ISE 配置为允许用户续订证书

您必须完成此程序中列出的任务，才能将Cisco ISE 配置为允许用户续订证书。

开始之前

在 WLC 上配置受限访问 ACL 以重定向 CWA 请求。

步骤 1 更新允许的协议配置， 第 89 页
步骤 2 为 CWA 重定向创建授权策略配置文件， 第 89 页
步骤 3 创建授权策略规则以更新证书， 第 90 页
步骤 4 在访客门户中启用 BYOD 设置， 第 91 页

更新允许的协议配置

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)** > **默认网络访问 (Default Network Access)**。

步骤 2 选中 EAP-TLS 协议以及 PEAP 和 EAP-FAST 协议的 EAP-TLS 内部方法下的 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** 复选框。

使用 EAP-TLS 协议的请求将通过 NSP 流。

对于 PEAP 和 EAP-FAST 协议，必须手动配置Cisco AnyConnect，使Cisco ISE 处理请求。

步骤 3 点击**提交 (Submit)**。

下一步做什么

为 CWA 重定向创建授权策略配置文件， 第 89 页

为 CWA 重定向创建授权策略配置文件

开始之前

确保您已在 WLC 上配置受限访问 ACL。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为授权配置文件输入名称。例如 CertRenewal_CWA。

步骤 4 在“常见任务”(Common Tasks) 区域，选中 **Web 重定向（CWA、DRW、MDM、NSP、CPP）(Web Redirection (CWA, DRW, MDM, NSP, CPP))** 复选框。

步骤 5 从下拉列表和受限访问 ACL 选择**集中式 Web 身份验证 (Centralized Web Auth)**。

步骤 6 选中**显示证书续订消息 (Display Certificates Renewal Message)** 复选框。

URL-redirect 属性值改变并且包含证书有效的天数。

步骤 7 点击**提交 (Submit)**。

注释 如果您为思科 ISE 1.2 中的无线设备配置了以下设备注册 Web 身份验证 (DRW) 策略：

- DRW-Redirect policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-drw-redirect
- DRW-Allow policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-Permit

在升级到 ISE 1.3 或更高版本后，您必须如下更新 DRW-Allow 策略条件：

- Condition = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) and Profile = Wireless-Permit

---

下一步做什么

创建授权策略规则以更新证书，第 90 页

创建授权策略规则以更新证书

开始之前

确保您已创建集中式 Web 身份验证重定向的授权配置文件。

在以下位置启用策略集 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **策略设置 (Policy Settings)**。

步骤 1 选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略集 (Policy Sets)**。

步骤 2 点击**创建于…之上 (Create Above)**。

步骤 3 输入新规则的名称。

步骤 4 选择以下简单条件和结果：

如果 CertRenewalRequired 等于 True，则为权限选择先前创建的授权配置文件 (CertRenewal_CWA)。

步骤 5 点击**保存 (Save)**。

下一步做什么

当使用其证书已到期的设备访问公司网络时，请点击**续订 (Renew)** 重新配置设备。

在访客门户中启用 BYOD 设置

要使用户能够更新个人设备证书，必须在所选访客门户中启用 BYOD 设置。

步骤 1 依次选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)**。

a) 选择所选 CWA 门户并点击**编辑 (Edit)**。

步骤 2 从 BYOD 设置中，选中**允许员工在网络上使用个人设备 (Allow employees to use personal devices on the network)** 复选框。

步骤 3 点击**保存 (Save)**。

Apple iOS 设备的证书续订失败

当您使用 ISE 在 Apple iOS 设备上续订终端证书时，您可能会遇到“Profiled Failed to Install”错误消息。如果在相同策略服务节点 (PSN) 或另一个 PSN 上，与处理续订所使用的证书不同的管理员 HTTPS 证书已签名要过期或已过期的网络配置文件，则系统会显示此错误消息。

作为一个解决方案，请为部署中的所有 PSN 上的管理员 HTTPS 使用多域 SSL 证书（通常称为统一通信证书 [UCC]）或通配符证书。

证书定期检查设置

Cisco ISE 定期检查证书撤销列表 (CRL)。使用此页面，您可以对Cisco ISE 进行配置以对照自动下载的 CRL 检查正在进行的会话。您可以指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间和Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 OCSP 服务器或 CRL 进行检查。

下表列出“证书定期检查设置”(Certificate Periodic Check Settings) 窗口中的字段，可以使用该窗口来指定检查证书（OCSP 或 CRL）状态时的时间间隔。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书定期检查设置 (Certificate Periodic Check Settings)**。

表 *14:* 证书定期检查设置

字段名称	使用指南
证书检查设置	

字段名称	使用指南
“对照自动撤销的 CRL 检查正在进行的会话”(Check ongoing sessions against automatically retrieved CRL)	如果您希望Cisco ISE 对照自动下载的 CRL 检查正在进行的会话，选中此复选框。
CRL/OCSP 定期检查证书	
首先检查	指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间。输入 00:00 和 23:59 小时之间的数值
检查每	指定Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 CRL 或 OCSP 服务器进行检查。

相关主题

OCSP 服务，第 124 页
添加 OCSP 客户端配置文件，第 126 页

思科 ISE CA 服务

证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。思科 ISE 内部证书颁发机构 (ISE CA) 从集中控制台为终端颁发和管理数字证书，以允许员工在公司网络上使用其个人设备。CA 签名的数字证书被视为行业标准而且更安全。主 PAN 为根 CA。策略服务节点 (PSN) 是主 PAN 的从属 CA (SCEP RA)。ISE CA 提供以下功能：

- 颁发证书：为连接您的网络的终端验证和签发证书签名请求 (CSR)。
- 密钥管理：在 PAN 和 PSN 节点上生成并安全地存储密钥和证书。
- 存储证书：存储向用户和设备颁发的证书。
- 支持在线证书状态协议 (OCSP)：提供 OCSP 响应器以检查证书的有效性。

当 CA 服务在主管理节点上禁用时，CA 服务仍被视为在辅助管理节点的 CLI 上运行。理想情况下，CA 服务应被视为禁用。此为已知的Cisco ISE 问题。

思科 ISE 证书指纹

证书指纹识别过程用于评估证书即时颁发者指纹 SHA256 以与受信任证书匹配。这将为多个 CA 实施安全机制，以支持不同的域，并允许锁定 802.1x 协议的受信任 CA。

确保在更新策略条件中的证书之前，将颁发者-指纹 SHA-256 证书添加到Cisco ISE 部署。

注释 为受信任证书配置策略后，无法删除该证书。以下消息显示在**受信任证书 (Trusted Certificates)** 窗口中的**此受信任证书由策略集引用 (This Trusted Certificate Refered by Policy Sets)** 部分中。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**：

无法删除证书，因为正在策略中使用它。要删除证书，请先修改策略条件。

要为Cisco ISE 配置证书指纹，请按照顺序执行以下步骤：

1. 创建内部用户。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“资产可视性”一章中的“添加用户”部分。
2. 添加网络设备。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“基本设置”一章中的“在Cisco ISE 中添加网络设备”部分。
3. 在外部证书中导入外部CA。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“基本设置”一章中的“导入系统证书”部分。

   您还可以使用SCEP协议导入颁发者-指纹SHA-256证书。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **外部 CA 设置 (External CA Settings)**。在显示的**添加 SCEP RA 配置文件 (Add SCEP RA Profile)** 窗口中，点击**添加 (Add)**。在**名称 (Name)** 字段中，输入证书名称。在 **URL** 字段中输入 CA 服务器 URL。点击**测试连接 (Test Connection)**。
4. 使用 SHA-256 指纹创建策略
5. 使用 SHA-256 指纹创建并映射身份验证策略
6. 创建授权策略。
7. 验证 PRRT 日志

使用 SHA-256 指纹创建策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Set)**。

步骤 2 在显示的**策略集 (Policy Set)** 窗口中，点击**设置 (Settings)**，然后从下拉列表中选择**插入新行 (insert a new row)**。

步骤 3 在**新策略名称 (New Policy Name)** 字段中输入名称。

步骤 4 输入策略的**说明**。

步骤 5 点击**条件 (Conditions)** 列下新**策略集名称 (Policy Set Name)** 旁边的**添加 (Add)** (+) 图标。

步骤 6 在显示的**条件 Studio (Condition Studio)** 窗口中，点击**点击以添加属性 (Click to Add Attribute)** 字段。

步骤 7 从**所有字典 (All dictionary)** 下拉列表中选择**网络访问-协议 (Network Access-Protocol)**（**字典-属性 (Dictionary-Attribute**）组合。

步骤 8 选择 **Equals** 运算符以构建逻辑条件。

步骤 9 从**从列表或类型中选择 (Choose from List or Type)** 下拉列表中选择 **RADIUS**。

步骤 10 点击**使用 (Use)**。

步骤 11 在显示的**策略集 (Policy Set)** 窗口中，从**允许的协议/服务器序列 (Allowed Protocols/Server Sequence)** 下拉列表中选择**默认网络访问 (Default Network Access)**。

步骤 12 点击**保存 (Save)**。

使用 SHA-256 指纹创建并映射身份验证策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Set)** > **默认值 (Default)**。

步骤 2 点击**身份验证策略 (Authentication Policy)**。

步骤 3 点击设置图标并选择**插入新行 (insert a new row)**。

步骤 4 在**身份验证规则名称 (Authentication Rule Name)**窗口中，输入名称。

步骤 5 点击规则名称旁的**添加 (Add)** 图标 (+)。

步骤 6 在显示的 **Condition Studio** 窗口中，点击**点击以添加属性 (Click to add Attributes)** 字段。

步骤 7 从**所有字典 (All Dictionary)** 下拉列表中，选择 **CERTIFICATE-Issuer- Fingerprint SHA-256** (**Dictionary-Attribute**) 组合。

步骤 8 选择**等于 (Equals)** 运算符以构建逻辑条件。

步骤 9 从**从列表或类型中选择 (Choose from List or Type)** 下拉列表中，选择**思科制造 SHA2 指纹 sha256CA (Cisco Manufacturing CA SHA2 fingerprint sha256)**。

步骤 10 点击**使用 (Use)**。

步骤 11 在显示的**策略集 (Policy Set)** 窗口中，从**允许的协议/服务器序列 (Allowed Protocols/Server Sequence)** 下拉列表中，选择 **Preloaded_Certificate_Profile**。

步骤 12 点击**保存 (Save)**。

创建授权策略

步骤 1 选择 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Set)** > **默认值 (Default)**。

步骤 2 点击**授权策略 (Authorization Policy)**。

步骤 3 点击设置图标，然后从下拉列表中选择**插入新行 (insert a new row)**。

步骤 4 在**授权规则名称 (Authorization Rule Name)** 窗口中，输入名称。

步骤 5 点击规则名称旁的**添加 (Add)** 图标 (+) 图标。

步骤 6 在显示的 **Condition Studio** 窗口中，点击**点击以添加属性 (Click to Add Attributes)** 字段。

步骤 7 从**所有字典 (All Dictionary)** 下拉列表中，选择 **CERTIFICATE-Issuer- Fingerprint SHA-256** (**Dictionary-Attribute**) 组合。

步骤 8 选择**等于 (Equals)** 运算符以构建逻辑条件。

步骤 9 从从列表或类型中选择 **(Choose from List or Type)** 下拉列表中，选择思科根 CA 2099 指纹 sha **(Cisco Root CA 2099 fingerprint sha)**。

步骤 10 点击使用 **(Use)**。

步骤 11 在显示的策略集 **(Policy Set)** 窗口中，从允许的协议/服务器序列 **(Allowed Protocols/Server Sequence)** 下拉列表中选择 **PermitAccess**。

步骤 12 点击保存 **(Save)**。

验证 PRRT 日志

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 操作 **(Operations)** > **RADIUS** > 实时日志 **(Live logs)**。

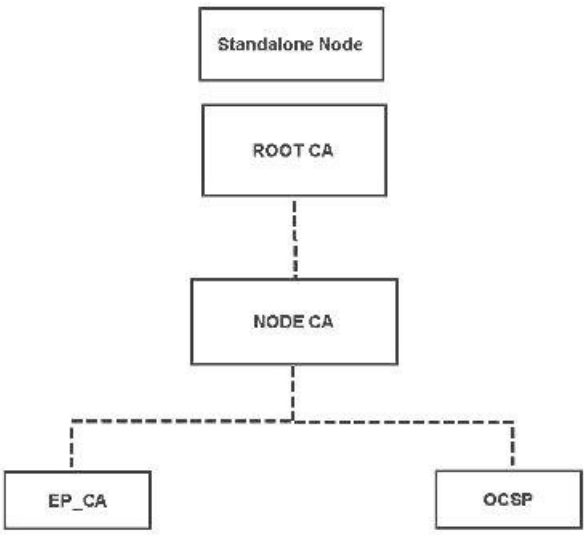
步骤 2 在显示的实时日志 **(Live Logs)** 窗口中，点击最新的日志详细信息。

步骤 3 在显示的身份验证详细信息 **(Authentication Details)** 窗口中，查看 **Issuer- Fingerprint SHA-256** 列中的 SHA-256 值，确认已成功添加并验证 **Issuer- Fingerprint SHA-256** 证书。

管理和策略服务节点上调配的 ISE CA 证书

安装Cisco ISE 节点后，系统会为它调配 CA 根证书和节点 CA 证书，以便为终端管理证书。

图 *6:* 在独立节点上调配 *ISE CA* 证书

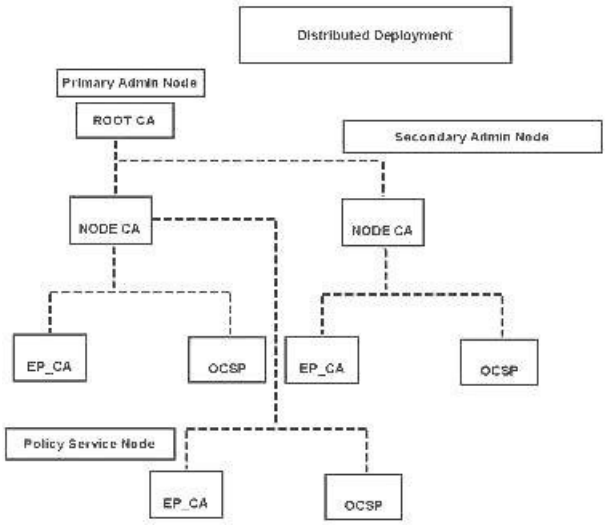


当您建立部署时，您指定为主管理节点 (PAN) 的节点将成为根 CA。PAN 具有一个根 CA 证书和一个由根 CA 签名的节点 CA 证书。

当您登记辅助管理节点至 PAN 时，会生成节点 CA 证书，并由主要管理节点的根 CA 签名。

系统将为您在 PAN 登记的所有策略服务节点 (PSN) 调配一个终端 CA 和一个由 PAN 的节点 CA 签名的 OCSP 证书。策略服务节点 (PSN) 是 PAN 的从属 CA。当您使用 ISE CA 时，PAN 上的终端 CA 颁发证书给访问您网络的终端。

图 *7:* 部署中管理和策略服务节点上调配的 ***ISE CA*** 证书



CA 与思科 ISE 实现互通性的要求

在 CA 服务器中使用Cisco ISE 时，请确保满足以下要求：

- 密钥大小应为 1024、2048 或更高。在 CA 服务器中，密钥大小使用证书模板定义。您可以使用请求方配置文件在Cisco ISE 上定义密钥大小。
- 密钥使用应允许在扩展中应用签名和加密。
- 通过 SCEP 协议使用 GetCACapabilities 时，应支持加密算法和请求散列。建议使用 RSA 和 SHA1。
- 支持在线证书状态协议 (OCSP)。虽然这在自带设备 (BYOD) 中并不会直接使用，但是可以使用能充当 OCSP 服务器的 CA 来撤销证书。

注释 Cisco ISE 支持使用企业 Java Beans 证书颁发机构 (EJBCA) 进行标准 EAP 身份验证（例如 PEAP、EAP-TLS 等）。您必须禁用 EJBCA 中的**启用终端实体配置文件限制 (Enable End Entity Profile Limitations)** 选项（在**系统 (System) > 基本配置 (Basic Configurations)** 下）才能启用对代理 SCEP 的 EJBCA 支持。

- 如果您使用企业 PKI 为 Apple iOS 设备颁发证书，请务必在 SCEP 模板中配置密钥用法并启用**密钥加密 (Key Encipherment)** 选项。

如果您使用 Microsoft CA，请在证书模板中编辑“密钥用法扩展”(Key Usage Extension)。在**加密 (Encryption)** 区域中，点击**只在密钥加密时允许密钥交换（密钥加密）(Allow Key Exchange only with Key Encryption (Key encipherment))** 单选按钮，并选中**允许对用户数据加密 (Allow encryption of user data)** 复选框。

- Cisco ISE 支持为信任证书和终端证书使用 RSASSA-PSS 算法，以进行 EAP-TLS 身份验证。查看证书时，签名算法以 1.2.840.113549.1.1.10 形式列出，而非算法名称。

注释 如果您对自带设备流量使用Cisco ISE 内部 CA，则不应使用 RSASSA-PSS 算法（由外部 CA 签名）对管理员证书签名。Cisco ISE 内部 CA 无法验证使用此算法签名的管理员证书，请求将会失败。

基于证书的身份验证对客户端证书的要求

要在Cisco ISE 上进行基于证书的身份验证，客户端证书应满足以下要求：

表 *15: RSA* 和 *ECC* 的客户端证书要求

RSA		
支持的密钥大小	1024、2048 和 4096 位	
支持的安全散列算法 (SHA)	SHA-1 和 SHA-2（包括 SHA-256）	
ECC [12]		
支持的曲线类型	P-192、P-256、P-384 和 P-521	
支持的安全散列算法 (SHA)	SHA-256	
客户端计算机操作系统和支持的曲线类型		
Windows	8 及更高版本	P-256、P-384 和 P-521
Android	4.4 及更高版本 **注释** Android 6.0 需要 2016 年 5 月的补丁以支持 ECC 证书。	所有曲线类型（Android v6.0 除外，它不支持 P-192 曲线类型）。

[1] Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。
[2] 此思科 ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

重新生成 ISE CA 链

当您重新生成Cisco ISE CA 链时，会重新生成所有证书，包括根 CA、节点 CA 和终端 CA 证书。更改 PAN 或 PSN 的域名或主机名时，必须重新生成 ISE CA 链。从较早版本升级到版本 2.0 或更高版本时，我们建议您重新生成 ISE CA 链，以便从两个根层次结构转变为单个根层次结构。

重新生成系统证书时，无论是根 CA 证书还是中间 CA 证书，ISE 消息服务都会重新启动以加载新的证书链。在 ISE 消息服务再次可用之前，审核日志将丢失。

注释 无论何时在部署中更换思科 ISE 内部 CA，到时都必须刷新 ISE 消息服务以检索完整的证书链。

重新生成思科 ISE 内部 CA 链时，链中所有证书的**有效期自 (Valid From)** 字段将显示重新生成日期前一天的日期。

省略曲线加密证书支持

Cisco ISE CA 服务支持基于忽略曲线加密 (ECC) 算法的证书。与其他加密算法相比，ECC 提供的安全性和性能更高，即使使用更小的密钥大小也是如此。

下表比较了 ECC 和 RSA 的密钥大小以及安全强度。

ECC 密钥大小（位）	**RSA 密钥大小（位）**
160	1024
224	2048
256	3072
384	7680
521	15360

由于密钥大小较小，加密速度更快。

Cisco ISE 支持以下 ECC 曲线类型。曲线类型越高，密钥规模越大，安全性就越强。

- P-192
- P-256
- P-384
- P-521

ISE 不支持证书中 EC 部分的显式参数。如果尝试导入具有显式参数的证书，将显示以下错误：“证书验证失败: 仅支持命名的 EC 参数”(Validation of certificate failed: Only named ECParameters supported)。

对于通过自有设备流量连接的设备， Cisco ISE CA 服务支持 ECC 证书。您也可以从以证书调配门户生成 ECC 证书。

注释 下表列出了支持ECC的操作系统和版本以及支持的曲线类型。如果设备未在受支持的操作系统或受支持的版本上运行，可以使用基于 RSA 的证书代替。

操作系统 (Operating System)	支持的版本 (Supported Versions)	支持的曲线类型 (Supported Curve Types)
Windows	8 及更高版本	P-256、P-384 和 P-521
Android	4.4 及更高版本 注释 Android 6.0 需安装 2016 年 5 月补丁才能支持 ECC 证书。	所有曲线类型（Android 6.0 除外，它不支持 P-192 曲线类型）。

Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。此Cisco ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

如果使用了 Enrollment over Secure Transport (EST) 协议的自带设备流量未正常工作，请检查以下项：

- 证书服务终端子 CA 证书链完整。要检查证书链是否完整，请执行以下操作：
  1. 选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**。
  2. 选中要检查的证书旁边的复选框，然后点击**查看 (View)**。
- 确保 CA 和 EST 服务正常运行。如果服务未运行，请转至**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 内部 CA 设置 (Internal CA Settings)** 启用 CA 服务。
- 如果您已将低于 2.0 版本的 ISE 升级到Cisco ISE 2.1，请在升级后替换 ISE CA 根证书链。为此：
  1. 选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书管理 (Certificate Management) > 证书颁发签名请求 (Certificate Signing Requests)**。
  2. 点击**生成证书签名请求 (Generate Certificate Signing Requests)**。
  3. 从一个或多个**证书将用于 (Certificates will be used for)** 下拉列表中选择“ISE 根 CA”(ISE Root CA)。
  4. 点击**替换 ISE CA 根证书链 (Replace ISE Root CA Certificate chain)**。

注释 此版本的思科 ISE 不支持 EST 客户端直接根据思科 ISE 内部的 EST 服务器进行身份验证。

在 Android 或 Windows 终端上登录时，如果该请求用于基于 ECC 的证书，则 ISE 将触发 EST 流。

思科 ISE 证书颁发机构证书

“证书颁发机构 (CA) 证书”(Certificate Authority (CA) Certificates) 页面列出了与内部Cisco ISE CA 相关的所有证书。在以前的版本中，这些 CA 证书存在于受信任证书存储中，现在已移至“CA 证书”(CA Certificates) 页面。此页面按节点列出这些证书。可以展开某个节点以查看该特定节点的所有 ISE CA 证书。主要和辅助管理节点具有根 CA、节点 CA、从属 CA 和 OCSP 响应器证书。部署中的其他节点具有终端从属 CA 和 OCSP 证书。

启用Cisco ISE CA 服务时，将在所有节点上自动生成和安装这些证书。此外，在替换整个 ISE 根 CA 链时，将在所有节点上自动重新生成和安装这些证书。不需要手动干预。

Cisco ISE CA 证书遵循以下命名约定：**证书服务 <终端从属 *CA*/节点 *CA*/根 *CA/OCSP* 响应器>-**<节点主机名>**#**证书编号。

在“CA 证书”(CA Certificates) 页面中，可以编辑、导入、导出、删除和查看Cisco ISE CA 证书。

编辑思科 ISE CA 证书

在添加证书到Cisco ISE CA 证书存储区之后，可以采用编辑设置对其进行进一步编辑。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

步骤 3 选中要编辑的证书旁边的复选框，然后点击**编辑 (Edit)**。

步骤 4 根据需要修改可编辑字段。有关字段的说明，请参阅编辑证书设置。

步骤 5 点击**保存 (Save)** 以保存对证书库所做的更改。

导出思科 ISE CA 证书

要导出Cisco ISE 根 CA 和节点 CA 证书：

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

步骤 3 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

步骤 4 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

导入思科 ISE CA 证书

如果终端尝试使用来自其他部署的Cisco ISE 颁发的证书对您的网络进行身份验证，您必须将来自该部署的Cisco ISE 根 CA 证书、节点 CA 证书和终端从属 CA 证书导入到Cisco ISE 受信任证书存储区。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 将 ISE 根 CA 证书、节点 CA 证书和终端从属 CA 证书从终端证书签名的部署中导出，并将其存储在浏览器运行所在的计算机的文件系统。

步骤 1 登录到终端正从其获得身份认证的部署的管理门员户。

步骤 2 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 3

步骤 4 点击**导入 (Import)**。

步骤 5 如有必要，配置这些字段值。有关详细信息，请参阅受信任证书导入设置。

如果启用基于证书的客户端身份验证，则Cisco ISE 将重新启动您的部署中每个节点上的应用服务器，从 PAN 上的应用服务器开始，然后依次是其他各个节点。

证书模板

证书模板包含证书颁发机构 (CA) 基于该模板颁发的所有证书通用的属性。证书模板定义了主题、主题备选名称 (SAN)、密钥类型、密钥大小、必须使用的 SCEP RA 配置文件、证书的有效期以及扩展密钥用法 (EKU)（指定必须将证书用于客户端身份验证、服务器身份验证，还是用于两者）。内部 Cisco ISE CA (ISE CA) 使用证书模板颁发基于该模板的证书。

Cisco ISE 为 ISE CA 提供了以下默认证书模板。如果需要，您可以创建其他证书模板。默认证书模板如下：

- CA_SERVICE_Certificate_Template - 用于使用Cisco ISE 作为证书颁发机构的其他网络服务。例如，在配置给 ASA VPN 用户颁发证书的 ISE 时使用此证书模板。您仅可在此证书模板中修改有效期。
- EAP_Authentication_Certificate_Template - 用于 EAP 身份验证。
- pxGrid_Certificate_Template - 用于从证书调配门户生成证书时的 pxGrid 控制器。

证书模板扩展名

Cisco ISE 内部 CA 包含一个扩展名，表示用于创建终端证书的证书模板。由内部 CA 颁发的所有终端证书都包含证书模板扩展名。此扩展名表示用于创建该终端证书的证书模板。扩展 ID 为 1.3.6.1.4.1.9.21.2.5。您可以在授权策略条件中使用 CERTIFICATE: Template Name 属性，并根据评估结果分配相应的访问权限。

在授权策略条件中使用证书模板

您可以在授权策略规则中使用证书模板名称扩展名。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开“默认策略集”(Default policy set) 以查看授权策略规则。

步骤 2 添加新规则或编辑现有规则。此示例对编辑 Compliant_Device_Access 规则描述如下：

a) 编辑 Compliant_Device_Access 规则

b) 选择**添加属性/值 (Add Attribute/Value)**。

c) 从字典选择**证书：模板名称 (CERTIFICATE: Template Name)** 属性和**等于 (Equals)** 运算符。

d) 输入证书模板名称值。例如，EAP_Authentication_Certificate_Template。

步骤 3 点击**保存 (Save)**。

为 pxGrid 控制器部署思科 ISE CA 证书

Cisco ISE CA 为 pxGrid 控制器提供一个证书模板，用于从证书调配门户生成证书。

开始之前

为 pxGrid 客户端生成证书签名请求 (CSR) 并复制 CSR 的内容到剪贴板。

步骤 1 创建网络访问用户帐户（通过“管理”(Administration) >“身份管理” (Identity Management) >“身份”(Identities) >“用户” (Users) >“添加”(Add)）。

记录用户分配到的用户组。

步骤 2 修改证书调配门户设置（通过“管理”(Administration) >“设备门户管理” (Device Portal Management) >“证书调配”(Certificate Provisioning)）。

a) 选择证书调配门户，然后点击**编辑 (Edit)**。

b) 点击**门户设置 (Portal Settings)** 下拉列表。从“配置授权组可用列表”(Configure authorized groups Available list)，选择网络访问用户所属的用户组并将其移至选定的列表。

c) 点击**证书调配门户设置 (Certificate Provisioning Portal Settings)** 下拉列表。选择 pxGrid_Certificate_Template。有关详细信息，请参阅证书调配门户的门户设置。

d) 保存门户设置。

步骤 3 启动“证书调配门户”(Certificate Provisioning Portal)。点击“门户测试 URL”(Portal test URL) 链接。

a) 使用在步骤 1 中创建的用户帐户登录证书调配门户。

b) 接受 AUP，然后点击**继续 (Continue)**。
c) 从**我想 (I want to)**下拉列表中，选择**生成单个证书（通过证书签名请求）(Generate a single certificate (with certificate signing request))**。
d) 在“证书签名请求详细信息”(Certificate Signing Request Details) 字段，从剪贴板粘贴 CSR 的内容。
e) 从**证书下载格式 (Certificate Download Format)** 下拉列表中，选择 **PKCS8 格式 (PKCS8 format)**。

注释 如果您选择PKCS12格式，则必须将单个证书文件转换为单独的证书和密钥文件。证书和密钥文件必须为二进制 DER 编码的或 PEM 格式，才能将其导入Cisco ISE。

f) 从**选择证书模板 (Choose Certificate Template)** 下拉列表中，选择 **pxGrid_Certificate_Template**。
g) 输入证书密码。
h) 点击**生成 (Generate)**。

系统将生成证书。

i) 导出证书

系统会将证书连同证书链一起导出。

步骤 4 将Cisco ISE CA 链导入至 pxGrid 客户端中受信任的证书存储库中。

简单证书注册协议配置文件

为了帮助为用户可在网络上注册的各类移动设备启用证书调配功能，Cisco ISE 允许您配置一个或多个简单证书注册协议 (SCEP) 证书颁发机构 (CA) 配置文件（称为Cisco ISE 外部 CA 设置），从而使Cisco ISE指向多个CA位置。允许多个配置文件的优点在于，可帮助确保高可用性并在您指定的CA位置执行负载均衡。如果对特定的 SCEP CA 请求连续三次未获得应答，则Cisco ISE 会声明该特定服务器不可用，并会自动移至下一个具有已知最低负载和最少响应次数的CA，然后即会开始进行定期轮询直至服务器恢复联机。

关于如何设置 Microsoft SCEP 服务器与Cisco ISE 互操作的详细信息，请参阅

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf。

已颁发的证书

管理门户列出了内部 ISE CA 颁发给终端的所有证书（“管理”(Administration) > “系统”(System) > “证书”(Certificates) > “终端证书”(Endpoint Certificates)）。已颁发的证书 (Issued Certificates) 页面提供证书状态概览。如果证书已被吊销，可以将鼠标悬停在 Status 列上找出吊销原因。您可以将鼠标悬停在“证书模板”(Certificate Template) 列上查看更多详细信息，如证书的密钥类型、密钥大小或曲线类型、主题、主题备选名称 (SAN) 和有效期。可以点击终端证书来查看证书。

“终端证书”(Endpoint Certificates) 页面列有 ISE CA 颁发的所有证书（通过自带设备流程自动调配证书并从证书调配门户获得证书）。您可以在此页面管理这些证书。

例如，如果要查看颁发给 user7 的证书，请在出现在 Friendly Name 字段下方的文本框中输入 user7。系统会显示Cisco ISE 颁发给此用户的所有证书。从文本框中删除搜索条件可取消筛选。还可以根据各种搜索条件，使用 Advanced Filter 选项查看记录。

此 Endpoint Certificates 页面还为您提供用于在必要时撤销终端证书的选项。

Certificate Management Overview 页面显示部署中每个 PSN 节点颁发的终端证书的总数。还可以查看每个节点的被吊销证书的总数，以及已失败的证书的总数。可以根据任意属性筛选此页面上的数据。

颁发及撤销的证书

下表介绍颁发及撤销的证书概述 页面中的字段。您的部署中的PSN节点会向终端发出证书。此页面向您提供关于您的部署中每个PSN节点发出的终端证书的信息。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **概述 (Overview)**。

表 *16:* 颁发及撤销的证书

字段	使用指南
Node name	发出证书的策略服务节点 (PSN) 的名称。
颁发的证书 (Certificates Issued)	PSN 节点发出的终端证书的数量。
撤销的证书 (Certificates Revoked)	已吊销的证书的数量（已由 PSN 节点发出的证书）。
证书请求 (Certificates Requests)	PSN 节点处理的基于证书的身份验证请求数量。
失败的证书 (Certificates Failed)	PSN 节点处理的失败身份验证请求数量。

相关主题

已颁发的证书，第 103 页
用户和终端证书续订，第 88 页
配置思科 ISE 以使用证书对个人设备进行身份验证，第 107 页
将思科 ISE 配置为允许用户续订证书，第 89 页
吊销终端证书，第 124 页

思科 ISE CA 证书和密钥的备份与恢复

必须安全地备份Cisco ISE CA 证书和密钥，以在出现 PAN 故障以及您要将辅助管理节点升级作为外部 PKI 的根 CA 或中间 CA 的情况下在辅助管理节点上恢复这些证书和密钥。Cisco ISE 配置备份不包括 CA 证书和密钥。您应使用命令行界面 (CLI) 将 CA 证书和密钥导出至存储库，然后再导入。**application configure ise** 命令现在包含导出和导入选项，用于备份和恢复 CA 证书和密钥。

来自受信任证书库的以下证书存储于辅助管理节点上：

- Cisco ISE Root CA 证书
- Cisco ISE 子 CA 证书
- Cisco ISE 终端 RA 证书
- Cisco ISE OCSP 响应器证书

在以下情况下，您必须备份和恢复Cisco ISE CA 证书和密钥：

- 部署中有辅助管理节点
- 替换整个Cisco ISE CA 根链
- 配置Cisco ISE 根 CA 作为外部 PKI 的从属 CA
- 从 1.2 版本升级到更高版本
- 从配置备份恢复数据。在这种情况下，必须首先重新生成Cisco ISE CA 根链，然后备份和恢复 ISE CA 证书和密钥。

注释 无论何时在部署中更换思科 ISE 内部 CA，到时都必须刷新 ISE 消息服务以检索完整的证书链。

导出思科 ISE CA 证书和密钥

您必须从 PAN 导出 CA 证书和密钥，才能将其导入到辅助管理节点。通过此选项，辅助管理节点可以在 PAN 关闭和您将辅助管理节点升级到 PAN 时为终端颁发和管理证书。

开始之前

确保您已经创建了用于存储 CA 证书和密钥的存储库。

步骤 1 从Cisco ISE CLI 输入 **application configure ise** 命令。

步骤 2 输入 7 以导出证书和密钥。

步骤 3 输入存储库名称。

步骤 4 输入加密密钥。

系统将显示成功消息和已导出的证书列表，以及主题、颁发机构和序列号。

示例：

```
以下 4 个 CA 密钥对导出到了存储库“sftp”，后者位于“ise_ca_key_pairs_of_ise-vm1”：Subject:CN=Cisco ISE
Self-Signed CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765 Subject:CN=Cisco ISE Endpoint CA of ise-vm1 Issuer:CN=Cisco
 ISE Self-Signed CA of ise-vm1 Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa Subject:CN=Cisco ISE Endpoint
 RA of ise-vm1 Issuer:CN=Cisco ISE Endpoint CA of ise-vm1 Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2
 Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
 Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1 ISE CA 密钥导出成功完成
```

导入思科 ISE CA 证书和密钥

在注册辅助管理节点之后，您必须从 PAN 导出 CA 证书和密钥并将它们导入到辅助管理节点。

步骤 1 从Cisco ISE CLI 中输入 **application configure ise** 命令。

步骤 2 输入 8 以导入 CA 证书和密钥。

步骤 3 输入存储库名称。

步骤 4 输入要导入的文件的名称。文件名应采用以下格式 **ise_ca_key_pairs_of_<vm hostname>**。

步骤 5 输入加密密钥以解密文件。

系统将显示一条成功消息。

示例：

```
导入了以下 4 个 CA 密钥对 (The following 4 CA key pairs were imported): Subject:CN=Cisco ISE Self-Signed CA
 of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1 Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4
 Subject:CN=Cisco ISE Endpoint CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56 Subject:CN=Cisco ISE Endpoint RA of ise-vm1 Issuer:CN=Cisco
 ISE Endpoint CA of ise-vm1 Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca Subject:CN=Cisco ISE OCSP
Responder Certificate of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5 正在停止 ISE 证书颁发机构服务...(Stopping ISE Certificate
Authority Service...) 正在启动 ISE 证书颁发机构服务...(Starting ISE Certificate Authority Service...) ISE
CA 密钥导入成功 (ISE CA keys import completed successfully)
```

在主 PAN 和 PSN 上生成根 CA 和从属 CA

设置部署时，Cisco ISE 会在主 PAN 上为思科 ISE CA 服务生成根 CA，在策略服务节点 (PSN) 上生成从属 CA 证书。但是，当更改 PAN 或 PSN 的域名或主机名时，必须分别在主 PAN 上重新生成根 CA，在 PSN 上重新生成从属 CA。

如果您要在 PSN 上更改主机名，而不是分别在 PAN 和 PSN 上重新生成根 CA 和从属 CA，则您可以在更改主机名之前对 PSN 取消注册，然后重新注册。新的辅助证书会在 PSN 上自动调配。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**

步骤 2 点击**生成证书签名请求 (Generate Certificate Signing Requests)**。

步骤 3 从 **Certificate(s) will be used for** 下拉列表中选择 ISE 根 CA。

步骤 4 点击 **Replace ISE Root CA Certificate chain**。

系统会为部署中的所有节点生成根 CA 和从属 CA 证书。

下一步做什么

如果部署中具有辅助 PAN，请从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助PAN可以在主PAN故障时用作根CA，您可将辅助PAN升级为主PAN。

将思科 ISE 根 CA 配置为外部 PKI 的从属 CA

如果您希望主 PAN 上的根 CA 作为外部 PKI 的从属 CA，则生成 ISE 中间 CA 证书签名请求，将其发送到外部 CA，获取根 CA 证书和 CA 签名的证书，将根 CA 证书导入受信任证书存储区，将 CA 签名的证书绑定到 CSR。在这种情况下，外部 CA 为根 CA，主 PAN 为外部 CA 的从属 CA，PSN 为 主 PAN 的从属 CA。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 点击 **Generate Certificate Signing Requests (CSR)**。

步骤 3 从 **Certificate(s) will be used for** 下拉列表选择 ISE 中级 CA。

步骤 4 点击**生成 (Generate)**。

步骤 5 导出 CSR，将其发送到外部 CA，获取 CA 签名的证书。

步骤 6 将根 CA 证书从外部 CA 导入受信任证书库。

步骤 7 将 CA 签名证书与 CSR 绑定。

下一步做什么

如果部署中具有辅助 PAN，请从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。然后，服务器和根证书会在辅助 PAN 中自动复制。这可确保在管理节点发生故障切换时，辅助 PAN 可用作外部 PKI 的从属 CA。

配置思科 ISE 以使用证书对个人设备进行身份验证

可以配置Cisco ISE，为连接到网络的终端（个人设备）发送和管理证书。可以使用内部Cisco ISE 证书授权 (CA) 服务签署来自终端的证书签名请求 (CSR)，或者将 CSR 转发到外部 CA。

开始之前

- 从主 PAN 获取Cisco ISE CA 证书和密钥备份，将其保存在安全位置，用于灾难恢复目的。
- 如果部署中具有辅助 PAN，请从主 PAN 备份Cisco ISE CA 证书和密钥，然后在辅助 PAN 上恢复备份。

步骤 1 将用户添加到 Employee 用户组，第 108 页

可以将用户添加到内部身份库或外部身份库，例如 Active Directory。

步骤 2 为基于 TLS 的身份验证创建证书身份验证配置文件，第 108 页

步骤 3 为基于 TLS 的身份验证创建身份源序列，第 109 页

步骤 4 创建客户端调配策略。

a) 配置证书颁发机构设置，第 109 页
b) 创建 CA 模板，第 111 页
c) 创建要用于客户端调配策略的本地请求方配置文件，第 113 页
d) 从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源，第 114 页
e) 为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则，第 114 页

步骤 5 为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 115 页

步骤 6 为基于 TLS 的身份验证配置授权策略规则。

a) 为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 115 页
b) 创建授权策略规则，第 116 页

当您使用基于 ECDHE-RSA 的证书时，从您的个人设备连接无线 SSID 期间，系统将提示您再次输入密码。

将用户添加到 Employee 用户组

以下程序介绍如何在Cisco ISE 身份库中将用户添加到 Employee 用户组。如果使用外部身份库，请确保具有可向其添加用户的 Employee 用户组。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入用户详细信息。

步骤 4 在**密码 (Passwords)** 部分，选择**登录密码 (Login Password)** 和 TACACS+ **启用密码 (Enable Password)** 设置网络设备的访问级别。

步骤 5 从 User Group 下拉列表中选择 Employee。

属于 Employee 用户组的所有用户共享同一组权限。

步骤 6 点击**提交 (Submit)**。

下一步做什么

为基于 TLS 的身份验证创建证书身份验证配置文件，第 108 页

为基于 TLS 的身份验证创建证书身份验证配置文件

要使用证书对连接到您网络的终端进行身份验证，您必须在Cisco ISE 中定义证书身份验证配置文件或编辑默认的 Preloaded_Certificate_Profile。证书身份验证配置文件包括应用作主体用户名的证书字段。例如，如果用户名在通用名称字段中，则您可以使用主体用户名定义证书身份验证配置文件，即主题 - 通用名称，该名称可对身份库进行验证。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > 证书验证配置文件 (Certificate Authentication Profile)。

步骤 2 输入证书身份验证配置文件的名称。例如，CAP。

步骤 3 选择主题 - 通用名称作为 **Principal Username X509 Attribute**。

步骤 4 点击保存 (Save)。

下一步做什么

为基于 TLS 的身份验证创建身份源序列， 第 109 页

为基于 TLS 的身份验证创建身份源序列

在创建证书身份验证配置文件后，必须将其添加到身份源序列，以便Cisco ISE 可从证书获取属性并将其与您在身份源序列中定义的身份源进行匹配。

开始之前

确保您已完成以下任务：

- 向 Employee 用户组添加用户。
- 为基于证书的身份验证创建证书身份验证配置文件。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)。

步骤 2 点击添加 (Add)。

步骤 3 输入身份源序列的名称。例如 Dot1X。

步骤 4 选中选择证书身份验证配置文件 (Select Certificate Authentication Profile) 复选框，然后选择之前创建的证书身份验证配置文件，即 CAP。

步骤 5 将包含您的用户信息的身份源移至 Authentication Search List 区域的 **Selected** 列表框。

您可以添加更多身份源，Cisco ISE 会按照顺序搜索这些数据存储区，直到找到匹配项。

步骤 6 点击 **Treat as if the user was not found and proceed to the next store in the sequence** 单选按钮。

步骤 7 点击提交 (Submit)。

下一步做什么

配置证书颁发机构设置， 第 109 页

配置证书颁发机构设置

如果您计划将外部 CA 用于为证书签名请求 (CSR) 提供签名，则必须配置外部 CA 设置。在以前版本的Cisco ISE 中，外部 CA 设置称为 SCEP RA 配置文件。如果您使用的是Cisco ISE CA，则不必明

确配置 CA 设置。您可以在 Administration > System > Certificates > Internal CA Settings 下查看内部 CA 设置。

用户的设备收到已验证的证书后，会按照下表中的说明驻留于设备上。

表 *17:* 设备证书位置

设备	证书存储位置	访问方法
iPhone/iPad	标准证书库	Settings > General > Profile
Android	加密证书库	不对最终用户显示。 **注释** 可以使用“设置”(Settings) > “位置和安全”(Location & Security) > “清除存储”(Clear Storage) 来删除证书。
Windows	标准证书库	从 **/cmd** 提示符启动 mmc.exe 或在 snap-in 证书中进行查看。
Mac	标准证书库	Application > Utilities > Keychain Access

开始之前

如果您计划将外部证书颁发机构用于为证书签名请求 (CSR) 提供签名，您必须拥有外部 CA 的 URL。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **外部 CA 设置 (External CA Settings)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为外部 CA 设置输入名称。例如 EXTERNAL_SCEP。

步骤 4 在 URL 文本框中输入外部 CA 服务器 URL。

点击 **Test Connection**，检查是否可以访问外部 CA。点击 + 按钮以添加更多 CA 服务器 URL。

步骤 5 点击**提交 (Submit)**。

下一步做什么

创建 CA 模板，第 111 页

创建 CA 模板

证书模板定义必须（用于内部或外部CA）的SCEP RA配置文件、密钥类型、密钥大小或曲线类型、使用者、使用者备选名称(SAN)、证书有效期和扩展密钥用法。此示例假定您即将使用内部Cisco ISE CA。对于外部 CA 模板，有效期由外部 CA 确定，而您无法指定有效期。

您可以创建新的 CA 模板或编辑默认证书模板 EAP_Authentication_Certificate_Template。

默认情况下，Cisco ISE 中的以下 CA 模板可用：

- CA_SERVICE_Certificate_Template - 用于使用 ISE CA 的其他网络服务。例如，在配置给 ASA VPN 用户颁发证书的 ISE 时使用此证书模板。
- EAP_Authentication_Certificate_Template - 用于 EAP 身份验证。
- pxGrid_Certificate_Template - 用于从证书调配门户生成证书时的 pxGrid 控制器。

注释 使用 ECC 密钥类型的证书模板仅可用于内部思科 ISE CA。

开始之前

确保您已配置 CA 设置。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **CA 服务 (CA Service)** > **内部 CA 证书模版 (Internal CA Certificate Template)**。

步骤 2 输入内部 CA 模板的名称。例如 Internal_CA_Template。

步骤 3 （可选）输入“组织单位”(Organizational Unit)、“企业”(Organization)、“城市”(City)、“省”(State) 和“国家/地区”(Country) 字段的值。

在证书模板字段（“组织单位”[Organizational Unit]、“企业”[Organization]、“城市”[City]、“省”[State] 和“国家/地区”[Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

生成证书的内部用户的用户名用作证书的通用名称。Cisco ISE 内部 CA 的“通用名称”(Common Name) 字段不支持“+”或“*”字符。确保用户名不包含特殊字符“+”或“*”。

步骤 4 指定使用者备选名称 (SAN) 和证书的有效期。

步骤 5 指定密钥类型。选择 RSA 或 ECC。

下表列出了支持 ECC 和曲线类型的操作系统和版本。如果设备未在受支持的操作系统或受支持的版本上运行，可以使用基于 RSA 的证书代替。

操作系统	支持的版本	支持的曲线类型
Windows	8 及更高版本	P-256、P-384 和 P-521

操作系统	支持的版本	支持的曲线类型
Android	4.4 和更高版本 注释 Android 6.0 需要 2016 年 5 月的补丁才能支持 ECC 证书。	所有曲线类型（Android 6.0 除外，它不支持 P-192 曲线类型）。

Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。此Cisco ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

如果您网络中的设备运行的操作系统不支持（Windows 7、Mac OS X 或 Apple iOS），我们建议您选择 RSA 为密钥类型。

步骤 6 （选择 RSA 密钥类型时适用）指定密钥大小。您必须选择 1024 或更高的密钥大小。

步骤 7 （仅在选择 ECC 密钥类型时适用）指定曲线类型。默认值为 P-384。

步骤 8 选择 ISE 内部 CA 作为 SCEP RA 配置文件。

步骤 9 输入有效期（天）。默认值为 730 天。有效范围为 1 到 730。

步骤 10 指定扩展密钥用法。如果要将证书用于客户端身份验证，选中**客户端验证 (Client Authentication)** 复选框。如果要将证书用于服务器身份验证，选中**服务器身份验证 (Server Authentication)** 复选框。

步骤 11 点击**提交 (Submit)**。

系统将创建内部 CA 证书模板并供内部客户端调配策略使用。

下一步做什么

创建要用于客户端调配策略的本地请求方配置文件，第 113 页

内部 CA 设置

下表介绍“内部 CA 设置 (Internal CA Settings)”窗口中的字段。您可以查看内部 CA 设置和从该页面禁用内部 CA 服务。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **内部 CA 设置 (Internal CA Settings)**。

表 *18:* 内部 *CA* 设置

字段名称	使用指南
禁用证书权限 (Disable Certificate Authority)	点击此按钮以禁用内部 CA 服务。
主机名 (Host Name)	运行 CA 服务的Cisco ISE 节点的主机名。
相关角色 (Personas)	在运行 CA 服务的节点上启用的Cisco ISE 节点角色。例如管理角色、策略服务角色等。

字段名称	使用指南
角色 [Role(s)]	运行 CA 服务的Cisco ISE 节点承担的职责。例如，独立、主要或辅助职责。
CA、EST 和 OCSP 响应方状态 (CA, EST & OCSP Responder Status)	启用或禁用
OCSP 响应者 URL (OCSP Responder URL)	Cisco ISE 节点用于访问 OCSP 服务器的 URL。
SCEP URL	Cisco ISE 节点用来访问 OCSP 服务器的 URL。

相关主题

思科 ISE CA 服务 ， 第 92 页
配置思科 ISE 以使用证书对个人设备进行身份验证 ， 第 107 页

创建要用于客户端调配策略的本地请求方配置文件

可以创建本地请求方配置文件，使用户能够将个人设备带入公司网络。Cisco ISE 对不同的操作系统使用不同的策略规则。每个客户端调配策略规则都包含一个本地请求方配置文件，其指定针对哪个操作系统而使用哪个调配向导。

开始之前

- 在Cisco ISE 中配置 CA 证书模板。
- 打开 TCP 端口 8905 和 UDP 端口 8905 以启用客户端代理和请求方调配向导的安装。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“Cisco ISE 设备端口参考”附录。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 选择 **添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

步骤 3 输入本地请求方配置文件的名称。例如 EAP_TLS_INTERNAL。

步骤 4 从**操作系统 (Operating System)** 下拉列表中选择“全部”(ALL)。

注释 MAC OS 版本 10.10 用户需手动连接到双 SSID PEAP 流的调配 SSID。

步骤 5 选中**有线 (Wired)** 或**无线 (Wireless)** 复选框。

步骤 6 从**允许协议 (Allowed Protocol)** 下拉列表中选择 TLS。

步骤 7 选择之前创建的 CA 证书模板。

步骤 8 点击**提交 (Submit)**。

下一步做什么

从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源，第 114 页

从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源

对于 Windows 和 Mac OS X 操作系统，您必须从Cisco站点下载远程资源。

开始之前

验证是否已为您的网络正确配置代理设置，确保能够访问相应的远程位置以将客户端调配资源下载至Cisco ISE。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **资源 (Resources)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 选择 **添加 (Add)** > **思科站点的代理资源 (Agent resources from Cisco site)**。

步骤 3 选中 **Windows** 和 **MAC OS X** 包旁边的复选框。确保包含最新的版本。

步骤 4 点击**保存 (Save)**。

下一步做什么

为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则，第 114 页

为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则

客户端调配资源策略可确定哪些用户会在登录和用户会话启动后从Cisco ISE 收到什么版本的资源（代理、代理合规性模块和代理自定义包/配置文件）。

当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。

要允许员工携带 iOS、Android、MACOSX 设备，必须在“客户端调配策略”(Client Provisioning Policy) 页面为上述每一种设备创建策略规则。

开始之前

您必须已经配置了所需的本地请求方配置文件并已从 Client Provisioning Policy 页面下载了所需的代理。

步骤 1 选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则。

步骤 3 点击**保存 (Save)**。

下一步做什么

为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 115 页

为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则

此任务显示如何为基于 TLS 的身份验证更新 Dot1X 身份验证策略规则。

开始之前

确保您已为基于 TLS 的身份验证创建证书身份验证配置文件。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

步骤 2 点击**视图 (View)** 列中的箭头图标 ›，打开集合视图屏幕，查看、管理和更新身份验证策略。

默认基于规则的身份验证策略包括一条适用于 Dot1X 身份验证的规则。

步骤 3 要编辑 Dot1X 身份验证策略规则的条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击 。Conditions Studio 将打开。

步骤 4 从 Dot1X 策略规则的**操作 (Actions)** 列中，点击齿轮图标，然后从下拉菜单中，根据需要通过选择任何插入或重复选项来插入新策略集。
“策略集”(Policy Sets) 表中会显示一个新行。

步骤 5 为规则输入名称。例如，eap-tls。

步骤 6 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 7 在 **Conditions Studio 页面**中创建所需的条件。在**编辑器 (Editor)** 部分中，点击文本框**点击以添加属性 (Click To Add an Attribute)**，选择所需的词典和属性（例如，Network Access:UserName Equals User1）。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 8 点击**使用 (Use)**。

步骤 9 保留默认规则。

步骤 10 点击**保存 (Save)**。

下一步做什么

为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 115 页

为集中式 Web 身份验证和请求方调配流程创建授权配置文件

必须定义授权配置文件以确定在基于证书的身份验证成功后必须授予用户的访问权限。

开始之前

确保已在无线 LAN 控制器 (WLC) 上配置所需的访问控制列表 (ACL)。有关如何在 WLC 上创建 ACL 的信息，请参阅《*TrustSec* 操作指南：将证书用于差异化访问》。

本示例假定已在 WLC 上创建以下 ACL。

- NSP-ACL - 适用于本地请求方调配
- BLACKHOLE - 适用于限制对列入阻止列表的设备的访问
- NSP-ACL-Google - 适用于调配 Android 设备

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 点击**添加 (Add)** 以创建新的授权配置文件。

步骤 3 为授权配置文件输入名称。

步骤 4 从 **Access Type** 下拉列表中选择 ACCESS_ACCEPT。

步骤 5 点击**添加 (Add)**，为集中式 Web 身份验证、适用于 Google Play 的集中式 Web 身份验证、本地请求方调配和适用于 Google 的本地请求方调配添加授权配置文件。

步骤 6 点击**保存 (Save)**。

下一步做什么

创建授权策略规则，第 116 页

创建授权策略规则

Cisco ISE 评估授权策略规则并授予对基于策略规则中指定的授权配置文件的网络资源的用户访问权限。

开始之前

确保已创建所需的授权配置文件。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集以查看授权策略规则。

步骤 2 请在默认规则之上插入其他策略规则。

步骤 3 点击**保存 (Save)**。

CA 服务策略参考

本节提供您在启用Cisco ISE CA 服务之前必须创建的授权和客户端调配策略规则的参考信息。

证书服务的客户端调配策略规则

本节将列出在使用Cisco ISE 证书服务时，您必须创建的客户端调配策略规则。下表将提供详细信息。

规则名称	身份组	操作系统	其他条件	结果
iOS	任意	Apple iOS 全部	条件	EAP_TLS_INTERNAL（较早创建的本地请求方配置文件）。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
Android	任意	Android	条件	EAP_TLS_INTERNAL（较早创建的本地请求方配置文件）。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
MACOSX	任意	MACOSX	条件	在本地请求方配置下，指定以下项目： 1. 配置向导：选择您从Cisco网站上下载的 MACOSX 请求方向导。 2. 向导配置文件：选择您较早创建的 EAP_TLS_INTERNAL 本地请求方配置文件。如要使用外部CA，请选择您已经为外部 CA 创建的本地请求方配置文件。

证书服务的授权配置文件

本节列出您为在Cisco ISE 中启用基于证书的身份验证而必须创建的授权配置文件。您必须已在无线 LAN 控制器 (WLC) 上创建 ACL（NSP-ACL 和 NSP-ACL-Google）。

- CWA - 此配置文件用于完成集中式 Web 身份验证流程的设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Centralized，然后在 ACL 文本字段中输入 NSP-ACL。
- CWA_GooglePlay - 此配置文件用于完成集中式 Web 身份验证流程的 Android 设备。此配置文件使 Android 设备能够访问 Google Play 商店并下载Cisco网络设置助理。选中 **Web Authentication** 复选框，从下拉列表中选择 Centralized，然后在 ACL 文本框中输入 NSP-ACL-Google。
- NSP - 此配置文件用于完成请求方调配流程的非 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Supplicant Provisioning，然后在 ACL 文本框中输入 NSP-ACL。
- NSP Google - 此配置文件用于完成请求方调配流程的 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Supplicant Provisioning，然后在 ACL 文本框中输入 NSP-ACL-Google。

查看默认 Blackhole_Wireless_Access 授权配置文件。Advanced Attributes Settings 应为如下所示：

- Cisco:cisco-av-pair = url-redirect=https://*ip*:*port*/blacklistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

证书服务的授权策略规则

本节列出您在启用Cisco ISE CA 服务时必须创建的授权策略规则。

- Corporate Assets - 此规则适用于使用 802.1X 和 MSCHAPV2 协议连接到公司无线 SSID 的公司设备。
- Android_SingleSSID - 此规则适用于访问 Google Play Store 以下载Cisco网络设置助理进行调配的 Android 设备。此规则专门针对单一 SSID 设置。
- Android_DualSSID - 此规则适用于访问 Google Play Store 以下载Cisco网络设置助理进行调配的 Android 设备。此规则专门针对双 SSID 设置。
- CWA - 此规则适用于需要完成集中式 Web 身份验证流程的设备。
- NSP - 此规则适用于需要通过使用证书进行 EAP-TLS 身份验证来完成本地请求方调配流程的设备。
- EAP-TLS - 此规则适用于已完成请求方调配流程并使用证书调配的设备。系统将向设备授予访问网络的权限。

下表列出您在配置适用于Cisco ISE CA 服务的授权策略规则时必须选择的属性和值。本示例假设您在Cisco ISE 中已配置相应的授权配置文件。

规则名称	条件	权限（要应用的授权配置文件）
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess

规则名称	条件	权限（要应用的授权配置文件）
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ISE CA 颁发证书给 ASA VPN 用户

ISE CA 可以向通过 ASA VPN 连接的客户端计算机颁发证书。使用此功能，您可以自动将证书调配给通过 ASA VPN 连接的终端设备。

Cisco ISE 使用简单证书注册协议 (SCEP) 进行注册并将证书调配给客户端计算机。AnyConnect 客户端通过 HTTPS 连接向 ASA 发送 SCEP 请求。ASA 将评估请求并实施策略，然后通过Cisco ISE 与 ASA 之间建立的 HTTP 连接将请求中继到Cisco ISE。来自Cisco ISE CA 的响应将被中继回客户端。ASA 无法读取 SCEP 消息的内容，将充当Cisco ISE CA 的代理。Cisco ISE CA 从客户端解密 SCEP 消息，并采用加密形式发送响应。

ISE CA SCEP URL 为 http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe。如果您将使用 ISE 节点的 FQDN，则连接到 ASA 的 DNS 服务器必须能够解析该 FQDN。

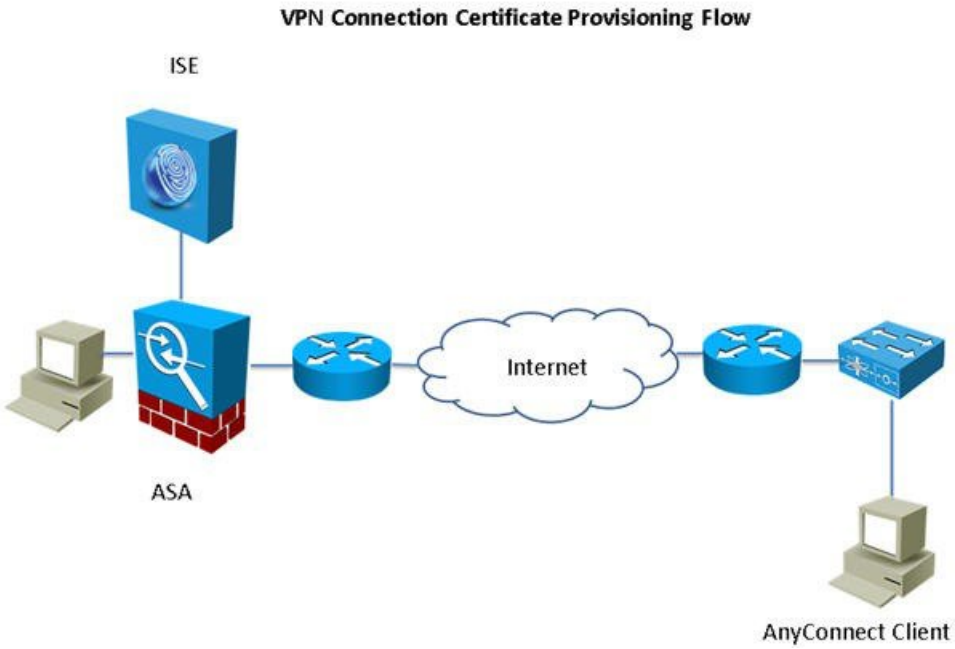
您可以在证书过期之前使用 AnyConnect 客户端配置文件配置续订。如果证书已过期，则续订流程类似于新的注册流程。

支持的版本包括：

- 运行软件版本 8.x 的 Cisco ASA 5500 系列自适应安全设备
- Cisco AnyConnect VPN 2.4 或更高版本

VPN 连接的证书调配流程

图 *8: ASA VPN* 用户的证书调配



1. 用户启动 VPN 连接。
2. AnyConnect 客户端扫描客户端机器，并将包括唯一设备标识符在内的属性（例如 IMEI）发送至 ASA。
3. ASA 从客户端请求基于证书的身份验证。身份验证因为没有证书失败。
4. ASA 使用用户名/密码执行主要用户身份验证 (AAA)，并将信息传递给身份验证服务器 (ISE)。
    1. 如果身份验证失败，连接将立即终止。
    2. 如果身份验证通过，将授予有限访问权限。您可以使用 aaa.cisco.sceprequired 属性为请求证书的客户端机器配置动态访问策略 (DAP)。您可以将此属性的值设置为“True”，并应用 ACL 和 Web ACL。
5. 在应用相关策略和 ACL 后，VPN 连接已建立。客户端仅在 AAA 身份验证成功和已建立 VPN 连接后开始 SCEP 密钥生成。
6. 客户端开始 SCEP 注册并将 SCEP 请求通过 HTTP 发送到 ASA。
7. 如果会话被允许注册，ASA 将查找请求的会话信息并将请求传递至 ISE CA。
8. ASA 将来自 ISE CA 的响应回传至客户端。
9. 如果注册成功，则客户端向用户显示一条可配置的消息，并断开 VPN 会话连接。
10. 用户可以使用证书重新验证，正常的 VPN 连接已建立。

配置思科 ISE CA 向 ASA VPN 用户颁发证书

您必须在Cisco ISE 和 ASA 上执行以下配置以向 ASA VPN 用户提供证书。

开始之前

- 确保Cisco ISE 内部或外部身份源中存在 VPN 用户帐户。
- 确保 ASA 和Cisco ISE 策略服务节点使用相同的 NTP 服务器进行同步。

步骤 1 将 ASA 定义为Cisco ISE 中的网络访问设备。参阅在思科 ISE 中添加网络设备，第 121 页查看有关如何将 ASA 添加为网络设备的信息。

步骤 2 在 ASA 上配置组策略，第 122 页。

步骤 3 为 SCEP 注册配置 AnyConnect 连接配置文件，第 122 页。

步骤 4 在 ASDM 中配置 VPN 客户端配置文件，第 123 页。

步骤 5 将思科 ISE CA 证书导入到 ASA。

在思科 ISE 中添加网络设备

您可以在Cisco ISE 中添加网络设备或使用默认网络设备。

您还可以在**网络设备 (Network Devices)** 窗口（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）中添加网络设备。

开始之前

必须在要添加的网络设备上启用 AAA 功能。请参阅启用 AAA 功能的命令。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)**、**说明** 和 **IP 地址 (IP Address)** 字段中输入相应的值。

步骤 4 从**设备配置文件 (Device Profile)**、**型号名称 (Model Name)**、**软件版本 (Software Version)** 和**网络设备组 (Network Device Group)** 字段的下拉列表中选择所需的值。

步骤 5 （可选）选中 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 复选框以配置用于身份验证的 RADIUS 协议。

步骤 6 （可选）选中 **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框以配置用于身份验证的 TACACS 协议。

步骤 7 （可选）选中 **SNMP 设置 (SNMP Settings)** 复选框以为Cisco ISE 分析服务配置 SNMP，以便从设备收集信息。

步骤 8 （可选）选中**高级 Trustsec 设置 (Advanced Trustsec Settings)** 复选框以配置启用Cisco Trustsec 的设备。

步骤 9 点击**提交 (Submit)**。

在 ASA 上配置组策略

配置 ASA 中的组策略以定义 ISE CA URL 供 AnyConnect 转发 SCEP 注册请求。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击**组策略 (Group Policies)**。

步骤 3 点击**添加 (Add)** 以创建组策略。

步骤 4 输入组策略的名称。例如 ISE_CA_SCEP。

步骤 5 在“转发 URL SCEP”(SCEP forwarding URL) 字段中，取消选中**沿用 (Inherit)** 复选框并输入带端口号的 ISE SCEP URL。

如果在使用 ISE 节点的 FQDN，连接至 ASA 的 DNS 服务器必须能够解析 ISE 节点的 FQDN。

示例：

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe。

步骤 6 点击**确定 (OK)** 保存组策略。

为 SCEP 注册配置 AnyConnect 连接配置文件

在 ASA 上配置 AnyConnect 连接配置文件可指定 ISE CA 服务器、身份验证方法和 ISE CA SCEP URL。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击 **AnyConnect 连接配置文件 (AnyConnect Connection Profile)**。

步骤 3 点击**添加 (Add)** 创建连接配置文件。

步骤 4 输入连接配置文件的名称。例如 Cert-Group。

步骤 5 （可选）在“别名”(Aliases) 字段中，输入连接配置文件的描述。例如 SCEP-Call-ASA。

步骤 6 在“身份验证”(Authentication) 区域，指定以下信息：

- “方法”(Method) - 点击**两者都 (Both)** 单选按钮
- “AAA 服务器组”(AAA Server Group) - 点击**管理 (Manage)** 并选择您的 ISE 服务器

步骤 7 在“客户端地址分配”(Client Address Assignment) 区域，选择要使用的 DHCP 服务器和客户端地址池。

步骤 8 在“默认组策略”(Default Group Policy) 区域中，点击**管理 (Manage)** 并选择已创建的带有 ISE SCEP URL和端口号的“组策略”(Group Policy)。

示例：

例如 ISE_CA_SCEP。

步骤 9 选择 **高级 (Advanced)** > **常规 (General)** 并为此连接配置文件选中**启用简单认证登记协议 (Enable Simple Certificate Enrollment Protocol)** 复选框。

步骤 10 点击**确定 (OK)**。

AnyConnect 连接配置文件已创建。

下一步做什么

在 ASDM 中配置 VPN 客户端配置文件

为 SCEP 注册在 AnyConnect 配置 VPN 客户端配置文件。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击 **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 3 选择要使用的客户端配置文件，然后点击**编辑 (Edit)**。

步骤 4 点击左侧“配置文件”(Profile) 导航窗格中的**认证登记 (Certificate Enrollment)**。

步骤 5 选中**认证登记 (Certificate Enrollment)** 复选框。

步骤 6 在以下字段中输入值：

- “证书过期阈值”(Certificate Expiration Threshold) - 在证书过期日前，AnyConnect 提醒用户其证书即将过期的天数（启用 SCEP 时不支持该功能）。默认值为零（不显示警告）。值范围为 0 到 180 天。
- “自动 SCEP 主机”(Automatic SCEP Host) - 输入已配置 SCEP 证书检索的 ASA 的主机名和连接配置文件（隧道组）。输入 ASA 的完全限定域名 (FQDN) 或连接配置文件名称。例如主机名 asa.cisco.com 和连接配置文件名称 scep_eng。
- CA URL - 识别 SCEP CA 服务器。输入 ISE 服务器的 FQDN 或 IP 地址。例如 http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe。

步骤 7 输入定义客户端如何请求证书内容的证书内容值。

步骤 8 点击**确定 (OK)**。

AnyConnect 客户端配置文件已创建。有关其他信息，请参阅适用于您的 AnyConnect 版本的《思科 AnyConnect 安全移动客户端》。

将思科 ISE CA 证书导入到 ASA

将Cisco ISE 内部 CA 证书导入到 ASA。

开始之前

导出Cisco ISE 内部 CA 证书。请转至 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。选中**证书服务节点 CA (Certificate Services Node CA)** 和**证书服务根 CA (Certificate Services Root CA)** 证书旁边的复选框并将其导出，一次导出一个证书。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，选择 **证书管理 (Certificate Management)** > **CA 证书 (CA Certificates)**。

步骤 3 点击**添加 (Add)**并选择Cisco ISE 内部 CA 证书可将其导入 ASA。

吊销终端证书

如果您需要吊销向员工个人设备颁发的证书，您可以从终端证书 (Endpoint Certificates) 页面进行吊销。例如，如果员工的设备被盗或丢失，您可以登录Cisco ISE Admin 门户，然后从终端证书 (Endpoint Certificates) 页面吊销颁发给该设备的证书。在此页面上，您可以根据友好名称 (Friendly Name)、设备唯一 Id (Device Unique Id) 或序列号 (Serial Number) 过滤数据。

如果 PSN（子 CA）已被破坏，您可以通过从终端证书 (Endpoint Certificates) 页面过滤 Issued By 字段，吊销 PSN 颁发的所有证书。

当您吊销颁发给员工的证书时，如果有活动会话（已使用该证书进行身份验证），会话将立即终止。吊销证书可确保证书一撤销，未授权的用户就无法访问资源。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发的证书 (Issued Certificates)**。

步骤 2 选中您要吊销的终端证书旁边的复选框，然后点击**吊销 (Revoke)**。

您可以根据友好名称 (Friendly Name) 和 设备类型 (Device Type) 搜索证书。

步骤 3 输入吊销证书的原因。

步骤 4 点击**是 (Yes)**。

OCSP 服务

在线证书状态协议 (OCSP) 是一种用于检查 x.509 数字证书状态的协议。此协议替代证书吊销列表 (CRL) 并解决导致处理 CRL 的问题。

Cisco ISE 能够通过 HTTP 与 OCSP 服务器进行通信，以在身份验证中验证证书的状态。OCSP 配置在可从Cisco ISE 中配置的任何证书颁发机构 (CA) 证书引用的可重用配置对象中进行配置。

您可以根据 CA 配置 CRL 和/或 OCSP 验证。如果同时选择两者，则Cisco ISE 会先通过 OCSP 执行验证。如果检测到主 OCSP 服务器和辅助 OCSP 服务器均有通信问题，或者如果针对给定证书返回未知状态，则Cisco ISE 会切换至检查 CRL。

思科 ISE CA 服务在线证书状态协议响应器

Cisco ISE CA OCSP 响应器是与 OCSP 客户端进行通信的服务器。Cisco ISE CA 的 OCSP 客户端包括内部Cisco ISE OCSP 客户端和自适应安全设备 (ASA) 上的 OCSP 客户端。OCSP 客户端应使用 RFC 2560 和 5019 中定义的 OCSP 请求/响应结构与 OCSP 响应器进行通信。

ISE CA 向 OCSP 响应器颁发证书。OCSP 响应器在端口 2560 上侦听任何传入请求。此端口配置为仅允许 OCSP 流量。

OCSP 响应器接受遵循 RFC 2560 和 5019 中定义的结构的请求。OCSP 请求中支持随机数扩展。OCSP 响应器获取证书的状态，然后创建 OCSP 响应并对其进行签名。OCSP 响应不会缓存到 OCSP 响应器上，但您可以将 OCSP 响应缓存到客户端上，最长期限为 24 小时。OCSP 客户端应验证 OCSP 响应中的签名。

PAN 上的自签名 CA 证书（如果 ISE 用作外部 CA 的中间 CA，则是中间 CA 证书）颁发 OCSP 响应器证书。PAN 上的此 CA 证书颁发 PAN 和 PSN 上的 OCSP 证书。此自签名 CA 证书也是整个部署的根证书。整个部署中的所有 OCSP 证书都放在 ISE 的受信任证书库中，以验证任何使用这些证书签名的响应。

OCSP 证书状态值

OCSP 服务面向给定的证书请求返回以下值：

- Good - 表示对状态查询的肯定回答。它意味着仅在下次时间间隔（存活时间）值之前证书未被吊销并且状态良好。
- Revoked - 证书被吊销。
- Unknown - 证书状态未知。如果证书不是由此 OCSP 响应者的 CA 颁发，则 OCSP 服务会返回此值。
- Error - 没有收到 OCSP 请求的任何响应。

OCSP 高可用性

Cisco ISE 能够为每个 CA 配置最多两台 OCSP 服务器，我们将其称为主 OCSP 服务器和辅助 OCSP 服务器。每个 OCSP 服务器配置均包含以下参数：

- URL - OCSP 服务器 URL。
- Nonce - 请求中发送的随机数。此选项可确保重放攻击无法利用旧通信数据。
- Validate response - Cisco ISE 验证从 OCSP 服务器接收到的响应签名。

在超时（5 秒钟）情况下，当Cisco ISE 与主要 OCSP 服务器进行通信时，它会切换为辅助 OCSP 服务器。

Cisco ISE 在尝试再次使用主要服务器之前，会在可配置的时间内使用辅助 OCSP 服务器。

OCSP 故障

以下是三个一般 OCSP 故障情况：

- OCSP 缓存或 OCSP 客户端（Cisco ISE）故障。
- OCSP 响应器故障情况，例如：

第一个主要 OCSP 响应器无响应，辅助 OCSP 响应器响应Cisco ISE OCSP 请求。

无法从Cisco ISE OCSP 请求接收错误或响应。

OCSP 响应器可能不向Cisco ISE OCSP 请求提供响应或可能返回一个不成功的 OCSP Response Status 值。可能的 OCSP Response Status 值如下所示：

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

  OCSP 请求中有很多日期时间检查、签名验证检查等。有关详细信息，请参阅 *RFC 2560 X.509* 互联网公钥基础结构在线证书状态协议 - *OCSP*，其中描述了所有可能的状态，包括错误状态。

- OCSP 报告故障

添加 OCSP 客户端配置文件

您可以使用 OCSP Client Profile 页面，将新 OCSP 客户端配置文件添加到Cisco ISE。

开始之前

如果 Certificate Authority (CA) 正在非标准端口（不是 80 或 443）上运行 OCSP 服务，则必须在交换机上配置 ACL，允许在Cisco ISE 和 CA 之间通过此端口进行通信。例如：

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* 端口号>

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **OCSP 客户端配置文件 (OCSP Client Profile)**。

步骤 2 输入值，添加 OCSP 客户端配置文件。

步骤 3 点击**提交 (Submit)**。

OCSP 客户端配置文件设置

下表介绍了“OCSP 客户端配置文件”(OCSP Client Profile) 窗口上的字段，可以使用此窗口配置 OCSP 客户端配置文件。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **OCSP 客户端配置文件 (OCSP Client Profile)**。

表 *19: OCSP* 客户端配置文件设置

字段名称	使用指南
名称 **(Name)**	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
配置 **OCSP** 响应器 **(Configure OCSP Responder)**	
启用辅助服务器 **(Enable Secondary Server)**	选中此复选框来以启用高可用性辅助 OCSP 服务器。
始终先访问主服务器 **(Always Access Primary Server First)**	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，Cisco ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。
在 ***n*** 分钟后回退至主服务器 **(Fallback to Primary Server After Interval n Minutes)**	当您希望Cisco ISE 移至辅助服务器，然后再回退到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
主服务器和辅助服务器 **(Primary and Secondary Servers)**	
URL	输入主要和/或辅助 OCSP 服务器的 URL。
启用 **Nonce** 扩展支持 **(Enable Nonce Extension Support)**	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。
验证响应签名 **(Validate Response Signature)**	OCSP 响应器用以下一个证书为响应签名： • CA 证书 • 与 CA 证书不同的证书 为了使Cisco ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供Cisco ISE 进行验证，就会如此。如果 OCSP 使用Cisco ISE 中未配置的其他证书给响应签名，响应验证将失败。
使用授权信息访问 **(AIA)** 中指定的 **OCSP URL**。**(Use OCSP URLs specified in Authority Information Access [AIA])**	点击单选按钮以使用授权信息访问扩展名中指定的 OCSP URL。
响应缓存 **(Response Cache)**	

字段名称	使用指南
缓存条目生存时间 *n* 分钟 (Cache Entry Time To Live n Minutes)	以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 nextUpdate 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 nextUpdate 值为 0，则根本不缓存响应。Cisco ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当Cisco ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因： • 减少网络流量和降低 OCSP 服务器对已知证书带来的负载 • 通过缓存已知证书状态提高Cisco ISE 性能 默认情况下，内部 CA 的 OCSP 客户端配置文件的缓存设置为 2 分钟。如果终端在第一次身份验证后 2 分钟内进行第二次验证，将使用 OCSP 缓存，而不查询 OCSP 响应器。如果终端证书在缓存期间内撤销，将使用之前 OCSP 的状态良好 (Good)，身份验证成功。将缓存设置为 0 分钟可阻止所有响应被缓存。此选项可提高安全性，但会降低身份验证性能。
清空缓存 (Clear Cache)	点击**清空缓存 (Clear Cache)** 以清除连接至 OCSP 服务的所有证书颁发机构的条目。 在部署中，**清空缓存 (Clear Cache)** 与所有节点交互并执行此操作。此机制可更新部署中的每个节点。

相关主题

OCSP 服务，第 124 页
思科 ISE CA 服务在线证书状态协议响应器，第 124 页
OCSP 证书状态值，第 125 页
OCSP 高可用性，第 125 页
OCSP 故障，第 125 页
OCSP 统计计数器，第 128 页
添加 OCSP 客户端配置文件，第 126 页

OCSP 统计计数器

Cisco ISE 使用 OCSP 计数器记录并监控 OCSP 服务器的数据和运行状况。日志记录每五分钟记录进行一次。Cisco ISE 将系统日志消息发送到监控节点，并在本地库中进行保存。本地库包含之前五分钟的数据。Cisco ISE 发送系统日志消息后，计数器会重新开始计算下一个间隔。这表示在五分钟后，新的五分钟时间间隔将会启动。

以下表格列出 OCSP 系统日志消息及其说明。

表 *20: OCSP* 系统日志消息

消息	说明
OCSPPrimaryNotResponsiveCount	无响应的主请求数量
OCSPSecondaryNotResponsiveCount	无响应的辅助请求数量
OCSPPrimaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”证书数量
OCSPSecondaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”状态数量
OCSPPrimaryCertsRevokedCount	对于使用 OCSP 主服务器的给定 CA 所返回的“revoked”状态数量
OCSPSecondaryCertsRevokedCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“revoked”状态数量
OCSPPrimaryCertsUnknownCount	对于使用 OCSP 主服务器的给定 CA 所返回的“Unknown”状态数量
OCSPSecondaryCertsUnknownCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“Unknown”状态数量
OCSPPrimaryCertsFoundCount	主源缓存中查找到的证书数量
OCSPSecondaryCertsFoundCount	辅助源缓存中查找到的证书数量
ClearCacheInvokedCount	经过间隔时间后触发缓存清理的次数
OCSPCertsCleanedUpCount	经过间隔时间后清除的已缓存条目的数量
NumOfCertsFoundInCache	缓存中已执行的请求数量
OCSPCacheCertsCount	在 OCSP 缓存中查找到的证书数量

配置管理员访问策略

管理员访问权限 (RBAC) 策略以 if-then 的格式表示，其中 if 是 RBAC Admin Group 的值，then 是 RBAC Permissions 的值。

RBAC 策略页面（**管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 授权 (Authorization) >RBAC 策略 (Policy)**）包含默认策略列表。您无法编辑或删除这些默认策略。 但是，您可以编辑只读管理员策略的数据访问权限。 通过 RBAC 策略页面，还可以为工作场所的专门管理员组创建自定义 RBAC 策略，并将其应用于个性化管理员组。

分配有限菜单访问权限时，请确保数据访问权限允许管理员访问使用指定菜单时所必需的数据。例如，如果给予对 MyDevices 门户的菜单访问权限，但不允许对终端身份组进行数据访问，则该管理员无法修改该门户。

注释 管理员用户可以将终端 MAC 地址从他们拥有只读访问权限的终端身份组移动到他们拥有完全访问权限的终端身份组。反之则不可能。

开始之前

- 确保您已创建您想要定义 RBAC 策略的所有管理员组。
- 确保这些管理员组映射到各对应的管理员用户。
- 确保您已配置 RBAC 权限，例如菜单访问和数据访问权限。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **RBAC 策略 (RBAC Policy)**。

RBAC Policies 页面包含一系列适用于默认管理员组的现成的预定义策略。您无法编辑或删除这些默认策略。 但是，您可以编辑默认只读管理员策略的数据访问权限。

步骤 2 点击任意默认 RBAC 策略规则旁边的 **Actions**。

在这里，您可以插入新的 RBAC 策略，复制现有 RBAC 策略和删除现有 RBAC 策略。

步骤 3 点击 **Insert new policy**。

步骤 4 为 Rule Name、RBAC Group(s) 和 Permissions 字段输入相应值。

在创建 RBAC 策略时，您不能选择多个菜单访问和数据访问权限。

步骤 5 点击**保存 (Save)**。

管理员访问设置

Cisco ISE 允许为管理员帐户定义某些规则以增强安全性。您可以限制对管理接口的访问，强制管理员使用强密码和定期更改密码等。在Cisco ISE 中的“管理员帐户设置”(Administrator Account Settings) 下定义的密码策略适用于所有管理员帐户。

Cisco ISE 支持包含 UTF-8 字符的管理员密码。

配置最大数量的并发管理会话和登录横幅

您可以配置最大数量的并发管理 GUI 或 CLI (SSH) 会话和登录横幅，它们对访问您的管理 Web 或 CLI 界面的管理员有帮助和指导作用。您可以将登录横幅配置为在管理员登录之前和登录之后显示。默认情况下，这些登录横幅处于禁用状态。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)** > **会话 (Session)**。

步骤 2 输入您要允许通过 GUI 和 CLI 界面的最大数量的并发管理会话。并发管理 GUI 会话的有效范围为 1 至 20。并发管理 CLI 会话的有效范围为 1 至 10。

步骤 3 如果希望Cisco ISE 在管理员登录之前显示消息，请选中**登录前横幅 (Pre-login banner)** 复选框，然后在文本框中输入消息。

步骤 4 如果希望Cisco ISE 在管理员登录之后显示消息，请选中**登录后横幅 (Post-login banner)** 复选框，然后在文本框中输入消息。

步骤 5 点击**保存 (Save)**。

相关主题

允许从“选择 IP 地址”(Select IP Addresses) 对思科 ISE 进行管理访问 ，第 131 页

允许从“选择 IP 地址”(Select IP Addresses) 对思科 ISE 进行管理访问

Cisco ISE 允许您配置 IP 地址列表，管理员可通过列表中的 IP 地址访问Cisco ISE 管理界面。

管理员访问控制设置仅适用于承担管理、策略服务或监控角色的Cisco ISE 节点。这些限制会从主要节点复制到辅助节点。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)** > **IP 访问 (IP Access)**。

步骤 2 选择**仅允许连接列出的 IP 地址 (Allow only listed IP addresses to connect)**。

注释 端口 161 上的连接 (SNMP) 用于管理访问。但是，在配置 IP 访问限制时，如果从一个节点执行 snmpwalk 而没有为其配置管理访问，则 snmpwalk 会失败。

步骤 3 在 Configure IP List for Access Restriction 区域中，点击**添加 (Add)**。

步骤 4 在 IP addresses 字段中输入无类域间路由 (CIDR) 格式的 IP 地址。

注释　此 IP 地址的范围可以是 IPv4 和 IPv6。您现在可以为 ISE 节点配置多个 IPv6 地址。

步骤 5 在网络掩码字段中输入 CIDR 格式的子网掩码。

步骤 6 点击**确定 (OK)**。重复此过程在此列表中添加更多 IP 地址范围。

步骤 7 点击**保存 (Save)** 保存所做的更改。

步骤 8 点击**重置 (Reset)** 以刷新 **IP 访问 (IP Access)** 页面。

允许访问思科 ISE 中的 MnT 部分

Cisco ISE 允许您配置节点列表，管理员可从这些节点访问Cisco ISE 中的 MnT 部分。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 从Cisco ISE 主页中，选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)**。

步骤 2 点击 **MnT 访问 (MnT Access)** 选项卡。

步骤 3 要允许部署内或部署外的节点或实体将系统日志发送到 MnT，请点击**允许任何 IP 地址连接到 MnT (Allow any IP address to connect to MnT)** 单选按钮。要仅允许部署内的节点或实体将系统日志发送到 MnT，请点击**仅允许部署中的节点连接到 MnT (Allow only the nodes in the deployment to connect to MnT)** 单选按钮。

注释　对于 ISE 2.6 P2 及更高版本，默认情况下打开使用 ISE 消息服务将 UDP 系统日志发送到 MnT (Use ISE Messaging Service for UDP Syslogs delivery to MnT)，此设置不允许来自部署外的任何其他实体的系统日志。

为管理员帐户配置密码策略

Cisco ISE 还允许您为管理员帐户创建密码策略，以增强安全性。您可以定义是使用基于密码的管理员身份验证还是使用基于客户端证书的管理员身份验证。您在此处定义的密码策略将应用于Cisco ISE 中的所有管理员帐户。

注释

- 内部管理员用户的电子邮件通知将发送到 root@host。无法配置电子邮件地址，并且许多 SMTP 服务会拒绝此电子邮件。

  可以遵循开放缺陷 CSCui5583，此增强允许您更改电子邮件地址。

- 思科 ISE 支持包含 UTF-8 字符的管理员密码。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 如果在部署中启用自动故障切换配置，请务必关闭此配置。当您更改身份验证方法时，需要重新启动应用服务器进程。这些服务重新启动时可能会出现延迟。由于服务重新启动时出现这种延迟，可能会触发辅助管理节点的自动故障切换。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

步骤 2 选择以下身份验证方法之一：

- “基于密码”(Password Based)- 如果想要对管理员登录使用标准用户 ID 和密码凭证，请选择**基于密码 (Password Based)** 选项并指定“内部”(Internal) 或“外部”(External) 身份验证类型。

  注释 如果您已配置外部身份源（如 LDAP）并且想要使用该身份源作为向管理员用户授予访问权限的身份验证源，则必须从“身份源”(Identity Source) 列表框中选择该特定身份源。

- Client Certificate Based - 如果您想要指定基于证书的策略，请选择 **Client Certificate Based** 选项，并选择现有的证书身份验证配置文件。

步骤 3 点击 **Password Policy** 选项卡并输入值。

步骤 4 点击**保存 (Save)** 保存管理员密码策略。

注释 如果在登录时使用外部身份库验证管理员的身份，请记住，即便为应用到该管理员配置文件的密码策略配置了此设置，外部身份库仍会验证管理员的用户名和密码。

相关主题

管理员密码策略设置

为管理员帐户配置帐户禁用策略，第 133 页
为管理员帐户配置锁定或暂停设置，第 134 页

为管理员帐户配置帐户禁用策略

如果在配置的连续几天内，管理员帐户没有通过身份验证，Cisco ISE 允许您禁用该管理员帐户。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)** > **帐户禁用策略 (Account Disable Policy)**。

步骤 2 选中**在 n 天不活跃之后禁用帐户 (Disable account after *n* days of inactivity)** 复选框，并输入天数。

如果管理员帐户在一段连续时间内处于不活跃状态，通过该选项，您可以禁用管理员帐户。但是，您可以使用**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)** 中提供的**从不禁用不活跃帐户 (Inactive Account Never Disabled)** 选项，从该帐户禁用策略中排除单个管理员帐户。

步骤 3 点击**保存 (Save)** 为管理员配置全局帐户禁用策略。

为管理员帐户配置锁定或暂停设置

Cisco ISE 允许您锁定或暂停失败登录尝试超过指定次数的管理员帐户（包括基于密码的内部管理员帐户和基于证书的管理员帐户）。

步骤 1 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 身份验证 (Authentication) > 锁定/暂停设置 (Lock/Suspend Settings)**。

步骤 2 选中“错误登录尝试之后锁定或暂停帐户”(Account With Incorrect Login Attempts) 复选框，并输入失败尝试次数，在此次数后将采取操作。有效范围为 3 到 20。

- “将帐户暂停 n 分钟”(Suspend Account For n Minutes) - 选择此选项可暂停错误登录尝试超过指定次数的帐户。有效范围为 15 到 1440。
- “锁定帐户”(Lock Account) - 选择此选项可锁定错误登录尝试超过指定次数的帐户。

可以输入自定义电子邮件补救消息，例如请最终用户联系服务中心以解锁帐户。

注释 锁定/暂停设置在思科 ISE 早期版本的“密码策略”(Password Policy) 选项卡中可用。

配置管理员会话超时

在Cisco ISE 中，可以确定管理 GUI 会话处于非活动状态但仍保持连接的时间长度。可以指定Cisco ISE 在注销管理员之前经过的时间（以分钟为单位）。会话超时后，管理员必须重新登录才能访问 Cisco ISE 管理员门户。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 设置 (Settings) > 会话 (Session) > 会话超时 (Session Timeout)**。

步骤 2 输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。

步骤 3 点击**保存 (Save)**。

终止活动管理会话

Cisco ISE 显示所有活动管理会话，您可以从中选择任意会话并在必要时随时终止所选会话。并行管理 GUI 会话的最大数量为 20 个。如果达到 GUI 会话的最大数量，属于超级管理员组的管理员可以登录并阻止某些会话。

开始之前

要执行以下任务，您必须是超级管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)** > **会话信息 (Session Info)**。

步骤 2 选中要终止的会话 ID 旁边的复选框，然后点击**失效 (Invalidate)**。

更改管理员名称

Cisco ISE 允许您从 GUI 更改用户名。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 登录到管理员门户。

步骤 2 点击Cisco ISE UI 右上角显示为链接的用户名。

步骤 3 在显示的 Admin User 页面中输入新用户名。

步骤 4 编辑有关要更改的帐户的任何其他详细信息。

步骤 5 点击**保存 (Save)**。

管理员访问设置

您可以通过这些页面为管理员配置访问设置。

管理员密码策略设置

下表介绍了“管理员密码策略”(Administrator Password Policy) 窗口中的字段，可以使用此窗口定义管理员密码应满足的条件。。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。

表 *21:* 管理员密码策略设置

字段名称	使用指南
最小长度 **(Minimum Length)**	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不得包含 **(Password must not contain)**	**管理员名称或其反向顺序的字符 (Admin name or its characters in reverse order)**：选中此复选框可限制使用管理员用户名或其反向顺序的字符。
	“cisco”或其反向顺序的字符 ("cisco" or its characters in reverse order)：选中此复选框可限制使用单词“cisco”或其反向顺序的字符。
	此单词或其反向顺序的字符 (This word or its characters in reverse order)：选中此复选框可限制使用您定义的任何单词或其反向顺序的字符。
	连续重复四次或以上的字符 (Repeated characters four or more times consecutively)：选中此复选框可限制使用连续重复四次或以上的字符。
	字典单词、其反向顺序的字符或其替换为其他字符的字母 (Dictionary words, their characters in reverse order or their letters replaced with other characters)：选中此复选框可限制使用字典单词、其反向顺序的字符或其替换为其他字符的字母。 不允许使用“$”替代“s”、“@”替代“a”、“0”替代“o”、“1”替代“l”、“!”替代“i”、“3”替代“e”。例如 Pa$$w0rd • **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。 默认情况下，此选项已选中。 • **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**浏览**选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。

字段名称	使用指南
密码必须包含每个所选类型的至少一个字符 **(Password must contain at least one character of each of the selected types)**	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符
密码历史记录 **(Password History)**	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
密码有效期 **(Password Lifetime)**	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
显示网络设备敏感数据 **(Display Network Device Sensitive Data)**	
要求管理员密码 **(Require Admin Password)**	如果您希望管理员用户输入登录密码来查看网络设备敏感数据，例如共享密钥和密码，请选中此复选框。
密码缓存用于 **(Password cached for)**	在此段时间内，会对管理员用户输入的密码进行缓存。在此期间，如果管理员用户要查看网络设备敏感数据，系统不会再次提示输入密码。有效范围为 1 至 60 分钟。

相关主题

思科 ISE 管理员

创建新管理员

会话超时和会话信息设置

下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *22:* 会话超时和会话信息设置

字段名称	使用指南
会话超时 (Session Timeout)	
会话空闲超时 (Session Idle Timeout)	输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。
会话信息 (Session Info)	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后点击**失效 (Invalidate)**。

相关主题

管理员访问设置，第 130 页
配置管理员会话超时，第 134 页
终止活动管理会话，第 135 页