自带设备 (BYOD)

公司网络上的个人设备 (BYOD)

支持公司网络上的个人设备时，必须验证和授权用户（员工、承包商和访客）及其设备，保护网络服务和企业数据。Cisco ISE 提供相关工具，允许员工在公司网络上安全地使用个人设备。

登录访客门户时，访客能够自动注册其设备。访客可以注册更多设备，直到达到您为其访客类型定义的最大限制。这些设备会根据门户配置注册到终端身份组中。

访客可以通过运行本地请求方调配（网络设置助手）或通过将其设备添加到“我的设备”(My Devices) 门户，将其个人设备添加到网络。您可以根据操作系统创建本地请求方配置文件，后者决定着应该使用的适当本地请求方调配向导。

因为不是所有设备都能够使用本地请求方配置文件，所以用户可以使用我的设备门户手动添加这些设备；或者您可以配置 BYOD 规则，注册这些设备。

思科 ISE 社区资源

分布式环境中的最终用户设备门户

Cisco ISE 最终用户 Web 门户根据管理、策略服务和监控角色，提供配置、会话支持和报告功能。

- **策略管理节点 (PAN)**：您对用户、设备和最终用户门户所做的配置更改会写入 PAN。
- **策略服务节点 (PSN)**：最终用户门户在 PSN 上运行，后者处理所有会话流量，包括网络访问、客户端调配、访客服务、终端安全评估和分析。如果 PSN 是节点组的一部分，并且一个节点发生故障，则其他节点会检测到故障，并重置任何挂起的会话。

- **监控节点（MnT 节点）**：MnT 节点在我的设备门户、发起人门户和访客门户上收集、聚合和报告有关最终用户和设备活动的数据。如果主 MnT 节点故障，则辅助 MnT 节点自动成为主 MnT 节点。

设备门户的全局设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)**。

您可以为 BYOD 门户和 My Devices 门户配置以下常规设置：

- **员工注册的设备 (Employee Registered Devices)**：在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。
- **重试 URL (Retry URL)**：在**重试激活 URL (Retry URL for onboarding)** 中输入可用于将设备重定向至Cisco ISE 的 URL。

当您配置这些常规设置后，它们适用于为您的公司设置的所有 BYOD 门户和 My Devices 门户。

相关主题

限制员工注册的个人设备的数量，第 7 页
提供用于重新连接 BYOD 注册流程的 URL，第 9 页
分布式环境中的最终用户设备门户，第 1 页

个人设备门户

Cisco ISE 提供若干基于 Web 的门户，支持员工自有的个人设备。这些设备门户不参与访客或发起人门户流。

- **黑名单门户 (Blacklist Portal)**：提供关于被列入阻止列表且无法用于获得网络访问权限的个人设备的信息。
- **BYOD 门户 (BYOD Portals)**：使员工能够使用本地请求方调配功能注册其个人设备。
- **证书调配门户 (Certificate Provisioning Portal)**：允许管理员和员工为无法完成 BYOD 流的设备请求用户/设备证书。
- **客户端调配门户 (Client Provisioning Portals)**：强制员工在其设备上下载终端安全评估代理，用来检查合规性。
- **MDM 门户 (MDM Portals)**：使员工能够在外部移动设备管理 (MDM) 系统中登记其移动设备。
- **我的设备门户 (My Devices Portals)**：使员工能够添加和注册个人设备，包括不支持本地请求方调配的个人设备，然后管理这些设备。

通过Cisco ISE，您可以在Cisco ISE 服务器上托管多个设备门户，包括一组预定义的默认门户。默认门户主题具有标准Cisco品牌，您可以通过管理员门户（**管理 (Administration)** > **设备门户管理 (Device**

Portal Management)）对其进行自定义。此外，还可以选择上传组织特有的图片、徽标和级联样式表 (CSS) 文件，进一步自定义门户。

访问设备门户

可以从Cisco ISE GUI 访问任何个人设备门户，如下所示：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)**。

步骤 2 选择您要配置的特定设备门户。

黑名单门户

员工不直接访问该门户，但可被重新定向到该门户。

如果员工丢失个人设备或设备被盗，他们可以在我的设备门户更新设备状态，将设备添加到**黑名单**终端身份组。这可以防止其他人使用该设备进行未经授权的网络访问。如果有人尝试使用黑名单中的某个设备连接网络，他们将被重新定向到 Blacklist 门户，并且被告知该设备禁止接入网络。如果找到设备，员工可以恢复设备（在我的设备门户），在无需重新注册设备的情况下重新获得网络访问权限。根据设备是丢失还是被盗，设备可能需要经过额外调配，才能连接到网络。

您可以为 Blacklist 门户配置端口设置（默认为端口 8444）。如果更改端口号，请确保此端口号未被其他最终用户门户使用。

有关配置黑名单门户的信息，请参阅编辑黑名单门户，第 13 页。

证书调配门户

员工可以直接访问证书调配门户。

通过证书调配门户，员工可以为无法完成自行激活流程的设备请求证书。例如，销售点终端等设备无法完成自带设备流程，需要手动颁发证书。通过证书调配门户，特权用户组可以为此类设备上传证书请求，生成密钥对（如果需要）以及下载证书。

员工可以访问此门户，并使用 CSV 文件请求单个证书或创建批量证书请求。

ISE 社区资源

有关Cisco ISE 证书调配门户的功能和配置的信息，请参阅ISE 2.0：证书调配门户。

自带设备门户

员工无法直接访问该门户。

当员工使用本地请求方注册个人设备时，员工会被重定向至自带设备 (BYOD) 门户。员工首次尝试使用个人设备访问网络时，系统会提示员工手动下载并启动网络设置助理 (NSA) 向导并引导他们完成注册和安装本地请求方。员工注册设备后，就可以使用 My Devices 门户管理设备。

注释 当设备连接到使用 AnyConnect 网络访问管理器 (NAM) 的网络时，不支持 BYOD 流。

相关主题

创建 BYOD 门户，第 15 页
公司网络上的个人设备 (BYOD)，第 1 页

客户端调配门户

员工不直接访问该门户，但可被重新定向到该门户。

客户端调配系统为尝试访问公司网络的设备提供终端安全评估和补救。当员工使用设备请求网络访问时，您可以将他们路由至客户端调配门户，要求他们首先下载终端安全评估代理。终端安全评估代理扫描设备以检查合规性，例如验证设备是否已安装病毒防护软件，操作系统是否受支持。

相关主题

创建客户端调配门户，第 17 页

移动设备管理门户

员工不直接访问该门户，但可被重新定向到该门户。

许多公司使用移动设备管理 (MDM) 系统管理员工的移动设备。

Cisco ISE 允许与外部 MDM 系统集成，员工使用这些系统注册他们的移动设备并访问公司网络。Cisco提供一个外部 MDM 接口，员工可用其注册他们的设备并连接到网络。

MDM 门户允许员工在一个外部 MDM 系统中注册。

员工可使用“我的设备”门户管理他们的移动设备，例如使用PIN码锁定设备、恢复设备出厂设置、或移除注册设备时所安装的应用和设置。

Cisco ISE 允许您为所有外部 MDM 系统设置单个 MDM 门户，或为每个 MDM 系统分别设置一个门户。

有关将 MDM 服务器配置为与Cisco ISE 配合使用的信息，请参阅创建 MDM 门户，第 19 页。

我的设备门户

员工可以直接访问我的设备门户。

某些需要网络接入的网络设备不受本地请求方调配支持，并且无法使用 BYOD 门户进行注册。但是，员工可以使用“我的设备”(My Devices) 门户添加和注册其操作系统不受支持或没有 Web 浏览器的个人设备（例如打印机、互联网广播和其他设备）。

员工可以通过输入设备的 MAC 地址添加和管理新设备。当员工使用“我的设备”(My Devices) 门户添加设备时，Cisco ISE 会将设备添加到“终端”(Endpoints) 窗口（**管理 (Administration)** > **情景可视性 (Context Visibility)** > **终端 (Endpoints)**）作为 **RegisteredDevices** 终端身份组的成员（除非已经静态分配到其他终端身份组）。设备如同Cisco ISE 中的任何其他终端一样进行分析，并且完成注册过程以接入网络。

当用户向“我的设备”(My Devices Portal) 门户中输入一台设备上的两个 MAC 地址时，分析会确定它们具有相同主机名，并在Cisco ISE 中将它们合并为单个条目。例如，用户注册具有有线和无线地址的笔记本电脑。该设备的所有操作（例如删除）对两个地址都会执行。

从门户中删除注册设备时，**DeviceRegistrationStatus** 和 **BYODRegistration** 属性会分别更改为**未注册 (Not Registered)** 和**否 (No)**。但是，当访客（不是员工）使用需要提供凭证的访客门户中的“访客设备注册”(Guest Device Registration) 窗口注册设备时，这些属性保持不变，因为这些 BYOD 属性仅在员工设备注册过程中使用。

无论员工使用 BYOD 门户还是我的设备门户注册其设备，他们都可以使用我的设备门户管理这些设备。

注释 当管理员门户关闭时，“我的设备”(My Devices) 门户不可用。

相关主题

创建我的设备门户 ，第 20 页

BYOD 部署选项和状态流程

支持个人设备的 BYOD 部署流程根据以下因素而略有不同：

- 单或双 SSID：使用单 SSID 时，认证登记、调配和网络访问都使用同一无线本地区域网络 (WLAN)。在双 SSID 部署中，有两个 SSID。一个用来登记和调配，另一个提供安全网络访问。
- Windows、MacOS、iOS 或 Android 设备：无论设备类型如何，本地请求方流程开始时都相似：将使用支持的个人设备的员工重定向至 BYOD 门户以确认其设备信息。此流程因设备类型而异。

员工连接至网络

1. Cisco ISE 根据公司 Active Directory 或其他公司身份存储区对员工的凭证进行身份验证并提供授权策略。
2. 设备被重定向至BYOD门户。设备的MAC地址字段已预配置，用户可以添加设备名称和说明。
3. 已配置本地请求方（MacOS、Windows、iOS、Android），但是此流程因设备而异：
   - MacOS 和 Windows 设备：员工在 BYOD 门户中点击**注册 (Register)** 以下载和安装请求方调配向导（网络设置助理），此向导会配置请求方并提供证书（如果必要），用于基于EAP-TLS 证书的身份验证。颁发的证书嵌有设备的 MAC 地址和员工的用户名。

注释 网络设置助理无法下载到 Windows 设备，除非该设备的用户具有管理权限。如果无法授予最终用户管理权限，则使用组策略对象 (GPO) 将证书推送到用户的设备，而不是使用 BYOD 流。

注释 从 MacOS 10.15 开始，用户必须允许下载请求方调配向导 (SPW)。用户设备上会显示一个窗口，要求他们允许或拒绝从Cisco ISE 服务器下载。

- iOS 设备：Cisco ISE 策略服务器使用 Apple 的 iOS 空中下载功能向 IOS 设备发送新配置文件，其中包括：
  - 颁发的证书（如已配置）嵌有 IOS 设备的 MAC 地址和员工的用户名。
  - 强制使用 EAP-TLS 进行 802.1X 身份验证的 Wi-Fi 请求方配置文件。
- Android 设备：Cisco ISE 会提示并引导员工从 Google Play 商店下载网络设置助理 (NSA)。安装应用后，员工可以打开 NSA 并启动设置向导，该向导会生成请求方配置和用于配置设备的已颁发证书。

4. 在用户完成激活流程后，Cisco ISE 会发起授权更改 (CoA)。这会导致 MacOS、Windows 和 Android 设备重新连接到安全 802.1X 网络。对于单 SSID，iOS 设备也会自动连接；但是对于双 SSID，向导会提示 iOS 用户手动连接新网络。

注释 您可以配置不使用请求方的 BYOD 流。请参阅Cisco ISE 社区文档https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning。

注释 仅在隐藏实际 Wi-Fi 网络时，选中**目标网络隐藏时启用 (Enable if Target Network is Hidden)** 复选框。否则，不能为某些 iOS 设备调配 Wi-Fi 网络配置，尤其是在单 SSID 流中（在这种情况下，激活和连接使用同一个 Wi-Fi 网络或 SSID）。

BYOD 会话终端属性

终端属性 *BYODRegistration* 的状态在 BYOD 流期间更改为以下状态。

- 未知 *(Unknown)*：设备尚未通过 BYOD 流。
- 是 *(Yes)*：设备已通过 BYOD 流，并已注册。
- 否 *(No)*：设备已通过 BYOD 流，但未注册。这意味着设备已删除。

设备注册状态终端属性

终端属性 *DeviceRegistrationStatus* 的状态在设备注册期间更改为以下状态。

- 已注册 *(Registered)*：设备已通过 BYOD 流，并且已注册。属性从待处理状态更改为已注册状态之间有 20 分钟的延迟。
- 待处理 *(Pending)*：设备已通过 BYOD 流，并且已注册。但是，Cisco ISE 尚未在网络上看到它。
- 未注册 *(Not Registered)*：设备尚未通过 BYOD 流。未注册 *(Not Registered)* 是 *DeviceRegistrationStatus* 属性的默认状态。
- 被盗 *(Stolen)*：用户登录我的设备门户，并将当前已激活的设备标记为“被盗”(Stolen)。这会在以下情况下发生：
  - 如果设备是通过调配证书和配置文件激活的，则Cisco ISE 会撤销调配到设备的证书，并将设备的 MAC 地址分配给**黑名单**终端身份组。该设备不再具有网络访问权限。
  - 如果设备是通过调配配置文件（无证书）激活的，则Cisco ISE 会将设备分配到**黑名单**终端身份组。设备仍然具有网络访问权限，除非您为此情况创建授权策略。例如，**IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess**。

  管理员执行能够禁用多个设备的网络访问的操作，如删除或撤销证书。

  如果用户恢复被盗的设备，则状态会恢复为未注册 *(Not Registered)*。用户必须删除该设备，然后重新添加。这会启动激活过程。
- 丢失 *(Lost)*：用户登录“我的设备”门户，并将当前已激活的设备标记为丢失 *(Lost)*，从而导致以下操作：
  - 设备被分配到**黑名单**身份组。
  - 调配到设备的证书不会被撤销。
  - 设备状态更新为丢失 *(Lost)*。
  - *BYODRegistration*状态更新为否 *(No)*。

  除非创建授权策略来阻止丢失的设备，否则丢失的设备仍具有网络访问权限。您可以在规则中使用**黑名单**身份组或 *endpoint:BYODRegistration* 属性。例如，**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD**。如需更精细的访问，还可以将 *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST”*，*InternalUser:IdentityGroup Equals* <<*group*>> 添加到规则的 IF 部分。

限制员工注册的个人设备的数量

可以允许员工注册 1 至 999 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。

步骤 2 在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

步骤 3 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

支持使用本地请求方注册设备

您可以创建本地请求方配置文件来支持Cisco ISE 网络上的个人设备。根据您与用户的授权要求相关联的配置文件，Cisco ISE 提供必要的请求方向导来设置用户的个人设备以访问网络。

员工首次尝试使用个人设备访问网络时，系统会自动引导其完成注册和请求方配置。在其注册设备后，可以使用我的设备门户管理其设备。

本地请求方支持的操作系统

以下操作系统支持本地请求方：

- Android（Amazon Kindle 和 B&N Nook 除外）
- Mac OS（适用于 Apple Mac 计算机）
- Apple iOS 设备（Apple iPod、iPhone 和 iPad）
- Microsoft Windows 7 和 8（RT 除外）、Vista 和 10

允许员工使用需要提供凭证的访客门户注册个人设备

使用需要提供凭证的访客门户的员工可以注册其个人设备。员工通过 BYOD 门户提供的自行调配流程可以使用本地请求方（可用于 Windows、MacOS、iOS 和 Android 设备）将设备直接连接至网络。

开始之前

您必须创建本地请求方配置文件。

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

步骤 2 选择您希望允许员工用于使用本地请求方注册其个人设备的需要提供凭证的访客门户，然后点击 **Edit**。

步骤 3 点击**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡。

步骤 4 在 **BYOD 设置 (BYOD Settings)** 下，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 5 点击**保存 (Save)**。

提供用于重新连接 BYOD 注册流程的 URL

您可以提供信息，让使用 BYOD 门户注册其个人设备遇到问题的员工重新连接到注册过程。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **重试 URL (Retry URL)**。

步骤 2 在**重试激活 URL (Retry URL for onboarding)** 字段中，输入用于将设备重定向至Cisco ISE 的 URL。

当设备在注册过程中遇到问题时，它将尝试自动重新连接到互联网。此时，您在此处输入的URL 会将设备重定向到Cisco ISE（重新启动激活过程）。默认值为 192.0.2.123。

步骤 3 点击**保存 (Save)**。

如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

设备门户配置任务

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和Cisco ISE提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

在创建新门户或编辑默认门户后，您必须授权使用该门户。授权使用门户后，您所进行的任何后续配置更改便会立即生效。

不需要授权使用我的设备门户。

如果您选择删除门户，则必须先删除与其关联的任何授权策略规则和授权配置文件，或者将其修改为使用其他门户。

使用以下针对配置不同设备门户相关任务编制的表格。

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
启用策略服务，第 10 页	必填	必填	必填	必填	必填
将证书添加到设备门户，第 11 页	必填	必填	必填	必填	必填
创建外部身份源，第 11 页	不是必填项	不是必填项	不是必填项	不是必填项	必填

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
创建身份源序列，第 12 页	不是必填项	不是必填项	不是必填项	不是必填项	必填
创建终端身份组，第 12 页	不是必填项	必填	不是必填项	必填	必填
编辑黑名单门户，第 13 页	必填	不适用	不适用	不适用	不适用
创建 BYOD 门户，第 15 页	不适用	必填	不适用	不适用	不适用
创建客户端调配门户，第 17 页	不适用	不适用	必填	不适用	不适用
创建 MDM 门户，第 19 页	不适用	不适用	不适用	必填	不适用
创建我的设备门户，第 20 页	不适用	不适用	不适用	不适用	必填
创建授权配置文件，第 21 页	不适用	必填	必填	必填	不是必填项
自定义设备门户，第 23 页	可选	可选	可选	可选	可选

启用策略服务

为了支持Cisco ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 点击节点并点击**编辑 (Edit)**。

步骤 3 在**常规设置 (General Settings)** 选项卡下，启用**策略服务 (Policy Service)** 切换按钮。

步骤 4 选中**启用会话服务 (Enable Session Services)** 复选框。

步骤 5 点击**保存 (Save)**。

将证书添加到设备门户

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为**默认门户证书组 (Default Portal Certificate Group)**。

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

步骤 2 添加一个系统证书并将其分配到您希望用于该门户的证书组标签。

在创建或编辑门户期间，此证书组标签可供选择。

步骤 3 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （**任意门户**） > **创建或编辑 (Create or Edit)** > **门户设置 (Portal Settings)**。

步骤 4 从与新添加证书关联的 **Certificate Group Tag** 下拉列表中选择特定的证书组标签。

注释

- BYOD 不支持超过三个证书的证书链。
- 在 BYOD 激活期间，系统会为 iOS 设备颁发两次证书。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务 提供程序。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅 将 Active Directory 用作外部身份源。
- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅 LDAP。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅 RADIUS 令牌身份源。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅 RSA 身份源。

- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅 SAMLv2 身份提供者作为外部身份源。
- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

创建终端身份组

Cisco ISE 将其所发现的终端划分至相应的终端身份组。Cisco ISE 拥有若干个系统定义的终端身份组。您还从 Endpoint Identity Groups 页面创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

步骤 4 为您想要创建的终端身份组输入**说明**。

步骤 5 点击**父级组 (Parent Group)** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

步骤 6 点击**提交 (Submit)**。

编辑黑名单门户

Cisco ISE 提供一个黑名单门户，它会在被列入Cisco ISE 阻止列表的丢失或被盗设备试图访问您的公司网络时显示信息。

您只能编辑默认门户设置以及自定义为门户显示的默认消息。您不能创建新的黑名单门户，也不能复制或删除默认门户。

开始之前

确保您具有为配合此门户使用而配置的证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portal)** > **编辑 (Edit)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用 **语言 (Languages)** 菜单导出和导入要与门户一起使用的语言文件。

步骤 4 点击**门户测试 URL** 链接以打开显示此门户 URL 的新浏览器标签页。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

注释　测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

步骤 5 在 **Portal Settings** 中更新证书组标签、语言等的默认值，然后定义适用于整个门户的行为。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释　我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x**、**x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。

- **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
- **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

步骤 6 在 **Portal Page Customization** 选项卡中，自定义在未授权的设备试图获取网络访问权限时显示在门户中的页面标题和消息文本。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

创建 BYOD 门户

可以提供自带设备 (BYOD) 门户，使员工能够注册其个人设备，以便可在允许访问网络之前完成注册和请求方配置。

您可以创建新 BYOD 门户，也可以编辑或复制现有 BYOD 门户。您可以删除任何 BYOD 门户，包括Cisco ISE 提供的默认门户。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新 **Support Information Page Settings** 以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在**门户页面自定义 (Portal Page Customization)** 选项卡上，自定义配置过程中在以下页面上显示的**内容区域 (Content Area)** 消息文本。

- **BYOD 欢迎 (BYOD Welcome)** 页面：
  - **需要设备配置 (Device Configuration Required)**：输入当设备首次重定向到 BYOD 门户并需要证书调配时应显示的内容。
  - **证书需要更新 (Certificate Needs Renewal)**：输入当需要更新先前证书时应显示的内容。

- **BYOD 设备信息 (BYOD Device Information)** 页面：
  - **达到最大设备数 (Maximum Devices Reached)**：输入当达到员工可注册的设备的最大限制时应显示的内容。
  - **需要的设备信息 (Required Device Information)**：输入当请求需要的设备信息以使员工能够注册设备时应显示的内容。
- **BYOD 安装 (BYOD Installation)** 页面：
  - **桌面安装 (Desktop Installation)**：输入当提供桌面设备的安装信息时应显示的内容。
  - **iOS 安装 (iOS Installation)**：输入当提供 iOS 移动设备的安装说明时应显示的内容。
  - **Android 安装 (Android Installation)**：输入当提供 Android 移动设备的安装说明时应显示的内容。
- **BYOD 成功 (BYOD Success)** 页面：
  - **成功 (Success)**：输入当设备已配置并自动连接到网络时应显示的内容。
  - **成功：手动说明 (Success: Manual Instructions)**：输入当设备配置成功并且员工必须手动连接到网络时应显示的说明。
  - **成功：不受支持的设备 (Success: Unsupported Device)**：输入当允许不受支持的设备连接到网络时应显示的内容。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

创建证书调配门户

对于无法完成登录流程的设备，Cisco ISE 提供证书调配门户，允许您为其申请证书。例如，销售点终端。使用 CSV 文件，您可以申请单个证书或进行批量证书申请。

您可以编辑默认门户设置以及自定义在门户中显示的消息。您还可以创建、复制和删除证书调配门户。

以下两种类型的用户可以访问证书调配门户：

- 具备管理权限的内部或外部用户：能够为他们自己及其他人生成证书。
- 所有其他用户：只能为自己生成证书。

分配有超级管理员或 ERS 管理员权限的用户（网络访问用户）有权访问该门户，并且可以为其他人申请证书。但是，如果您创建一个新的内部管理员用户，并为其分配超级管理员或 ERS 管理员权限，内部管理员用户将无权访问此门户。您必须首先创建一个网络访问用户，并将该用户添加到超

级管理员或ERS管理员组。添加至超级管理员或ERS管理员组的所有现有网络访问用户可以访问此门户。

对于能够访问该门户并为自己生成证书的其他用户，请配置“证书调配门户”(Certificate Provisioning Portal) 设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配 (Certificate Provisioning)** > **编辑 (Edit)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。确保您在**身份验证方法 (Authentication Method)** 下选择适当的身份源或身份源序列，并且在**配置授权组 (Configure Authorized Groups)** 下选择用户组。属于您所选择用户组的所有用户可以访问该门户，并且可以生成自己的证书。

开始之前

确保您具有为配合此门户使用而配置的证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配 (Certificate Provisioning)** > **创建 (Create)**。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 2 在 **门户名称** 中提供唯一的门户名称，并在 **说明** 中提供门户说明。

步骤 3 使用“**语言文件**”**(Language File)** 菜单导出和导入要与门户一起使用的语言文件。

步骤 4 在 **Portal Settings** 中更新证书组标签、语言等的默认值，然后定义适用于整个门户的行为。

步骤 5 在“**门户页面定制**”**(Portal Page Customization)** 选项卡上，请自定义在门户中显示的页面标题和消息文本。

步骤 6 点击**保存 (Save)**，然后点击**关闭 (Close)**。

创建客户端调配门户

可以提供一个客户端调配门户，使员工可以下载Cisco AnyConnect 终端安全评估组件，此组件或代理将在允许设备访问网络之前验证设备的终端安全评估合规性。

您可以创建新 Client Provisioning 门户，也可以编辑或复制现有 Client Provisioning 门户。您可以删任意 Client Provisioning 门户，包括Cisco ISE 提供的默认门户。

分配有超级管理员或 ERS 管理员权限的用户（网络访问用户）有权访问该门户。但是，如果您创建一个新的内部管理员用户，并为其分配超级管理员或 ERS 管理员权限，内部管理员用户将无权访问此门户。您必须首先创建一个网络访问用户，并将该用户添加到超级管理员或 ERS 管理员组。添加至超级管理员或 ERS 管理员组的所有现有网络访问用户可以访问此门户。

对于能够访问该门户并为自己生成证书的其他用户，请配置“证书调配门户”(Certificate Provisioning Portal) 设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配 (Client Provisioning)** > **编辑 (Edit)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。确保您在**身份验证方法 (Authentication Method)** 下选择适当的身份源或身份源序列，并且在**配置授权组 (Configure**

Authorized Groups) 下选择用户组。属于您所选择用户组的所有用户可以访问该门户，并且可以生成自己的证书。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保已为此门户配置必需的证书和客户端调配策略。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配 (Client Provisioning)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新 **Support Information Page Settings** 以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在 **Portal Page Customization** 选项卡上，自定义在调配过程中在 Client Provisioning 门户上显示的 **Content Area** 消息文本：

a) 在**客户端调配门户 (Client Provisioning Portals)** 页面上：

- **未知代理 (Agent Unknown)**：输入当代理未知时应显示的内容。
- **检查、扫描和合规 (Checking, Scanning and Compliant)**：输入当终端安全评估代理已安装成功并且检查、扫描和验证设备是否符合终端安全评估要求时应显示的内容。
- **不合规 (Non-compliant)**： 输入当终端安全评估代理确定设备不符合终端安全评估要求时应显示的内容。

b) 在 Client Provisioning (Agent Not Found) 页面上：

- **未找到代理 (Agent Not Found)**：输入在设备上未检测到终端安全评估代理时应显示的内容。
- **手动安装说明 (Manual Installation Instructions)**：输入当设备上未安装 Java 或 Active X 软件时应显示的内容，说明如何手动下载和安装终端安全评估代理。
- **安装，无 Java/ActiveX (Install, No Java/ActiveX)**：输入当设备上未安装 Java 或 Active X 软件时应显示的内容，说明如何下载和安装 Java 插件。
- **已安装代理 (Agent Installed)**：输入在设备上检测到终端安全评估代理时应显示的内容，说明如何启动终端安全评估代理以检查设备是否符合终端安全评估要求。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

相关主题

授权门户
自定义设备门户，第 23 页

创建 MDM 门户

您可以提供移动设备管理 (MDM) 门户，以使员工能够管理其注册以供在公司网络上使用的移动设备。

您可以创建新 MDM 门户，也可以编辑或复制现有 MDM 门户。您可以为所有 MDM 系统创建单个 MDM 门户，也可以为每个系统创建一个门户。您可以删除任何 MDM 门户，包括Cisco ISE 提供的默认门户。默认门户用于第三方 MDM 提供商。

您可以创建新 MDM 门户，也可以编辑或复制现有 MDM 门户。您可以删除任何 MDM 门户，包括 Cisco ISE 提供的默认门户。默认门户用于第三方 MDM 提供商。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **移动设备管理 (Mobile Device Management)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新以下适用于每个特定页面的设置：

- 在**员工移动设备管理设置 (Employee Mobile Device Management Settings)** 中，访问提供用于配置第三方 MDM 提供商的链接，然后使用 MDM 门户定义员工的接受策略行为。
- **支持信息页面设置 (Support Information Page Settings)**，用于帮助访客提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在**门户页面自定义 (Portal Page Customization)** 选项卡上，自定义设备注册过程中显示在 MDM 门户中的**内容区域 (Content Area)** 消息。

- **无法接通 (Unreachable)**：输入当无法访问所选 MDM 系统时显示的内容。

- **不合规 (Non-compliant)**：输入当正在注册的设备不符合 MDM 系统要求时显示的内容。
- **继续 (Continue)**：输入当设备在发生连接问题的情况下尝试连接网络时显示的内容。
- **注册 (Enroll)**：输入当设备需要 MDM 代理并需要在 MDM 系统中注册时显示的内容。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。另请参阅以下主题：

- 将证书添加到设备门户 ， 第 11 页
- 创建终端身份组 ， 第 12 页
- 创建授权配置文件 ， 第 21 页
- 自定义设备门户 ， 第 23 页

创建我的设备门户

您可以提供我的设备门户，以使员工能够添加并注册其个人设备，这些设备不支持本地请求方且无法使用自带设备 (BYOD) 门户进行添加。然后，您可以使用我的设备门户管理已使用任一门户添加的所有设备。

您可以创建新的我的设备门户，也可以编辑或复制现有我的设备门户。您可以删除任何我的设备门户，包括Cisco ISE 提供的默认门户。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书、外部身份存储区、身份源序列和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备 (My Devices)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新 **Portal Settings** 中的端口、证书组标签、身份源序列、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新以下适用于每个特定页面的设置：

- **登录页面设置 (Login Page Settings)**：指定员工凭证和登录准则。
- **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)**：添加单独的 AUP 页面，并规定员工的可接受使用政策行为。
- **登录后横幅页面设置 (Post-Login Banner Page Settings)**：在员工登录到门户后向其通知其他信息。
- **员工更改密码设置 (Employee Change Password Settings)**：允许员工更改其自己的密码。仅在员工是内部用户数据库的一部分时，才会启用此选项。

步骤 6 在 **Portal Page Customization** 选项卡中，自定义注册和管理过程中显示在我的设备门户中的以下信息：

- 标题、说明、内容、字段和按钮标签
- 错误消息和通知消息

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

如果希望更改门户外观，您可以对其进行自定义。请参阅

相关主题

自定义设备门户 ，第 23 页
我的设备门户 ，第 4 页
显示员工添加的设备 ，第 23 页

创建授权配置文件

当授权门户时，将会设置网络访问的网络授权配置文件和规则。

开始之前

您必须先创建门户，然后才能对其进行授权。

步骤 1 为门户设置特殊授权配置文件。

步骤 2 为配置文件创建授权策略规则。

创建授权配置文件

各门户要求您为其设置特殊的授权配置文件。

开始之前

如果不打算使用默认门户，您必须先创建门户以便将门户名称与授权配置文件关联。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 使用您希望授权门户使用的名称创建授权配置文件。

下一步做什么

您应当创建门户授权策略规则，用于新创建的授权配置文件。

创建授权策略规则

要配置供门户在响应用户（访客、发起人、员工）的访问请求时使用的重定向 URL，请为该门户定义授权策略规则。

url-redirect 会根据门户类型采取以下形式，其中：

ip:port：IP 地址和端口号

PortalID：唯一端口名称

对于热点访客门户：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

对于移动设备管理 (MDM) 门户：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

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 Sets)** 以在**标准 (Standard)** 策略下创建新授权策略。

步骤 2 对于**条件 (Conditions)**，请选择要用于门户验证的终端身份组。例如，对于热点访客门户，选择默认的 **GuestEndpoints** 终端身份组；而对于 MDM 门户，选择默认的 **RegisteredDevices** 终端身份组。

注释 由于热点访客门户仅颁发终止 CoA，请不要将 Network Access:UseCase EQUALS Guest Flow 用作热点访客授权策略中的一个验证条件。而是匹配终端归属的身份组用于验证。例如，

- 如果为访客终端 + 无线 MAB，则允许访问
- 如果为无线 MAB，则热点重定向

步骤 3 对于 **Permissions**，请选择创建的门户授权配置文件。

注释 在使用启用了 MAC 选项的字典属性创建授权条件（例如 RADIUS.Calling-Station-ID）时，必须使用 Mac 运算符（例如 Mac_equals）支持不同的 MAC 格式。

自定义设备门户

可以通过自定义门户主题、更改门户页面上的UI元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户（访客、发起人，在适当的情况下也可以是员工）体验。有关自定义门户的详细信息，请参阅 自定义最终用户 Web 门户。

管理员工添加的个人设备

当员工使用自带设备 (BYOD) 或我的设备门户注册设备时，此注册设备将显示在**终端 (Endpoints)** 列表中。虽然员工可以通过删除设备取消该设备与其帐户之间的关联，但设备依然留在Cisco ISE 数据库中。因此，当员工使用自己的设备时，可能需要您协助他们解决遇到的错误。

显示员工添加的设备

您可以使用**终端 (Endpoints)** 列表窗口上显示的**门户用户 (Portal User)** 字段查找特定员工添加的设备。如果需要删除特定用户注册的设备，这可能会有所帮助。默认情况下，此字段不显示，因此在搜索之前必须先将其启用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 在 Dashlet 下方，点击终端列表右上角可用的**设置 (Settings)** 图标。

步骤 3 选中**门户用户 (Portal User)**复选框启用**门户用户 (Portal User)**切换按钮以在终端列表中显示这些信息。

步骤 4 点击 **Go**（前往）。

步骤 5 点击**过滤器 (Filter)** 下拉列表，并选择**快速过滤器 (Quick Filter)**。

步骤 6 在 **Portal User** 字段中输入用户的名称，以仅显示分配给该特定用户的终端。

向我的设备门户添加设备时出错

如果设备已由其他员工添加，并且该设备仍在终端数据库中，则员工无法添加该设备。

如果员工尝试添加Cisco ISE 数据库中已存在的设备：

- 如果设备支持本地请求方调配，则我们建议通过 BYOD 门户添加设备。此操作将覆盖该设备最初添加到网络时创建的任何注册详细信息。
- 如果该设备是 MAC 身份验证绕行 (MAB) 设备，如打印机，则必须先解决设备的所有权。如果适当，您可以使用管理员的门户从终端数据库中删除该设备，以便新的所有者可以使用“我的设备”(My Devices) 门户成功添加该设备。

注释 当管理员门户关闭时，“我的设备”(My Devices) 门户不可用。

从我的设备门户删除的设备仍保留在终端数据库中

当员工从“我的设备”(My Devices) 门户删除设备时，系统会从员工的已注册设备列表删除设备，但是设备仍保留在Cisco ISE 终端数据库中并且显示于**终端 (Endpoints)** 列表上。

您可以从“终端”(Endpoints) 窗口永久删除设备。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

限制员工注册的个人设备的数量

可以允许员工注册 1 至 999 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。

步骤 2 在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

步骤 3 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

监控我的设备门户和终端活动

Cisco ISE 提供各种报告和日志，您可以通过这些报告和日志查看终端与用户管理信息以及访客与发起人活动。

您可以按需或按计划运行这些报告。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)**。

步骤 2 选择**访客 (Guest)** 或**终端和用户 (Endpoints and Users)** 以查看各种访客、发起人和终端相关报告

步骤 3 选择要使用**过滤器 (Filters)** 下拉列表搜索的数据。

步骤 4 在 **Time Range** 中选择您想要查看的数据的时间范围。

步骤 5 点击**运行 (Run)**。

我的设备登录和审核报告

我的设备登录和审核 (My Devices Login and Audit) 报告是跟踪以下信息的一种综合报告：

- 员工在 My Devices 门户上的登录活动。
- 员工在“我的设备”(My Devices) 门户中执行的与设备相关的操作。

此报告位于： **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **访客 (Guest)** > **我的设备登录和审核 (My Devices Login and Audit)**。

注册的终端报告

注册终端 (Registered Endpoints) 报告提供有关由员工注册的所有终端的信息。此报告位于： **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **注册终端 (Registered Endpoints)**。可以过滤**身份 (Identity)**、**终端 ID (Endpoint ID)**、**身份组 (Identity Group)**、**终端配置文件 (Endpoint Profile)** 等属性并生成报告。

可以查询分配给**注册设备 (Registered Devices)** 终端身份组的终端的终端数据库。还可以为将**门户用户 (Portal User)** 属性设置为非空值的特定用户生成报告。

注册终端 (Registered Endpoints) 报告提供有关选定时间段内由特定用户通过设备注册门户注册的终端列表的信息。