Cisco Business Dashboard 和 Probe 管理指南，版本 2.5

首次发布日期: 2020 年 7 月 14 日

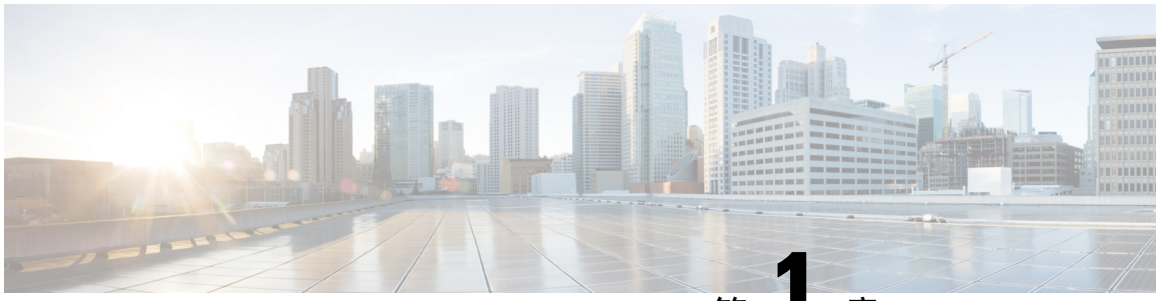
上次修改日期: 2022 年 7 月 27 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

 Java 徽标是 Sun Microsystems, Inc. 在美国或其他国家/地区的商标或注册商标。

目录



第 1 章

Cisco Business Dashboard概况

本章包含以下各节：

关于Cisco Business Dashboard

Cisco Business Dashboard 为您监控和管理 Cisco Business 网络中的设备提供了有用的工具。它能自动发现您的网络，便于您配置和监控所有受支持设备（例如交换机、路由器和无线接入点）。另外，当有可用的固件更新，以及设备保修期或支持合同过期时，它会向您发出通知。

Cisco Business Dashboard 是一款分布式应用，由两个单独的组件（应用）组成，具体如下：

Dashboard

Cisco Business Dashboard（也称为 *Dashboard*）安装在网络中的一个便利的位置。在 Dashboard 的用户界面上，可以获得网络中所有站点状态的概要视图，也可以集中关注单个站点或设备以查看特定于该站点或设备的信息。

Probe

Cisco Business Dashboard Probe（也称为 *Probe*）安装在网络中的各个站点，并与 Dashboard 相关联。Probe 执行网络发现并代表 Dashboard 直接与各受管设备通信。

注释 某些网络设备支持直接与 Dashboard 关联并在不存在 Probe 的情况下进行管理。当以这种方式直接管理网络设备时，所有管理功能均可用于设备，但网络发现过程可能不像存在 Probe 的情况下全面。

受众

本指南主要面向负责安装和管理 Cisco Business Dashboard 软件的网络管理员。

新版本信息和更新

本节提供有关截至 2022 年 9 月的思科业务仪表板版本 2.5.x 中的新功能的信息。

Table 1: 思科业务仪表板（***2.5.1*** 版）中的新功能和更改的行为

功能	说明	记录位置
无线网络访客门户	无线网络的访客门户可由思科业务仪表板集中托管。	看配置无线局域网, on page 49 看 配置访客门户, on page 51

Table 2: 思科业务仪表板 ***2.5*** 版中的新功能和更改的行为。

功能	说明	记录位置
无线配置增强功能	现在可以管理其他无线配置，包括无线电设置、射频优化、恶意接入点和干扰源检测。	看 查看详细设备信息, on page 29 看配置无线局域网, on page 49 看配置无线电, on page 50
用于基于用户的网络访问的身份验证服务	可以使用思科业务仪表板作为身份验证服务器，在无线LAN和交换机端口上启用基于用户的身份验证。See关于端口管理, on page 39	看 配置无线局域网, on page 49 看 用户, on page 86 看 安全注意事项常见问题, on page 144
新通知	添加了其他通知，用于标识设备的管理密码何时过期，以及当前设备配置与所需配置何时不匹配。	看 支持的通知, on page 129
让我们从 GUI 加密证书管理	让我们加密证书现在可以完全通过管理 GUI 进行安装和管理。	看 管理证书, on page 99

Dashboard 和 Probe 的系统要求已更新。有关详细信息，请参阅相关文档, on page 3中的《安装指南》。

所有正式版本说明均载于 Cisco Business Dashboard 版本说明中。

.

相关文档

Cisco Business Dashboard 文档由许多单独的指南组成，其中包括：

- **管理指南（即本文档）**-这是一份参考指南，详细介绍该软件提供的所有功能和选项，以及其配置和使用方法。
- **设备支持列表** - 此列表提供 Cisco Business Dashboard 支持设备以及每种设备类型可用功能的详细信息。有关 Cisco Business Dashboard 支持的所有设备列表，请参阅 Cisco Business Dashboard 技术参考。
- **快速入门指南** - 此指南详细介绍如何使用最常用的选项对 Cisco Business Dashboard 进行初始设置。有关管理网络所需执行的基本任务的概述，请参阅 Cisco Business Dashboard Probe 快速入门指南。
- **版本说明** - 这些文档列出了每个新固件版本的所有新功能和修复程序。您可以在 Cisco Business Dashboard 版本说明中找到它们。
- **安装指南**

  下表列出了可部署在不同平台上的 Cisco Business Dashboard 软件的所有安装指南。

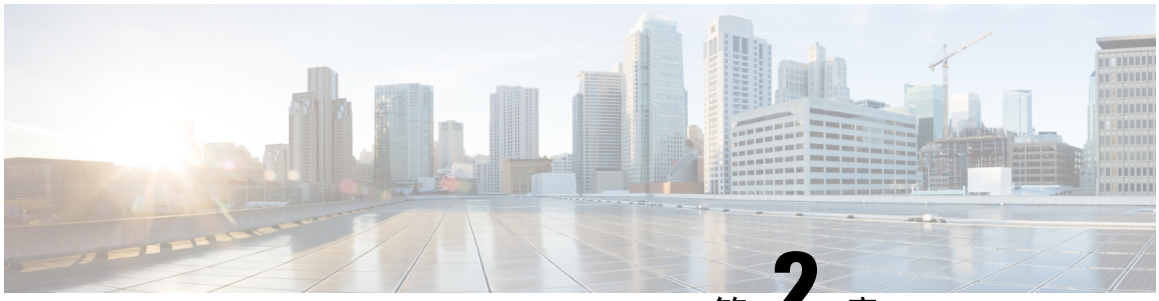
  有关 Cisco Business Dashboard 和 Cisco Business Dashboard Probe 的系统要求，请参阅这些指南。

支持的平台	位置
Amazon Web Services	面向 Amazon Web Services (AWS) 的 Cisco Business Dashboard 安装指南
Micorsoft Azure	面向 Microsoft Azure 的 Cisco Business Dashboard 安装指南
Oracle VirtualBox	面向 Oracle VirtualBox 的 Cisco Business Dashboard 和 Probe 安装指南
Microsoft Hyper-V	面向 Microsoft Hyper-V 的 Cisco Business Dashboard 安装指南
VMware vSphere、Workstation 和 Fusion	面向 VMware 的 Cisco Business Dashboard 和 Probe 安装指南
Ubuntu Linux（Dashboard 和 Probe）及 Raspbian Linux（仅限 Probe）	面向 Linux 的 Cisco Business Dashboard 和 Probe 安装指南

术语

术语	说明
Hyper-V	Microsoft Corporation 提供的虚拟化平台。

术语	说明
开放式虚拟化格式 (OVF)	TAR 存档，包含一个或多个 OVF 格式的虚拟机。这是一种不限定于平台的虚拟机 (VM) 封装和分布方法。
开放式虚拟设备或应用程序 (OVA) 文件	包含以下虚拟机描述文件，并以 **.TAR** 封装形式保存为单一存档的程序包： • 描述符文件 (.OVF) • Manifest (.MF) 和证书文件（可选）
Raspberry Pi	Raspberry Pi Foundation 开发的一种成本极低的单板计算机。有关详细信息，请参阅 *https://www.raspberrypi.org/*。
Raspberry Pi OS	Raspberry Pi OS 旧称 Raspbian，是面向基于 Debian 的 Linux 发行版操作系统而优化的 Raspberry Pi。有关更多信息，请参阅 *https://www.raspberrypi.org/software/*。
VirtualBox	Oracle Corporation 提供的虚拟化平台。
虚拟硬盘 (VHD)	虚拟硬盘是存储硬盘驱动器完整内容的磁盘映像文件格式。
虚拟机 (VM)	可以运行访客操作系统及相关应用程序软件的虚拟计算环境。在同一主机系统中可并行运行多个 VM。
• VMware ESXi • VMware Fusion • vSphere Server • VMware Workstation	VMware Inc. 提供的虚拟化平台。
vSphere 客户端	使用户可以从任何 Windows PC 远程连接到 vCenter Server 或 ESXi 的用户界面。用户可以使用 vSphere Client 的主接口创建、管理和监控 VM 以及 VM 的资源和主机。vSphere Client 还可提供通过控制台访问 VM 的权限。
虚拟机监控程序	也称为虚拟机监控系统或 VMM，是专门用于创建和运行虚拟机 (VM) 的软件。借助虚拟机监控程序，用户可以在一台主机计算机上支持多个访客 VM，这些访客 VM 将以虚拟方式共享该主机计算机的资源（例如内存和进程）。
Amazon Web Services (AWS)	一个按需云计算平台。
Micosoft Azure Active Directory	一种基于云的身份和访问管理服务，可提供单点登录和多因素身份验证，帮助用户防范 99.9% 的网络安全攻击。



第 2 章

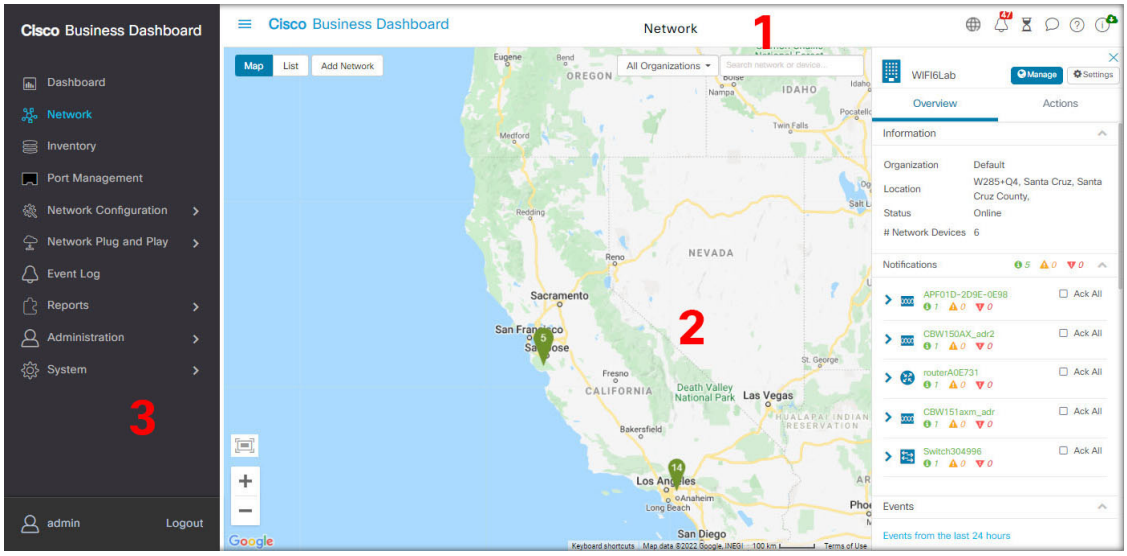
使用 Cisco Business Dashboard & Probe

本章包含以下各节：

使用 Cisco Business Dashboard GUI

本章概述 Cisco Business Dashboard GUI，包括导航窗格链接的说明。

主页窗口



1. **标题**窗格

   标题工具栏包含以下选项：

   - 显示导航窗格的菜单按钮

- 标题文本
- 一系列功能图标，例如语言选择、通知、任务活动、反馈、上下文相关帮助及版本信息。

2. **工作**窗格是功能界面的显示区域。

   当点击**导航**窗格中的选项时，对应的窗口将在此区域打开。

3. **导航**窗格提供访问 Cisco Business Dashboard 功能的选项。点击**菜单**图标时，会显示导航窗格；做出选择后，导航窗格会滑动离开。

   当前登录用户显示在导航窗格底部。

导航窗格选项

导航窗格提供访问Cisco Business Dashboard 主要功能的选项。

图标	说明
	通过 **Dashboard**，您可以监控网络性能随时间推移的变化情况。Dashboard 还可用于监控流量级别、连接的设备数以及有关网络的其他详细信息。
	**网络**图标以地图或列表的形式显示网络中所有位置的概况。它还包含每个网络及所发现的设备的不同视图。视图包括网络拓扑和平面图视图，使您可以跟踪网络的物理布局。
	**设备清单**工具提供网络中所有设备的列表，使您可以查看设备的详细信息，并执行更新固件、备份配置和重新启动等操作。
	**端口管理**选项提供所有网络设备的前面板视图，并且可用于查看有关各个端口的详细信息以及进行配置更改。
	通过**网络配置**页面，您可以管理用于您的网络的配置文件。
	利用 **Network Plug and Play** 页面，可以实现网络设备的零接触部署，让它们在安装时自动从 Cisco Business Dashboard 下载固件和配置文件。
	**事件日志**页面提供网络中发生的所有事件的列表，并允许使用过滤器将结果限制为仅包含需要关注的事件。
	**报告**选项将显示许多提供网络设备生命周期信息的报告，包括生命周期终止公告、保修信息和服务合同详细信息。

图标	说明
	通过**管理**页面可维护 Cisco Business Dashboard。
	**系统**页面用于管理 Cisco Business Dashboard 应用。
	当前登录用户与**注销**选项一起显示在导航栏底部。点击用户名将显示用户配置文件页面。

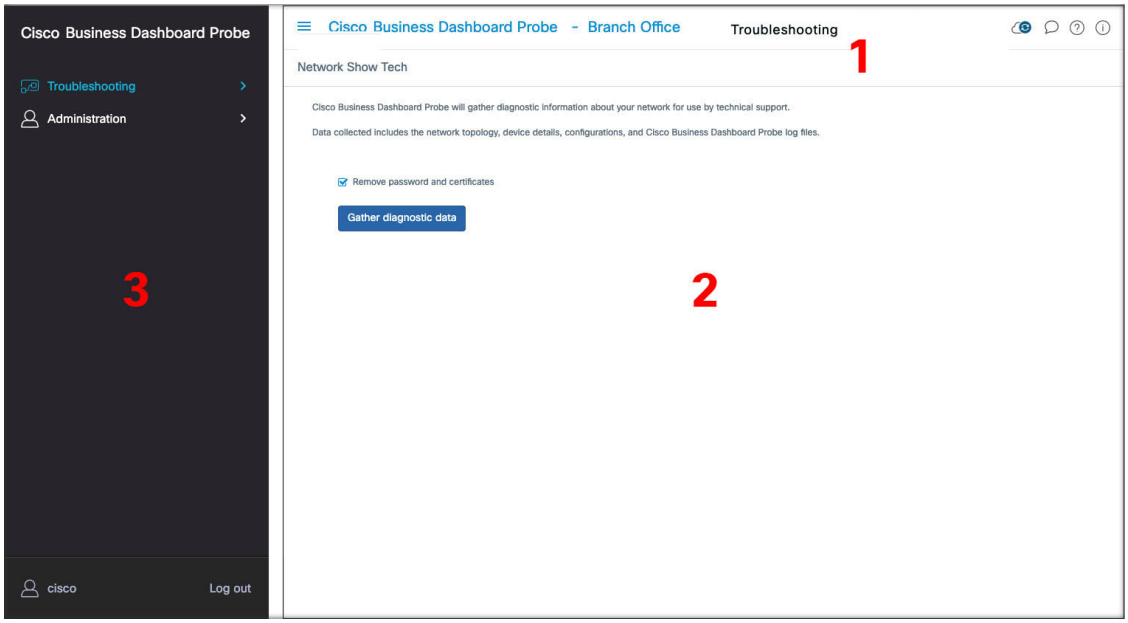
标题工具栏选项

标题工具栏可用于访问其他系统功能，并会显示系统通知。

图标	说明
	**菜单按钮**位于标题左上角 - 点击此按钮可显示导航窗格。
	**语言选择**下拉列表可选择用户界面的语言。
	**通知中心**图标显示 Cisco Business Dashboard 中待处理通知的数量和严重性。点击此图标可显示通知中心面板，其中提供了筛选所显示的通知事件的选项。有关更多详细信息，请参阅本指南中的查看和过滤当前设备通知，第 131 页。
	**作业中心**图标显示当前正在执行作业的状态和过去作业的历史记录。作业包括 Cisco Business Dashboard 执行的任何操作，包括用户发起作业和系统作业。点击此图标可显示待处理，正在进行和已完成的作业，以及计划在稍后日期执行的任何作业。
	点击**反馈**图标可提供有关 Cisco Business Dashboard 使用体验的反馈，以及任何改进建议。
	点击**帮助**图标可打开 Cisco Business Dashboard 的在线文档。
	点击**关于 Cisco Business Dashboard** 图标可查看有关此版本的信息，包括当前版本。如果存在新版本，该图标上将显示一个带箭头的绿色图标，并且弹出窗口中将显示一个应用更新的链接。

使用 Cisco Business Dashboard Probe GUI

登录 Cisco Business Dashboard Probe 后，系统将显示**主页**页面。



1. **标题**窗格

   标题工具栏包含以下选项：

   - 显示导航窗格的菜单按钮
   - 标题文本
   - 一系列功能图标，例如语言选择、通知、任务活动、反馈、上下文相关帮助及版本信息。

2. **工作**窗格是功能界面的显示区域。

   当点击**导航**窗格中的选项时，对应的窗口将在此区域打开。

3. **导航**窗格提供访问 Cisco Business Dashboard Probe 功能的选项。点击**菜单**图标时，会显示导航窗格；做出选择后，导航窗格会滑动离开。

   当前登录用户显示在导航窗格底部。

导航窗格选项

导航窗格提供访问Cisco Business Dashboard Probe 主要功能的选项。

图标	名称	说明
	故障排除	点击此按钮可查看页面，其中的**故障排除**部分包含各种有助于识别网络问题的诊断工具。
	管理	通过“管理”页面，您可以维护 Cisco Business Dashboard Probe 网络应用。
	用户选项	当前登录用户与**注销**选项一起显示在导航栏底部。点击用户名将显示用户配置文件页面。

标题栏选项

标题栏提供访问其他系统功能的权限，并显示系统通知。

图标	选项	说明
	“菜单”按钮	位于标题左上角 - 点击此按钮可显示导航窗格。
	选择语言	通过此下拉列表可选择用户界面的语言。
	**Dashboard** 状态	此图标显示 Cisco Business Dashboard 和 Probe 之间的连接状态。点击此图标可打开 Dashboard GUI。
	反馈	点击此图标可提供有关Cisco Business Dashboard Probe使用体验的反馈，以及任何改进建议。
	帮助	点击此图标可打开 Cisco Business Dashboard Probe 的在线文档。
	关于 Cisco Business Dashboard Probe	点击此图标可查看有关 Cisco Business Dashboard Probe 的信息，包括当前版本。如果存在新版本，图标上将显示一个标记，并且弹出窗口中将显示一个应用更新的链接。有关详细信息，请参阅升级 Cisco Business Dashboard & Probe，第 9 页

升级 Cisco Business Dashboard & Probe

思科会不时发行 Cisco Business Dashboard 和 Probe 的新版本和更新，并将其发布到 cisco.com 上的软件中心。Cisco Business Dashboard 会定期检查软件中心中是否有更新，如果找到更新，则会在用户

界面顶部面板中的  图标上显示一个标记。您可以点击下载 Dashboard 并应用更新，也可以选择自行下载更新并手动进行应用。

要设置 Dashboard 以下载并应用更新，请执行以下操作：

1. 点击**关于 Cisco Business Dashboard**，打开弹出窗口。如果 Dashboard 或任何关联 Probe 有任何可用更新，将会列在此处。
2. 如果 Dashboard 有可用更新，请选择该更新旁边的单选按钮，然后点击**升级**。

   Dashboard 将会下载并应用更新，您可以随时在**关于 Cisco Business Dashboard** 弹出窗口中查看进度。更新完成后，Dashboard 应用将会重新启动。

要手动应用 Dashboard 更新，请执行以下操作：

1. 通过导航至 *https://cisco.com/go/cbd-sw* 并从右下角的产品选择面板中选择**下载软件**选项，下载 Cisco Business DashboardLinux 安装程序文件。
2. 将安装程序文件复制到 Dashboard 文件系统。
3. 使用 Sudo 命令 `sh <filename of installer>` 执行安装程序。例如，`sh cisco-business-dashboard-2.2-ubuntu-xenial-amd64.sh`。如有必要，请在 sudo 提示符处输入密码。在此过程中，Dashboard 应用将会重新启动。

此外，您还可以通过 Dashboard 将更新应用到网络中的所有 Probe。您可以并行更新所有 Probe 或单独更新 Probe。

要通过 Dashboard 并行更新所有 Probe，请执行以下操作：

1. 点击**关于 Cisco Business Dashboard**，打开弹出窗口。

   如果 Dashboard 或任何关联 Probe 有可用更新，将会列在此处。

注释 如果 Dashboard 有可用更新，请先执行更新，然后再升级 Probe。

如果先更新 Probe，会收到错误消息。

2. 选择 Probe 更新旁边的单选按钮，然后点击**升级**。
3. 您可以在 Probe 用户界面中查看更新进度。

要通过 Dashboard 更新单个 Probe，请执行以下操作：

1. 如果 Dashboard 有可用更新，请先执行更新，然后再升级任何 Probe。

   如果先更新 Probe 再更新 Dashboard，会收到错误消息。
2. 在导航面板中选择**网络**。
3. 在**地图视图**或**列表视图**中选择要更新的网络。

4. 在网络的**基本信息**面板中，选择**操作**选项卡。
5. 点击**升级**。

   您可以在作业中心中查看更新进度。

注释 使用在网络设备上运行的嵌入式 Probe 时，应参阅适用于该设备的文档以执行更新。某些设备不支持独立于设备固件对 Probe 应用进行更新。

注释 在 Amazon Web Services (AWS) 或 Microsoft Azure 中运行的 Cisco Business Dashboard 从版本 2.4.1（或更低版本）升级到版本 2.5.0（或更高版本）时，应手动更新 AWS/Azure 安全策略，才能使传入 UDP 流量到达端口 1812。

升级 Cisco Business Dashboard 或 Probe 操作系统

Cisco Business Dashboard 和 Probe 2.3.x 之前的版本（包括版本 2.3.x）在 Ubuntu Linux 发行版 16.04 (Xenial Xerus) 上运行。

Cisco Business Dashboard 未来版本将仅支持 Ubuntu 20.04 (Focal Fossa)。因此，将现有 Cisco Business Dashboard 或 Probe 安装升级到 2.3.x 之后的版本需要更新的操作系统。

由于从 Ubuntu 16.04 到 20.04 进行了大量更改，为不同的 Cisco Business Dashboard 和 Probe 操作系统版本提供了单独的安装程序。无法在现有的 Dashboard 或 Probe 安装上执行操作系统的就地升级。以下各部分介绍针对更新 Dashboard 和 Probe 操作系统的建议方法。

升级 Cisco Business Dashboard 操作系统

要将现有 Cisco Business Dashboard 操作系统升级到新版本，请使用以下过程：

1. 备份现有 Cisco Business Dashboard 应用。
   1. 登录 Dashboard GUI 并从导航窗格打开**系统** > **备份**。
   2. 在屏幕上的字段中输入密码以保护备份，然后点击**备份与下载**按钮。
2. 创建在更新的操作系统上运行的 Cisco Business Dashboard 的新实例。
   - 如果现有 Dashboard 在虚拟机或 Amazon Web Services 等云提供商中运行，则应关闭现有实例，然后使用预构建 Cisco Business Dashboard 映像创建新实例。
   - 如果现有 Dashboard 直接安装在服务器上运行的 Ubuntu Linux 安装上，则应使用更新的 Ubuntu 版本重新映像服务器，然后安装 Cisco Business Dashboard。

   有关安装 Cisco Business Dashboard 的详细信息，请参阅以下网址中的安装指南：*https://cisco.com/go/cbd-docs*。

3. 登录到 Cisco Business Dashboard 的新实例并恢复您在步骤 1 中创建的备份。
   - 导航到**系统** > **恢复**。
   - 在提供的字段中输入用于保护备份的密码。
   - 点击**上传与恢复**按钮上传备份文件。
4. 恢复过程完成并且确认新实例正常运行后，请删除旧实例。

   有关备份和恢复过程的详细信息，请参阅本指南后面的备份和恢复 Dashboard 配置，第 107 页。

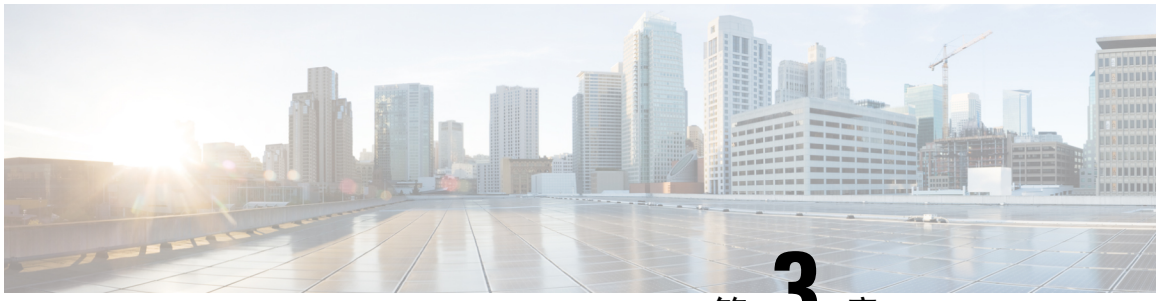
注释 Cisco Business Dashboard 备份文件可以恢复到与刚备份的系统运行相同版本的系统，也可以恢复到一个最多一个的次要版本。例如，从运行版本 2.2.0 的系统获取的备份可以恢复到运行 2.3.1 的系统，但不能恢复到运行 2.4.0 的系统。

升级 Cisco Business Dashboard Probe 操作系统

Cisco Business Dashboard Probe 存储的配置数据非常少，而且不会存储长期统计数据。因此，在升级托管 Probe 的操作系统时，思科建议您删除现有 Probe 实例并安装在新操作系统上运行的新 Probe 实例。然后，将新的 Probe 与 Cisco Business Dashboard 关联，并在关联过程中选择现有网络记录。

有关安装 Cisco Business Dashboard Probe 软件的详细信息，请参阅 Cisco Business Dashboard 安装文档中的安装指南。有关将 Probe 与 Cisco Business Dashboard 关联的详细信息，请参阅 Cisco Business Dashboard 快速入门指南中的快速入门指南。

注释 使用嵌入式 Probe 或直接设备管理时，无需从设备操作系统单独升级 Probe 或代理。Probe/代理包含在设备固件中，在升级设备时会自动更新。



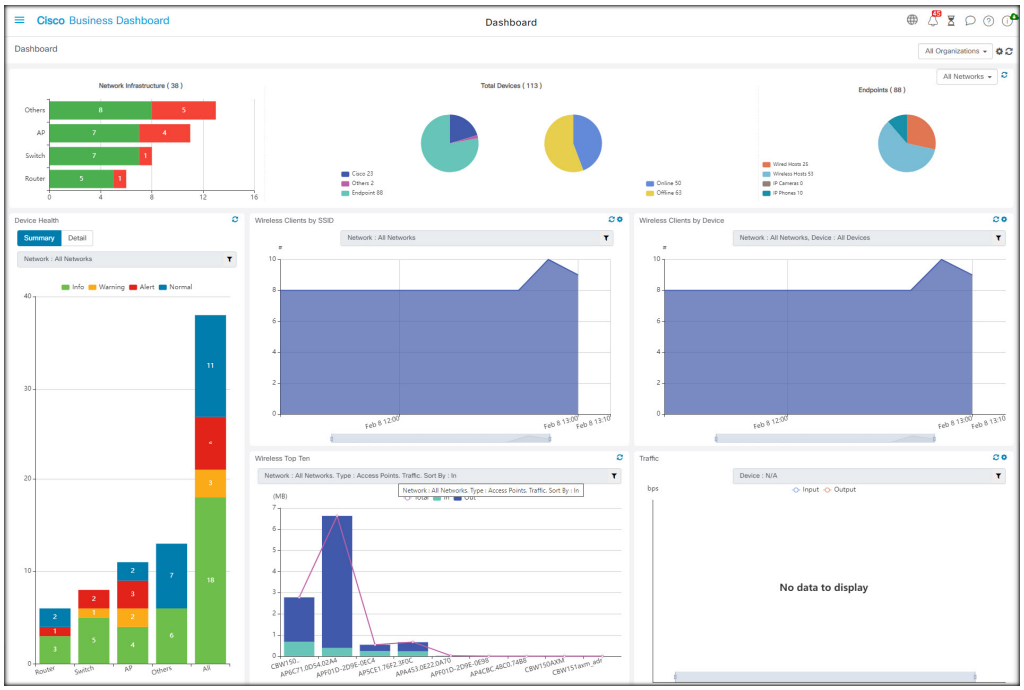
第 3 章

监控控制面板

本章包含以下各节：

关于监控控制面板

Cisco Business Dashboard 的**控制面板**页面可用于实时查看网络性能。它以图形格式显示所有设备并提供数据。



此监控控制面板包含您可以选择的的构件，构件的排列可以自定义。下面是控制面板中默认包含的构件：

构件	说明
资产摘要	显示网络中发现的设备的细分信息。
设备运行状况	显示网络中设备的总体运行状况。
WLAN 客户端计数	显示与所选无线网络关联的设备数。
设备客户端计数	显示与所选无线接入点关联的设备数。
前十个无线设备	显示基于流量或客户端数排名前十位的无线网络、无线接入点或客户端。
流量	显示所选接口的流量图。

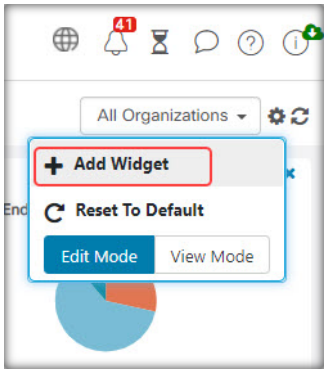
每个构件上的控件可用于自定义显示的数据。Dashboard右上角的“组织”下拉列表可用于将显示的信息限制在特定组织范围内。

在图形构件中，可点击图形图例中的标签以切换每组数据的显示。这使您可以进一步优化显示的数据，并有助于排除网络中的特定设备甚至网络本身的故障。

添加构件

通过此功能，您可以向 Dashboard 中显示的现有默认构件中添加一个或多个构件，以便监控要查看的设备或网络的特定任务。

步骤 1 点击 Dashboard 窗口右上角的齿轮图标，然后选择**添加构件**。



步骤 2 从弹出列表中选择要添加的构件类型。Dashboard 中将显示新构件。

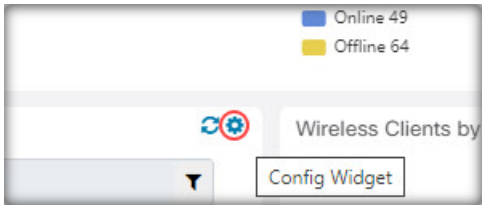
步骤 3 将新构件拖动到 Dashboard 中的所需位置，并在必要时调整大小。

步骤 4 再次点击齿轮图标并选择**查看模式**以保留更改。

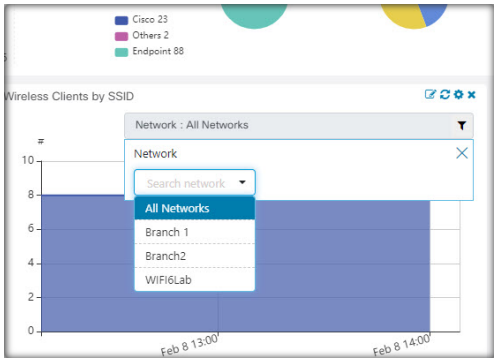
修改构件

您可以通过以下步骤修改 Dashboard 上的任何构件：

步骤 1 点击构件右上角的**配置构件**图标以修改采样间隔或阈值等参数。



步骤 2 使用新构件中的下拉列表选择您想要显示的特定数据。



步骤 3 要更改构件的标题，请点击“编辑模式”图标。

重要事项 必须在 Dashboard 中处于**编辑模式**才能更改构件标题。

删除构件

步骤 1 点击 Dashboard 窗口右上角的齿轮图标，然后选择**编辑模式**。

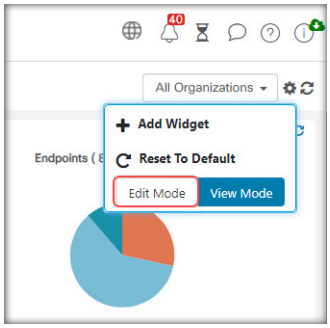
步骤 2 点击要删除的构件右上方的**删除构件**图标。根据需要重新排列其余构件。

步骤 3 再次点击齿轮图标并选择**查看模式**以保留更改。

修改 Dashboard 布局

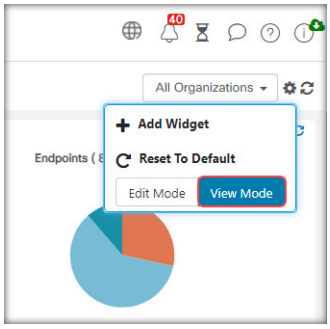
使用以下步骤可以轻松自定义 **Dashboard** 布局：

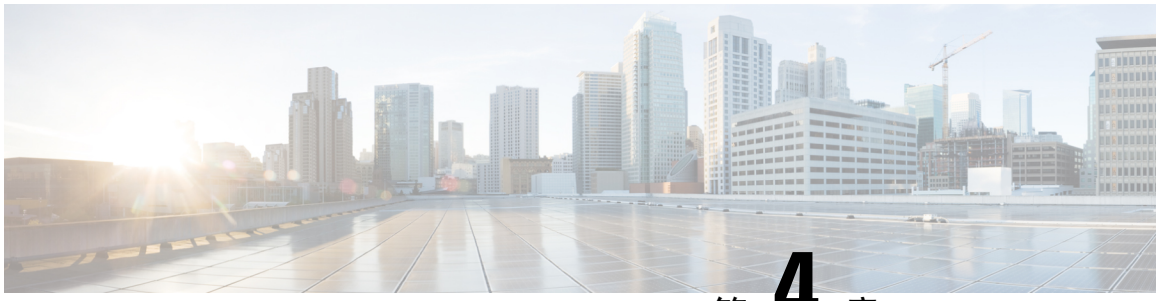
步骤 1 点击 Dashboard 窗口右上角的齿轮图标，然后选择**编辑模式**。



步骤 2 点击构件顶部并拖动以在 **Dashboard** 中移动构件。其他构件将动态调整以腾出空间。点击并拖动构件的边或角可调整其大小。重新排列布局时，Dashboard 将动态调整大小以适应可用宽度。

步骤 3 再次点击齿轮图标并选择**查看模式**以保留更改。





第 4 章

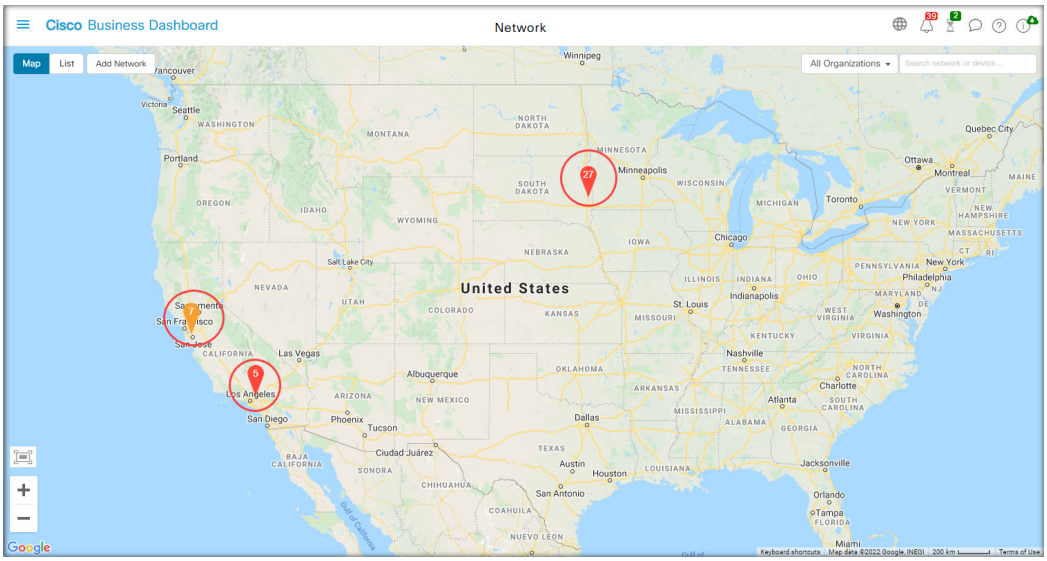
网络

本章包含以下各节：

关于网络

访问“网络”页面可查看位置和网络中所有设备的概览。您还可以注意到附近的其他网络和设备。您可以选择网络，然后查看有关该网络和设备以及它们的运行方式的更多详细信息。

网络页面提供两种形式的网络概览视图：用于显示网络中每个站点的位置和状态的地图，或所有站点的列表。

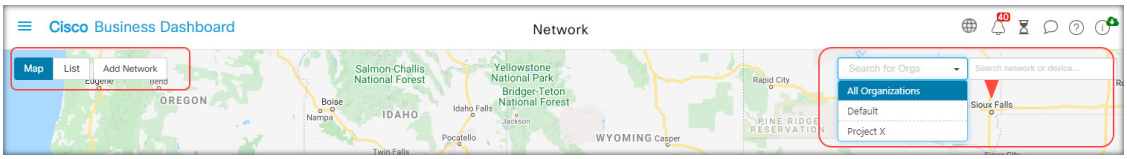


在**地图视图**中， 每个网络图标上显示的数字表示该站点存在的待确认通知数，图标颜色表示待确认的最高严重性级别。

注释 当两个或多个网络图标在地图上的位置过近而不便于区分时，它们将被替换为一个集群图标。点击集群图标可自动把地图缩放到可以将该集群中网络分开的程度。

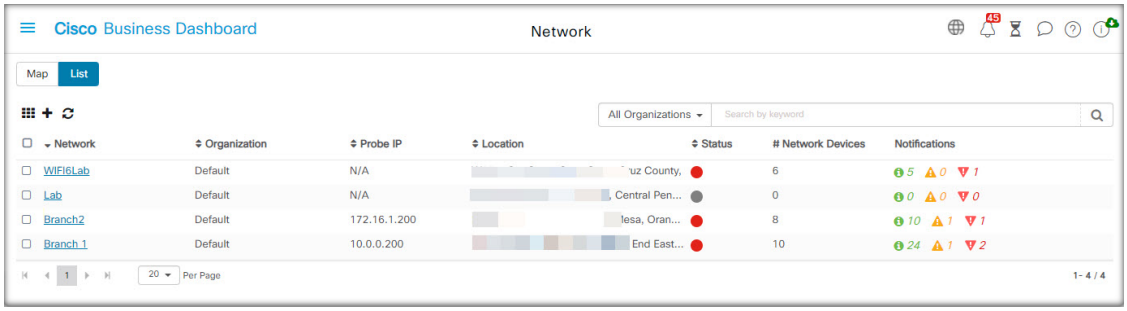
网络地图提供以下控件：

另外，您还可以点击地图区域的任何位置并进行拖动，在**工作**窗格中自由移动地图。



控件名称	控制操作
“地图”/“列表”选择	使用此控件可选择在地图还是在表格中查看网络。
“添加网络”按钮	使用此按钮可创建新的网络记录，然后再为该网络部署 Probe。
“组织”下拉列表	从下拉列表中选择单个组织来限制显示的网络。
搜索框	输入完整或部分网络名称、地址或IP地址，以便在地图中查找该网络。或者，可以输入完整或部分设备名称、IP 地址、序列号或 MAC 地址，以查明设备所在的网络。当您键入内容时，系统会显示匹配项列表。 • 将鼠标悬停在某个匹配项上，相应的网络将高亮显示。 • 选择某个匹配项后，相应的网络将在视图中变为选中状态，并居中显示。

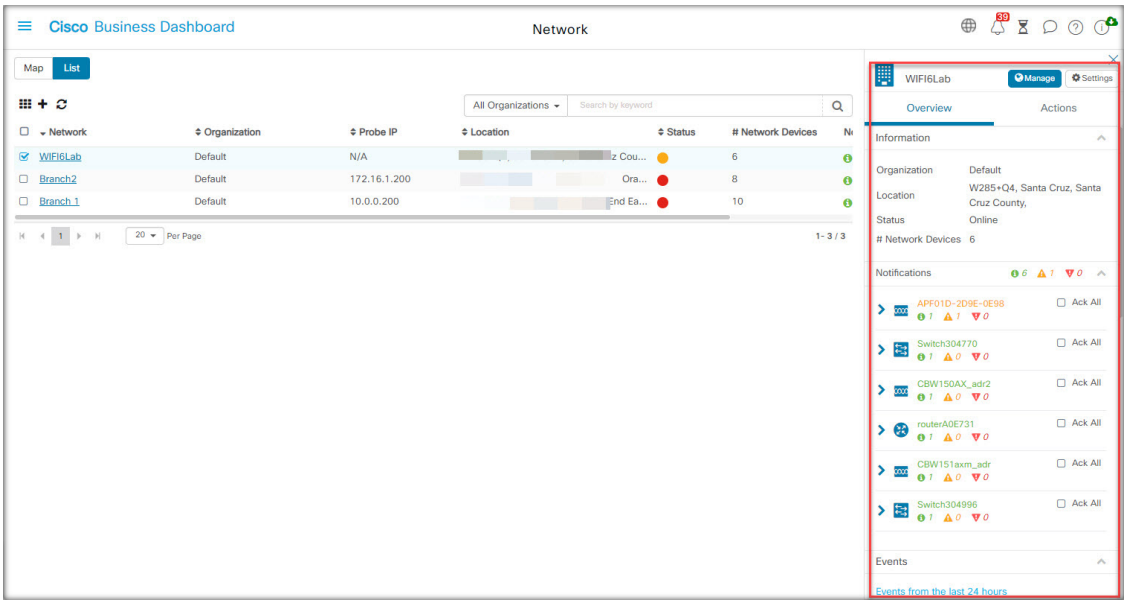
控件名称	控制操作
缩放控件	使用这些控件可缩放地图。单击加号 ( ) 可放大，点击减号 (—) 可缩小。
适应视图按钮	此按钮用于自动缩小地图，以便可以显示所有网络标记。



在**列表视图**中，可以在表格的最后一列中看到相同的信息。要查看有关某个网络的更多信息，请点击网络图标或该站点的表格行。

在**列表视图**中，以下控件可用：

控件名称	控制操作
“地图”/“列表”选择	使用此控件可选择在地图还是在表格中查看网络。
“列选择”图标	此图标用于选择要显示的列。点击列标题可对表进行排序。
添加网络	点击 ( ) 加号可添加新网络，然后可为该网络部署 Probe。
刷新	点击“刷新”按钮可更新表并显示最新信息。
“组织”下拉列表	从下拉列表中选择单个组织来限制显示的网络。
搜索框	输入完整或部分网络名称、地址或 IP 地址，以便仅在表中列出匹配的网络。



点击网络图标或行可打开该网络的**基本信息**面板。**基本信息**面板包含以下信息：

- 网络的名称。
- 网络所属的组织。
- 网络的物理地址。
- 网络的 Probe IP 地址和在网络中发现的 IP 子网。
- Probe 的软件版本。
- 连接状态。
- 该网络中托管的设备的数量。
- 该网络所有最新的未确认通知的列表。
- 在过去 24 小时内发生的有关该网络的事件列表。

另外，在**基本信息**面板中还可以对网络执行以下操作：

- 点击**管理**可查看网络的详细信息，包括网络拓扑和平面图。
- 点击**设置**可显示**网络详细信息**面板。有关**网络详细信息**面板的详细信息，请参阅下面的“关于网络详细信息”部分。
- 点击**操作**选项卡可显示可用于该网络的其他操作。
  - 点击**删除**可从 Dashboard 中删除该网络以及所有关联数据。
  - 点击**升级**可更新该网络中的 Probe 软件。
  - 点击**显示技术**可生成该网络的“网络显示技术”存档。

关于“网络详细信息”面板

通过**网络详细信息**面板可以查看和更新特定于该网络的信息。此信息包括：

- 关键网络参数，包括网络名称、说明、组织和默认设备组。
- 网络的位置。
- 将设备清单信息上传到 Cisco Active Advisor 时用于网络的凭证。
- 该网络中 Probe 的日志记录配置。请参阅管理 Probe 日志设置，第 140 页。
- 用于根据相应 IP 地址限制 Cisco Business Dashboard 发现和管理的设备的控件。

关于“网络视图”面板

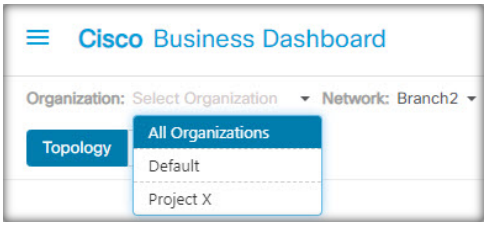
打开此面板可查看和管理有关您的网络的详细信息。

点击网络**基本信息**面板中的**管理**可显示该网络的**网络视图**，其中包含多个视图。

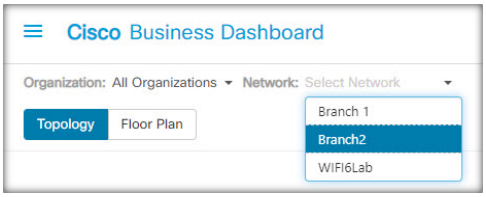
选择**拓扑**可显示网络中发现的所有设备的逻辑拓扑。显示有关每个设备的信息，并且您可以针对所选的思科产品执行操作。

选择**平面图**可记录并显示网络设备在您环境中的物理位置。

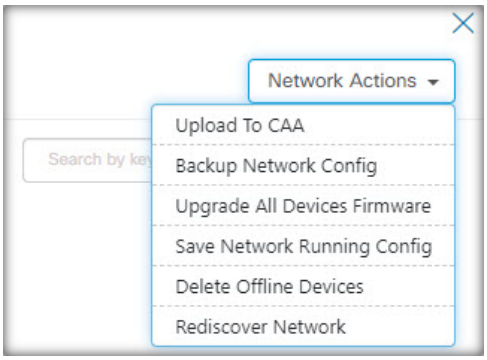
从**组织**下拉列表中选择组织可在组织间切换，而无需返回到主网络页面。



从**网络**下拉列表中选择网络可在网络间切换，而无需返回到主网络页面。



使用**网络操作**下拉列表可对网络中支持所选操作的所有设备执行选定的操作。例如，您可以一键备份所有网络设备配置。



另外，您还可以使用**网络操作**下拉菜单重新启动对网络的发现流程，并且将设备清单上传到 Cisco Active Advisor（位于 Cisco Active Advisor）。

拓扑地图和工具概述

关于拓扑地图

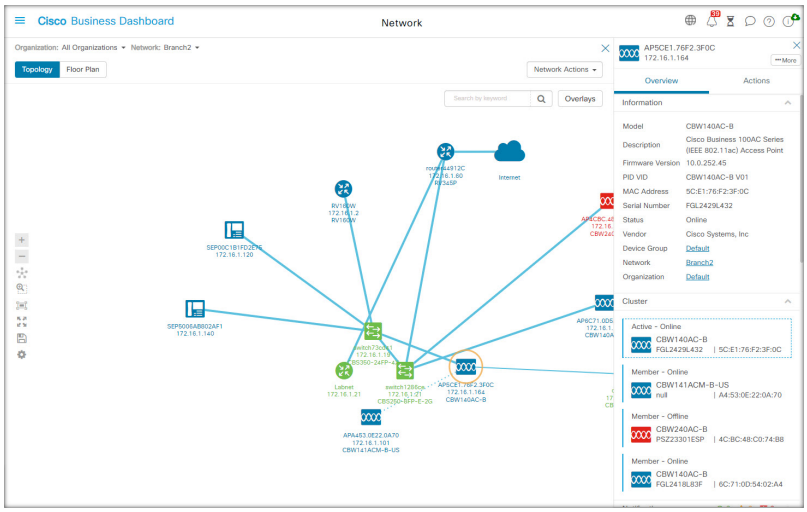
Cisco Business Dashboard 可向发现的设备查找络连接详细信息，并基于所收集的信息构建图示或拓扑。收集的数据包括：

- CDP 和 LLDP 邻居信息
- MAC 地址表
- 来自 Cisco Business 交换机的关联设备表
- 路由器
- 无线接入点

这些信息可确定网络的构成方式。如果网络中包含出于任何原因而无法管理的网络基础设施设备，Cisco Business Dashboard 将尝试基于可收集的信息理解拓扑。

点击拓扑中的设备或链路，可显示该设备或链路的**基本信息**面板。此面板将提供有关该设备或链路的更多详细信息，并允许您针对设备执行不同的操作。

点击**拓扑地图**中的**重叠网络**可显示**重叠网络和过滤器**面板。通过此面板，您可以按设备类型或标记限制拓扑中显示的设备。另外，由此还可增强拓扑以显示其他信息，例如链路中的流量负载或特定 VLAN 在网络中的配置方式。



访问拓扑地图

要访问**拓扑地图**，请执行以下操作：

1. 从**导航**窗格打开**网络**面板。
2. 点击您感兴趣的网络的图标或表行。

该网络的**拓扑**将显示在工作窗格中。

拓扑控件

拓扑控件位于**拓扑地图**的左上方。

图标	说明
+	**缩小** - 调整**拓扑**窗口的视图。单击菜单栏上的 （加号）图标，可放大查看区域中网络的大小。
—	**放大** - 调整**拓扑**窗口的视图。点击**—**（减号）图标，可缩小查看区域中网络的大小。
	点击**重新布局拓扑**可在通过手动更改禁用拓扑的自动布局后，重新启用该布局。使用自动布局算法重绘拓扑。
	点击并拖动**通过选择进行缩放**可选择要放大的区域。

图标	说明
	点击**适应屏幕**可执行缩放，直到整个网络填满查看区域。
	点击**进入全屏模式**可使 Cisco Business Dashboard 用户界面填满屏幕。
	点击**导出拓扑**可将当前拓扑视图导出为 PNG 格式的映像。该映像将保存到浏览器的默认下载位置。
	点击**拓扑设置**可调整针对拓扑图标显示的标签。

拓扑图标

拓扑窗口中显示以下图标：

图标	说明
	**无线接入点**
	**云** - 此图标展示并非由 Cisco Business Dashboard 管理的网络或部分网络。
	**链路** - 链路是指设备之间的连接线路。点击某个链路将显示目标与源设备名称，以及速度等其他基本详细信息。 链路厚度表示链接速度，薄线路表示速度为 100Mbps 或以下，厚线路表示速度为 1Gbps 或以上。虚线表示无线连接。
	**路由器**
	**交换机**
	**主机** - 使用有线连接方式连接网络的主机。

图标	说明
	**无线主机** - 使用无线连接方式连接网络的主机。

重叠和过滤面板

点击**重叠**时，此面板将显示在**拓扑**地图右侧。它位于拓扑屏幕右上方，**搜索**框旁边。

项目	说明
选择重叠	此功能可根据视图选择增强**拓扑**地图及其他信息。它可以是下列类型之一： • **链路利用率视图**通过监控流量确定当前的网络性能。**拓扑**地图中使用彩色编码的链路显示这些流量。颜色代码根据链路的使用百分比而变化。绿色表示链路负载较轻，橙色和红色表示链路负载接近容量极限。 利用提供的控件可以调整不同颜色的阈值。 • **VLAN视图**显示网络中启用VLAN的位置。此视图可用来确定分区的VLAN或其他错误配置。 在“重叠网络”下拉列表中选择 **VLAN 视图**时，此字段下方将另外显示一个下拉框，从中可选择要显示的 VLAN ID。 • **POE 视图**会在拓扑地图中高亮显示表示设备目前正在由支持 POE 的交换机供电的链路。 • **L2路径跟踪**显示两个选定设备之间的流量在流经网络时采用的第2层路径。可通过在提供的字段中输入主机名、MAC地址或IP地址或交替点击拓扑地图中的两个设备来选择设备。
选择标记	在**选择标记**下方的文本框中指定**设备标记**可过滤拓扑，以显示与指定标记匹配的设备。设备标记在**详细信息**面板中分配。
仅显示： • 路由器 • 交换机 • 无线 • 非受管网络 • 主机 • 其他	选中列表中您想在**拓扑**地图中查看的设备的复选框。此功能可帮助您过滤要在地图中查看的设备，并将删除设备列表中未选中的设备。

项目	说明
显示发现： • 两者 • 已阻止 • 已启用	使用单选按钮控制是否希望查看 Dashboard 找到的已阻止管理的设备。

查看基本设备信息

点击网络设备（例如交换机或路由器）或连接两个设备的链路，可查看有关该设备的基本信息，包括待解决的通知和可执行的操作。

通过**基本信息**面板，还可访问设备的更多详细信息，并可直接访问设备的管理界面。

注释 要查看设备的详细信息，请参阅查看和过滤当前设备通知，第 131 页。

要查看有关访问设备管理界面的更多信息，请参阅访问设备管理界面，第 29 页。

以下部分的表格介绍显示的设备详细信息类型。要查看基本设备信息，请执行以下步骤。

步骤 1 在**网络**页面中，选择网络并点击**管理**可显示拓扑。

步骤 2 在拓扑地图中，点击要查看其详细信息的网络设备，例如交换机或路由器。

步骤 3 在**基本信息**面板中，设备详细信息显示在**概述**选项卡下方。有关这些设备项目的说明，请见下表：

信息面板	
型号	设备的型号名称。
说明	设备或产品描述。
固件版本	设备的固件版本。
PID VID	产品 ID 和版本 ID。
MAC 地址	介质访问控制 *(MAC)* 地址是某些网络接口类型所需的标准化数据链接层地址。每个设备的这些地址都是特定且唯一的，不能用于网络中的其他设备。
序列号	设备序列号。
状态	设备的在线/离线状态。
域	设备的域名。
供应商	设备的制造商。

网络	设备所在网络的名称。
组织	设备所属的组织。

通知面板	**通知面板标题** - 通知面板标题显示设备的待处理通知的汇总数量。 **通知面板主体** - 通知面板主体列示设备的待处理通知。要查看和过滤所有设备通知的完整列表，请参阅查看和过滤当前设备通知，第 131 页。选中某个通知的相应复选框，可确认该通知并将其从通知列表中删除。如果需要，您可以使用通知过滤功能来显示确认的通知。
事件面板	“事件面板”显示特定设备在过去 24 小时发生的所有通知及其他事件的列表。要查看和过滤所有设备的所有事件的完整列表，请访问 Dashboard 上的事件日志。
POE 面板	“POE 面板”显示在启用 POE 的交换机上，提供设备各个端口的电量使用情况摘要。
堆栈信息面板	交换机堆栈显示“堆栈信息面板”，面板上显示每个堆栈成员的硬件详细信息，包括型号信息、序列号和 MAC 地址
服务面板	列出设备上标识的网络服务。
已连接设备面板	主机设备包括**已连接设备**面板。此面板显示主机如何连接到网络，列出上游网络设备，在适用情况下还将列出主机连接的端口。

除**概述**选项卡以外，**基本信息**面板还包含一个**操作**选项卡，您可以通过它在设备上执行各种操作任务。有关详细信息，请参阅执行设备操作，第 27 页。

执行设备操作

您可以轻松地对网络中的设备执行固件更新、配置备份及恢复和重新启动等操作。要执行这些操作，请执行以下步骤：

步骤 1 在**拓扑地图**或**设备清单**页面中，点击要对其执行操作的网络设备，例如交换机或路由器。

步骤 2 在**基本信息**面板中，选择**操作**选项卡。根据设备功能，系统将显示以下一项或多项操作：

将固件更新为最新版本	用于将最新固件更新应用于设备。Cisco Business Dashboard 将从思科下载更新，然后将其上传到设备。设备在完成更新后将重新启动。
从本地升级	用于从本地驱动器上传固件升级文件。Cisco Business Dashboard 将文件上传到设备，并且设备将在更新完成时重新启动。

备份配置	用于在 Dashboard 上保存当前设备配置的副本。 **1.** 点击**备份配置**。 **2.** 在**备份配置**窗口中，可以在文本框中为要执行的备份添加注释（可选）。 **注释** 无论何时 GUI 中列出该备份时，都会显示此注释。 **3.** 点击**保存备份**完成此操作；如果不想再继续，可点击**取消**。 系统将创建备份配置作业，并且可在**任务中心**中查看该作业。
恢复配置	允许对设备恢复以前备份的配置。 点击**恢复配置**。 系统将提供以下备份配置选项： • **用于以下设备的备份：设备名称** - 列出可为特定设备配置的所有备份 • **用于其他设备的备份** - 列出可为同类或产品 ID 相同的其他设备配置的所有备份 • **用于其他兼容设备的备份** - 列出可为与所选设备兼容的其他系列设备配置的所有备份 要执行备份配置，请执行以下操作： **1.** 在**恢复配置**窗口中，选择想要为设备恢复的备份。 使用滚动条查看所有可用的备份，然后点击相应的单选按钮。此操作将启用**恢复配置**按钮。 或者，您可以选择上传配置文件。要执行此操作，请拖动配置文件以将其放到目标区域，或者点击目标区域以从文件系统中选择文件。 **2.** 点击**恢复配置**完成此操作。 系统将创建恢复配置作业，可在**任务中心**中查看该作业。
重启	重新启动设备。 点击此按钮时，系统将提示您再次点击该按钮进行确认。
保存运行配置	对于支持单独运行和启动配置的设备，此操作会将当前运行的配置复制到启动配置中。这样可确保设备在下次重启时保留所有配置更改。
删除	从“拓扑”和“设备清单”中删除离线设备。

步骤 3 设备操作可以选择安排在稍后执行。要安排设备操作，请点击**计划**按钮并填写表单以创建新的**计划配置文件**。有关计划配置文件的详细信息，请参阅管理计划配置文件 ， 第 135 页。

访问设备管理界面

在某些情况下，您可能需要直接访问网络设备的管理界面。要访问管理界面，请执行以下操作：

步骤 1 在**拓扑**或**设备清单**页面中，点击您想要访问其管理界面的网络设备（例如交换机或路由器）。

步骤 2 在**基本信息**面板中，点击右上角的**查看**。您的浏览器中将打开一个新窗口，显示设备管理界面

注释 点击**查看**访问管理界面时，您的浏览器将通过Dashboard连接到设备。这意味着，如果您正在远程访问网络，只需可从站点外部直接连接 Dashboard。

由于这些连接全部通过同一主机（即 Dashboard）传递，所以系统会将一台设备的 Cookie 提供给其他设备，而且如果 Cookie 的名称相同，这台设备的 Cookie 可能会被其他设备的 Cookie 更新。这种问题的常见症状是，当浏览器连接到第二台设备时，第一台设备上的浏览器会话会由于会话 Cookie 已更新而立即退出。

查看详细设备信息

步骤 1 在**拓扑**或**设备清单**页面中，点击要查看其详细信息的网络设备，例如交换机或路由器。

步骤 2 在**基本信息**面板中，点击右上角的**更多**。

步骤 3 在**详细信息**面板中，左侧将显示详细的设备信息列表，并且以下选项卡下将显示其他功能：

- **控制面板** - 显示一系列特定于设备的控制面板构件
- **PnP** - 可用于管理设备的 Network Plug and Play 设置
- **端口管理** - 管理交换机端口的配置

  注释 只有具有交换机端口的设备，才会显示这些信息。

- **无线局域网** - 可用于查看无线局域网，并管理设备上的无线电配置。

  可以通过此选项卡启用或禁用每个无线电，并控制信道和传输功率。

  注释 只有无线设备才会有这些信息。

- **事件日志** - 提供此设备过去的操作和通知列表
- **配置备份** - 可用于查看设备的备份配置列表，以及执行恢复、保存或删除配置等操作

  注释 只有支持备份配置操作的设备，才会有这些信息。

- **待处理配置** - 将基于定义的配置文件的所需配置与设备上的当前配置进行比较，并且突出所有差异。

注释　仅对于支持配置操作并且当前配置与所需配置不匹配的设备，系统才显示此面板。

以下步骤将介绍上述各项设置：

步骤 4　左侧将显示详细的设备信息列表。此列表包含以下信息：

项目名称	说明
主机名	点击设备名称旁边的**编辑**，可修改设备主机名。点击**保存**保存更改。
型号	设备的型号名称。
MAC 地址	介质访问控制 *(MAC)* 地址是某些网络接口类型所需的标准化数据链接层地址。每个设备的这些地址都是特定且唯一的，不能用于网络中的其他设备。
状态	显示设备的当前状态。例如，在线或离线。
行动	**操作**下拉列表和**打开设备 GUI** 图标可用于从**详细信息**面板对设备执行操作。
IP	设备的 IP 地址。
域	设备的域名。
PID VID	产品 ID 和版本 ID。
序列号	设备的序列号。
供应商	设备的制造商。
说明	设备或产品描述。
网络	此设备所属的网络。
组织	此设备所属的组织。
设备组	点击设备组旁边的**编辑**可更改设备所属的组。 点击**保存**可保存所做的更改。
监控配置文件	点击监控配置文件旁边的**编辑**可选择要用于此设备的监控配置文件。或者，可以从此设备所属的设备组继承监控配置文件。 点击**保存**可保存所做的更改。
标记	在“标记”字段中，输入任意字母数字字符，然后按 **Enter**，可为此设备创建新标记。要删除现有的标记，可点击标记中的　。点击**保存**保存更改。 标记用于帮助识别具有常见特征的设备。您可以在的Cisco Business Dashboard Probe其他位置使用标记来限制网络视图，使之仅显示一部分设备。
发现方法	按发现的设备显示协议和设备。
待处理配置	显示设备配置的状态以及设备的当前配置与预期配置之间是否存在任何差异。

步骤 5 点击**控制面板**可显示一组显示设备的当前状态的构件。有关详细信息，请参阅关于监控控制面板。

步骤 6 点击 **PnP** 以查看要应用于使用 Network Plug and Play 的设备的设置。

步骤 7 使用表单进行更改，然后点击**保存**以应用更改。

步骤 8 点击**端口管理**以查看和管理设备交换机端口的配置。系统将显示设备图示，与**端口管理**页面所示的图表类似。

此窗口将在图示中指定设备的端口详细信息。设备的型号和序列号显示在映像上方，端口的表格视图显示在下方。有关操作的更多详细信息，请参阅关于端口管理，第 39 页。

步骤 9 点击 **WLAN** 以管理无线电设置并查看此设备上配置的无线局域网。

步骤 10 点击**事件日志**可查看为该设备记录的历史通知及其他事件列表。您可以使用过滤器来限制显示的条目数。有关详细信息，请参阅关于事件日志，第 67 页。

步骤 11 点击**配置备份**以查看和管理该设备的配置备份。在此选项卡中，您可以看到一个表格，其中列出了 Probe 中存储的各个备份及以下详细信息：

表 *3:* 配置备份

项目	说明
时间戳	执行配置备份的日期和时间。
备注	用户在执行备份时输入的注释。
备份方式	执行配置的用户。
行动	选择以下备份操作之一： • **恢复配置到设备** - 将所选的备份恢复到设备 • **保存配置到 PC** - 以 zip 文件格式将备份保存到 PC 的本地硬盘中 • **删除配置** - 删除备份 • **查看配置** - 帮助在浏览器中查看配置备份的内容

还可以通过点击**备份配置**从选项卡触发配置备份。

步骤 12 点击**待处理配置**，可并排查看和比较当前设备配置与基于向设备应用的配置文件的预期配置。配置以独立于设备的格式表示，并且将突出显示所有差异。您可以使用页面顶部的按钮应用任何待处理的更改、接受当前设备配置或重新读取当前设备配置。

使用平面图

通过平面视图，您可以跟踪网络设备的物理位置。您可以上传楼宇每个楼层的平面图，然后在平面图中定位各个网络设备。如果需要维护，这样可帮助您轻松找到设备。平面图的操作方式与拓扑地图类似，而且放置在平面图中的设备可与拓扑图中的设备按相同的方式操作。

创建新平面图

1. 导航到**网络视图**，然后点击**建筑平面图**。如果系统显示现有建筑平面图，请点击建筑平面图左上角的**主页**图标。
2. 如果已创建您要为之添加平面图的楼宇，请转到下一步。否则，向**新建筑**字段中输入包含楼层的楼宇名称。点击**保存**图标。
3. 拖动包含平面图的图像文件以将其放到新楼层的目标区域，或点击目标区域指定要上传的文件。支持的图像格式为 `png`、`gif` 和 `jpg`。图像文件最大为 500KB。
4. 向**新楼层**字段中输入楼层的名称。点击**保存**图标。
5. 对于包含网络设备的每栋建筑和每个楼层，重复步骤 2 至 4。

在平面图中放置网络设备

1. 导航到**网络视图**，然后点击**建筑平面图**。如果您关注的平面图尚未显示，可点击平面图。
2. 点击**添加设备**，然后使用左下角的搜索框查找您要放置的设备。您可以按主机名、设备类型或 IP 地址进行搜索。随着您键入信息，系统将在搜索框下方显示匹配的设备。灰色图标表示设备已被放置到平面图中。
3. 单击并拖动设备，将其添加到建筑平面图中正确的位置。如果所选的设备已被放置到另一个平面图中，系统会从另一个平面图中删除该设备，而将其添加到此平面图中。
4. 重复步骤 2 和 3，直到所有设备都被添加到平面图中。

从平面图中删除设备

1. 导航到**网络视图**，然后点击**建筑平面图**。如果您关注的平面图尚未显示，可点击平面图。
2. 确定要删除的设备，然后点击该设备将其选中。
3. 点击显示的红色十字，系统将从平面图中删除该设备。

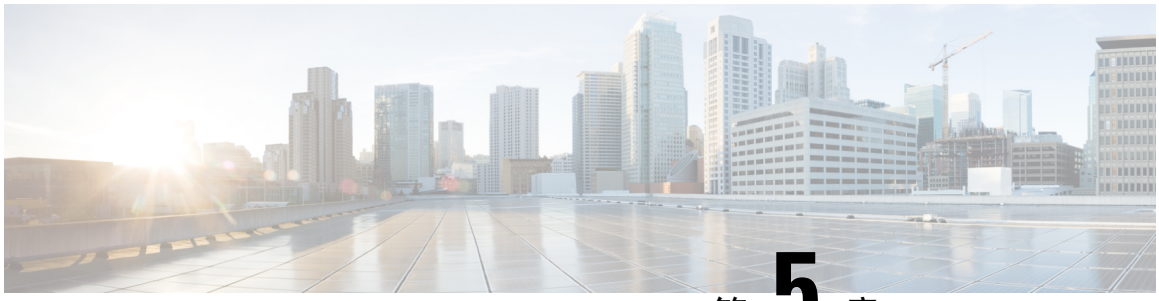
更改平面图

1. 导航到**网络视图**，然后点击**建筑平面图**。如果系统显示现有建筑平面图，请点击建筑平面图左上角的**主页**图标。
2. 要更改楼宇名称，请点击名称旁边的**编辑**图标。完成更改后，点击**保存**图标。
3. 要更改平面图，请点击平面图名称旁边的**编辑**图标。更改平面图的方法有两种：拖动新图像文件以将其放到目标区域，或点击目标区域从 PC 中上传新文件。另外，还可以更改平面图的名称。完成更改后，点击**保存**图标。

删除平面图

1. 导航到**网络视图**，然后点击**建筑平面图**。如果系统显示现有建筑平面图，请点击建筑平面图左上角的**主页**图标

2. 确定要移除的建筑平面图，然后点击映像目标区域右上角的**删除**图标。
3. 如果要删除包含所有平面图的整个楼宇，请点击建筑名称旁边的**删除**图标。



第 5 章

资产

查看设备清单

访问此页面可查看、监控和支持您网络中的所有设备和设备清单。**设备清单**页面以表格视图的形式显示完整的设备列表及其详细信息。另外，其中还提供执行配置任务和对支持的设备应用最新固件更新的操作按钮。下表介绍所显示信息的详情：

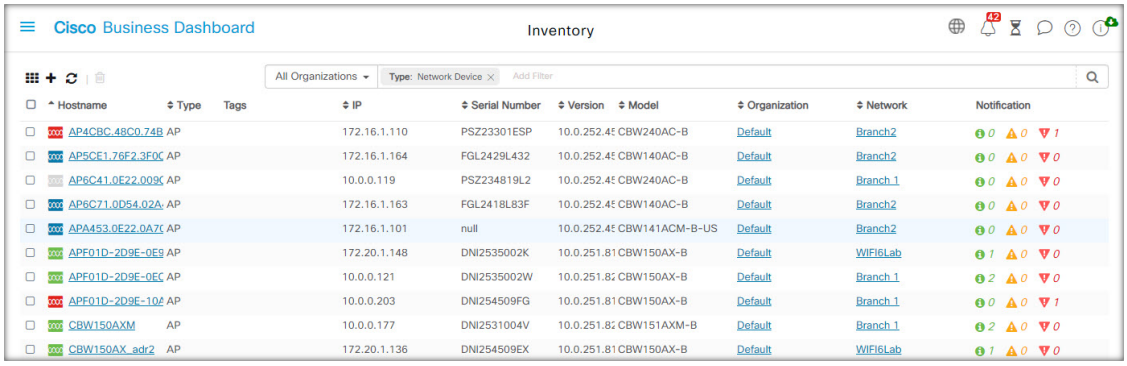


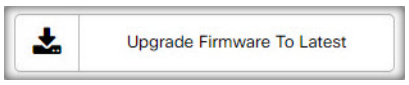
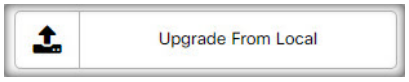
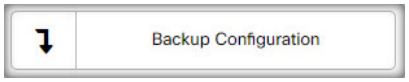
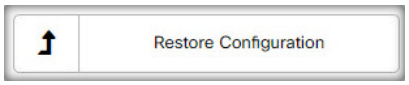
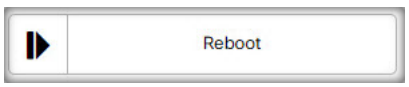
表 4: 设备清单详细信息

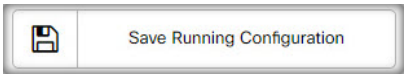
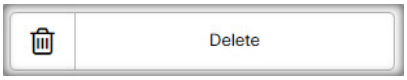
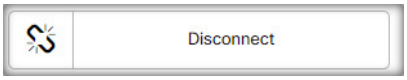
项目	说明
主机名	显示设备的名称。
类型	设备类型，例如交换机、路由器或无线接入点 (WAP)。
标记	列出与设备关联的所有标记。
IP	设备的互联网协议 (IP) 地址。
MAC（默认情况下隐藏）	介质访问控制(MAC)地址是某些网络接口类型所需的标准化数据链接层地址。每个设备的这些地址都是特定且唯一的，不能用于网络中的其他设备。

项目	说明
序列号	设备的序列号。
版本	设备的当前固件版本。
供应商（默认情况下隐藏）	制造设备的供应商。
型号	设备的型号名称。
组织	设备所属的组织。
网络	设备所属的网络
通知	设备的待确认通知计数
PnP 状态（默认情况下隐藏）	设备的当前 Network Plug and Play 状态。有关详细信息，请参阅 **Network Plug and Play** 页面。

设备清单页面上提供以下其他控件：

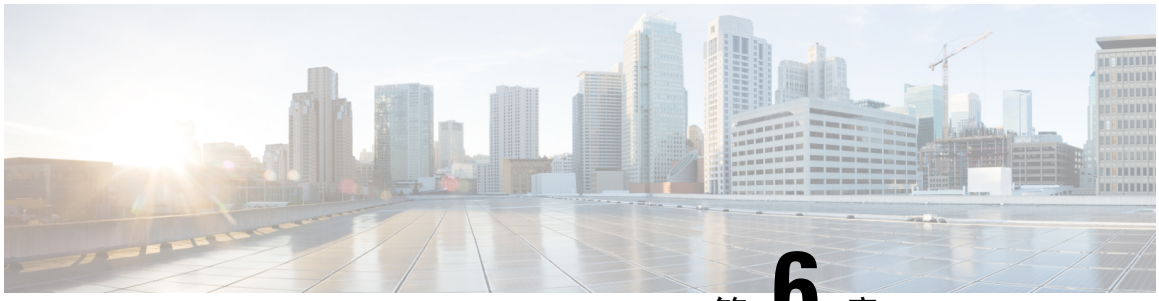
- **选择列**按钮 - 使用表左上角的此按钮可选择要显示哪些列
- **过滤器框** - 可以在**过滤器框**中键入设备名称、设备类型、序列号等来限制显示结果。默认情况下，系统将过滤设备清单以仅显示网络设备
- **添加**图标 - 单击 ( ) 加号图标，可在系统发现新设备之前将该设备添加到设备清单中。手动将设备添加到设备清单中时，可以提供设备的基本信息，包括身份信息、组织和设备组以及 PnP 设置。提前提供此信息可确保设备在连接到网络时得到正确管理
- **刷新**按钮 - 点击此按钮可更新表格以显示最新的可用信息
- **操作**按钮 - 以下操作按钮可用于对一个或多个选定设备执行操作

	将固件升级为最新版本
	从本地升级
	备份配置
	恢复配置
	重启

	保存运行配置
	删除
	断开连接

仅当选择一个或多个支持操作的设备时，系统才会显示操作按钮。

注释 有关这些操作的更多详细信息，请参阅执行设备操作



第 6 章

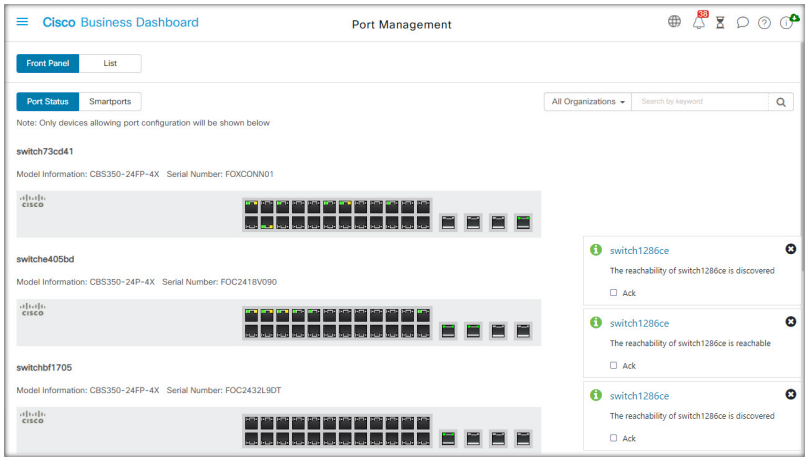
端口管理

关于端口管理

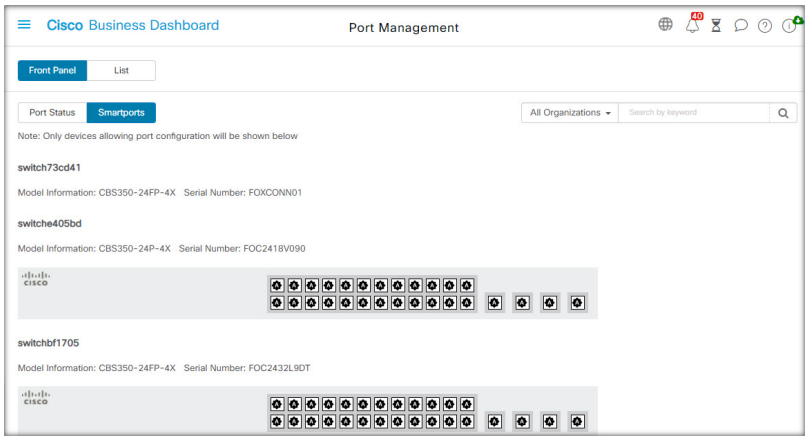
端口管理页面提供每个设备的前面板视图，包括可由 Cisco Business Dashboard 配置的交换机端口。此页面可用于查看端口的状态（包括流量计数器）和更改端口配置。另外，此页面还可用于查看支持智能端口的设备端口并可为这些端口配置智能端口角色。您可以使用搜索框来限制显示的设备。键入完整或部分设备名称、产品 ID 或序列号，可查找所需的设备。

此外还提供相同信息的列表视图，以表格格式显示所有交换机端口。**端口管理**页面的前面板视图提供两种不同的设备视图：

物理视图可用于查看状态和在物理层更改端口配置。您可以查看或更改速度、双工、节能以太网 (EEE)、以太网供电 (PoE) 和 VLAN 的设置。每个端口均显示一个绿色 LED 和一个黄色 LED，前者表示链路，后者表示正在向连接的设备供电。

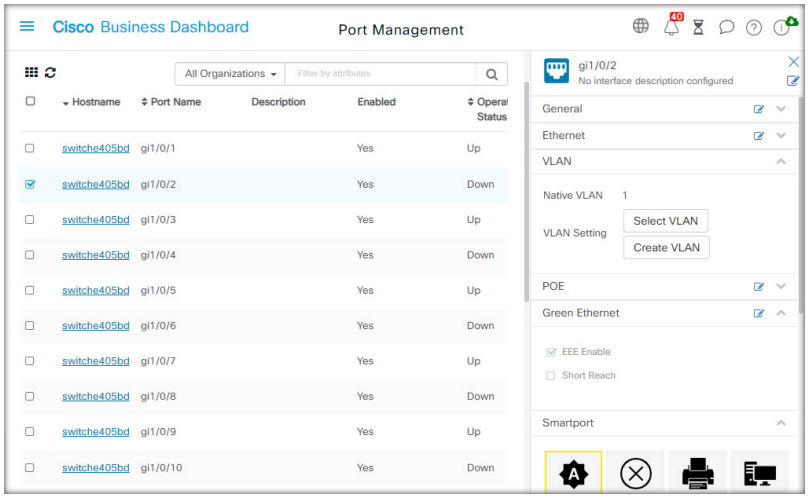


智能端口视图可用于查看每个端口当前的智能端口角色，并可用于更改该角色。每个端口均覆盖了一个图标，该图标表示当前的角色



注释 **智能端口**是可应用内置（或用户定义）模板的接口。这些模板旨在提供一种快速配置设备的方法，从而满足通信要求并利用各种网络设备的功能。

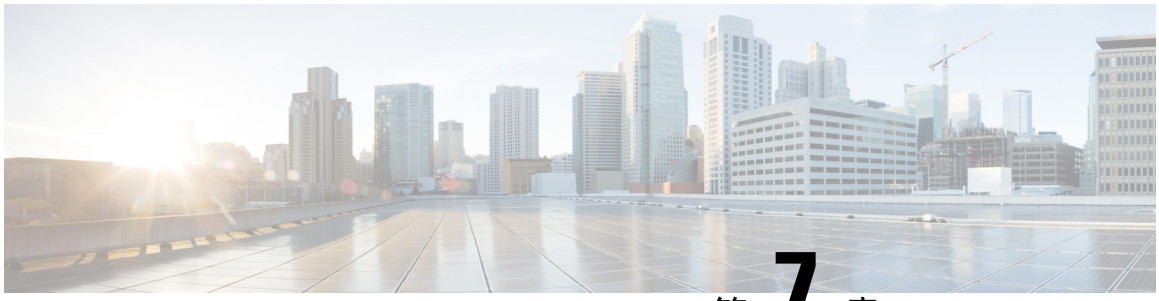
要查看端口的状态，请点击前面板视图或列表视图中的端口。此时屏幕上将显示端口的**基本信息**面板，该面板中显示下列面板：



常规	此面板显示端口的物理层状态，允许您启用或关闭端口
以太网	使用此面板控制速度和双工设置
端口验证	使用此面板，您可以在此端口上启用 802.1x 端口身份验证。将针对分配给设备的身份验证配置文件中指定的身份验证服务器执行身份验证。 如果未定义身份验证服务器，Cisco Business Dashboard 将用作默认身份验证服务器。
VLAN	此面板显示当前在端口上配置的 VLAN。点击**选择 VLAN** 或**创建 VLAN** 按钮可修改此配置

POE	此面板仅针对支持 POE 的端口显示，并且可用于配置端口的 POE 设置。此外，您还可以点击“切换电源”按钮，重新启动连接的 POE 设备
绿色以太网	通过此面板，您可以管理端口的节能以太网 (EEE) 配置
Smartport	此面板显示可用于此端口的智能端口角色。点击某个角色可将该配置应用到端口。当前配置的角色将突出显示。

要更改端口设置，请点击包含该设置的窗格右上角的**编辑**图标。完成更改后，点击**保存**图标。



第 7 章

网络配置

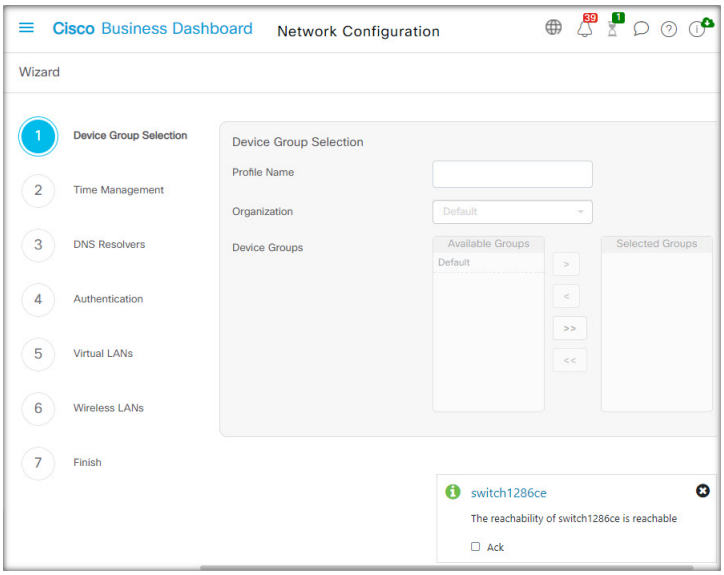
本章包含以下各节：

关于网络配置

通过**网络配置**页面，可以定义通常适用于网络中部分或所有设备的各种配置参数。这些参数包括时间设置、域名服务、管理员身份验证以及虚拟局域网和无线局域网等配置。您可以针对其中每个区域单独创建配置文件，也可以使用向导在单一工作流程中为每个区域创建配置文件。系统会将这些配置文件应用到一个或多个设备组，然后再推送至设备。

使用向导

使用向导为每个网络配置元素创建配置文件，并且将这些配置文件分配给单个工作流程中的一个或多个设备组。



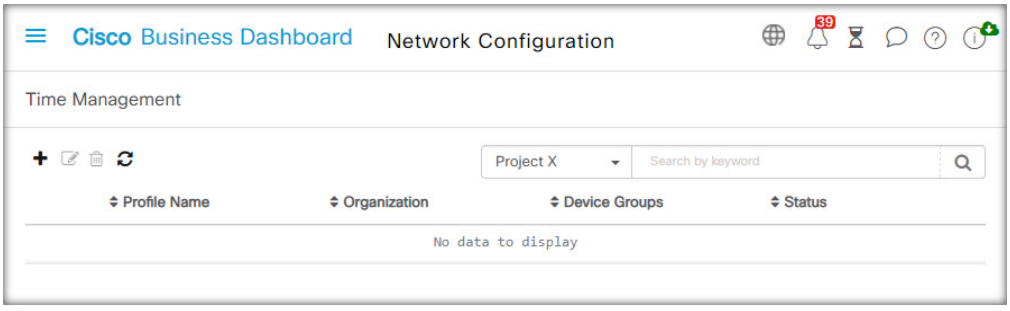
1. 导航到**网络配置** > **向导**。
2. 在**设备组选择**屏幕中输入此配置的配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
3. 点击**下一步**。

   在后面的每个屏幕中，根据需要选择配置。有关这些参数的更多详细信息，请参阅以下部分。
4. 完成每个屏幕上的配置设置，然后点击**下一步**。

   如果不想在特定屏幕上为此配置文件配置设置，可点击**跳过**。
5. 点击**返回**可访问之前的屏幕，或者可以点击左侧的标题。
6. 完成配置，并检查最终屏幕上的设置。点击**完成**将该配置应用于所选的设备。

配置时间管理

通过**时间管理**页面，可以为网络配置时区、夏令时和 NTP 服务器。以下部分介绍如何创建、修改和删除时间设置配置文件。



创建时间管理配置文件

1. 导航到**网络配置** > **时间管理**。
2. 单击 （加号）图标以添加新配置文件。
3. 在**设备组选择**部分，输入此配置的配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
4. 在**时间设置**部分，从下拉列表中选择适当的时区。
5. 或者选中**夏令时**复选框启用该设置，然后在提供的字段中指定夏令时的参数。您可以选择指定固定日期或循环模式。另外，也可以指定要使用的时差。
6. 或者，在时钟同步的**使用 NTP** 部分选中“网络时间协议 (NTP)”复选框以启用该设置。在提供的框中，指定至少一个 NTP 服务器地址。
7. 点击**保存**。

修改时间管理配置文件

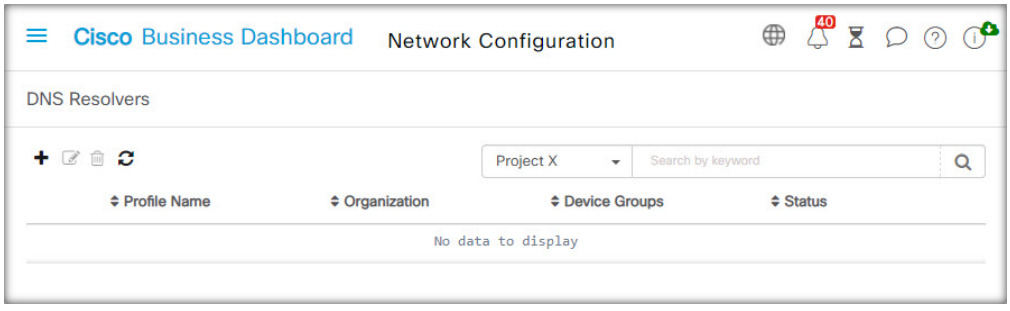
1. 选择要更改的配置文件旁边的单选按钮，然后点击**编辑**图标。
2. 对配置文件设置进行必要的更改，然后点击**更新**。

删除时间管理配置文件

1. 选择需要删除的配置文件旁边的单选按钮。
2. 点击**删除**图标。

配置 DNS 解析器

通过**DNS 解析器**页面，您可以为网络配置域名和域名服务器。以下部分介绍如何创建、修改和删除 DNS 解析器配置文件。



创建 DNS 解析器配置文件

1. 导航到**网络配置** > **DNS 解析器**。

2. 单击 （加号）图标以添加新配置文件。
3. 在**设备组选择**部分，输入此配置的配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
4. 指定网络的域名。
5. 指定至少一个 DNS 服务器地址。
6. 点击**保存**。

修改 DNS 解析器配置文件

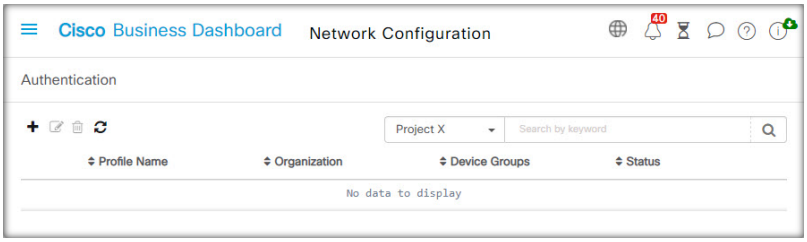
1. 选择要更改的配置文件旁边的单选按钮，然后点击**编辑**图标。
2. 对配置文件设置进行必要的更改，然后点击**更新**。

删除 DNS 解析器配置文件

1. 选择要删除的配置文件旁边的单选按钮。
2. 点击**删除**图标。

配置身份验证

通过**身份验证**页面，您可以配置对网络设备的管理用户访问权限，并设置在基于用户对网络访问进行身份验证时要使用的身份验证服务器（RADIUS 服务器）。以下部分介绍如何创建、修改和删除身份验证配置文件。



创建身份验证配置文件

1. 导航到**网络配置** > **身份验证**。
2. 单击 （加号）图标以添加新配置文件。
3. 在**设备组选择**部分，输入此配置的配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
4. 也可以指定一个或多个用户名和密码组合以进行本地用户身份验证。单击 （加号）图标可添加其他用户。

5. 另外，您还可以选择要求使用复杂密码。
6. 也可以指定一个或多个 RADIUS 服务器用于身份验证。您可以选中此复选框，以启用使用 Cisco Business Dashboard 进行身份验证。
7. 点击**保存**。

注释 需要访问网络的用户必须被授予网络访问权限。有关详细信息，请参阅用户，第 86 页。

注释 使用 Cisco Business Dashboard 进行网络访问身份验证时，强烈建议 Dashboard 使用由公共证书颁发机构签名的证书。如果不这样做，大多数客户端设备会向用户显示证书警告，并且某些客户端根本不会继续进行身份验证。

修改身份验证配置文件

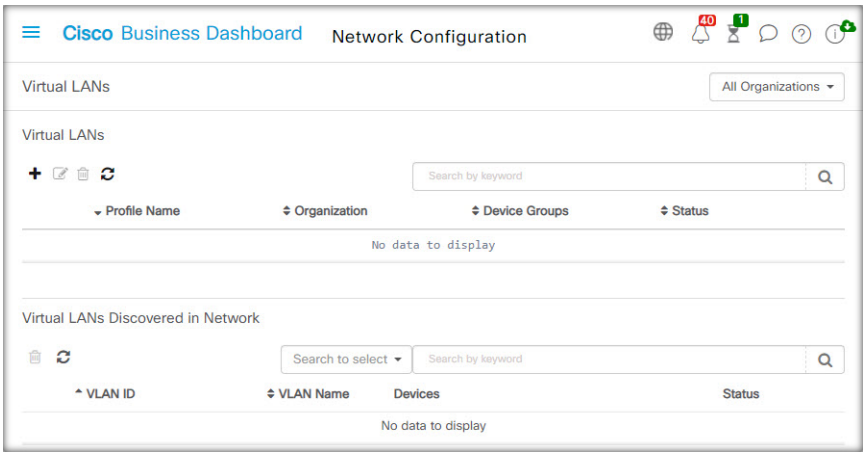
1. 选择要更改的配置文件旁边的单选按钮，然后点击**编辑**图标。
2. 对配置文件设置进行必要的更改，然后点击**更新**。

删除身份验证配置文件

1. 选择需要删除的配置文件旁边的单选按钮。
2. 点击**删除**图标。

配置虚拟局域网

通过**虚拟局域网**页面，可以将交换机网络分为多个虚拟网络或 VLAN。您可以查找网络中未经 Cisco Business Dashboard 配置但也在此页显示在单独的表中的现有 VLAN。以下部分介绍如何创建、修改和删除虚拟局域网配置文件。



创建虚拟局域网

1. 导航到**网络配置** > **虚拟局域网**。
2. 单击 （加号）图标以添加新 VLAN。
3. 在**设备组选择**部分，输入此配置的配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
4. 为该 VLAN 指定一个描述性名称和要使用的 VLAN ID。VLAN ID 应为 1-4094 范围内的数值。
5. 您可以使用单个配置文件创建多个VLAN。如果要在此配置文件中创建其他VLAN，请点击**再添加一个**并返回步骤 4。
6. 点击**保存**。系统将在所选组中支持 VLAN 的所有设备上创建新的 VLAN。

如果新创建的 VLAN 的 VLAN ID 与设备组中设备上已存在的现有 VLAN 匹配，则该 VLAN 将被 Cisco Business Dashboard 采用并从发现的虚拟局 LAN 表中删除。

修改 VLAN

1. 选中要更改的 VLAN 旁边的单选按钮，然后点击**编辑**图标。
2. 对 VLAN 设置进行必要的更改，然后点击**更新**。

删除 VLAN

选中要删除的 VLAN 旁边的单选按钮，然后点击**删除**图标。

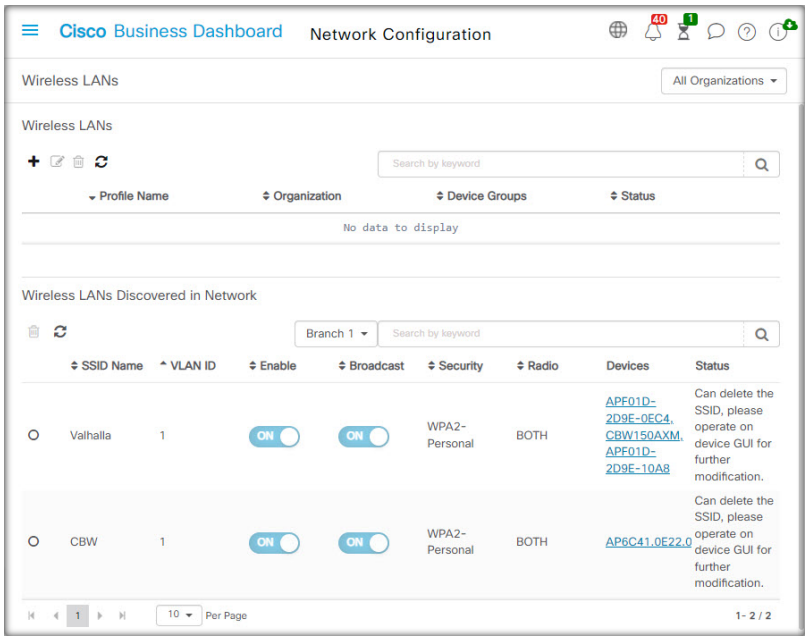
删除不是通过 Cisco Business Dashboard 创建的 VLAN

在发现的 VLAN 表中，点击要删除的一个或多个 VLAN 旁边的**删除**图标。

注释 VLAN 1 无法删除。

配置无线局域网

通过**无线局域网**页面，您可以管理您的环境中的无线网络。您可以查找网络中未经 Cisco Business Dashboard 配置但也显示在单独的表中的现有无线局域网。以下部分介绍如何创建、修改和删除无线局域网配置文件。



创建无线局域网

1. 导航到**网络配置** > **无线局域网**。
2. 点击 （加号）图标以添加新无线局域网配置文件。
3. 在**设备组选择**部分，输入配置文件名称，选择相应组织并选择要配置的一个或多个设备组。
4. 点击 （加号）图标以添加新 SSID。
5. 指定无线局域网的 SSID 名称和应与之关联的 VLAN ID。VLAN ID 编号应在 1-4095 范围内，如果网络中尚不存在该编号，将自动创建一个新 VLAN。
6. 选择所需的安全类型。

   如果选择**访客**作为安全类型，则需要指定要与访客门户结合使用的身份验证类型。选项包括“用户名/密码”、“Web 同意”和“邮箱地址”。如需了解这些选项的详情，请参阅配置访客门户，第 51 页。

   如果选择**企业**安全类型，请确保为包含要使用的首选 RADIUS 服务器的设备分配身份验证配置文件。如果尚未为该设备定义身份验证配置文件，则默认使用 Cisco Business Dashboard。
7. 或者，点击展开“高级设置”以更改**广播**、**应用可视性**、**本地分析**和**无线电**设置，以满足您的要求。

8. 点击**保存**以继续，或点击**取消**以放弃更改。
9. 您可以使用单个配置文件创建多个无线局域网。如果要在此配置文件中创建其他无线局域网，请返回步骤 4。
10. 点击**保存**。系统将在所选组中具备无线接入点功能的所有设备上创建新的 WLAN。

如果新创建的配置文件的无线局域网配置与设备组中设备上已存在的现有无线局域网匹配，则该无线局域网将被 Cisco Business Dashboard 采用并从发现的无线局域网表中删除。

修改无线局域网

1. 选中要更改的无线局域网旁边的单选按钮，然后点击**编辑**图标。
2. 对无线局域网设置进行必要的更改，然后点击**更新**。

删除无线局域网

选择要删除的无线局域网旁边的单选按钮，然后点击**删除**图标。

注释 如果在创建无线局域网时由系统自动创建虚拟局域网，则在删除无线局域网时系统不会删除该虚拟局域网。可以在**虚拟局域网**页面上删除该虚拟局域网。

删除不是通过 Cisco Business Dashboard 创建的无线局域网

在已发现的无线局域网表中，点击与要删除的无线局域网对应的单选按钮，然后点击**删除**图标。在某些情况下，可能无法从特定设备中删除 WLAN。这些情况下，需要直接更改设备配置。

配置无线电

通过“无线电”页面，您可以管理环境中的无线网络射频 (RF) 优化。使用无线电配置文件，您可以控制无线接入点是否应自动调整其无线电设置以适应环境，还可以启用欺诈无线接入点和干扰源检测及报告。

以下部分介绍如何创建、修改和删除无线电配置文件。

创建无线电配置文件

1. 导航到**网络配置** > **无线电**。
2. 点击 （加号）图标以添加新无线电配置文件。
3. 在“设备组选择”部分，完成以下操作：
   - 为此配置输入配置文件名称。
   - 选择组织。

- 选择要配置的一个或多个设备组。

4. 选择是否应由网络中的无线接入点执行自动射频优化。如果启用射频优化，请确保为“客户端密度”和“流量类型”选择适当的值。
5. （可选）启用欺诈无线接入点检测。
6. （可选）启用干扰源检测。
7. 点击**保存**。

   系统会将新的无线优化设置应用于所选组中具有射频优化功能的所有无线接入点。

修改无线电配置文件

1. 选中要更改的无线电配置文件旁边的单选按钮，然后点击编辑图标。
2. 对射频优化设置进行必要的更改，然后点击“更新”。

删除无线电配置文件

1. 选择要删除的无线电配置文件旁边的单选按钮，然后点击删除图标。

配置访客门户

通过“访客门户”页面，您可以集中管理在连接到访客无线网络时向访客用户显示的网页。Cisco Business Dashboard 为每个组织托管一个访客门户，并且每个门户可以单独定制，以代表组织的身份。

访客门户支持多种用户身份验证方法，同一门户可以在不同的网络上显示不同的身份验证方法。支持的身份验证方法包括：

- 用户名/密码 - 必须提前在 Dashboard 中定义每个访客用户，并为其分配用户名和密码。连接到无线网络时，必须在访客门户中输入用户名和密码。
- Web 同意 - 向访客用户显示组织的可接受使用政策，必须接受该政策才能访问网络。
- 邮箱地址 - 在访问网络之前，系统会提示访客用户提供邮箱地址。邮箱地址被记录为客户端的用户名，可以在无线客户端报告和设备用户界面中看到。
- 社交媒体登录 - 访客用户必须使用 Facebook 或 Google 凭证进行身份验证。Facebook/Google 用户名被记录为客户端的用户名，可以在无线客户端报告和设备用户界面中看到。

可以通过更改所有文本字段（包括使用的字体）、修改颜色以及更新背景和徽标图像来定制每个访客门户的外观。

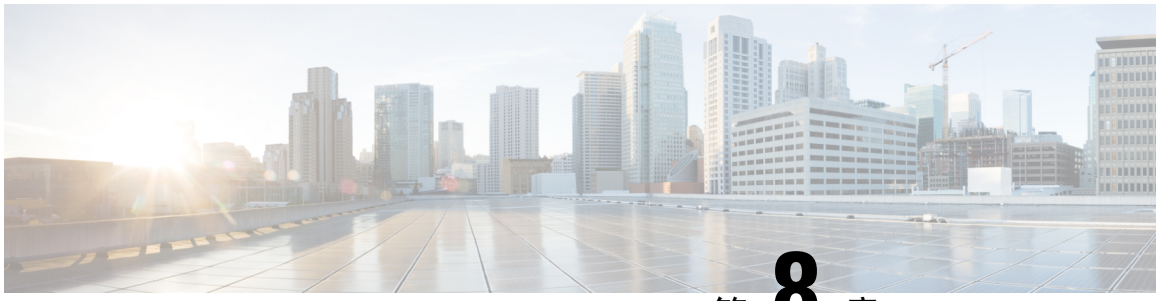
要定制访客门户，请执行以下操作：

1. 导航到**网络配置 > 访客门户**。

2. 选择要定制的访客门户的单选按钮，然后点击编辑图标。
3. 使用所显示的表单更新强制网络门户的外观。您可以修改任何文本字段，上传要用作背景和徽标的新图像，以及修改所使用的颜色和字体。

   访客门户的内容略有不同，具体取决于所选的身份验证方法。选择页面底部的选项卡，更新不同版本门户的字段。

   您可以点击每种不同身份验证方法的“预览”按钮，在保存之前查看更改。要将门户恢复为默认外观，请点击右上角的“重置为默认值”按钮。
4. 点击**更新**以保存更改，或点击**取消**以放弃更改。



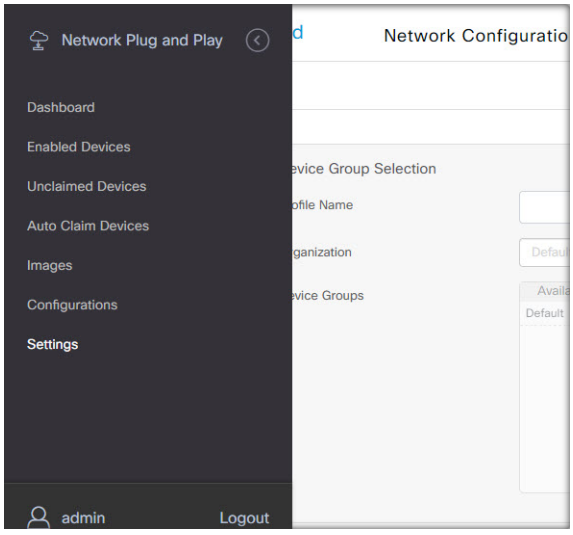
第 8 章

Network Plug and Play

本章包含以下各节：

关于 Network Plug and Play

Network Plug and Play 是一种与支持 Network Plug and Play 的设备配合使用的服务，不仅可以集中管理固件和配置，还可零接触部署新的网络设备。设备可以使用 Network Plug and Play 协议直接部署，或者在与 Dashboard 关联的探测器发现时的情况下间接部署。



安装后，支持 Network Plug and Play 的设备将通过手动配置、DHCP、DNS 或 Plug and Play Connect 服务其中之一来识别 Network Plug and Play 服务器。以下部分将提供有关Cisco Business Dashboard中的 Network Plug and Play 服务配置的更多详细信息。

网络要求

Network Plug and Play 设备会通过以下其中一种方法自动查找 Network Plug and Play 服务器的地址。它会依次尝试每种方法，直至找到地址或所有方法都失败。采用的方法依次为：

- **手动配置** - 可通过管理界面对支持 Network Plug and Play 的设备手动配置服务器地址
- **DHCP** - 可在“供应商特定信息”选项中向设备提供服务器地址
- **DNS** - 如未提供 DHCP 供应商特定信息选项，则设备将使用众所周知的主机名对服务器执行 DNS 查找
- **Plug and Play Connect 服务** - 如果其他方法都不成功，设备将尝试连接 Plug and Play Connect 服务。然后，该服务会将设备重定向到您的服务器。

设备识别服务器后，便会连接服务器，并且按照服务器的指定更新固件和配置。

证书要求

与 Network Plug and Play 服务器建立连接时，客户端会执行检查以确保服务器提供的证书有效且可以信任。要使证书可接受并继续执行连接，证书必须满足以下条件：

- 证书必须由受信任的证书颁发机构 (CA) 签名，或者证书本身必须受客户端信任。从向 DHCP 获知的 TrustpoolBundleURL 下载的证书或从 Plug and Play Connect 服务下载的证书受客户端信任
- 如果服务器身份是使用手动配置、DHCP 或 Plug and Play Connect 发现的并且是 IP 地址，则**通用名称**字段或**使用者备用名称**字段必须包含该 IP 地址
- 如果服务器身份是使用手动配置、DHCP 或 Plug and Play Connect 发现的并且是主机名，则**通用名称**字段或**使用者备用名称**字段必须包含该主机名
- 如果服务器身份是使用 DNS 发现功能发现的，则**通用名称**字段或**使用者备用名称**字段必须包含与已知主机名 pnpserver.<本地域> 对应的 IP 地址。

注释 某些较旧的 Network Plug and Play 客户端实施不验证证书中是否存在服务器身份。

使用 DHCP 设置发现

要使用 DHCP 发现服务器地址，设备会发送带有选项 60（包含字符串“ciscopnp”）的 DHCP 发现消息。DHCP 服务器必须发送含有供应商特定信息选项（选项 43）的响应。设备会从该选项中提取服务器地址，并使用该地址连接服务器。含有 Network Plug and Play 服务器地址的选项 43 字符串示例：“5A1N;B2;K4;I172.19.45.222;J80”。

选项 43 字符串包含以下组成部分（以分号分隔）：

- 5A1N - 指定即插即用的 DHCP 子选项、主动操作、版本 1、无调试信息。无需更改这部分字符串。
- B2 - IP 地址类型：
  - B1 = 主机名
  - B2 = IPv4
- K4 - 思科即插即用代理和服务器之间使用的传输协议：
  - K4 = HTTP（默认值）
  - K5 = HTTPS
- Ixxx.xxx.xxx.xxx - 服务器的 IP 地址或主机名（后面跟大写字母 I）。在本例中，IP 地址为 172.19.45.222。
- Jxxxx - 用于连接服务器的端口号。在本例中，端口号为 80。HTTP 的默认端口为 80，HTTPS 的默认端口为 443。
- T*trustpoolBundleURL* - 如果是从服务器以外的其他位置检索，可选择此参数指定 trustpool 捆绑包的外部 URL。例如，要从 TFTP 服务器 10.30.30.10 下载捆绑包，您可以指定如下参数：Ttftp://10.30.30.10/ca.p7b
- 如果您使用的是 trustpool 安全防护，而且未指定 T 参数，则设备将从服务器检索 trustpool 捆绑包。
- Zxxx.xxx.xxx.xxx; - NTP 服务器的 IP 地址。当使用信任池安全确保所有设备均已同步时，此参数为必需参数。

查看 DHCP 服务器文档，获取关于如何配置 DHCP 选项的详细信息。

使用 DNS 设置发现

如果 DHCP 发现无法获取服务器的 IP 地址，设备将回退到 DNS 查找方法。根据 DHCP 服务器返回的网络域名，设备将使用预设主机名“pnpserver”为服务器构建完全限定域名 (FQDN)。

例如，如果 DHCP 服务器返回域名“example.com”，则设备创建的 FQDN 为“pnpserver.example.com”。然后，它使用本地名称服务器解析此 FQDN 的 IP 地址。

使用即插即用连接设置发现

Plug and Play Connect 是思科提供的一种服务，是支持 Network Plug and Play 的设备用来发现服务器的最后手段。要使用 Plug and Play Connect 发现服务器，必须先创建代表 PnP 服务器的控制器配置文件，然后向 Plug and Play Connect 注册每个设备。

访问即插即用连接服务

要访问 Plug and Play Connect Service，请执行以下操作：

1. 在 Web 浏览器中，导航到 *https://software.cisco.com*

2. 点击屏幕右上角的**登录**按钮。使用与思科智能账户关联的 cisco.com ID 登录。
3. 选择 **Network Plug and Play** 标题下面的 **Plug and Play Connect** 链接。**Plug and Play Connect** 服务主页将会显示出来。

创建控制器配置文件

要为 PnP 服务器创建控制器配置文件，请执行以下操作：

1. 在浏览器中打开 Plug and Play Connect 网页。如有必要，请选用正确的虚拟账户。
2. 选择控制器配置文件链接，然后点击“添加配置文件”按钮。
3. 从下拉列表中选择 PnP 服务器的控制器类型。然后点击“下一步”。
4. 为该配置文件指定名称和描述（可选）。
5. 在“主控制器”标题下面，使用提供的下拉列表选择是按名称还是 IP 地址指定服务器。在提供的字段中填写服务器的名称或地址。
6. 选择用来与服务器通信的协议。强烈建议使用 HTTPS 来确保调配过程的完整性。
7. 如果选择的协议是 HTTPS，则应使用提供的控件上传服务器使用的证书。有关从Cisco Business Dashboard下载证书的详细信息，请参阅管理证书，第 99 页。
8. 可选择指定辅助控制器。
9. 点击**下一步**，查看设置，然后点击**提交**。

注册设备

某些直接从思科购买的产品可能在订购时便与您的思科智能账户相关联，这些产品将自动添加到Plug and Play Connect。但大多数支持 Cisco Business Plug and Play 的产品都需要进行手动注册。要向 Plug and Play Connect 注册设备，请执行以下操作：

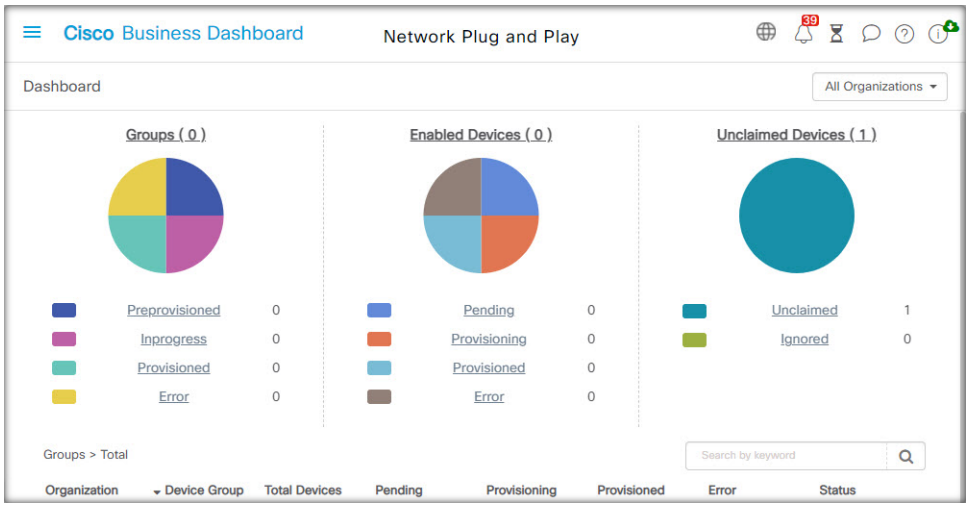
1. 在浏览器中打开 Plug and Play Connect 网页。如有必要，请选用正确的虚拟账户。
2. 选择**设备**链接，然后点击**添加设备**。要将设备手动添加到您的账户，您可能需要获得批准。这是一种一次性过程，如果需要的话，获得批准后，您将收到邮件通知。
3. 选择手动添加设备还是通过上传 CSV 格式的详细信息添加多个设备。点击提供的链接，下载 CSV 样本文件。如果选择上传 CSV 文件，请点击**浏览**按钮选择文件。
4. 点击**下一步**。
5. 如果选择手动添加设备，请点击**识别设备**。为要添加的设备指定序列号和产品 ID。从下拉列表中选择一个控制器配置文件。可选择输入此设备的描述。
6. 重复步骤 4，直至添加所有设备，然后点击**下一步**。
7. 查看已添加的设备，然后点击**提交**。

配置 Network Plug and Play 服务

在为您的环境设置 Network Plug and Play 服务时，需要执行几项任务。其中包括上传配置和映像、添加并配置设备以使用 Network Plug and Play 服务，以及管理连接到该服务的设备（如果它们先前未向该服务注册）。以下部分将详细介绍这些任务。

使用 Network Plug and Play Dashboard

Network Plug and Play Dashboard 概要介绍了当前正在使用 Network Plug and Play 调配的设备。



将显示三个图表，其中显示按以下方式细分的设备状态：

- 设备组
- 已启用 PnP 的设备
- Cisco Business Dashboard 设备清单中未定义的设备（未申领设备）

每个图表均显示处于所列各个状态的设备或组的数量。您可以点击任何图表上的状态标题，查看属于该类别的设备或组的详细列表。下表提供了不同状态的细分：

表 *5: Network Plug and Play Dashboard* - 状态定义

状态	说明
组	
已进行预调配	仅启用 PnP 的设备处于“待处理”状态的设备组
进行中	一些启用 PnP 的设备处于“待处理”状态、一些处于“调配”或“已调配”状态的设备组。
已调配	所有启用 PnP 的设备均处于“已调配”状态的设备组。
Error	一个或多个启用 PnP 的设备处于“错误”状态的设备组。

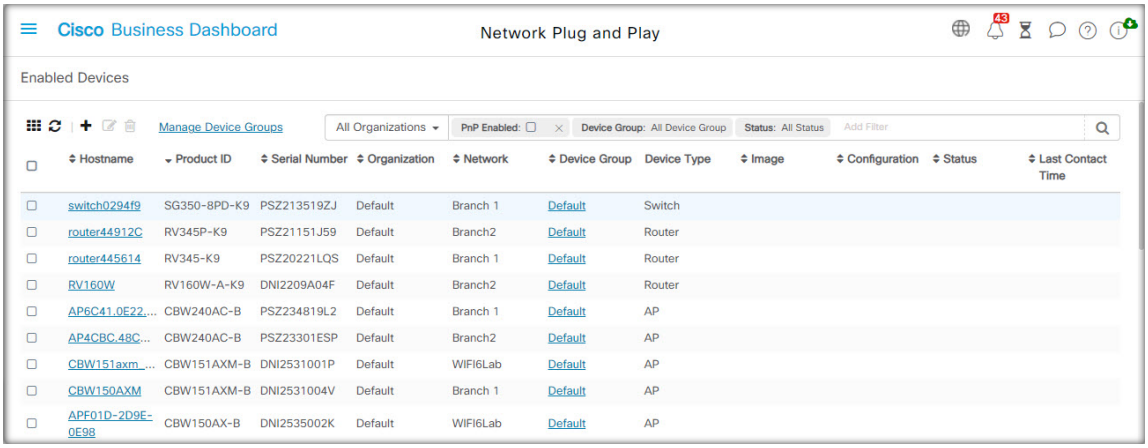
状态	说明
已启用设备	
待处理	设备清单中已启用 PnP 但尚未连接 PnP 服务器的设备。
调配	已连接 PnP 服务器并开始调配但尚未完成调配过程的设备。
已调配	已使用 PnP 成功调配的设备。
Error	PnP 调配过程失败的设备。
未申领设备	
未申领	已连接 PnP 服务器但未在设备清单中定义的设备。
完全不需要	用户已明确忽略的未申领设备。

您可以使用该页面右上角的“组织”下拉列表将显示的数据限制在特定组织范围内。查看设备组时，在搜索框中键入全部或部分组名称可以限制表中显示的组。或者，您在查看调配规则时可以在搜索框中输入设备名称、产品 ID 或序列号，以显示各个设备的当前状态。

注释 未申领设备的图表仅向查看**所有组织**的数据的**管理员**显示。

管理已启用设备

已启用设备是指设备清单中已配置为通过映像或配置文件进行调配的设备，或以前被 Cisco Business Dashboard 发现并且尝试使用 Network Plug and Play 协议进行连接的设备。



已配置映像或配置文件的已启用设备将在下次机会将该映像和配置文件应用于该设备。如果设备连接到 Dashboard 并由 Dashboard 管理，更改将立即应用。否则，更改将在设备下次连接（通过探测器或直接管理）时应用，或者在设备使用 Network Plug and Play 协议进行签入时应用。

要创建新的已启用设备，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **已启用设备**。

2. 点击 （加号）图标，将新的已启用设备添加到设备清单中。
3. 使用请求的参数（包括标识设备详细信息、组织、网络以及所属的设备组）填写**添加新设备**表单，然后点击**下一步**。
4. 或者，选择要应用于设备的固件映像。如果您为映像选择了**默认**，则当设备连接到服务器时，它使用的映像将是为该产品 ID 指定的默认映像。
5. 或者，选择要应用于设备的配置，以及配置版本（如果有多个版本）。如果配置是包含占位符的模板，则系统会显示一个表单，提示您应用于该设备的值。根据需要填写这些字段。如果模板使用系统定义的参数，可以选中该复选框，以显示将使用的值。
6. 点击**下一步**转到**摘要**屏幕。查看输入的数据，确保正确无误。您还可以在底部的预览窗口中查看最终的设备配置。如果对配置结果满意，请点击**完成**。

要编辑现有设备，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **已启用设备**。
2. 选中要修改的设备的复选框，然后点击**编辑**。或者，您还可以点击设备的名称。
3. 点击**下一步**以显示**调配设备**屏幕。如果需要，请更改映像和/或配置文件，并对与配置相关联的参数值进行任何更改。
4. 点击**下一步**转到**摘要**屏幕。查看输入的数据，确保正确无误。您还可以在底部的预览窗口中查看最终的设备配置。如果对配置结果满意，请点击**完成**。

注释 如果为已调配的设备更改映像或配置文件，则该设备的状态将重置为待处理，并且该设备将在下次签入 Dashboard 进行重新调配。

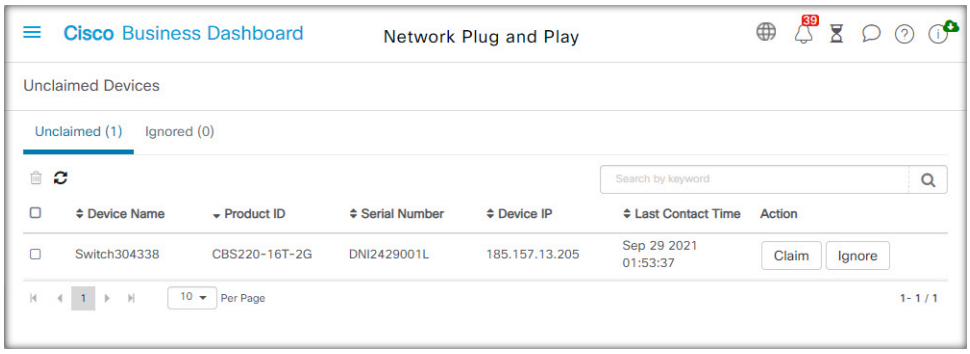
要删除已启用设备，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **已启用设备**。
2. 选中要删除的设备的一个或多个复选框，然后点击**删除**图标。

注释 如果在 Dashboard 本可获知已启用设备且该设备处于在线状态时删除该设备，则系统只会删除该设备的映像和配置文件。该设备将保留在设备清单中，类似于任何其他托管设备。如果随后某设备使用 PnP 连接到 Dashboard，则“已启用设备”表中将添加一个新条目。

未申领设备

注释 **未申领设备**页面仅对管理员可用。



未申领设备是指已连接服务但设备清单中没有与该设备匹配的设备记录的设备。要查看未申领设备的列表，并申领未申领设备，以便可以使用Network Plug and Play对其进行管理，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **未申领设备**，然后选择**未申领**选项卡。
2. 点击与要管理的设备对应的申领按钮。
3. 使用请求的参数（包括组织、网络以及所属的设备组）填写未申领设备表，然后点击**下一步**。
4. 或者，选择要应用于设备的固件映像。如果您为映像选择了**默认**，则当设备连接到服务器时，它使用的映像将是为该产品 ID 指定的默认映像。
5. 或者，选择要应用于设备的配置，以及配置版本（如果有多个版本）。如果配置是包含占位符的模板，则系统会显示一个表单，提示您应用于该设备的值。根据需要填写这些字段。

   如果模板使用系统定义的参数，您可以选中该复选框，以显示将使用的值。
6. 点击**下一步**转到**摘要**屏幕。查看输入的数据，确保正确无误。您还可以在底部的预览窗口中查看最终的设备配置。如果对配置结果满意，请点击**完成**。

要从“未申领”列表中删除设备并且不进行调配，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **未申领设备**，然后选择**未申领**选项卡。
2. 点击与要从列表中删除的设备对应的**忽略**。

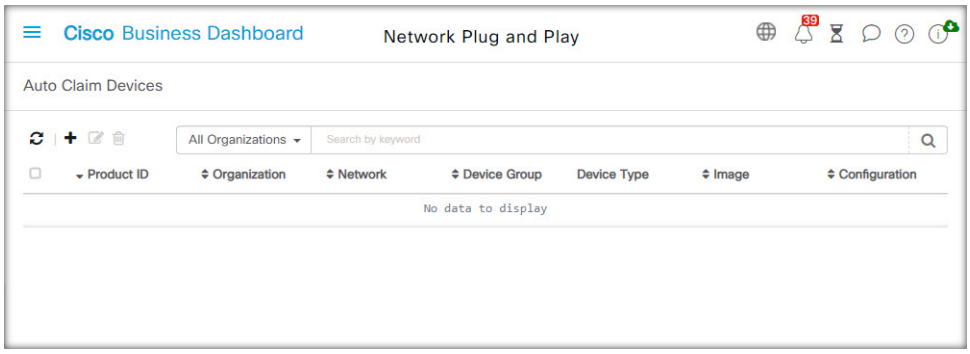
这些设备将被移动到**已忽略**列表，并且不会执行其他操作。要重新申领已忽略的设备，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **未申领设备**，然后选择**已忽略**选项卡。
2. 点击与要重新申领的设备对应的**取消忽略**按钮。

这些设备将被移动到**未申领**列表，然后您可以按上述方法申领设备。

自动申领设备

注释 **自动申领**页面仅对管理员可用。



可以通过为相应产品 ID 创建自动申领规则来利用服务器自动申领和调配未申领设备。要创建自动申领规则，请执行以下步骤。

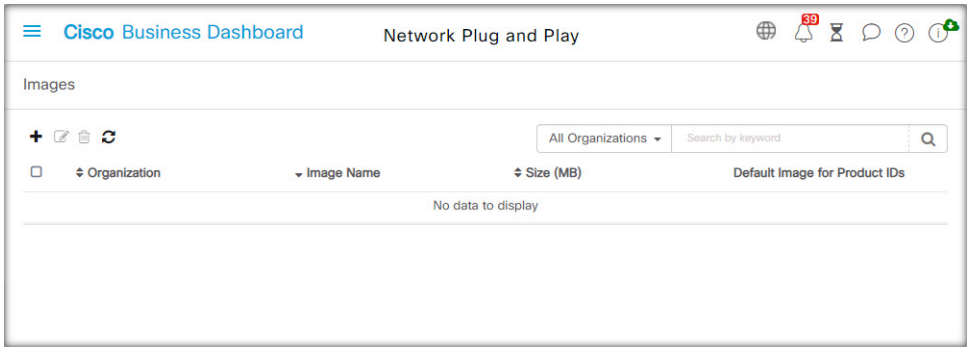
1. 导航到 **Network Plug and Play** > **自动申领设备**。
2. 单击 （加号）图标可创建新的**自动申领**规则。
3. 使用请求的参数（包括要匹配的产品 ID [PID]，以及新申领的设备应归属的组织、网络和设备组）填写自动申领设备表，然后点击**下一步**。
4. 或者，选择要应用于设备的固件映像。如果您为映像选择了**默认**，则当设备连接到服务器时，它使用的映像将是为该产品 ID 指定的默认映像。
5. 或者，选择要应用于设备的配置，以及配置版本（如果有多个版本）。如果配置是包含占位符的模板，则系统会显示一个表单，提示您应用于该设备的值。根据需要填写这些字段。

   如果模板使用系统定义的参数，您可以选中该复选框，以显示将使用的值。
6. 点击**下一步**转到**摘要**屏幕。查看输入的数据，确保正确无误。您还可以在底部的预览窗口中查看最终的设备配置。如果对配置结果满意，请点击**完成**。

系统将参照自动申领规则列表比对未列入设备清单中的新设备。如果有匹配项，则系统将使用由**自动申领**规则定义的映像和配置文件在设备清单中创建新设备记录。然后，相应地调配设备。如果设备与**自动申领**规则不匹配，则系统会将其添加到“未申领”列表中，并且不会执行其他操作。

设备固件映像

通过**映像**页面，您可以上传之后可能部署到设备的固件映像。



固件映像可指定为不同平台的默认映像，从而可让您非常轻松地更新整个设备系列的固件。固件映像特定于组织，只能用于与同一组织关联的调配设备。

要上传固件映像，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **映像**。
2. 单击 （加号）图标。
3. 从下拉列表中选择映像所属的组织。
4. 将 PC 中的固件映像拖放到**上传文件**窗口的目标区域。或者，单击目标区域并选择要上传的固件映像。
5. 点击**上传**。

您可以将映像指定为一种或多种设备类型的默认映像。要将某个映像指定为默认映像，请执行以下步骤。

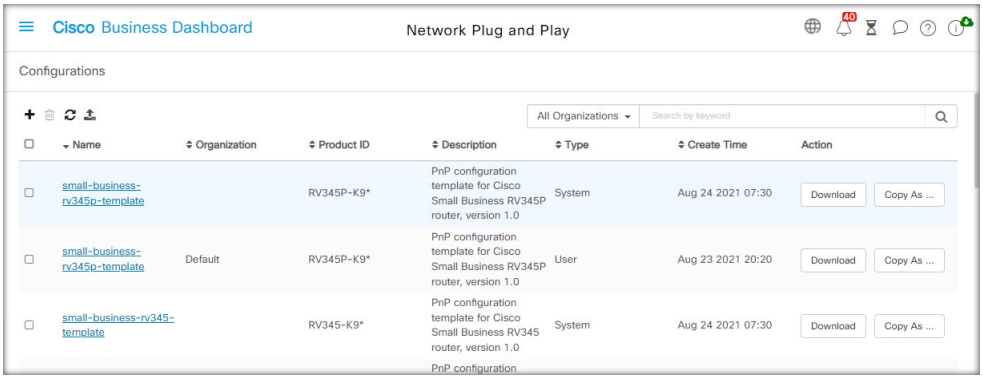
1. 导航到 **Network Plug and Play** > **映像**。
2. 在**映像**表格中选中与该映像对应的单选按钮，然后点击**编辑**。
3. 在**产品 ID 的默认映像**字段中输入以逗号分隔的产品 ID 列表。产品 ID 可以包含通配符“？”（表示单个字符）和“*”（表示字符串）。
4. 点击**保存**。

要删除映像，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **映像**。
2. 选择与要删除的映像对应的单选按钮，然后点击**删除**。

设备配置文件

通过“配置”页面，您可以上传或创建之后可能部署到设备的配置文件。配置文件特定于组织，只能用于与同一组织关联的调配设备。



配置文件可以是简单文本文件，也可以包含占位符和关联的元数据，以允许同一配置文件与多个设备一起使用，同时仍允许逐个设备来设置唯一参数。例如，单个配置模板可应用于多个设备，但是允许为每个设备分别指定主机名。

Dashboard应用中包含多个配置模板作为系统模板，可供所有组织使用。这些模板允许修改经常更改的设置，并且可以按原样使用，也可以复制并用作新模板的基础。

要手动创建新配置，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **配置**。
2. 单击 （加号）图标。
3. 系统将打开模板编辑器，左侧是用于配置的空白区域，右侧表单用于管理与模板关联的元数据。

   在左上角字段中输入配置的名称。选择组织，然后在右侧字段中输入支持此配置的用逗号分隔的产品 ID 列表。或者，输入说明。产品 ID 可以包含通配符“？”（表示单个字符）和“*”（表示字符串）。
4. 在左侧的文本区域中输入或粘贴文本，以创建配置。如有必要，请使用右侧的控件对元数据进行适当的更改。

   您可以使用**预览**按钮查看配置模板在分配给设备时将如何显示。
5. 完成所需配置后，点击**保存**。

要上传配置文件，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **配置**。
2. 点击**上传**图标。
3. 从下拉列表中选择配置所属的组织。为配置指定名称，并添加说明（可选）。
4. 将 PC 中的配置文件拖放到**上传文件**窗口的目标区域。或者，点击目标区域并选择要上传的配置文件。
5. 点击**上传**。

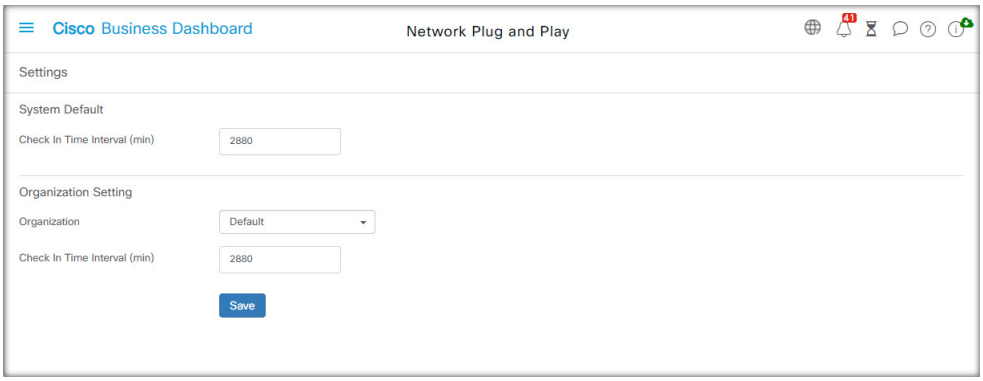
如果您愿意，可以点击已上传配置文件的文件名，在模板编辑器中查看内容。

要删除配置，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **配置**。
2. 选中要删除的配置的一个或多个复选框，然后点击**删除**图标。

管理设置

通过“Network Plug and Play 设置”页面，您可以控制 Network Plug and Play 协议的运行。



签入时间间隔用于控制设备在初始调配后连接到Network Plug and Play服务的频率。要修改此参数，请执行以下步骤。

1. 导航到 **Network Plug and Play** > **设置**。
2. 在所提供的字段中输入连接之间所需的时间间隔。时间单位为分钟，默认为 2880 分钟（即 2 天）。
3. 点击**保存**。

签入时间间隔是为整个系统设置的，但可以在组织级别进行覆盖。如果未为组织设置间隔，则将使用系统值。

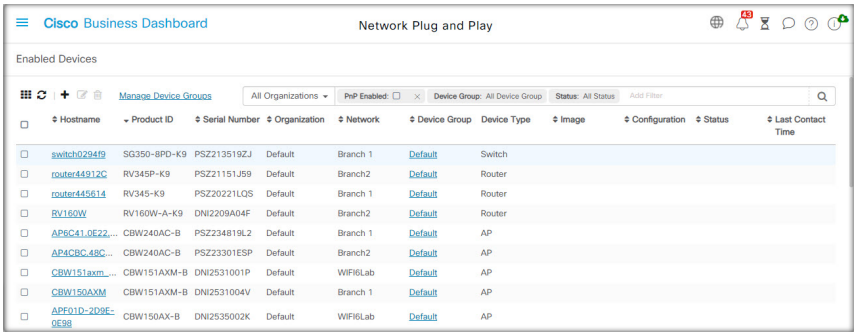
配置证书

在第一次启动期间 Cisco Business Dashboard自动生成的证书是自签名证书。在大多数情况下，这不足以让 Network Plug and Play 客户端接受该证书，并且需要生成新的证书。生成新的自签名证书或证书签名请求 (CSR) 时，除了 GUI 上**使用者备用名称**字段中指定的所有值外，Dashboard 还将在**使用者备用名称**字段中包括**通用名称**的内容。

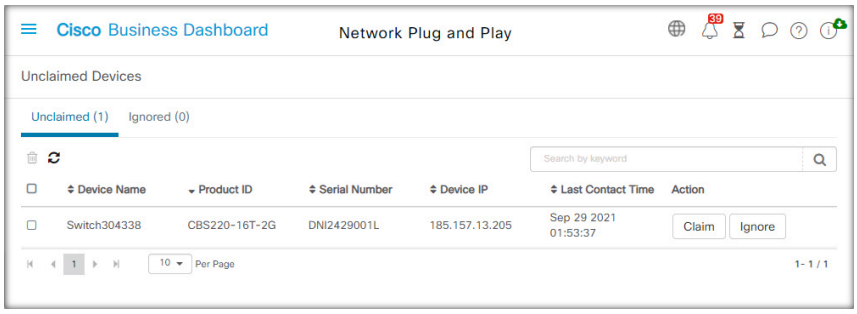
有关配置 Dashboard 证书的详细信息，请参阅 管理证书，第 99 页。

监控 Network Plug and Play

Network Plug and Play 服务已知的每个设备都显示在**启用的设备**页面



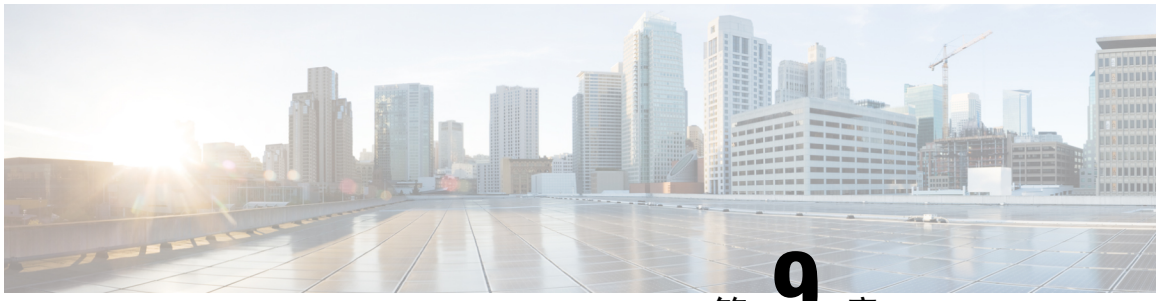
或**未申领设备**页面上，并且其状态也会显示出来。



还可以通过启用 **PnP 状态**列的显示，在**设备清单**页面上查看此状态。状态字段显示设备的当前状态，并含有以下表格中所列的某个值。点击状态字段可以查看更多详细信息，包括一段时间内设备的状态更改历史记录。

表 *6: Network Plug and Play* - 设备状态

状态	说明
待处理	设备已定义，但尚未与服务建立连接。
调配	设备已与服务进行初次连接。
Provisioning_Image	设备正在应用固件映像。
Provisioned _Image_Rebooting	设备正在重新启动，以运行新固件。
Provisioned_Image	已成功应用新固件。
Provisioning_Config	正在将配置文件应用到设备。
Provisioned_Config	已成功将配置文件应用到设备。根据设备类型，可能要重新启动才能应用配置。
Error	出现错误。请查看日志文件，了解更多详细信息。
已调配	设备的调配过程完成。



第 9 章

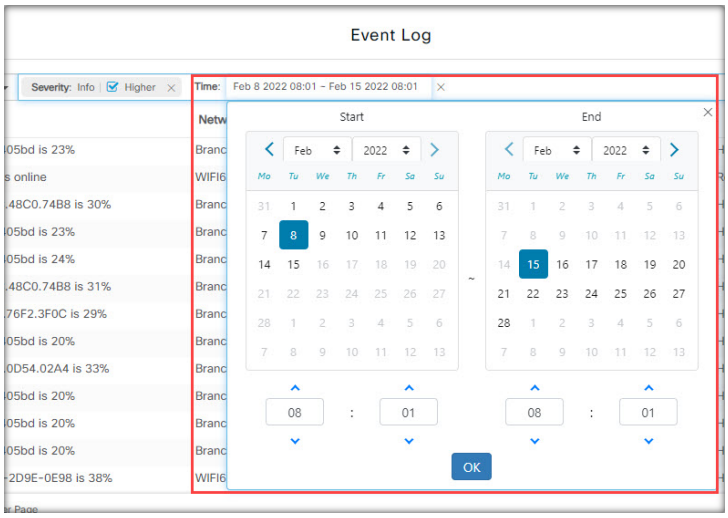
事件日志

本章包含以下各节：

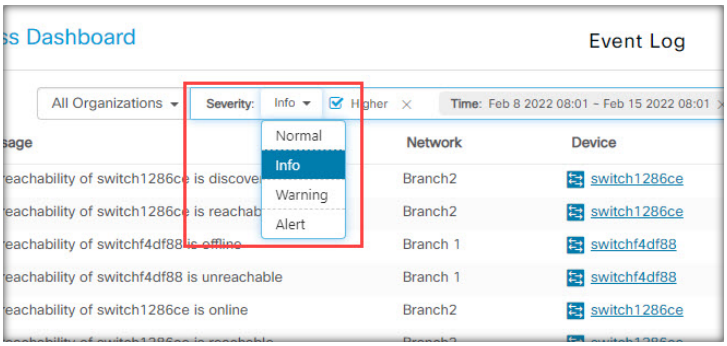
关于事件日志

打开“事件日志”屏幕，搜索整个网络中发生的事件。此屏幕提供了一个界面，您可以在其中搜索和排序整个网络中生成的事件。最多可存储 500,000 个事件，最长存储期限为 90 天。您可以使用提供的过滤器控件来限制基于以下参数的任何组合显示的事件：

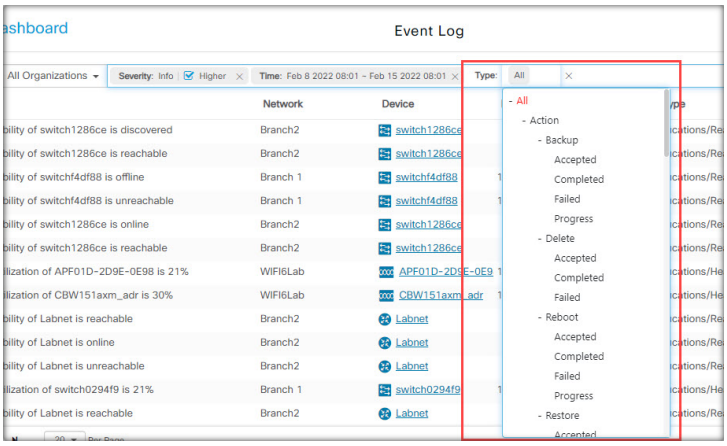
添加**时间**以指定需要关注的时间段的开始和结束时间。系统将只显示在此时间段内发生的事件。



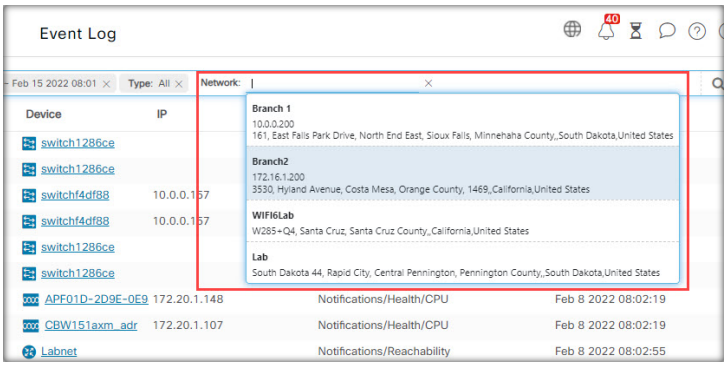
添加**严重性**以选择要显示的事件的级别。您还可以选中更高复选框，将具有更高严重性级别的事件包括在内。



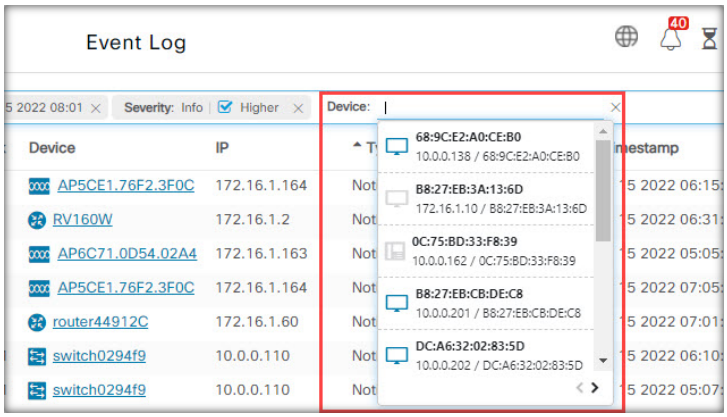
添加**类型**过滤器以选择要显示的一个或多个事件类型。类型以树结构排列，并且选择某个类型将自动包括树中所选类型下的所有事件类型。



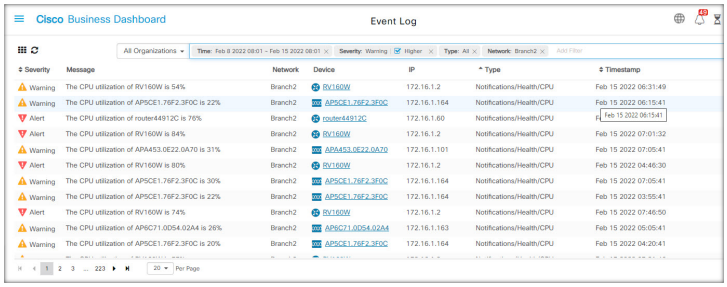
使用**网络**过滤器以显示一个或多个网络的事件。当您键入内容时，系统将显示匹配的站点。



使用**设备**过滤器以显示一个或多个设备的事件。当您键入内容时，系统将显示匹配的设备。您还可以按名称、IP 地址或 MAC 地址指定设备。



与过滤条件相匹配的事件将显示在如下所示的表格中。您还可以使用列标题对表中的信息进行排序。



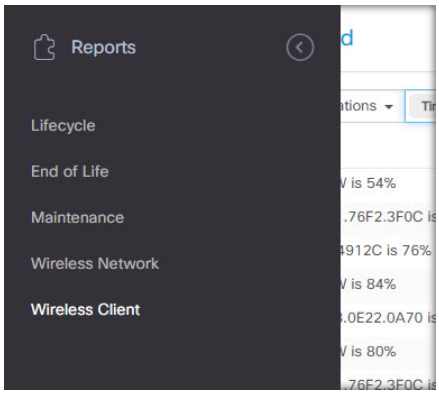
第 10 章

报告

本章包含以下各节：

关于报告

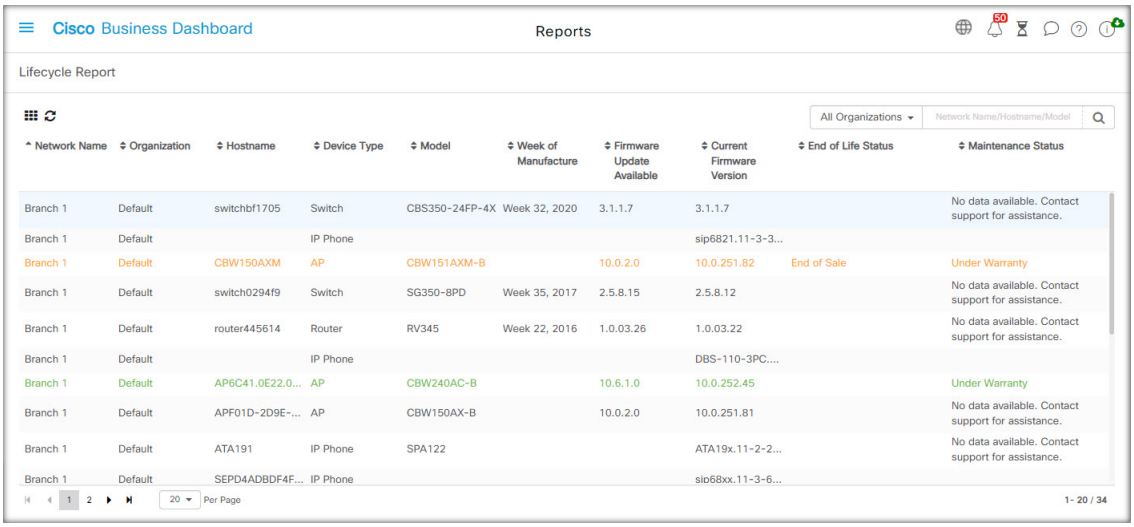
Cisco Business Dashboard 中的**报告**选项可提供有关您的网络的一系列报告。提供的报告包括：



- **生命周期** - 提供网络中的设备生命周期状态摘要。
- **生命周期终止** - 显示已发布生命周期终止公告的任何设备。
- **维护** - 列出所有设备及其保修状态，以及设备是否具有有效的支持合同。
- **无线网络** - 显示有关无线环境的信息，包括 SSID、无线接入点和频谱使用情况。
- **无线客户端** - 显示有关网络中的无线客户端的详细信息。

查看生命周期报告

生命周期报告提供网络设备状态的概要视图，其中还包括软件和硬件的生命周期状态。



此报告中提供的信息如下表所示。

字段	说明
网络名称	设备所在网络的名称。
组织	设备所属的组织。
主机名	设备的主机名。
设备类型	设备类型。
型号	设备的型号。
制造周	设备的制造日期，以周数和年份显示。
可用的固件更新	显示设备可用的最新固件版本，或表明该设备固件当前为最新版本。
固件版本	显示正在设备上运行的当前固件版本。
生命周期终止状态	指定是否已发布设备的生命周期终止公告，以及生命周期终止过程中的下一个关键里程碑日期。
维护状态	指定设备当前是否处于保修期内或受支持合同覆盖。

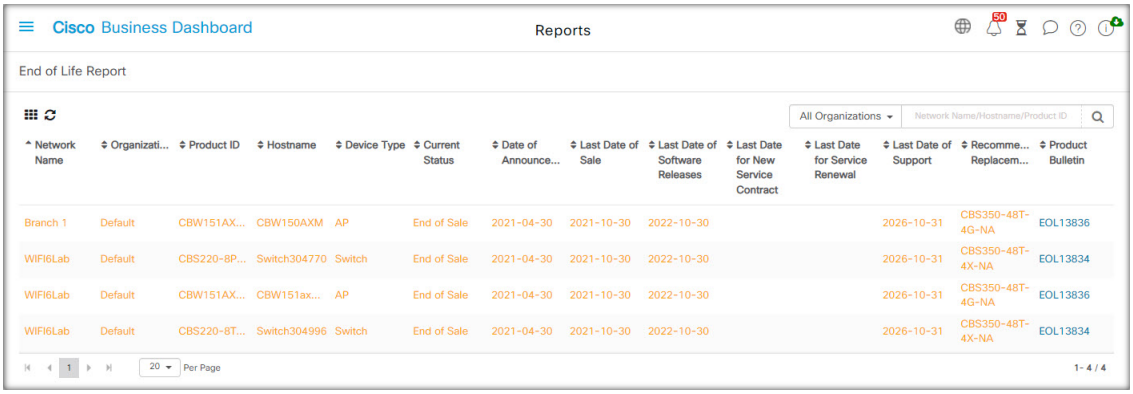
设备表中可能需要注意的行带有颜色编码，以表明紧急性。例如，已发布了生命周期终止公告但尚未到达“支持终止”里程碑的设备将标为橙色；如果思科不再支持该设备，该设备将标为红色。

使用报告顶部的搜索框可过滤结果。在搜索框中输入文本可限制匹配文本中显示的条目数。使用“组织”下拉列表可将结果限制为特定组织范围内。

使用报告顶部的“列选择”图标，可自定义显示的信息。点击此图标，然后使用显示的复选框可选择希望报告中包括的列。

查看生命周期终止报告

生命周期终止报告列示所有已发布**生命周期终止**公告的设备、生命周期终止过程的重要日期，以及建议的更换平台。



报告中提供的信息如下表所示：

字段	说明
网络名称	设备所在网络的名称。
组织	设备所属的组织。
产品 ID	设备的产品 ID 或零部件编号。
主机名	设备的主机名。
设备类型	设备类型。
当前的状态	产品在生命周期终止过程中所处的阶段。
通告日期	生命周期终止公告的发布日期。
销售的最后日期	思科此后不再销售该产品的最终日期。
软件发布的最后日期	此后不再为该产品发布软件版本的最终日期。
新服务合同的最后日期	该设备可以签订新支持合同的最终日期。
服务续约的最后日期	该设备的现有支持合同可以续约的最终日期。
最后支持日期	思科此后不再对该产品提供支持的最终日期。
建议更换	建议的更换产品。
产品资料	产品公告编号和指向思科网站上该公告的链接。

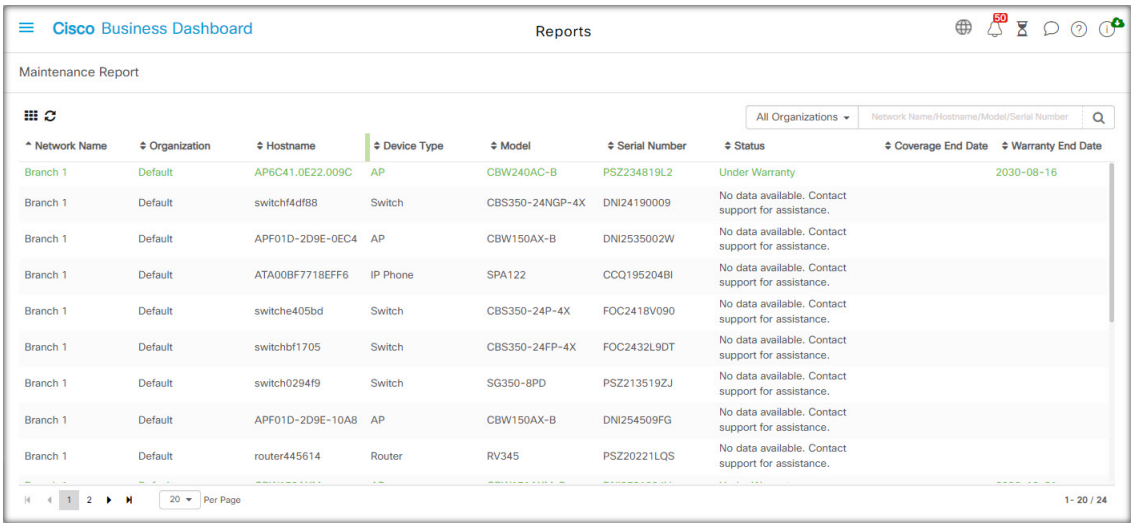
表格的每行都有颜色编码，以表明设备在生命周期终止过程中所处的阶段。例如，已超过“销售的最后日期”但尚未到达“支持的最后日期”的设备将标为橙色，而已超过“支持的最后日期”的设备将标为红色。

使用报告顶部的搜索框可过滤结果。在搜索框中输入文本可限制匹配文本中显示的条目数。使用“组织”下拉列表可将结果限制为特定组织范围内。

使用报告顶部的“列选择”图标，可自定义显示的信息。点击此图标，然后使用显示的复选框可选择希望报告中包括的列。

查看维护报告

维护报告列示所有网络设备，其中包括每个设备的保修信息和支持合同状态信息。



此报告中提供的信息如下表所示。

字段	说明
网络名称	设备所在网络的名称。
组织	设备所属的组织。
主机名	设备的主机名。
设备类型	设备类型。
型号	设备的型号。
序列号	设备的序列号。
状态	设备的当前支持状态。
覆盖结束日期	当前支持合同的到期日期。

字段	说明
保修结束日期	设备保修的到期日期。

表格的每行都有颜色编码，以表明设备的支持状态。例如，接近保修或支持合同到期日期的设备将标为橙色，而超出保修和当前没有支持合同的设备将标为红色。

使用报告顶部的搜索框可过滤结果。在搜索框中输入文本可限制匹配文本中显示的条目数。使用“组织”下拉列表可将结果限制为特定组织范围内。

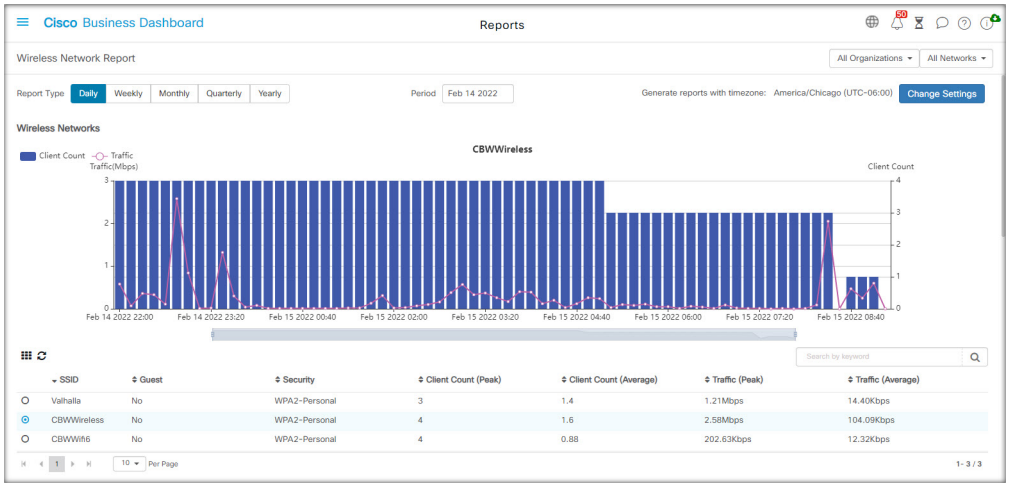
使用报告顶部的“列选择”图标，可自定义显示的信息。点击此图标，然后使用显示的复选框可选择希望报告中包括的列。

查看无线网络报告

无线网络报告显示有关按SSID、无线频谱使用情况和无线接入点细分的无线网络的详细信息，包括被检测到的非法无线接入点列表。可使用页面顶部的控件生成特定时间范围（包括从每天到每年）的报告。

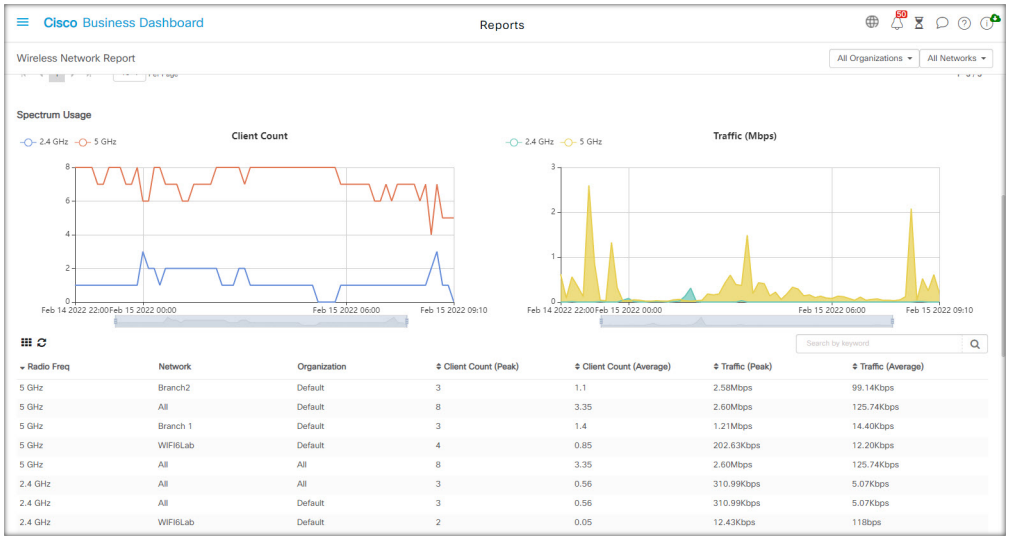
其中几个数据集包括一个图形，用于显示所选行的时间细分信息。您可以点击图形图例中的标签以切换每组数据的显示。

报告中不同部分提供的信息如下表所示。

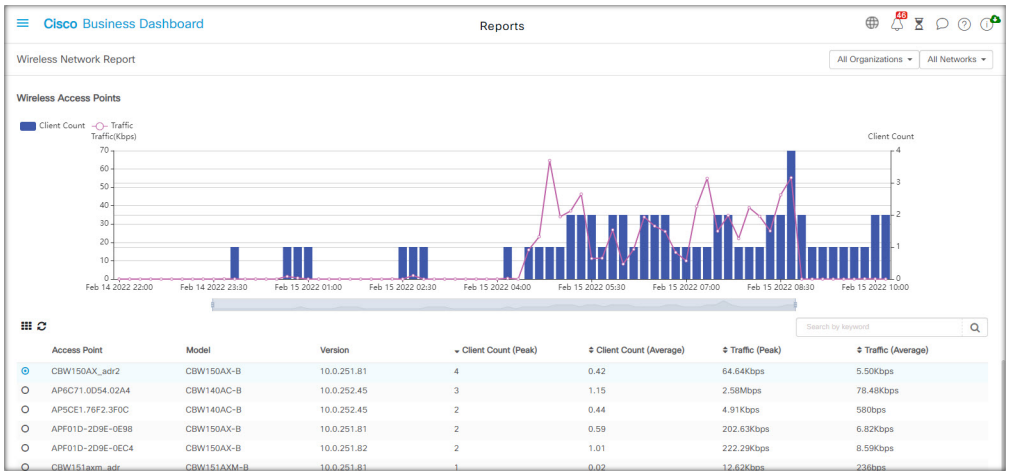


无线网络表	
SSID	无线网络名称。
网络（默认情况下隐藏）	SSID 所在的网络。
组织（默认情况下隐藏）	SSID 所属的组织。
访客	是否为访客访问配置了 SSID。

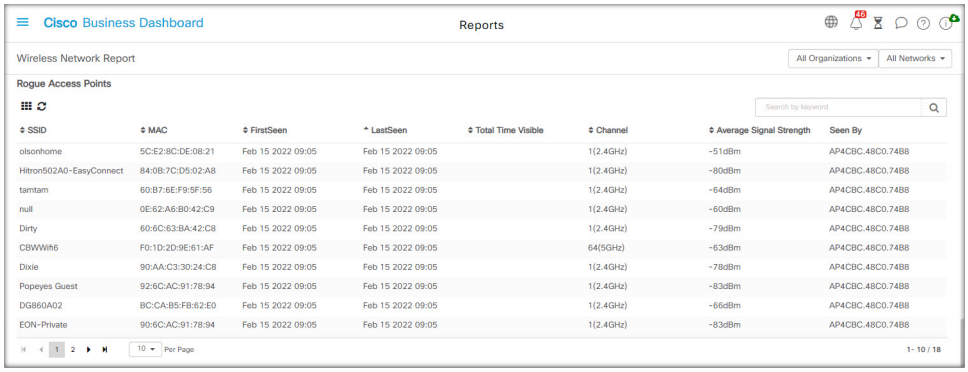
无线网络表	
安全	为 SSID 配置的安全方法。
客户端数（峰值）	报告涉及的时间段内与 SSID 关联的最大客户端数。
客户端数（平均）	报告涉及的时间段内与 SSID 关联的平均客户端数。
流量（峰值）	报告涉及的时间段内经过 SSID 的最大总流量。
流量（平均）	报告涉及的时间段内经过 SSID 的平均总流量。



频谱使用情况表	
无线频率	使用的无线频带 - 2.4GHz 或 5GHz。
网络	应用所显示的频谱使用数据的网络。
组织	应用频谱使用数据的组织。
客户端数（峰值）	报告涉及的时间段内使用频带的最大客户端数。
客户端数（平均）	报告涉及的时间段内使用频带的平均客户端数。
流量（峰值）	报告涉及的时间段内通过频带的最大总流量。
流量（平均）	报告涉及的时间段内通过频带的平均总流量。



无线接入点表	
无线接入点	无线接入点的名称。
网络（默认情况下隐藏）	无线接入点所在的网络。
组织（默认情况下隐藏）	无线接入点所属的组织。
型号	无线接入点的型号。
版本	无线接入点运行的固件版本。
客户端数（峰值）	报告涉及的时间段内与无线接入点关联的最大客户端数。
客户端数（平均）	报告涉及的时间段内与无线接入点关联的平均客户端数。
流量（峰值）	报告涉及的时间段内通过无线接入点的最大总流量。
流量（平均）	报告涉及的时间段内通过无线接入点的平均总流量。



非法无线接入点表	
SSID	检测到的 SSID。

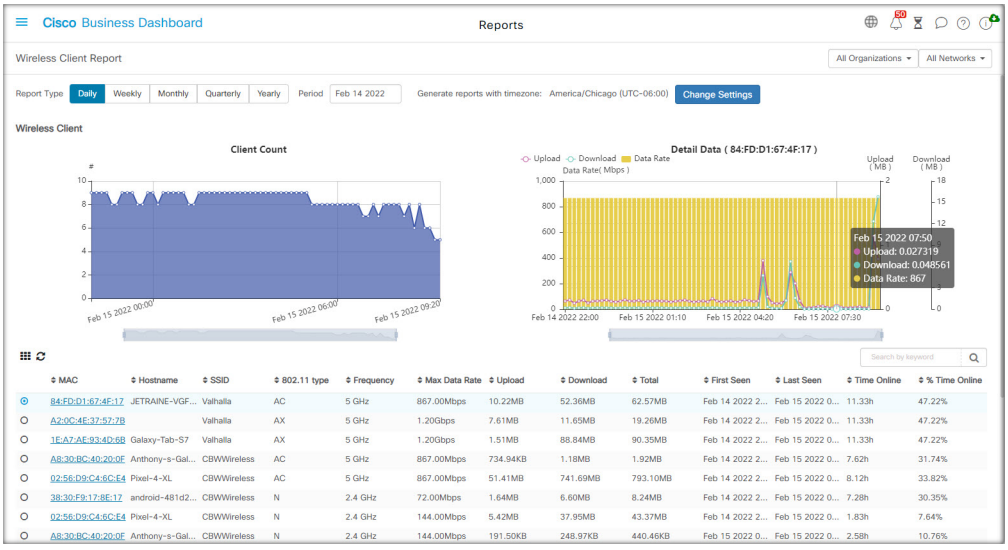
非法无线接入点表	
网络（默认情况下隐藏）	检测无线接入点所在的网络。
组织（默认情况下隐藏）	检测无线接入点所属的组织。
MAC	非法无线接入点的 MAC 地址。
首次显示	首次检测到非法无线接入点的时间。
上次显示	最后一次检测到非法无线接入点的时间。
总可视时间	非法无线接入点在线的总时间。
信道	非法无线接入点使用的无线信道。
平均信号强度	检测无线接入点时观察到的非法无线接入点的平均信号强度。
检测主体	检测到非法无线接入点的无线接入点。

查看无线客户端报告

无线客户端报告显示有关网络中的无线客户端的详细信息。可使用页面顶部的控件生成特定时间范围（包括从每天到每年）的报告。

每个数据集均包括一个图形，用于显示所选行的时间细分信息。您可以点击图形图例中的标签以切换每组数据的显示。

各报告中提供的信息如下表所示。



无线客户端表	
MAC	客户端的 MAC 地址
主机名	客户端的主机名（如果可用）。
组织	最后一次看到客户端的组织。
网络	最后一次看到客户端的网络。
SSID	最后一次与客户端关联的 SSID。
802.11 类型	客户端使用的 802.11 变体。
频率	客户端使用的频带。
最大数据速率	客户端使用的最大数据速率。
上传	客户端上传的数据量。
下载	客户端下载的数据量。
总计	客户端发送和接收的总数据量。
首次显示	首次检测到客户端的时间。
上次显示	最后一次检测到客户端的时间。
在线时间	客户端在线的总时间。
在线时间百分比	客户端在线时间在网络知晓客户端的总时间中所占的百分比。

表 *7:* 无线访客表

无线访客表	
MAC	客户端的 MAC 地址。
主机名	客户端的主机名（如果可用）。
用户名	客户端在访客门户输入的用户名。
组织	最后一次看到客户端的组织。
网络	最后一次看到客户端的网络。
SSID	最后一次与客户端关联的 SSID。
802.11 类型	客户端使用的 802.11 变体。
频率	客户端使用的频带。
最大数据速率	客户端使用的最大数据速率。
上传	客户端上传的数据量。
下载	客户端下载的数据量。
总计	客户端发送和接收的总数据量。
首次显示	首次检测到客户端的时间。
上次显示	最后一次检测到客户端的时间。
在线时间	客户端在线的总时间。
在线时间百分比	客户端在线时间在网络知晓客户端的总时间中所占的百分比。

注释 **第一次看到的时间**和**最后一次看到的时间**是无线接入点报告的时间。建议所有网络设备使用网络时间协议 (NTP) 等机制实现时钟同步。

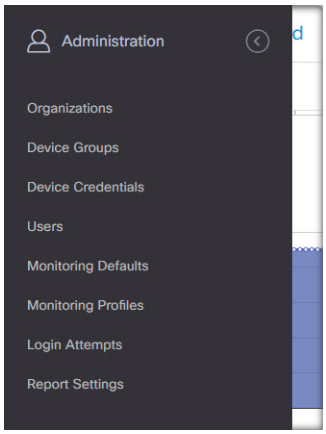
第 11 章

管理

本章包含以下各节：

关于管理

Cisco Business Dashboard 中的**管理**选项可用于在组织级别控制应用的运行。



此选项分为以下几页：

- **组织** - 在 Cisco Business Dashboard 中创建和维护组织。
- **设备组** - 将网络设备分配到组中，以方便管理。

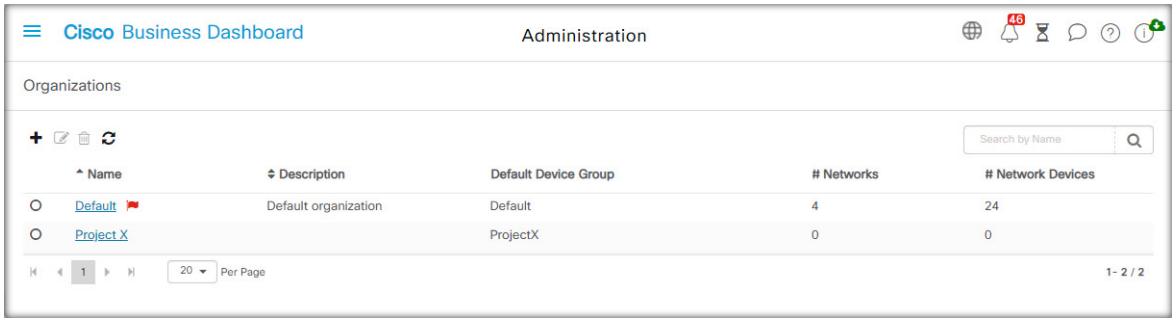
- **设备凭证** - 输入访问网络设备时要使用的凭证。
- **用户** - 定义用户对 Cisco Business Dashboard 的访问权限。
- **通知默认设置** - 更改 Cisco Business Dashboard 的默认通知行为。
- **登录尝试** - 提供所有用户访问 Cisco Business Dashboard 的日志。
- **报告设置** - 更改控制报告生成方式的设置。

并非所有页面对所有角色都可见。操作员无法管理用户设置。**通知默认设置**和**报告设置**仅对管理员可见。

组织

组织在 Cisco Business Dashboard中用于将网络、用户和设备分为若干组，这些组通常单独管理。每个网络或设备都属于一个组织，每个用户可以管理一个或多个组织。组织可代表客户或部门或区域（只要适合您的公司需求），但在任何情况下，使用组织都可以更精细地控制谁可以查看和管理网络的不同部分。默认情况下，在安装 Cisco Business Dashboard 时将只创建一个名为 **Default** 的组织。

创建新组织



1. 导航至**管理** > **组织**。
2. 单击表顶部的 （加号）图标。
3. 为组织指定名称并输入所需的详细信息。
4. 为应该用作新发现设备的默认组的新设备组输入名称。新设备组将与组织一起创建。
5. 指定组织变更窗口的开始时间和持续时间。
6. 点击**保存**。
7. 对要创建的每个组织重复上述步骤。

修改现有组织

1. 导航至**管理** > **组织**。

2. 选择与要修改的组织对应的单选按钮，然后点击**编辑**图标。
3. 进行必要的更改，然后点击**保存**。

删除组织

1. 导航至**管理** > **组织**。
2. 选择与要修改的组织对应的单选按钮，然后点击**删除**图标。

管理组织的监控配置文件

监控配置文件使您能够控制如何在整个组织中执行网络设备监控。在组织级别选择的配置文件将应用于组织中的所有网络。

要更改组织的监控配置文件，请执行以下操作：

1. 导航至**管理** > **组织**。
2. 点击要修改的组织的名称，然后选择**监控配置文件**选项卡。
3. 使用下拉列表选择要应用于对应类型设备的相应监控配置文件。有关创建监控配置文件的详细信息，请参阅 监控配置文件，第 90 页。

   此外，还可以选中单个设备类型或整个组织的继承**监控默认设置**复选框来遵循在系统级别定义的行为。
4. 点击**保存**。

注释 有关可以执行的监控类型及其管理方式的详细信息，请参阅监控配置文件。有关在系统级别更改监控配置文件的详细信息，请参阅 监控默认设置，第 89 页。

管理与组织关联的用户

具有**组织管理员**或更低角色的用户必须显式与组织关联，才能查看或管理该组织中的设备。

要将用户与组织关联，请执行以下步骤。

1. 导航至**管理** > **组织**。
2. 点击要修改的组织的名称，然后选择**用户**选项卡。
3. 单击 （加号）图标。从下拉列表中选择用户。

注释 **管理员**级别用户隐式与所有组织关联，并且不会显示在下拉列表中。

要从组织中删除用户，请执行以下步骤。

1. 导航至**管理** > **组织**。
2. 点击要修改的组织的名称，然后选择**用户**选项卡。
3. 点击表中用户旁边的**删除**图标。

管理与组织关联的网络

Cisco Business Dashboard中的每个网络都属于单个组织。您可以通过选择**组织详细信息**页面上的**网络**选项卡来查看与组织关联的网络列表。

首次创建网络时即已将网络与组织关联。要更改与网络关联的组织，请执行以下步骤。

1. 导航到**网络**并选择要更改的网络。点击**更多**以显示**网络详细信息**面板。
2. 点击网络名称旁边的**编辑**图标。
3. 从下拉列表中选择新组织。
4. 点击**确定**。

您可以在此视图中为组织创建新网络。点击 （加号）图标可创建新网络并在显示的表单中填写相应的值。

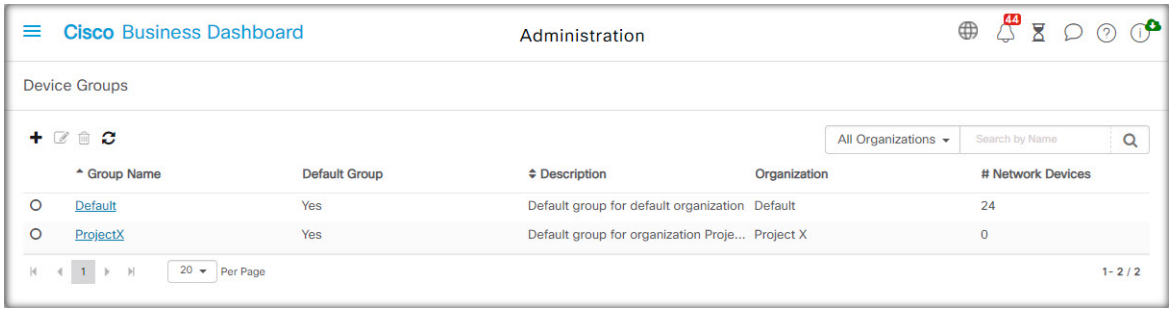
设备组

Cisco Business Dashboard 使用设备组执行大多数配置任务。为了便于在单一操作中配置设备组，可将多个设备组组合在一起，例如仅为设备的子集创建 VLAN 或 WLAN。

每个设备组可包含多种类型的设备，并且将配置应用于设备组时，该配置仅会应用于该组中支持相应功能的设备。例如，如果某个设备组包含无线接入点、交换机和路由器，则新无线 SSID 的配置将只会应用于无线接入点，并且只有路由器为无线路由器时才会应用于它们当中。

设备组可以包括来自多个网络的设备，但所有设备必须属于单个组织。设备组可以指定为组织或网络的默认组，并且该网络或组织的任何新发现设备都将放入默认设备组中。

创建新设备组



1. 导航到**管理** > **设备组**。

2. 单击 （加号）创建新组。
3. 为该组输入组织、名称和说明。点击**保存**。
4. 或者，单击 （加号）图标并使用搜索框选择要添加到组的设备，将设备添加到设备组。您可以逐个添加设备，也可以按网络添加设备。如果所选设备已是另一组的成员，则添加该设备会将其从另一组中删除。每个设备只能是一个组的成员。

修改设备组

1. 导航到**管理** > **设备组**。
2. 选择要更改的组旁边的单选按钮，然后点击**编辑**图标。
3. 如有必要，更改名称和说明。点击**保存**。
4. 根据需要在该组中添加和删除设备。要删除之前添加到该组中的某个设备，请点击该设备旁边的**垃圾桶**图标。该设备将被移到网络或组织的**默认**组中。

注释 无法删除**默认**组中的设备。要从**默认**组中删除设备，必须将其添加到新组中。

删除设备组

1. 导航到**管理** > **设备组**。
2. 点击与要删除的设备组对应的单选按钮，然后点击**删除**图标。

注释 无法删除**默认**组。

设备凭证

Cisco Business Dashboard要完全发现和管理网络，就必须具有对网络设备执行身份验证的凭证。当Probe首次发现设备时，它将尝试使用默认凭证对设备执行身份验证，凭证中的用户名为：`cisco`，密码为：`cisco`，SNMP社区为：`public`。如果尝试失败，系统将生成一条通知，且必须由用户提供有效的凭证。要提供有效的凭证，请执行以下步骤。

1. 导航到**管理** > **设备凭证**。此页上的第一个表列出 Probe 发现的所有需要凭证的设备。
2. 在任意或所有**用户名/密码**字段、**SNMP 社区**字段和 **SNMPv3** 凭证字段中输入有效的凭证。单击相应字段旁边的 （加号）图标，可为每种凭证类型输入多达三个凭证。确保使用纯文本输入密码。

注释 对于 **SNMPv3** 凭证，支持的身份验证协议有“无”、“MD5”和“SHA”，支持的加密协议有“无”、“DES”和“AES”

3. 点击**应用**。Probe 将为需要该类凭证的每个设备测试每个凭证。如果凭证有效，系统将存储该凭证以便日后用于该设备。
4. 根据需要重复步骤 2 至 3，直到每个设备均存储了有效的凭证。

要为特定设备输入单个凭证，请执行以下步骤。

1. 点击发现的设备表中针对设备显示的**编辑**按钮。这时将显示一个弹出窗口，提示您输入与所选凭证类型对应的凭证。
2. 在提供的字段中输入用户名和密码或 SNMP 凭证。
3. 点击**应用**。要关闭窗口而不应用，请点击弹出窗口右上角的 。

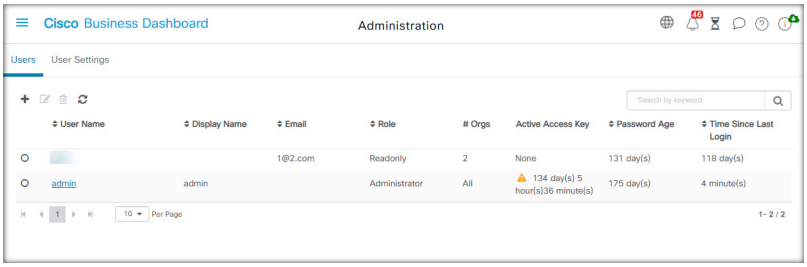
添加新凭证部分下方是一个表，表中显示 Probe 为之存储了有效凭证的各个设备的身份以及凭证的最后使用时间。要显示为设备存储的凭证，可点击设备旁边的**显示密码**图标。要重新隐藏凭证，可点击**隐藏密码**图标。您还可以使用表顶部的按钮显示和隐藏所有设备的凭证。另外，您还可以删除不再需要的凭证。要删除存储的凭证，请执行以下步骤。

1. 导航到**管理** > **设备凭证**。
2. 在**已保存的凭证**表中，选中要删除的一组或多组凭证的相应复选框。您也可以选中表顶部的复选框，选择所有凭证。
3. 点击**删除所选凭证**。

要删除单个设备的凭证，还可以点击设备旁边的**删除**图标。

用户

通过**用户管理**页面，您可以控制授予用户对 Cisco Business Dashboard 的访问权限的方式，更改影响这些用户与 Dashboard 交互方式的设置，并控制在执行基于用户的网络身份验证时是否也应允许这些用户访问网络。当您需要添加新用户或从网络中删除新用户时，此工具非常有用。



Cisco Business Dashboard 包含控制使用“Dashboard 访问”下拉列表提供的 Dashboard 功能的设置，以及当进行基于用户的网络访问时，用户是否可以访问网络（“网络访问”复选框）的设置。这些设置的可用选项包括：

- **管理员** - 管理员对 Dashboard 功能具有完全访问权限，包括能够维护系统。
- **组织管理员** - 组织管理员仅限于管理一个或多个组织，但不能对系统进行更改。
- **操作员** - 操作员拥有与组织管理员类似的权限，但不能管理用户。
- **只读** - 只读用户仅可查看网络信息，不能进行任何更改。
- **无访问权限** - 无访问权限用户无法使用任何 Dashboard 功能，但可以登录 Dashboard 来管理其用户配置文件。
- **网络访问** - 此设置控制在使用基于用户的网络访问时用户是否可以访问网络。如果 Dashboard 访问设置设为“组织管理员”或以下级别，则仅允许用户的组织列表中的组织进行访问。

Cisco Business Dashboard 使用户能够根据本地用户数据库进行身份验证。从版本 2.2.1 开始，还可以使用户能够根据 Microsoft Azure Active Directory 实例进行身份验证。

注释 对基于用户的网络访问执行身份验证时，仅检查本地用户。

首次安装 Cisco Business Dashboard 时，系统将在本地用户数据库中创建默认的**管理员**，其用户名和密码均设置为 `cisco`。

注释 用户设置只能由**管理员**和**组织管理员**管理。

将新用户添加到本地用户数据库

1. 导航到**管理** > **用户**并选择**用户**选项卡。
2. 单击 （加号）图标创建新用户。
3. 在提供的字段中，输入用户名、显示名称、邮箱地址和密码，并指定 Dashboard 访问和网络访问设置。您还可以为用户提供联系人详细信息。
4. 点击**保存**。

如果用户不是**管理员**，则必须将用户添加到一个或多个组织。为此，请选择**组织**选项卡，然后单击（加号）图标。从下拉列表中选择所需组织。

修改用户

1. 导航到**管理** > **用户**并选择**用户**选项卡。
2. 选择需要更改的用户旁边的单选按钮，然后点击**编辑**图标。

3. 根据需要进行修改。
4. 点击**保存**。

要将用户添加到新组织，请选择**组织**选项卡，然后单击 （加号）图标。从下拉列表中选择所需组织。要将其从组织中删除，请点击表中的组织旁边的**删除**图标。

删除用户

1. 导航到**管理** > **用户**并选择**用户**选项卡。
2. 选择需要删除的用户旁边的单选按钮，然后点击表顶部的**删除**。

更改密码复杂性

要启用或更改密码复杂性要求，请执行以下步骤。

1. 导航到**管理** > **用户**并选择**用户设置**选项卡。
2. 选择**身份验证源**下的**本地**选项卡，根据需要修改**用户密码复杂性**设置，然后点击**保存**。

注释 根据 Azure Active Directory 实例进行身份验证时，在 Active Directory 中管理密码复杂性。

启用 Azure Active Directory 身份验证

Cisco Business Dashboard 支持使用 Microsoft Azure Active Directory 实例进行用户身份验证。根据用户所属的 Active Directory 组，为 Active Directory 用户分配角色和组织列表。

要启用 Azure Active Directory 作为身份验证源，请执行以下步骤。

1. 在 **Azure Active Directory** 中，为 Cisco Business Dashboard 创建新的应用注册，从 **Microsoft Graph API** 为其分配 User.Read 和 Domain.Read.All 的授权权限，然后创建**客户端密钥**。记录应用（客户端）ID、客户端密钥和目录（租户）ID。
2. 打开 Cisco Business Dashboard Web GUI，然后导航到**管理** > **用户**。选择**用户设置**选项卡，然后选择**身份验证源**下的 **Azure AD** 选项卡。
3. 点击**启用**复选框。
4. 在提供的字段中输入在步骤 1 中收集的**客户端 ID**、**客户端密钥**和**租户 ID**。
5. 或者，指定应允许访问 Dashboard 的域的列表（以逗号分隔）。点击**保存**。
6. 点击**用户组映射**标题下的 （加号）图标，创建新的组映射。在提供的字段中输入 Active Directory 组的**对象 ID**，然后选择要应用于此组中用户的角色和组织列表。对需要映射的所有组重复此步骤。

   如果用户与多个组匹配，则会使用第一个匹配项的角色和组织映射。

7. 记录**启用**复选框下方显示的**重定向 URL**。返回到 Azure Active Directory 并将 URL 添加到应用注册的重定向 URI 列表。

注释 应能够通过访问 Dashboard 的用户的 Web 浏览器访问重定向 URL 中显示的主机和端口。如果无法访问当前显示值，请更新**系统变量**选项卡上的相应字段，该选项卡位于**系统** > **平台设置**页面。

管理本地身份验证

默认情况下，对本地用户数据库启用身份验证。要禁用本地身份验证，请执行以下步骤。

1. 确保已按照上述要求设置根据 Azure Active Directory 进行身份验证。使用通过 Active Directory 进行身份验证的“管理员”账户登录 Dashboard。
2. 导航到**管理** > **用户**并选择**用户设置**选项卡。在**身份验证源**下，选择**本地**选项卡。
3. 取消选中**启用**复选框，然后点击**保存**。

要再次启用本地身份验证，请执行以下步骤。

1. 导航到**管理** > **用户**并选择**用户设置**选项卡。在**身份验证源**下，选择**本地**选项卡。
2. 选中**启用**复选框，然后点击**保存**。

在丢失“所有管理访问权限”后恢复访问

如果丢失对 Cisco Business Dashboard 应用的管理访问权限，请执行以下步骤恢复该访问权限。

1. 使用 SSH 或通过控制台登录主机操作系统。
2. 输入命令 **cisco-business-dashboard recoverpassword**

输入命令后，系统将启用本地用户身份验证，并恢复用户名为 **cisco** 且密码为 **cisco** 的默认管理员。

更改会话超时

要更改用户会话的空闲超时和绝对超时，请执行以下步骤。

1. 导航到**管理** > **用户**并选择**用户设置**选项卡。
2. 根据需要，修改**用户会话**参数，然后点击**保存**。将鼠标悬停在帮助图标上，查看这些参数的允许范围。

监控默认设置

监控配置文件使您能够控制在网络中执行的设备监控。监控配置文件可以在组织级别或系统级别应用。对于选择继承系统级别监控配置文件的组织，其行为将由**监控默认设置**页面控制。

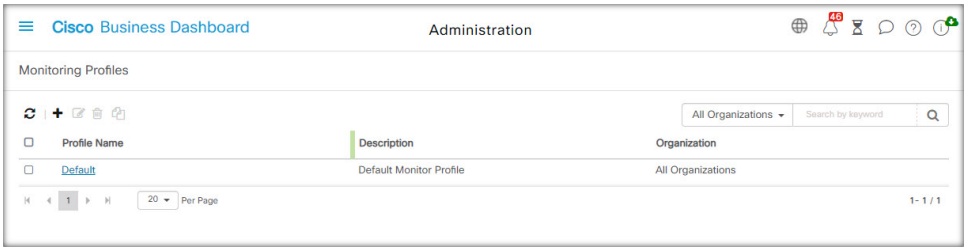
要更改在整个系统中应用的**监控配置文件**，请执行以下步骤。

1. 导航到**管理** > **监控默认设置**。
2. 使用下拉列表选择要应用于对应类型设备的相应监控配置文件。有关创建监控配置文件的详细信息，请参阅“管理监控配置文件”。
3. 点击**保存**。

有关可以执行的监控类型及其配置方式的详细信息，请参阅监控配置文件。有关在组织级别更改监控设置的详细信息，请参阅 组织，第 82 页。

监控配置文件

监控配置文件控制从设备收集的数据和生成的通知。



配置文件可应用于组织内或整个系统的不同类型的设备。例如，某些设备可能需要不同的监控要求，具体取决于其位置或安全要求。在配置文件中，支持两种类型的监控器 - **通知监控器**和**报告监控器**。

通知监控器通常会由于设备状态更改或参数超出阈值而生成通知和警报。通知具有不同级别的严重性（信息、警告和警报），并且可以通过以下渠道传送：

- Web UI 的弹出通知。
- 邮件。这需要正确配置邮件设置。有关更多详细信息，请参阅管理邮件设置，第 104 页。
- 服务中心通知单。这需要与提供服务中心服务的应用集成。有关更多详细信息，请参阅管理集成设置，第 116 页。
- 协作消息。这需要与协作应用集成。有关更多详细信息，请参阅管理集成设置，第 116 页。

注释 思科建议您配置监控配置文件，以确保不超过每小时 60 条通知单和/或协作消息的平均速率。在与外部应用通信时，超过此速率的持续速率可能会导致 API 拥塞和事件丢失。

此外，活动通知在**通知中心**可见，并显示在设备信息视图中。通知中的更改也会记录在**事件日志**中。

报告监控器在监控控制面板中收集用于无线报告和流量图的数据。

可以创建多个监控配置文件，并且可以在系统级别或按组织将不同的配置文件分配给不同的设备类型。有关将监控配置文件分配给设备的更多信息，请参阅组织，第 82 页和监控默认设置，第 89 页。

添加新监控配置文件

1. 导航到**管理** > **监控配置文件**。
2. 点击 **+**（加号）图标以创建新配置文件
3. 指定配置文件的名称以及要与配置文件关联的组织。此外，还可以在此处指定“所有组织”，从而使配置文能够件与任何组织一起使用或用作系统级默认值。
4. 另外，还可以提供配置文件说明和用于接收通知的邮件地址的列表（以逗号分隔）。
5. 点击**保存**
6. 屏幕更新，以显示不同的通知和报告监控器。可以使用提供的控件启用和禁用单个监控器。
7. 通知监控器具有其他设置，可以通过点击监控器的**编辑**图标进行修改。设置因显示器而异，但包括应生成的通知类型、通知的严重性和应触发通知的阈值。

复制现有监控配置文件

要复制现有监控配置文件，请执行以下步骤。

1. 导航至**管理** > **监控配置文件**。
2. 选中要复制的配置文件旁边的复选框，然后点击**另存为**图标。
3. 根据需要更新配置文件名称、说明、组织和邮件地址，然后点击**保存**。
4. 根据需要对通知和报告监控器进行更改。可以通过点击**重置为默认值**按钮将显示器设置恢复为默认值。

修改监控配置文件

要修改现有监控配置文件，请执行以下步骤。

1. 导航至**管理** > **监控配置文件**
2. 选中要复制的配置文件旁边的复选框，然后点击**编辑**图标。
3. 根据需要更新配置文件设置和邮件地址，然后点击**保存**。
4. 根据需要对通知和报告监控器进行更改。可以通过点击**重置为默认值**按钮将显示器设置恢复为默认值。

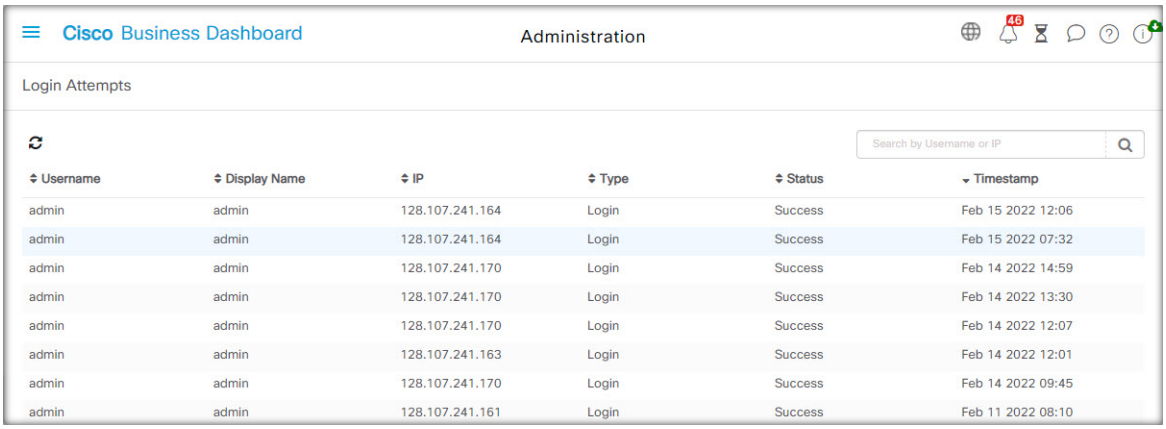
删除监控配置文件

1. 导航至**管理** > **监控配置文件**。
2. 选中要复制的配置文件旁边的复选框，然后点击**删除**图标。

注释 如果配置文件用作组织级监控配置文件，将更新相应的组织和设备类型以继承系统级配置。无法删除用作系统级监控配置文件的配置文件。删除配置文件之前，请从**管理 > 监控默认设置**页面中删除该配置文件。

查看登录尝试

Cisco Business Dashboard记录每次做出的登录和退出系统的尝试，无论尝试是成功还是失败。



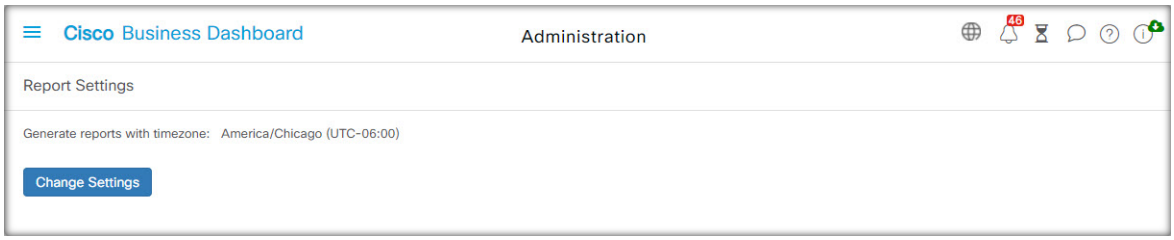
要查看这些日志，请导航到**管理 > 登录尝试**。该表将显示以下信息：

字段	说明
用户名	与事件关联的用户名。
显示名称	用户的显示名称。
IP	用户登录时所用设备的 IP 地址。
类型	事件的类型包括： • 登录 • 注销
状态	指示尝试是成功还是失败。
时间戳	事件发生的日期和时间。

您可以使用表上方的搜索框使表格仅显示与特定用户或 IP 地址匹配的条目。

管理报告设置

使用**报告设置**页面可设置生成报告的时区。



报告期间的开始和结束时间将为所设置时区的本地时间。

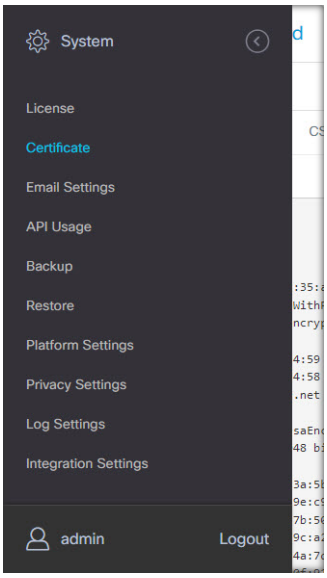
第 12 章

系统

本章包含以下各节：

关于系统

Cisco Business Dashboard 中的“系统”选项可用于管理平台的运行。



该部分分为以下几个页面：

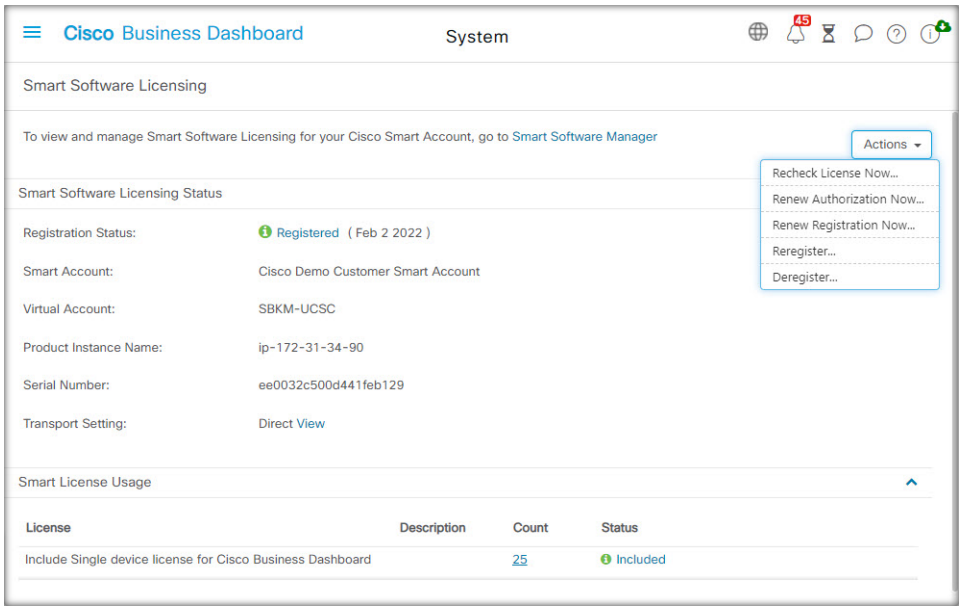
页面名称	页面功能
许可	管理 Dashboard 的软件许可。
证书	管理 Dashboard 的安全证书。
邮件设置	设置邮件并管理设置。
API 使用情况	监控 Cisco Business Dashboard API 的使用。
备份	备份 Dashboard 的配置和其他数据。
恢复	恢复 Dashboard 的配置和其他数据。
平台设置	管理 Dashboard 的网络配置。
隐私设置	控制可与思科共享的数据。
日志设置	更改 Dashboard 的日志设置。
本地 Probe	管理 Dashboard 上托管的 Probe。
集成设置	管理 Cisco Business Dashboard 与外部应用的集成。

注释 这些页面仅对**管理员**可用。

管理许可证

注释 在适用于 AWS 的 Cisco Business Dashboard计量版本中无此页面。

通过**许可证**页面，您可以查看网络所需的许可证数量和类型，并将 **Dashboard** 连接到思科智能许可系统。如果您的设备未超过 25 台，则无需额外许可。此页面上有两个信息面板。



- **智能软件许可状态**

  此面板显示智能许可证客户端的注册状态以及有关正在使用的智能账户的信息。

- **智能许可证使用**

  此面板列示当前网络状态下所需的许可证数量和类型。该信息将随着网络的变化自动更新，Dashboard将会更新智能账户请求的许可证数量。“状态”字段会显示是否已成功获取所需的许可证数量。

此页面还包含可让您通过智能账户注册和取消注册 Dashboard 的控件。

如果Dashboard无法获取足够的许可证来管理网络，则Dashboard将在评估模式下运行并且其用户界面的标题中将会显示消息。在评估模式下运行时，您有 90 天的时间纠正这种情况。如果问题未在 90 天内得到解决，则 Dashboard 的某些功能将会受到限制，直至通过获取更多许可证或减少管理的设备数量将其解决。

向智能账户注册 Dashboard

要向智能账户注册 Dashboard，请执行以下步骤：

1. 访问 *https://software.cisco.com*，登录您的智能账户。

   选择位于“许可证”部分下面的**智能软件许可**链接。

2. 选择**资产**页面，如有必要，更改所选的默认虚拟账户。
3. 点击**常规**选项卡。
4. 点击**新建令牌...**按钮新建**产品实例注册令牌**。可以选择添加描述，并更改**到期时间**时间设置。
5. 单击**创建令牌**。
6. 从位于令牌右侧的**操作**下拉列表中选择**复制**，将新建的令牌复制到剪切板。
7. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
8. 点击**注册**按钮，将令牌粘贴到提供的字段中。
9. 单击**确定**。

Dashboard将注册到思科智能许可系统中，并针对管理的网络设备数量请求足够的许可证。如果可用的许可证数量不足，用户界面上将会显示消息，您将有90天的时间获取足够的许可证，否则系统功能将受到限制。

从智能账户中删除 Dashboard

要从智能账户中删除 Dashboard，并将分配的任何许可证退回许可证池中，请执行以下步骤：

1. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
2. 从位于右上角的下拉列表中选择**取消注册...**。在弹出窗口中点击**取消注册**进行确认。

立即检查许可证

Cisco Business Dashboard 每日都会进行检查，以确保一直有足够的许可证供网络使用，如果所需的许可证数量减少，将会立即更新。但如果所需的许可证数量增加，或者如果从池中添加/删除许可证，Dashboard 可能需要一天时间才会更新。要使 Dashboard 立即更新许可证分配，请执行以下步骤。

1. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
2. 从位于右上角的下拉列表中选择**立即重新检查许可证…**。Cisco Business Dashboard将立即查询思科智能许可，以确保有足够的许可证供 Dashboard 执行操作。

立即续约授权

通过“立即重新注册”操作，Dashboard可以更新用来验证与思科智能许可系统通信的证书。通常，只有当思科支持部门纠正扩展通信中断时才需要执行此操作。要重新注册，请执行以下步骤。

1. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
2. 从位于右上角的下拉列表中选择**立即更新授权...**。

立即重新注册

通过“立即重新注册”操作，Dashboard可以更新用来验证与思科智能许可系统通信的证书。通常，只有当思科支持部门纠正扩展通信中断时才需要执行此操作。要重新注册，请执行以下步骤。

1. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
2. 从位于右上角的下拉列表中选择**立即重新注册...**。

将 Dashboard 转到其他账户

通过重新注册Dashboard，可以将其从一个虚拟账户移动到另一个。要在各个账户之间移动Dashboard，请执行以下步骤。

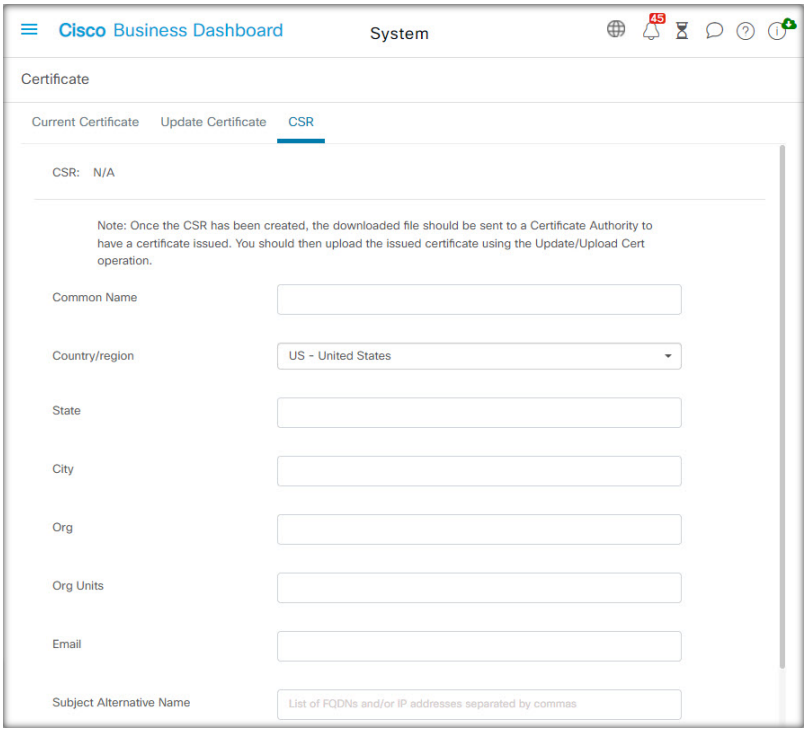
1. 导航到 Cisco Business Dashboard用户界面并选择**系统** > **许可证**。
2. 从位于右上角的下拉列表中选择**重新注册...**。
3. 在提供的框中输入新的注册令牌。如果Dashboard当前已注册到另一账户，请确保选中**如果已注册，请注册此产品实例**复选框，然后点击**确定**。

管理证书

在安装过程中，Cisco Business Dashboard 会生成自签名证书，以保护 Web 以及与服务器的其他通信。您可以选择由受信任的证书颁发机构(CA)签发的证书替换此证书。为此，您需要生成证书签名请求 (CSR) 以便 CA 进行签名。

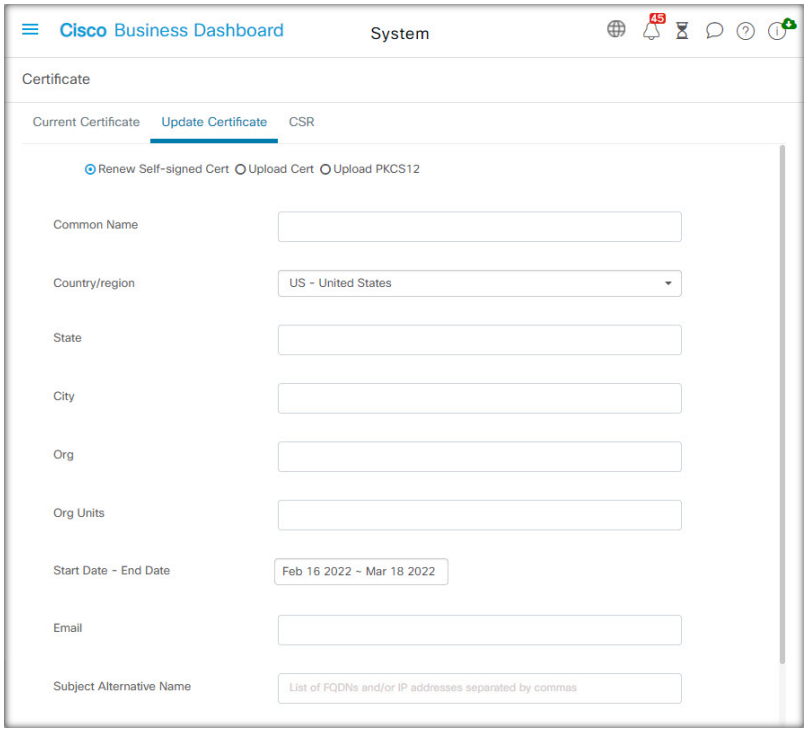
您也可以选择生成证书以及完全独立于 Dashboard 的对应私钥。如果是这样的话，可以先将证书和私钥合并到 PKCS#12 格式文件中，然后再上传。

生成证书签名请求 (CSR)



1. 导航到**系统** > **证书**并选择 **CSR** 选项卡。
2. 在显示的表格提供的字段中输入适当的值。这些值用于构建CSR，将包含在您从CA收到的签名证书中。
3. 点击**创建**，CSR 将自动下载到您的 PC 中。或者，您也可以在日后某个日期点击 CSR 标签旁边的**下载**以下载 CSR。
4. 如有必要，您可以返回步骤 2 修改 CSR。

上传新证书



要使用管理 GUI 上传新证书，请执行以下步骤。

1. 导航到**系统** > **证书**，选择**更新证书**选项卡。
2. 选择**上传证书**单选按钮。可将含有证书的文件拖放到目标区域，也可以点击目标区域，浏览文件系统。文件应为 PEM 格式。

   您也可以选择**上传 PKCS12** 选项，上传带有关联私钥的 PKCS#12 格式的证书。应在提供的字段中指定用来解锁文件的密码。
3. 点击**上传**上传文件并替换当前证书。

要使用命令行上传新证书，请执行以下操作：

1. 使用 SCP 或类似工具将证书和私钥文件复制到 Cisco Business Dashboard 文件系统。私钥是敏感信息，因此确保仅授权人员才能访问这些文件。
2. 使用控制台或 SSH 登录操作系统。
3. 使用命令 **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>** 将证书应用于 Dashboard 应用。证书和私钥将加载到 Dashboard 应用中并替换当前证书。有关此命令及其选项的详细信息，请输入 **cisco-business-dashboard importcert -h**。

注释 对于由知名证书颁发机构签名的证书，某些浏览器会生成证书警告，而有些浏览器则会接受此类证书而不发出任何警告。Network Plug and Play 客户端也可能不接受此类证书。这是因为证书颁发机构给证书签名时使用的中间证书未包含在浏览器或 PnP 客户端的受信任颁发机构存储区中。在这种情况下，证书颁发机构应提供一个证书捆绑包，这些证书在上传到 Dashboard 之前必须与服务器证书连接。服务器证书必须出现在所连接捆绑包中的第一个位置。

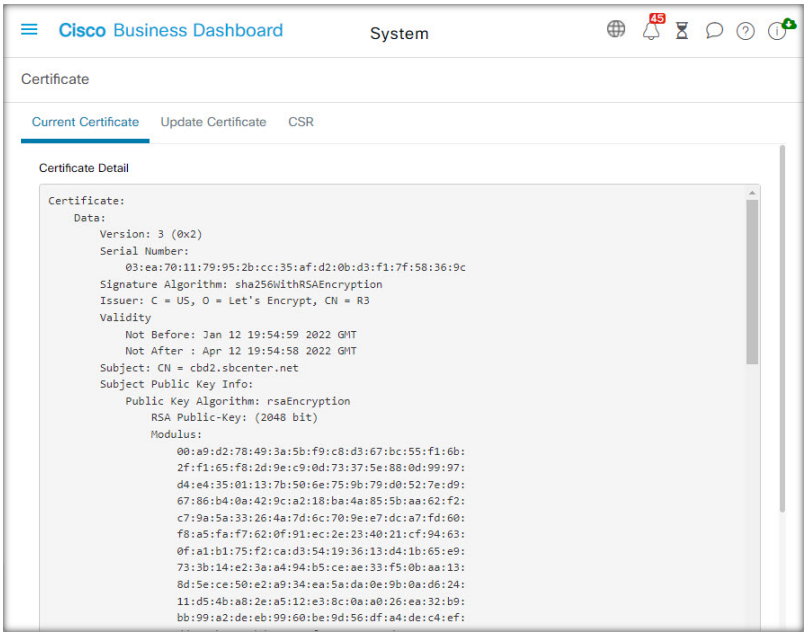
重新生成自签名证书

要重新生成自签名证书，请执行以下步骤。

1. 导航到**系统** > **证书**，选择**更新证书**选项卡。
2. 点击**更新自签名证书**。在显示的表格提供的字段中输入适当的值。这些值将用于构建证书。
3. 点击**保存**。

查看当前证书

要查看当前证书，请执行以下步骤。



1. 导航到**系统** > **证书**，选择**当前证书**选项卡。
2. 您的浏览器中将显示纯文本格式的证书。

下载当前证书

要下载当前证书的副本，请执行以下步骤。

1. 导航到**系统** > **证书**，选择**当前证书**选项卡。
2. 点击页面底部的**下载**。您的浏览器将以 PEM 格式下载该证书。

自动安装加密证书

从版本 2.2.1 开始，Cisco Business Dashboard 可以自动从 **Let's Encrypt 证书颁发机构** (https://letsencrypt.org) 获取并更新域验证证书。在版本 2.5.0 中，可以通过“管理”页面管理这些证书。

重要事项 您必须注册一个完全限定域名，并拥有指向公共 IP 地址的 DNS 记录。有关详细信息，请参阅管理平台设置，第 108 页。

要使用管理 GUI 安装 Let’s Encrypt 证书，请执行以下操作：

1. 导航到**系统** > **证书**，选择“更新证书”选项卡。
2. 选择 *Let’s Encrypt* 证书单选按钮。
3. 选中此复选框以启用 Let’s Encrypt 证书。
4. 在提供的字段中输入一个或多个完全限定域名。这些域名必须在域名系统 (DNS) 中定义，并解析为 Cisco Business Dashboard 服务器的地址。
5. 提供用于紧急续约和安全通知的邮箱地址。
6. 使用提供的链接查看《Let’s Encrypt 用户协议》，然后选中复选框以接受该协议。
7. 或者，选中复选框以与电子前线基金会 (https://www.eff.org) 共享邮箱地址。
8. 点击“获取证书”按钮。

Dashboard 将联系 Let's Encrypt 证书颁发机构，并使用 HTTP 验证方法获取证书。该页面将更新，以显示证书的详细信息以及到期日期。证书将在到期前约 30 天自动续约。

如果您需要随时更新证书，请执行以下步骤：

1. 导航到**系统** > **证书**，选择**更新证书**选项卡。
2. 选择 **Let’s Encrypt 证书**单选按钮。
3. 使用提供的复选框和字段更新要应用于证书的名称。

   或者，您可以在屏幕底部更新联系详细信息。
4. 点击“获取证书”按钮。

您还可以在正常续约时间之前强制重新生成证书，方法是保持页面上的字段不变，然后点击“强制续约”按钮。

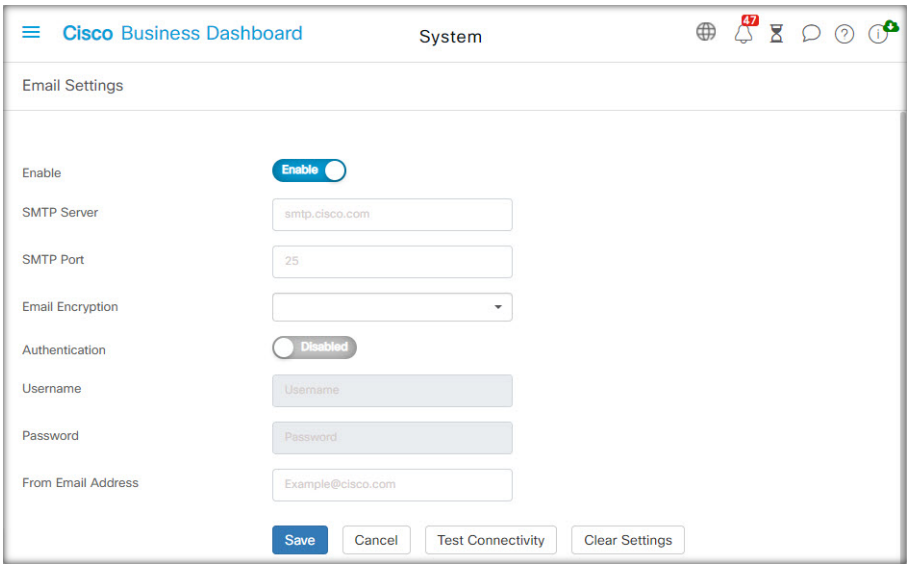
要使用命令行安装 Let’s Encrypt 证书，请执行以下操作：

1. 使用 SSH 或通过控制台登录主机操作系统。
2. 执行 **cisco-business-dashboard letsencrypt** 命令，并使用 **-d** 选项指定一个或多个完全限定的主机名。（例如，**cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**。）命令中列出的所有名称都必须解析为 Dashboard 服务器的 IP 地址。
3. 按照提示颁发证书并将其应用于 Dashboard 应用。Dashboard 会自动更新即将到期的证书。

注释 **加密**服务需要连接到 Dashboard Web 服务器，以验证主机名的所有权。要允许此操作，必须可从互联网访问 Dashboard Web 服务器。有关如何确保只有授权 IP 地址才能访问 Dashboard 应用的详细信息，请参阅管理平台设置，第 108 页。

管理邮件设置

通过**邮件设置**页面，您可以控制 Cisco Business Dashboard 如何发送邮件。



访问此页面可设置以下参数。

字段	说明
SMTP 服务器	要使用的 SMTP 服务器的域名或 IP 地址。
SMTP 端口	用于发送邮件的 TCP 端口。

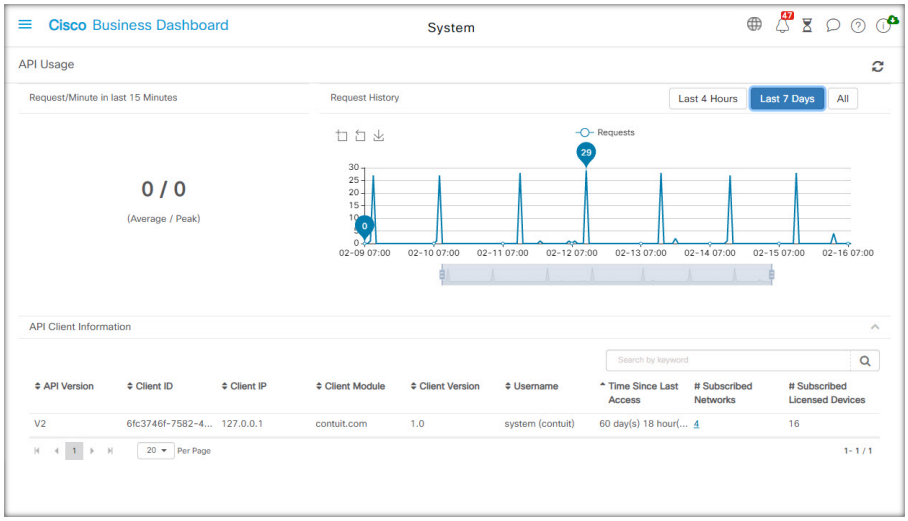
字段	说明
电子邮件加密	要使用的加密方法，包括以下类型： • 无 • TLS • SSL
身份验证	启用或禁用邮件身份验证。
用户名	如果启用了身份验证，要提供的用户名。
密码	如果启用了身份验证，要提供的密码。
发件人电邮地址	始发邮件的邮件地址。

要测试配置，请点击**测试连接**。这将提示目标邮件地址，并生成发送到指定地址的测试邮件。

查看 API 使用情况

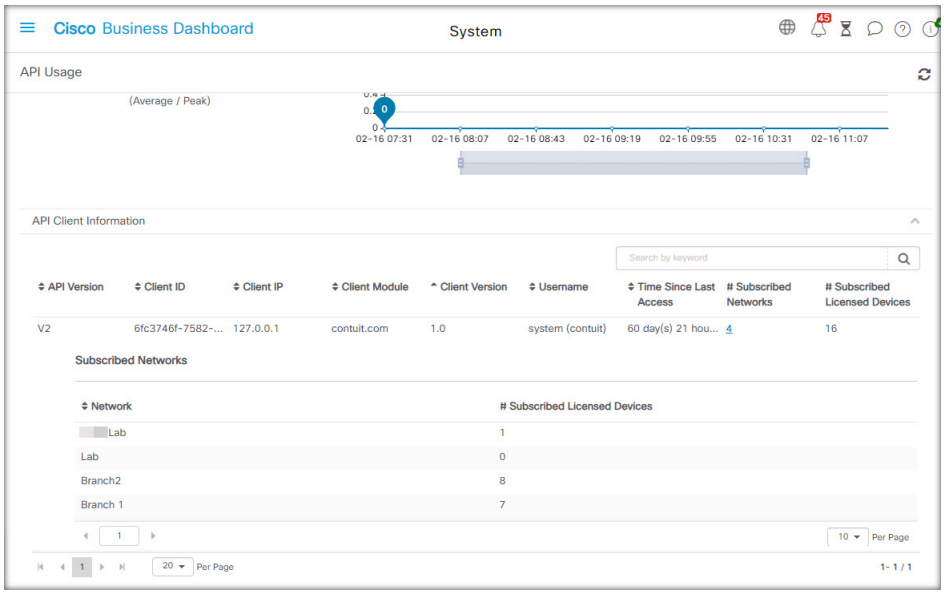
“API 使用情况”页面显示有关已与 Cisco Business Dashboard 集成的任何外部应用的信息。本报告分为以下三个部分：

- **15 分钟请求监视器** - 显示最近 15 分钟内的平均请求率和峰值请求速率
- **请求历史记录**图 - 显示一段时间内的请求活动图。您可以选择最近四小时或最近七天的时间段，或选择显示所有可用信息。然后，您可以使用图下面的滑块将图的焦点缩小到您关注的特定时间段。
- **API 客户端信息**表 - 列出至少使用了一次 API 的所有客户端。下表介绍 **API 客户端信息**表中提供的信息：



字段	说明
API 版本	客户端在访问 API 时使用的版本。
客户 ID	客户端应用的特定实例的标识符。
客户端 IP	与此客户端关联的 IP 地址。此外还显示回调 URL，当 API 版本为 v1 且已请求通知时，Dashboard 应该向此 URL 发布事件通知。
客户端模块	与此客户端关联的应用类型。
客户端版本	与此客户端关联的应用的版本。
用户名	对于使用 v1 API 的客户端，此字段显示应用在向 Dashboard 进行身份验证时提供的用户名。对于使用 v2 API 的客户端，此字段显示客户端使用**的访问密钥 ID** 和与密钥关联的用户名。
上次访问后已过时间	自此客户端的最后一个活动以来经过的时间。
已订用网络的数量	其中应用已请求事件通知的网络数。此数字是一个链接，点击该链接将显示此客户端的“订用网络”表。“订用网络”表如下所述。
已订用许可设备的数量	系统将为其向此客户端发送事件通知的托管设备数。

要查看有关客户端已请求通知的网络的信息，请点击 **API 客户端信息**表中的客户端**订用网络数**链接。系统将针对该客户端显示**订用网络**表，其中包含客户端已请求通知的网络列表。下表介绍**订用网络**表中提供的信息：



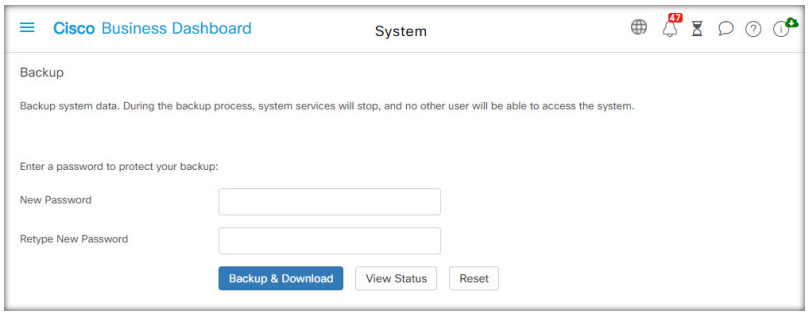
字段	说明
网络	客户端监控的网络的名称。
已订用许可设备的数量	在该网络中系统将为其发送事件通知的托管设备数

备份和恢复 Dashboard 配置

Cisco Business Dashboard 使用的配置和其他数据可进行备份，以用于灾难恢复目的，或将 Dashboard 轻松迁移到新的主机。为保护敏感数据，备份使用密码加密。

Cisco Business Dashboard 备份文件可以恢复到与备份系统运行相同版本的系统，也可以恢复到最多一个更新的次要版本。例如，从运行版本 2.2.0 的系统获取的备份可以恢复到运行 2.3.1 的系统，但不能恢复到运行 2.4.0 的系统。

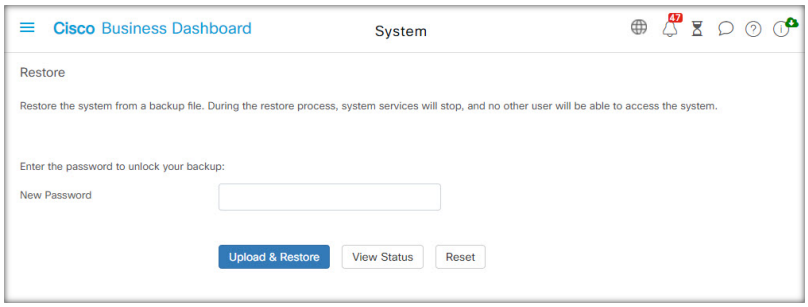
要执行备份，请执行以下步骤。



1. 导航到**系统** > **备份**。
2. 在**密码**字段和**确认密码**字段输入用于加密备份的密码。
3. 点击**备份与下载**。此时将显示弹出窗口，显示备份进度。较大的系统要完成备份可能需要一些时间，因此您可以关闭进度条，稍后再使用**查看状态**按钮让其重新显示。

完成后，备份文件将下载至您的 PC。

要将配置备份恢复到 Dashboard，请执行以下步骤。



1. 导航到**系统** > **恢复**。
2. 在**密码**字段输入用于加密备份的密码。
3. 点击**上传与恢复**以继续。系统将显示一个弹出窗口，用于从您的 PC 上传备份文件。您可以将备份文件拖放到提供的目标区域，也可以点击目标区域来指定 PC 文件系统中的文件。点击**恢复**以继续。

如果控制面板版本为 2.5.0 或更高版本，则应用将在恢复过程完成后重新启动。

管理平台设置

通过**平台设置**页面，您可以修改主要系统设置，而无需直接访问操作系统。由于 Cisco Business Dashboard 支持的平台存在差异，因此并非所有设置都可在每个平台上使用。

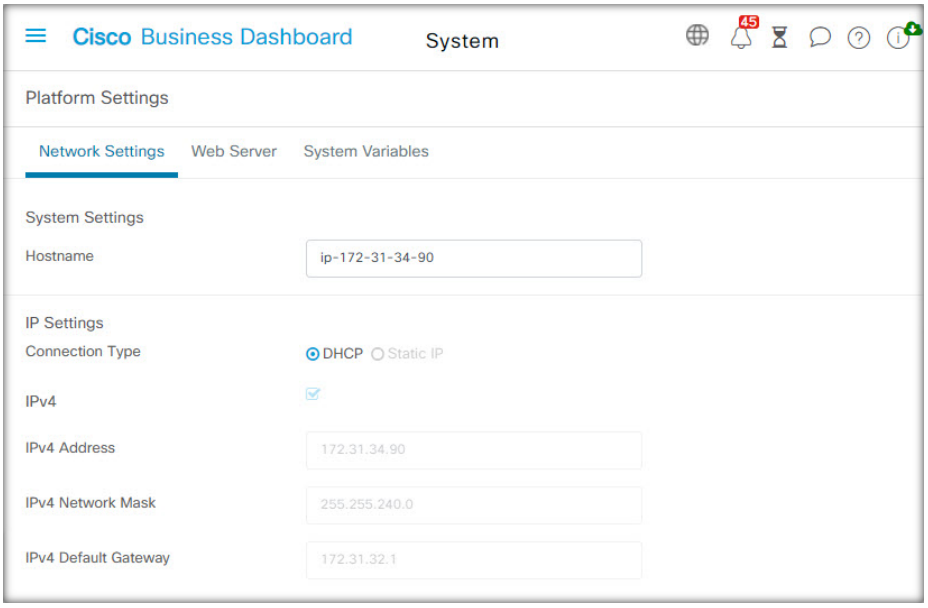
平台设置分为三组：

- 网络设置
- Web 服务器
- 系统变量

以下部分介绍每个选项卡上的可用设置。

更改主机名（“网络设置”选项卡）

主机名是操作系统用来识别系统的名称，并可供 Cisco Business Dashboard 在生成 Bonjour 通告时识别 Dashboard。

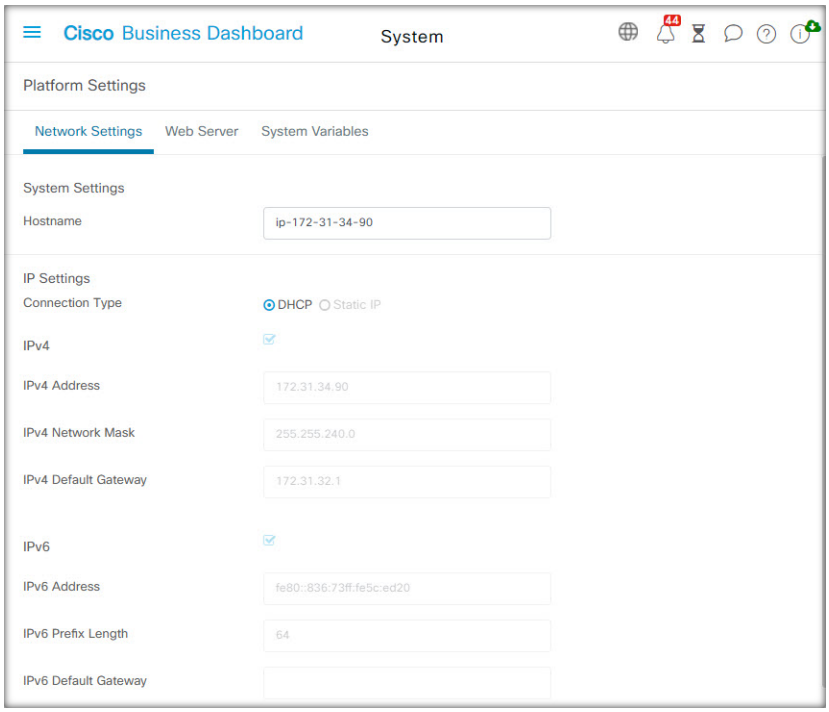


要更改 Dashboard 的主机名，请执行以下步骤。

1. 导航到**系统** > **平台设置**，然后选择**网络设置**选项卡。
2. 在提供的字段中指定 Dashboard 的主机名。
3. 点击**保存**。

更改网络设置（“网络设置”选项卡）

注释 这对适用于 AWS 或 Azure 的 Cisco Business Dashboard 不适用。要修改网络配置，对于 AWS 实例，请在 AWS 中使用 EC2 控制台；对于 Azure 实例，请使用 Azure 门户。

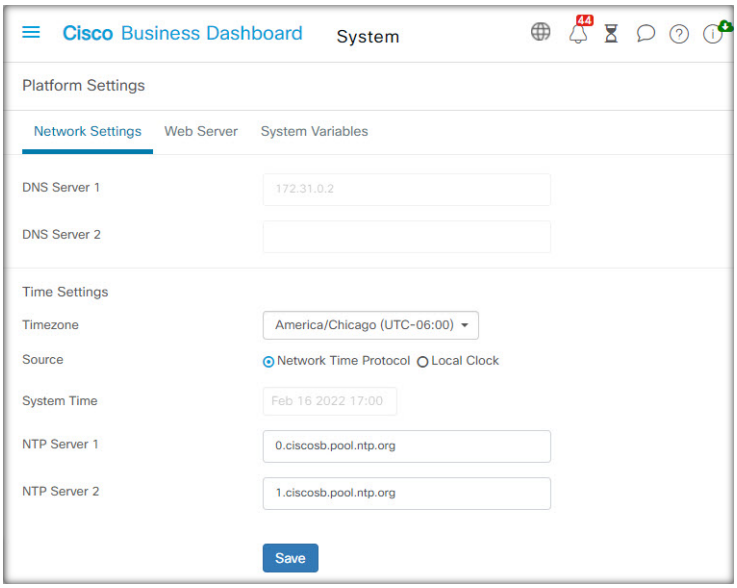


要更改 Dashboard 的网络配置，请执行以下步骤。

1. 导航到**系统** > **平台设置**，然后选择**网络设置**选项卡。
2. 选择 IP 地址的分配方法。可用选项有“DHCP”（默认）和“静态 IP”。如果选择“静态 IP”选项，请在相应的字段中指定地址、子网掩码、默认网关和 DNS 服务器。
3. 点击**保存**

更改时间设置（“网络设置”选项卡）

时间设置用于为 Dashboard 管理系统时钟。要调整系统时钟，请执行以下步骤。



1. 导航到**系统** > **平台设置**，然后选择**网络设置**选项卡。
2. 为 Dashboard 选择相应的时区。
3. 选择时间同步方法。可用选项有 **NTP**（**默认**）和**本地时钟**。如果选择“NTP”选项，则可以选择修改用于同步的 NTP 服务器。

   如果选择**本地时钟**，可使用提供的控件手动调整日期和时间。或者，可以点击**时钟**以使时间与 PC 同步。
4. 点击**保存**。

注释 如果将虚拟机配置为使本地时钟与主机同步，则通过**平台设置**页面完成的任何本地时钟更改将被虚拟机监控程序覆盖。

如果使用的虚拟机监控程序是 VirtualBox，并且 VM 中安装的是 VirtualBox Guest Additions，则 NTP 服务（时间同步）将不会运行。

更改端口设置（“Web 服务器”选项卡）

端口设置用来控制托管 Dashboard 用户界面的 TCP 端口。要更改默认的 Web 服务器端口，请执行以下步骤。

1. 导航到**系统** > **平台设置**，然后选择 **Web 服务器**选项卡。
2. 更改 Web 服务器用于 HTTP 和 HTTPS 协议的端口。
3. 更改用于通过 Cisco Business Dashboard 远程访问网络设备的端口。
4. 点击**保存**。

限制访问 Dashboard（“Web 服务器”选项卡）

您可以使用“访问控制”设置来限制可以访问 Dashboard 的 IP 地址。您可以为 Dashboard GUI、Dashboard API 以及探测器和受管设备连接指定不同的 IP 范围。

要限制访问 Dashboard，请执行以下步骤。

1. 导航到**系统** > **平台设置**，然后选择 **Web 服务器**选项卡。
2. 在提供的字段中输入网络前缀和掩码。如果任何部分需要多个前缀，请点击 **(+)** 加号图标添加更多条目。同样，可以点击垃圾桶图标删除现有条目。
3. 点击**保存**。

管理系统变量（“系统变量”选项卡）

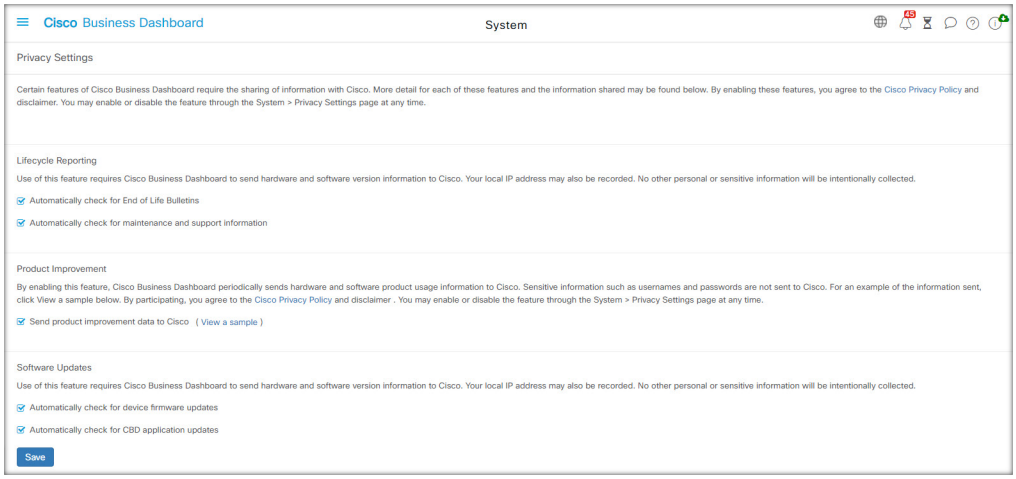
Cisco Business Dashboard 生成配置模板和其他任务时，使用系统变量提供与 Dashboard 相关的某些参数。有些系统变量可能由Dashboard 自动确定，但有些变量需要用户输入。特别地，如果Dashboard 部署在 Web 代理或 NAT 网关之后，管理员需要为 Dashboard 提供外部编址信息。

要更新 Dashboard 的外部地址信息，请执行以下步骤。

1. 导航到**系统** > **平台设置**，然后选择**系统变量**选项卡。
2. 根据需要在“外部系统设置”参数中输入IP 地址和端口信息。如果留空，Dashboard将使用相应系统变量的平台地址和端口信息。
3. 点击**保存**。

管理隐私

Cisco Business Dashboard 的某些功能要求使用思科托管的在线服务，并且会导致与思科共享某些信息。这些服务包括：



- **思科 Active Advisor**Cisco Business Dashboard - 可以将网络设备清单信息上传到思科 Active Advisor 服务：*https://www.ciscoactiveadvisor.com*。默认情况下会禁用此功能。
- **生命周期报告** - 此功能包括在 Cisco Business Dashboard 中生成**生命周期报告**、**生命周期结束报告和维护报告**。默认情况下启用“生命周期报告”。
- **软件更新** - 针对网络设备的软件更新可用性通知，以及自动应用这些更新的功能。默认情况下启用“软件更新”。
- **产品改进** - 此功能允许 Cisco Business Dashboard 发送有关网络中硬件和软件使用情况的信息，以便进一步开发思科产品组合。默认情况下启用“产品改进”。

所有这些功能均受思科隐私政策的约束，您可以随时启用或禁用这些功能。在 Dashboard 的初始设置期间会显示**隐私设置**页面，使您可以在收集任何网络数据之前禁用任何默认启用的功能。在下方可以找到有关所有这些功能以及共享信息的更多详情。

思科 Active Advisor

思科 Active Advisor (CAA) 是一项基于云的服务，可提供有关您的网络资产的基本生命周期信息。通过启用此功能，Dashboard 会向 CAA 发送网络设备清单信息，并且您在 CAA 门户中查看生命周期信息。它不会发送用户名和密码等敏感信息。

上传可以自动执行或按需执行。要执行按需上传，请执行以下操作：

1. 导航到**网络**页面并选择查看网络。
2. 从**网络操作**下拉列表中选择**上传到 CAA**。
3. 如果出现提示，请提供 cisco.com 凭证。
4. 或者，选择要应用于上传的标签。
5. 点击**上传**。您还可以在发送设备清单数据之前点击**查看设备清单数据**，以便在上传之前检查数据。

注释 所提供的 cisco.com 凭证在用于上传之前，必须至少已用于登录思科 Active Advisor 门户 (*https://www.ciscoactiveadvisor.com*) 一次。

要启用自动上传，请执行以下步骤。

1. 导航到**网络**页面，选择网络并点击**更多**。然后选择 CAA 选项卡。
2. 在提供的字段中输入您的 cisco.com 凭证。

   或者，您可以选择要应用于上传的标签。
3. 确保选中**自动上传新发现的设备**复选框。
4. 点击**保存**。您还可以通过点击此页面上的链接查看要上传的数据的示例。

要禁用自动上传，请执行以下步骤。

1. 导航到**网络**页面，选择网络并点击**更多**。然后选择 CAA 选项卡。
2. 取消选中**自动上传新发现的设备**复选框。
3. 点击**保存**。

生命周期报告

Cisco Business Dashboard提供网络中每部思科设备的生命周期状态信息。为此，Dashboard 必须向思科提供每部思科设备的产品 ID、序列号以及硬件和软件版本。还可以记录 Dashboard 的 IP 地址。在此过程中，思科不会故意收集任何个人信息或敏感信息。

要禁用生成生命周期报告，请执行以下步骤。

1. 导航到**系统** > **隐私设置**。
2. 取消选中要禁用的报告的复选框。
3. 点击**保存**。

产品提升

通过启用此功能，Cisco Business Dashboard 会定期向思科发送硬件和软件产品使用情况信息。还可以记录 Dashboard 的 IP 地址。在此过程中，思科不会故意收集任何个人信息或敏感信息。

要查看所发送信息的示例，请执行以下步骤。

1. 导航到**系统** > **隐私设置**。
2. 点击**向思科发送产品改进数据**复选框旁边的**查看示例**链接。系统将显示包含示例数据的上传示例。

要禁用生成产品改进数据，请执行以下操作：

1. 导航到**系统** > **隐私设置**。
2. 取消选中**向思科发送产品改进数据**复选框。
3. 点击**保存**。

软件更新

使用此功能需要 Cisco Business Dashboard 向思科发送每部设备的硬件和软件版本信息。还可能会记录您的本地 IP 地址。在此过程中，思科不会故意收集任何个人信息或敏感信息。

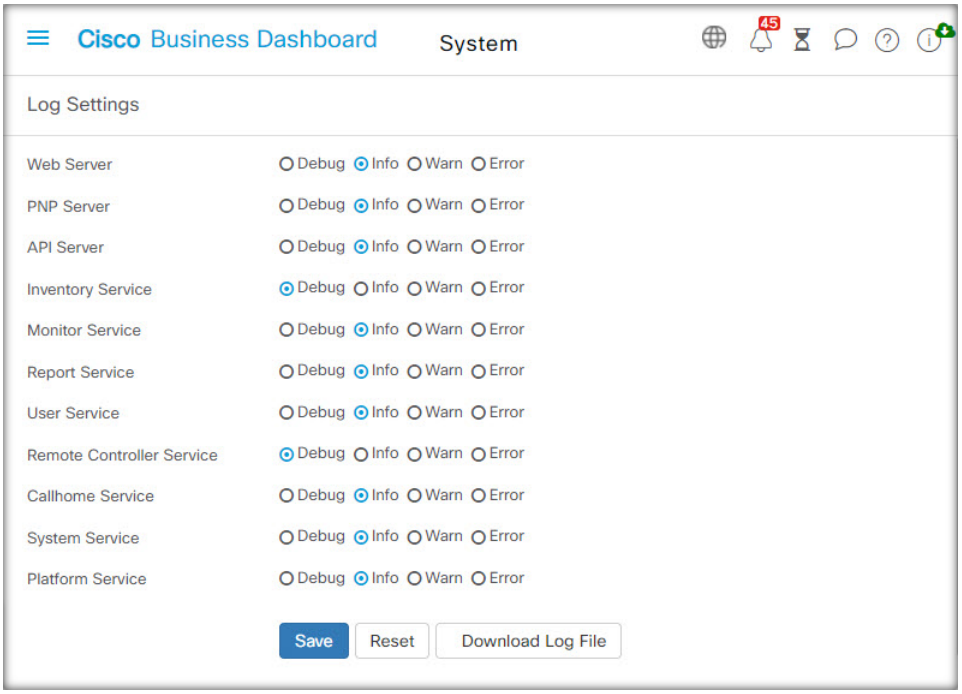
要禁用自动软件更新，请执行以下操作：

1. 导航到**系统** > **隐私设置**。
2. 取消选中设备固件检查复选框和 Cisco Business Dashboard 应用检查复选框。
3. 点击**保存**。

管理日志记录设置

通过**日志设置**页面，您可以按不同的软件模块控制日志文件中包含的详细信息量。默认日志记录级别为**信息**，但您可以选择**警告**或**错误**来减少记录的消息数量，或选择**调试**来查看更多详细信息。

要更改 Dashboard 的日志级别，请执行以下步骤。



1. 导航到**系统** > **日志设置**。
2. 使用单选按钮为每个软件模块选择所需的日志记录级别。
3. 点击**保存**。

Dashboard 的日志文件位于本地文件系统上的 `/var/log/ciscobusiness/dashboard/` 目录中。您可以点击**下载日志文件**以下载此目录内容的存档。收集所有数据可能需要几分钟时间。

记录到系统日志

从版本 2.2.1 开始，Cisco Business Dashboard 应用日志可以发送到主机的系统日志服务，并从那里定向到外部系统日志服务器。

要启用将文件发送到主机系统日志服务，请执行以下步骤。

1. 使用 SSH 或通过控制台登录到主机操作系统，并编辑文件 `/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf`
2. 编辑 `xxx.logger` 行，指定**文件**和/或**系统日志**（用逗号分隔）。以下模块可用：`redis`、`mongo`、`rabbitmq`、`nginx` 和 `cbd`。如果指定文件，会将日志消息定向到

/var/log/ciscobusiness/dashboard/ 目录中的默认日志文件。如果指定**系统日志**，会将日志消息定向到主机中的系统日志服务。

注释 mongo模块不支持多个日志记录目标。如果列出多个目标，第一个条目优先。此外，无论记录器配置中是否存在关键字**文件**，cbd 模块都将始终记录到文件系统。

3. 或者，修改xxx.syslog.facility行，指定用于每个模块的系统日志工具。默认情况下，每个模块会记录到单独的 local<*n*> 工具，其中 <*n*> 的范围介于 1 和 5 之间。
4. 先后使用命令 **cisco-business-dashboard stop** 和 **cisco-business-dashboard start** 重新启动 Cisco Business Dashboard。

修改日志记录配置以将日志消息定向到**系统日志**后，应更新 /etc/rsyslog.conf 文件以接收日志并将 Dashboard 日志消息定向到所需目标。有关配置文件的详细信息，请参阅 https://www.rsyslog.com/doc/v8-stable/configuration/index.html。

执行以下步骤：

1. 应更新 /etc/rsyslog.conf 文件，以允许通过环回接口接收日志消息。编辑文件，确保包括以下行，以启用此设置并限制服务器仅在环回接口上侦听：

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. 在目录 /etc/rsyslog.d/ 中创建一个新文件，以包含特定于 Cisco Business Dashboard 的配置指令。文件名格式应与 40-cisco-business-dashboard-syslog.conf 类似。
3. 编辑在第 2 步中创建的文件，确保包含将日志输出发送到所需目标的指令。例如，假设使用 cisco-business-dashboard-logger.conf 文件中的默认工具，以下配置会将警告级别和上述消息从 Dashboard 应用定向到名称为 logger.example.com 的系统日志服务器：

```
local2.warning  @logger.example.com
```

4. 使用命令 **sudo systemctl restart rsyslog.service** 重新启动 rsyslog 后台守护程序以应用更改

管理本地 Probe

注释 对适用于 AWS 或 Azure 的 Cisco Business Dashboard，此页不存在。

Cisco Business Dashboard Probe 可安装在与 Cisco Business Dashboard 相同的主机上，以便管理 Dashboard 本地网络中的设备，而且 Dashboard 的思科虚拟机映像中包 Probe。如果不想管理 Dashboard 的本地网络，可通过以下步骤禁用此同位 Probe。

1. 导航到**系统** > **本地 Probe**。
2. 点击切换开关禁用本地 Probe。
3. 点击**保存**。

要从 Dashboard 完全删除 Probe 软件，请登录操作系统，然后使用命令 `sudo apt-get --purge autoremove cbd-probe`。这将删除任何其他应用不需要的 Probe 软件、配置和依赖项。

管理集成设置

Cisco Business Dashboard 可与思科和其他供应商提供的各种应用和服务集成。当与应用集成时，可以在应用和执行的网络操作之间交换数据和事件。

以下应用和服务支持集成：

- ConnectWise Manage
- Webex

有关设置集成以及与每个应用交换信息的详细信息，请阅读以下部分。

ConnectWise Manage

ConnectWise Manage 是专为托管服务提供商设计的一款专业服务自动化工具 (PSA)。其功能包括资产管理、记账和计费以及服务中心服务。将 Cisco Business Dashboard 与 ConnectWise Manage 集成可帮助您确保及时更新网络设备的资产记录，并通过服务中心通知单管理事件和网络操作。

支持的功能

Cisco Business Dashboard 与 ConnectWise Manage 集成后，可在三个主要方面提供额外功能：资产管理、事件管理和自动化。

对于资产管理，Cisco Business Dashboard 将在 ConnectWise Manage 中为 Dashboard 管理的每个网络设备自动创建并定期更新配置记录。配置记录包括大量信息，例如设备类型和型号、序列号、软件信息、保修到期日期和生命周期等。如果从 Dashboard 设备清单中删除设备，该配置将标记为非活动，但不会从 ConnectWise Manage 中删除。

除了创建配置记录外，您还可以选择将网络设备类型与 ConnectWise Manage 中的特定产品相关联，并制定包含这些产品以及与该客户相关联的设备数量的 Cisco Business Dashboard 更新协议。

管理网络事件时，您可以配置 Cisco Business Dashboard 监控配置文件，以便 Dashboard 在出现所选通知时创建服务中心通知单。这些通知单包含事件的详细信息，并与生成通知的设备的配置记录相关联。对于固件通知，也可以将通知单创建为自动化通知单，以便在下一个变更窗口期间将固件更新应用到设备。

自动化通知单是能使Cisco Business Dashboard执行网络操作的特殊通知单。自动化通知单在Dashboard监控的专用服务面板中创建，可用于自动执行以下操作：

- 对配置进行备份
- 升级到最新固件版本
- 重新启动设备
- 保存运行配置
- 删除设备

自动化通知单可以创建为立即执行，或者在下一个变更窗口期间执行，也可以设置为在执行前需要审批。通知单将在执行过程中更新进度信息，并在操作完成后更新结果。

前提条件

在设置 ConnectWise Manage 集成之前，必须满足以下先决条件：

- 如果将使用自动化通知单，ConnectWise Manage 应用必须能够与 Cisco Business Dashboard Web 服务器建立连接。此外，Cisco Business Dashboard 必须具有 ConnectWise Manage 信任的证书。在大多数情况下，这意味着证书需要由公共 CA 签名。有关为 Cisco Business Dashboard 设置证书的详细信息，请参阅管理证书，第 99 页。
- 如果 Dashboard 位于 NAT 网关或防火墙后面，请确保使用 ConnectWise Manage 应用将用于连接到 Dashboard 的主机名和 Web 服务器端口来填充**系统** > **平台设置**下的“系统变量”页面。
- 必须为 Cisco Business Dashboard 创建一组 API 密钥，并且必须至少具有下表中列出的权限。

表 *8: API* 密钥所需的权限

权限	添加级别	编辑级别	删除级别	查询级别
公司				
公司维护	无	无	无	全部
配置	全部	全部	全部	全部
财务				
协议	无	全部	无	全部
采购				
产品目录	无	无	无	全部
服务台				
服务申请单	全部	全部	全部	全部
系统				

权限	添加级别	编辑级别	删除级别	查询级别
表设置	全部	全部	全部	全部

- 必须确定或创建适用于自动化通知单的服务面板。此服务面板有许多设置要求，这些要求将在集成过程中应用，建议将此服务面板专用于网络运营。有关如何设置此服务面板的详细信息，请参阅以下部分。
- 必须确定或创建适用于通知单的服务面板。此服务面板没有相关的特定要求，可以是现有的通用服务面板。通知面板也可以是用于自动化通知单的服务面板。

设置 ConnectWise Manage 集成

设置 ConnectWise Manage 集成涉及多个步骤。

- 与 ConnectWise Manage 服务建立通信。
- 将 ConnectWise 公司映射到 Cisco Business Dashboard 组织。
- 配置资产同步过程。
- 选择用于事件通知和自动化的服务面板。

本部分介绍如何执行正确设置所有配置的每个过程。

与 ConnectWise Manage 服务建立通信

1. 导航到**系统** > **集成设置**。
2. 找到代表 ConnectWise Manage 集成的磁贴，并确保切换开关设置为**启用**。
3. 点击**设置**图标以显示 ConnectWise Manage 设置页面，然后选择**连接**选项卡。
4. 填写提供的表单中的字段，然后点击**保存**。有关请求的参数的详细信息，请参阅下表。

表 9: ConnectWise Manage 连接参数

参数	说明
API 主机名	要连接的 ConnectWise Manage 服务的协议和主机名。默认为 https://na.connectwise.net。
公司 ID	ConnectWise Manage 中公司的标识符。此值与登录 ConnectWise Manage GUI 时使用的值相同。
公钥	面向 Cisco Business Dashboard 的 ConnectWise Manage 中定义的 API 密钥的公钥。
私钥	面向 Cisco Business Dashboard 的 ConnectWise Manage 中定义的 API 密钥的私钥。

点击**保存**后，Cisco Business Dashboard 将测试连接，然后从 ConnectWise Manage 读取稍后在设置过程中所需的信息。这些信息包括公司列表、配置类型、产品、协议类型和服务面板。如果在 ConnectWise Manage 中对这些信息中的任何信息进行了更改，则点击此页面上的**刷新 ConnectWise 数据**按钮以重新读取数据。

将 ConnectWise 公司映射到 Cisco Business Dashboard 组织

在 Cisco Business Dashboard 和 ConnectWise Manage 之间建立连接后，需要将 Cisco Business Dashboard 中的组织映射到 ConnectWise Manage 中的公司。通过将公司映射到组织，可以将网络设备和事件与 ConnectWise Manage 中的正确客户相关联。要完成映射，请执行以下步骤。

1. 导航到**系统** > **集成设置**。
2. 点击 **ConnectWise Manage** 磁贴上的**设置**图标，然后选择**组织映射**选项卡。
3. 点击**从 ConnectWise 导入**按钮。这会将公司列表和组织列表进行比较，并在公司名称或公司 ID 与组织名称匹配时创建映射。
4. 可以手动或使用逗号分隔值 (CSV) 文件在公司和组织之间进行任意映射。

   要手动创建映射，请执行以下操作：

   1. 点击映射表上方的 （加号）图标以在表中创建新条目。
   2. 从下拉列表中，选择要映射的公司和组织名称。

   注释 如果下拉菜单中未列出所需的公司名称，则返回到**连接**选项卡，然后点击**刷新 ConnectWise 数据**按钮以更新公司列表。

   3. 点击**保存**图标。

   要使用 CSV 文件创建映射，请执行以下操作：

   1. 创建包含组织和公司名称之间所需映射的 CSV 文件。
   2. 点击映射表上方的**下载**图标，以获取包含现有映射列表的模板 CSV 文件。
   3. 模板文件更新后，点击表上方的**上传**按钮以创建文件中指定的新映射。

   要更改现有映射，请执行以下操作：

   1. 点击映射旁边的单选按钮。
   2. 点击**编辑**图标。
   3. 进行必要更改。
   4. 点击**保存**图标。

   要删除现有映射，请执行以下操作：

1. 点击映射旁边的单选按钮。
2. 点击**删除**图标。

配置资产同步过程

在 ConnectWise Manage 中创建配置记录以表示网络设备是事件管理和自动化功能正常运行的先决条件。Cisco Business Dashboard 将自动为映射到 ConnectWise Manage 公司的组织中的每个网络设备创建和更新配置记录。要设置资产同步，请执行以下步骤。

1. 导航到**系统** > **集成设置**。
2. 点击 **ConnectWise Manage** 磁贴上的设置图标，然后选择**资产同步**选项卡。
3. 点击**在 ConnectWise 中创建默认配置类型**按钮。

   这将创建三种配置类型 - CBD 受管路由器、CBD 受管交换机和 CBD 受管 WAP - 每个类型均具有适用于网络设备的字段和问题。如果这些配置类型已经存在，将使用字段和问题进行更新。
4. 点击**保存**图标。

每天午夜，Cisco Business Dashboard 将为映射到公司的每个组织执行资产同步。系统会为该组织中的每个网络设备创建一条配置记录，其中包含该设备的相关信息。如果配置记录已存在，则会根据设备信息的更改对其进行更新。与已从 Cisco Business Dashboard 中删除的设备相关联的配置记录将标记为**非活动**。

在同步过程中，Cisco Business Dashboard 还将执行以下操作：

1. 对于每个公司，Cisco Business Dashboard 将标识与您指定的协议类型匹配的任何协议。
2. 对于每个协议，Cisco Business Dashboard 将标识与您选择并与每种设备类型相关联的产品匹配的任何添加项。
3. 对于每个添加项，Cisco Business Dashboard 将根据选择了相应产品的设备类型的数量来更新数量。

要实现此目的，请执行以下操作：

1. 导航到**系统** > **集成设置**。
2. 点击 **ConnectWise Manage** 磁贴上的**设置**图标，然后选择**资产同步**选项卡。
3. 对于每种设备类型，点击**产品**字段，然后选择一个或多个要与此类型的设备关联的产品。
4. 在**协议类型**标题下，选择一个或多个协议类型以标识要更新的协议。
5. 点击**保存**图标。

注释 如果下拉列表中未列出所需的产品或协议类型，则返回到**连接**选项卡，然后点击**刷新 ConnectWise 数据**按钮以更新列表。

选择用于事件通知和自动化的服务面板

通过指定应用于每个功能的服务面板来启用事件管理和自动化功能。要指定要使用的服务面板，请执行以下操作：

1. 导航到**系统** > **集成设置**。
2. 点击 **ConnectWise Manage** 磁贴上的**设置**图标，然后选择**通知单设置**选项卡。
3. 从**通知面板**下拉菜单中，选择用于为响应网络事件而创建的通知单的相应服务面板。
4. 从**自动化面板**下拉菜单中，选择应监控自动化通知单的服务面板。

注释 如果下拉列表中未列出所需的服务面板，则返回到**连接**选项卡，然后点击**刷新 ConnectWise 数据**按钮以更新服务面板列表。

5. 点击**保存**图标。

   Cisco Business Dashboard 将更新 ConnectWise Manage 中自动化面板的设置，以包含支持自动化功能所需的适当状态值、类型和子类型。有关将要创建的状态、类型和子类型的详细信息，请参阅使用自动化通知单自动执行网络操作，第 122 页中的表 30-32。

使用 ConnectWise Manage 集成

在 ConnectWise Manage 提供的三种集成类型中，事件管理和自动化需要用户主动与功能交互。资产同步通常不需要用户交互。以下部分将详细介绍每项功能的用法。

使用资产同步

除上述初始设置外，资产同步无需任何特定操作。Cisco Business Dashboard 中的网络设备清单会自动同步到包含下表所示信息的 ConnectWise Manage 配置记录。与“资产同步”设置中指定的类型匹配的任何协议都将更新与所选产品匹配的任何添加数量，以反映网络中存在的相应类型的设备数量。

资产同步过程每天午夜自动进行。如果需要立即同步，可以点击“资产同步”屏幕上的**同步资产**按钮来启动同步。如果已与 Cisco Business Dashboard 集成，也可以通过协作工具完成此操作。

注释 资产同步过程通常需要几分钟，在大型网络中可能需要更长时间。

表 *10: ConnectWise Manage* 配置字段用法

字段	说明
配置名称	设置为设备主机名
配置详情	
类型	配置类型是根据设备类型以及在“资产同步”页面中配置的映射设置的。

字段	说明
状态	如果设备已从 Dashboard 设备清单中删除，则设置为**非活动**，否则设置为**活动**。
型号	设备的型号。
序列号	设备的序列号。
公司	
公司	与**组织映射**页面中定义的设备组织相对应的公司。
备注	
供应商备注	包含一条备注，指示配置是由 Cisco Business Dashboard 创建的，并显示创建时间戳。
配置问题	配置问题包含以下信息： • **设备产品 ID**：此字段类似于型号，但它是购买新设备时使用的标识符。 • **软件版本**：此信息包括当前版本和最新的可用版本以及版本说明。 • **生命周期信息**：此字段包括保修结束日期以及适用的生命周期终止公告的详细信息。
设备详细信息	
IP 地址	设备的管理 IP 地址。
MAC 地址	设备的基本 MAC 地址。

使用自动化通知单自动执行网络操作

自动化通知单允许通过提交特殊格式的通知单对网络设备执行操作。

通知单可以指定操作应立即执行还是在下一个变更窗口期间执行，并且可以选择在执行之前需要审批步骤。当满足所有前提条件时，Cisco Business Dashboard 将执行通知单中指定的操作，并根据操作是否成功更新通知单。

要创建自动化通知单，请创建具有以下特征的新通知单：

- 服务面板应设置为设置集成时创建的自动化面板。
- 该通知单应该只与代表 Cisco Business Dashboard 管理的网络设备的一个配置相关联。
- 类型应设置为所需的操作。有关可用操作的列表，请参阅表 11: 自动化通知单类型，第 123 页。
- 应根据所需的执行时间以及是否需要审批来选择子类型。有关可用选项的列表，请参阅表 12: 自动化通知单子类型，第 124 页。

- 状态应设置为**开始**以开始自动化过程。如果在自动化开始之前需要执行其他工作，则可以将状态设置为**需要关注**，直到工作完成。有关所有可能的状态值的完整列表，请参阅表 13: 自动化通知单状态，第 124 页。

创建自动化通知单且状态为**开始**时，Cisco Business Dashboard 会控制通知单并执行以下步骤：

1. CBD 会检查通知单，以确保所有所需的信息都存在。如果存在问题，系统会更新内部备注，并将状态更改为**需要关注**。
2. 如果通知单格式正确，则检查子类型，以查看是否需要审批。如果是，则状态将更改为**需要审批**，并且在状态更新为**已批准**之前不会执行进一步操作。
3. 系统会检查子类型，以了解何时应执行该操作。如果通知单设置为立即运行，Dashboard 将立即执行操作。如果将操作设置为在下一个变更窗口期间运行，则会创建新的计划配置文件，并更新通知单状态以显示作业处于待处理状态。
4. 操作完成后，Dashboard 会根据操作是否成功来更新通知单中的备注。如果操作成功完成，则关闭通知单。如果操作失败，则状态更新为**需要关注**。解决失败原因后，可以将状态重新更改为**开始**以重新安排通知单；如果不再需要执行此操作，则可以将状态更改为已关闭。

自动化通知单审批选项允许在自动化过程中插入一定程度的变更控制。将自动化通知单指定为需要审批，可以确保在执行操作之前由人工进行验证，并且验证记录在通知单历史记录中。

ConnectWise Manage 中的自动化通知单审批是通过指示需要审批并且已授权审批的状态更改来实现的。

需要审批的通知单（状态为“需要审批”）可以通过以下两种方式之一进行批准：

- 可以使用 ConnectWise Manage 界面直接更新通知单状态。建议在记录批准的同时向通知单添加备注。但是，审批的详细信息也将记录在通知单审计追踪中。
- 通知单可以通过已与 Cisco Business Dashboard 集成的协作工具进行审批。在这种情况下，系统会在通知单中添加一条备注，记录审批和审批人的身份。

注释 无论是 ConnectWise Manage 还是 Cisco Business Dashboard，都不能强制要求审批人必须与通知单创建者的身份不同。审批人不能仅限于指定的工作人员名单。任何可以编辑通知单或有权访问协作空间的用户都可以批准通知单。实施此类限制需要相应操作流程。

表 *11:* 自动化通知单类型

类型	说明
备用配置	复制设备的当前运行配置，并保存在 Cisco Business Dashboard 上。
删除	从 Cisco Business Dashboard 设备清单中删除离线设备。
重新启动	重启设备。
保存运行配置	在设备上保存运行配置，以供启动时使用。

类型	说明
将固件更新为最新版本	将设备上的软件升级到思科发布的最新版本。

表 *12:* 自动化通知单子类型

子类型	说明
需要审批 - 在变更窗口期间运行	此操作需要审批，并且应安排在通知单获批后的下一个变更窗口期间执行。
需要审批 - 立即运行	此操作需要审批，并且应在通知单获批后立即执行。
在变更窗口期间运行	操作应安排在下一个变更窗口期间执行。
立即运行	操作应立即执行。

表 *13:* 自动化通知单状态

状态	说明
开始	向 Dashboard 指示通知单已做好自动化准备。
需要关注	表示需要人为干预。如果在自动化开始之前需要执行某些工作，则可以手动设置此状态；在自动化操作失败的情况下，将通过 Dashboard 设置此状态。
正在进行	Dashboard 正在主动处理通知单。
需要审批	表示需要审批才能继续处理的有效自动化通知单。需要人为干预才能继续操作。
已批准	表示通知单已获批准，准备执行。可以通过在 ConnectWise Manage 用户界面中选择此状态来批准通知单，或者通过已与 Cisco Business Dashboard 集成的协作工具中的审批命令来批准通知单。
已使用 CBD 安排	已在 Cisco Business Dashboard 中安排作业，但尚未执行。作业执行后，通知单将更新。
完成（已关闭）	请求的操作已成功完成。

使用通知单管理网络事件

要在启用通知单创建以响应网络事件，必须更新 Cisco Business Dashboard 监控配置文件，以将**提交服务中心通知单**操作添加到一个或多个通知监控器。有关管理监控配置文件的详细信息，请参阅监控配置文件，第 90 页。

注释 思科建议您配置监控配置文件，以确保在持续变化的基础上不超过每小时 60 条通知单和/或协作消息的平均速率。在与外部应用通信时，超过此速率的持续速率可能会导致 API 拥塞和事件丢失。

当通知与启用**提交服务中心通知单**的监控配置文件相匹配时，会在通知面板中提交新的通知单，并与相应设备的配置关联。系统使用有关通知的相关信息更新通知单的正文。

对于大多数通知监控器，只能提交通知单。但是，对于固件通知，可以使用其他选项。当发现设备的新固件版本时，所创建的通知单也可以作为自动化通知单提交，它将在下一个变更窗口期间将固件更新应用于该设备。

在监控配置文件中配置固件通知时，会提供两个附加选项 - **包含自动化**和**包含审批**。如果启用了**包含自动化**复选框，则将创建自动化通知单，而不是通知单。此通知单将在自动化面板中提交，与设备配置关联，类型设置为**将固件升级为最新版本**。

最后，子类型将设置为安排在下一个变更窗口期间进行升级。如果启用了**包含审批**复选框，则子类型还将设置为在计划升级之前需要审批。有关自动化通知单中使用的不同子类型的详细信息，请参阅表 12: 自动化通知单子类型，第 124 页。

Webex

Webex 是一套协作工具和服务，包括消息、呼叫和会议功能。将 Cisco Business Dashboard 与 Webex 集成，让您随时了解关键网络事件，并允许您采取行动。您可以在桌面或移动设备上使用 Webex 应用。

支持的功能

与 Webex 集成后，Cisco Business Dashboard 可以将通知转发到协作空间，以通知用户网络事件。您可以通过更新监控配置文件来自定义通知，然后选择要转发的通知。

此外，还提供了一个有限的控制界面，允许用户从 Webex 界面执行某些操作。支持的操作包括：

- 查看 Cisco Business Dashboard 创建的未处理服务中心通知单列表。
- 查看需要审批的自动化通知单列表。
- 批准自动化通知单。
- 查看具有可用固件更新的网络设备列表。
- 启动网络设备升级。

前提条件

在设置 Webex 集成之前，必须创建 Webex 机器人程序并邀请其加入协作空间。要设置机器人程序，请执行以下操作：

1. 导航至 https://developer.webex.com/my-apps/new/bot 并登录您的 Webex 账户。

2. 填写提供的表单以创建您的机器人程序。您需要为机器人程序提供名称、用户名和说明，也可以选择为之提供自定义图标。

注释 虽然 Webex 允许机器人程序名称包含空格字符，但 Cisco Business Dashboard 要求机器人程序名称只能是一个没有空格的单词。

3. 点击**添加机器人程序**以创建机器人程序。记下显示的机器人程序令牌，因为在设置 Webex 集成时需要此令牌。

记住 机器人程序令牌仅显示一次，因此请务必将它记录在安全的位置，以供将来参考。

创建机器人程序后，必须邀请它加入协作空间。为与 Cisco Business Dashboard 交互而创建专用空间，不过也可以使用现有空间。但是，该空间的任何成员都可以查看所有事件并能够执行所有受支持的命令，因此该空间应该只授权用户管理网络。

有关创建空间和邀请用户的详细信息，请查阅 Webex 文档或 Webex 应用的在线帮助。

注释 在与 Cisco Business Dashboard 集成时，只可邀请机器人程序加入单个协作空间。如果被邀请加入多个空间，机器人程序的行为将不可预测。

除了创建机器人程序外，还应确保 Webex 基础设施能够建立与 Cisco Business Dashboard Web 服务器的连接。如果 Dashboard 位于 NAT 网关或防火墙后面，请确保使用 Webex 基础设施将用于连接到 Dashboard 的主机名和 Web 服务器端口来填充**系统** > **平台设置**下的“系统变量”页面。

设置 Webex 集成

要设置 Webex 集成，请执行以下操作：

1. 导航到**系统** > **集成设置**。
2. 找到 Webex 集成磁贴，并确保切换开关设置为**启用**。
3. 点击**设置**图标以显示 **Webex 设置**页面。
4. 将创建机器人程序时收到的机器人程序令牌复制到提供的字段中，然后点击**保存**图标。
5. 确保状态字段显示正确的机器人程序名称和协作空间。

注释 该机器人程序只能由单个 Cisco Business Dashboard 实例使用，不能与任何其他应用一起使用。如果有多个应用与机器人程序关联，则行为将不可预测。

Cisco Business Dashboard 配置机器人程序详细信息后，即可配置监控配置文件以将通知转发到协作空间。有关监控配置文件配置的详细信息，请参阅监控配置文件，第 90 页。

使用 Webex 集成

“使用 Webex 集成”分为两个主要方面：

- 设置和接收网络事件通知。
- 通过有限的控制界面与 Cisco Business Dashboard 进行交互。

以下各部分更详细地描述了每一项活动。

管理网络事件通知

要在 Webex 中启用通知以响应网络事件，必须更新 Cisco Business Dashboard 监控配置文件，以将**发送到协作空间**操作添加到一个或多个通知监控器。有关管理监控配置文件的详细信息，请参阅监控配置文件，第 90 页。

注释 思科建议您配置监控配置文件，以确保在持续变化的基础上不超过每小时 60 条通知单和/或协作消息的平均速率。在与外部应用通信时，超过此速率的持续速率可能会导致 API 拥塞和事件丢失。

当出现与启用了**发送到协作空间**的监控配置文件匹配的通知时，系统会向协作空间推送一条消息。该消息包括与通知相关的信息（包括通知详细信息），以及用于在 Cisco Business Dashboard 中查看设备的链接和在 ConnectWise Manage 中查看相关服务中心通知单（如果已为该事件创建服务中心通知单）的链接。

通过 Webex 与 Cisco Business Dashboard 交互

与 Webex 集成时，Cisco Business Dashboard 提供了一个有限的命令界面，可用于查询 Dashboard 和执行操作。下表提供了可用命令和相关操作的列表。

该界面要求用户调用机器人程序，才能接受命令。虽然该界面可以允许在一定程度上灵活输入，但它不提供自然语言处理功能，而仅限于支持一组预定义的命令。该界面还部分区分大小写，它将识别常见用法，但可能无法识别使用不常见大写模式的命令。

表 *14:* 支持的协作命令

命令	说明
Menu Help ?	提供了所有可用命令的列表和说明。
审批	提供了需要审批的自动化通知单的列表。 仅当 Dashboard 与 ConnectWise Manage 集成时，此命令才可用。
Approve <Ticket#>	将指定自动化通知单标记为已批准执行。

命令	说明
资产	启动资产同步过程。 仅当 Dashboard 与 ConnectWise Manage 集成时，此命令才可用。
固件	提供了具有可用固件更新的所有网络设备的列表。
Upgrade <Serial#>	将指定设备的固件更新安排在下一个变更窗口期间进行。 如果 Dashboard 与 ConnectWise Manage 集成，则将为此任务创建需要审批的自动化通知单，或直接在 Cisco Business Dashboard 中安排该通知单。

第 13 章

通知

本章包含以下各节：

关于通知

Cisco Business Dashboard 在网络中发生不同事件时生成通知，包括 ConnectWise 或 Webex 团队集成通知。通知可生成邮件或弹出警报，显示在浏览器的右下角，而且系统会记录所有通知以供日后查看。

当不再需要查看通知时，也可以确认通知已收悉。默认情况下，**通知中心**将隐藏这些通知。

支持的通知

下表列出了 Cisco Business Dashboard 支持的通知：

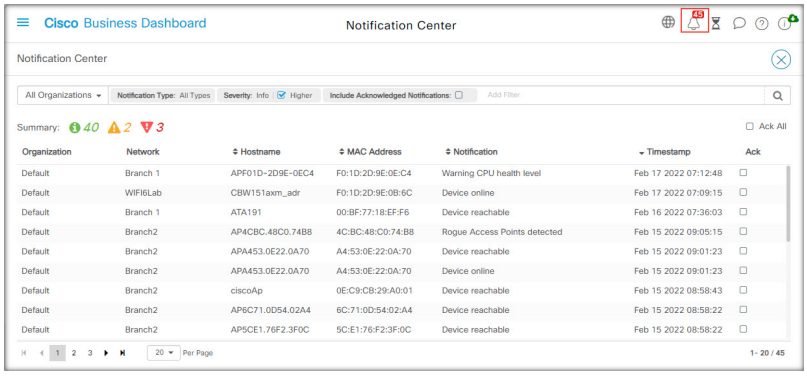


表 *15:* 支持的通知

事件	级别	说明	是否自动清除？
无线接入点、路由器、IP 电话和交换机的设备通知			
可访问性/已发现设备	信息	在网络中检测到新设备。	是，在发现设备 5 分钟以后。
可访问性/设备无法访问	警告	通过发现协议可识别设备，但无法使用 IP 访问该设备。	是，当可以通过 IP 再次访问设备时。
可访问性/设备离线	警报	在网络中检测不到设备。	是，当设备被重新发现时。
所需凭证/SNMP	警告	由于身份验证错误，Probe 无法访问设备。	是，当 Probe 进行身份验证时。
所需凭证/用户 ID	警告	由于身份验证错误，Probe 无法访问设备。	是，当 Probe 进行身份验证时。
所需凭证/密码已过期	警告	设备上管理员用户的密码已过期。	是，当设备上的密码已重置时。
配置不匹配	警报	当前设备配置与 Cisco Business Dashboard 配置文件和设备设置中指定的配置不匹配。	是，当配置不匹配问题得以解决时。
设备服务/SNMP	警告	SNMP 在设备上为禁用状态。	是，当启用 SNMP 时。
设备服务/Web 服务	警告	设备上已禁用 Web 服务。	是，当启用 Web 服务 API 时
运行状况	警告/警报	设备运行状况变为“警告”或“警报”级别。	是，当设备运行状况恢复正常时。
思科支持通知			
固件	信息	Cisco.com 上有可用的较高版本固件	是，当设备更新为最新版本时。
寿命终止	警告/警报	发现了设备的“寿命终止”公告，或者已到达“寿命终止”里程碑。	否
维护到期	警告/警报	设备超出保修期，且/或当前没有有效的维护合同。	是，当获得新的维护合同时。
设备运行状况通知			

事件	级别	说明	是否自动清除？
CPU	警告/警报	设备 CPU 使用率超过最大阈值。	是，当CPU使用率恢复到正常水平时。
运行时间	警告/警报	设备正常运行时间低于最小阈值。	是，当设备正常运行时间超过最低值时。
连接的客户端	警告/警报	连接的客户端数超过最大阈值。	是，当连接的客户端数恢复可接受的水平时。

查看和过滤当前设备通知

要查看单个设备或所有设备当前活动的通知，请执行以下步骤。

1. 在**主页**窗口中，点击全局工具栏右上角的**通知中心**图标。图标上的数字标记指定未确定和待解决的通知总数，标记颜色表示当前待解决的最高严重性级别。

   当前待处理的任何通知都列在**通知中心**的图标下方。严重性图标中的数字表示以下各个类别的通知总数：

图标	说明
	信息（绿色圆形图标）
	警告（橙色三角形图标）
	警报（红色倒三角形图标）

2. 在**通知中心**中，您可以执行以下操作：
   - 确认通知 - 选中要确认其通知的相应复选框。选中**全部确认**复选框，可以确认显示的所有通知。
   - 过滤显示的通知 - 有关说明，请参阅步骤 3。

3. “过滤器”框用于限制表中显示的通知。默认情况下，系统将显示所有类型和所有严重性级别的通知。要更改现有过滤器，请双击该过滤器以更改设置。要添加新过滤器，请点击“添加过滤器”标签，然后从下拉列表中选择过滤器。下表列出了所有可用的过滤器。

过滤器	说明
通知类型	要显示的通知的类型。例如，要显示离线设备的通知，可从下拉列表中选择**离线设备**。
严重性	要显示的通知的严重性级别，包括： • 信息 • 警告 • 警报 您可以选中**更高**复选框，以包含更高的严重性级别。
包括确认	包括已确认的通知。
网络	显示指定网络的通知。开始在过滤器中键入，匹配的网络将列在下拉列表中。点击以选择所需的网络。 过滤器中可能包含多个网络。
设备	显示指定设备的通知。开始在过滤器中键入，匹配的设备将列在下拉列表中。点击可选择所需的设备。 过滤器中可以包含多个设备。

注释 在设备的**基本信息**和**详细信息**面板中可查看各个设备的通知。

要控制如何接收通知，可在组织或系统级别更改通知设置。有关详细信息，请参阅组织，第 82 页或监控默认设置。

查看和过滤历史设备通知

任何通知的发生或状态更改将在 Dashboard 上记录为事件，并且可以通过事件日志查看。可以通过以下面板查看事件日志的子集：

基本信息面板或**设备详细信息**面板显示单个设备。

基本信息面板仅显示最近 24 小时的事件。

设备详细信息面板显示可用设备的所有历史数据。

注释 可过滤**设备详细信息**面板，以便将您关注的事件分离出来。有关查看和过滤历史事件的详细信息，请参阅关于事件日志。

第 14 章

作业管理

本章包含以下各节：

关于作业和作业中心

Cisco Business Dashboard 执行的任何任务或操作都称为作业，并在**作业中心**进行跟踪。作业包括用户发起的作业和系统自动发起的作业。

作业中心在**作业**选项卡上列出当前正在执行或过去发生的所有作业，包括作业类型、受影响设备和当前状态或作业是否成功完成等详细信息。

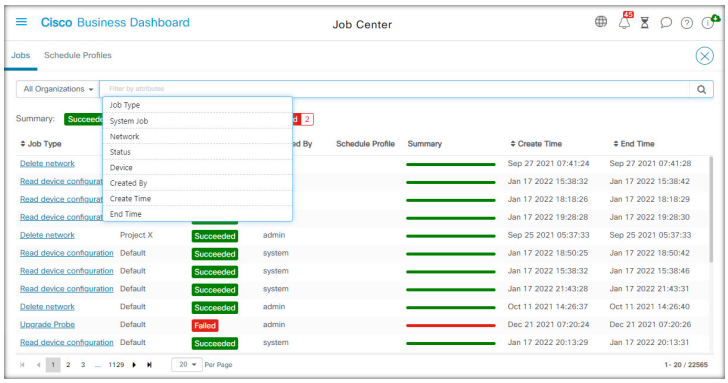
除了显示当前正在执行的作业和历史作业之外，作业中心还有另一个用于**计划配置文件**的选项卡。计划配置文件表示尚未执行的作业，因为它已安排在以后的某个日期执行。计划配置文件包括仅运行一次的任务，以及已定义为定期运行的任务。

查看和过滤作业和计划配置文件

要查看当前活动的作业、历史作业和尚未执行的作业的计划配置文件，请执行以下步骤。

步骤 1 在**主页**窗口中，点击全局工具栏右上角的**作业中心**图标。

图标上的数字标记指定当前正在执行的作业总数。



当前活动的作业和历史作业列在作业中心的**作业**选项卡上，而计划配置文件可以在“计划配置文件”选项卡上找到。系统会显示诸如作业类型、创建者和时间以及状态信息等全部信息。您可以点击特定作业或计划配置文件的**作业类型**参数，以显示更多详细信息。

步骤 2 **过滤器**框限制表格中显示的作业或配置文件。默认情况下，将列出所有作业和配置文件。要更改现有过滤器，请双击该过滤器以更改设置。要添加新过滤器，请点击**按属性过滤**标签，然后从下拉列表中选择过滤器。系统提供以下过滤器：

表 *16:* 可用过滤器

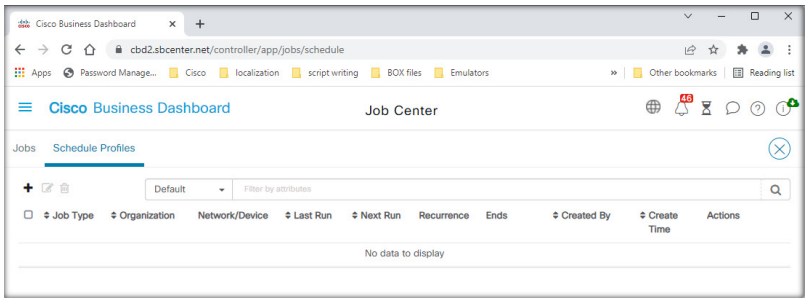
过滤器	说明
作业类型	从提供的下拉列表中选择要显示的作业或配置文件类型。
系统作业	使用此复选框可控制仅显示系统发起的作业，还是仅显示用户发起的作业。此过滤器仅在**作业**选项卡上可用。
状态	从下拉列表中选择一个状态值，以限制为仅显示处于该状态的作业。此过滤器仅在**作业**选项卡上可用。
设备	限制为仅显示影响所选设备的作业或配置文件。
创建者	在选择此过滤器时，在提供的字段中输入文本。系统将显示与输入的文本匹配的用户创建的作业或配置文件。
创建时间	使用此过滤器中提供的控件指定时间间隔。系统将显示在此间隔期间创建的作业或配置文件。
结束时间	使用此过滤器中提供的控件指定时间间隔。系统将显示在此时间间隔内完成执行的作业。此过滤器仅在**作业**选项卡上可用。
重复发生率	从下拉列表中选择一个支持的频率。将显示设置为以该频率重复执行的配置文件。此过滤器仅在**计划配置文件**选项卡上可用。
网络	限制为仅显示影响所选网络的配置文件。

过滤器	说明
下次运行时间	使用此过滤器中提供的控件指定时间间隔。将显示在此间隔期间下一次执行的配置文件。此过滤器仅在**计划配置文件**选项卡上可用。

管理计划配置文件

计划配置文件选项卡不仅可用于查看已定义的配置文件，还可以创建新配置文件以及编辑或删除现有配置文件。您还可以搜索通过配置文件创建的所有作业。

要创建新的计划配置文件，请执行以下步骤。



1. 在**主页**窗口中，点击**作业中心**图标

（位于全局工具栏右上角）。选择**计划配置文件**。

2. 点击表格左上角的 （加号）图标。
3. 在所显示的表单的**作业详细信息**部分，选择作业类型、组织以及目标设备或网络。请注意，所选作业类型可能无法应用于网络。
4. 在表单的**计划**部分，选择重复发生率并指定作业的开始时间。对于周期性作业，还要指定作业应何时结束。

   还可以将作业安排在下一个变更窗口或每个变更窗口期间进行。作业的时间由在网络或组织级别应用的变更窗口设置控制。有关变更窗口的更多详细信息，请参阅管理变更窗口，第 136 页。
5. 根据所选的作业类型，可能需要其他信息。如果需要的话，表单的“计划”部分下面会显示其他字段。按需填写这些字段。
6. 完成所需配置后，点击**保存**。

   要退出而不创建配置文件，请点击**取消**。

要编辑现有计划配置文件，请执行以下步骤。

1. 在**主页**窗口中，点击全局工具栏右上角的**作业中心**图标。选择**计划配置文件**选项卡。
2. 确定需要编辑的配置文件。可使用上述过滤器来帮助您识别正确的配置文件。
3. 查看表格最右侧的**操作**列。点击**编辑**图标。
4. 使用提供的表单更新配置文件。请注意，您无法更改配置文件的作业类型。
5. 完成所需更改后，点击**保存**。要放弃更改，请点击**取消**。

要删除现有计划配置文件，请执行以下步骤。

1. 在**主页**窗口中，点击全局工具栏右上角的**作业中心**图标。选择**计划配置文件**选项卡。
2. 确定要删除的配置文件。可使用上述过滤器来帮助您识别正确的配置文件。
3. 点击**操作**列中的**删除**图标以删除配置文件。

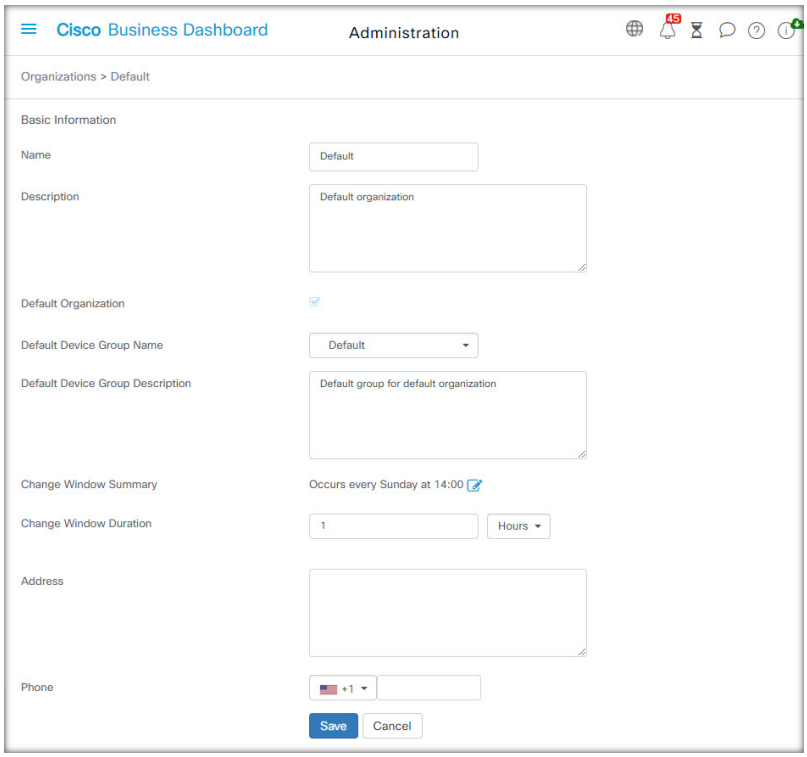
要查看与计划配置文件关联的所有作业，请执行以下步骤。

1. 在**主页**窗口中，点击全局工具栏右上角的**作业中心**图标。选择**计划配置文件**选项卡。
2. 确定要搜索其关联作业的配置文件。可使用上述过滤器来帮助您识别正确的配置文件。
3. 点击**操作**列中的**查看作业**图标。该视图切换到包含所显示筛选项的**作业**选项卡，以仅显示与此配置文件关联的作业。

管理变更窗口

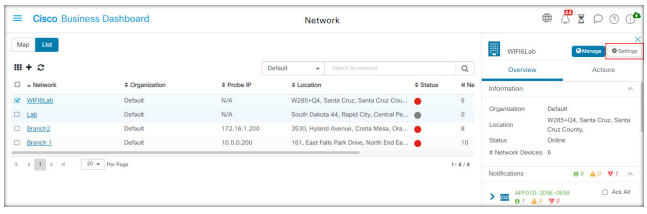
变更窗口是可用于在不影响用户的情况下执行可能中断网络的操作的时段。变更窗口通常定义为在周末或夜间的非工作时间发生，但可以根据组织的要求设置为任何时间。变更窗口是一个周期性间隔，在 Cisco Business Dashboard 中默认为每周周日凌晨 2:00 至凌晨 3:00 发生。

变更窗口在组织级别定义，但如果需要，可以在网络级别覆盖该设置。要修改组织的变更窗口，请执行以下步骤。



1. 导航到**管理** > **组织**。
2. 选择与要修改的组织对应的单选按钮，然后点击**编辑**图标。
3. 点击**变更窗口摘要**参数旁边的**编辑**图标。系统将打开一个弹出窗口，您可以在其中更改变更窗口的发生频率以及窗口应启动的日期和时间。选择适当的时区后，您可以将开始时间指定为组织的本地时间，从而降低出错的可能性。更新完成后，点击**保存**以关闭该弹出窗口。
4. 您还应设置变更窗口的持续时间。变更窗口可以分钟或小时为单位指定，且持续时间必须至少为 30 分钟。
5. 完成所需更改后，点击**保存**。要放弃更改，请点击**取消**。

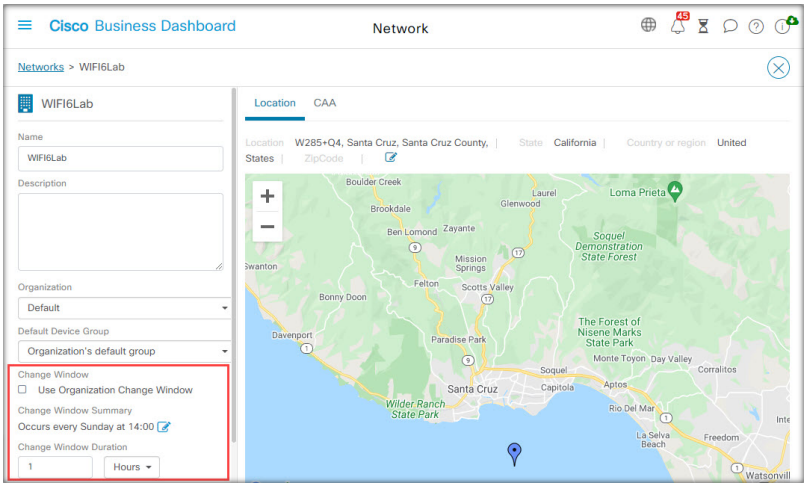
要为特定网络设置与组织的变更窗口不同的变更窗口，请执行以下步骤。



1. 导航到**网络**页面。
2. 选中要修改的网络的复选框，然后在显示的**网络信息**面板中点击**设置**。
3. 点击位于网络名称左上角的**编辑**图标。

4. 在**变更窗口**标题下，取消选中**使用组织变更窗口**复选框。
5. 点击**变更窗口摘要**参数旁边的**编辑**图标。系统将打开一个弹出窗口，您可以在其中更改变更窗口的发生频率以及窗口应启动的日期和时间。选择适当的时区后，您可以将开始时间指定为组织的本地时间，从而降低出错的可能性。更新完成后，点击**保存**以关闭该弹出窗口。
6. 您还应设置变更窗口的持续时间。变更窗口可以分钟或小时为单位指定，且持续时间必须至少为 30 分钟。
7. 完成所需更改后，点击**确定**。要放弃更改，请点击**取消**。

要将网络配置为使用组织变更窗口，请执行以下步骤。



1. 导航到**网络**页面。
2. 选中要修改的网络的复选框，然后在显示的**网络信息**面板中点击**设置**按钮。
3. 点击位于网络名称左上角的**编辑**图标。
4. 在**变更窗口**标题下，选中**使用组织变更窗口**复选框。
5. 完成所需更改后，点击**确定**。要放弃更改，请点击**取消**。

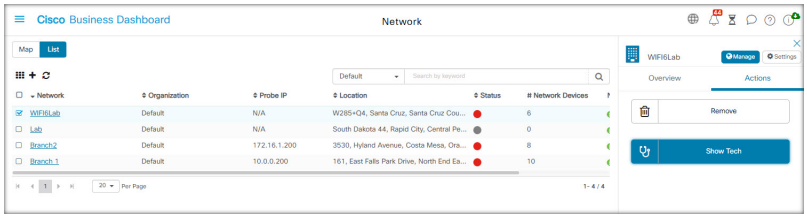
第 15 章

故障排除

本章包含以下各节：

捕获网络诊断信息

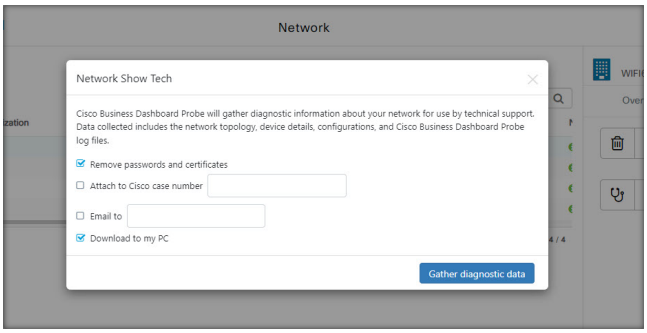
通过**网络显示技术**功能，您可以用某种形式轻松捕获网络诊断信息，以便日后进行分析或发给支持工程师。**网络显示技术**可以从Dashboard用户界面生成，也可以直接从Probe用户界面生成，以便对Dashboard 与 Probe 的连接问题进行故障排除。要捕获**网络显示技术**信息，请执行以下步骤。



1. 导航到**网络**，然后点击复选框以选择您要为其收集诊断信息的网络。
2. 选择**操作**选项卡，然后点击**显示技术**。

   或者，登录到 Probe 用户界面并导航到**故障排除** > **网络显示技术**。
3. 使用复选框可控制是否从设备配置中排除密码和凭证，以及应将诊断信息发送至何处。可提供以下选项：
   - 将诊断信息关联至现有的思科支持案例。为此，请在提供的字段中输入案例编号。
   - 使用邮件发送诊断信息。在提供的字段中输入邮件地址的逗号分隔列表。
   - 将诊断信息下载至您的 PC。

   如果要从Probe生成**网络显示技术**，则不提供通过邮件发送诊断信息或将其添加到支持案例的选项。您必须将诊断信息下载到您的 PC 上。
4. 点击**收集诊断数据**。



诊断信息将以 zip 文件形式提供，其中包括帮助导航所收集数据的基本网页。要访问数据，请执行以下步骤。

1. 将诊断信息文件解压缩至您的 PC。
2. 使用 Web 浏览器打开目录中的 index.html 文件。

管理 Probe 日志设置

Probe **日志设置**可以从 Dashboard 用户界面进行管理，也可以直接从 Probe 用户界面进行管理，以便排除 Dashboard 与 Probe 的连接问题。日志设置用于控制 Probe 在其日志文件中保留的信息。

此信息对于诊断 Cisco Business Dashboard 问题的支持工程师非常重要。

要更改给定网络的日志设置，请执行以下步骤。

1. 打开**网络**页面，然后点击要更改设置的网络旁边的复选框。
2. 点击网络概述面板顶部的**设置**按钮。
3. 选择**日志设置**选项卡。

   或者，登录 Probe 用户界面并导航到**管理** > **日志设置**。

可用的设置包含以下参数：

表 *17:* 日志设置

字段	说明
日志级别	应记录的详细信息级别。 • **错误** - 仅限错误级别消息 • **警告** - 警告和错误 • **信息**（默认）- 参考消息及以上类型 • **调试** - 所有消息，包括低级别调试消息

字段	说明
日志模块	应记录消息的模块。 • **全部（默认）** - 所有模块 • **报障代理** - Probe 和 Dashboard 之间的通信 • **发现** - 设备发现和拓扑发现事件 • **北向** - Dashboard 和 Probe 之间的通信 • **服务** - 北向和南向之间的消息转换 • **南向** - Probe 和设备之间的低电平通信 • **系统** - 任何其他模块都不包含的核心系统进程 您可以根据需要选择多个模块。

Probe日志文件包含在**网络显示技术**内容中。有关**网络显示技术**选项的更多详细信息，请参阅捕获网络诊断信息，第 139 页部分。

第 16 章

常见问题解答

本章解答有关 Cisco Business Dashboard功能的常见问题和可能出现的问题。涉及的主题分为以下几类：

一般常见问题

问： Cisco Business Dashboard 支持哪些语言？

答： Cisco Business Dashboard 已翻译为以下语言：

- 中文
- 英语
- 法语
- 德语
- 日语
- 西班牙语

发现常见问题

问： Cisco Business Dashboard 使用哪些协议来管理我的设备？

答： Cisco Business Dashboard 使用多种协议来发现和管理网络。具体针对某个特定设备使用哪种协议视设备类型而异。

使用的协议包括：

- 多播 DNS 和 DNS 服务发现协议（亦称 *Bonjour*，请参阅 *RFC 6762* 和 *6763*）
- 思科发现协议 (CDP)
- 链路层发现协议（请参阅 *IEEE* 规格 *802.1AB*）
- 简单网络管理协议 (SNMP)
- RESTCONF（请参阅 *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/*）
- 专有 Web 服务 API

问： Cisco Business Dashboard 如何发现我的网络？

答： Cisco Business Dashboard Probe 通过侦听 CDP、LLDP 和 mDNS 通告构建网络中的初始设备列表。然后，Probe 将通过支持的协议连接到每个设备并收集其他信息，例如 CDP 和 LLDP 相邻表、MAC 地址表以及关联设备列表。这些信息用于标识网络中的其他设备，该过程将重复执行，直到发现所有设备。

问： Cisco Business Dashboard 是否会执行网络扫描？

答： Cisco Business Dashboard 不会主动扫描更广泛的网络。Probe 会使用 ARP 协议扫描其直接连接的 IP 子网，但不会尝试扫描任何其他地址范围。Probe 还会在标准端口上测试每个发现的设备是否存在 Web 服务器和 SNMP 服务器。

配置常见问题

问： 当发现新设备时会发生什么情况？新设备的配置是否会发生更改？

答： 新设备将被添加到默认设备组中。如果已对默认设备组分配了配置文件，系统会对新发现的设备应用该配置。

问： 当我将设备从一个设备组移到另一个设备组时，会发生什么情况？

答： 与当前应用于原始设备组而未应用于新设备组的配置文件相关联的任何 VLAN 或 WLAN 配置都将被删除，而与应用于新组而未应用于原始组的配置文件相关联的 VLAN 或 WLAN 配置将被添加到设备中。系统配置设置将被应用于新组的配置文件覆盖。如果未对新组定义系统配置文件，则设备的系统配置不会改变。

安全注意事项常见问题

问： Cisco Business Dashboard 所需的端口范围和协议是什么？

答： 下表列出了 Cisco Business Dashboard 使用的协议和端口：

表 *18: Cisco Business Dashboard* - 协议和端口

端口	方向	协议	使用方式
TCP 22	入站	SSH	通过命令行访问 Dashboard。默认情况下，思科虚拟机映像上禁用 SSH。
TCP 80	入站	HTTP	通过 Web 访问 Dashboard。重定向到安全 Web 服务器（端口 443）。
TCP 443	入站	HTTPS 多路复用 TCP	通过安全 Web 访问 Dashboard。 Probe 与 Dashboard 之间的通信。
UDP 1812	入站	RADIUS	对用户访问进行身份验证时，通过设备访问 Dashboard。
TCP 50000 - 51000 （从 Microsoft Azure 市场部署的系统使用 TCP 50000-50049）	入站	HTTPS	远程访问设备。 此范围可使用“系统”>“平台设置”页面进行控制。
UDP 53	出站	DNS	域名解析。
UDP 123	出站	NTP	时间同步。
TCP 443	出站	HTTPS	访问思科 Web 服务以获取软件更新、支持状态和生命周期终止通知等信息。访问操作系统和应用更新服务。
UDP 5353	出站	mDNS	面向通告 Dashboard 的本地网络的多播 DNS 服务通告。

问: Cisco Business Dashboard Probe 所需的端口范围和协议是什么？

答: 下表列出了 Cisco Business Dashboard Probe 使用的协议和端口：

表 *19: Cisco Business Dashboard* - 协议和端口

端口	方向	协议	使用方式
TCP 22	入站	SSH	通过命令行访问 Probe。默认情况下，思科虚拟机映像上禁用 SSH。
TCP 80	入站	HTTP	通过 Web 访问 Probe。重定向到安全 Web 服务器（端口 443）。
TCP 443	入站	HTTPS	通过安全 Web 访问 Probe。

端口	方向	协议	使用方式
UDP 5353	入站	mDNS	来自本地网络的多播 DNS 服务通告。用于发现设备。
UDP 53	出站	DNS	域名解析。
UDP 123	出站	NTP	时间同步
TCP 80	出站	HTTP	在不启用安全 Web 服务的情况下管理设备。
UDP 161	出站	SNMP	管理网络设备。
TCP 443	出站	HTTPS 多路复用 TCP	启用安全 Web 服务来管理设备访问思科 Web 服务以获取软件更新、支持状态和生命周期终止通知等信息。 访问操作系统和应用更新服务。 Probe 与 Dashboard 之间的通信。
UDP 5353	出站	mDNS	面向通告 Probe 的本地网络的多播 DNS 服务通告。

问: Cisco Business Dashboard 会与哪些思科服务器通信？通信的目的是什么？

答: 下表列出了会与 Cisco Business Dashboard 通信的思科服务器及通信目的：

表 ***20: Cisco Business Dashboard*** **-** 思科服务器

主机名	用途
tools.cisco.com	出于智能许可目的，用于验证智能账户中是否有充足的许可证可供 Dashboard 使用。仅当 Dashboard 实例已注册思科智能许可功能时，才会使用此服务器。
api.cisco.com	用于检索软件更新信息和产品生命周期信息。仅当“系统”>“隐私设置”中启用了软件更新或生命周期报告功能时，才会使用此服务器。
dl.cisco.com download-ssc.cisco.com	用于从思科下载软件更新文件。 仅当“**系统**”>“**隐私设置**”中启用了软件更新，且用户对网络设备或 Cisco Business Dashboard 执行更新操作时，才会使用这些服务器。
cloudsso.cisco.com	用于在 Cisco Business Dashboard 与 api.cisco.com 建立通信前执行身份验证。仅当“**系统**”>“**隐私设置**”中启用了软件更新或生命周期报告功能时，才会使用此服务器。

主机名	用途
ciscoactiveadvisor.cisco.com	用于收集产品改进数据以及支持“CAA 上传”功能。当“**系统**”>“**隐私设置**”中选择了产品改进选项，或者在使用“CAA 上传”功能时，才会使用此服务器。
www.cisco.com	用于检索根 CA（证书颁发机构）签名证书的更新。出于保护网络通信的目的，思科和第三方服务使用这类证书来验证 X509 证书。

问: Cisco Business Dashboard 需要使用哪些进程和系统服务？

答: 下表列出安装了 Cisco Business Dashboard 的思科服务器所使用的进程和系统服务：

表 *21: Cisco Business Dashboard* - 进程和系统服务

进程	补充说明
Dashboard 必要的进程	
/usr/lib/jvm/java-8-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	Dashboard 主应用程序
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	Web 服务器
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod /usr/lib/postgresql/xx/bin/postgres postgres: xx/main:	数据库服务
/bin/bash /usr/lib/ciscobusiness/dashboard/bin/freeradiussvc /usr/lib/ciscobusiness/dashboard/bin/freeradius	用户身份验证服务
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	内存缓存服务
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	消息代理
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	组播 DNS 通告

进程	补充说明
Dashboard 必要的进程	
/bin/sh /usr/share/contuit/contuit /bin/sh /usr/share/contuit-computations/contuit-computations /bin/sh /usr/share/contuit-monorepo/contuit-mop /bin/sh /usr/share/contuit-scheduler/contuit-scheduler /bin/sh /usr/share/contuit-shim/contuit-shim	仅在启用了外部应用程序集成时需要
Dashboard 必要的系统服务	
/usr/sbin/rsyslog	日志记录服务
/usr/sbin/cron	计划服务
systemd-timesyncd	时间服务
avahi-daemon	组播 DNS 侦听程序

问: Cisco Business Dashboard Probe 需要使用哪些进程和系统服务？

答: 下表列出安装了 Cisco Business Dashboard Probe 的思科服务器所使用的进程和系统服务：

表 *22: Cisco Business Dashboard* - 进程和系统服务

进程	补充说明
Probe 必要的进程	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	Probe 主应用程序
/usr/lib/ciscobusiness/probe/bin/fpscan	设备扫描工具
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	组播 DNS 通告
nginx	Web 服务器 当 Probe 托管在 Dashboard 服务器上时，会使用 Dashboard 的 Web 服务器
Probe 必要的系统服务	
/usr/sbin/rsyslogd	日志记录服务
/usr/sbin/cron	计划服务

进程	补充说明
Probe 必要的进程	
systemd-timesyncd	时间服务
avahi-daemon	组播 DNS 侦听程序
lldpd	LLDP 邻居发现

问: Cisco Business Dashboard 与 Probe 之间通信的安全状况如何？

答: Dashboard 与 Probe 之间的所有通信均使用 TLS 1.2 会话加密，使用客户端和服务器证书进行身份验证。会话由 Probe 向 Dashboard 发起。首次建立 Dashboard 与 Probe 之间的关联时，用户必须通过 Probe 登录到 Dashboard。

问: Cisco Business Dashboard 是否存在可访问我的设备的“后门”？

答: 不存在。当 Cisco Business Dashboard 发现支持的设备时，会尝试使用该设备的出厂默认凭证访问该设备，凭证中用户名和密码均为：`cisco`，或者使用 SNMP 社区：`public` 作为凭证。如果设备配置已与默认值不同，则用户需要向 Cisco Business Dashboard 提供正确的凭据。

问: Cisco Business Dashboard 中存储的凭据的安全状况如何？

答: 访问 Cisco Business Dashboard 的凭据已使用 SHA512 算法执行不可逆的散列处理。设备和其他服务（例如 **Cisco Active Advisor**）使用 AES-128 算法进行可逆的加密。

问: 如何找回丢失的 Web UI 密码？

答: 如果 Web UI 的所有管理员账户密码丢失，可登录 Probe 控制台并运行 **cbdprobe recoverpassword** 工具，或登录 Dashboard 控制台并运行 **cisco-business-dashboard recoverpassword** 工具来找回密码。此工具会将账户 cisco 的密码重置为默认值 cisco；如果已删除账户 cisco，系统会重新创建该账户及默认密码。下面是使用此工具恢复密码的命令示例。

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

注释 使用适用于 AWS 的 Cisco Business Dashboard 时，密码将设置为 AWS 实例 ID。

问: 虚拟机引导加载程序的默认用户名和密码是什么？

答: 虚拟机引导加载程序默认凭证的用户名是 **root**，密码是 **cisco**。可以通过运行 config_vm 工具并在系统询问您是否要更改引导加载程序密码时回答 yes 以更改这些密码。

问: Dashboard 如何对网络接入设备进行身份验证？

答: Dashboard 使用两个级别的身份验证。

- 级别一：当使用 NAT 时，将传入请求的源 IP 地址与 Dashboard 管理的网络的外部 IP 地址进行比较，或者当未使用 NAT 时，与网络的内部子网进行比较。
- 级别二：为每个组织创建一个唯一的随机 RADIUS 密钥，网络访问设备在其请求中必须使用该密钥。

远程访问常见问题

问: 当从 Cisco Business Dashboard 连接到设备的管理接口时，会话是否安全？

答: Cisco Business Dashboard 在设备与用户之间建立远程会话隧道。Probe 和设备之间使用的协议取决于终端设备配置，但是如果启用了安全协议，Cisco Business Dashboard 将始终使用安全协议建立会话（例如，HTTPS 将优先于 HTTP）。如果用户正在通过 Dashboard 连接到设备，则会话将通过加密隧道传递（就像在 Dashboard 与 Probe 之间传递一样），无论设备上启用何种协议。用户的 Web 浏览器和 Dashboard 之间的连接将始终为 HTTPS。

问: 为什么在我打开与另一台设备的远程访问会话时，我与当前设备的远程访问会话会立即退出？

答: 当您通过 Cisco Business Dashboard 访问设备时，浏览器会将每个连接视为来自同一个 Web 服务器 (Dashboard)，所以会将每部设备的 Cookie 提供给所有其他设备。如果多台设备使用相同的 Cookie 名称，则一台设备的 Cookie 可能会被其他设备覆盖。对于会话 Cookie，这种情况最常出现，并导致 Cookie 仅对最新访问的设备有效。而使用相同 Cookie 的所有其他设备则会将该 Cookie 视为无效，并退出会话。

问: 为什么我的远程访问会话失败并显示如下错误？**访问错误：请求实体过大 HTTP 标头字段超过支持的大小**

答: 在与不同设备执行许多远程访问会话后，浏览器会为 Dashboard 域存储大量 Cookie。要解决此问题，请使用浏览器控件清除该域的 Cookie，然后再重新加载页面。

软件更新常见问题

问: 如何确保 Dashboard 操作系统是最新的？

答: Dashboard 使用特定版本的 Ubuntu Linux 作为操作系统。程序包和内核可使用标准 Ubuntu 进程进行更新。例如，要执行手动更新，可使用 cisco 用户身份登录控制台，并输入命令 `sudo apt-get update` 和 `sudo apt-get upgrade`。请不要将系统升级到新版 Ubuntu，建议不要安装思科提供的虚拟机映像中未包含的其他程序包，或作为最低 Ubuntu 安装版本组成部分安装的程序包。

问: 如何在 Dashboard 上更新 Java？

答: Cisco Business Dashboard 使用 Ubuntu 存储库中的 OpenJDK 程序包。在更新核心操作系统的过程中，OpenJDK 将自动进行更新。

问: 如何确保 Probe 操作系统是最新的？

答: Cisco Business Dashboard 使用特定版本的 Ubuntu Linux 作为操作系统。程序包和内核可使用标准 Ubuntu 进程进行更新。例如，要执行手动更新，可使用 cisco 用户身份登录控制台，并输入

命令 `sudo apt-get update` 和 `sudo apt-get upgrade`。请不要将系统升级到新版 Ubuntu，建议不要安装思科提供的虚拟机映像中未包含的其他程序包，或作为最低 Ubuntu 安装版本组成部分安装的程序包。

问： 使用 Raspberry Pi 时，如何确保 Probe 操作系统是最新的？

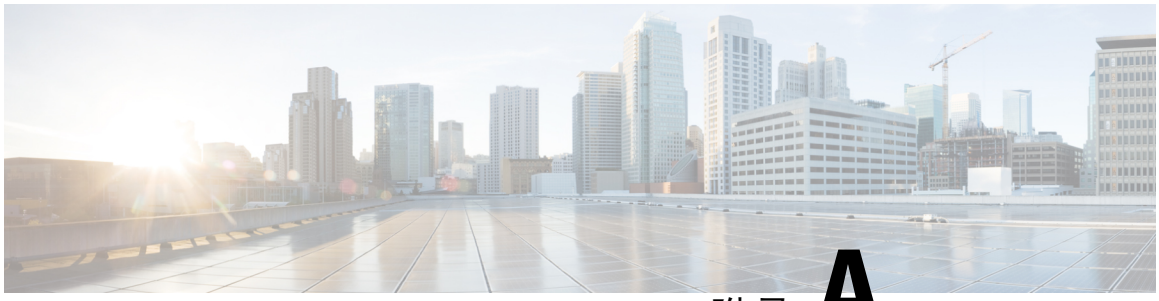
答： Raspbian 软件包和内核可以使用用于基于 Debian 的 Linux 发行版的标准流程进行更新。例如，要执行手动更新，可使用 cisco 用户身份登录控制台，并输入命令 `sudo apt-get update` 和 `sudo apt-get upgrade`。系统不应升级到新的 Raspbian 主要版本。建议除了作为 Raspbian 发行版“Lite”版本安装的和 Probe 安装程序添加的软件包之外，不要安装其他软件包。

问： 我发现 Cisco Business Dashboard 2.3.0 增加了对 Ubuntu 20.04 (Focal Fossa) 的支持。如果我已将 Dashboard 升级到 2.3.0，可否把我的操作系统从 Ubuntu 16.04 升级到 Ubuntu 20.04？

答： 很遗憾，由于这两个版本的操作系统差异过多，因此无法执行免重装升级。如果您当前使用的系统运行的是 Ubuntu 16.04，而且您已将 Dashboard 升级到版本 2.3.0，请在**系统** > **备份**页面中备份 Dashboard。然后，您可以使用 Ubuntu 20.04 重新构建 Dashboard，或者在运行 Ubuntu 20.04 的系统中安装新的 Dashboard。最后，请在新 Dashboard 中恢复旧 Dashboard 的备份数据。

问： 我发现 Cisco Business Dashboard 2.3.0 增加了对 Ubuntu 20.04 (Focal Fossa) 的支持。如果我已将 Dashboard 升级到 2.3.0，可否把我的操作系统从 Ubuntu 16.04 升级到 Ubuntu 20.04？

答： 很遗憾，由于这两个版本的操作系统差异过多，因此无法执行免重装升级。如果您当前使用的系统运行的是 Ubuntu 16.04，而且您已将 Dashboard 升级到版本 2.3.0，请在**系统** > **备份**页面中备份 Dashboard。然后，您可以使用 Ubuntu 20.04 重新构建 Dashboard，或者在运行 Ubuntu 20.04 的系统中安装新的 Dashboard。最后，请在新 Dashboard 中恢复旧 Dashboard 的备份数据。



附录 A

附录 A：管理配置模板

本附录包含以下部分：

管理配置模板

当有多个设备具有非常相似的配置要求时，可以使用配置模板，其中包含少量参数，而每个设备需要不同的参数。例如，网络可以为所有交换机使用相同的配置，只是每台交换机都有唯一的主机名和管理 IP 地址。配置模板允许您有一个包含所有公共配置的配置文件，并用占位符表示需要具有唯一性的配置元素。

配置模板包含两个部分 - 配置本身，以及元数据，该元数据控制在创建设备记录时如何在用户界面中显示占位符。以下部分将详细介绍这些内容。

配置语法

配置模板的配置部分是文本文档，与常规设备配置非常相似。在创建配置模板时，建议的方法是从已配置有模板应启用的功能和设置的示例设备获取的配置备份开始。配置模板与设备配置的不同之处在于，设备特定的参数（例如主机名）将替换为占位符。

创建新设备记录时，系统将显示一个表单，允许您为配置模板中的每个占位符提供正确的值。这些值将与配置模板合并，以生成发送到设备的实际配置。

注释 在将配置发送到设备时，占位符值将与配置模板合并。这意味着，如果在设备连接到 Manager 之前更改了任何系统变量，则最终的设备配置可能与预览中所示的配置有所不同。

配置将创建为 Mustache 模板 *https://mustache.github.io/*。Mustache 允许使用各种占位符（在 Mustache 文档中称为标签），包括：

附录 A：管理配置模板

- 简单变量，其中占位符将替换为设备记录中指定的值。简单变量的形式为 **{{name}}**。
- 代码块，即用占位符包围的整块配置，也可以选择包括其他占位符。代码块的内容可以从最终配置中排除，也可以包含在最终配置中一次，或重复多次。

  此类占位符的行为由模板中的元数据和用户在创建设备记录时提供的值定义。

  代码块的形式为 **{{#name}}…{{/name}}**，其中第一个标签标记代码块的开始，第二个标签标记代码块的结束。
- 注释可用于记录配置模板。注释的形式为 {{! **这是注释** }}。

以下是简单模板的示例：

```
!
hostname {{hostname}}
!
{{! Insert a list of VLANs}}
{{#vlans}}
interface vlan {{vlan-id}}
 name {{vlan-name}}
!
{{/vlans}}
```

在本示例中，有几个不同的占位符：

- **{{hostname}}** 是一个简单变量。它将替换成设备记录中为主机名设置的值。
- 在主机名配置之后放置注释。注释不会包含在发送给设备的配置中。
- **{{#vlans}}…{{/vlans}}** 是本示例中用于保存各个 VLAN 的列表的代码块。对于设备记录中定义的每个 VLAN，将在设备配置中创建此容器内容的副本。
- **{{vlan-id}}** 和 **{{vlan-name}}** 都是简单变量，但它们包含在 {{#vlans}} 列表中。创建设备记录时，您可以为**{{vlan-id}}** 和 **{{vlan-name}}** 指定多个值，用于生成创建每个 VLAN 所需的配置。

有关 Mustache 语法的更多详细信息，请参阅 Mustache 手册页面，网址为 *https://mustache.github.io/mustache.5.html*。

模板元数据

每个配置模板均包含元数据，描述在创建设备记录时应如何向用户呈现每个占位符。使用模板编辑器创建模板时会生成这种元数据。

在您创建或编辑配置模板时，系统将显示模板编辑器，其中左侧显示配置本身，右侧显示一个表单，可用于为每个占位符设置元数据。

配置中的每个占位符以及以下控件均显示在右侧：

- **必填**复选框。此控件用于确定用户是否必须为此占位符提供值。
- **类型**下拉列表。通过此列表，可以选择占位符的类型，这将控制如何向用户显示占位符。
- **标题**。这可用于为 GUI 上的参数提供更易理解的名称。如果没有为占位符指定标题，则显示占位符本身。

附录 A：管理配置模板

- **编辑**图标。某些类型有更多可用于控制显示的设置。例如，可以将字符串占位符进一步细化为IP 地址或URL，如果输入的文本格式不正确，则输入表单将显示错误。还可以根据系统信息而不是用户输入来设置某些类型。有关详细信息，请参阅下面的“系统和动态变量”。
- **上移/下移**控件。利用这些箭头可以更改向用户显示占位符的顺序。占位符可根据对用户最有意义的方式（而非它们在配置中出现的顺序）进行分组。

模板编辑器还提供预览功能，可用于提供示例，说明创建和编辑设备记录时如何向用户显示占位符表单。

占位符类型

可用的占位符类型如下：

- **字符串** - 此类占位符将在 GUI 中显示为简单的文本输入框。
- **整数** - 整数显示为带有控件的文本输入框，其中控件用于增加或减少所显示数字的值。在此字段中只能输入数字。
- **布尔值** - 布尔值占位符在 GUI 中显示为复选框。如果选中此复选框，则会将占位符设置为字符串值“true”。如果未选中此复选框，则值为“false”。代码块也可以指定为布尔值，在这种情况下，仅当选中代码块的复选框时，才会包含代码块中所含的配置。
- **容器** - 容器类型可用于对表单中的其他占位符进行分组。
- **列表** - 列表是配置的容器或代码块，可在生成的配置文件中重复多次。当为列表中的占位符生成表单元素时，会添加其他控件用以添加或删除列表中的元素。

除了上面列出的简单类型之外，还可以通过点击**编辑**图标进一步细化字符串变量。可用的选项包括：

- 为占位符指定默认值。
- 为字符串占位符设置最小和/或最大长度。
- 指定可以选择的预定义选项列表（使用“枚举”选项）。
- 将字符串的格式限制为主机名、URI、IPv4 地址或 IPv6 地址之一。如果可能要输入大量内容，也可以将字符串指定为文本区域。

系统和动态变量

占位符不仅可以从用户输入中获取值，还可以从系统中定义的参数中获取值。系统变量是为Manager本身定义的参数，例如 Manager IP 地址。

通过设置占位符以从系统变量中获取值，Manager 可将该值插入到配置中，无需任何用户干预。一些更复杂的部署可能需要用户输入才能使系统变量正常工作。有关更多详细信息，请参阅管理平台设置，第 108 页。

动态变量与系统变量相似，但动态变量是基于登录用户或设备所属设备组之类的信息动态生成的值。系统和动态变量用于允许模板在设备和系统之间更具可移植性。

创建配置模板

推荐的创建配置模板方法是，首先使用所需的设置配置适当类型的网络设备，然后备份设备配置，并将其上传到 Manager 以用作起点。

或者，可使用“另存为”功能创建现有模板的副本。无论采用哪种方式，从现有配置起，可帮助您减少创建模板所花费的时间，并且还可以减少实现所需结果所需的修订次数。

创建新模板时，需要指定模板所属的组织以及模板可以使用的产品 ID (PID)。产品 ID 可以包含 ***'s** 和 **?'s** 作为通配符。

完成启动配置的创建后，可使用以下过程对其进行更新：

1. 导航到 **Network Plug and Play** > **配置**：
2. 选择配置并点击**编辑**图标，可在模板编辑器中打开启动配置。

   系统将显示模板编辑器，并在文本编辑器窗口的左侧显示初始配置文件。文本编辑器支持许多常见的编辑功能，包括搜索、替换和多个光标操作键序列。有关命令列表，请参阅下表。
3. 根据配置语法，第 153 页中的说明，通过插入占位符来修改配置。每次插入新占位符时，都会在右侧表单中添加对应的条目。
4. 使用右侧的表单修改与每个占位符相关联的元数据，以确保占位符以最适当的方式呈现给用户。有关指定元数据的更多详细信息，请参阅上面的管理配置模板，第 153 页。您可以使用“预览”功能，查看创建设备记录时表单将如何呈现给用户。
5. 重复步骤 3 和 4，直到为所有应在设备之间有所不同的配置参数创建占位符。
6. 完成模板并且觉得满意后，点击**保存**。

注释 每次保存模板时，都会创建新版本的模板。模板的较旧版本将保留在 Manager 中，除非您显式删除这些模板。将模板分配给设备后，将分配模板的特定版本（默认情况下为最新版本）。创建新版本时，现有设备将继续使用在创建时分配的版本。当前分配给设备的模板版本可能不会被删除。

表 *23:* 常用编辑器命令

功能	说明	键绑定	
		PC	**Mac**
全选	选择编辑器的全部内容。	Ctrl-A	Cmd-A
Kill Line	删除光标之后的行部分。如果仅包含空格，则该行末尾的换行符也会被删除。		Ctrl-K
删除行	删除光标下的整行，包括末尾的换行符。	Ctrl-D	Cmd-D

附录 A：管理配置模板

功能	说明	键绑定	
		PC	**Mac**
撤消	撤消上次更改。	Ctrl-Z	Cmd-Z
恢复	恢复上次撤消的更改。	Ctrl-Y	Shift-Cmd-Z Cmd-Y
Go Doc Start	将光标移到文档开头。	Ctrl-Home	Cmd-Up Cmd-Home
Go Doc End	将光标移到文档末尾。	Ctrl-End	Cmd-End Cmd-Down
Go 行开始	将光标移到行首。	Alt-Left	Ctrl-A
Go Line End	将光标移到行尾。	Alt-Right	Ctrl-E
更多缩进	缩进当前行或选定内容。	Ctrl-]	Cmd-]
减少缩进	减少缩进当前行或选定内容。	Ctrl-[	Cmd-[
查找		Ctrl-F	Cmd-F
查找下一个		Ctrl-G	Cmd-G
查找上一个		Shift-Ctrl-G	Shift-Cmd-G
更换		Shift-Ctrl-F	Cmd-Alt-F
全部替换		Shift-Ctrl-R	Shift-Cmd-Alt-F

附录 A：管理配置模板

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。