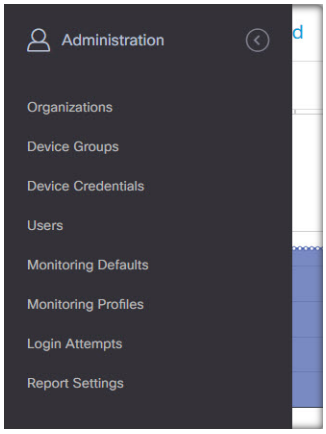
管理

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。

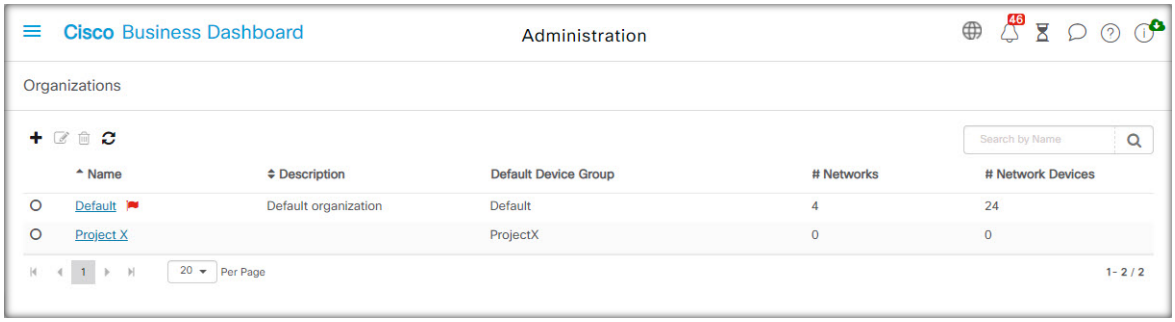
- **设备凭证** - 输入访问网络设备时要使用的凭证。
- **用户** - 定义用户对 Cisco Business Dashboard 的访问权限。
- **通知默认设置** - 更改 Cisco Business Dashboard 的默认通知行为。
- **登录尝试** - 提供所有用户访问 Cisco Business Dashboard 的日志。
- **报告设置** - 更改控制报告生成方式的设置。

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 10 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 9 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。

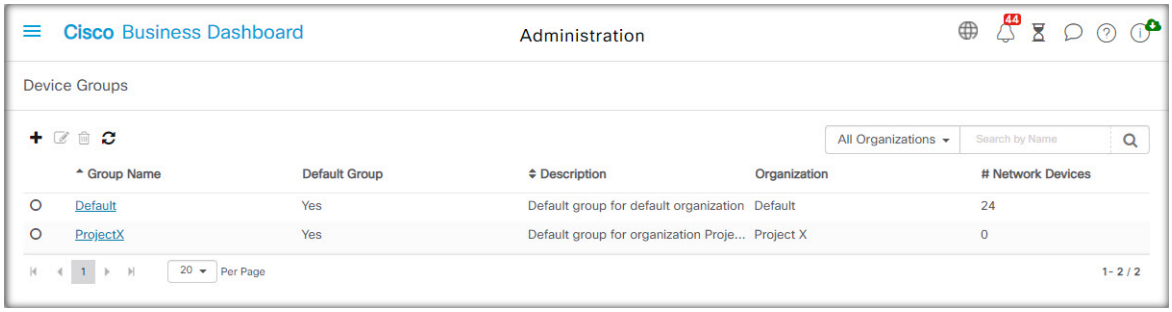
设备组

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 。

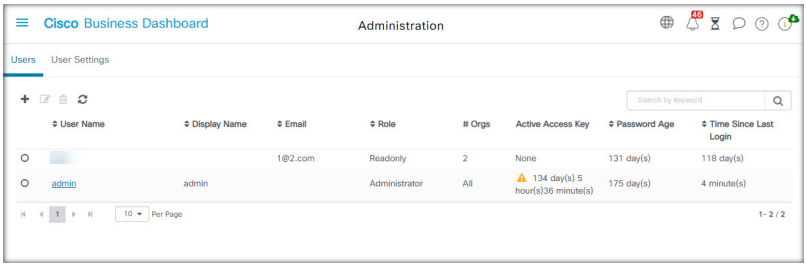
添加新凭证部分下方是一个表，表中显示 Probe 为之存储了有效凭证的各个设备的身份以及凭证的最后使用时间。要显示为设备存储的凭证，可点击设备旁边的**显示密码**图标。要重新隐藏凭证，可点击**隐藏密码**图标。您还可以使用表顶部的按钮显示和隐藏所有设备的凭证。另外，您还可以删除不再需要的凭证。要删除存储的凭证，请执行以下步骤。

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。

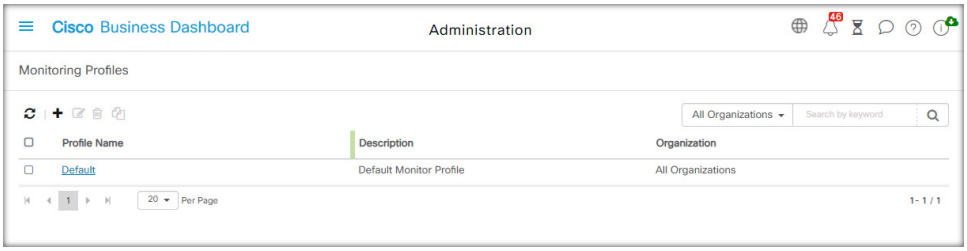
要更改在整个系统中应用的**监控配置文件**，请执行以下步骤。

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 2 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。
- 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。
- 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。

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 2 页和监控默认设置，第 9 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。

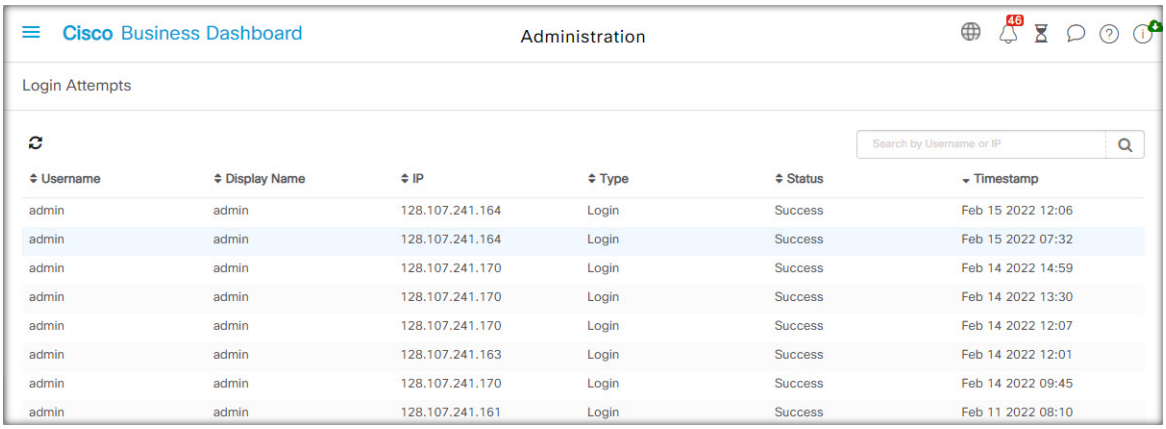
删除监控配置文件

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。



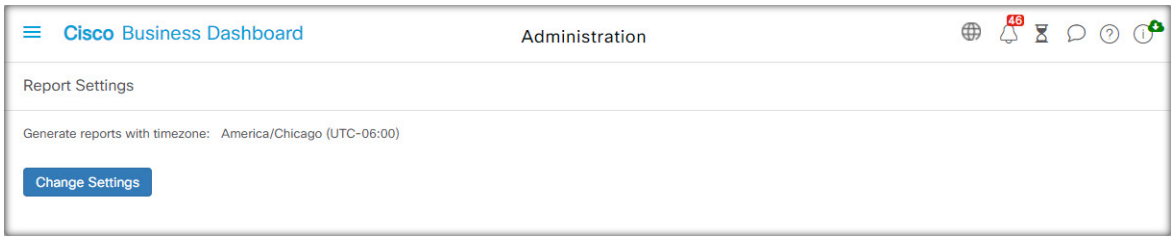
要查看这些日志，请导航到**管理 > 登录尝试**。该表将显示以下信息：

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。

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。