思科 ISA 3000 的报警

您可以配置思科 ISA 3000 设备上的报警系统，以便在出现不正常情况时发出警告。

关于报警

您可以将 ISA 3000 配置为在多种条件下发出报警。如果有任何条件与配置的设置不匹配，系统会触发报警，报警的报告方式为 LED、系统日志消息、SNMP 陷阱以及连接到报警输出接口的外部设备。默认情况下，触发的报警仅会发出系统日志消息。

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

ISA 3000 具有内部传感器、2 个报警输入接口以及 1 个报警输出接口。您可以将外部传感器（如门禁传感器）连接到报警输入接口，将外部报警设备（如蜂鸣器或指示灯）连接到报警输出接口。

报警输出接口是一个中继装置。根据报警条件，中继处于连接或断开状态。当处于连接状态时，连接至该接口的任何设备都将被激活。当中继处于断开状态时，会导致连接的任何设备都处于非活动状态。只要触发了报警，中继就会保持连接状态。

有关连接外部传感器和报警中继装置的信息，请参阅思科 ISA 3000 工业安全设备硬件安装指南。

报警输入接口

您可以将报警输入接口（或触点）连接到外部传感器，例如检测门是否打开的传感器。

每个报警输入接口都有一个对应的LED。这些LED负责传达每个报警输入的报警状态。您可以为每个报警输入配置触发器和严重性。除了 LED，您还可以配置触点来触发输出中继（用于激活外部报警），以发送系统日志消息和 SNMP 陷阱。

下表介绍与报警输入的报警条件所对应的LED状态。表中还介绍了启用这些报警输入响应时输出中继、系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	-	—	—
未触发任何报警	绿灯常亮	-	—	—
已激活报警	次要报警 - 红色长亮 重大报警 - 红色闪烁	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

报警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

报警输出接口充当一个中继，并且还有一个对应的 LED，用于传达连接到输入接口的外部传感器以及内部传感器（例如双电源和温度传感器）的报警状态。请配置哪些报警应该激活输出中继（如果有）。

下表介绍与报警条件对应的LED和输出中继的状态。表中还介绍了启用这些报警响应时系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	-	—	—
未触发任何报警	绿灯常亮	-	—	—
已激活报警	红色常亮	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

系统日志报警

默认情况下，触发任何报警时，系统都会发送系统日志消息。如果您不希望收到这些消息，可以禁用系统日志消息传递。

要让系统日志报警正常工作，您还必须启用诊断日志记录。选择**设备 (Device)** > **平台设置 (Platform Settings)**，添加或编辑分配给设备的 FTD 平台设置策略，并在**系统日志 (Syslog)** 页面上配置目标和设置。例如，您可以配置系统日志服务器、控制台日志记录或内部缓冲区日志记录。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 报警

您可以选择配置报警，将 SNMP 陷阱发送到 SNMP 服务器。要让 SNMP 陷阱报警正常使用，您还必须配置 SNMP 设置。

选择**设备 (Device)** > **平台设置 (Platform Settings)**，添加或编辑分配给设备的 FTD 平台设置策略，并在 **SNMP** 页面上启用 SNMP 并配置设置。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
报警触点 1	启用	关闭状态	次要	Disabled	Disabled	已启用
报警触点 2	启用	关闭状态	次要	Disabled	Disabled	已启用
冗余电源（在启用时）	启用	-	—	Disabled	Disabled	已启用
温度	为主温度报警启用（高阈值和低阈值的默认值分别为 92°C 和 -40°C） 为辅助报警禁用。	-	—	为主温度报警启用	为主温度报警启用	为主温度报警启用

报警的要求和必备条件

型号支持

ISA 3000 上的 威胁防御。

支持的域

任意

用户角色

管理员

配置 ISA 3000 的报警

请使用 FlexConfig 为 ISA 3000 配置报警。以下主题介绍如何配置不同类型的报警。

配置报警输入触点

如果您将报警输入触点（接口）连接到外部传感器，可以将触点配置为基于传感器的输入发出报警。事实上，如果触点关闭，即电流停止流经触点，系统会默认启用触点来发送系统日志消息。只有当默认设置不符合您的要求时，才需要配置触点。

报警触点的编号分别是 1 和 2，您需要了解如何连接物理引脚以配置正确的设置。单独配置每个触点。

过程

步骤 1 创建 FlexConfig 对象以配置警报输入联系人。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Configure_Alarm_Contacts。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置警报联系人所需的命令。以下步骤介绍了这些命令。

d) 配置报警触点的说明。

alarm contact {**1** | **2**} **description** *string*

例如，要将触点 1 的说明设置为“Door Open”，请输入以下命令：

```
alarm contact 1 description Door Open
```

e) 配置报警触点的严重性。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

您可以指定 **any** 更改所有触点的严重性，而不是配置一个触点。严重性控制与触点关联的 LED 指示灯的行为。

- **major**- LED 指示灯红色闪烁。
- **minor**- LED 指示灯红色长亮。这是默认值。
- **none**- LED 指示灯熄灭。

例如，要将触点 1 的严重级别设置为“Major”，请输入以下命令：

```
alarm contact 1 severity major
```

f) 配置报警触点的触发器。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

您可以指定 **any** 更改所有触点的触发器，而不是配置一个触点。触发器决定发出报警信号的电气条件。

- **open**- 触点的正常状态为闭合，即电流流经触点。如果触点变成打开状态，即电流停止流动，会触发警报。
- **closed**- 触点的正常状态为打开，即电流不通过触点。如果触点变成闭合状态，即电流开始流经触点，会触发警报。这是默认值。

例如，将门禁传感器连接到报警输入触点1，该触点的正常状态为没有电流流经报警触点（即打开）。如果门被打开，触点会变成闭合状态，电流将流经报警触点。您应将报警触发器设为关闭，以便当电流开始流动时，警报响起。

```
alarm contact 1 trigger closed
```

g) 配置触发报警触点时采取的操作。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

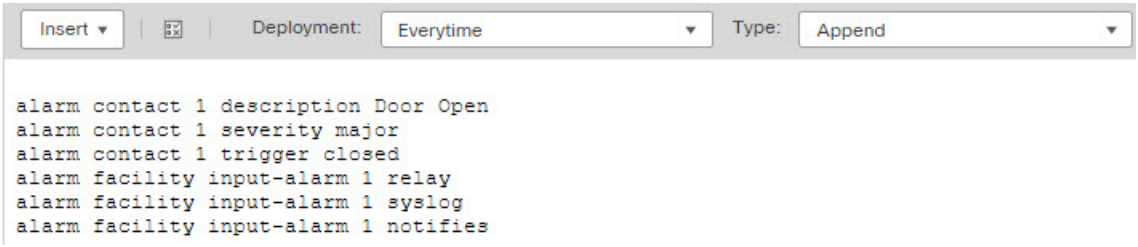
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

h) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

此对象正文应如下所示：



i) 单击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

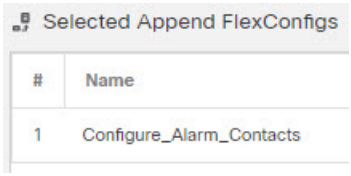
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择警报联系人 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 单击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于警报联系人命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

配置电源报警

ISA 3000 包含两个电源。默认情况下，系统在单电源模式下运行。但是，您可以配置系统在双电源模式下运行，其中第二个电源会在主电源发生故障时自动供电。启用双电源模式时，自动启用电源报警来发送系统日志警报，但您可以完全禁用警报，或同时启用 SNMP 陷阱或报警硬件中继。

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 创建 FlexConfig 对象以配置电源警报。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Power_Supply_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置电源警报所需的命令。以下步骤介绍了这些命令。

d) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

e) 配置触发电源报警时要采取的操作。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。
- **禁用** - 禁用电源报警。为电源报警配置的任何其他操作都无法运行。

例如，要启用电源报警的所有操作，请输入以下命令：

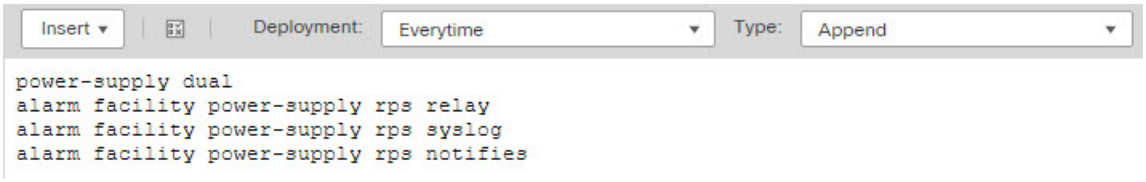
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

f) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

此对象正文应如下所示：



g) 单击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择电源警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。

d) 单击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于电源警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

您可以设置主要和辅助温度范围。如果温度低于低阈值，或超过高阈值，则触发报警。

默认对所有报警操作启用主温度报警：输出中继、系统日志和 SNMP。主要温度范围的默认设置为 -40°C 至 92°C。

默认情况下，禁用辅助温度报警。您可以将辅助温度范围设置为 -35°C 至 85°C。

由于辅助温度范围比主范围更严格，如果您设置辅助低温度或高温度，该设置将禁用对应的主要设置，即使您为主设置配置非默认值。您不能启用两个单独的高温度报警和两个单独的低温度报警。

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 创建 FlexConfig 对象以配置温度警报。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Configure_Temperature_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。

- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置温度警报所需的命令。以下步骤介绍了这些命令。

d) 配置可接受的温度范围。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度单位为摄氏度。主要报警的允许范围为 -40 至 92，这也是默认的范围。辅助报警的允许范围是 -35 到 85。低值必须小于高值。

例如，要设置更严格的 -20 至 80 温度范围（在辅助报警的允许范围内），请按如下所示配置辅助报警：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

e) 配置触发温度报警时要采取的操作。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。
- **通知** - 发送 SNMP 陷阱。

例如，要启用辅助温度报警的所有操作，请输入以下命令：

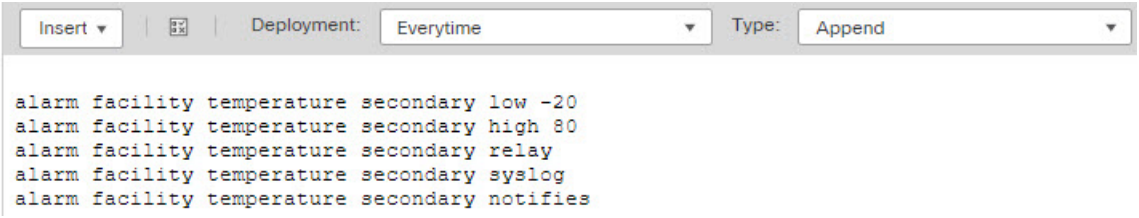
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

f) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

此对象正文应如下所示：



g) 单击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

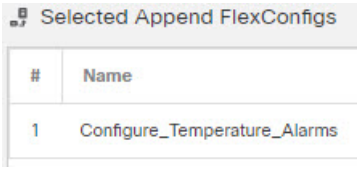
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择温度警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 单击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于温度警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

监控报警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

  显示每个可能的报警的当前配置。

- **show environment alarm-contact**

  显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

  显示有关已触发输出中继的报警信息。

- **show facility-alarm status** [**info** | **major** | **minor**]

  显示所有已触发报警的信息。您可以通过过滤 **major** 或 **minor** 状态来限制视图。**info** 关键字提供与不使用关键字时相同的视图。

监控报警系统日志消息

根据您配置的报警类型，您可能会看到以下系统日志消息。

双电源报警

- %FTD-1-735005：电源设备冗余正常
- %FTD-1-735006：电源设备冗余丢失

温度报警

在这些报警中，*Celsius* 将替换为设备上检测到的温度，以摄氏为单位。

- %FTD-6-806001：主要报警 CPU 温度高 *Celsius*
- %FTD-6-806002：CPU 高温主要报警已清除
- %FTD-6-806003：主要报警 CPU 温度低 *Celsius*
- %FTD-6-806004：CPU 低温主要报警已清除
- %FTD-6-806005：辅助报警 CPU 温度高 *Celsius*
- %FTD-6-806006：CPU 高温辅助报警已清除
- %FTD-6-806007：辅助报警 CPU 温度低 *Celsius*

- %FTD-6-806008：CPU 低温辅助报警已清除

报警输入触点报警

在这些报警中，*description* 是您所配置触点的说明。

- %FTD-6-806009：与 ALARM_IN_1 *alarm_1_description* 对应的报警已确定
- %FTD-6-806010：与 ALARM_IN_1 *alarm_1_description* 对应的报警已清除
- %FTD-6-806011：与 ALARM_IN_2 *alarm_2_description* 对应的警报已确定
- %FTD-6-806012：与 ALARM_IN_2 *alarm_2_description* 对应的报警已清除

关闭外部报警

如果您使用连接到报警输出的外部报警，并触发了报警，可以使用 **clear facility-alarm output** 命令从设备 CLI 关闭外部报警。此命令会断开输出引脚，同时关闭输出 LED。

报警历史记录

特性	最低 管理中心	最低 威胁防御	说明
思科 ISA 3000 系列的报警。	6.7	任意	已使用 FlexConfig 验证思科 ISA 3000 系列的警报配置。您应该能够在支持 FlexConfig 的旧版本中配置警报，但双电源警报除外。 支持的平台：ISA 3000 上的 Cisco Secure Firewall Threat Defense

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。