# 设备管理



# TACACS+ 设备管理

思科 ISE 支持设备管理通过使用终端访问控制器访问控制系统 (TACACS+) 安全协议控制，来控制和审计网络设备的配置。网络设备可以配置为向思科 ISE 查询对设备管理员操作所进行的身份验证和授权，并发送思科 ISE 的记账信息以记录操作。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。思科 ISE 管理员可以创建策略集，允许在设备管理访问服务的授权策略规则中选择 TACACS 结果（如命令集和外壳配置文件）。思科 ISE 监控节点可提供与设备管理相关的增强型报告。“工作中心”(Work Center) 菜单中包含所有设备管理页面，可作为 ISE 管理员的单一入手点。

思科 ISE 需要设备管理许可证才能使用 TACACS+。

设备管理中存在两种类型的管理员

- 设备管理员
- 思科 ISE 管理员

设备管理员是指登录到交换机、无线接入点、路由器和网关（一般通过 SSH）等网络设备以执行对所管理设备进行配置和维护的用户。思科 ISE 管理员可登录思科 ISE，配置并协调设备管理员所登录的设备。

思科 ISE 管理员是本文档的目标读者，他们可登录思科 ISE 以配置相应的设置，控制设备管理员的操作。思科 ISE 管理员使用设备管理功能（**工作中心 (Work Centers) > 设备管理 (Device**

**Administration)**）来控制和审核网络设备的配置。设备可配置为使用终端访问控制器访问控制系统 (TACACS) 安全协议来查询思科 ISE 服务器。思科 ISE 监控节点可提供与设备管理相关的增强型报告。思科 ISE 管理员可以执行以下任务：

- 配置带有 TACACS+ 详细信息（共享密钥）的网络设备。
- 添加设备管理员为内部用户，并根据需要为其设置启用密码。
- 创建策略集，这些策略集可使得 TACACS 结果（例如，命令集和 shell 配置文件）被选中到设备管理访问服务中的的授权策略规则中。
- 在思科 ISE 中配置 TACACS 服务器，允许设备管理员基于策略集来访问设备。

设备管理员负责设置设备以与思科 ISE 服务器进行通信。当设备管理员登录到设备时，设备将查询思科ISE服务器，后者进而查询内部或外部身份存储区，以验证设备管理员的详细信息。当思科ISE服务器完成验证后，设备将通知思科 ISE 服务器每个会话或用于记账和审核的命令授权操作的最终结果。

思科 ISE 管理员可以使用 TACACS 和思科 ISE 2.0 及更高版本来进行设备管理。与设备管理相关的配置也可以从思科安全访问控制系统 (ACS) 服务器版本 5.5 和 5.6 中迁移。更早期的版本需在迁移之前升级到版本 5.5 或 5.6。

**注释** 您应勾选以下页面中的**启用设备管理服务 (Enable Device Admin Service)** 复选框来启用 TACACS+ 操作：**管理 (Administration)** > **系统 (System)** > **发展 (Deployment)** > **通用设置 (General Settings)**。确保部署中每个 PSN 都启用了此选项。

**注释** 思科 ISE 需要设备管理许可证才能在现有的 Base 或 Mobility 许可证之上使用 TACACS+ 服务。设备管理许可证是一种永久许可证。当从较早版本升级到思科 ISE 版本 2.0 及更高版本，并且要启用 TACACS+ 服务时，必须订购设备管理许可证作为单独的附加许可证。整个 ISE 部署需要一个设备管理许可证。

# 设备管理工作中心

“工作中心”(Work Center) 菜单中包含所有设备管理页面，可以作为思科 ISE 管理员的单一入手点。然而，未指定用于设备管理的页面（例如，“用户”(Users)、“用户身份组”(User Identity Groups)、“网络设备”(Network Devices)、“默认网络设备”(Default Network Devices)、“网络设备组”(Network Device Groups)、“身份验证”(Authentication) 和“授权条件”(Authorization Conditions)）依然可从其原始菜单选项（例如，“管理”(Administration)）访问。仅在获得并安装了正确的 TACACS+ 许可证后，“工作中心”(Work Centers) 选项才可用。

“设备管理菜单”(Device Administration Menu) 包含了以下菜单选项：“概述”(Overview)、“设备管理策略集”(Device Admin Policy Sets)、“身份”(Identities)、“用户身份组”(User Identity Groups)、

“网络资源”(Network Resources)、“网络设备组”(Network Device Groups)、“策略条件”(Policy Conditions)、“策略结果”(Policy Results)、“报告”(Reports) 和“设置”(Settings)。

# 设备管理策略集

常规策略集包括一个身份验证规则表和一个授权规则表。身份验证规则表由一组“外部”规则组成，这些规则用于选择可支持的协议。每个“外部”规则包含一个或多个用于选择要使用的特定身份存储的“内部”规则。这些授权规则表由一组规则组成，这些规则用于选择要实施授权业务模式所需的特定授权结果。每个规则都包含一个或多个条件（匹配时才能使用该规则）、一组命令集和/或一个外壳配置文件，选中后即可控制授权过程。每个规则集有一个可用于在特定条件下覆盖这些规则的授权例外规则表，例外表通常在临时情况下使用。

注释 不支持 TACACS + CHAP 出站身份验证。

一个代理策略集包含单个的所选代理顺序。如果策略集处于此模式，则使用一个或多个远程代理服务器处理请求（虽然本地计费可由代理顺序进行配置）。

# 创建设备管理策略集

创建设置的设备管理策略集：

开始之前

- 确保已为 TACACS+ 操作启用**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **编辑节点 (Edit Node)** > **常规设置 (General Settings)** 窗口中的**启用设备管理服务 (Enable Device Admin Service)** 复选框。
- 确保用户身份组（例如 System_Admin、服务中心）已创建。（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **用户身份组 (User Identity Groups)** 窗口）
- 确保成员用户（例如 ABC、XYZ）包含在用户身份组中。（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **身份 (Identities)** > **用户 (Users)** 窗口）
- 确保在需要管理的设备上配置 TACACS 设置。（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框已启用，并且用于 TACACS 和设备的共享密钥相同，以便于设备查询思科 ISE。）
- 确保网络设备组已根据设备类型和位置创建。（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络设备组 (Network Device Groups)** 窗口）

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

**步骤 2** 在左侧窗格中，选择一个新策略集将要添加至其之上（之下）的当前策略集。

**步骤 3** 在左侧窗格中，点击**创建于…之上 (Create Above)** 创建新策略集。

**步骤 4** 点击**编辑 (Edit)** 并输入名称、说明和条件，（例如，名称：Device_Admin_Policy_1，说明：ISE 管理员、条件：DEVICE:Device Type EQAULS Device Type#All Device Types #Cisco_switches）以配置基于该条件的规则。

**步骤 5** 点击 **Done**。

**步骤 6** 创建所需的身份验证策略，（例如名称：ATN_Internal_Users，规则：if DEVICE:Location EQUALS Location #All Locations#Europe，条件：Allow Protocols: Device_Admin_protocols 和默认：Use Internal Users - 该策略仅匹配位于欧洲的设备，支持在设备管理员协议下定义的协议和对内部用户的身份验证）。

**步骤 7** 创建所需的授权策略。

示例 1：规则名称：Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8 - 该策略匹配用户名为 ABC 的系统管理员，支持要执行的指定命令，并分配权限级别 8。

示例 2：规则名称：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1 - 该策略匹配用户名为 XYZ 系统管理员，支持要执行的指定命令，并分配权限级别 1。

在上述示例中：

- cmd_Sys_Admin 和 cmd_HDesk 命令集是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **TACACS 命令集 (TACACS Command Sets)** > **添加 (Add)** 窗口中创建的。
- TACACS 配置文件 Profile_Priv_1 和 Profile_priv_8 是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略结果 (Policy Results)** > **TACACS 配置文件 (TACACS Profiles)** > **添加 (Add)** 窗口中创建的。

**注释** 建议在策略集创建之前创建策略结果，以便当创建授权结果时策略结果随时可用。

**步骤 8** 点击**提交 (Submit)** 以创建新的策略集。

# 设备管理 - 授权策略结果

思科 ISE 管理员可以使用 TACACS+ 命令集和 TACACS+ 配置文件（策略结果）对授予给设备管理员的权限和命令进行控制。策略与网络设备协同工作，从而防止可能发生的意外或恶意配置更改。如果发生此种更改，您可以使用设备管理审计报告对执行特定命令的设备管理员进行跟踪。

## TACACS+ 命令集

命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询思科 ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

### 命令集中的通配符和正则表达式

命令行包括命令和零个或多个参数。当思科 ISE 收到命令行（请求）时，它可以以不同的方式处理命令及其参数：

- 使用通配符匹配模式将请求中的命令与命令集列表中指定的命令进行匹配。

  示例：Sh?? or S*

- 使用正则表达式 (regex) 匹配模式将请求中的参数与命令集列表中指定的参数进行匹配。

  示例：Show interface[1-4] port[1-9]:tty*

## 命令行和命令集列表匹配

将请求的命令行与包含通配符和 Regrex 的命令集列表进行匹配：

1. 循环访问命令集列表以检测匹配的命令。

   通配符匹配允许：

   - 不区分大小写。
   - 命令集的命令中的任意字符都可以为“?”，它与请求的命令中必须存在的任意单个字符匹配。
   - 命令集的命令中的任意字符都可以为“*”，它与请求的命令中的 0 或多个字符匹配。

     示例：

| 请求 | 命令集 | 匹配 | 备注 |
|---|---|---|---|
| show | show | 支持 | — |
| show | SHOW | 支持 | 不区分大小写 |
| show | Sh?? | 支持 | 匹配任意字符 |
| show | Sho?? | N | 第二个“?”与不存在的字符相交 |
| show | S* | 支持 | “*”匹配任意字符 |
| show | S*w | 支持 | “*”匹配字符“ho” |
| show | S*p | N | 请求中没有字符与字符“p”对应 |

2. 对于每个匹配的命令，思科 ISE 会验证参数。

   对于每个命令，命令集列表包含一组以空格隔开的参数。

   示例：Show interface[1-4] port[1-9]:tty.*

   该命令含有两个参数。

   1. 参数 1：interface[1-4]

   2. 参数 2：port[1-9]:tty.*

对于请求中的命令参数，按照它们在数据包中的位置重要性顺序进行匹配。如果命令定义中的所有参数与请求中的参数匹配，那么该命令或参数可被认为是匹配的。请求中的任何外来参数都会被忽略。

注释 在参数中使用标准 Unix 正则表达式。

## 含多个命令集的处理规则

1. 如果命令集包含命令及其参数的匹配项，并且匹配项具有“始终拒绝”(Deny Always)，则思科 ISE 会指定该命令集为 Commandset-DenyAlways。
2. 如果命令集中不包含与命令匹配的“始终拒绝”，思科ISE会按顺序检查命令集中的所有命令，查找第一个匹配命令。
    1. 如果第一个匹配项具有“允许”(Permit)，则思科 ISE 会指定命令集为 Commandset-Permit。
    2. 如果第一个匹配项具有“拒绝”(Deny)，则思科 ISE 会指定命令集为 Commandset-Deny。
3. 在思科 ISE 分析所有命令集后，它会授权以下命令：
    1. 如果思科 ISE 指定任何命令集为 Commandset-DenyAlways，则思科 ISE 拒绝该命令。
    2. 如果没有 Commandset-DenyAlways，且任意命令集为 Commandset-Permit，则思科 ISE 允许该命令；否则，思科 ISE 将拒绝该命令。唯一的例外情况是**不匹配 (Unmatched)** 复选框已选中。

# 创建 TACACS+ 命令集

要使用 TACACS+ 命令集策略结果创建策略集，请按照以下步骤操作：

**步骤 1** 依次选择**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略结果 (Policy Results)** > **TACACS 命令集 (TACACS Command Sets)**。

**步骤 2** 您还可以在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 页面中配置 TACACS 命令集。

**步骤 3** 点击**添加 (Add)**。

**步骤 4** 输入名称和说明。

**步骤 5** 点击**添加 (Add)** 指定授予权限、命令和参数。

**步骤 6** 在**授予 (Grant)** 下拉列表，您可以选择以下选项之一：

- **允许 (Permit)** ：允许指定的命令（例如，permit show, permit con* Argument terminal）。
- **拒绝 (Deny)** ：拒绝指定的命令（例如，deny mtrace）。

- **始终拒绝 (Deny Always)** ：覆盖在其他命令集中允许的命令（例如，clear auditlogs）

**注释** 单击操作图标以增加或减少授予、命令和参数字段的列宽。

**步骤 7** 选中**允许以下未列出的任何命令 (Permit any command that is not listed below)** 复选框允许未在“授予”列中指定为允许、拒绝或始终拒绝的命令和参数。

# TACACS+ 配置文件

TACACS+ 配置文件控制设备管理员的初始登录会话。会话是指每个单独的身份验证、授权或记帐请求。对网络设备的会话授权请求会引发思科 ISE 响应。响应包括由网络设备解释的令牌，限制可能在会话期限执行的命令。用于设备管理访问服务的授权策略可以包含单个外壳配置文件和多个命令集。TACACS+ 配置文件定义分为两个组件：

- 常见任务
- 自定义用户属性

“TACACS+ 配置文件”页面存在两种视图（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略结果 (Policy Results)** > **TACACS 配置文件 (TACACS Profiles)**）-“任务属性视图”(Task Attribute View) 和“原始视图”(Raw View)。您可以使用“任务属性视图”(Task Attribute View) 输入普通任务，并在“任务属性视图”(Task Attribute View) 和“原始视图”(Raw View) 中创建自定义属性。

您可通过**常见任务 (Common Tasks)** 部分为配置文件选择并配置常用的属性。这里包含的属性为由与外壳服务特别相关的 TACACS+ 协议草案说明定义的那些属性。但是值可用于来自其他服务的请求授权。在**任务属性视图 (Task Attribute View)** 中，思科 ISE 管理员可以设置分配给设备管理员的权限。

- 外壳
- 思科 WLC
- 思科 Nexus
- 通用

**自定义属性 (Custom Attributes)** 部分允许您配置其他属性。它提供不被**常见任务 (Common Tasks)** 部分识别的属性列表。每个定义包括属性名称、该属性是强制还是可选的说明和属性值。

**注释** 您可以为启用 TACACS 的网络设备定义总共 24 个任务属性。如果定义的任务属性超过 24 个，则不会将这些属性发送到启用 TACACS 的网络设备。

在**原始视图 (Raw View)** 中，可以在属性名称及其值之间使用等号 (=) 输入强制属性，在属性名称及其值之间使用一个星号 (*) 可输入可选属性。**原始视图 (Raw View)** 中输入的属性反映在**任务属性视图 (Task Attribute View)** 中的**自定义属性 (Custom Attributes)** 部分，反之亦然。**原始视图 (Raw View)**

部分也用于将属性列表（例如，另一产品的属性列表）从剪贴板复制并粘贴到思科 ISE 上。可为非外壳服务定义自定义属性。

## 创建 TACACS+ 配置文件

要创建 TACACS+ 配置文件：

**步骤 1** 选择**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results** > **TACACS 配置文件 (TACACS Profiles)**。

**步骤 2** 点击**添加 (Add)**。

**步骤 3** 在 **TACACS 配置文件 (TACACS Profile)** 部分中，请输入名称和说明。

**步骤 4** 在**任务属性视图 (Task Attribute View)** 选项卡**自定义属性 (Custom Attributes)** 部分中，点击**添加 (Add)** 输入必要的属性。

# 通过 CLI 更改启用密码

要更改启用密码，请执行以下步骤：

### 开始之前

某些命令会分配到特权模式。因此，只能在设备管理员经过身份验证进入此模式时执行它们。

当设备管理员尝试进入特权模式时，设备会发送特殊的启用身份验证类型。思科 ISE 支持使用单独的启用密码来验证此特殊的启用身份验证类型。当使用内部身份库对设备管理员进行身份验证时，系统将使用单独的启用密码。对于使用外部身份库进行的身份验证，系统将使用相同的密码来进行常规登录。

**步骤 1** 登录到交换机。

**步骤 2** 按 Enter 键显示以下提示符：

```
Switch>
```

**步骤 3** 执行以下命令来配置启用密码。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

注释　如果为登录密码和启用密码配置了密码有效期，则在指定时段内未更改密码时，用户账号将禁用。如果将思科 ISE 配置为 TACACS+ 服务器，并在网络设备上配置了**启用旁路 (Enable Bypass)** 选项，则无法通过 CLI（通过 telnet）更改启用密码。选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**，更改内部用户的启用密码。

# 配置全局 TACACS+ 设置

配置全局 TACACS+ 设置

**步骤 1**　选择**工作站 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)**。

在**连接设置 (Connection Settings)** 选项卡，您可以更改所需字段的默认值。

- **单连接支持 (Single Connect Support)**：如果禁用单连接模式，则 ISE 对每个 TACACS+ 请求使用新的 TCP 连接。

**步骤 2**　在**密码更改控制 (Password Change Control)** 选项卡，定义所需字段以控制是否通过 TACACS+ 允许密码更新。

只有选中此选项，才会启用**启用 Telnet 更改密码 (Enable Telnet Change Password)** 部分中的提示。否则，会启用**禁用 Telnet 更改密码 (Disable Telnet Change Password)** 提示。密码提示可完全自定义，并可根据需要进行修改。

**步骤 3**　在**会话密钥分配 (Session Key Assignment)** 选项卡，请选择所需的字段以将 TACACS+ 请求链接到会话。

监控节点使用会话密钥来链接来自客户端的 AAA 请求。默认设置为启用 NAS 地址、端口、远程地址和用户字段。

**步骤 4**　点击**保存 (Save)**。

相关主题

TACACS+ 身份验证设置和共享密钥

# 从思科安全 ACS 将数据迁移至思科 ISE

您可以使用迁移工具导入来自 ACS 5.5 和 5.6 的数据，然后为所有网络设备设置默认 TACACS+ 密钥。导航至 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)**，然后在**准备 (Prepare)** 部分，单击迁移工具链接以打开迁移工具。将工具保存到您的 PC，然后在 migTool 文件夹中，运行 migration.bat 文件以开始迁移过程。有关迁移的完整信息，请参阅您的思科 ISE 版本的迁移指南。

# 监控设备管理活动

思科ISE提供各种报告和日志，通过这些报告和日志，您可以查看通过TACACS+配置的设备计费、身份验证、授权和命令计费相关的信息。您可以按需或按计划运行这些报告。

**步骤 1** 选择工作中心 **(Work Centers)** > 设备管理 **(Device Administration)** > 报告 **(Reports)** > **ISE** 报告 **(ISE Reports)**。

您还可以在操作 **(Operations)** > 报告 **(Reports)** > **ISE** 报告 **(ISE Reports)** 页面查看报告。

**步骤 2** 在报告选择器 **(Report Selector)** 中，展开设备管理 **(Device Administration)** 以查看、**TACACS** 记账 **(TACACS Accounting)**、**TACACS** 身份验证 **(TACACS Authentication)**、**TACACS** 授权 **(TACACS Authorization)**和 报告。

**步骤 3** 选择报告并选取您想要使用 **Filters** 下拉列表搜索的数据。

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

**步骤 5** 点击运行 **(Run)**。

# TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 窗口的字段，其中会显示 TACACS+ AAA 详细信息。此页面的导航路径为：**操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 *1: TACACS* 实时日志

| 字段名称 | 使用指南 |
|---|---|
| 生成时间 **(Generated Time)** | 根据特定事件触发时间显示系统日志生成时间。 |
| 日志记录时间 **(Logged Time)** | 显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。 |
| 状态 | 显示身份验证成功还是失败。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。 |
| 详细信息 | 在单击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。 |
| 会话密钥 **(Session Key)** | 显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。 |
| 用户名 | 显示设备管理员的用户名。此列为必选项，无法取消选择。 |
| **Type** | 包括两种类型 - 身份验证和授权。显示身份验证或授权已成功或失败的用户名称，或二者均成功和失败的用户名称。此列为必选项，无法取消选择。 |

| 字段名称 | 使用指南 |
| --- | --- |
| **身份验证策略 (Authentication Policy)** | 显示为特定身份验证选择的策略的名称。 |
| **授权策略 (Authorization Policy)** | 显示为特定授权选择的策略的名称。 |
| **ISE 节点 (ISE Node)** | 显示处理访问请求的 ISE 节点的名称。 |
| **网络设备名称** | 显示网络设备的名称。 |
| **网络设备 IP (Network Device IP)** | 显示访问请求已处理的网络设备的 IP 地址。 |
| **网络设备组 (Network Device Groups)** | 显示网络设备所属相应网络设备组的名称。 |
| **设备类型 (Device Type)** | 显示用于处理来自不同网络设备的访问请求的设备类型。 |
| **位置** | 显示用于处理来自网络设备的访问请求的基于位置的策略。 |
| **设备端口 (Device Port)** | 显示发出访问请求的设备端口号。 |
| **故障原因 (Failure Reason)** | 显示拒绝网络设备发出的访问请求的原因。 |
| **远程地址 (Remote Address)** | 显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。 |
| **匹配的命令集** | 如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。 |
| **外壳配置文件 (Shell Profile)** | 显示已授予设备管理员用于在网络设备执行命令的权限。 |

您可以在**TACACS 实时日志 (TACACS Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。

- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

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。