配置 API 的外部用户

版本要求：要使用外部 AAA，您必须运行 威胁防御版本 6.3(0) 或更高版本，以及 威胁防御 REST API v2 或更高版本。

您可以将设备配置为使用外部 RADIUS AAA 服务器在用户访问 威胁防御 REST API 时进行身份验证和授权。您可以使用 RADIUS 用户账户取代内置本地 **admin** 用户账户，或作为后者的补充。

使用外部 AAA 时，您可以定义账户具有不同的授权级别。通过此功能限制可以更改设备配置的用户，同时仍然为支持人员提供只读权限。

以下过程介绍　设置 RADIUS 账户和配置设备使用外部 AAA 进行身份验证和授权的端到端流程。

开始之前

使用外部授权时，请记住以下操作因素。

- 如果设备已配置为高可用性，请在主用设备上配置外部授权。然后，您必须运行授权设置的部署作业，以允许用户访问备用设备。
- 每次新用户访问系统，系统都会为该用户创建用户资源。您需要部署配置以保存该用户对象。

  （威胁防御 6.6 之前的版本。）如果在高可用性 (HA) 模式下运行，必须先部署配置，用户才能登录备用设备。由于只有管理员或读写用户可以启动部署作业，因此首次操作的只读用户必须让其他人部署配置，才能保存“用户”对象。

  从 威胁防御 6.6 开始，将删除对 HA 的限制。外部用户无需先登录主用设备并部署配置即可登录备用设备。系统不会在备用设备上创建用户对象，但会缓存用户特征并为用户提供访问权限（假设用户提供了有效的用户名/密码）。

过程

步骤 1 使用 RADIUS 用户账户定义授权权限，第 2 页。

步骤 2 定义 RADIUS 服务器，第 2 页。

步骤 3 创建 RADIUS 服务器的 AAA 服务器组，第 4 页。

步骤 4 创建 AAA 服务器作为 HTTPS 访问的身份验证源，第 6 页。

步骤 5 使用 **POST /operational/deploy** 启动部署作业。

curl 命令类似于下文：

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'

'https://ftd.example.com/api/fdm/最新/operational/deploy'
```

有关部署更改的详细信息，请参阅部署配置更改。

步骤 6 验证外部用户访问，第 9 页。

使用 RADIUS 用户账户定义授权权限

您可以从外部 RADIUS 服务器提供对 威胁防御 REST API 的访问权限。通过启用 RADIUS 身份验证和授权，您可以提供不同级别的访问权限，使并非每个用户都通过本地 **admin** 账户登录。

注释 这些外部用户也会获得 设备管理器 授权。

要提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户，以定义 **cisco-av-pair** 属性。必须在用户账户上正确定义此属性，否则系统会拒绝用户访问 REST API。以下是受支持的 cisco-av-pair 属性值：

- **fdm.userrole.authority.admin** 提供完全管理员访问权限。这些用户可以执行本地 **admin** 用户可以执行的所有操作。
- **fdm.userrole.authority.rw** 提供读写访问权限。这些用户可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行系统关键型操作，包括安装升级、创建和恢复备份、查看审核日志以及注销其他用户。
- **fdm.userrole.authority.ro** 提供只读访问权限。这些用户可以查看控制面板和配置，但无法进行任何更改。如果用户尝试进行更改，会显示错误消息，指明权限不足。

定义 RADIUS 服务器

在 RADIUS 服务器配置用户账户，以定义相应的授权权限之后，可以配置设备使用服务器对 REST API 访问进行身份验证和授权。

使用 **POST /object/radiusidentitysources** 资源为您想要定义的每个 RADIUS 服务器创建对象。

过程

步骤 1 为 RADIUS 服务器创建 JSON 对象正文。

以下是要与此调用结合使用的 JSON 对象示例。

```
{
  "name": "aaa-server-1",
  "description": "RADIUS server for API access.",
  "host": "172.16.246.220",
  "timeout": 10,
  "serverAuthenticationPort": 1812,
  "serverSecretKey": "secret123",
  "type": "radiusidentitysource"
}
```

属性包括：

- **name** - 对象名称。不需要与 RADIUS 服务器上定义的内容匹配。
- **description** -（可选。）对象的说明。
- **host** - RADIUS 服务器的 IP 地址或完全限定主机名。
- **timeout** -（可选。）系统将请求发送至下一服务器之前等待服务器响应的时长，1-300 秒之间的数值。如果不包含此属性，默认值为 10 秒。
- **serverAuthenticationPort** -（可选。）执行 RADIUS 身份验证和授权的端口。如果不包含此属性，默认值为 1812。
- **serverSecretKey** -（可选。）用于加密 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 2 发布对象。

例如，**curl** 命令会如下所示：

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
 -d '{
    "name": "aaa-server-1",
   "description": "RADIUS server for API access.",
   "host": "172.16.246.220",
   "timeout": 10,
   "serverAuthenticationPort": 1812,
   "serverSecretKey": "secret123",
   "type": "radiusidentitysource"
 }' 'https://ftd.example.com/api/fdm/最新/object/radiusidentitysources'
```

步骤 3 验证响应。

您应获得的响应代码为 200。成功的响应正文应类似如下内容。请注意，响应中的密钥等敏感信息会被屏蔽。

```
{
  "version": "nfamb3cr2jlyi",
  "name": "aaa-server-1",
  "description": "RADIUS server for API access.",
  "host": "172.16.246.220",
  "timeout": 10,
  "serverAuthenticationPort": 1812,
  "serverSecretKey": "*********",
  "capabilities": [
    "AUTHENTICATION",
    "AUTHORIZATION"
  ],
  "id": "1b962e3b-6e56-11e8-bd65-379fa8aaaba1",
  "type": "radiusidentitysource",
  "links": {
    "self": "https://ftd.example.com/api/fdm/最新/object/
radiusidentitysources/1b962e3b-6e56-11e8-bd65-379fa8aaaba1"
  }
}
```

创建 RADIUS 服务器的 AAA 服务器组

创建 RADIUS 服务器对象后，使用 **POST /object/radiusidentitysourcegroups** 资源创建 AAA 组，以包含 radiusidentitysource 对象。

您可以向 RADIUS AAA 服务器组添加最多 16 个 RADIUS 服务器。这些服务器必须彼此备份，即它们必须具有相同的用户账户列表。

过程

步骤 1 为 RADIUS 服务器组创建 JSON 对象正文。

以下是要与此调用结合使用的 JSON 对象示例。

```
{
  "name": "radius-group",
  "maxFailedAttempts": 3,
  "deadTime": 10,
  "description": "AAA RADIUS server group.",
  "radiusIdentitySources": [
    {
      "id": "1b962e3b-6e56-11e8-bd65-379fa8aaaba1",
      "type": "radiusidentitysource",
      "version": "nfamb3cr2jlyi",
      "name": "aaa-server-1"
    }
  ],
  "type": "radiusidentitysourcegroup"
}
```

属性包括：

- **name** - 对象名称。不需要与 RADIUS 成员服务器上定义的内容匹配。

- **maxFailedAttempts** -（可选。）只有在所有服务器都发生故障后才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间，其值为 0-1440 分钟。如果不包含此属性，默认值为 10 分钟。
- **deadTime** -（可选。）尝试组中下一个服务器之前发送到 RADIUS 服务器的失败请求（即未收到响应的请求）数。您可以指定 1 到 5 之间的数字，默认值为 3。超过最大失败尝试次数时，系统会将服务器标记为故障。

  对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。
- **description** -（可选。）对象的说明。
- **radiusIdentitySources** - 这是一组定义每个 radiusidentitysource 对象的项目，其中 radiusidentitysource 对象定义包含在组中的 RADIUS 服务器。将项目放置在方括号 [] 中。以下是每个对象的属性和语法。从单个对象获取 **id**、**version** 和 **name** 属性的值；创建对象时，信息位于响应正文中。您还可以从 **GET/object/radiusidentitysources** 调用获取信息。**类型**必须为 **radiusidentitysource**。

```
{
  "id": "1b962e3b-6e56-11e8-bd65-379fa8aaaba1",
  "type": "radiusidentitysource",
  "version": "nfamb3cr2jlyi",
  "name": "aaa-server-1"
}
```

步骤 2 发布对象。

例如，**curl** 命令会如下所示：

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
 -d '{
   "name": "radius-group",
   "maxFailedAttempts": 3,
   "deadTime": 10,
   "description": "AAA RADIUS server group.",
   "radiusIdentitySources": [
     {
       "id": "1b962e3b-6e56-11e8-bd65-379fa8aaaba1",
       "type": "radiusidentitysource",
       "version": "nfamb3cr2jlyi",
       "name": "aaa-server-1"
     }
   ],
   "type": "radiusidentitysourcegroup"
 }' 'https://ftd.example.com/api/fdm/最新/object/radiusidentitysourcegroups'
```

步骤 3 验证响应。

您应获得的响应代码为 200。成功的响应正文应类似如下内容。

```
{
  "version": "7r572novdiyy",
```

```
  "name": "radius-group",
  "maxFailedAttempts": 3,
  "deadTime": 10,
  "description": "AAA RADIUS server group.",
  "radiusIdentitySources": [
    {
      "version": "nfamb3cr2jlyi",
      "name": "aaa-server-1",
      "id": "1b962e3b-6e56-11e8-bd65-379fa8aaaba1",
      "type": "radiusidentitysource"
    }
  ],
  "activeDirectoryRealm": null,
  "id": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
  "type": "radiusidentitysourcegroup",
  "links": {
    "self": "https://ftd.example.com/api/fdm/最新/object/
radiusidentitysourcegroups/0a7996ae-6e5b-11e8-bd65-dbab801c44b9"
  }
}
```


创建 AAA 服务器作为 HTTPS 访问的身份验证源

使用 **PUT /devicesettings/default/aaasettings/{objId}** 资源确定作为用户授权身份源的 RADIUS AAA 服务器组。

没有 POST 方法：系统身份验证所需的对象已存在。必须首先执行 GET 命令，以确定相关的 ID 和版本值。

过程

步骤 1 使用 **GET /devicesettings/default/aaasettings** 确定 aaasettings 对象的属性。

curl 命令类似于下文：

```
curl -X GET --header 'Accept: application/json'
'https://ftd.example.com/api/fdm/最新/devicesettings/default/aaasettings'
```

例如，响应正文类似于下文。本例展示本地身份源是为HTTPS访问定义的身份源。它还用于与REST API 不相关的 SSH 访问。


```
{
  "items": [
    {
      "version": "du52clrtmawlt",
      "name": "HTTPS",
      "identitySourceGroup": {
        "version": "cynutari5ffkl",
        "name": "LocalIdentitySource",
        "id": "e3e74c32-3c03-11e8-983b-95c21a1b6da9",
        "type": "localidentitysource"
      },
      "description": null,
      "protocolType": "HTTPS",
```

```
      "useLocal": "NOT_APPLICABLE",
      "id": "00000003-0000-0000-0000-000000000007",
      "type": "aaasetting",
      "links": {
        "self": "https://ftd.example.com/api/fdm/最新/
devicesettings/default/aaasettings/00000003-0000-0000-0000-000000000007"
      }
    },
    {
      "version": "fgkhvu4kwucgv",
      "name": "SSH",
      "identitySourceGroup": {
        "version": "cynutari5ffkl",
        "name": "LocalIdentitySource",
        "id": "e3e74c32-3c03-11e8-983b-95c21a1b6da9",
        "type": "localidentitysource"
      },
      "description": null,
      "protocolType": "SSH",
      "useLocal": "NOT_APPLICABLE",
      "id": "00000003-0000-0000-0000-000000000008",
      "type": "aaasetting",
      "links": {
        "self": "https://ftd.example.com/api/fdm/最新/
devicesettings/default/aaasettings/00000003-0000-0000-0000-000000000008"
      }
    }
  ],
  "paging": {
    "prev": [],
    "next": [],
    "limit": 10,
    "offset": 0,
    "count": 2,
    "pages": 0
  }
}
```


步骤 2 （可选。）使用 **GET /devicesettings/default/aaasettings/{objId}** 获取 HTTPS AAA 设置对象副本，以缩小查找范围。

PUT 调用仅更新 HTTPS 对象。不需要更新 SSH 对象。

在本示例中，HTTPS 对象的 ID 是 00000003-0000-0000-0000-000000000007，因此 **curl** 应类似于以下命令：

```
curl -X GET --header 'Accept: application/json'
'https://ftd.example.com/api/fdm/最新/devicesettings/
default/aaasettings/00000003-0000-0000-0000-000000000007'
```

响应正文类似于下文：


```
{
  "version": "ha4653ootep7z",
  "name": "HTTPS",
  "identitySourceGroup": {
    "version": "cynutari5ffkl",
    "name": "LocalIdentitySource",
    "id": "e3e74c32-3c03-11e8-983b-95c21a1b6da9",
    "type": "localidentitysource"
  },
```

```
  "description": null,
  "protocolType": "HTTPS",
  "useLocal": "NOT_APPLICABLE",
  "id": "00000003-0000-0000-0000-000000000007",
  "type": "aaasetting",
  "links": {
    "self": "https://ftd.example.com/api/fdm/最新/
devicesettings/default/aaasettings/00000003-0000-0000-0000-000000000007"
  }
```

步骤 3 为 AAA 管理访问创建 JSON 对象正文。

以下是要与此调用结合使用的 JSON 对象示例。

```
{
  "version": "ha4653ootep7z",
  "name": "HTTPS",
  "identitySourceGroup": {
    "id": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
    "type": "radiusidentitysourcegroup",
    "version": "7r572novdiyy",
    "name": "radius-group"
  },
  "description": null,
  "protocolType": "HTTPS",
  "useLocal": "BEFORE",
  "id": "00000003-0000-0000-0000-000000000007",
  "type": "aaasetting"
}
```

属性包括：

- **version** - HTTPS 对象的版本。在响应正文中找到 GET 调用的此值。
- **name** - 对象名称，**HTTPS**。在响应正文中找到 GET 调用的此值。
- **identitySourceGroup** - 可识别 RADIUS 服务器组。创建服务器（或 **GET/object/radiusidentitysourcegroups** 调用）时，从响应正文获取 **id**、**version** 以及 **name** 值。类型必须是 **radiusidentitysourcegroup**。
- **description** -（可选。）对象的说明。
- **protocolType** - 此源应用的协议，**HTTPS**。
- **useLocal** - 如何使用本地身份源，其中包含本地管理员用户账户。输入以下选项之一：
  - **之前** - 系统首先对照本地源检查用户名和密码。
  - **之后** - 仅当外部源不可用或在外部源中找不到用户账户时，检查本地源。
  - **从不** -（不推荐。）从不使用本地源，因此不能以 **admin** 用户身份登录。

    注意 如果您选择 **从不**，将无法使用 **管理员** 账户登录 设备管理器 或使用 API。如果 RADIUS 服务器不可用，或者未在 RADIUS 服务器中配置账户，您将被锁定在系统外面。

- **id** - HTTPS 对象的 ID 值。在响应正文中找到 GET 调用的此值。

- **类型** - 对象类型，**aaasetting** 。

步骤 4 放置对象。

例如，**curl** 命令会如下所示：注意，URL 中的 {objId} 与 JSON 对象中 aaasettings 对象的 ID 相同。

```
curl -X PUT --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{
   "version": "ha4653ootep7z",
   "name": "HTTPS",
   "identitySourceGroup": {
     "id": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
     "type": "radiusidentitysourcegroup",
     "version": "7r572novdiyy",
     "name": "radius-group"
   },
   "description": null,
   "protocolType": "HTTPS",
   "useLocal": "BEFORE",
   "id": "00000003-0000-0000-0000-000000000007",
   "type": "aaasetting"
 }' 'https://ftd.example.com/api/fdm/最新/devicesettings/
default/aaasettings/00000003-0000-0000-0000-000000000007'
```

步骤 5 验证响应。

您应获得的响应代码为 200。成功的响应正文应类似如下内容。

```
{
  "version": "ehxcytq4iccb3",
  "name": "HTTPS",
  "identitySourceGroup": {
    "version": "7r572novdiyy",
    "name": "radius-group",
    "id": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
    "type": "radiusidentitysourcegroup"
  },
  "description": null,
  "protocolType": "HTTPS",
  "useLocal": "BEFORE",
  "id": "00000003-0000-0000-0000-000000000007",
  "type": "aaasetting",
  "links": {
    "self": "https://ftd.example.com/api/fdm/最新/devicesettings/
default/aaasettings/00000003-0000-0000-0000-000000000007"
  }
}
```

验证外部用户访问

部署作业完成后，您可以测试外部用户对 设备管理器 和 REST API 的访问权限。

过程

步骤 1 使用具有有效 cisco-av-pair 属性的外部用户名登录到 设备管理器。

登录应该是成功的，且页面的右上方应显示用户名和权限级别。

步骤 2 为外部用户获取 REST API 令牌。

如果用户可以获取令牌，用户就可以使用所分配的权限级别所允许的资源和方法。

a) 为简单的密码授予的令牌创建 JSON 对象正文。

```
{
  "grant_type": "password",
  "username": "radiusreadwriteuser1",
  "password": "Readwrite123!"
}
```

b) 使用 **POST /fdm/token** 获取令牌。

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
 -d '{
   "grant_type": "password",
   "username": "radiusreadwriteuser1",
   "password": "Readwrite123!"
 }' 'https://ftd.example.com/api/fdm/最新/fdm/token'
```

c) 评估响应以验证是否已授予令牌。

您应获得的响应代码为 200。获取令牌意味着系统能够对用户进行身份验证。

```
{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1Mjg4MjM
3MTAsInN1YiI6InJhZGl1c3JlYWR3cml0ZXVzZXIxIiwianRpIjoiMjk5Zj
Q5YjYtNmU2NC0xMWU4LWJkNjUtNmY0ZmVmYjY1MzI5IiwibmJmIjoxNTI4O
DIzNzEwLCJleHAiOjE1Mjg4MjU1MTAsInJlZnJlc2hUb2tlbkV4cGlyZXNB
dCI6MTUyODgyNjExMDg4OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInV
zZXJVdWlkIjoiMjliMjBlNjctNmU2NC0xMWU4LWJkNjUtMzU4MmUwZjU5Yj
Q4IiwidXNlclJvbGUiOiJST0xFX1JFQURfV1JVEUiLCJvcmlnaW4iOiJwY
XNzd29yZCJ9.dtKsl9IB4ds3RAktEeaSuQy_Zs2SrzLr976UtblBt28",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1Mjg4Mj
M3MTAsInN1YiI6InJhZGl1c3JlYWR3cml0ZXVzZXIxIiwianRpIjoiMjk5Z
jQ5YjYtNmU2NC0xMWU4LWJkNjUtNmY0ZmVmYjY1MzI5IiwibmJmIjoxNTI4
ODIzNzEwLCJleHAiOjE1Mjg4MjYxMTAsImFjY2Vzc1Rva2VuRXhwaXJlc0F
0IjoxNTI4ODI1NTEwODg5LCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cG
UiOiJKV1RfUmVmcmVzaCIsInVzZXJVdWlkIjoiMjliMjBlNjctNmU2NC0xM
WU4LWJkNjUtMzU4MmUwZjU5YjQ4IiwidXNlclJvbGUiOiJST0xFX1JFQURf
V1JVEUiLCJvcmlnaW4iOiJwYXNzd29yZCJ9.Lc7MYmieNMMrjx7XoTiW-x
8Z8qFCnzfNM1apgbwLQvo",
  "refresh_expires_in": 2400
}
```

步骤 3 使用 **GET /object/users** 验证是否已为每个用户创建用户对象。

系统将为每个登录到设备管理器或获取访问令牌的新用户自动创建用户对象。您必须运行部署作业才能保存这些用户对象。在高可用性模式下，运行部署作业之后，用户才可以登录到备用设备。

例如，**curl** 命令会如下所示：

```
curl -X GET --header 'Accept: application/json'
'https://ftd.example.com/api/fdm/最新/object/users'
```

以下响应正文显示两个外部用户登录。请注意，**userRole** 显示从RADIUS服务器所配置的cisco-av-pair中获取的针对这些用户账户的权限。使用此信息验证是否已正确配置 RADIUS 用户账户。**admin** 用户是本地定义的用户。


```
{
  "items": [
    {
      "version": "h2vom4wckm2js",
      "name": "radiusadminuser1",
      "password": null,
      "newPassword": null,
      "userPreferences": {
        "preferredTimeZone": "(UTC+00:00) UTC",
        "colorTheme": "NORMAL_CISCO_IDENTITY",
        "type": "userpreferences"
      },
      "userRole": "ROLE_ADMIN",
      "identitySourceId": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
      "userServiceTypes": [
        "MGMT"
      ],
      "id": "150d9754-6e63-11e8-bd65-ed9b20f62114",
      "type": "user",
      "links": {
        "self": "https://ftd.example.com/api/fdm/最新/
object/users/150d9754-6e63-11e8-bd65-ed9b20f62114"
      }
    },
    {
      "version": "p4rgwcjr5colj",
      "name": "admin",
      "password": null,
      "newPassword": null,
      "userPreferences": {
        "preferredTimeZone": "(UTC-07:00) America/Los_Angeles",
        "colorTheme": "NORMAL_CISCO_IDENTITY",
        "type": "userpreferences"
      },
      "userRole": "ROLE_ADMIN",
      "identitySourceId": "e3e74c32-3c03-11e8-983b-95c21a1b6da9",
      "userServiceTypes": [
        "MGMT"
      ],
      "id": "5023d3ab-6dc5-11e8-b9ed-db6dba9bf94c",
      "type": "user",
      "links": {
        "self": "https://ftd.example.com/api/fdm/最新/
object/users/5023d3ab-6dc5-11e8-b9ed-db6dba9bf94c"
      }
    },
    {
      "version": "ngx7a2dixngoq",
      "name": "radiusreadwriteuser1",
      "password": null,
      "newPassword": null,
      "userPreferences": {
```

```
        "preferredTimeZone": "(UTC+00:00) UTC",
        "colorTheme": "NORMAL_CISCO_IDENTITY",
        "type": "userpreferences"
      },
      "userRole": "ROLE_READ_WRITE",
      "identitySourceId": "0a7996ae-6e5b-11e8-bd65-dbab801c44b9",
      "userServiceTypes": [
        "MGMT"
      ],
      "id": "29b20e67-6e64-11e8-bd65-3582e0f59b48",
      "type": "user",
      "links": {
        "self": "https://ftd.example.com/api/fdm/最新/
object/users/29b20e67-6e64-11e8-bd65-3582e0f59b48"
      }
    }
  ],
  "paging": {
    "prev": [],
    "next": [],
    "limit": 10,
    "offset": 0,
    "count": 3,
    "pages": 0
  }
}
```

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。