动态访问策略

动态访问策略(DAP)让您能够配置解决VPN环境动态问题的授权。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。

关于 Cisco Secure Firewall Threat Defense 动态访问策略

VPN 网关在动态环境下运行。多个变量可能会影响每个 VPN 连接。例如，频繁更改内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点尝试登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。

您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。 会根据您定义的策略，为特定的会话向特定用户授予访问权限。 设备会通过从一个或多个 DAP 记录中选择或汇总属性，从而在用户身份验证期间生成 DAP。然后，设备会根据远程设备的终端安全信息，以及经过身份验证的用户的AAA授权信息，选择这些 DAP 记录。然后，设备会将 DAP 记录应用至用户隧道或会话。

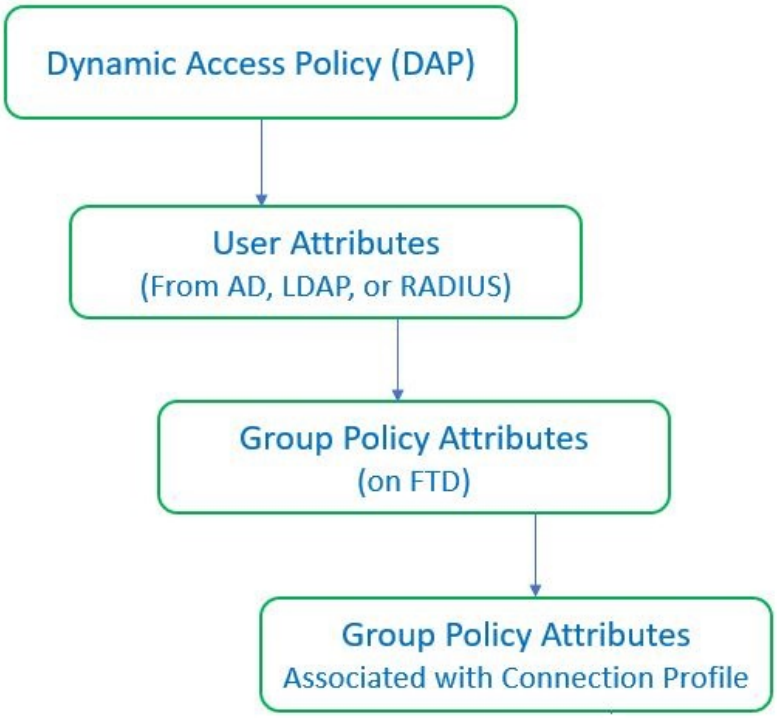
中权限和属性的策略实施层次结构

设备支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接。从 上的 DAP、外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或从 设备上的组策略应用属性。

如果 设备收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果来自 DAP、AAA 服务器或组策略的属性之间存在冲突，从 DAP 获得的属性始终会被优先考虑。

设备按照以下顺序应用属性：

图 *1:* 策略实施流程



1. **FTD 上的 DAP 属性** - DAP 属性优先于所有其他的属性。
2. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
3. **FTD 上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS 类属性 IETF-Class-25 (OU=group-policy) 值， 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
4. **连接配置文件 (也称为隧道组) 分配的组策略**- 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。

注释 设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。对于用户会话，设备会使用您分配给连接配置文件的组策略上的属性，除非它们被来自 AAA 服务器的用户属性或组策略覆盖。

动态访问策略的前提条件

许可：

- 必须至少拥有以下 Secure Client 许可证之一：

- Secure Client Premier
- Secure Client Advantage
- 仅限 Secure Client VPN

- 基础版许可证必须允许出口控制功能。

动态访问策略的准则与限制

- 只有当AAA服务器被配置为在对远程接入VPN会话进行身份验证或授权时返回正确的属性时，才能匹配 DAP 中的 AAA 属性。
- DAP 支持的最低 安全客户端 和 Cisco Secure Firewall 终端安全评估 软件包版本为 4.6。但是强烈建议使用最新版本的 安全客户端。
- DAP 不支持集群或多实例模式。
- 具有已分配 IPv4 或 IPv6 地址的 DAP 条件不适用于本地身份验证。

配置动态访问策略 (DAP)

创建动态访问策略

开始之前

在配置动态访问策略之前，请确保您拥有 Cisco Secure Firewall 终端安全评估 软件包。您可以通过**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **安全客户端文件 (Secure Client File)** 来添加 Cisco Secure Firewall 终端安全评估 文件。

过程

步骤 1 选择 **设备** > **VPN** > **动态访问策略**，然后点击**创建动态访问策略**。

步骤 2 为 DAP 策略指定**名称 (Name)** 和可选的**说明 (Description)**。

步骤 3 从下拉列表中选择 **Cisco Secure Firewall 终端安全软件包 (Secure Firewall Posture Package)**。

步骤 4 点击**保存**。

下一步做什么

要配置 DAP 记录，请参阅 创建动态访问策略记录

创建动态访问策略记录

动态访问策略(DAP)可以包含多个DAP记录，您可以在这些记录中配置用户和终端属性。您可以确定 DAP 内的 DAP 记录的优先级，以便 在用户尝试 VPN 连接时选择和排序所需的条件。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。

步骤 2 编辑现有的动态访问策略，或者点击**创建动态访问策略 (Create Dynamic Access Policy)** 以创建新策略，然后编辑该策略。

步骤 3 点击**创建 DAP 记录 (Create DAP Record)**。

步骤 4 点击**常规 (General)**选项卡。

步骤 5 指定 DAP 记录的**名称 (Name)**。

步骤 6 为 DAP 记录输入**优先级 (Priority)**。

数值越低，优先级越高。

步骤 7 选择当 DAP 记录匹配时要执行的以下操作之一：

- **继续** - 将访问策略属性应用于会话。如果有的话，接下来会评估下一个 DAP 记录（优先级较低的下一个策略行）。
- **终止 (Terminate)** - 终止会话。
- **隔离 (Quarantine)** - 隔离连接。

步骤 8 选中 **在条件匹配时显示用户消息** 复选框并添加用户消息。

当 DAP 记录匹配， 将此消息显示给用户。

步骤 9 选中**对流量应用网络 ACL (Apply a Network ACL on Traffic)** 复选框，然后从下拉列表中选择访问控制列表。

步骤 10 选中**应用一个或多个 Secure Client 自定义属性 (Apply one or more Secure Client Custom Attributes)** 复选框，然后从下拉列表中选择自定义属性对象。

步骤 11 点击**保存**。

配置终端安全评估条件

对于 DAP 策略，可以使用唯一的终端 ID 配置文件、进程或注册表终端属性。这些 ID 可用作 Lua 脚本中的终端条件以配置 DAP 记录。

过程

步骤 1 选择**设备** > **VPN** > **动态访问策略**。

步骤 2 点击**创建动态访问策略 (Create Dynamic Access Policy)** 以创建新的 DAP 策略，然后编辑策略。

步骤 3 点击 DAP 策略旁边的编辑图标。

步骤 4 点击**添加终端安全评估条件 (Add Posture Assessment Criteria)**。

步骤 5 执行以下操作之一：

- 配置文件终端属性：
  1. 点击**文件 (File)** 单选按钮。
  2. 在**终端 ID (Endpoint ID)** 字段中，输入文件的唯一 ID。它可以是一个字符串或数字。
  3. 在**文件路径 (File Path)** 字段中，指定文件路径。
- 配置注册表终端属性：
  1. 点击**注册表 (Registry)** 单选按钮。
  2. 在**终端 ID (Endpoint ID)** 字段中，输入注册表的唯一 ID。它可以是一个字符串或数字。
  3. 在**条目路径 (Entry Path)** 字段中，指定文件路径。
- 配置进程终端属性：
  1. 点击**进程 (Process)** 单选按钮。
  2. 在**终端 ID (Endpoint ID)** 字段中，输入进程的唯一 ID。它可以是一个字符串或数字。
  3. 在**进程名称 (Process Name)** 字段中，指定进程名称。

注释
终端 ID 一旦保存，就无法编辑。

步骤 6 点击**保存**。

下一步做什么

您可以使用 Lua 脚本来通过终端 ID 配置高级终端安全评估条件。有关详细信息，请参阅配置 DAP 的高级设置，第 12 页。

配置 DAP 的 AAA 条件设置

DAP 可提供一组限定的授权属性，这些属性可覆盖 AAA 提供的属性，从而补充 AAA 服务。 会根据用户的 AAA 授权信息和会话的终端安全评估信息选择 DAP 记录。 可根据此信息选择多个 DAP 记录，然后将其汇聚以创建 DAP 授权属性。

过程

步骤 1 选择**设备** > **VPN** > **动态访问策略**。

步骤 2 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。

步骤 3 选择 DAP 记录或创建新记录，然后编辑 DAP 记录。

步骤 4 点击 **AAA 条件 (AAA Criteria)**。

步骤 5 选择**部分之间匹配条件**之一。

- 任意 (Any) - 匹配任意条件。
- 全部 (All) - 匹配所有条件。
- 无 (None) - 不匹配任何设定的条件。

步骤 6 点击**添加 (Add)** 以添加所需的**思科 VPN 条件**。

思科 VPN 条件包括组策略的属性、分配的 IPv4 地址、分配的 IPv6 地址、连接配置文件、用户名、用户名 2 和所需的 SCEP。

a) 选择属性并指定 **值**。

b) 点击**添加其他条件 (Add another criteria)** 以添加更多条件。

c) 点击**保存**。

需要 SCEP

步骤 7 选择 **LDAP 条件**、 **RADIUS 条件**或 **SAML 条件** 并指定 **属性 ID** 和 **值 (**。

步骤 8 点击**保存**。

在 DAP 中配置终端属性选择条件

终端属性包含终端系统环境、终端安全评估结果和应用的相关信息。 会在会话建立期间动态生成终端属性的集合，并将这些属性存储在与此会话关联的数据库中。每个DAP记录指定终端选择属性，这些属性必须得到满足， 才能选择将其用于会话。 仅选择满足每个配置的条件的 DAP 记录。

过程

步骤 1 选择 **设备** > **VPN** > **动态访问策略**，然后点击**创建动态访问策略**。

步骤 2 编辑 DAP 策略，然后编辑 DAP 记录。

注释
创建 DAP 策略和 DAP 记录（如果尚未创建）。

步骤 3 点击**终端条件 (Endpoint Criteria)** 并配置以下终端条件属性：

注释
您可以创建每个终端属性类型的多个实例。每个 DAP 记录的终端属性数量没有限制。

- 向 DAP 添加 Anti-Malware 终端属性
- 向 DAP 添加设备终端属性
- 向 DAP 添加 安全客户端终端属性 ， 第 8 页
- 向 DAP 添加 NAC 终端属性
- 向 DAP 添加应用属性
- 向 DAP 添加个人防火墙终端属性
- 向 DAP 添加操作系统终端属性
- 向 DAP 添加流程终端属性
- 向 DAP 添加注册表终端属性
- 向 DAP 添加文件终端属性
- 向 DAP 添加多证书身份验证属性

步骤 4 点击**保存**。

向 DAP 添加 Anti-Malware 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **防恶意软件 (Anti-Malware)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加防恶意软件属性。

步骤 4 点击**已安装 (Installed)** 以指示安装还是不安装所选终端属性及其附带限定词。

步骤 5 选择 **已启用** 或 **已禁用** 以激活或停用实时恶意软件扫描。

步骤 6 从列表中选择防恶意软件**供应商**的名称。

步骤 7 选择防恶意软件的**产品说明 (Product Description)**。

步骤 8 选择防恶意软件产品的**版本 (Version)**。

步骤 9 指定距离**上次更新 (Last Update)** 的天数。

您可以指明防恶意软件更新时间应小于 (<) 或大于 (>) 您指定的天数。

步骤 10 点击**保存**。

向 DAP 添加设备终端属性

过程

步骤 1 编辑 DAP 记录，然后选择 **终端条件** > **设备**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 并选择 = 或 ≠ 运算符，以检查属性是否等于或不等于你为以下属性输入的值。

- **主机名**-要测试的设备的主机名。此处仅会使用计算机的主机名，而不是完全限定域名(FQDN)。
- **MAC 地址 (MAC Address)** - 要测试的网络接口卡的 MAC 地址。 地址必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。
- **BIOS 序列号 (BIOS Serial Number)** - 要测试的设备的 BIOS 序列号值。此编号格式由制造商指定。
- **端口号 (Port Number)** - 设备的侦听端口号。
- **安全桌面版本 (Secure Desktop Version)** - 在终端上运行的主机扫描映像的版本。
- **OPSWAT 版本 (OPSWAT Version)** - OPSWAT 客户端版本。
- **隐私保护 (Privacy Protection)** - 无、缓存清理器、安全桌面。
- **TCP/UDP 端口号**- 您正在测试的处于侦听状态的 TCP 或 UDP 端口。

步骤 4 点击**保存**。

向 DAP 添加 安全客户端终端属性

过程

步骤 1 编辑 DAP 记录，然后选择 **终端条件** > **安全客户端**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 并选择 = 或 ≠ 运算符，以检查属性是否等于您输入的值。

步骤 4 选择**客户端版本 (Client Version)** 和**平台 (Platform)**。

步骤 5 选择**平台版本 (Platform Version)**，然后指定**设备类型 (Device Type)** 和**设备唯一 ID (Device Unique ID)**。

步骤 6 将 **MAC 地址**添加到 MAC 地址池中。

注释
MAC 地址必须是 XX-XX-XX-XX-XX-XX 格式，其中每个 X 都是十六进制字符。您可以点击**添加另一个 MAC 地址 (Add another MAC Address)** 以添加更多地址。

步骤 7 点击**保存**。

向 DAP 添加 NAC 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **NAC**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加 NAC 属性。

步骤 4 将运算符设置为等于 = 或不等于 ≠ 安全评估状态字符串。在**安全评估状态 (Posture Status)** 框中输入安全评估标记字符串。

步骤 5 点击**保存**。

向 DAP 添加应用属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **应用 (Application)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击 **添加** 以添加应用属性。

步骤 4 选择等于 (=) 或不等于 (≠) 并指定表明远程访问连接类型的 **客户端类型** 。

步骤 5 点击**保存**。

向 DAP 添加个人防火墙终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **个人防火墙 (Personal Firewall)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击 **添加** 以添加个人防火墙属性。

步骤 4 点击 **已安装** 以指示安装还是不安装个人防火墙终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

步骤 5 选择 **启用** 或 **禁用** 以激活或停用防火墙保护。

步骤 6 从列表中选择防火墙**供应商 (Vendor)** 的名称。

步骤 7 选择防火墙的**产品说明 (Product Description)**。

步骤 8 选择等于 (=) 或不等于 (≠) 运算符，然后选择防恶意软件产品的**版本**。

步骤 9 点击**保存**。

向 DAP 添加操作系统终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **操作系统 (Operating System)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击 **添加** 以添加终端属性。

步骤 4 选择等于 (=) 或不等于 (≠) 运算符，然后选择**操作系统 (Operating System)**。

步骤 5 选择等于 (=) 或不等于 (≠) 运算符，然后制定操作系统**版本 (Version)**。

步骤 6 点击**保存**。

向 DAP 添加流程终端属性

过程

步骤 1 编辑 DAP 记录。

步骤 2 点击**终端条件 (Endpoint Criteria)** 选项卡。

步骤 3 点击**处理 (Process)**。

步骤 4 选择**全部 (All)** 或**任意 (Any)** 作为**匹配条件 (Match Criteria)**。

步骤 5 点击 + 以添加流程属性。

步骤 6 选择**存在 (Exists)** 或**不存在 (Does not exist)**。

步骤 7 指定**进程名称 (Process Name)**。

步骤 8 从**终端 ID (Endpoint ID)** 下拉列表中，选择进程的 ID 或点击 +，为该进程配置安全评估条件。有关详细信息，请参阅 配置终端安全评估条件，第 4 页。

步骤 9 点击**存在 (Exists)** 或**不存在 (Does not exist)**。

步骤 10 点击**保存**。

向 DAP 添加注册表终端属性

扫描注册表终端属性仅适用于 Windows 操作系统。

开始之前

在配置注册表终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的注册表项。

过程

步骤 1 编辑 DAP 记录。

步骤 2 点击**终端条件 (Endpoint Criteria)** 选项卡。

步骤 3 点击**注册表 (Registry)**。

步骤 4 选择**全部 (All)** 或**任意 (Any)** 作为**匹配条件 (Match Criteria)**。

步骤 5 点击 + 以添加注册表属性。

步骤 6 选择注册表的**条目路径 (Entry Path)** 并指定路径。

步骤 7 从**终端 ID (Endpoint ID)** 下拉列表中，选择注册表的 ID 或点击 +，为该注册表配置安全评估条件。有关详细信息，请参阅 配置终端安全评估条件，第 4 页。

步骤 8 选择注册表是**存在 (Exists)** 还是**不存在 (Does not exist)**。

步骤 9 从列表中选择注册表**类型 (Type)**。

步骤 10 选择等于 (=) 或不等于 (≠) 运算符，然后输入注册表项的**值**。

步骤 11 选择**不区分大小写 (Case insensitive)** 以便在扫描时忽略注册表项的大小写。

步骤 12 点击**保存**。

向 DAP 添加文件终端属性

过程

步骤 1 编辑 DAP 记录。

步骤 2 点击**终端条件 (Endpoint Criteria)** 选项卡。

步骤 3 点击**文件**。

步骤 4 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 5 点击 + 以添加文件属性。

步骤 6 指定**文件路径**。

步骤 7 从**终端 ID (Endpoint ID)** 下拉列表中，选择文件的 ID 或点击 **+**，为该文件配置安全评估条件。有关详细信息，请参阅 配置终端安全评估条件 ， 第 4 页。

步骤 8 选择 **存在** 或 **不存在** 以指明文件是否存在。

步骤 9 选择小于 (<) 或大于 (>) 并指定文件的**上次修改 (Last Modified)** 天数。

步骤 10 选择等于 (=) 或不等于 ≠ 运算符，然后输入**校验和**。

步骤 11 点击**保存**。

向 DAP 添加证书身份验证属性

您可以对每个证书编制索引，以便配置的规则可以引用接收到的任何证书。以这些证书字段为基础，您可以配置 DAP 规则来允许或禁止连接尝试。

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **证书 (Certificate)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加证书属性。

步骤 4 选择证书 **Cert1** 或 **Cert2**。

步骤 5 选择**使用者 (Subject)** 并指定使用者值。

步骤 6 选择**颁发机构 (Issuer)** 并指定颁发机构值。

步骤 7 选择**使用者替代名称 (Subject Alternate Name)** 并指定使用者值。

步骤 8 指定**序列号 (Serial Number)**。

步骤 9 选择 **证书存储区**：无、计算机或用户。

VPN 客户端发送证书存储区信息。

步骤 10 点击**保存**。

配置 DAP 的高级设置

您可以使用**高级 (Advanced)** 选项卡来添加除 AAA 和端点属性区域中可能存在的选择条件。例如，在您将 配置为使用 AAA 属性（这些属性满足任意、所有指定条件，或者不需要满足指定条件）时，

终端属性是累计的，并且必须全部满足。要让安全设备使用一个或另一个终端属性，您必须创建适当的 Lua 逻辑表达式，并在此处输入它们。

过程

步骤 1 选择**设备** > **VPN** > **动态访问策略**。

步骤 2 编辑 DAP 策略，然后编辑 DAP 记录。

注释
创建 DAP 策略和 DAP 记录（如果尚未创建）。

步骤 3 点击 **Advanced** 选项卡。

步骤 4 选择 **AND** 或 **OR** 作为要在 DAP 配置上使用的匹配条件。

步骤 5 在 **用于高级属性匹配的 Lua 脚本** 字段中添加 Lua 脚本。

步骤 6 要在 Lua 脚本中使用端点标准 ID，请执行以下操作：

1. 将光标放在要插入终端条件 ID 的位置。
2. 从**终端条件 (Endpoint Criteria)** 下拉列表中选择条件 a
3. 从相邻的下拉列表中选择相应的 ID。

示例：

在以下示例中，DAPTESTFILE、LIBAGENT、vpnagent 和 DUOAGENT 已被插入 Lua 脚本中：

```
EVAL(endpoint.file["DAPTESTFILE"].exists,"EQ","true") or
EVAL(endpoint.file["LIBAGENT"].exists,"EQ","true") and
EVAL(endpoint.process[""vpnagent""].exists,"EQ","true") and
EVAL(endpoint.registry[""DUOAGENT""].exists,"EQ","true")
```

步骤 7 点击**保存**。

将动态访问策略与远程访问 VPN 关联

您可以将动态访问策略 (DAP) 与远程访问 VPN 策略关联，以便在 VPN 会话身份验证和授权期间匹配动态访问策略属性。您可以在 上部署远程访问 VPN。

过程

步骤 1 选择**设备** > **远程访问**。

步骤 2 点击要与动态访问策略关联的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击远程访问 VPN 中的链接以选择动态访问策略。

步骤 4 从 **动态访问策略** 下拉列表中选择策略，或点击 **创建新的动态访问策略** 以配置新的动态访问策略。

步骤 5 点击**确定**。

步骤 6 点击**保存**以保存远程访问 VPN 策略。

当远程访问 VPN 用户尝试连接时，VPN 会检查配置的动态访问策略记录和属性。VPN 根据匹配的动态访问策略记录创建动态访问策略，并对 VPN 会话执行适当的操作。

动态访问策略的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
轻松配置动态访问策略的安全评估条件	7.7	任意	对于 DAP 策略，可以使用唯一的终端 ID 配置文件、进程或注册表终端属性。这些 ID 可用作 Lua 脚本中的终端条件以配置 DAP 记录。 新增/修改的屏幕： • 设备 > 动态访问策略 > 添加/编辑策略 > 添加状态评估条件 • 设备 **(Devices)** > 动态访问策略 **(Dynamic Access Policy)** > 添加/编辑策略 **(Add/Edit Policy)** > 添加/编辑 **DAP** 记录 **(Add/Edit DAP Record)** > 高级 **(Advanced)** > 终端条件 **(Endpoint Criteria)**
动态访问策略	7.0	任意	引入了此功能。

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。