为 VPN 配置外部 AAA 服务器

关于外部 AAA 服务器

此 ASA 可配置为使用外部 LDAP、RADIUS 或 TACACS+ 服务器来支持 ASA 的认证、授权和审计 (AAA)。外部 AAA 服务器会实施配置的权限和属性。将 ASA 配置为使用外部服务器之前，必须使用正确的 ASA 授权属性来配置外部 AAA 服务器，并从其中一部分属性向个人用户分配特定权限。

了解授权属性的策略实施

ASA 支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接的多种方法。您可以将 ASA 配置为通过以下任意组合获取用户属性：

- ASA 上的动态访问策略 (DAP)
- 外部 RADIUS 或 LDAP 身份验证和/或授权服务器
- ASA 上的组策略

如果ASA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。如果属性之间有冲突，DAP 属性优先。

ASA 按照以下顺序应用属性：

1. ASA 上的 DAP 属性 - 在 8.0(2) 版本中引入，这些属性优先于所有其他的属性。如果您在 DAP 中设置书签或 URL 列表，它会覆盖组策略中设置的书签或 URL 列表。
2. 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。请不要将这些属性与 ASA 本地 AAA 数据库中为单个用户（ASDM 中的用户账户）设置的属性混淆。

3. 在 ASA 上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=*group-policy*) 值， ASA 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。

   对于 LDAP 服务器，任何属性名称都可用于设置会话的组策略。您在 ASA 上配置的 LDAP 属性映射会将该 LDAP 属性映射至思科属性 IETF-Radius-Class。

4. 连接配置文件（在 CLI 中称为隧道组）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。连接至 ASA 的所有用户最初都属于此组，这可以提供 DAP、服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

5. ASA 分配的默认组策略 (DfltGrpPolicy) - 系统默认属性提供 DAP、用户属性、组策略或连接配置文件中缺失的所有值。

外部 AAA 服务器使用准则

ASA 会根据属性名称而不是数值 ID 来实施 LDAP 属性。RADIUS 属性会按数值 ID 而不是名称来实施。

对于 ASDM 7.0 版本，LDAP 属性包含 cVPN3000 前缀。对于 ASDM 7.1 版本及更高版本，此前缀已移除。

LDAP 属性是已在 Radius 章节中列出的 Radius 属性的子集。

配置多证书身份验证

现在，您可以使用 Secure Client SSL 和 IKEv2 客户端协议验证每个会话的多重证书。例如，可以确保计算机证书的颁发者名称匹配特定的 CA，因此，设备是公司发布的设备。

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果没有此选项，则只能对其中之一执行证书身份验证，但不能二者兼顾。

注释 由于多证书身份验证需要一个计算机证书和一个用户证书（或两个用户证书），因此不能使用 Secure Client 登录前启动 (SBL) 功能。

通过预填充用户名字段，可以解析第二个（用户）证书中的字段并将其用于 AAA 和证书身份验证连接中的后续 AAA 身份验证。始终从自客户端收到的第二个（用户）证书检索主用和辅助用户名预填充。

从 9.14(1) 开始，ASA 允许您在配置多证书身份验证并使用“身份验证”或“授权”的预填充用户名选项时指定主用户名和辅助用户名应来自哪个证书。有关信息，请参阅配置多证书用户名，第 3 页

通过多证书身份验证对两个证书进行身份验证：从自客户端收到的第二个（用户）证书解析 pre-fill 和 username-from-certificate 主用和辅助用户名。

您也可以配置通过 SAML 进行多证书身份验证。

修改现有身份验证 webvpn 属性，以包含多证书身份验证选项：

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml]
 | saml [certificate | multiple-certificate]}
```

通过多证书身份验证，可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。将在多证书身份验证期间从客户端收到的用户和计算机证书加载到 DAP，以确保能够根据证书字段配置策略。要使用动态访问策略 (DAP) 添加多证书身份验证，以设置允许或禁止连接尝试的规则，请参阅中向 *DAP* 添加多证书身份验证一节相应版本的《ASA VPN ASDM 配置指南》。

配置多证书用户名

ASA 9.14(1) 中引入了一个新命令，可用于配置 ASA 必须用作身份验证或授权的主要和辅助用户名的证书。您可以指定是使用 SSL 或 IKE 中发送的计算机证书（第一个证书）还是来自客户端的用户证书（第二个证书）来获取身份验证和授权参数。无论身份验证类型如何（**aaa**、**证书**或**多证书**），均可为任何隧道组配置此选项。但是，此配置仅对多证书身份验证（**多证书**或 **aaa 多证书**）有效。当该选项未用于多证书身份验证时，默认情况下会使用第二个证书来进行身份验证或授权。

过程

步骤 1 指定是使用第一个证书还是第二个证书中的主用户名：

username-from-certificate-choice {first-certificate | second-certificate}

步骤 2 指定是使用第一个证书还是第二个证书中的辅助用户名：

secondary-username-from-certificate-choice {first-certificate | second-certificate}

示例：

```
tunnel-group tg1 webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tg1 type remote-access
tunnel-group tg1 general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

为 VPN 配置 LDAP 授权

在 VPN 访问的 LDAP 身份验证成功后，ASA 将查询 LDAP 服务器，这会返回 LDAP 属性。这些属性通常包括应用到 VPN 会话的授权数据。

您可能需要来自 LDAP 目录服务器的授权，此授权是独立的且与身份验证机制不同。例如，如果您使用 SDI 或证书服务器进行身份验证，系统不会传回任何授权信息。对于这种情况下的用户授权，您可在身份验证成功后查询 LDAP 目录，分两步完成身份验证和授权。

如要使用 LDAP 设置 VPN 用户授权，请执行以下步骤。

过程

步骤 1 创建一个 AAA 服务器组。

aaa-server *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

示例：

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

步骤 2 创建一个名为 remotegrp 的 IPsec 远程访问隧道组。

tunnel-group *groupname*

示例：

```
hostname(config)# tunnel-group remotegrp
```

步骤 3 将服务器组和隧道组关联。

tunnel-group *groupname* **general-attributes**

示例：

```
hostname(config)# tunnel-group remotegrp general-attributes
```

步骤 4 将新隧道组分配到先前创建的 AAA 服务器组进行授权。

authorization-server-group *group-tag*

示例：

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

示例

以下示例显示启用 LDAP 的用户授权的命令。然后，该示例将创建一个名为 RAVPN 的 IPsec 远程访问隧道组，将新隧道组分配到先前创建的 LDAP AAA 服务器组进行授权：

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
```

```
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

在完成此配置工作后，接着您可以通过输入以下命令，配置其他的 LDAP 授权参数，如目录密码、搜索目录的起点和目录搜索的范围：

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

定义 ASA LDAP 配置

本节介绍如何定义 LDAP AV 对属性语法，其中包括以下信息：

- LDAP 授权支持的思科属性，第 5 页
- 思科 AV 对属性语法，第 16 页
- 思科 AV 对 ACL 示例，第 17 页

注释 ASA 会根据属性名称而不是数值 ID 来实施 LDAP 属性。另一方面，RADIUS 属性会按数值 ID 而不是名称来实施。

授权是指执行权限或属性的过程。LDAP 服务器的定义是实施权限或属性的身份验证或授权服务器（如已配置）。

对于 ASA 7.0 版本，LDAP 属性包含 cVPN3000 前缀。对于软件 7.1 及更高版本，此前缀已移除。

LDAP 授权支持的思科属性

本节提供 ASA 5500、VPN 3000 集中器和 PIX 500 系列 ASA 的完整属性列表（请参阅）。该表包括 VPN 3000 集中器和 PIX 500 系列 ASA 的属性支持信息，以帮助您配置这些设备的组合。

表 *1: ASA* 支持的思科 *LDAP* 授权属性

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Access-Hours	是	支持	支持	字符串	单值	时间范围的名称（例如，工作时间）

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Allow-Network-Extension-Mode	支持	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	支持	支持	支持	整数	单值	1 - 35791394 分钟
Authorization-Required	支持			整数	单值	0 = 否 1 = 是
Authorization-Type	是			整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	是	支持	支持	字符串	单值	无客户端和客户端 SSL VPN 以及 IPsec 客户端的标语字符串。
Banner2	是	支持	支持	字符串	单值	无客户端和客户端 SSL VPN 以及 IPsec 客户端的标语字符串。
Cisco-AV-Pair	支持	支持	支持	字符串	多值	以下格式的八位组字符串： *[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]* 有关详细信息，请参阅“思科 AV 对属性语法”部分。
Cisco-IP-Phone-Bypass	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Client-Intercept-DHCP-Configure-Msg	支持	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Client-Type-Version-Limiting	是	支持	支持	字符串	单值	IPsec VPN 客户端版本号字符串
Confidence-Interval	支持	支持	支持	整数	单值	10 - 300 秒
DHCP-Network-Scope	是	支持	支持	字符串	单值	IP 地址
DN-Field	支持	支持	支持	字符串	单值	可能的值：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER 和 use-entire-name

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Firewall-ACL-In		支持	支持	字符串	单值	访问列表 ID
Firewall-ACL-Out		支持	支持	字符串	单值	访问列表 ID
Group-Policy		是	支持	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2 版本及更高版本，请改用此属性而非 IETF-Radius-Class。您可以使用以下三种格式之一： • 组策略名称 • OU= 组策略名称 • OU= 组策略名称：
IE-Proxy-Bypass-Local				布尔值	单值	0 = 已禁用 1 = 已启用
IE-Proxy-Exception-List				字符串	单值	DNS 域列表。条目必须以新的行字符序列 (\n) 分隔。
IE-Proxy-Method	支持	支持	支持	整数	单值	1 = 不修改代理设置 2 = 不使用代理 3 = 自动检测 4 = 使用 ASA 设置
IE-Proxy-Server	支持	支持	支持	整数	单值	IP 地址
IETF-Radius-Class	支持	支持	支持		单值	为远程访问 VPN 会话设置组策略。对于 8.2 版本及更高版本，请改用此属性而非 IETF-Radius-Class。您可以使用以下三种格式之一： • 组策略名称 • OU= 组策略名称 • OU= 组策略名称：
IETF-Radius-Filter-Id	支持	支持	支持	字符串	单值	在 ASA 上定义的访问列表名称。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	支持	支持	支持	字符串	单值	IP 地址。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IETF-Radius-Framed-IP-Netmask	支持	支持	支持	字符串	单值	IP 地址掩码。该设置适用于 VPN 远程访问 IPsec 和 SSL VPN 客户端。
IETF-Radius-Idle-Timeout	支持	支持	支持	整数	单值	秒
IETF-Radius-Service-Type	支持	支持	支持	整数	单值	1 = 登录 2 = 成帧 5 = 远程访问 6 = 管理 7 = NAS 提示符
IETF-Radius-Session-Timeout	支持	支持	支持	整数	单值	秒
IKE-Keep-Alives	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication	支持	支持	支持	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅限授权） 3 = NT 域 4 = SDI (RSA) 5 = 内部 6 = 具有有效期的 RADIUS 7 = Kerberos 或 Active Directory
IPsec-Auth-On-Rekey	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	是	支持	支持	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	是	支持	支持	字符串	单值	1 = 使用客户端配置的列表 2 = 已禁用并清除客户端列表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name	支持			字符串	单值	指定要作为防火墙策略推送到客户端的过滤器的名称。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IPsec-Client-Firewall-Filter-Optional	支持	支持	支持	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	是	支持	支持	字符串	单值	指定要发送到客户端的单个默认域名（1 到 255 个字符）。
IPsec-Extended-Auth-On-Rekey		支持	支持	字符串	单值	字符串
IPsec-IKE-Peer-ID-Check	是	支持	支持	整数	单值	1 = 必需 2 = 如果受对等体证书支持 3 = 不检查
IPsec-IP-Compression	是	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	是	支持	支持	整数	单值	4001 - 49151；默认值为 10000。
IPsec-Required-Client-Firewall-Capability	是	支持	支持	整数	单值	0 = 无 1 = 远程防火墙 Are-You-There (AYT) 定义的策略 2 = 策略推送的 CPP 4 = 来自服务器的策略
IPsec-Sec-Association	支持			字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	是	支持	支持	字符串	单值	指定要发送到客户端的辅助域名列表（1 到 255 个字符）。
IPsec-Split-Tunneling-Policy	是	支持	支持	整数	单值	0 = 全部隧道化 1 = 分割隧道 2 = 允许本地 LAN
IPsec-Split-Tunnel-List	是	支持	支持	字符串	单值	指定用于描述分割隧道包含列表的网络或访问列表的名称。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
IPsec-Tunnel-Type	是	支持	支持	整数	单值	1 = LAN 对 LAN 2 = 远程访问
L2TP-Encryption	支持			整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 无状态请求 15 = 40/128 位加密/无状态请求
L2IP-MPPC-Compression	支持			整数	单值	0 = 已禁用 1 = 已启用
MS-Client-Subnet-Mask	是	支持	支持	字符串	单值	IP 地址
PFS-Required	支持	支持	支持	布尔值	单值	0 = 否 1 = 是
Port-Forwarding-Name	支持	支持		字符串	单值	名称字符串（例如，“Corporate-Apps”）
PPTP-Encryption	支持			整数	单值	位图： 1 = 要求加密 2 = 40 位 4 = 128 位 8 = 无状态请求 示例： 15 = 40/128 位加密/无状态请求
PPTP-MPPC-Compression	支持			整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	是	支持	支持	字符串	单值	IP 地址
Primary-WINS	是	支持	支持	字符串	单值	IP 地址
Privilege-Level				整数	单值	对于用户名，0 - 15

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Required-Client-Firewall-Vendor-Code	是	支持	支持	整数	单值	1 = 思科系统公司（带思科集成客户端） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5=思科系统公司（带思科入侵防御安全代理）
Required-Client-Firewall-Description	支持	支持	支持	字符串	单值	—
Required-Client-Firewall-Product-Code	支持	支持	支持	整数	单值	思科系统公司产品： 1=思科入侵防御安全代理或思科集成客户端 (CIC) Zone Labs 产品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defender/代理 Sygate 产品： 1 = 个人防火墙 2 = 个人防火墙专业版 3 = 安全代理
Require-HW-Client-Auth	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
Require-Individual-User-Auth	支持	支持	支持	整数	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	是	支持	支持	字符串	单值	IP 地址
Secondary-WINS	是	支持	支持	字符串	单值	IP 地址
SEP-Card-Assignment				整数	单值	未使用
Simultaneous-Logins	是	支持	支持	整数	单值	0-2147483647

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
Strip-Realm	是	支持	支持	布尔值	单值	0 = 已禁用 1 = 已启用
TACACS-Authtype	支持	支持	支持	整数	单值	—
TACACS-Privilege-Level	支持	支持	支持	整数	单值	—
Tunnel-Group-Lock		是	支持	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	是	支持	支持	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 和 4 相互排斥 （合法值为 0-11、16-27、32-43，以及 48-59 ）。
Use-Client-Address	支持			布尔值	单值	0 = 已禁用 1 = 已启用
User-Auth-Server-Name	支持			字符串	单值	IP 地址或主机名
User-Auth-Server-Port	支持	支持	支持	整数	单值	服务器协议的端口号
User-Auth-Server-Secret	支持			字符串	单值	服务器密码
WebVPN-ACL-Filters		支持		字符串	单值	Webtype 访问列表名称
WebVPN-Apply-ACL-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用 对于 8.0 及更高版本，此属性并非必需。
WebVPN-Citrix-Support-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用 对于 8.0 及更高版本，此属性并非必需。

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
WebVPN-Enable-functions				整数	单值	未使用 - 已弃用
WebVPN-Exchange-Server-Address				字符串	单值	未使用 - 已弃用
WebVPN-Exchange-Server-NETBIOS-Name				字符串	单值	未使用 - 已弃用
WebVPN-File-Access-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Forwarded-Ports		支持		字符串	单值	端口转发列表名称
WebVPN-Homepage	支持	支持		字符串	单值	URL，例如 http://www.example.com
WebVPN-Macro-Substitution-Value1	支持	支持		字符串	单值	例如，请参阅位于以下 URL 的《SSL VPN 部署指南》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution-Value2	支持	支持		字符串	单值	例如，请参阅位于以下 URL 的《SSL VPN 部署指南》： http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Auto-Download-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用

属性名称	VPN 3000	ASA	PIX	语法/类型	单值或多值	可能的值
WebVPN-Single-Sign-On-Server-Name	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Client-DPD	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Compression	是	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Enable	支持	支持		布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Gateway-DPD	支持	支持		整数	单值	0 = 已禁用 n = 失效对等体检测值，以秒为单位 (30 - 3600)
WebVPN-SVC-Keepalive	支持	支持		整数	单值	0 = 已禁用 n = 保持连接值，以秒为单位 (15 - 600)
WebVPN-SVC-Keep-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-Rekey-Method	是	支持		整数	单值	0 = 无 1 = SSL 2 = 新隧道 3 = 任意（设置为 SSL）
WebVPN-SVC-Rekey-Period	支持	支持		整数	单值	0 = 已禁用 n = 重试时间，以分钟为单位 (4 - 10080)
WebVPN-SVC-Required-Enable	支持	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-Entry-Enable	是	支持		整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-List		是		字符串	单值	URL 列表名称

ACL 中支持的 URL 类型

URL 可以是部分 URL，包含服务器的通配符或包含端口。

支持以下 URL 类型。

任何 URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

使用思科 AV 对 (ACL) 的准则

- 使用带有 ip:inacl# 前缀的思科 AV 对条目来对远程 IPsec 和 SSL VPN 客户端 (SVC) 隧道实施访问列表。
- 使用带有 webvpn:inacl# 前缀的思科 AV 对条目来对 SSL VPN 无客户端（浏览器模式）隧道实施访问列表。
- 对于 Webtype ACL，您不用指定源，因为 ASA 就是源。

表 *2: ASA* 支持的令牌

令牌	语法字段	说明
ip:inacl# *Num* =	不适用（标识符）	（其中 *Num* 是唯一的整数。）启动所有 AV 对访问控制列表。对远程 IPsec 和 SSL VPN (SVC) 隧道实施访问列表。
webvpn:inacl# *Num* =	不适用（标识符）	（其中 *Num* 是唯一的整数。）启动所有无客户端 SSL AV 对访问控制列表。对无客户端（浏览器模式）隧道实施访问列表。
deny	操作	拒绝操作。（默认）
permit	操作	允许操作。
icmp	协议	互联网控制消息协议 (ICMP)
1	协议	互联网控制消息协议 (ICMP)
IP	协议	Internet 协议 (IP)
0	协议	Internet 协议 (IP)
TCP	协议	传输控制协议 (TCP)
6	协议	传输控制协议 (TCP)

令牌	语法字段	说明
UDP	协议	用户数据报协议 (UDP)
17	协议	用户数据报协议 (UDP)
any	主机名	规则适用于任何主机。
host	主机名	表示主机名的任何字母数字字符串。
log	记录	发生该事件时，系统会显示过滤器日志消息。（与 permit 和 log 或 deny 和 log 相同。）
lt	运算符	小于值
gt	运算符	大于值
eq	运算符	等于值
neq	运算符	不等于值
range	运算符	包含范围。应后跟两个值。

思科 AV 对属性语法

思科属性值 (AV) 对（ID 编号 26/9/1）可用于从 RADIUS 服务器（例如思科 ACS）或通过 LDAP 属性映射从 LDAP 服务器来实施访问列表。

每个 Cisco-AV-Pair 规则的语法如下：

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 *3: AV* 对属性语法规则

字段	说明
操作	规则与拒绝或允许匹配时要执行的操作。
目标	接收数据包的网络或主机。将其指定为 IP 地址、主机名或 **any** 关键字。如果使用 IP 地址，则必须遵循源通配符掩码。
目标通配符掩码	适用于目标址的通配符掩码。
记录	生成过滤器日志消息。您必须使用此关键字生成严重性级别为 9 的事件。
运算符	逻辑运算符：大于、小于、等于、不等于。
端口	TCP 或 UDP 端口号，范围为 0 - 65535。

字段	说明
前缀	AV 对的唯一标识符（例如：ip:inacl#1= 表示标准访问列表或 webvpn:inacl# = 无客户端 SSL VPN 访问列表）。仅当过滤器作为 AV 对发送时才会显示此字段。
协议	IP 协议的名称或编号。0-255 范围内的整数或以下关键字之一：**icmp**、**igmp**、**ip**、**tcp**、**udp**。
源	发送数据包的网络或主机。将其指定为 IP 地址、主机名或 **any** 关键字。如果使用 IP 地址，则必须遵循源通配符掩码。此字段不适用于无客户端 SSL VPN，因为 ASA 具有源或代理角色。
源通配符掩码	适用于源地址的通配符掩码。此字段不适用于无客户端 SSL VPN，因为 ASA 具有源或代理角色。

思科 AV 对 ACL 示例

本节显示思科 AV 对的示例，并介绍导致的允许或拒绝操作。

注释 inacl# 中的每个 ACL # 必须是唯一的。但是，它们不需要是连续的（例如，1、2、3、4）。也就是说，它们可能是 5、45、135。

表 4: 思科 *AV* 对及其允许或拒绝操作的示例

思科 AV 对示例	允许或拒绝操作
`ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log`	允许使用完整隧道 IPsec 或 SSL VPN 客户端的两台主机之间的 IP 流量。
`ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log`	仅允许使用完整隧道 IPsec 或 SSL VPN 客户端将 TCP 流量从端口 80 传输到特定主机。
`webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share`	允许流向指定 URL 的无客户端 SSL VPN 流量，拒绝流向特定服务器的 SMTP 流量，并允许流向指定服务器的文件共享访问 (CIFS)。
`webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log`	拒绝 Telnet 访问并允许分别在非默认端口 2323 和 2222 上进行 SSH 访问，或允许使用这些端口的其他应用流量进行无客户端 SSL VPN 访问。
`webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23`	分别允许对默认端口 22 进行无客户端 SSL VPN SSH 访问，并拒绝对端口 23 进行 Telnet 访问。此示例假定您使用的是这些 ACL 实施的 Telnet 或 SSH Java 插件。

Active Directory/LDAP VPN 远程访问授权示例

本节提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例程序。包括以下主题：

Cisco.com 提供的其他配置示例包括以下技术说明。

- ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例
- PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略

基于用户的属性的策略实施

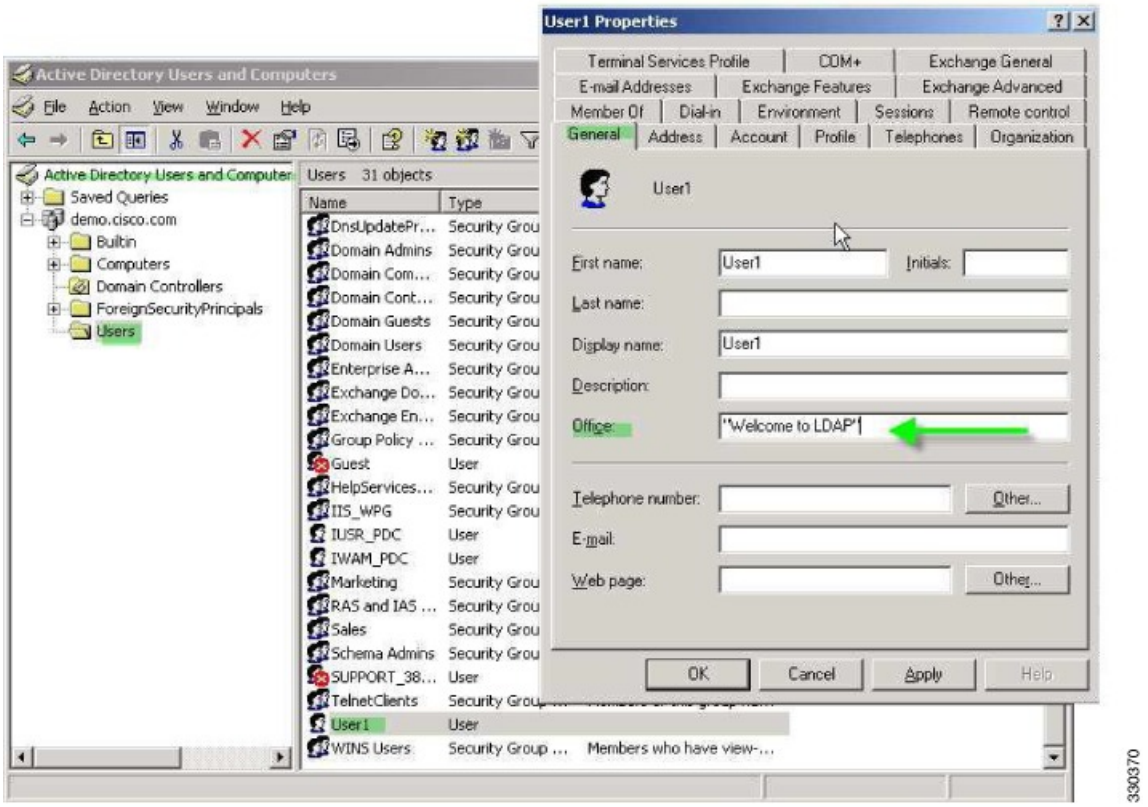
此示例向用户显示一个简单的欢迎信息，说明如何将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，或者将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。此示例适用于任意连接类型，包括 IPSec VPN 客户端和 Secure Client。

如要为 AD LDAP 服务器上配置的用户实施简单的欢迎信息，请使用 General 选项卡中的 Office 字段输入欢迎信息文本。此字段使用名为 physicalDeliveryOfficeName 的属性。在 ASA 中，创建将 physicalDeliveryOfficeName 映射至思科属性 Banner1 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射至思科属性 Banner1，然后向用户显示该欢迎信息。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**常规 (General)** 选项卡，在“办公室”(Office) 字段中输入欢迎信息文本，该字段使用 AD/LDAP 属性 physicalDeliveryOfficeName。



步骤 2 在 ASA 上创建一个 LDAP 属性映射。

创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至思科属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

步骤 4 测试此欢迎信息的实施。

为 Secure Client 隧道实施静态 IP 地址分配

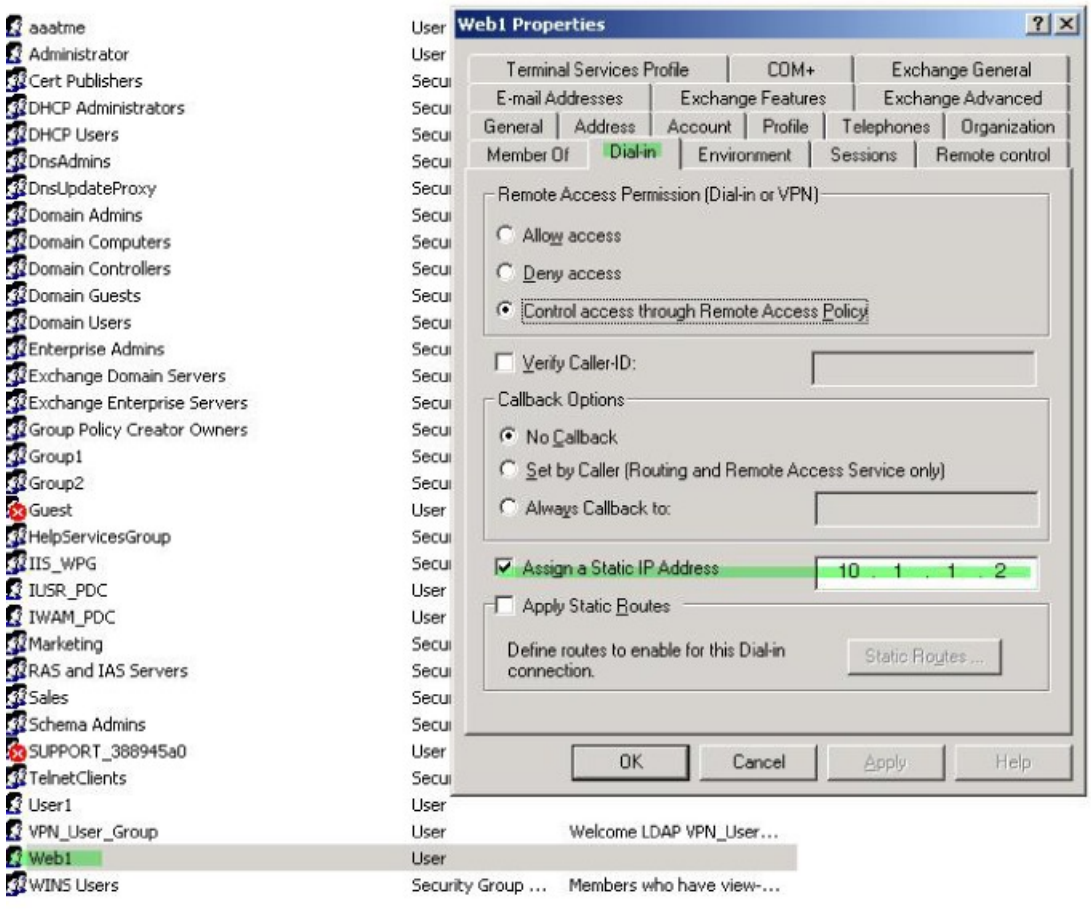
此示例适用于完全隧道客户端，例如 IPsec 客户端和 SSL VPN 客户端。

如要实施静态 Secure Client 静态 IP 分配，请将 Secure Client用户 Web1 配置为接受静态 IP 地址，在 AD LDAP 服务器上的 Dialin 选项卡的 Assign Static IP Address 字段中输入地址（此字段使用 msRADIUSFramedIPAddress 属性），然后创建一个可将该属性映射至思科属性 IETF-Radius-Framed-IP-Address 的属性映射。

在身份验证过程中，ASA 从服务器检索 msRADIUSFramedIPAddress 的值，将该值映射至思科属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，选中**分配静态 IP 地址 (Assign Static IP Address)** 复选框并输入 IP 地址 10.1.1.2。



步骤 2 为显示的 LDAP 配置创建一个属性映射。

将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至思科属性 IETF-Radius-Framed-IP-Address：

```
hostname(config)# ldap attribute-map static_address
```

```
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 static_address：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

步骤 4 通过查看此部分的配置，验证是否已配置 **vpn-address-assignment** 命令来指定 AAA：

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

步骤 5 使用 Secure Client建立与 ASA 的连接。观察用户是否收到在服务器上配置并映射至 ASA 的 IP 地址。

步骤 6 使用 **show vpn-sessiondb svc** 命令来查看会话详细信息，并验证分配的地址：

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

实施拨入允许或拒绝访问

本示例创建指定用户允许的隧道协议的 LDAP 属性映射。您可以将 Dialin 选项卡中的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持以下映射值：

值	隧道协议
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec

值	隧道协议
16	无客户端 SSL
32	SSL 客户端 - Secure Client 或 SSL VPN 客户端
64	IPsec (IKEv2)

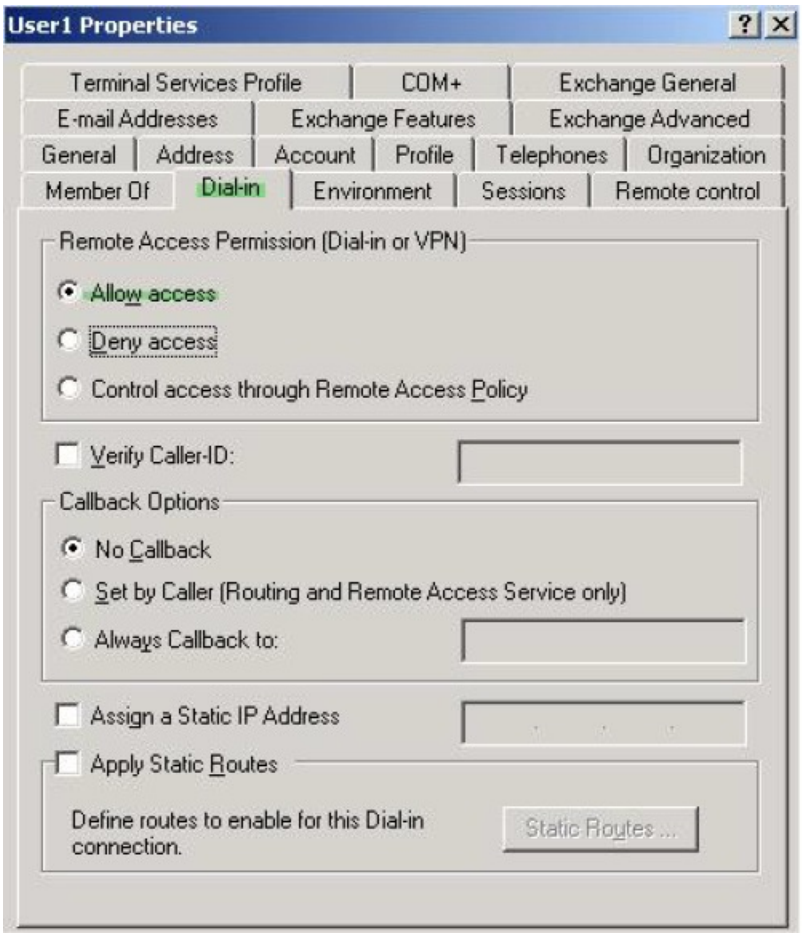
[1] (1) 不能同时支持 IPsec 和 L2TP over IPsec。因此，值 4 和 8 只能二选其一。
[2] (2) 请参阅注释 1。

使用此属性创建协议的允许访问 (TRUE) 或拒绝访问 (FALSE) 条件，并实施允许用户访问的方法。

有关实施拨入允许访问或拒绝访问的其他示例，请参阅以下技术说明：ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，再点击“允许访问”(Allow Access) 单选按钮。



注释
如果您通过“远程访问策略”(Remote Access Policy) 选项选择控制访问，则服务器不会返回值，而实施的权限则根据 ASA 的内部组策略设置而定。

步骤 2 创建一个允许 IPsec 和 Secure Client 连接，但是拒绝无客户端 SSL 连接的属性映射。

a) 创建映射 tunneling_protocols：

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) 将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射至思科属性 Tunneling-Protocols：

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 添加映射值：

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

a) 进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 关联您创建的属性映射 tunneling_protocols：

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

步骤 4 验证属性映射是否按配置工作。

尝试使用无客户端 SSL 的连接，用户应接到通知，告知其未经授权的连接机制是连接失败的原因。IPSec 客户端应该可以连接，因为根据属性映射，IPsec 是允许的隧道协议。

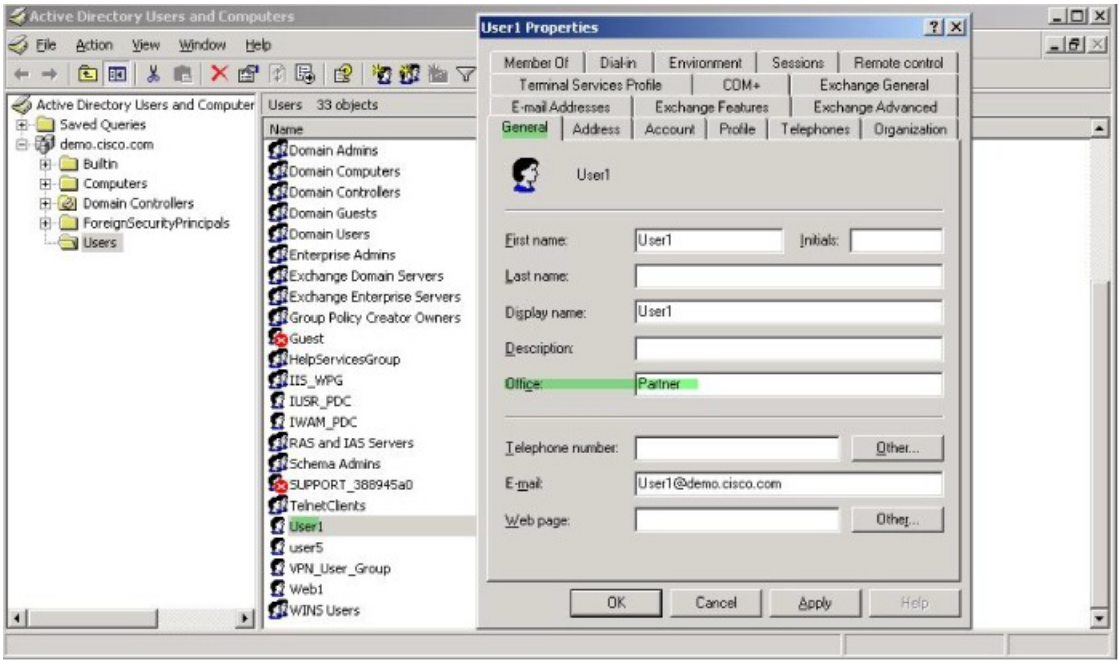
实施登录时长和时间规则

以下示例展示如何配置和实施允许无客户端 SSL 用户（例如业务合作伙伴）访问网络的时长。

在 AD 服务器上，使用 Office 字段输入合作伙伴的名称，该字段使用 physicalDeliveryOfficeName 属性。然后我们在 ASA 上创建一个可将该属性映射至思科属性 Access-Hours 的属性映射。在身份验证过程中，ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射至 Access-Hours。

过程

步骤 1 选择用户，右键点击**属性 (Properties)**，然后打开**常规 (General)** 选项卡：



步骤 2 创建属性映射。

创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射至思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您创建的属性映射 access_hours：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

步骤 4 为服务器上允许的每个值配置时间范围。

将合作伙伴访问时长配置为周一至周五上午 9 点到下午 5 点：

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

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。