# 领域

以下主题介绍领域和身份策略：



## 领域的许可证要求

**威胁防御 许可证**

任意

## 领域的要求和前提条件

**型号支持**

任意。

**支持的域**

任意

### 用户角色

- 管理员
- 访问管理员
- 网络管理员

# 创建 Microsoft Azure AD (SAML) 领域

您可以将 Microsoft Azure Active Directory（AD，现称为 *Entra ID*）领域用于被动身份验证或主动身份验证。

如果启用了变更管理，则必须批准此程序中使用的所有证书。打开新故障单或编辑现有故障单。有关详细信息，请参阅创建变更管理故障单和。支持变更管理的策略和对象

### 被动身份验证

被动身份验证发生在用户利用 Cisco ISE 进行身份验证时。

您有以下选项，具体取决于您选择的用户和组存储库：

- 将 Cisco ISE 用作用户存储库，并使用 Entra ID 执行被动身份验证。有关详细信息，请参阅：
  - 关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE ，第 4 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ，第 4 页
- 要从 Entra ID 下载组。

  有关设置 Entra ID 的详细信息，请参阅为被动身份验证配置 Microsoft Entra ID，第 5 页。

### 主动身份验证

主动身份验证发生在用户通过预先配置的托管设备进行身份验证时。强制网络门户又称为主动身份验证。主动身份验证通常使用与被动身份验证相同的用户存储库（ISE/ISE-PIC TS 代理和 被动身份代理例外，它们仅是被动身份验证）。

要将 Microsoft Entra ID 用作强制网络门户，需要用户使用 Entra ID 进行身份验证。我们将领域称为安全断言标记语言 (SAML) 领域，因为 SAML 用于在以下各项之间建立信任关系：

- 服务提供商 （向其发送身份验证请求的 Cisco Secure Firewall Threat Defense 个设备）。
- 身份提供程序 (Microsoft Entra ID)。

SAML 是由 OASIS 标准机构开发的开放标准；有关详细信息，请参阅 SAML 概述。

有关详细信息，请参阅如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户），第 13 页。

# 如何为被动身份验证创建 Microsoft Azure AD (SAML)

本主题讨论创建 Microsoft Azure AD (SAML) 领域以用于 Cisco Secure Firewall Management Center 的被动身份验证（现在被称作额外 *ID*）的高级任务。

## 过程

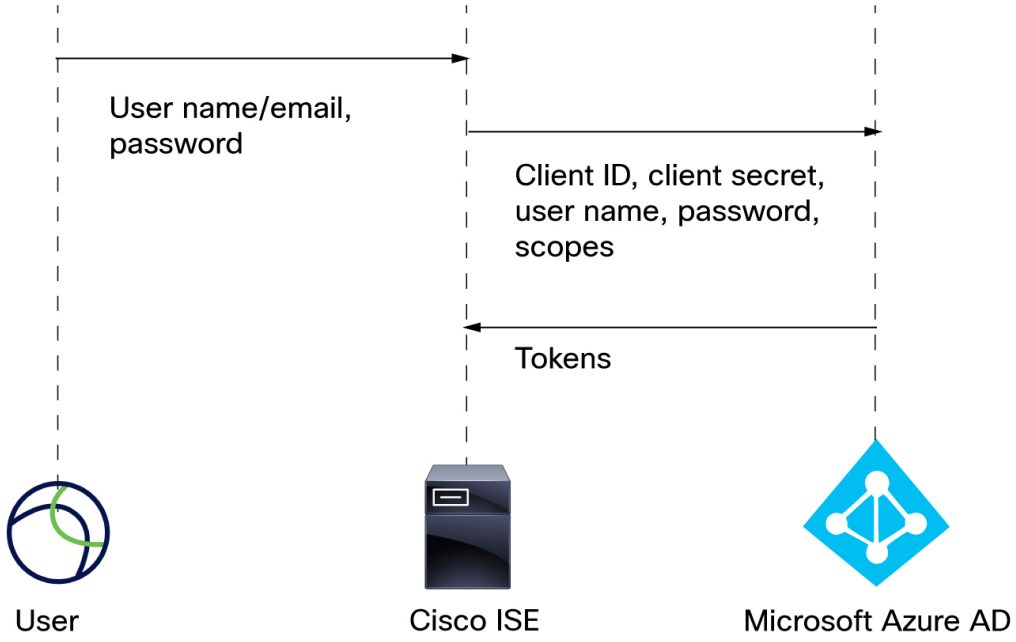
| | 命令或操作 | 目的 |
|---|---|---|
| **步骤 1** | 启用Cisco Secure Dynamic Attributes Connector。 | Cisco Secure Dynamic Attributes Connector 要使用 Microsoft Azure AD (SAML) 领域。您可以先执行此操作，也可以在创建领域时启用它。有关详细信息，请参阅启用 Cisco Secure Dynamic Attributes Connector。 |
| **步骤 2** | 配置 Microsoft Entra ID | 需要执行多项配置任务，包括设置事件中心、向应用授予访问 Microsoft Graph API 的权限以及启用审核日志。<br><br>请参阅为被动身份验证配置 Microsoft Entra ID ， 第 5 页。 |
| **步骤 3** | 配置 Cisco ISE。 | 配置 ISE 的方式取决于用户对您的系统进行身份验证的方式。有关详细信息，请参阅如何为 Microsoft Azure AD (SAML)配置 ISE ，第 5 页。 |
| **步骤 4** | 创建 Cisco ISE 身份源。 | 身份源使 ISE 能够与 Cisco Secure Firewall Management Center通信。 |
| **步骤 5** | 获取配置 Microsoft Azure AD (SAML) 领域所需的信息。 | 此信息包括客户端和租户 ID、客户端密钥以及 Microsoft Azure AD 中存储的其他信息。 |
| **步骤 6** | 配置并验证您的领域。 | 在开始在访问控制策略中使用该领域的配置之前，请对其进行测试。<br><br>如创建 Microsoft Azure AD (SAML) 领域 ， 第 2 页中所述，创建 Microsoft Azure AD (SAML) 领域。 |
| **步骤 7** | 使用 Microsoft Azure AD (SAML) 领域创建访问控制策略和规则。 | 与其他类型的领域不同，您不需要创建身份策略或将身份策略与访问控制策略相关联。<br><br>请参阅创建基本访问控制策略和创建和编辑访问控制规则。 |

### 下一步做什么

请参阅关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE ， 第 4 页。

# 关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE

下图总结了具有 Cisco ISE 和资源拥有的密码凭证 (ROPC) 的 Azure AD 领域：




使用 ROPC，

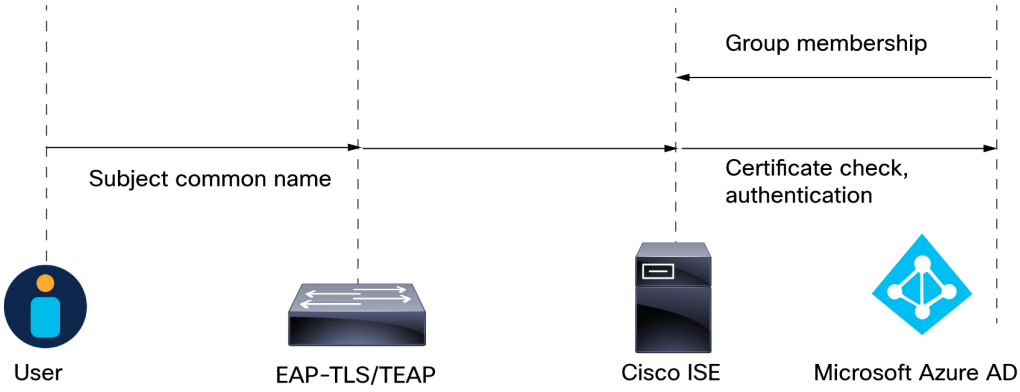
1. 用户使用 VPN 客户端（例如 Cisco Secure Client）使用用户名（或邮件地址）和密码登录。
2. 客户端 ID、客户端密钥、用户名、密码和范围将发送到 Entra ID。
3. 令牌从 Azure AD 发送到 Cisco ISE，然后将用户会话发送到 Cisco Secure Firewall Management Center。

有关配置 Cisco ISE 的详细信息，请参阅 使用 Azure Active Directory 配置 ISE 3.0 REST ID。

其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

# 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE

RFC7170定义的隧道可扩展身份验证协议 (TEAP) 可与 ISE 配合使用， Cisco Secure Firewall Management Center 如下所示：




以下内容基于 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS：

1. 用户的证书通过 EAP-TLS 或使用 EAP-TLS 作为内部方法的 TEAP 发送到 ISE。
2. ISE 评估用户的证书（有效期、受信任的证书颁发机构、证书吊销列表等）。
3. ISE 获取证书使用者名称 (CN) 并查询 Azure Graph API 以获取用户的组和其他属性。这被 Azure 称为用户主体名称 (UPN)。
4. ISE 授权策略根据从 Azure 返回的用户属性进行评估。

## 如何为 Microsoft Azure AD (SAML)配置 ISE

在 Microsoft Azure AD (SAML)（现在称为 *Entra ID*）领域，ISE 负责向 Cisco Secure Firewall Management Center 发送用户会话（登录、注销）。本主题讨论如何设置 ISE 以便与 Azure AD 领域配合使用。

### 资源拥有的密码凭证身份验证

要在资源所有者密码凭证 (ROPC) 的帮助下，通过具象状态传输 (REST) 身份 (ID) 服务将 ISE 与 Microsoft Azure AD (SAML) 配合使用，请参阅使用 Azure Active Directory 配置 ISE 3.0 REST ID。

### TEAP/EAP-TLS

要将 ISE 与基于 Azure AD 组成员身份和其他用户属性的授权策略配合使用，并将 EAP-TLS 或 TEAP 作为身份验证协议，请参阅 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS。

### 后续操作

获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页

## 为被动身份验证配置 Microsoft Entra ID

本主题提供有关如何设置 Microsoft Entra ID（以前称为 *Microsoft Azure Active Directory (AD)*）作为您可以与 Cisco Secure Firewall Management Center 一起使用的领域的基本信息。我们假设您已经熟悉 Entra ID；如果不熟悉，请在开始之前查阅文档或支持资源。

### 为您的应用授予 Microsoft Graph 权限

如 Microsoft 网站上的《授权和 Microsoft Graph 安全 API》中所述，向您的 Entra ID 应用授予以下 Microsoft Graph 权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限使 Cisco Secure Firewall Management Center 能够首次从 Entra ID 下载用户和组。

在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域所需的此步骤的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

### 设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。Cisco Secure Firewall Management Center 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

**重要事项** 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域所需的此步骤的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

### 启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

### 为 Entra ID 配置 Cisco ISE

要向 Cisco Secure Firewall Management Center 发送用户会话信息，请按照《配置 ISE 3.0 REST ID 与 Azure Active Directory》中所述为 Entra ID 配置 Cisco ISE。

### 后续操作

请参阅如何为 Microsoft Azure AD (SAML)配置 ISE，第 5 页。

## 配置 Entra ID 基本设置

### 为您的应用授予 Microsoft Graph 权限

如 Microsoft 站点上的授权和 Microsoft Graph 安全 API 中所述，向 Entra ID（之前称为 *Azure AD*）应用授予 Microsoft Graph 的以下权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限让 防火墙管理中心 能够首次从 Entra ID 下载用户和组。

对于在 防火墙管理中心 中设置 Entra ID 领域，此步骤所需的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

### 设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。防火墙管理中心 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

**重要事项** 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

对于在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

### 启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

## 获取 Microsoft Azure AD (SAML) 领域所需的信息

本任务介绍如何获取在 Cisco Secure Firewall Management Center 中设置 Microsoft Azure AD (SAML)（现称为 *Entra ID*）领域所需的信息。您在按照 为被动身份验证配置 Microsoft Entra ID，第 5 页中的说明设置 Microsoft Entra ID 时，可能已获取此信息。

### 过程

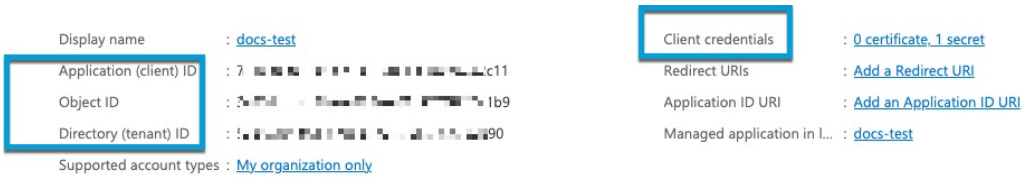
**步骤 1** 以至少具有产品设计师角色的用户身份登录 https://portal.azure.com/。

**步骤 2** 在页面顶部，点击 **Microsoft Entra ID**。

**步骤 3** 在左侧列中，点击**应用注册 (App Registrations)**。

**步骤 4** 如有必要，过滤显示的应用列表以便显示要使用的应用。

**步骤 5** 点击应用的名称。




**步骤 6** 点击此页面上以下值旁边的 **复制** ()，然后将这些值粘贴到文本文件中。

- **应用（客户端）ID**
- **目录（租户）ID**

**步骤 7** 点击**客户端凭证 (Client Credentials)**。

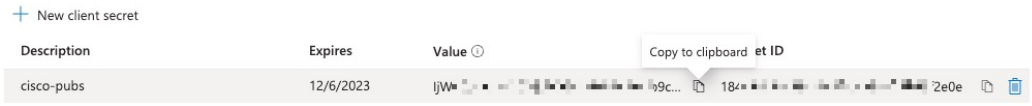
**步骤 8** 除非您已经知道客户端密钥值 （而不是客户端密钥 *ID*），否则必须按如下方式创建新的客户端密钥：

a) 点击**新建客户端密钥 (New Client Secret)**。

b) 在提供的字段中输入要求的信息。

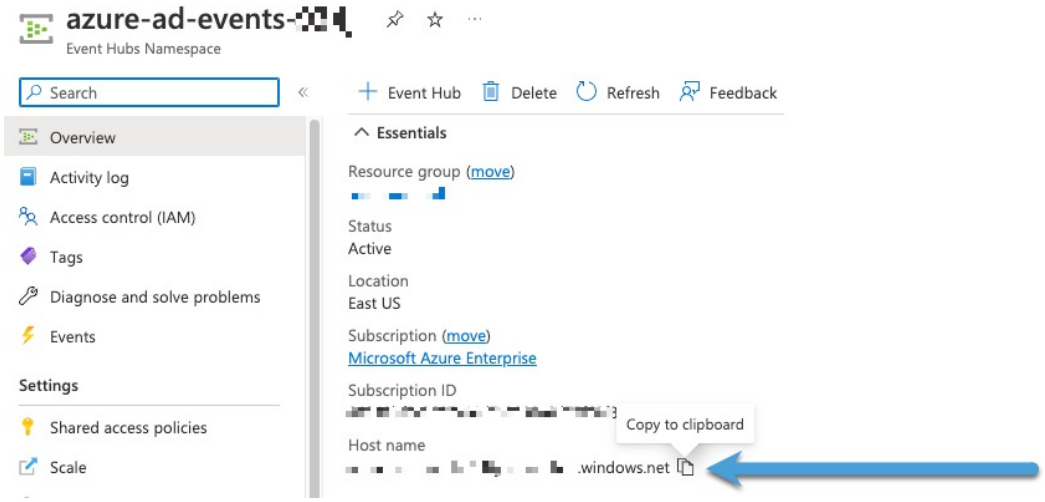
c) 点击**添加 (Add)**。

d) 点击 Value 旁边的 **复制** ()，如下图所示。




**步骤 9** 在 https://portal.azure.com/ 中，点击**事件中心 (Event Hubs)** > （事件中心的名称）。

**步骤 10** 在右侧窗格中，点击 **主机名 (Host name)** 值旁边的 **复制** (⧉) 并将值粘贴到剪贴板。这是事件中心主机名。

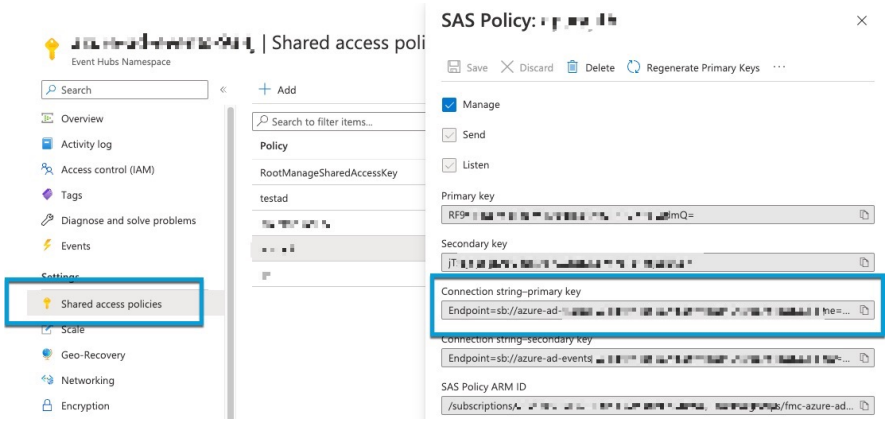



**步骤 11** 记下事件中心的名称或将其复制到文本文件（与页面顶部的**事件中心命名空间 (Event Hubs Namespace)** 相同）。

**步骤 12** 在左侧窗格中的设置下，点击**共享访问策略 (Shared access policies)**。

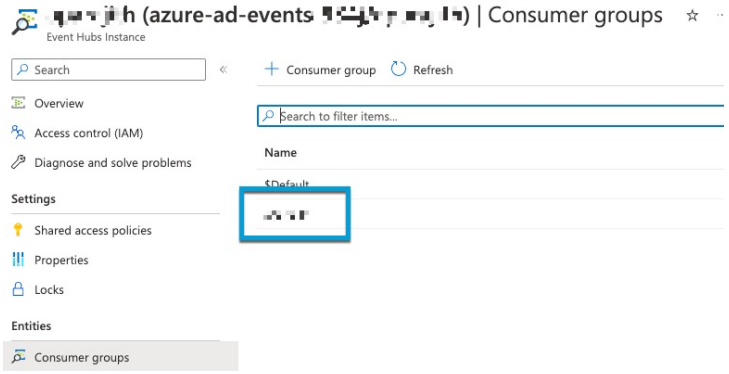
**步骤 13** 点击策略名称。

**步骤 14** 点击**连接字符串 - 主键 (Connection string-primary key)** 旁边的 **复制** (⧉)。




**步骤 15** 点击 **概述 (Overview)** > **实体 (Entities)** > **事件中心 (Event Hubs)** > （事件中心的名称） > **实体 (Entities)** > **使用者组 (Consumer Groups)**。

记下以下值或将其复制到剪贴板。这是您的使用者组名称。




**步骤 16** 在左侧窗格中点击**概览 (Overview)**。

**步骤 17** 点击**命名空间 (Namespace)** 旁边的 **复制** ()。


这是事件中心主题名称。

# 为被动身份验证创建 Microsoft Azure AD (SAML) 领域

以下主题讨论如何运行创建用于被动身份验证的 Microsoft Azure AD (SAML)（现称为 *Entra ID*）领域所需的多步骤向导。

您可以将 Microsoft Azure Active Directory (AD) 领域与 Cisco ISE 配合使用来对用户进行身份验证并获取用户会话以进行用户控制。我们从 Entra ID 获取组，并从 Cisco ISE 获取已登录用户会话数据。

您有以下选择：

- 资源拥有的密码凭证 (ROPC)：使用户能够使用用户名和密码通过 Cisco Secure Client 等客户端登录。ISE 将用户会话发送到 Cisco Secure Firewall Management Center。有关详细信息，请参阅关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE ， 第 4 页。

  其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

- 可扩展身份验证协议 (EAP) 链与基于隧道的可扩展身份验证协议 (TEAP) 和传输层安全 (TLS)，缩写为 EAP/TEAP-TLS：TEAP 是一种基于隧道的 EAP 方法，可建立安全隧道并执行其他 EAP 方法在该安全隧道的保护下。ISE 用于验证用户凭证并将用户会话发送到 Cisco Secure Firewall Management Center。有关详细信息，请参阅关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ， 第 4 页。

要配置领域，请按以下顺序完成所有任务：

1. 配置 Entra ID 基本设置， 第 7 页。

2. 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页 中所述。
3. Microsoft Azure AD (SAML) 领域：SAML 详细信息，第 11 页。

## Microsoft Azure AD (SAML) 领域：SAML 详细信息

此任务讨论创建 Microsoft Azure AD (SAML) 领域的多步骤向导中的第一步。您必须完成向导中的所有步骤才能设置领域。根据您创建的领域是用于主动身份验证还是被动身份验证，这些步骤会有所不同。

### 开始之前

在创建领域之前，请完成以下所有任务：

- （仅使用 Cisco ISE 进行被动身份验证。）如果您使用 Cisco ISE 作为用户和组的存储库，请设置 ISE：
  - 关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE，第 4 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE，第 4 页
- 要将 Entra ID 用作用户和组的存储库，请参阅为被动身份验证配置 Microsoft Entra ID，第 5 页。
- 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页中所述。

### 过程

**步骤 1** 登录Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 点击 **添加领域** > **SAML - Azure AD**。

**步骤 4** 输入以下信息。

| 项目 | 说明 |
|---|---|
| 名称 | 用于标识领域的唯一名称。 |
| 说明 | （可选。）领域的描述。 |
| 身份提供程序 | 始终显示 **Azure AD**。 |

| 项目 | 说明 |
| --- | --- |
| 配置类型 | 点击以下选项之一：<br>• **使用 ISE 进行被动身份验证，以**进行被动身份验证。<br>• **使用 Azure AD 的被动身份验证或强制网络门户**，以便将 Entra ID 用作被动身份验证或主动身份验证（即强制网络门户）的用户存储。 |

**步骤 5** 点击**下一步 (Next)**。

### 下一步做什么

以下项之一：

- 被动身份验证：Microsoft Azure AD (SAML) 领域：Azure AD 详细信息，第 12 页。
- 主动身份验证：Microsoft Azure AD (SAML) 领域：SAML 服务提供商 (SP) 元数据，第 24 页

## Microsoft Azure AD (SAML) 领域：Azure AD 详细信息

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

### 过程

**步骤 1** 从向导中的上一步继续操作。

**步骤 2** 输入以下信息。

| 项目 | 说明 |
| --- | --- |
| 名称 | 输入可标识领域的唯一名称。 |
| 客户端密钥<br>租户 ID<br>事件中心主机名<br>事件中心名称<br>事件中心连接字符串 | 输入您找到的信息，如中所述：<br>• 被动身份验证：如何为被动身份验证创建 Microsoft Azure AD (SAML)，第 3 页<br>• 主动身份验证：获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 19 页 |
| （可选。）**用户组** | 滑动到 **滑块已启用** (  ) 以指定要包含在策略中或从策略中排除的组。 |
| （可选。）**排除的用户组** | 如果在此字段中输入一个或多个组名称，则为 它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。<br>每行输入一个组名，后跟一个换行符。组名区分大小写。 |

| 项目 | 说明 |
| --- | --- |
| （可选。）**包含的用户组** | 如果在此字段中输入一个或多个组名称，则为 只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。<br>每行输入一个组名，后跟一个换行符。组名区分大小写。 |

**步骤 3** 点击**测试**。
在继续下一步之前，请确保测试连接成功。

**步骤 4** 点击**下一步 (Next)**。

### Microsoft Azure AD (SAML) 领域：用户会话超时

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

此选项设置系统终止非活动会话之前的秒数。

过程

**步骤 1** 从向导中的上一步继续操作。

**步骤 2** 输入以下信息。

| 项目 | 说明 |
| --- | --- |
| **ISE 用户** | 默认为 1440 秒（24 小时）。 |
| **强制网络门户用户** | 默认为 1440 秒（24 小时）。 |

超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则防火墙管理中心会将该用户视为未知（**失败的强制网络门户用户**除外）。

**步骤 3** 点击**保存**。

# 如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）

本主题讨论创建用于 Cisco Secure Firewall Management Center 的 Microsoft Azure Active Directory (AD) 领域（现在被称作*Entra ID*）的高级任务。

### 开始之前

如果启用了“更改管理”(hange Management)，则必须为以下每个对象打开或编辑、分配和批准票单，然后才能创建领域：

- 基本 URL
- 服务提供商证书注册（PKCS12 格式）
- 身份供应商证书注册（手动格式）
- 领域本身（创建并分配通知单，直到领域创建完成，然后批准它）

有关详细信息，请参阅提交配置更改请求和支持变更管理的策略和对象。

### 过程

| | 命令或操作 | 目的 |
|---|---|---|
| **步骤 1** | 使用 DNS 服务器创建完全限定的主机名 (FQDN) 并将 的内部证书上传至 Cisco Secure Firewall Management Center。如果您之前从未使用过例如 此类 资源，可以咨询此类资源。在 Cisco Secure Firewall Management Center 托管的一台设备上指定路由接口的 IP 地址。 | 请参阅 DNS 服务器参考。 |
| **步骤 2** | 启用Cisco Secure Dynamic Attributes Connector。 | 要使用 Microsoft Azure AD 领域， Cisco Secure Dynamic Attributes Connector 为必填项。您可以先执行此操作，也可以在创建领域时启用它。有关详细信息，请参阅启用 Cisco Secure Dynamic Attributes Connector。 |
| **步骤 3** | 使用关联的内部证书创建网络对象。 | 请参阅创建网络对象。 |
| **步骤 4** | 获取签名证书并将其上传到将向其发送Entra ID 身份验证请求的 Cisco Secure Firewall Threat Defense。 | 该证书应由受信任的证书颁发机构 (CA) 签署并以**.p12**以下格式（也称为PKCS#12；另请参阅 ssl.com 上的这篇文章）交付给您。<br>有关背景信息，请参阅 Cisco Secure Firewall Management Center 设备配置指南 或 stackoverflow.com中有关公钥基础设施的部分。<br>上传签名证书，请参阅 使用 PKCS12 文件安装证书。 |
| **步骤 5** | 配置 Microsoft Entra ID 基本设置。 | 需要执行多项配置任务，包括设置事件中心、向应用授予访问 Microsoft Graph API 的权限以及启用审核日志。 |

| | 命令或操作 | 目的 |
|---|---|---|
| | | 请参阅配置 Entra ID 基本设置，第 7 页。 |
| **步骤 6** | 在 Azure AD 中创建单点登录 (SSO) 应用。 | SSO 应用使请求访问受保护网络资源的用户能够使用 Entra ID 进行身份验证。SSO 应用具有可用于简化领域创建的联合XML，以及 Cisco Secure Firewall Threat Defense 使用 Entra ID 进行安全身份验证所需的身份提供程序证书。<br>请参阅在 Azure AD 中创建单点登录 (SSO) 应用，第 17 页。 |
| **步骤 7** | 获取配置 Microsoft Azure AD (SAML) 领域所需的信息。 | 此信息包括客户端和租户 ID、客户端密钥以及 Microsoft Azure AD 中存储的其他信息。<br>请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页。 |
| **步骤 8** | 使用 Azure 身份验证服务的**解密 - 重新签名**规则配置 a 解密策略，以便用户可以使用 HTTPS 协议访问网页。 | 只有在将 HTTPS 流量发送到领域之前，Microsoft Azure AD (SAML) 领域才能对用户进行身份验证。Microsoft Azure AD (SAML) 领域本身被系统视为 **Azure 身份验证服务** 应用。<br>创建具有解密规则操作的解密规则，第 18 页。 |
| **步骤 9** | 使用主动身份验证规则创建身份策略。 | 在使用 Microsoft Azure AD (SAML) 领域执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。<br>有关详细信息，请参阅创建身份策略。 |
| **步骤 10** | 使用 Microsoft Azure AD 领域创建访问控制策略和规则。 | 与其他类型的领域不同，您不需要创建身份策略或将身份策略与访问控制策略相关联。<br>请参阅创建基本访问控制策略和创建和编辑访问控制规则。 |
| **步骤 11** | 将身份和 解密策略 与第 3 步的访问控制策略相关联。 | 这是最后一步，此后系统即可使用 Microsoft Azure AD (SAML) 领域进行用户身份验证。<br>有关详细信息，请参阅将其他策略与访问控制相关联。 |

## 下一步做什么

请参阅配置 Entra ID 基本设置，第 7 页。

# 配置 Entra ID 基本设置

### 为您的应用授予 Microsoft Graph 权限

如 Microsoft 站点上的授权和 Microsoft Graph 安全 API 中所述，向 Entra ID（之前称为 *Azure AD*）应用授予 Microsoft Graph 的以下权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限让 防火墙管理中心 能够首次从 Entra ID 下载用户和组。

对于在 防火墙管理中心 中设置 Entra ID 领域，此步骤所需的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

### 设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。防火墙管理中心 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

**重要事项** 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

对于在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

### 启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

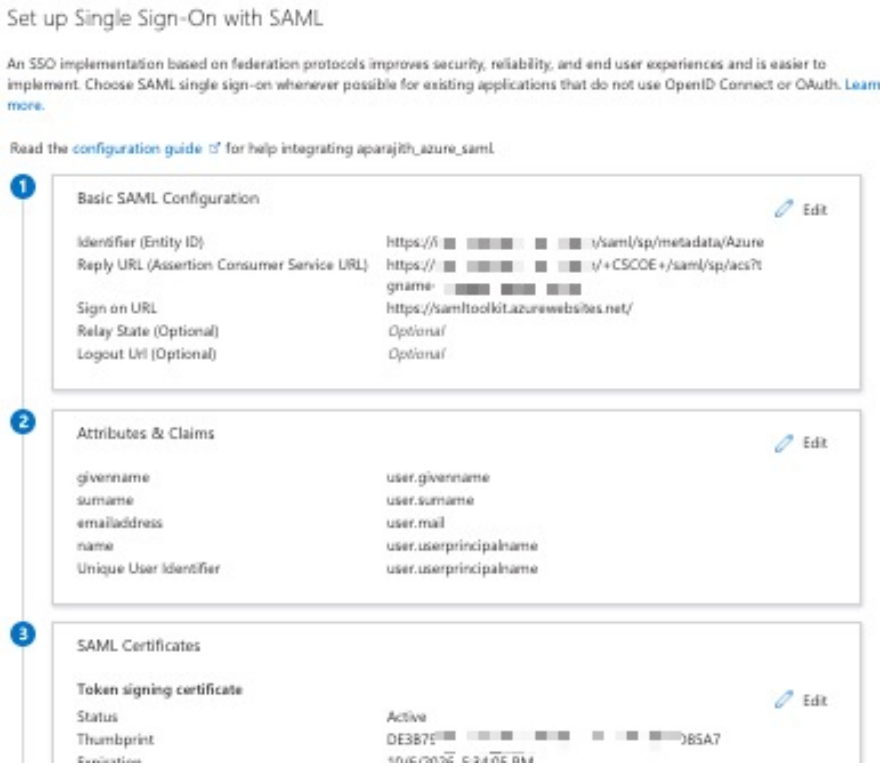
# 在 Azure AD 中创建单点登录 (SSO) 应用

本主题讨论当网络用户尝试访问受保护的网络时，如何在 Microsoft Azure AD 中创建应用来处理来自 Azure AD 的单点登录 (SSO)。

### 创建应用

在 Microsoft Azure AD 门户中，点击主页上的 **企业应用**，然后按照learn.microsoft.com 上 配置 Microsoft Entra SSO 中的说明进行操作。

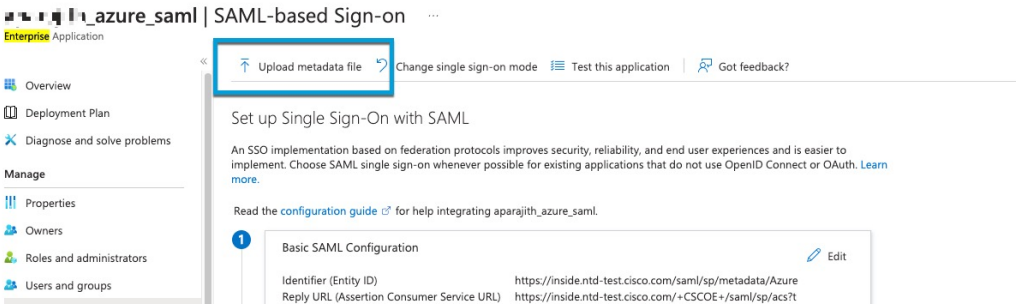
下图显示了 SSO 应用配置的一部分。配置 Microsoft Azure AD (SAML) 领域时，必须在此页面上提供一些信息。有关详细信息，请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 19 页。




### （可选。）上传服务提供程序元数据

如果您已配置 Microsoft Azure AD (SAML) 领域，请点击页面顶部的上传元数据文件，以快速提供 SSO 应用的配置值。

下图显示了一个示例。




### 将用户和组添加到 SSO 应用

按照learn.microsoft.com 上 的将用户账号添加到企业应用 中所述，将用户和组添加到您的应用

### 后续操作

请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 19 页。

## 创建具有解密规则操作的解密规则

程序的此部分介绍如何创建 a 解密策略，以在流量到达 SAML 领域之前解密和重签流量。领域仅可对解密的流量进行身份验证。

### 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 如果尚未进行此操作，则请创建内部证书授权对象，以 TLS/SSL 流量进行解密，如PKI中所述。

**步骤 3** 请点击 **策略** > **访问控制标题** > **解密**。

**步骤 4** 点击**新建策略 (New Policy)**。

**步骤 5** 为策略输入**名称**，然后选择**默认操作**。默认操作将在解密策略 默认操作中讨论。

**步骤 6** 点击**保存**。

**步骤 7** 点击**添加规则**。

**步骤 8** 为规则输入**名称 (Name)**。

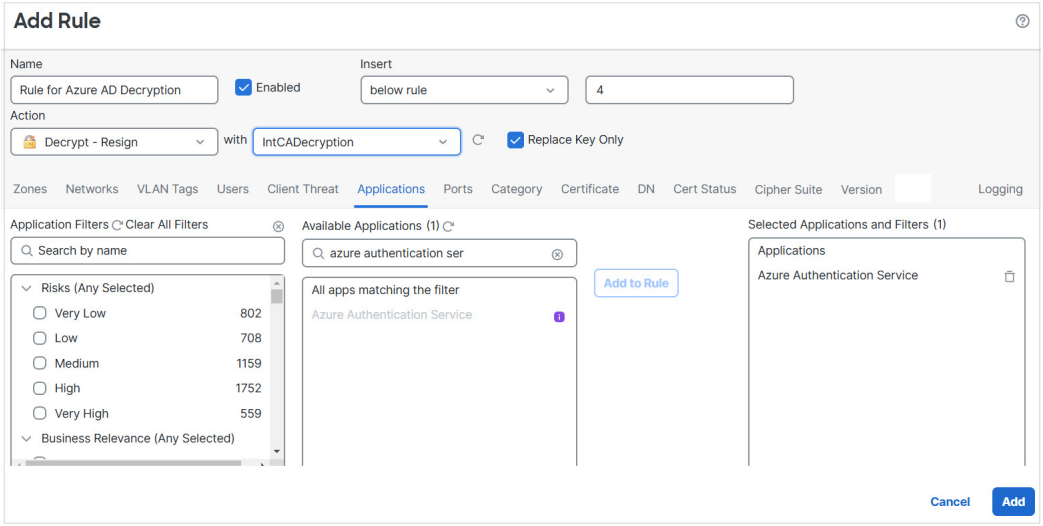
**步骤 9** 从**操作**列表中，选择**解密 - 放弃**。

**步骤 10** 从**通过 (with)** 列表中，选择您的服务提供商证书对象。

**步骤 11** 点击**应用 (Applications)** 选项卡页面。

**步骤 12** 在可用应用部分，搜索 **Azure Authentication Service** 。

**步骤 13** 点击 **Azure 身份验证 (Azure Authentication)**，然后点击**添加到规则 (Add to Rule)**。
下图显示了一个示例。




**步骤 14** （可选。）设置其他选项，如解密规则 条件中所述。

**步骤 15** 点击**添加 (Add)**。

**步骤 16** 在该页面顶部，点击**保存**。

### 下一步做什么

# 获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证）

此任务说明如何获取在防火墙管理中心 中设置 Microsoft Azure AD (SAML) 领域所需的信息 （现在被称作 *Entra ID*）。

### 过程

**步骤 1** 以至少具有产品设计师角色的用户身份登录 https://portal.azure.com/。

**步骤 2** 在页面顶部，点击 **Microsoft Entra ID**。

**步骤 3** 在左侧列中，点击**应用注册 (App Registrations)**。

**步骤 4** 如有必要，过滤显示的应用列表以便显示要使用的应用。

**步骤 5** 点击应用的名称。

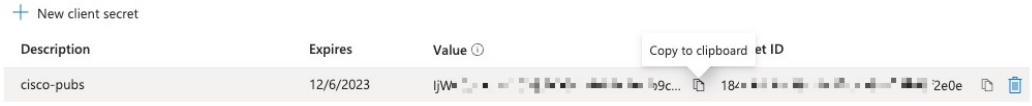

**步骤 6** 点击此页面上以下值旁边的 **复制** ( )，然后将这些值粘贴到文本文件中。

- 应用（客户端）ID
- 目录（租户）ID

**步骤 7** 点击客户端凭证 **(Client Credentials)**。

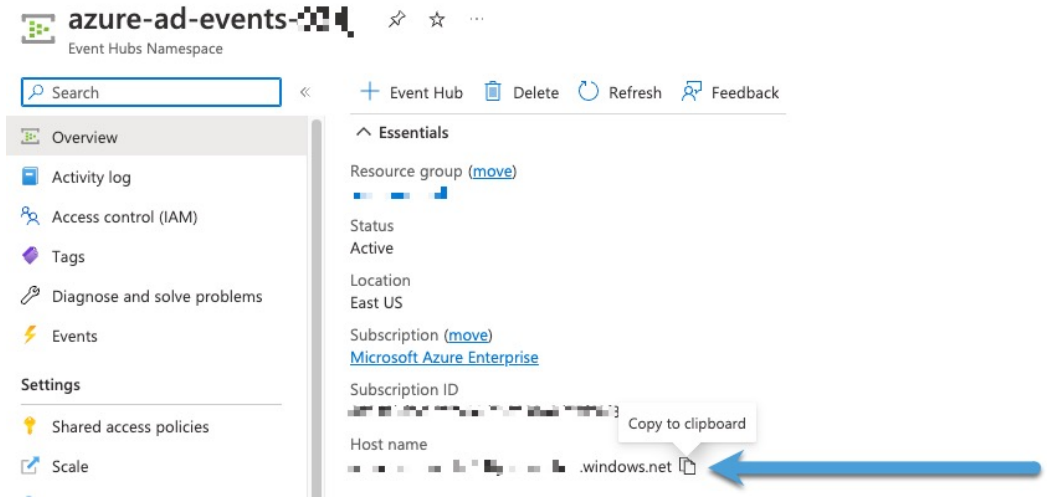
**步骤 8** 除非您已经知道客户端密钥值 （而不是客户端密钥 *ID*），否则必须按如下方式创建新的客户端密钥：

a) 点击新建客户端密钥 **(New Client Secret)**。
b) 在提供的字段中输入要求的信息。
c) 点击添加 **(Add)**。
d) 点击 Value 旁边的 复制 ()，如下图所示。




**步骤 9** 在 https://portal.azure.com/ 中，点击事件中心 **(Event Hubs)** > （事件中心的名称）。

**步骤 10** 在右侧窗格中，点击 主机名 **(Host name)** 值旁边的 复制 () 并将值粘贴到剪贴板。这是事件中心主机名。

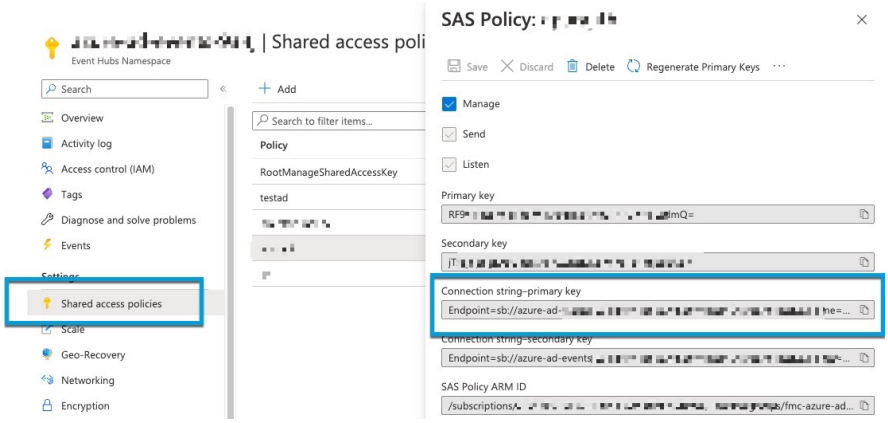



**步骤 11** 记下事件中心的名称或将其复制到文本文件（与页面顶部的事件中心命名空间 **(Event Hubs Namespace)** 相同）。

**步骤 12** 在左侧窗格中的设置下，点击共享访问策略 **(Shared access policies)**。

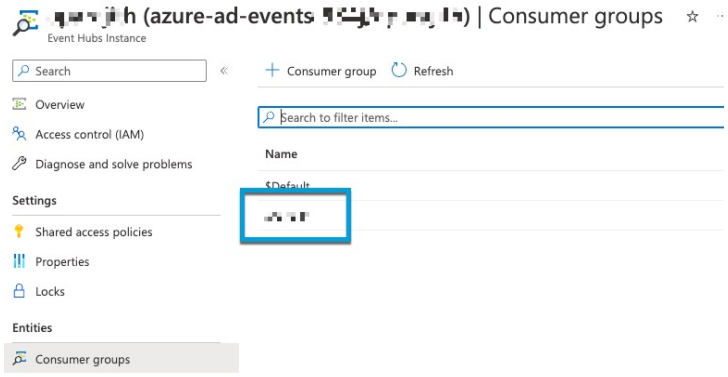
**步骤 13** 点击策略名称。

**步骤 14** 点击连接字符串 - 主键 **(Connection string-primary key)** 旁边的 复制 ()。




**步骤 15** 点击 概述 **(Overview)** > 实体 **(Entities)** > 事件中心 **(Event Hubs)** > （事件中心的名称） > 实体 **(Entities)** > 使用者组 **(Consumer Groups)**。

记下以下值或将其复制到剪贴板。这是您的使用者组名称。




**步骤 16** 在左侧窗格中点击概览 **(Overview)**。

**步骤 17** 点击命名空间 **(Namespace)** 旁边的 复制 ()。


这是事件中心主题名称。

**步骤 18** 返回主页并在必要时登录：https://portal.azure.com/#home。

**步骤 19** 点击 **Microsoft Entra ID**。

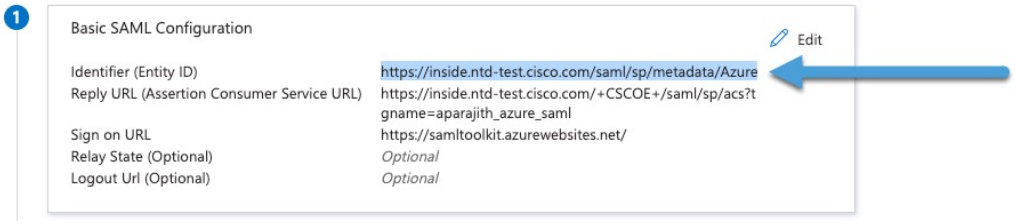
**步骤 20** 在左侧窗格中，点击企业应用 **(Enterprise Applications)**。

**步骤 21** 如有必要，请过滤应用列表以查找您的应用。

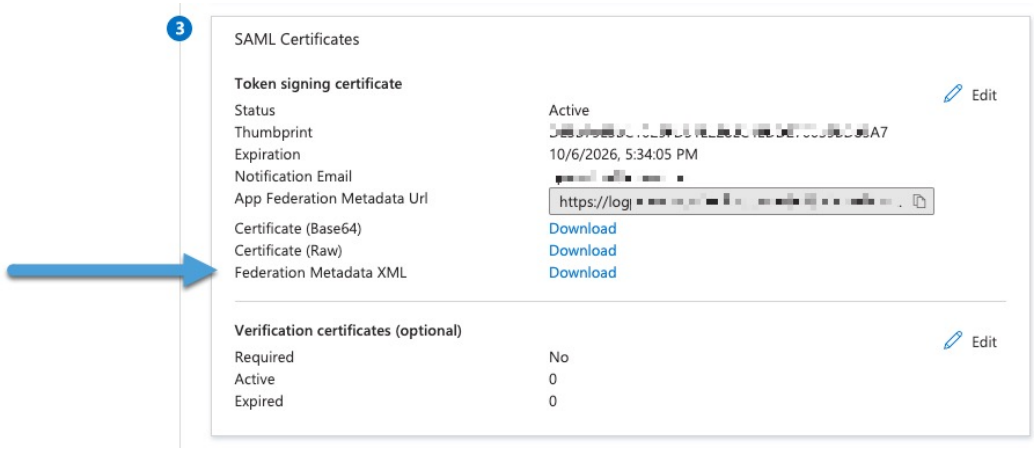
**步骤 22** 点击企业应用的名称。

**步骤 23** 点击“设置单点登录 (Set up single sign on)”下的 启动 **(Get Started)** 。

**步骤 24** 在 SSO 应用页面上，将标识符（实体 ID）的值复制到剪贴板。
下图显示了一个示例。




**步骤 25** 在 SSO 应用页面上，点击联合元数据 XML 旁边的**下载 (Download)** 链接，如下图所示。
下图显示了一个示例。




**步骤 26** 如果您已经设置了 SSO 应用， 可以在此处停止。联合元数据 XML 包含在 Cisco Secure Firewall Management Center中配置身份提供程序所需的所有信息。

**步骤 27** （如果已下载联合 XML，则可选。）点击以下两个值旁边的 **复制** (⧉) 并将其保存到文本文件。
下图显示了一个示例。


## 下一步做什么

请参阅创建具有解密规则操作的解密规则，第 18 页。

# 创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）

以下主题讨论如何运行创建 Microsoft Azure AD (SAML) 领域（现在称为 *Entra ID*）所需的多步骤向导以进行主动身份验证。

在主动身份验证（也称为强制网络门户）中，Microsoft Entra ID 是用户存储。当用户尝试访问访问控制规则中定义的受保护资源时，该用户必须首先通过 Microsoft Entra ID 进行身份验证。

要配置领域，请按以下顺序完成所有任务：

1. 配置 Entra ID 基本设置，第 7 页。
2. 在 Azure AD 中创建单点登录 (SSO) 应用，第 17 页。
3. 获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 19 页

## Microsoft Azure AD (SAML) 领域：SAML 详细信息

此任务讨论创建 Microsoft Azure AD (SAML) 领域的多步骤向导中的第一步。您必须完成向导中的所有步骤才能设置领域。根据您创建的领域是用于主动身份验证还是被动身份验证，这些步骤会有所不同。

### 开始之前

在创建领域之前，请完成以下所有任务：

- （仅使用 Cisco ISE 进行被动身份验证。）如果您使用 Cisco ISE 作为用户和组的存储库，请设置 ISE：
  - 关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE，第 4 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE，第 4 页
- 要将 Entra ID 用作用户和组的存储库，请参阅为被动身份验证配置 Microsoft Entra ID，第 5 页。
- 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页中所述。

### 过程

**步骤 1** 登录Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 点击 **添加领域** > **SAML - Azure AD**。

**步骤 4** 输入以下信息。

| 项目 | 说明 |
|---|---|
| 名称 | 用于标识领域的唯一名称。 |

| 项目 | 说明 |
|---|---|
| 说明 | （可选。）领域的描述。 |
| 身份提供程序 | 始终显示 **Azure AD**。 |
| 配置类型 | 点击以下选项之一：<br>• **使用 ISE 进行被动身份验证，以**进行被动身份验证。<br>• **使用 Azure AD 的被动身份验证或强制网络门户**，以便将 Entra ID 用作被动身份验证或主动身份验证（即强制网络门户）的用户存储。 |

**步骤 5** 点击**下一步 (Next)**。

### 下一步做什么

以下项之一：

- 被动身份验证：Microsoft Azure AD (SAML) 领域：Azure AD 详细信息，第 12 页。
- 主动身份验证：Microsoft Azure AD (SAML) 领域：SAML 服务提供商 (SP) 元数据，第 24 页

## Microsoft Azure AD (SAML) 领域：SAML 服务提供商 (SP) 元数据

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

### 开始之前

完成 Microsoft Azure AD (SAML) 领域：SAML 详细信息，第 11 页中讨论的任务

### 过程

**步骤 1** 继续 Microsoft Azure AD (SAML) 领域：SAML 详细信息，第 11 页。

**步骤 2** 输入以下信息。

| 项目 | 说明 |
|---|---|
| **基本 URL** | 从列表中，点击之前创建的网络对象。网络用户在尝试访问受保护的网络资源时会被定向到此 URL。<br>您也可以点击 **添加** (+) 立即创建对象。 |
| **实体 ID** | SSO 应用的实体 ID。 |

| 项目 | 说明 |
| --- | --- |
| 断言使用者服务 (ACS) URL | 根据之前的值自动生成。 |
| 服务提供程序证书 | 从列表中，点击要用于解密对 Cisco Secure Firewall Threat Defense 的请求的证书。<br>您也可以点击 添加 (+) 立即创建对象。 |
| 下载服务提供程序元数据 | （可选。）下载与服务提供程序（即托管设备）相关联的元数据，以简化 Microsoft Entra ID SSO 应用的配置。 |

**步骤 3** 点击**下一步 (Next)**。

### 下一步做什么

Microsoft Azure AD (SAML) 领域：SAML 身份提供程序 (IdP) 元数据 ，第 25 页。

## Microsoft Azure AD (SAML) 领域：SAML 身份提供程序 (IdP) 元数据

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

### 开始之前

完成 Microsoft Azure AD (SAML) 领域：SAML 服务提供商 (SP) 元数据 ，第 24 页中讨论的任务。

### 过程

**步骤 1** 继续 Microsoft Azure AD (SAML) 领域：SAML 服务提供商 (SP) 元数据 ，第 24 页。

**步骤 2** 如果之前下载了 Entra ID SSO 应用的联合 XML，请点击**上传 XML** 并立即上传。然后您可以跳过此步骤。

**步骤 3** 输入以下信息。

| 项目 | 说明 |
| --- | --- |
| 实体 ID | 输入身份提供程序的实体 ID。 |
| 单点登录 (SSO) URL | 输入应用的 SSO URL。 |
| IdP 证书 | 从列表中，点击用于与 Microsoft Entra ID 进行身份验证的证书。<br>您也可以点击 添加 (+) 立即创建对象。 |

**步骤 4** 点击**下一步 (Next)**。

### 下一步做什么

Microsoft Azure AD (SAML) 领域：SAML 详细信息，第 11 页。

## Microsoft Azure AD (SAML) 领域：Azure AD 详细信息

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

### 过程

**步骤 1** 从向导中的上一步继续操作。

**步骤 2** 输入以下信息。

| 项目 | 说明 |
|---|---|
| 名称 | 输入可标识领域的唯一名称。 |
| 客户端密钥<br>租户 ID<br>事件中心主机名<br>事件中心名称<br>事件中心连接字符串 | 输入您找到的信息，如中所述：<br>• 被动身份验证：如何为被动身份验证创建 Microsoft Azure AD (SAML)，第 3 页<br>• 主动身份验证：获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 19 页 |
| （可选。）**用户组** | 滑动到 **滑块已启用** (  ) 以指定要包含在策略中或从策略中排除的组。 |
| （可选。）**排除的用户组** | 如果在此字段中输入一个或多个组名称，则为 它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。<br>每行输入一个组名，后跟一个换行符。组名区分大小写。 |
| （可选。）**包含的用户组** | 如果在此字段中输入一个或多个组名称，则为 只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。<br>每行输入一个组名，后跟一个换行符。组名区分大小写。 |

**步骤 3** 点击**测试**。

在继续下一步之前，请确保测试连接成功。

**步骤 4** 点击**下一步 (Next)**。

### Microsoft Azure AD (SAML) 领域：用户会话超时

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

此选项设置系统终止非活动会话之前的秒数。

过程

**步骤 1** 从向导中的上一步继续操作。

**步骤 2** 输入以下信息。

| 项目 | 说明 |
|---|---|
| **ISE 用户** | 默认为 1440 秒（24 小时）。 |
| **强制网络门户用户** | 默认为 1440 秒（24 小时）。 |

超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则防火墙管理中心会将该用户视为未知（**失败的强制网络门户用户**除外）。

**步骤 3** 点击**保存**。

# 为被动身份验证 创建 Microsoft Azure AD (SAML)领域

您可以将 Microsoft Azure Active Directory (AD) 领域与 ISE 配合使用来对用户进行身份验证并获取用户会话以进行用户控制。我们从 Azure AD 获取组，从 ISE 获取登录用户会话数据。

您有以下选择：

- 资源拥有的密码凭证 (ROPC)：使用户能够使用用户名和密码通过 AnyConnect 等客户端登录。ISE 将用户会话发送到 Cisco Secure Firewall Management Center。有关详细信息，请参阅关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE ，第 4 页。

  其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

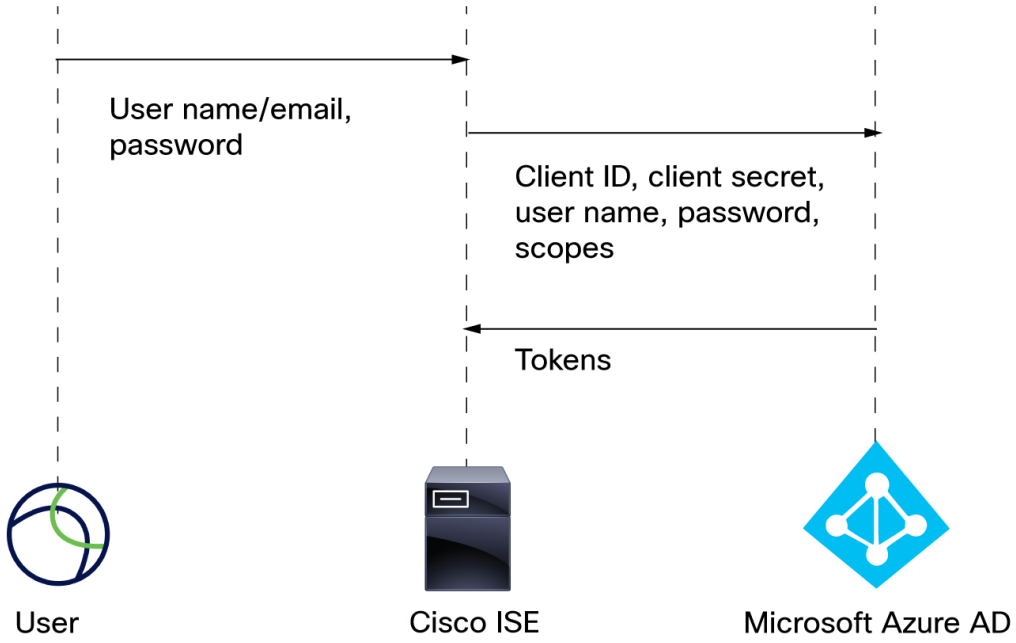
- 可扩展身份验证协议 (EAP) 链与基于隧道的可扩展身份验证协议 (TEAP) 和传输层安全 (TLS)，缩写为 EAP/TEAP-TLS：TEAP 是一种基于隧道的 EAP 方法，可建立安全隧道并执行其他 EAP 方法在该安全隧道的保护下。ISE 用于验证用户凭证并将用户会话发送到 Cisco Secure Firewall Management Center。有关详细信息，请参阅关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ，第 4 页。

这种类型的身份验证是 被动 身份验证，而不是 创建 Microsoft Azure AD (SAML) 领域，第 2 页中使用的主动身份验证。

注释 在部署与 Microsoft Azure AD 领域相关的策略之前，请参阅Microsoft Azure Active Directory 领域的用户限制。

# 关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE

下图总结了具有 Cisco ISE 和资源拥有的密码凭证 (ROPC) 的 Azure AD 领域：




使用 ROPC，

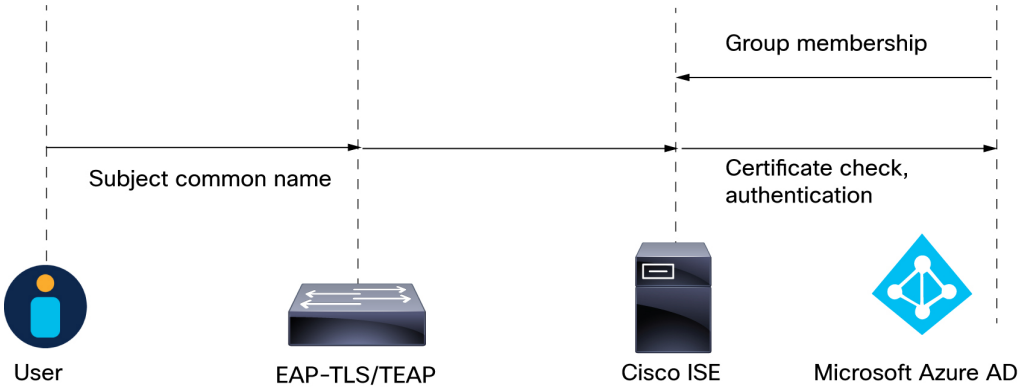
1. 用户使用 VPN 客户端（例如 Cisco Secure Client）使用用户名（或邮件地址）和密码登录。
2. 客户端 ID、客户端密钥、用户名、密码和范围将发送到 Entra ID。
3. 令牌从 Azure AD 发送到 Cisco ISE，然后将用户会话发送到 Cisco Secure Firewall Management Center。

有关配置 Cisco ISE 的详细信息，请参阅 使用 Azure Active Directory 配置 ISE 3.0 REST ID。

其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

# 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE

RFC7170定义的隧道可扩展身份验证协议 (TEAP) 可与 ISE 配合使用， Cisco Secure Firewall Management Center 如下所示：




以下内容基于 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS：

1. 用户的证书通过 EAP-TLS 或使用 EAP-TLS 作为内部方法的 TEAP 发送到 ISE。
2. ISE 评估用户的证书（有效期、受信任的证书颁发机构、证书吊销列表等）。
3. ISE 获取证书使用者名称 (CN) 并查询 Azure Graph API 以获取用户的组和其他属性。这被 Azure 称为用户主体名称 (UPN)。
4. ISE 授权策略根据从 Azure 返回的用户属性进行评估。

# 如何为被动身份验证创建 Microsoft Azure AD (SAML)

本主题讨论创建 Microsoft Azure AD (SAML) 领域以用于 Cisco Secure Firewall Management Center 的被动身份验证（现在被称作额外 *ID*）的高级任务。

过程

| | 命令或操作 | 目的 |
|---|---|---|
| 步骤 1 | 启用Cisco Secure Dynamic Attributes Connector。 | Cisco Secure Dynamic Attributes Connector 要使用 Microsoft Azure AD (SAML) 领域。您可以先执行此操作，也可以在创建领域时启用它。有关详细信息，请参阅启用 Cisco Secure Dynamic Attributes Connector。 |
| 步骤 2 | 配置 Microsoft Entra ID | 需要执行多项配置任务，包括设置事件中心、向应用授予访问 Microsoft Graph API 的权限以及启用审核日志。<br>请参阅为被动身份验证配置 Microsoft Entra ID，第 5 页。 |
| 步骤 3 | 配置 Cisco ISE。 | 配置 ISE 的方式取决于用户对您的系统进行身份验证的方式。有关详细信息，请参阅如 |

| | 命令或操作 | 目的 |
|---|---|---|
| | | 何为 Microsoft Azure AD (SAML)配置 ISE，第 5 页。 |
| **步骤 4** | 创建 Cisco ISE 身份源。 | 身份源使 ISE 能够与 Cisco Secure Firewall Management Center通信。 |
| **步骤 5** | 获取配置 Microsoft Azure AD (SAML) 领域所需的信息。 | 此信息包括客户端和租户 ID、客户端密钥以及 Microsoft Azure AD 中存储的其他信息。 |
| **步骤 6** | 配置并验证您的领域。 | 在开始在访问控制策略中使用该领域的配置之前，请对其进行测试。<br>如创建 Microsoft Azure AD (SAML) 领域，第 2 页中所述，创建 Microsoft Azure AD (SAML) 领域。 |
| **步骤 7** | 使用 Microsoft Azure AD (SAML) 领域创建访问控制策略和规则。 | 与其他类型的领域不同，您不需要创建身份策略或将身份策略与访问控制策略相关联。<br>请参阅创建基本访问控制策略和创建和编辑访问控制规则。 |

### 下一步做什么

请参阅关于具有资源拥有的密码凭证的额外 ID 和 Cisco ISE ，第 4 页。

## 为被动身份验证配置 Microsoft Entra ID

本主题提供有关如何设置 Microsoft Entra ID（以前称为 *Microsoft Azure Active Directory (AD)*）作为您可以与 Cisco Secure Firewall Management Center 一起使用的领域的基本信息。我们假设您已经熟悉 Entra ID；如果不熟悉，请在开始之前查阅文档或支持资源。

### 为您的应用授予 Microsoft Graph 权限

如 Microsoft 网站上的《授权和 Microsoft Graph 安全 API》中所述，向您的 Entra ID 应用授予以下 Microsoft Graph 权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限使 Cisco Secure Firewall Management Center 能够首次从 Entra ID 下载用户和组。

在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域所需的此步骤的信息：

- 您注册的应用的名称
- **应用（客户端）ID**

- 客户端密钥
- 目录（租户）ID

### 设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。Cisco Secure Firewall Management Center 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

**重要事项** 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

在 Cisco Secure Firewall Management Center 中设置 Entra ID 领域所需的此步骤的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

### 启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

### 为 Entra ID 配置 Cisco ISE

要向 Cisco Secure Firewall Management Center 发送用户会话信息，请按照《配置 ISE 3.0 REST ID 与 Azure Active Directory》中所述为 Entra ID 配置 Cisco ISE。

### 后续操作

请参阅如何为 Microsoft Azure AD (SAML)配置 ISE， 第 5 页。

## 如何为 Microsoft Azure AD (SAML)配置 ISE

在 Microsoft Azure AD (SAML)（现在称为 *Entra ID*）领域，ISE 负责向 Cisco Secure Firewall Management Center 发送用户会话（登录、注销）。本主题讨论如何设置 ISE 以便与 Azure AD 领域配合使用。

### 资源拥有的密码凭证身份验证

要在资源所有者密码凭证 (ROPC) 的帮助下，通过具象状态传输 (REST) 身份 (ID) 服务将 ISE 与 Microsoft Azure AD (SAML) 配合使用，请参阅使用 Azure Active Directory 配置 ISE 3.0 REST ID。

### TEAP/EAP-TLS

要将 ISE 与基于 Azure AD 组成员身份和其他用户属性的授权策略配合使用，并将 EAP-TLS 或 TEAP 作为身份验证协议，请参阅 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS。

### 后续操作

获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页

## 获取 Microsoft Azure AD (SAML) 领域所需的信息

本任务介绍如何获取在 Cisco Secure Firewall Management Center 中设置 Microsoft Azure AD (SAML)（现称为 *Entra ID*）领域所需的信息。您在按照 为被动身份验证配置 Microsoft Entra ID，第 5 页 中的说明设置 Microsoft Entra ID 时，可能已获取此信息。

### 过程

**步骤 1** 以至少具有产品设计师角色的用户身份登录 https://portal.azure.com/。

**步骤 2** 在页面顶部，点击 **Microsoft Entra ID**。

**步骤 3** 在左侧列中，点击**应用注册 (App Registrations)**。

**步骤 4** 如有必要，过滤显示的应用列表以便显示要使用的应用。

**步骤 5** 点击应用的名称。


**步骤 6** 点击此页面上以下值旁边的 **复制** ()，然后将这些值粘贴到文本文件中。

- **应用（客户端）ID**
- **目录（租户）ID**

**步骤 7** 点击**客户端凭证 (Client Credentials)**。

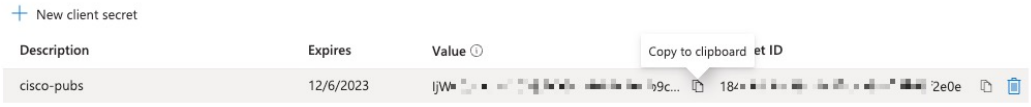
**步骤 8** 除非您已经知道客户端密钥值 （而不是客户端密钥 *ID*），否则必须按如下方式创建新的客户端密钥：

a) 点击**新建客户端密钥 (New Client Secret)**。

b) 在提供的字段中输入要求的信息。

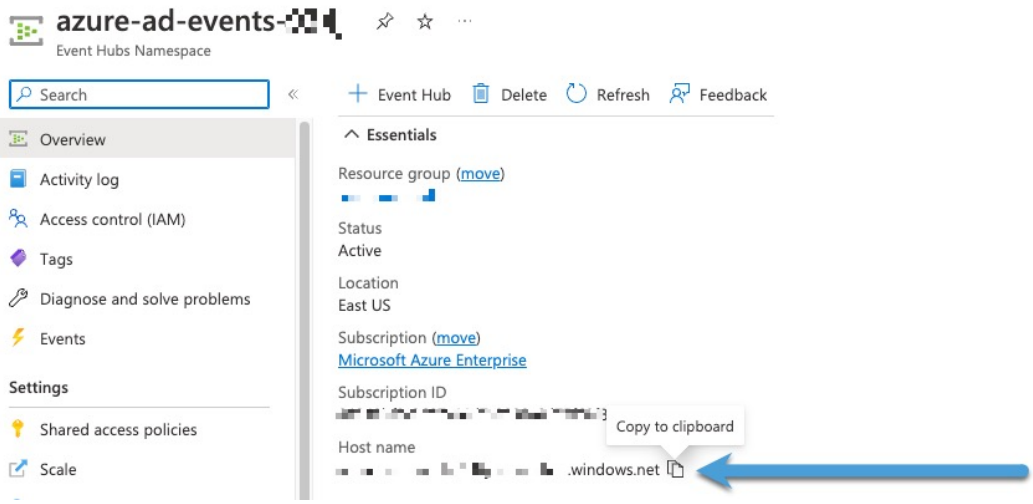
c) 点击**添加 (Add)**。

d) 点击 Value 旁边的 **复制** ()，如下图所示。




**步骤 9** 在 https://portal.azure.com/ 中，点击**事件中心 (Event Hubs)** > （事件中心的名称）。

**步骤 10** 在右侧窗格中，点击 **主机名 (Host name)** 值旁边的 **复制** () 并将值粘贴到剪贴板。这是事件中心主机名。

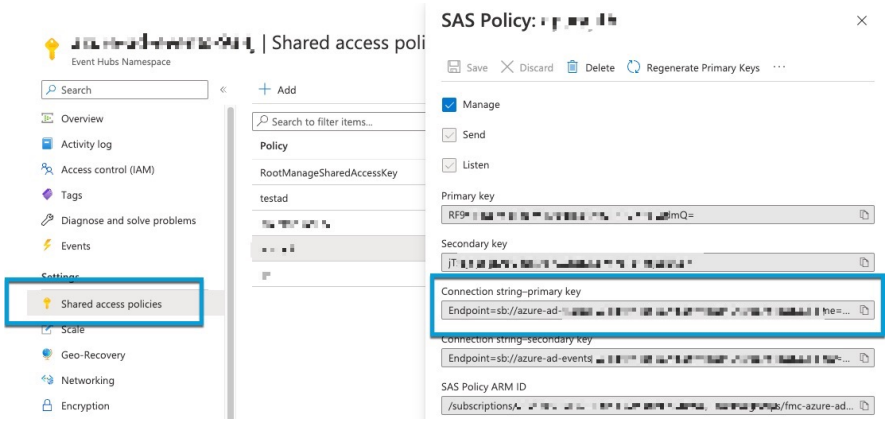



**步骤 11** 记下事件中心的名称或将其复制到文本文件（与页面顶部的**事件中心命名空间 (Event Hubs Namespace)** 相同）。

**步骤 12** 在左侧窗格中的设置下，点击**共享访问策略 (Shared access policies)**。

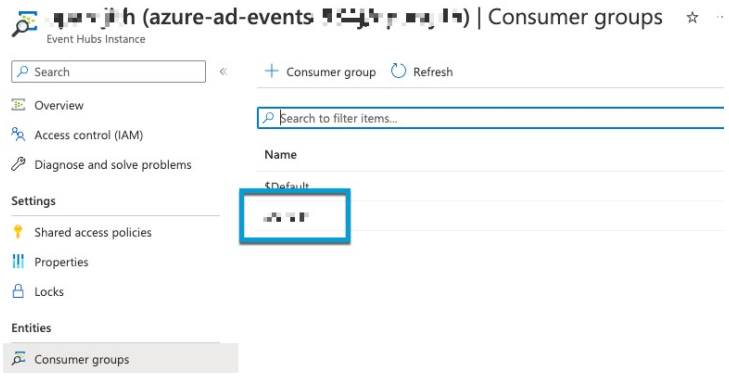
**步骤 13** 点击策略名称。

**步骤 14** 点击**连接字符串 - 主键 (Connection string-primary key)** 旁边的 **复制** ()。




**步骤 15** 点击 **概述 (Overview)** > **实体 (Entities)** > **事件中心 (Event Hubs)** > （事件中心的名称） > **实体 (Entities)** > **使用者组 (Consumer Groups)**。

记下以下值或将其复制到剪贴板。这是您的使用者组名称。




**步骤 16** 在左侧窗格中点击**概览 (Overview)**。

**步骤 17** 点击**命名空间 (Namespace)** 旁边的 **复制** ()。


这是事件中心主题名称。

# 创建 Azure AD 领域

通过以下程序，您可以创建领域（防火墙管理中心 和 Microsoft Azure AD 领域之间的连接）。

### 开始之前

完成以下所有任务：

- 按照如何为 Microsoft Azure AD (SAML)配置 ISE， 第 5 页中所述配置 ISE
- 创建 ISE 身份源，如配置 ISE/ISE-PIC中所述
- 启用 Cisco Secure Dynamic Attributes Connector，如启用 Cisco Secure Dynamic Attributes Connector中所述。
- 获取 Azure AD 领域所需的值，如 获取 Microsoft Azure AD (SAML) 领域所需的信息， 第 8 页中所述。
- 配置 Azure AD，如为被动身份验证配置 Microsoft Entra ID， 第 5 页中所述

如果启用了变更管理，则必须批准此程序中使用的所有证书。打开新故障单或编辑现有故障单。有关详细信息，请参阅创建变更管理故障单和。支持变更管理的策略和对象

注释 要使用 Azure AD 领域执行用户和身份控制，只需要具有关联的 Azure AD 领域的访问控制策略。您不需要创建身份策略。

过程

步骤 1 登录 Cisco Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **其他集成** > **领域** > **领域**。

步骤 3 要创建新的领域，请点击**添加领域** > **Azure AD**。

步骤 4 输入以下信息。

| 项目 | 说明 |
|---|---|
| 名称 | |
| （可选。）**说明** | |
| **客户 ID** | 输入您找到的信息，如获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页中所述。 |
| **客户端密钥** | |
| **租户 ID** | |
| **事件中心主机名** | |
| **事件中心名称** | |
| **事件中心连接字符串** | |
| （可选。）**排除的用户组** | 输入一个或多个 不 从中下载用户以进行身份控制的组。这些组中的用户将无法用于访问控制策略。<br>每行输入一个组名，后跟一个换行符。组名区分大小写。 |

步骤 5 要执行其他任务（如启用、禁用或删除领域），请参阅管理领域，第 65 页。

步骤 6 输入您找到的值，如获取 Microsoft Azure AD (SAML) 领域所需的信息，第 8 页中所述。

步骤 7 点击**测试**。

步骤 8 修复测试中显示的任何错误。

步骤 9 点击**保存**。

### 下一步做什么

创建访问控制策略和规则，如创建基本访问控制策略中所述。

注释 在部署与 Microsoft Azure AD 领域相关的策略之前，请参阅Microsoft Azure Active Directory 领域的用户限制。

## Azure AD (SAML) 用户会话超时

编辑 Azure AD 领域时， **用户会话超时**页面上会显示 ISE/ISE-PIC 的 Azure AD 用户会话超时。

默认值为 1440 秒（24 小时）。超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则 防火墙管理中心 会将该用户视为未知（**失败的强制网络门户用户**除外）。

# 创建 LDAP 领域或 Active Directory 领域和领域目录

如果要设置没有领域的 ISE/ISE-PIC，请注意，存在会影响 Cisco Secure Firewall Management Center 用户查看方式的用户会话超时。有关详细信息，请参阅领域字段，第 46 页。

通过以下程序，您可以创建 领域 （ 防火墙管理中心 与 Active Directory 目录领域之间的连接）和 目录 （ 防火墙管理中心 与 LDAP 服务器或 Active Directory 域控制器之间的连接）。

（推荐。）要从 防火墙管理中心 安全连接到 Active Directory 服务器，请先执行以下任务：

- 导出 Active Directory 服务器的根证书，第 53 页
- 查找 Active Directory 服务器名称，第 52 页

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

有关领域目录配置字段的详细信息，请参阅领域字段，第 46 页和领域目录和同步字段，第 49 页。

配置 防火墙管理中心 的跨域信任：设置，第 57 页中显示了使用跨域信任设置领域的分步示例。

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

如果要设置没有领域的 ISE/ISE-PIC，请注意，存在会影响 Cisco Secure Firewall Management Center 用户查看方式的用户会话超时。有关详细信息，请参阅领域字段，第 46 页。

### 开始之前

如果您对强制网络门户使用 Kerberos 身份验证，请在开始之前参阅以下部分：Kerberos 身份验证的前提条件，第 46 页。

如果启用了“更改管理”(hange Management)，则必须为以下每个对象打开或编辑、分配和批准票单，然后才能创建领域：

- 如果要安全连接 Microsoft AD 或 LDAP，服务器的受信任证书颁发机构
- 领域本身

有关详细信息，请参阅提交配置更改请求和支持变更管理的策略和对象。

**重要事项** 要减少 Cisco Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Cisco Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Cisco Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

### 过程

**步骤 1** 登录Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 要创建新领域，请从**添加领域**下拉列表中选择。

**步骤 4** 要执行其他任务（如启用、禁用或删除领域），请参阅管理领域，第 65 页。

**步骤 5** 按照领域字段，第 46 页中的描述输入领域信息。

**步骤 6** 在目录服务器配置部分中，输入目录信息，如 领域目录和同步字段，第 49 页中所述。

**步骤 7** （可选。）要为此领域配置其他域，请点击**添加其他目录**。

**步骤 8** 点击**配置组和用户**。
输入以下信息：

| 信息 | 说明 |
|---|---|
| **AD 主域 (AD Primary Domain)** | 用于需要对用户进行身份验证的 Active Directory 服务器的域。有关其他信息，请参阅领域字段，第 46 页。<br>您必须使用域的原始域名而不是该域的任何备用用户主体名称 (UPN) 后缀创建领域。否则，用户和组将无法下载，并且身份策略不会实施。例如，如果原始域为 `domain.example.com`，备用 UPN 名称为 `domain2.mydomain.com`，则必须将领域配置为使用 `domain.example.com`。有关配置备用 UPN 后缀的详细信息，请参阅 learn.microsoft.com 上的配置备用登录 ID 等资源。 |
| **基本 DN** | 防火墙管理中心应在其上开始搜索用户数据的服务器上的目录树。 |

| 信息 | 说明 |
| --- | --- |
| **组 DN (Group DN)** | 防火墙管理中心 应在其上开始搜索组数据的服务器上的目录树。 |
| **加载组** | 点击以从 Active Directory 服务器加载组。如果未显示组，请在 **AD 主域 (AD Primary Domain)**、**基本 DN (Base DN)** 和**组 DN (Group DN)** 字段中输入或编辑信息，然后点击**加载组 (Load Groups)**。<br>有关这些字段的信息，请参阅领域字段，第 46 页。 |
| 可用组部分 | 通过将组移动到 **包含的组和用户** 或 **排除的组和用户** 列表中，限制要在策略中使用的组。<br>例如，将一个组移动到 **包含的组和用户** 列表中，仅允许在策略中使用该组。<br>**排除的组和用户** 中的组及其包含的用户将被排除在用户感知和控制之外。所有其他组和用户 均为 可用。<br>有关详细信息，请参阅领域目录和同步字段，第 49 页。 |

**步骤 9** 点击**领域配置**选项卡。

**步骤 10** 输入 **组属性**，然后（如果您对强制网络门户使用 Kerberos 身份验证）输入 **AD 加入用户名** 和 **AD 加入密码**。有关详细信息，请参阅领域目录和同步字段，第 49 页。

**步骤 11** 如果使用 Kerberos 身份验证，请点击 **测试**。如果测试失败，请等待片刻，然后重试。

**步骤 12** 输入用户会话超时值，以分钟为单位，为 **ISE/ISE-PIC 用户**、**终端服务器代理用户**、**强制网络门户用户**、**出现故障的强制网络门户用户**、和 **访客强制网络门户用户**。

**步骤 13** 完成配置领域后，点击 **保存**。

### 下一步做什么

- 配置 防火墙管理中心 的跨域信任：设置，第 57 页
- 同步用户和组，第 55 页
- 编辑、删除、启用或禁用领域；请参阅管理领域，第 65 页。
- 比较领域，第 66 页。
- 或者，监控任务状态；请参阅《Cisco Secure Firewall Management Center 管理指南》中的查看任务消息。

# 关于领域和领域序列

领域是 Cisco Secure Firewall Management Center 和您监控的服务器上的用户账号之间的连接。它们可指定该服务器的连接设置和身份验证过滤器设置。领域可以：

- 指定要监控其活动的用户和用户组。

- 查询用户存储库上有关授权用户以及某些非授权用户的用户元数据：通过基于流量的检测而检测到的 POP3 和 IMAP 用户以及通过基于流量的检测、TS 代理/或 ISE/ISE-PIC 而检测到的用户。

（仅限 *Microsoft AD* 领域。）领域序列是要在身份策略中使用的两个或更多 Active Directory 领域的排序列表。将领域序列与身份规则关联时，系统会按照领域序列中指定的从第一个到最后的顺序来搜索 Active Directory 域。

您可以将多个域控制器添加为一个领域内的目录，但它们必须共享相同的基本领域信息。领域内的目录必须为专门的 LDAP 或专门的 Active Directory (AD) 服务器。启用领域后，保存的更改将在 Cisco Secure Firewall Management Center下一次查询服务器时生效。

要执行用户感知，必须为任何一种支持的服务器类型配置一个领域。系统使用这些连接查询服务器上与 POP3 和 IMAP 用户关联的数据，并收集有关通过基于流量的检测发现的 LDAP 用户的数据。

系统使用 POP3 和 IMAP 登录中的邮件地址与 Active Directory、Microsoft Azure Active Directory 或 OpenLDAP 上的 LDAP 用户相关联。例如，如果托管设备检测到某个用户使用与某个 LDAP 用户相同的邮件地址登录 POP3，则系统会将 LDAP 用户的元数据与该用户关联。

要执行用户控制，可以配置以下任何项目：

- Active Directory、Microsoft Azure Active Directory、 服务器或 ISE/ISE-PIC 的领域或领域序列

**注释** 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置 Microsoft AD 领域或领域序列。

领域序列不适用于 Microsoft Azure AD 领域。

- TS 代理的 Microsoft AD 服务器的领域或领域序列。
- 对于强制网络门户，则为 LDAP 领域。

  LDAP 不支持领域序列。

您最多可以嵌套 Microsoft AD 组， Cisco Secure Firewall Management Center 将下载这些组及其包含的用户。您可以选择限制下载的组和用户，如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页中所述。

### 关于用户同步

您可以配置领域或领域序列以便在 防火墙管理中心 和 LDAP 或 Microsoft AD 服务器之间建立连接，以检索检测到的某些用户的用户和用户组元数据：

- 由强制网络门户进行身份验证或由 ISE/ISE-PIC 报告的 LDAP 和 Microsoft AD 用户。这些元数据可用于用户感知和用户控制。
- 基于流量的检测功能检测到的 POP3 和 IMAP 用户登录（如果这些用户的电子邮件地址与 LDAP 或 AD 用户相同）。这些元数据可用于用户感知。

防火墙管理中心获取关于每个用户的以下信息和元数据：

- LDAP 用户名
- 名字和姓氏
- 电子邮件地址
- 部门
- 电话号码

**重要事项** 要减少 Cisco Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Cisco Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Cisco Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

### 关于用户活动数据

用户活动数据存储在用户活动数据库，而用户身份数据存储在用户数据库。可在访问控制中存储和使用的最大用户数取决于防火墙管理中心 型号。选择要包含的用户和组时，请确保用户总数小于型号限制。如果访问控制参数范围太宽泛，则 防火墙管理中心会获取尽可能多的用户的信息，并报告其无法在消息中心的“任务”选项卡页面中检索的用户数。

要选择性地限制托管设备监控用户感知数据的子网，您可以使用Cisco Secure Firewall Threat Defense 命令参考中所述的 **configure identity-subnet-filter** 命令。

**注释** 即使您从存储库移除系统检测到的用户，防火墙管理中心也不会从其用户数据库中移除这些用户；您必须手动删除。但是，在 防火墙管理中心下次更新其授权用户列表时，LDAP 更改会反映在访问控制规则中。

## 领域和受信任的域

在 防火墙管理中心中配置 Microsoft Active Directory (AD) 领域 时，该领域与 Microsoft Active Directory 或 LDAP 域 关联。

一组相互信任的 Microsoft Active Directory (AD) 域通常被称为林。此信任关系可使域以不同方式访问彼此的资源。例如，在域 A 中定义的用户账号可以标记为域 B 中所定义组的成员。

**注释** 受信任的域仅适用于 Microsoft Active Directory 域。它们不适用于 Microsoft Azure Active Directory 或 LDAP 域。

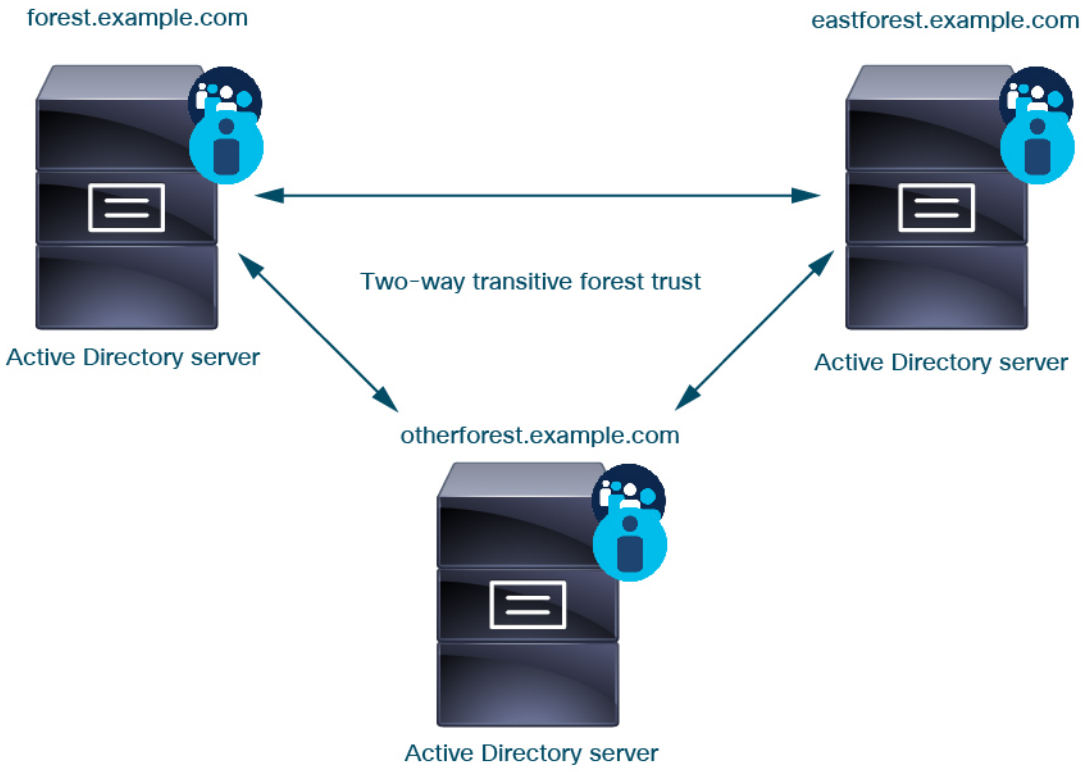
### 系统和受信任的域

系统支持在信任关系中配置的AD林。有几种类型的信任关系；本指南讨论双向传递森林信任关系。以下简单示例显示两个林： **forest.example.com** 和 **eastforest.example.com**。每个林中的用户和组可以通过另一个林中的 AD 进行身份验证，前提是您以这种方式配置了这些林。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

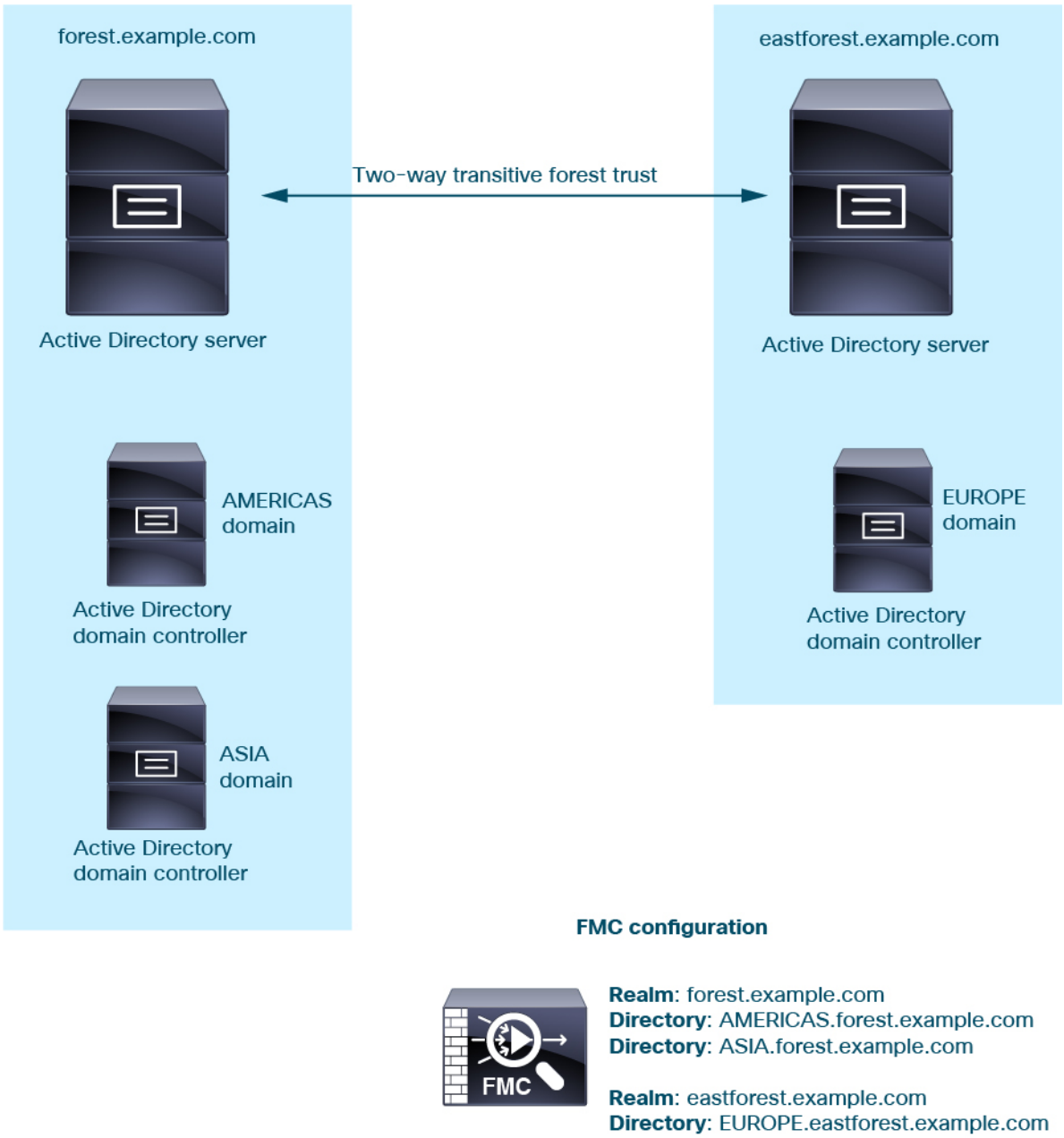
您无需为没有您希望在访问控制策略中使用的用户的任何域配置领域。


继续本示例，假设您有三个 AD 林（其中一个可以是子域或独立林），都设置为双向传递林关系，所有用户和组在所有三个林中以及系统。（如上例所示，必须将所有三个 AD 域设置为领域，并将所有域控制器配置为这些领域中的目录。）




最后，您可以将防火墙管理中心设置为能够在具有双向传递林信任的双林系统中对用户和组实施身份策略。假设每个林至少有一个域控制器，每个域控制器对不同的用户和组进行身份验证。要使 防火墙管理中心能够在这些用户和组上实施身份策略，必须将每个包含相关用户的域设置为 防火墙管理中心 领域，并将每个域控制器设置为相应领域中的 防火墙管理中心 目录。

未能正确配置防火墙管理中心会阻止某些用户和组在策略中使用。在这种情况下，当您尝试同步用户和组时，您将看到警告。




使用前面的示例，设置 防火墙管理中心 如下：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **AMERICAS.forest.example.com**领域中的目录
  - **ASIA.forest.example.com**领域中的目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **EUROPE.eastforest.example.com**领域中的目录

注释 防火墙管理中心 使用 AD 字段 **msDS-PrincipalName** 来解析引用，以查找每个域控制器中的用户名和组名。 **msDS-PrincipalName** 返回 NetBIOS 名称。

## 领域支持的服务器

可以配置领域以连接到以下类型的服务器（如果这些服务可从 防火墙管理中心进行 TCP/IP 访问）：

| 服务器类型 | 支持 ISE/ISE-PIC 数据检索？ | 支持 TS 代理数据检索？ | 支持强制网络门户数据检索？ |
|---|---|---|---|
| Windows 服务器 2012、2016 和 2019 上的 Microsoft Active Directory | 是 | 是 | 是 |
| Microsoft Azure AD | 是 | 否 | 否 |
| Linux 上 的 OpenLDAP | 否 | 否 | 是 |

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 如果 TS 代理安装在与另一个被动身份验证身份源（ISE/ISE-PIC）共享的 Microsoft Active Directory Windows 服务i去上，则 防火墙管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 防火墙管理中心。

请注意以下与服务器组配置有关的事项：

- 要对用户组或组内用户执行用户控制，则必须在 LDAP 或 Active Directory 服务器上配置用户组。
- 组名称不能以 `s-` 开头，因为它由 LDAP 在内部使用。

  组名称和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 或反斜线 (\)；否则，这些组或组织单位中的用户不会被下载，也不会可用于身份策略。
- 要配置包含或排除作为服务器上某个子组成员的用户的 Active Directory 领域，请注意，Microsoft 建议在 Windows 服务器 2012 上，Active Directory 每组包含不超过 5000 个用户。有关详细信息，请参阅 MSDN 上的“Active Directory 的最大限制-可扩展性”。

  如果需要，可以修改 Active Directory 服务器配置以增加此默认限制并容纳更多用户。

- 要在您的远程桌面服务环境中唯一识别由服务器报告的用户，则必须配置 Cisco 终端服务 (TS) 代理。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可唯一识别这些用户。（Microsoft将 终端服务 名称更改为 远程桌面服务。）

  有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

## 支持的服务器对象类和属性名称

领域中的服务器必须使用下表中列出的属性名称，以使 Cisco Secure Firewall Management Center能够检索服务器中的用户元数据。如果服务器中的属性名称不正确，Cisco Secure Firewall Management Center将无法使用该属性中的信息来填充其数据库。

**表 *1:* 属性名称与 *Cisco Secure Firewall Management Center*字段的映射**

| 元数据 | 防火墙管理中心属性 | LDAP ObjectClass | Active Directory 属性 | OpenLDAP 属性 |
|---|---|---|---|---|
| LDAP 用户名 | 用户名 | • 用户<br>• inetOrgPerson | samaccountname | cn<br>uid |
| 名字 | 名字 | | givenname | givenname |
| 姓氏 | 姓氏 | | sn | sn |
| 电子邮件地址 | 电子邮件 | | mail<br>Userprincipalname（如果 mail 没有值） | mail |
| department | 部门 | | department<br>distinguishedname（如果 department 没有值） | ou |
| 电话号码 | 电话 | | telephonenumber | telephonenumber |

**注释** 组的 LDAP ObjectClass 为 `group`、`groupOfNames`（`group-of-names` 适用于 Active Directory）或 `groupOfUniqueNames`。

有关 ObjectClasses 和属性的详细信息，请参阅以下参考资料：

- Microsoft Active Directory：
  - ObjectClasses：MSDN 上的所有类
  - 属性：MSDN 上的所有属性
- OpenLDAP：RFC 4512

# Kerberos 身份验证的前提条件

如果使用 Kerberos 对强制网络门户用户进行身份验证，请记住以下几点。

### 主机名字符限制

如果使用Kerberos身份验证，则托管设备的主机名必须少于15个字符（这是Windows设置的NetBIOS限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

### DNS 响应字符数限制

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

# 领域字段

以下字段用于配置领域。

### 领域配置字段

这些设置适用于领域中的所有 Active Directory 服务器或域控制器（也称为目录）。

**名称**

领域的唯一名称。

- 要在身份策略中使用领域，系统需支持字母数字和特殊字符。
- 要在 RA-VPN 配置中使用领域，系统需支持字母数字、连字符 (-)、下划线 (_) 和加号 (+) 字符。

**说明**

（可选。）输入领域的描述。

**类型 (Type)**

领域类型， **AD** 表示 Microsoft Active 目录， **LDAP** 表示其他支持的 LDAP 存储库，或 **本地**。有关支持的 LDAP 存储库的列表，请参阅领域支持的服务器，第 44 页。您可以使用 LDAP 存储库对强制网络门户用户进行身份验证；所有其他都需要 Active Directory。

注释 仅强制网络门户支持 LDAP 领域。

领域类型 **LOCAL** 用于配置本地用户设置。LOCAL 领域用于远程访问用户身份验证。

为 LOCAL 领域添加以下本地用户信息：

- **用户名**-用户的名称。
- **密码**-本地用户密码。

- **确认密码**-确认本地用户密码。

注释 **点击添加其他本地用户** 以将更多用户添加到 LOCAL 领域。

您可以在创建领域并为本地用户更新密码后添加更多用户。您还可以创建多个 LOCAL 领域，但不能将其禁用。

**AD 主域 (AD Primary Domain)**

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

**AD 加入用户名和 AD 加入密码 (AD Join Username and AD Join Password)**
（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

用于专为 Kerberos 强制网络门户主动身份验证设计的 Microsoft Active Directory 领域，表示具有可在 Active Directory 域中创建域计算机帐户的适当权限的任何 Active Directory 用户的标识用户名和密码。

记住以下几点：

- DNS 必须能够将域名解析为 Active Directory 域控制器的 IP 地址。
- 指定的用户必须能够将计算机加入到 Active Directory 域。
- 用户名必须是完全限定的（例如，**`administrator@mydomain.com`**，而不是 **`administrator`**）。

如果选择 **`Kerberos`**（或 **`HTTP 协商`**，如果希望 Kerberos 作为选项）作为身份规则中的**身份验证协议**，则必须为您所选的 **领域** 配置 **AD 加入用户名** 和 **AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。

注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

### 目录用户名和目录密码 (Directory Username and Directory Password)

为具有检索用户信息的相应权限的用户提供的标识用户名和密码。

请注意以下事项：

- 对于某些版本的 Microsoft Active Directory，可能需要特定权限才能读取用户和组。有关详细信息，请参阅 Microsoft Active Directory 提供的文档。
- 对于 OpenLDAP，用户的访问权限由 OpenLDAP 规范第 8 部分中讨论的 `<level>` 参数确定。用户的 `<level>` 应为 `auth` 或更高。
- 用户名必须是完全限定的（例如，**`administrator@mydomain.com`**，而不是 **`administrator`**）。

注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

### 基本 DN

（可选。）Cisco Secure Firewall Management Center应在其上开始搜索用户数据的服务器上的目录树。如果未指定 **基本 DN**，则系统会检索可连接到服务器的顶级 DN。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **`ou=security,dc=example,dc=com`**。

### 组 DN (Group DN)

（可选。）Cisco Secure Firewall Management Center应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 45 页中显示。如果未指定 **组 DN**，则系统会检索可连接到服务器的顶级DN。

注释 以下是系统在您的目录服务器中的用户、组和 DN 中 支持 的字符列表。使用除以下字符以外的任何字符可能会导致系统无法下载用户和组。

| 实体 | 支持的字符 |
|---|---|
| 用户名 | **a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `** |
| 组名称 | **a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `** |
| 基础 DN 和组 DN | **a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `** |

用户名中的任何位置均不支持空格，包括末尾。

编辑现有领域时，以下字段可用。

### 用户会话超时

（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

输入用户会话超时前持续的分钟数。在用户登录事件后，默认值为 1440（24 小时）。超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则 Cisco Secure Firewall Management Center 会将该用户视为未知（**失败的强制网络门户用户**除外）。

此外，如果在没有领域的情况下设置 ISE/ISE-PIC，并且超时，则需要解决方法。有关详细信息，请联系 思科技术支持中心。

您可以为以下内容设置超时值：

- **用户代理和 ISE/ISE-PIC 用户**：由用户代理或 ISE/ISE-PIC（被动身份验证类型）跟踪的用户的超时。

  您指定的超时值 不 适用于 pxGrid SXP 会话主题订用（例如，目标 SGT 映射）。相反，只要没有来自 ISE 的给定映射的删除或更新消息，会话主题映射就会保留。

  有关 ISE / ISE-PIC 的详细信息，请参阅 ISE/ISE-PIC 身份源。

- **终端服务代理用户**：由 TS 代理（一种被动身份验证类型）跟踪的用户的超时。有关详细信息，请参阅终端服务 (TS) 代理身份源。

- **强制网络门户用户**：使用强制网络门户（一种主动身份验证类型）成功登录的用户的超时。有关详细信息，请参阅强制网络门户身份源。

- **失败的强制网络门户用户**：未使用强制网络门户成功登录的用户的超时。您可以配置 Cisco Secure Firewall Management Center 将用户视为身份验证失败的用户之前的 **最大登录尝试次数** 。可以选择使用访问控制策略为身份验证失败的用户授予对网络的访问权限，如果是这样，此超时值将应用于这些用户。

  有关失败的强制网络门户登录的详细信息，请参阅强制网络门户字段。

- **访客强制网络门户用户**：以访客用户身份登录到强制网络门户的用户的超时。有关详细信息，请参阅强制网络门户身份源。

# 领域目录和同步字段

### 领域目录字段

这些设置适用于领域中的各个服务器（例如 Active Directory 域控制器）。

#### 主机名/IP 地址

Active Directory 域控制器计算机的完全限定主机名。要查找完全限定名称，请参阅 查找 Active Directory 服务器名称，第 52 页。

如果您使用 Kerberos 对强制网络门户进行身份验证，还请确保您了解以下内容：

如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

**端口 (Port)**

服务器的端口。

**加密**

（强烈建议。）要使用的加密方法：

- **STARTTLS** - 加密的 LDAP 连接
- **LDAPS** - 加密的 LDAP 连接
- 无 **(None)** - 未加密的 LDAP 连接（不安全的流量）

要与 Active Directory 服务器安全通信，请参阅 安全连接到 Active Directory 或 LDAP，第 52 页。

**CA 证书**

用于对服务器进行身份验证的 TLS/SSL 证书。必须配置 **STARTTLS** 或 **LDAPS** 作为 **加密** 类型才能使用 TLS/SSL 证书。

如果使用证书进行身份验证，则证书中的服务器名称必须与服务器**主机名/IP 地址 (Hostname / IP Address)** 匹配。例如，如果将 10.10.10.250 作为 IP 地址，而不是证书中的 **computer1.example.com**，连接会失败。

**用于连接目录服务器的接口**

仅 RA VPN 身份验证需要，以便 Cisco Secure Firewall Threat Defense 可以安全地连接到 Active Directory 服务器。但是，此接口不用于下载用户和组。

只能选择路由接口组。有关详细信息，请参阅接口。

点击以下选项之一：

- **通过路由查找进行解析**：使用路由连接到 Active Directory 服务器。
- **选择接口**：选择要连接到 Active Directory 服务器的特定托管接口。

### 用户 同步 字段

**AD 主域 (AD Primary Domain)**

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

**输入查询以查找用户和组**

**基本 DN：**

（可选。）防火墙管理中心应在其上开始搜索用户数据的服务器上的目录树。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **ou=security,dc=example,dc=com**。

**组 DN (Group DN)：**

（可选。）防火墙管理中心应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 45 页中显示。

注释 组名和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 和后斜线 (\)，因为这些组中的用户不会被下载，也不能用于身份策略。

**加载组**

让您能够下载要用于用户感知和用户控制的用户和组。

**可用组 (Available Groups)、添加以包含 (Add to Include)、添加以排除 (Add to Exclude)**

限制可在策略中使用的组。

- 除非将组移至 **包含的组和用户** 或 **排除的组或用户** 字段，否则 **可用组** 字段中显示的组可用于策略。
- 如果您将组移动到**包含的组和用户** 字段中，只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。
- 如果您将组移动到**排除的组和用户**字段中，它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。

注释 使用公式 **R = I - (E+e) + i**计算下载到 防火墙管理中心 的用户，其中：

- R 是已下载用户的列表
- I 是包含的组
- E 是排除的组
- e 是排除的用户
- i 是包含的用户

**立即同步**
点击以将组和用户与 AD 同步。

**开始自动 同步 ， 在**
输入从 AD下载用户和组的时间和时间间隔。

# 安全连接到 Active Directory 或 LDAP

要在 Active Directory 或 LDAP 服务器与 Cisco Secure Firewall Management Center 之间创建安全连接（我们强烈建议这样做），必须执行以下所有任务：

- 导出服务器的根证书。
- 将根证书作为受信任 CA 证书导入 Cisco Secure Firewall Management Center (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **受信任 CA (Trusted CAs)**)。
- 查找服务器的完全限定名称。
- 创建领域目录。

有关详细信息，请参阅以下任务之一。

**相关主题**

导出 Active Directory 服务器的根证书 ， 第 53 页
查找 Active Directory 服务器名称 ， 第 52 页
创建 LDAP 领域或 Active Directory 领域和领域目录 ， 第 36 页

## 查找 Active Directory 服务器名称

要在 防火墙管理中心中配置领域目录，您必须知道完全限定服务器名称，您可以在后续程序中找到该名称。

这些任务仅适用于 Microsoft Active Directory。如果您使用 LDAP，请咨询相应的参考人员以了解该程序。

### 开始之前

您必须以具有足够权限查看计算机名称的用户身份登录 Active Directory 服务器。

### 过程

**步骤 1** 登录 Active Directory 服务器

**步骤 2** 点击**开始 (Start)**。

**步骤 3** 右键点击 **此 PC (This PC)**。

**步骤 4** 点击**属性 (Properties)**。

**步骤 5** 点击**高级系统设置 (Advanced System Settings)**。

**步骤 6** 点击**计算机名称 (Computer Name)** 选项卡。

**步骤 7** 注意 **完整计算机名称**的值。
在 防火墙管理中心 中配置领域目录时，必须输入此确切名称。

### 下一步做什么

创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页。

### 相关主题

导出 Active Directory 服务器的根证书，第 53 页

## 导出 Active Directory 服务器的根证书

接下来的任务讨论如何导出 Active Directory 服务器的根证书，这是安全连接到 防火墙管理中心 以获取用户身份信息所必需的。

这些任务仅适用于 Microsoft Active Directory。如果您使用 LDAP，请咨询相应的参考人员以了解该程序。

### 开始之前

您必须知道 Active Directory 服务器的根证书的名称。根证书的名称可能与域的名称相同，或者证书的名称可能不同。后面的程序显示了查找名称的一种方法；可能还有其他方式。

### 过程

**步骤 1** 以下是查找 Active Directory 服务器根证书名称的一种方法；有关详细信息，请参阅 Microsoft 文档：

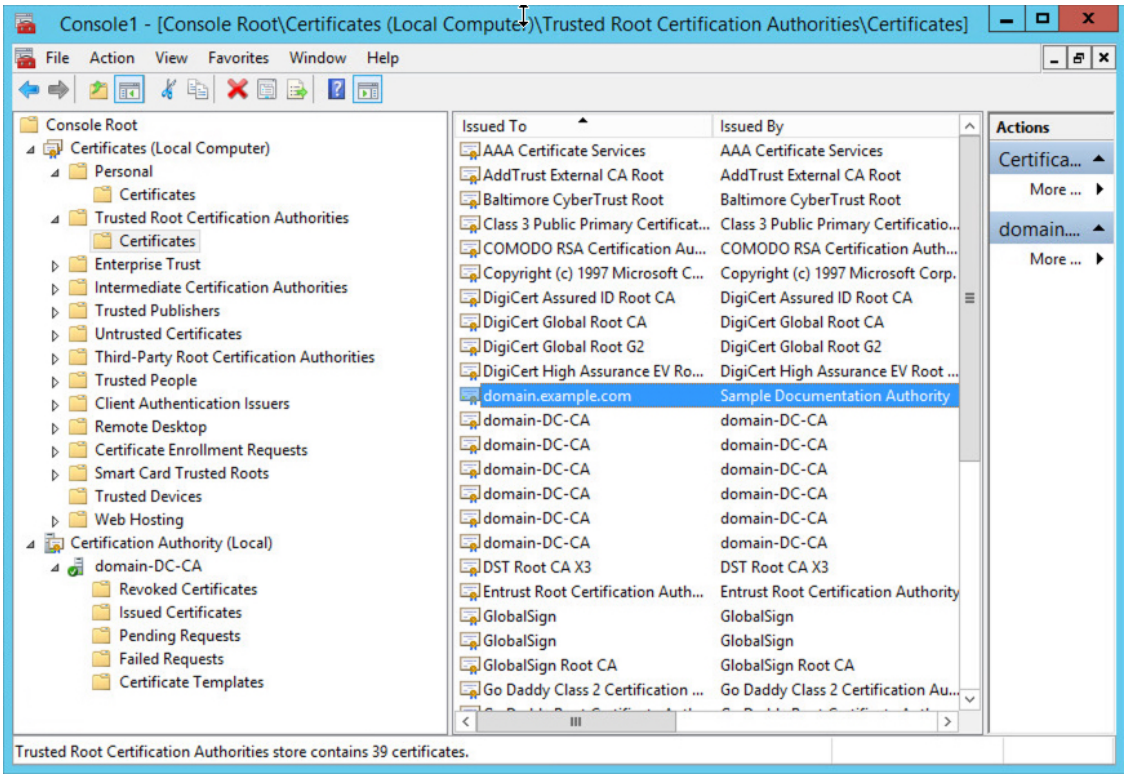
a) 以具有运行 Microsoft 管理控制台权限的用户身份登录 Active Directory 服务器。

b) 点击 **开始** 并输入 **mmc**。

c) 点击 **文件** > **添加/删除 Snap-in**

d) 从左侧窗格的可用管理单元列表中，点击 **证书（本地）**。

e) 点击**添加 (Add)**。
f) 在证书管理单元对话框中，点击 **计算机帐户** 然后点击 **下一步**。
g) 在“选择计算机”对话框中，点击 **本地计算机** 然后点击 **完成**。
h) 仅限 *Windows Server 2012*。重复上述步骤以添加证书颁发机构管理单元。
i) 点击 **控制台根** > **受信任证书颁发机构** > **证书**。
服务器的受信任证书显示在右侧窗格中。下图只是 Windows Server 2012 的示例；您的产品可能看起来有所不同。




**步骤 2** 使用 **certutil** 命令导出证书。

这只是导出证书的一种方式。这是导出证书的便捷方式，尤其是在您可以运行Web浏览器并从Active Directory 服务器连接到 防火墙管理中心 的情况下。

a) 点击 **开始** 并输入 **cmd**。
b) 输入命令 **certutil -ca.cert** 证书-名称。
服务器的证书显示在屏幕上。
c) 将整个证书复制到剪贴板，以 **-----BEGIN CERTIFICATE-----** 开头和以 **-----END CERTIFICATE-----** 结尾（包括这些字符串）。

### 下一步做什么

将 Active Directory 服务器的证书作为受信任 CA 证书导入 防火墙管理中心，如 添加受信任 CA 对象中所述。

### 相关主题

查找 Active Directory 服务器名称，第 52 页

# 同步用户和组

同步 用户和组意味着 防火墙管理中心 查询您为组和这些组中的用户配置的领域和目录。所有用户都可以在身份策略中使用 防火墙管理中心 查找。

如果发现问题，您很可能需要添加包含 防火墙管理中心 无法加载的用户和组的领域。有关详细信息，请参阅领域和受信任的域，第 40 页。

### 开始之前

为每个 Active Directory 域创建一个 Cisco Secure Firewall Management Center 领域，并为每个林中的每个 Active 导向器域控制器创建一个 防火墙管理中心 目录。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页。

**注释** Microsoft Azure AD 领域不需要同步用户和组。

必须仅为具有要在用户控制中使用的用户的域创建领域。

您最多可以嵌套 Microsoft AD 组， Cisco Secure Firewall Management Center 将下载这些组及其包含的用户。您可以选择限制下载的组和用户，如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页中所述。

您必须使用域的原始域名而不是该域的任何备用用户主体名称 (UPN) 后缀创建领域。否则，用户和组将无法下载，并且身份策略不会实施。例如，如果原始域为 `domain.example.com`，备用 UPN 名称为 `domain2.mydomain.com`，则必须将领域配置为使用 `domain.example.com`。有关配置备用 UPN 后缀的详细信息，请参阅 learn.microsoft.com 上的 配置备用登录 ID 等资源。

### 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 点击每个领域旁边的 **下载** （）。

**步骤 4** 要查看结果，请点击**同步结果 (Sync Results)** 选项卡。
“领域”列指示 Active Directory 林中的用户和组同步是否存在问题。查找每个领域旁边的以下指示器。

| 领域中的指示器列 | 含义 |
|---|---|
| （无） | 所有用户和组同步无错误。无需任何操作。 |

| 领域中的指示器列 | 含义 |
| --- | --- |
| 黄色三角形 (⚠) | 同步用户和组时出现问题。确保为每个 Active Directory 域添加了一个领域，并为每个 Active Directory 域控制器添加了一个目录。<br>有关详细信息，请参阅排除跨域信任故障，第 71 页。 |

# 创建领域序列

通过以下程序，您可以创建领域序列，这是系统在应用身份策略时搜索的领域的有序列表。将领域序列添加到身份规则的方式与添加领域的方式完全相同；区别在于系统在应用身份策略时按领域序列中指定的顺序搜索所有领域。

### 开始之前

您必须创建并启用至少两个领域，每个领域对应于与 Active Directory 服务器的连接。您无法为 LDAP 领域创建领域序列。

按创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页中所述创建领域。

### 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域序列**。

**步骤 3** 点击 **领域序列** 选项卡。

**步骤 4** 点击**添加序列**。

**步骤 5** 在 **名称** 字段中，输入用于标识领域序列的名称。

**步骤 6** （可选。）在 **说明**字段中，输入领域序列的说明。

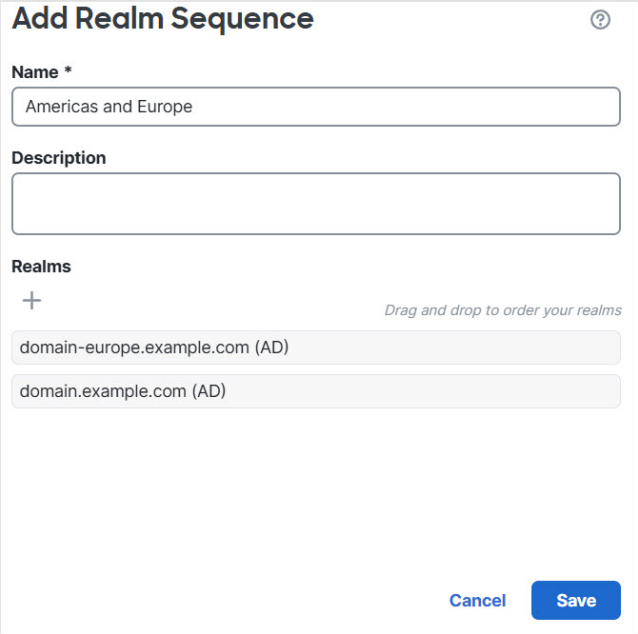
**步骤 7** 在领域下，点击 **添加** (+)。

**步骤 8** 点击每个领域的名称以添加到序列。

要缩小搜索范围，请在**过滤器**字段中输入全部或部分领域名称。

**步骤 9** 点击**确定**。

**步骤 10** 在添加领域序列对话框中，按照您希望系统搜索这些领域的顺序拖放领域。
下图显示由两个领域组成的领域序列的示例。 **domain-europe.example.com** 领域将用于搜索 **domain.example.com** 领域前的用户。




**步骤 11** 点击**保存**。

### 下一步做什么

请参阅创建身份策略。

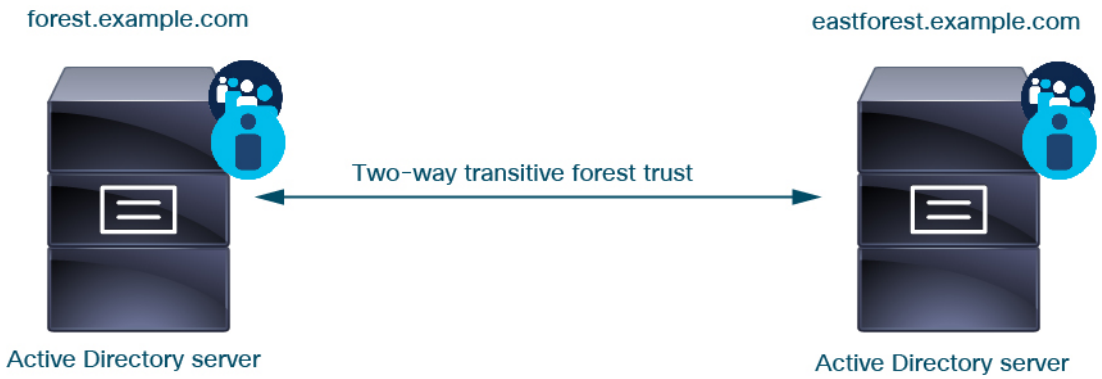
# 配置 防火墙管理中心 的跨域信任：设置

这是对几个主题的介绍，这些主题将引导您配置 防火墙管理中心 使用跨域信任的两个领域。

此分步示例涉及两个林： **forest.example.com** 和 **eastforest.example.com**。配置目录林，以便每个目录林中的某些用户和组可以由另一个目录林中的 Microsoft AD 进行身份验证。

**注释** 本主题仅适用于 Microsoft AD 领域。它不适用于 Microsoft Azure AD 领域。

以下是本示例中使用的示例设置。




使用前面的示例，您可以按如下所示设置 防火墙管理中心 ：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录

示例中的每个领域都有一个域控制器，在 防火墙管理中心 中配置为目录。本示例中的目录配置如下：

- **forest.example.com**
  - 用户的基本可分辨名称 (DN)： **ou=UsersWest,dc=forest,dc=example,dc=com**
  - 组的基本 DN： **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - 用户的基本 DN： **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - 组的基本 DN： **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

相关主题

为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录 ，第 58 页

# 为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录

这是分步程序中的第一个任务，解释如何配置防火墙管理中心来识别在跨域信任关系中配置的Active Directory 服务器，这是企业组织越来越常见的配置。有关此样本配置的概述，请参阅配置 防火墙管理中心 的跨域信任：设置 ，第 57 页。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

### 开始之前

您必须在跨域信任关系中配置 Microsoft Active Directory 服务器；有关详细信息，请参阅领域和受信任的域，第 40 页。

如果使用 LDAP 或 Microsoft Azure AD 对用户进行身份验证，则无法使用此程序。

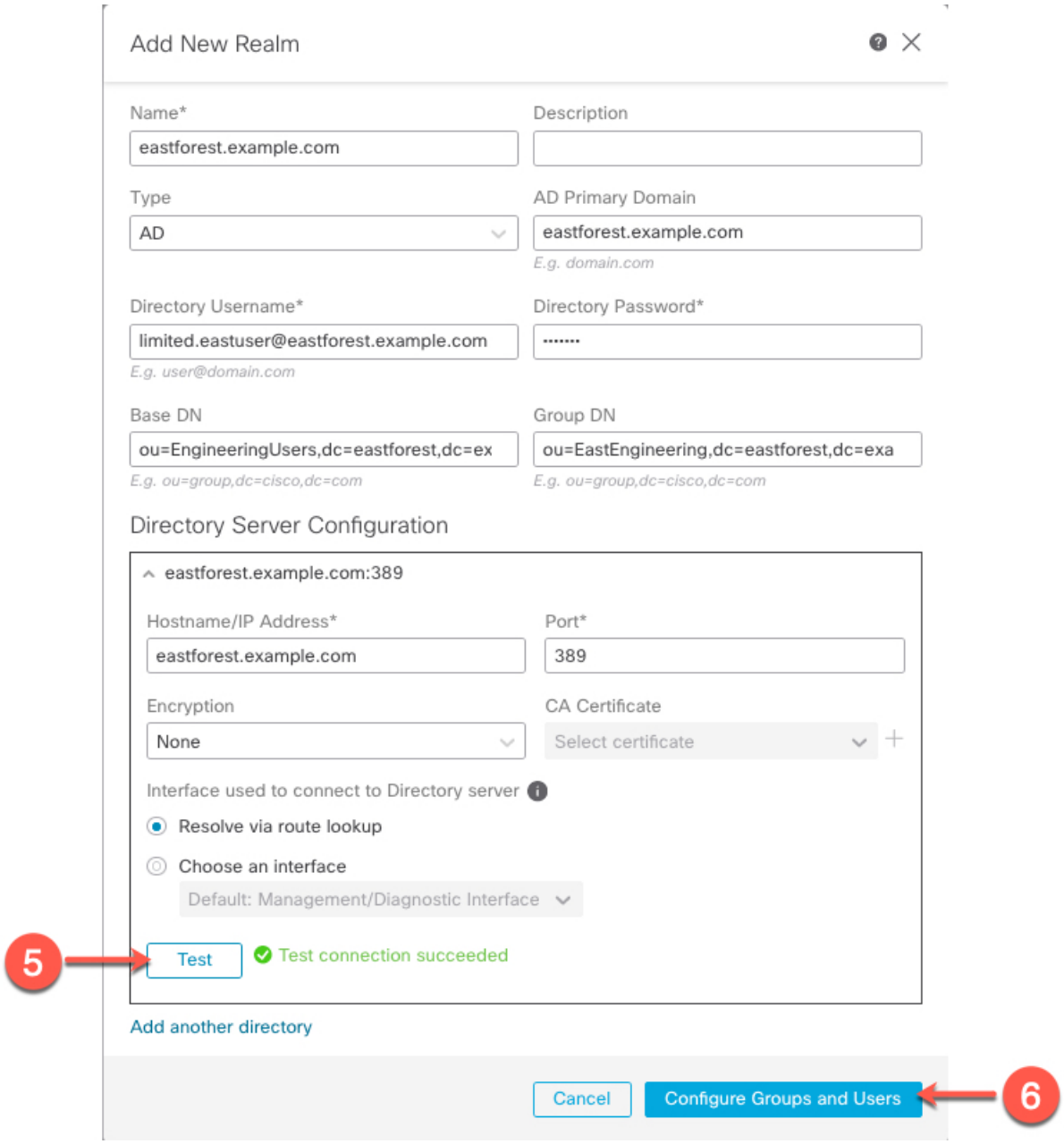
## 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 点击 **添加领域** > **Active Directory/LDAP**。

**步骤 4** 要配置 **forest.example.com**，请输入以下信息。




注释

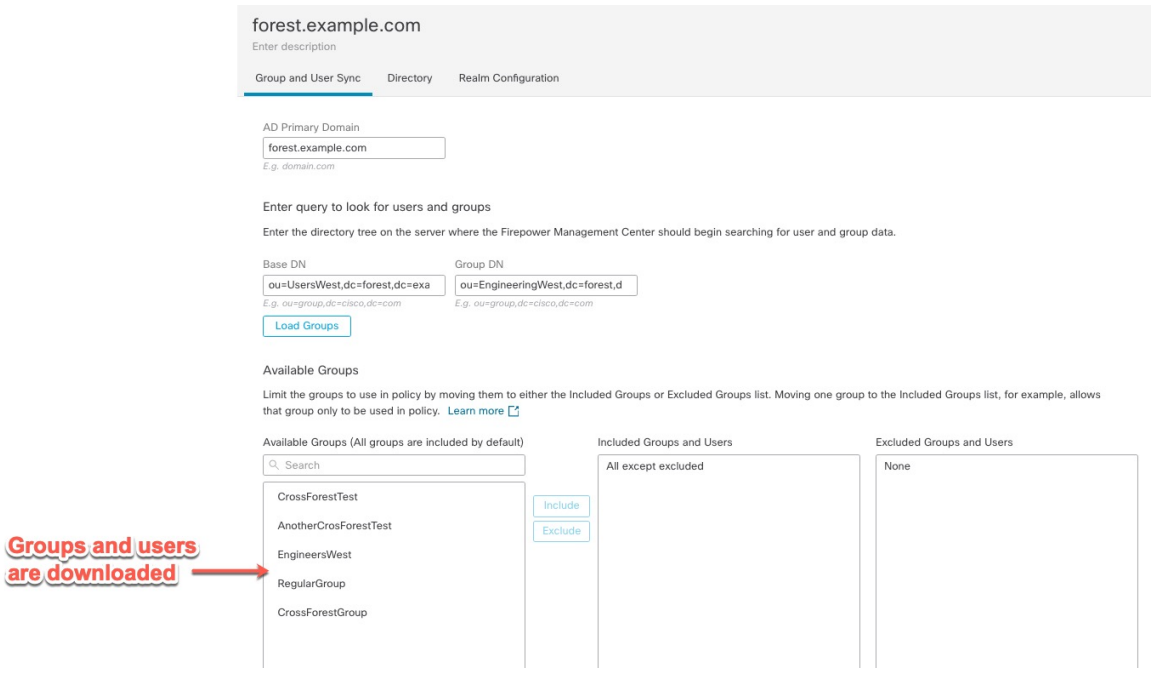
**目录用户名** 可以是 Active Directory 域中的任何用户；无需特殊权限。

**用于连接到目录服务器的接口** 可以是可以连接到 Active Directory 服务器的任何接口。

**步骤 5** 点击**测试**并确保测试成功后再继续。

**步骤 6** 点击**配置组和用户**。

**步骤 7** 如果配置成功，则会显示下一页，如下所示。




**注释**

如果未下载组和用户，请验证 **基本 DN** 和 **组 DN** 字段中的值，然后点击 **加载组**。

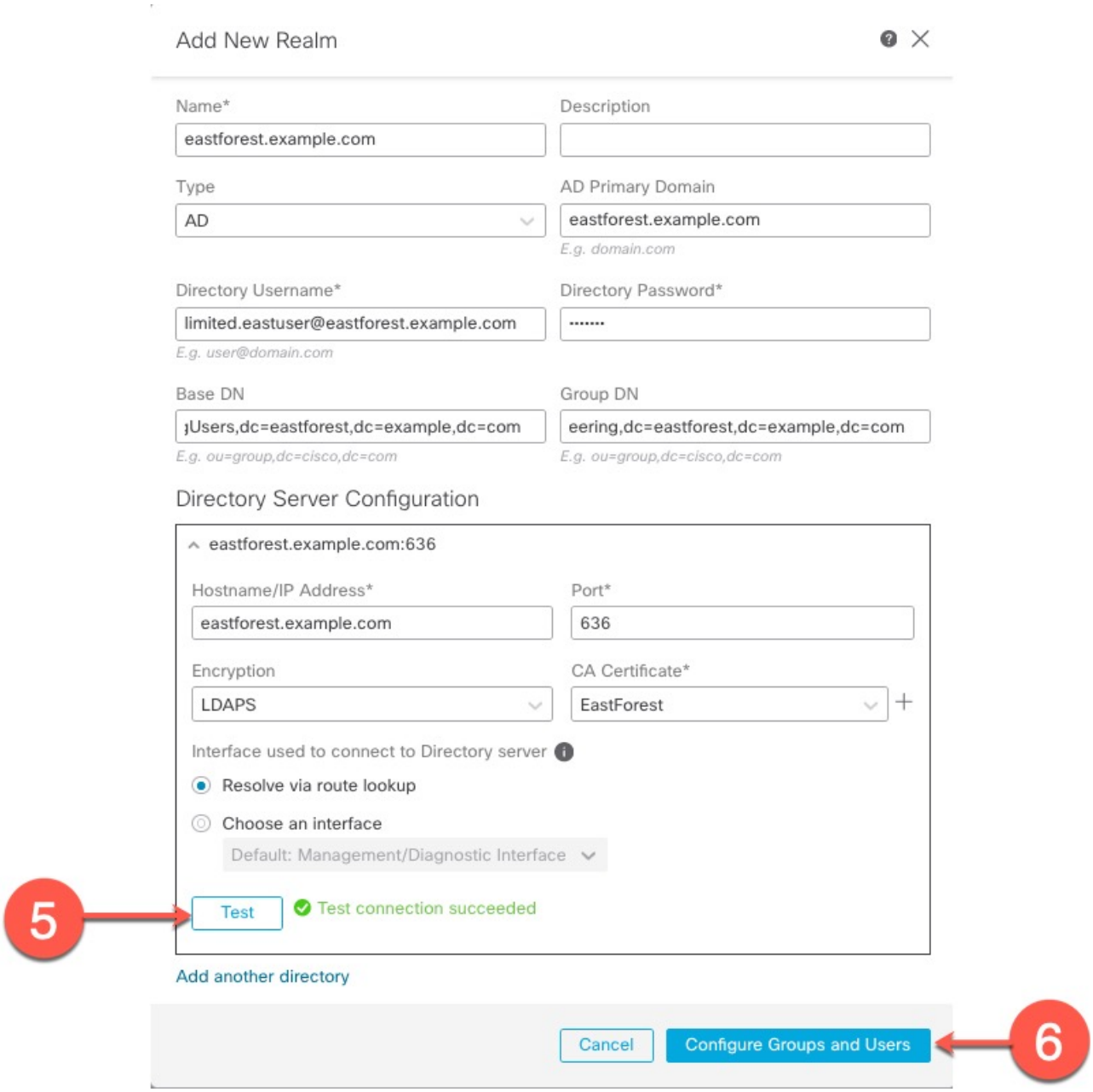
此页面上还有其他可选配置；有关它们的详细信息，请参阅 领域字段，第 46 页 和 领域目录和同步字段，第 49 页。

**步骤 8** 如果在此页面或选项卡页面上进行了更改，请点击 **保存**。

**步骤 9** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 10** 点击**添加领域**。

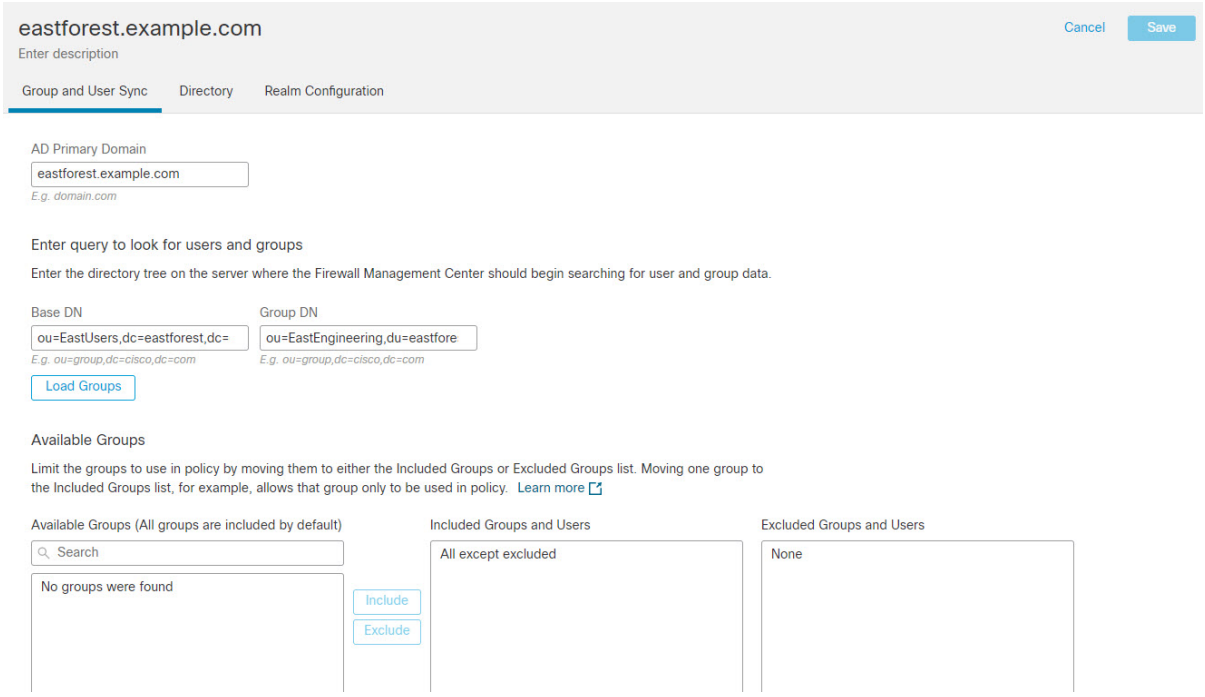
**步骤 11** 要配置 **eastforest.example.com**，请输入以下信息。




**步骤 12** 点击**测试**并确保测试成功后再继续。

**步骤 13** 点击**配置组和用户**。

**步骤 14** 如果配置成功，则会显示下一页，如下所示。




### 相关主题

为跨域信任配置配置 Cisco Secure Firewall Management Center 步骤 2：同步用户和组，第 63 页

# 为跨域信任配置配置 Cisco Secure Firewall Management Center 步骤 2：同步用户和组

配置两个或多个具有跨域信任关系的 Active Directory 服务器后，必须下载用户和组。该过程会暴露 Active Directory 配置的可能问题（例如，为一个 Active Directory 域而不是为另一个 Active Directory 域下载的组或用户）。

### 开始之前

确保您已执行 为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录，第 58 页中讨论的任务。

### 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 在跨域信任中任何领域行的末尾，点击 **立即下载** （），然后点击**是**。

**步骤 4** 点击 **复选标记**（） （通知） > **任务**。

如果组和用户下载失败，请重试。如果后续尝试失败，请查看您的领域和目录设置，如领域字段，第 46 页 和 领域目录和同步字段，第 49 页中所述。

**步骤 5** 请点击 **集成** > **其他集成** > **领域** > **同步结果**。

**相关主题**

为跨域信任配置 Cisco Secure Firewall Management Center 步骤 3：解决问题，第 64 页

# 为跨域信任配置 Cisco Secure Firewall Management Center 步骤 3：解决问题

在防火墙管理中心中设置跨域信任的最后一步是确保下载的用户和组没有错误。用户和组无法正确下载的一个典型原因是它们所属的领域尚未下载到 防火墙管理中心。

本主题讨论如何诊断由于某个域未配置为在域控制器层次结构中查找该组而无法下载一个林中引用的组。

**开始之前**

**过程**

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

在领域列中，如果领域名称旁边显示 **黄色三角形**（  ），则您必须解决问题。否则，您的结果配置正确，您可以退出。

**步骤 3** 从显示问题的领域重新下载用户和组。

a) 点击 **领域 (Realms)** 选项卡。

b) 点击  （立即下载），然后点击**是**。

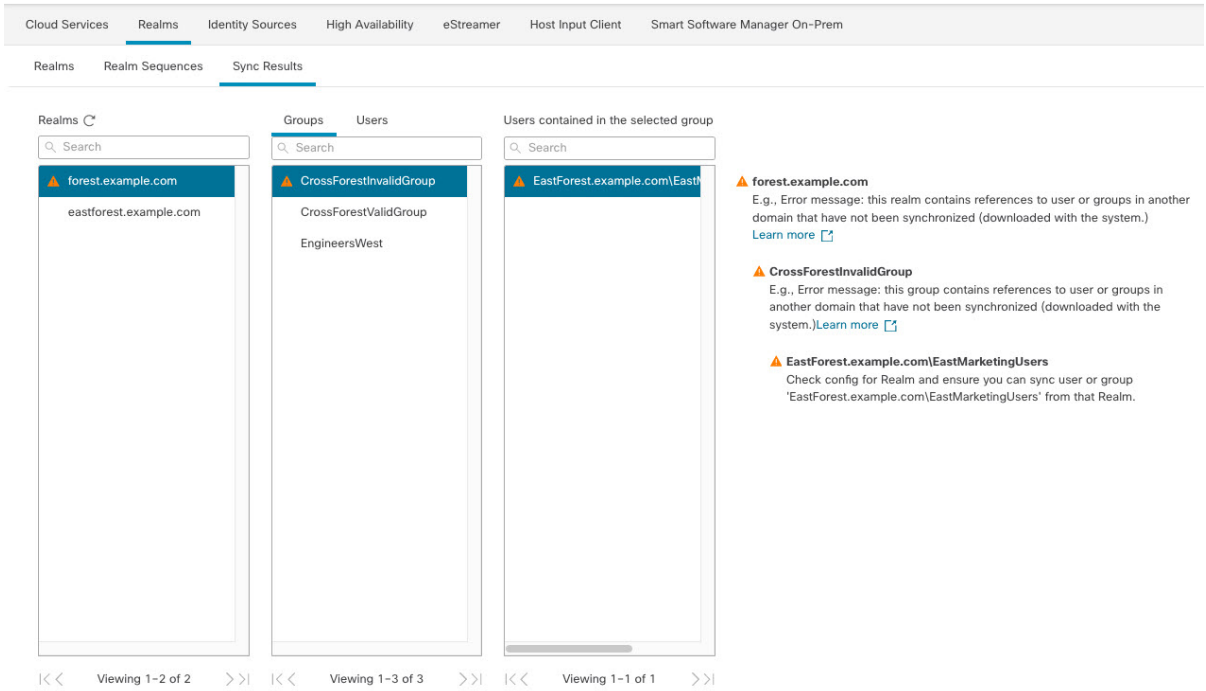
**步骤 4** 点击 **同步结果 (Sync Results)** 选项卡页面。

如果“领域”(Realms) 列中显示 **黄色三角形**（  ），请点击存在问题的领域旁边的 **黄色三角形**（  ）。

**步骤 5** 在中间列中，点击**组**或**用户** 以查找更多信息。

**步骤 6** 在组或用户选项卡页面中，点击 **黄色三角形**（  ）以显示更多信息。

右列应显示足够的信息，以便您可以确定问题的来源。




在上述示例中， **forest.example.com** 包括一个跨域组 **CrossForestInvalidGroup** ，其中包含未由 防火墙管理中心下载的另一个组 **EastMarketingUsers** 。如果在再次同步 **eastforest.example.com** 领域后，错误未解决，则可能意味着 Active Directory 域控制器不包括 **EastMarketingUsers**。

要解决此问题，您可以：

- 从 **CrossForestInvalidGroup**中删除 **EastMarketingUsers** ，再次同步 **forest.example.com** 领域，然后重新检查。
- 从 **eastforest.example.com** 领域的 **组 DN** 中删除 **ou=EastEngineering** 值，这会导致 防火墙管理中心 从 Active Directory 层次结构的最高级别检索组，进行 **eastforest.example.com**同步并重新检查。

# 管理领域

本部分讨论如何使用“领域”页上的控件来为领域执行各种维护任务：

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。。如果显示**视图**( )，则表明配置属于祖先域，或者您没有修改配置的权限。

## 过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 要删除领域，请点击 **删除** ()。

**步骤 4** 要编辑领域，请点击领域旁边的 **编辑** () 并进行更改，如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页中所述。

**步骤 5** 要启用领域，请将**状态**向右滑动；要禁用某个领域，请将其向左滑动。

**步骤 6** 要下载用户和用户组，请点击 **下载** （）。

**步骤 7** 要复制领域，请点击 **复制** ()。

**步骤 8** 要比较领域，请参阅比较领域，第 66 页。

# 比较领域

您必须是 管理员、 访问管理员、 网络管理员或 安全审批人 才能执行此任务。

过程

**步骤 1** 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

**步骤 2** 请点击 **集成** > **其他集成** > **领域** > **领域**。

**步骤 3** 点击**比较领域 (Compare Realms)**。

**步骤 4** 从**比较对象**下拉列表中选择**比较领域**。

**步骤 5** 从**领域 A** 和**领域 B** 下拉列表中选择要比较的领域。

**步骤 6** 点击**确定**。

**步骤 7** 如果要逐一浏览更改，请点击标题栏上方的**上一个**或**下一个**。

**步骤 8** （可选。）点击**比较报告**生成领域比较报告。

**步骤 9** （可选。）点击**新增比较**生成新的领域比较视图。

# 领域和用户下载故障排除

如果发现意外的服务器连接行为，请考虑调整领域配置、设备设置或服务器设置。有关其他相关故障排除信息，请参阅：

- 排除 ISE / ISE-PIC 或 Cisco TrustSec 问题
- TS 代理身份源故障排除
- 强制网络门户身份源故障排除
- 远程访问 VPN 身份源故障排除

- 用户控制故障排除

### 症状：报告但不下载领域和组

Cisco Secure Firewall Management Center的运行状况监控器会通知您用户或领域不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 Cisco Secure Firewall Management Center 。

  造成用户不匹配通常是因为该用户属于不予下载至 Cisco Secure Firewall Management Center。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 防火墙管理中心未知的某个领域。

例如，如果您定义了一个与 防火墙管理中心 中名为 **domain.example.com** 的域相对应的领域，但系统报告从名为 **another-domain.example.com**的域进行了登录，这种情况就属于 领域不匹配。 防火墙管理中心 将此域中的用户识别为“未知”。

您将不匹配阈值设置为某个百分比，高于此百分比时会触发运行状况警告。示例：

- 如果您使用默认为 50% 的不匹配阈值，则在八个传入会话中有两个不匹配领域（不匹配百分比为 25%）的情况下不会触发任何警告。
- 如果您将不匹配阈值设置为 30%，在五个传入会话中有三个不匹配领域（不匹配百分比为 60%）的情况下则会触发警告。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

有关详细信息，请参阅检测领域或用户不匹配 ， 第 70 页。

### 症状：无法下载用户

可能的原因如下：

- 如果您配置的领域**类型**不正确，则将由于系统期望的属性与存储库提供的属性之间不匹配而无法下载用户和组。例如，如果您为 Microsoft Active Directory 领域将**类型**配置为 **LDAP**，则系统期望 `uid` 属性，而在 Active Directory 上它将被设置为`无`。（Active Directory 存储库将 `sAMAccountName` 用于用户 ID。）

  **解决方案**：适当设置领域**类型**字段：对于 Microsoft Active Directory，设置为 **AD**；对于其他受支持的 LDAP 存储库，设置为 **LDAP**。

- 组或组织单位名称中包含特殊字符的 Active Directory 组中的用户，可能不可用于身份策略规则。例如，如果组或组织单位名称包含字符星号 (*)、等号 (=) 或反斜线 (\)，则这些组中的用户无法下载，并且无法用于身份策略。

  **解决方案**：从组或组织单位名称中删除特殊字符。

**重要事项** 要减少 Cisco Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Cisco Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Cisco Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

### 症状：并非一个领域的所有用户都被下载

可能的原因如下：

- 如果尝试下载的用户数超过任何一个领域的最大数量，则下载将在达到最大用户数时停止，同时显示运行状况警报。用户下载限制按 Cisco Secure Firewall Management Center 型号来设置。有关详细信息，请参阅Microsoft Active Directory 的用户限制。
- 每个用户都必须是组的成员。不属于任何组的用户不会被下载。

### 症状：访问控制策略不匹配组成员

此解决方案适用于与其他 AD 域建立信任关系的 AD 域。在以下讨论中，外部域指用户登录的域之外的域。

如果用户属于受信任的外部域中定义的某个组， Cisco Secure Firewall Management Center 则不会跟踪外部域中的成员。例如，请考虑以下情景：

- 域控制器 1 和 2 相互信任
- A 组在域控制器 2 上定义
- 控制器 1 中的用户 `mparvinder` 是 A 组的成员

即使用户 `mparvinder` 在 A 组中，指定 A 组成员身份的 Cisco Secure Firewall Management Center 访问控制策略规则也不与之匹配。

**解决方案：**在包含属于 B 组的所有域 1 帐户的域控制器 1 中创建类似的组。更改访问控制策略规则以匹配 A 组或 B 组的任何成员。

### 症状：访问控制策略与子域成员资格不匹配

如果用户属于母域的子域，Firepower 不跟踪域之间的母/子关系。例如，请考虑以下情景：

- 域 `child.parent.com` 是域 `parent.com` 的子域
- 用户 `mparvinder` 在 `child.parent.com` 中定义

即使用户 `mparvinder` 在子域中，与 `parent.com` 匹配的 Firepower 访问控制策略规则也与 `child.parent.com` 域中的 `mparvinder` 不匹配。

**解决方案：**将访问控制策略规则更改为匹配 `parent.com` 或 `child.parent.com` 中的成员。

### 症状：领域或领域目录测试失败

目录页面上的**测试**按钮将向您输入的主机名或 IP 地址发送 LDAP 查询。如果该查询失败，请检查以下事项：

- 您输入的**主机名**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- 您输入的 **IP 地址**无效。

领域配置页面上的 **测试 AD 加入** 按钮将验证以下事项：

- DNS 将 **AD 主域**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- **AD 加入用户名**和 **AD 加入密码**正确无误。

  **AD 加入用户名**必须是完全限定的（例如， **`administrator@mydomain.com`** ，而不是 **`administrator`**）。
- 用户有足够的权限在域中创建计算机，并将 Cisco Secure Firewall Management Center 作为域计算机加入到该域。

### 症状：在非正常时间发生用户超时

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 服务器上的时间与 Cisco Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 或 TS 代理服务器上的时间与 Cisco Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

### 症状：先前未发现的 ISE/ISE-PIC 用户代理用户的用户数据未显示在 Web 界面上

在系统检测到其数据尚未包含在数据库中的 ISE/ISE-PIC 或 TS 代理用户的活动后，系统会从服务器检索其有关信息。在某些情况下，系统需要额外时间来从 Microsoft Windows 服务器成功检索此信息。在数据检索成功之前，ISE/ISE-PIC 或 TS 代理用户发现的活动不显示在 Web 界面中。

请注意，这还可防止系统使用访问控制规则处理用户的流量。

### 症状：事件中的用户数据为意外

如果您发现用户或用户活动事件包含意外 IP 地址，请检查您的领域。系统不支持为多个领域配置相同的 **AD 主域**值。

### 症状：源于终端服务器登录的用户未被系统唯一识别

如果部署包括终端服务器，并为连接到该终端服务器的一个或多个服务器配置领域，则必须部署思科终端服务 (TS) 代理以准确报告终端服务器环境中的用户登录。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可在 Web 界面中唯一识别这些用户。

有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

# 检测领域或用户不匹配

本部分讨论如何检测领域或用户不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 Cisco Secure Firewall Management Center 。

  造成用户不匹配通常是因为该用户属于不予下载至 Cisco Secure Firewall Management Center。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 防火墙管理中心未知的某个领域。

有关其他详细信息，请参阅领域和用户下载故障排除，第 66 页。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

## 过程

**步骤 1** 启用领域或用户不匹配检测：

a) 如果尚未登录，请登录 管理中心。
b) 请点击 **系统** (⚙) > **运行状况** > **策略**。
c) 创建新运行状况策略或编辑现有运行状况策略。
d) 在“编辑策略”页面上，设置**策略运行时间间隔**。
这是所有运行状况监控任务的运行频率。
e) 在左侧窗格中，点击**领域**。
f) 输入以下信息：

- **启用**：点击**打开**
- **警告用户匹配阈值百分比**：在运行状况监控器中触发警告的领域不匹配或用户不匹配的百分比。有关详细信息，请参阅领域和用户下载故障排除，第 66 页。

g) 在页面底部，点击**保存策略并退出**。
h) 如《Cisco Secure Firewall Management Center 管理指南》中的应用运行状况策略所述，对托管设备应用运行状况策略。

**步骤 2** 通过以下任意方式查看用户和领域不匹配：

- 如果超出警告阈值，点击 防火墙管理中心顶部导航中的 **经过** > **运行状况** 。这将打开运行状况监控器。
- 请点击 **系统** (⚙) > **健康** > **监控器**。

**步骤 3** 在“运行状况监控器”页面上的“显示”列中，展开**领域：域**或**领域：用户**来查看有关不匹配的详细信息。

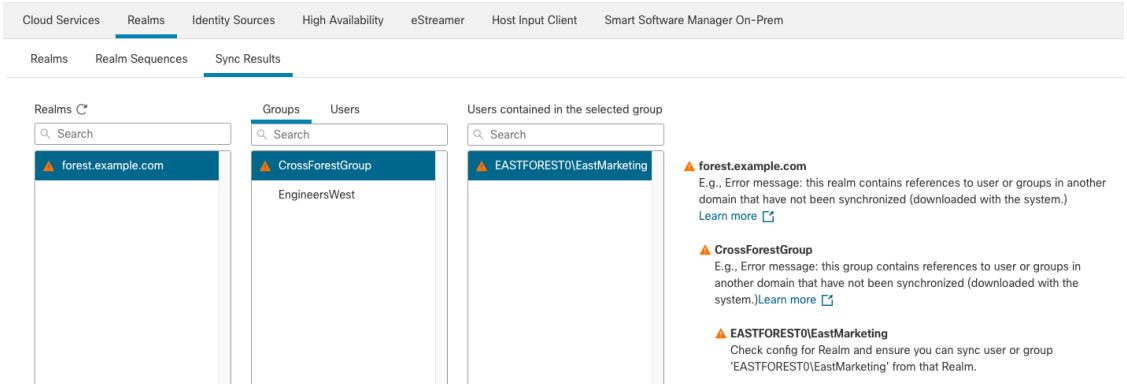
# 排除跨域信任故障

对跨域信任 管理中心 配置进行故障排除的典型问题包括：

- 不为具有共享组的所有林添加领域或目录。
- 配置领域以排除下载用户，并且这些用户在不同领域的组中被引用。
- 某些临时问题。

## 了解问题

如果 管理中心 能够将用户和组与您的 Active Directory 目录林同步存在问题，系统将显示“同步结果”选项卡页面，如下所示。




下表介绍如何解释信息。

| 列 | 含义 |
|---|---|
| 领域 | 显示系统中配置的所有领域。点击 **刷新** （）以更新领域列表。<br>**黄色三角形**（）显示来指示领域中的问题。<br>如果所有用户和组成功同步，则领域旁边不显示任何内容。 |
| 组 | 点击**组 (Groups)** 以显示领域中的所有组。与领域一样，**黄色三角形**（）显示表示问题。<br>点击 **黄色三角形**（）查看有关此问题的更多详细信息。 |
| 用户 | 点击**用户**以显示按组排序的所有用户。 |
| 所选组中包含的用户 | 显示您在“组”列中选择的组中的所有用户。点击 **黄色三角形**（）可在表的右侧显示更多信息。 |
| 包含所选用户的组 | 显示所选用户所属的所有组。点击 **黄色三角形**（）可在表的右侧显示更多信息。 |

| 列 | 含义 |
| --- | --- |
| 错误详细信息（显示在表的右侧）。 | 系统会显示无法同步的 NetBIOS 林名称和组名称。系统无法同步这些用户和组的典型原因如下：<br>• **问题**：包含组和用户的林没有在 管理中心中配置相应的领域。<br>**解决方案**：如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 36 页中所述，为包含该组的林添加一个领域。<br>• **问题**：已将组下从载到 管理中心中排除。<br>**解决方案**：点击**领域** 选项卡页面，点击 **编辑** ()，然后从**排除的组和用户**列表中移动指示的组或用户。 |

### 再次尝试下载用户和组

如果问题是临时的，请下载所有领域的用户和组。

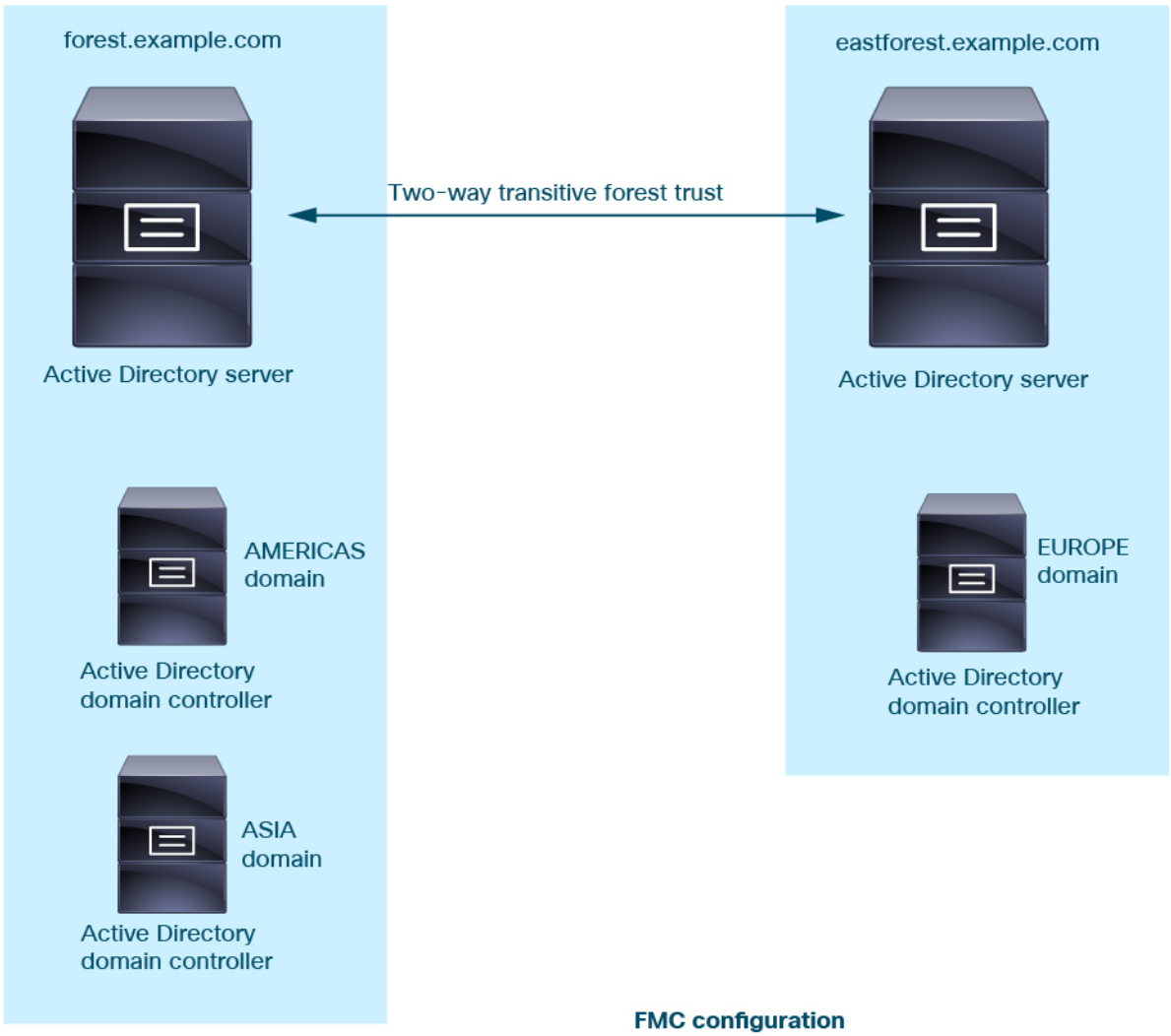
1. 如果尚未登录，请登录 管理中心。
2. 请点击 **集成** > **其他集成** > **领域** > **领域**。
3. 请点击 **下载** （）。
4. 点击 **同步结果 (Sync Results)** 选项卡页面。
5. 如果“领域”列中的条目未显示指示器，则问题已解决。

### 为所有林添加领域

确保已配置：

- 具有要在身份策略中使用的用户的每个林的管理中心 领域。
- 该林中每个域控制器的 管理中心 目录，其中包含要在身份策略中使用的用户。

下图显示了一个示例。




**FMC configuration**


**Realm**: forest.example.com
**Directory**: AMERICAS.forest.example.com
**Directory**: ASIA.forest.example.com

**Realm**: eastforest.example.com
**Directory**: EUROPE.eastforest.example.com

# 领域的历史记录

*表 2:*

| 功能 | 防火墙管理中心最低版本 | 最低版本 | 详细信息 |
|---|---|---|---|
| Microsoft Azure Active Directory (SAML) 领域。 | 7.6.0 | 7.4.0 | 您现在可以使用 Microsoft Azure Active Directory (AD) 领域进行主动和被动身份验证：<br>• 使用 Azure AD 进行主动身份验证：使用 Azure AD 作为强制网络门户。<br>• 使用思科 ISE（版本 7.4.0 中引入）的被动身份验证：防火墙管理中心从 Azure AD 获取组，从 ISE 获取登录用户会话数据。<br>我们使用 SAML（安全断言标记语言）在服务提供程序（处理身份验证请求的设备）和身份提供程序 (Azure AD) 之间建立信任关系。<br>**升级影响**。如果您在升级之前配置了 Microsoft Azure AD 领域，它将显示为 SAML - 为被动身份验证配置的 Azure AD 领域。所有以前的用户会话数据都将保留。<br>新增/修改的屏幕：**集成** > **其他集成** > **领域** > **添加领域** > **SAML - Azure AD**<br>新增/修改的 CLI 命令：无 |
| Microsoft Azure Active Directory (AD) 领域。 | 7.4.0 | 7.4.0 | 您可以将 Microsoft Azure Active Directory (AD) 领域与 ISE 配合使用来对用户进行身份验证并获取用户会话以进行用户控制。<br>新增/修改的屏幕：**系统** > **集成** > **领域** > **添加领域** > **Azure AD** |
| 代理序列。 | 7.2.0 | 7.2.0 | 与领域序列类似，代理序列是在 思科安全云控制 无法与 LDAP 或 Active Directory 服务器通信的情况下可以与 思科安全云控制 通信的一个或多个托管设备。<br>新增/修改的屏幕：**集成** > **其他集成** > **领域** > **代理序列** |
| Active Directory 域的跨域信任。 | 7.2.0 | 7.0.0 | 一组相互信任的 Microsoft Active Directory (AD) 域通常被称为林。此信任关系可使域以不同方式访问彼此的资源。例如，在域 A 中定义的用户账号可以标记为域 B 中所定义组的成员。<br>防火墙管理中心 可以从 Active Directory 目录林获取用户以进行身份规则。 |

| 功能 | 防火墙管理中心最低版本 | 最低版本 | 详细信息 |
| --- | --- | --- | --- |
| 领域序列。 | 7.2.0 | 6.7.0 | 领域序列是要应用身份规则的两个或多个领域的排序列表。将领域序列与身份策略关联时，Firepower 系统会按照领域序列中指定的从第一个到最后的顺序来搜索 Active Directory 域。<br>新增/修改的屏幕：**集成** > **其他集成** > **领域** > **领域序列系统** > **集成** > **领域** > **领域序列** |
| 用于用户控制的领域。 | 7.2.0 | 任意 | 领域是 防火墙管理中心（Active Directory 或 LDAP 用户存储库）之间的连接。 |

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。