领域

以下主题介绍领域和身份策略：

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帐户之间的连接。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。

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 管理中心下一次查询服务器时生效。

要执行用户感知，必须为任何一种领域支持的服务器配置一个领域。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 或 OpenLDAP 上的 LDAP 用户相关联。例如，如果受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。

- 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。

关于用户同步

您可以配置领域或领域序列以便在 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（如果这些用户的邮箱地址与 LDAP 或 AD 用户相同）。这些元数据可用于用户感知。

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 要以尽可能低的延迟启用 管理中心 ，我们强烈建议您配置一个在地理位置上尽可能靠近 管理中心 的领域目录（即域控制器）。

例如，如果您的 管理中心 位于北美，请配置一个也位于北美的领域目录。

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。如果访问控制参数范围太宽泛，则 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，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 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 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 中定义的用户帐户可以标记为域 B 中所定义组的成员。

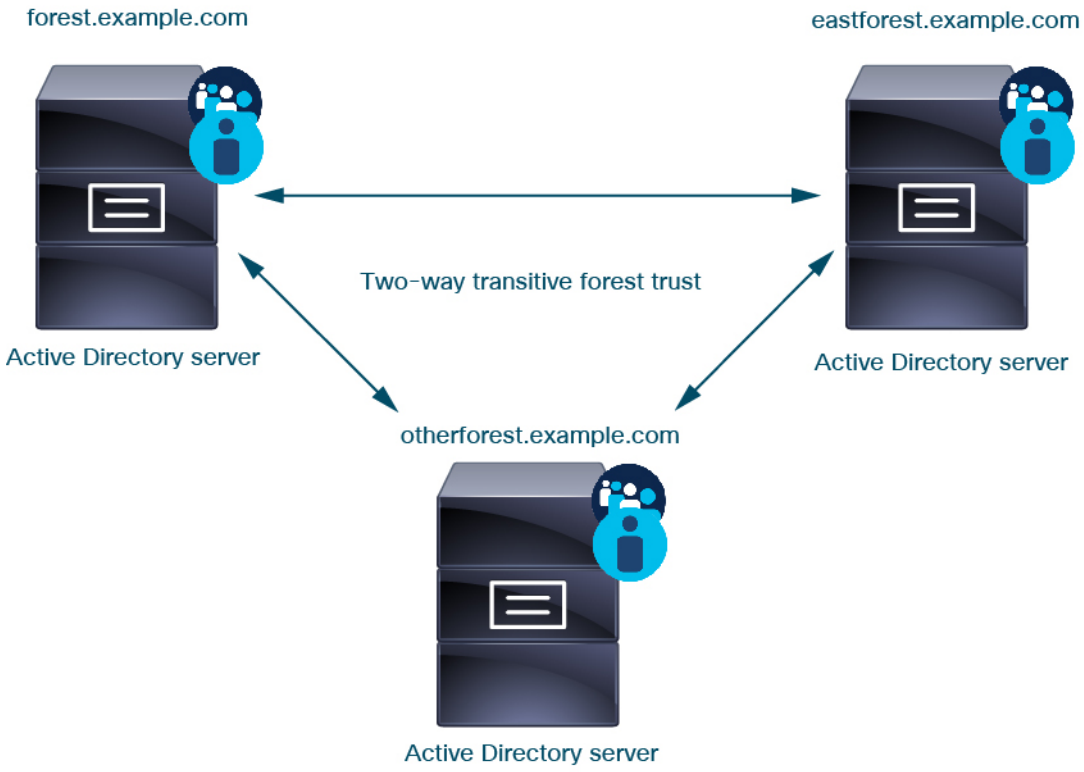
系统和受信任的域

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。

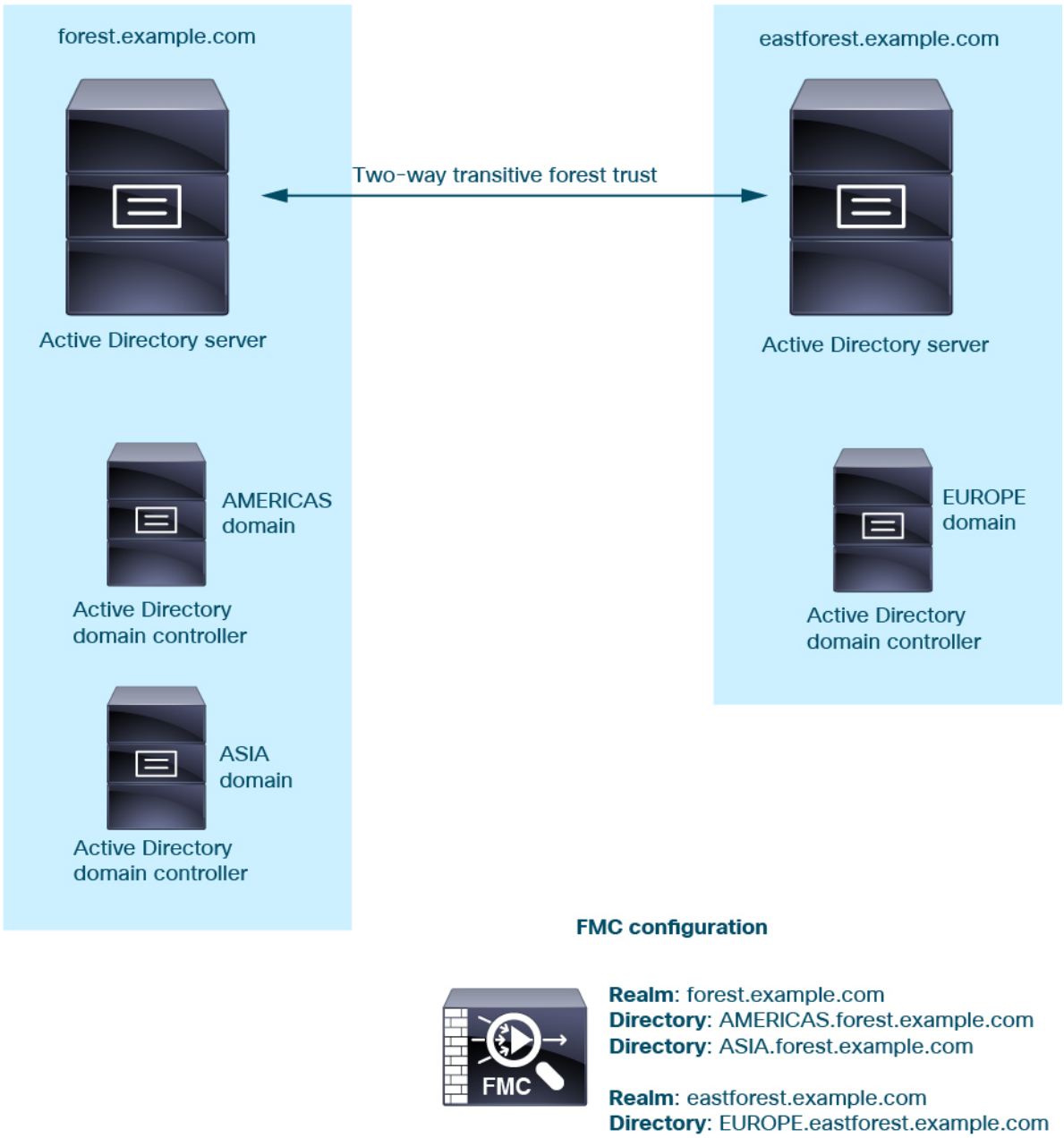
您无需为没有您希望在访问控制策略中使用的用户的任何域配置领域。

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 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 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 管理中心 领域，并将每个域控制器设置为相应领域中的 管理中心 目录。

未能正确配置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 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 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 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
Linux 上 的 OpenLDAP	不支持	不支持	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 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 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 管理中心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，管理中心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	管理中心属性	LDAP ObjectClass	Active Directory 属性	OpenLDAP 属性
LDAP 用户名	用户名	• 用户 • [illegible]	samaccountname	cn uid
名字	名字		givenname	givenname
姓氏	姓氏		sn	sn
邮箱地址	电子邮件		mail Userprincipalname（如果 mail 没有值）	mail
department	部门		department distinguishedname（如果 department 没有值）	ou
telephone number	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

领域的许可证要求

威胁防御 许可证

任意

经典许可证

控制

领域的要求和必备条件

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

创建代理序列

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

开始之前

您必须至少添加两个受管设备至 CDO，所有这些设备都必须能够与 Active Directory 或 ISE / ISE-PIC 通信。

过程

步骤 1 如果尚未登录，请登录 管理中心。

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

步骤 3 点击 **添加代理序列**。

步骤 4 在 **名称** 字段中输入用于标识代理序列的名称。

步骤 5 （可选。）在**说明**字段中，输入代理序列的说明。

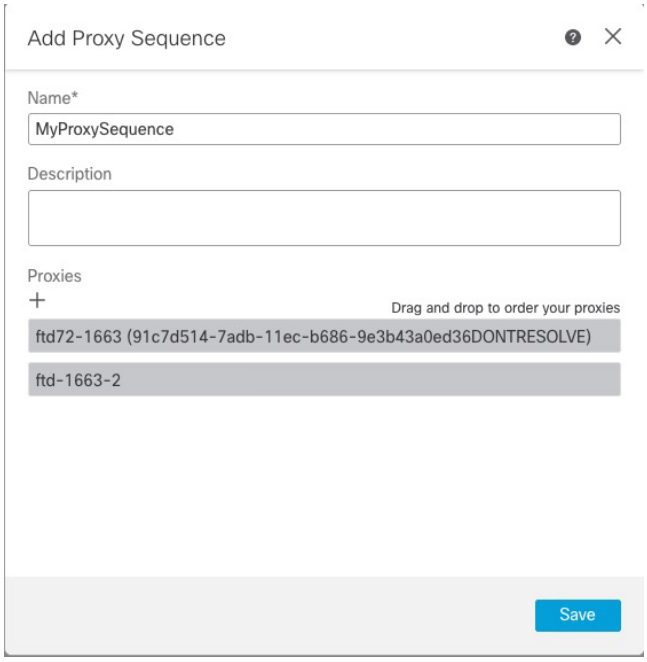
步骤 6 在代理下，点击 **添加**（+）。

步骤 7 点击每个受管设备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 8 点击**确定**。

步骤 9 在添加代理序列对话框中，按要 CDO 来搜索的顺序拖放代理。
下图显示由两个代理组成的代理序列示例。顶部代理将在底部代理之前搜索用户。两个代理都必须能够与 Active Directory 或 ISE / ISE-PIC 进行通信。



步骤 10 点击**保存**。

下一步做什么

请参阅创建身份策略。

创建 Active Directory 领域和领域目录

通过以下程序，您可以创建 领域 （ 管理中心 与 Active Directory 目录领域之间的连接）和 目录 （ 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 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 19 页
- 查找 Active Directory 服务器名称， 第 19 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 12 页 和 领域目录和 同步 字段， 第 16 页。

配置 管理中心 的跨域信任：设置， 第 23 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。

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 身份验证的必备条件， 第 12 页。

如果使用 思科防御协调器（CDO）管理设备，请首先创建代理序列，如 创建代理序列， 第 8 页中所述

重要事项 要以尽可能低的延迟启用 管理中心，我们强烈建议您配置一个在地理位置上尽可能靠近 管理中心 的领域目录（即域控制器）。

例如，如果您的 管理中心 位于北美，请配置一个也位于北美的领域目录。

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**。

步骤 3 要创建新的领域，请点击 **添加领域**。

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 30 页。

步骤 5 按照领域字段，第 12 页中的描述输入领域信息。

步骤 6 （可选。）从 **代理** 列表中，点击受管设备或代理序列以与 ISE / ISE-PIC 通信（如果 CDO 无法执行此操作）。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 7 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 16 页中所述。

步骤 8 （可选。）要为此领域配置其他域，请点击 **添加其他目录**。

步骤 9 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 12 页。
基本 DN (Base DN)	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。
组 DN (Group DN)	Cisco Secure Firewall Management Center 应在其上开始搜索组数据的服务器上的目录树。
代理	从列表中，点击一个或多个受管设备或代理序列。这些设备必须能够与 Active Directory 或 ISE / ISE-PIC 通信，以检索身份策略的用户数据。
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**、**基本DN**、 和 **组 DN** 字段中输入或编辑信息，然后点击 **加载组**。 有关这些字段的信息，请参阅领域字段，第 12 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。 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。 **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。 有关详细信息，请参阅领域目录和 同步 字段，第 16 页。

步骤 10 点击**领域配置**选项卡。

步骤 11 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 16 页。

步骤 12 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 13 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 14 完成配置领域后，点击 **保存 (Save)**。

下一步做什么

- 配置 管理中心 的跨域信任：设置，第 23 页
- 同步用户和组，第 21 页
- 编辑、删除、启用或禁用领域；请参阅管理领域，第 30 页。
- 比较领域，第 31 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 。

Kerberos 身份验证的必备条件

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，则受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受管设备主机名。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，测试连接 AD 连接失败。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 6 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。

请注意以下提示：

- 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 7 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。

代理

从列表中，点击一个或多个受管设备或代理序列。这些设备必须能够与 Active Directory 或 ISE / ISE-PIC 通信，以检索身份策略的用户数据。

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 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）。

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 管理中心 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 19 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，则受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受管设备主机名。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，测试连接 AD 连接失败。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 安全地连接到 Active Directory ， 第 18 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

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 (Choose an interface)**：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。）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：

（可选。）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 7 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，他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 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。

安全地连接到 Active Directory

要在 Active Directory 服务器和 管理中心 （我们强烈建议）之间创建安全连接，您必须执行以下所有任务：

- 导出 Active Directory 服务器的根证书。
- 将根证书导入 管理中心 作为受信任 CA 证书。
- 查找 Active Directory 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 19 页

查找 Active Directory 服务器名称，第 19 页
创建 Active Directory 领域和领域目录，第 10 页

查找 Active Directory 服务器名称

要在 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。

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**。

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

步骤 6 点击 **计算机名称** 选项卡。

步骤 7 注意 **完整计算机名称**的值。
在 FMC 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 Active Directory 领域和领域目录，第 10 页。

相关主题

导出 Active Directory 服务器的根证书，第 19 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 管理中心 以获取用户身份信息所必需的。

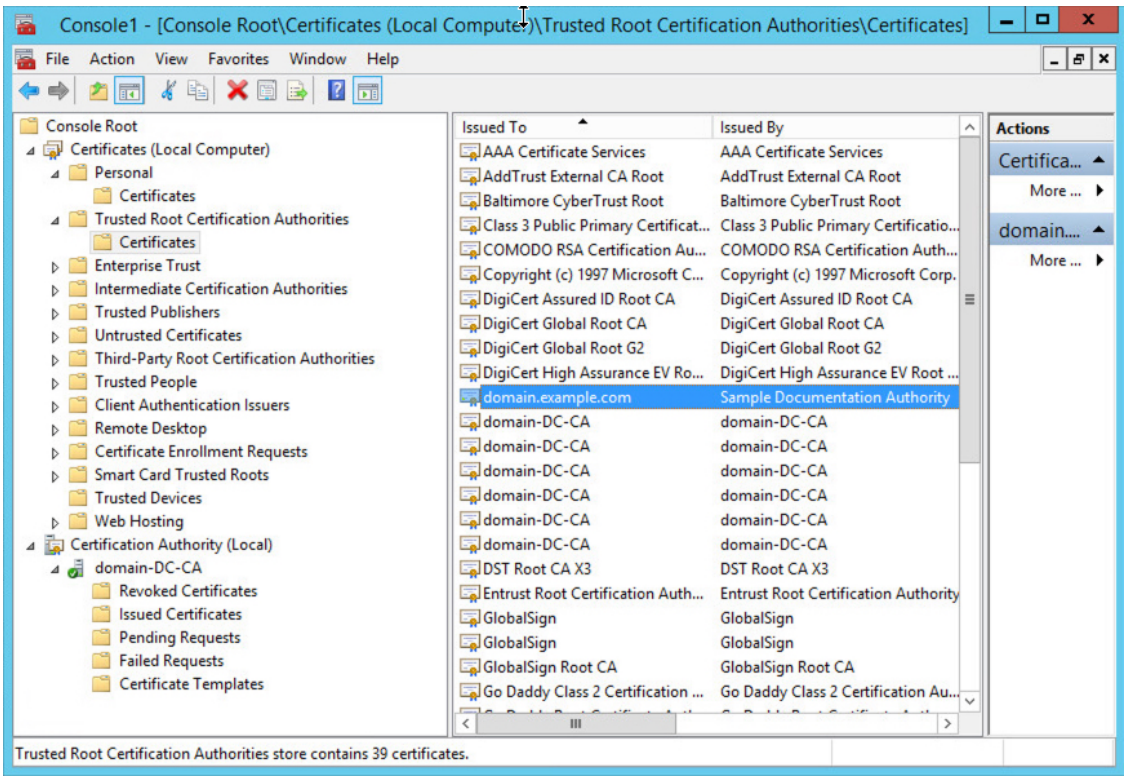
开始之前

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 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 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 19 页

同步用户和组

同步 用户和组意味着 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 管理中心 查找。

如果发现问题，您很可能需要添加包含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 3 页。

开始之前

为每个 Active Directory 域创建一个 管理中心 领域，并为每个林中的每个 Active 导向器域控制器创建一个 管理中心 目录。请参阅创建 Active Directory 领域和领域目录，第 10 页。

必须仅为具有要在用户控制中使用的用户的域创建领域。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **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** 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。
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。 有关详细信息，请参阅 排除跨域信任故障，第 35 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 Active Directory 领域和领域目录，第 10 页中所述创建领域。

过程

步骤 1 如果尚未登录，请登录 管理中心。

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

步骤 3 点击**添加序列 (Add Sequence)**。

步骤 4 在 **名称** 字段中，输入用于标识领域序列的名称。

步骤 5 （可选。）在 **说明**字段中，输入领域序列的说明。

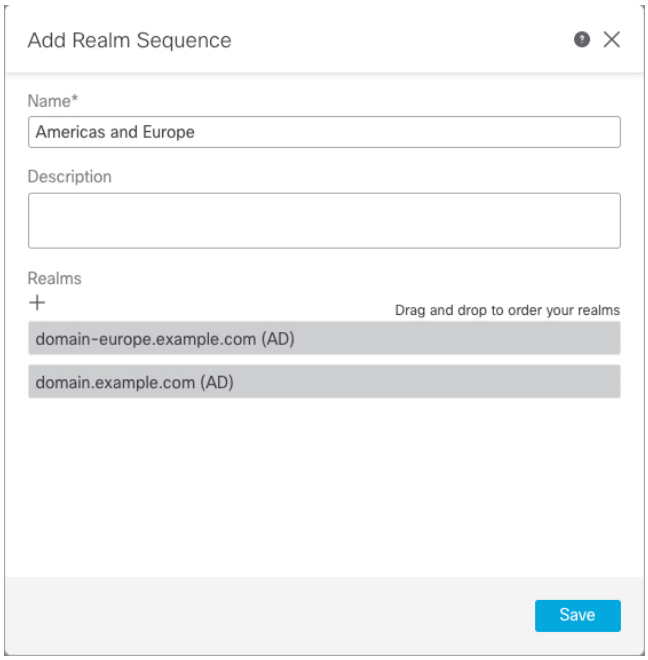
步骤 6 在领域下，点击 **添加**（）。

步骤 7 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 8 点击**确定**。

步骤 9 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 10 点击保存。

下一步做什么

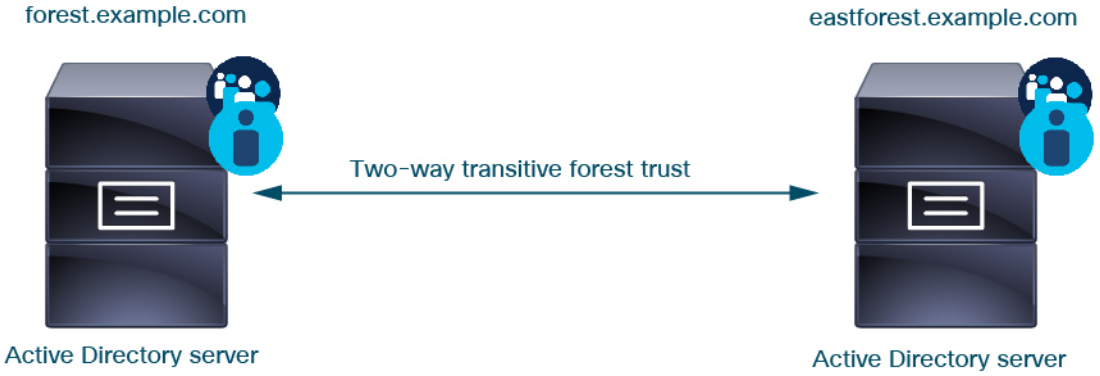
请参阅创建身份策略。

配置 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 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。

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 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 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 24 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 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 管理中心 的跨域信任：设置 ，第 23 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 3 页 。

如果使用 LDAP 对用户进行身份验证，则无法使用此程序。

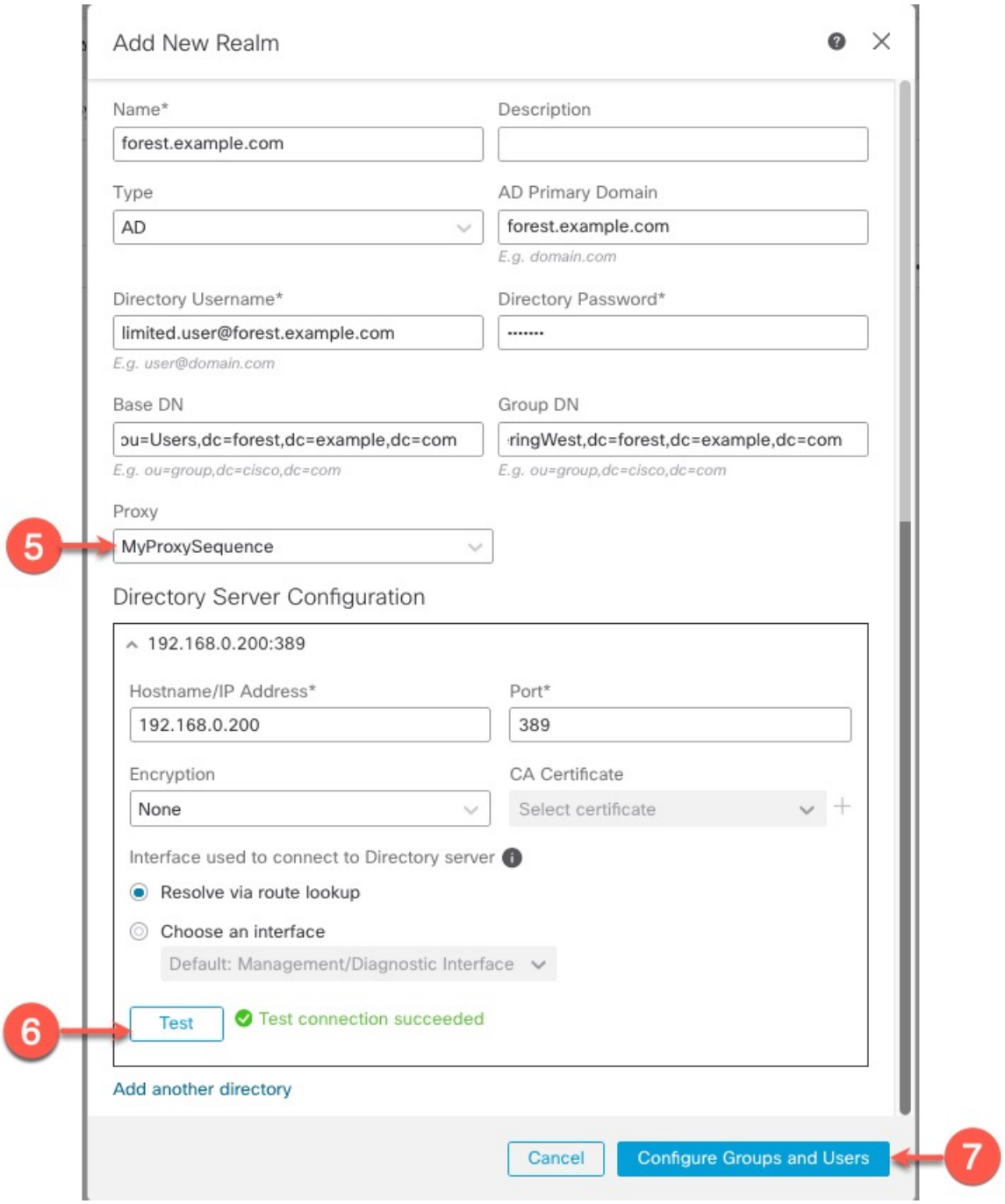
过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 点击**添加领域 (Add Realm)**。

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。

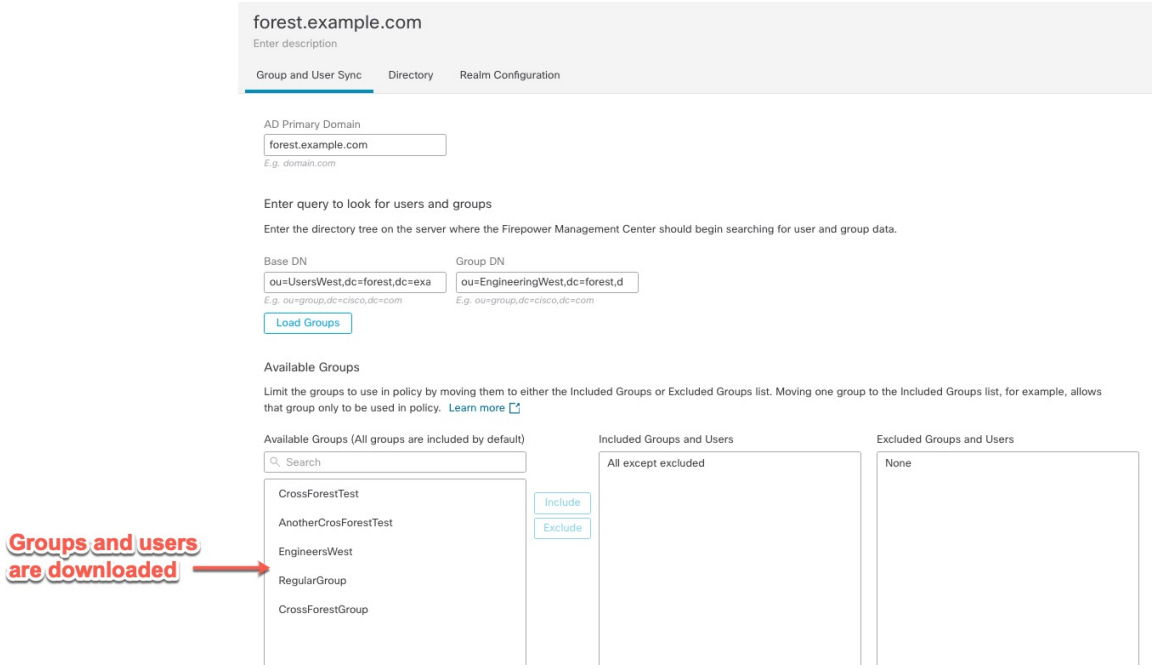
用于连接到目录服务器的接口 可以是可以连接到 Active Directory 服务器的任何接口。

步骤 5 **代理** 是可选的受管设备或代理序列，用于在 CDO 无法执行时与 ISE / ISE-PIC 通信。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 6 点击**测试 (Test)** 并确保测试成功后再继续。

步骤 7 点击 **配置组和用户**。

步骤 8 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**。

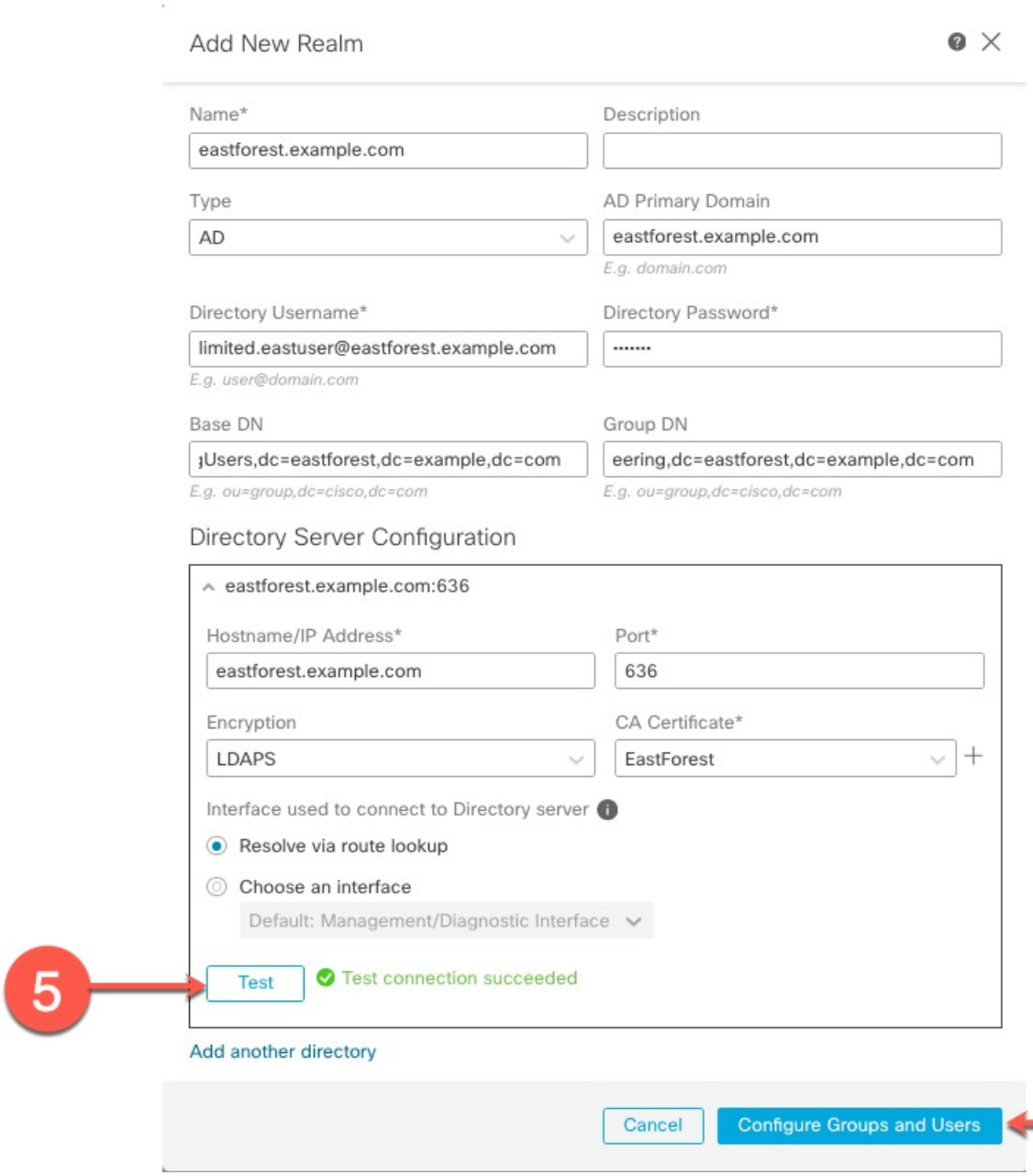
此页面上还有其他可选配置；有关它们的详细信息，请参阅 领域字段，第 12 页 和 领域目录和 同步 字段，第 16 页。

步骤 9 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 10 请点击 **集成** > **其他集成** > **领域**。

步骤 11 点击**添加领域 (Add Realm)**。

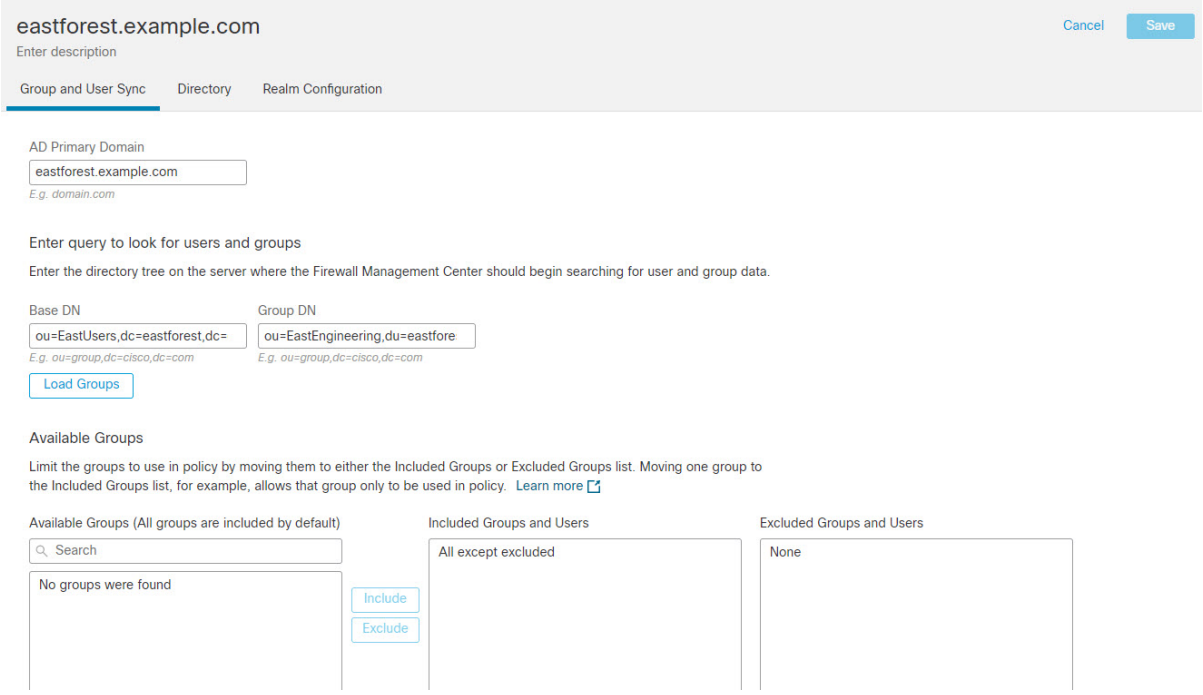
步骤 12 要配置 **eastforest.example.com**，请输入以下信息。



步骤 13 点击**测试 (Test)** 并确保测试成功后再继续。

步骤 14 点击 **配置组和用户**。

步骤 15 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 管理中心 步骤 2：同步用户和组，第 28 页

为跨域信任配置配置 管理中心 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 24 页中讨论的任务。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **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 12 页 和 领域目录和 同步 字段，第 16 页中所述。

如果您使用的是代理或代理序列，请确保所有受管设备都可以与 Active Directory 或 ISE / ISE-PIC 通信。如果多个受管设备可以与 ISE / ISE-PIC 通信，我们强烈建议您为领域设置代理序列，如 创建代理序列，第 8 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 管理中心 步骤 3：解决问题，第 29 页

为跨域信任配置 管理中心 步骤 3：解决问题

在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 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 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域** > **同步结果**。

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** 选项卡。

b) 点击  （立即下载），然后点击 **是**。

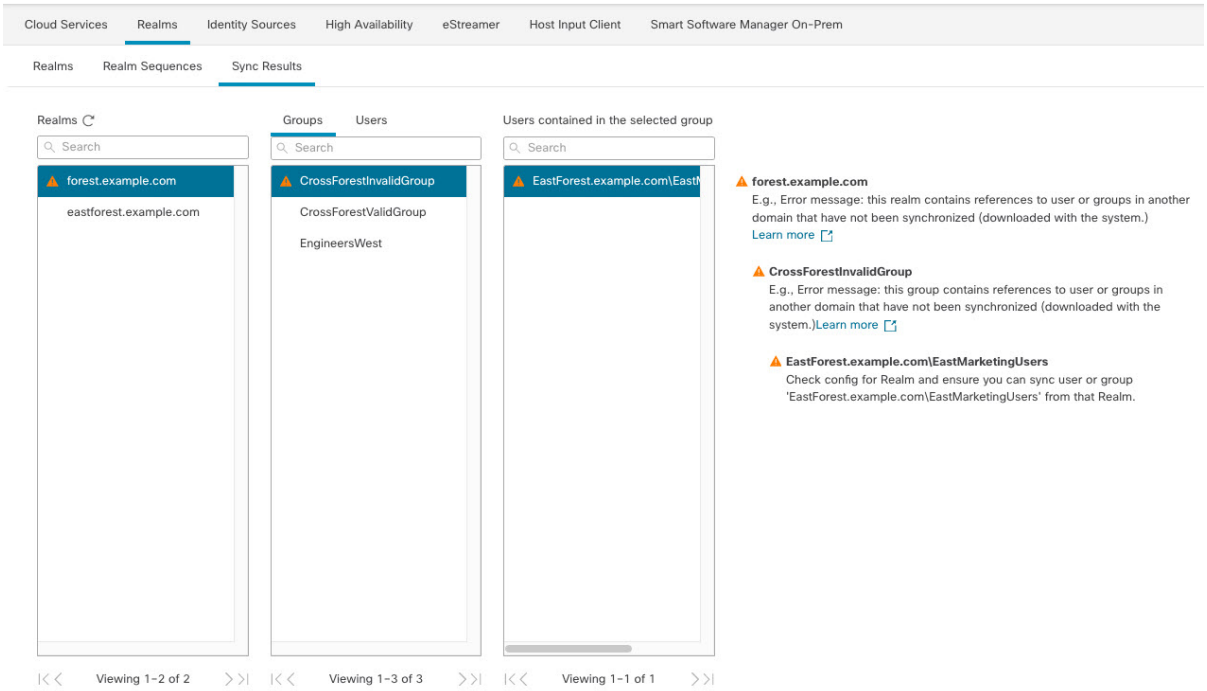
步骤 4 点击 **同步结果** 选项卡页面。

如果“领域”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 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 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。请注意以下提示：

- 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，请登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **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 Active Directory 领域和领域目录，第 10 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 31 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 登录管理中心。

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

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
- 远程接入 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

管理中心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 管理中心 。

  造成用户不匹配通常是因为该用户属于不予下载至 管理中心。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 管理中心未知的某个领域。

例如，如果您定义了一个与 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。 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 34 页。

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，管理中心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 管理中心 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 管理中心 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，系统可在非预期时间间隔时执行用户超时。

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。

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。
- 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：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 管理中心 。

  造成用户不匹配通常是因为该用户属于不予下载至 管理中心。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 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 31 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) 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 31 页。

g) 在页面底部，点击**保存策略并退出**。
h) 如在 《Cisco Secure Firewall Management Center 管理指南》中 运行状况策略 所述，对受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 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。
- 点击 **系统** > **运行状况** > **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。

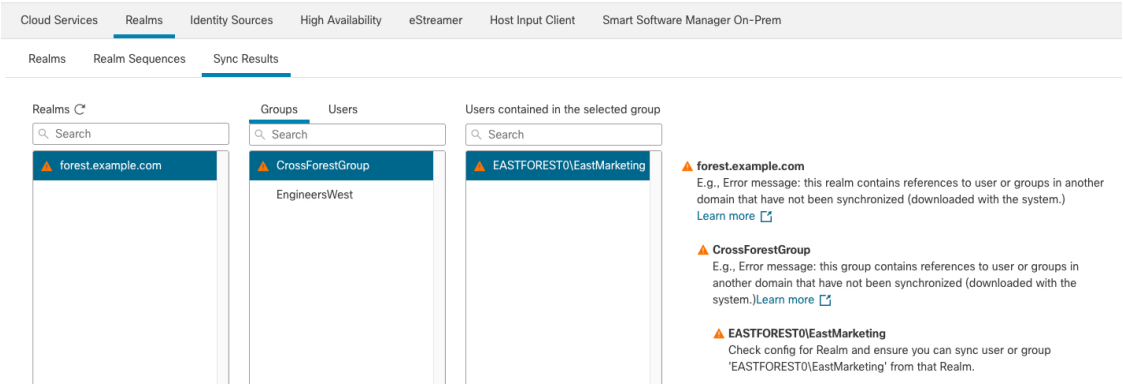
排除跨域信任故障

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。 **黄色三角形**（）显示来指示领域中的问题。 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** 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。 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。
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： • **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。 **解决方案：**如 创建 Active Directory 领域和领域目录，第 10 页中所述，为包含该组的林添加一个领域。 • **问题：**已将组下从载到 管理中心中排除。 **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。

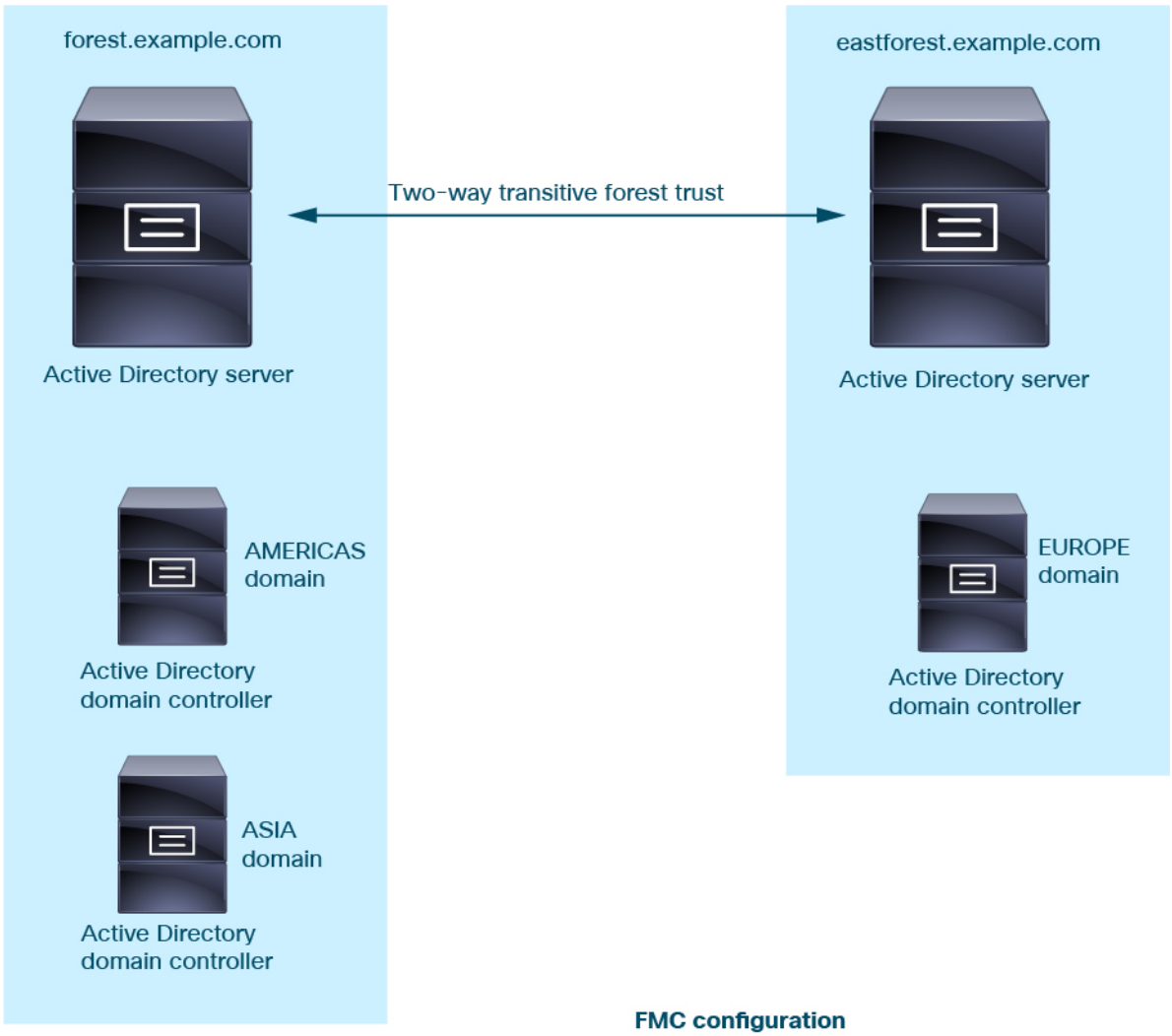
1. 如果尚未登录，请登录 管理中心。
2. 请点击 **集成** > **其他集成** > **领域**。
3. 请点击 **下载**（ ）。
4. 点击 **同步结果** 选项卡页面。
5. 如果“领域”列中的条目未显示指示器，则问题已解决。

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。


forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

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。