身份源：被动身份代理

以下主题讨论如何配置和使用被动身份代理。

- 被动身份代理身份源， 第 1 页
- 部署 被动身份代理， 第 3 页
- 如何创建 被动身份代理 身份源， 第 8 页
- 配置 被动身份代理， 第 10 页
- 监控 被动身份代理， 第 27 页
- 管理被动身份代理， 第 28 页
- 被动身份代理 故障排除， 第 30 页
- 被动身份代理 的安全要求， 第 31 页
- 被动身份代理的互联网接入要求， 第 32 页
- 被动身份代理 的历史记录， 第 33 页

被动身份代理身份源

被动身份代理 身份源将会话数据从 Microsoft Active Directory (AD) 发送到 Secure Firewall Management Center。您只需要 关于领域和领域序列中讨论的受支持的 Microsoft AD 设置即可。

被动身份代理 版本 1.0 仅发送 IPv4 用户会话，但版本 1.1 发送 IPv4 和 IPv6 用户会话。

注释 您无需配置Cisco Identity Services Engine (ISE) 即可使用此身份源。

被动身份代理 角色

被动身份代理 支持以下角色：

- 独立：不属于冗余对的 被动身份代理 。独立代理可以从多个 Active Directory 服务器和域控制器下载用户和组，前提是所有这些服务器和域控制器上都安装了该软件。
- 主：（冗余对中的主代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

处理与 Secure Firewall Management Center 的所有通信，除非它停止通信，在这种情况下，通信将由辅助代理处理。

- 辅助：（冗余对中的辅助或备份代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  监控主代理的运行状况，并在主代理停止与 Secure Firewall Management Center通信时进行接管。

被动身份代理 系统要求

被动身份代理 需要满足以下条件：

- 如果将 被动身份代理 安装在 Windows Active Directory 服务器上，则该服务器必须运行以下版本之一：
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022
- 如果将 被动身份代理 安装在连接到域的 Windows 客户端上，则客户端必须运行 Windows 11 或更高版本。
- 所有系统的系统时钟必须同步。强烈建议在所有这些服务器上使用相同的 NTP 服务器。这意味着：
  - Secure Firewall Management Center。

    有关详细信息，请参阅时间同步。
  - 所有 Windows Active Directory 服务器和域控制器。
  - 安装了 被动身份代理 的计算机。
- Secure Firewall Management Center 必须运行 7.6 或更高版本。
- 由 Secure Firewall Management Center 托管的任何 Cisco Secure Firewall Threat Defense 必须运行 7.1 或更高版本。
- 您必须在 Cisco Secure Firewall Threat Defense 设备上启用 Snort 3。

被动身份代理 限制

被动身份代理 以下限制：

- 最多同时有 10 个代理
- 一个 被动身份代理 身份源最多可以监控 50 个 AD 目录
- 最多 300,000 个并发用户会话
- 不支持 IPv6 地址 (被动身份代理 1.0)

- 不支持 IPv6 地址 (被动身份代理 1.1)

部署 被动身份代理

有关部署选项的信息，请参阅 部署 被动身份代理，第 3 页。

注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件，第 27 页

部署 被动身份代理

您可以在属于您想要用于用户感知和控制的 Microsoft Active Directory (AD) 域的任何计算机上安装 被动身份代理 软件。换句话说，您可以将其安装在以下任何位置：

- Microsoft Active Directory 服务器
- 域控制器
- 连接到网络的客户端既不是目录服务器，也不是域控制器

任何特定 被动身份代理 都可以监控一个或多个 Active Directory 域。

被动身份代理 必须使用 TLS/SSL 协议与 Secure Firewall Management Center] 通信的计算机。有关详细信息，请参阅被动身份代理的互联网接入要求，第 32 页。

代理类型

您可以在 Microsoft AD 目录服务器、域控制器或连接到域的任何客户端上配置以下类型的代理：

- 独立代理：一个代理，可以监控同一域中的一个或多个 Active Directory 域控制器。
- 可以监控同一域中的一个或多个 AD 域控制器的主代理和辅助代理：为了提供冗余，您可以在不同的计算机上安装主代理和辅助代理。主代理负责与 Secure Firewall Management Center 进行通信，但如果通信失败，则由辅助代理接管。

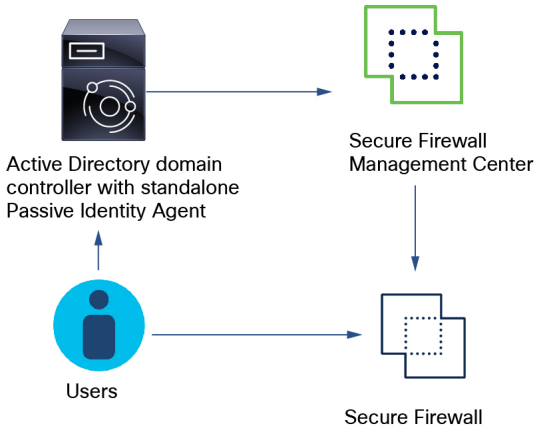
有关详细信息，请参阅以下主题之一：

相关主题

简单 被动身份代理 部署，第 4 页
单 被动身份代理 监控多个域控制器，第 4 页
多个 被动身份代理 监控多个域控制器，第 5 页
被动身份代理 主/辅助代理部署，第 7 页

简单 被动身份代理 部署

下图显示了最简单的 被动身份代理 部署。

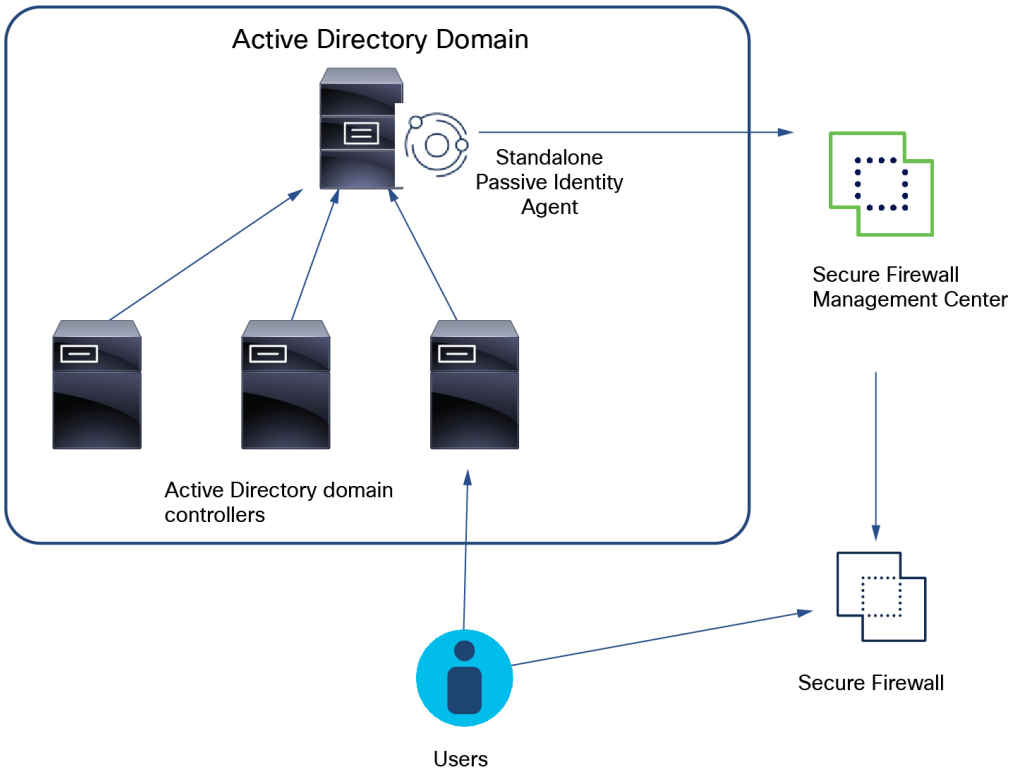


在前面的示例中，一个独立的 被动身份代理 安装在 AD 域控制器上。用户登录和注销 AD 域，代理会将用户名和 IP 地址信息发送到 Secure Firewall Management Center。当用户访问网络时，部署到 Cisco Secure Firewall Threat Defense 的访问控制和身份策略会确定是否允许访问以及如何访问。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

单 被动身份代理 监控多个域控制器

下图显示了监控多个 AD 域控制器的独立 被动身份代理。



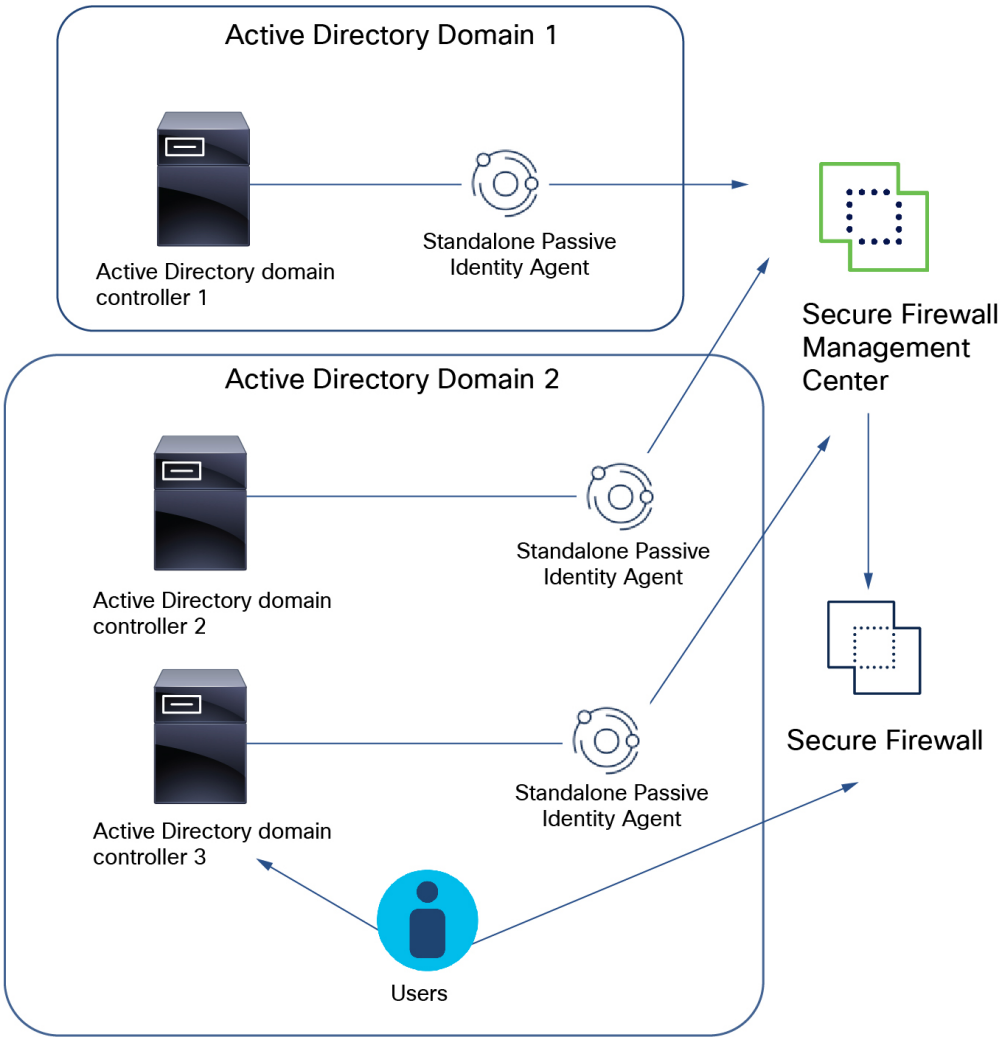
在上图中，独立 被动身份代理 安装在连接到 AD 域的客户端上（或域控制器本身）。登录到任何域控制器的用户和代理会将用户和 IP 地址信息发送到 Secure Firewall Management Center。当用户访问网络时，部署到 Cisco Secure Firewall Threat Defense 的访问控制和身份策略会确定是否允许访问以及如何访问。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

多个 被动身份代理 监控多个域控制器

下图显示了监控多个 AD 域控制器的独立集群：

- 在 AD 域 1 中，安装在与 AD 域控制器 1 连接的计算机上的独立 被动身份代理 会将用户和 IP 地址映射数据发送到 Secure Firewall Management Center。
- 在 AD 域 2 中，AD 域控制器 1 和 2 上安装的独立代理会将用户和 IP 地址映射数据发送到 Secure Firewall Management Center。



您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

上图显示了三个 被动身份代理，而每个均配置为独立端口。为此：

1. 创建两个 Microsoft AD 领域：每个 AD 域一个。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。

2. 对于 AD 域 2，创建两个目录，每个域控制器一个。

3. 在可以登录该域的客户端上安装 被动身份代理 软件。

   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件 ， 第 23 页。

4. 创建 被动身份代理 身份源。

   请参阅创建主身份源或辅助被动身份代理身份源 ， 第 14 页。

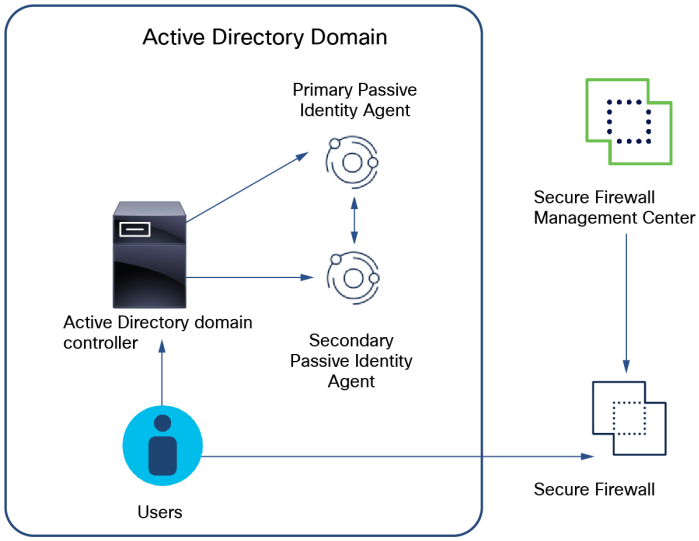
被动身份代理 主/辅助代理部署

要提供冗余并避免单点故障，您可以按照本主题中所示的任何方式配置主和辅助 被动身份代理。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

带主代理和辅助代理的单个 AD 域控制器

下图显示如何在一个 AD 域控制器上设置主和辅助 被动身份代理。如果主代理发生故障，则辅助代理将接管其任务。



要进行此项设置，请执行以下操作：

1. 创建一个 Microsoft AD 领域，其中包含一个用于域控制器的目录。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。

2. 在连接到域控制器的任意两台网络计算机上安装 被动身份代理 软件。

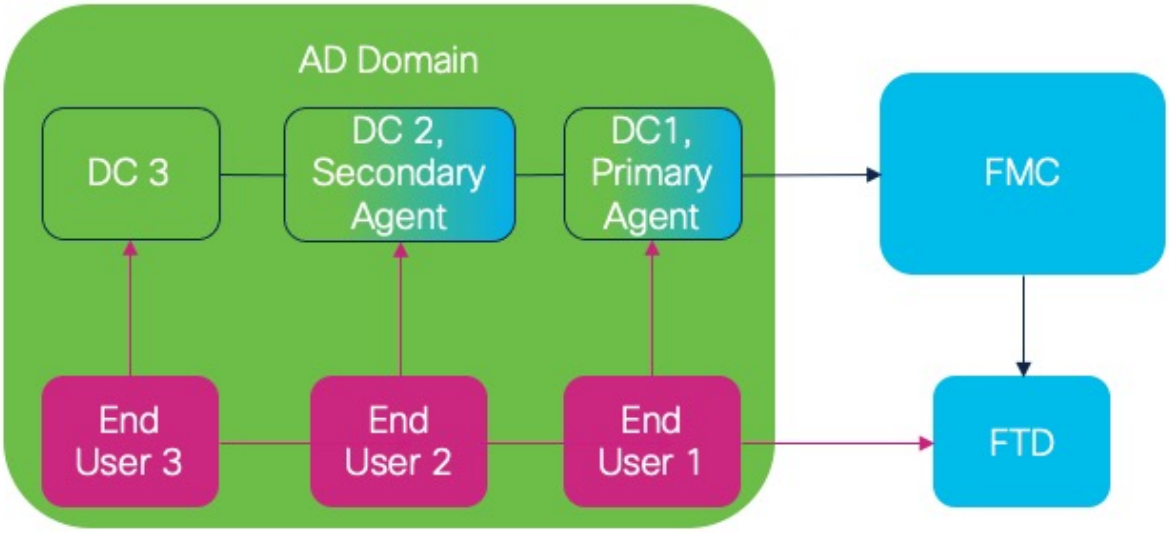
   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件 ， 第 23 页。

3. 创建身份源。

   请参阅创建主身份源或辅助被动身份代理身份源 ， 第 14 页。

多个 **AD** 域控制器、主和辅助代理



上图显示了如何配置主和辅助代理以监控三个 AD 域控制器。如果主代理发生故障，则辅助代理将接管其任务。

要进行此项设置，请执行以下操作：

1. 创建一个 Microsoft AD 领域，其中包含一个用于域控制器的目录。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。

2. 在连接到域控制器的任何计算机上安装 被动身份代理 软件。

   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件 ， 第 23 页。

3. 创建身份源。

   请参阅创建主身份源或辅助被动身份代理身份源 ， 第 14 页。

如何创建 被动身份代理 身份源

以下提供了在 Secure Firewall Management Center 中配置 被动身份代理 身份源以及将代理软件部署到您的 Microsoft Active Directory (AD) 服务器所需的高级任务。

过程

	命令或操作	目的
步骤 1	启用Dynamic Attributes Connector。	dynamic attributes connector 是使用 被动身份代理 的一项要求。 请参阅启用 dynamic attributes connector， 第 10 页。
步骤 2	为您的 Microsoft AD 域和域控制器创建一个领域。	领域是 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。 有关详细信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
步骤 3	创建 被动身份代理 身份源。	身份源允许 Secure Firewall Management Center 和 被动身份代理 相互通信。根据需要创建独立、主或辅助代理。 有关详细信息，请参阅： • 关于被动身份代理角色， 第 16 页 • 创建被动身份代理身份源， 第 11 页
步骤 4	在 Secure Firewall Management Center上创建 被动身份代理 用户。	我们为代理和管理器提供了一个足以相互沟通的角色。我们建议将该角色用于 被动身份代理 用户而不是其他角色。
步骤 5	安装 被动身份代理 软件。	代理的安装方式取决于您的部署。 您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。 有关详细信息，请参阅： • 部署 被动身份代理， 第 3 页 • 安装 被动身份代理 软件， 第 23 页

下一步做什么

创建 LDAP 领域或 Active Directory 领域和领域目录。

配置 被动身份代理

以下主题讨论如何配置 被动身份代理。

相关主题

创建 LDAP 领域或 Active Directory 领域和领域目录
创建被动身份代理身份源，第 11 页
安装 被动身份代理 软件，第 23 页
为被动身份代理创建Secure Firewall Management Center用户，第 17 页

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

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

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器。

相关主题

关于 动态防火墙
如何配置 动态防火墙

创建 Microsoft Active Directory 领域

被动身份代理 要求您创建 Microsoft Active Directory (AD) 领域和 Secure Firewall Management Center 中的目录，如创建 LDAP 领域或 Active Directory 领域和领域目录中所述。

创建被动身份代理身份源

此任务讨论如何创建一个会将用户会话活动发送到 Secure Firewall Management Center 的 被动身份代理。

开始之前

完成以下操作：

- 查看关于被动身份代理角色，第 16 页中讨论的 被动身份代理 角色。
- 如创建 LDAP 领域或 Active Directory 领域和领域目录中所述，创建 Microsoft AD 领域。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **身份源**。

步骤 3 点击**被动身份代理**。

步骤 4 如果尚未启用 dynamic attributes connector，系统会提示您启用。

有关启用 dynamic attributes connector 的详细信息，请参阅启用 dynamic attributes connector，第 10 页。

步骤 5 点击**创建代理**。

步骤 6 在“配置代理”对话框中，输入以下信息：

项目	说明
名称	输入可标识 被动身份代理 的唯一名称。
说明	输入可选的说明。
角色	点击以下选项之一： • **主 (Primary)**：负责与 Secure Firewall Management Center 通信的代理。 如果您选择**独立**则不可用。 • **辅助 (Secondary)**：如果主代理与 Secure Firewall Management Center 失去联系，则其会成为主代理。 如果您选择**独立**则不可用。 • **独立**：如果只有一个 被动身份代理。 有关角色的详细信息，请参阅关于被动身份代理角色，第 16 页。

步骤 7 继续：

- 创建独立被动身份代理身份源， 第 12 页
- 创建主身份源或辅助被动身份代理身份源， 第 14 页

创建独立被动身份代理身份源

此任务讨论如何配置独立 被动身份代理。

开始之前

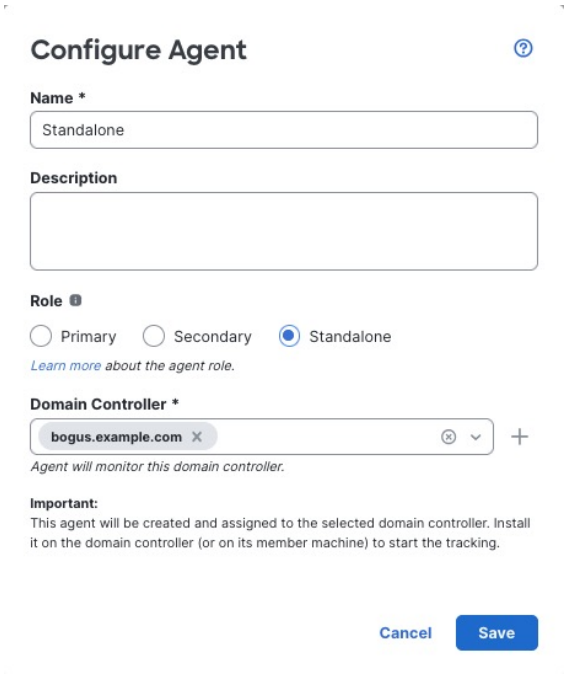
完成 创建被动身份代理身份源， 第 11 页中讨论的任务。

过程

步骤 1 在“配置代理”对话框中，输入以下信息：

项目	说明
角色	点击**独立**。
域控制器	从列表中选择每个域控制器旁边的复选框，该域控制器有一个您希望用于身份管理和用户控制的 被动身份代理。 （可选。）点击 **添加** (+) 添加新的。

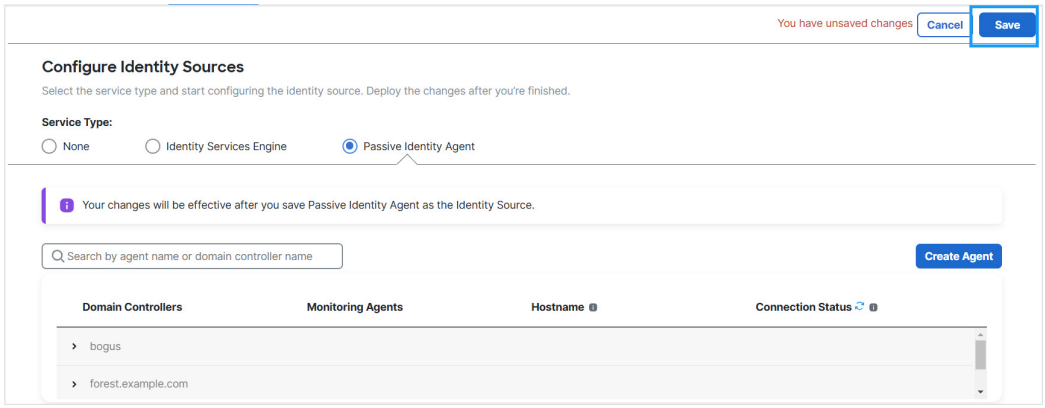
下图显示了独立 被动身份代理 身份源的示例。



步骤 2 在“配置代理”对话框中，点击**保存**。

步骤 3 在页面右上角，点击**保存**。

下图显示了一个示例。



注释
在您创建用户并安装软件之前，被动身份代理 不会处于活动状态。

下一步做什么

- 请参阅为被动身份代理创建Secure Firewall Management Center用户，第 17 页
- 请参阅关于被动身份代理安装，第 18 页

创建主身份源或辅助被动身份代理身份源

以下任务会从 创建被动身份代理身份源，第 11 页继续。

开始之前

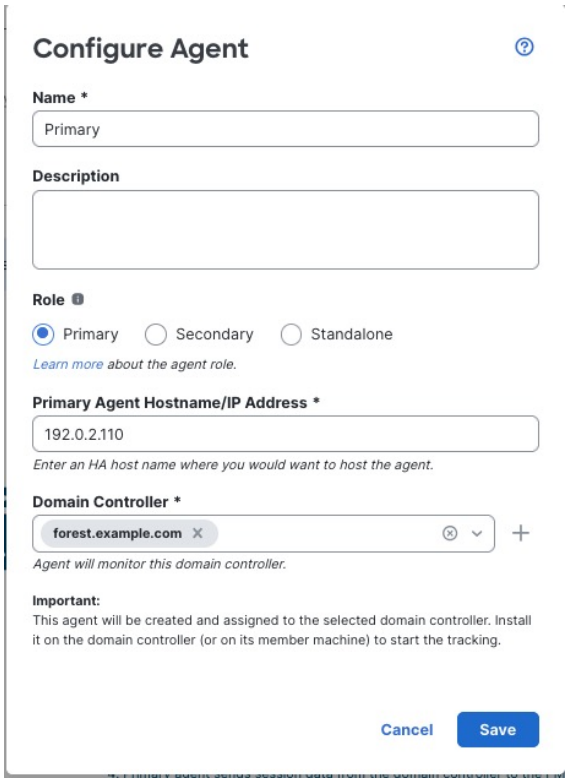
完成 创建被动身份代理身份源，第 11 页中讨论的任务。

过程

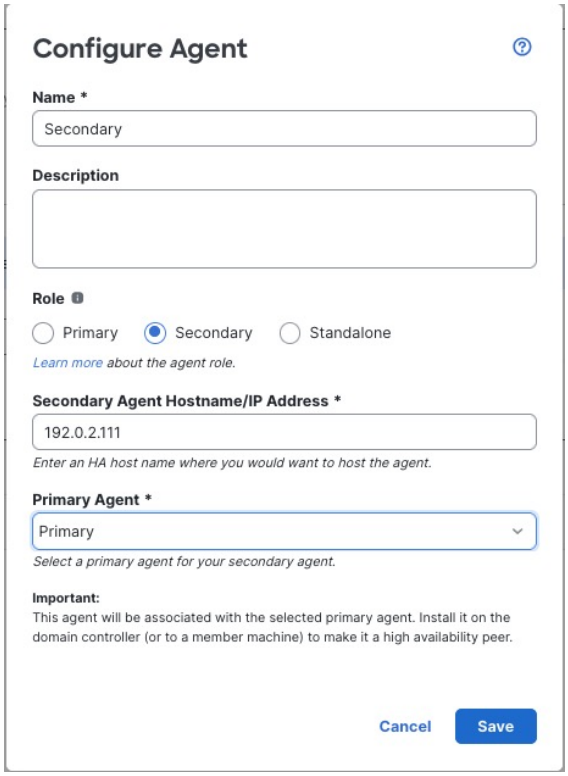
步骤 1 在“配置代理”对话框中，输入以下信息：

项目	说明
角色	点击以下选项之一： • **主 (Primary)**：负责与 Secure Firewall Management Center 通信的代理。 • **辅助 (Secondary)**：如果主代理与 Secure Firewall Management Center 失去联系，则其会成为主代理。 有关角色的详细信息，请参阅关于被动身份代理角色，第 16 页。
主代理主机名/IP 地址	（仅限主代理。）输入安装了主被动身份代理的服务器的完全限定域名或 IP 地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
辅助代理主机名/IP 地址	（仅限辅助代理。）输入安装了辅助 被动身份代理 的服务器的完全限定主机名或 IP 地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
主代理	（仅限辅助代理。）在列表中点击主设备的名称 被动身份代理。
域控制器	（仅限主代理。）从列表中选择每个域控制器旁边的复选框，该域控制器有一个您希望用于身份管理和用户控制的 被动身份代理。

下图显示了主代理的示例：



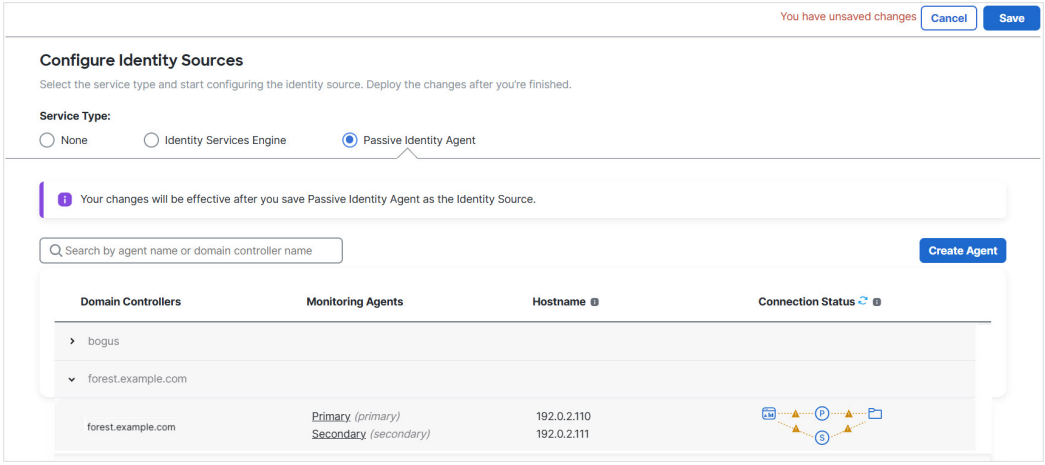
下图显示了辅助代理的示例：



步骤 2 在“配置代理”对话框中，点击**保存**。

步骤 3 在页面右上角，点击**保存**。

下图显示了一个示例。



注释
在您创建用户并安装软件之前，被动身份代理 不会处于活动状态。

下一步做什么

- 请参阅为被动身份代理创建Secure Firewall Management Center用户，第 17 页
- 请参阅关于被动身份代理安装，第 18 页

关于被动身份代理角色

被动身份代理 具有以下角色：

- 独立：不属于冗余对的 被动身份代理 。独立代理可以从多个 Active Directory 服务器和域控制器下载用户和组，前提是所有这些服务器和域控制器上都安装了该软件。
- 主：（冗余对中的主代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  处理与 Secure Firewall Management Center 的所有通信，除非它停止通信，在这种情况下，通信将由辅助代理处理。
- 辅助：（冗余对中的辅助或备份代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  监控主代理的运行状况，并在主代理停止与 Secure Firewall Management Center通信时进行接管。

可以监控属于同一域的多个 AD 域控制器。

为被动身份代理创建Secure Firewall Management Center用户

此任务讨论如何创建具有足够权限的 Secure Firewall Management Center 用户以便与 被动身份代理通信。此用户具有执行其他任务的有限权限；预期用户只能启用与 被动身份代理 通信。

注释 请仅对 被动身份代理 用户使用 **Passive Identity User** 角色。特别是， 请勿对 被动身份代理 用户 使用 **Administrator** 角色，因为当 被动身份代理 与 Secure Firewall Management Center通信时，**Administrator** 将被定期注销。

开始之前

完成 创建被动身份代理身份源， 第 11 页中讨论的任务。

注释 您不能对 被动身份代理 用户使用外部身份验证。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。

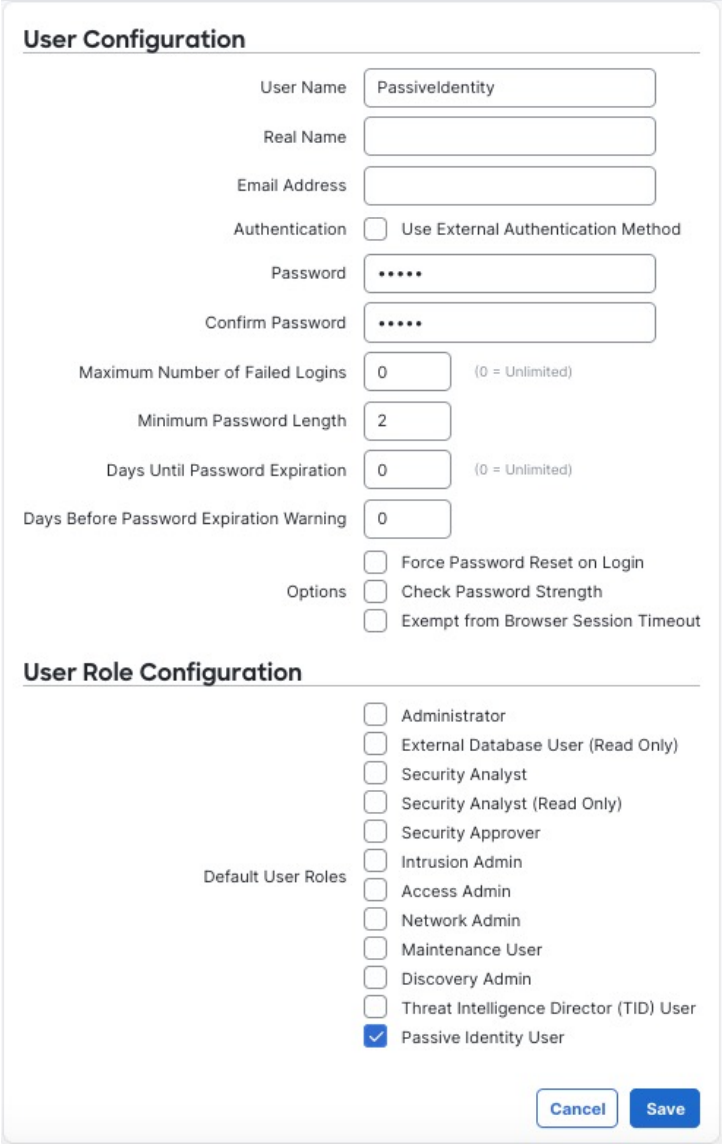
步骤 2 请点击 **管理** > **用户**、 > **用户账户**、 。

步骤 3 点击**创建用户**。

步骤 4 按照《*Cisco Secure Firewall Management Center* 管理指南》中的添加或编辑内部用户所述创建用户。

步骤 5 选择**被动身份用户**角色。

下图显示了一个示例。



注释
不要为 被动身份代理 用户选择 **Passive Identity User** 之外的角色，否则代理将无法正常工作。

步骤 6 点击**保存**。

下一步做什么

关于被动身份代理安装，第 18 页。

关于被动身份代理安装

以下主题讨论安装 被动身份代理 所需的前提条件和任务。

注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件 ，第 27 页

安装 被动身份代理 的先决条件

在安装 被动身份代理 软件之前，您必须完成以下所有任务。

被动身份代理 系统要求

被动身份代理 系统要求

被动身份代理 需要满足以下条件：

- 如果将 被动身份代理 安装在 Windows Active Directory 服务器上，则该服务器必须运行以下版本之一：
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022
- 如果将 被动身份代理 安装在连接到域的 Windows 客户端上，则客户端必须运行 Windows 11 或更高版本。
- 所有系统的系统时钟必须同步。强烈建议在所有这些服务器上使用相同的 NTP 服务器。这意味着：
  - Secure Firewall Management Center。

    有关详细信息，请参阅时间同步。
  - 所有 Windows Active Directory 服务器和域控制器。
  - 安装了 被动身份代理 的计算机。
- Secure Firewall Management Center 必须运行 7.6 或更高版本。
- 由 Secure Firewall Management Center 托管的任何 Cisco Secure Firewall Threat Defense 必须运行 7.1 或更高版本。
- 您必须在 Cisco Secure Firewall Threat Defense 设备上启用 Snort 3。

启用 Windows 事件查看器以记录 Kerberos 身份验证尝试

以下任务显示如何配置 Windows 组策略对象 (GPO) 安全设置，以便让 记录成功和失败的 Kerberos 身份验证尝试。 被动身份代理 会从事件查看器中读取用户会话，因此要 被动身份代理 正常运行，需要此设置。

有关详细信息，请参阅 learn.microsoft.com 上的审核策略建议。

过程

步骤 1 以管理员身份登录 Active Directory 服务器。

步骤 2 以管理员身份打开 DOS 命令提示符。

步骤 3 输入 `gpmc.msc` 以启动组策略管理编辑器。

步骤 4 如有必要，创建新 GPO；如已存在，则进行编辑。

有关创建 GPO 的详细信息，请参阅 learn.microsoft.com 上的创建组策略对象等资源。

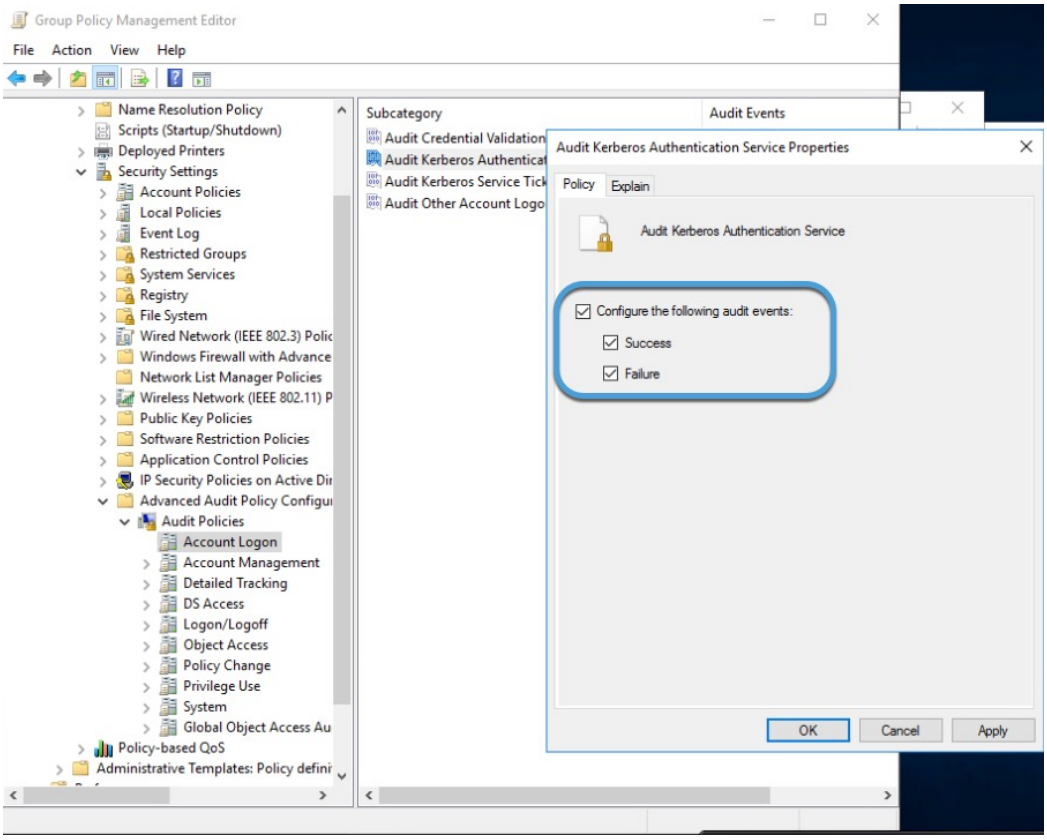
步骤 5 在 GPO 中，展开**计算机配置 (Computer Configuration)** > **策略 (Policies)** > **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)** > **高级策略配置 (Advanced Policy Configuration)** > **审核策略 (Audit Policies)**。

步骤 6 点击**帐户登录 (Account Logon)**。

步骤 7 在右侧窗格中，双击**审核 Kerberos 验证服务 (Audit Kerberos Authentication Service)**。

步骤 8 在显示的对话框中，选中让系统能够记录成功和失败的所有复选框。

下图显示了一个示例。



步骤 9 按照屏幕上的提示保存更改。

步骤 10 （可选。）要立即更新 GPO，请在 DOS 命令提示符窗口中输入 **gpupdate /force**。

下一步做什么

请参阅将 Active Directory 用户添加到组 ，第 21 页。

将 Active Directory 用户添加到组

使用此程序为 Active Directory 和 被动身份代理 服务用户授予足够的 Active Directory 权限。

要正常工作， 被动身份代理 必须能够连接域并读取 Windows 事件日志。本主题讨论如何对以下项授予相应权限：

- 被动身份代理 服务用户的设备。
- Active Directory 用户（即 Secure Firewall Management Center上 Active Directory 领域的 “**目录用户名**”用户）。

Before you begin

您必须是 Microsoft 服务器管理员，熟悉如何将用户添加到组以及如何将 Windows 服务设置为以特定用户身份运行。

过程

步骤 1 以管理员身份登录运行 被动身份代理 的系统。

您可以登录以下任一设备：

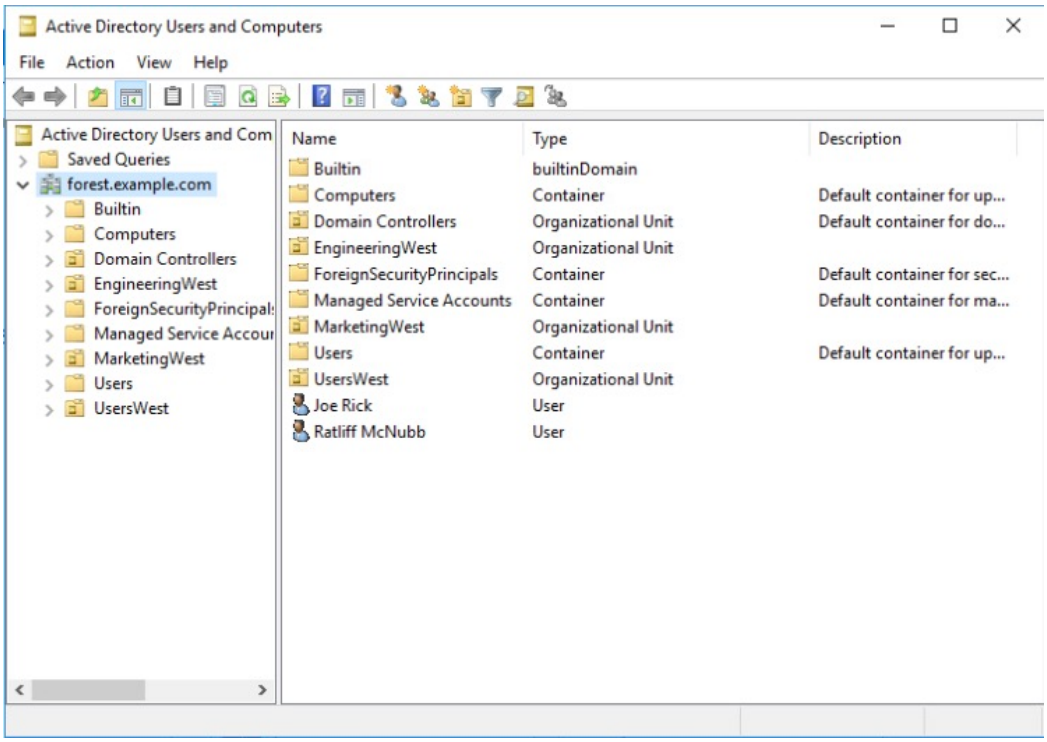
- 域控制器
- Active Directory 服务器。

步骤 2 启动服务器管理器工具。

步骤 3 点击**Active Directory** > **用户和计算机**。

步骤 4 在“Active Directory 用户和计算机”下，展开定义目录用户的林。

下图显示了一个示例。

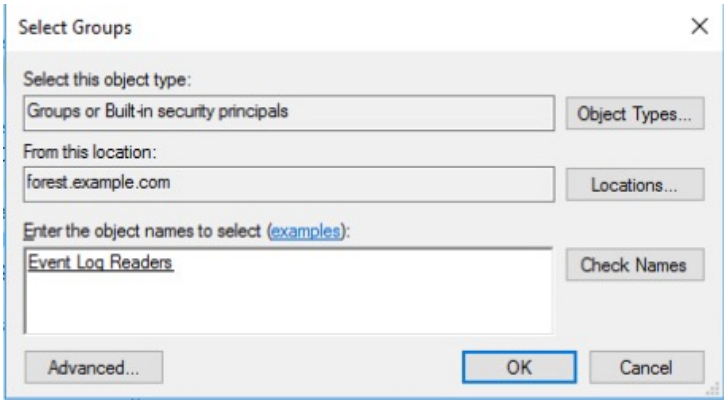


步骤 5 展开组织单位或组以显示目录用户。（点击 **新建用户 (New > User)** 可创建新用户。）

步骤 6 右键点击目录用户，然后点击 **添加到组 (Add to a group)**。

步骤 7 在选择组 (Select Groups) 对话框中，输入 **事件日志读取器 (Event Log Readers)**，然后点击 **检查名称 (Check Names)**。

下图显示了一个示例。



步骤 8 重复前述任务，将该用户添加到域用户组。

步骤 9 在“添加组”对话框中，点击 **确定**。

目录用户现在拥有适当的权限，并且 被动身份代理 服务会以该用户的身份运行。

下一步做什么

请参阅安装 被动身份代理 软件 ， 第 23 页。

安装 被动身份代理 软件

此任务讨论如何安装 被动身份代理 软件。对于简单安装，您可以将其安装在 Microsoft Active Directory (AD) 域控制器上；有关其他选项，请参阅部署 被动身份代理 ， 第 3 页。

注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件 ， 第 27 页

开始之前

完成以上全部任务…

- 启用 Windows 事件查看器以记录 Kerberos 身份验证尝试 ， 第 19 页
- 将 Active Directory 用户添加到组 ， 第 21 页
- 将登录添加到 被动身份代理 服务 ， 第 25 页

过程

步骤 1 从 software.cisco.com 下载 被动身份代理。

步骤 2 以管理员组成员身份登录到要安装 被动身份代理 的计算机。

步骤 3 双击 **CiscoPassiveIdentityAgentInstaller-1.1.1.msi**。

步骤 4 点击**下一步 (Next)**。

步骤 5 选择要在其中安装 被动身份代理 的文件夹，然后点击**下一步 (Next)**。

默认安装文件夹为 **Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**。

步骤 6 点击**下一步 (Next)**。

步骤 7 点击 **Install**。

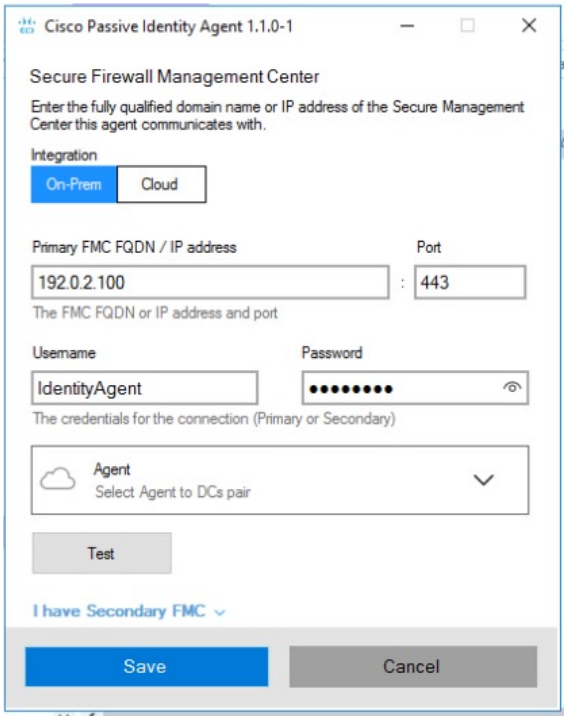
步骤 8 完成安装后，点击**完成 (Finish)** ，然后可以选中此复选框以启动 被动身份代理。

步骤 9 当 被动身份代理 启动时，如果您将代理与本地 Secure Firewall Management Center（物理或虚拟）配合使用，则点击**本地 (On-Prem)** 选项卡；如果您将代理与 云交付的防火墙管理中心 配合使用，则点击**云 (Cloud)** 选项卡。

步骤 10 在“思科被动代理”对话框中，输入以下信息：

项目	说明
FMC FQDN / IP 地址	输入您在上面创建 被动身份代理 身份源的 Secure Firewall Management Center 的地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
端口	输入 Secure Firewall Management Center 侦听端口（默认情况下为 443）。
用户名	输入您在 为被动身份代理创建Secure Firewall Management Center 用户，第 17 页 中创建的用户的用户名。
密码	输入用户的密码。
代理	点击列表找到您先前在 Secure Firewall Management Center 上创建的 被动身份代理 的域控制器。

下图显示了一个示例。

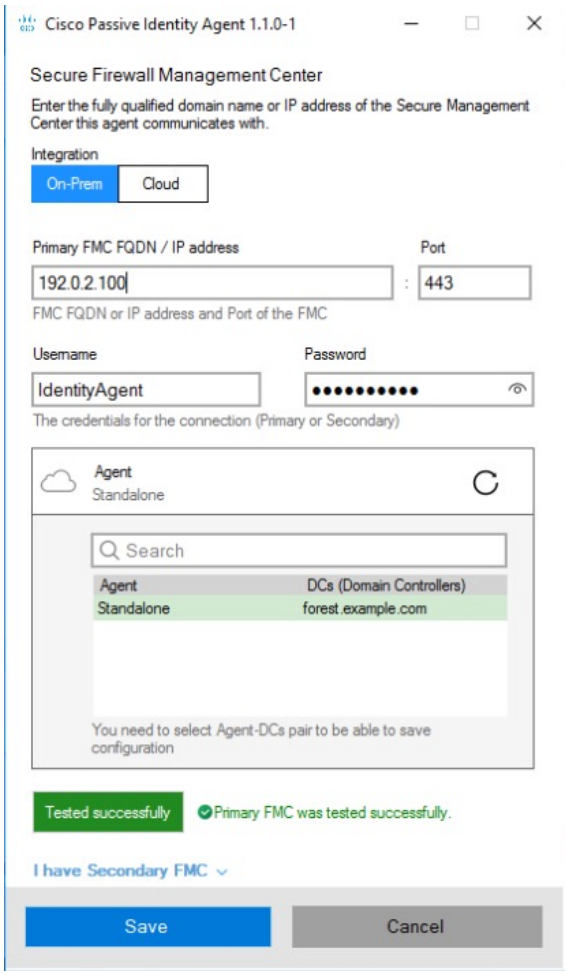


步骤 11 点击**代理**列表。

步骤 12 在列表中点击要监控的域控制器名称。

步骤 13 点击**测试**。

下图显示了一个示例。



步骤 14 如果您有高可用性对，请点击**我有辅助 FMC (I have Secondary FMC)**，然后输入辅助的 IP 地址或完全限定主机名及其侦听端口。

步骤 15 仅在测试成功时点击**保存**。

下一步做什么

请参阅将登录添加到 被动身份代理 服务，第 25 页。

将登录添加到 被动身份代理 服务

使用此程序启用 被动身份代理 服务以 Active Directory 用户身份运行。（即 Secure Firewall Management Center上 Active Directory 领域的 “**目录用户名**” 用户）。

此任务是可选的，但建议执行此任务，以便 被动身份代理 服务使用将登录信息发送到 Secure Firewall Management Center所需的最小权限运行

Before you begin

完成 将 Active Directory 用户添加到组，第 21 页中讨论的任务。

您必须是 Microsoft 服务器管理员，熟悉如何将用户添加到组以及如何将 Windows 服务设置为以特定用户身份运行。

过程

步骤 1 以管理员身份登录运行 被动身份代理 的系统。

您可以登录以下任一设备：

- 域控制器
- Active Directory 服务器。

步骤 2 在 Windows 搜索栏中，输入 **服务**。

步骤 3 在服务 (Services) 窗口中，右键点击 **Cisco 被动身份代理 (Cisco Passive Identity Agent)**。

步骤 4 点击**属性 (Properties)**。

步骤 5 在“属性”(Properties) 对话框中，点击 **登录 (Log On)** 选项卡。

步骤 6 点击 **此账户**。

步骤 7 点击 **浏览 (Browse)** 并按照屏幕上的提示选择目录用户。

步骤 8 在提供的字段中输入用户名和密码。

步骤 9 点击**应用 (Apply)**。

下一步做什么

- 使用创建身份策略中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到托管设备，如部署配置更改中所述。
- 监控用户活动，如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程所述。

卸载被动身份代理软件

此任务讨论如何从 Microsoft AD 服务器卸载 被动身份代理 软件。

过程

步骤 1 以管理员身份登录安装了 被动身份代理 的计算机。

步骤 2 搜索“添加或删除程序”。

步骤 3 点击**思科被动身份代理 (Cisco Passive Identity Agent)**。

步骤 4 点击**卸载 (Uninstall)**。

步骤 5 您需要确认卸载。

升级被动身份代理软件

要升级到较新版本的 被动身份代理，您必须卸载较早的版本并安装较新的版本。

请参阅以下信息：

- 卸载被动身份代理软件，第 26 页
- 关于被动身份代理安装，第 18 页

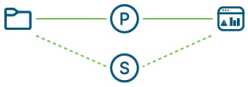
监控 被动身份代理

被动身份代理 指示如果其配置为主要-辅助代理，它是否可以与 Secure Firewall Management Center 和其他代理通信。您可以在 **集成** > **身份** > **身份源** 中查看状态。

部署

独立的 被动身份代理 表示如下。

主-辅助对表示如下。



下表解释了指示灯的含义。

对象	含义
	Secure Firewall Management Center
	独立 被动身份代理
	Active Directory 域控制器
	主代理
	辅助代理

状态指示灯和颜色

被动身份代理 使用线条（指明与 Secure Firewall Management Center 的通信是主用还是备用状态）和颜色（指示通信是否成功）指示状态。

下表显示了各行和颜色的含义：

对象	含义
实线	负责与 Secure Firewall Management Center 通信的代理。
虚线	仅限主/辅助配置。充当备份代理的代理。如果活动（实线）代理之间发生通信故障，此代理将与 Secure Firewall Management Center 之间的通信。
蓝色	代理通信正常。
琥珀色 	代理从未成功与 Secure Firewall Management Center 通信。新创建的代理线路显示为琥珀色，并在配置完成之前保持该状态。
红色 	通信失败。要解决此问题，请执行以下操作： • 检查以确保代理和 Secure Firewall Management Center 之间建立网络连接。 • 确保您已完成系统（Microsoft AD 服务器、域控制器和 Secure Firewall Management Center）的配置。 有关详细信息，请参阅如何创建 被动身份代理 身份源，第 8 页。

管理被动身份代理

以下主题讨论如何编辑或删除您先前在 Secure Firewall Management Center 上配置的 被动身份代理。

相关主题

编辑 被动身份代理，第 29 页
删除独立 被动身份代理，第 29 页
删除主和辅助 被动身份代理，第 29 页
卸载被动身份代理软件，第 26 页

编辑 被动身份代理

此任务讨论如何编辑您之前在 Secure Firewall Management Center 中配置的 被动身份代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。
步骤 4 点击代理旁边的 **编辑** (✎) 进行编辑。
步骤 5 进行所需的更改。
步骤 6 点击**保存**。

删除独立 被动身份代理

此任务讨论如何删除独立 被动身份代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。
步骤 4 点击要删除的代理旁边的 **编辑** (✎)。
步骤 5 点击**删除 (Delete)**。
步骤 6 您需要确认操作。

删除主和辅助 被动身份代理

此任务讨论如何删除主和辅助 被动身份代理。您必须先删除辅助代理，然后才能删除主代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。

步骤 4 点击要删除的辅助代理旁边的 **编辑** (✎)。

步骤 5 点击**删除 (Delete)**。

步骤 6 您需要确认操作。

步骤 7 如果要删除主代理，请先删除所有辅助代理。

被动身份代理 故障排除

本主题讨论如何对 Windows AD 域控制器或目录服务器上的 被动身份代理 软件进行故障排除。

（可选。）设置日志级别

默认情况下，被动身份代理 会在 INFO 级别进行日志记录。（可选）要更改日志级别，请在文本编辑器中打开 **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**，保存文件，然后重新启动思科被动身份代理服务。

请勿重命名日志记录服务

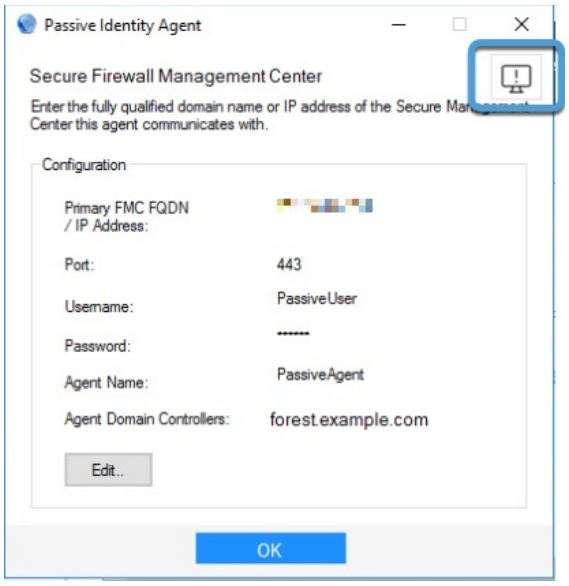
请勿重命名 **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**；否则，被动身份代理 将停止生成日志文件。请勿删除或更改 **.exe.config** 文件扩展名。

生成故障排除文件

要生成包含故障排除文件的 .zip 文件，请执行以下操作：

1. 登录 Microsoft Active Directory 域控制器。
2. 启动 被动身份代理 软件。
3. 点击窗口右上角的“故障排除”(Troubleshooting) 按钮。

   下图显示了一个示例。



屏幕上将显示一条确认消息。

您的故障排除日志将保存到系统的 Downloads 文件夹；文件名以 **TroubleshootLogs** 开头。

手动查看日志文件

被动身份代理 日志文件以纯文本格式存储在代理的安装目录中：**C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**。

使用记事本或其他文本编辑器查看这些文件。日志文件大小在达到 10 MB 后轮换。

使用 Microsoft Active Directory 事件查看器

如果在 Secure Firewall Management Center 中看不到用户会话，您可以在 Microsoft Active Directory 服务器的事件查看器中查找以下 Kerberos 相关事件：

- 4770
- 4768

有关审核策略的一般信息，请参阅 learn.microsoft.com 上的审核策略建议。

有关 Windows 组策略对象设置的详细信息，请参阅 learn.microsoft.com 上的组策略对象。

被动身份代理 的安全要求

为了保护，应将 被动身份代理 安装在受保护的内部网络中。虽然被动身份代理被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到攻击。

如果 被动身份代理 和 Secure Firewall Management Center 位于同一个网络，您可以将 Secure Firewall Management Center 连接到与 被动身份代理 相同的受保护内部网络。

无论如何部署设备，内部系统通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

被动身份代理的互联网接入要求

默认情况下，被动身份代理 会被配置为使用端口 443/tcp (HTTPS) 上的 HTTPS 通过互联网与 Firepower 系统通信。如果您不希望 被动身份代理 直接访问互联网，则可以配置代理服务器。

以下信息告知您 被动身份代理 用于相互通信、与 Secure Firewall Management Center 以及与 Microsoft Active Directory 通信的端口。

表 *1:* 被动身份代理 端口要求

端口	原因
443	与 Secure Firewall Management Center 通信。
135	使用 MSRPC 协议与 Microsoft Active Directory 通信。
9095	使用 UDP 协议相互通信。

被动身份代理 的历史记录

表 *2:* 被动身份代理 的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
被动身份代理	7.6	7.1	引入了此功能。 被动身份代理 版本 1.1 与 7.6.0 及更高版本兼容，并添加了以下内容： • 您可以使用 FQDN、IPv4 或 IPv6 从 被动身份代理 连接到 Secure Firewall Management Center 或 Security Cloud Control。 • 从 Microsoft Active Directory (AD) 向防火墙管理中心发送 IPv4 和 IPv6 用户会话。 • 您可以压缩故障排除日志。 • 在启动 被动身份代理 软件时，系统将显示前提条件列表。 被动身份代理 身份源将会话数据从 Microsoft Active Directory (AD) 发送到 防火墙管理中心。以下设备支持被动身份代理软件： • Microsoft AD 服务器（Windows Server 2008 或更高版本） • Microsoft AD 域控制器（Windows Server 2008 或更高版本） • 连接到要监控的域的任何客户端（Windows 8 或更高版本）

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。

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。

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。