Active Directory 作为探测器和提供程序

Active Directory (AD) 是一种高度安全且精确的源，可以从中接收用户身份信息，包括用户名、IP 地址和域名。

通过配置 Active Directory 探测器，您还可以快速配置并启用以下其他探测器（它们也使用 Active Directory 作为源）：

- Active Directory 代理

注释 仅在 Windows Server 2008 及更高版本上支持 Active Directory 代理。

- SPAN
- 终端探测器

此外，配置 Active Directory 探测器，以便在收集用户信息时使用 AD 用户组。您可以对 AD、代理、SPAN 和系统日志探测使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 6 页。

- 使用 Active Directory，第 1 页
- Active Directory 设置，第 10 页

使用 Active Directory

在为 被动身份服务 配置 Active Directory 探测器之前，请确保：

- Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。
- 用于加入操作的 Microsoft Active Directory 帐户有效，且未配置为下次登录时修改密码。
- 确保您已正确配置 DNS 服务器，包括从 ISE-PIC 配置客户端机器的反向查找。有关详细信息，请参阅DNS 服务器。

- 同步 NTP 服务器的时钟设置。有关详细信息，请参阅指定系统时间和网络时间协议服务器设置。

注释 如果您在思科 ISE-PIC 连接到 Active Directory 时发现操作问题，请查看**报告 (Reports)** 下的 AD 连接器操作报告。有关详细信息，请参阅可用报告。

PassiveID 设置入门

ISE-PIC 提供向导，从中可以轻松快速地将 Active Directory 配置为第一个用户身份提供程序，以便从 Active Directory 接收用户身份。通过为 ISE-PIC 配置 Active Directory，还可以简化稍后配置其他提供程序类型的过程。一旦配置了 Active Directory，就必须配置用户（例如思科 Firepower 管理中心 (FMC) 或 Stealthwatch），以便定义将要接收用户数据的客户端。

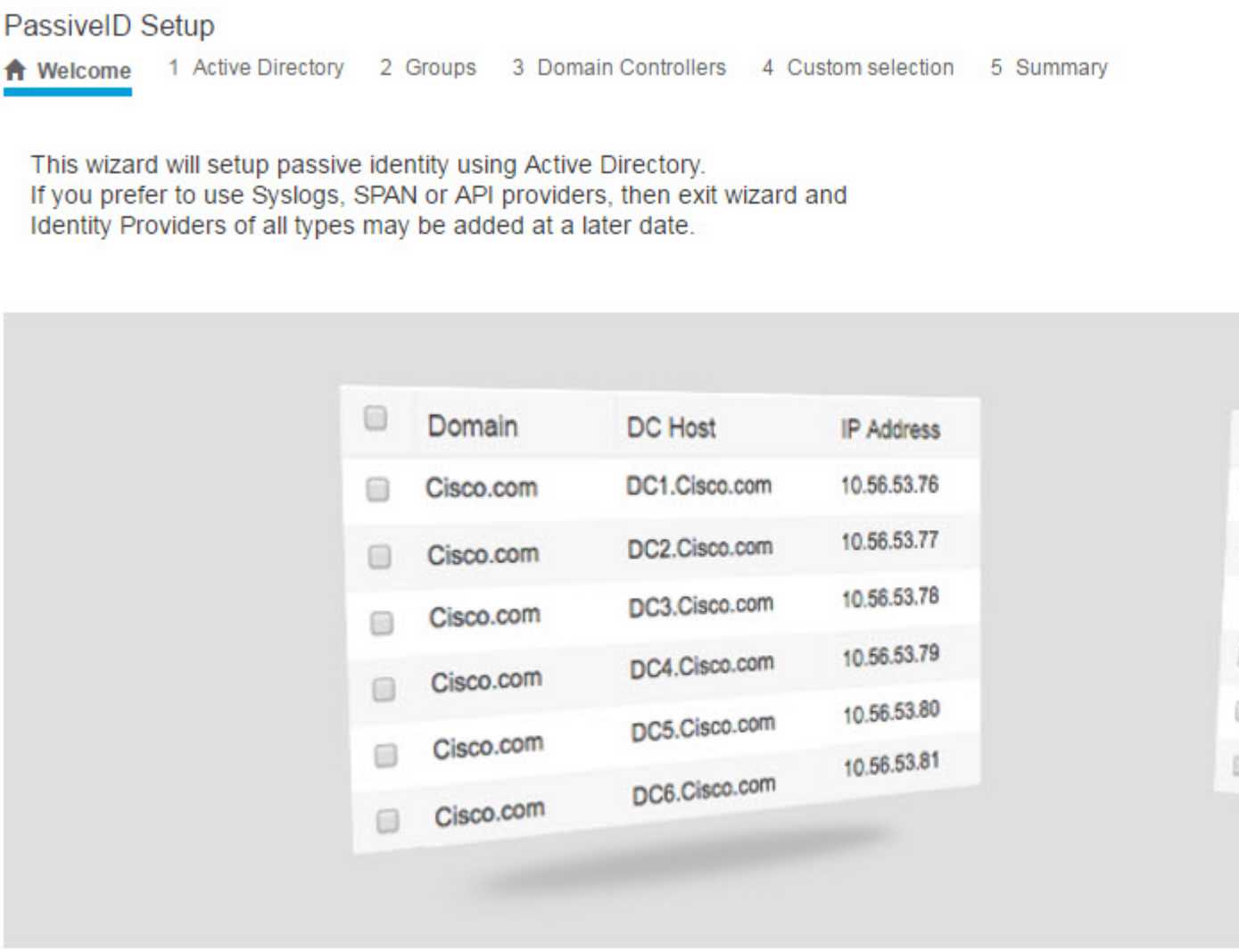
开始之前

- 确保 Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。
- 确保旨在用于加入操作的 Microsoft Active Directory 账户有效，并且未配置为下次登录时更改密码。
- 确保 ISE-PIC 在域名服务器 (DNS) 中具有条目。确保您已从 ISE-PIC 正确配置客户端机器的反向查找。有关详细信息，请参阅DNS 服务器

步骤 1 选择**主页 (Home)** > **简介 (Introduction)**。从“被动身份连接器概述”(Passive Identity Connector Overview) 屏幕中，点击**被动身份向导 (Passive Identity Wizard)**。

系统将打开“PassiveID 设置”(PassiveID Setup)：

图 *1: PassiveID* 设置



步骤 2 点击**下一步 (Next)** 以开始向导。

步骤 3 输入此 Active Directory 加入点的唯一名称。输入此节点连接的 Active Directory 域的域名，然后输入 Active Directory 管理员用户名和密码。

您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

步骤 4 点击**下一步 (Next)** 以定义 Active Directory 组并选中要包含和监控的任何用户组。
Active Directory 用户组根据您在上一步中配置的 Active Directory 加入点自动显示。

步骤 5 点击**下一步 (Next)**。选择要监控的 DC。如果选择“自定义”(Custom)，则从下一个屏幕中选择用于监控的特定 DC。完成后，点击**下一步 (Next)**。

步骤 6 点击**退出 (Exit)** 以完成向导。

下一步做什么

完成将 Active Directory 配置为初始提供程序时，还可以轻松配置其他提供程序类型。有关详细信息，请参阅提供程序。此外，现在还可以配置指定要接收由任何已定义的提供程序收集到的用户身份信息的用户。

分步设置 Active Directory (WMI) 探测器

要为 被动身份服务 配置 Active Directory 和 WMI，请使用 PassiveID 设置入门，第 2 页 或按照本章中的步骤操作，如下所示：

1. 配置 Active Directory 探测器。请参阅添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点，第 4 页。
2. 为 WMI 配置的用于接收 AD 登录事件的一个或多个节点创建 Active Directory 域控制器列表。
3. 配置 Active Directory，以使其与 ISE-PIC 集成。
4. （可选）管理 Active Directory 提供程序，第 7 页。

添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点

开始之前

确保思科 ISE-PIC 节点可以与 NTP 服务器、DNS 服务器、域控制器和全局日志服务器所在的网络通信。

必须创建加入点才能使用 Active Directory 以及使用的代理、系统日志、SPAN 和终端探测器。

在与 Active Directory 集成时，如果需要使用 IPv6，则必须确保已为相关 ISE-PIC 节点配置 IPv6 地址。

如果您使用 Google Chrome 浏览器并启用了广告拦截软件，则必须禁用广告拦截器。此任务包含受广告拦截器影响的思科 ISE GUI 元素。或者，您可以在 Google Chrome 隐身模式浏览器中执行此任务。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 点击**添加 (Add)** 并从 **Active Directory 加入点名称 (Active Directory Join Point Name)** 设置中输入域名和身份存储库名称。

步骤 3 点击**提交 (Submit)**。

此时将出现弹出窗口，询问您是否要将新创建的加入点加入到域中。如果要立即加入，请点击**是 (Yes)**。

如果已点击**否 (No)**，则保存配置将会全局保存 Active Directory 域配置，但不会将任何 ISE-PIC 节点加入到该域。

步骤 4 选中所创建的新 Active Directory 加入点旁边的复选框并点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。

步骤 5 如果加入点没有在步骤 3 中加入域，请选中相关思科 ISE-PIC 节点旁边的复选框，然后点击**加入 (Join)** 将思科 ISE-PIC 节点加入到 Active Directory 域。

您必须明确地执行此操作，即使已保存配置。要通过单个操作将多个思科 ISE-PIC 节点加入到域，所要使用的账户的用户名和密码必须对于所有加入操作都相同。如果需要不同的用户名和密码以加入每个思科 ISE-PIC 节点，则应对每个思科 ISE-PIC 节点分别执行加入操作。

步骤 6 在**加入域 (Join Domain)** 对话框中输入 Active Directory 用户名和密码。

您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

用于加入操作的用户本身应存在于域中。如果该用户存在于其他域中或子域中，应使用 UPN 符号注解用户名，如 jdoe@acme.com。

步骤 7 （可选） 选中**指定组织单位 (Specify Organizational Unit)** 复选框。

如果思科 ISE-PIC 节点机器帐户要位于除 CN=Computers,DC=someDomain,DC=someTLD 以外的特定组织单位中，应选中此复选框。思科 ISE-PIC 会在指定的组织单位下创建机器账户，如果该机器账户已存在，则会将该账户移至此位置。如果未指定组织单位，思科 ISE-PIC 将使用默认位置。应以完整可分辨名称 (DN) 格式指定值。语法必须符合 Microsoft 规范。特殊保留字符，例如 /'+,;=<> 换行符、空格和回车符，必须用反斜线 (\) 转义。例如，OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 和 Workstations,DC=someDomain,DC=someTLD。如果计算机帐户已经创建，则您不需要选中此复选框。加入 Active Directory 域之后，您还可以更改计算机帐户的位置。

步骤 8 点击**确定 (OK)**。

您可以选择多个要加入 Active Directory 域的节点。

如果加入操作不成功，则系统会显示失败消息。点击每个节点的失败消息可查看该节点的详细日志。

在配置加入点时，请注意以下几点：

- 在使用多个连接点时，如果只为单个连接点或域配置了备用 UPN 后缀，则仅在该连接点或域内执行身份查找。在这种情况下，身份验证可能会失败。作为一种解决方法，您可以为所有联合点或域配置备用 UPN 后缀。
- 在 ISE 上最多只能添加 200 个域控制器。如果超出此限制，您将收到错误“创建 <*DC FQDN*> 时出错 - DC 数超出允许的最大值 200”(Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200)。有关用于部署的域控制器的经过测试的扩展限制的详细信息，请参阅《Cisco Identity Services Engine 性能和可扩展性指南》。
- 加入完成后，思科 ISE-PIC 将更新其 AD 组和对应的安全标识符 (SID)。思科 ISE-PIC 自动启动 SID 更新过程。您必须确保允许此过程完成。
- 如果缺少 DNS 服务 (SRV) 记录，您可能无法将思科 ISE-PIC 加入 Active Directory 域（域控制器不会对您尝试加入到的域公告其 SRV 记录）。
- 建议您在指定的维护窗口后重新加入 AD。这可确保使用最新更新刷新 AD 缓存。

添加域控制器

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。

步骤 3 **注释** 要为被动身份服务添加新域控制器 (DC)，您需要该 DC 的登录凭证。

转至 PassiveID 选项卡，然后点击**添加 DC (Add DCs)**。

步骤 4 选中要添加到加入点以进行监控的域控制器旁边的复选框，然后点击**确定 (OK)**。
域控制器显示在 PassiveID 选项卡的“域控制器”(Domain Controllers) 列表中。

步骤 5 配置域控制器：

a) 选中域控制器，然后点击**编辑 (Edit)**。系统将显示**编辑项目 (Edit Item)** 屏幕。

b) 或者，编辑不同的域控制器字段。

DC 故障切换机制根据 DC 优先级列表进行管理，该列表确定在故障切换情况下选择 DC 的顺序。如果 DC 由于错误而离线或无法访问，则其优先级在优先级列表中会降低。当 DC 恢复在线时，其优先级会在优先级列表中相应地进行调整（提高）。

配置 Active Directory 用户组

配置 Active Directory 用户组，以使其可供在运用不同探测器从 Active Directory 收集用户身份信息时使用。在内部，思科 ISE 使用安全标识符 (SID) 帮助解决组名称不明确问题和增强组映射。SID 提供准确的组分配匹配。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。点击要为其添加组的加入点。

步骤 2 点击**组 (Groups)** 选项卡。

步骤 3 执行以下操作之一：

a) 选择**添加 (Add)** > **从目录中选择组 (Select Groups From Directory)** 以选择现有组。

b) 选择**添加 (Add)** > **添加组 (Add Group)** 以手动添加组。您可以同时提供组名称和 SID，也可以仅提供组名称并按**获取 SID (Fetch SID)**。

对于用户界面登录，请勿在组名称中使用双引号 (”)。

步骤 4 如果您手动选择组，您可以使用过滤器进行搜索。例如，输入 **admin*** 作为搜索条件，然后点击**检索组 (Retrieve Groups)**，即可查看以 admin 开头的用户组。您还可以输入星号 (*) 通配符过滤结果。一次只能检索 500 个组。

步骤 5 选中想要可用于授权策略的组旁边的复选框，然后点击**确定 (OK)**。

步骤 6 如果您选择手动添加组，请为新组输入名称和 SID。

步骤 7 点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

注释　如果删除某个组，然后创建一个与此组相同名称的新组，则必须点击**更新 SID 值 (Update SID Values)**以向新创建的组分配新 SID。升级之后，SID 会在首次联接之后自动更新。

管理 Active Directory 提供程序

创建并配置 Active Directory 加入点之后，通过以下任务继续管理 Active Directory 探测器：

- 对用户进行 Active Directory 组测试，第 7 页
- 查看节点的 Active Directory 加入，第 8 页
- 诊断 Active Directory 问题，第 8 页
- 退出 Active Directory 域，第 9 页
- 删除 Active Directory 配置，第 9 页
- 启用 Active Directory 调试日志，第 10 页

对用户进行 Active Directory 组测试

“测试用户”工具可用于从 Active Directory 验证用户组。您可以对单个加入点或对范围运行测试。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 选择以下选项之一：

- 要对所有加入点运行测试，请选择**高级工具 (Advanced Tools)** > **就所有加入点测试用户 (Test User for All Join Points)**。
- 要对特定加入点运行测试，请选择该加入点并点击**编辑 (Edit)**。选择思科 ISE-PIC 节点并点击**测试用户 (Test User)**。

步骤 3 在 Active Directory 中输入用户（或主机）的用户名和密码。

步骤 4 选择身份验证类型。如果选择“查找”(Lookup) 选项，则无需步骤 3 中的密码输入。

步骤 5 如果您是对所有加入点运行此测试，请选择要对其运行此测试的思科 ISE-PIC 节点。

步骤 6 从 Active Directory 检索组，请选中“检索组”(Retrieve Groups) 和“检索属性”(Retrieve Attributes) 复选框。

步骤 7 点击**测试 (Test)**。

系统将显示测试操作的结果和步骤。这些步骤可帮助确定故障原因并进行故障排除。

您还可以查看 Active Directory 执行每个处理步骤所需的时间（以毫秒为单位）。如果操作所需的时间超过阈值，思科 ISE-PIC 将显示警告消息。

查看节点的 Active Directory 加入

您可以使用 **Active Directory** 页面上的**节点视图 (Node View)** 按钮查看给定思科 ISE-PIC 节点的所有 Active Directory 加入点的状态或所有思科 ISE-PIC 节点上的所有加入点列表。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 点击**节点视图 (Node View)**。

步骤 3 从 **ISE 节点 (ISE Node)** 下拉列表中选择节点。
表格按节点列出 Active Directory 的状态。如果部署中有多个加入点和多个思科 ISE-PIC 节点，则更新此表可能需要几分钟时间。

步骤 4 点击加入点**名称 (Name)** 链接以转至该 Active Directory 加入点页面，然后执行其他特定操作。

步骤 5 点击**诊断摘要 (Diagnostic Summary)** 列中的链接以转至**诊断工具 (Diagnostic Tools)** 页面来对特定问题进行故障排除。诊断工具显示每个节点的每个加入点的最新诊断结果。

诊断 Active Directory 问题

诊断工具是在每个思科 ISE-PIC 节点上运行的服务。当思科 ISE-PIC 使用 Active Directory 时，通过该工具可自动测试和诊断 Active Directory 部署并执行一组测试，以检测可能导致功能或性能故障的问题。

思科 ISE-PIC 无法加入 Active Directory 或对其进行身份验证有多个原因。此工具帮助确保正确配置用于将思科 ISE-PIC 连接到 Active Directory 的前提条件。该工具有助于检测网络、防火墙配置、时钟同步、用户身份验证等问题。此工具以逐步操作指南的形式工作，并帮助您根据需要解决中间每层的问题。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 点击**高级工具 (Advanced Tools)** 下拉列表，选择**诊断工具 (Diagnostic Tools)**。

步骤 3 选择要运行诊断的思科 ISE-PIC 节点。

如果未选择思科 ISE-PIC 节点，则在所有节点上运行测试。

步骤 4 选择特定的 Active Directory 加入点。

如果不选择 Active Directory 加入点，则在所有加入点上运行测试。

步骤 5 您可以按需或按计划运行诊断测试。

- 要立即运行测试，请选择**立即运行测试 (Run Tests Now)**。
- 要按计划间隔运行测试，请选中**运行计划测试 (Run Scheduled Tests)** 复选框并指定必须运行测试的开始时间和间隔（以小时、天或周为单位）。启用此选项后，将在所有节点和实例上运行所有诊断测试，并在**主页 (Home)** 控制面板上的**警报 (Alarms)** 面板中报告故障。

步骤 6 点击**查看测试详情 (View Test Details)** 查看具有警告或失败状态的测试的详细信息。

下表允许您重新运行特定测试、停止正在运行的测试和查看特定测试的报告。

退出 Active Directory 域

如果不再需要使用此 Active Directory 域或此加入点收集用户身份，则可以退出 Active Directory 域。

从命令行界面重置思科 ISE-PIC 应用配置或在备份或升级后恢复配置时，它将执行退出操作，从而将思科 ISE-PIC 节点与 Active Directory 域断开连接（如果已加入该节点）。但是，不会从 Active Directory 域中删除思科 ISE-PIC 节点账户。我们建议您使用 Active Directory 凭证从 Admin 门户执行退出操作，因为这也会从 Active Directory 域删除节点帐户。在更改思科 ISE-PIC 主机名时，也建议您如此操作。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。

步骤 3 选中思科 ISE-PIC 节点旁边的复选框，然后点击**退出 (Leave)**。

步骤 4 输入 Active Directory 用户名和密码，然后点击**确定 (OK)** 以退出该域并从思科 ISE-PIC 数据库中删除机器账户。

如果输入 Active Directory 凭证，则思科 ISE-PIC 节点将退出 Active Directory 域并从 Active Directory 数据库中删除思科 ISE-PIC 机器账户。

注释 要从 Active Directory 数据库中删除思科 ISE-PIC 机器账户，此处提供的 Active Directory 凭证必须具有从域中删除机器账户的权限。

步骤 5 如果您没有 Active Directory 凭证，请选中**无可用凭证 (No Credentials Available)** 复选框，然后点击**确定 (OK)**。

如果选中**退出没有凭证的域 (Leave domain without credentials)** 复选框，则主思科 ISE-PIC 节点将退出 Active Directory 域。Active Directory 管理员必须手动删除加入期间在 Active Directory 中创建的设备帐户。

删除 Active Directory 配置

如果您不会使用特定 Active Directory 配置作为探测器，则应删除 Active Directory 配置。如果您希望加入其他 Active Directory 域，则请勿删除该配置。您可以退出当前所加入的域并加入新的域。如果该配置是以下位置中的唯一配置，请勿将其删除： ISE-PIC

开始之前

确保您已退出 Active Directory 域。

步骤 1 选择**提供程序 (Providers)** > **Active Directory**。

步骤 2 选中已配置的 Active Directory 旁边的复选框。

步骤 3 检查并确保列出的本地节点状态为未加入。

步骤 4 点击删除 **(Delete)**。

您已从 Active Directory 数据库中移除该配置。如果希望以后再使用 Active Directory，您可以重新提交有效的 Active Directory 配置。

启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。启用 Active Directory 调试日志可能会影响 ISE-PIC 性能。

步骤 1 选择管理 **(Administration)** > 日志记录 **(Logging)** > 调试日志配置 **(Debug Log Configuration)**。

步骤 2 点击要从中获取 Active Directory 调试信息的Cisco ISE-PIC节点旁边的单选按钮，然后点击编辑 **(Edit)**。

步骤 3 点击 **Active Directory** 单选按钮，然后点击编辑 **(Edit)**。

步骤 4 从 Active Directory 旁的下拉列表中选择 **DEBUG**。这将包括错误、警告和 verbose 日志。要获得完整日志，请选择 **TRACE**。

步骤 5 点击保存 **(Save)**。

Active Directory 设置

Active Directory AD 是用于从中接收用户信息（包括用户名和 IP 地址）的高度安全且精确的源。

要通过创建和编辑加入点来创建和管理 Active Directory 探测器，请依次选择提供程序 **(Providers)** > **Active Directory**。

有关详细信息，请参阅添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点 ， 第 4 页。

依次选择提供程序 **(Providers)** > **Active Directory**，然后选中要编辑的加入点并点击编辑 **(Edit)**。对于“加入域”(Join Domain) 屏幕，请依次选择提供程序 **(Providers)** > **Active Directory**，选中要编辑的加入点并点击加入 **(Join)**。

表 *1: Active Directory* 加入点名称设置和加入域窗口

字段名称	说明
加入点名称	用于快速轻松地区分此已配置加入点的唯一名称。
Active Directory 域	此节点连接到的 Active Directory 域的域名。
域管理员	这是具有管理员权限的 Active Directory 用户的用户主体名称或用户账户名称。
密码	这是 Active Directory 中配置的域管理员的密码。
指定组织单位	输入管理员的组织单位信息

字段名称	说明
存储凭证	您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。 对于终端探测器，必须选择**存储凭证 (Store credentials)**。

选择**提供程序 (Providers)** > **Active Directory**。

表 *2: Active Directory* 加入/退出窗口

字段名称	说明
ISE 节点 (ISE Node)	安装中的特定节点的 URL。
ISE 节点角色	表示节点是安装中的主节点还是辅助节点。
状态	指示节点是否主动加入 Active Directory 域。
域控制器	对于加入 Active Directory 的节点，此列指示节点在 Active Directory 域中连接到的特定域控制器。
站点	仅对于完整 ISE 安装相关。有关详细信息，请参阅将 ISE-PIC 升级到完整 ISE 安装。

表 *3:* 被动 *ID* 域控制器 *(DC)* 列表

字段	说明
域	域控制器所在的服务器的完全限定域名。
DC 主机	域控制器所在的主机。
站点	仅对于完整 ISE 安装相关。有关详细信息，请参阅将 ISE-PIC 升级到完整 ISE 安装。
IP 地址	域控制器的 IP 地址。
监控方法	通过以下方法之一监控 Active Directory 域控制器的用户身份信息： • WMI：使用 WMI 基础设施直接监控 Active Directory。 • 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理”(Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅 Active Directory 代理。

表 *4:* 被动 *ID* 域控制器 *(DC)* 编辑窗口

字段名称	说明
主机 FQDN	输入域控制器所在的服务器的完全限定域名。

字段名称	说明
Description	输入此域控制器的唯一说明，以便轻松标识此域控制器。
用户名	用于访问 Active Directory 的管理员的用户名。
密码	用于访问 Active Directory 的管理员的密码。
协议	通过以下方法之一监控 Active Directory 域控制器的用户身份信息： • WMI：使用 WMI 基础设施直接监控 Active Directory。 • 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理”(Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅 Active Directory 代理。

系统从 Active Directory 来定义和管理 Active Directory 组，并且可从此选项卡查看加入此节点的 Active Directory 的组。有关 Active Directory 的详细信息，请参阅 https://msdn.microsoft.com/en-us/library/bb742437.aspx。

依次选择**提供程序 (Providers)** > **Active Directory** > **高级设置 (Advanced Settings)**。

表 *5: Active Directory* 高级设置

字段名称	说明
历史记录间隔	被动身份服务 读取已出现的用户登录信息的时间段。启动或重新启动 被动身份服务 以跟进在其不可用情况下生成的事件时需要此项。当终端探测器处于活动状态时，它将保持此间隔的频率。
用户会话老化时间	用户可以登录的时间量。被动身份服务 会识别 DC 中的新用户登录事件，但是 DC 在用户注销时不会进行报告。通过老化时间，ISE-PIC 可以确定用户登录的时间间隔。
NTLM 协议设置	您可以选择 NTLMv1 或 NTLMv2 作为ISE-PIC 和 DC 之间的通信协议。NTLMv2 是建议默认值。

字段名称	说明
授权流程	选中此复选框可为 PassiveID 登录用户配置授权策略。 您可以配置授权策略，以根据 Active Directory 组成员身份将 SGT 分配给用户。这允许您为 PassiveID 授权创建 TrustSec 策略规则。 可以使用 PassiveID 词典中的 **PassiveID_Provider**、 **PassiveID_Username** 或 **PassiveID_Groups** 属性为 **PassiveID** 登录用户创建授权规则。可以为 **PassiveID_Provider** 属性设置以下值： • **API** • 代理 • **SPAN** • 系统日志 • **WMI** • 其他 PassiveID 登录用户的 IP-SGT 映射和 Active Directory 组详细信息包含在会话主题中。这些详细信息可以通过 pxGrid、pxGrid 云或 SXP 发布。 您可以在 **RADIUS 实时日志** 窗口（**操作 > RADIUS > 实时日志**）和 **RADIUS 实时会话** 窗口（**操作 > RADIUS > 实时会话**）中查看授权策略状态和 SGT 详细信息。 注释 • 确保在节点上启用 PassiveID、pxGrid、pxGrid Cloud 和 SXP 服务。选择 **管理 > 系统 > 部署**以启用 pxGrid 服务。 • 您必须在 **SXP 设置** 窗口（**工作中心 > TrustSec > 设置 > SXP 设置**）中启用 **将 RADIUS 和 PassiveID 映射添加到 SXP IP SGT 映射表中** 选项，才能在 SXP 映射中包含 PassiveID 映射。 • 无法使用 SXP 发布使用 API 提供程序进行身份验证的 PassiveID 登录用户的 SGT 详细信息。但是，这些用户的 SGT 详细信息可以通过 pxGrid 和 pxGrid 云发布。

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。