资产可视性

使用外部身份库对思科 ISE 进行管理访问

在Cisco ISE 中，您可以通过外部身份库（例如，Active Directory、LDAP 或 RSA SecureID）对管理员进行身份验证。您可以使用两种模式，通过外部身份库提供身份验证：

- 外部身份验证和授权：没有在本地Cisco ISE 数据库中为管理员指定的凭证，授权仅基于外部身份库组成员身份。此模式用于 Active Directory 和 LDAP 身份验证。

- 外部身份验证和内部授权：管理员的身份验证凭证来自外部身份源，并使用本地Cisco ISE 数据库分配授权和管理员职责。此模式用于 RSA SecurID 身份验证。此方法要求您同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。

在身份验证过程中，如果与外部身份库的通信尚未建立或失败，Cisco ISE 将“后退”，并尝试从内部身份数据库执行身份验证。此外，无论已为其设置外部身份验证的管理员何时启动浏览器和发起登录会话，该管理员都可以从登录对话中的**身份存储区 (Identity Store)** 下拉列表中选择**内部 (Internal)**，请求通过Cisco ISE 本地数据库进行身份验证。

属于超级管理员组且配置为使用外部身份存储区进行身份验证和授权的管理员也可以使用外部身份存储区进行身份验证，以访问命令行界面 (CLI)。

注释 您可以将此方法配置为仅通过 Admin 门户提供外部管理员身份验证。Cisco ISE CLI 不具备这些功能。

如果网络没有一个或多个现有外部身份库，请确保已安装必要的外部身份库，并已将Cisco ISE 配置为访问这些身份库。

外部身份验证和授权

默认情况下，Cisco ISE 提供内部管理员身份验证。要设置外部身份验证，您必须为您在外部身份库中定义的外部管理员帐户创建密码策略。然后，您可以将此策略应用于最终成为外部管理员 RBAC 策略一部分的外部管理员组。

除了通过外部身份库提供身份验证之外，您的网络还可能要求您使用通用访问卡 (CAC) 身份验证设备。

要配置外部身份验证，必须执行以下操作：

- 使用外部身份库，配置基于密码的身份验证。
- 创建外部管理员组。
- 为外部管理员组配置菜单访问和数据访问权限。
- 为外部管理员身份验证创建 RBAC 策略。

使用外部身份库配置基于密码的身份验证

必须先为使用外部身份库（例如 Active Directory 或 LDAP）进行身份验证的管理员配置基于密码的身份验证。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

步骤 2 在**身份验证方式 (Authentication Method)** 选项卡上，选择**基于密码 (Password Based)**，然后选择您应已配置的外部身份源之一。例如，您已创建的 Active Directory 实例。

步骤 3 为使用外部身份库进行身份验证的管理员配置您所需的特定密码策略设置。

步骤 4 点击**保存 (Save)**。

创建外部管理员组

您需要创建一个外部 Active Directory 或 LDAP 管理员组。这可确保Cisco ISE 使用外部 Active Directory 或 LDAP 身份存储区中定义的用户名验证您登录时输入的管理员用户名和密码。

Cisco ISE 将从外部资源导出 Active Directory 或 LDAP 组信息并将其存储为字典属性。然后，在为此外部管理员身份验证方法配置 RBAC 策略时，您可以将该属性指定为策略元素之一。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**

映射的外部组 (External Groups Mapped) 列显示映射到内部 RBAC 角色的外部组数量。您可以点击与管理员角色对应的数字以查看外部组（例如，如果点击超级管理员对应显示的 2，则系统将显示两个外部组的名称）。

步骤 2 点击**添加 (Add)**。

步骤 3 输入名称和可选说明。

步骤 4 点击**外部 (External)**。

如果已连接并加入 Active Directory 域，则**名称 (Name)** 字段中会显示 Active Directory 实例名称。

步骤 5 从**外部组 (External Groups)** 下拉列表框中，选择要为此外部管理员组映射的 Active Directory 组。

点击“+”号以将更多 Active Directory 组映射至此外部管理员组。

步骤 6 点击**保存 (Save)**。

创建内部只读管理员

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)** 。

步骤 2 点击**添加 (Add)**，然后选择**创建管理员用户 (Create An Admin User)**。

步骤 3 选中**只读 (Read Only)** 复选框以创建只读管理员。

将外部组映射至只读管理员组

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** 以配置外部身份验证源。

步骤 2 点击需要的外部身份源（例如 Active Directory 或 LDAP），然后从选定身份源检索组。

步骤 3 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)**，将管理员访问权限的身份验证方法映射到身份源。

步骤 4 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**，然后选择**只读管理员 (Read Only Admin)** 组。

步骤 5 选中**外部 (External)** 复选框，并选择您想要为其提供只读权限的所需外部组。

步骤 6 点击**保存 (Save)**。

无法将映射到只读管理员组的外部组分配到任何其他管理员组。

为外部管理员组配置菜单访问和数据访问权限

您必须配置可以分配给外部管理员组的菜单访问和数据访问权限。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **权限 (Permissions)**。

步骤 2 点击以下选项之一：

- **菜单访问 (Menu Access)**：属于外部管理员组的所有管理员都可以获得菜单或子菜单级别的权限。菜单访问权限决定着管理员可以访问的菜单或子菜单。
- **数据访问 (Data Access)**：属于外部管理员组的所有管理员都可以获得数据级别的权限。数据访问权限决定着管理员可以访问的数据。

步骤 3 为外部管理员组指定菜单访问或数据访问权限。

步骤 4 点击**保存 (Save)**。

创建用于外部管理员身份验证的 RBAC 策略

必须配置新的RBAC策略， 以便使用外部身份存储区对管理员进行身份验证，并指定自定义菜单和数据访问权限。此策略必须拥有用于身份验证的外部管理员组以及Cisco ISE 菜单和数据访问权限以管理外部身份验证和授权。

注释 您无法修改现有（系统预设）RBAC 策略以指定这些新外部属性。如果想要将某个现有策略用作模板，则必须复制该策略，为其重命名，然后分配新属性。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **RBAC 策略 (RBAC Policy)**。

步骤 2 指定规则名称、外部管理员组和权限。

请记住，必须向正确的管理员用户 ID 分配相应的外部管理员组。确保管理员与正确的外部管理员组关联。

步骤 3 点击**保存 (Save)**。

如果您以管理员身份登录，而且Cisco ISE RBAC 策略无法验证您的管理员身份，则Cisco ISE 会显示“unauthenticated”消息，而且您无法访问 Admin 门户。

使用外部身份库配置管理员访问权限以使用内部授权进行身份验证

此方法要求您同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。当您配置Cisco ISE 使用外部 RSA SecurID 身份库来提供管理员身份验证时，管理员凭证身份验证将由 RSA 身份库执行。但是，授权（策略应用）仍根据Cisco ISE 内部数据库进行。此外，还要记住两个与外部身份和授权不同的重要因素：

- 您不需要为管理员指定任何特定的外部管理员组。
- 您必须同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)**。

步骤 2 确保外部 RSA 身份库中的管理员用户名也存在于Cisco ISE 中。确保点击“密码”(Password) 下的 **外部 (External)** 选项。

注释 您不需要为此外部管理员用户 ID 指定密码，也不需要将任何特殊配置的外部管理员组应用到关联的RBAC策略。

步骤 3 点击**保存 (Save)**。

外部身份验证流程

当管理员登录时，登录会话会完成流程中的以下步骤：

1. 管理员发送 RSA SecurID 质询。
2. RSA SecurID 返回质询响应。
3. 管理员在Cisco ISE 登录对话框中输入用户名和 RSA SecurID 质询响应，就像输入用户 ID 和密码。
4. 管理员确保指定的身份库为外部 RSA SecurID 资源。
5. 管理员点击 **Login**。

登录之后，管理员仅可查看在 RBAC 策略中指定的菜单和数据访问项目。

外部身份源

您可以通过这些页面配置和管理包含Cisco ISE 用于身份验证和授权的用户数据的外部身份源。

LDAP 身份源设置

下表介绍“LDAP 身份源”(LDAP Identity Sources) 窗口上的字段，您可以使用此窗口创建 LDAP 实例并连接该实例。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 *1: LDAP* 常规设置

字段名称	使用指南
名称 (Name)	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
说明	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。
注释 仅当选择自定义架构时，才可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组名称属性 **(Group Name Attribute)**	• CN：根据通用名称检索 LDAP 身份存储区组。 • DN：根据可分辨名称检索 LDAP 身份存储区组。
证书属性 **(Certificate Attribute)**	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
组映射属性 **(Group Map Attribute)**	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 **(Subject Objects Contain Reference To Groups)**	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 **(Group Objects Contain Reference To Subjects)**	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 **(Subjects in Groups Are Stored in Member Attribute As)**	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。
用户信息属性	默认情况下，预定义属性用于收集以下内置架构类型的用户信息（例如，名字、姓氏、电子邮件、电话，位置等）： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。 您还可以选择架构 (Schema) 下拉菜单中的定制 (Custom) 选项，根据要求编辑用户信息属性。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 *2: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器 (Enable Secondary Server)	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器 (Primary and Secondary Servers)	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效IP地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
为每个 ISE 节点指定服务器	选中此复选框可配置每个PSN的主辅LDAP服务器主机名/IP 及其端口。 启用此选项后，将显示一个表，列出部署中的所有节点。您需要选择节点并配置主要和辅助LDAP服务器主机名/IP 及所选节点的端口。
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 DN (Admin DN)	输入管理员的DN。管理员DN是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。

字段名称	使用指南
安全身份验证 **(Secure Authentication)**	点击此字段以对Cisco ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“**LDAP 服务器根 CA**”**(LDAP Server Root CA)**	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 **(Server Timeout)**	以秒为单位输入Cisco ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 **(Max. Admin Connections)**	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
每 **N** 秒强制重新连接	选中此复选框并在**秒 (Seconds)** 字段中输入所需的值可强制服务器按照指定的时间间隔续订 LDAP 连接。有效范围为 1 至 60 分钟。
测试与服务器的绑定 **(Test Bind to Server)**	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望Cisco ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 **(Failback to Primary Server after)**	如果Cisco ISE 尝试连接的主 LDAP 服务器无法访问，Cisco ISE 会尝试连接辅助 LDAP 服务器。如果您希望Cisco ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍目录组织 **(Directory Organization)** 选项卡上的字段。

表 *3: LDAP* 目录组织设置

字段名称	使用指南
主题搜索库 (Subject Search Base)	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 (Group Search Base)	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个MAC地址格式供Cisco ISE用于在LDAP数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当Cisco ISE 收到主机查找请求时，Cisco ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，Cisco ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则Cisco ISE 会向 LDAP 服务器提交 user1。 **注释** <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，Cisco ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则Cisco ISE 会向 LDAP 服务器提交 *user1*。 **注释** *<end_string>* 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *4: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *5: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

LDAP 高级设置

下表介绍“高级设置”(Advanced Settings) 选项卡中的字段。

表 *6: LDAP* 高级设置

字段名称	使用指南
启用密码更改 (Enable Password Change)	在使用 PAP 协议进行设备管理和使用 RADIUS EAP-GTC 协议进行网络访问时，选中此复选框可让用户在密码到期或重置密码的情况下更改密码。对于不受支持的协议，用户身份验证会失败。此选项还可以让用户在下次登录时更改密码。

相关主题

LDAP 目录服务，第 123 页
LDAP 用户身份验证，第 124 页
LDAP 用户查找，第 127 页
添加 LDAP 身份源，第 128 页

RADIUS 令牌身份源设置

下表介绍“RADIUS 令牌身份源”(Token Identity Sources) 窗口上的字段，您可以使用此窗口配置和连接外部 RADIUS 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

表 *7: RADIUS* 令牌身份源设置

字段名称	使用指南
名称	输入 RADIUS 令牌服务器名称。允许的最大字符数为 64。
说明	输入 RADIUS 令牌服务器说明。允许的最大字符数为 1024。

字段名称	使用指南
SafeWord Server	如果 RADIUS 身份源为 SafeWord 服务器，请选中此复选框。
Enable Secondary Server	选中此复选框，为Cisco ISE 启用辅助 RADIUS 令牌服务器，在主要服务器发生故障时用作备份。如果选中此复选框，必须配置辅助 RADIUS 令牌服务器。
Always Access Primary Server First	如果希望Cisco ISE 总是首先访问主服务器，请点击此选项。
Fallback to Primary Server after	点击此选项可指定在无法连接主服务器时，Cisco ISE 能够在多长时间里（分钟）使用辅助 RADIUS 令牌服务器进行身份验证。这段时间过后，Cisco ISE 重新尝试对照主服务器进行身份验证。
主服务器	
Host IP	输入主要 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在主要 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入主要 RADIUS 令牌服务器侦听的端口号。
Server Timeout	指定Cisco ISE 在确定主服务器关闭之前，等待主要 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在迁移到辅助服务器（如果已定义）或放弃请求（如果未定义辅服务器）之前，尝试重新连接到主服务器的次数。
辅助服务器	
Host IP	输入辅助 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在辅助 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入辅助 RADIUS 令牌服务器侦听的端口号。有效值为 1 至 65535。默认值为 1812。
Server Timeout	指定Cisco ISE 在确定辅助服务器关闭之前，等待辅助 RADIUS 令牌服务器发出响应的秒数。

字段名称	使用指南
Connection Attempts	指定Cisco ISE 在放弃请求之前应当尝试重新连接辅助服务器的次数。

相关主题

RADIUS 令牌身份源，第 144 页
添加 RADIUS 令牌服务器，第 149 页

RSA SecurID 身份源设置

下表介绍“RSA SecurID 身份源”(RSA SecurID Identity Sources) 窗口上的字段，您可以使用此窗口创建和连接 RSA SecurID 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 *8: RSA* 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 *9: RSA* 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。

字段名称	使用指南
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源，第 150 页
思科 ISE 和 RSA SecurID 服务器集成，第 151 页
添加 RSA 身份源，第 154 页

思科 ISE 用户

在本章中，“用户”一词是指定期访问网络的员工和承包商，以及发起人和访客用户。发起人用户是通过发起人门户创建和管理访客用户帐户的组织的员工或承包商。访客用户是在一段有限时间内需要访问组织的网络资源的外部访问者。

您必须为任何要获取对Cisco ISE 网络上的资源和服务的访问权限的用户创建帐户。员工、承包商和发起人用户可从管理门户创建。

用户身份

用户身份就像一个容纳关于用户的信息并形成其网络访问凭证的容器。每个用户的身份都由数据定义并且包括：用户名、邮件地址、密码、帐户说明、关联管理组、用户组和角色。

用户组

用户组是单个用户的集合，这些用户拥有一系列允许其访问特定Cisco ISE 服务和功能的相同权限。

用户身份组

用户的组身份包含用于标识和说明属于同一个组的一组特定用户的元素。组名是此组的成员具有的功能角色的说明。组是属于此组的用户的列表。

默认用户身份组

Cisco ISE 提供以下预定义用户身份组：

- Employee - 贵公司的员工属于此组。
- SponsorAllAccount - 可以暂停或恢复Cisco ISE 网络中的所有访客帐户的发起人用户。
- SponsorGroupAccounts - 可以暂停由同一发起人用户组中的发起人用户创建的访客帐户的发起人用户。
- SponsorOwnAccounts - 只能暂停其已创建的访客帐户的发起人用户。
- Guest - 需要临时访问网络中的资源的访问者。
- ActivatedGuest - 其帐户已启用并处于活动状态的访客用户。

用户角色

用户角色是决定用户可以执行什么任务以及可以访问Cisco ISE 网络上的什么服务的一系列权限。用户角色与用户组关联。例如，网络接入用户。

用户帐户自定义属性

Cisco ISE 允许根据用户属性限制网络访问用户和管理员的网络访问。Cisco ISE 具有一系列预定义的用户属性并且允许创建自定义属性。两种属性都可以用于定义身份验证策略的条件中。您还可以为用户帐户定义密码策略，以使密码符合指定的条件。

自定义用户属性

您可以在**用户自定义属性 (User Custom Attributes)** 窗口（**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户自定义属性 (User Custom Attributes)**）配置其他用户帐户属性。在此窗口中，您还可以查看预定义用户属性列表。不能编辑预定义用户角色。

在**用户自定义属性 (User Custom Attributes)** 窗格输入必填的详细信息以添加新的自定义属性。在添加或编辑网络访问用户（**管理 [Administration] > 身份管理 [Identity Management] > 身份 [Identities] > 用户 [Users] > 添加/编辑 [Add/Edit]**）或管理员用户（**管理 [Administration] > 系统 [System] > 管理访问 [Admin Access] > 管理员 [Administrators] > 管理员用户 [Admin Users] > 添加/编辑 [Add/Edit]**）时，会显示您在**用户自定义属性 (User Custom Attributes)** 窗口添加的自定义属性和默认值。在添加或编辑网络访问或管理员用户时，您可以更改默认值。

您可以在**用户自定义属性 (User Custom Attributes)** 窗口为自定义属性选择以下数据类型：

- 字符串 (String)：您可以指定最大字符串长度（字符串属性值允许的最大长度）。

- 整数 (Integer)：您可以配置最小和最大值（指定最低和最高的可接受整数值）。
- 枚举 (Enum)：您可以为每个参数指定以下值：
  - 内部使用
  - 显示值

  您还可以指定默认参数。在显示 (Display) 字段中添加的值会在添加或编辑网络访问或管理员用户时显示。
- Float
- 密码 (Password)：您可以指定最大字符串长度。
- 长 (Long)：您可以配置最小和最大值。
- IP：您可以指定默认 IPv4 或 IPv6 地址。
- Boolean：您可以设置 True 或 False 作为默认值。
- 日期(Date)：您可以从日历中选择一个日期并将其设置为默认值。该日期显示格式为 yyyy-mm-dd。

如果要在添加或编辑网络访问或管理员用户时将一个属性设置为强制属性，请选中**强制 (Mandatory)** 复选框。您还可以设置自定义属性的默认值。

自定义属性可在身份验证策略中使用。您为自定义属性设置的数据类型和允许范围将应用于策略条件中的自定义属性值。

用户身份验证设置

并非所有外部身份存储区都允许网络访问用户更改其密码。有关详细信息，请参阅每个身份源对应的部分。

网络使用密码规则是在以下位置配置的： **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **用户身份验证设置 (User Authentication Settings)**。

以下部分提供有关**密码策略 (Password Policy)** 选项卡上某些字段的更多信息。

- **必要字符 (Required Characters)**：如果配置要求使用大写或小写字符的用户密码策略，而用户的语言不支持这些字符，则用户无法设置密码。要支持 UTF-8 字符，请取消选中以下复选框：
  - 小写字母字符。
  - 大写字母字符
- **密码更改增量 (Password Change Delta)**：指定在将当前密码更改为新密码时必须更改的最小字符数。Cisco ISE 不会将字符位置更改视为更改。

  例如，如果密码增量为 3，当前密码为“?Aa1234?”，则“?Aa1567?”（“5”、“6”和“7”是三个新字符）是有效的新密码。“?Aa1562?”失败，因为“?”、“2”和“?”字符包含在当前密码中。“Aa1234??”失败，因为尽管字符位置已更改，但当前密码中的字符是相同的。

密码更改增量也会考虑以前的 X 个密码，其中 X 是**密码必须与以前的版本不同 (Password must be different from the previous versions)** 的值。如果密码增量为 3，密码历史记录为 2，则必须更改未包含在过去 2 个密码中的 4 个字符。

- **字典单词 (Dictionary words)**：选中此复选框可限制使用任何字典单词、它的逆序字符或用其他字符替换的字母。

  不允许用“$”替换“s”、“@”替换“a”、“0”替换“o”、“1”替换“l”、“!”替换“i”、“3”替换“e”。例如，“Pa$$w0rd”。

  - **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。
  - **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**选择文件 (Choose File)** 以选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。

- 最终用户需要定期更改密码，否则用户帐户将被临时禁用。您可以使用**密码生存期 (Password Lifetime)** 部分更新密码重置间隔和提醒。要设置密码的生存期，请选中**若不更改密码则在 __ 天后禁用用户帐户 (Disable user account after __ days if password was not changed)** 复选框，然后在输入框中输入天数。要启用密码重置提醒，请选中**在密码到期前 __ 天显示提醒 (Display reminder __ days prior to password expiration)** 复选框，在输入值中输入天数，以便在密码到期之前向用户发送通知。
- **锁定/暂停帐户前的错误登录尝试数 (Lock/Suspend Account with Incorrect Login Attempts)**：如果登录尝试失败次数超过所指定的值，可以使用此选项暂停或锁定帐户。有效范围为 3 到 20。
- 在**帐户禁用策略 (Account Disable Policy)** 选项卡中，可以配置有关何时禁用现有用户帐户的规则。有关详细信息，请参阅全局禁用用户帐户。

相关主题

用户帐户自定义属性，第 17 页
添加用户，第 20 页

为用户和管理员生成自动密码

Cisco ISE 在用户和管理员创建页面引入了**生成密码 (Generate Password)** 选项，可根据Cisco ISE 密码策略生成即时密码。通过此选项，用户或管理员可使用Cisco ISE 生成的密码，而不用花时间思考需配置的安全密码。

Cisco ISE Web 界面中的以下三个位置可支持**生成密码 (Generate Password)** 选项

- 用户 - **管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)**。
- 管理员 - **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员用户 (Admin Users)**。
- 登录的管理员（当前管理员） - **设置 (Settings) > 帐户设置 (Account Settings) > 更改密码 (Change Password)**。

内部用户操作

添加用户

通过Cisco ISE，您可以查看、创建、修改、复制、删除、导入、导出、搜索Cisco ISE 用户的属性，或更改用户属性的状态。

如果您使用Cisco ISE 内部数据库，则必须为需要访问Cisco ISE 中资源或服务的任何新用户创建帐户。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

您还可以通过访问以下位置来创建用户： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **身份 (Identities)** > **用户 (Users)** 页面。

步骤 2 点击 **添加 (+) (Add[+])** 以创建新用户。

步骤 3 为字段输入值。

请勿在用户名中包含!、%、:、;、[、{、|、}、]、`、?、=、<、>、\和控制字符。此外，也不允许只包含空格的用户名。如果您使用用于自带设备的Cisco ISE 内部证书授权 (CA)，您在此处提供的用户名会用作终端证书的通用名称。Cisco ISE 内部 CA 的“通用名称”(Common Name) 字段不支持“+”或“*”字符。

步骤 4 点击**提交 (Submit)** 在Cisco ISE 内部数据库中创建新用户。

导出思科 ISE 用户数据

您可能需要从Cisco ISE 内部数据库中导出用户数据。Cisco ISE 允许您以受密码保护的 csv 文件格式导出用户数据。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 选中与要导出其数据的用户对应的复选框。

步骤 3 点击**导出所选 (Export Selected)**。

步骤 4 在 Key 字段中输入加密密码的密钥。

步骤 5 点击**开始导出 (Start Export)** 创建 users.csv 文件。

步骤 6 点击**确定 (OK)** 导出 users.csv 文件。

导入思科 ISE 内部用户

您可以使用 csv 文件将新用户数据导入 ISE 以创建新的内部帐户。可以在可导入用户帐户的页面上下载模板 csv 文件。您可以在以下位置导入用户： **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。 发起人可以在发起人门户上导入用户。“发起人门户指南”可以告诉发起人如何导入访客帐户。 请参阅 为创建发起人帐户配置帐户内容， 了解有关配置发起人访客帐户使用的信息类型的信息。

注释 如果 csv 文件包含自定义属性，则在导入期间，您为自定义属性设置的数据类型和允许范围将应用于自定义属性值。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 点击**导入 (Import)**，从逗号隔开的文本文件导入用户。

如果没有逗号分隔的文本文件，请点击**生成模版 (Generate a Template)**，以创建已填充标题行的 csv 文件。

步骤 3 在文件 (File) 文本框中，输入包含要导入的用户的文件名，或者点击**浏览 (Browse)**，导航至文件所在位置。

步骤 4 如果想要创建新的用户和更新现有用户，请选中**以新数据创建新用户和更新现有用户 (Create new user(s) and update existing user(s) with new data)** 复选框。

步骤 5 点击**保存 (Save)**，将更改保存到Cisco ISE 内部数据库。

注释 我们建议您不要一次性删除所有网络访问用户，因为这可能会导致 CPU 使用率达到峰值和服务崩溃，尤其是在使用一个非常大的数据库时。

终端设置

下表介绍**终端 (Endpoints)** 窗口上的字段，您可以使用此窗口创建终端和为终端分配策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *10:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的MAC地址以静态创建终端。 MAC 地址是连接到启用Cisco ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在 Endpoints 页面静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。

字段名称	使用指南
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

字段名称	使用指南

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	Cisco ISE 包括以下系统创建的终端身份组：
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 221 页
使用策略和身份的静态分配创建终端，第 217 页

从 LDAP 设置导入终端

下表介绍“从 LDAP 导入”(Import from LDAP) 窗口上的字段，您可以使用此窗口从 LDAP 服务器导入终端。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *11:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 Cisco ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。

字段名称	使用指南
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在Cisco ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与Cisco ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间（单位：秒），值介于 1 和 60 秒之间。

相关主题

已识别的终端，第 221 页
从 LDAP 服务器导入终端，第 220 页

身份组操作

创建用户身份组

您必须创建用户身份组，才能为其分配用户。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **身份组 (Identity Groups)** > **用户身份组 (User Identity Groups)** > **添加 (Add)**。

您还可以用另一种方法创建用户身份组，访问 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **用户身份组 (User Identity Groups)** > **身份组 (Identity Groups)** > **用户身份组 (User Identity Groups)** > **添加 (Add)** 页面。

步骤 2 在 名称 字段和 描述 字段输入相应值。“名称”(Name) 字段支持的字符为空格 # $ & ‘ ( ) * + - . / @ _。

步骤 3 点击**提交 (Submit)**。

相关主题

用户身份组，第 17 页

导出用户身份组

Cisco ISE 允许您以 csv 文件格式导出本地配置的用户身份组。

步骤 1 选择**管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 身份组 (Identity Groups) > 用户身份组 (User Identity Groups)**。

步骤 2 选中想要导出的用户身份组对应的复选框，点击**导出 (Export)**。

步骤 3 点击**确定 (OK)**。

导入用户身份组

Cisco ISE 允许以 CSV 文件的形式导入用户身份组。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **身份组 (Identity Groups)** > **用户身份组 (User Identity Groups)**。

步骤 2 点击**生成模板 (Generate a Template)** 获取用于导入文件的模板。

步骤 3 点击“导入”(Import)以从逗号分隔的文本文件导入网络访问用户。

步骤 4 如果您想要同时添加新用户身份组并更新现有用户身份组，请选中 **用新数据覆盖现有数据 (Overwrite existing data with new data)** 复选框。

步骤 5 点击**导入 (Import)**。

步骤 6 点击**保存 (Save)** 以将您的更改保存至Cisco ISE 数据库。

终端身份组设置

下表介绍“终端身份组”(Endpoint Identity Groups) 窗口上的字段，您可以使用此窗口创建终端组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

表 *12*: 终端身份组设置

字段名称	使用指南
名称	输入您要创建的终端身份组的名称。
说明	输入对您要创建的终端身份组的说明。
Parent Group	从 Parent Group 下拉列表选择您要关联新创建的终端身份组的终端身份组。

相关主题

已识别终端划分为终端身份组，第 224 页
创建终端身份组，第 223 页

配置最大并发会话数

为了获得最佳性能，您可以限制并发用户会话的数量。您可以在用户级别或组级别上设置限制。系统根据最大用户会话配置，将会话计数应用于用户。

您可以为每个 ISE 节点的每个用户配置最大并发会话数。超过此限制的会话将被拒绝。

步骤 1 选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话数 (Max Sessions) > 用户 (User)**。

步骤 2 执行以下操作之一：

- 输入**每个用户最大会话数 (Maximum Sessions per User)** 字段中允许的每个用户的最大并发会话数。

  或

- 如果您希望用户拥有无限会话，请选中**无限会话 (Unlimited Sessions)** 复选框。默认情况下，此选项已选中。

步骤 3 点击**保存 (Save)**。

如果在用户和组级别上配置最大会话数，则较小的值将具有优先级。例如，如果用户的最大会话值设置为 10，用户所属组的最大会话值设置为 5，则用户最多只能有 5 个会话。

组的最大并发会话数

您可以配置身份组的最大并发会话数。

有时，组中的几个用户可以使用所有会话。其他用户创建新会话的请求被拒绝，因为会话数已达到配置的最大值。Cisco ISE 允许您为组中的每个用户配置最大会话限制；属于特定身份组的每个用户能够打开的会话数不可超过该会话限制，无论同一组的其他用户打开了多少会话。当计算特定用户的会话限制时，最低配置值优先 - 无论每个用户的全局会话限制、用户所属的每个身份组的会话限制或组中每个用户的会话限制为何。

要为身份组配置最大并发会话数，请执行以下操作：

步骤 1 请选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话 (Max Sessions) > 组 (Group)**。

列出所有已配置的身份组。

步骤 2 点击要编辑的组旁边的编辑 (Edit) 图标，然后输入以下内容的值：

- 该组允许的并发会话的最大数。如果一个组的最大会话数设置为 100，则该组的所有成员建立的所有会话总数不能超过 100。

  注释 组级别会话限制基于组层次结构而实施。

- 该组中每个用户允许的最大并发会话数。此选项将覆盖组的最大会话数。

如果要将组的最大并发会话数或组中用户的最大并发会话数设置为无限制，请将**组的最大会话数/组中用户的最大会话数 (Max Sessions for Group/Max Sessions for User in Group)** 字段留空，点击勾选图标，然后点击“保存”(Save)。默认情况下，这两个值都设置为无限制。

步骤 3 点击**保存 (Save)**。

配置计数器时间限制

您可以为并发用户会话配置超时值。

步骤 1 选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话数 (Max Sessions) > 计数器时间限制 (Counter Time Limit)**。

步骤 2 选择以下选项之一：

- **无限 (Unlimited)**：如果您不想为会话设置任何超时或时间限制，请选中此复选框。
- **删除会话前等待 (Delete sessions after)**：您可以输入并发会话的超时值（分钟、小时或天）。当会话超过时间限制时，Cisco ISE 会从计数器中删除会话，并更新会话计数，从而允许新的会话。用户的会话超过时间限制时，并不会注销用户。

步骤 3 点击**保存 (Save)**。

您可以从 RADIUS 实时日志 (RADIUS Live Logs) 页面重置会话计数。点击身份 (Identity)、身份组 (Identity Group) 或服务器 (Server) 列上显示的操作 (Actions) 图标以重置会话计数。当您重设会话时，会话从计数器中删除（从而允许新的会话）。当会话从计数器中删除时，用户不会断开连接。

帐户禁用策略

Cisco ISE 为用户和管理员引入了帐户禁用策略，以实现与 Cisco Secure ACS 同等的功能。对用户或管理员进行身份验证或查询时，Cisco ISE 会在**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户身份验证设置 (User Authentication Settings)** 页面中检查全局帐户禁用策略设置，并根据配置进行身份验证或返回结果。

Cisco ISE 会验证以下三个策略：

- 禁用超过指定日期 (yyyy-mm-dd) 的用户帐户 - 在指定日期禁用用户帐户。但是，在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 帐户禁用策略 (Account Disable Policy)** 中为单个网络访问用户配置的帐户禁用策略设置优先于全局设置。
- 在帐户创建或最后一次启用 *n* 天后禁用用户帐户 - 在帐户创建或帐户最后一次处于活动状态的日期过去指定天数后禁用用户帐户。您可以在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 状态 (Status)** 中检查用户状态。

- 处于非活动状态 *n* 天后禁用帐户 - 禁用在配置的连续天数内尚未进行身份验证的管理员和用户帐户。

从Cisco Secure ACS 迁移至Cisco ISE 后，为Cisco安全 ACS 中的网络访问用户指定的帐户禁用策略设置迁移至Cisco ISE。

禁用单个用户帐户

如果禁用帐户日期超过管理员用户指定的日期，Cisco ISE 允许您禁用每个用户的用户帐户。

步骤 1 依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)**。

步骤 2 点击**添加 (Add)** 创建新用户或者选中现有用户旁边的复选框并点击**编辑 (Edit)** 编辑现有用户的详细信息。

步骤 3 选中**禁用帐户，如果日期超出 (Disable account if the date exceeds)** 复选框并选择日期。

此选项允许您在已配置日期超出用户级别时禁用用户帐户。您可以根据需要为不同用户配置不同的到期日期。此选项将否决每个用户的全局配置。已配置日期可以是当前系统日期或未来日期。

注释 不允许输入早于当前系统日期的日期。

步骤 4 点击**提交 (Submit)** 配置个人用户帐户的帐户禁用策略。

全局禁用用户帐户

您可以在特定日期、超过帐户创建日期或最后一次访问日期一定天数后，以及帐户处于非活动状态一定天数后，禁用用户帐户。

步骤 1 依次选择**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户身份验证设置 (User Authentication Settings) > 帐户禁用策略 (Account Disable Policy)**。

步骤 2 执行下列操作之一：

- 选定**如果日期超过...则禁用帐户 (Disable account if date exceeds)** 复选框，并按照 yyyy-mm-dd 格式选择合适的日期。通过该选项，您可以在用户帐户超过设定的日期时，禁用该帐户。用户级别的**如果日期超过...则禁用帐户 (Disable account if date exceeds)** 设置优先于此全局配置。
- 选定**在帐户创建 n 天后或最后一次启用后禁用帐户 (Disable account after n days of account creation or last enable)** 复选框，并输入天数。此选项在帐户创建日期或最后一次访问的日期超过指定天数时禁用用户帐户。管理员可以手动启用已禁用的用户帐户，这会重置天数计数。
- 选定**在 n 天不活跃之后禁用帐户**复选框，并输入天数。此选项在帐户不活跃天数超过指定天数时禁用用户帐户。

步骤 3 点击**提交 (Submit)** 配置全局帐户禁用策略。

内部和外部身份源

身份源是存储用户信息的数据库。Cisco ISE 在身份验证期间使用身份源中的用户信息来验证用户凭证。用户信息包括组信息和与用户关联的其他属性。您可以添加、编辑以及从身份源删除用户信息。

Cisco ISE 支持内部和外部身份源。您可以使用两个来源对发起人和访客用户进行身份验证。

内部身份源

Cisco ISE 有一个内部用户数据库，可用来存储用户信息。内部用户数据库中的用户称为内部用户。Cisco ISE 还有一个内部终端数据库，存储关于所有设备以及与其相连的终端的信息。

外部身份源

Cisco ISE 允许您配置包含用户信息的外部身份源。Cisco ISE 连接外部身份源，获取身份验证所需的用户信息。外部身份源还包括Cisco ISE 服务器的证书信息以及证书身份验证配置文件。Cisco ISE 使用身份验证协议与外部身份源进行通信。

为内部用户配置策略时，请注意以下几点：

- 配置身份验证策略，以根据内部身份存储区对内部用户进行身份验证。
- 通过选择以下选项为内部用户组配置授权策略：

  `Identitygroup.Name EQUALS User Identity Groups:` **`Group_Name`**

下表列出了身份验证协议以及它们支持的外部身份源。

表 *13:* 身份验证协议和支持的外部身份源

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	REST
EAP-GTC，PAP（纯文本密码）	支持	支持	支持	支持	支持
MS-CHAP 密码散列： MSCHAPv1/v2 EAP-MSCHAPv2（作为 PEAP、EAP-FAST、EAP-TTLS 或 TEAP 的内部方法） LEAP	支持	支持	不支持	否	否

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	REST
EAP-MD5 CHAP	支持	不支持	否	否	否
EAP-TLS PEAP-TLS （证书检索） 注释 对于 TLS 身份验证（EAP-TLS 和 PEAP-TLS），身份源不是必需的，但是可以选择为授权策略条件添加。	不支持	支持	支持	不支持	否

凭证的存储方式不同，具体取决于外部数据源连接类型和使用的功能。

- 当加入 Active Directory 域（但不用于被动 ID）时，不会保存用于加入的凭证。CiscoISE会创建AD计算机帐户（如果不存在），并使用该帐户对用户进行身份验证。
- 对于 LDAP 和被动 ID，用于连接到外部数据源的凭证也用于对用户进行身份验证。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务提供程序，第 84 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅将 Active Directory 用作外部身份源，第 33 页。

- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅 LDAP，第 123 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅 RADIUS 令牌身份源，第 144 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅 RSA 身份源，第 150 页。
- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅 SAMLv2 身份提供者作为外部身份源，第 156 页。
- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录。

利用外部身份存储密码验证内部用户

Cisco ISE 允许您利用外部身份存储密码验证内部用户。Cisco ISE 可通过以下页面为内部用户提供选择密码身份存储的选项：**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)** 页面。在“用户”(Users) 页面添加或编辑用户时，管理员可以从Cisco ISE 外部身份源列表中选择身份存储。内部用户的默认密码身份存储为内部身份存储。Cisco Secure ACS 用户在从 Cisco Secure ACS 迁移至Cisco ISE 过程中及之后将会保持相同的密码身份存储。

Cisco ISE 支持以下密码类型的外部身份存储：

- Active Directory
- LDAP
- ODBC
- RADIUS 令牌服务器
- RSA SecurID 服务器

证书身份验证配置文件

对于每个配置文件，必须指定应用作主体用户名的证书字段，以及是否希望对证书进行二进制比较。

添加证书身份验证配置文件

您必须创建证书验证配置文件，如果您想要使用可扩展身份验证协议 - 传输层安全 (EAP-TLS) 基于证书的身份验证方法，即必须创建证书身份验证配置文件。Cisco ISE 不是通过传统的用户名与密码方法进行身份验证，而是将从客户端接收的证书与服务器中的证书进行比较，从而验证用户的身份。

开始之前

您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **证书身份验证配置文件 (Certificate Authentication Profile)** > **添加 (Add)**。

步骤 2 为证书身份验证配置文件输入名称和可选说明。

步骤 3 从下拉列表中选择身份库。

基本证书检查不需要使用身份源。如果希望对证书进行二进制比较，就必须选择身份源。如果您选择 Active Directory 作为身份源，使用者和通用名称以及使用者替代名称（所有值）都可用于查找用户。

步骤 4 从**证书属性**或**证书中的任何主体或备选名称属性**中选择身份的使用。此身份将用于日志以及查找。

如果选择**证书中的任何主体或备选名称属性**，则 Active Directory UPN 将用作日志的用户名，并将尝试使用证书中的所有主体名称和备选名称来查找用户。只有选择 Active Directory 作为身份源时，此选项才可用。

步骤 5 如果您想要将客户端证书与身份库中的证书进行匹配，请选择 **Match Client Certificate Against Certificate In Identity Store**。为此，您必须选择身份源（LDAP 或 Active Directory）。如果您选择 Active Directory，您可以选择仅为解决身份不明情况而匹配证书。

- **从不 (Never)**：此选项从不执行二进制比较。
- **仅用于解决身份模糊 (Only to resolve identity ambiguity)**：此选项仅在遇到身份不明情况时，才将客户端证书与 Active Directory 中帐户的证书进行二进制比较。例如，系统发现若干个 Active Directory 帐户与证书中的身份名称匹配，就属于身份不明情况。
- **始终执行二进制比较 (Always perform binary comparison)**：此选项始终将客户端证书与身份库（Active Directory 或 LDAP）中帐户的证书进行二进制比较。

步骤 6 点击**提交 (Submit)** 以添加证书身份验证配置文件或保存更改。

将 Active Directory 用作外部身份源

Cisco ISE 使用 Microsoft Active Directory 作为外部身份源以访问用户、设备、组和属性等资源。Active Directory 中的用户和设备身份验证仅允许对 Active Directory 中列出的用户和设备进行网络访问。

ISE 社区资源

使用 AD 凭证的 ISE 管理门户访问配置示例

支持 Active Directory 的身份验证协议和功能

Active Directory 支持使用某些协议对用户和设备进行身份验证、更改 Active Directory 用户密码等功能。下表列出了 Active Directory 支持的身份验证协议及相应功能。

表 *14: Active Directory* 支持的身份验证协议

身份验证协议	功能
EAP-FAST 和基于密码的受保护的可扩展身份验证协议 (PEAP)	用户和设备身份验证，能够使用 EAP-FAST 和 PEAP 结合 MS-CHAPv2 和 EAP-GTC 的内部方法更改密码
密码身份验证协议 (PAP)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)	用户和设备身份验证
可扩展身份验证协议 - 通用令牌卡 (EAP-GTC)	用户和设备身份验证
可扩展身份验证协议 - 传输层安全 (EAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
可扩展身份验证协议 - 通过安全隧道的灵活身份验证-传输层安全 (EAP-FAST-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
受保护的可扩展身份验证协议 - 传输层安全 (PEAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
轻型可扩展身份验证协议 (LEAP)	用户身份验证

用于授权策略的 Active Directory 属性和组检索

Cisco ISE 从 Active Directory 检索用户或设备属性和组以用于授权策略规则。这些属性可用于Cisco ISE 策略并且决定了用户或设备的授权级别。Cisco ISE 在身份验证成功后会检索用户和设备 Active Directory 属性，还可以为与身份验证无关的授权检索属性。

Cisco ISE 可以使用外部身份存储区中的组来为用户或计算机分配权限；例如，将用户映射到发起人组。请注意 Active Directory 中的以下组成员身份限制：

- 策略规则条件可引用以下任意组：用户或计算机的主要组、用户或计算机作为直接成员的组，或者间接（嵌套）组。

- 不支持在用户或计算机的帐户域外的域本地组。

注释 您可以使用 Active Directory 属性 (msRadiusFramedIPAddress) 的值作为 IP 地址。可将此 IP 地址发送给授权配置文件中的网络接入服务器 (NAS)。msRADIUSFramedIPAddress 属性仅支持 IPv4 地址。在进行用户身份验证时，为用户获取的 msRadiusFramedIPAddress 属性值将转换为 IP 地址格式。

系统按加入点检索和管理属性和组。这些属性和组将用于授权策略（方法是首先选择加入点，然后选择属性）。您无法按范围为授权定义属性或组，但可以对身份验证策略使用范围。当您在身份验证策略中使用范围时，可以通过一个加入点对用户进行身份验证，但要通过另一个具有用户帐户域信任路径的加入点检索属性和/或组。您可以使用身份验证域来确保一个范围中的任两个加入点在身份验证域中都没有任何重叠。

注释 在多加入点配置的授权过程中，Cisco ISE 会按照加入点在授权策略中列出的顺序搜索它们，直到找到特定用户才会停止。找到用户后，在加入点中分配给用户的属性和组将用于评估授权策略。

注释 请参阅 Microsoft 对可用 Active Directory 组施加的最大数量限制： http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

如果规则包含带有特殊字符（例如 /、!、@、\、#、$、%、^、&、*、(、)、_、+ 或 ~）的 Active Directory 组名称，则授权策略会失败。

如果管理员用户名包含 $ 字符，则通过 Active Directory 进行的管理员用户登录可能会失败。

使用显式 UPN

要在将用户信息与 Active Directory 的用户主体名称 (UPN) 属性进行匹配时降低模糊性，您必须将 Active Directory 配置为使用显式 UPN。如果两个用户具有相同的 *sAMAccountName* 值，则使用显式 UPN 可能会产生模糊结果。

要在 Active Directory 中设置显式 UPN，请打开**高级调整**页面，并将属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* 设置为 1。

支持 Boolean 属性

Cisco ISE 支持从 Active Directory 和 LDAP 身份库中检索 Boolean 属性。

在配置 Active Directory 或 LDAP 的目录属性时，您可以配置 Boolean 属性。一旦使用 Active Directory 或 LDAP 进行身份验证，即可检索这些属性。

Boolean 属性可用于配置策略规则条件。

可从 Active Directory 或 LDAP 服务器抓取作为字符串类型的 Boolean 属性值。Cisco ISE支持以下 Boolean 属性值：

Boolean 属性	支持的值
真	t、T、true、TRUE、True、1
错误	f、F、false、FALSE、False、0

注释 Boolean 属性不支持属性替代。

如果您将 Boolean 属性（例如 msTSAllowLogon）配置为字符串类型，则 Active Directory 或 LDAP 服务器中该属性的 Boolean 值是为Cisco ISE 中字符串属性设置的。您可以将属性类型更改为 Boolean 或将该属性作为 Boolean 类型进行手动添加。

基于证书的身份验证的 Active Directory 证书检索

Cisco ISE 支持为使用 EAP-TLS 协议的用户和设备身份验证检索证书。Active Directory 上的用户或设备记录包括二进制数据类型的证书属性。此证书属性可以包含一个或多个证书。Cisco ISE 将此属性标识为 userCertificate，并且不允许为此属性配置任何其他名称。Cisco ISE 会检索此证书并将其用于执行二进制比较。

证书身份验证配置文件决定从哪个字段（例如 Subject Alternative Name (SAN) 或 Common Name 字段）获取用户名以在 Active Directory 中查找用于检索证书的用户。Cisco ISE 检索到证书后，会将此证书与客户端证书进行二进制比较。当接收到多个证书时，Cisco ISE 会对这些证书进行比较以确定相匹配的证书。找到匹配的证书后，则用户或设备身份验证通过。

Active Directory 用户身份验证流程

当对用户进行身份验证或查询时，Cisco ISE 会检查以下内容：

- MS-CHAP 和 PAP 身份验证会检查用户是否被禁用、锁定、过期或者登录超时，如果上述任一条件为真，则身份验证失败。
- EAP-TLS 身份验证会检查用户是否被禁用或锁定，如果满足上述任一条件，则身份验证失败。

配置资源所有者密码凭证流以使用 Azure Active Directory 对用户进行身份验证

注意 Cisco ISE 中的资源所有者密码凭证 (ROPC) 流是一种受控引入功能。我们建议您在生产环境中使用此功能之前，在测试环境中全面测试此功能。

资源所有者密码凭证 (ROPC) 是一种 OAuth 2.0 授予类型，允许Cisco ISE 使用基于云的身份提供程序在网络中执行授权和身份验证。

通过 ROPC 流，Cisco ISE 使用基于云的身份源验证用户的凭证。ROPC 流支持明文身份验证协议。Cisco ISE 目前通过 ROPC 流支持 Azure Active Directory。

在 Azure Active Directory 中为资源所有者密码凭证流配置应用

步骤 1 登录到 Azure 门户。

步骤 2 点击顶部导航栏中的**目录+应用 (Directory+Application)** 过滤器图标。选择必须向其添加支持 ROPC 的应用的 Azure Active Directory 租户。

步骤 3 使用搜索栏查找并选择**应用注册 (App Registrations)**。

步骤 4 点击 **+ 新注册 (+ New Registration)**。

步骤 5 在显示的**注册应用 (Register an Application)** 窗口中，在**名称 (Name)** 字段中为此应用输入有意义的名称。

步骤 6 在**支持的帐户类型 (Supported account types)** 区域中，点击**仅此组织目录中的帐户 (Accounts in this organizational directory only)**。

步骤 7 点击**注册**。

步骤 8 在显示的新窗口中，点击左侧菜单窗格中的**证书和密钥 (Certificates & Secrets)**。

步骤 9 在**客户端密钥 (Client Secrets)** 区域中，点击 **+ 新客户端密钥 (+ New Client Secret)**。

步骤 10 在显示的**添加客户端密钥 (Add a Client Secret)** 对话框中，在**说明 (Description)** 字段中输入说明。

步骤 11 在**到期 (Expiry)** 区域中，点击**从不 (Never)**。

步骤 12 点击**添加 (Add)**。

步骤 13 点击复制到剪贴板图标以复制共享密钥。在Cisco ISE 中配置 ROPC 流时，需要此值。

步骤 14 点击左侧菜单窗格中的**概述 (Overview)**，然后在配置 ROPC 流时复制以下值以在Cisco ISE 中使用。

- 应用（客户端）ID。
- 目录（租户）ID。

步骤 15 要为此应用启用 ROPC 流，请点击左侧菜单窗格中的**身份验证 (Authentication)**。在**高级设置 (Authentication)** 区域中，确保切换按钮设置为**是 (Yes)**。

步骤 16 要向应用添加组声明，请点击左侧菜单窗格中的**令牌配置 (Token Configuration)**。

步骤 17 点击 **+ 添加组声明 (+ Add Groups Claim)**。

步骤 18 在**编辑组声明 (Edit Groups Claim)** 对话框中，选中**安全组 (Security groups)** 复选框。

步骤 19 点击**保存 (Save)**。

步骤 20 要启用 API 的使用，请点击左侧菜单窗格中的 **API 权限 (API Permissions)**。

步骤 21 点击 **+ 添加权限 (+ Add A Permission)**。

步骤 22 在 **Microsoft API** 区域中，点击 **Microsoft Graph**。

步骤 23 点击**应用权限 (Application Permissions)**。

步骤 24 在**组 (Group)** 下拉区域中，选中 **Group.Read.All** 复选框。

步骤 25 点击**添加权限 (Add Permissions)**。

步骤 26 点击为 **<user>** 授予管理员同意，然后点击是 **(Yes)**。

在思科 ISE 中配置资源所有者密码凭证流

开始之前

在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后依次选择 **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **受信任证书 (Trusted Certificates)**。检查 **DigiCert Global Root G2** 是否显示在受信任证书列表中。

如果此证书在受信任证书存储区中不可用，请将 PEM 格式的公共根证书 DigiCert Global Root G2 导入Cisco ISE 受信任证书存储区。

请参阅 https://www.digicert.com/kb/digicert-root-certificates.htm。

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **REST ID 存储设置 (REST ID Store Settings)**。

步骤 2 点击已启用 **(Enabled)**，然后点击提交 **(Submit)**。

步骤 3 在 ISE 节点中通过以下 CLI 命令验证 REST 身份验证服务的状态：

```
show application status ise
```

如果响应中显示消息 **REST 身份验证服务正在运行 (REST Auth Service running)**，则表明已成功启用 REST ID 存储设置。现在可以继续配置 ROPC 流。

步骤 4 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **REST (ROPC)**。

步骤 5 点击添加 **(Add)**。

步骤 6 在显示的新窗口中，在名称 **(Name)** 字段中输入值。

步骤 7 从 **REST 身份提供程序 (REST Identity Provider)** 下拉列表中，选择要配置的身份源。

步骤 8 对于字段客户端 **ID (Client ID)**、客户端密钥 **(Client Secret)** 和租户 **ID (Tenant ID)**，通过在先前任务中配置 Azure Active Directory 时保存的信息输入所需值。

步骤 9 点击测试连接 **(Test Connection)** 以检查Cisco ISE 能否连接到所选身份源。

步骤 10 点击加载组 **(Load Groups)** 以从连接的身份源导入用户组。然后可以从组 **(Groups)** 下拉列表中选择特定组。

步骤 11 （可选）在用户名后缀 **(Username Suffix)** 字段中输入值，以按用户名对 Azure Active Directory 租户的用户进行身份验证。

例如，如果用户的 Azure Active Directory 用户专用名称 (UPN) 为 *example@myTest.onMicrosoft.com*，则后缀为分隔符，域名为 *@ myTest.onMicrosoft.com*。

步骤 12 点击提交 **(Submit)**。

支持 Active Directory 多域林

Cisco ISE 支持带多域林的 Active Directory。在每个林中，Cisco ISE 连接到单个域，但如果在Cisco ISE 连接到的域与其他域之间建立信任关系，则可从 Active Directory 林中的其他域访问资源。

请参阅Cisco身份服务引擎的版本说明，以获取支持 Active Directory 服务的 Windows 服务器操作系统列表。

注释 思科 ISE 不支持位于网络地址转换器背后并具有网络地址转换 (NAT) 地址的 Microsoft Active Directory 服务器。

Active Directory 与思科 ISE 集成的先决条件

本节介绍配置 Active Directory 以与Cisco ISE 集成所需的手动步骤。但是，在大多数情况下，可以启用Cisco ISE 来自动配置 Active Directory。以下是将 Active Directory 与Cisco ISE 集成的先决条件。

- 确保您拥有对 AD 域配置进行更改所需的 Active Directory 域管理员凭证。
- 确保您在Cisco ISE 中具有超级管理员或系统管理员权限。
- 使用网络时间协议 (NTP) 服务器设置来同步Cisco ISE 服务器和 Active Directory 之间的时间。您可以从Cisco ISE CLI 配置 NTP 设置。
- Cisco ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。如果要从特定加入点查询其他域，请确保加入点和其他具有需要访问的用户和计算机信息的域之间存在信任关系。如果信任关系不存在，您必须为不受信任的域创建另一个加入点。有关建立信任关系的详细信息，请参阅 Microsoft Active Directory 文档。
- 您必须在Cisco ISE 加入到的域中具有至少一个可由Cisco ISE 运行并访问的全局目录服务器。

执行各种操作所需的 Active Directory 帐户权限

加入操作	退出操作	Cisco ISE 机器账户
加入操作需要以下帐户权限： • 搜索 Active Directory（以查看Cisco ISE 机器账户是否存在） • 将Cisco ISE 机器账户创建到域（如果机器账户尚不存在） • 在新机器账户上设置属性（例如，Cisco ISE 机器账户密码、SPN、dnsHostname） 不必是域管理员即可执行加入操作。	退出操作需要以下帐户权限： • 搜索 Active Directory（以查看Cisco ISE 机器账户是否存在） • 从域中删除Cisco ISE 机器帐户 如果执行强制退出（在没有密码的情况下退出），则不会从域中删除计算机帐户。	用于传达到 Active Directory 连接的Cisco ISE 机器帐户需要以下权限： • 更改密码 • 读取与已身份验证的用户和机器对应的用户和机器对象。 • 查询 Active Directory 以获取信息（例如，受信任域和替代 UPN 后缀等） • 读取 tokenGroups 属性 可以在 Active Directory 中预创建机器帐户。如果 SAM 名称与 Cisco ISE 设备主机名匹配，则应在加入操作期间找到该名称并重复使用。 如果具有多个加入操作，则会在 Cisco ISE 中维护多个机器帐户，每个加入操作对应一个账户。

注释 用于加入或退出操作的凭证不存储在Cisco ISE 中。仅存储新创建的Cisco ISE 机器帐户凭证。

Microsoft Active Directory 中的**网络访问权限：限制允许远程调用 SAM 的客户端**安全策略已修改。因此，Cisco ISE 可能无法每 15 天更新一次其机器帐户密码。如果机器帐户密码未更新，Cisco ISE 不会再通过 Microsoft Active Directory 对用户进行身份验证。您将在Cisco ISE 控制板上收到 **AD: ISE 密码更新失败 (AD: ISE password update failed)** 警报，以通知您此事件。

安全策略可使用户枚举本地安全帐户管理器 (SAM) 数据库和 Microsoft Active Directory 中的用户和组。要确保Cisco ISE 可更新其机器帐户密码，请检查 Microsoft Active Directory 中的配置是否正确。有关受影响的 Windows 操作系统和 Windows Server 版本的详细信息，包括这对您的网络意味着什么、可能需要哪些更改，请参阅：

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

必须开放用于通信的网络端口

协议	端口（远程-本地）	目标	已通过身份验证	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	否	-
MSRPC	445	域控制器	支持	-
Kerberos (TCP/UDP)	88	域控制器	是 (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	支持	-
LDAP (GC)	3268	全局目录服务器	支持	-
NTP	123	NTP 服务器/域控制器	否	-
IPC	80	部署中的其他 ISE 节点	是（使用 RBAC 凭证）	-

DNS 服务器

在配置您的 DNS 服务器时，请确保注意以下事项：

- 您在Cisco ISE 中配置的 DNS 服务器必须能够解析要使用的域的所有正向和反向 DNS 查询。
- 建议使用权威 DNS 服务器来解析 Active Directory 记录，因为 DNS 递归可能会导致延迟并对性能造成重大不利影响。
- 所有 DNS 服务器都必须能够对 DC、GC 和 KDC（无论它们是否具有额外的站点信息）的 SRV 查询作出应答。
- Cisco建议向 SRV 响应添加服务器 IP 地址以提高性能。
- 避免使用查询公共互联网的DNS服务器。当必须解析未知名称时，这些服务器可能会泄漏有关网络的信息。

将 Active Directory 配置为外部身份源

在功能部件（例如 Easy Connect 和 被动 ID 工作中心）的配置过程中将 Active Directory 配置为外部身份源。有关这些功能部件的详细信息，请参阅 Easy Connect，第 72 页 和 被动 ID 工作中心，第 76 页。

在您将 Active Directory 配置为外部身份源之前，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。
- 您拥有 ISE 的超级管理员或系统管理员权限。

注释 如果在思科 ISE 连接到 Active Directory 时发现操作问题，请参阅**操作** > **报告** 下的“AD 连接器操作报告”(AD Connector Operations Report)。

您必须执行以下任务，从而将 Active Directory 配置配为外部身份源。

1. 添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点， 第 42 页
2. 配置身份验证域， 第 47 页
3. 配置 Active Directory 用户组， 第 48 页
4. 配置 Active Directory 用户和计算机属性， 第 49 页
5. （选件）修改密码更改、设备身份验证和设备访问限制设置， 第 49 页

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

开始之前

确保Cisco ISE 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。您可以通过运行域诊断工具来检查这些参数。

必须创建加入点才能使用 Active Directory 以及使用被动 ID 工作中心的代理、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 节点配置 IPv6 地址。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **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**，则保存配置将会全局保存 Active Directory 域配置（在主策略服务节点和辅助策略服务节点中），但不会将任何 ISE 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)**，或者从左侧的导航窗格中点击新的 Active Directory 加入点。系统将显示部署加入/退出表，其中包含所有Cisco ISE 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Cisco ISE 节点旁边的复选框，然后点击**加入 (Join)** 将Cisco ISE 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Cisco ISE 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Cisco ISE 节点，则应对每个Cisco ISE 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。

强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存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Cisco ISE 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。Cisco ISE 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，Cisco ISE 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。

注释 加入完成后，Cisco ISE 将更新其 AD 组和对应的 SID。Cisco ISE 自动启动 SID 更新过程。您必须确保允许此过程完成。

注释 如果缺少 DNS SRV 记录，您可能无法将Cisco ISE 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）。有关故障排除信息，请参阅以下 Microsoft Active Directory 文档：

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

注释 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)。

下一步做什么

配置 Active Directory 用户组，第 48 页

配置身份验证域。

添加域控制器

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **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Cisco ISE 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的域控制器 (DC)，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”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。有关详细信息，请参阅Active Directory 设置，第 81 页。

c) 如果选择 WMI 协议，请点击**配置 (Configure)**以自动配置 WMI，然后点击**测试 (Test)** 以测试连接。有关自动配置 WMI 的详细信息，请参阅对被动 ID 配置 WMI，第 46 页。

DC 故障转移机制根据 DC 优先级列表进行管理，该列表确定在故障转移情况下选择 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）。

注释 思科 ISE 不支持将只读域控制器用于身份验证流程。

用于被动 ID 的 MSRPC 协议

从Cisco ISE 版本 3.0 开始，可以将 MS-Eventing API 或 MSRPC（Microsoft 远程过程调用）协议用于被动身份。MSRPC 协议用于在Cisco ISE 中的节点之间建立节点通信并监控心跳。除 WMI 协议外，此选项也可用。

当Cisco ISE 或Cisco ISE-PIC 从多个域控制器收集或监控事件时，MSRPC 协议可提供一种可靠机制。它还可减少 Active Directory 域控制器用户登录事件的延迟。

对于Cisco ISE 3.0 及更高版本，MSRPC 是默认协议。建议您为 MSPRC 的高可用性功能启用主代理和辅助代理，以便在主代理安装的服务器发生故障时，辅助代理变为活动状态并监控域控制器。

也可以在创建代理时选择对 MSPRC 使用独立选项。但是，如果代理故障并且无法监控 DC 事件，辅助代理不会备份独立代理。

从Cisco ISE 2.x 升级到 3.0 版本时，如果使用现有代理更新成员服务器，则代理版本将在**代理 (Agents)** 窗口的**版本 (Version)** 列中显示 2.0.0.1。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **被动 ID (Passive ID)** > **提供程序 (Providers)** > **代理 (Agents)**。

为 MSRPC 部署代理

开始之前

启用被动身份服务。为此：

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后选中部署节点旁的复选框。点击**编辑 (Edit)**。在**编辑节点 (Edit Node)** 窗口中，选中**启用被动身份服务 (Enable Passive Identity Service)** 复选框并点击**保存 (Save)**。

在Cisco ISE-PIC GUI 中，选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后选中部署节点旁的复选框。点击**编辑 (Edit)**。在**编辑节点 (Edit Node)** 窗口中，选中**启用被动身份服务 (Enable Passive Identity Service)** 复选框并点击**保存 (Save)**。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **被动 ID (Passive ID)** > **提供程序 (Providers)** > **代理 (Agents)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**代理 (Agents)** 窗口中，如果要部署新代理，请点击**部署新代理 (Deploy New Agent)**，或者，如果要注册现有代理，请点击**注册现有代理 (Register Existing Agents)**。

如果选择**注册现有代理 (Register Existing Agent)** 选项，由于协议不受支持，因此可能会丢弃来自受支持注册客户端的请求。在这种情况下，需要使用支持的协议配置Cisco ISE 客户端。

步骤 4 在**名称 (Name)** 字段中输入名称。

步骤 5 在**主机 FQDN (Host FQDN)** 字段中输入主机 FQDN URL。

步骤 6 输入**用户名 (User Name)** 和**密码 (Password)**。

步骤 7 从**协议 (Protocol)** 下拉列表中选择 **MSRPC**。

步骤 8 点击**高可用性设置 (High Availability Settings)** 部分中的 **主 (Primary)**。

成功部署主代理后，应重复上述步骤，通过选择**高可用性设置 (High Availability Settings)** 部分中的**辅助 (Secondary)** 选项来部署辅助代理。在部署辅助代理时，应从**主代理 (Primary Agent)** 下拉列表中选择已配置的主代理。

步骤 9 点击 **Deploy**（部署）。

通过主代理映射域控制器

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **PassiveID** > **提供方 (Providers)** > **Active Directory**。

步骤 2 在 **Active Directory** 窗口中，点击**添加 (Add)**。

步骤 3 在**连接 (Connection)** 部分中，输入域控制器的**加入点名称 (Join Point Name)** 和 **Active Directory 域 (Active Directory Domain)**。

步骤 4 点击**提交 (Submit)**。

系统随即会显示以下消息：

是否要将所有 ISE 节点都加入到此 Active Directory 域？(Would you like to Join all ISE Nodes to this Active Directory Domain?)

步骤 5 点击**是 (Yes)** 以加入所有 ISE 节点。

步骤 6 在**加入域 (Join Domain)** 弹出窗口中，输入 **AD 用户名 (AD User name)** 和**密码 (Password)**。

步骤 7 点击**确定 (OK)**。

步骤 8 点击 **PassiveID** 选项卡。

步骤 9 在 **PassiveID 域控制器 (PassiveID Domain Controllers)** 窗口中，点击要映射的 ISE 域旁的复选框。

对于多个 DC 映射，可以通过**使用现有代理 (Use Existing Agent)** 选项选择现有代理。

步骤 10 点击**编辑 (Edit)**。

步骤 11 在**主机 FQDN (Host FQDN)** 字段中输入主机 FQDN URL。

步骤 12 在 **AD 用户名 (AD User Name)** 和**密码 (Password)** 字段中输入 AD 凭证。

步骤 13 从**协议 (Protocol)** 下拉列表中选择**代理 (Agent)**。

步骤 14 从**代理 (Agent)** 下拉列表中选择相应的代理（满足高可用性需求的**主要 (Primary)** 代理或**独立 (Standlone)** 代理）。

步骤 15 点击**保存 (Save)**。

在**控制板 (Dashboard)** 中可以查看代理映射状态、监控域控制器的代理以及代理角色。（ 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **PassiveID** > **概览 (Overview)**.）

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时会话 (Live Sessions)** 查看域控制器事件日志。

对被动 ID 配置 WMI

开始之前

确保您具有 Active Directory 域管理员凭证，这样才能对任何 AD 域配置进行更改。确保已在**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** 下对此节点启用被动 ID。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

图 *1:*

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Cisco ISE 节点、节点角色及其状态。有关详细信息，请参阅表 17: Active Directory 加入/退出窗口 ，第 82 页。

步骤 3 转至“被动 ID”选项卡，选中相关域控制器旁边的复选框，然后点击**配置 WMI** 以使 ISE 能够自动配置所选的域控制器。

要手动配置 Active Directory 和域控制器或对任何配置问题进行故障排除，请参阅Active Directory 与思科 ISE 集成的先决条件 ，第 39 页。

退出 Active Directory 域

如果不再需要从此 Active Directory 域或从此加入点对用户或机器进行身份验证，则可以退出 Active Directory 域。

从命令行界面重置Cisco ISE 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 Cisco ISE 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Cisco ISE 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Cisco ISE 主机名时，也建议您如此操作。

开始之前

如果您退出 Active Directory 域，但是仍然使用 Active Directory 作为身份验证的身份源（直接使用或作为身份源序列的一部分），则身份验证会失败。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **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Cisco ISE 节点、节点角色及其状态。

步骤 3 选中Cisco ISE 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Cisco ISE 数据库中删除机器账户。

如果输入 Active Directory 凭证，则Cisco ISE 节点将退出 Active Directory 域并从 Active Directory 数据库中删除Cisco ISE 机器账户。

注释 要从 Active Directory 数据库中删除思科 ISE 计算机帐户，此处提供的 Active Directory 凭证必须具有从域中删除计算机帐户的权限。

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Cisco ISE 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。

配置身份验证域

对于与其有信任关系的其他域，Cisco ISE 加入的域具有可视性。默认情况下，Cisco ISE 设置为允许依据所有可信任域进行身份验证。可以将与 Active Directory 部署的交互限制到身份验证域子集。通过配置身份验证域，可以为每个加入点选择特定域，以便仅对选择的域执行身份验证。身份验证域可以提高安全性，因为这些域指示Cisco ISE 仅对来自所选域（而不是来自加入点信任的所有域）的用户进行身份验证。身份验证域还可改善性能以及身份验证请求处理延迟，因为身份验证域限制搜索区域（即，将搜索帐户与传入用户名或身份匹配的范围）。这在传入用户名或身份不包含域标记（前缀或后缀）时尤为重要。由于上述原因，配置身份验证域是最佳实践，我们强烈推荐此最佳实践。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

步骤 2 点击 Active Directory 加入点。

步骤 3 点击 Authentication Domains 选项卡。

系统会显示一个表，其中包含受信任域列表。默认情况下，Cisco ISE 允许对所有受信任域执行身份验证。

步骤 4 要仅允许指定域，请取消选中 Use all Active Directory domains for authentication 复选框。

步骤 5 选中想要允许对其执行身份验证的域旁边的复选框，并点击 Enable Selected。在身份验证 (Authenticate) 列中，此域的状态会更改为“是”(Yes)。

还可以禁用选定的域。

步骤 6 点击 Show Unusable Domains 以查看无法使用的域的列表。无法使用的域是Cisco ISE 由于单向信任、选择性身份验证等原因而无法用于身份验证的域。

下一步做什么

配置 Active Directory 用户组。

配置 Active Directory 用户组

您必须配置 Active Directory 用户组，使其可以用于授权策略中。在内部，Cisco 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 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

步骤 2 点击 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 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 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。

下一步做什么

配置 Active Directory 用户属性。

配置 Active Directory 用户和计算机属性

必须配置 Active Directory 用户和计算机属性，以便在授权策略的条件中使用这些属性。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Attributes** 选项卡。

步骤 3 选择 **添加 (Add)** > **添加属性 (Add Attribute)** 以手动添加属性，或选择 **添加 (Add)** > **从目录中选择属性 (Select Attributes From Directory)** 以从目录中选择属性列表。

Cisco ISE 允许您在手动添加属性类型 IP 时使用 IPv4 或 IPv6 地址配置 AD 以进行用户身份验证。

步骤 4 如果选择从目录添加属性，请在**示例用户或机器账户**字段中输入用户的名称，然后点击**检索属性**以获取用户属性的列表。例如，输入 **administrator** 以获取管理员属性列表。您还可以输入星号 (*) 通配符过滤结果。

注释　当输入示例用户名时，确保从Cisco ISE 连接到的 Active Directory 域选择用户。当您选择示例计算机获得计算机属性时，请务必在计算机名称前面加上“host/”或使用SAM$格式。例如，可以使用host/myhost。检索属性时显示的示例值仅用于说明，不能存储。

步骤 5 选中想要选择的 Active Directory 的属性旁边的复选框，并且点击**确定 (OK)**。

步骤 6 如果选择手动添加属性，请输入新属性的名称。

步骤 7 点击**保存 (Save)**。

修改密码更改、设备身份验证和设备访问限制设置

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。有关详细信息，请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 42 页。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选中相关Cisco ISE 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**高级设置 (Advanced Settings)** 选项卡。

步骤 4 根据需要，修改 Password Change、Machine Authentication 和 Machine Access Restrictions (MAR) 设置。

步骤 5 选中**启用拨入检查 (Enable dial-in check)** 复选框以在身份验证或查询期间检查用户的拨入权限。如果拨入权限被拒绝，检查的结果可能导致身份验证被拒绝。

步骤 6 如果您希望在身份验证或查询期间服务器回拨用户，请选中**对拨入客户端启用回拨检查**复选框。服务器使用的 IP 地址或电话号码可以由主叫方或网络管理员来设置。检查结果返回到 RADIUS 响应上的设备。

步骤 7 如果您想要使用 Kerberos 进行纯文本身份验证，请选中 **Use Kerberos for Plain Text Authentications** 复选框。默认和推荐选项为 MS-RPC。

计算机访问限制 (MAR) 缓存

当手动停止应用服务时，Cisco ISE 会将 MAR 缓存内容、主叫站 ID 列表和相应的时间戳存储到其本地磁盘上的文件中。如果意外重新启动应用服务，则Cisco ISE 不会存储实例的 MAR 缓存条目。重新启动应用服务时，Cisco ISE 会根据缓存条目有效时间从其本地磁盘上的文件中读取 MAR 缓存条目。当应用服务在重新启动后出现时，Cisco ISE 会将该实例的当前时间与 MAR 缓存条目时间进行比较。如果当前时间与 MAR 条目时间之间的差大于 MAR 缓存条目有效时间，则Cisco ISE 不会从磁盘中检索该条目。否则，Cisco ISE 将检索该 MAR 缓存条目并更新其 MAR 缓存条目有效时间。

要配置 MAR 缓存

在外部身份源中定义的 Active Directory 的**高级设置 (Advanced Settings)** 选项卡上，验证是否选中了以下选项：

- **启用计算机身份验证 (Enable Machine Authentication)**：启用计算机身份验证。
- **启用计算机访问限制 (Enable Machine Access Restriction)**：在授权之前结合用户和计算机身份验证。

在授权中使用 MAR 缓存

在授权策略中使用 `WasMachineAuthenticated is True`。您可以使用此规则和凭证规则执行双重身份验证。计算机身份验证必须在 AD 凭证之前完成。

如果在**系统 (System) > 部署 (Deployment)** 页面上创建了节点组，请启用 MAR 缓存分布。MAR 缓存分布会将 MAR 缓存复制到同一节点组中的所有 PSN。

有关详细信息，请参阅

请参阅以下Cisco ISE 社区页面：

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

相关主题

将 Active Directory 配置为外部身份源 ， 第 41 页

配置自定义架构

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选择加入点。

步骤 3 点击 **Advanced Settings** 选项卡。

步骤 4 在**架构 (Schema)** 部分下，选择**架构 (Schema)** 下拉列表中的**定制 (Custom)** 选项。您可以根据需要更新用户信息属性。这些属性用于收集用户信息，例如名字、姓氏、电子邮件、电话、地点等。

预定义的属性用于 Active Directory 架构（内置架构）。如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。

对 Active Directory 多加入配置的支持

Cisco ISE 支持对 Active Directory 域执行多加入。Cisco ISE 最多支持 50 个 Active Directory 加入。Cisco ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。Active Directory 多域加入包括一组不同的 Active Directory 域，每个加入均有其自己的组、属性和授权策略。

您可以多次联接同一个域林，也即是说，如有必要，您可以在同一个域林中联接不止一个域。

Cisco ISE 现在允许联接具有单向信任的域。此选项有助于绕过单向信任导致的权限问题。您可以联接以下任一受信任域，因此能够看见这两个域。

- 加入点 - 在Cisco ISE 中，每个到 Active Directory 域的独立加入都叫作一个加入点。Active Directory 加入点是Cisco ISE 身份库，可用于身份验证策略。它有用于属性和组的关联字典，这些属性和组可用于授权条件。
- 范围 - 一部分 Active Directory 加入点组合到一起就叫做范围。您可以在身份验证策略中使用范围代替单个加入点并用作身份验证结果。范围用于按照多个加入点对用户进行身份验证。如果您使用范围，就无需为每个加入点设置多个规则，可以创建只有单个策略的相同策略，节约了 Cisco ISE 用于处理请求的时间并且有助于提高性能。一个加入点可以用于多个范围中。范围可以包含在身份源序列中。因为范围不具有任何关联字典，所以您无法将范围用于授权策略条件中。

  当您执行Cisco ISE 全新安装时，默认情况下并无范围。这称为无范围模式。当您添加范围时，Cisco ISE 进入多范围模式。如果需要，您可以返回无范围模式。所有加入点将移至 Active Directory 文件夹。

  - Initial_Scope 是用于存储在无范围模式中添加的 Active Directory 加入点的隐式范围。当启用多范围模式时，所有 Active Directory 加入点将移至自动创建的 Initial_Scope。您可以重命名 Initial_Scope。

- All_AD_Instances 是在 Active Directory 配置中不显示的一个内置伪范围。它只在策略和身份序列中作为身份验证结果显示。如果您要选择Cisco ISE 中配置的所有 Active Directory 加入点，就可以选择此范围。

创建新范围，添加 **Active Directory** 加入点

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Scope Mode**。
默认情况下，系统创建名为 Initial_Scope 的范围，当前所有加入点都放在此范围中。

步骤 3 要创建更多范围，请点击 **Add**。

步骤 4 输入新范围的名称和说明。

步骤 5 点击**提交 (Submit)**。

身份重写

身份重写是一种定向Cisco ISE 的高级功能，使其在传递至外部 Active Directory 系统之前处理其身份。您可以创建规则以将身份改为包含或排除域前缀和/或后缀或您所选择的其他附加标记的相应格式。

身份重写规则应用于传递至 Active Directory 之前从客户端接收的用于使用者搜索、身份验证和授权查询等操作的用户名或主机名。Cisco ISE 将匹配条件标记，在发现第一个匹配项时，Cisco ISE 停止处理策略并根据结果重写身份字符串。

在重写期间，以方括号"[]"括起来的所有内容（例如 [IDENTITY]）是变量，在评估端不会对其进行评估，但会添加与字符串中该位置匹配的字符串。没有方括号的所有内容在规则的评估端和重写端都会评估为固定字符串。

以下是身份重写的一些示例，假设用户输入的身份是 ACME\jdoe：

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

  结果是 jdoe。此规则指示Cisco ISE 删掉所有用户名的 ACME 前缀。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@ACME.com**。

  结果是 jdoe@ACME.com。此规则指示Cisco ISE 将格式从前缀更改为后缀表示法，或从 NetBIOS 格式更改为 UPN 格式。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **ACME2\[IDENTITY]**。

  结果是 ACME2\jdoe。此规则指示Cisco ISE 将具有特定前缀的所有用户名更改为使用备用前缀。

- 如果身份与 **[ACME]\jdoe.USA** 匹配，则重写为 **[IDENTITY]@[ACME].com**。

结果是jdoe\ACME.com。此规则指示Cisco ISE删掉点后面的领域（在本例中是国家/地区），替换为正确的领域。

- 如果身份与 **E=[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

  结果是jdoe。如果身份来自证书，字段是邮件地址，而且Active Directory配置为按使用者搜索，则可以创建此示例规则。此规则指示Cisco ISE 删除“E=”。

- 如果身份与 **E=[EMAIL],[DN]** 匹配，则重写为 **[DN]**。

  此规则会将证书使用者从E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com转变为纯DN, CN=jdoe, DC=acme, DC=com。如果身份取自证书使用者，且Active Directory配置为按DN搜索用户，则可以创建此示例规则。此规则指示Cisco ISE 删掉邮件前缀并生成DN。

以下是编写身份重写规则的一些常见错误：

- 如果身份与 **[DOMAIN]\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@DOMAIN.com**。

  结果是 jdoe@DOMAIN.com。此规则在规则的重写端没有用方括号 [] 括起来的 [DOMAIN]。

- 如果身份与 **DOMAIN\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@[DOMAIN].com**。

  同样，结果是jdoe@DOMAIN.com。此规则在规则的评估端没有用方括号[]括起来的[DOMAIN]。

身份重写规则始终应用在 Active Directory 加入点的情景中。即使由于身份验证策略而选择了范围，重写规则也适用于每个Active Directory加入点。如果使用的是EAP-TLS，这些重写规则还适用于取自证书的身份。

启用身份重写

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Rewrite** 部分下，选择是否要应用重写规则来修改用户名。

步骤 4 输入匹配条件和重写结果。您可以删除出现的默认规则并根据要求输入规则。Cisco ISE 按顺序处理规则，并会应用与请求用户名相匹配的第一个条件。您可以使用匹配令牌（方括号中包含的文本）将原始用户名的元素传输到结果。如果无任何规则匹配，则身份名称保持不变。您可以点击 **Launch Test** 按钮预览重写处理。

身份解析设置

某些身份类型包括域标记，如前缀或后缀。例如，在如 ACME\jdoe 这样的 NetBIOS 身份中，“ACME”是域标记前缀，同样在如jdoe@acme.com这样的UPN身份中，“acme.com”是域标记后缀。域前缀应该与组织中 Active Directory 域的 NetBIOS (NTLM) 名称匹配，域后缀应该与组织中 Active Directory 域的 DNS 名称或备选 UPN 后缀匹配。例如，jdoe@gmail.com 会视为没有域标记，因为 gmail.com 不是 Active Directory 域的 DNS 名称。

身份解析设置允许您配置重要设置来调整安全和性能的平衡，以符合您的 Active Directory 部署。您可以使用这些设置来调整没有域标记的用户名和主机名的身份验证。在Cisco ISE 不知道用户域的情况下，可以将其配置为在所有身份验证域中搜索用户。即使在一个域中找到了用户，Cisco ISE 仍将等待所有响应以确保不存在模糊身份。这可能需要较长时间，具体取决于域的数量、网络中的延迟、负载等。

避免身份解析问题

强烈建议在身份验证期间，使用完全限定的用户和主机名称（即，带有域标记的名称）。例如，用户使用 UPN 和 NetBIOS 名称，主机使用 FQDN SPN 名称。这在您频繁遇到模糊错误的情况下尤其重要，例如，多个 Active Directory 帐户匹配传入用户名；例如，jdoe m 匹配 jdoe@emea.acme.com 和 jdoe@amer.acme.com。在某些情况下，使用完全限定名称是解决问题的唯一方法。在其他情况下，保证用户拥有唯一密码即可。因此，如果最初使用唯一身份，则更加高效，而且可以减少密码锁定问题。

配置身份解析设置

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Resolution**（身份解析）部分下，对用户名或计算机名称的身份解析定义以下设置。此设置可提供用于用户搜索和身份验证的高级控制。

第一个设置适用于没有标记的身份。在这种情况下，可以选择以下任一选项：

- **拒绝请求 (Reject the request)**：此选项将导致没有任何域标记的用户（例如 SAM 名称）的身份验证失败。如果有多个加入域，而Cisco ISE 必须在所有加入的全局目录中查找身份（这可能不太安全），则此选项非常有用。此选项强制用户使用具有域标记的名称。

- **仅搜索加入的林中的“身份验证域”(Only search in the “Authentication Domains” from the joined forest)**：此选项只在加入点所在林的域（这些域在身份验证域部分中指定）中搜索身份。对于SAM帐户名称，这是默认选项，并且与Cisco ISE 1.2 的行为相同。
- **搜索所有“身份验证域”部分 (Search in all the “Authentication Domains” sections)**：此选项在所有受信任林的所有身份验证域中搜索身份。这可能会增加延迟并影响性能。

根据身份验证域在Cisco ISE 中的配置方式来选择选项。如果只选择特定身份验证域，将只搜索这些域（无论是选择“加入的林”还是“所有林”）。

如果Cisco ISE 无法与它所需的所有全局目录 (GC) 通信，则使用第二个设置，以符合在“Authentication Domains”部分中指定的配置。在这种情况下，可以选择以下任一选项：

- **继续使用可用域 (Proceed with available domains)**：如果在任一可用的域中找到匹配项，此选项将继续执行身份验证。
- **丢弃请求 (Drop the request)**：如果身份解析遇到某些无法访问或不可用的域，此选项将删除身份验证请求。

就 Active Directory 测试用户 (Test Users for Active Directory)身份验证

“测试用户”工具可用于从 Active Directory 验证用户身份验证。您还可以获取组和属性并对其进行检查。您可以对单个加入点或对范围运行测试。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选择以下选项之一：

- 要在所有加入点上运行测试，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Cisco ISE 节点并点击**测试用户**。

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Cisco ISE 节点。

步骤 6 如果要从 Active Directory 检索组和属性，请选中“检索组”(Retrieve Groups) 和“检索属性”(Retrieve Attributes) 复选框。

步骤 7 点击 **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（用于身份验证、查找或获取组/属性）所需的时间（以毫秒为单位）。如果操作所需的时间超过阈值，Cisco ISE 将显示警告消息。

删除 Active Directory 配置

如果您不会使用 Active Directory 作为外部身份源，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。

开始之前

确保您已退出 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **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 **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。

查看节点的 Active Directory 加入

您可以使用 **Active Directory** 页面上的**节点视图**按钮查看给定Cisco ISE 节点的所有 Active Directory 加入点的状态或所有Cisco ISE 节点上的所有加入点列表。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Node View**。

步骤 3 从 **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Cisco ISE 节点，则更新此表可能需要几分钟时间。

步骤 4 点击加入点 **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**列中的链接以转至**诊断工具**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Cisco ISE 节点上运行的服务。当Cisco ISE 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。

Cisco ISE 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Cisco ISE 连接到 Active Directory 的先决条件。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 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **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Cisco ISE 节点。

如果未选择Cisco ISE 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**控制面板上的**警报** dashlet 中报告故障。

步骤 6 点击 **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。

启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。必须在您的部署中承担策略服务角色的思科 ISE 节点上启用此选项。启用 Active Directory 调试日志可能会影响 ISE 性能。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **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 策略服务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)**。

获取 Active Directory 日志文件来进行故障排除

下载并查看 Active Directory 调试日志，对您可能遇到的问题进行故障排除。

开始之前

必须启用 Active Directory 调试日志记录。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)**。

步骤 2 点击您要从其获得 Active Directory 调试日志文件的节点。

步骤 3 点击 **Debug Logs** 选项卡。

步骤 4 向下滚动此页面找到 ad_agent.log 文件。点击该文件并下载该文件。

Active Directory 警报和报告

Cisco ISE 提供多种警报和报告，用于对 Active Directory 相关活动进行监控和故障排除。

警报

Active Directory 错误和故障会触发以下警报：

- 配置的名称服务器不可用
- 所加入的域不可用
- 身份验证域不可用
- Active Directory 林不可用
- AD 连接器必须重新启动
- AD：ISE 帐户密码更新失败
- AD：计算机 TGT 刷新失败

报告

您可以通过以下两种报告监控 Active Directory 相关活动：

- RADIUS Authentications Report - 此报告显示 Active Directory 身份验证和授权的详细步骤。您可以在此处查找该报告： **操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **RADIUS 身份验证 (RADIUS Authentications)**。
- AD Connector Operations Report - AD 连接器操作报告提供 AD 连接器所执行后台操作的日志，例如Cisco ISE 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理。如果遇到 Active Directory 失败，您可以查看此报告的详细信息以确定可能的原因。您可以在此处查找该报告： **操作 (Operations)** > **报告 (Reports)** > **诊断 (Diagnostics)** > **AD 连接器操作 (AD Connector Operations)**。

Active Directory 高级调整

高级调整功能提供节点特定的设置，用于在Cisco支持人员指导下的支持操作，更深入地调整系统中的参数。这些设置不适用于正常管理流程，只应在指导下使用。

Active Directory 身份搜索属性

Cisco ISE 使用 SAM、CN 或这两者来识别用户。Cisco ISE 版本 2.2 补丁 5 及更高版本，版本 2.3 补丁 2 及更高版本，将 sAMAccountName 属性用作默认属性。在早期版本中，默认搜索 SAM 和 CN 属性。此行为已在版本 2.2 补丁 5 及更高版本，以及版本 2.3 补丁 2 及更高版本中发生更改，是 CSCvf21978 漏洞修复的组成部分。在这些版本中，仅 sAMAccountName 属性用作默认属性。

如果环境需要，您可以配置Cisco ISE 以使用 SAM、CN 或者这两者。使用 SAM 和 CN 时，SAMAccountName 属性的值不唯一，Cisco ISE 还将比较 CN 属性值。

注释 默认情况下，身份搜索行为已在Cisco ISE 2.4 中更改为仅搜索 SAM 帐户名称。要修改此默认行为，请按照“配置 Active Directory 身份搜索的属性”部分所述更改“IdentityLookupField”标志的值。

配置 Active Directory 身份搜索的属性

1. 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。在 **Active Directory** 窗口中，点击**高级工具 (Advanced Tools)**，然后选择**高级调整 (Advanced Tuning)**。输入下列详细信息：
   - **ISE Node** - 选择连接 Active Directory 的 ISE 节点。
   - **Name** - 输入您正更改的注册表项。要更改 Active Directory 搜索属性，请输入：`REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
   - **Value** - 输入 ISE 用于识别用户的属性：
     - *SAM* - 在查询中仅使用 SAM（此选项为默认选项）。
     - *CN* - 在查询中仅使用 CN。
     - *SAMCN* - 在查询中使用 CN 和 SAM。
   - **Comment** - 说明您正在更改的内容，例如：将默认行为更改为 SAM 和 CN
2. 点击**更新值 (Update Value)** 以更新注册表。

   系统将显示一个弹出窗口。阅读消息并接受更改。ISE 中的 AD 连接器服务重新启动。

搜索字符串示例

在以下示例中，假设用户名为 *userd2only*：

- SAM 搜索字符串—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM 和 CN 搜索字符串—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

使用 Active Directory 设置思科 ISE 的补充信息

要使用 Active Directory 配置Cisco ISE，必须配置组策略，并配置请求方以对计算机进行身份验证。

在 Active Directory 中配置组策略

有关如何访问组策略管理编辑器的详细信息，请参阅 Microsoft Active Directory 文档。

步骤 1 打开组策略管理编辑器，如下图所示。

组策略对象选择

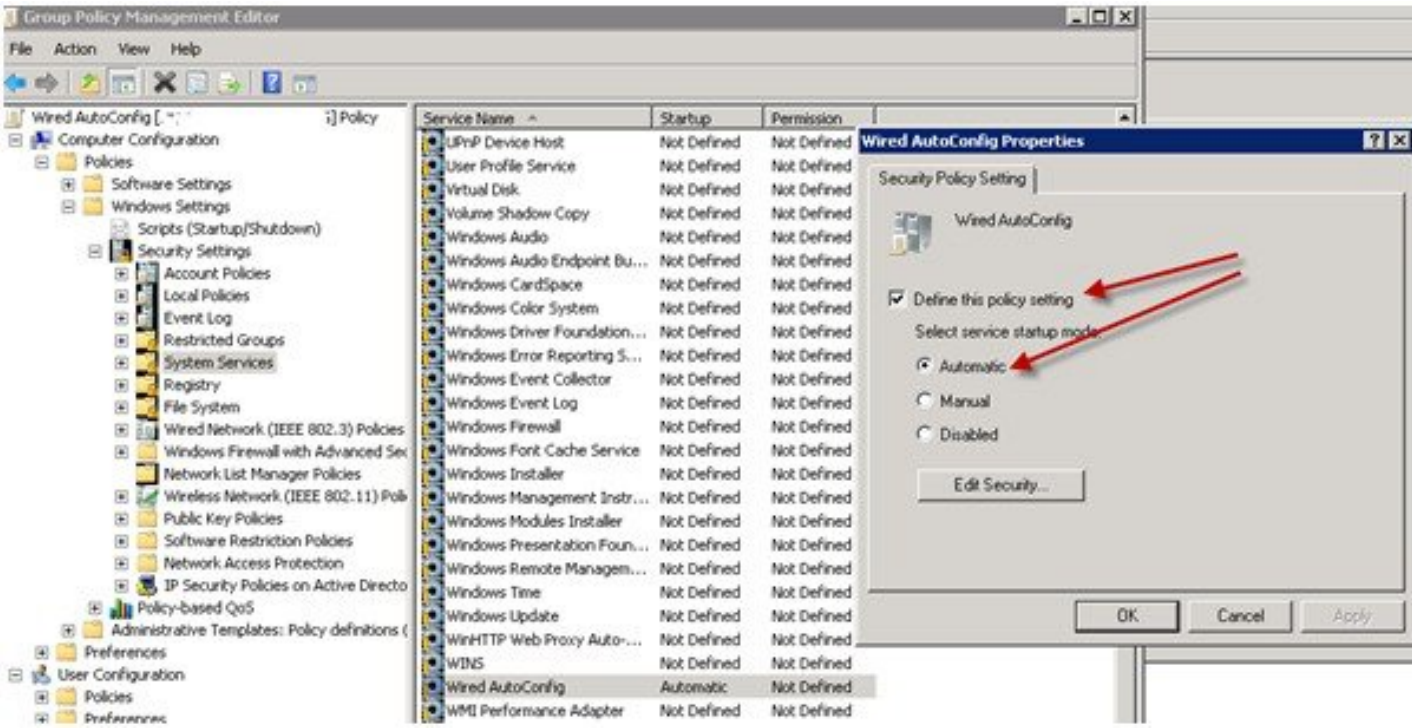
步骤 2 创建新策略并为其输入描述性名称，或者将其添加到现有域策略。

示例：

在以下示例中，使用 Wired Autoconfiguration 作为策略名称。

步骤 3 选中 **Define this policy setting** 复选框，然后针对服务启动模式点击 **Automatic** 单选按钮，如下图所示。

策略属性



步骤 4 在所需的组织单元或域 Active Directory 级别应用策略。

配置 Odyssey 5.X 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证

如果使用 Odyssey 5.x 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证，则必须在请求方进行以下配置。

步骤 1 启动 Odyssey 访问客户端。

步骤 2 从 Tools 菜单选择 **Odyssey Access Client Administrator**。

步骤 3 双击 **Machine Account** 图标。

步骤 4 从**计算机帐户 (Machine Account)** 窗口，必须配置 EAP-TLS 身份验证配置文件：

a) 选择 **配置 (Configuration)** > **配置文件 (Profiles)**。

b) 为 EAP-TLS 配置文件输入名称。

c) 在“身份验证”(Authentication) 选项卡上，选择 **EAP-TLS** 作为身份验证方法。

d) 在“证书”(Certificate) 选项卡上，选中**允许使用我的证书登录 (Permit login using my certificate)** 复选框，然后为请求方计算机选择证书。

e) 在**用户信息 (User Info)** 选项卡上，选中**使用计算机凭证 (Use machine credentials)** 复选框。

如果启用此选项，Odyssey 请求方将以 host\<*machine_name*> 格式发送计算机名称，Active Directory 识别来自计算机的请求，并且查找要执行身份验证的计算机对象。如果禁用此选项，Odyssey 请求方将发送不带 host\ 前缀的计算机名称，Active Directory 将查找用户对象，身份验证失败。

用于计算机身份验证的 AnyConnect 代理

当您为计算机身份验证配置 AnyConnect 代理时，可以执行下列操作之一：

- 使用默认的计算机主机名，包括前缀“host/”。
- 配置新的配置文件，在这种情况下必须包括前缀“host/”，然后是计算机名称。

支持 Easy Connect 和 被动身份服务 的 Active Directory 要求

Easy Connect 和 被动身份服务 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。必须正确配置 Active Directory 服务器，才能使 ISE 用户能够连接和获取用户登录信息。以下各部分说明如何配置 Active Directory 域控制器（Active Directory 端的配置）以支持 Easy Connect 和 被动身份服务。

要配置 Active Directory 域控制器（Active Directory 端的配置）以支持 Easy Connect 和被动身份服务，请按照以下步骤操作：

注释 必须配置所有域中的所有域控制器。

1. 从 ISE 设置 Active Directory 加入点和域控制器。请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 42 页 和 添加域控制器，第 44 页。
2. 根据域控制器配置 WMI。请参阅对被动 ID 配置 WMI，第 46 页。
3. 从 Active Directory 执行以下步骤：
   - 配置 Active Directory 以服务 被动身份服务，第 63 页
   - 设置 Windows 审核策略，第 65 页
4. （可选）使用以下步骤在 Active Directory 上对 ISE 执行的自动配置进行故障排除：
   - 为域管理员组中的 Microsoft Active Directory 用户设置权限，第 66 页
   - 不在域管理员组中的 Microsoft Active Directory 用户的权限，第 66 页
   - 在域控制器上使用 DCOM 的权限，第 68 页
   - 设置访问 WMI Root/CIMv2 名称空间的权限，第 69 页
   - 授权访问 AD 域控制器上的安全事件日志，第 70 页

配置 Active Directory 以服务 被动身份服务

ISE Easy Connect 和 被动身份服务 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。ISE 连接到 Active Directory 并获取用户登录信息。

应从 Active Directory 域控制器执行以下步骤：

步骤 1 确保相关 Microsoft 补丁安装在 Active Directory 域控制器上。

a) 需要以下 Windows Server 2008 补丁：

- http://support.microsoft.com/kb/958124

  此补丁可修复 Microsoft WMI 中的内存泄漏，这会阻止 ISE 与域控制器建立成功连接。

- http://support.microsoft.com/kb/973995

  此补丁修复 Microsoft 的 WMI 中的不同的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录事件写入至域控制器的安全日志。

b) Windows Server 2008 R2 需要以下补丁（除非安装 SP1）：

- http://support.microsoft.com/kb/981314

  此补丁修复 Microsoft 的 WMI 中的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录活动事件写入至域控制器的安全日志。

- http://support.microsoft.com/kb/2617858

  此补丁修复 Windows Server 2008 R2 中的启动或登录过程意外缓慢。

c) 需要以下链接中列出的 Windows 平台 WMI 相关问题补丁：

- http://support.microsoft.com/kb/2591403

这些热修复与 WMI 服务及其相关组件的操作和功能相关。

步骤 2 确保 Active Directory 在 Windows 安全日志中记录用户登录事件。

验证“审核策略”(Audit Policy) 设置（“组策略管理” [Group Policy Management] 设置的一部分）支持成功登录在 Windows 安全日志中生成必要事件（这是 Windows 默认设置，但是，您必须明确保证此设置正确）。

步骤 3 您必须拥有具备足够权限的 Active Directory 用户才能将 ISE 连接到 Active Directory。以下说明显示如何为管理域组用户或无管理域组用户定义权限：

- Active Directory 用户为域管理员组成员时需要的权限
- Active Directory 用户不是域管理员组成员时需要的权限

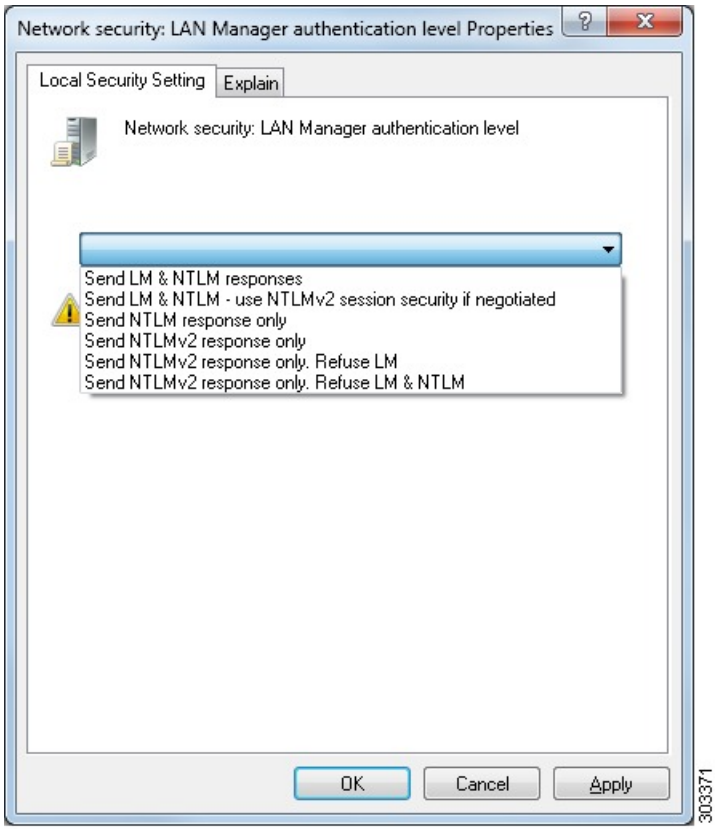
步骤 4 ISE 使用的 Active Directory 用户可以通过 NT LAN Manager (NTLM) v1 或 v2 进行身份验证。您需要验证 Active Directory NTLM 设置是否与 ISE NTLM 设置一致，以确保 ISE 和 Active Directory 域控制器之间的连接成功进行身

份验证。下表显示所有 Microsoft NTLM 选项及支持哪些 ISE NTLM 操作。如果 ISE 设置为 NTLMv2，则支持所述的全部六个选项。如果 ISE 设置为支持 NTLMv1，则仅支持前五个选项。

表 *15:* 基于 *ISE* 和 *AD NTLM* 版本设置的受支持身份验证类型

ISE NTLM 设置选项/Active Directory (AD) NTLM 设置选项 NTLMv1 NTLMv2	**NTLMv1**	**NTLMv2**
发送 LM & NTLM 响应	允许连接	允许连接
发送 LM & NTLM - 如果有协商，使用 NTLMv2 会话安全	允许连接	允许连接
仅发送 NTLM 响应	允许连接	允许连接
仅发送 NTLMv2 响应	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM & NTLM	拒绝连接	允许连接

图 *2: MS NTLM* 身份验证类型选项



步骤 5 确保您已创建一个防火墙规则允许流量去往 Active Directory 域控制器中的 `dllhost.exe`。

您可以关闭防火墙，或者允许在特定 IP（ISE IP 地址）访问以下端口：

- TCP 135：通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端为此请求服务的组件使用哪个端口。
- UDP 137：Netbios 名称解析
- UDP 138：Netbios 数据报服务
- TCP 139：Netbios 会话服务
- TCP 445：SMB

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 %SystemRoot%\System32\dllhost.exe 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP (ISE IP)。

设置 Windows 审核策略

确保**审核策略 (Audit Policy)**（**组策略管理 (Group Policy Management)** 设置的一部分）支持成功登录。此为在 AD 域控制器机器的 Windows 安全日志中生成必要事件所需要的。这是 Windows 默认设置，但是，您必须验证此设置的正确性。

步骤 1 选择 **开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **组策略管理 (Group Policy Management)**。

步骤 2 在域 (Domain) 下导航至相关的域，并展开导航树。

步骤 3 依次选择**默认域控制器策略 (Default Domain Controller Policy)**，右键点击并选择**编辑 (Edit)**。

组策略管理编辑器 (Group Policy Management Editor) 出现。

步骤 4 选择 **默认域控制器策略 (Default Domain Controllers Policy)** > **计算机配置 (Computer Configuration)** > **策略 (Policies)** > **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)**。

- 对于 Windows Server 2003 或 Windows Server 2008（非 R2），依次选择 **本地策略 (Local Policies)** > **审核策略 (Audit Policy)**。对于这两个策略项目（**审核帐户登录事件 [Audit Account Logon Events]** 和**审核日志事件 [Audit Logon Events]**），请确保相应的**策略设置 (Policy Setting)** 直接或间接包含**成功 (Success)** 条件。要间接包含成功 (Success) 条件，**策略设置 (Policy Setting)** 必须设置为**未定义 (Not Defined)**，表示有效值将从较高级别的域沿用，并且该高级别域的**策略设置 (Policy Setting)** 必须配置为明确包含**成功 (Success)** 条件。
- 对于 Windows Server 2008 R2 和 Windows 2012，请选择 **高级审核策略配置 (Advanced Audit Policy Configuration)** > **审核策略 (Audit Policies)** > **帐户登录 (Account Logon)**。对于这两个策略项目（**审核 Kerberos 身份验证服务 [Audit Kerberos Authentication Service]** 和**审核 Kerberos 服务申请单操作 [Audit Kerberos Service Ticket Operations]**），请确保相应的“策略设置”(Policy Setting) 直接或间接包括成功 (Success) 如上所述的成功条件。

注释 Cisco ISE 在与 Active Directory 通信时使用 Kerberos 协议中的 RC4 密码（除非在 Active Directory 域控制器配置中禁用此加密类型）。可以使用 Active Directory 中的**网络安全: 配置 Kerberos 允许的加密类型 (Network Security: Configure Encryption Types Allowed for Kerberos)** 选项来配置 Kerberos 协议允许的加密类型。

步骤 5 如果更改了任何“审核策略”(Audit Policy) 项目设置，那么您应运行 `gpupdate /force` 强制新设置生效。

为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

步骤 1 右键点击注册表项图标，然后选择**所有者 (Owner)** 选项卡。

步骤 2 点击 **Permissions**（权限）。

步骤 3 点击 **Advanced**。

不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
  ```

- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许思科 ISE 连接到域控制器。
- 在域控制器上使用 DCOM 的权限，第 68 页
- 设置访问 WMI Root/CIMv2 名称空间的权限，第 69 页

只有以下 Active Directory 版本要求具有这些权限：

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

添加注册表项以允许思科 ISE 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许思科 ISE 以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根秘钥的所有者。

```
Windows 注册表编辑器版本 5.00 [HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
 "AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

确保DllSurrogate注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

在域控制器上使用 DCOM 的权限

用于思科 ISE 被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

步骤 1 从命令行运行 **dcomcnfg** 工具。

步骤 2 扩展**组件服务 (Component Services)**。

步骤 3 扩展 **计算机 (Computers)** > **我的计算机 (My Computer)**。

步骤 4 从菜单栏中选择**操作 (Action)**，点击**属性 (Properties)**，然后点击 **COM 安全性 (COM Security)**。

步骤 5 Cisco ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)** 的**编辑限制设置 (Edit Limits)** 和**编辑默认设置 (Edit Default)**）。

步骤 6 对于**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)**，允许所有本地和远程访问。

图 *3:* 访问权限的本地和远程访问

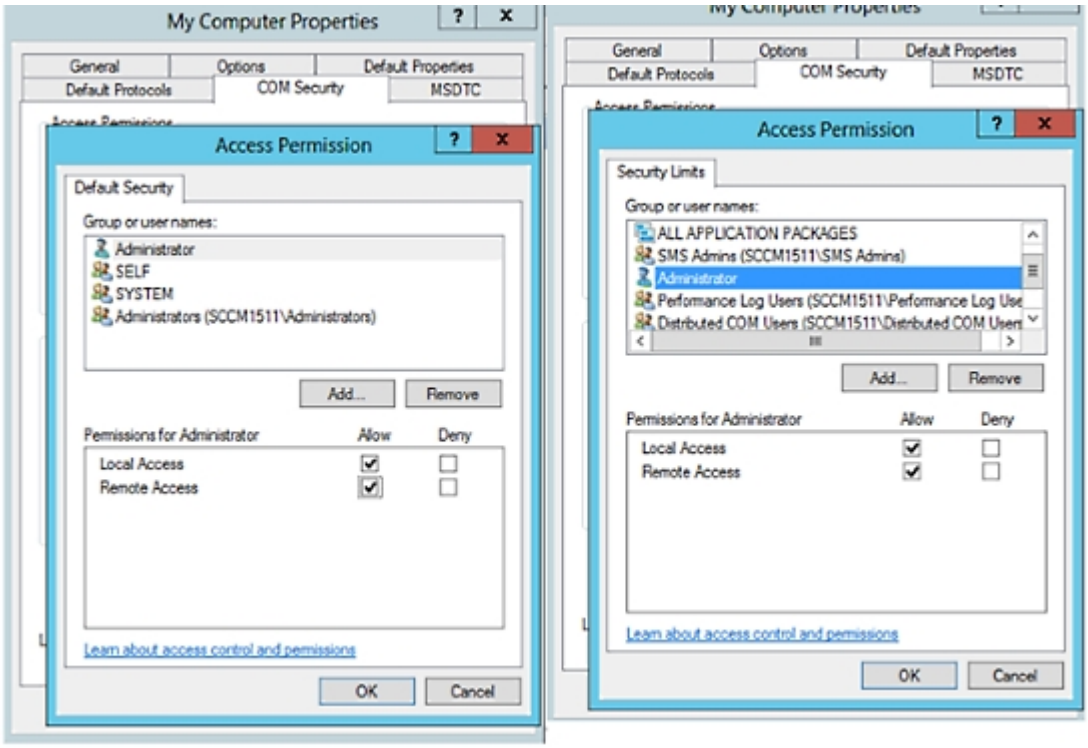
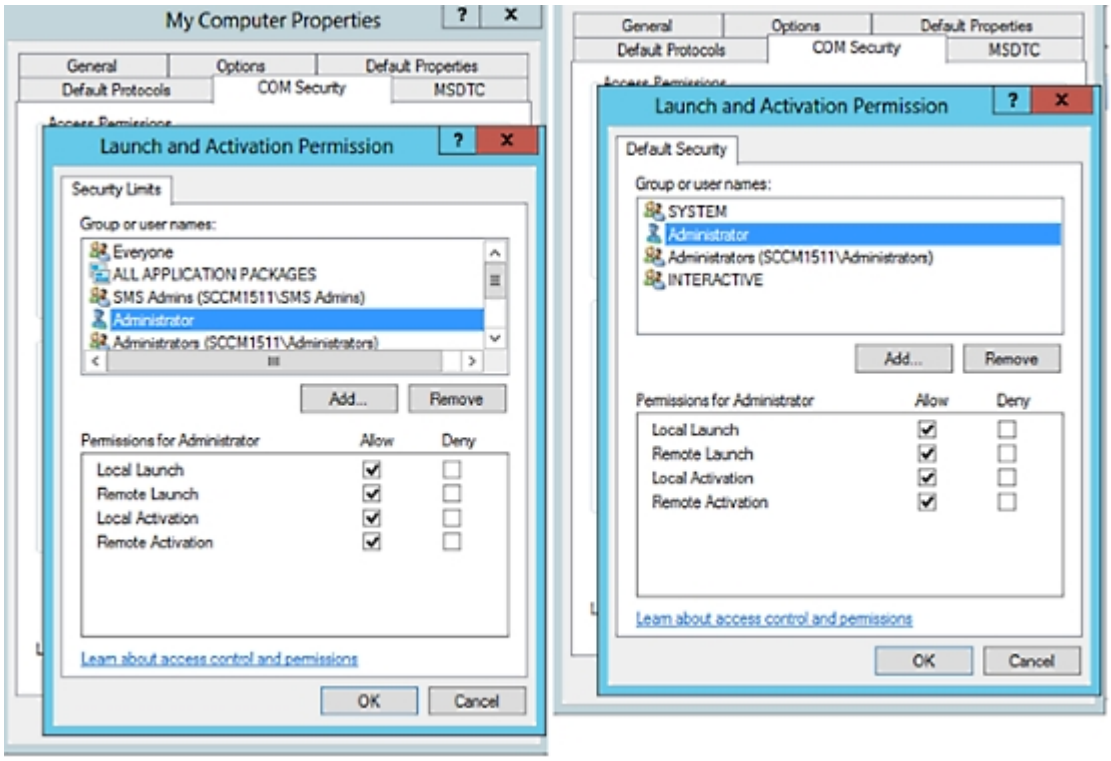


图 *4:* 启动以及激活权限的本地和远程访问



设置访问 WMI Root/CIMv2 名称空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法”(Execute Methods) 和“远程启用”(Remote Enable) 的权限。您可以使用 wmimgmt.msc MMC 控制台授予访问权限。

步骤 1 选择 **开始 (Start)** > **运行 (Run)** 并键入 `wmimgmt.msc`。

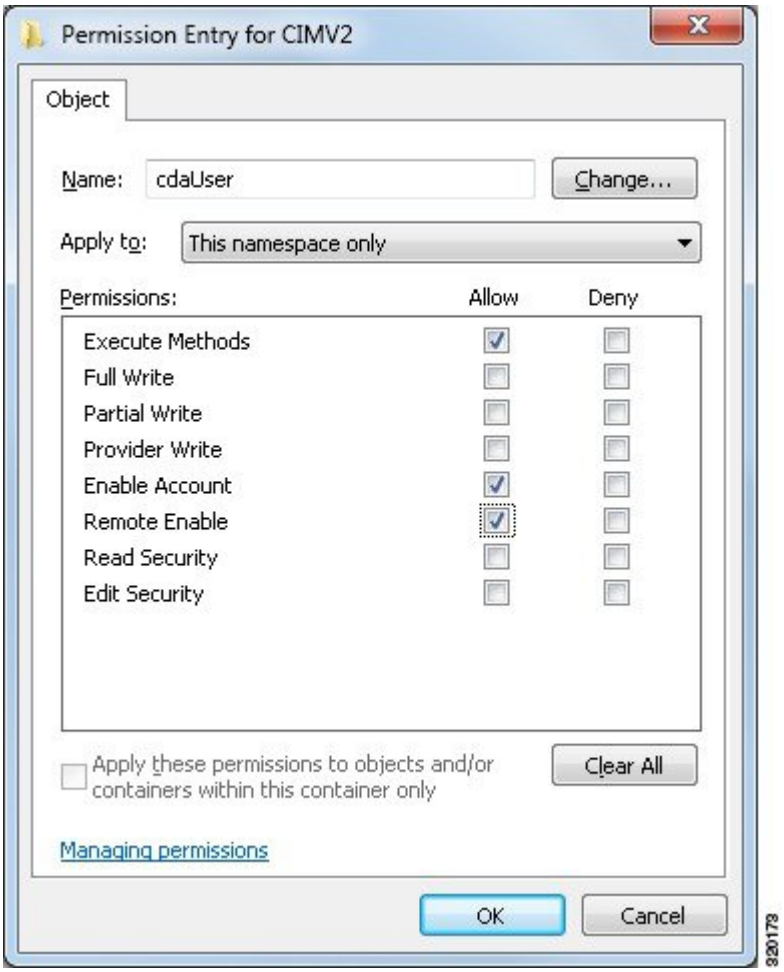
步骤 2 右键点击 **WMI 控制 (WMI Control)** 并点击**属性 (Properties)**。

步骤 3 在**安全 (Security)** 选项卡下，展开**根 (Root)** 并选择 **CIMV2**。

步骤 4 点击 **Security**。

步骤 5 添加 Active Directory 用户，并按如下所示配置所需的权限。

图 *5: WMI Root\CIMv2* 名称空间所需的权限



授权访问 AD 域控制器上的安全事件日志

在 Windows 2008 及更高版本上，您可以通过将 ISE ID 映射用户添加到名为“事件日志读取器”的组中来授予对 AD 域控制器日志的访问权限。

在 Windows 所有旧版本上，您必须编辑一个注册表项，如下所示。

步骤 1 要委托访问至安全事件日志，请查找该帐户的 SID。

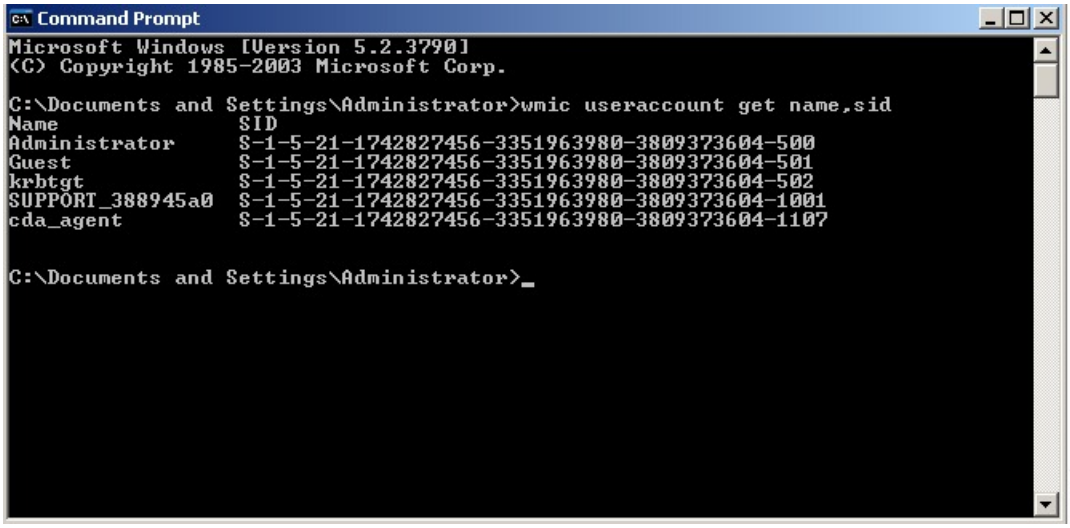
步骤 2 在命令行处使用以下命令，列出所有 SID 帐户，也如下图所示。

```
wmic useraccount get name,sid
```

您可以使用用于特定用户名和域的以下命令：

```
wmic useraccount where name=“iseUser” get domain,name,sid
```

图 *6:* 列出所有 ***SID*** 帐户



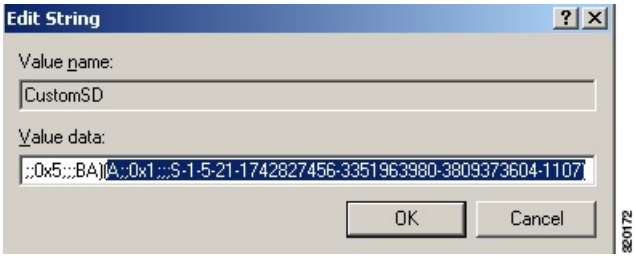
步骤 3 查找 SID，打开“注册表编辑器”(Registry Editor)，并对以下位置进行浏览：

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

步骤 4 点击**安全 (Security)** 和双击 **CustomSD**。

例如，要允许读访问 ise_agent 账户 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`，请输入 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`。

图 *7:* 编辑 ***CustomSD*** 字符串



步骤 5 重启域控制器上的 WMI 服务。您可以通过以下两种方式重启 WMI 服务：

a) 在 CLI 处运行以下命令：

net stop winmgmt

net start winmgmt

b) 运行 `Services.msc`，打开 Windows 服务管理工具。在 Windows 服务管理窗口中，找到 **Windows 管理规范 (Windows Management Instrumentation)** 服务，右键点击，然后选择**重启 (Restart)**。

Easy Connect

使用 Easy Connect，您可以轻松地以安全方式将用户从有线终端连接到网络，并通过 Active Directory 域控制器（而不是通过Cisco ISE）对这些用户进行身份验证，从而监控他们。通过 Easy Connect，Cisco ISE 可以从 Active Directory 域控制器收集用户身份验证信息。Easy Connect 使用 MS WMI 接口连接至 Windows 系统 (Active Directory) 并从 Windows 事件消息查询日志，因此它当前仅支持安装了 Windows 的终端。Easy Connect 使用 MAB 支持有线连接，这与 802.1X 相比更易于配置。与 802.1X 不同的是，使用 Easy Connect 和 MAB：

- 您无需配置请求方
- 您无需配置 PKI
- ISE 会在外部服务器 (AD) 对用户进行身份验证后发出 CoA

Easy Connect 支持以下操作模式：

- 实施模式：ISE 主动将授权策略下载到网络设备，以基于用户凭证进行实施。
- 可视性模式：Cisco ISE 发布从 NAD 设备传感器接收的会话合并和帐户信息，以便将该信息发送至 pxGrid。

在这两种情况下，通过 Active Directory (AD) 进行身份验证的用户会显示在Cisco ISE 实时会话视图中，而且可以使用Cisco pxGrid 接口由第三方应用从会话目录进行查询。已知信息为用户名、IP 地址、AD DC 主机名以及 AD DC NetBios 名称。有关 pxGrid 的详细信息，请参阅思科 pxGrid 节点。

设置 Easy Connect 后，即可根据用户的名称或 IP 地址过滤特定用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。要过滤被动身份服务，请参阅过滤被动身份服务，第 117 页。

Easy Connect 限制

- MAC 身份验证绕行 (MAB) 支持 Easy Connect。MAB 和 802.1X 可以在同一端口上进行配置，但您必须为每个服务设置不同的 ISE 策略。
- 当前仅支持 MAB 连接。您无需唯一身份验证策略来进行连接，因为将根据授权策略中定义的 Easy Connect 条件来授权连接及授予权限。
- 在高可用性模式下支持 Easy Connect。可以定义多个节点，并使用被动 ID 来启用它们。然后，ISE 会自动激活一个 PSN，而其他节点将保持备用状态。
- 仅支持 Cisco Network Access Devices (NAD)。
- 不支持 IPv6。
- 当前不支持无线连接。
- 系统仅跟踪 Kerberos 身份验证事件，因此 Easy Connect 仅启用用户身份验证，不支持机器身份验证。

Easy Connect 需要 ISE 中的配置，而 Active Directory 域服务器还必须根据 Microsoft 发布的说明和准则进行正确的补丁安装和配置。有关为Cisco ISE 配置 Active Directory 域控制器的信息，请参阅 支持 Easy Connect 和 被动身份服务 的 Active Directory 要求 ， 第 62 页

Easy Connect 实施模式

Easy Connect 允许用户从有线终端（通常为 PC）使用 Windows 操作系统通过以下方式登录到安全网络：使用 MAC 地址绕行 (MAB) 协议并访问 Active Directory (AD) 以进行身份验证。Easy Connect 从 Active Directory 服务器侦听 Windows Management Instrumentation (WMI) 事件，以获取有关已通过身份验证的用户的信息。AD 对用户进行身份验证后，域控制器将生成一份事件日志，此日志中包含用户名和为此用户分配的 IP 地址。Cisco ISE 从 AD 接收登录通知，然后发出 RADIUS 授权更改 (CoA)。

注释 如果将 Radius 服务类型设置为 call-check，则不会对 MAB 请求执行 MAC 地址查找。因此，将针对请求返回 access-accept。这是默认配置。

Easy Connect 实施模式流程

Easy Connect 实施模式流程如下所示：

1. 用户从有线终端（如 PC）连接到 NAD。
2. NAD（为 MAB 所配置）将访问请求发送至Cisco ISE。ISE 根据用户配置使用访问权限进行响应，以允许用户访问 AD。配置必须至少允许访问 DNS、DHCP 和 AD。
3. 用户登录到域，系统将一份安全审核事件发送至Cisco ISE。
4. ISE 从 RADIUS 收集 MAC 地址以及 IP 地址和域名，并从安全审核事件收集用户的帐户信息（登录信息）。
5. 将所有数据收集并合并到会话目录中后，Cisco ISE 向 NAD 发出 CoA（根据在策略服务节点中管理的相应策略），NAD 根据此策略为用户提供对网络的访问权限。

图 *8: Easy Connect* 实施模式基本流程

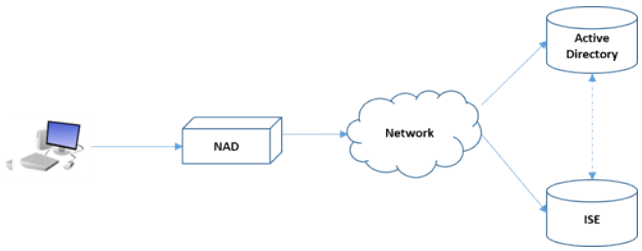
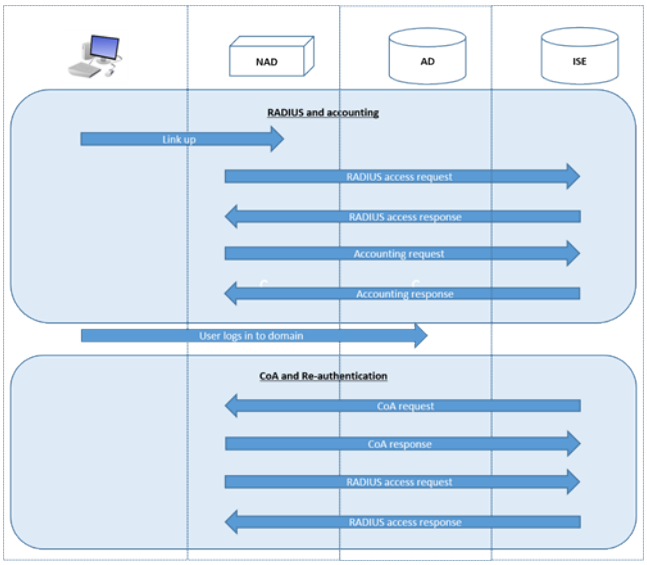


图 *9: Easy Connect* 实施模式详细流程

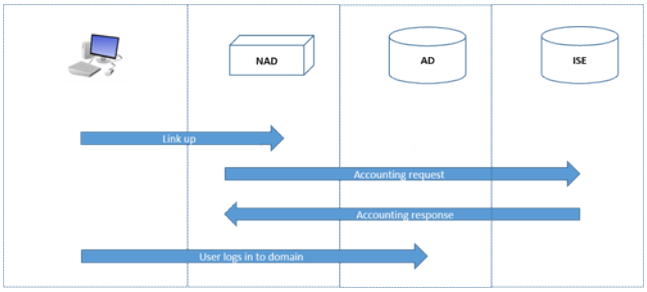


有关配置实施模式的详细信息，请参阅配置 Easy Connect 实施模式，第 74 页。

Easy Connect 可见性模式

对于可视性模式，Cisco ISE 仅从 RADIUS 监控帐户信息（NAD 中设备传感器功能的一部分）且不执行授权。Easy Connect 侦听 RADIUS 帐户和 WMI 事件，并将该信息发布到日志和报告（或者发布到 pxGrid）。设置 pxGrid 时，系统会使用 Active Directory 将用户登录期间的 RADIUS 帐户开始和会话终止信息同时发布到 pxGrid。

图 *10: Easy Connect* 可见性模式流程



有关配置 Easy Connect 可视性模式的详细信息，请参阅配置 Easy Connect 可视性模式，第 75 页。

配置 Easy Connect 实施模式

开始之前

- 为了获得最佳性能，请部署专用的 PSN 来接收 WMI 事件。
- 为接收 AD 登录事件的 WMI 节点创建 Active Directory 域控制器列表。

- 确定Cisco ISE 必须加入的 Microsoft 域以从 Active Directory 中提取用户组。
- 确定在授权策略中用于参考的 Active Directory 组。
- 如果您使用 pxGrid 与其他支持 pxGrid 的系统共享来自网络设备的会话数据，则需要在您的部署中定义 pxGrid 角色。有关 pxGrid 的详细信息，请参阅 思科 pxGrid 节点
- 在 MAB 成功之后，NAD 必须提供一个具有限访问权限的配置文件，该配置文件允许该端口的用户访问 Active Directory 服务器（如概述中所述）。

注释 被动身份服务可在多个节点上启用，但是，Easy Connect 一次只能在一个节点上运行。如果您在多个节点上启用该服务，ISE 会自动确定使用哪个节点用于活动的 Easy Connect 会话。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开一个节点，然后在**常规设置 (General Settings)** 之下，启用**启用被动身份服务 (Enable Passive Identity Service)**。

步骤 2 配置要由 Easy Connect 使用的 Active Directory 加入点和域控制器。有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求 ， 第 62 页。

步骤 3 （可选）选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。点击**组 (Groups)** 选项卡，然后添加您计划在授权策略中使用的 Active Directory 组。
为域控制器映射的 Active Directory 组会在 PassiveID 字典中动态更新，然后可以在您设置策略条件规则时使用。

步骤 4 **注释** 为了便于 Easy Connect 进程正常运行以及使 ISE 能够发出 CoA，必须为所有用于 Easy Connect 授权的配置文件启用**被动身份跟踪 (Passive Identity Tracking)**。

选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。对于所有 Easy Connect 要使用的配置文件，请打开配置文件并启用**被动身份跟踪 (Passive Identify Tracking)** 选项。

步骤 5 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **授权 (Authorization)** > **简单条件 (Simple Conditions)**，为 Easy Connect 创建规则。点击**添加 (Add)** 并定义条件：

a) 输入名称和说明。
b) 从**属性 (Attribute)** 选项，转至 PassiveID 字典并选择 PassiveID_Groups 为域控制器组创建条件或选择 PassiveID_user 为单个用户创建条件。
c) 输入正确的操作。
d) 输入策略中需包含的用户名或组名。

步骤 6 点击**提交 (Submit)**。

配置 Easy Connect 可视性模式

开始之前

- 为了获得最佳性能，请部署专用的 PSN 来接收 WMI 事件。

- 为接收 AD 登录事件的 WMI 节点创建 Active Directory 域控制器列表。
- 确定Cisco ISE 必须加入的 Microsoft 域以从 Active Directory 中提取用户组。
- 如果您使用 pxGrid 与其他支持 pxGrid 的系统共享来自网络设备的会话数据，则需要在您的部署中定义 pxGrid 角色。有关 pxGrid 的详细信息，请参阅 思科 pxGrid 节点

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开一个节点，然后在**常规设置 (General Settings)** 之下，启用**启用被动身份服务 (Enable Passive Identity Service)**。

步骤 2 配置要由 Easy Connect 使用的 Active Directory 加入点和域控制器。有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求 ， 第 62 页。

被动 ID 工作中心

被动身份连接器(被动ID工作中心)提供集中的一站式安装和实施，使您能够轻松简单地配置网络，以便接收用户身份信息并与各种不同的安全产品用户（例如Cisco Firepower 管理中心 [FMC] 和 Stealthwatch）进行共享。作为用于被动识别的全面代理，被动 ID 工作中心 从不同提供程序源（例如 Active Directory 域控制器 [AD DC]）收集用户身份，将用户登录信息映射到使用中的相关 IP 地址，然后将该映射信息与已配置的任何用户安全产品进行共享。

什么是被动身份？

由思科身份服务引擎 (ISE) 提供的标准流程，用于提供身份验证、授权和记账 (AAA) 服务器，并利用 802.1X 或 Web 身份验证之类的技术，直接与用户或终端进行通信，从而请求访问网络，然后使用其登录凭证来确认其身份并主动进行身份验证。

被动身份服务不直接对用户进行身份验证，而是从 Active Directory 之类的外部身份验证服务器（称为提供程序）收集用户身份和 IP 地址，然后与用户共享该信息。被动 ID 工作中心首先从提供程序接收用户身份信息（通常根据用户登录名和密码），然后执行必要的检查和服务，以便将用户身份与相关 IP 地址进行匹配，从而向用户传送经过身份验证的 IP 地址。

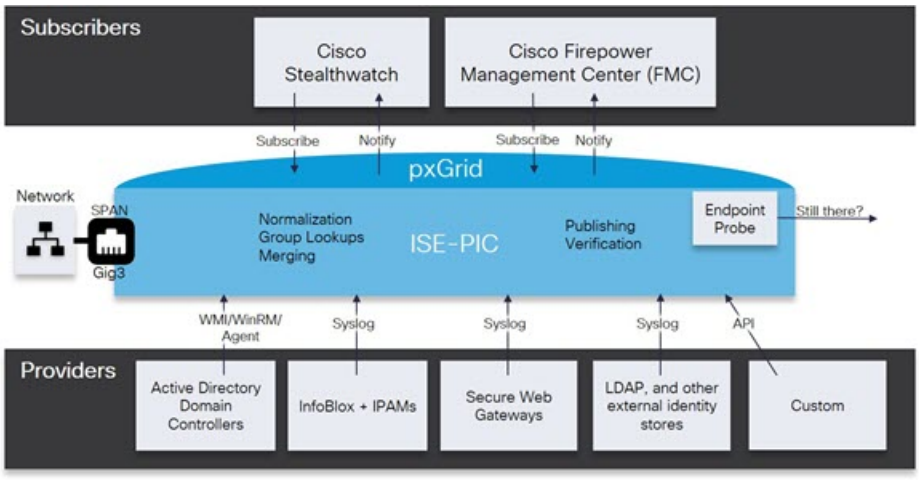
Passive Identity Connector (被动 ID 工作中心) 流程

被动 ID 工作中心 的流程如下：

1. 提供程序对用户或终端执行身份验证。
2. 提供程序将经过身份验证的用户信息发送到Cisco ISE。
3. 思科 ISE 将用户信息规范化，执行查找、合并、解析并将其映射到 IP 地址，然后将映射的详细信息发布到 pxGrid。
4. pxGrid 用户接收映射的用户详细信息。

下图说明了思科 ISE 提供的概要流程。

图 *11:* 概要流程



初始设置和配置

要快速开始使用Cisco 被动 ID 工作中心，请遵循以下流程：

1. 确保您已正确配置 DNS 服务器，包括从Cisco ISE 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， 第 41 页。
2. 在您打算用于任何被动身份服务的专用策略服务器 (PSN) 上启用被动身份和 pxGrid 服务。选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开相关节点，并在**常规设置 (General Settings)** 下启用**开启被动身份服务 (Enable Passive Identity Service)** 和 **pxGrid**。
3. 同步 NTP 服务器的时钟设置。
4. 使用 ISE 被动身份设置来配置初始提供程序。有关详细信息，请参阅PassiveID 设置入门 ， 第 79 页
5. 配置单个或多个用户。有关详细信息，请参阅用户 ， 第 120 页

设置初始提供程序和用户后，可以轻松创建其他提供程序（请参阅其他被动身份服务提供程序，第 84 页）并从 被动 ID 工作中心：

- RADIUS实时会话 (Live Sessions)
- 思科 ISE 警报

被动 ID 工作中心 控制板 (Dashboard)

Cisco被动 ID 工作中心 控制板显示对于有效监控和故障排除很重要的综合性相关摘要和统计数据，并实时更新。Dashlet 显示过去 24 小时的活动，另有说明的情况除外。要访问控制板，请依次选择 **工作中心 (Work Centers)** > **被动 ID (PassiveID)**，然后从左侧面板中选择**控制板 (Dashboard)**。只能在主管理节点 (PAN) 上查看Cisco 被动 ID 工作中心 控制板。

- **主要 (Main)** 视图具有线性指标控制板、饼形图 Dashlet 和列表 Dashlet。在 被动 ID 工作中心 中，Dashlet 不可配置。可用 Dashlet 包括：
  - **被动身份指标 (Passive Identity Metrics)** - 显示当前跟踪的唯一实时会话总数、系统中配置的身份提供程序总数、主动提供身份数据的代理总数，以及当前配置的用户总数。
  - **提供程序** - 提供程序向 被动 ID 工作中心 提供用户身份信息。可以配置 ISE 探测器（从给定源收集数据的机制），并通过此探测器从提供程序源接收信息。例如，Active Directory (AD) 探测器和代理探测器均可帮助 ISE-PIC 从 AD 收集数据（每个采用不同的技术），而系统日志探测器可从读取系统日志消息的解析器收集数据。
  - **用户 (Subscribers)** - 用户连接至 ISE 以解锁用户身份信息。
  - **操作系统类型 (OS Types)** - 可以显示的唯一操作系统类型为 Windows。Windows 类型按 Windows 版本显示。提供程序不报告操作系统类型，但 ISE 可查询 Active Directory 以获取此信息。Dashlet 中最多显示 1000 个条目。
  - **警报 (Alarms)** - 用户身份相关警报。

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。

AD 探测器 (被动身份服务) 通过 WMI 技术从 AD 收集用户身份信息，而其他探测器则通过其他技术和方法将 AD 用作用户身份提供程序。有关 ISE 提供的其他探测器和提供程序类型的详细信息，请参阅其他被动身份服务 提供程序，第 84 页。

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，第 86 页

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

- SPAN，第 95 页
- 终端探测器，第 117 页

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 48 页。

设置 Active Directory (WMI) 探测

要为被动身份服务配置 Active Directory 和 WMI，可以使用被动 ID 工作中心向导（请参阅PassiveID 设置入门 ，第 79 页），也可以遵循如下步骤：

1. 配置 Active Directory 探测器。请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点 ，第 42 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。请参阅添加域控制器 ，第 44 页。
3. 配置 Active Directory，以使其与 ISE 集成。请参阅对被动 ID 配置 WMI ，第 46 页。
4. （可选）管理 Active Directory 提供程序 ，第 81 页。

有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求 ，第 62 页。

PassiveID 设置入门

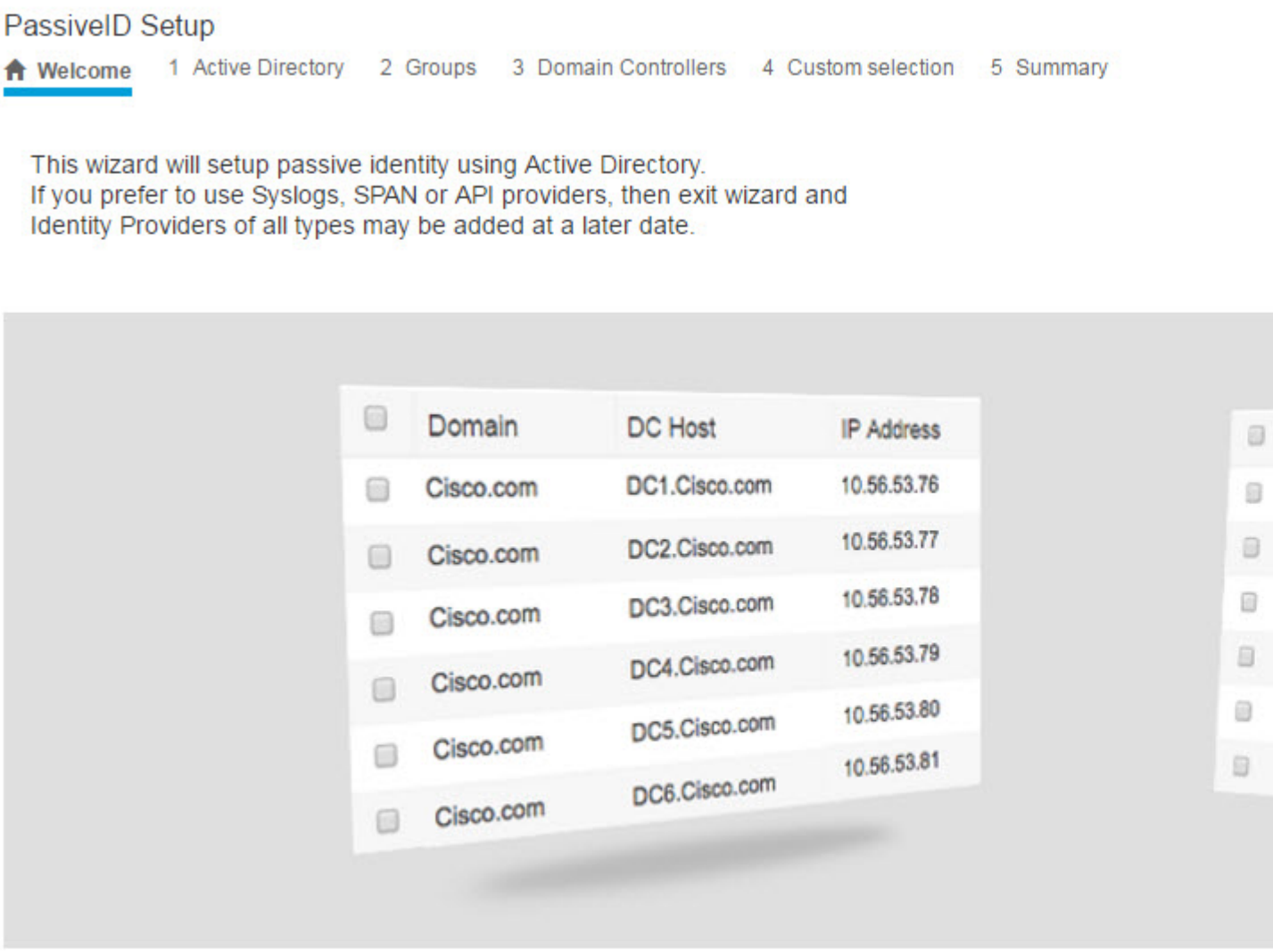
ISE-PIC 提供向导，从中可以轻松快速地将 Active Directory 配置为第一个用户身份提供程序，以便从 Active Directory 接收用户身份。通过为 ISE-PIC 配置 Active Directory，还可以简化稍后配置其他提供程序类型的过程。一旦配置了 Active Directory，就必须配置用户（例如Cisco Firepower 管理中心 (FMC) 或 Stealthwatch），以便定义将要接收用户数据的客户端。有关用户的详细信息，请参阅用户 ，第 120 页。

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。
- 确保您在 ISE 中具有超级管理员或系统管理员权限。
- 在您打算用于任何被动身份服务的专用策略服务器 (PSN) 上启用被动身份和 pxGrid 服务。选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开相关节点，并在**常规设置 (General Settings)** 下启用**开启被动身份服务 (Enable Passive Identity Service)** 和 **pxGrid**。
- 确保 ISE 在域名服务器 (DNS) 中具有条目。确保您已从 ISE 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 ，第 41 页

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID**。从“被动身份连接器概述”屏幕中，点击**被动身份向导**。

图 *12: 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。有关 Active Directory 设置的详细信息，请参阅Active Directory 设置，第 81 页。

强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存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”，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，请参阅其他被动身份服务 提供程序，第 84 页。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。有关详细信息，请参阅用户，第 120 页。

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：

- 就 Active Directory 测试用户 (Test Users for Active Directory)身份验证，第 55 页
- 查看节点的 Active Directory 加入，第 56 页
- 诊断 Active Directory 问题，第 56 页
- 退出 Active Directory 域，第 47 页
- 删除 Active Directory 配置，第 56 页
- 启用 Active Directory 调试日志，第 57 页

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，请选择 **工作中心 (Work Centers)** > **PassiveID** > **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 节点加入到该加入点，第 42 页。

表 *16: 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 (Store credentials)	强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存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**。

表 *17: 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	使用 ISE 加入 Active Directory 林时，此字段按照特定 Active Directory 站点在“Active Directory 站点和服务”区域中的显示来指示林中的该站点。

表 *18:* 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	使用 ISE 加入 Active Directory 林时，此字段按照特定 Active Directory 站点在“Active Directory 站点和服务”区域中的显示来指示林中的该站点。
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，第 86 页。

表 *19:* 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。
说明	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，第 86 页。

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。

表 *20: 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，思科 ISE 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 作为思科 ISE 和 DC 之间的通信协议。NTLMv2 是建议默认值。

其他被动身份服务 提供程序

为了使 ISE 能够向订用服务的使用者（用户）提供身份信息（被动身份服务 ），您必须首先配置 ISE 探测器，它连接到身份提供程序。

下表提供了有关 ISE 中所有提供程序和探测类型的详细信息。有关 Active Directory 的详细信息，请参阅 Active Directory 作为探测器和提供程序， 第 78 页。

您可以定义下列提供程序类型：

表 *21:* 提供程序类型

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
Active Directory (AD)	用于从中接收用户信息的高度安全而精确且最常用的源。 作为探测器，AD 运用 WMI 技术传送经过身份验证的用户身份。 此外，AD 本身而不是探测器，而是用作其他探测器从中检索用户数据的源系统（提供程序）。	Active Directory 域控制器	WMI	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 作为探测器和提供程序，第 78 页
代理	Active Directory 域控制器或成员服务器上安装的本地 32 位应用。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。		域控制器或成员服务器上安装的代理。	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 代理，第 86 页
终端	除其他已配置的探测器以外，始终在后台运行，以便验证用户是否仍然处于连接状态。		WMI	用户是否仍然处于连接状态	终端探测器，第 117 页
SPAN	位于网络交换机上，以便侦听网络流量并根据 Active Directory 数据提取用户身份信息。		交换机上安装的 SPAN，以及 Kerberos 消息	• 用户名 • IP 地址 • 域 (Domain)	SPAN，第 95 页

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
API 提供程序	使用 ISE 提供的 RESTful API 服务从编程为与 RESTful API 客户端进行通信的任何系统收集用户身份信息。	编程为与 REST API 客户端进行通信的任何系统。	RESTful API。以 JSON 格式发送到用户的用户身份。	• 用户名 • IP 地址 • 端口范围 • 域	API 提供程序，第 90 页
系统日志	解析系统日志消息和检索用户身份，包括 MAC 地址。	• 常规系统日志消息提供程序 • DHCP 服务器	系统日志消息	• 用户名 • IP 地址 • MAC 地址 • 域	系统日志提供程序，第 96 页

Active Directory 代理

从 被动身份服务 工作中心在 Active Directory (AD) 域控制器 (DC) 或成员服务器上的任意位置（根据配置）安装本地 32 位应用（即域控制器 [DC] 代理），以从 AD 检索用户身份信息，然后将这些身份发送给已配置的用户。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。代理可安装在单独的域中，也可安装在 AD 域中，并且一旦安装，它们就会每分钟提供一次 ISE 的状态更新。

代理可由 ISE 自动安装和配置，您也可以手动对其进行安装。安装时，会发生以下情况：

- 代理及其关联文件安装在以下路径：**`Program Files/Cisco/Cisco ISE PassiveID Agent`**
- 系统将安装一个名为 **`PICAgent.exe.config`** 的配置文件，其中会指示代理的日志记录级别。您可以从该配置文件内手动更改日志记录级别。
- CiscoISEPICAgent.log 文件与所有日志记录消息一起存储。
- nodes.txt 文件包含部署中可与代理进行通信的所有节点的列表。代理会访问列表中的第一个节点。如果无法访问该节点，代理将根据列表中节点的顺序继续尝试通信。对于手动安装，必须打开文件并输入节点 IP 地址。（手动或自动）安装完成后，便只能通过手动更新该文件来对其进行更改。打开文件，然后根据需要添加、更改或删除节点 IP 地址。
- Cisco ISE PassiveID 代理服务在机器上运行，您可从“Windows 服务”对话框管理该机器。
- ISE 最多支持 100 个域控制器，而每个代理最多可以监控 10 个域控制器。

注释 要监控 100 个域控制器，必须配置 10 个代理。

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

如果无法安装代理，则对被动身份服务使用 Active Directory 探测器。有关详细信息，请参阅Active Directory 作为探测器和提供程序，第 78 页。

自动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何自动安装并配置代理以监控域控制器。

开始之前

准备工作：

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE 的 DNS 服务器配置要求的详细信息，请参阅DNS 服务器，第 41 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 活动的被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 77 页。
- 创建AD加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序，第 78 页。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 48 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 2 要添加新客户端，请从表的顶部点击**添加 (Add)**。

步骤 3 要创建新代理并将其自动安装到您在此配置中指示的主机上，请选择**部署新代理 (Deploy New Agent)**。

步骤 4 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅Active Directory 代理设置，第 89 页。

步骤 5 点击 **Deploy**（部署）。
代理将根据您在配置中指示的域自动安装到主机上，并保存设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 6 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory** 以查看当前配置的所有接入点。

步骤 7 点击您要从中启用所创建代理的接入点的链接。

步骤 8 选择**被动 ID (Passive ID)** 选项卡以配置您作为先决条件的一部分而添加的域控制器。

步骤 9 选择您要通过所创建代理来监控的域控制器，然后点击**编辑 (Edit)**。

步骤 10 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 11 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您为代理创建的用户名和密码凭证（如果有），然后点击**保存 (Save)**。

手动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何手动安装并配置代理以监控域控制器。

开始之前

准备工作：

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器，第 41 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 活动的被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 77 页。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序，第 78 页。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 48 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 2 点击**下载代理 (Download Agent)** 以下载 **`picagent-installer.zip`** 文件进行手动安装。
此文件将下载至标准 Windows 下载文件夹。

步骤 3 将此 zip 文件置于指定主机并运行安装。

步骤 4 在 ISE GUI 中，再次选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 5 要配置新代理，请从表的顶部点击**添加 (Add)**。

步骤 6 要配置已在主机上安装的代理，请选择**注册现有代理 (Register Existing Agent)**。

步骤 7 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅Active Directory 代理设置，第 89 页。

步骤 8 点击**保存 (Save)**。
系统会保存代理设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 9 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory** 以查看当前配置的所有接入点。

步骤 10 点击您要从中启用所创建代理的接入点的链接。

步骤 11 选择**被动 ID (Passive ID)** 选项卡以配置您作为先决条件的一部分而添加的域控制器。

步骤 12 选择您要通过所创建代理来监控的域控制器，然后点击**编辑 (Edit)**。

步骤 13 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 14 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您为代理创建的任何用户名和密码凭证，然后点击**保存 (Save)**

卸载代理

可以直接从 Windows 轻松（手动）卸载自动或手动安装的代理。

步骤 1 在 Windows 对话框中，转至**程序和功能**。

步骤 2 在已安装程序的列表中，查找并选择Cisco ISE 被动 ID 代理。

步骤 3 点击**卸载**。

Active Directory 代理设置

允许 ISE 在网络中的指定主机上自动安装代理，以从不同的域控制器 (DC) 检索用户身份信息并向被动身份服务 订户提供此信息。

要创建和管理代理，请选择 **提供程序 (Providers)** > **代理 (Agents)**. 请参阅自动安装并部署 Active Directory 代理，第 87 页。

表 *22:* 代理窗口

字段名称	说明
名称	您配置的代理名称。
主机	安装代理的主机的完全限定域名。
监控	此为指定代理所监控的域控制器的逗号分隔列表。

表 *23:* 新建代理 *(Agents New)*

字段	说明
“部署新代理”(Deploy New Agent) 或“注册现有代理”(Register Existing Agent)	• “部署新代理”(Deploy New Agent)：在指定主机上安装新代理。 • “注册现有代理”(Register Existing Agent)：在主机上手动安装代理，然后从此屏幕为 被动身份服务 配置此代理以启用服务。
名称	输入可用于轻松识别代理的名称。
说明	输入可用于轻松识别代理的说明。
主机 FQDN	此为已安装代理（注册现有代理）或将要安装代理（自动部署）的主机的完全限定域名。
用户名	输入用户名以访问要安装代理的主机。 被动身份服务 将使用这些凭证为您安装代理。
密码	输入用户密码以访问要安装代理的主机。 被动身份服务 将使用这些凭证为您安装代理。

API 提供程序

通过Cisco ISE 中的“API 提供程序”功能，可将用户身份信息从自定义程序或从终端服务器 (TS) 代理推送到内置的 ISE 被动身份服务 REST API 服务。通过此方式，可以自定义网络中的可编程客户端，以将从任何网络访问控制 (NAC) 系统收集到的用户身份发送到服务。此外，通过Cisco ISE API 提供程序，还可与网络应用（例如 Citrix 服务器上的 TS 代理，其中所有用户都具有同一 IP 地址但分配有唯一端口）接合。

例如，在 Citrix 服务器上运行的用于为根据 Active Directory (AD) 服务器进行身份验证的用户提供身份映射的代理可向 ISE 发送 REST 请求，请求只要有新用户登录或注销便添加或删除用户会话。然后，ISE 获取从客户端传送的用户身份信息（包括 IP 地址和已分配的端口），并将其发送到预配置用户，例如Cisco Firepower 管理中心 (FMC)。

ISE REST API 框架通过 HTTPS 协议实施 REST 服务（无需客户端证书验证），并以 JSON (JavaScript Object Notation) 格式传送用户身份信息。有关 JSON 的详细信息，请参阅 http://www.json.org/。

ISE REST API 服务会解析用户身份，此外还会将该信息映射到端口范围，以便区分同时登录到一个系统的不同用户。每次将端口分配给用户时，API 都会向 ISE 发送一条消息。

REST API 提供程序流程

配置了从 ISE 到自定义客户端的网桥后（通过将该客户端声明为 ISE 的提供程序，并使该特定自定义程序 (客户端) 能够发送 RESTful 请求），ISE REST 服务便通过以下方式进行工作：

1. 对于客户端身份验证，Cisco ISE 需要身份验证令牌。客户端机器上的自定义程序在发起联系时发送身份验证令牌的请求，然后 ISE 每次都会通知先前令牌已到期。系统会返回令牌以响应请求，从而启用客户端和 ISE 服务之间的持续通信。
2. 用户登录到网络中后，客户端便会检索用户身份信息，并使用 API 添加命令将该信息发布到 ISE REST 服务。
3. Cisco ISE 接收并映射用户身份信息。
4. Cisco ISE 向用户发送已映射的用户身份信息。
5. 只要有必要，自定义机器即可发送用于移除用户信息的请求，方法是发送“删除 API”调用并包含在发送“添加”调用后作为响应接收到的用户 ID。

在 ISE 中使用 REST API 提供程序

按照以下步骤激活 ISE 中的 REST 服务：

1. 配置客户端。有关详细信息，请参阅客户端用户文档。
2. 激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置， 第 77 页。
3. 确保您已正确配置 DNS 服务器，包括从 ISE 配置客户端机器的反向查找。有关 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器， 第 41 页
4. 请参阅为 被动身份服务 配置与 ISE REST 服务的桥接， 第 91 页。

注释 要将 API 提供程序配置为使用 TS 代理，请在创建从 ISE 到该代理的网桥时添加 TS 代理信息，然后参考 TS 代理文档以获取有关发送 API 调用的信息。

5. 生成身份验证令牌并向 API 服务发送添加和删除请求。

为 被动身份服务 配置与 ISE REST 服务的桥接

为了使 ISE REST API 服务能够从特定客户端接收信息，必须首先从 ISE 定义该特定客户端。您可以定义多个具有不同 IP 地址的 REST API 客户端。

开始之前

准备工作：

- 确保您已激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置， 第 77 页。
- 确保您已正确配置 DNS 服务器，包括从Cisco ISE 配置客户端机器的反向查找。有关Cisco ISE 的 DNS 服务器配置要求的详细信息，请参阅DNS 服务器， 第 41 页

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **API 提供程序 (API Providers)**

系统将显示“API 提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要添加新客户端，请从表的顶部点击**添加**。

步骤 3 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅API 提供程序设置，第 92 页。

步骤 4 点击**提交 (Submit)**。
系统将保存客户端配置，并其屏幕会显示更新后的“API 提供程序”表。客户端现在可以将发布内容发送到 ISE REST 服务。

下一步做什么

设置自定义客户端，以将身份验证令牌和用户身份发布到 ISE REST 服务。请参阅将 API 调用发送到 被动 ID REST 服务，第 92 页。

将 API 调用发送到 被动 ID REST 服务

开始之前

为 被动身份服务 配置与 ISE REST 服务的桥接，第 91 页

步骤 1 在浏览器的地址栏中输入Cisco ISE URL（例如 *https://<ise hostname or ip address>/admin/*）

步骤 2 在以下位置中输入已从“API 提供程序”屏幕中指定并配置的用户名和密码：ISE GUI。有关详细信息，请参阅为 被动身份服务 配置与 ISE REST 服务的桥接，第 91 页。

步骤 3 按 **Enter** 键。

步骤 4 在目标节点的“URL 地址”(URL Address) 字段中输入 API 调用。

步骤 5 点击**发送**以发出 API 调用。

下一步做什么

请参阅 API 调用，第 93 页以获取有关不同 API 调用、其架构及其结果的更多信息和详细信息。

API 提供程序设置

注释 完整 API 定义和对象架构可通过请求调用进行检索，如下所示：

- 对于完整 API 规范 (wadl) - https://YOUR_ISE:9094/application.wadl
- 对于 API 模型和对象方案 - https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *24: API* 提供程序设置

字段	说明
名称 (Name)	输入此客户端的用于快速轻松地将其与其他客户端进行区分的唯一名称。
说明	输入此客户端的明确说明。
状态	选择**已启用 (Enabled)** 以使客户端能够在完成配置时立即与 REST 服务进行交互。
主机/IP	输入客户端主机器的 IP 地址。确保您已正确配置 DNS 服务器，包括从 ISE 配置客户端机器的反向查找。
用户名	创建在发布到REST服务时要使用的唯一用户名。
密码	创建在发布到 REST 服务时要使用的唯一密码。

API 调用

这些 API 调用用于通过Cisco ISE 来管理 被动身份服务 的用户身份事件。

目的：生成身份验证令牌

- **请求**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  请求应包含 BasicAuth 授权报头。提供先前从 ISE-PIC GUI 创建的 API 提供程序凭证。有关详细信息，请参阅API 提供程序设置，第 92 页。

- **响应报头**

  该报头包含 X-auth-access-token。这是发布其他 REST 请求时要使用的令牌。

- **响应正文**

  HTTP 204 No Content

目的：添加用户

- **请求**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  在发布请求标头中添加 X-auth-access-token，例如，标头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

  201创建

- 响应正文

  {

  "user": "<username>",

  "srcPatRange": {

  "userPatStart": <user PAT start value>,

  "userPatEnd": <user PAT end value>,

  "patRangeStart": <PAT range start value>

  },

  "srcIpAddress": "<src IP address>",

  "agentInfo": "<Agent name>",

  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<domain>"

  }

- 注

  - 可在以上 JSON 中删除 srcPatRange 以创建单个 IP 用户绑定。
  - 响应正文包含“ID”，这是所创建的用户会话绑定的唯一标识符。发送 DELETE 请求时使用此 ID，以指示应删除哪个用户。
  - 此响应还包含自链接，这是此新创建的用户会话绑定的 URL。

目的：删除用户

- 请求

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  在 <id> 中，输入从“添加”响应接收到的 ID。

  在删除请求信头中添加 X-auth-access-token，例如，信头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

  200 OK

- 响应正文

  响应正文包含有关已删除的用户会话绑定的详细信息。

SPAN

SPAN 是 被动身份服务，可以让您快速轻松地启用Cisco ISE 以侦听网络和检索用户信息，而不必将 Active Directory 配置为直接使用Cisco ISE。SPAN 嗅探网络流量（专门检查 Kerberos 消息），提取 Active Directory 也已存储的用户身份信息，并将该信息发送到 ISE。然后，ISE 解析信息，最终将用户名、IP 地址和域名传送到您也已从 ISE 配置的用户。

为了使 SPAN 侦听网络和提取 Active Directory 用户信息，ISE 和 Active Directory 必须连接到网络上的同一交换机。这样，SPAN 便可以从 Active Directory 复制并镜像所有用户身份数据。

使用 SPAN，将通过以下方式检索用户信息：

1. 用户终端登录网络。
2. 登录和用户数据存储在 Kerberos 消息中。
3. 一旦用户登录且用户数据通过交换机进行传递，SPAN 就会镜像网络数据。
4. Cisco ISE 侦听网络以获取用户信息，并从交换机检索镜像的数据。
5. Cisco ISE 解析用户信息并更新被动 ID 映射。
6. Cisco ISE 将已解析的用户信息传送到用户。

使用 SPAN

开始之前

要使 ISE 从网络交换机接收 SPAN 流量，必须先定义侦听此交换机的节点和节点接口。可以配置 SPAN 以侦听安装的不同 ISE 节点。对于每个节点，只能配置一个接口来侦听网络，用于侦听的接口只能专用于 SPAN。

在开始之前，请确保您已激活被动 ID 和 pxGrid 服务。只有已启用被动 ID 的节点才会显示在可用于配置 SPAN 的接口列表中。有关详细信息，请参阅初始设置和配置，第 77 页。

此外，您必须牢记：

- 确保已在网络上配置 Active Directory。
- 在同样连接至 Active Directory 的网络中的交换机上运行 CLI，以确保交换机可以与 ISE 通信。
- 配置交换机以从 AD 镜像网络。
- 配置专用于 SPAN 的 ISE 网络接口卡 (NIC)。此 NIC 仅用于 SPAN 流量。
- 通过命令行界面，确保激活专用于 SPAN 的 NIC。
- 创建仅将 Kerberos 流量发送到 SPAN 端口的 VACL。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **SPAN** 以配置 SPAN。

步骤 2 注释　建议 GigabitEthernet0 网卡 (NIC) 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

输入有意义的说明（可选），选择状态**已启用 (Enabled)**，并选择将用于侦听网络交换机的节点和相关 NIC。有关详细信息，请参阅SPAN 设置，第 96 页。

步骤 3 点击**保存 (Save)**。
系统将保存 SPAN 配置， ISE-PIC ISE 现在主动侦听网络流量。

SPAN 设置

从已部署的每个节点，通过在客户端网络上安装 SPAN，可快速轻松地配置 ISE 以接收用户身份。

表 25: SPAN 设置

字段	说明
说明	输入唯一说明以向您提醒当前启用的节点和接口。
状态	选择**已启用 (Enabled)** 可在完成配置时立即启用客户端。
接口 NIC (Interface NIC)	为 ISE 选择一个或两个节点，然后对于每个选定节点，选择用于侦听网络以获取信息的节点接口。 **注释** 建议将 GigabitEthernet0 NIC 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

系统日志提供程序

被动身份服务会解析来自任何传送系统日志消息的客户端（身份数据提供程序）的系统日志消息，包括常规系统日志消息（来自 InfoBlox、Blue Coat、BlueCat 和 Lucent 之类的提供程序）以及 DHCP 系统日志消息，并发回用户身份信息，包括 MAC 地址。然后将此映射的用户身份数据传送到用户。

您可以指定接收用户身份数据的系统日志客户端（请参阅配置系统日志客户端，第 97 页）。配置提供程序时，您必须指定连接方法（TCP 或 UDP）以及要用于解析的系统日志模板。

注释 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则 ISE 会尝试将数据包中接收到的 IP 地址与已为 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。要查看此列表，请依次选择**工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)** > **系统日志提供程序 (Syslog Providers)**。建议您检查消息报头并根据需要进行自定义，以便保证解析成功。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 103 页。

系统日志探测器会将接收到的系统日志消息发送到 ISE 解析器，该解析器会映射用户身份信息，并将该信息发布到 ISE。然后， ISE 将已解析和已映射的用户身份信息传送给 被动身份服务用户。

要从 ISE-PIC ISE 解析用户身份的系统日志消息，请执行以下操作：

- 配置要从中接收用户身份数据的系统日志客户端。请参阅配置系统日志客户端，第 97 页。
- 自定义单个消息报头。请参阅自定义系统日志报头，第 103 页。
- 通过创建模板来自定义消息正文。请参阅自定义系统日志消息正文，第 102 页。
- 在将系统日志客户端配置为用于解析的消息模板时使用 ISE 中预定义的消息模板，或者基于这些预定义的模板自定义报头或正文模板。请参阅使用系统日志预定义消息模板，第 106 页。

配置系统日志客户端

为了使Cisco ISE 能够从特定客户端侦听系统日志消息，必须首先从Cisco ISE 定义该特定客户端。您可以使用不同 IP 地址定义多个提供程序。

开始之前

在开始之前，请确保您已激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 77 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要配置新系统日志客户端，请从表的顶部点击**添加**。

步骤 3 填写所有必填字段（请参阅系统日志设置，第 97 页以获取更多详细信息），并在必要时创建消息模板（请参阅自定义系统日志消息正文，第 102 页以获取更多详细信息），以便正确配置客户端。

步骤 4 点击**提交 (Submit)**。

系统日志设置

配置Cisco ISE 以通过来自特定客户端的系统日志消息接收用户身份，包括 MAC 地址。您可以使用不同 IP 地址定义多个提供程序。

表 *26:* 系统日志提供程序

字段名称	说明
名称	输入用于快速轻松地区分此已配置客户端的唯一名称。
说明	此系统日志提供程序的有意义说明。
状态	选择**已启用 (Enabled)** 可在完成配置时立即启用客户端。
主机	输入主机器的 FQDN。
连接类型	输入 UDP 或 TCP 以指示 ISE 用于侦听系统日志消息的通道。 **注释** 当所配置的连接类型为 TCP 时，如果消息信头存在问题且无法解析主机名，则思科 ISE 会尝试将数据包中接收到的 IP 地址与已为思科 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。 要查看此列表，请依次选择**工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)** > **系统日志提供程序 (Syslog Providers)**。建议您检查消息信头并根据需要进行自定义，以便确保解析成功。有关自定义信头的详细信息，请参阅自定义系统日志报头，第 103 页。

字段名称	说明
模板	

字段名称	说明
	模板指示精确正文消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。 例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。 从此字段中，指示要使用的模板（适用于系统日志消息的正文），以便识别并正确解析系统日志消息。 从预定义下拉列表中进行选择，或者点击**新建**以创建自己的自定义模板。有关创建新模板的详细信息，请参阅自定义系统日志消息正文，第 102 页。大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。 **注释** 只能编辑或删除自定义模板，而无法修改下拉列表中的预定义系统模板。 ISE 当前提供下列预定义 DHCP 提供程序模板： • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP **注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的DHCP 系统日志消息中列出的IP地址进行匹配，从而正确解析和传送用户身份信息。 如果从DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。 Cisco ISE 提供下列预定义常规系统日志提供程序模板：

字段名称	说明
	• ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 有关模板的信息，请参阅使用系统日志预定义消息模板，第 106 页。
默认域	如果在特定用户的系统日志消息中未识别域，则会将此默认域自动分配给用户，以便确保为所有用户都分配域。 通过默认域或通过从消息中解析的域，会将用户名附加到 username@domain，从而包含该域，以便获取有关用户和用户组的详细信息。

自定义系统日志消息结构（模板）

模板指示精确消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。模板可确定新增和删除映射消息的受支持结构。

通过Cisco ISE，您可以自定义单个消息报头和多个正文结构以供 被动 ID 解析器使用。

模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 被动 ID 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

自定义消息模板时，可以选择基于 ISE-PIC ISE 中预定义的消息模板进行自定义，参考这些预定义选项中使用的正则表达式和消息结构。有关预定义模板、正则表达式、消息结构、示例等的详细信息，请参阅使用系统日志预定义消息模板，第 106 页。

可以自定义：

- 单个消息报头 -自定义系统日志报头，第 103 页
- 多个消息正文 - 自定义系统日志消息正文，第 102 页。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

自定义系统日志消息正文

通过Cisco ISE，您可以自定义将由 被动 ID 解析器解析的自有系统日志消息模板（通过自定义消息正文）。模板应包含正则表达式，以定义用户名、IP 地址、MAC 地址和域的结构。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

从系统日志客户端配置屏幕中创建和编辑系统日志消息正文模板。

注释 您只能编辑自己的自定义模板。无法更改系统提供的预定义模板。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 点击**添加 (Add)**以添加新系统日志客户端，或者点击**编辑 (Edit)**来更新已配置的客户端。有关配置和更新系统日志客户端的详细信息，请参阅配置系统日志客户端，第 97 页。

步骤 3 在**系统日志提供程序 (Syslog Providers)** 窗口中，点击**新建 (New)** 以创建新消息模板。要编辑现有模板，请从下拉列表中选择该模板，然后点击**编辑 (Edit)**。

步骤 4 填写所有必填字段。

有关如何正确输入值的信息，请参阅系统日志自定义模板设置和示例，第 104 页。

步骤 5 点击**测试**以根据所输入的字符串正确解析消息。

步骤 6 点击**保存 (Save)**。

自定义系统日志报头

系统日志报头还包含消息源于的主机名。如果Cisco ISE 消息解析器未识别系统日志消息，则可能需要通过配置前置于主机名的分隔符来自定义消息报头，从而使Cisco ISE 能够正确识别主机名并解析消息。有关此屏幕中的字段的更多详细信息，请参阅系统日志自定义模板设置和示例，第 104 页。只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

注释 只能自定义单个报头。自定义信头后，点击**自定义信头 (Custom Header)** 并创建模板时，仅会保存最新的配置。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 点击**自定义报头**以打开“系统日志自定义报头”屏幕。

步骤 3 在**粘贴示例系统日志 (Paste sample syslog)** 字段中，输入系统日志消息中报头格式的示例。例如，从其中一条消息复制并粘贴以下信头：**<181>Oct 10 15:14:08 Cisco.com**。

步骤 4 在**分隔符 (Separator)** 字段中，指示单词是以空格还是制表符分隔。

步骤 5 在**报头中的主机名位置 (Position of hostname in header)** 字段中，指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。

主机名 (Hostname) 字段根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下：

<181>Oct 10 15:14:08 Cisco.com

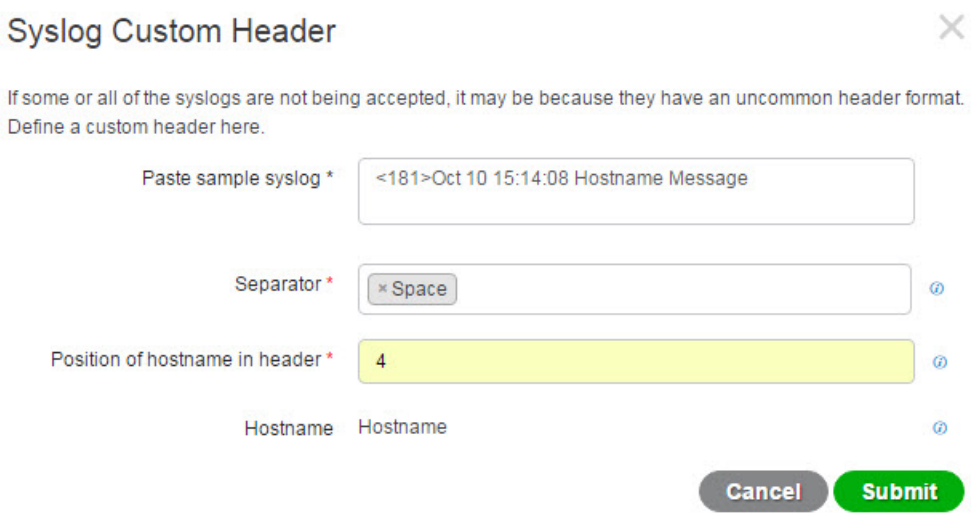
分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。

主机名将自动显示为 Cisco.com，这是**粘贴示例系统日志**字段中粘贴的报头短语中的第四个单词。

如果未正确显示主机名，请检查您已在**分隔符 (Separator)** 和**报头中的主机名位置 (Position of hostname in header)** 字段中输入的数据。

此示例与以下截屏相同：

图 *13:* 自定义系统日志报头



步骤 6 点击**提交 (Submit)**。

只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

系统日志自定义模板设置和示例

通过Cisco ISE，您可以自定义将由 被动 ID 解析器解析的自有系统日志消息模板。自定义模板确定了新增和删除映射消息的受支持结构。模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 被动 ID 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

注释 大多数预定义模板都使用正则表达式。自定义模板也应使用正则表达式。

系统日志报头部分

您可以通过配置前置于主机名的分隔符来自定义系统日志探测器可识别的单个报头。

下表介绍可在自定义系统日志报头中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 29: 自定义模板的正则表达式，第 106 页。

表 *27:* 系统日志自定义报头

字段	说明
粘贴示例系统日志	输入系统日志消息中的报头格式的示例。例如，复制并粘贴以下报头： **`<181>Oct 10 15:14:08 Hostname Message`**
分隔符	指示单词是以空格还是制表符分隔。
报头中的主机名位置	指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。
主机名 (Hostname)	根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下： <181>Oct 10 15:14:08 Hostname Message 分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。 **主机名**将自动显示为 Hostname。 如果未正确显示主机名，请检查您已在**分隔符**和**报头中的主机名位置**字段中输入的数据。

消息正文的系统日志模板部分和说明

下表介绍可在自定义系统日志消息模板中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 29: 自定义模板的正则表达式，第 106 页。

表 *28:* 系统日志模板

部件	字段	说明
	名称 (Name)	用于识别此模板的用途的唯一名称。
映射操作	新映射	描述与此模板配合用于添加新用户的映射类型的正则表达式。例如，在此字段中输入“on from”可指示已登录到 F5 VPN 的新用户。
	已删除的映射	描述与此模板配合用于删除用户的映射类型的正则表达式。例如，在此字段中输入“disconnect”可指示应为 ASA VPN 删除的用户。

部件	字段	说明
用户数据	IP 地址	指示要捕获的 IP 地址的正则表达式。 例如，对于 Bluecat 消息，要捕获此 IP 地址范围内的用户的身份，请输入： (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]
	用户名	指示要捕获的用户名格式的正则表达式。
	域	指示要捕获的域的正则表达式。
	MAC 地址	指示要捕获的 MAC 地址格式的正则表达式。

正则表达式示例

要解析消息，请使用正则表达式。此部分提供正则表达式示例，以便解析 IP 地址、用户名和添加映射消息。

例如，使用正则表达式解析以下消息：

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

正则表达式按下表中进行定义。

表 *29:* 自定义模板的正则表达式

部件	正则表达式
IP 地址	Address <([^\s]+)>|address ([^\s]+)
用户名	User <([^\s]+)>| Username = ([^\s]+)
添加映射消息	(%ASA-4-722051|%ASA-6-713228)

使用系统日志预定义消息模板

系统日志消息具有包含报头和消息正文的标准结构。

本节介绍了Cisco ISE 提供的预定义模板，包括根据消息源支持的报头以及受支持正文结构的内容详细信息。

此外，您可以使用系统中未预定义的源的自定义正文内容来创建自己的模板。本节还介绍了自定义模板的受支持结构。解析消息时，除系统中预定义的报头以外，您还可以配置要使用的单个自定义报头，并且可为消息正文配置多个自定义模板。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 103 页。有关自定义正文的详细信息，请参阅自定义系统日志消息正文，第 102 页。

注释 大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。

消息报头

有两种可由解析器识别的报头类型：适用于所有消息类型（新增和删除）和适用于所有客户端机器。这些报头如下：

- <171>Host message
- <171>Oct 10 15:14:08 Host message

收到后，系统将解析报头以获取主机名，它可以是 IP 地址、主机名或完整 FQDN。

此外，还可以自定义报头。要自定义报头，请参阅自定义系统日志报头，第 103 页。

系统日志 ASA VPN 预定义模板

ASA VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

正文消息	解析示例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 注释 从此消息类型解析的 IP 地址是私有 IP 地址，如消息中所示。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 注释 从此消息类型解析的 IP 地址是 IPv4 地址。

删除映射正文消息

解析器支持的 ASA VPN 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[UserA,10.1.1.1]

正文消息
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason

正文消息
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

系统日志 Bluecat 预定义模板

支持的系统日志消息格式和 Bluecoat 类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

Bluecat 系统日志的新映射支持的消息如本部分所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

正文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

删除映射消息

Bluecat 没有已知的删除映射消息。

系统日志 F5 VPN 预定义模板

F5 VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 F5 VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=UserA,ip=172.16.0.12]

正文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security [nnnnn]：[UserA @ vendor-abcr] User UserA login on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz \

删除映射消息

目前没有支持的 F5 VPN 删除消息。

系统日志 Infoblox 预定义模板

Infoblox 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

正文消息
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

删除映射消息

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

- 如果包含 MAC 地址：

  [00:0c:29:a2:18:34,10.0.10.100]

- 如果不包含 MAC 地址：

  [10.0.10.100]

正文消息
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

系统日志 Linux DHCPd3 预定义模板

Linux DHCPd3 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射消息

如下表所述，解析器可识别不同的 Linux DHCPd3 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

删除映射正文消息

解析器支持的 Linux DHCPd3 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[00:0c:29:a2:18:34 ,10.0.10.100]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

系统日志 MS DHCP 预定义模板

MS DHCP 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板， 第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 MS DHCP 正文消息，如下表所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,,0x4D53465420352E30,MSFT,5.0

删除映射正文消息

解析器解析的 MS DHCP 支持的删除映射消息如此部分所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

系统日志 SafeConnect NAC 预定义模板

SafeConnect NAC 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板， 第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 SafeConnect NAC 正文消息，如下表所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

正文消息
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

删除映射消息

目前没有 Safe Connect 支持的删除消息。

系统日志 Aerohive 预定义模板

Aerohive 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Aerohive 正文消息。

从正文解析的详细信息包括用户名和 IP 地址。用于解析的正则表达式如以下示例所示：

- 新映射—`auth\:`
- IP—`ip ([A-F0-9a-f:.]+)`
- 用户名—`UserA ([a-zA-Z0-9\_]+)`

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,10.5.50.52]

正文消息
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

删除映射消息

系统当前不支持从 Aerohive 删除映射消息。

系统日志 Blue Coat 预定义模板 - 主代理、代理 SG、Squid Web 代理

系统支持 Blue Coat 的以下消息类型：

- BlueCoat 主代理
- BlueCoat 代理 SG
- BlueCoat Squid Web 代理

支持的系统日志消息格式和 Bluecoat 消息类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 Blue Coat 正文消息，如下表所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,192.168.10.24]

正文消息（此示例摘自 **BlueCoat** 代理 **SG** 消息）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

下表介绍了每个客户端用于新映射消息的不同正则表达式结构。

客户端	正则表达式
BlueCoat 主代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\s** 用户名 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat 代理 SG	新映射 **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\s[a-zA-Z0-9_]+\s-** 用户名 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web 代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\sTCP** 用户名 **\s([a-zA-Z0-9\._]+)\s\-\/**

删除映射消息

Blue Coat 客户端支持删除映射消息，但当前没有提供相关示例。

下表介绍了每个客户端用于删除映射消息的不同的已知正则表达式结构示例。

客户端	正则表达式
BlueCoat 主代理	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat 代理 SG	当前无可用示例。
BlueCoat Squid Web 代理	**(TCP_MISS|TCP_NC_MISS){1}**

系统日志 ISE 和 ACS 预定义模板

侦听 ISE 或 ACS 客户端时，解析器将接收以下消息类型：

- 通过身份验证 - 当用户经 ISE 或 ACS 进行身份验证后，通过身份验证消息将发出以通知身份验证已成功，并包含用户详细信息。系统将解析此消息，并保存此消息中的用户详细信息和会话 ID。
- 记帐启动和记帐更新消息（新映射）- 从 ISE 或 ACS 接收的记帐启动或记帐更新消息将进行解析，并包含在通过身份验证消息中保存的用户详细信息和会话 ID，然后映射用户。
- 记帐停止（删除映射）- 从 ISE 或 ACS 接收后，用户应设将从系统中删除。

ISE 和 ACS 支持的系统日志消息格式与类型如下所述。

通过身份验证消息

通过身份验证类型支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 解析示例

  仅解析用户名和会话 ID。

  [UserA,5]

记帐启动/更新（新映射）消息

新映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

删除映射消息

删除映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

系统日志 Lucent QIP 预定义模板

Lucent QIP 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 106 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Lucent QIP 正文消息。

这些消息的正则表达式结构如下：

DHCP_GrantLease|:DHCP_RenewLease

收到正文消息后，如下解析正文以获取用户详细信息：

[00:0C:29:91:2E:5D,10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

删除映射正文消息

这些消息的正则表达式结构如下所示：

删除租约:|DHCP 自动释放:

收到正文消息后，如下解析正文以获取用户详细信息：

[10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

过滤被动身份服务

您可以根据用户名称或 IP 地址过滤某些用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。实时会话显示映射过滤器未过滤掉的被动身份服务组件。您可以按照需要添加很多过滤器。“OR”逻辑运算符适用于过滤器之间。如果在单个过滤器中同时指定两个字段，则在这两个字段之间使用“AND”逻辑运算符。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**映射过滤器 (Mapping Filters)**。

步骤 2 选择 **提供程序 (Providers)** > **映射过滤器 (Mapping Filters)**。

步骤 3 点击 **Add**，输入您想要过滤的用户的用户名和 Ip 地址，然后点击**提交 (Submit)**。

步骤 4 要查看当前已记录到监控会话目录中未过滤用户，请选择 **操作 (Operations)** > **RADIUS 实时日志 (RADIUS Livelog)**。

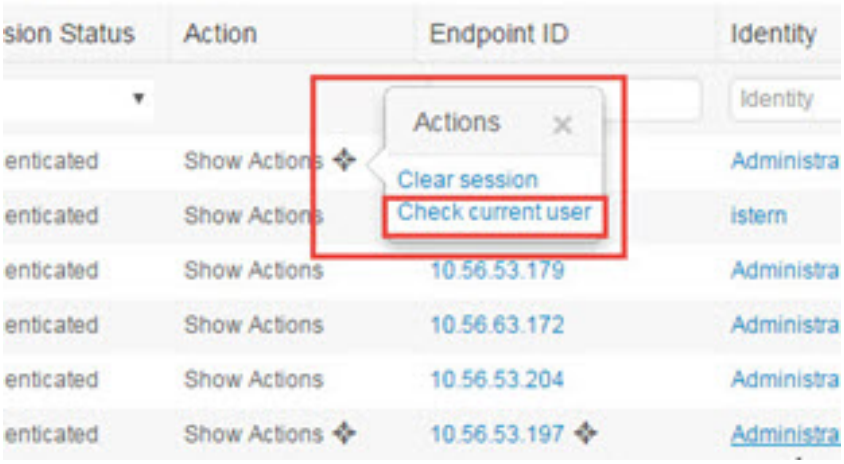
终端探测器

除可以配置的自定义提供程序以外，当激活 被动身份服务 时会在 ISE 中启用终端探测器，并且始终在后台运行。终端探测器会定期检查每个特定用户是否仍已登录到系统。

注释 为了确保终端在后台运行，必须首先配置初始 Active Directory 加入点，并确保选择**存储凭证 (Store Credentials)**。有关配置终端探测器的详细信息，请参阅使用终端探测器，第 118 页。

要手动检查终端状态，请转至**实时会话 (Live Sessions)**，从**操作 (Actions)** 列点击**显示操作 (Show Actions)**，然后选择**检查当前用户 (Check current user)**，如下图所示。

图 *14:* 检查当前用户



有关终端用户状态和手动执行检查的详细信息，请参阅RADIUS实时会话 (Live Sessions)。

当终端探测器识别用户已连接时，如果自上次为特定终端更新会话已经过 4 小时，则它将检查该用户是否仍已登录并收集以下数据：

- MAC 地址
- 操作系统版本

根据此检查，探测器将执行以下操作：

- 当用户仍处于登录状态时，探测器将使用“活动用户”(Active User) 状态更新Cisco ISE。
- 当用户已注销时，会话状态更新为“已终止”，15 分钟后，将从会话目录中删除用户。
- 当无法联系用户时（例如，当防火墙阻止联系或者终端已关闭时），状态更新为“无法访问”，并且用户策略将确定如何处理用户会话。终端将保持处于会话目录中。

使用终端探测器

开始之前

根据子网范围创建并启用终端探测器。每个 PSN 可以创建一个终端探测器。要使用终端探测器，请首先确保您已配置下列各项：

- 终端必须具有与端口 445 的网络连接。
- 从 ISE 配置初始 Active Directory 加入点，并确保在出现提示时选择**选择凭证**。有关加入点的详细信息，请参阅 Active Directory 作为探测器和提供程序，第 78 页。

注释 为了确保终端在后台运行，必须首先配置初始 Active Directory 加入点，通过它可使终端探测器即便在 Active Directory 未完全配置时也能够运行。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后选择**终端探测 (Endpoint Probes)**。

步骤 2 点击**添加 (Add)**以创建新终端探测器。

步骤 3 填写必填字段，从而确保您从**状态**字段中选择**启用**，然后点击**提交 (Submit)**。有关详细信息，请参阅终端探测器设置，第 119 页。

终端探测器设置

根据子网范围，为每个 PSN 创建单个终端探测器。如果部署中有多个 PSN，则可以为一组单独的子网分配每个 PSN。

表 *30:* 终端探测器设置

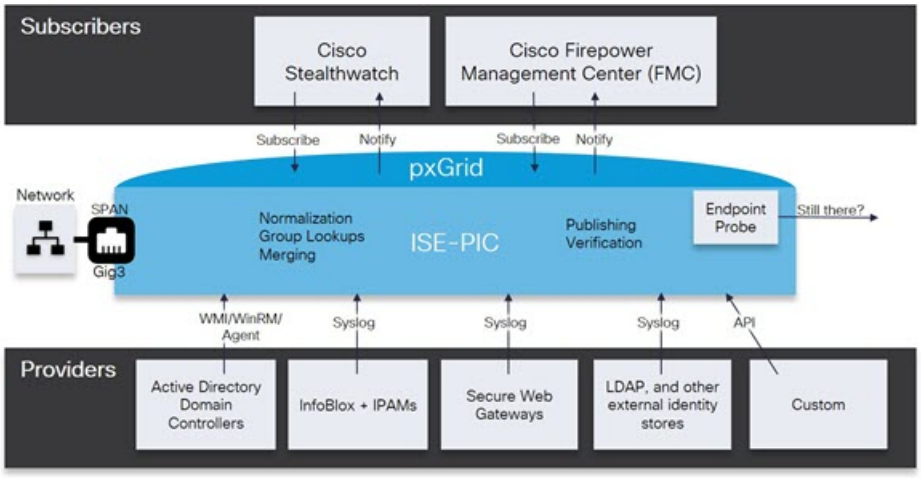
字段名称	说明
名称	输入用于识别此探测器的使用的唯一名称。
说明	输入用于介绍此探测器的使用的唯一说明。
状态	选择**启用 (Enable)** 以激活此探测器。
主机名	从部署中的可用 PSN 的列表中选择此探测器的 PSN。
子网	输入此探测器应检查的终端组的子网范围。使用标准子网掩码范围并以逗号分隔子网地址。 例如：10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 每个范围必须唯一并与所有其他范围分隔开来。例如，不能为同一探测器输入以下范围，因为它们相互重叠：2.2.2.0/16,2.2.3.0/16

用户

被动身份服务 使用Cisco pxGrid 服务，以便将从各种提供程序收集并由Cisco ISE 会话目录存储的经过身份验证的用户身份传送到其他网络系统，例如Cisco Stealthwatch 或Cisco Firepower 管理中心 (FMC)。

在下图中，pxGrid 节点从外部提供程序收集用户身份。这些身份经过解析、映射和设置格式。pxGrid 获取这些设置格式的用户身份，并将其发送到 被动身份服务 用户。

图 *15*: 被动身份服务 流



连接到Cisco ISE 的用户必须注册才能使用 pxGrid 服务。用户应通过 pxGrid SDK 采用思科提供的 pxGrid 客户端库以成为客户端。用户可以使用唯一名称和基于证书的相互身份验证登录 pxGrid。一旦他们发送了有效证书，ISE 便会自动批准Cisco pxGrid 用户。

用户可连接到已配置的 pxGrid 服务器主机名或 IP 地址。我们建议您使用主机名，以避免出现不必要的错误，尤其是为了确保 DNS 查询正常工作。功能是指在 pxGrid 上创建的供用户发布和订用的信息主题或通道。在Cisco ISE 中，仅支持 SessionDirectory 和 IdentityGroup。功能信息可通过发布、定向查询或批量下载查询从发布者获取，并可导航至**功能 (Capabilities)** 选项卡中的**用户 (Subscribers)** 进行查看。

要使用户能够从 ISE 接收信息，必须执行以下操作：

1. 或者，从用户端生成证书。
2. 从 PassiveID 工作中心生成用户的 pxGrid 证书，第 121 页。
3. 启用用户，第 122 页。执行此步骤，或者自动启用批准，以便允许订户从ISE接收用户身份。请参阅 配置用户设置，第 122 页。

生成用户的 pxGrid 证书

开始之前

您可以生成 pxGrid 用户的证书，以便保证 pxGrid 和用户之间的相互信任，从而使用户身份能够从 ISE 传递到用户。要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择**工作中心 (Work Centers)** > **PassiveID** > **订户 (Subscribers)**，然后转至**证书 (Certificates)** 选项卡。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **“生成无证书签名请求的单个证书”(Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。在“通用名称”字段中，输入包含 pxGrid 作为前缀的 pxGrid FQDN。例如，www.pxgrid-ise.ise.net。或者，使用通配符。例如，*.ise.net
- **“生成有证书签名请求的单个证书”(Generate a single certificate with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载 ISE 公共根证书，以便将其添加到 pxGrid 客户端的受信任证书存储区。ISE pxGrid 节点仅信任新签名的 pxGrid 客户端证书，反之亦然，从而无需外部证书颁发机构。

步骤 3 （可选）您可以输入此证书的说明。

步骤 4 查看或编辑此证书所基于的 pxGrid 证书模板。证书模板包含证书颁发机构 (CA) 基于该模板颁发的所有证书通用的属性。证书模板定义了主题、主题备选名称 (SAN)、密钥类型、密钥大小、必须使用的 SCEP RA 配置文件、证书的有效期以及扩展密钥用法 (EKU)（指定必须将证书用于客户端身份验证、服务器身份验证，还是用于两者）。内部Cisco ISE CA (ISE CA) 使用证书模板颁发基于该模板的证书。要编辑此模板，请选择 **管理 (Administration)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**。

步骤 5 指定使用者备选名称 (SAN)。可以添加多个 SAN。可提供以下选项：

- **FQDN**：输入 ISE 节点的完全限定域名。例如 www.isepic.ise.net。或者，使用通配符表示 FQDN。例如，*.ise.net

  可以为 FQDN 添加其中还可输入 pxGrid FQDN 的附加行。这应与您在“通用名称”(Common Name) 字段中使用的 FQDN 相同。

- **“IP 地址”(IP address)**：输入将与证书关联的 ISE 节点的 IP 地址。如果用户使用 IP 地址而不是 FQDN，则必须输入此信息。

  注释 如果选定“生成批量证书”(Generate Bulk Certificate) 选项，则不会显示此字段。

步骤 6 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE)

----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。

- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format [including certificate chain; one file for both the certificate chain and key])**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 7 输入证书密码。

步骤 8 点击**创建**。

启用用户

必须执行此任务，或者自动启用审批，才能允许用户从Cisco ISE 接收用户身份。请参阅配置用户设置，第 122 页。

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看Cisco pxGrid 客户端发送的请求。
- 启用被动身份服务。有关详细信息，请参阅Easy Connect，第 72 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **订户 (Subscribers)** 并确保查看的是**客户端 (Clients)** 选项卡。

步骤 2 选中用户旁边的复选框，然后点击**审批**。

步骤 3 点击**刷新 (Refresh)** 查看最新的状态。

从实时日志查看用户事件

“实时日志”(Live Logs) 页面显示所有用户事件。事件信息包括用户和功能名称，以及事件类型和时间戳。

导航至 **用户** 并选择**实时日志 (Live Log)** 选项卡以查看事件列表。您还可以清除日志并重新同步或刷新列表。

配置用户设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **pxGrid服务 (pxGrid Services)** > **设置 (Settings)**。

步骤 2 根据您的需求选择以下选项：

- 自动审批新账户 - 选中此复选框可自动审批来自新 pxGrid 客户端的连接请求。
- 允许基于密码的账户创建 - 选中此复选框可为 pxGrid 客户端启用基于用户名/密码的身份验证。如果启用此选项，系统无法自动审批 pxGrid 客户端。

  pxGrid 客户端可以通过使用 REST API 发送用户名向 pxGrid 控制器注册。在客户端注册时，pxGrid 控制器为 pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。

步骤 3 点击**保存 (Save)**。

中的监控和故障排除服务被动 ID 工作中心

详细了解如何使用监控、故障排除和报告工具来管理 被动 ID 工作中心。

- RADIUS实时会话 (Live Sessions)
- 请参阅 中的“报告”部分 思科 ISE 报告
- 用于验证传入流量的 TCP Dump 实用工具

LDAP

轻型目录访问协议 (LDAP) 是 RFC 2251 定义用于查询和修改在 TCP/IP 上运行的目录服务的网络协议。LDAP 是用于访问基于 X.500 的目录服务器的轻型机制。

Cisco ISE 使用 LDAP 协议集成 LDAP 外部数据库，此外部数据库也称为身份源。

LDAP 目录服务

LDAP 目录服务以客户端-服务器模式为基础。客户端通过连接至 LDAP 服务器并向服务器发送运行请求，启动 LDAP 会话。然后服务器发送其响应。一个或多个 LDAP 服务器包含来自 LDAP 目录树或 LDAP 后端数据库的数据。

目录服务管理一个目录，此目录是存储信息的一个数据库。目录服务使用分布式模式存储信息，而且通常会在目录服务器之间复制这些信息。

LDAP 目录以简单树状层次结构排列，可以分布在多个服务器中。每台服务器都可包含整个目录的复制版本，系统会定期同步此复制版本。

树中的每个条目都包含一组属性，其中每个属性都有一个名称（属性类型或属性说明）以及一个或多个值。这些属性在架构中定义。

每个条目都有一个唯一标识符：其可分辨名称 (DN)。此名称包含相对可分辨名称 (RDN)，RDN 由条目中的属性，然后加上父条目的 DN 构成。您可以将 DN 视为完整文件名，将 RDN 视为文件夹的相对文件名。

多个 LDAP 实例

通过使用不同的 IP 地址或端口设置创建多个 LDAP 实例，可以将Cisco ISE 配置为使用不同的 LDAP 服务器或同一个 LDAP 服务器中的不同数据库进行身份验证。每个主要服务器 IP 地址和端口配置，以及辅助服务器 IP 地址和端口配置，组成对应于一个Cisco ISE LDAP 身份源实例的一个 LDAP 实例。

Cisco ISE 不要求每个 LDAP 实例都对应一个 LDAP 数据库。可以设置多个 LDAP 实例来访问同一个数据库。当 LDAP 数据库包含多个用户或组子树时，此方法非常有用。由于每个 LDAP 实例仅支持一个用户子树目录和一个组子树目录，因此，必须为每个用户目录和组目录子树组合配置单独的 LDAP 实例，Cisco ISE 为该组合提交身份验证请求。

LDAP 故障转移

Cisco ISE 支持在主要 LDAP 服务器和辅助 LDAP 服务器之间进行故障转移。当 LDAP 服务器宕机或因其他原因而无法访问，导致Cisco ISE 无法连接 LDAP 服务器，从而使得身份验证请求失败时，就会发生故障转移。

如果您建立故障转移设置并且Cisco ISE 尝试连接的第一个 LDAP 服务器无法访问，Cisco ISE 始终会尝试连接第二个 LDAP 服务器。如果您希望Cisco ISE 再次使用第一个 LDAP 服务器，您必须在 Failback Retry Delay 文本框中输入一个值。

注释 Cisco ISE 始终使用主要 LDAP 服务器从 Admin 门户获取用于授权策略的组和属性，因此当您配置这些项目时必须可以访问主要 LDAP 服务器。根据故障转移配置，Cisco ISE 仅将辅助 LDAP 服务器用于运行时的身份验证和授权。

LDAP 连接管理

Cisco ISE 支持多个并行 LDAP 连接。首次进行 LDAP 身份验证时，根据需要打开连接。为每个 LDAP 服务器配置最大连接数。事先打开连接可缩短身份验证时间。可以设置最大连接数以用于并发绑定连接。每台 LDAP 服务器（主要或辅助）的打开连接数量可以不同，此数量根据为每台服务器配置的最大管理连接数来确定。

Cisco ISE 会为Cisco ISE 中配置的每台 LDAP 服务器保留打开的 LDAP 连接列表（包括绑定信息）。在身份验证流程中，连接管理器会尝试从池中查找打开的连接。如果打开的连接不存在，系统会打开新的连接。

如果 LDAP 服务器关闭连接，则连接管理器会在对搜索目录的第一个调用过程中报告错误，并会尝试更新连接。身份验证流程完成之后，连接管理器会发布连接。

LDAP 用户身份验证

您可以将 LDAP 配置为外部身份存储库。Cisco ISE 使用明文密码身份验证。用户身份验证包括：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目。

- 使用 LDAP 服务器中查找到的用户密码检查用户密码。
- 检索用于策略的组成员信息。
- 检索指定属性的值以用于策略和授权配置文件。

若要验证用户，Cisco ISE 会向 LDAP 服务器发送绑定请求。绑定请求会包含明文显示的用户 DN 和密码。如果用户的 DN 和密码与 LDAP 目录中的用户名和密码匹配，则用户通过身份验证。

当 Active Directory 用作 LDAP 时，UPN 名称用于用户身份验证。当 Sun ONE Directory Server 用作 LDAP 时，SAM 名称用于用户身份验证

注释 Cisco ISE 会为每个用户身份验证发送两条 searchRequest 消息。这不会影响Cisco ISE 授权或网络性能。第二个 LDAP 请求用于确保Cisco ISE 与正确的身份通信。

注释 思科 ISE 作为 DNS 客户端，仅使用 DNS 响应中返回的第一个 IP 来执行 LDAP 绑定。

我们建议您使用安全套接字层 (SSL) 保护与 LDAP 服务器的连接。

注释 仅当密码到期后，帐户仍有剩余宽限登录次数时，LDAP才支持密码更改。如果密码更改成功，LDAP 服务器的 bindResponse 应为 LDAP_SUCCESS，且 bindResponse 消息中应包含剩余宽限期登录控制字段。如果 bindResponse 消息包含任何额外的控制字段（除剩余宽限登录外），Cisco ISE 可能无法对消息进行解码。

在授权策略中使用的 LDAP 组和属性检索

Cisco ISE 可以依据 LDAP 身份源验证主题（用户或主机），具体方法是在目录服务器上执行绑定操作，查找和验证主题。成功进行身份验证后，Cisco ISE 可以在必要时检索属于主题的组和属性。可以配置属性以在Cisco ISE 管理员门户中进行检索，方法是选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。Cisco ISE 可以使用这些组和属性授权主题。

要验证用户或查询 LDAP 身份源，Cisco ISE 连接到 LDAP 服务器并维护连接池。

当 Active Directory 配置为 LDAP 存储时，应当注意下列关于组成员身份的限制：

- 用户或计算机必须是策略条件中定义的组的直接成员，才符合策略规则。
- 定义的组可能不是用户或计算机的主组。此限制仅在 Active Directory 配置为 LDAP 存储时适用。

LDAP 组成员身份信息检索

对于用户身份验证、用户查找和 MAC 地址查找，Cisco ISE 必须从 LDAP 数据库检索组成员身份信息。LDAP 服务器通过以下其中一种方式表示使用者（用户或主机）与组之间的关联：

- 组引用使用者 - 组对象包含用于指定使用者的属性。使用者的标识符可以作为以下内容在组中寻源：
  - 可分辨名称
  - 明文用户名
- 使用者引用组 - 使用者对象包含用于指定其所属的组的属性。

LDAP 身份源包含以下用于组成员身份信息检索的参数：

- 引用方向 - 此参数指定在确定组成员身份时要使用的方法（组引用使用者或使用者引用组）。
- 组映射属性 - 此参数指示包含组成员身份信息的属性。
- 组对象类 - 此参数确定特定对象可识别为组。
- 组搜索子树 - 此参数指示用于组搜索的搜索库。
- 成员类型选项 - 此参数指定成员在组成员属性中的存储方式（作为 DN 或明文用户名）。

LDAP 属性检索

针对用户身份验证、用户查找和 MAC 地址查找，Cisco ISE 必须从 LDAP 数据库检索主题属性。对于 LDAP 身份源的每个实例，将创建身份源字典。这些字典支持以下数据类型的属性：

- 字符串
- 无符号整数 32
- IPv4 地址

对于无符号整数和IPv4属性，Cisco ISE会对已检索的相应数据类型的字符串进行转换。如果转换失败或未检索到属性的值，则Cisco ISE 将记录调试消息，但身份验证或查找进程不会失败。

您同样可以配置属性的默认值，当转换失败或Cisco ISE未检索到任何属值时，Cisco ISE即可使用该默认值。

LDAP 证书检索

如果您已将证书检索配置为用户查找的一部分，那么Cisco ISE 必须从 LDAP 检索证书属性值。要从LDAP检索证书属性值，在配置LDAP身份源时，先前必须将属性列表中的证书属性配置为可访问。

LDAP 服务器返回的错误

在身份验证过程中可能会出现以下错误：

- 身份验证错误 - Cisco ISE 会在Cisco ISE 日志文件中记录身份验证错误。

LDAP 服务器返回绑定（身份验证）错误的可能原因如下：

- 参数错误 - 输入了无效的参数
- 用户帐户受限制（已禁用、已锁定、已到期、密码已到期等）
- 初始化错误 - 使用 LDAP 服务器超时设置配置Cisco ISE 在确定该服务器上的连接或身份验证是否已失败之前，应该等待从 LDAP 服务器接收响应的秒数。

  LDAP 服务器返回初始化错误的可能原因如下：

  - 不支持 LDAP。
  - 服务器宕机。
  - 服务器内存不足。
  - 用户无权限。
  - 管理员凭证配置不正确。

以下错误记录为外部资源错误，指示 LDAP 服务器可能有问题：

- 发生连接错误
- 超时到期
- 服务器宕机
- 服务器内存不足

以下错误记录为 Unknown User 错误：

- 用户在数据库中不存在

以下错误记录为 Invalid Password 错误，虽然用户存在，但是发送的密码无效：

- 输入了无效密码

LDAP 用户查找

Cisco ISE 支持 LDAP 服务器的用户查找功能。通过此功能，可以在未经身份验证的情况下在 LDAP 数据库中搜索用户和检索信息。用户查找流程包括以下操作：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目
- 检索要用于策略的用户组成员身份信息
- 检索指定属性的值以用于策略和授权配置文件

LDAP MAC 地址查找

Cisco ISE 支持 MAC 地址查找功能。您可以通过此功能在 LDAP 数据库中搜索 MAC 地址以及在未经身份验证的情况下检索信息。MAC 地址查找过程包括以下操作：

- 在 LDAP 服务器中搜索与设备 MAC 地址匹配的条目
- 为策略中使用的设备检索 MAC 地址组信息
- 为策略中使用的指定属性检索值

添加 LDAP 身份源

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- Cisco ISE 始终使用主要 LDAP 服务器获取用于授权策略的组和属性。因此，当您配置这些项目时，必须可访问您的主要 LDAP 服务器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP** > **添加 (Add)**。

步骤 2 输入相应值。

步骤 3 点击**提交 (Submit)** 以创建 LDAP 实例。

LDAP 身份源设置

下表介绍“LDAP 身份源”(LDAP Identity Sources) 窗口上的字段，您可以使用此窗口创建 LDAP 实例并连接该实例。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 31: LDAP 常规设置

字段名称	使用指南
名称 (Name)	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
说明	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。

字段名称	使用指南
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。
注释　仅当选择自定义架构时，才可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
组名称属性 (Group Name Attribute)	• CN：根据通用名称检索 LDAP 身份存储区组。 • DN：根据可分辨名称检索 LDAP 身份存储区组。
证书属性 (Certificate Attribute)	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
组映射属性 (Group Map Attribute)	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。

字段名称	使用指南
用户信息属性	默认情况下，预定义属性用于收集以下内置架构类型的用户信息（例如，名字、姓氏、电子邮件、电话，位置等）： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。 您还可以选择架构 (Schema) 下拉菜单中的定制 (Custom) 选项，根据要求编辑用户信息属性。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 *32: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器 **(Enable Secondary Server)**	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器 **(Primary and Secondary Servers)**	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
为每个 **ISE** 节点指定服务器	选中此复选框可配置每个 PSN 的主辅 LDAP 服务器主机名/IP 及其端口。 启用此选项后，将显示一个表，列出部署中的所有节点。您需要选择节点并配置主要和辅助 LDAP 服务器主机名/IP 及所选节点的端口。

字段名称	使用指南
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对Cisco ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA”(LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入Cisco ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
每 **N** 秒强制重新连接	选中此复选框并在**秒 (Seconds)** 字段中输入所需的值可强制服务器按照指定的时间间隔续订LDAP 连接。有效范围为 1 至 60 分钟。

字段名称	使用指南
测试与服务器的绑定 **(Test Bind to Server)**	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望Cisco ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果Cisco ISE 尝试连接的主 LDAP 服务器无法访问，Cisco ISE 会尝试连接辅助 LDAP 服务器。如果您希望Cisco ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍目录组织 **(Directory Organization)** 选项卡上的字段。

表 ***33: LDAP*** 目录组织设置

字段名称	使用指南
主题搜索库 **(Subject Search Base)**	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 **(Group Search Base)**	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。

字段名称	使用指南
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个MAC地址格式供Cisco ISE用于在LDAP数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当Cisco ISE 收到主机查找请求时，Cisco ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果Cisco ISE在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，Cisco ISE会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则Cisco ISE 会向 LDAP 服务器提交 user1。 **注释** <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

字段名称	使用指南
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，Cisco ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则Cisco ISE 会向 LDAP 服务器提交 *user1*。 注释 <*end_string*> 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *34: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *35: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

LDAP 高级设置

下表介绍“高级设置”(Advanced Settings) 选项卡中的字段。

表 *36: LDAP* 高级设置

字段名称	使用指南
启用密码更改 (Enable Password Change)	在使用 PAP 协议进行设备管理和使用 RADIUS EAP-GTC 协议进行网络访问时，选中此复选框可让用户在密码到期或重置密码的情况下更改密码。对于不受支持的协议，用户身份验证会失败。此选项还可以让用户在下次登录时更改密码。

相关主题

LDAP 目录服务，第 123 页
LDAP 用户身份验证，第 124 页
LDAP 用户查找，第 127 页
添加 LDAP 身份源，第 128 页

配置 LDAP 方案

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选择 LDAP 实例。

步骤 3 点击**常规**选项卡。

步骤 4 点击**方案 (Schema)** 选项旁的下拉箭头。

步骤 5 从**方案 (Schema)** 下拉列表中选择所需方案。可以根据需要选择**自定义 (Custom)** 选项。

预定义属性用于内置方案，例如 Active Directory、Sun directory Server、Novell eDirectory。如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。

配置主要和辅助 LDAP 服务器

在创建 LDAP 实例之后，您必须为主要 LDAP 服务器配置连接设置。配置辅助 LDAP 服务器为可选操作。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Connection** 选项卡以配置主要和辅助服务器。

步骤 4 输入作为 LDAP 身份源设置中描述的值。

步骤 5 点击**提交 (Submit)** 保存连接参数。

允许思科 ISE 从 LDAP 服务器获取属性

为了让Cisco ISE 从 LDAP 服务器获取用户和组数据，您必须在Cisco ISE 中配置 LDAP 目录详细信息。对于 LDAP 身份源，适用以下三种搜索：

- 搜索组子树中的所有组用于管理
- 搜索主题子树中的用户以定位用户
- 搜索用户在其中为成员的组

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Directory Organization** 选项卡。

步骤 4 输入作为 LDAP 身份源设置中描述的值。

步骤 5 点击**提交 (Submit)** 保存配置。

从 LDAP 服务器检索组成员身份详细信息

您可以添加新组或从 LDAP 目录选择组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击**组 (Groups)** 选项卡。

步骤 4 选择 **添加 (Add)** > **添加组 (Add Group)** 添加新组或选择 **添加 (Add)** > **从目录中选择组 (Select Groups From Directory)** 从 LDAP 目录中选择组。

a) 如果您选择添加组，请输入新组的名称。
b) 如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。搜索条件可以包含星号 (*) 通配符。

步骤 5 点击要选择的组旁边的复选框，然后点击**确定 (OK)**。

选择的组将显示在“组”(Groups) 页面。

步骤 6 点击**提交 (Submit)** 保存组选择。

注释 当 Active Directory 配置为思科 ISE 中的 LDAP 身份存储时，不支持 Active Directory 内置组。

从 LDAP 服务器检索用户属性

可以从 LDAP 服务器获取用户属性，以便在授权策略中使用。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Attributes** 选项卡。

步骤 4 选择 **添加 (Add)** > **添加属性 (Add Attribute)** 添加新属性或选择 **添加 (Add)** > **从目录中选择属性 (Select Attributes From Directory)** 从 LDAP 服务器选择属性。

a) 如果选择添加属性，则为新属性输入名称。

b) 如果从目录选择，则输入示例用户，点击**检索属性 (Retrieve Attributes)**，检索用户的属性。可以使用星号 (*) 通配符。

Cisco ISE 允许您在手动添加属性类型 IP 时使用 IPv4 或 IPv6 地址配置 LADP 服务器以进行用户身份验证。

步骤 5 选中想要选择的属性旁边的复选框，然后点击**确定 (OK)**。

步骤 6 点击**提交 (Submit)**，保存属性选择。

使用 LDAP 身份源进行安全身份验证

在“LDAP 配置”(LDAP configuration) 页面上选择“安全身份验证”(Secure Authentication) 选项时，Cisco ISE 使用 SSL 保护与 LDAP 身份源的通信。通过以下方式建立到 LDAP 身份源的安全连接：

- SSL 隧道 - 使用 SSL v3 或 TLS v1（LDAP 服务器支持的最强大的版本）
- 服务器身份验证（LDAP 服务器身份验证）- 基于证书
- 客户端身份验证（Cisco ISE 身份验证）- 无（在 SSL 隧道中使用管理员绑定）
- 密码套件 - Cisco ISE 支持的所有密码套件

我们建议您使用带有Cisco ISE 支持的最强加密和密码的 TLS v1。

要使Cisco ISE 与 LDAP 身份源安全通信，请执行以下操作：

开始之前

- Cisco ISE 必须连接到 LDAP 服务器
- TCP 端口 636 应当开放

步骤 1 将向 LDAP 服务器颁发服务器证书的 CA 的完整证书颁发机构 (CA) 链导入Cisco ISE （**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）。

完整 CA 链指的是根 CA 和中级 CA 证书；不是 LDAP 服务器证书。

步骤 2 将Cisco ISE 配置为在与 LDAP 身份源通信时使用安全身份验证（**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**；务必选中“连接设置”(Connection Settings) 选项卡中的“安全身份验证”(Secure Authentication) 复选框）。

步骤 3 在 LDAP 身份存储区中选择根 CA 证书。

ODBC 身份源

您可以使用符合开放式数据库连接 (ODBC) 的数据库作为外部身份源，以便对用户和终端进行身份验证。ODBC 身份源可在身份存储区序列中使用，用于访客和发起人身份验证。它可以用于 BYOD 流。

支持以下数据库引擎：

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

配置Cisco ISE 对 ODBC 兼容数据库进行身份验证不会影响该数据库的配置。要管理您的数据库，请参阅您的数据库文档。

ODBC 数据库凭证检查

对于 ODBC 数据库，Cisco ISE 支持三种类型的凭证检查。您必须为每种凭证检查类型配置适当的 SQL 已存储程序。Cisco ISE 使用已存储程序在 ODBC 数据库中查询相应的表并接收 ODBC 数据库的输出参数或记录集。在响应 ODBC 查询时，该数据库会返回记录集或一组命名参数。

密码可以明文或加密格式存储在ODBC数据库中。当Cisco ISE 调用密码时，存储程序可以将密码解密为明文。

凭证检查类型	ODBC 输入参数	ODBC 输出参数	凭证检查	身份验证协议
ODBC 数据库中明文密码身份验证	用户名 密码	结果 Group 帐户信息 错误字符串	如果用户名和密码匹配，会返回相关用户信息。	PAP EAP-GTC（作为 PEAP或 EAP-FAST 的内部方法） TACACS

凭证检查类型	ODBC 输入参数	ODBC 输出参数	凭证检查	身份验证协议
从 ODBC 数据库获取明文密码	用户名	结果 Group 帐户信息 错误字符串 Password	如果找到用户名，存储程序会返回其密码和相关用户信息。Cisco ISE 基于身份验证方式计算密码散列值并将其与从客户端收到的值进行比较。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2（作为 PEAP 或 EAP-FAST 的内部方法） TACACS
查询	用户名	结果 Group 帐户信息 错误字符串	如果找到用户名，则会返回相关用户信息。	MAB PEAP、EAP-FAST 和 EAP-TTLS 快速重连

注释 在Cisco ISE 中没有使用输出参数返回的组。在Cisco ISE 中只使用获取组 (Fetch Groups) 存储程序检索的组。该帐户信息仅包含在身份验证审核日志中。

下表列出了 ODBC 数据库存储过程返回的结果代码和Cisco ISE 身份验证结果代码之间的映射：

结果代码（由存储过程返回）	说明	Cisco ISE 身份验证结果代码
0	CODE_SUCCESS	NA（身份验证已通过）
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	失败
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

注释 思科 ISE 根据此映射的身份验证结果代码执行实际身份验证或查找操作。

您可以使用该存储程序从 ODBC 数据库中获取组和属性。

返回用于明文密码身份验证的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset] @username varchar(64), @password
 varchar(255) AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username
 AND password = @password ) SELECT 0,11,'give full access','No Error' FROM NetworkUsers
WHERE username = @username ELSE SELECT 3,0,'odbc','ODBC Authen Error' END
```

返回用于获取明文密码的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset] @username varchar(64) AS BEGIN
IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username) SELECT 0,11,'give
 full access','No Error',password FROM NetworkUsers WHERE username = @username ELSE SELECT
 3,0,'odbc','ODBC Authen Error' END
```

返回用于查找的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset] @username varchar(64) AS BEGIN IF
EXISTS( SELECT username FROM NetworkUsers WHERE username = @username) SELECT 0,11,'give
full access','No Error' FROM NetworkUsers WHERE username = @username ELSE SELECT
3,0,'odbc','ODBC Authen Error' END
```

返回用于明文密码身份验证的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters] @username varchar(64), @password
 varchar(255), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT,
 @errorString varchar(255) OUTPUT AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers
WHERE username = @username AND password = @password ) SELECT @result=0, @group=11,
@acctInfo='give full access', @errorString='No Error' FROM NetworkUsers WHERE username =
@username ELSE SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen
Error' END
```

返回用于获取明文密码的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters] @username varchar(64), @result
INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString
varchar(255) OUTPUT, @password varchar(255) OUTPUT AS BEGIN IF EXISTS( SELECT username FROM
 NetworkUsers WHERE username = @username) SELECT @result=0, @group=11, @acctInfo='give full
 access', @errorString='No Error', @password=password FROM NetworkUsers WHERE username =
@username ELSE SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen
Error' END
```

返回用于查找的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters] @username varchar(64), @result INT
 OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255)
 OUTPUT AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username)
SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error' FROM
NetworkUsers WHERE username = @username ELSE SELECT @result=3, @group=0, @acctInfo='odbc',
 @errorString='ODBC Authen Error' END
```

从 Microsoft SQL Server 获取组的示例程序

```
CREATE PROCEDURE [dbo].[ISEGroupsH] @username varchar(64), @result int output AS BEGIN if
exists (select * from NetworkUsers where username = @username) begin set @result = 0 select
 'accountants', 'engineers', 'sales','test_group2' end else set @result = 1 END
```

当用户名为 "*" 时，获取所有用户的所有组的示例程序（适用于 Microsoft SQL Server）

```
ALTER PROCEDURE [dbo].[ISEGroupsH] @username varchar(64), @result int output AS BEGIN if
@username = '*' begin -- if username is equal to '*' then return all existing groups set
```

```
@result = 0 select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4' end else if exists (select
 * from NetworkUsers where username = @username) begin set @result = 0 select 'accountants'
 end else set @result = 1 END
```

从 Microsoft SQL Server 获取属性的示例程序

```
CREATE PROCEDURE [dbo].[ISEAttrsH] @username varchar(64), @result int output AS BEGIN if
exists (select * from NetworkUsers where username = @username) begin set @result = 0 select
 phone as phone, username as username, department as department, floor as floor, memberOf
as memberOf, isManager as isManager from NetworkUsers where username = @username end else
set @result = 1 END
```

ODBC 配置的其他示例

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

添加 ODBC 身份源

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 点击 **ODBC**。

步骤 3 点击**添加 (Add)**。

步骤 4 在**常规** (General) 选项卡，请输入 ODBC 身份源的名称和说明。

步骤 5 在**连接 (Connection)** 选项卡中，输入以下详细信息：

- ODBC 数据库的主机名或 IP 地址。如果对数据库使用非标准 TCP 端口，则可以使用以下格式指定端口号：主机名或 IP 地址端口:端口
- ODBC 数据库名称
- 管理员用户名和密码（Cisco ISE 使用这些凭证连接到数据库）
- 服务器超时（单位：秒；默认为 5 秒）
- 连接尝试（默认为 1）
- 数据库类型。选择以下其中一个选项：
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**

- **Microsoft SQL Server**
- **Sybase**

步骤 6 点击**测试连接 (Test Connection)** 以检查与 ODBC 数据库的连接，并且对于已配置的使用案例验证是否存在已存储程序。

步骤 7 在已存储程序 (**Stored Procedures**) 选项卡，输入以下详细信息：

- **已存储程序类型 (Stored Procedure Type)**：选择您数据库支持的输出类型。
  - **返回记录集 (Returns Recordset)**：数据库返回记录集以响应 ODBC 查询。
  - **返回参数 (Returns Parameters)**：数据库返回一组具名参数以响应 ODBC 查询。
- **明文密码身份验证 (Plain Text Password Authentication)**：输入在 ODBC 服务器上运行的已存储程序的名称，该已存储程序用于明文密码身份验证。用于 PAP、EAP-GTC 内部方法和 TACACS。
- **明文密码获取 (Plain Text Password Fetching)**：输入在 ODBC 服务器上运行的、用于获取明文密码的已存储程序的名称。用于 CHAP、MS CHAPv1/v2、LEAP、EAP-MD5、EAP-MSCHAPv2 内部方法和 TACACS。
- **检查存在用户名或机器 (Check Username or Machine Exists)**：输入在 ODBC 服务器上运行的、用于用户/MAC 地址查询的已存储程序的名称。用于 MAB 和 PEAP、EAP-FAST和EAP-TTLS 快速重连。
- **获取组 (Fetch Groups)**：输入从 ODBC 数据库中检索组的已存储程序的名称。
- **获取属性 (Fetch Attributes)**：输入从 ODBC 数据库中检索属性及其值的已存储程序的名称。
- **高级设置 (Advanced Settings)**：点击此选项可使用以下字词典下的属性作为**获取属性 (Fetch Attributes)** 已存储程序中的输入参数（除了用户名和密码）：
  - **RADIUS**
  - **设备**
  - **网络接入**

  注释 只能在**网络访问 (Network Access)** 字典中使用以下属性：**AuthenticationMethod**、**设备 IP 地址 (Device IP Address)**、**EapAuthentication**、**EapTunnel**、**ISE 主机名 (ISE Host Name)**、**协议 (Protocol)**、**用户名 (UserName)**、**VN** 和 **WasMachineAuthenticated**。

  在**已存储程序中的属性名称 (Attribute Name in Stored Procedure)** 字段中，指定已存储程序中使用的属性名称。

  您可以将已存储程序配置为从 ODBC 数据库检索以下输出参数：
  - ACL
  - 安全组
  - VLAN（名称或编号）
  - Web 重定向 ACL

- Web 重定向门户名称

您可以使用这些属性配置授权配置文件。这些属性列在**授权配置文件 (Authorization Profiles)** 窗口的**常见任务 (Common Tasks)** 部分中（在**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results)** 下）。以下是一些可以使用这些属性的用例场景：

- 根据指定的输入属性（MAC 地址、用户名、呼叫站 ID 或设备位置），配置授权配置文件以使用从 ODBC 数据库返回的 VLAN，而不是手动为每个授权配置文件指定 VLAN 。
- 配置授权配置文件，阻止在 ODBC 身份存储区中被阻止的呼叫站 ID 的访问。
- 配置授权配置文件，根据 MAC 地址、用户名、呼叫站 ID 或设备位置从 ODBC 数据库检索 Web 重定向 ACL 或 Web 重定向门户名称。

在配置授权策略时，可以在**策略集 (Policy Sets)** 窗口中选择从 ODBC 数据库检索的安全组。

注释 使用**高级设置 (Advanced Settings)** 选项时，会在 ODBC 数据库中创建名为 user_attributes_detail 的新表来存储其他详细信息。您必须将所有输出参数的数据类型设置为 VARCHAR2。否则，已存储程序可能会在合并和编译过程中失败。例如，如果将 SGTNAME 设置为 VARCHAR2 并将 VLANNUMBER 设置为 NUMBER，则编译以下已存储程序时可能会失败：

```
select ATTR_NAME, value from ATTRIBUTES where user_id=userid union select 'SGTNAME', SGTNAME
 from user_attributes_detail where USER_ID = userid and
user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE union select 'VLANNUMBER', VLANNUMBER
 from user_attributes_detail where USER_ID = userid and
user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- **搜索格式 MAC 地址 (Search for MAC Address in Format)**：根据所选的 MAC 格式对接收的 MAC 地址进行标准化处理。

步骤 8 在**属性 (Attributes)** 选项卡中，添加所需的属性。在添加属性时，您可以指定属性名称在授权策略规则中的显示方式。

您还可以从 ODBC 数据库获取属性。这些属性可在授权策略中使用。

步骤 9 在**组 (Groups)** 选项卡中，添加用户组。您可以通过指定用户名或 MAC 地址从 ODBC 数据库获取组。这些组可在授权策略中使用。

您可以对组和属性进行重命名。默认情况下，**ISE 中名称 (Name in ISE)** 字段中显示的名称与 ODBC 数据库中的名称相同，但是，您可以修改此名称。此名称在授权策略中使用。

步骤 10 点击**提交 (Submit)**。

有关如何配置 ODBC 身份源的详细信息，请参阅以下链接：

- 在采用 Oracle 数据库的思科 ISE 上配置 ODBC
- 使用 ODBC 配置采用 MS SQL 的思科 ISE
- 在采用 PostgreSQL 的思科 ISE 上配置 ODBC
- 配置思科 ISE 以与 MySQL 服务器集成

注释 如果已配置输入属性，则必须在复制 ODBC 身份存储区时执行以下操作。否则，输入参数可能会在复制的 ODBC 身份存储区中丢失。

1. 点击**高级设置 (Advance Settings)**。
2. 验证输入参数是否设置正确。
3. 点击**确定 (OK)** 以将这些输入参数保存在复制的 ODBC 身份存储区中。

RADIUS 令牌身份源

支持 RADIUS 协议并向用户和设备提供身份验证、授权和记账 (AAA) 服务的服务器称为 RADIUS 服务器。RADIUS 身份源只是一个外部身份源，包含一系列的主题及其凭证，使用 RADIUS 协议进行通信。例如，Safeword 令牌服务器是一个身份源，可以包含若干用户以及作为一次性密码的凭证，提供一个您可以使用 RADIUS 协议查询的界面。

Cisco ISE 支持任何符合 RADIUS RFC 2865 的服务器作为外部身份源。Cisco ISE 支持多个 RADIUS 令牌服务器身份，例如 RSA SecurityID 服务器和 SafeWord 服务器。RADIUS 身份源可以与任何用于验证用户的 RADIUS 令牌服务器配合使用。

注释 必须为 MAB 身份验证启用“处理主机查找”(Process Host Lookup) 选项。我们建议不要为 MAB 身份验证配置用作外部身份源的 RADIUS 令牌服务器，因为使用 MAB 身份验证的设备无法生成 OTP 或 RADIUS 令牌（这是 RADIUS 令牌服务器身份验证所需的）。因此，身份验证将失败。您可以使用外部 RADIUS 服务器选项来处理 MAB 请求。

支持 RADIUS 令牌服务器的身份验证协议

对于 RADIUS 身份源，Cisco ISE 支持以下身份验证协议：

- RADIUS PAP
- 使用内部可扩展身份验证协议 - 通用令牌卡 (EAP-GTC) 的受保护的可扩展身份验证协议 (PEAP)
- 使用内部 EAP-GTC 的 EAP-FAST

RADIUS 令牌服务器用于通信的端口

RADIUS 令牌服务器将 UDP 端口用于身份验证会话。此端口用于所有 RADIUS 通信。为了让Cisco ISE 将 RADIUS 一次性密码 (OTP) 消息发送到已启用 RADIUS 的令牌服务器，必须确保Cisco ISE 和已启用 RADIUS 的令牌服务器之间的网关设备能够通过 UDP 端口进行通信。您可以通过管理员门户配置 UDP 端口。

RADIUS 共享密钥

您在Cisco ISE 中配置 RADIUS 身份源时必须提供共享密钥。此共享密钥应与 RADIUS 令牌服务器上配置的共享密钥相同。

RADIUS 令牌服务器中的故障转移

Cisco ISE 允许您配置多个 RADIUS 身份源。每个 RADIUS 身份源可以使用 RADIUS 主服务器和辅助服务器。当Cisco ISE 无法连接到主服务器时，则会使用辅助服务器。

RADIUS 令牌服务器中的可配置密码提示

RADIUS 身份源允许您配置密码提示。您可以通过管理员门户配置密码提示。

RADIUS 令牌服务器用户身份验证

Cisco ISE 会获取用户凭证（用户名和密码）并将这些凭证发送到 RADIUS 令牌服务器。Cisco ISE 还会将 RADIUS 令牌服务器身份验证处理的结果中继到用户。

RADIUS 令牌服务器中的用户属性缓存

默认情况下，RADIUS 令牌服务器不支持用户查找。但是，用户查找功能对于以下Cisco ISE 功能非常重要。

- PEAP 会话恢复：此功能允许在建立 EAP 会话期间在身份验证成功之后恢复 PEAR 会话。
- EAP/FAST 快速重新连接：此功能允许在建立 EAP 会话期间在身份验证成功之后快速进行重新连接。
- TACACS+ 授权：在 TACACS+ 身份验证成功后发生。

Cisco ISE 缓存成功的身份验证的结果以为这些功能处理用户查找请求。对于每次成功的身份验证，系统会缓存经过身份验证的用户的名称和所检索的属性。失败的身份验证不写入缓存。

在运行时内存中可提供缓存，在分布式部署中不可在Cisco ISE 节点之间进行复制。您可以通过 Admin 门户为缓存配置有效时间 (TTL) 限制。从 ISE 2.6 开始，您可以选择启用身份缓存选项并以分钟为单位设置老化时间。该选项默认被禁用，启用之后，在指定的持续时间里，可在内存中使用缓存。

身份序列中的 RADIUS 身份源

您可以在身份源序列中添加身份验证序列的 RADIUS 身份源。但是，由于您无法查询不带身份验证的 RADIUS 身份源，因此无法添加属性检索序列的 RADIUS 身份源。Cisco ISE 在使用 RADIUS 服务器进行身份验证时无法区分不同的错误。RADIUS 服务器针对所有错误都返回 Access-Reject 消息。例如，当在 RADIUS 服务器中找不到用户时，RADIUS 服务器会返回 Access-Reject 消息，而不是返回 User Unknown 状态。

RADIUS 服务器为所有错误返回相同消息

当在 RADIUS 服务器中未找到某名用户时，RADIUS 服务器会返回一条访问 - 拒绝消息。Cisco ISE 提供一个选项可通过管理员门户配置此消息，显示为身份验证失败或未找到用户的消息。但是，对于用户未知和所有失败的情况，此选项均会返回一条未找到用户的消息。

下表列出 RADIUS 身份服务器可能出现的各种失败情况。

表 *37*: 错误处理

失败情况	失败的原因
身份验证失败	• 用户未知。 • 用户尝试使用错误的验证码登录。 • 用户登录时长过期。
处理失败	• RADIUS 服务器在Cisco ISE 中配置错误。 • RADIUS 服务器不可用。 • 检测到 RADIUS 包错误。 • 发送或接收 RADIUS 服务器包期间出现问题。 • 超时。
未知用户	身份验证失败，并且 Fail on Reject 选项设置为 False。

Safeword 服务器支持特殊用户名格式

Safeword 令牌服务器支持使用以下用户名格式进行身份验证：

Username—Username, OTP

Cisco ISE 一收到身份验证请求，便会解析用户名并将其转换为以下用户名：

Username—Username

SafeWord 令牌服务器同时支持这两种格式。Cisco ISE 适用于各种令牌服务器。在配置 SafeWord 服务器时，您必须选中Cisco ISE 的管理门户中的 SafeWord Server 复选框，以解析用户名并将其转换为指定格式。在将请求发送到 RADIUS 令牌服务器之前，系统会在 RADIUS 令牌服务器身份源中执行此转换。

RADIUS 令牌服务器中的身份验证请求和响应

当Cisco ISE 向支持 RADIUS 的令牌服务器转发身份验证请求时，RADIUS 身份验证请求包含以下属性：

- 用户名（RADIUS 属性 1）
- 用户密码（RADIUS 属性 2）
- NAS IP 地址（RADIUS 属性 4）

Cisco ISE 预期收到以下任一响应：

- 接受访问 - 无需任何属性，但是响应可能包含根据 RADIUS 令牌服务器配置的各种属性。
- 拒绝访问 - 无需任何属性。
- 质询访问 - 每个 RADIUS RFC 所需的属性如下：
  - 状态（RADIUS 属性 24）
  - 回复信息（RADIUS 属性 18）
  - 以下一个或多个属性：供应商特定、空闲超时（RADIUS 属性 28）、会话超时（RADIUS 属性 27）、代理状态（RADIUS 属性 33）

    质询访问中不允许使用任何其他属性。

RADIUS 令牌身份源设置

下表介绍“RADIUS 令牌身份源”(Token Identity Sources) 窗口上的字段，您可以使用此窗口配置和连接外部 RADIUS 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

表 *38: RADIUS* 令牌身份源设置

字段名称	使用指南
名称	输入RADIUS 令牌服务器名称。允许的最大字符数为 64。
说明	输入RADIUS 令牌服务器说明。允许的最大字符数为 1024。
SafeWord Server	如果 RADIUS 身份源为 SafeWord 服务器，请选中此复选框。

字段名称	使用指南
Enable Secondary Server	选中此复选框，为Cisco ISE 启用辅助 RADIUS 令牌服务器，在主要服务器发生故障时用作备份。如果选中此复选框，必须配置辅助 RADIUS 令牌服务器。
Always Access Primary Server First	如果希望Cisco ISE 总是首先访问主服务器，请点击此选项。
Fallback to Primary Server after	点击此选项可指定在无法连接主服务器时，Cisco ISE 能够在多长时间里（分钟）使用辅助 RADIUS 令牌服务器进行身份验证。这段时间过后，Cisco ISE 重新尝试对照主服务器进行身份验证。
主服务器	
Host IP	输入主要 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在主要 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入主要 RADIUS 令牌服务器侦听的端口号。
Server Timeout	指定Cisco ISE 在确定主服务器关闭之前，等待主要 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在迁移到辅助服务器（如果已定义）或放弃请求（如果未定义辅服务器）之前，尝试重新连接到主服务器的次数。
辅助服务器	
Host IP	输入辅助 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在辅助 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入辅助 RADIUS 令牌服务器侦听的端口号。有效值为 1 至 65535。默认值为 1812。
Server Timeout	指定Cisco ISE 在确定辅助服务器关闭之前，等待辅助 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在放弃请求之前应当尝试重新连接辅助服务器的次数。

相关主题

RADIUS 令牌身份源，第 144 页
添加 RADIUS 令牌服务器，第 149 页

添加 RADIUS 令牌服务器

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)** > **添加 (Add)**。

步骤 2 在 **General** 和 **Connection** 选项卡中输入值。

步骤 3 点击 **Authentication** 选项卡。

通过此选项卡，您可以控制 RADIUS 令牌服务器对 Access-Reject 消息的响应。此响应可能意味着凭证无效或用户未知。Cisco ISE 收到以下其中一个响应：Failed authentication 或 User not found。通过此选项卡，您可以启用身份缓存和设置缓存的老化时间。您还可以配置请求密码的提示。

a) 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为失败身份验证，请点击**将拒绝视为“身份验证失败”(Treat Rejects as ‘authentication failed’)** 单选按钮。

b) 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为未知用户失败，请点击**将拒绝视为“未找到用户”(Treat Rejects as ‘user not found’)** 单选按钮。

步骤 4 如果您希望Cisco ISE 在使用 RADIUS 令牌服务器进行首次成功身份验证后将密码存储在缓存中，并为后续身份验证使用缓存的用户凭证（如果它们在配置的时间段内发生），请选中**启用密码缓存 (Enable Passcode Caching)** 复选框。

在**老化时间 (Aging Time)** 字段输入密码必须在缓存中存储的秒数。在此时间段内，用户可以使用同一密码执行多个身份验证。默认值为 30 秒。有效范围是从 1 到 300 秒。

注释 Cisco ISE 在首次身份验证失败后清除缓存。用户必须输入新的有效密码。

注释 我们强烈建议您仅在支持密码加密的协议（例如，EAP-FAST-GTC）中启用此选项。有关 RADIUS 令牌服务器支持的身份验证协议的信息，请参阅 支持 RADIUS 令牌服务器的身份验证协议，第 144 页

步骤 5 如果要允许处理没有在服务器上执行身份验证的请求，请选中**启用身份缓存 (Enable Identity Caching)** 复选框。

您可以启用身份缓存选项并以分钟为单位设置老化时间。默认值为 120 分钟。有效范围为 1 至 1440 分钟。从上次成功的身份验证中获得的结果和属性将在缓存中保留指定的时长。

默认情况下该选项处于禁用状态。

步骤 6 点击 **Authorization** 选项卡。

通过此选项卡，您可以配置该属性的显示名称。该属性是 RADIUS 令牌服务器向Cisco ISE 发送 Access-Accept 响应时返回的属性。此属性可用于授权策略条件。默认值为 CiscoSecure-Group-Id。

注释　如果要从外部 ID 源发送 Access-Accept 中的任何属性，则外部 ID 源需要发送 <ciscoavpair> 作为属性名称，值格式为 ACS:<attrname>=<attrvalue>，其中 <attrname> 是在**授权 (Authorization)** 选项卡中配置的。

步骤 7 点击**提交 (Submit)**。

删除 RADIUS 令牌服务器

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保您未选择身份源序列中的 RADIUS 令牌服务器。如果您选择身份源序列中的 RADIUS 令牌服务器，删除操作将失败。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

步骤 2 选中要删除的 RADIUS 令牌服务器旁边的复选框，然后点击 **Delete**。

步骤 3 点击**确定 (OK)** 以删除您已选择的 RADIUS 令牌服务器。

如果您选择删除多个RADIUS令牌服务器，且其中一个服务器用于身份源序列，则删除操作将失败，任何RADIUS令牌服务器都不会被删除。

RSA 身份源

Cisco ISE 支持 RSA SecurID 服务器作为外部数据库。RSA SecurID 双因素身份验证由用户的 PIN 和单独注册的 RSA SecurID 令牌组成，该令牌基于时间代码算法生成一次性令牌代码。其他令牌代码按固定时间间隔（通常每 30 或 60 秒）生成。RSA SecurID 服务器会验证此动态身份验证代码。每个 RSA SecurID 令牌都是唯一的，并且无法根据以往令牌预测未来令牌的值。因此，在提供正确的令牌代码与 PIN 时，大致可以确定该人员是有效用户。因此，RSA SecurID 服务器提供的身份验证机制比传统可重用密码更可靠。

Cisco ISE 支持以下 RSA 身份源：

- RSA ACE/Server 6.x 系列
- RSA Authentication Manager 7.x 和 8.0 系列

您可以通过以下任何一种方式与 RSA SecurID 身份验证技术集成：

- 使用 RSA SecurID 代理 - 用户通过 RSA 本地协议使用其用户名和密码进行身份验证。
- 使用 RADIUS 协议 - 用户通过 RADIUS 协议使用其用户名和密码进行身份验证。

Cisco ISE 中的 RSA SecurID 令牌服务器通过使用 RSA SecurID 代理与 RSA SecurID 身份验证技术相连接。

Cisco ISE 仅支持一个 RSA 领域。

思科 ISE 和 RSA SecurID 服务器集成

以下是将Cisco ISE 与 RSA SecurID 服务器连接所涉及的两个管理角色：

- RSA 服务器管理员 - 配置和维护 RSA 系统与集成
- Cisco ISE 管理员 - 将Cisco ISE 配置为连接到 RSA SecurID 服务器并维护配置

本节介绍将Cisco ISE 与 RSA SecurID 服务器连接作为外部身份源所涉及的流程。有关 RSA 服务器的更多信息，请参考 RSA 文档。

思科 ISE 中的 RSA 配置

RSA 管理系统生成 sdconf.rec 文件，RSA 系统管理员将为您提供此文件。您可以通过此文件在领域中添加Cisco ISE 服务器作为 RSA SecurID 代理。您必须浏览至此文件并将其添加至Cisco ISE 中。通过复制过程，主要Cisco ISE 服务器将此文件分发至所有辅助服务器。

针对 RSA SecurID 服务器进行的 RSA 代理身份验证

在所有Cisco ISE 服务器上安装 sdconf.rec 文件之后，RSA 代理模块进行初始化，并且每个Cisco ISE 服务器上都将使用 RSA 生成的凭证进行身份验证。在部署中的每个Cisco ISE 服务器上的代理都成功通过身份验证之后，RSA 服务器和代理模块将一起下载 securid 文件。此文件位于Cisco ISE 文件系统中，而且是在 RSA 代理定义的已知位置。

思科 ISE 分布式环境中的 RSA 身份源

管理分布式Cisco ISE 环境中的 RSA 身份源涉及以下操作：

- 将主服务器上的 sdconf.rec 和 sdopts.rec 文件分布到辅助服务器。
- 删除 securid 和 sdstatus.12 文件。

思科 ISE 部署中的 RSA 服务器更新

在Cisco ISE 中添加 sdconf.rec 文件后，RSA SecurID 管理员可能在停用 RSA 服务器或添加新的 RSA 辅助服务器时更新 sdconf.rec 文件。RSA SecurID 管理员将为您提供更新的文件。您可以使用更新的文件重新配置Cisco ISE。在Cisco ISE 中的复制流程将更新的文件分布到部署中的辅助Cisco ISE 服务器。Cisco ISE 首先更新文件系统中的文件，然后与 RSA 代理模块协调，酌情逐步执行重启流程。更新 sdconf.rec 文件时，将重置（删除）sdstatus.12 和 securid 文件。

覆盖自动 RSA 路由

一个领域中可以有不止一个 RSA 服务器。sdopts.rec 文件执行负载均衡器的职责。Cisco ISE 服务器和 RSA SecurID 服务器通过代理模块运行。位于Cisco ISE 上的代理模块维护一分基于成本的路由表

以充分利用领域中的 RSA 服务器。但是，您可以通过 Admin 门户使用名称为 sdopts.rec 的文本文件为该领域的每个Cisco ISE 服务器进行手动配置，以选择覆盖此路由。有关如何创建此文件的信息，请参阅 RSA 文档。

RSA 节点密钥重置

SecurID 文件是秘密节点密钥文件。RSA 经过初始设置后，会使用密钥验证代理。位于Cisco ISE 中的 RSA 代理第一次成功对 RSA 服务器进行身份验证后，会在客户端计算机上创建一个名为 SecurID 的文件，并会使用该文件确保在设备之间交换的数据有效。有时，可能必须从部署中的特定Cisco ISE 服务器或一组服务器中删除 SecurID 文件（例如，在 RSA 服务器上重置密钥之后）。可以使用 Cisco ISE 管理门户从该领域的Cisco ISE 服务器中删除此文件。Cisco ISE 中的 RSA 代理在下一次成功进行身份验证时，会创建新的 SecurID 文件。

注释 如果在升级到最新版本的思科 ISE 之后，身份验证失败，请重置 RSA 密钥。

RSA 自动可用性重置

sdstatus.12 文件提供有关领域中的 RSA 服务器可用性的信息。例如，它提供有关哪些服务器处于活动状态和哪些已关闭的信息。代理模块与领域中的 RSA 服务器协作维护此可用性状态。此信息在 sdstatus.12 文件中连续列出，此文件位于Cisco ISE 文件系统中的常见位置。有时，此文件会变成旧文件，而当前状态未反映在此文件中。您必须删除此文件，以便可以重新创建当前状态。您可以使用管理门户从特定领域的特定Cisco ISE 服务器中删除此文件。Cisco ISE 与 RSA 代理协调并确保正确的重新启动阶段化。

每当重置 securid 文件或者更新 sdconf.rec 或 sdopts.rec 文件时，便会删除 sdstatus.12 文件。

RSA SecurID 身份源设置

下表介绍“RSA SecurID 身份源”(RSA SecurID Identity Sources) 窗口上的字段，您可以使用此窗口创建和连接 RSA SecurID 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 *39: RSA* 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。

字段名称	使用指南
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 *40: RSA* 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源，第 150 页
思科 ISE 和 RSA SecurID 服务器集成，第 151 页
添加 RSA 身份源，第 154 页

添加 RSA 身份源

要创建 RSA 身份源，必须导入 RSA 配置文件 (sdconf.rec)。必须从 RSA 管理员那里获取 sdconf.rec 文件。要执行此任务，您必须是超级管理员或系统管理员。

添加 RSA 身份源需要执行以下任务：

导入 RSA 配置文件

必须导入 RSA 配置文件，才能在Cisco ISE 中添加 RSA 身份源。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 2 点击**浏览 (Browse)**，从正运行客户端浏览器的系统中选择新建或更新的 sdconf.rec 文件。

首次创建 RSA 身份源时，Import new sdconf.rec file 字段为必填字段。从那以后，可以用更新的 sdconf.rec 文件替换现有的 sdconf.rec 文件，但替换现有文件是可选操作。

步骤 3 以秒为单位输入服务器超时值。在超时之前，Cisco ISE 将在指定的时间内等待 RSA 服务器做出响应。该值可以是 1 至 199 之间的任意整数。默认值为 30 秒。

步骤 4 PIN 发生更改时，选中 **Reauthenticate on Change PIN** 复选框，强制执行重新验证。

步骤 5 点击**保存 (Save)**。

Cisco ISE 也支持以下场景：

- 为Cisco ISE 服务器配置选项文件，重置 SecurID 和 sdstatus.12 文件。
- 为 RSA 身份源配置身份验证控制选项。

为思科 ISE 服务器配置选项文件并重置 SecurID 和 sdstatus.12 文件

步骤 1 登录Cisco ISE 服务器。

步骤 2 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 3 点击 **RSA Instance Files** 选项卡。

此页面列出您的部署中所有Cisco ISE 服务器的 sdopts.rec 文件。

当用户经过 RSA SecurID 令牌服务器的身份验证后，节点密钥状态会显示为已创建 *(Created)*。节点密钥状态可为以下其中一种：“已创建”(Created) 或“未创建”(Not Created)。清除节点密钥状态后，它会显示为未创建 *(Not Created)*。

步骤 4 点击特定Cisco ISE 服务器 sdopts.rec 文件旁边的单选按钮，然后点击 **Update Options File**。

Current File 区域会显示现有文件。

步骤 5 选择如下选项之一：

- Use the Automatic Load Balancing status maintained by the RSA agent - 如果希望 RSA 代理自动管理负载均衡，请选择此选项。
- Override the Automatic Load Balancing status with the sdopts.rec file selected below - 如果想要根据您的具体需求手动配置负载均衡，请选择此选项。如果选择此选项，则必须点击**浏览 (Browse)**，然后从运行客户端浏览器的系统选择新的 sdopts.rec 文件。

步骤 6 点击**确定 (OK)**。

步骤 7 点击与Cisco ISE 服务器对应的行以重置该服务器的 securid 和 sdstatus.12 文件：

a) 点击下拉箭头，然后在“重置 securid 文件”(Reset securid File) 列和“重置 sdstatus.12 文件”(Reset sdstatus.12 File) 列中选择**提交时删除 (Remove on Submit)**。

注释 Reset sdstatus.12 File 字段隐藏在您的视线之外。在最内部的框中使用垂直和水平滚动条，向下滚动，然后向右滚动以查看此字段。

b) 在此行中点击**保存 (Save)** 以保存更改。

步骤 8 点击**保存 (Save)**。

为 RSA 身份源配置身份验证控制选项

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 2 点击 **Authentication Control** 选项卡。

步骤 3 选择如下选项之一：

- Treat Rejects as "authentication failed" - 如果您希望将拒绝的请求视为失败的身份验证，请选择此选项。
- Treat Rejects as "user not found" - 如果您希望将拒绝的请求视为“未找到用户”错误，请选择此选项。

步骤 4 如果希望Cisco ISE 在第一次身份验证成功后在缓存中存储密码，并为在配置的时间段内发生的后续身份验证使用缓存的用户凭据，请选中**启用密码缓存 (Enable Passcode Caching)** 复选框。

在**老化时间 (Aging Time)** 字段输入密码必须在缓存中存储的秒数。在此时间段内，用户可以使用同一密码执行多个身份验证。默认值为 30 秒。有效范围是从 1 到 300 秒。

注释 Cisco ISE 在首次身份验证失败后清除缓存。用户必须输入新的有效密码。

注释 我们强烈建议您仅在支持密码加密的协议（例如，EAP-FAST-GTC）中启用此选项。

步骤 5 如果要允许处理没有在服务器上执行身份验证的请求，请选中**启用身份缓存 (Enable Identity Caching)** 复选框。

您可以启用身份缓存选项并以分钟为单位设置老化时间。默认值为 120 分钟。有效范围为 1 至 1440 分钟。从上次成功的身份验证中获得的结果和属性将在缓存中保留指定的时长。

默认情况下该选项处于禁用状态。

步骤 6 点击**保存 (Save)** 保存配置。

配置 RSA 提示

Cisco ISE 允许您配置系统在处理发送给 RSA SecurID 服务器的请求时向用户显示的 RSA 提示。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

步骤 2 点击 **Prompts**。

步骤 3 输入“RSA SecurID 身份源设置”中所述的值。

步骤 4 点击**提交 (Submit)**。

配置 RSA 消息

通过Cisco ISE，您可以配置在处理发送到 RSA SecurID 服务器的请求时向用户显示的消息。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

步骤 2 点击 **Prompts**。

步骤 3 点击 **Messages** 选项卡。

步骤 4 输入“RSA SecurID 身份源设置”中所述的值。

步骤 5 点击**提交 (Submit)**。

SAMLv2 身份提供者作为外部身份源

安全断言标记语言 (SAML) 是基于 XML 的开放标准数据格式，可让管理员在登录到其中一个应用后能够无缝访问定义的一组应用。SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。SAML 实现了身份提供者 (IdP) 和服务提供者（在这里是指 ISE）之间安全身份验证信息的交换。

SAML 单点登录 (SSO) 在调配过程中通过在 IdP 和服务提供者之间交换元数据和证书建立信任圈 (CoT)。服务提供者信任 IdP 的用户信息，提供对各种服务或应用的访问权限。

启用 SAML SSO 可提供以下优势：

- 无需输入不同的用户名和密码组合，降低了密码管理难度。
- 由于重新输入同一身份的凭证所需的时间减少，提高了效率。
- 将身份验证从托管应用的系统转移到第三方系统。
- 降低成本，由于请求重置密码的服务中心呼叫减少，从而节省更多成本。

IdP 是身份验证模块，可以创建、保留并管理用户、系统或服务的身份信息。IdP 存储和验证用户凭证，并生成 SAML 响应以允许用户访问受服务提供者保护的资源。

注释 您必须熟悉自己的 IdP 服务，确保该服务当前已安装并且可以运行。

以下门户支持 SAML SSO：

- 访客门户（发起人管理或自助注册）
- 发起人门户
- 我的设备门户
- 证书调配门户

您不能选择 IdP 作为 BYOD 门户的外部身份源，但可以为访客门户选择 IdP 并启用 BYOD 流程。

Cisco ISE 符合 SAMLv2，支持符合 SAMLv2 且使用 Base64 编码的证书的所有 IdP。下面列出的 IdP 已使用Cisco ISE 进行了测试：

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP 无法添加到身份源序列。

SSO 会话将终止，并且如果在指定的时间（默认为 5 分钟）内没有任何活动，会显示一条 Session Timeout 错误消息。

如果想要在门户的 Error 页面中添加 Sign On Again 按钮，请在 Portal Error 页面的 Optional Content 字段中添加以下 JavaScript：

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">重新登录</button>
```

在思科 ISE 中配置 SAML 身份提供程序

要在Cisco ISE 中配置 SAML 身份提供程序，请执行以下操作：

- 您必须是Cisco ISE 中的超级管理员或系统管理员。
- 如果要使用的证书不是身份提供程序 (IdP) 自签名的，则将证书颁发机构 (CA) 证书导入受信任证书库。
- 您必须对正在配置的IdP门户具有管理员访问权限。以下任务需要在IdP门户中执行一些步骤。

要在Cisco ISE 中配置 SAML 身份提供程序，请执行以下操作：

1. 将 SAML 身份提供程序添加至Cisco ISE。
2. 添加 SAML 身份提供程序作为门户的身份验证方法。
3. 配置 SAML ID 提供程序。

将 SAML 身份提供程序添加至思科 ISE

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在显示的**SAML 身份提供程序 (SAML Identity Provider)** 窗口中，在**常规 (General)** 选项卡中输入 **ID 提供程序名称 (Id Provider Name)** 和**说明 (Description)**。

步骤 4 点击**提交 (Submit)**。

步骤 5 在**身份提供程序配置 (Identity Provider Config)** 选项卡中，导入相关的 metadata.xml 文件，然后点击**提交 (Submit)**。

将 SAML 身份提供程序添加为门户的身份验证方法

您可以将刚刚创建的 SAML 身份提供程序添加到以下门户：

1. 自注册访客门户和发起的访客门户（**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)**）
2. 证书调配门户（**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配** > **证书调配门户 (Certificate Provisioning Portal)**

步骤 1 在要配置的门户的门户自定义窗口中，点击**门户设置 (Portal Settings)**。

步骤 2 在显示的下拉部分中，转到**身份验证方法 (Authentication Method)** 部分，然后使用菜单选择所添加的 SAML IP 提供程序。

步骤 3 点击**保存 (Save)**。

配置 SAML ID 提供程序

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。选择刚才链接到门户的 IdP，然后点击**编辑 (Edit)**。

步骤 2 （可选）如果使用负载均衡器来优化Cisco ISE 节点上的负载，则可以在**服务提供商 (Service Provider Info)** 信息选项卡中添加其详细信息，以简化 IdP 的配置。可以添加软件或硬件负载均衡器。

负载均衡器应该能够使用**端口设置 (Portal Settings)** 中指定的端口，将请求转发到部署中的Cisco ISE 节点。

当添加负载均衡器时，在服务提供商元数据文件中只提供其负载均衡器 URL。如果负载均衡器不存在，则在服务提供商元数据文件中会包含多个 **AssertionConsumerService** URL。

注释 我们建议避免在门户 FQDN 设置中使用相同的负载均衡器 IP 地址。

步骤 3 在**服务提供商信息 (Service Provider Info)** 选项卡中，点击**导出 (Export)** 导出服务提供者元数据文件。导出的元数据包括Cisco ISE 的签名证书，与所选门户的证书完全相同。

导出的元数据压缩文件夹包括一个自述文件，其中含有配置每个 IdP （包括 Azure Active Directory、PingOne、PingFederate、SecureAuth 和 OAM）的基本操作说明。

如果以下方面有以下任何更改，则必须重新导出服务提供商元数据：

- 新Cisco ISE 节点的注册。
- 节点的主机名或 IP 地址。
- 我的设备门户、发起人门户或证书调配门户的完全限定域名 (FQDN)。
- 端口和接口设置。
- 关联的负载均衡器。

如果不重新导出更新后的的元数据，则 IdP 可能会拒绝用户身份验证请求。

步骤 4 转到您的 IdP 门户并以管理员用户身份登录，导入刚才从Cisco ISE 导出的服务提供商元数据文件。您需要首先解压导出的文件夹和具有门户名称的元数据文件。该元数据文件包括提供商 ID 和绑定 URI。

步骤 5 返回Cisco ISE 门户。

步骤 6 （可选）在 **SAML 身份提供程序 (SAML Identity Provider)** 窗口的**组 (Groups)** 选项卡中，添加所需的用户组。

输入在**组成员**属性 (Group Membership Attribute) 字段中指定用户组成员的声明属性。

步骤 7 （可选）在**属性 (Attributes)** 选项卡中添加用户属性，以指定属性如何显示在从 IdP 返回的断言中。

您在 **ISE 中名称 (Name in ISE)** 中指定的名称会在策略规则中显示。

对于属性，支持以下的数据类型：

- 字符串
- 整数
- IPv4
- 布尔值

步骤 8 在**高级设置 (Advanced Settings)** 选项卡中，配置以下选项：

选项	描述
身份属性	通过点击显示的选项对应的单选按钮以选择属性，用来指定要进行身份验证的用户身份。 **注释** Cisco ISE 不支持包含临时或永久格式的使用者名称 (NameID) 的 SAML IdP 响应。如果使用这些方法，Cisco ISE 无法从 SAML IdP 响应中检索用户名属性断言，并且身份验证将失败。
电子邮件属性	从下拉列表中，选择返回用户电子邮件地址的断言属性。如果计划过滤（限制）由同一发起人批准的发起访客名单，则必须配置电子邮件属性。
多值属性	选择以下一个选项： • **每个单独 XML 中各一个值 (Each value in a separate XML)**：如果您的 IdP 在不同 XML 元素中返回同一属性的多个值，则点击该选项。 • **单个 XML 中多个值 (Multiple values in a single XML)**：如果您的 IdP 在单个 XML 元素中返回多个值，则点击该选项。在文本框中指定分隔符。
注销设置	如果希望对注销请求进行签名，请选中**签署注销请求 (Sign Logout Requests)** 复选框。如果正在配置的 IdP 是 Oracle Access Manager 或 Oracle Identity Federation，则不会显示此选项。 **注释** SecureAuth 不支持 SAML 注销。 以下选项仅在配置 Oracle Access Manager 或 Oracle Identity Federation IdP 且未配置负载均衡器时显示： • **注销 URL (Logout URL)**：输入一个页面 URL，当用户从发起人门户或我的设备门户注销时，他们将重定向到该页面以终止 SSO 会话。 • **重定向参数名称 (Redirect Parameter Name)**：当 SSO 会话终止时，用户将返回到 IdP 的登录页面。重定向参数名称可能因 IdP 而异，例如，**end_url** 或 **returnURL**。该字段区分大小写。 如果注销操作未按预期运行，请查看 IdP 的文档，了解有关使用注销 URL 和重定向参数名称的详细信息。
身份验证上下文	使用此部分可编辑 SAML IdP 身份验证上下文类引用。Cisco ISE SAML 请求通常在 SAML 请求标题中使用 **PasswordProtectedTransport** 身份验证方法。这导致在使用多因素身份验证的情况下发生身份验证失败。

选项	描述
	要避免这种情况，您可以使用 **AuthnContextClassRef SAML 元素 (AuthnContextClassRef SAML Element)** 部分指定身份验证方法。如果不确定所使用的身份验证方法，我们建议将此部分留空，以避免身份验证失败。

步骤 9 点击**提交 (Submit)**。

删除身份提供者

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

确保您要删除的 IdP 未链接至任何门户。如果 IdP 与任何门户链接，删除操作将失败。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > 网络访问 (Network Access) > 分机 ID 源 (Ext Id Sources) > SAML ID 提供商 (SAML Id Providers)**。

步骤 2 选中您要删除的 IdP 旁边的复选框，然后点击 **删除 (Delete)**。

步骤 3 点击**确定 (OK)** 以删除您所选择的 IdP。

身份验证失败日志

当按照 SAML ID 库进行身份验证失败并且 IdP 将用户重定向回 ISE 门户（通过 SAML 响应），ISE 将在身份验证日志中报告失败原因。对于访客门户（启用或不启用自带设备流量的情况下），您可以检查 RADIUS 实时日志 (RADIUS Livelog)（操作 (Operations) > RADIUS > 实时日志 (Live Log)）了解身份验证失败原因。对于我的设备门户和发起人门户，您可以查看我的设备登录/审计报告和发起人登录/审计报告（操作 (Operations) > 报告 (Reports) > 访客 (Guest)）了解身份验证失败原因。

如果出现注销故障，您可以查看报告，并通过登录了解我的设备、发起人和访客门户出现故障的原因。

身份验证可能由于以下原因而失败：

- SAML 响应解析错误
- SAML 响应验证错误（例如 Wrong Issuer）
- SAML 断言验证错误（例如 Wrong Audience）
- SAML 响应签名验证错误（例如 Wrong Signature）
- IdP 签名证书错误（例如 Certificate Revoked）

注释 Cisco ISE 不支持具有加密断言的 SAML 响应。如果在 IdP 中配置了此选项，您将在 ISE 中看到以下错误消息：`FailureReason = 24803 无法找到“用户名”属性断言 (FailureReason=24803 Unable to find 'username' attribute assertion)`。

如果身份验证失败，我们建议您检查身份验证日志中的“DetailedInfo”属性。此属性提供关于失败原因的更多信息。

身份源序列

身份源序列定义Cisco ISE 在不同数据库中查找用户凭证的顺序。

如果您在多个连接到Cisco ISE 的数据库中有用户信息，您可以定义您希望Cisco ISE 在这些身份源中查找信息的顺序。找到匹配后，Cisco ISE 不会继续查找，而是评估证书，将结果返回给用户。此策略是第一个匹配策略。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

删除身份源序列

您可以删除不再在策略中使用的身份源序列。

开始之前

- 确保您即将删除的身份源序列未在任何身份验证策略中使用。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

步骤 2 选中要删除的一个或多个身份源序列旁边的复选框，然后点击 **Delete**。

步骤 3 点击**确定 (OK)** 删除一个或多个身份源序列。

报告中的身份源详细信息

Cisco ISE 通过 Authentications dashlet 报告和 Identity Source 报告提供关于身份源的信息。

身份验证面板

在身份验证面板中，您可以逐步向下展开，找到包括故障原因在内的更多信息。

选择操作 (Operations) > RADIUS 实时日志 (RADIUS Livelog) 以查看实时身份验证概述。有关 RADIUS 实时日志的详细信息，请参阅 RADIUS 实时日志。

身份源报告

Cisco ISE 提供包含身份源相关信息的各种报告。有关这些报告的说明，请参阅“可用报告”一节。

网络上已分析的终端

分析器服务可协助识别、查找和确定您的网络上所有终端的功能（在Cisco ISE 中叫作身份），而无论其设备类型如何，从而确保和保持对您的企业网络的适当访问。Cisco ISE 分析器功能使用大量的探测功能收集您的网络上所有终端的属性，并将这些属性传递至分析服务分析器，此分析器根据已知终端的关联策略和身份组给已知终端分类。

分析器源服务允许管理员通过Cisco ISE 中的订用从指定Cisco源服务器检索新的和已更新的终端分析策略以及作为源的已更新 OUI 数据库。

分析器条件设置

下表介绍“分析器条件”(Profiler Condition) 窗口中的字段。此窗口的导航路径是 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)**。

表 *41:* 分析器条件设置

字段名称	使用指南
名称 (Name)	分析器条件的名称。
说明	分析器条件的说明。
类型	选择任何一个预定义类型。
Attribute Name	选择分析器条件所基于的属性。
运算符	选择运算符。
Attribute Value	输入已选择的属性的值。对于包含预定义属性值的属性名称，此选项显示具有预定义值的下拉列表，并且您可以选择值。
System Type	分析条件可以是以下任何一个类型： • **思科提供 (Cisco Provided)**：在部署时由Cisco ISE 提供的分析条件标识为“Cisco提供”(Cisco Provided)。您不能从系统编辑或删除这些条件。 • **管理员创建 (Administrator Created)**：您以Cisco ISE 管理员身份创建的分析条件标识为“管理员创建”(Administrator Created)。

相关主题

思科 ISE 分析服务，第 165 页
分析器条件，第 189 页
分析器源服务，第 226 页
创建分析器条件，第 204 页

思科 ISE 分析服务

Cisco身份服务引擎 (ISE) 中的分析服务能够识别连接到网络的设备及其位置。它根据在Cisco ISE 中配置的终端分析策略来分析终端。然后，Cisco ISE 会根据策略评估的结果，向终端授予访问网络资源的权限。

分析服务：

- 利用 IEEE 802.1X 基于端口的标准身份验证访问控制、MAC 身份验证绕行 (MAB) 身份验证，以及适用于各种规模和复杂性的任何企业网络的网络准入控制 (NAC)，可以实现高效和有效的部署以及对身份验证的持续管理。
- 识别、查找并确定连接的所有网络终端的功能，无论终端类型是什么都如此。
- 防止意外拒绝对某些终端的访问。

ISE 社区资源

ISE 终端配置文件

操作方法：ISE 分析设计指南

分析器工作中心

分析器工作中心菜单（“工作中心”(Work Centers) > “分析器”(Profiler)）包含所有分析器页面，作为 ISE 管理员的单一起点。分析器工作中心菜单包含以下选项：“概述”(Overview)、“外部 ID 库”(Ext ID Stores)、“网络设备”(Network Devices)、“终端分类”(Endpoint Classification)、“节点配置”(Node Config)、“源”(Feeds)、“手动扫描”(Manual Scans)、“策略元素”(Policy Elements)、“分析策略”(Profiling Policies)、“授权策略”(Authorization Policy)、“故障排除”(Troubleshoot)、“报告”(Reports)、“设置”(Settings) 和“字典”(Dictionaries)。

分析器控制面板

分析器控制面板（工作中心 (Work Centers) > 分析器 (Profiler) > 终端分类 (Endpoint Classification)）是一种集中式监控网络中配置文件、终端和资产的工具。该控制面板同时以图形和表格格式展示数据。“配置文件”(Profiles) dashlet 显示当前在网络中处于活动状态的逻辑和终端配置文件。“终端”(Endpoints) dashlet 显示连接到网络的终端的身份组、PSN 和操作系统类型。“资产”(Assets) dashlet 显示访客、自带设备和公司等流程。下表显示了连接的各种终端，您也可以添加新的终端。

使用分析服务的终端资产

您可以使用分析服务发现、找到和确定连接到网络的所有终端的功能。无论设备类型如何，都可以确保和维护终端对企业网络的适当访问。

分析服务从网络设备和网络收集终端属性，根据配置文件将终端归到特定组，以及在Cisco ISE 数据库中存储终端及其匹配的配置文件。分析服务处理的所有属性都需要在分析器字典中定义。

分析服务识别网络上的每个终端，并根据配置文件将这些终端归入系统中的现有终端身份组，或者归入您在系统中创建的新组。通过对终端分组以及将终端分析策略应用到终端身份组，您可以确定终端到相应终端分析策略的映射。

思科 ISE 分析器队列限制配置

Cisco ISE 分析器可在短时间内从网络收集大量终端数据。由于某些速度较慢的Cisco ISE 组件在处理分析器生成的数据时会产生积压（造成性能下降和稳定性问题），因此这将导致 Java 虚拟机 (JVM) 内存使用率增加。

为确保分析器不会增加 JVM 内存使用率并防止 JVM 内存不足和重新启动，系统会对分析器的以下内部组件应用限制：

- 终端缓存 - 内部缓存大小有限，当大小超过限制时，必须定期清除（根据最近最少使用的策略）。
- 转发器 - 分析器收集的终端信息的主入口队列。
- 事件处理程序 - 用于断开快速组件（该组件会向较慢的处理组件 [通常与数据库查询相关] 提供数据）的连接的内部队列。

终端缓存

- maxEndPointsInLocalDb = 100000（缓存中的终端对象数）
- endPointsPurgeIntervalSec = 300（终端缓存清除线程时间间隔，以秒为单位）
- numberOfProfilingThreads = 8（线程数）

限制适用于所有分析器内部事件处理程序。当达到队列大小限制时，会触发监控警报。

思科 ISE 分析器队列大小限制

- forwarderQueueSize = 5000（终端集合事件数）
- eventHandlerQueueSize = 10000（事件数）

事件处理程序

- NetworkDeviceEventHandler - 除筛选已经缓存的重复网络接入设备 (NAD) IP 地址外，还用于处理网络设备事件。
- ARPCacheEventHandler - 用于处理 ARP 缓存事件。

Martian IP 地址

Martian IP 地址不会在 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** 和 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **终端分类 (Endpoint Classification)** 窗口中显示，因为 RADIUS 解析器会在这些

地址到达分析服务之前将其删除。Martian IP 地址容易受到攻击，因此是安全隐患。但是，出于审核目的，MnT 日志中会显示 Martian IP 地址。此行为在组播 IP 地址的情况下也是如此。有关 Martian IP 地址的详细信息，请参阅 https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html

分析转发器持久化队列

分析转发器持久化队列会存储事件，然后再将事件发送到分析器模块进一步处理。此外，还增加了队列容量，以支持增加的事件处理工作。这可以减少因事件数量突然增加而丢失的事件数量。这继而会减少队列达到其最大限制时发出的警报。

默认情况下启用此功能。如果需要，您可以禁用此功能以回退到原始机制，在该机制中，事件直接发送到分析器模块。要启用或禁用此功能，请选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **分析 (Profiling)** 并选中或取消选中**启用分析转发器持久化队列 (Enable Profiler Forwarder Persistence Queue)** 复选框。

在思科 ISE 节点中配置分析服务

可以配置分析服务，该服务为您提供正在任何启用Cisco ISE 的网络中使用网络资源的所有终端的上下文资产。

可以将分析服务配置为在单一Cisco ISE 节点上运行，默认情况下，此节点承担所有管理、监控和策略服务角色。

在分布式部署中，分析服务仅在承担策略服务角色的Cisco ISE 节点上运行，不在承担管理和监控角色的其他Cisco ISE 节点上运行。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选择承担策略服务角色的Cisco ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击**编辑 (Edit)**。

步骤 4 在**常规设置 (General Settings)** 选项卡上，选中**策略服务 (Policy Service)** 复选框。如果取消选中 Policy Service 复选框，会话服务和分析服务复选框均被禁用。

步骤 5 执行以下任务：

a) 选中 **Enable Session Services** 复选框，运行网络访问、终端安全评估、访客和客户端调配会话服务。

b) 选中 **Enable Profiling Services** 复选框，运行分析服务。

c) 选中**启用设备管理服务 (Enable Device Admin Service)** 复选框运行设备管理服务，对企业网络设备进行控制和审计。

步骤 6 点击**保存 (Save)**，保存节点配置。

分析服务使用的网络探测功能

网络探测功能是一种用于从网络上的终端收集属性或属性集的方法。通过探测功能，您可以使用Cisco ISE 数据库中的终端匹配配置文件创建或更新终端。

Cisco ISE 可以使用许多网络探测功能来分析设备，这些网络探测功能会分析网络上设备的行为并确定设备的类型。网络探测功能可帮助您获取更多网络可视性。

IP 地址和 MAC 地址绑定

您只能通过在企业网络中使用终端的 MAC 地址来创建或更新终端。如果您在 ARP 缓存中找不到条目，则可以通过在Cisco ISE 中使用 HTTP 数据包的 L2 MAC 地址和 NetFlow 数据包的 IN_SRC_MAC 来创建或更新终端。当终端只是一个跃点之隔时，分析服务依赖于 L2 邻接。当终端是 L2 邻接时，表明已映射终端的 IP 地址和 MAC 地址，无需进行 IP-MAC 缓存映射。

如果终端不是L2 邻接并且间隔多个跃点，则映射可能不可靠。您收集的NetFlow 数据包的一些已知属性包括 PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC 和 OUT_SRC_MAC。当终端不是 L2 邻接并且间隔多个 L3 跃点时，IN_SRC_MAC 属性只能运载 L2 网络设备的 MAC 地址。当在Cisco ISE 中启用 HTTP 探测时，您只能通过使用 HTTP 数据包的 MAC 地址创建终端，因为 HTTP 请求消息在负载数据中不会运载终端的 IP 地址和 MAC 地址。

Cisco ISE 在分析服务中实施 ARP 缓存，以便您能够可靠地映射终端的 IP 地址和 MAC 地址。为使 ARP 缓存正常运行，您必须启用 DHCP 探测或 RADIUS 探测。DHCP 和 RADIUS 探测在负载数据中运载终端的 IP 地址和 MAC 地址。DHCP 探测中的 dhcp-requested 地址属性和 RADIUS 探测中的 Framed-IP-address 属性运载终端的 IP 地址，及其可在 ARP 缓存中映射和存储的 MAC 地址。

NetFlow 探测功能

Cisco ISE 分析器使用Cisco IOS NetFlow 版本 9。我们建议使用 NetFlow 版本 9，因为其具有增强此分析器以支持Cisco ISE 分析服务的更多功能。

您可以从支持 NetFlow 的网络访问设备收集 NetFlow 版本 9 属性以在Cisco ISE 数据库中创建终端或更新现有终端。您可以将 NetFlow 版本 9 配置为连接终端和更新终端的源与目标 MAC 地址。您还可以创建 NetFlow 属性字典以支持基于 NetFlow 的分析。

有关NetFlow 版本 9 记录格式的更多信息，请参阅 NetFlow 版本 9 流程-记录格式文档的表 6“NetFlow 版本 9 字段类型定义”。

此外，Cisco ISE 支持低于 5 以下的 NetFlow 版本。如果您在网络使用 NetFlow 版本 5，则只能在接入层主要网络访问设备 (NAD) 上使用版本 5，因为此版本在其他位置无法运行。

Cisco IOS NetFlow 版本 5 程序包不包含终端的 MAC 地址。从 NetFlow 版本 5 收集的属性不能直接添加至Cisco ISE 数据库。您可以通过使用终端的 IP 地址发现终端，并且通过将网络访问设备的 IP 地址与从 NetFlow 版本 5 属性获取的 IP 地址组合，将 NetFlow Version 5 属性附加到终端上。但是，之前必须已使用 RADIUS 或 SNMP 探测功能发现这些终端。

在早版 NetFlow 版本 5 中，MAC 地址不是 IP 流的组成部分，这就要求您关联从终端缓存中的网络访问设备收集的属性信息，才能用终端 IP 地址分析终端。

有关 NetFlow 版本 5 记录格式的更多信息，请参阅《NetFlow 服务解决方案指南》中表 2“Cisco ISE NetFlow 流程记录和导出格式内容信息”。

DHCP 探测功能

在Cisco ISE 部署中，动态主机配置协议探测功能允许Cisco ISE 分析服务仅根据 INIT-REBOOT 和 SELECTING 消息类型的新请求，重新分析终端。虽然系统会处理 RENEWING 和 REBINDING 等其他 DHCP 消息类型，但是这些消息类型不会用于分析终端。在 DHCP 数据包之外解析的任何属性都会映射至终端属性。

在 INIT-REBOOT 状态期间生成的 DHCPREQUEST 消息

如果 DHCP 客户端进行检查以验证之前分配和缓存的配置，则客户端不得填写 Server identifier (server-ip) 选项，而应该用之前分配的 IP 地址填写 Requested IP address (requested-ip) 选项，并且在其 DHCPREQUEST 消息中用零填写 Client IP Address (ciaddr) 字段。然后，如果所请求的 IP 地址不正确或客户端位于错误的网络上，则 DHCP 服务器将向该客户端发送 DHCPNAK 消息。

在 SELECTING 状态期间生成的 DHCPREQUEST 消息

DHCP 客户端在 Server identifier (server-ip) 选项中插入所选 DHCP 服务器的 IP 地址，用客户端选择的 DHCPOFFER 的 Your IP Address (yiaddr) 字段的值填写 Requested IP address (requested-ip) 选项，并且在“ciaddr”字段中填写零。

表 *42:* 来自不同状态的 *DHCP* 客户端消息

-	INIT-REBOOT	SELECTING	RENEWING	REBINDING
广播 / 单播	广播	广播	单播	广播
server-ip	不得填写	必须填写	不得填写	不得填写
requested-ip	必须填写	必须填写	不得填写	不得填写
ciaddr	零	零	IP 地址	IP 地址

DHCP 桥接模式下的无线 LAN 控制器配置

我们建议您在动态主机配置协议 (DHCP) 桥接模式下配置无线 LAN 控制器 (WLC)，这样您就可以将所有来自无线客户端的 DHCP 数据包转发至Cisco ISE。您必须在 WLC Web 界面取消选中“启用 DHCP 代理” (Enable DHCP Proxy) 复选框： **控制器 (Controller)** > **高级 (Advanced)** > **DHCP 主控制器模式 (DHCP Master Controller Mode)** > **DHCP 参数 (DHCP Parameters)**。您还必须确保 DHCP IP 帮助程序命令指向Cisco ISE 策略服务节点。

DHCP SPAN 探测功能

当在Cisco ISE 节点中初始化 DHCP 交换端口分析器 (SPAN) 探测功能时，即可监听网络流量，而该网络流量来自特定接口的网络接入设备。您需要对网络接入设备进行配置，从DHCP服务器向Cisco ISE 分析器转发 DHCP SPAN 数据包。分析器接收这些 DHCP SPAN 数据包并对其进行分析以抓取终端的属性，而这些属性可用于分析终端。

例如，

```
switch(config)# monitor session 1 source interface Gi1/0/4 switch(config)# monitor session
1 destination interface Gi1/0/2
```

HTTP 探测功能

在 HTTP 探测中，标识字符串在 HTTP 请求报头字段 User-Agent 中进行传输，该字段是可用于创建 IP 类型的分析条件以及检查 Web 浏览器信息的属性。分析器从 User-Agent 属性以及请求消息中的其他 HTTP 属性捕获 Web 浏览器信息，并将其添加到终端属性列表。

Cisco ISE 同时在端口 80 和端口 8080 上侦听来自 Web 浏览器的通信。Cisco ISE 提供许多默认配置文件，这些配置文件内置到系统中以根据 User-Agent 属性识别终端。

默认情况下，HTTP 探测器处于启用状态。多个 ISE 服务（例如 CWA、热点、BYOD、MDM 和终端安全评估）依赖于客户端 Web 浏览器的 URL 重定向。重定向的流量包括所连接终端的 RADIUS 会话 ID。当 PSN 终止这些 URL 重定向的流时，它对已解密的 HTTPS 数据具有可视性。即使在 PSN 上禁用 HTTP 探测器，节点也会通过 Web 流量来解析浏览器用户代理字符串，并根据其关联的会话 ID 将数据关联到终端。通过此方法收集浏览器字符串时，数据源将列出为访客门户或 CP（客户端调配），而不是 HTTP 探测器。

HTTP SPAN 探测功能

Cisco ISE 部署中的 HTTP 探测功能随交换端口分析器 (SPAN) 探测功能一起启用时，允许分析器从指定的接口捕获 HTTP 数据包。您可以在端口 80 上使用 SPAN 功能，在该端口上Cisco ISE 服务器会侦听来自 Web 浏览器的通信。

HTTP SPAN 收集 HTTP 请求报头消息的 HTTP 属性以及 IP 报头（L3 报头）中的 IP 地址，IP 地址可根据 L2 报头中终端的 MAC 地址与某个终端关联。此信息有助于识别具备 IP 功能的不同的移动和便携式设备（例如 Apple 设备）以及安装不同操作系统的计算机。由于Cisco ISE 服务器在访客登录或下载客户端调配期间会重定向捕获的数据包，因此能够更加可靠地识别具备 IP 功能的不同的移动和便携式设备。这样，分析器就可以从请求消息中收集用户-代理属性和其他 HTTP 属性，然后识别设备，例如 Apple 设备。

无法在 VMware 上运行的思科 ISE 中收集 HTTP 属性

如果您在 ESX 服务器 (VMware) 上部署Cisco ISE，Cisco ISE 分析器会收集动态主机配置协议流量，但由于 vSphere 客户端上的配置问题，它不会收集 HTTP 流量。要在 VMware 设置上收集 HTTP 流量，请将您为Cisco ISE 分析器创建的虚拟交换机的 Promiscuous Mode 从 Reject（默认设置）改为 Accept，配置安全设置。当为 DHCP 和 HTTP 启用交换端口分析器 (SPAN) 探测功能时，Cisco ISE 分析器会同时收集 DHCP 流量和 HTTP 流量。

pxGrid 探测器

pxGrid 探测器利用Cisco pxGrid 从外部源接收终端情景。在早于Cisco ISE 2.4 的版本中，Cisco ISE 仅充当发布程序，并向外部用户共享各种情景信息，例如会话身份和组信息以及配置元素。当在Cisco ISE 2.4 中引入 pxGrid 探测器后，其他解决方案将充当发布程序，Cisco ISE 策略服务节点将成为用户。

pxGrid 探测器基于 pxGrid v2 规范并使用终端资产主题 */topic/com.cisco.endpoint.asset* 和服务名称 *com.cisco.endpoint.asset*。下表显示了主题属性，所有这些属性前面都带有前缀 *asset*。

表 *43:* 终端资产主题

属性名称	类型	说明
assetId	长	资产 ID
assetName	字符串	资产名称
assetIpAddress	字符串	IP 地址
assetMacAddress	字符串	MAC 地址
assetVendor	字符串	Manufacturer
assetProductId	字符串	产品代码
assetSerialNumber	字符串	序列号
assetDeviceType	字符串	设备类型
assetSwRevision	字符串	软件修订号
assetHwRevision	字符串	硬件修订号
assetProtocol	字符串	协议
assetConnectedLinks	阵列	网络链接对象阵列
assetCustomAttributes	阵列	自定义名称-值对数组

除了通常用于跟踪网络资产的属性（例如设备 MAC 地址 (assetMacAddress) 和 IP 地址 (assetIpAddress)）之外，该主题还允许供应商将唯一终端信息发布为自定义属性 (assetCustomAttributes)。在Cisco ISE

中使用终端自定义属性，使主题可扩展到各种使用情形，而无需为通过 pxGrid 共享的每组新的唯一供应商属性更新架构。

RADIUS 探测功能

您可以将Cisco ISE配置为使用 RADIUS 进行身份验证，您可以定义在客户端服务器交易中使用的共享密钥。利用从 RADIUS 服务器接收的 RADIUS 请求和响应消息，分析器可以收集 RADIUS 属性，用于分析终端。

Cisco ISE 可以用作 RADIUS 服务器以及其他 RADIUS 服务器的 RADIUS 代理客户端。充当代理客户端时，它可以使用外部 RADIUS 服务器处理 RADIUS 请求和响应消息。

RADIUS 探测还会收集设备传感器在 RADIUS 记账数据包中发送的属性。有关详细信息，请参阅从 IOS 传感器嵌入式交换机收集属性，第 184 页和支持 IOS 传感器的网络访问设备的配置检查表，第 184 页。

默认情况下，即使对于未配置分析服务的系统，RADIUS 探测也会运行，以确保 ISE 可以跟踪终端身份验证和授权详细信息，以便在情景可视性服务中使用。RADIUS 探测和分析服务还用于跟踪已注册终端的创建和更新时间，以进行清除操作。

表 *44:* 使用 *RADIUS* 探测功能收集的常见属性。

User-Name	Calling-Station-Id	Called-Station-Id	Framed-IP-Address
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
设备类型 (NAD)	位置 (NAD)	身份验证策略 (Authentication Policy)	授权策略

注释 收到记账停止消息时，如果最初使用IP地址进行了分析，则会触发Cisco ISE重新分析相应的终端。因此，如果您为使用IP地址分析的终端配置了自定义配置文件，则满足这些配置文件的总确定性因素的唯一方法是匹配相应的 IP 地址。

网络扫描 (NMAP) 探测功能

通过Cisco ISE，您可以使用 NMAP 安全扫描器检测子网中的设备。您可以在已启用运行分析服务的策略服务节点上启用 NMAP 探测功能。可以在终端分析策略中使用该探测的结果。

每个 NMAP 手动子网扫描都有唯一的数字 ID，用于使用该扫描 ID 更新终端源信息。检测终端时，终端源信息也被更新，表示网络扫描探测功能发现此终端。

NMAP 手动子网扫描对于检测持续连接Cisco ISE 网络的设备（例如，已为其分配静态 IP 地址的打印机）很有帮助，因此，这些设备无法被其他探测器发现。

NMAP 扫描限制

扫描子网会耗费大量资源。扫描子网的过程很漫长，具体取决于子网的规模和密度。活动扫描的数量始终限制为一个扫描，这意味着您一次只能扫描一个子网。在子网扫描期间，您可以随时取消子网扫描。您可以使用**点击 (Click)** 查看最新扫描结果链接，查看存储在以下位置的最近网络扫描结果： **工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描结果 (Manual NMAP Scan Results)**。

手动 NMAP 扫描

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log：

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>
```

表 *45:* 用于手动子网扫描的 *NMAP* 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如，U:161，162
oN	正常输出
oX	XML 输出

NMAP 手动子网扫描的 SNMP 只读社区字符串

只要 NMAP 手动子网扫描发现 UDP 端口 161 在终端上处于打开状态，该扫描就会使用 SNMP 查询进行扩展，导致收集更多属性。在NMAP手动子网扫描过程中，网络扫描探测功能会检测SNMP端口161在设备上是否处于打开状态。如果端口处于打开状态，则系统会使用SNMP版本为2c的默认社区字符串 (public) 触发 SNMP 查询。

如果设备支持SNMP，并且默认只读社区字符串设置为public，则您可以从MIB值“ifPhysAddress”获取设备的 MAC 地址。

此外，还可以在**分析器配置 (Profiler Configuration)** 窗口中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。您也可以为 SNMP 版本为 1 和 2c 的 SNMP MIB walk 指定新的只读社区字符串。有关配置 SNMP 只读社区字符串的信息，请参阅设置 CoA、SNMP RO 社区和终端属性过滤器，第 178 页。

手动 NMAP 扫描结果

最新网络扫描结果存储位置为工作中心 (Work Centers) > 分析器 (Profiler) > 手动扫描 (Manual Scans) > 手动 NMAP 扫描结果 (Manual NMAP Scan Results)。手动 NMAP 扫描结果 (Manual NMAP Scan Results) 页面仅显示检测到的最新终端、其关联终端的配置文件、其 MAC 地址和作为您在任何子网上执行的手动网络扫描结果的静态分配状态。如有必要，您可以通过此页面编辑从终端子网检测的点以实现更好的分类。

Cisco ISE 允许您从已启用运行分析服务的策略服务节点执行手动网络扫描。您必须从您的部署中的主要管理 ISE 节点用户界面选择策略服务节点，才能从策略服务节点运行手动网络扫描。在任何子

网上执行手动网络扫描期间，网络扫描探测功能都会检测指定子网上的终端、其操作系统并检查 UDP 端口 161 和 162 是否在运行 SNMP 服务。

下面提供了与手动 NMAP 扫描结果相关的其他信息：

- 要检测未知终端，NMAP 应能够通过 NMAP 或支持的 SNMP 扫描获知 IP/MAC 绑定。
- ISE 通过 Radius 身份验证或 DHCP 分析了解已知终端的 IP/MAC 绑定。
- IP/MAC 绑定不会跨部署中的 PSN 节点复制。因此，必须从 PSN 触发手动扫描，此 PSN 在其本地数据库中具有 IP/MAC 绑定（例如，上次对其进行 MAC 地址身份验证的 PSN）。
- NMAP 扫描结果不显示与 NMAP 之前手动或自动扫描的终端相关的任何信息。

DNS 探测功能

您的Cisco ISE 部署中的域名服务 (DNS) 探测功能允许分析器查找终端并获取完全限定域名 (FQDN)。在启用Cisco ISE 的网络中检测到终端之后，系统会从 NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP 探测功能收集一系列终端属性。

当您首次在独立环境或分布式环境中部署Cisco ISE 时，系统将提示您运行设置实用程序以配置Cisco ISE 设备。当您运行实用程序设置时，您要配置域名系统 (DNS) 域和主要名称服务器（主要 DNS 服务器），其中您可以配置一个或多个名称服务器。您也可以在部署Cisco ISE 之后，随时使用 CLI 命令更改或添加 DNS 名称服务器。

DNS FQDN 查找

在可执行 DNS 查找前，必须随 DNS 探测功能一起启用以下一个探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。这将允许分析器中的 DNS 探测功能对您在Cisco ISE 部署中定义的指定名称服务器执行 DNS 反向查找（FQDN 查找）。系统会为终端在属性列表中添加新属性，可将此属性用于终端分析策略评估。FQDN 是系统 IP 字典中存在的新属性。您可以创建终端分析条件以验证 FQDN 属性及其用于分析的值。以下是 DNS 查找和收集这些属性的探测功能需要的特定终端属性：

- dhcp-requested-address 属性 - DHCP 和 DHCP SPAN 探测功能收集的属性。
- SourceIP 属性 - HTTP 探测功能收集的属性。
- Framed-IP-Address 属性 - RADIUS 探测功能收集的属性
- cdpCacheAddress 属性 - SNMP 探测功能收集的属性

在 WLC Web 界面中配置呼叫站 ID 类型

可以使用 WLC Web 界面配置呼叫站 ID 类型信息。可以转到 WLC Web 界面的 Security 选项卡，在 RADIUS Authentication Servers 页面配置呼叫站 ID。默认情况下，WLC 用户界面中的 MAC Delimiter 字段设置为 Colon。

关于如何在 WLC Web 界面中进行配置的详细信息，请参阅《Cisco无线 LAN 控制器配置指南》7.2 版第 6 章“配置安全解决方案”。

关于如何使用 config radius callStationIdType 命令在 WLC CLI 中进行配置的详细信息，请参阅《Cisco 无线 LAN 控制器命令参考指南》7.2 版第 2 章“控制器命令”。

步骤 1 登录无线 LAN 控制器用户界面。

步骤 2 点击 **Security**。

步骤 3 展开 **AAA**，然后选择 **RADIUS** > **身份验证 (Authentication)**。

步骤 4 从 Call Station ID Type 下拉列表选择 **System MAC Address**。

步骤 5 从 MAC Delimeter 下拉列表选择 **Colon**。

SNMP 查询探测功能

除在“编辑节点”(Edit Node) 页面中配置 SNMP 查询探测以外，还必须在以下位置配置其他简单管理协议设置：**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

您可以在 Network Devices 列表页面中的新网络接入设备 (NAD) 中配置 SNMP 设置。在 SNMP 查询探测中或在网络接入设备中的 SNMP 设置中指定的轮询间隔按定期间隔查询 NAD。

您可以根据以下配置为特定 NAD 打开和关闭 SNMP 查询：

- 在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 针对Cisco发现协议信息，在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 默认情况下，SNMP 查询计时器针对每个交换机每小时进行一次计时

对于 iDevice 和其他不支持 SNMP 的移动设备，可以通过 ARP 表发现 MAC 地址，而该表可由 SNMP 查询探测功能从网络接入设备进行查询。

使用 SNMP 查询的思科发现协议支持

当在网络设备上配置SNMP设置时，必须确保网络设备的所有端口上均启用Cisco发现协议（默认情况下）。如果在网络设备的任意端口上禁用Cisco发现协议，则可能会因为缺少有关所有已连接终端的Cisco发现协议信息而无法进行正确的分析。可以通过在网络设备上使用 cdp run 命令来全局启用Cisco发现协议，或通过在网络接入设备的任意接口上使用 cdp enable 命令来启用Cisco发现协议。要禁用网络设备或接口上的Cisco发现协议，请在命令开头使用 no 关键字。

使用 SNMP 查询的链路层发现协议支持

Cisco ISE 分析器使用 SNMP 查询收集 LLDP 属性。您也可以使用 RADIUS 探测功能从Cisco IOS 传感器（嵌入网络设备中）收集 LLDP 属性。以下是默认 LLDP 配置设置，您可以使用这些设置在网络访问设备上配置 LLDP 全局配置命令和 LLDP 接口配置命令。

表 *46:* 默认 *LLDP* 配置

属性	设置
LLDP 全局状态	已禁用
LLDP 维持时间（丢弃前）	120 秒
LLDP 计时器（数据包更新频率）	30 秒
LLDP 重新初始化延迟	2 秒
LLDP tlv-select	启用，发送和接收所有 TLV。
LLDP 接口状态	已启用
LLDP 接收	已启用
LLDP 传输	已启用
LLDP med-tlv 选择	启用，发送所有 LLDP-MED TLV

以单个字符显示的 CDP 和 LLDP 功能代码

终端的 Attribute List 显示 lldpCacheCapabilities 和 lldpCapabilitiesMapSupported 属性的单一字符值。这些值是对于运行 CDP 和 LLDP 的网络访问设备显示的功能代码。

示例 1

```
lldpCacheCapabilities S lldpCapabilitiesMapSupported S
```

示例 2

```
lldpCacheCapabilities B;T lldpCapabilitiesMapSupported B;T
```

示例 3

```
Switch#show cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route
 Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M
- Two-port Mac Relay ... Switch# Switch#show lldp neighbors Capability codes: (R) Router,
(B) Bridge, (T) Telephone, (C) DOCSIS Cable Device (W) WLAN Access Point, (P) Repeater, (S)
 Station, (O) Other ... Switch#
```

SNMP 陷阱探测功能

SNMP 陷阱探测功能能够接收来自支持 MAC 通知、LinkUp、LinkDown 和 INFORM 的网络访问设备的信息。SNMP 陷阱探针能够在端口连接或中断以及端点与您的网络断开连接或进行连接时接收来自特定网络访问设备的信息。

要使 SNMP 陷阱探测功能充分运行并创建终端，您必须启用 SNMP 查询，从而在收到陷阱时，使 SNMP 查询探测功能在网络访问设备的特定端口上触发轮询事件。要使此功能充分运行，您应该配置网络访问设备和 SNMP 陷阱。

注释 思科 ISE 不支持从无线 LAN 控制器 (WLC) 和接入点 (AP) 接收的 SNMP 陷阱。

Active Directory 探测

Active Directory (AD) 探测器：

- 提高 WINDOWS 终端操作系统信息的保真度。Microsoft AD 对加入 AD 的计算机操作系统的详细信息进行跟踪，包括版本和服务包级别。AD探测使用AD运行时连接器直接检索此信息，从而提供一个关于客户操作系统信息的高度可靠的来源。
- 帮助区别公司和非公司资产之间的不同之处。AD探测具备的一个基本而重要的属性就是终端是否存在于 AD 中。可使用此信息把 AD 中包含的终端归为受管设备或公司资产类别。

可以在以下位置下启用 AD 探测器 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **分析配置 (Profiling Configuration)**。启用此探测器后，Cisco ISE 在接收到主机名后，将立即获取新终端的 AD 属性。主机名通常是从 DHCP 或 DNS 中获取的。一旦检索成功，直到重新扫描计时器过期，ISE 才会再次尝试对同一个终端进行 AD 查询。这是为了限制 AD 负载，以便于属性查询。重新扫描计时器在**天数之后重新扫描 (Days Before Rescan)** 字段（**管理 [Administration]** > **系统 [System]** > **部署 [Deployment]** > **文件配置 [Profiling Configuration]** > **Active Directory**）中是可配置的。如果终端上有其他配置文件活动，会再次对 AD 进行查询。

可以使用 ACTIVEDIRECTORY 条件，在 **策略 (Policy)** > **策略元素 (Policy Elements)** > **分析 (Profiling)** 匹配以下 AD 探测器属性。使用 AD 探测器收集的 AD 属性在**情景可视性 (Context Visibility)** > **终端 (Endpoints)** 窗口的终端详细信息中通过 "AD" 前缀显示出来。

- AD 主机存在
- AD 连接点
- AD 操作系统
- AD 操作系统版本
- AD 服务包

为每个思科 ISE 节点配置探测功能

您可以在 Profiling Configuration 选项卡上为您的部署中承担策略服务角色的每个Cisco ISE 节点配置一个或多个探测功能，其中节点可能是以下节点：

- 独立节点：如果在默认承担所有管理、监控和策略服务角色的单一节点中部署了Cisco ISE。

- 多个节点：如果在部署中部署了承担策略服务角色的多个节点。

注释 并非全部探测都默认处于启用状态。某些探测器即使未通过复选标记显式启用，也会部分启用。目前，分析配置对于每个 PSN 来说是唯一的。我们建议为部署中的每个 PSN 配置相同的分析器配置设置。

开始之前

您只能从管理节点为每个Cisco ISE 节点配置探测功能，在分布式部署的辅助管理节点上无法执行此配置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选择承担策略服务角色的Cisco ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击**编辑 (Edit)**。

步骤 4 在**常规设置 (General Settings)** 选项卡上，选中**策略服务 (Policy Service)** 复选框。如果取消选中 Policy Service 复选框，会话服务和分析服务复选框均被禁用。

步骤 5 选中 **Enable Profiling Services** 复选框。

步骤 6 点击 **Profiling Configuration** 选项卡。

步骤 7 为每个探测功能配置相应值。

步骤 8 点击**保存 (Save)** 以保存探测功能配置。

设置 CoA、SNMP RO 社区和终端属性过滤器

Cisco ISE 允许全局配置在 Profiler Configuration 页面中发布授权更改 (CoA)，从而增强分析服务对已通过身份验证的终端的控制。

此外，您还可以在 Profiler Configuration 页面中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。SNMP RO 社区字符串使用的顺序与它们在当前自定义 SNMP 社区字符串字段中显示的顺序相同。

您还可以在 Profiler Configuration 页面中配置终端属性筛选。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **分析 (Profiling)**。

步骤 2 选择以下设置之一配置 CoA 类型：

- **No CoA**（默认）- 可以使用此选项禁用 CoA 的全局配置。此设置会根据终端分析策略覆盖任何已配置的 CoA。如果只是为了获得可视性，请保留默认值**无 CoA (No CoA)**。

- **Port Bounce** - 如果交换机端口只存在一个会话，您可以使用此选项。如果端口存在多个会话，则使用 Reauth 选项。如果目标是根据配置文件更改立即更新访问策略，请选择**端口退回 (Port Bounce)** 选项，这将确保重新授权所有无客户端终端，并在需要时刷新 IP 地址。
- **Reauth** - 您可以使用此选项强制重新验证分析时已通过身份验证的终端。如果在重新授权当前会话后预计不会发生 VLAN 或地址更改，请选择**重新验证 (Reauth)** 选项。

  注释　如果一个端口上有多个活动会话，分析服务会通过**重新验证 (Reauth)** 选项发放 CoA，即便您已使用**端口退回 (Port Bounce)** 选项配置了 CoA 也是如此。该功能可避免断开其他会话，而使用**端口退回 (Port Bounce)** 选项就有可能发生这种情况。

步骤 3 在**更改自定义 SNMP 社区字符串 (Change Custom SNMP Community Strings)** 字段中输入新的 SNMP 社区字符串（用逗号分隔）以执行 NMAP 手动网络扫描，然后在**确认自定义 SNMP 社区字符串 (Confirm Custom SNMP Community Strings)** 字段中重新输入字符串进行确认。

默认 SNMP 社区字符串为 *public*。点击**当前自定义 SNMP 社区字符串 (Current Custom SNMP Community Strings)** 部分中的**显示 (Show)** 以验证这一点。

步骤 4 选中 **Endpoint Attribute Filter** 复选框启用终端属性筛选。

启用**终端属性过滤器 (EndPoint Attribute Filter)** 后，Cisco ISE 分析器仅保留重要属性并丢弃所有其他属性。有关详细信息，请参阅过滤器终端属性的全局设置，第 182 页和针对 ISE 数据库持久性和性能的属性过滤器，第 181 页两节。作为最佳实践，我们建议您在生产部署中启用**终端属性过滤器 (EndPoint Attribute Filter)**。

步骤 5 如果您希望Cisco ISE 将终端探测数据发布到需要此数据以对 ISE 上自行激活的终端进行分类的 pxGrid 用户，请选中**启用探测数据发布器 (Enable Probe Data Publisher)** 复选框。在初始部署阶段，pxGrid 用户可以使用批量下载从 Cisco ISE 拉取终端记录。Cisco ISE 会随时将 PAN 中更新的终端记录发送给 pxGrid 用户。默认情况下该选项处于禁用状态。

启用此选项时，请确保在部署中启用 pxGrid 角色。

步骤 6 点击**保存 (Save)**。

对已通过身份验证的终端的授权更改全局配置

您可以使用全局配置功能以通过使用默认的“无 CoA”(No CoA) 选项禁用授权更改 (CoA)，或使用端口退回和重新身份验证选项启用 CoA。如果您在Cisco ISE 中配置了 CoA 的端口回退，则分析服务可能仍会发出“CoA 例外”一节描述的其他 CoA。

所选的全局配置仅在没有更具体的设置的情况下规定默认 CoA 行为。请参阅每个终端分析策略的授权更改配置，第 211 页。

您可以使用 RADIUS 探测或监控角色 REST API 对终端进行身份验证。您可以启用 RADIUS 探测获得更快的性能。如果您已启用 CoA，我们建议您在Cisco ISE 应用中启用 RADIUS 探测时同时启用您的 CoA 配置以获得更快的性能。通过使用已收集的 RADIUS 属性，分析服务可发出终端适当的 CoA。

如果您已在Cisco ISE 应用中禁用 RADIUS 探测，那么您可以通过监控角色 REST API 来发出 CoA。这将允许分析服务支持更多种类的终端。在分布式部署中，您的网络必须至少有一个作为监控角色的Cisco ISE 节点从而通过监控角色 REST API 发出 CoA。

因为主要和次要监控节点都具有相同的会话目录信息，Cisco ISE 会随意指定主要或次要监控节点作为您分布式部署中 REST 查询的默认目标。

发出授权更改的使用案例

分析服务在以下情况下会发出授权更改：

- 删除终端 - 当从 Endpoints 页面删除终端并且从网络上断开或移除该终端时。
- 配置例外操作 - 如果您根据配置文件配置了例外操作，导致该终端出现异常或不可接受的事件。分析服务会通过发出 CoA 将该终端移至相应的静态配置文件。
- 首次分析某个终端 - 当在未静态分配某个终端的情况下首次分析该终端时；例如配置文件从未知配置文件变为已知配置文件。
    - 终端身份组已更改 - 当为授权策略使用的终端身份组添加或删除终端时。

      当某个终端身份组中有任何变更并且在以下情况下将该终端身份组用于授权策略时，分析服务会发出 CoA：

        - 动态分析终端时，终端身份组因这些终端而变更
        - 当某个动态终端的静态分配标志设置为 true 时，终端身份组变更

- 终端身份组策略已变更并且此策略用于授权策略中 - 当终端分析策略变更，并且用于授权策略的逻辑配置文件中包含该策略时。终端分析策略可能因分析策略匹配或终端被静态分配至与逻辑配置文件关联的终端分析策略而改变。在这两种情况下，都只有在将终端分析策略用于授权策略时，分析服务才会发出 CoA。

发出授权更改的豁免

当终端身份组发生更改且静态分配已设置为 true 时，分析服务不会发出 CoA。

出于以下原因，Cisco ISE 不会发出 CoA：

- An Endpoint disconnected from the network - 当发现与网络断开连接的终端时。
- Authenticated wired (Extensible Authentication Protocol) EAP - 当发现支持 EAP 且经过身份验证的有线终端时。
- Multiple active sessions per port - 当一个端口上存在多个活动会话时，分析服务会发出带 Reauth 选项的 CoA，即使您已配置带 Port Bounce 选项的 CoA 亦如此。
- Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected - 如果发现的终端为无线终端，则分析服务会发出 Packet-of-Disconnect (Terminate-Session)，而不是 Port Bounce CoA。此更改的益处是支持无线 LAN 控制器 (WLC) CoA。

- 当**在逻辑配置文件中抑制终端的分析器 CoA (Suppress Profiler CoA for endpoints in Logical Profile)** 选项用于在授权配置文件中配置的逻辑配置文件时，将抑制分析器 CoA。默认情况下，将为所有其他终端触发分析器 CoA。
- Global No CoA Setting overrides Policy CoA - Global No CoA 设置会覆盖终端分析策略中的所有配置设置，因为不管每个终端分析策略是否配置了 CoA，Cisco ISE 中都不会发出 CoA。

注释 “无 CoA”(No CoA) 和“Reauth CoA”(重新授权 CoA) 配置不受影响，并且分析器服务会为有线和无线终端应用相同的 CoA 配置。

对各类型 CoA 配置发出的授权更改

表 *47:* 对各类型 *CoA* 配置发出的授权更改

情景	No CoA 配置	端口重启配置	Reauth 配置	更多信息
Cisco ISE 中的 CoA 全局配置（典型配置）	No CoA	端口重启	重新身份验证	-
终端与您的网络断开连接	No CoA	No CoA	No CoA	授权更改由 RADIUS 属性 Acct-Status -Type 值停止决定。
支持相同交换机端口上的多个活动的会话	No CoA	重新身份验证	重新身份验证	重新身份验证可避免断开其他会话连接。
无线终端	No CoA	Packet-of-Disconnect CoA（终止会话）	重新身份验证	支持无线局域网控制器。
不完整的 CoA 数据	No CoA	No CoA	No CoA	由于缺少 RADIUS 属性。

针对 ISE 数据库持久性和性能的属性过滤器

Cisco ISE 为动态主机配置协议（DHCP 帮助程序和 DHCP SPAN）、HTTP、RADIUS 和简单网络管理协议探测功能（针对性能下降问题的 NetFlow 探测功能除外）实施过滤器。每个探测功能过滤器都包含与终端分析无关的临时属性的列表，并且会从探测功能收集的属性中移除那些属性。

isebootstrap 日志 (isebootstrap-yyyymmdd-xxxxxx.log) 包含处理字典创建和从字典中过滤属性的消息。您还可以配置在终端经过过滤阶段时记录调试消息以指示已经进行过滤。

Cisco ISE 分析器会调用以下终端属性过滤器：

- 用于 DHCP 帮助程序和 DHCP SPAN 的 DHCP 过滤器包含所有不必要并且在解析 DHCP 数据包后被移除的属性。对于终端，过滤之后的属性会与终端缓存中的现有属性合并。
- 系统使用 HTTP 过滤器从 HTTP 数据包过滤属性，过滤之后属性集中不会有重大变更。
- 系统日志解析完成后会立即使用 RADIUS 过滤器，并且终端属性会并入终端缓存中以进行分析。
- 用于 SNMP 查询的 SNMP 过滤器包括单独的 CDP 过滤器和 LLDP 过滤器，这些过滤器都用于 SNMP-Query 探测功能。

过滤器终端属性的全局设置

您可以通过在收集点减少不会频繁变更的终端属性的数量，减少持久性事件和复制事件的数量。启用**终端属性过滤器 (EndPoint Attribute Filter)** 会使Cisco ISE 分析器仅保留重要属性并丢弃所有其他属性。重要属性是指Cisco ISE 系统使用的属性或特别用于终端分析策略或规则的属性。

要启用**终端属性过滤器 (EndPoint Attribute Filter)**，请参阅设置 CoA、SNMP RO 社区和终端属性过滤器，第 178 页部分。

允许列表是自定义终端分析策略中用于分析终端的一系列属性，这些属性至关重要，关系到授权更改 (CoA)、自带设备 (BYOD)、设备注册 WebAuth (DRW) 等在Cisco ISE 中是否正常运行。允许列表始终用作终端所有权变更时（由多个策略服务节点收集属性时）的标准，即使禁用允许列表也不例外。

默认情况下禁用允许列表，并且只有在启用属性过滤器时才会丢弃属性。当终端分析策略变更（包括数据源变更，以在分析策略中包含新属性）时，允许列表会动态更新。在收集属性时，允许列表中不存在的任何属性会被立即丢弃，并且这些属性不用于分析终端。当与缓冲相结合时，可以减少持久性事件的数量。

您必须确保允许列表包含根据以下两个来源确定的一系列属性：

- 用于默认配置文件中的一系列属性，从而使您可以将终端与配置文件进行匹配。
- 对于使授权更改 (CoA)、自带设备 (BYOD)、设备注册 Web 身份验证 (DRW) 等正常运行很重要的一系列属性。

注释 要向允许列表添加新属性，管理员需要创建使用该属性的新分析器条件和策略。该新属性将自动添加到已存储和复制属性的允许列表。

表 *48:* 允许的属性

AAA-Server	BYODRegistration

Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	说明
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	-
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities

lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	-

从 IOS 传感器嵌入式交换机收集属性

IOS 传感器集成允许Cisco ISE 运行时间和Cisco ISE 分析器收集交换机发送的任何或所有属性。您可以利用 RADIUS 协议，直接从交换机收集 DHCP、CDP 和 LLDP 属性。系统会收集 DHCP、CDP 和 LLDP 的属性，进行解析后，会将其映射至以下位置的分析器词典中的属性：**策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)**。

有关设备传感器支持的 Catalyst 平台的信息，请参阅 https://communities.cisco.com/docs/DOC-72932。

IOS 传感器嵌入式网络接入设备

将 IOS 传感器嵌入式网络接入设备与Cisco ISE 集成涉及以下组件：

- IOS 传感器
- 嵌入在网络接入设备（交换机）中的数据收集器，用于收集 DHCP、CDP 和 LLDP 数据
- 用于处理数据并确定终端的设备类型的分析器

  部署分析器有两种方法，但它们不应相互结合使用：

  - 分析器可以部署在Cisco ISE 中
  - 分析器可以作为传感器嵌入在交换机中

支持 IOS 传感器的网络访问设备的配置检查表

本节概述您必须在支持 IOS 传感器的交换机上和Cisco ISE 中配置的一系列任务，以直接从交换机收集 DHCP、CDP 和 LLDP 属性。

- 确保在Cisco ISE 中启用 RADIUS 探测功能。
- 确保网络访问设备支持用于收集 DHCP、CDP 和 LLDP 信息的 IOS 传感器。
- 确保网络访问设备运行以下 CDP 和 LLDP 命令以从终端捕获 CDP 和 LLDP 信息：

  ```
  cdp enable lldp run
  ```

- 确保通过使用标准 AAA 命令和 RADIUS 命令，单独启用会话记帐。

  例如，使用以下命令：

  ```
  aaa new-model aaa accounting dot1x default start-stop group radius radius-server host
  <ip> auth-port <port> acct-port <port> key <shared-secret> radius-server vsa send
  accounting
  ```

- 确保运行 IOS 传感器特定的命令。
  - 启用计帐扩大

    您必须启用网络访问设备以向 RADIUS 记帐消息添加 IOS 传感器协议数据以及在其检测到新传感器协议数据时生成更多记帐事件。这意味着所有 RADIUS 记帐消息都应包含所有 CDP、LLDP 和 DHCP 属性。

    请输入以下全局命令：

    device-sensor accounting

  - 禁用计帐扩大

    对于在特定端口上托管的会话，要禁用（记帐）网络访问设备和向 RADIUS 记帐消息添加 IOS 传感器协议数据（如果已全局启用记帐功能），请在相应端口输入以下命令：

    no device-sensor accounting

  - TLV 更改跟踪

    默认情况下，对于每个支持的对等协议，只有在传入数据包包含之前在特定会话情景中未接收过的类型、长度和值 (TLV) 时，才会生成客户端通知和记帐事件。

    您必须为所有 TLV 更改（即出现新 TLV，或之前接收的 TLV 拥有不同的值的情况）启用客户端通知和记帐事件。请输入以下命令：

    device-sensor notify all-changes

- 请务必在网络访问设备中禁用 IOS 设备分类器（本地分析器）。

  请输入以下命令：

```
no macro auto monitor
```

注释 此命令可阻止网络访问设备对一项更改发送两个相同的RADIUS记帐消息。

ISE 分析器对思科 IND 控制器的支持

Cisco ISE 可以分析和显示连接到Cisco工业网络设备 (IND) 的设备的状态。PxGrid 连接Cisco ISE 和 Cisco Industrial Network Director 以传送终端（物联网）数据。Cisco ISE 上的 pxGrid 使用Cisco IND 事件，并查询Cisco IND 以更新终端类型。

Cisco ISE 分析器具有物联网设备的词典属性。选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)**，然后从系统词典列表中选择 *IOTASSET* 以查看词典属性。

准则和建议

如果您为分析配置了多个 ISE 节点，我们建议您仅在一个节点上为 Cisco IND 启用 pxGrid。

多个Cisco IND 设备可以连接到单个 ISE。

如果从两个或更多发布者（Cisco IND）收到同一终端信息，则Cisco ISE仅为该终端保留最后一个发布者的数据。

Cisco ISE 从 pxGrid 中的 *com.cisco.endpoint.asset* 和 */topic/com.cisco.endpoint.asset* 服务获取Cisco IND 数据。

思科 IND 分析流程

Cisco IND 资产发现功能查找物联网设备，并将该设备的终端数据发布到 pxGrid。Cisco ISE 看到 pxGrid 上的事件，获取终端数据。Cisco ISE 中的分析器策略将设备数据分配给 ISE 分析器词典中的属性，并将这些属性应用于Cisco ISE 中的终端。

不符合Cisco ISE 中的现有属性的物联网终端数据不会保存。但是，您可以在Cisco ISE 中创建更多属性，并向Cisco IND 注册这些属性。

通过 pxGrid 首次建立与Cisco IND 的连接时，Cisco ISE 会批量下载终端。如果发生网络故障，Cisco ISE 会再次批量下载累积的终端更改。

配置思科 ISE 和思科 IND 进行 IND 分析

注释 您必须在思科 IND 中安装思科 ISE 证书，并在 ISE 中安装思科 IND 证书，然后才能在思科 IND 中激活 pxGrid。

1. 选择 **管理 (Administration)** > **部署 (Deployment)**。编辑您计划用作 pxGrid 使用者的 PSN，并启用 pxGrid。此 PSN 根据Cisco IND 和分析发布的 pxGrid 数据创建终端。
2. 选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** 验证 pxGrid 是否正在运行。然后点击**证书 (Certificates)** 选项卡，并填写证书字段。点击**创建 (Create)** 颁发证书并下载证书。
   - 对于**我想要 (I want to)**，请选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))**，**通用名称 (Common Name)**，并输入要连接的Cisco IND 的名称。
   - 对于**证书下载格式 (Certificate Download Format)**，选择 **PKS12 格式**。
   - 对于**证书密码 (Certificate Password)**，请创建密码。

   注释 必须启用 ISE 内部 CA。如果您的浏览器阻止弹出窗口，您将无法下载证书。解压缩证书，以使 PEM 文件可用于下一步。
3. 在Cisco IND 中，选择 **设置 (Settings)** > **pxGrid**，然后点击**下载 .pem IND 证书 (Download .pem IND certificate)**。保持打开此窗口。
4. 在Cisco ISE 中，选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **所有客户端 (All Clients)**。当您看到Cisco IND pxGrid 客户端时，请批准该客户端。

5. 在Cisco IND 中，移动滑块以启用 pxGrid。系统将打开另一个屏幕，您可以在其中定义 ISE 节点的位置、您在 ISE 中为此 pxGrid 服务器输入的证书的名称以及您提供的密码。点击**上传证书 (Upload Certificate)**，并找到 ISE pxGrid PEM 文件。
6. 在 ISE 中，选择 **管理 (Administration)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。点击**导入 (Import)**，输入从Cisco IND 获取的证书的路径。
7. 在Cisco IND 中，点击**激活 (Activate)**。
8. 在Cisco ISE 中，依次选择**管理 (Adminstration) > 部署 (Deployment)**。选择要用于Cisco IND 连接的 PSN，选择“分析”(Profiling) 窗口，并启用 pxGrid 探测。
9. ISE 与Cisco IND 之间的 pxGrid 连接现在处于活动状态。通过显示Cisco IND 已找到的物联网终端来验证这一点。

添加属性以执行 IND 分析

Cisco IND 可能会返回不在 ISE 词典中的属性。您可以向Cisco ISE 添加更多属性，以便更准确地分析该物联网设备。要添加新属性，请在Cisco ISE 中创建自定义属性，然后通过 pxGrid 将该属性发送到Cisco IND。

1. 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)**，然后选择**终端自定义属性 (Endpoint Custom Attributes)**。创建属性终端属性。
2. 现在，您可以在分析器策略中使用此属性来标识具有新属性的资产。选择 **策略 (Policy)** > **分析 (Profiling)**，并创建新的分析器策略。在**规则 (Rules)** 部分中，创建新规则。添加**属性/值**时，请选择 **CUSTOMATTRIBUTE** 文件夹以及您创建的自定义属性。

ISE 支持 MUD

制造商使用描述符 (MUD) 是一种 IETF 标准，定义了自行激活物联网设备的方式。它提供物联网设备的无缝可视性和分段自动化。MUD 已在 IETF 流程中获得批准，并发布为 RFC8520。有关详细信息，请参阅 https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/。

Cisco ISE 版本 2.6 及更高版本支持识别物联网设备。Cisco ISE 会自动创建分析策略和终端身份组。MUD 支持分析物联网设备，动态创建分析策略，以及自动执行创建策略和终端身份组的整个过程。管理员可以使用这些分析策略手动创建授权策略和配置文件。在 DHCP 和 LLDP 数据包中发送 MUD URL 的物联网设备使用这些配置文件和策略自行激活。

Cisco ISE 对物联网设备执行未签名分类。Cisco ISE 不存储 MUD 属性；属性仅在当前会话中使用。在**情景和可视性 (Context and Visibility)** > **终端 (Endpoints)** 窗口中，可以按**终端配置文件 (Endpoint Profile)** 字段过滤物联网设备。

以下设备支持将 MUD 数据发送到Cisco ISE：

- 运行 Cisco IOS XE 版本 16.9.1 和 16.9.2 的Cisco Catalyst 3850 系列交换机
- 运行 Cisco IOS 版本 15.2(6)E2 的Cisco Catalyst 全数字化楼宇系列交换机

- 运行 Cisco IOS 版本 15.2(6)E2 的Cisco工业以太网 4000 系列交换机
- 具有嵌入式 MUD 功能的物联网 (IoT) 设备

Cisco ISE 支持以下分析协议和分析探测器：

- LLDP 和 Radius - TLV 127
- DHCP - 选项 161

两个字段均可通过 IOS 设备传感器发送到Cisco ISE。

为 MUD 配置 ISE

1. 选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **分析器设置 (Profiler Settings)**，选中**为 MUD 启用分析 (Enable profiling for MUD)** 复选框。
2. 添加可向 ISE 发送 MUD URI 的网络访问设备。要添加网络设备，请选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。
3. 验证 MUD-URL 连接是否正常。
    1. 选择 **情景可视性 (Context Visibility)** > **端点 (Endpoints)**，查找 ISE 成功分类的物联网终端。您可以按终端配置文件名称（以 **IOT-MUD** 开头）过滤物联网设备。
    2. 点击一个物联网设备的终端 MAC 地址，然后选择属性标签。验证属性列表中是否有一个 mud-url。
    3. 选择 **策略 (Policy)** > **分析 (Profiling)** 并在**系统类型 (System Type)** 中选择**物联网创建 (IOT Created)** 以过滤列表。
4. （可选）为新的物联网设备配置调试日志记录。
    1. 选择 **系统 (System)** > **日志记录 (Logging)** > **调试日志配置 (Debug Log Configuration)**，然后选择具有 MUD 配置的 ISE 节点。
    2. 在左侧菜单中选择**调试日志配置 (Debug Log Configuration)**，然后选择**分析器 (profiler)**。

随着分类的物联网设备的增加，MUD-URL 相同的同类别或同组的所有设备都分配到同一终端组。例如，Molex 灯已连接并分类，系统会为该 Molex 灯创建分析器组。随着分类的同类型（有相同的 MUD-URL）的 Molex 灯越来越多，它们会继承相同的分类或终端身份组。

验证 ISE 和交换机中的 MUD 流量

1. 在打开物联网设备之前，请**连接端口**或**取消关闭**接口。
    1. 开始在 ISE 上进行数据包捕获。
    2. 开始在交换端口上进行数据包捕获。
2. 查看交换机上的以下输出。

1. **show device-sensor cache all**
2. **show access-session**
3. **show radius statistics**

3. 打开物联网设备。
4. 每分钟重复以下步骤。
   1. **show device-sensor cache all**
   2. **show access-session**
   3. **show radius statistics**
5. 等待 3 到 5 分钟，以便 ISE 上显示所有设备。
6. 停止 ISE 和交换机的数据包捕获。
7. 每分钟重复以下步骤。
   1. **show device-sensor cache all**
   2. **show access-session**
   3. **show radius statistics**

分析器条件

分析条件是策略元素，而且与其他条件相似。但是不同于身份验证、授权和访客条件，分析条件可以基于有限数量的属性。Profiler Conditions 页面列出Cisco ISE 中可用的属性及其说明。

分析器条件可以是以下任一条件：

- Cisco Provided - Cisco ISE 包含部署时预定义的分析条件，在 Profiler Conditions 页面中标识为 Cisco Provided。您不能删除 Cisco Provided 分析条件。

  您还可以在以下位置在系统分析字典中找到 Cisco Provided 条件：Policy > Policy Elements > Dictionaries > System。

  例如，MAC 字典。对于某些产品，OUI（组织唯一标识符）是您可以首先用于标识设备的生产组织的唯一属性。它是设备 MAC 地址的组成部分。MAC 字典包含 MACAddress 和 OUI 属性。

- Administrator Created - 您以Cisco ISE 管理员的身份创建的分析器条件或复制的预定义分析条件标识为 Administrator Created 条件。您可以使用 Profiler Conditions 页面中的分析字典，创建 DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP 和 NMAP 类型的分析器条件。

虽然建议的分析策略数上限为 1000，但是您可以扩展到多达 2000 个分析策略。

分析网络扫描操作

终端扫描操作是终端分析策略中可以引用的一种可配置操作，当满足与网络扫描操作关联的条件时，就会触发该操作。

终端扫描用于扫描终端，从而限制Cisco ISE 系统中的资源使用。网络扫描操作扫描的是单个终端，而不像涉及整体资源的网络扫描。它可以提高终端的整体分类，并且可以为终端重新定义终端配置文件。一次仅能处理一个终端扫描。

您可以将单个网络扫描操作与终端分析策略关联。Cisco ISE 为网络扫描操作预定义三个扫描类型，一个扫描操作可以包含一个扫描类型，也可以包含全部三个扫描类型：例如 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描。您不能编辑或删除 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描，这些扫描是Cisco ISE 中预定义的网络扫描操作。您还可以创建自己的新网络扫描操作。

正确分析某个终端之后，就无法对该终端使用所配置的网络扫描操作。例如，您可以通过扫描 Apple-Device 将所扫描的终端归类为 Apple 设备。OS 扫描确定了终端运行的操作系统之后，终端就不再与 Apple-Device 配置文件匹配，而是与 Apple 设备的相应配置文件匹配。

创建新的网络扫描操作

与终端分析策略关联的网络扫描操作会扫描终端的操作系统、简单网络管理协议 (SNMP) 端口和通用端口。Cisco为最常见的NMAP扫描提供网络扫描操作，但是您也可以创建自己的网络扫描操作。

当您创建新的网络扫描时，可定义 NMAP 检测要扫描的信息类型。

开始之前

必须首先启用网络扫描 (NMAP) 检测，才能定义规则触发网络扫描操作。关于启用网络扫描检测的操作程序，请参阅为每个思科 ISE 节点配置探测功能。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。或者，您可以选择**工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **NMAP 扫描操作 (NMAP Scan Actions)** 。

步骤 2 点击**添加 (Add)**。

步骤 3 输入要创建的网络扫描操作的名称和说明。

步骤 4 当您要对终端扫描以下各项时，请选中一个或多个复选框：

- “扫描操作系统”(Scan OS) - 扫描操作系统
- Scan SNMP Port - 扫描 SNMP 端口（161、162）
- Scan Common Port - 扫描通用端口。
- “扫描自定义端口”(Scan Custom Ports) - 扫描自定义端口。

- “扫描包括业务版本信息”(Scan Include Service Version Information) - 扫描业务版本信息，可能包含设备的详细说明。
- “运行 SMB 发现脚本”(Run SMB Discovery Script) - 扫描 SMB 端口(端口号为：445 和 139）以检索操作系统和计算机名称等信息。
- “跳过 NMAP 主机发现”(Skip NMAP Host Discovery) - 跳过 NMAP 扫描的初始主机发现阶段。

  注释　对于自动 NMAP 扫描，默认选择“跳过 NMAP 主机发现”(Skip NMAP Host Discovery) 选项，但是，必须选择该选项才能运行手动 NAMP 扫描。

步骤 5　点击**提交 (Submit)**。

NMAP 操作系统扫描

操作系统扫描（OS 扫描）类型用于扫描终端运行的操作系统（OS 版本）。这种扫描会占用大量资源。

NMAP 工具对可能导致不可靠的结果的 OS 扫描有限制。例如，当扫描交换机和路由器等网络设备的操作系统时，NMAP 操作系统扫描针对这些设备提供的操作系统数据不正确。即使准确度不是 100%，Cisco ISE 也会显示操作系统属性。

您应将在规则中使用 NMAP 操作系统属性的终端分析策略配置为具有较低的可信度值条件（可信度值）。我们建议，每当您基于 NMAP:operating-system 属性创建终端分析策略时，都应包含 AND 条件以帮助从 NMAP 中过滤掉错误结果。

以下 NMAP 命令用于在您将操作系统扫描与终端分析策略关联时扫描操作系统：

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log：

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>
```

表 *49:* 用于手动子网扫描的 *NMAP* 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如，U:161，162
oN	正常输出
oX	XML 输出

操作系统端口

下表列出 NMAP 用于 OS 扫描的 TCP 端口。此外 NMAP 使用 ICMP 和 UDP 端口 51824。

1	3	4	6	7	9	13	17	19

20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407 个	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720

1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972 年	1974	1984	1998-2010	2013	2020 年	2021
2022	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959

5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774

32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP 端口扫描

SNMPPortsAndOS 扫描类型扫描终端运行的操作系统（和操作系统版本）并在打开 SNMP 端口（161 和 162）时触发 SNMP 查询。其可用于一开始识别为与 Unknown 配置文件匹配的终端，以更好地进行分类。

以下 NMAP 命令用于在将 Scan SNMP 端口与终端分析策略关联时扫描 SNMP 端口（UDP 161 和 162）：

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 *50:* 用于终端 *SNMP* 端口扫描的 *NMAP* 命令

-sU	UDP 扫描。
-p <端口范围>	仅扫描指定端口。例如，扫描 UDP 端口 161 和 162。
oN	正常输出。
oX	XML 输出。
IP-address	所扫描终端的 IP 地址。

NMAP 通用端口扫描

CommonPortsAndOS-scan type 扫描终端所运行的操作系统（和操作系统版本）以及通用端口（TCP 和 UDP），但不扫描 SNMP 端口。当您将 Scan Common Port 与终端分析策略关联时，以下 NMAP 命令会扫描通用端口：nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP 地址>

表 *51:* 用于终端通用端口扫描的 *NMAP* 命令

-sTU	TCP 连接扫描和 UDP 扫描。
-p <端口范围>	扫描 TCP 端口：21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080 和 UDP 端口：53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900
oN	正常输出。
oX	XML 输出。
IP 地址	所扫描终端的 IP 地址。

通用端口

下表列出 NMAP 用于扫描的端口。

表 *52:* 通用端口

TCP 端口		**UDP** 端口	
端口	服务	端口	服务
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP 自定义端口扫描

除了通用端口，还可以使用自定义端口（**工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **NMAP 扫描操作 (NMAP Scan Actions)** 或 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan [NMAP]**

Actions)）以指定自动和手动 NMAP 扫描操作。NMAP 探测通过开放的特定自定义端口收集来自终端的属性。这些属性在“ISE 身份”(ISE Identities) 页面中的终端属性列表中进行更新（**工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**）。您最多可以为每项扫描操作指定 10 个 UDP 端口和 10 个 TCP 端口。您无法使用您已指定为常见端口的相同端口号。有关详细信息，请参阅 使用 McAfee ePolicy Orchestrator 配置分析器策略。

NMAP 包括服务版本信息扫描

“包括服务版本信息 NMAP”探测通过收集与在设备上运行的软件相关的信息自动扫描终端，以便更好地对它们进行分类。服务版本选项可与通用端口或自定义端口结合使用。

示例：

CLI 命令：nmap -sV -p T:8083 172.21.75.217

输出：

端口	省/自治区	服务	版本
8083/tcp	open	http	McAfee ePolicy Orchestrator 代理 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {15D79A24-3BAB-A0FA-E76C-2F})

NMAP SMB 发现扫描

NMAP SMB 发现扫描有助于区分 Windows 版本并实现更佳终端分析。您可以配置 NMAP 扫描操作来运行 NMAP 提供的 SMB 发现脚本。

NMAP 扫描操作包含在 Windows 默认策略中，而且当终端与策略和扫描规则匹配时，对终端进行扫描，其结果有助于确定确切的 Windows 版本。策略将在源服务上进行配置，新的预定义 NMAP 扫描通过 SMB 发现选项进行创建。

NMAP 扫描操作通过 Microsoft-Workstation 策略调用，而且扫描结果保存在该操作系统属性下的终端中并应用于 Windows 策略。您还可以通过手动扫描子网找到 SMB 发现脚本选项。

注释 对于 SMB 发现，请务必在终端启用 Windows 文件共享选项。

SMB 发现属性 (SMB Discovery Attributes)

当在终端上执行 SMB 发现脚本时，新的 SMB 发现属性（例如 SMB.Operating-system）被添加到终端。当在源服务上更新 Windows 终端分析策略时会考虑这些属性。当运行 SMB 发现脚本时，SMB 发现属性增加了 SMB 前缀，例如 SMB.operating-system、SMB.lanmanager、SMB.server、SMB.fqdn、SMB.domain、SMB.workgroup 和 SMB.cpe。

跳过 NMAP 主机发现

浏览每个 IP 地址的每各端口是一个耗时的过程。根据扫描的目的，您可以跳过活动终端的 NMAP 主机发现。

如果在终端分类后触发 NMAP 扫描，分析器会始终跳过终端的主机发现。但是，如果在启用“跳过 NMAP 主机发现扫描”(Skip NMAP Host Discovery Scan) 之后手动扫描操作被触发，则跳过主机发现。

NMAP 扫描工作流程

执行 NMAP 扫描应遵循以下步骤：

开始之前

要运行 NMAP SMB 发现脚本，必须在系统中启用文件共享。关于示例，请参阅启用文件共享以运行 NMAP SMB 发现脚本主题。

步骤 1 创建 SMB 扫描操作。

步骤 2 使用 SMB 扫描操作配置分析器策略。

步骤 3 使用 SMB 属性添加新条件。

创建 SMB 扫描操作

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。

步骤 2 输入**操作名称**和**描述** 。

步骤 3 选中**运行 SMB 发现脚本 (Run SMB Discovery Script)** 复选框。

步骤 4 点击**添加 (Add)**，创建网络访问用户。

下一步做什么

应使用 SMB 扫描操作配置分析器策略。

使用 SMB 扫描操作配置分析器策略

开始之前

您必须创建一个新的分析器策略以通过 SMB 扫描操作对终端进行扫描。例如，您可以通过指定一条规则来扫描 Microsoft 工作站，该条规则规定如果 DHCP 类标识符包含 MSFT 属性，则应采取网络操作。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称** 和**描述**。

步骤 3 在下拉列表中，选择您已创建的扫描操作（例如，SMBScanAction）。

下一步做什么

您应该使用 SMB 属性添加新的条件。

使用 SMB 属性添加新条件

开始之前

您应创建新的分析器策略扫描终端版本。例如，您可以在 Microsoft Workstation 父策略下扫描 Windows 7。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称** （例如 Windows 7Workstation）和**说明**。

步骤 3 在**网络扫描 (NMAP) 操作 (Network Scan (NMAP) Action)** 下拉列表中，选择**无 (None)**。

步骤 4 在**父组策略 (Parent Policy)** 下拉列表中选择 Microsoft-Workstation 策略。

启用文件共享以运行 NMAP SMB 发现脚本

以下是在 Windows OS 版本 7 中启用文件共享运行 NMAP SMB 发现脚本的示例。

步骤 1 选择**控制面板 (Control Panel)** > **网络和 Internet (Network and Internet)**。

步骤 2 点击**网络和共享中心**。

步骤 3 点击**更改高级共享设置 (Change Advanced Sharing Settings)**。

步骤 4 点击**打开文件和打印机共享 (Turn on File and Printer Sharing)**。

步骤 5 启用以下选项：**为使用 40 或 56 位加密的设备启用文件共享 (Enable File Sharing for Devices That Use 40- or 56-bit Encryption)** 和**打开密码保护共享 (Turn on Password Protected Sharing)**。

步骤 6 点击**保存更改 (Save Changes)**。

步骤 7 配置防火墙设置。

a) 在控制面板中，导航至 **系统和安全 (System and Security)** > **Windows 防火墙 (Windows Firewall)** > **允许程序通过 Windows 防火墙 (Allow a Program Through Windows Firewall)**。

b) 选中**文件和打印机共享 (File and Printer Sharing)** 复选框。

c) 点击**确定 (OK)**。

步骤 8 配置共享文件夹。

a) 右键点击目标文件夹，并选择**属性 (Properties)**。
b) 点击**共享 (Sharing)** 选项卡，然后点击**共享 (Share)**。
c) 在**文件共享 (File Sharing)** 对话框中，添加所需名称并点击**共享 (Share)**。
d) 在选定文件夹共享后，点击**完成 (Done)**。
e) 点击**高级共享 (Advanced Sharing)**，并选择**共享此文件夹 (Share This Folder)** 复选框。
f) 点击 **Permissions**（权限）。
g) 在**扫描权限 (Permissions for Scans)** 对话框中，选择**所有人 (Everyone)**，并选中**完全控制 (Full Control)** 复选框。
h) 点击**确定 (OK)**。

从 NMAP 扫描中排除子网

您可以执行 NMAP 扫描以识别终端的操作系统或 SNMP 端口。

当执行 NMAP 扫描时，您可以排除不应由 NMAP 扫描的完整子网或 IP 范围。您可以在 **NMAP 扫描子网排除项 (NMAP Scan Subnet Exclusions)** 窗口中配置子网或 IP 范围（**工作中心 (Work Centers) > 分析器 (Profiler) > 设置 (Settings) > NMAP 扫描子网排除 (Settings)**）。这有助于限制网络上的负载并节省大量时间。

要进行手动 NMAP 扫描，您可以使用**运行手动 NMAP 扫描 (Run Manual NMAP Scan)** 窗口（**工作中心 (Work Centers) > 分析器 (Profiler) > 手动扫描 (Manual Scans) > 手动 NMAP 扫描 (Manual NMAP Scan) > 在以下范围配置 NMAP 扫描子网排除项 (Configure NMAP Scan Subnet Exclusions At)**）来指定子网或 IP 范围。

手动 NMAP 扫描设置

您可以使用自动 NMAP 扫描的可用选项，执行手动 NMAP 扫描（**工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描 (Manual NMAP Scan)**）。您可以选择扫描选项或预定义选项。

表 *53:* 手动 *NMAP* 扫描设置

字段名称	使用指南
节点	选择 NMAP 扫描可运行的 ISE 节点。
手动扫描子网 (Manual Scan Subnet)	输入您要运行 NMAP 扫描的终端的子网 IP 地址范围。
在...配置 NMAP 扫描子网例外情况 (Configure NMAP Scan Subnet Exclusions At)	您将定向到 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **设置 (Settings)** > **NMAP 扫描子网排除项 (NMAP Scan Subnet Exclusions)** 窗口。指定应排除的 IP 地址和子网掩码。如果匹配，则 NMAP 扫描不运行。

字段名称	使用指南
NMAP 扫描子网	• 指定扫描选项 • 或者选择现有的 NMAP 扫描
指定扫描选项	选择所需的扫描选项：OS、SNMP 端口 (SNMP Port)、通用端口 (Common Ports)、自定义端口 (Custom Ports)、包括服务版本信息 (Include Service Version Information)、运行 SMB 发现脚本 (Run SMB Discovery Script)、跳过 NMAP 主机发现 (Skip NMAP Host Discovery)。有关详细信息，请参阅创建新的网络扫描操作。
选择现有的 NMAP 扫描 (Select an Existing NMAP Scan)	显示会显示默认分析器 NMAP 扫描操作的**现有 NMAP 扫描操作 (Existing NMAP Scan Actions)** 下拉列表。
重置为默认扫描选项	点击此选项可恢复默认设置（选中所有扫描选项）。
保存 NMAP 扫描操作 (Save as NMAP Scan Action)	输入操作名称和说明。

运行手动 NMAP 扫描

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描 (Manual NMAP Scan)**。

步骤 2 在**节点 (Node)** 下拉列表中，选择要运行 NMAP 扫描的 ISE 节点。

步骤 3 在**手动扫描子网 (Manual Scan Subnet)** 文本框中输入要检查开放端口终端的子网地址。

步骤 4 选择以下一个选项：

a) 选择**指定扫描选项 (Specify Scan Options)**，并且在页面右侧选择必填扫描选项。有关详细信息，请参阅创建新的网络扫描操作 页面。

b) 选择**选择现有 NMAP 扫描操作 (Select An Existing NMAP Scan Action)**，以选择默认 NMAP 扫描操作，如 MCAFeeEPOOrchestratorClientScan。

步骤 5 点击**运行扫描 (Run Scan)**。

使用 McAfee ePolicy Orchestrator 配置分析器策略

Cisco ISE 分析服务可以检测终端上是否存在 McAfee ePolicy Orchestrator (McAfee ePO) 客户端。这有助于确定给定终端是否属于您的组织。

在该流程中涉及的实体如下：

- ISE 服务器
- McAfee ePO 服务器
- McAfee ePO 代理

Cisco ISE 能够提供内置的 NMAP 扫描操作 (MCAFeeEPOOrchestratorClientscan) 以便于在配置的端口上使用 NMAP McAfee 脚本来检查 McAfee 代理是否在终端上运行。您还可以使用自定义端口（例如，8082）创建新的 NMAP 扫描选项。您可以按照以下步骤使用 McAfee ePO 软件配置新的 NMAP 扫描操作：

步骤 1 配置 McAfee ePo NMAP 扫描操作。

步骤 2 配置 McAfee ePO 代理。

步骤 3 使用 McAfee ePO NMAP 扫描操作配置分析器策略。

配置 McAfee ePo NMAP 扫描操作

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入**操作名称 (Action Name)** 和**说明**。

步骤 4 在**扫描选项 (Scan Options)**中，选择**自定义端口 (Custom Ports)**。

步骤 5 在**自定义端口 (Custom Ports)** 对话框中，添加所需的 TCP 端口。默认情况下，8080 TCP 端口为 McAfee ePO 启用。

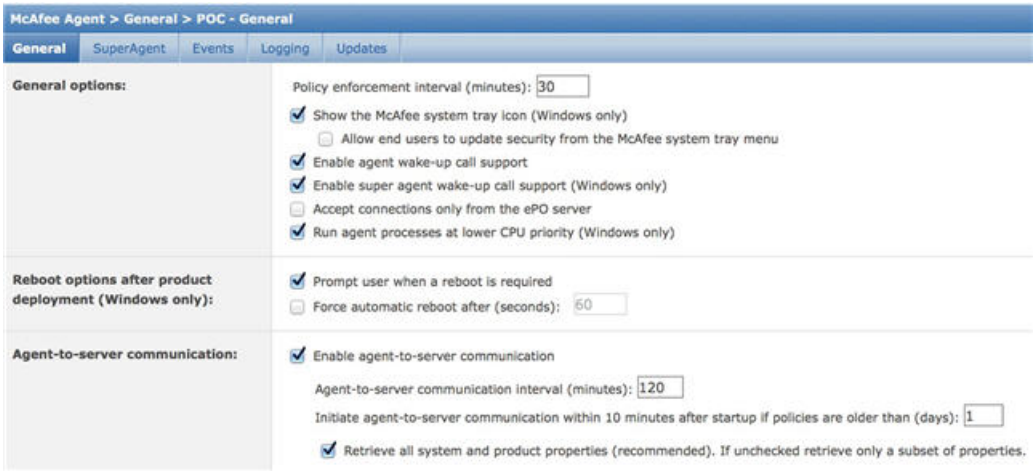
步骤 6 选中**包括服务版本信息 (Include Service Version Information)** 复选框。

步骤 7 点击**提交 (Submit)**。

配置 McAfee ePO 代理

步骤 1 在您的 McAfee ePO 服务器上，选中推荐设置促进 McAfee ePO 代理和 ISE 服务器之间的通信。

图 *16: McAfee ePO* 代理的推荐选项



步骤 2 验证**仅接受来自 ePO 服务器的连接 (Accept Connections Only From The ePO Server)** 已取消选中。

使用 McAfee ePO NMAP 扫描操作配置分析器策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称**和**描述**。

步骤 3 在**网络扫描 (NMAP) 操作 (Network Scan (NMAP) Action)** 下拉列表，请选择所需的操作（例如，MCAFeeEPOOrchestratorClientscan）。

步骤 4 创建父分析器策略（例如，Microsoft 工作站）以包含一条规则用于检查 DHCP 类标识符是否包含 MSFT 属性。

步骤 5 在父 NMAP McAfee ePO 策略（例如，Microsoft 工作站）中创建新策略（例如，CorporateDevice）以检查 McAfee ePO 座席是否在终端上安装。

满足条件的终端作为企业设备进行分析。您可以使用策略将通过 McAfee ePO 代理进行分析的终端移动至新的 VLAN。

分析器终端自定义属性

选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)**，将属性分配给终端，终端通过检测收集的属性除外。终端自定义属性可用于授权策略，以分析终端。

最多可以创建 100 个终端自定义属性。支持的终端自定义属性类型有：Int、String、Long、Boolean 和 Float。

您可以在以下位置添加终端自定义属性的值：**情景目录 (Context Directory)** > **终端 (Endpoints)** > **终端分类 (Endpoint Classification)** 窗口。

终端自定义属性的使用案例包括，基于某些属性允许或阻止设备，或基于授权分配某些权限。

在授权策略中使用终端自定义属性

终端自定义属性部分允许您配置其他属性。每个定义包括属性和类型（String、Int、Boolean、Float、Long)。可以使用终端自定义属性分析设备。

注释　您必须具有思科 ISE Advantage 许可证才能向终端添加自定义属性。

以下步骤演示如何使用终端自定义属性创建授权策略。

步骤 1 创建终端自定义属性并分配值。

a) 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 页面。

b) 在**终端客户属性 (Endpoint Custom Attributes)** 区域，输入**属性名称 (Attribute Name)**（例如 deviceType）、数据类型（例如 String）和参数。

c) 点击**保存 (Save)**。

d) 选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **摘要 (Summary)**。

e) 分配自定义属性值。

- 选中所需的 MAC 地址复选框，然后点击**编辑 (Edit)**。
- 或者，点击所需的 MAC 地址，然后在“终端”(Endpoints) 页面上，点击**编辑 (Edit)**。

f) 在**编辑终端 (Edit Endpoint)** 对话框，在**自定义属性 (Custom Attributes)** 区域中输入所需的属性值（例如 deviceType = Apple iPhone ）。

g) 点击**保存 (Save)**。

步骤 2 使用自定义属性和值创建授权策略。

a) 选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

b) 通过从终端词典选择自定义属性创建授权策略（例如规则名称：企业设备，条件：终端：deviceType 包含 Apple-iPhone，权限：则 PermitAccess）。

c) 点击**保存 (Save)**。

相关主题

分析器终端自定义属性 ，第 203 页

创建分析器条件

Cisco ISE 中的终端分析策略允许您对网络上已发现的终端进行分类，并将它们分配到特定的终端身份组。这些终端分析策略由分析条件构成，Cisco ISE 评估这些条件对终端进行分类和分组。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入终端分析策略设置，第 205 页中所描述的字段的值。

步骤 3 点击**提交 (Submit)** 保存分析器条件。

步骤 4 重复此过程创建更多条件。

终端分析策略规则

您可以定义一条规则来允许您从库中选择您之前创建并保存在策略元素库中的一个或多个分析条件，并且允许关联针对每个条件的可信度的整数值，或者为该条件关联例外操作或网络扫描操作。例外操作或网络扫描操作用于触发可配置的操作，而Cisco ISE 则就终端整体分类对分析策略进行评估。

使用 OR 运算符单独评估特定策略中的规则时，每个规则的可信度都会影响终端配置文件与特定终端类别的整体匹配。如果终端分析策略的规则匹配，在您的网络上动态发现分析策略和匹配的策略时，对于该终端分析策略和匹配的策略相同。

规则中的逻辑分组条件

终端分析策略（配置文件）包含单已条件或使用 AND 或 OR 运算符从逻辑上组合的多个单一条件，您可以根据这些条件为策略中的具体规则对终端进行检查、分类和分组。

条件用于按照终端条件中指定的值检查所收集的终端属性值。如果映射不止一个属性，您可以按逻辑给条件分组，这样可以帮助您给您的网络上的终端分类。您可以根据一个或多个条件检查终端，在规则中为其关联相应的可信度指标（即您所定义的整数值），也可以触发与条件关联的例外操作或与条件关联的网络扫描操作。

可信度

分析策略中的最低可信度用于评估终端的匹配配置文件。终端分析策略中每条规则都有一个与分析条件关联的最低可信度指标（一个整数）。可信度指标是为终端分析策略中所有有效规规则增加的一个衡量标准，用于衡量终端分析策略中各个条件对于提高终端整体分类的影响。

各条规则的可信度都会影响终端配置文件与具体终端类别的整体匹配度。所有有效规则的可信度相加形成匹配可信度。它必须超过终端分析策略中定义的最低可信度。默认情况下，所有新分析策略规则和预定义分析策略的最低可信度为 10。

终端分析策略设置

下表列出了**终端策略 (Endpoint Policies)** 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

表 *54:* 终端分析策略设置

字段名称	使用指南
Name	输入要创建的终端分析策略的名称。
Description	输入要创建的终端分析策略的说明。
Policy Enabled	默认情况下，**Policy Enabled** 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
Minimum Certainty Factor	输入要与分析策略相关联的最小值。默认值为 10。
Exception Action	选择在分析策略中定义规则时要与条件关联的例外操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 例外操作 (Exception Actions)**。
Network Scan (NMAP) Action	从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。
Create an Identity Group for the policy	选择以下选项之一以创建终端身份组： • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	选择此选项以使用现有的分析策略。 此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。 例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。

字段名称	使用指南
No, use existing Identity Group hierarchy	选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。 通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。 例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与 Unknown 配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入 Profiled 终端身份组中。例如， • 如果终端与 Cisco-IP-Phone 配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。 • 如果终端与 Workstation 配置文件相匹配，则这些终端会归入 Workstation 终端身份组中。 Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。
Parent Policy	选择在系统中定义的、要与新终端分析策略相关联的父分析策略。 可以选择可将规则和条件继承到其子项的父分析策略。
Associated CoA Type	选择以下要与终端分析策略相关联的 CoA 类型之一： • No CoA • Port Bounce • Reauth • Global Settings，该设置是从在 Administration > System > Settings > Profiling 中设置的分析器配置进行应用
Rules	在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。 策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。

字段名称	使用指南
Conditions	点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。 点击 **从库中选择现有条件 (Select Existing Condition from Library)** 或 **创建新条件（高级选项）(Create New Condition (Advanced Option))**。 **从库中选择现有条件 (Select Existing Condition from Library)**：可以通过从策略元素库中选择Cisco预定义条件来定义表达式。 **创建新条件（高级选项）(Create New Condition (Advanced Option))**：可以通过从各种系统或用户定义的字典中选择属性来定义表达式。 可以将以下其中一项与分析条件相关联： • 每种条件的可信度的整数值。 • 为该条件输入例外操作或网络扫描操作 选择以下其中一个要与分析条件相关联的预定义设置： • “可信度增加”(Certainty Factor Increases)：为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。 • “采取例外操作”(Take Exception Action)：触发在此终端分析策略的“例外操作”(Exception Action) 字段中配置的例外操作。 • “采取网络扫描操作”(Take Network Scan Action)：触发在此终端分析策略的“网络扫描 (NMAP) 操作”(Network Scan (NMAP) Action) 字段中配置的网络扫描操作。

字段名称	使用指南
Select Existing Condition from Library	可以执行以下操作： • 可以选择策略要素库中可用的Cisco预定义条件，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。
创建新条件（高级选项）	可以执行以下操作： • 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。可以使用 AND 或 OR 运算符

相关主题

思科 ISE 分析服务 ， 第 165 页

创建终端分析策略，第 210 页
使用 UDID 属性的终端情景可视性，第 241 页

创建终端分析策略

您可以通过使用 New Profiler Policy 页面中的以下选项，创建用于分析终端的新分析策略：

- Policy Enabled
- Create an Identity Group，让策略创建匹配的终端身份组或使用终端身份组层次结构
- Parent Policy
- Associated CoA Type

注释 当您选择在**分析策略 (Profiling Policies)** 窗口中创建终端策略时，请勿使用 Web 浏览器中的“停止”(Stop) 按钮。此操作会导致以下结果：停止加载**新分析器策略 (New Profiler Policy)** 窗口、在访问时加载其他列表页面及列表页面内的菜单，以及防止您对列表页面内的所有菜单执行操作，“过滤器”(Filter) 菜单除外。您可能需要注销Cisco ISE，然后重新登录才能对列表菜单内的所有菜单执行操作。

您可以通过复制终端分析策略来创建类似特征的分析策略，这样您就可以修改现有的分析策略，而不是通过重新定义所有条件来创建新分析策略。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入要创建的新终端政策的名称和说明。**Policy Enabled** 复选框在默认情况下处于选中状态，以包含用于在分析终端时进行验证的终端分析策略。

步骤 4 输入最低可信度的值，有效范围为 1 至 65535。

步骤 5 点击 **Exception Action** 下拉列表旁边的箭头以关联例外操作，或点击 **Network Scan (NMAP) Action** 下拉列表旁边的箭头以关联网络扫描操作。

步骤 6 为 **Create an Identity Group for the policy** 选择以下其中一个选项：

- **Yes, create matching Identity Group**
- **No, use existing Identity Group hierarchy**

步骤 7 点击 **Parent Policy** 下拉列表旁边的箭头将父策略关联到新终端策略。

步骤 8 在 **Associated CoA Type** 下拉列表中选择要关联的 CoA 类型。

步骤 9 点击规则以添加条件并为每个条件的可信度关联一个整数值或为该条件关联例外操作或网络扫描操作，以对终端进行整体分类。

步骤 10 在新建分析器策略 (New Profiler Policy) 页面中点击**提交 (Submit)** 以添加终端策略，或点击**分析器策略列表 (Profiler Policy List)** 链接以返回分析策略 (Profiling Policies) 页面。

每个终端分析策略的授权更改配置

除了Cisco ISE 中授权更改 (CoA) 类型的全局配置，您还可以配置为每个终端分析策略发出特定类型的关联 CoA。

全局 No CoA 类型配置会覆盖终端分析策略中配置的每个 CoA 类型。如果全局 CoA 类型设置的不是 No CoA 类型，则系统允许每个终端分析策略覆盖全局 CoA 配置。

当触发 CoA 时，每个终端分析策略都可以决定实际 CoA 类型，如下所示：

- General Setting - 这是适用于所有终端分析策略的根据全局配置发出 CoA 的默认设置。
- No CoA - 此设置会覆盖任何全局配置并为配置文件禁用 CoA。
- Port Bounce - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并发出端口退回 CoA。
- Reauth - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并且发出重新身份验证 CoA。

注释 如果分析器全局 CoA 配置设置为 Port Bounce（或 Reauth），请确保您将相应终端分析策略配置为基于策略的 CoA 选项 No CoA，从而使您的移动设备不会出现自带设备流程中断。

请参阅下表中对所有 CoA 类型和根据全局和终端分析策略设置在每个案例中实际发出的 CoA 类型的配置总结。

表 *55:* 为各种配置组合发出的 *CoA* 类型

全局 **CoA** 类型	根据策略设置的默认 **CoA** 类型	根据策略的 **No CoA** 类型	根据策略的端口退回类型	根据策略的重新身份验证类型
No CoA	No CoA	No CoA	No CoA	No CoA
Port Bounce	Port Bounce	No CoA	Port Bounce	Re-Auth
Reauth	Reauth	No CoA	Port Bounce	Re-Auth

导入终端分析策略

使用可以在导出功能中创建的相同格式，从 XML 文件导入终端分析策略。如果导入已关联父策略的新建分析策略，则必须在定义子策略之前定义父策略。

导入的文件包含终端分析策略层级结构，首先包含父策略，其次是导入的配置文件，然后是在策略中定义的规则和考核。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)**，找到您之前导出而现在想要导入的文件。

步骤 4 点击**提交 (Submit)**。

步骤 5 点击**分析器策略列表 (Profiler Policy List)** 链接，返回“分析策略”(Profiling Policies) 页面。

导出终端分析策略

您可以将终端分析策略导出到其他Cisco ISE 部署中。或者，您可以使用 XML 文件作为模板创建您自己的策略并导入。您还可以将该文件下载到您系统中的默认位置，以用于日后的导入。

当您导出终端分析策略时会出现一个对话框，提示您使用适当的应用打开 profiler_policies.xml 或将其保存。此文件的格式为 XML，您可以使用网页浏览器打开，也可以用其他适当的应用打开。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 选择**导出 (Export)**，并选择以下一项：

- **导出所选 (Export Selected)**：您仅可以导出在“分析策略”(Profiling Policies) 页面中选择的终端分析策略。
- **导出所选及终端 (Export Selected with Endpoints)**：可以导出所选择的终端分析策略，以及使用所选择的终端分析策略分析的终端。
- **全部导出 (Export All)**：默认情况下，可以导出“分析策略”(Profiling Policies) 页面中的所有分析策略。

步骤 3 点击“确定”(OK) 以在 profiler_policies.xml 文件中导出终端分析策略。

预定义终端分析策略

部署Cisco ISE 时，Cisco ISE 包含预定义的默认分析策略，这些策略的分层结构允许您对网络上的已识别终端进行分类，并将它们分配给匹配的终端身份组。因为终端分析策略采用分层结构，所以您会发现，Profiling Policies 页面显示设备的通用（母）策略列表，Profiling Policies 列表页面显示与母策略关联的子策略。

无论是否启用以用于验证，Profiling Policies 页面都显示终端分析策略及其名称、类型、描述和状态。

终端分析策略类型分类如下：

- Cisco Provided - 在Cisco ISE 中预定义的终端分析策略被识别为 Cisco Provided 类型。
  - Administrator Modified - 修改预定义的终端分析策略时，终端分析策略被识别为 Administrator Modified 类型。Cisco ISE 将在升级过程中覆盖您在预定义终端分析策略中所做的更改。
- Administrator Created - 您创建的终端分析策略或者当您复制Cisco提供的终端分析策略时，被识别为 Administrator Created 类型。

我们建议为一组终端创建通用策略（母策略），其子策略能够继承规则和条件。如果终端必须归类，那么终端配置文件必须首先匹配母策略，当您分析终端时，再匹配后代（子）策略。

例如，Cisco-Device 是一个适用于所有Cisco设备的通用终端分析策略，适用于Cisco设备的其他策略则为 Cisco-Device 的子策略。如果终端必须归类为 Cisco-IP-Phone 7960，那么此终端的终端配置文件必须首先匹配母 Cisco-Device 策略、子 Cisco-IP-Phone 策略，然后匹配 Cisco-IP-Phone 7960 分析策略，以便更好地分类。

注释 Cisco ISE 不会覆盖管理员修改的策略及其子策略，即使这些策略仍标记为Cisco提供。如果管理员修改的策略被删除，它会恢复为以前的Cisco提供的策略。下一次发生源更新时，所有子策略都会更新。

在升级期间覆盖预定义终端分析策略

您可以在 Profiling Policies 页面编辑现有的终端分析策略。此外，当您想要修改预定义终端分析策略时，必须在预定义终端配置文件副本中保存所有配置。

在升级过程中，Cisco ISE 重写您在预定义终端配置文件中保存的任何配置。

无法删除终端分析策略

您可以在**分析策略 (Profiling Policies)** 窗口中删除选定的或所有终端分析策略。默认情况下，可以从**分析策略 (Profiling Policies)** 窗口删除所有终端分析策略。当在**分析策略 (Profiling Policies)** 窗口中选择所有终端分析策略并尝试删除它们时，如果其中有些终端分析策略映射至其他终端分析策略或映射至授权策略，则可能不会删除它们。

- 您无法删除Cisco提供的终端分析策略，
- 当终端配置文件定义为其他终端配置文件的父级时，您无法在**分析策略 (Profiling Policies)** 窗口中删除父配置文件。例如，Cisco-Device 是用于Cisco设备的其他终端分析策略的父级。
- 当某个终端配置文件映射至授权策略时，您无法删除此终端配置文件。例如，Cisco-IP-Phone 映射至 Profiled Cisco IP Phones 授权策略而且是用于Cisco IP 电话的其他终端分析策略的父级。

用于 Draeger 医疗设备的预定义分析策略

Cisco ISE 包含默认终端分析策略，这些策略包括用于 Draeger 医疗设备的通用策略、用于 Draeger-Delta 医疗设备的策略，以及用于 Draeger-M300 医疗设备的策略。两个医疗设备共用端口 2050 和 2150，因此当您使用默认 Draeger 终端分析策略时，您无法给 Draeger-Delta 和 Draeger-M300 医疗设备分类。

如果这些 Draeger 设备在您的环境中共用端口 2050 和 2150，除了在默认 Draeger-Delta 和 Draeger-M300 终端分析策略中检查设备目标 IP 地址之外，您还必须增加一条规则以确保您可以区分这些医疗设备。

Cisco ISE 包括用于 Draeger 医疗设备终端分析策略的以下分析策略：

- 包含端口 2000 的 Draeger-Delta-PortCheck1
- 包含端口 2050 的 Draeger-Delta-PortCheck2
- 包含端口 2100 的 Draeger-Delta-PortCheck3
- 包含端口 2150 的 Draeger-Delta-PortCheck4
- 包含端口 1950 的 Draeger-M300PortCheck1
- 包含端口 2050 的 Draeger-M300PortCheck2
- 包含端口 2150 的 Draeger-M300PortCheck3

用于未知终端的终端分析策略

不匹配现有的配置文件且无法在Cisco ISE 中分析的终端为未知终端。未知配置文件是分配给终端的默认系统分析策略，为此终端收集的一个属性或一组属性与Cisco ISE 中现有的配置文件不匹配。

在以下情境中分配未知配置文件：

- 在Cisco ISE 中动态地发现终端，并且没有适用于此终端的匹配终端分析策略时，将终端分配给未知配置文件。
- 当Cisco ISE 中静态地添加终端，且没有适用于静态添加的终端的匹配终端分析策略时，将终端分配给未知配置文件。

  如果将终端静态地添加到网络，Cisco ISE 中的分析服务不分析静态添加的终端。稍后，您可以将未知配置文件更改为相应的配置文件，Cisco ISE 不会重新分配您已分配的分析策略。

用于静态添加的终端的终端分析策略

对于静态添加以进行分析的终端，分析服务将新的 MATCHEDPROFILE 属性添加到终端，为终端计算配置文件。如果动态分析终端，那么计算的配置文件则是该终端的实际配置文件。这样，您可以发现静态添加的终端的计算配置文件与动态分析的终端的匹配配置文件不匹配的情况。

静态 IP 设备的终端分析策略

如果您的终端拥有静态分配的 IP 地址，则您可以为这些静态 IP 设备创建配置文件。

必须启用 RADIUS 探测功能或 SNMP 查询和 SNMP 陷阱探测功能，分析拥有静态 IP 地址的终端。

终端分析策略匹配

当在分析策略中满足一个或多个规则中定义的分析条件时，Cisco ISE 会始终将终端的所选策略视为匹配策略而不是已评估的策略。此处，该终端的静态分配的状态在系统中设置为 false。但是，通过在终端编辑过程中使用静态分配功能，可以在将该终端重新静态分配给系统中的现有分析策略后将状态设置为 true。

以下操作适用于终端的匹配策略：

- 对于静态分配的终端，分析服务会计算 MATCHEDPROFILE。
- 对于动态分配的终端，MATCHEDPROFILE 与匹配终端配置文件相同。

您可以使用分析策略中定义的一个或多个规则确定动态终端的匹配分析策略，并且相应地分配终端身份组以进行分类。

当终端映射到现有策略时，分析服务会搜索分析策略的层次结构以查找具有匹配策略组的最近父配置文件，并将终端分配给相应的终端策略。

用于授权的终端分析策略

您可以在授权规则中使用终端分析策略，在其中您可以创建作为属性的新条件，使之包含终端分析策略检查，并且该属性以终端分析策略的名称作为属性值。您可以从终端字典选择终端分析策略，其中包含以下属性：PostureApplicable、EndPointPolicy、LogicalProfile 和 BYODRegistration。

PostureApplicable 的属性值根据操作系统自动设置。对于 IOS 和 Android 设备，它设置为否 *(No)*，因为这些平台上不能使用 AnyConnect 支持来执行终端安全评估。对于 Mac OSX 和 Windows 设备，该值设置为是 *(Yes)*。

您可以定义包括 EndPointPolicy、BYODRegistration 和身份组的组合的授权规则。

终端分析策略分组为逻辑配置文件

逻辑配置文件是一类配置文件或相关联配置文件的容器，无需考虑终端分析策略是由Cisco提供还是由管理员创建。终端分析策略可以与多个逻辑配置文件关联。

您可以在授权策略条件中使用逻辑配置文件，来帮助您创建针对某类别配置文件的整体网络接入策略。您可以创建授权的简单条件，该条件可包括在授权规则中。您可以在授权条件中使用的属性-值对是逻辑配置文件（属性）和逻辑配置文件名称（值），该属性-值对位于终端系统字典中。

例如，通过将与移动设备类别匹配的终端分析策略分配至逻辑配置文件，可以为所有移动设备（如安卓、苹果 iPhone 或黑莓）创建一个逻辑配置文件。Cisco ISE 包含 IP 电话，这是一个针对所有 IP

电话的默认逻辑配置文件，包括 IP 电话、Cisco IP 电话、Nortel IP 电话 2000 系列和 AVAYA IP 电话配置文件。

创建逻辑配置文件

您可以创建可用于对某个类别的终端分析策略进行分组的逻辑配置文件，借此可创建整体类别的配置文件或关联配置文件。您还可以从分配的集合中删除终端分析策略，从而将其移回到可用集合。有关逻辑配置文件的详细信息，请参阅终端分析策略分组为逻辑配置文件，第 215 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **逻辑配置文件 (Logical Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)** 和**说明 (Description)** 的文本框中输入新逻辑配置文件的名称和说明。

步骤 4 从**可用策略 (Available Policies)** 中选择终端分析策略以在逻辑配置文件中对其进行分配。

步骤 5 点击向右箭头以将所选终端分析策略移至**分配策略 (Assigned Policies)**。

步骤 6 点击**提交 (Submit)**。

分析例外操作

例外操作是终端分析策略中可以引用的一个可配置操作，当符合该操作关联的例外条件时就会触发例外操作。

例外操作可以是以下任一类型：

- Cisco-provided - 您不能删除Cisco提供的例外操作。当您要在Cisco ISE 中分析终端时，Cisco ISE 从系统中触发以下非可编辑的分析例外操作：
  - Authorization Change - 当从授权策略使用的终端身份组添加或删除终端时，此分析服务发出授权更改。
  - Endpoint Delete - 当在 Endpoints 页面从系统中删除终端或在Cisco ISE 网络中从 Edit 页面向已知配置文件分配终端时，在Cisco ISE 中会触发例外操作并且会发出 CoA。
  - FirstTimeProfiled - 当在Cisco ISE 中首次分析某个终端时，如果该终端的配置文件从未知配置文件转变为现有配置文件，但是在Cisco ISE 网络中该终端身份验证未成功，则在Cisco ISE 中会触发例外操作并且会发出 CoA。
- Administrator-created - Cisco ISE 触发您所创建的分析例外操作。

创建例外操作

您可以定义一个或多个例外规则并将其关联到单个分析策略。此关联会在分析策略和至少一个例外规则在Cisco ISE 中的分析终端中匹配时触发例外操作（单个可配置操作）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **例外操作 (Exception Actions)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在 **名称** 和 **说明** 的文本框中输入例外操作的名称和说明。

步骤 4 选中 **CoA Action** 复选框。

步骤 5 选中 **Policy Assignment** 下拉列表以选择终端策略。

步骤 6 点击**提交 (Submit)**。

使用策略和身份的静态分配创建终端

在终端页面中，您可以使用终端的 MAC 地址静态创建新的终端。在终端页面中，您还可以选择静态分配的终端分析策略和身份组。

常规和移动设备 (MDM) 终端会显示在终端身份列表中。在列表页面中会显示 MDM 终端的属性列，这些属性包括主机名、设备类型、设备标识符。其他列如静态分配和静态组分配在默认情况下不显示。

注释 您无法使用此页面添加、编辑、删除、导入或导出 MDM 终端。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入十六进制格式的终端 MAC 地址，以冒号分隔。

步骤 4 从 **Policy Assignment** 下拉列表中选择一个匹配的终端策略，将其静态分配状态从动态更改为静态。

步骤 5 选中 **Static Assignment** 复选框，将分配到终端的静态分配的状态从动态更改为静态。

步骤 6 从 **Identity Group Assignment** 下拉列表中选择您希望分配到新创建终端的终端身份组。

步骤 7 选中 **Static Group Assignment** 复选框，将终端身份组的动态分配更改为静态。

步骤 8 点击**提交 (Submit)**。

从 CSV 文件导入终端

您可以从已从Cisco ISE 模板创建的 CSV 文件导入终端，并使用终端详细信息进行更新。从 ISE 导出的终端包含约 75 个属性，因此无法直接导入到另一 ISE 部署中。如果 CSV 文件中存在不允许导入的列，则会显示包含列列表的消息。尝试再次导入文件之前，必须删除指定的列。

注释 要导入终端自定义属性，必须使用正确的数据类型在**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 页面创建与 CSV 文件中相同的自定义属性。这些属性必须添加“CUSTOM.”前缀以便与终端属性区分。

大约有 30 个可以导入的属性。此列表包括 MACAddress、EndPointPolicy 和 IdentityGroup。可选属性为：

说明	PortalUser	lastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	设备类型	host-name
PortalUser.GuestStatus	StaticAssignment	位置
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<自定义属性名称>	-	-

文件标题行必须是在默认导入模板中指定的格式，使终端列表按以下顺序显示：MACAddress、EndpointPolicy、IdentityGroup <以上作为可选属性的属性列表>。可以创建以下文件模板：

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <以上作为可选属性的属性列表>

所有属性值（MACAddress 除外）对于从 CSV 文件导入终端均是可选的。如果想要导入终端而无需特定值，值依然用逗号分隔。

例如，

- MAC1, Endpoint Policy1, Endpoint Identity Group1

- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, 等

步骤 1 选择 情景可视性 **(Context Visibility)** > 终端 **(Endpoints)** > 导入 **(Import)**。

步骤 2 点击从文件导入 **(Import From File)**。

步骤 3 点击浏览 **(Browse)** 找到您已创建的 CSV 文件。

步骤 4 点击提交 **(Submit)**。

可用于终端的默认导入模板

您可以生成可以在其中更新终端的模板，您可将其用于导入终端。默认情况下，您可以使用 生成模板 链接，在 Microsoft Office Excel 应用中创建 CSV 文件并将文件保存在您的系统本地位置上。文件位于以下位置： **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **导入 (Import)** > **从文件导入 (Import From File)**。您可以使用 生成模板 链接创建模板，并且Cisco ISE 服务器将显示 Opening template.csv 对话框。您可以通过此对话框打开默认 template.csv 文件，或将 template.csv 文件保存在您的系统本地位置上。如果您选择从此对话框打开 template.csv 文件，系统会使用 Microsoft Office Excel 应用打开此文件。默认的 template.csv 文件包含一个标题行，其中显示 MAC 地址、终端策略、终端身份组和其他可选属性。。

您必须更新终端的 MAC 地址、终端分析策略、终端身份组和任何要导入的可选属性值，并使用新文件名保存文件。此文件可用于导入终端。请参阅您使用 生成模板 时创建的 template.csv 文件中的标题行。

表 ***56: CSV*** 模板文件

MAC	EndpointPolicy	IdentityGroup	其他可选属性
11:11:11:11:11:11	Android	Profiled	<空>/<值>

导入过程中重新分析的未知终端

如果用于导入的文件包含具有 MAC 地址的终端，并且其已分配的终端分析策略是 Unknown 配置文件，则这些终端会在Cisco ISE 中立即重新分析到导入过程中的匹配终端分析策略。但是，系统不会将它们静态分配到 Unknown 配置文件。如果终端在 CSV 文件中没有向其分配的终端分析策略，则它们会分配到 Unknown 配置文件，然后重新分析到匹配的终端分析策略。请参阅以下内容，了解 Cisco ISE 如何在导入过程中重新分析与 Xerox_Device 配置文件匹配的 Unknown 配置文件，以及Cisco ISE 如何重新分析未分配的终端。

表 *57: Unknown* 配置文件：从文件导入

MAC 地址	Cisco ISE 中导入前分配的终端分析策略	Cisco ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Unknown。	Xerox-Device
00:00:00:00:01:03	Unknown。	Xerox-Device
00:00:00:00:01:04	Unknown。	Xerox-Device
00:00:00:00:01:05	如果未向终端分配配置文件，则该终端会分配到 Unknown 配置文件，并且还会重新分析到匹配的配置文件。	Xerox-Device

不导入具有无效属性的终端

如果 CSV 文件中存在的任何终端具有无效属性，则不导入该终端，并显示错误消息。

例如，如果终端被分配至用于导入的文件中的无效配置文件，因为Cisco ISE 中没有匹配的配置文件，所以不会导入这些无效配置文件。请参阅下文，了解当终端被分配至CSV 文件中的无效配置文件时，如何不导入终端。

表 *58:* 无效配置文件：从文件导入

MAC 地址	Cisco ISE 中导入前分配的终端分析策略	Cisco ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Unknown。	Xerox-Device
00:00:00:00:01:05	如果向无效配置文件而不是向 Cisco ISE 中可用的配置文件分配 00:00:00:00:01:05 等终端，则 Cisco ISE 会显示警告消息，提示此策略名称无效并且将不导入该终端。	因为Cisco ISE 中没有匹配的配置文件，所以不会导入该终端。

从 LDAP 服务器导入终端

可以安全地从 LDAP 服务器导入终端的 MAC 地址、关联的配置文件和终端身份组。

开始之前

在开始导入终端之前，请确保已安装 LDAP 服务器。

必须配置连接设置和查询设置才能从 LDAP 服务器导入。如果Cisco ISE 中的连接设置或查询设置配置不正确，则系统会显示“LDAP import failed:”错误消息。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **导入 (Import)** > **从 LDAP 导入 (Import From LDAP)**。

步骤 2 输入连接设置的值。

步骤 3 输入查询设置的值。

步骤 4 点击**提交 (Submit)**。

使用逗号分隔值文件导出终端

您可以从Cisco ISE 服务器将选定的终端或所有终端导出到 CSV 文件中，其中会列出约 75 个属性以及终端的 MAC 地址、终端分析策略和终端身份组。在Cisco ISE 中创建的自定义属性也会导出到 CSV 文件并增加“CUSTOM.”前缀，以便与其他终端属性区分。

注释 要将从一个部署导出的终端自定义属性导入到另一部署，必须在**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 窗口中创建相同的自定义属性，并使用原始部署中指定的相同数据类型。

导出全部 (Export All) 可导出Cisco ISE 中的所有终端，而**导出所选 (Export Selected)** 可仅导出用户选择的终端。默认情况下，profiler_endpoints.csv 是 CSV 文件，而 Microsoft Office Excel 是打开 CSV 文件的默认应用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。

步骤 2 点击**导出 (Export)**，并选择下列选项之一：

- **导出所选 (Export Selected)**：只能导出在**终端 (Endpoints)** 窗口中选定的终端。
- **全部导出 (Export All)**：默认情况下，可以导出**终端 (Endpoints)** 窗口中的所有终端。

步骤 3 点击**确定 (OK)** 保存 profiler_endpoints.csv 文件。

已识别的终端

Cisco ISE 显示已识别的终端，这些终端在终端页面中连接到您的网络并使用您网络上的资源。终端通常是一个支持网络的设备，该设备通过有线和无线网络接入设备和VPN连接到您的网络。终端可以是个人计算机、笔记本、IP 电话、智能手机、游戏主机、打印机、传真机等等。

以十六进制显示的终端 MAC 地址通常唯一地表示一个终端，但是您也可以使用一组变化的属性以及与这些属性关联的值（属性-值对）来标识终端。您可以根据终端的功能、网络接入设备的配置以及您用于收集这些属性的方法（探测），收集一组变化的终端属性。

已动态分析的终端

当在您的网络上发现终端时，根据已配置的终端分析策略，即可对这些终端进行动态分析，并按照配置文件将这些终端分配到匹配的终端身份组。

已静态分析的终端

当您使用终端的 MAC 地址在Cisco ISE 中创建终端并将配置文件及终端身份组与其关联时，即可静态分析该终端。Cisco ISE 不会重新分配已静态分配终端的分析策略和身份组。

未知终端

如果终端缺少匹配的分析策略，您可以分配一个未知分析策略（未知），而终端则会被分析为未知。由未知终端策略分析的终端需要您使用已收集的一个终端属性或一组终端属性来创建配置文件。与所有配置文件均不匹配的终端会被分组到未知终端身份组中。

策略服务节点数据库中本地存储的已识别终端

Cisco ISE 在本地将已识别的终端写入策略服务节点数据库。将这些终端在本地存储于数据库中之后，只有在终端中重要属性出现变更时，在管理节点数据库中这些终端才可用（远程写入），并且被复制到其他策略服务节点数据库中。

以下是重要属性：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

当您在Cisco ISE 中更改终端配置文件定义时，所有终端都必须重新进行分析。收集终端属性的策略服务节点负责重新分析这些终端。

当策略服务节点开始收集关于某个终端的属性时，如果一开始该终端是由另一个不同的策略服务节点收集其属性，则该终端的所有权就改为属于当前策略服务节点。新策略服务节点会从之前的策略服务节点检索最新属性，并且将所收集的这些属性与已经收集的那些属性进行比较。

当终端中某个重要属性发生变更时，该终端的属性会自动保存在管理节点数据库中，这样您就会获得该终端中最新的重要变更。如果拥有某个终端的策略服务节点由于某些原因不可用，则管理员 ISE 节点将会重新分析失去所有者的终端而且您必须为这些终端配置新的策略服务节点。

集群中的策略服务节点

Cisco ISE 将策略服务节点组用作集群，如果集群中两个或多个节点为同一终端收集属性，集群将允许交换终端属性。我们建议您为负载均衡器后面的所有策略服务节点创建集群。

如果与当前所有者不同的节点接收到同一终端的属性，此节点会在集群中发送一条向当前所有者请求最新属性的消息以合并属性并确定是否需要更改所有权。如果您未在Cisco ISE 中定义节点组，系统会假定所有节点都处于同一集群中。

Cisco ISE 不会更改终端创建和复制，只会根据从静态属性和动态属性构建的用于分析的许可属性列表决定是否更改终端的所有权。

在以后的属性收集中，如果以下任一属性发生更改，管理节点上会更新终端：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

在管理节点中编辑和保存终端时，系统会从当前终端所有者检索属性。

创建终端身份组

Cisco ISE 将其所发现的终端划分至相应的终端身份组。Cisco ISE 拥有若干个系统定义的终端身份组。您还从 Endpoint Identity Groups 页面创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

步骤 4 为您想要创建的终端身份组输入**说明**。

步骤 5 点击**父级组 (Parent Group)** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

步骤 6 点击**提交 (Submit)**。

已识别终端划分为终端身份组

Cisco ISE 根据终端分析策略，将已发现的终端划分为对应的终端身份组。分析策略分为不同的层级，在Cisco ISE 中在终端身份组级应用。通过将终端划分为终端身份组，并且将分析策略应用到终端身份组，Cisco ISE 使您能够查看对应的终端分析策略，确定终端到终端配置文件的映射。

默认情况下，Cisco ISE 创建终端身份组集合，允许您创建自己的身份组，动态或静态地向其分配终端。您可以创建终端身份组，将身份组关联到系统创建的身份组之一。此外，您还可以将您创建的终端静态地分配到系统中存在的身份组之一，分析服务不能重新分配身份组。

为终端创建的默认终端身份组

Cisco ISE 创建以下终端身份组：

- “黑名单”(Blacklist) - 此终端身份组包括Cisco ISE 中静态分配给此组的终端和在设备注册门户中列入黑名单的终端。可以在Cisco ISE 中定义授权配置文件以允许或拒绝为该组中的终端提供网络接入。
- GuestEndpoints - 此终端身份组包括访客用户使用的终端。
- “分析”(Profiled) - 此终端身份组包括Cisco ISE 中除Cisco IP 电话和工作站之外与终端分析策略匹配的终端。
- RegisteredDevices - 此终端身份组包括属于员工通过设备注册门户添加的已注册设备的终端。当这些设备分配至该组时，分析服务会继续正常分析这些设备。终端在Cisco ISE 中会静态分配至该组，而且分析服务无法将其重新分配到任何其他身份组。这些设备会像任何其他终端一样显示在终端列表上。您可以在Cisco ISE 中的“终端”(Endpoints) 窗口从终端列表编辑、删除和阻止通过设备注册门户添加的这些设备。您在设备注册门户中阻止的设备会分配至“黑名单”终端身份组，而且Cisco ISE 中存在的一个授权配置文件会将被阻止的设备重定向显示“未授权的网络访问”(Unauthorised Network Access) 的 URL，这是被阻止设备的默认门户页面。
- “未知”(Unknown) - 此终端身份组包括与Cisco ISE 中任何配置文件都不匹配的终端。

除了上述系统创建的终端身份组，Cisco ISE还会创建以下终端身份组，这些身份组与“分析”(Profiled) 身份组关联：父组是系统中存在的默认身份组：

- Cisco-IP-Phone - 此身份组包含您的网络上所有已分析的Cisco IP 电话。
- Workstation - 此身份组包含您的网络上所有已分析的工作站。

为匹配的终端分析策略创建的终端身份组

如果您有终端策略与现有策略匹配，则分析服务可以创建一个匹配的终端身份组。此身份组就成为已分析终端身份组的子级。当您创建终端策略时，您可以在 Profiling Policies 页面选中 Create Matching Identity Group 复选框，以创建匹配的终端身份组。除非删除配置文件的映射，否则无法删除匹配的身份组。

向终端身份组中添加静态终端

您可以在任意终端身份组中添加或移除静态添加的终端。

您仅可从 Endpoints 小组件向特定身份组添加终端。如果您向某个终端身份组添加某个终端，该终端就会从其之前动态分组的终端身份组删除。

在从您最近添加了某个终端的终端身份组删除该终端后，系统会重新分析该终端，使之回到相应身份组。这不会从系统删除终端，而只是从终端身份组删除终端。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 选择终端身份组，然后点击**编辑 (Edit)**。

步骤 3 点击**添加 (Add)**。

步骤 4 在 Endpoints 小组件中选择终端，以将所选终端添加至终端身份组。

步骤 5 点击 **Endpoint Group List** 链接以返回 Endpoint Identity Groups 页面。

在身份组中添加或删除终端后重新分析动态终端

如果终端身份组分配不是静态的，则在终端身份组中添加或删除终端后重新分析终端。由 ISE 分析器动态识别的终端显示在相应的终端身份组中。如果从终端身份组删除动态添加的终端，Cisco ISE 则显示一条消息，指明您已成功从身份组删除终端，但在终端身份组中重新分析这些终端。

用于授权规则的终端身份组

您可以在授权策略中有效地使用终端身份组来向所发现的终端提供相应的网络接入权限。例如，在 Cisco ISE 中，以下位置默认提供适用于所有类型Cisco IP 电话的授权规则： **策略 (Policy)** > **策略集 (Policy Sets)** > **默认 (Default)** > **授权策略 (Authorization Policy)**。

您必须确保终端分析策略为独立策略（而不是其他终端分析策略的父策略），或确保未禁用终端分析策略的父策略。

任意播和分析器服务

任意播是一种网络技术，其中将相同的IP地址分配给两个或更多主机，并允许路由确定接收数据的最适当目标。与提供单一分析数据目标（RADIUS、DHCP中继、SNMP陷阱和NetFlow）的负载均衡器用例类似，任意播允许为源配置单一IP目标，以避免将相同数据发送到多个目标。

任意播IP地址可分配给实际PSN接口IP地址或负载均衡器虚拟IP地址，以支持跨数据中心的冗余。不得将任意播IP地址分配给ISE千兆以太网0管理接口。

用于任意播的接口必须是专供分析器探测器使用的接口。当任意播IP地址分配给负载均衡器虚拟IP地址时，不适用这一要求。

使用任意播时，关键在于自动检测任何节点故障，并从路由表中删除故障节点的对应路由。如果任意播目标是链路或VLAN上的唯一主机，则故障可能会导致自动删除路由。

部署IP任意播时，务必确保通往每个目标的路由度量具有重大的权重或偏重。如果通往任意播目标的路由摆动或导致等价多路径路由(ECMP)场景，则给定服务（RADIUS AAA、DHCP或SNMP陷阱分析、HTTPS门户）的流量可能会分配给每个目标，从而导致流量过多和服务故障（RADIUS AAA和HTTPS门户）或次优分析和数据库复制（分析服务）。

IP任意播的主要优势在于，它可以极大简化接入设备、配置文件数据源和DNS上的配置。它还可以通过确保给定终端的数据仅发送到单个PSN来优化ISE分析。必须仔细规划其他路由配置并使用适当的监控器进行管理。但是，由于没有使用不同的子网和IP地址，所以故障排除可能比较困难。

分析器源服务

分析器条件、例外操作和NMAP扫描操作分类为由Cisco提供或由管理员创建，如“系统类型”(System Type)属性所示。终端分析策略会分类为由Cisco提供、由管理员创建或由管理员修改。这些分类显示在“系统类型”(System Type)属性中。

您可以根据系统类型属性，对分析器条件、例外操作、NMAP操作和终端分析策略执行不同的操作。您无法编辑或删除由Cisco提供的条件、例外操作和NMAP扫描操作。无法删除由Cisco提供的终端策略。编辑策略时，这些策略称为管理员修改的策略。源服务更新策略后，管理员修改的策略将替换为所基于的由Cisco提供的最新版本策略。

可以从Cisco源服务器检索新的和更新后的策略及更新的OUI数据库。必须已订阅Cisco ISE。还可以接收有关已应用、成功和失败消息的电子邮件通知。可以将有关源服务操作的匿名信息发送回Cisco，这有助于Cisco改进源服务。

OUI数据库包含分配给供应商的MAC OUI。以下是OUI列表：http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE会在本地Cisco ISE服务器时区每天凌晨1:00下载策略和OUI数据库更新。Cisco ISE自动应用这些已下载的源服务器策略，其中存储了更改，因此可以将这些更改恢复到先前状态。恢复到先前状态时，将删除新的终端分析策略，而已更新的终端分析策略将恢复到先前状态。此外，分析器源服务将自动禁用。

您还可以在离线模式下手动更新源服务。如果您无法将 ISE 部署连接到Cisco源服务，则可以通过使用此选项手动下载更新。

注释 许可证在 60 天时段内处于不合规 (OOC) 状态 45 天后，不允许来自源服务的更新。当许可证已过期或使用量超过允许的会话数时，许可证即为不合规。

配置分析器源服务

分析器源服务会从Cisco源服务器中检索新的和更新后的终端分析策略及 MAC OUI 数据库更新。如果源服务不可用或发生其他错误，系统会在 Operations Audit 报告中进行报告。

您可以将Cisco ISE 配置为将匿名的馈送服务使用情况报告发回Cisco，这会向Cisco发送以下信息：

- Hostname - Cisco ISE 主机名
- MaxCount - 终端总数
- ProfiledCount - 已分析的终端计数
- UnknownCount - 未知终端计数
- MatchSystemProfilesCount - Cisco提供的配置文件计数
- UserCreatedProfiles - 用户创建的配置文件计数

您可以更改由Cisco提供分析策略中的 CoA 类型。当源服务更新该策略时，CoA 类型不会更改，但该策略的其余属性仍会更新。

Cisco ISE 2.7 及更高版本可以让您手动下载 OUI 更新，而无需下载策略更新。如果您对某些分析器条件进行了自定义以不止更改 CoA 类型，则可能不希望分析器馈送替换这些条件。您可能仍希望更新 OUI，以便分析器可以在制造商添加新设备时识别它们。“馈送服务”(Feed Service) 门户上提供仅下载 OUI 的选项。

开始之前

分析器源服务只可以从分布式部署中的Cisco ISE 管理门户或在独立 ISE 节点中配置。

如果计划从管理员门户发送有关馈送更新的电子邮件通知，请设置简单邮件传输协议 (SMTP) 服务器（**管理 (Administration)** > **系统 (System)** > **设置 (Settings)**）。

在线更新源服务：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**，然后检查是否已启用 **QuoVadis 根 CA 2 (QuoVadis Root CA 2)**。

步骤 2 选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **馈送 (Feeds)**。
您还可以在以下位置访问该选项： **管理 (Administration)** > **Feed 服务 (FeedService)** > **分析器 (Profiler)** 页面。

步骤 3 点击**在线订用更新 (Online Subscription Update)** 选项卡。

步骤 4 点击 **Test Feed Service Connection** 按钮以验证是否存在到Cisco源服务的连接，以及证书是否有效。

步骤 5 选中**启用临时计费更新 (Enable Interim Accounting Update)** 复选框。

步骤 6 以 HH:MM 格式（Cisco ISE 服务器的本地时区）输入时间。默认情况下，Cisco ISE 源服务安排在每天凌晨 1.00 点运行。

步骤 7 选中**在下载发生时通知管理员 (Notify administrator when download occurs)** 复选框，并在**管理员电子邮件地址 (Administrator email address)** 文本框输入您的电子邮件地址。如果您想要允许Cisco ISE 收集非敏感的信息（用于在将来的版本中提供更好的服务和附加功能），请选中**向思科提供匿名信息以帮助提高分析准确性 (Provide Cisco anonymous information to help improve profiling accuracy)** 复选框。

步骤 8 点击**保存 (Save)**。

步骤 9 点击 **Update Now**。

指示Cisco ISE 联系Cisco源服务对自上次源服务以来创建的新的和更新后的配置文件进行更新。此操作会重新分析系统中的所有终端，这可能导致系统负载增加。由于终端分析策略经过更新，某些当前连接到Cisco ISE 的终端的授权策略可能会发生更改。

当您对自上次源服务以来创建的新的和更新后的配置文件进行更新时，**立即更新 (Update Now)** 按钮会被禁用，并且只会在下载完成后启用。您必须通过导航操作离开分析器源服务的 Configuration 页面，然后返回此页面。

相关主题

离线配置分析器源服务 ， 第 228 页

离线配置分析器源服务

当Cisco ISE 未直接连接到Cisco源服务器时，您可以离线更新源服务。您可以从Cisco源服务器下载离线更新包，并使用离线源更新将其上传到Cisco ISE。您还可以设置关于添加到源服务器的新策略的邮件通知。

离线配置分析器源服务包括以下任务：

1. 下载离线更新包
2. 应用离线源更新

下载离线更新包

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **源 (Feeds)**。
您还可以在以下位置访问该选项： **管理 (Administration)** > **Feed 服务 (FeedService)** > **分析器 (Profiler)** 页面。

步骤 2 点击**离线手动更新 (Offline Manual Update)** 选项卡。

步骤 3 点击**下载更新的配置文件策略 (Download Updated Profile Policies)** 链接。您将被重定向至源服务合作伙伴门户。
您还可以从浏览器转到 https://ise.cisco.com/partner/，直接访问源服务合作伙伴门户。

步骤 4 如果您是新用户，请接受条款和协议。
系统将触发邮件给源服务管理员以便审批您的申请。批准后，您将收到一封确认邮件。

步骤 5 使用您的 Cisco.com 凭证登录合作伙伴门户。

步骤 6 选择**离线源 (Offline Feed) > 下载数据包 (Download Package)**。

步骤 7 点击**生成数据包 (Generate Package)**。

步骤 8 点击**点击以查看离线更新包内容 (Click to View the Offline Update Package contents)** 链接以查看生成的数据包中包含的所有配置文件和 OUI。

- 源分析器 1 和源 OUI 下的策略将下载到所有版本的Cisco ISE 。
- 源分析器 2 下的策略将仅下载到Cisco ISE 版本 1.3 和更高版本。
- 源分析器 3 下的策略将仅下载到Cisco ISE 版本 2.1 和更高版本。

步骤 9 点击**下载数据包 (Download Package)** 并将文件保存到您的本地系统。
您可以将文件上传并保存到Cisco ISE 服务器以应用已下载数据包中的源更新。

应用离线源更新

开始之前

您必须先下载离线更新数据包，才能应用源更新。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **馈送 (Feeds)** 。
您还可以在以下位置访问该选项： **管理 (Administration)** > **FeedService** > **分析器 (Profiler)** 窗口。

步骤 2 点击**离线手动更新 (Offline Manual Update)** 选项卡。

步骤 3 点击**浏览 (Browse)** 并选择已下载的分析器源数据包。

步骤 4 点击**应用更新 (Apply Update)**。

为配置文件和 OUI 更新配置邮件通知

您可以配置您的邮箱地址，以接收有关配置文件和 OUI 更新的通知。

步骤 1 下载离线更新包 部分中执行**第 1 步 (Step 1)** 至**第 5 步 (Step 5)**，转到源服务合作伙伴门户。

步骤 2 选择**离线源 (Offline Feed)** > **邮件首选项 (Email Preferences)**。

步骤 3 选中**启用通知 (Enable notification)** 复选框以接收通知。

步骤 4 从**天数 (days)** 下拉列表中选择天数，以设置您希望接收新更新通知的频率。

步骤 5 输入单个/多个邮箱地址并点击**保存 (Save)**。

撤消源更新

您可以恢复在之前更新中已经更新的终端分析策略，并删除通过之前更新分析器源服务新添加的终端分析策略和 OUI，。

如果在源服务器更新之后修改了终端分析策略，则系统中的终端分析策略不会更改。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **源 (Feeds)**。

步骤 2 如果想要查看在 Change Configuration Audit 报告中所做的配置更改，请点击**转到更新报告页面 (Go to Update Report Page)**。

步骤 3 点击 **Undo Latest**。

分析器报告

Cisco ISE 为您提供关于终端分析的各种报告，以及可用于管理您的网络的故障排除工具。可以生成历史以及当前数据的报告。您还可以向下钻取报告的某个部分以查看更多详细信息。对于大型报告，您还可以安排报告计划并以各种格式下载这些报告。

您可以从**操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** 为终端运行以下报告：

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

检测终端的异常行为

Cisco ISE 可保护您的网络，避免非法使用 MAC 地址问题。Cisco ISE 可以检测涉及 MAC 地址欺骗的终端，可以让您限制可疑终端的许可。

以下是异常行为的分析器配置页面中的两个选项：

- 启用异常行为检测
- 启用异常行为实施

如果启用异常行为检测，则Cisco ISE 会探测数据，并检查在与 NAS-Port-Type、DHCP 类标识符和终端策略相关的属性更改方面，是否存在与现有数据的任何冲突。如果是，则向终端添加名为

AnomalousBehavior 且设置为 true 的属性，这有助于过滤和查看“可视性情景”（Visibility Context）页面中的终端。系统还会为相应的 MAC 地址生成审核日志。

启用异常行为检测后，Cisco ISE 会检查现有终端的以下属性是否已更改：

1. 端口类型 - 确定终端的访问方法是否已更改。这仅适用于通过有线 Dot1x 连接的同一 MAC 地址用于无线 Dot1x 的情况，反之亦然。
2. DHCP 类标识符 - 确定终端的客户端类型或供应商类型是否已更改。这仅适用于 DHCP 类标识符属性已填充某个值，然后更改为另一个值的情况。如果为终端配置了静态 IP，则Cisco ISE 中的 DHCP 类标识符属性为空。稍后，如果另一台设备伪造此终端的 MAC 地址并使用 DHCP，则类标识符将从空值更改为特定字符串。这不会触发异常行为检测。
3. 终端策略 - 确定是否有重大配置文件更改。这仅适用于终端的配置文件从“电话”或“打印机”更改为“工作站”的情况。

如果启用“异常行为实施”，则在检测到异常行为时会发出 CoA，可根据**分析器配置 (Profiler Configuration)** 窗口中配置的授权规则对可疑终端进行重新授权。

针对带有异常行为的终端设置授权策略规则

可以通过在“授权策略”(Authorization Policy) 页面上设置相应的规则，选择要针对带有异常行为的任何终端执行的操作。

步骤 1 选择**策略 (Policy)** > **策略集 (Policy Sets)**

步骤 2 点击**视图 (View)** 列中与默认策略对应的箭头图标 ，打开“集”(Set) 视图屏幕，然后查看和管理默认授权策略。

步骤 3 在任意行的**操作 (Actions)** 列中，点击齿轮图标，然后从下拉列表中根据需要选择插入或复制选项，插入新的授权规则。

“策略集”(Policy Sets) 表中会显示一个新行。

步骤 4 输入规则名称。

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在**Conditions Studio 页面**中创建所需的条件。在**编辑器 (Editor)**部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性（例如，Endpoints.AnomalousBehaviorEqualsTrue）。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)**，为具有异常行为的终端设置授权策略规则。

步骤 8 点击**完成 (Done)**。

查看带有异常行为的终端

您可以使用以下任一选项查看有异常行为的终端：

- 从**主页 (Home)** > **摘要 (Summary)** > **指标 (Metrics)** 中，点击“异常行为”(Anomalous Behavior)。此操作将打开一个新选项卡，页面底部窗格中有“异常行为”(Anomalous Behavior) 列。
- 依次选择**情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **终端分类 (Endpoint Classification)**。您可以在页面的下方窗格中查看“异常行为”(Anomalous Behavior) 列。
- 您可以在“情景可视性”（Context Visibility）页面的“身份验证”（Authentication）视图或“受危害终端”（Compromised Endpoints）视图中创建新的“异常行为”（Anomarous Behavior）列，如以下步骤所述：

步骤 1 依次选择**情景可视性 (Context Visibility)** > **端点 (Endpoints)** > **身份验证 (Authentication)** 或**情景可视性 (Context Visibility)** > **端点 (Endpoints)** > **受损终端 (Compromised Endpoints)**。

步骤 2 点击页面下方窗格中的“设置”(Settings) 图标，并选中**异常行为 (Anomalous Behavior)** 复选框。

步骤 3 点击 **Go**（前往）。
您可以在身份验证或受损终端视图中查看异常行为列。

客户端设备上的代理下载问题

问题

执行用户身份验证和授权之后，客户端设备浏览器显示“no policy matched”错误消息。此问题适用于身份验证的客户端调配阶段的用户会话。

可能的原因

客户端调配策略缺失必要的设置。

安全评估代理下载问题

请记住，下载安全评估代理安装程序需要满足以下要求：

- 首次在客户端设备上安装代理时，用户必须在浏览器会话中允许 ActiveX 安装程序。（客户端调配下载页面会提示此要求。）
- 客户端设备必须接入互联网。

解决方法

- 确保Cisco ISE 中已有客户端调配策略。如果有，则验证策略中定义的策略身份组、条件和代理类型。（另外，请确认在以下位置是否配置了任何代理配置文件：**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**添加 **(Add)AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)**，包括采用所有默认值的配置文件。）

- 尝试在接入交换机上回弹端口，对客户端设备重新执行身份验证。

终端

通过这些页面，您可以配置和管理连接到您的网络的终端。

终端设置

下表介绍**终端 (Endpoints)** 窗口上的字段，您可以使用此窗口创建终端和为终端分配策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *59:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的MAC地址以静态创建终端。 MAC 地址是连接到启用Cisco ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在 Endpoints 页面静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。

字段名称	使用指南
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	Cisco ISE 包括以下系统创建的终端身份组：
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 221 页
使用策略和身份的静态分配创建终端，第 217 页

从 LDAP 设置导入终端

下表介绍“从 LDAP 导入”(Import from LDAP) 窗口上的字段，您可以使用此窗口从 LDAP 服务器导入终端。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *60:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 Cisco ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在Cisco ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与Cisco ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间（单位：秒），值介于 1 和 60 秒之间。

相关主题

已识别的终端，第 221 页
从 LDAP 服务器导入终端，第 220 页

终端分析策略设置

下表列出了**终端策略 (Endpoint Policies)** 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

表 *61:* 终端分析策略设置

字段名称	使用指南
Name	输入要创建的终端分析策略的名称。
Description	输入要创建的终端分析策略的说明。
Policy Enabled	默认情况下，**Policy Enabled** 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
Minimum Certainty Factor	输入要与分析策略相关联的最小值。默认值为 10。

字段名称	使用指南
Exception Action	选择在分析策略中定义规则时要与条件关联的例外操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 例外操作 (Exception Actions)**。
Network Scan (NMAP) Action	从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。
Create an Identity Group for the policy	选择以下选项之一以创建终端身份组： • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	选择此选项以使用现有的分析策略。 此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。 例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。

字段名称	使用指南
No, use existing Identity Group hierarchy	选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。 通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。 例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与Unknown配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入Profiled终端身份组中。例如， • 如果终端与Cisco-IP-Phone配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。 • 如果终端与Workstation配置文件相匹配，则这些终端会归入Workstation终端身份组中。 Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。
Parent Policy	选择在系统中定义的、要与新终端分析策略相关联的父分析策略。 可以选择可将规则和条件继承到其子项的父分析策略。
Associated CoA Type	选择以下要与终端分析策略相关联的CoA类型之一： • No CoA • Port Bounce • Reauth • Global Settings，该设置是从在 Administration > System > Settings > Profiling 中设置的分析器配置进行应用
Rules	在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。 策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。

字段名称	使用指南
Conditions	点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。 点击 **从库中选择现有条件 (Select Existing Condition from Library)** 或 **创建新条件（高级选项）(Create New Condition (Advanced Option))**。 **从库中选择现有条件 (Select Existing Condition from Library)**：可以通过从策略元素库中选择Cisco预定义条件来定义表达式。 **创建新条件（高级选项）(Create New Condition (Advanced Option))**：可以通过从各种系统或用户定义的字典中选择属性来定义表达式。 可以将以下其中一项与分析条件相关联： • 每种条件的可信度的整数值。 • 为该条件输入例外操作或网络扫描操作 选择以下其中一个要与分析条件相关联的预定义设置： • “可信度增加”(Certainty Factor Increases)：为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。 • “采取例外操作”(Take Exception Action)：触发在此终端分析策略的“例外操作”(Exception Action) 字段中配置的例外操作。 • “采取网络扫描操作”(Take Network Scan Action)：触发在此终端分析策略的“网络扫描 (NMAP) 操作”(Network Scan (NMAP) Action) 字段中配置的网络扫描操作。

字段名称	使用指南

Select Existing Condition from Library	可以执行以下操作：
	• 可以选择策略要素库中可用的Cisco预定义条件，然后使用 AND 或 OR 运算符添加多个条件。
	• 点击 Action 图标，在后续步骤中执行以下操作：
	  • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对
	  • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件
	  • **复制 (Duplicate)**：创建选定条件的副本
	  • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中
	  • **删除 (Delete)**：删除所选条件。

创建新条件（高级选项）	可以执行以下操作：
	• 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。
	• 点击 Action 图标，在后续步骤中执行以下操作：
	  • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对
	  • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件
	  • **复制 (Duplicate)**：创建选定条件的副本
	  • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中
	  • **删除 (Delete)**：删除所选条件。可以使用 AND 或 OR 运算符

相关主题

思科 ISE 分析服务，第 165 页

创建终端分析策略，第 210 页
使用 UDID 属性的终端情景可视性，第 241 页

使用 UDID 属性的终端情景可视性

唯一标识符 (UDID) 是终端属性，用于识别特定终端的 MAC 地址。一个终端可以有多个 MAC 地址。例如，一个 MAC 地址用于有线接口，另一个用于无线接口。AnyConnect 代理会为该终端生成 UDID，并将其保存为终端属性。 您可以在授权查询中使用 UDID。 终端的 UDID 保持不变，不会随 AnyConnect 的安装或卸载而更改。使用 UDID 时，**情景可视性 (Context Visibility)** 窗口（**情景可视性 (Context Visibility) > 终端 (Endpoints) > 合规性 (Compliance)**）会为具有多个网卡的终端显示一个条目，而不是多个。您可以确保对特定终端（而不是 MAC 地址）的安全评估控制。

注释 终端必须具有 AnyConnect 4.7 或更高版本才能创建 UDID。

适用于 Windows 和 Macintosh 终端的终端脚本向导

终端脚本向导可以让您在连接的终端上运行脚本，以执行符合组织要求的管理任务。这包括卸载过时软件、启动或终止进程或应用以及启用或禁用特定服务等任务。

终端脚本可通过终端脚本向导在 Windows 终端和 Macintosh 终端上运行。

开始之前

- 您必须具有超级管理员用户角色。
- 为Cisco ISE 配置登录凭证，以便使用管理权限访问 Macintosh 和 Windows 终端。

  在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **终端登录配置 (Endpoint Login Configuration)**，并配置以下内容：

  - Cisco ISE 可用于登录终端的域凭证。
  - 适用于 Windows 和 Macintosh 的本地用户凭证，Cisco ISE 可以使用这些凭证作为本地用户登录到终端。

    域用户优先于本地用户。如果同时配置了两者，并且需要使用本地用户凭证运行脚本，则必须删除域凭证。

- Windows 终端必须安装 Windows PowerShell 5.1 或更高版本。必须启用 PowerShell 远程处理。
- Macintosh 终端必须安装 Bash。
- Windows 终端和 Macintosh 终端都必须安装 cURL 7.34 或更高版本。
- Windows 终端和 Macintosh 终端必须连接到网络并在Cisco ISE 中具有活动会话。

步骤 1 在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**

步骤 2 点击窗口右上角的链接图标，然后从下拉列表中选择**运行终端脚本 (Run Endpoint Scripts)**。

欢迎 (Welcome) 选项卡包含指向**终端登录配置 (Endpoint Login Configuration)** 窗口的链接，用于配置登录凭证（如果尚未配置）。只有在配置登录凭证后，才能点击此选项卡右下角的**开始 (Start)** 按钮。

步骤 3 在**选择类别 (Select Category)** 选项卡中，可以根据终端的操作系统或终端上可用的应用选择终端。点击**按操作系统 (By OS)** 或**按应用 (By Application)** 单选按钮做出选择。点击 **下一步 (Next)** 继续操作。

步骤 4 在**选择终端 (Select Endpoints)** 窗口中，一个 Dashlet 会显示适用于操作系统类型或应用（如适用）的过滤器。在 Dashlet 中，点击要应用的过滤器，该过滤器的所有终端都列在一个表中。

- 要选择选定过滤器的所有终端，请选中表标题行中的复选框。
- 要选择特定终端，请选中表中该条目的复选框。要从表中查找特定终端，请点击表上方的**过滤器 (Filter)** 按钮，然后选择**快速过滤器 (Quick Filter)**。您可以按显示的任何参数进行过滤，以查找所需的终端。

注释　如果在**选择类别**步骤中选择了**按应用 (By Application)**，请记住选择属于该步骤中同一操作系统类型的终端。对于基于应用的脚本，请在终端脚本向导中为每种操作系统类型创建脚本，并为每种操作系统类型设置单独的作业。

步骤 5 选择要运行脚本的终端后，点击**下一步 (Next)**。

步骤 6 在**选择脚本 (Select Scripts)** 选项卡中，点击**添加 (Add)**。

步骤 7 点击**添加脚本 (Add Script)** 以从系统中选择脚本。点击**开始上传 (Start Upload)**，将脚本添加到**选择脚本 (Select Scripts)** 选项卡。

步骤 8 选中要运行的脚本的复选框，然后点击**下一步 (Next)**。

步骤 9 **摘要 (Summary)** 选项卡显示所选择的终端和脚本。在此处检查所做的选择，然后点击**返回 (Back)** 以更改任何详细信息。点击**完成 (Finish)** 以启动脚本运行。

系统将显示名为**终端脚本报告 (Endpoints Script Report)** 的弹出窗口，其中包含此任务的**作业 ID (Job ID)**。点击**终端脚本调配报告 (Endpoint Scripts Provisioning report)** 以重定向到包含此任务详细信息的窗口。

要查看通过终端脚本向导运行的作业报告，请选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)**。

终端脚本调配摘要报告

在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)**

“终端脚本调配摘要”(Endpoint Scripts Provisioning Summary) 窗口显示过去 30 天内通过终端脚本向导运行的作业的详细信息。点击窗口右上角的**计划 (Schedule)**，安排导出报告并跟踪较旧的报告。

点击**导出到 (Export To)** 并从下拉列表中选择一个选项，将报告的 CSV 或 PDF 版本保存到存储库或本地目标。

默认情况下，**终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)** 窗口显示包含以下列的表格：

列的名称	显示的信息
记录时间	提交作业的时间戳。
作业 **ID**	点击作业 ID 条目可查看条目的详细信息。系统将打开一个包含**终端脚本调配详细信息**的新选项卡，其中有时间戳、所选终端的 MAC 地址、每个终端的脚本状态和脚本调配状态、调配作业的 PSN 名称以及作业 ID。 **注释　　注意** ：点击 MAC 地址可查看脚本运行的详细分步信息。
管理员用户名	提交作业的管理员的名称。
操作系统	为其运行所选脚本的操作系统。
总数/成功/失败/正在进行的终端	• 所选终端的总数。 • 成功运行脚本的终端数量。 • 脚本运行失败的终端数量。 • 仍在运行脚本的终端数量。
脚本名称	作业中包含的脚本的名称。

IF-MIB

对象	**OID**
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

对象	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

对象	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

对象	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3

对象	OID
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

对象	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

对象	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

对象	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

对象	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

对象	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9

对象	OID
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

对象	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

对象	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.5

对象	OID
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

对象	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

对象	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

对象	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7

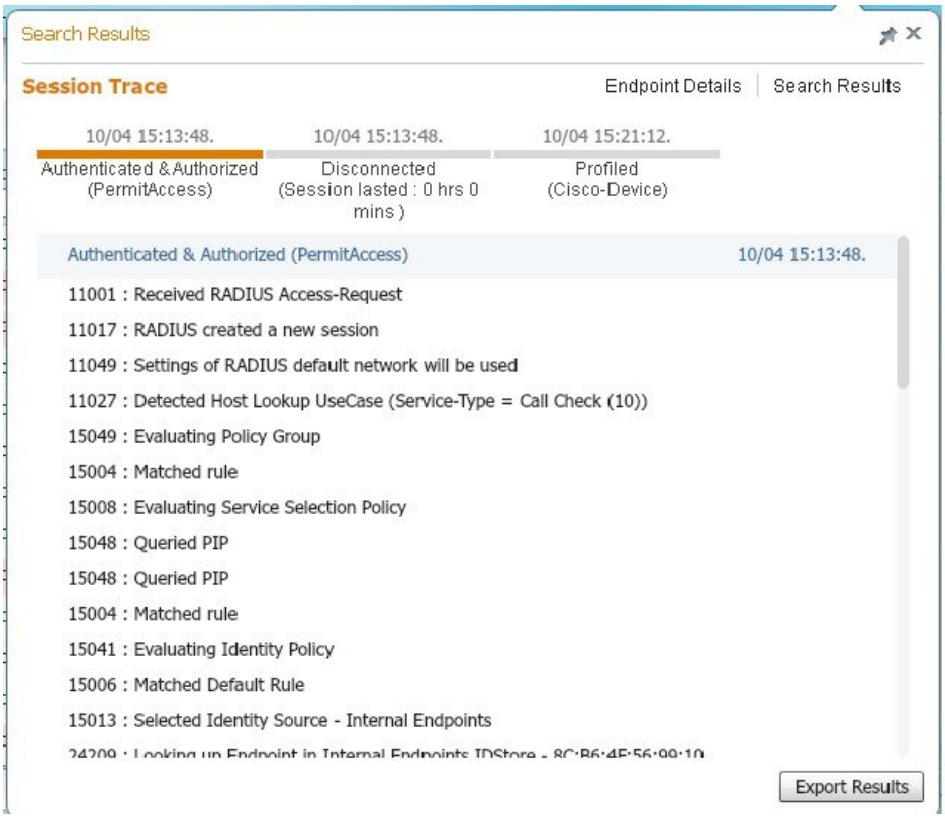
对象	OID
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

终端的会话跟踪

您可以使用Cisco ISE 首页顶部的全局搜索框来获得某个终端的会话信息。当使用条件进行搜索时，您将会看到终端列表。点击其中任意终端以查看该终端的会话跟踪信息。下图所示为终端会话跟踪信息的示例。

注释 用于搜索的数据集基于作为索引的终端 ID。因此，当进行身份验证时，对于包括在搜索结果集中的身份验证，必须具有终端 ID。

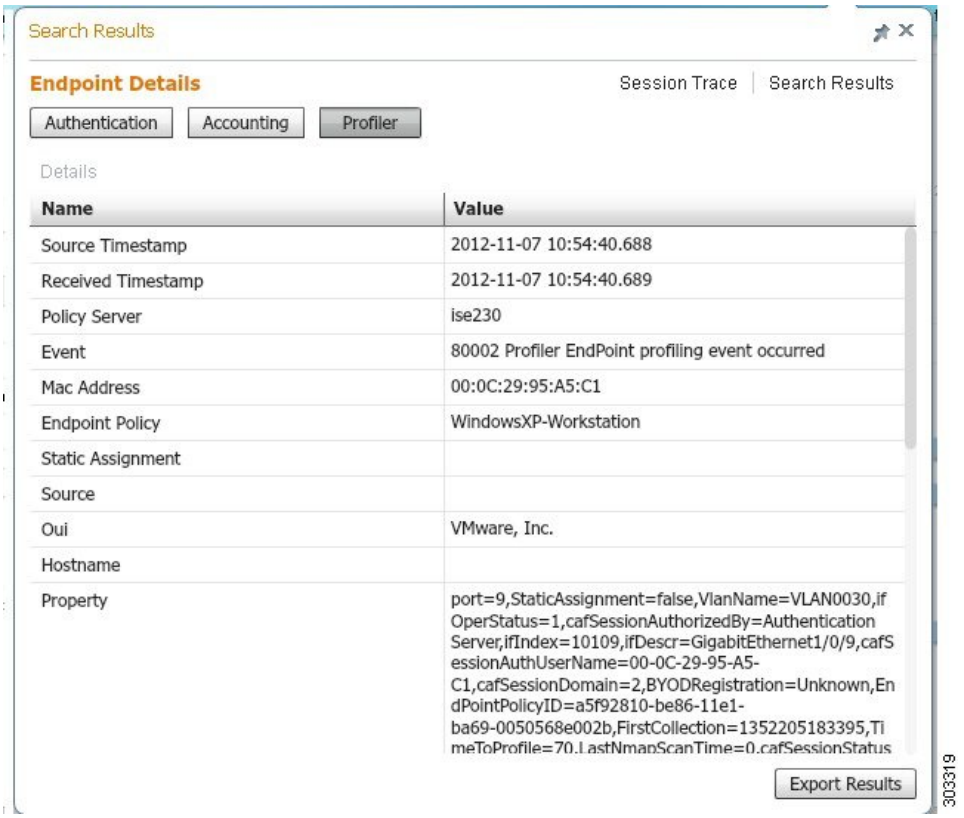
图 *17:* 终端的会话跟踪



您可以使用顶部可点击的时间表来查看主要的授权过渡。还可以使用**导出结果 (Export Results)** 选项导出 .csv 格式的结果。报告会下载到您的浏览器。

可以点击**终端详细信息 (Endpoint Details)** 链接查看特定终端的更多身份验证、记帐和分析器信息。下图所示为所显示的终端详细信息。

图 *18:* 终端详细信息



从目录清除会话

在监控和故障排除节点上，会话按以下方式从会话目录中清除：

- 已终止会话会在终止 15 分钟后清除。
- 如果存在身份验证但无记账，则此类会话将在一个小时后清除。
- 所有非活动会话在五天之后清除。

终端的全局搜索

您可以使用Cisco ISE 首页顶部的全局搜索框搜索终端。您可以使用以下任何条件搜索终端：

- 用户名
- MAC 地址
- IP 地址
- 授权配置文件

- 终端配置文件
- 失败原因
- 身份组
- 身份库
- 网络设备名称
- 网络设备类型
- 操作系统
- 安全评估状态
- 位置
- 安全组
- 用户类型

对于任何搜索条件，您应在搜索字段中至少输入三个字符以显示数据。

注释 如果终端已由Cisco ISE 进行身份验证，或其审计更新已收到，则可通过全局搜索找到该终端。搜索结果中不会显示已手动添加但未由Cisco ISE 进行身份验证或未在Cisco ISE 中说明的终端。

搜索结果提供终端当前状态的详细和概览信息，可用于故障排除。搜索结果仅显示前25个条目。建议使用过滤器缩小结果范围。

您可以使用左侧面板中的任何属性过滤结果。您也可以点击任意终端查看该终端的详细信息，例如：

- 跟踪会话
- 身份验证详细信息
- 记帐详细信息
- 安全评估详细信息
- 分析器详细信息
- 客户端调配详细信息
- 访客记帐和活动