资产可视性

使用外部身份库对思科 ISE 进行管理访问

在思科 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：没有在本地思科 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，并使用本地思科 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思科 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，思科 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)**，请求通过思科 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。思科 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，并已将思科 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，思科 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。

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。

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。

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

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。这可确保思科 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。

思科 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 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**

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)**。

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 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思科 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 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **策略 (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 **Save**。

如果您以管理员身份登录，而且思科ISE RBAC策略无法验证您的管理员身份，则思科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思科 ISE 数据库中配置相同的用户名。当您配置思科 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）仍根据思科 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思科 ISE 数据库中配置相同的用户名。

步骤 1

步骤 2 确保外部 RSA 身份库中的管理员用户名也存在于思科 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. 管理员在思科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

您可以通过这些窗口配置和管理包含思科 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

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
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。
Description	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，思科 ISE 会自动创建自定义架构。
注释　仅在您选择定制架构时，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。
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。

字段名称	使用指南
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。

注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

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	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	
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。

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)	点击此字段以对思科 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)	以秒为单位输入思科 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。
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	如果您希望思科 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)	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 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 地址格式供思科 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，当思科 ISE 收到主机查找请求时，思科 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。 如果思科 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，思科 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，则思科 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 (<)。思科 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。 如果思科 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，思科 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*，则思科 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 (<)。思科 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”。

相关主题

LDAP 目录服务，第 44 页
LDAP 用户身份验证，第 45 页
LDAP 用户查找，第 48 页
添加 LDAP 身份源，第 48 页

RADIUS 令牌身份源设置

相关主题

RADIUS 令牌身份源，第 56 页
添加 RADIUS 令牌服务器，第 60 页

RSA SecurID 身份源设置

RSA 提示设置

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

表 *6: 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。

字段名称	使用指南
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 *7: 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 61 页
思科 ISE 和 RSA SecurID 服务器集成， 第 62 页
添加 RSA 身份源， 第 64 页

思科 ISE 用户

在本主题中，用户一词是指定期访问网络的员工和承包商，以及发起人用户和访客用户。发起人用户是通过发起人门户创建和管理访客用户账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。

您必须为所有要获取对思科 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都应从管理门户创建。

从思科 ISE 版本 3.2 起，您可以选择将**启用日期 (Date Enabled)** 列（**设置 (Settings)** > **列 (Columns)** > **启用日期 (Date Enabled)**）和**密码过期前天数 (Days Until Password Expires)** 列（**设置 (Settings)** > **列 (Columns)** > **密码过期前天数 (Days Until Password Expires)**）添加到**网络访问用户 (Network Access Users)** 窗口中的**网络访问用户 (Network Access User)** 表（**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**），以便帮助您根据密码到期信息对网络访问用户进行排序。默认情况下并未添加**启用日期 (Date Enabled)** 和**密码过期前天数 (Days Until Password Expires)** 字段。您可以使用窗口中的自定义选项将它们添加到**网络访问用户 (Network Access User)** 表中。

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思科 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

思科 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 - 可以暂停或恢复思科 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思科 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

思科 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。思科 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

在**用户自定义属性设置 (User Custom Attributes Setting)** 窗口上，您可以使用**自定义属性 (Custom Attributes)** 窗格定义更多的用户帐户属性。思科 ISE 提供一系列不可配置的预定义属性。然而，通过配置下列内容，您可以定义自定义属性：

- 属性名称
- 数据类型

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 **管理** > **身份管理** > **设置** > **用户身份验证设置**中配置的。

以下部分提供有关 **密码策略** 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。思科 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两个密码中的 四个字符。

- 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。要设置密码的有效期，请选中**每__天更改密码**（**有效范围1到3650**）复选框，并在输入字段中输入天数。如果用户未在指定时间内更改密码，则可以通过选择 **禁用用户账户** 选项来禁用用户账户。选择 **下次登录时需要更改密码** ，以提示用户在下次登录思科 ISE 时更改其密码。

  要发送密码重置提醒邮件，请选中**在密码到期前 __ 天显示提醒 (Display reminder __ days prior to password expiration)** 复选框，然后输入将提醒邮件发送到为网络访问用户配置的邮件地址的提前天数。在创建网络访问用户时，您可以在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 添加网络访问用户 (Add Network Access User)** 窗口中添加邮件地址，以发送密码重置邮件通知。

注释

- 提醒邮件从以下邮件地址发送：iseadminportal@<ISE-Primary-FQDN>. 您必须明确允许该发件人的访问权限。
- 默认情况下，提醒邮件包含以下内容：您的网络访问密码将在 <密码到期日期和时间> 到期。如需帮助，请联系您的系统管理员。

  从思科 ISE 版本 3.2 开始，您可以在邮件通知的 请联系系统管理员寻求帮助 部分之后自定义邮件内容。

- **锁定/暂停账户前的错误登录尝试数**：如果登录尝试失败次数超过所指定的值，使用此选项暂停或锁定账户。有效范围为 3 到 20。
- **账号禁用策略**：配置有关何时禁用现有用户账户的规则。

相关主题

用户帐户自定义属性 ，第 14 页
添加用户 ，第 15 页

内部用户操作

添加用户

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

如果您使用思科ISE内部数据库，则必须为需要访问思科ISE中资源或服务的任何新用户创建账户。

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 **Add (+)** 以创建新用户。

步骤 3 在所有字段中输入值。

注释 用户名中不要包含空格、+ 和 * 字符。

步骤 4 点击 **Submit** 在思科 ISE 内部数据库中创建新用户。

导出思科 ISE 用户数据

您可以从思科 ISE 内部数据库中导出用户数据。思科 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 **Export Selected**。

步骤 4 在**密钥 (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 **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思科 ISE 以创建新的内部帐户。可在导入用户账号时下载模板 CSV 文件。

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，请单击**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)** 字段中，输入包含要导入的用户名的文件名，或者点击**浏览 (Browse)**，导航至文件所在的位置。

步骤 4 要创建新的用户和更新现有用户详细信息，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**。

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

表 *8:* 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 地址是连接到启用思科 ISE 的网络的接口设备标识符。

字段名称	使用指南
Static Assignment	如果您想要在“终端”(Endpoints) 窗口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。
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。
	思科 ISE 包括以下系统创建的终端身份组：
	• 黑名单
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 112 页
使用策略和身份的静态分配创建终端，第 108 页

从 LDAP 设置导入终端

表 *9:* 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 思科 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。您可以在思科 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，以确保终端策略与思科 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	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

相关主题

已识别的终端，第 112 页
从 LDAP 服务器导入终端，第 111 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)**。

步骤 2 在“名称”(Name) 字段和“描述”(Description) 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 13 页

导出用户身份组

思科 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

思科 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 **Generate a Template** 获取用于导入文件的模板。

步骤 3 点击 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 **Overwrite existing data with new data** 复选框。

步骤 5 点击 **Import**。

步骤 6 点击 **Save** 以将您的更改保存至思科 ISE 数据库。

终端身份组设置

表 *10:* 终端身份组设置

字段名称	使用指南
Name	输入您要创建的终端身份组的名称。
Description	输入对您要创建的终端身份组的说明。
Parent Group	从**父级组 (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。 思科 ISE 包括以下终端身份组： • Blacklist • GuestEndpoints • Profiled • RegisteredDevices • Unknown 此外，它还会再创建两个身份组：Cisco-IP-Phone 和 Workstation，这两个身份组与 Profiled（父）身份组关联。

相关主题

已识别终端划分为终端身份组，第 114 页
创建终端身份组，第 114 页

内部和外部身份源

身份源是存储用户信息的数据库。思科 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。

思科 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

思科 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。思科 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

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

下表列出了身份验证协议以及它们支持的外部身份源。

表 *11:* 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	ODBC
EAP-GTC，PAP（纯文本密码）	是	是	是	是	是
MS-CHAP 密码散列： MSCHAPv1/v2 EAP-MSCHAPv2（作为 PEAP 或 EAP-FAST 的内部方法） LEAP	是	是	否	否	是
EAP-MD5 CHAP	是	否	否	否	是

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	ODBC
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，可选择性地添加到授权策略条件中。	否	是	是	否	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。思科ISE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

思科 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。

步骤 1 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 23 页。
- 选择 **LDAP** 以添加 LDAP 身份源。有关更多详细信息，请参阅LDAP，第 44 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关更多详细信息，请参阅RADIUS 令牌身份源，第 56 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关更多详细信息，请参阅RSA 身份源，第 61 页。

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。思科 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

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 **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

思科 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。

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 *12: 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

思科 ISE 从 Active Directory 检索用户或设备属性和组以用于授权策略规则。这些属性可用于思科 ISE 策略并且决定了用户或设备的授权级别。思科 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。

思科 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。

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，思科 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。

基于证书的身份验证的 Active Directory 证书检索

思科 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。思科 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。思科 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。思科 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，思科 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，思科 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。

支持 Active Directory 多域林

思科 ISE 支持带多域林的 Active Directory。在每个林中，思科 ISE 连接到单个域，但如果在思科 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。

请参阅思科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。

将 Active Directory 与思科 集成的前提条件

本节介绍配置 Active Directory 以与思科 集成所需的手动步骤。但是，在大多数情况下，可以启用思科 来自动配置 Active Directory。以下是将 Active Directory 与思科 集成的前提条件。

- 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。
- 确保您在思科 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) 服务器设置来同步思科 服务器和 Active Directory 之间的时间。您可以从思科 CLI 配置 NTP 设置。
- 思科 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。
- 您必须在思科 加入到的域中具有至少一个可由思科 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	思科 机器账户
加入操作需要以下帐户权限： • 搜索 Active Directory（以查看思科 机器账户是否存在） • 将思科 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，思科 机器账户密码、SPN、dnsHostname）	退出操作需要以下帐户权限： • 搜索 Active Directory（以查看思科 机器账户是否存在） • 从域中删除思科 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 连接的思科 机器帐户需要以下权限： • 更改密码 • 读取与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 名称与思科 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，则会在思科 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思科 中。仅存储新创建的思科 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，思科 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，思科 ISE 不会再通过 Microsoft Active Directory 对用户进行身份验证。您将在思科 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。

注释 由于 Windows Server 2016 Active Directory 或更高版本以及 Windows 10 版本 1607 中的限制，会出现此问题。要克服此限制，当您将 Windows Server 2016 Active Directory 或更高版本或 Windows 10 版本 1607 与思科 ISE 集成时，您需要将以下注册表中的注册表值从非零设置为空，以提供对所有项的访问权限：Registry:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam 这允许思科 ISE 更新其计算机账户密码。

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。要确保思科 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	兼容	—
Kerberos (TCP/UDP)	88	域控制器	是 (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	兼容	—
LDAP (GC)	3268	全局目录服务器	兼容	—
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：

- 您在思科 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。
- 思科建议向 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

在您将 Active Directory 配置为外部身份源之前，请确保：

- 思科 ISE 主机名长度为 15 个字符及以下。Active Directory 不允许主机名长度超过 15 个字符。
- 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 如果您在思科 ISE 连接到 Active Directory 时发现操作问题，请查看**操作** > **报告**下的“AD 连接器操作报告”。

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 29 页
2. 配置身份验证域， 第 33 页
3. 配置 Active Directory 用户组， 第 33 页
4. 配置 Active Directory 用户和计算机属性， 第 34 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 35 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

确保思科 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。

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

步骤 3 点击**提交 (Submit)**。

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

如果已点击**否 (No)**，则保存配置将会全局保存 Active Directory 域配置（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，其中包含所有思科 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，请选中相关思科 ISE 节点旁边的复选框，然后点击**加入 (Join)** 将思科 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思科 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思科 ISE 节点，则应对每个思科 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**，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。

如果思科 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。思科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，思科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。

在配置加入点时，请注意以下几点：

- 加入完成后，思科 ISE 将更新其 AD 组和对应的安全标识符 (SID)。思科 ISE 自动启动 SID 更新过程。您必须确保允许此过程完成。
- 如果缺少 DNS 服务 (SRV) 记录，您可能无法将思科 ISE 加入 Active Directory 域（域控制器不会对您尝试加入到的域公告其 SRV 记录）。
- 建议您在指定的维护窗口后重新加入 AD。这可确保使用最新更新刷新 AD 缓存。

添加域控制器

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

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

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

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

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

步骤 5 配置域控制器：

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

b) 或者，编辑不同的域控制器字段。

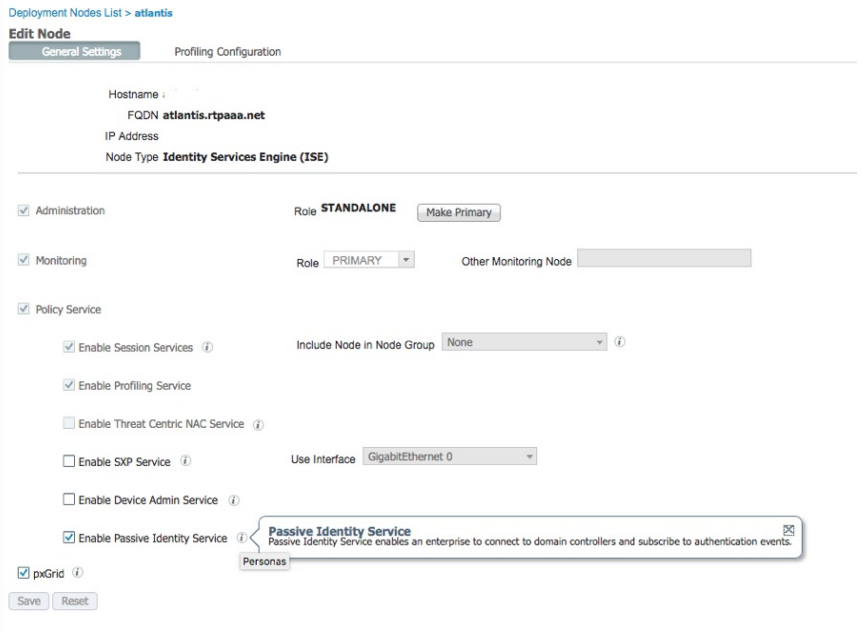
c) 如果选择 WMI 协议，请点击**配置 (Configure)**以自动配置 WMI，然后点击**测试 (Test)** 以测试连接。

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。

图 *1:*

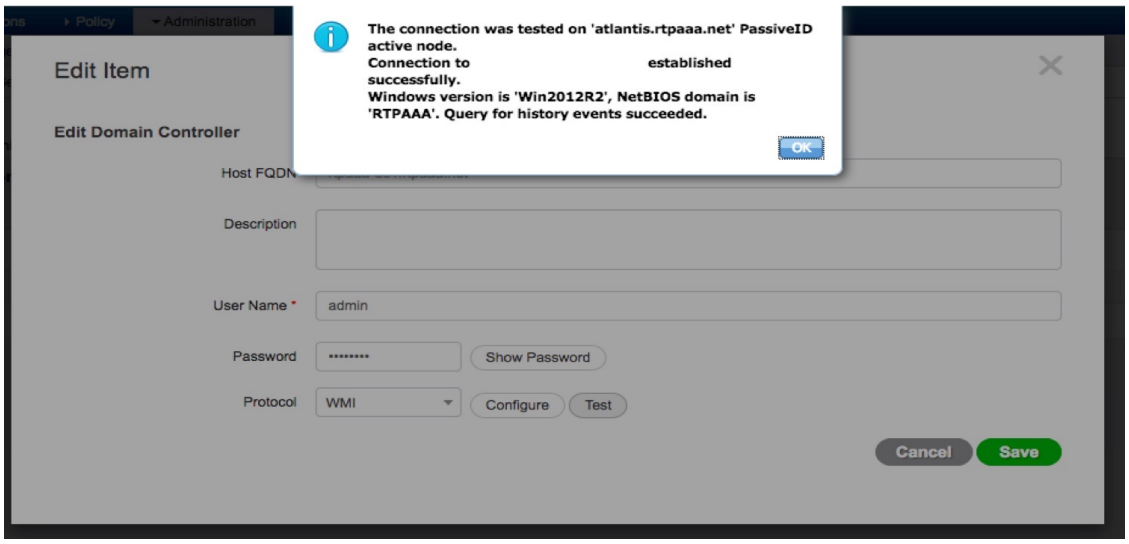


步骤 1 选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

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，其中包含所有思科 节点、节点角色及其状态。

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 (Config WMI)** 以使 能够自动配置所选的域控制器。

图 *2:*



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，请参阅将 Active Directory 与思科 集成的前提条件 ，第 26 页。

图 *3:*

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。

从命令行界面重置思科 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，从而将思科 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 域中删除思科 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。在更改思科 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** > **身份管理** > **外部身份源** > **Active Directory**。

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

步骤 3 选中思科 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)** 以退出该域并从思科 ISE 数据库中删除机器账户。

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

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

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

如果选中**退出没有凭证的域 (Leave domain without credentials)** 复选框，则主思科 ISE 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，思科 ISE 加入的域具有可视性。默认情况下，思科 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，因为这些域指示思科 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** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Active Directory** 加入点。

步骤 3 点击**身份验证域 (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，思科 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**启用已选择 (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**显示无法使用的域 (Show Unusable Domains)** 以查看无法使用的域的列表。无法使用的域是思科 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，思科 ISE 使用安全标识符 (SID) 帮助解决组名称不明确问题和增强组映射。SID 提供准确的组分配匹配。

步骤 1 选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击**组 (Groups)** 选项卡。

步骤 3 执行以下操作之一：

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

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

对于用户界面登录，请勿在组名称中使用双引号 (”)。

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

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

步骤 6 如果您选择手动添加组，请为新组输入名称和 SID。

步骤 7 点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

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

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**属性 (Attributes)** 选项卡。

步骤 3 依次选择**添加 (Add)** > **添加属性 (Add Attribute)**以手动添加属性，或者依次选择**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。

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 (Sample User or Machine Account)** 字段中输入用户的名称，然后点击**检索属性 (Retrieve Attributes)** 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，确保从思科 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

您必须将思科 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 29 页。

步骤 1 选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 选中相关思科 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 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。

对 Active Directory 多加入配置的支持

思科 ISE 支持对 Active Directory 域执行多加入。思科 ISE 最多支持 50 个 Active Directory 加入。思科 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。

思科 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：在思科 ISE 中，每个到 Active Directory 域的独立加入都叫作一个加入点。Active Directory 加入点是思科 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，节约了思科 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。

  当您执行思科 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，思科 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。如果您要选择思科 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 依次选择 **Administration** > **Identity Management** > **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思科 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。思科 ISE 将匹配条件标记，在发现第一个匹配项时，思科 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。此规则指示思科 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。此规则指示思科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。此规则指示思科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。此规则指示思科 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。此规则指示思科 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。此规则指示思科 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

您必须将思科 ISE 加入到 Active Directory 域。

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **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。思科 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。在思科 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，思科 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

您必须将思科 ISE 节点加入到 Active Directory 域。

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **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，而思科 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。这是默认选项。

- **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。

根据身份验证域在思科 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”）。

如果思科 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。

对用户进行 Active Directory 身份验证测试

“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** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 选择以下选项之一：

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

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

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

步骤 5 如果您是对所有加入点运行此测试，请选择要对其运行此测试的思科 ISE 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**测试 (Test)**。
系统将显示测试操作的结果和步骤。这些步骤可帮助确定故障原因并进行故障排除。

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 > 身份管理 > 外部身份源 > **Active Directory**。

步骤 2 选中已配置的 Active Directory 旁边的复选框。

步骤 3 检查并确保列出的本地节点状态为未加入。

步骤 4 点击删除 **(Delete)**。

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

查看节点的 Active Directory 加入

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

步骤 1 选择管理 > 身份管理 > 外部身份源 > **Active Directory**。

步骤 2 点击**节点视图 (Node View)**。

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

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

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

诊断 Active Directory 问题

诊断工具是在每个思科 ISE 节点上运行的服务。当思科 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。

思科 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思科 ISE 连接到 Active Directory 的前提条件。该工具有助于检测网络、防火墙配置、时钟同步、用户身份验证等问题。此工具以逐步操作指南的形式工作，并帮助您根据需要解决中间每层的问题。

步骤 1 选择管理 > 身份管理 > 外部身份源 > **Active Directory**。

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

步骤 3 选择要运行诊断的思科 ISE 节点。

如果未选择思科 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 点击**在所有节点上运行测试 (Run All Tests on Node)** 开始测试。

步骤 6 点击**查看测试详情 (View Test Details)** 查看具有警告或失败状态的测试的详细信息。
下表允许您重新运行特定测试、停止正在运行的测试和查看特定测试的报告。

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 调试信息的思科 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 依次选择**操作** > **故障排除** > **下载日志**。

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

思科 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 身份验证报告”(RADIUS Authentications Report)：此报告显示 Active Directory 身份验证和授权的详细步骤。您可以在以下位置找到此报告：**操作 (Operations)** > **报告 (Reports)** > **身份验证服务状态 (Auth Services Status)** > **RADIUS 身份验证 (RADIUS Authentications)**。
- “AD 连接器操作报告”(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，例如思科 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。您可以在以下位置找到此报告：**操作 (Operations)** > **报告 (Reports)** > **身份验证服务状态 (Auth Services Status)** > **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，用于在思科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。

使用 Active Directory 设置思科 ISE 的补充信息

要使用 Active Directory 配置思科 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

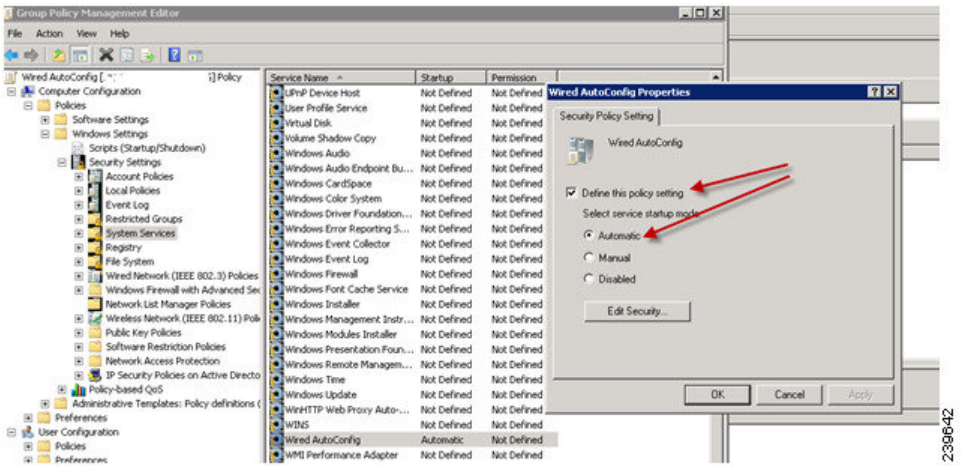
有关如何访问组策略管理编辑器的详细信息，请参阅 Microsoft Active Directory 文档。

步骤 1 打开组策略管理编辑器，如下图所示。

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。

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。



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。

为机器身份验证配置代理

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。

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。

思科 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，可以将思科 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，组成对应于一个思科 ISE LDAP 身份源实例的一个 LDAP 实例。

思科 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，思科 ISE 为该组合提交身份验证请求。

LDAP 故障切换

思科 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，导致思科 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思科 ISE 尝试连接的第一个 LDAP 服务器无法访问，思科 ISE 始终会尝试连接第二个LDAP服务器。如果您希望思科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 思科 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。根据故障切换配置，思科 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

思科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。

思科 ISE 会为思科 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。思科 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，思科 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。

注释

- 思科 ISE 会为每个用户身份验证发送两条 searchRequest 消息。这不会影响思科 ISE 授权或网络性能。第二个 LDAP 请求用于确保思科 ISE 与正确的身份通信。
- 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。

在授权策略中使用的 LDAP 组和属性检索

思科 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，思科 ISE 可以在必要时检索属于主题的组和属性。通过选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**，您可以在思科 ISE 管理员门户中配置要检索的属性。思科 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，思科 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，思科 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 (Groups Refer to Subjects)：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 (Subjects Refer to Groups)：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 (Reference direction)：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 (Group map attribute)：此参数指示包含组成员身份信息的属性。
- 组对象类 (Group object class)：此参数确定特定对象可识别为组。
- 组搜索子树 (Group search subtree)：此参数指示用于组搜索的搜索库。

- 成员类型选项 (Member type option)：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，思科 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，思科 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，则思科 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，当转换失败或思科 ISE 未检索到任何属值时，思科 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，那么思科 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 - 思科 ISE 会在思科 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思科 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

思科 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

思科 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。
- 思科 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 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 **Submit** 以创建 LDAP 实例。

LDAP 身份源设置

LDAP 常规设置

下表介绍常规 (General) 选项卡上的字段。

表 *13: LDAP* 常规设置

字段名称	使用指南
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。
Description	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，思科 ISE 会自动创建自定义架构。
注释　仅在您选择定制架构时，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。
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。

字段名称	使用指南
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。

注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

LDAP 连接设置

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

表 *14: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器	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	
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。

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)	点击此字段以对思科 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)	以秒为单位输入思科 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。
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	如果您希望思科 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)	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 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 ***15: 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 地址格式供思科 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，当思科 ISE 收到主机查找请求时，思科 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。 如果思科 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，思科 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，则思科 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 (<)。思科 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。 如果思科 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，思科 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*，则思科 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 (<)。思科 ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *16: 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 *17: 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”。

相关主题

LDAP 目录服务，第 44 页
LDAP 用户身份验证，第 45 页
LDAP 用户查找，第 48 页
添加 LDAP 身份源，第 48 页

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 选择在思科 ISE GUI 中，点击**菜单**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 **Submit** 保存连接参数。

允许思科 ISE 从 LDAP 服务器获取属性

为了让思科 ISE 从 LDAP 服务器获取用户和组数据，您必须在思科 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 选择在思科 ISE GUI 中，点击**菜单**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 **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 **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 选择在思科 ISE GUI 中，点击**菜单**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)** 可添加新组，或选择**添加 (Add)** > **从目录选择组 (Select Groups From Directory)** 可从 LDAP 目录选择组。

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 **Edit**。

步骤 3 点击 **Attributes** 选项卡。

步骤 4 选择**添加 (Add)** > **添加属性 (Add Attribut)** 添加新属性，或选择**添加 (Add)** > **从目录中选择属性 (Select Attributes From Directory)** 以便从 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。

步骤 5 选中想要选择的属性旁边的复选框，然后点击 **OK**。

步骤 6 点击 **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，思科 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（思科 ISE 身份验证）：无（在 SSL 隧道中使用管理员绑定）
- 密码套件：思科 ISE 支持的所有密码套件

我们建议您使用带有思科 ISE 支持的最强加密和密码的 TLS v1。

要使思科 ISE 与 LDAP 身份源安全通信，请执行以下操作：

开始之前

- 思科 ISE 必须连接到 LDAP 服务器
- TCP 端口 636 应当开放

步骤 1 将向 LDAP 服务器签发服务器证书的 CA 的完整证书授权 (CA) 链导入思科 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 配置思科 ISE 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。

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。

思科 ISE 支持任何符合 RADIUS RFC 2865 的服务器作为外部身份源。思科 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。 RADIUS 身份源将用户数据报协议 (UDP) 端口用于身份验证会话。所有 RADIUS 通信都使用同一 UDP 端口。

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，思科 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。为了让思科 ISE 将 RADIUS 一次性密码 (OTP) 消息发送到已启用 RADIUS 的令牌服务器，必须确保思科 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

您在思科 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切换

思科 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。当思科 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

思科 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。思科 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思科 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。

思科 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思科 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。您还必须启用身份缓存选项并以分钟为单位设置老化时间。在指定的时间内，内存中可提供缓存。

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。思科 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。思科 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 *18:* 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 服务器在思科 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

思科 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。思科 ISE 适用于各种令牌服务器。在配置 SafeWord 服务器时，您必须选中思科 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

当思科 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）

思科 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

相关主题

RADIUS 令牌身份源，第 56 页
添加 RADIUS 令牌服务器，第 60 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 选择在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择 **管理 (Administration)** **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。思科 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 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 令牌服务器向思科 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 5 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 选择在思科 ISE GUI 中，点击**菜单**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 **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

思科 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。

思科 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。

思科 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。

思科 ISE 仅支持一个 RSA 领域。

思科 ISE 和 RSA SecurID 服务器集成

以下是将思科 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
- 思科 ISE 管理员：将思科 ISE 配置为连接到 RSA SecurID 服务器并维护配置

本节介绍将思科 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思科 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思科 ISE 中。通过复制过程，主要思科 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

在所有思科 ISE 服务器上安装 sdconf.rec 文件之后，RSA 代理模块进行初始化，并且每个思科 ISE 服务器上都将使用 RSA 生成的凭证进行身份验证。在部署中的每个思科 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。此文件位于思科 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

管理分布式思科 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

在思科 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思科 ISE。在思科 ISE 中的复制流程将更新的文件分布到部署中的辅助思科 ISE 服务器。思科 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。思科 ISE 服务器和 RSA SecurID 服务器通过代理模块运行。位于思科 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

为该领域的每个思科 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。位于思科 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思科 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）。可以使用思科 ISE 管理门户从该领域的思科 ISE 服务器中删除此文件。思科 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，此文件位于思科 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思科 ISE 服务器中删除此文件。思科 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

RSA 提示设置

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

表 *19: 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。

字段名称	使用指南
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 *20: 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 61 页
思科 ISE 和 RSA SecurID 服务器集成，第 62 页
添加 RSA 身份源，第 64 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，才能在思科 ISE 中添加 RSA 身份源。

步骤 1 选择在思科 ISE GUI 中，点击**菜单**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 **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，思科 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 **Save**。

思科 ISE 也支持以下场景：

- 为思科 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 登录思科 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思科 ISE 服务器的 sdopts.rec 文件。

步骤 4 点击特定思科 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 **OK**。

步骤 7 点击与思科 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

您可以指定思科 ISE 如何定义身份验证失败和启用身份缓存。RSA 身份源不会区分“Authentication failed”和“User not found”错误，并且会发送 Access-Reject 响应。

您可以定义在处理请求和报告失败时思科 ISE 应如何处理此类失败。身份缓存让思科 ISE 可以第二次处理在思科 ISE 服务器上验证失败的请求。缓存中具有从上一次身份验证检索的结果和属性。

配置 RSA 提示

思科 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 选择在思科 ISE GUI 中，点击**菜单**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

通过思科 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 选择在思科 ISE GUI 中，点击**菜单**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)**。

身份源序列

身份源序列定义思科 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思科 ISE 的数据库中有用户信息，您可以定义您希望思科 ISE 在这些身份源中查找信息的顺序。找到匹配后，思科 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

确保您已经在思科 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 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，调整为您希望思科 ISE 搜索数据库的顺序。

步骤 6 如果无法访问所选身份库进行身份验证，请在 **高级搜索列表** 区域中选择以下选项之一：

- **请勿访问序列中的其他库并将 “AuthenticationStatus” 属性设置为 “ProcessError”**
- **将用户视为未找到，然后继续到序列中的下一个库**

  在处理请求时，思科 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思科 ISE 搜索身份源的顺序。

步骤 7 点击 **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 **OK** 删除一个或多个身份源序列。

报告中的身份源详细信息

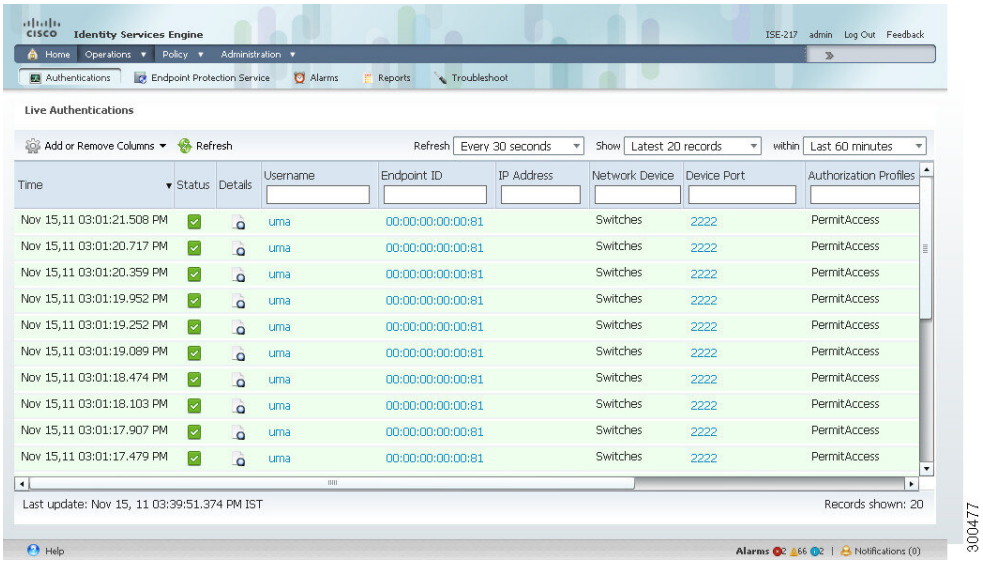
思科 ISE 通过 Authentications dashlet 报告和 Identity Source 报告提供关于身份源的信息。

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。

下图显示 Authentications 页面，并突出显示您必须点击才能深入了解详细信息的放大镜图标。

图 *4: Authentications* 页面



身份源报告

思科 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（在思科 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。思科 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思科 ISE 中的订用从指定思科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。此页面的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)**。

表 *21:* 分析器条件设置

字段名称	使用指南
Name	分析器条件的名称。
Description	分析器条件的说明。
Type	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。
Operator	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)**：在部署时由思科 ISE 提供的分析条件标识为“思科提供”(Cisco Provided)。您不能从系统编辑或删除这些条件。 • **管理员创建 (Administrator Created)**：您以思科 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 70 页

分析器条件，第 89 页
分析器源服务，第 116 页
创建分析器条件，第 96 页

思科 ISE 分析服务

思科身份服务引擎(ISE)中的分析服务能够识别连接到网络的设备及其位置。它根据在思科ISE中配置的终端分析策略来分析终端。然后，思科 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。

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，以及在思科 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

思科 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思科 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

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思科 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思科 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思科 ISE 节点上运行，不在承担管理和监控角色的其他思科 ISE 节点上运行。

步骤 1

步骤 2 选择承担策略服务角色的思科 ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击 **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。

步骤 6 点击 **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，您可以使用思科 ISE 数据库中的终端匹配配置文件创建或更新终端。

思科 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，则可以通过在思科 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。当在思科 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。

思科 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

思科 ISE 分析器使用思科 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思科 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 属性以在思科 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，思科 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。

思科 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思科 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“思科 ISE NetFlow 流程记录和导出格式内容信息”。

DHCP 探测功能

在思科 ISE 部署中，动态主机配置协议探测功能允许思科 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 *22:* 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 数据包转发至思科 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 帮助程序命令指向思科 ISE 策略服务节点。

DHCP SPAN 探测功能

当在思科 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 服务器向思科 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。

思科 ISE 同时在端口 80 和端口 8080 上侦听来自 Web 浏览器的通信。思科 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

思科 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，在该端口上思科 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。由于思科 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) 上部署思科 ISE，思科 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，请将您为思科 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，思科 ISE 分析器会同时收集 DHCP 流量和 HTTP 流量。

pxGrid 探测器

pxGrid 探测器利用思科 pxGrid 从外部源接收终端情景。在早于思科 ISE 2.4 的版本中，思科 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。当在思科 ISE 2.4 中引入 pxGrid 探测器后，其他解决方案将充当发布程序，思科 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 *23:* 终端资产主题

属性名称	Type	Description
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)。在思科 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

您可以将思科 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。

思科 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，请参阅从思科 IOS 传感器嵌入式交换机收集属性，第 87 页和支持思科 IOS 传感器的网络访问设备的配置核对表，第 88 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 *24:* 使用 *RADIUS* 探测功能收集的常见属性

用户名 (User Name)	正在呼叫站 ID	已呼叫站 ID	成帧的 IP 地址
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

网络扫描 (NMAP) 探测功能

通过思科 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思科 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 **Click** 按钮查看最新扫描结果链接，了解存储于 **Administration** > **Identities** > **Latest Network Scan Results** 位置的最新网络扫描结果。

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 *25:* 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 82 页。

最新网络扫描结果

最新网络扫描结果存储位置为：管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 最新网络扫描结果 (Latest Manual Network Scan Results)。

最新网络扫描结果终端 (Latest Network Scan Results Endpoints) 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。

思科 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

您的思科 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)。在启用思科 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思科 ISE 时，系统将提示您运行设置实用程序以配置思科 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。您也可以在部署思科 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 探测功能对您在思科 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

在桥接模式下通过 Inline Posture 节点部署执行 DNS 查找

要在桥接模式下配合 Inline Posture 部署使用域名服务探测功能，您必须为无线 LAN 控制器 (WLC) 配置在 RADIUS 消息中发送的 callStationIdType 信息。RADIUS 消息中的 Framed-IP-Address 属性不包含 MAC 地址格式的呼叫站 ID 类型。因此，RADIUS 消息不能与终端的 MAC 地址关联，DNS 探测功能也无法执行反向 DNS 查找。为了分析终端，您必须在思科 ISE 中启用 RADIUS 和 DNS 探测，然后将 WLC 配置为在 RADIUS 消息中以 MAC 地址格式（而不是当前的 IP 地址格式）发送呼叫站 ID。必须将 WLC 配置为在 RADIUS 消息中以 MAC 地址格式（而不是当前的 IP 地址格式）发送呼叫站 ID。在 WLC 中配置 callStationIdType 后，该配置会使用选定的呼叫站 ID 与 RADIUS 服务器及其他应用进行通信。该配置引发终端身份验证后，DNS 探测功能会根据指定名称服务器执行反向 DNS 查找（FQDN 查找）并更新终端的 FQDN。

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《思科无线 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《思科无线 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 在 FIPS 模式下运行思科 ISE 时，请选中 **AES Key Wrap** 复选框。

步骤 6 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，您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
- 针对思科发现协议信息，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思科发现协议（默认情况下）。如果在网络设备的任意端口上禁用思科发现协议，则可能会因为缺少有关所有已连接终端的思科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 命令来全局启用思科发现协议，或通过在网络接入设备的任意接口上使用 cdp enable 命令来启用思科发现协议。要禁用网络设备或接口上的思科发现协议，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

思科 ISE 分析器使用 SNMP 查询收集 LLDP 属性。您也可以使用 RADIUS 探测功能从思科 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 *26:* 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终端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。

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思科 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思科 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 并非所有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思科 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 依次选择在思科 ISE GUI 中，点击**菜单**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思科 ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击 **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 **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

思科 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 如果一个端口有多个活动会话，分析服务会通过**重新验证 (Reauth)** 选项发布 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，思科 ISE 分析器仅保留允许的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 86 页和针对 ISE 数据库持久性和性能的属性过滤器，第 85 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 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。如果您在思科 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 102 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，我们建议您在思科 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。

如果您已在思科 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思科 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，思科 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“终端”(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，思科 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，思科 ISE 中都不会发出 CoA。

注释 No CoA 和 Reauth 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 *27:* 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
思科 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

思科 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。

思科 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)** 会使思科 ISE 分析器仅保留允许的属性并丢弃所有其他属性。

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 82 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) 等在思科 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 *28:* 允许的属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
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	—

从思科 IOS 传感器嵌入式交换机收集属性

思科 IOS 传感器集成允许思科 ISE 运行时间和思科 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。

思科 IOS 传感器嵌入式网络接入设备

将思科 IOS 传感器嵌入式网络接入设备与思科 ISE 集成涉及以下组件：

- 思科 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：

  - 分析器可以部署在思科 ISE 中
  - 分析器可以作为传感器嵌入在交换机中

支持思科 IOS 传感器的网络访问设备的配置核对表

本节概述您必须在支持思科 IOS 传感器的交换机上和思科 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。

- 确保在思科 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 记帐消息添加思科 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 记帐消息添加思科 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思科 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。

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 页面列出思科 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：

- “思科提供”(Cisco Provided)：思科 ISE 包含部署时预定义的分析条件，在“分析器条件”(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“思科提供”(Cisco Provided) 条件：**策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (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。

- “管理员创建”(Administrator Created)：您以思科 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“管理员创建”(Administrator Created) 条件。您可以使用**分析器条件 (Profiler Conditions)** 窗口中的分析字典，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，从而限制思科 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。思科 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，这些扫描是思科 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。思科为最常见的 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)**。

步骤 2 点击 **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 OS (Scan OS)：扫描操作系统
- 扫描 SNMP 端口 (Scan SNMP Port)：扫描 SNMP 端口（161、162）
- “扫描通用端口”(Scan Common Port)：扫描通用端口。

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%，思科 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 *29:* 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 *30:* 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 *31:* 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 *32*: 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

创建分析器条件

思科 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，思科 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 97 页中所描述的字段的值。

步骤 3 点击 **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，而思科 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

表 *33:* 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。
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。

字段名称	使用指南
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 • 端口重启 • 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。
条件	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 **Select Existing Condition from Library** 或 **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思科预定义条件来定义表达式。 **创建新条件 (Create New Condition)**（高级选项）：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思科预定义条件，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)**：可以添加思科预定义条件 • **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。
Create New Condition (Advance Option)	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)**：可以添加思科预定义条件 • **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 70 页
创建终端分析策略，第 100 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。您可能需要注销思科 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 选择 **策略 (Policy)** > **分析 (Profiling)** > **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。

注释 创建自定义分析策略时，必须考虑以下注意事项：

- 如果自定义策略中配置的相同属性已被默认分析策略配置为评估对象，并且默认分析策略的确定性因素 (CF) 大于自定义策略，则自定义分析策略将永远不会被分配给任何终端。这是因为 CF 增幅较高的分析政策将优先于 CF 增幅较低的其他政策。
- 许多默认分析策略都被配置为 10、20 和 30 的 CF 增量。

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

除了思科 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 *34:* 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
端口重启	Port Bounce	No CoA	端口重启	Re-Auth
Reauth	Reauth	No CoA	端口重启	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 选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击 **Import**。

步骤 3 点击 **Browse**，找到您之前导出而现在想要导入的文件。

步骤 4 点击 **Submit**。

步骤 5 单击**分析器策略列表 (Profiler Policy List)** 链接，返回**分析策略 (Profiling Policies)** 窗口。

导出终端分析策略

您可以将终端分析策略导出到其他思科 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 选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 选择 **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)** 窗口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)** 窗口中的所有分析策略。

步骤 3 单击**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

部署思科 ISE 时，思科 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，**分析策略 (Profiling Policies)** 窗口显示设备的通用（母）策略列表，“分析策略”(Profiling Policies) 列表窗口显示与母策略关联的子策略。

无论是否启用以用于验证，**分析策略 (Profiling Policies)** 窗口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：

- “思科提供”(Cisco Provided)：在思科 ISE 中预定义的终端分析策略被识别为“思科提供”(Cisco Provided) 类型。

- “管理员已修改”(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“管理员已修改”(Administrator Modified) 类型。思科 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。

- “管理员已创建”(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“管理员已创建”(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 是一个适用于所有思科设备的通用终端分析策略，适用于思科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 思科 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“思科提供”(Cisco Provided)。如果管理员修改的策略被删除，它会恢复为以前的思科提供的策略。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，思科 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。

- 您无法删除思科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 是用于思科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思科 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

思科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。

思科 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思科 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思科 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：

- 在思科 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。
- 当思科 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，思科 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，思科 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，思科 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思科提供还是由管理员创建。一个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。思科 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、思科 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。

步骤 1 选择 **政策 (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 - 您不能删除思科提供的例外操作。当您要在思科 ISE 中分析终端时，思科 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思科 ISE 网络中从 Edit 页面向已知配置文件分配终端时，在思科 ISE 中会触发例外操作并且会发出 CoA。
  - FirstTimeProfiled - 当在思科 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，但是在思科 ISE 网络中该终端身份验证未成功，则在思科 ISE 中会触发例外操作并且会发出 CoA。
- Administrator-created - 思科 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思科 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 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 **Name** 和 **Description** 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 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **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

您可以从已从思科 ISE 服务器为其导出终端的 CSV 文件或者从思科 ISE 创建并使用终端详情更新的 CSV 文件导入终端。

文件格式必须是在默认导入模板指定的格式，使终端列表看起来如下所示：MAC、Endpoint Policy、Endpoint Identity Group。

对于在CSV文件中导入终端，终端策略和终端身份组都是可选的。如果想要导入终端身份组而不导入终端的终端策略，值依然用逗号分隔。

例如，

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4

步骤 1 选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)** > **导入 (Import)**。

步骤 2 点击 **Import From File**。

步骤 3 点击 Browse，找到已从思科 ISE 服务器导出的 CSV 文件或者以指定文件格式创建并使用终端更新的 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Generate a Template 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。此文件位于**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)** > **导入 (Import)** > **从文件导入 (Import From File)**。您可以使用 Generate a Template 链接创建模板，并且思科 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 列。

您必须更新终端的 MAC 地址、终端分析策略和终端身份组并以不同文件名保存该文件以用于导入终端。请参阅您使用 Generate a Template 时创建的 template.csv 文件中的标题行。

表 *35: CSV* 模板文件

MAC	终端策略	终端身份组
00:1f:f3:4e:c1:8e	Cisco-Device	RegisteredDevices

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，则这些终端会在思科 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，了解思科 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，以及思科 ISE 如何重新分析未分配的终端。

表 *36: Unknown* 配置文件：从文件导入

MAC 地址	思科 ISE 中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	未知	Xerox-Device
00:00:00:00:01:03	未知	Xerox-Device
00:00:00:00:01:04	未知	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

静态分配导入过程中保留的终端的策略和身份组

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静态分配，则在导入过程中不会对其重新分析。请参阅以下内容，了解思科 ISE 如何保留 Cisco-Device 配置文件，即在导入过程中静态分配终端。

表 *37:* 静态分配：从文件导入

MAC 地址	思科 ISE 中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Cisco-Device（静态分配）	Cisco-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，因为思科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 *38:* 无效配置文件：从文件导入

MAC 地址	思科ISE中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	未知	Xerox-Device
00:00:00:00:01:05	如果向无效配置文件而不是向思科 ISE 中可用的配置文件分配 00:00:00:00:01:05 等终端，则思科 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。	因为思科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。如果思科 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 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **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)**。

以 CSV 文件导出终端

您可以使用 CSV 文件导出所有终端，或者只导出所选的终端。列出的终端将包括其 MAC 地址、终端分析策略以及为其分配的终端身份组。

注释 要将从一个部署导出的终端自定义属性导入到另一个中，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，并使用与原始部署中相同的数据类型。

默认选项为**全部导出 (Export All)**。如果已在**终端 (Endpoints)** 窗口中过滤终端，则当使用**全部导出 (Export All)** 选项时，系统只会导出过滤的终端。默认情况下，profiler_endpoints.csv 是 CSV 文件，而 Microsoft Office Excel 是默认应用，用于从 Opening profiler_endpoints.csv 对话框打开 CSV 文件，或保存 CSV 文件。例如，您可以在 profiler_endpoints.csv 文件中导出选定的终端或所有终端，也可以使用该文件导入上述终端。

要使用 CSV 文件导出终端，请执行以下操作：

步骤 1 选择 **选择管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 从**导出 (Export)** 下拉列表中，选择以下选项之一：

步骤 3 单击**确定 (OK)** 以保存 CSV 文件。

导出的电子表格中的大多数属性都很简单。以下属性需要说明：

- *UpdateTime*：由于终端属性更改，分析器上次更新终端的时间。如果自终端会话启动以来没有更新，则值为 0。在更新期间，它将短暂为空

- *InactivityTime*：终端处于活动状态后的时间。

已识别的终端

思科 ISE 显示已识别的终端，这些终端在**终端 (Endpoints)** 窗口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 地址在思科 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。思科 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

思科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。重要属性是指思科 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。

以下是重要属性：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment

- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

当您在思科 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

思科 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。如果您未在思科 ISE 中定义节点组，系统会假定所有节点都处于同一集群中。

思科 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

思科ISE将其所发现的终端划分至相应的终端身份组。思科ISE拥有若干个系统定义的终端身份组。您还从**终端身份组 (Endpoint Identity Groups)** 窗口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 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 单击**添加**。

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 **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

思科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，在思科 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，思科 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，思科 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

思科 ISE 创建以下终端身份组：

- 黑名单：此终端身份组包括思科 ISE 中静态分配给此组的终端和在设备注册门户中列入阻止名单的终端。可以在思科 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。
- Profiled：此终端身份组包括思科 ISE 中除思科 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。终端在思科 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。您可以在思科 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，而且思科 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。

- Unknown：此终端身份组包括与思科 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，思科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思科 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 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 **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，思科 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，在思科 ISE 中，以下位置默认提供适用于所有类型思科 IP 电话的授权规则：**策略 (Policy)** > **授权 (Authorization)** > **标准 (Standard)**。

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。

分析器源服务

分析器条件、例外操作和NMAP扫描操作分类为由思科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思科提供、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思科提供的条件、例外操作和NMAP扫描操作。无法删除由思科提供的终端策略。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思科提供的最新版本策略。

可以从思科源服务器检索新的和更新后的策略及更新的 OUI 数据库。必须已订阅思科 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思科，这有助于思科改进源服务。

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

默认情况下，分析器源服务被禁用，并且需要 Plus 许可证启用该服务。启用分析器源服务时，思科 ISE 会在本地思科 ISE 服务器时区每天凌晨 1:00 下载策略和 OUI 数据库更新。思科 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。

配置分析器源服务

分析器源服务会从思科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。

您可以将思科 ISE 配置为将匿名的馈送服务使用情况报告发回思科，这会向思科发送以下信息：

- Hostname：思科 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：思科提供的配置文件计数

- UserCreatedProfiles：用户创建的配置文件计数

您可以更改由思科提供分析策略中的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。

开始之前

分析器源服务只可以从分布式部署中的思科 ISE 管理门户或在独立 ISE 节点中配置。

如果您计划从管理门户发送有关馈送更新的邮件通知，请设置简单邮件传输协议 (SMTP) 服务器 (**Administration** > **System** > **Settings**)。

步骤 1 选择 **管理 (Administration)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**，然后检查是否已启用 **Verisign Class 3 Public Primary Certification Authority** 和 **Verisign Class 3 Server CA - G3**。

步骤 2 择**管理 (Administration)** > **FeedService** > **分析器 (Profiler)**。

步骤 3 选中 **Enable Profiler Feed Service** 复选框。

步骤 4 在 Feed Service Scheduler 部分以 HH:MM 格式（思科 ISE 服务器的本地时区）输入时间。默认情况下，思科 ISE 源服务安排在每天凌晨 1.00 点运行。

步骤 5 选中 Administrator Notification Options 部分中的 **Notify administrator when download occurs** 复选框，然后在 **Administrator email address** 文本框中输入您作为思科 ISE 管理员的邮箱地址。

步骤 6 选中 Feed Service Subscriber Information 部分中的 **Provide subscriber information to Cisco** 复选框，然后输入您作为思科 ISE 管理员的详细信息，以及作为备用思科 ISE 管理员的详细信息。

步骤 7 点击 **Accept**。

步骤 8 点击 **Save**。

步骤 9 点击 **Update Now**。

指示思科ISE联系思科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，某些当前连接到思科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，**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配置窗口，然后返回此窗口。

步骤 10 点击 **Yes**。

相关主题

离线配置分析器源服务

删除终端分析策略的更新

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，但 OUI 更新不会更改。

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 选择 **选择管理 (Administration)** > **FeedService** > **分析器 (Profiler)**。

步骤 2 选中 **Enable Profiler Feed Service** 复选框。

步骤 3 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 4 点击 **Undo Latest**。

分析器报告

思科 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

思科 ISE 与思科 NAC 设备集成

思科 ISE 仅支持与思科网络准入控制 (NAC) 设备版本 4.9 集成，并在思科 ISE 中已安装高级或无线许可证时可用。

思科 ISE 分析器类似于管理思科 NAC 部署中的终端的思科网络准入控制 (NAC) 分析器。通过此集成，您可以替换安装在思科 NAC 部署中的现有思科 NAC 分析器。您还可以将思科 ISE 分析器的配置文件名称和终端分类结果同步到 Cisco Clean Access Manager (CAM)。

管理节点中的思科 Clean Access Manager 配置

思科 ISE 允许您在分布式部署中的主 PAN 上注册多个 Clean Access Manager (CAM)，用于 REST API 通信设置。在思科 ISE 中注册的 CAM 列表是接收所有分析器配置更改通知的列表。主 PAN 负责思科 ISE 和思科 NAC 设备之间的所有通信。只能在思科 ISE 的主 PAN 中配置 CAM。在主 PAN 中注册一个或多个 CAM 时使用的凭证用来验证与 CAM 的连接。

思科 ISE 和思科网络准入控制设备之间通过安全套接字层 (SSL) 进行通信，安全可靠。此通信在本质上也是双向的，因为思科 ISE 将分析器配置更改推送到 CAM，CAM 会从思科 ISE 定期获取终端 MAC 地址及其对应配置文件的列表和所有配置文件名称列表。

您必须从 Clean Access Manager（管理 (Administration) > Clean Access Manager > SSL）导出 X509 证书的内容，并将其导入思科 ISE 中“管理”(Administration) >“系统”(System) >“证书”(Certificates) >“受信任证书库”(Trusted Certificates Store) 下的主 PAN，确保思科 ISE 和 CAM 之间实现正确、安全的通信。

关于如何设置 CAM 对以实现高可用性的详细信息，请参考下面的链接。

思科 ISE 分析器和思科 Clean Access Manager 通信

思科 ISE 分析器会向从主 PAN 注册的所有 Clean Access Manager (CAM) 通知分析器配置的更改。这样，可以避免在思科 ISE 分布式部署中发出重复通知。当思科 ISE 数据库中添加或删除终端并且终端分析策略发生变更时，分析器会使用 REST API 通知分析器配置的更改。导入终端期间，思科 ISE 分析器仅会在导入完成后通知 CAM。

实施以下 REST API 流程，将分析器配置的更改推送到 CAM：

思科 ISE 分析器终端更改推送 - 当终端经过分析并且思科 ISE 中的终端配置文件发生更改时，思科 ISE 分析器会向注册的所有 CAM 通知终端配置文件中的更改。

您可以在 CAM 中配置思科 ISE，这样便可以根据 CAM 中的同步设置，将 CAM 与思科 ISE 进行同步。您必须创建规则，即从思科 ISE 配置文件列表中选择一个或多个匹配的配置文件，并将终端映射到 CAM 中的任何一种访问类型。CAM 会定期从思科 ISE 分析器检索终端及其相应的配置文件，以及所有配置文件名称的列表。

实施以下 REST API 流程，从思科 ISE 分析器提取分析器配置的更改：

- NAC 管理器终端提取 - 提取终端的 MAC 地址列表以及已知终端相应的配置文件。
- NAC 管理器配置文件提取 - 从思科 ISE 分析器提取配置文件的名称。

思科 ISE 分析器向思科 ISE 监控角色通知可用于监控思科 ISE 和思科网络准入控制设备版本 4.9 集成并排除其故障的所有事件。

思科 ISE 分析器日志捕获以下事件，以实现监控和故障排除的集成：

- NAC 设置的配置更改（信息）
- NAC 通知事件故障（错误）

添加思科 Clean Access Manager

如果将思科 ISE 与思科 NAC 设备版本 4.9 集成，您就可以在思科 NAC 部署中使用思科 ISE 分析服务。

您可以通过 NAC Managers 页面配置多个思科访问管理器 (CAM)，CAM 提供用于过滤您已注册的 CAM 的选项。此页面列出 CAM 及其名称、说明、IP 地址和显示是否已为这些 CAM 启用终端通知的状态。

步骤 1 选择管理 **(Administration)** > 网络资源 **(Network Resources)** > **NAC** 管理器 **(NAC Managers)**。

步骤 2 点击 **Add**。

步骤 3 输入思科访问管理器的名称。

步骤 4 点击 **Status** 复选框，启用从对连接进行身份验证的思科 ISE 分析器服务到 CAM 的 REST API 通信。

步骤 5 为 CAM 输入 IP 地址，0.0.0.0 和 255.255.255.255 这两个 IP 地址除外。

步骤 6 输入用于登录 CAM 用户界面的 CAM 管理员的用户名和密码。

步骤 7 点击提交 **(Submit)**。

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

- 确保思科 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)NAC 或 AnyConnect 终端安全评估配置文件 (NAC or 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

通过这些窗口，您可以配置和管理连接到您的网络的终端。

终端设置

表 *39:* 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 地址是连接到启用思科 ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在“终端”(Endpoints) 窗口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。
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。
	思科 ISE 包括以下系统创建的终端身份组：
	• 黑名单
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 112 页
使用策略和身份的静态分配创建终端，第 108 页

从 LDAP 设置导入终端

表 *40:* 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　思科 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。您可以在思科 ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。

字段名称	使用指南
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。
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，以确保终端策略与思科 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	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

相关主题

已识别的终端，第 112 页
从 LDAP 服务器导入终端，第 111 页

终端分析策略设置

表 *41:* 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。

字段名称	使用指南
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 • 端口重启 • 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
条件	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 **Select Existing Condition from Library** 或 **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思科预定义条件来定义表达式。 **创建新条件 (Create New Condition)**（高级选项）：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。

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思科预定义条件，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)**：可以添加思科预定义条件
	  • **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。

字段名称	使用指南
Create New Condition (Advance Option)	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)**：可以添加思科预定义条件 • **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 70 页
创建终端分析策略，第 100 页

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

对象	OID
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

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
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

对象	OID
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	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5

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

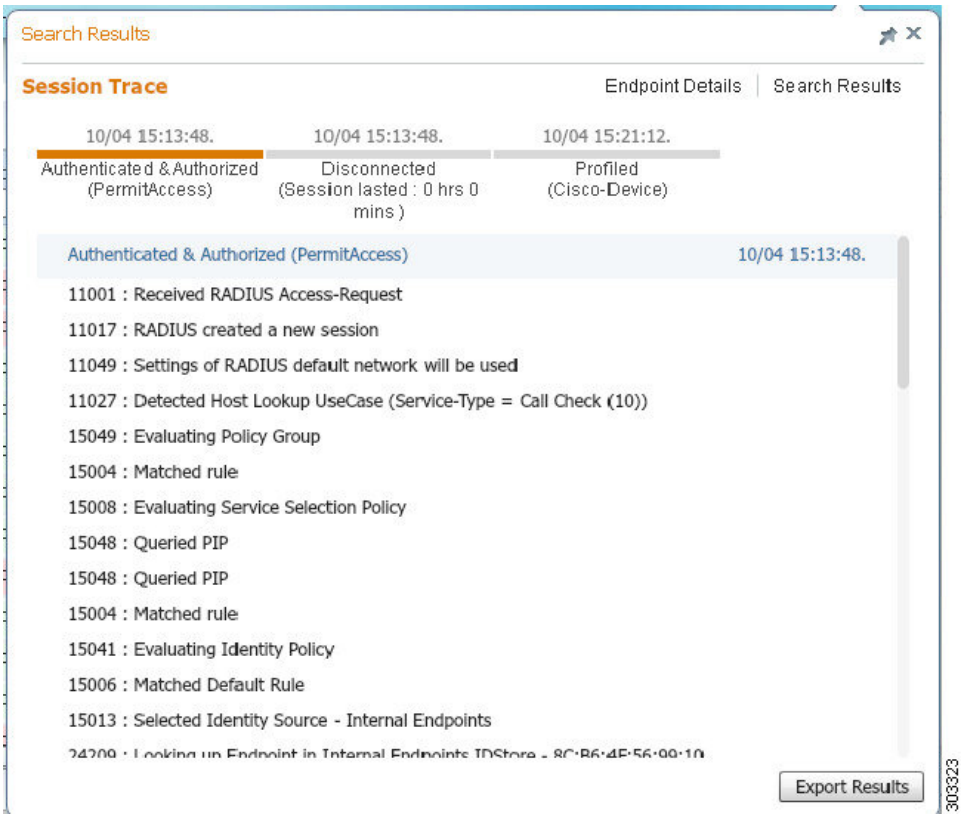
对象	OID
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
lldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

终端的会话跟踪

您可以使用思科 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。

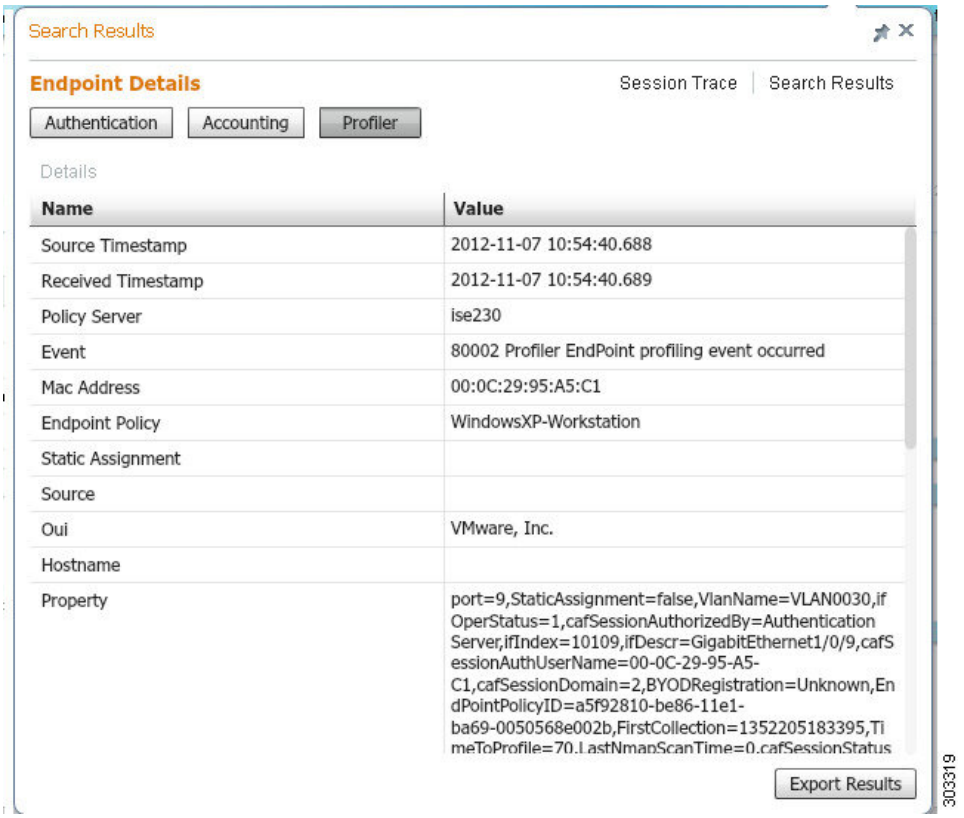
图 *5:* 终端的会话跟踪



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 *6:* 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

您可以使用思科 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

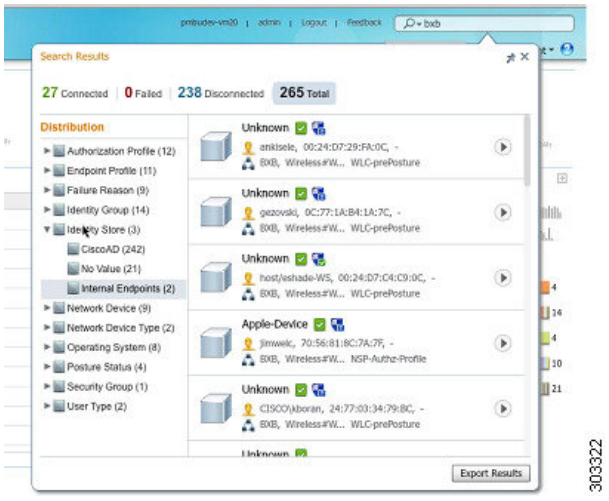
对于任何搜索条件，您应在搜索字段中至少输入三个字符以显示数据。

注释 如果终端已由思科 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思科 ISE 进行身份验证或未在思科 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。您可以使用过滤器来缩小结果范围。

下图为搜索结果的示例：

图 7: 终端的搜索结果



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

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。