身份源

身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与IP地址关联的用户身份，或是对远程访问 VPN 连接或到 设备管理器的访问进行身份验证。

以下主题介绍如何定义身份源。后期配置需要使用身份源的服务时，可以使用这些对象。

- 关于身份源， 第 1 页
- Active Directory (AD) 身份领域， 第 3 页
- RADIUS 服务器和组， 第 8 页
- 身份服务引擎 (ISE)， 第 12 页
- SAML 服务器， 第 15 页
- 本地用户， 第 18 页

关于身份源

身份源是为组织内的人员定义用户账户的AAA服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到 设备管理器的访问进行身份验证。

使用**对象 (Objects)** > **身份源 (Identity Sources)** 页面可以创建和管理您的源。后期在配置需要身份源的服务时，会用到这些对象。

以下是受支持的身份源及其用途：

Active Directory (AD) 身份领域

Active Directory 可提供用户账户和身份验证信息。请参阅 Active Directory (AD) 身份领域， 第 3 页。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，用于主动身份验证，并作为用户身份源用于被动身份验证。

Active Directory (AD) 领域序列

AD 领域序列是 AD 领域对象的有序列表。如果您在网络中管理多个 AD 域，则领域序列将非常有用。请参阅 配置 AD 领域序列， 第 7 页。

您可以将此源用于以下目的：

- 身份策略，作为用户身份源用于被动身份验证。序列中的领域顺序决定了在存在冲突的极少数情况下系统确定用户身份的方式。

思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE-PIC)

如果使用 ISE，可以将 威胁防御设备与您的 ISE 部署集成。请参阅 身份服务引擎 (ISE)，第 12 页。

您可以将此源用于以下目的：

- 身份策略，作为被动身份源来从 ISE 收集用户身份信息。

RADIUS 服务器、RADIUS 服务器组

如果您使用的是RADIUS 服务器，还可以将其与 设备管理器配合使用。必须将每个服务器定义为单独的对象，然后将其归入服务器组（其中，指定组中的服务器是彼此的副本）。为服务器组分配功能，但不为单个服务器分配功能。请参阅 RADIUS 服务器和组，第 8 页。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。
- 对 设备管理器 或 威胁防御 CLI 管理用户进行外部身份验证。可以支持具有不同授权级别的多个管理用户。这些用户可以登录到系统进行设备配置和监控。

SAML 服务器

安全断言标记语言 2.0 (SAML 2.0) 是一种开放标准，用于在各方（尤其是身份提供程序 [IdP] 和运营商 [SP]）之间交换身份验证和授权数据。

您可以将此源用于以下目的：

- 远程访问 VPN，作为单点登录 (SSO) 身份验证源。
- 对 设备管理器用户进行外部身份验证。可以支持具有不同授权级别的多个管理用户。这些用户可以登录到系统进行设备配置和监控。

LocalIdentitySource

这是本地用户数据库，其中包括您在 设备管理器中定义的用户。选择 **对象** > **用户** 管理此数据库中的用户账户。请参阅本地用户，第 18 页。

注释 本地身份源数据库不包含您在 CLI 中配置（使用 **configure user add** 命令）以进行 CLI 访问的用户。CLI 用户与您在 设备管理器中创建的用户是完全独立的。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源或回退身份源。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

Active Directory (AD) 身份领域

Microsoft Active Directory (AD) 定义用户账户。您可以为 Active Directory 域创建 AD 身份领域。以下主题介绍如何定义 AD 身份领域。

支持的目录服务器

可以使用 Windows Server 2012、2016 和 2019 上的 Microsoft Active Directory (AD)。

请注意以下有关服务器配置的信息：

- 如果要对用户组或组内用户执行用户控制，则必须在目录服务器上配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。
- 目录服务器必须使用下表中列出的字段名称，以便系统从该域的服务器中检索用户元数据。

元数据	**Active Directory** 字段
LDAP 用户名	samaccountname
名字	givenname
姓氏	sn
邮箱地址	mail Userprincipalname（如果 mail 没有值）
部门	department distinguishedname（如果 department 没有值）
电话号码	telephonenumber

对用户数量的限制

设备管理器 可以从目录服务器下载多达 50,000 个用户的信息。

如果您的目录服务器上有超过 50,000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

此限制也适用于与组相关联的名称。如果组成员超过 50,000 个，则只能将下载的 50,000 个名称与组成员身份进行匹配。

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名(DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。

提示 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 Active Directory 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入 **dsquery user** 命令时加上已知用户名（部分或完整），以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

```
C:\Users\Administrator>dsquery user -name “John*”
“CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com”
```

基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

组搜索基准

输入 **dsquery group** 命令时加上已知用户名，以确定基准标识名。例如，以下命令使用组名称 Employees 返回标识名：

```
C:\>dsquery group -name “Employees”
“CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com”
```

组基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

此外，还可以使用 ADSI Edit 程序浏览 Active Directory 结构（**开始** > **运行** > **adsiedit.msc**）。在“ADSI 编辑”(ADSI Edit) 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择**属性 (Properties)** 查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

1. 点击目录属性中的“测试连接”(Test Connection) 按钮验证连接。解决所有问题后，保存目录属性。
2. 提交对设备的更改。
3. 创建访问规则，选择**用户**选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

配置 AD 身份领域

身份领域是目录服务器加上提供身份验证服务所需的其他属性。目录服务器包含有权访问您网络的用户和用户组的相关信息。

对于 Active Directory，领域就等于 Active Directory 域。为需要支持的各个 AD 域创建单独的领域。

领域用于以下策略中：

- 身份 - 领域提供用户身份和组成员身份信息，然后您可将这些信息用于访问控制规则。系统每天都会在当天的最后一个小时 (UTC) 下载有关所有用户和组更新后的信息。必须能够从管理接口访问目录服务器。
- 远程访问 VPN - 领域提供身份验证服务，用于确定是否允许接入某个连接。必须能够从 RA VPN 外部接口访问目录服务器。
- 访问控制和 SSL 解密 - 您可以在规则的用户条件中选择领域，以便对此领域内的所有用户应用此规则。

与您的目录管理员一起获取配置目录服务器属性所需的值。

注释 如果目录服务器不在相连的网络中或无法通过默认路由使用，请为该服务器创建静态路由。依次选择**设备** > **路由** > **查看配置**，创建静态路由。或者，在定义服务器时选择适当的接口。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑领域属性时，点击对象列表中所示的**创建新身份领域**链接来创建身份领域对象。

开始之前

确保目录服务器、威胁防御 设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建 AD 领域，请点击 + > **AD**。
- 要编辑领域，请点击此领域的编辑图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置基本领域属性。

- **名称** - 目录领域的名称。

- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释　系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名，第 4 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

步骤 4 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **接口** - 应通过其访问 AD 服务器的接口。如果不选择接口，系统会使用数据路由表查找合适的接口。如果您要使用某个管理专用接口，则必须明确选择该接口；不能在管理专用路由表中使用路由查找。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为**无**，也就是说以明文形式下载用户和组信息。
  - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
  - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

步骤 5 如果领域有多个服务器，请点击**添加其他配置**，并输入每个额外服务器的属性。

您可以将最多 10 个 AD 服务器添加到领域。这些服务器需要彼此复制并支持相同的 AD 域。

为方便起见，您可以折叠和展开每个服务器条目。用主机名/IP 地址和端口标记各个部分。

步骤 6 点击**测试**按钮验证系统是否可以与服务器通信。

系统使用单独的进程和接口访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程访问 VPN。如果无法访问服务器，请确认IP地址和主机名正确、DNS服务器具有该主机名的条目等。您可能需要为该服务器配置静态路由。有关详细信息，请参阅目录服务器连接故障排除，第 7 页。

步骤 7 点击**确定 (OK)**。

配置 AD 领域序列

您可以在被动身份规则中使用 AD 领域序列，以便系统可以尝试匹配多个 AD 服务器中的用户。在领域序列中，配置 AD 领域的有序列表，其中每个 AD 服务器管理不同的领域或域，例如 engineering.example.com 和 marketing.example.com。

仅当您支持多个 AD 域且来自不同域的用户可能通过 威胁防御 设备发送流量时，领域序列才有用。这些领域可用于为使用被动身份验证的用户会话查找身份。在极少数可能发生冲突的情况下，可以使用领域顺序解决身份冲突。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建 AD 领域序列，请依次点击 + > **AD 领域序列**。
- 要编辑 AD 领域序列，请点击该对象的编辑图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置领域序列属性：

- **名称** - 对象的名称。
- **说明** - 对象的可选说明。
- **AD 领域** - 点击 + 将 AD 领域对象添加到序列中。添加领域后，点击并将领域拖放到所需的有序序列中。

步骤 4 点击**确定**。

现在，您可以在被动身份规则中选择 AD 领域序列。

目录服务器连接故障排除

系统使用不同的进程与您的目录服务器通信，具体取决于服务器的功能。因此，身份策略的连接可以正常工作，而远程访问 VPN 的连接则失败。

这些进程使用不同的接口与目录服务器进行通信。您必须确保这些接口的连接性。

- 管理接口，用途：身份策略。
- 数据接口，用途：远程访问 VPN（外部接口）。

配置身份领域时，请使用**测试**按钮验证连接是否可以正常工作。失败消息应指示该功能存在连接问题。根据身份验证属性和路由/接口配置，以下是您可能会遇到的常规问题。

目录用户身份验证问题。

如果问题是系统因用户名或密码而无法登录目录服务器，请确保用户名和密码正确并在目录服务器上有效。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

此外，系统还会根据用户名和密码信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

目录服务器可通过数据接口进行访问。

如果目录服务器所在的网络直接连接到数据接口（例如千兆以太网接口）或是可从直连网络路由，那么您必须确保虚拟管理接口与目录服务器之间存在路由。

- 使用 **data-interfaces** 作为管理网关应该能够确保路由成功。
- 如果管理接口上有显式网关，则该网关路由器需要与目录服务器之间建立路由。
- 如果直连网络与托管目录服务器的网络之间存在路由器，则为目录服务器配置静态路由(**设备** > **路由**)。
- 验证数据接口的 IP 地址和子网掩码是否正确。

目录服务器位于外部网络上。

如果目录服务器位于外部（上行链路）接口另一端的网络，您可能需要配置站点间VPN连接。有关详细程序，请参阅如何通过远程访问 VPN 使用外部网络上的目录服务器。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对 远程访问 VPN 连接以及 设备管理器 和 威胁防御 CLI 管理用户进行身份验证和授权。例如，如果您还使用 Cisco Identity Services Engine (ISE) 及其 RADIUS 服务器，可以将该服务器与 设备管理器 搭配使用。

配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

以下主题介绍如何配置 RADIUS 服务器和组，以便它们可用于支持的功能。

配置 RADIUS 服务器

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。如果您使用 RADIUS 服务器进行用户身份验证和授权，可以将这些服务器与 设备管理器搭配使用。

为每个 RADIUS 服务器创建对象后，创建 RADIUS 服务器组，以包含每个重复服务器组。

开始之前

如果您想要为 RA VPN 配置重定向 ACL，在创建和编辑服务器对象之前，您必须使用 Smart CLI 创建扩展 ACL。在编辑对象时，您无法创建 ACL。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 **+** > **RADIUS 服务器**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置的任何内容匹配。
- **服务器名称或 IP 地址** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。例如，radius.example.com 或 10.100.10.10.
- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。如果您将此服务器用作远程访问 VPN 的辅助身份验证源，例如用于提示输入身份验证令牌，请将超时时间至少延长到 60 秒，以便让用户有时间获取和输入令牌。
- **服务器密钥** -（可选。）用于加密 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 4 （可选。）如果您使用服务器进行远程访问 VPN 授权更改配置，您可以点击**仅限于 RA VPN** 链接并配置以下选项。

- **重定向 ACL** - 选择要用于 RA VPN 重定向 ACL 的扩展 ACL。在**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**页面上使用 Smart CLI **扩展访问列表 (Extended Access List)**创建扩展 ACL。

重定向 ACL 的目的是将初始流量发送到思科身份服务引擎 (ISE)，以便 ISE 可以评估客户端安全状况。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。有关示例，请参阅在 威胁防御 设备上配置授权更改。

- **用于连接 RADIUS 服务器的接口** - 与该服务器通信时要使用的接口。如果您选择**通过路由查找解决**，系统将始终使用数据路由表来确定要使用的接口。如果您选择**手动选择接口**，系统将始终使用您选择的接口。如果您要使用某个管理专用接口，则必须明确选择该接口；不能对管理专用路由表使用路由查找。

  如果您在配置授权更改，则必须选择特定接口，以便系统可以在该接口上正确启用 CoA 侦听程序。

  如果此服务器还用于 设备管理器 管理访问，则此接口将被忽略。系统始终通过管理 IP 地址对管理访问尝试进行身份验证。

步骤 5 （可选，仅编辑对象时）点击**测试**检查系统是否可以连接到服务器。

系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 6 点击**确定 (OK)**。

配置 RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

在一项功能中配置 RADIUS 支持时，必须选择服务器组。因此，即使只有一台 RADIUS 服务器，也必须创建包含该服务器的组。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 + > **RADIUS 服务器组 (RADIUS Server Group)**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置内容匹配。
- **断路时间** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间，其值为 0-1440 分钟。仅当配

置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。

- **最大失败尝试次数** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败 AAA 事务（即，未收到响应的请求）的数量。您可以指定 1 到 5 之间的数字，默认值为 3。超过最大失败尝试次数时，系统会将服务器标记为故障。

  对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。

- **动态授权（仅限于 RA VPN）**、**端口** - 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从思科身份服务引擎 (ISE) 进行更新。默认侦听端口为 1700，也可以指定 1024 到 65535 范围内的其他端口。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权

- **支持 RADIUS 服务器的领域** - 如果 RADIUS 服务器配置为使用 AD 服务器对用户进行身份验证，请选择指定了与此 RADIUS 服务器结合使用的 AD 服务器的 AD 领域。如果尚不存在此领域，请点击列表底部的**创建新身份领域 (Create New Identity Realm)** 立即配置。

- **RADIUS 服务器列表** - 选择为该组定义服务器的最多 16 个 RADIUS 服务器对象。按优先级顺序添加这些对象。使用列表中的第一个服务器，直至此服务器无法响应。添加对象后，您可以通过拖放重新排列对象。如果所需的对象尚不存在，请点击**创建新的 RADIUS 服务器 (Create New RADIUS Server)** 立即添加对象。

  您也可以点击**测试 (Test)** 链接，验证系统是否可以连接到服务器。系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 4 （可选。）点击**测试所有服务器 (Test All Servers)** 按钮，检查到组中每台服务器的连接。

系统会提示输入用户名和密码。系统会检查是否可以连接每个服务器，以及用户名是否可在每台服务器上进行身份验证。

步骤 5 点击**确定 (OK)**。

RADIUS 服务器和组故障排除

当外部授权无法使用时，您可以检查以下事项。

- 使用 RADIUS 服务器和服务器组对象中的**测试**按钮，验证是否可以从设备连接到服务器。务必在测试之前保存对象。如果测试失败：
  - 请注意，测试会忽略为服务器配置的接口，且始终使用管理接口。如果未将 RADIUS 身份验证代理配置为响应来自管理 IP 地址的请求，则测试预期失败。
  - 验证您在测试期间是否输入了正确的用户名/密码组合。如果用户名/密码组合不正确，您将收到凭证错误消息。

- 验证服务器的加密密钥、端口和 IP 地址。如果使用主机名，验证是否为管理接口配置了 DNS。考虑在 RADIUS 服务器上更改了密钥，但未在设备配置中更改的可能性。
- 如果测试仍然失败，您可能需要配置到 RADIUS 服务器的静态路由。请尝试从 CLI 控制台或 SSH 会话对服务器执行 ping 操作，检查是否可以访问服务器。

- 如果外部身份验证一直都在工作，却停止了工作，请考虑是否会出现所有服务器均处于空载时间的情况。如果配置回退到本地身份验证，在组内的所有 RADIUS 服务器都发生故障时，空载时间是系统在再次尝试连接第一个服务器之前等待的分钟数。在停滞时间内会使用本地身份验证，因此给定用户的用户名和密码将是本地用户名/密码。默认时间为 10 分钟，不过您可以配置最长 1440 分钟。
- 如果 HTTPS 外部身份验证对一部分用户适用，对另一部分用户不适用，请评估 RADIUS 服务器中为每个用户账户定义的 cisco-av-pair 属性。此属性可能未正确配置。属性缺失或不正确将阻止对该用户账户的所有 HTTS 访问。
- 如果 SSH 外部身份验证对一部分用户适用，对另一部分用户不适用，请评估 RADIUS 服务器中为每个用户账户定义的 Service-Type 属性。此属性可能未正确配置。属性缺失或不正确将阻止对该用户账户的所有 SSH 访问。

身份服务引擎 (ISE)

您可以将思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与 威胁防御设备相集成，以使用 ISE/ISE-PIC 进行被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。但是，对于 威胁防御，您只能将 ISE 与 AD 配合使用，以获悉用户身份。除查看各种监控控制面板和事件中的用户信息之外，还可以将用户身份用作访问控制和SSL 解密策略中的匹配条件。

有关 Cisco ISE/ISE-PIC 的更多信息，请参阅《思科身份服务引擎管理员指南》(https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) 和《身份服务引擎被动身份连接器 *(ISE-PIC)* 安装和管理员指南》(https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html)。

ISE 的准则和限制

- 由于系统不将设备身份验证与用户关联，因此防火墙系统不支持与 Active Directory 身份验证同时进行 802.1x 设备身份验证。如果使用 802.1x 主动登录，则将 ISE 配置为仅报告 802.1x 主动登录（设备和用户）。这样，仅向系统报告一次设备登录。
- ISE/ISE-PIC 不报告 ISE 访客服务用户的活动。
- 同步 ISE/ISE-PIC 服务器和设备上的时间。否则，系统可能会以意外间隔执行用户超时。
- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。

- 有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅 *Cisco Secure Firewall* 兼容性指南，https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html。
- 使用 ISE 服务器的 IPv4 地址，除非您确认您的 ISE 版本支持 IPv6。

配置身份服务引擎

要使用思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) 作为被动身份源，您必须配置与 ISE 平台交换网格 (pxGrid) 服务器的连接。

开始之前

- 从 ISE 中导出 pxGrid 和 MNT 服务器证书。例如，在 ISE PIC 2.2 上，可在**证书 (Certificates)** > **证书管理 (Certificate Management)** > **系统证书 (System Certificates)** 页面找到这些证书。MNT（监控和故障排除节点）在证书列表的“使用者”列中显示为 Admin。您可以在**对象 (Objects)** > **证书 (Certificates)**页面将它们上传为受信任的 CA 证书，也可以在以下过程中上传这些证书。这些节点可能使用相同的证书。
- 您还必须配置 AD 身份领域。系统从 AD 获取用户列表，从 ISE 获取用户到 IP 地址映射的信息。
- 如果您将使用安全组标记 (SGT) 进行访问控制（无论是否具有静态安全组标记映射），并侦听 SXP 主题，则还需要在 ISE 中配置 SXP 和这些映射。请参阅在 ISE 中配置安全组和 SXP 发布。

过程

步骤 1 选择**对象**，然后从目录中选择**身份源**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + > **身份服务引擎 (Identity Services Engine)**。可创建最多一个 ISE 对象。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。
- **状态 (Status)** - 点击开关以启用或禁用对象。禁用对象时，您不能将 ISE 用作身份规则中的身份源。
- **说明** - 对象的可选说明。
- **主节点主机名/IP 地址** - 主要 pxGrid ISE 服务器的主机名或 IP 地址。不要指定 IPv6 地址，除非确认您的 ISE 版本支持 IPv6。

- **辅助节点主机名/IP 地址 (Secondary Node Hostname/IP Address)** - 如果您设置辅助 ISE 服务器以实现高可用性，请点击**添加辅助节点主机名/IP 地址 (Add Secondary Node Hostname/IP Address)** 并输入辅助 pxGrid ISE 服务器的主机名或 IP 地址。
- **pxGrid 服务器 CA 证书** - 受信任的 pxGrid 框架证书颁发机构证书。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。
- **MNT 服务器 CA 证书** - 执行批量下载时 ISE 证书的受信任的证书颁发机构证书。如果您的 MNT（监控和故障排除）服务器不是单独的服务器，此证书可能与 pxGrid 服务器证书相同。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。
- **服务器证书** - 连接 ISE 或执行批量下载时，威胁防御设备必须向 ISE 提供的内部身份证书。
- **订用** - 选择应订用哪个 ISE pxGrid 主题。订用主题意味着您将下载与该主题相关的数据。
  - **会话目录主题** - 是否获取有关用户会话的信息，包括用户会话的 SGT 映射。默认情况下，此选项已启用。如果要获取被动用户身份以在安全策略中使用并在监控控制面板中实现可视化，则应选择此选项。
  - **SXP 主题** - 是否获取静态“SGT 到 IP”地址映射。如果要基于安全组标记 (SGT) 编写访问控制规则，请选择此主题。
- **ISE 网络过滤器** - 可设置用来限制 ISE 向系统报告的数据的可选过滤器。如果提供网络过滤器，ISE 会仅报告网络上符合过滤器要求的数据。点击 **+**，选择标识网络的网络对象，然后点击**确定 (OK)**。如果您需要创建对象，点击**创建新网络 (Create New Network)**。仅配置 IPv4 网络对象。

步骤 4 点击**测试 (Test)** 按钮，验证系统是否可以连接到 ISE 服务器。

如果测试失败，请点击**查看日志 (See Logs)** 链接了解详细的错误消息。例如，以下消息表示系统无法在规定端口连接到服务器。存在的问题可能是，没有路由到主机（即 ISE 服务器未使用预期端口），或访问控制规则阻止这类连接。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

步骤 5 点击**确定 (OK)** 保存对象。

下一步做什么

配置 ISE 后，启用身份策略，配置被动身份验证规则，并部署配置。然后，您必须转到 ISE/ISE PIC 并接受设备作为订阅方。如果您配置 ISE/ISE PIC 自动接受订阅方，无需手动接受订用。

ISE/ISE-PIC 身份源故障排除

ISE/ISE-PIC 连接

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 威胁防御设备成功集成。
- 在 ISE 服务器与 威胁防御设备成功建立连接之前，您必须手动在 ISE 中批准客户端。

  或者，您可以在ISE中启用**自动审批新账户**，具体操作请参照《思科身份服务引擎管理员指南》中有关管理用户和外部身份源的章节。
- 威胁防御设备（服务器）证书必须包含 **clientAuth** 扩展密钥用法值，否则不能包含任何扩展密钥用法值。如果设置了 clientAuth 扩展密钥用法，还必须选择不设置密钥用法，或设置数字签名密钥用法值。使用 设备管理器 创建的自签名身份证书满足这些要求。
- ISE 服务器上的时间必须与 威胁防御上的时间同步。如果设备不同步，系统可能会以非预期时间间隔执行用户超时。

ISE/ISE-PIC 用户数据

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中成功检索到这些活动的相关信息之前，活动不会显示在控制面板中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- 系统不会收到 ISE 访客服务用户的用户数据。

SAML 服务器

您可以将安全断言标记语言 2.0 (SAML 2.0) 服务器配置为远程访问 VPN 连接 和设备管理器用户的单点登录 (SSO) 身份验证源。SAML 是用于在各方（尤其是身份提供程序 [IdP] 和服务提供商 [SP]）之间交换身份验证和授权数据的开放标准。

配置 SAML 服务器

您可以将安全断言标记语言 2.0 (SAML 2.0) 服务器配置为远程访问 VPN 连接 和设备管理器用户的单点登录 (SSO) 身份验证源。例如，Duo 接入网关 (DAG) 是 SAML 服务器。

当您使用 SAML 服务器作为身份验证方法时，SAML 服务器充当身份提供程序 (IdP)，而 威胁防御设备充当服务提供商 (SP)。

对于 RA VPN，您可以使用 SAML 服务器作为主要身份验证源，但不能配置辅助身份验证源，也不能配置回退源。

对于设备管理器登录，如果配置 SAML 服务器以支持通用访问卡 (CAC)，则可以在使用 SAML 服务器时使用该卡登录。

开始之前

从 SAML 服务器身份提供程序获取以下信息：如果可能，请以 XML 文件形式下载用户信息，以便轻松上传。

- 实体 ID URL，其提供 SAML 服务器元数据。
- 登录 URL。
- 注销 URL。
- 身份提供程序证书。

过程

步骤 1 执行以下任一项操作即可转到“SAML 服务器”(SAML Servers) 页面：

- 选择**对象**，然后从目录中选择**身份源**。
- 依次选择**设备** > **远程访问 VPN** > **SAML 服务器**。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 **+** > **SAML 服务器**。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置以下属性：

- **名称** - 对象的名称。
- **说明** - 对象的可选说明。
- **身份提供程序 (IDP) 实体 ID URL** - 这是用于提供元数据 XML 的页面的 URL（元数据 XML 说明 SAML 颁发者将如何响应请求）。有些 SAML 服务器产品称之为实体 ID，有些称之为元数据 URL。此 URL 必须为 4-256 个字符，包括协议 https://。例如 https://191.168.2.21/dag/saml2/idp/metadata.php。

  注释 如果以 XML 文件形式从 SAML 服务器下载信息，请点击**从 XML 文件填充 (Populate from XML file)** 并选择该文件。可以从 XML 文件中填充此字段以及**登录 URL (Sign-In URL)** 和**身份提供程序证书 (Identity Provider Certificate)**。

- **登录 URL** - 用于登录到身份提供程序 SAML 服务器的 URL。此 URL 必须介于 4-500 个字符之间，包括协议。允许使用 http:// 和 https://。例如 https://191.168.2.21/dag/saml2/idp/SSOService.php。
- **注销 URL** - 用于注销身份提供程序 SAML 服务器的 URL。此 URL 必须介于 4-500 个字符之间，包括协议。允许使用 http:// 和 https://。例如 https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php。

- **服务提供商证书**- 用于 威胁防御 设备的内部证书。理想情况下，您已上传由获认可的第三方签名的证书，现在可以选择该证书。您还可以使用内置的DefaultInternalCertificate，或点击**创建新内部证书**并立即上传签名证书。SAML 服务器身份提供程序必须信任此证书，因此您可能需要将其上传到 SAML 服务器。有关如何上传证书或以其他方式启用与服务提供商的信任关系的信息，请参阅 SAML 服务器文档。
- **身份提供程序证书** - SAML 服务器身份提供程序的受信任 CA 证书。从 SAML 服务器下载此证书。如果尚未上传，请点击**创建新的受信任 CA 证书**并立即上传。
- **请求签名** - 为登录请求签名时使用的加密算法。选择“无”可禁用加密。否则，请选择以下一个选项（按从弱到强的顺序排序）：SHA1、SHA256、SHA384、SHA512。
- **请求超时** - SAML 断言具有有效时间段：用户必须在此有效时间段内完成单点登录请求。您可以设置超时时间值（以秒为单位）以更改此有效时间段。如果设置的超时时间长于断言的 NotOnOrAfter 条件，系统将忽略您设置的超时时间值，并且NotOnOrAfter 条件将生效。范围为 1-7200 秒。默认值为 300 秒。
- **此 SAML 身份提供程序 (IDP) 位于内部网络上** - SAML 服务器是否在内部网络上运行，而不是在受保护网络外部运行。
- **在登录时请求重新执行 IDP 身份验证** - 选择此选项可使用户在每次登录时重新进行身份验证，而不是让 SAML 服务器重新使用以前的身份验证会话。默认情况下，此选项已启用。

步骤 4 点击 **用户角色** 并为外部用户配置 RBAC 授权角色。

- **默认用户角色**-分配用户的授权角色（如果无法通过此页面上的设置确定）。
- **组成员属性**-SAML 服务器中定义用户的 RBAC 授权角色的用户属性。
- **角色映射**-对于每个角色，键入将在SAML用户记录的组成员属性中显示的字符串，该字符串应与该角色对应。
  - **管理员**-对应用的所有方面具有完全读写访问权限的用户。
  - **加密管理员 (Cryptographic Admin)** - 可以配置与加密相关的功能（例如证书、解密策略和密钥）的用户。对其他功能的只读权限。
  - **审核管理员 (Audit Admin)** - 可以查看用户登录历史记录和审计日志并执行审核相关操作的用户。对配置功能的只读权限。
  - **读写**-用户可以执行只读用户可以执行的任何操作，但还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止其他设备管理器 用户的会话。
  - **只读**-用户可以查看控制面板和配置，但不能进行任何更改。如果尝试进行更改，错误消息会解释由于缺乏权限出错。

步骤 5 点击**确定 (OK)**。

下一步做什么

如果启用了**请求签名 (Request Signature)** 来加密通信，则需要将设备管理器信息上传到 SAML 服务器。从身份源列表中，点击服务器的**下载 (Download)** ( ) 按钮，然后保存 XML 文件。然后，登录 SAML 服务器并上传信息。有关详细信息，请参阅 SAML 提供商文档。

如果使用服务器进行设备管理器登录，但无法正常工作，请验证 SAML 服务器配置。

- 登录 SAML IdP 并验证设备管理器 SAML 响应使用者是否已正确配置。值应为：https://<FDM_URL>/api/fdm/latest/fdm/token
- 如果在 SAML 服务器对象中启用了签名，请确保将设备管理器公共证书上载到 SAML 应用中，然后启用加密。上传设备管理器 XML 文件应会将证书添加到 SAML 服务器。您也可以通过 FDM API 来检索设备管理器证书：https://<FDM_URL>/saml/metadata

本地用户

本地用户数据库 (LocalIdentitySource) 包括您在 设备管理器中定义的用户。

您可以将本地定义的用户用于以下目的：

- 远程访问 VPN，作为主要身份源或回退身份源。
- 管理访问权限，作为 设备管理器 用户的主要或辅助源。

  admin 用户是系统定义的本地用户。但是，管理员用户无法登录远程访问 VPN。您不能创建额外的本地管理用户。

  如果您定义管理访问的外部身份验证，登录到设备的外部用户将显示在本地用户列表中。
- 身份策略，作为被动身份源间接从远程访问 VPN 登录收集用户身份。

以下主题介绍如何配置本地用户。

配置本地用户

您可以直接在设备上创建与远程访问VPN搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。

如果您使用本地用户数据库作为远程访问VPN的回退身份验证方式，请确保在本地数据库中配置与外部数据库中的名称相同的用户名/密码。否则，回退机制将无效。

此处定义的用户无法登录设备 CLI。

过程

步骤 1 依次选择**对象** > **用户**。

列表将显示用户名和服务类型，可以是：

- MGMT - 针对可以登录到 设备管理器的管理用户。始终定义管理员用户，并且无法将其删除。也不能配置其他MGMT用户。但是，如果您定义管理访问的外部身份验证，登录到设备的外部用户将作为 MGMT 用户显示在本地用户列表中。
- 远程访问 VPN - 针对可以登录到设备上配置的远程访问 VPN 的用户。您还必须选择主要或辅助（回退）源的本地数据库。

步骤 2 执行以下操作之一：

- 要添加用户，请点击 +。
- 要编辑用户，请点击该用户的编辑图标 ( )。

如果您不再需要特定用户账户，请点击该用户的删除图标 ( )。

步骤 3 配置用户属性：

用户名和密码可以包含除空格和问号之外的任何可打印 ASCII 字母数字或特殊字符。可打印的字符为 ASCII 代码 33-126。

- **名称** - 用于登录远程访问 VPN 的用户名。名称可以是 4 至 64 个字符，但不能包含空格。例如，johndoe。
- **密码、确认密码** - 输入账户的密码。密码长度必须介于 8 到 16 个字符之间。它不能包含相同的连续字母。它还必须至少包含以下各项中的一项：数字、大写和小写字符，以及特殊字符。

注释 用户无法更改其密码。告诉他们密码，需要更改密码时，必须编辑用户账户。此外，不要更新外部 MGMT 用户的密码：密码由外部 AAA 服务器控制。

步骤 4 点击**确定 (OK)**。

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。