使用ISE配置EAP-TLS身份验证

目录

简介

本文档介绍使用Cisco ISE引入可扩展身份验证协议 — 传输层安全身份验证的初始配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解EAP和RADIUS通信流程。
- RADIUS身份验证基础知识，包括基于证书的身份验证方法（根据通信流）。
- 了解Dot1x和MAC身份验证旁路(MAB)之间的区别。

- 基本了解公钥基础设施(PKI)。
- 了解如何从证书颁发机构(CA)获取签名证书并管理终端上的证书。
- 在网络设备（有线或无线）上配置与身份验证、授权和记帐(AAA)(RADIUS)相关的设置。
- 与RADIUS/802.1x一起使用的请求方配置（在终端上）。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)版本3.x。
- CA — 颁发证书(可以是企业CA、第三方/公共CA，或者使用证书调配门户)。
- Active Directory（外部身份源） — 来自Windows Server；其中与ISE兼容。
- 网络接入设备(NAD) — 可以是为802.1x/AAA配置的交换机（有线）或无线LAN控制器(WLC)（无线）。
- 终端 — 颁发给（用户）身份和请求方配置的证书，可以通过RADIUS/802.1x对网络访问进行身份验证：用户身份验证。可以获取计算机证书，但本示例中未使用该证书。

注意：由于本指南使用ISE版本3.1，因此所有文档参考都基于此版本。但是，在早期版本的Cisco ISE上完全支持相同/类似的配置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

主要重点是ISE配置，该配置可应用于多个场景，例如（但不限于）通过有线或无线连接的IP电话/终端进行身份验证。

在本指南的范围内，了解ISE(RADIUS)身份验证流的以下阶段非常重要：

- 身份验证 — 识别并验证请求网络访问的最终身份（计算机、用户等）。
- 授权 — 确定终端身份在网络上可以授予哪些权限/访问权限。
- 记帐 — 在网络访问完成之后报告和跟踪终端身份的网络活动。

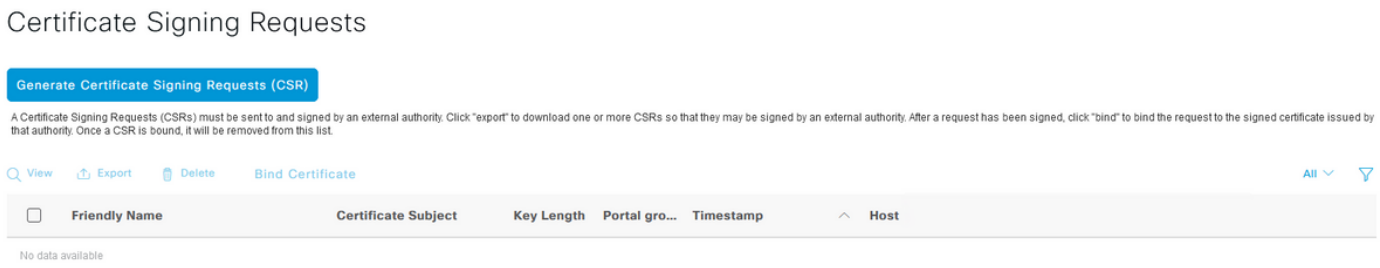
配置

获取服务器和客户端证书

步骤1:从ISE生成证书签名请求

第一步是从ISE生成证书签名请求(CSR)并将其提交到CA（服务器），以获取颁发给ISE的签名证书作为系统证书。在可扩展身份验证协议 — 传输层安全身份验证(EAP-TLS)身份验证期间，ISE可以将此证书显示为服务器证书。这在ISE UI中执行。导航至 **Administration > System: Certificates > Certificate Management > Certificate Signing Requests.**低于 **Certificate Signing Requests** ，单击 **Generate Certificate Signing Requests (CSR)**

如本图所示。



证书类型需要不同的扩展密钥用法。此列表概述了每种证书类型需要哪些扩展密钥用法：

ISE身份证书

- 多用途(Admin、EAP、Portal、pxGrid) — 客户端和服务器身份验证
- Admin — 服务器身份验证
- EAP身份验证 — 服务器身份验证
- 数据报传输层安全(DTLS)身份验证 — 服务器身份验证
- 门户 — 服务器身份验证
- pxGrid — 客户端和服务器身份验证
- 安全断言标记语言(SAML)- SAML签名证书
- ISE消息传送服务 — 生成签名证书或生成全新的消息传送证书

默认情况下，ISE消息服务系统证书用于部署、节点注册和其他节点间通信中的每个ISE节点之间的数据复制，由ISE内部证书颁发机构(CA)服务器（ISE内部）提供和颁发。无需对该证书执行任何操作。

管理员系统证书用于标识每个ISE节点，例如何时使用与管理员UI（管理）关联的API，以及用于某些节点间通信。要首次设置ISE，请设置管理员系统证书。该操作与本配置指南不直接相关。

要通过EAP-TLS（基于证书的身份验证）执行IEEE 802.1x，请对EAP身份验证系统证书执行操作，因为该证书在EAP-TLS流程期间用作提供给终端/客户端的服务器证书；因此结果在TLS隧道内是安全的。要开始使用，请创建一个CSR以创建EAP身份验证系统证书，并将其提供给管理组织中的CA服务器（或公共CA提供商）的人员进行签名。最终结果是绑定到CSR并通过这些步骤关联到ISE的CA签名证书。

在证书签名请求(CSR)表单上，选择以下选项以完成CSR并获取其内容：

- Certificate Usage，对于此配置示例，选择 **EAP Authentication**.
- 如果您计划在证书中使用通配符语句， ***.example.com** ，那么您还必须检查 **Allow Wildcard Certificate** 复选框。最佳位置是主题备用名称(SAN)证书字段，用于兼容任何用途以及环境中存在的多个不同类型终端操作系统。
- 如果未选择在证书中放置通配符语句，请选择您想要将CA签名的证书关联到的ISE节点（签名后）。

> 注意：将包含通配符语句的CA签名证书绑定到CSR中的多个节点时，证书将分发到ISE部署中的每个ISE节点（或所选节点），服务可以重新启动。但是，服务重新启动一次自动限制为一个节点。通过监控服务重新启动 **show application status ise** ISE CLI命令。

接下来，您需要完成该表单以定义主题。这包括公用名(CN)、组织单位(OU)、组织(O)、城市(L)、州(ST)和国家/地区(C)证书字段。$FQDN$变量是表示与每个ISE节点相关的管理完全限定域名（主机名+域名）的值。

- 此 Subject Alternative Name (SAN) 字段也需填写，以包含任何建立信任所需的信息。作为要求，您需要在证书签名后定义指向与此证书关联的ISE节点的FQDN的DNS条目。

- 最后，确保定义符合CA服务器功能和良好安全实践的适当密钥类型、密钥长度和要签名的摘要。默认值为：RSA、4096位和SHA-384。可用的选择和兼容性会显示在此页面的ISE管理员UI中。

这是一个不使用通配符语句的完整CSR表单示例。确保使用特定于环境的实际值：

Usage

Certificate(s) will be used for: EAP Authentication

Allow Wildcard Certificates: ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise	ise#EAP Authentication
☑ ise2	ise2#EAP Authentication
☑ ise3	ise3#EAP Authentication

Subject

Common Name (CN)
$FQDN$

Organizational Unit (OU)

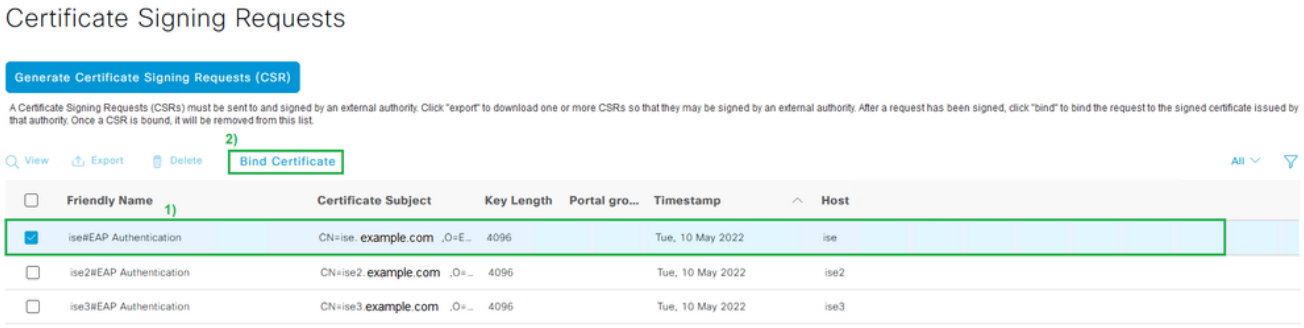
Organization (O)
Example Company

City (L)
San Jose

State (ST)
California

Country (C)
US

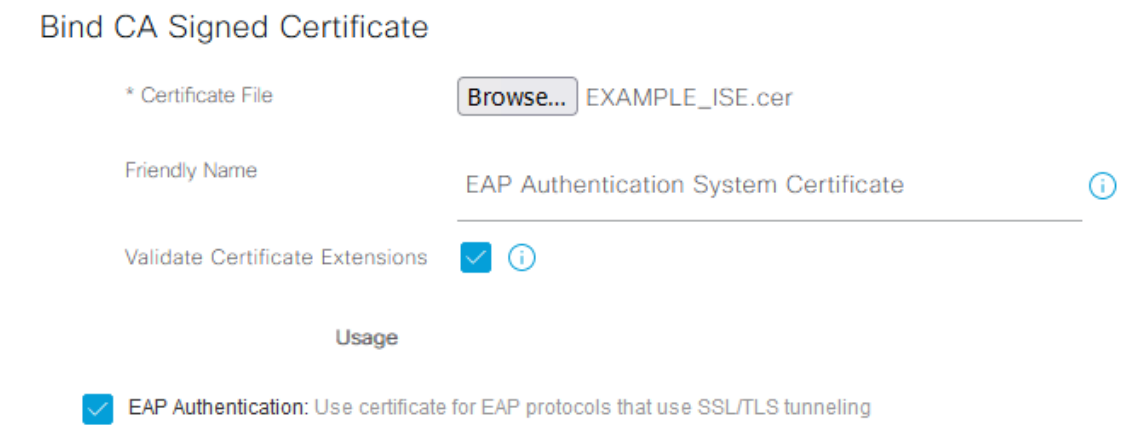
3. 所有证书作为完整CA链的一部分导入ISE中的受信任证书存储后，返回到ISE GUI并导航至 **Administration > System: Certificates > Certificate Management: Certificate Signing Requests.**找到与签名证书对应的友好名称下的CSR条目，点击证书的复选框，然后点击 **Bind Certificate.**



将证书绑定到CSR

注意：您需要将单个CA签名的证书一次绑定到每个CSR。对为部署中的其他ISE节点创建的所有剩余的CSR重复上述步骤。

在下一页上，单击 **Browse** 并选择签名证书文件，定义所需的友好名称，然后选择Certificate Usage(s)。提交以保存更改。



选择要绑定到CSR的证书

4. 此时，签名证书将移动到ISE GUI。导航至 **Administration > System: Certificates > Certificate Management: System Certificates** 并分配到为其创建CSR的同一节点。对其他节点和/或其他证书使用重复相同的过程。

第三步：获取终端的客户端证书

创建与EAP-TLS配合使用的客户端证书时，需要浏览终端上的类似进程。在本示例中，您需要一个签名并颁发给用户帐户的客户端证书才能使用ISE执行用户身份验证。有关如何从Active Directory环境获取终端客户端证书的示例，请参阅：了解并使用WLC和ISE>配置EAP-TLS的>配置EAP-TLS。

由于终端和操作系统的类型多种多样，流程也可能有所不同，因此未提供其他示例。但是，整个过程在概念上是相同的。生成CSR，该CSR包含证书中包含的所有相关信息，并且由CA签名，无论该CA是环境中的内部服务器，还是提供此类服务的公共/第三方公司。

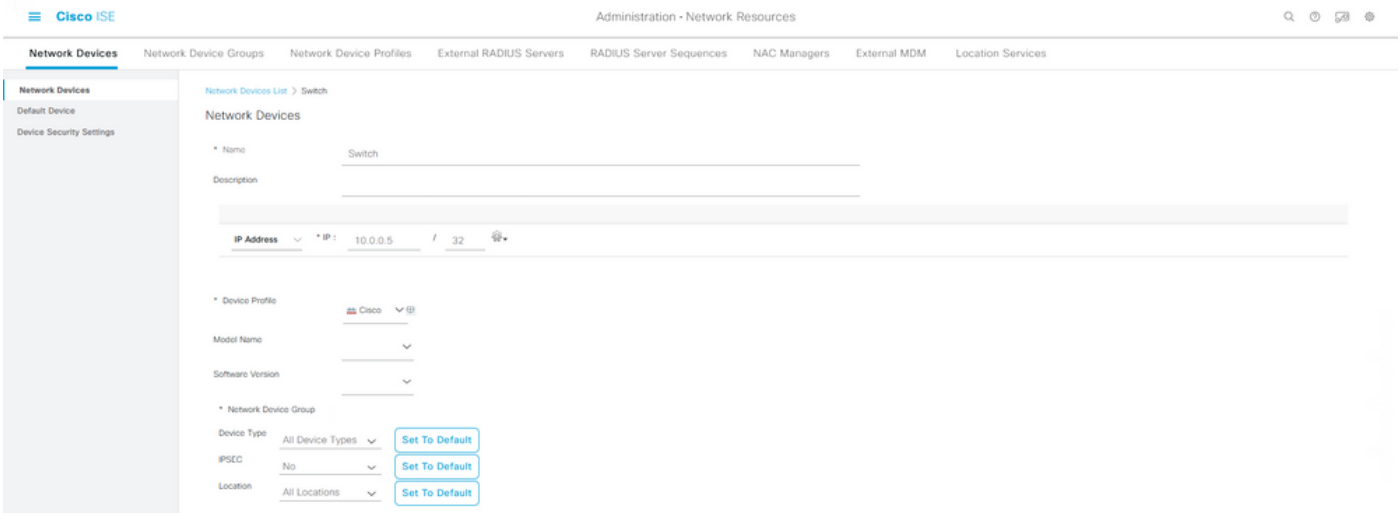
此外，公用名(CN)和主体备用名(SAN)证书字段包含在身份验证流程中使用的身份。这还指示请求方在身份方面如何配置EAP-TLS：机器和/或用户身份验证、机器身份验证或用户身份验证。本示例在本文档的其余部分中仅使用用户身份验证。

网络设备

第四步：在ISE中添加网络接入设备

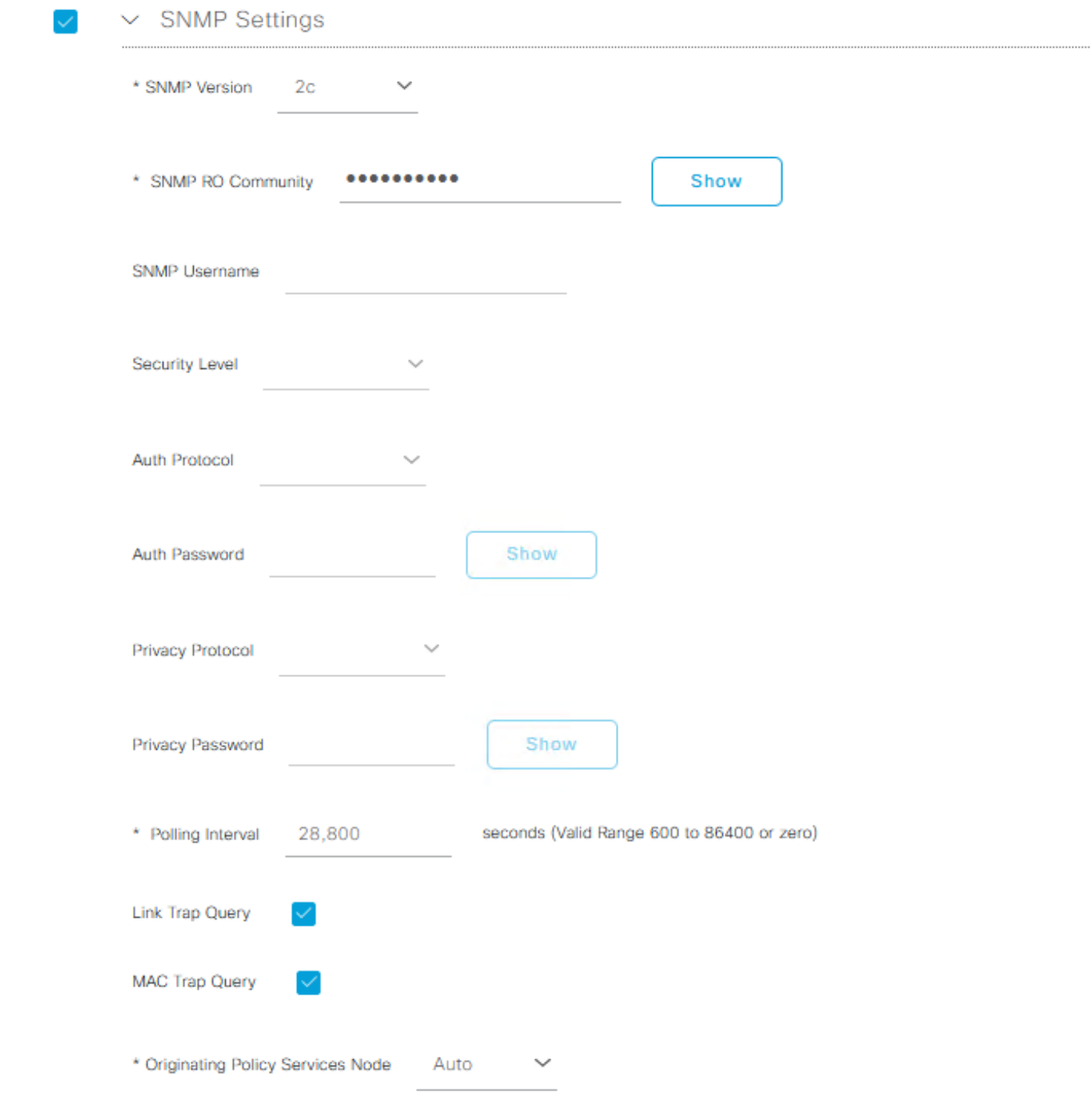
终端连接的网络接入设备(NAD)也在ISE中配置，以便可以进行RADIUS/TACACS+（设备管理员）通信。在NAD和ISE之间，共享密钥/密码用于信任目的。

要通过ISE GUI添加NAD，请导航至 **Administration > Network Resources: Network Devices > Network Devices** 并点击 **Add**，如图所示。



网络设备示例配置

为了与ISE分析一起使用，您还需要配置SNMPv2c或SNMPv3（更安全），以允许ISE策略服务节点(PSN)通过SNMP查询与NAD联系，SNMP查询涉及对终端进行ISE身份验证，以便收集属性以对使用的终端类型做出准确决策。下一个示例显示如何设置SNMP(v2c)，与上一个示例中的页面相同：



SNMPv2c配置示例

有关详细信息，请参阅《思科身份服务引擎管理员指南，版本3.1 >章节：安全访问>在Cisco ISE中定义网络设备。

此时，如果您尚未执行此操作，您需要在NAD上配置所有与AAA相关的设置，以通过Cisco ISE进行身份验证和授权。

策略要素

这些设置是最终绑定到身份验证策略或授权策略的元素。在本指南中，主要构建每个策略元素，然后将其映射到身份验证策略或授权策略。在成功完成到身份验证/授权策略的绑定之前，策略不会生效，了解这一点很重要。

第五步：使用外部身份源

外部身份源只是在ISE身份验证阶段使用的终端身份（计算机或用户）帐户驻留的源。Active Directory通常用于支持计算机帐户的计算机身份验证和/或Active Directory中最终用户帐户的用户身份验证。内部终端（内部）源不存储计算机帐户/主机名，因此，它不能用于计算机身份验证。

此处显示的是支持ISE的身份源以及可用于每个身份源的协议（身份验证类型）：

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP	Yes	Yes	No	No
EAP-MD5 CHAP	Yes	No	No	No
EAP-TLS PEAP-TLS (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

身份库功能

有关策略元素的更多信息，请参阅《思科身份服务引擎管理员指南，版本3.1 >章节：分段>策略集。

将Active Directory安全组添加到ISE

要在ISE策略中使用Active Directory安全组，必须先将该组添加到Active Directory加入点。从ISE GUI中，选择 **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory.**

有关将ISE 3.x与Active Directory集成的更多信息和要求，请完整阅读本文档：Active Directory与Cisco ISE 2.x集成。

注意：相同的操作适用于将安全组添加到LDAP实例。从ISE GUI中，选择 **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory.**

第六步：创建证书身份验证配置文件

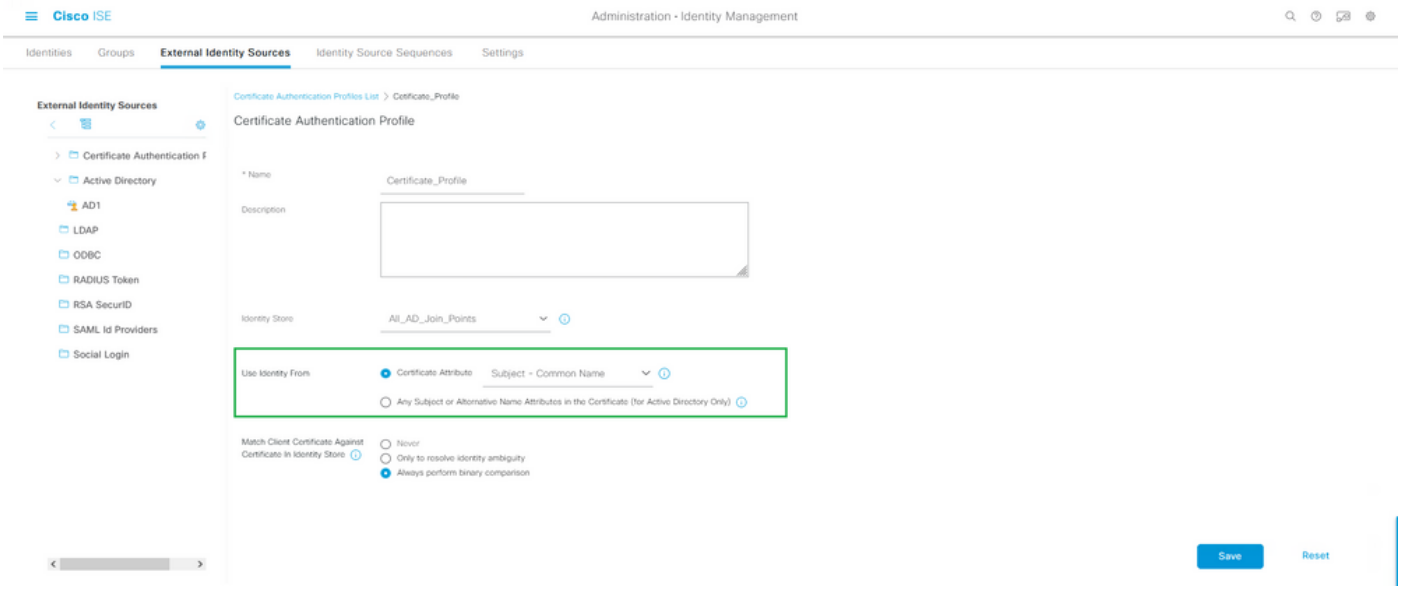
证书身份验证配置文件的目的是告知ISE身份（机器或用户）在EAP-TLS期间在ISE提供的客户端证书（终端身份证书）上可以找到哪个证书字段（在其他基于证书的身份验证方法期间）。这些设置绑定到身份验证策略以验证身份。从ISE GUI导航至 **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** 并点击 **Add.**

Use Identity From用于选择证书属性，从中可以找到身份的特定字段。选项包括：

> Subject - Common Name
> Subject Alternative Name
> Subject - Serial Number
> Subject
> Subject Alternative Name - Other Name
> Subject Alternative Name - EMail
> Subject Alternative Name - DNS

如果要将身份库指向Active Directory或LDAP（外部身份源），则可以使用Binary Comparison功能。二进制比较执行从使用身份源选择从客户端证书获取的Active Directory中的身份查找，在ISE身份验证阶段执行。如果不进行二进制比较，则仅从客户端证书获取身份，并且直到将Active Directory外部组用作条件时的ISE授权阶段或在ISE外部需要执行的任何其他条件时，才在Active Directory中查找身份。要使用二进制比较，请在身份库中选择可找到终端身份帐户的外部身份源（Active Directory或LDAP）。

这是身份位于客户端证书的Common Name(CN)字段中且启用了Binary Comparison（可选）时的配置示例：



证书身份验证配置文件

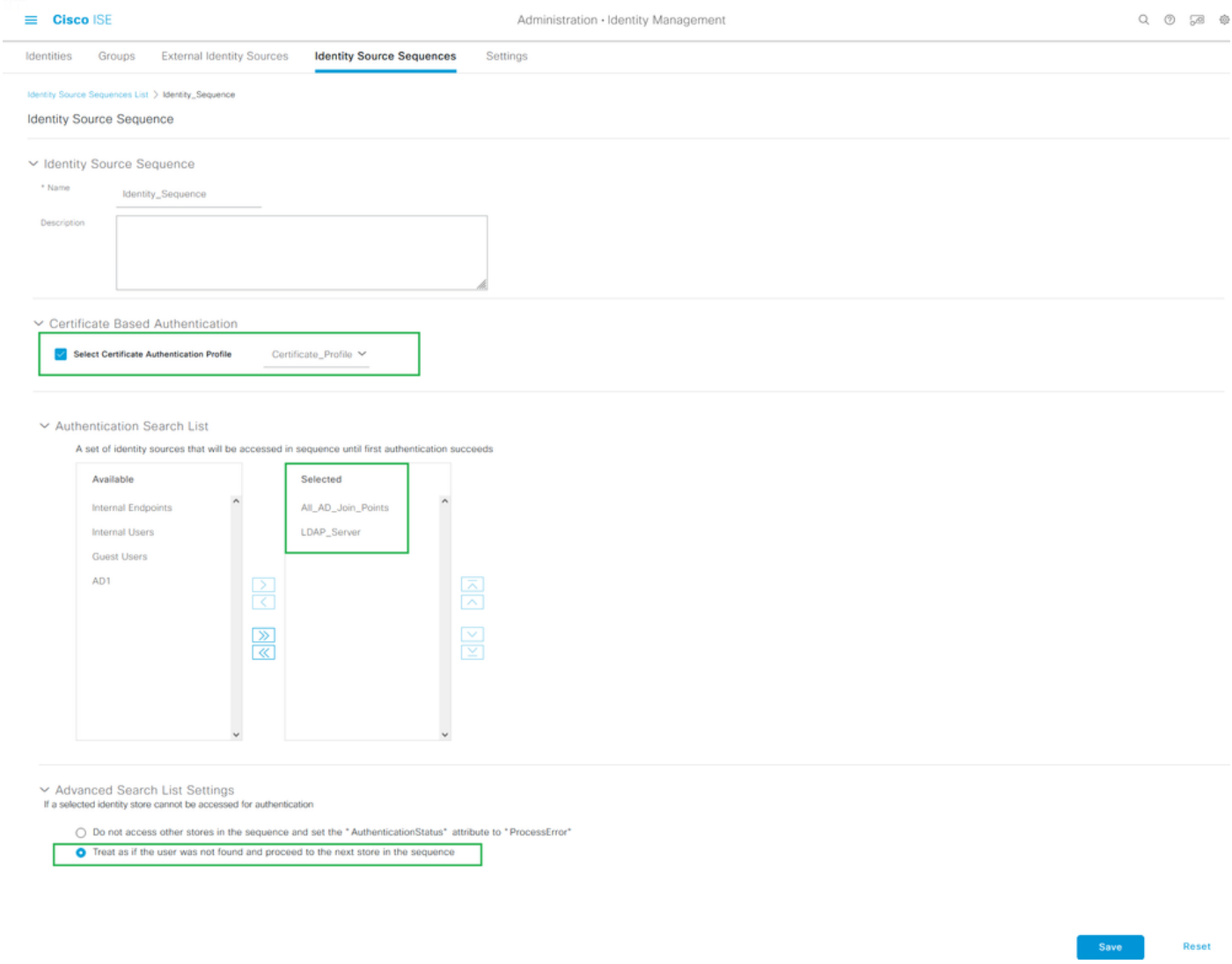
有关详细信息，请参阅Cisco身份服务引擎管理员指南，版本3.1 >章节：基本设置>Cisco ISE CA服务>配置Cisco ISE使用证书对个人设备进行身份验证>创建基于TLS的身份验证的证书身份验证配置文件。

步骤 7.添加到身份源序列

可以从ISE GUI创建身份源序列。导航至 **Administration > Identity Management**.低于 **Identity Source Sequences** ，单击 **Add**.

下一步是将证书身份验证配置文件添加到身份源序列，该序列授予包含多个Active Directory加入点或将内部/外部身份源的组合组合组合组合组合在一起的能力（根据需要），然后，该组合将绑定到 **Use** 列.

此处显示的示例允许首先对Active Directory执行查找，如果找不到用户，则随后在LDAP服务器上查找。对于多个身份源。请始终确保 **Treat as if the user was not found and proceed to the next store in the sequence** 复选框处于选中状态。因此，在身份验证请求期间会检查每个身份源/服务器。



身份源序列

否则，您也可以仅将证书身份验证配置文件绑定到身份验证策略。

步骤 8定义允许的协议服务

Allowed Protocols Service仅启用ISE在RADIUS身份验证期间支持的身份验证方法/协议。要从ISE GUI进行配置，请导航到Policy > Policy Elements: Results > Authentication > Allowed Protocols，然后作为元素绑定到身份验证策略。

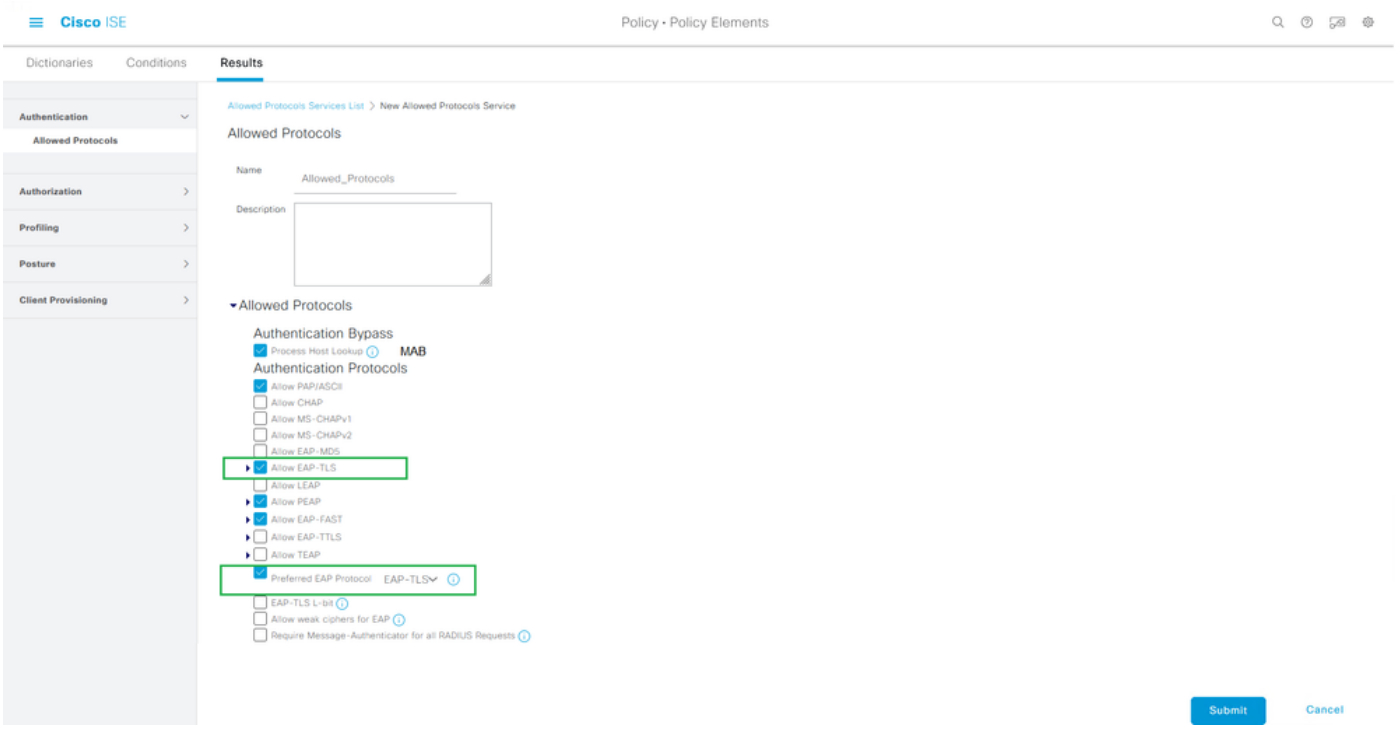
注意：Authentication Bypass > Process Host Lookup与ISE上启用的MAB相关。

这些设置必须与请求方（终端）上支持和配置的设置相同。否则，不会按预期协商身份验证协议，并且RADIUS通信可能会失败。在实际的ISE配置中，建议启用环境中使用的任何身份验证协议，以便ISE和请求方可以按预期进行协商和身份验证。

这些是默认值（折叠），在创建允许协议的新服务实例时。

注意：在此配置示例中，由于ISE和我们的请求方通过EAP-TLS进行身份验证，因此至少必须

启用EAP-TLS。



允许ISE在终端请求方的身份验证请求期间使用的协议

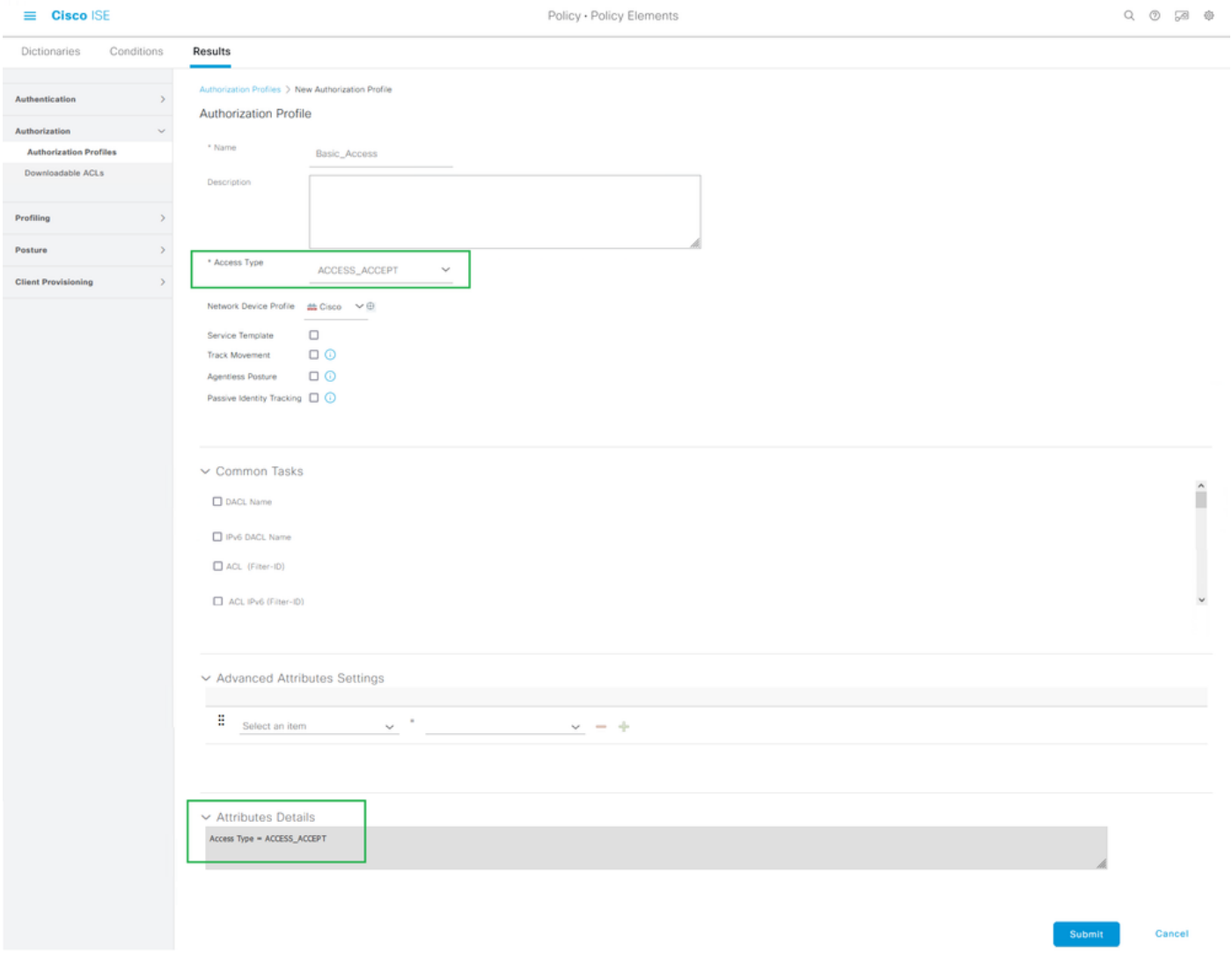
注：使用首选EAP协议设置为EAP-TLS的值会导致ISE请求EAP-TLS协议作为提供给终端IEEE 802.1x请求方的第一个协议。如果您打算经常在通过ISE进行身份验证的大多数终端上通过EAP-TLS进行身份验证，此设置非常有用。

步骤 9创建授权配置文件

需要构建的最后一个策略元素是授权配置文件，它绑定到授权策略并提供所需的访问级别。授权配置文件已绑定到授权策略。要从ISE GUI对其进行配置，请导航至 **Policy > Policy Elements: Results > Authorization > Authorization Profiles** 并点击 **Add**.

授权配置文件包含一个配置，该配置会生成从ISE传递至给定RADIUS会话的NAD的属性，这些属性用于实现所需的网络访问级别。

如图所示，它只是将RADIUS Access-Accept作为访问类型传递，但是，在初始身份验证时可以使用其他项目。注意最底层的属性详细信息，它包含ISE在匹配给定授权配置文件时发送到NAD的属性摘要。



授权配置文件 — 策略元素

有关ISE授权配置文件和策略的详细信息，请参阅《思科身份服务引擎管理员指南，版本3.1 >章节：分段>授权策略》。

安全策略

从ISE GUI创建身份验证和授权策略，选择 **Policy > Policy Sets.**默认情况下，在ISE 3.x上启用这些功能。安装ISE时，始终定义一个策略集，即默认策略集。默认策略集包含预定义和默认身份验证、授权和例外策略规则。

策略集按层次配置，允许ISE管理员将相似的策略按意图分组为不同的策略集，以便在身份验证请求中使用。自定义和分组策略几乎是无限的。因此，一个策略集可用于网络访问的无线终端身份验证，而另一个策略集可用于网络访问的有线终端身份验证；或用于任何其他独特和差异化策略管理方式。

思科ISE可以评估策略集，并且其中的策略使用自上而下的方法，当所述集的所有条件评估为True时，首先匹配给定的策略集；ISE根据此进一步评估与策略集匹配的身份验证策略和授权策略，如下所示：

1. 策略集和策略集条件的评估

2. 匹配策略集中的身份验证策略
3. 授权策略 — 本地例外
4. 授权策略 — 全局例外
5. 授权策略

策略例外全局存在于所有策略集，或者本地存在于特定策略集内。这些策略例外作为授权策略的一部分处理，因为它们处理为给定临时场景的网络访问授予的权限或结果。

下一部分介绍如何组合配置和策略元素以绑定到ISE身份验证和授权策略，以通过EAP-TLS对终端进行身份验证。

步骤 10创建策略集

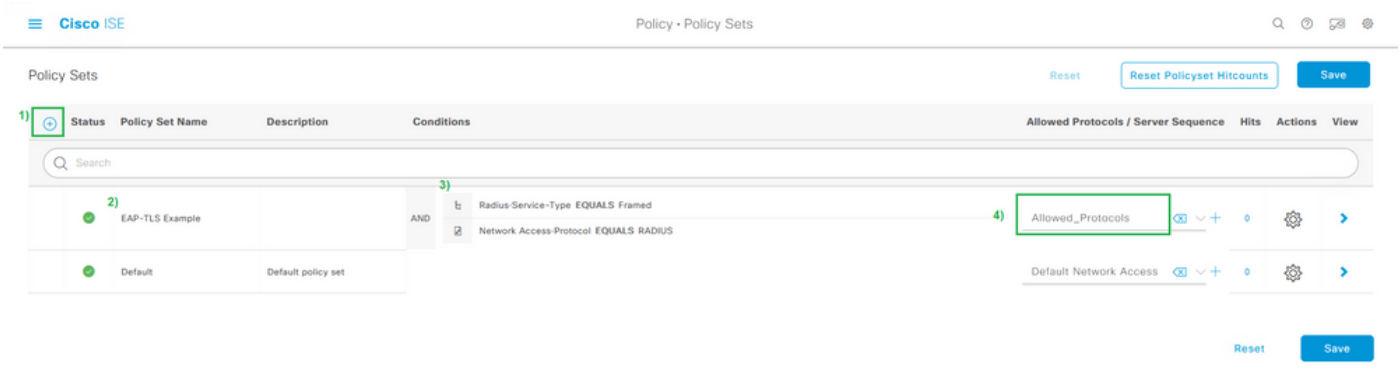
策略集是一个分层容器，由单个用户定义的规则组成，该规则指示允许的网络访问协议或服务器序列，以及身份验证和授权策略及策略例外，所有这些策略也都配置了用户定义的基于条件的规则。

要从ISE GUI创建策略集，请导航至 **Policy > Policy Set** 然后单击左上角的加号(+)图标，如图所示。

添加新策略集

策略集可以绑定/组合先前配置的此策略元素，并且用于确定在给定RADIUS身份验证请求(Access-Request)中要匹配的策略集：

- 绑定：允许的协议服务



定义策略集条件和允许的协议列表

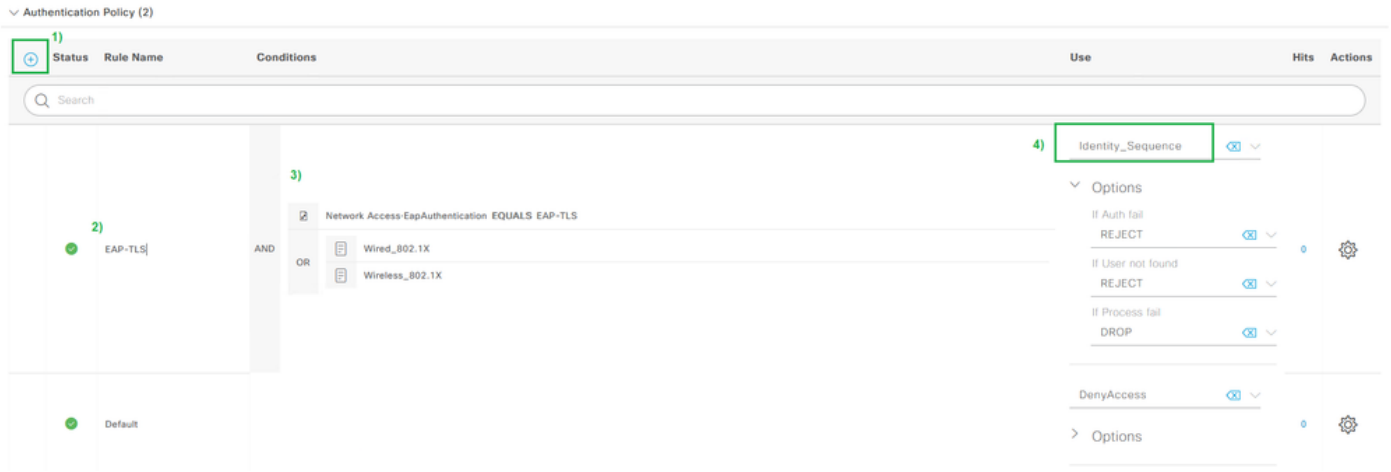
此示例使用在RADIUS会话中出现的特定属性和值来实施IEEE 802.1x（帧属性），即使重新实施RADIUS协议可能冗余也是如此。为了获得最佳效果，请仅使用适用于所需目的的唯一RADIUS会话属性，例如网络设备组或特定于有线802.1x、无线802.1x或有线和无线802.1x。

有关ISE上策略集的详细信息，请参阅《思科身份服务引擎管理员指南，版本3.1 >章节：分段>策略集、身份验证策略和授权策略部分。

步骤 11创建身份验证策略

在策略集内，身份验证策略绑定/组合这些之前配置为与条件一起使用的策略元素，以确定何时匹配身份验证规则。

- 绑定：证书身份验证配置文件或身份源序列。

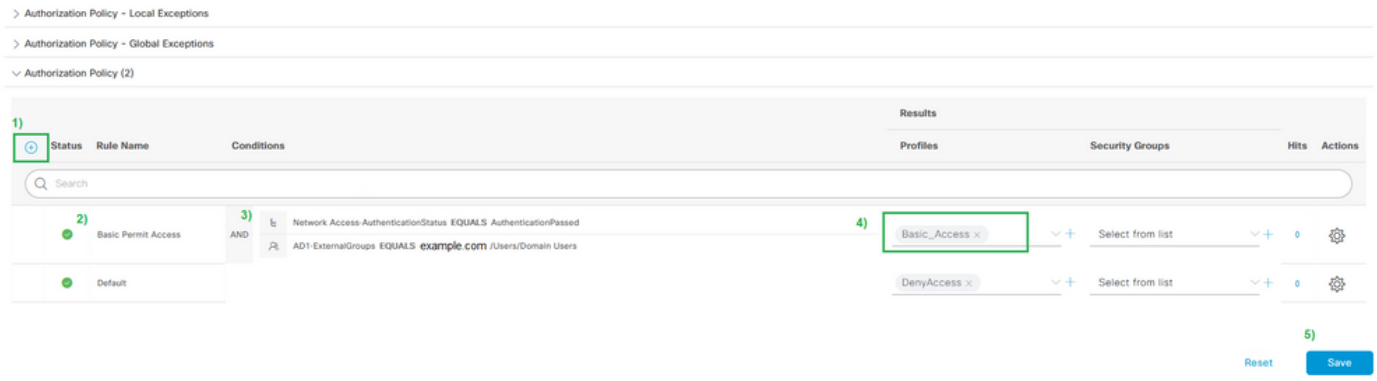


身份验证策略规则示例

步骤 12创建授权策略

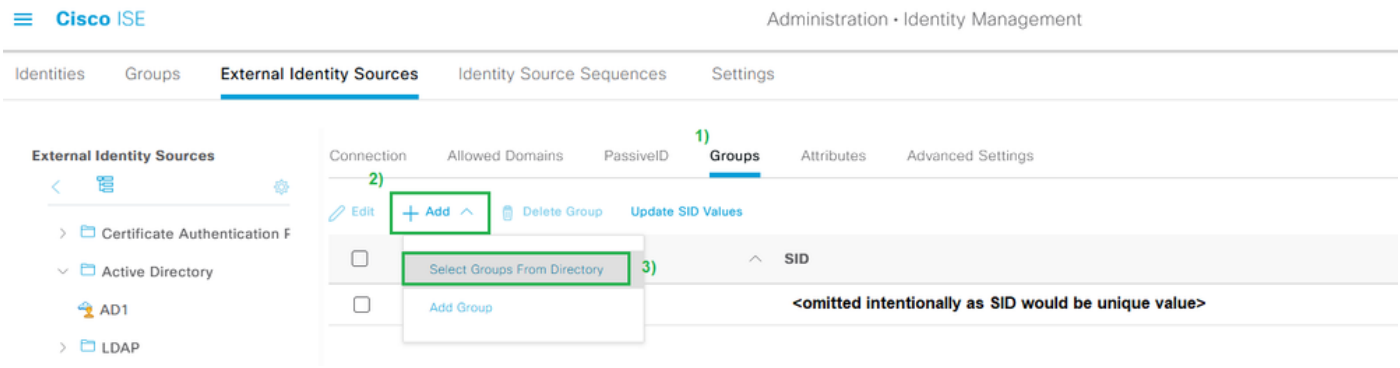
在策略集内部，授权策略绑定/组合这些之前配置为与条件一起使用的策略元素，以确定何时匹配授权规则。此示例适用于用户身份验证，因为条件指向Active Directory中的Domain Users安全组。

- 绑定：授权配置文件

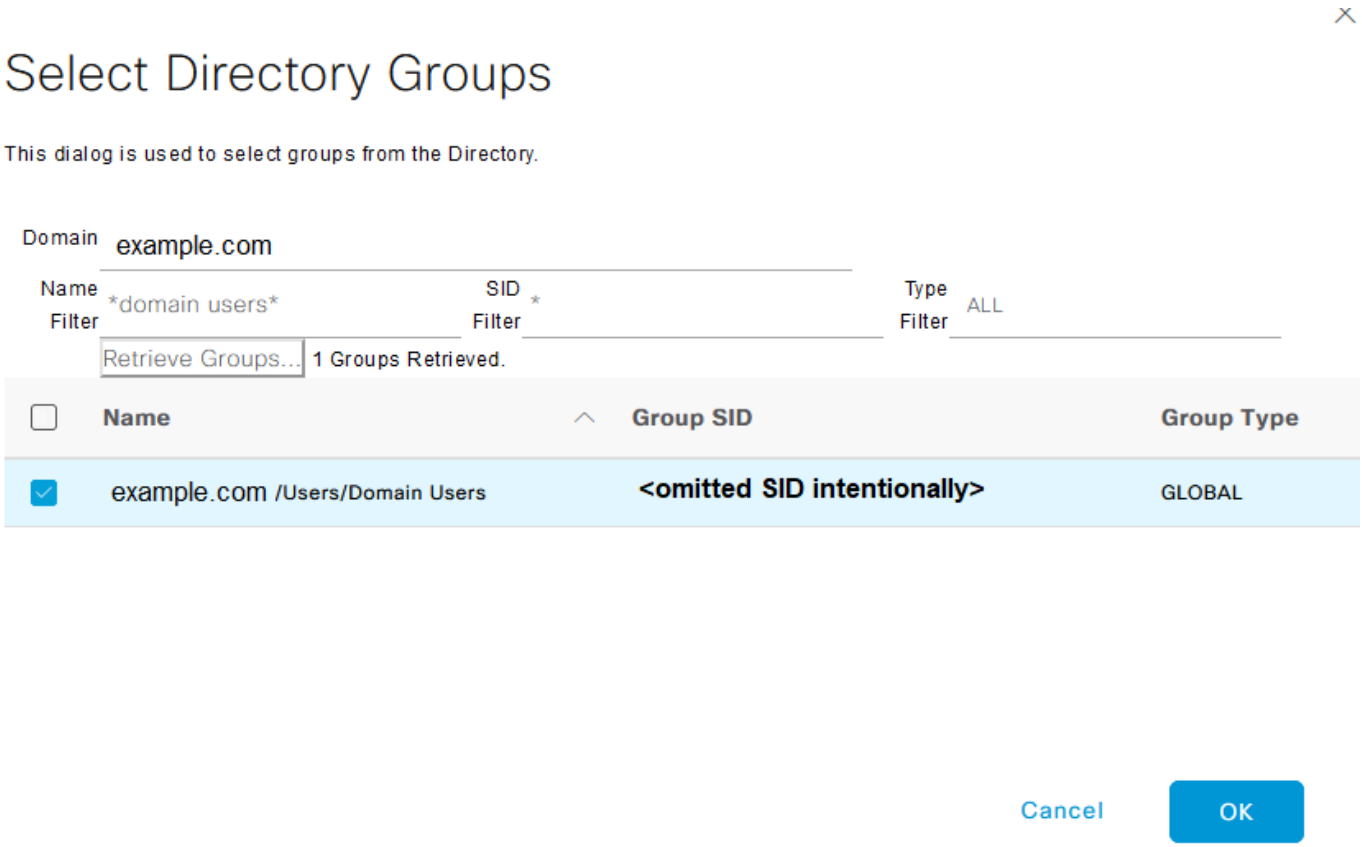


授权策略规则示例

要添加外部组（例如从Active Directory或LDAP），必须从外部服务器实例添加该组。在本示例中，它来自ISE UI: **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**.从“组”选项卡中，选择 **Add > Select Groups from Directory** 并使用名称过滤器搜索所有组(*)或特定组，例如域用户（*域用户*）以检索组。



要在ISE策略中使用外部组，必须从目录添加组



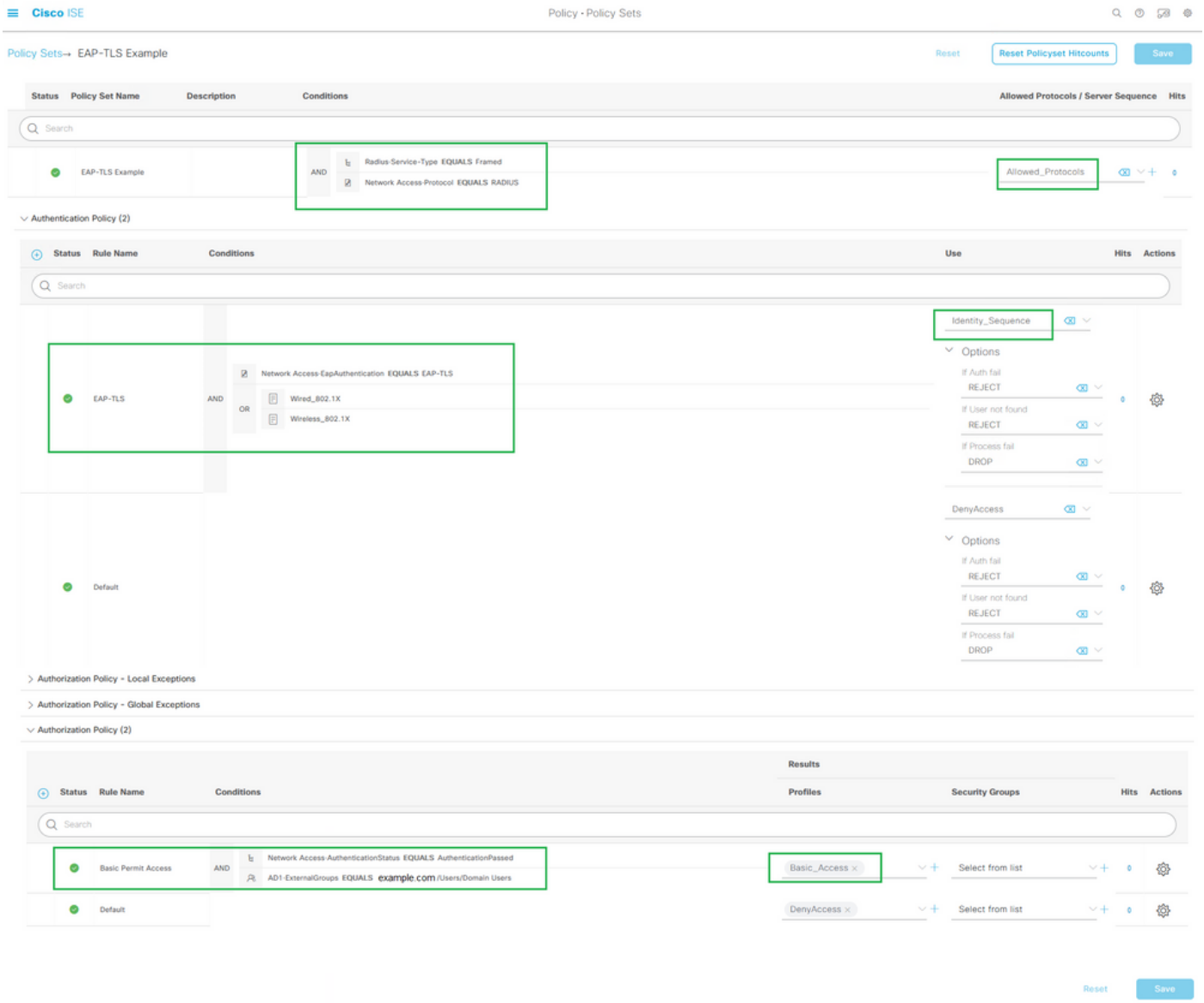
在外部目录内搜索 — Active Directory示例

选中每个组旁边的复选框后，您将在ISE内的策略中使用。要保存更改，请不要忘记单击Ok和/或Save。

验证

使用本部分可确认配置能否正常运行。

所有全局配置和策略元素绑定策略集后，配置看起来与通过EAP-TLS进行用户身份验证的此映像类似：

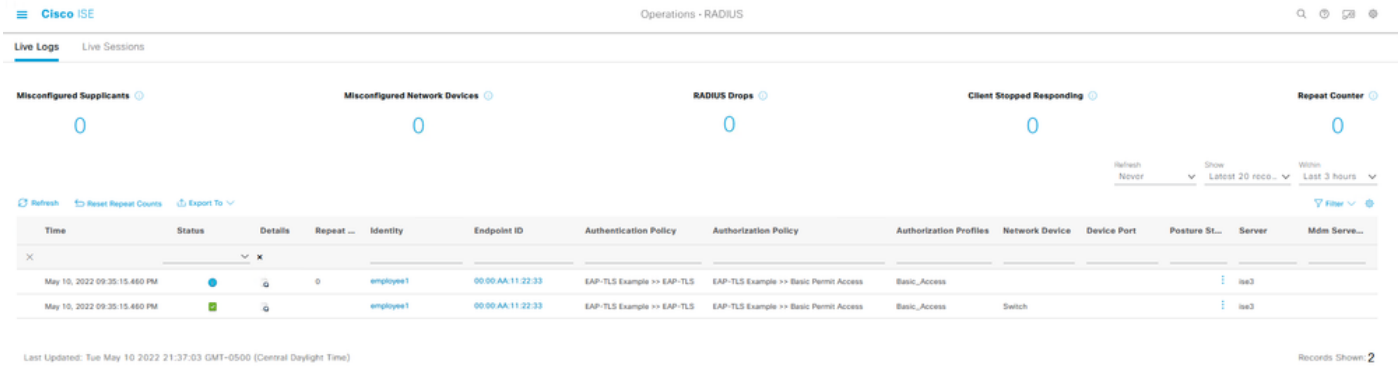


故障排除

本部分提供了可用于对配置进行故障排除的信息。

配置完成后，连接终端以测试身份验证。结果可在ISE GUI中找到。选择 **Operations > Radius > Live Logs**，如图所示。

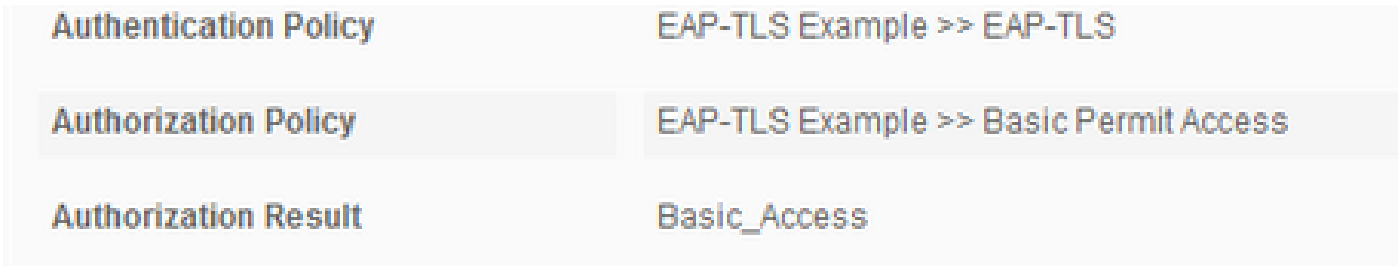
为了便于感知，RADIUS和TACACS+（设备管理）的实时日志可用于身份验证尝试/活动，直至过去24小时和过去100条记录。如果您希望在此时间之后看到此类报告数据，则需要使用报告，具体如下： **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications.**



Radius > Live Logs的输出示例

在ISE的RADIUS实时日志中，您期望找到有关RADIUS会话的信息，包括会话属性和其他有用信息，以诊断在身份验证流程期间观察到的行为。单击 **details** 图标可打开会话的详细视图，查看特定于此身份验证尝试的会话属性和相关信息。

要进行故障排除，必须确保匹配的策略正确无误。对于此配置示例，所需的身份验证和授权策略按预期匹配，如图所示：



在详细视图中，检查这些属性以验证身份验证是否按照本配置示例中的设计按照预期运行：

- Event
  - 这包含身份验证是否成功。
  - 在工作场景中，值为：5200 Authentication succeeded。

- 用户名
  - 这包括从提供给ISE的客户端证书提取的终端身份。
  - 在工作场景中，这是登录终端的用户的用户名（即来自上一个映像的employee1）。

- 端点 ID
  - 对于有线/无线，此值是来自终端的网络接口卡(NIC)的MAC地址。
  - 在工作场景中，这成为终端的MAC地址，除非连接是通过VPN进行的，在这种情况下，连接可以是终端的IP地址。

- 验证策略
  - 根据与策略条件匹配的会话属性显示给定会话的匹配身份验证策略。
  - 在工作场景中，这是配置的预期身份验证策略。
  - 如果看到其他策略，则表示与策略中的条件比较时的预期策略未评估为真。在这种情况下，请检查会话属性，并确保每个策略包含每个策略的不同但唯一的条件。

- 授权策略
  - 根据与策略条件匹配的会话属性显示给定会话的匹配授权策略。
  - 在工作场景中，这是配置的预期授权策略。
  - 如果看到其他策略，则表示与策略中的条件相比时的预期策略未评估为真。在这种情况下，请检查会话属性，并确保每个策略包含每个策略的不同但唯一的条件。

- 授权结果
  - 根据匹配的授权策略，这显示了在给定会话中使用的授权配置文件。
  - 在工作场景中，此值与策略中配置的值相同。为了便于审核，最好进行审核，并确保配置正确的授权配置文件。

- 策略服务器
  - 这包括身份验证尝试所涉及的ISE策略服务节点(PSN)的主机名。
  - 在工作场景中，您只能看到转到在需要（也称为边缘设备）上配置的第一个PSN节点的身份验证，除非PSN未运行或发生故障切换（例如由于延迟高于预期或身份验证超时）。

- 认证方法
  - 显示给定会话中使用的身份验证方法。在本例中，您看到值为dot1x。
  - 在基于此配置示例的工作场景中，您会看到值为dot1x。如果看到另一个值，则可能意味着dot1x失败或未尝试。

- 身份验证协议
  - 显示给定会话中使用的身份验证方法。在本示例中，您看到值为EAP-TLS。
  - 在基于此配置示例的工作方案中，您始终看到值为EAP-TLS。如果您看到另一个值，则请求方和ISE未成功协商EAP-TLS。

- 网络设备
  - 显示终端和ISE之间身份验证尝试所涉及的NAD（也称为边缘设备）的网络设备名称（在ISE中配置）。
  - 在工作场景中，此名称始终在ISE UI中指定： **Administration > System: Network Devices**. 根据该配置，NAD的IP地址（也称为边缘设备）用于确定身份验证来自哪个网络设备，该网络设备包含在NAS IPv4 Address会话属性中。

这绝不是为了进行故障排除或其他可视性而要检查的所有可能会话属性的完整列表，因为还有其他要验证的有用属性。建议查看所有会话属性，以开始熟悉所有信息。您可以看到包括步骤部分的右侧，它显示了ISE执行的操作或行为。

常见问题和故障排除技术

此列表包括一些常见问题和故障排除建议，但绝不是完整列表。相反，请以此为指南，开发您自己的技术，在涉及ISE时排除故障。

问题：遇到身份验证失败(5400 Authentication failed)或任何其他不成功的身份验证尝试。

- 如果遇到身份验证失败，请点击details图标，提供有关身份验证失败的原因和采取的步骤的信息。这包括故障原因和可能的根本原因。

- 由于ISE对身份验证结果做出决策，因此ISE具有信息来了解身份验证尝试失败的原因。

问题：身份验证未成功完成，失败原因显示“5440终端已放弃EAP会话并已启动新的”或“5411请求方停止响应ISE”。

- 此故障原因表明RADIUS通信在超时前未完成。由于EAP在终端和NAD之间，因此您需要检查在NAD上使用的超时并确保它至少设置五秒。

- 如果五秒还不足以解决此问题，则建议再增加五秒几次，然后重新测试以验证此技术是否解决了此问题。

- 如果上述步骤未解决此问题，则建议确保身份验证由相同且正确的ISE PSN节点处理，并且整体行为不指示异常行为，例如NAD和ISE PSN节点之间的延迟高于正常值。

- 此外，如果ISE未收到客户端证书，则最好验证终端是否通过数据包捕获发送客户端证书，然后终端（用户证书）无法信任ISE EAP身份验证证书。如果发现为true，则在正确的证书存储中导入CA链（根CA =受信任的根CA）| 中间CA =受信任中间CA)。

问题：身份验证成功，但是与正确的身份验证和/或授权策略不匹配。

- 如果遇到成功的身份验证请求，但是与正确的身份验证和/或授权规则不匹配，则建议查看会话属性，以确保使用的条件准确且存在于RADIUS会话中。

- ISE从自上而下方法评估这些策略（安全评估策略除外）。您需要首先确定匹配的策略是否高于或低于要匹配的所需策略。首先评估身份验证策略，与授权策略无关。如果身份验证策略正确匹配，则其在名为Steps的右侧部分的Authentication Details22037Authentication Passed。

- 如果所需策略高于匹配策略，则这意味着所需策略上的条件总和未评估为真。它会检查条件和会话中的所有属性和值，以确保其存在且不存在拼写错误。

- 如果所需策略低于匹配的策略，则意味着匹配了另一个策略（上述）而不是所需策略。这可能意味着条件值不够具体，条件会在其他策略中重复，或者策略的顺序不正确。虽然故障排除变得更加困难，但建议开始检查策略，以确定未匹配所需策略的原因。这有助于确定下一步要执行的操作。

问题：身份验证期间使用的身份或用户名不是预期值。

- 发生这种情况时，如果终端发送客户端证书，则很可能ISE不使用证书身份验证模板中的正确证书字段；在身份验证阶段进行评估。

- 检查客户端证书，找到所需的身份/用户名所对应的确切字段，并确保从中选择相同的字段：**ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

问题：由于客户端证书链中存在未知的CA，身份验证不成功，失败原因为EAP-TLS SSL/TLS握手12514。

- 如果客户端证书在CA链中具有在ISE UI上不受信任的证书，则会发生这种情况： **Administration > System: Certificates > Trusted Certificates.**

- 当客户端证书（在终端上）的CA链不同于签到ISE进行EAP身份验证的证书CA链时，通常会发生这种情况。

- 对于解决方案，请确保客户端证书CA链在ISE上受信任，ISE EAP身份验证服务器证书CA链在终端上受信任。
  — 对于Windows操作系统和Chrome，请导航至 **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.**
  — 对于Firefox：导入Web服务器受信任的CA链（不是终端身份证书）。

相关信息

- 思科身份服务引擎>安装和升级指南
- 思科身份服务引擎>配置指南
- 思科身份服务引擎>兼容性信息
- 思科身份服务引擎管理员指南，版本3.1 >章节：安全访问>在思科ISE中定义网络设备
- 思科身份服务引擎管理员指南，版本3.1 >章节：分段>策略集
- 思科身份服务引擎管理员指南，版本3.1 >章节：分段>身份验证策略
- 思科身份服务引擎管理员指南，版本3.1 >章节：分段>授权策略
- 思科身份服务引擎>配置指南> Active Directory与思科ISE 2.x的集成
- 思科身份服务引擎管理员指南，版本3.1 >章节：分段>网络访问服务>用户的网络访问
- 思科身份服务引擎管理员指南，版本3.1 >章节：基本设置>思科ISE中的证书管理
- 思科身份服务引擎管理员指南，版本3.1 >章：基本设置>思科ISE CA服务>配置思科ISE使用证书对个人设备进行身份验证>为基于TLS的身份验证创建证书身份验证配置文件
- 思科身份服务引擎>配置示例和技术说明>配置ISE 2.0证书调配门户
- 思科身份服务引擎>配置示例和技术说明>在ISE中安装第三方CA签名的证书
- 无线LAN(WLAN)>配置示例和技术说明>了解并使用WLC和ISE配置EAP-TLS
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。