Cisco TrustSec 操作指南：集中式 Web 身份验证

当前文档版本：3.0

2012 年 8 月 7 日

目录

简介

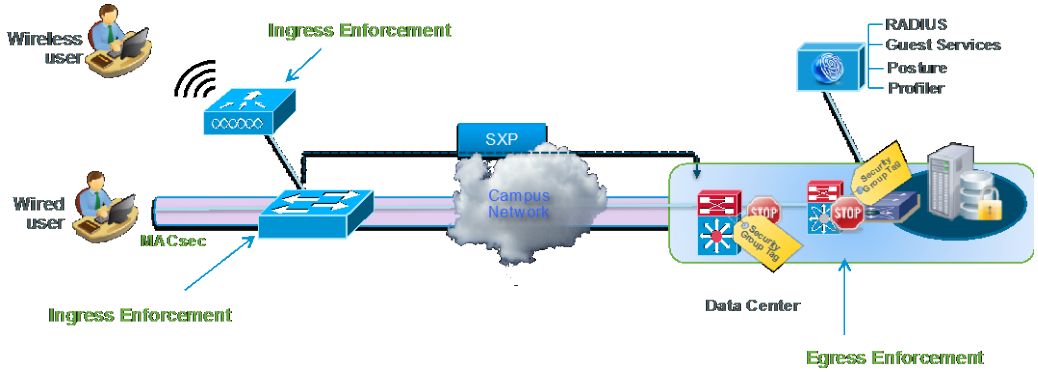
什么是 Cisco TrustSec 系统?

Cisco TrustSec® 是 Cisco SecureX Architecture™ 的一个核心组件，同时也是一种智能访问控制解决方案。TrustSec 针对整个网络基础设施中连接的用户和设备提供全面的可视性，并具有出色的内容和位置访问可控性，从而降低安全风险。

TrustSec 构建于您现有的身份感知接入层基础设施（交换机、无线控制器等）之上。该解决方案及其内部所有组件都已作为一个集成系统经过了全面的审核和严格的测试。

除了结合 IEEE 802.1X 与 VLAN 控制等基于标准的身份和实施模式外，TrustSec 系统还包括高级身份和实施功能，例如灵活的身份验证、可下载的访问控制列表 (dACL)、安全组标记 (SGT)、设备分析、安全状态评估等。

图 1：TrustSec 架构概览

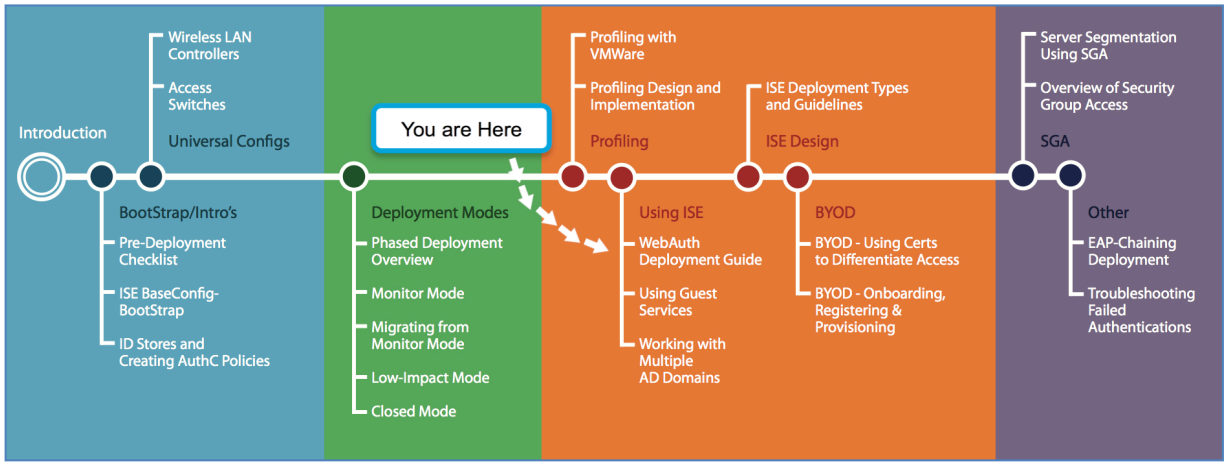


关于 TrustSec 操作指南

本系列操作指南文档由 TrustSec 团队编制，旨在介绍 TrustSec 部署的最佳实践。本系列文档相辅相成，引导读者成功实施 TrustSec 系统。您可以使用这些文档按照规定的路径部署整个系统，也可以只选择满足您特定需求的单独的使用案例。

此系列的每个指南都随附地铁式“定位”地图，帮助您确定文档所描述的阶段并准确查明您在 TrustSec 部署流程中所处的位置（图 2）。

图 2：操作指南导航图



“TrustSec 认证”意味着什么?

每个 TrustSec 版本（例如，TrustSec 版本 2.0、版本 2.1 等）都是通过认证的设计或架构。组成架构的所有技术都已通过全面的架构设计开发和实验室测试。操作指南要获得“TrustSec 认证”标记，其文档中论述的所有元素都必须符合以下条件：

- 设计中包含的产品必须为稳定版本。
- 系统中组件的部署、运行和管理必须表现为可重复的流程。
- 设计中使用的所有配置和产品均必须作为集成解决方案经过充分测试。

可能有许多功能都会对您的部署有所帮助，但如果它们未包括在经过测试的解决方案之中，则不会标记为“TrustSec 认证”。TrustSec 团队会竭力为这些文档提供定期更新，以及时包括新功能，并集成到 TrustSec 测试计划、试点部署和系统修订中。（例如，TrustSec 2.2 认证）。

此外，许多功能和方案虽已经过测试，但并不是最佳实践，因此不包括在这些文档中。例如，某些 IEEE 802.1X 计时器和本地 Web 身份验证功能不包含在内。

注：在本文档中，我们介绍了推荐的部署方法以及一些根据您环境所需的安全级别而定的不同选项。这些方法是思科最佳实践规定的 TrustSec 部署的示例和分步指导，有助于确保成功部署项目。

Web 身份验证

为什么要使用 Web 身份验证?

TrustSec 解决方案依赖于三种机制对用户和设备进行身份验证:

- IEEE 802.1X 是用于具有嵌入式请求方的用户和终端的主要身份验证协议。
- MAC 身份验证绕行 (MAB) 用于对不能执行 IEEE 802.1X 的终端进行身份验证，它需要维护所有可信任终端的 MAC 地址的数据库。
- Web 身份验证是第三种机制。它向用户提供一个 Web 门户，用户可以通过其提交凭证和对网络进行身份验证。

Web 身份验证主要在以下案例中使用:

- 对临时用户进行身份验证。

  组织必须为临时用户（如访客和承包商）提供网络访问权限。临时用户很可能使用不受组织的 IT 服务控制的设备。因此，临时用户将不会将终端配置为用于 IEEE 802.1X。Web 身份验证是用于对此类用户进行身份验证和签署可接受的用户策略的一种便利机制。对临时访问用户进行身份验证还有额外好处，即能够监控其活动，从而使组织满足合规性要求。

- 作为常规网络用户的备用身份验证机制。

  通常，如果常规网络用户将设备配置为 IEEE 802.1X 设备，则可能会出现身份验证失败的情况。造成这种情况的原因很多，例如密码/证书到期以及请求方配置错误。Web 身份验证可为此类用户提供一种对其自身进行身份验证的方法，并对阻止其通过 IEEE 802.1X 进行身份验证的问题加以修复。

- 设备注册。

  用户通常具有用于访问互联网和其他企业应用的个人设备，如平板电脑和智能手机。对于 IT 而言，能够将每个此类设备与用户关联起来，从而帮助确保设备具有适当的网络资源访问权限，其重要性日益增加。Web 身份验证可以用作一种允许用户注册其个人设备的方法。注册后，即可根据组织的安全策略和用户在组织中的角色，为设备提供完整或有限的网络资源访问权限。

Web 身份验证流程

典型的 Web 身份验证流程包括以下活动:

1. 用户尝试连接到有线网络。用户可以是 IEEE 802.1X 身份验证失败的访客/承包商或员工。IEEE 802.1X 身份验证失败的原因不尽相同，可能是请求方配置错误，也可能是凭证到期。
2. IEEE 802.1X 超时后，交换机将尝试执行 MAB。MAB 也会造成身份验证失败。
3. 此时，系统会调用 Web 身份验证。可以使用以下两种方式之一完成此任务:
   - 本地 Web 身份验证 (LWA) 。

     LWA 是网络接入设备、交换机或无线局域网控制器 (WLC) 在本地处理 Web 身份验证的过程。它要求通过 Web 门户页面配置每个网络接入设备。在生产网络中，配置和管理每个网络接入设备上的 Web 门户是一项艰难的任务。LWA 仅支持基于访问控制列表 (ACL) 的实施，并不支持 RADIUS 授权变更 (CoA)。根据分析，安全状态评估和实施需要进行 RADIUS CoA。

- 集中式 Web 身份验证 (CWA) 。

  CWA 是使用诸如思科身份服务引擎 (ISE) 之类的策略服务器，通过 Web 身份验证对用户集中进行身份验证的过程。利用中央策略服务器进行 Web 身份验证在操作上更易于实施。CWA 同时支持基于 ACL 和基于 VLAN 的实施。此外，CWA 还支持 RADIUS CoA。这样可根据分析进行状态评估和实施。

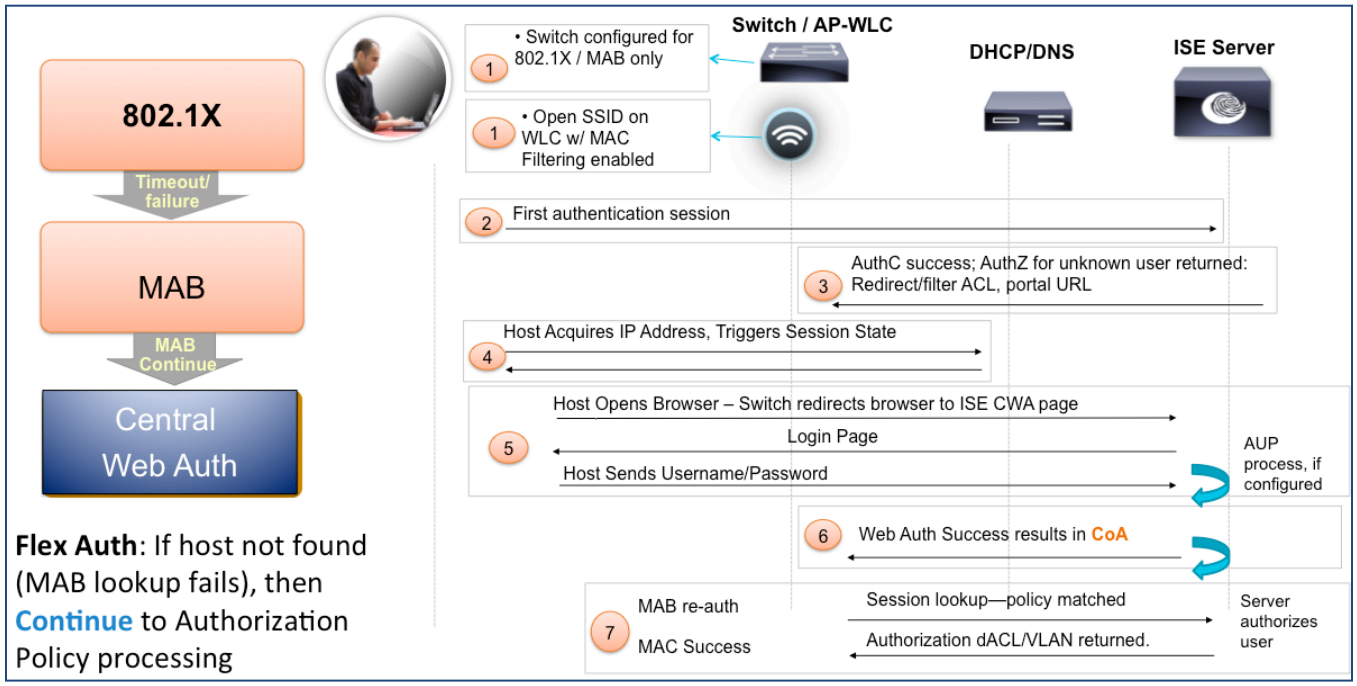
注：在思科无线局域网控制器软件版本 7.2 中推出了无线网络 CWA

Web 身份验证流程对于无线用户略有不同，此处用户连接到配置为仅接受 Web 身份验证的开放式 SSID。这种方式非常有效，用户与开放式 SSID 相关联后，他们便会位于 Web 身份验证过程的步骤 3。

思科建议使用 CWA，因为其操作更高效，并且根据分析支持其他功能，如状态评估和实施。为限制本文档的范围，我们将仅讨论 CWA。有关本地 Web 身份验证的信息，请参阅《TrustSec 2.0 设计和实施指南》。

图 3 详细说明 CWA 流程。

图 3 集中式 Web 身份验证处理流程



步骤 1 思科交换机针对 IEEE 802.1X 和 MAB 进行了配置。Cisco WLC 配置为具有支持 MAC 过滤的开放式 SSID。

注：有关为 CWA 配置交换机和 Cisco WLC 的详细步骤，请参阅以下操作指南。

HowTo-10-Universal_Switch_Configuration

HowTo-11-Universal_WLC_Configuration

步骤 2 用户连接到有线端口或与开放式无线 SSID 相关联。如果用户连接到有线端口，则第一个 IEEE 802.1X 超时或失败。思科交换机然后回退到 MAB。Cisco ISE 在内部终端身份库中找不到终端。此时，Cisco ISE 发送 RADIUS access-accept，而不是向交换机发送 RADIUS access-reject 消息。

步骤 3 连同 RADIUS access-accept 一起，Cisco ISE 还向下推送过滤器 ACL (PERMIT_ALL_TRAFFIC)、重定向 ACL (ACL-WEBAUTH-REDIRECT) 和 Web 门户 URL。RADIUS access-accept 指示交换机为常规网络流量打开端口，现在根据端口和重定向 ACL 会限制打开。

步骤 4 终端现在能够获取 IP 地址并解析 DNS 查询。它还会在 ISE 上触发新会话，此会话具有唯一会话 ID。

步骤 5 用户启动 Web 浏览器后，交换机或 Cisco WLC 就会将浏览器重定向到 ISE CWA Web 门户 URL。此时，用户会输入其凭证并接受任何已配置的可接受使用策略 (AUP)。

步骤 6 Cisco ISE 向网络接入设备发送 RADIUS CoA 信息。

步骤 7 网络接入设备重新验证终端并将其放在以前创建的同一会话中。Cisco ISE 现在向网络接入设备发送相应的访问策略。

CWA 配置说明

本节说明 Cisco ISE、思科交换机和思科无线局域网控制器上的各种重定向/过滤 ACL 和重定向策略如何操作以启用 CWA。

注：有关详细配置步骤，请参阅

交换机：全球交换机配置

WLC：无线局域网控制器的基本配置

在思科交换机上为 CWA 定义的访问控制列表

交换机端口 ACL

这是 ACL-ALLOW 或 ACL-DEFAULT，具体视部署使用监控模式还是低影响模式而定。此 ACL 控制在重定向之前允许哪些流量通过端口。此 ACL 仅特定于 Cisco IOS® 软件设备，其主要用途是在使用 Authentication Open 命令时限制流量。

思科交换机上的重定向 ACL

重定向 ACL 是 ACL-WEBAUTH-REDIRECT，在交换机上定义如下：

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the
redirection
```

Cisco ISE 指示交换机通过供应商特定属性来调用此重定向 ACL。供应商特定属性 (VSA) 在 ISE 中定义为授权配置文件的一部分。此 ACL 帮助交换机识别应重定向到 ISE 以允许进行集中式 Web 身份验证 (CWA) 的流量。

为使 Web 身份验证适用，您希望主机对诸如 DHCP 和 DNS 等基本网络服务具有访问权限。因此，不要重定向 DHCP 和 DNS 流量。ACL 中的 deny udp any any eq 53 语句指示交换机拒绝端口 53 上的用户数据报协议 (UDP) 流量的重定向，因此，主机将具有 DNS 服务访问权限。

注：由于现有错误，思科交换机会重定向 DNS 流量。变通方法是专门指示交换机不要重定向 DNS 流量。

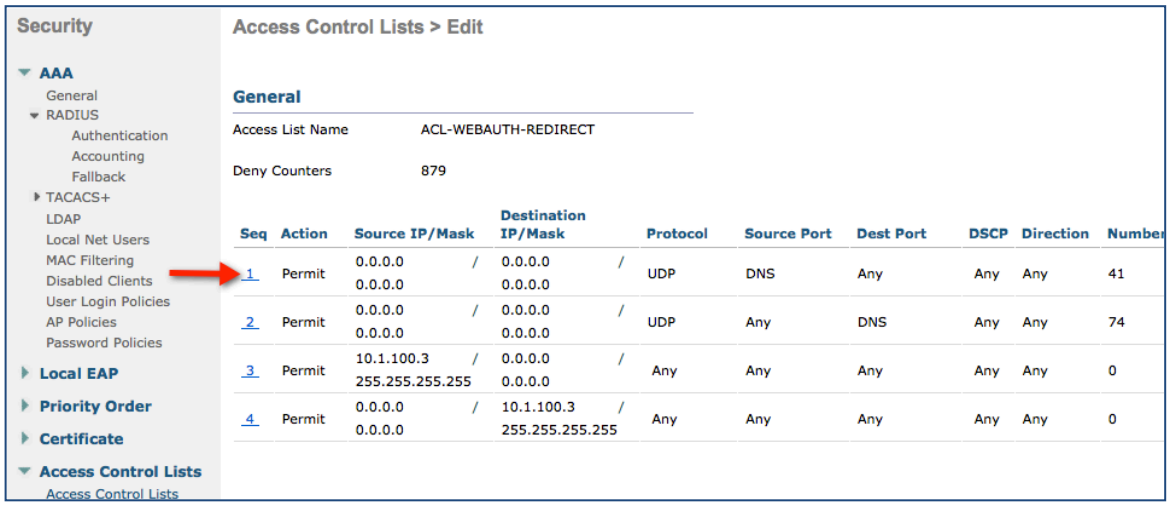
虽然我们允许主机访问基本网络服务，但是希望重定向来自主机的所有网络流量。ACL 中的 permit tcp any any eq 80 和 permit tcp any any eq 443 语句指示交换机重定向 HTTP 和 HTTPS 流量。流量应重定向到的 URL 在另一个 VSA 中定义，并会在后续部分中进行讨论。

在 Cisco WLC 上为 CWA 定义的访问控制列表

1. Cisco WLC 上的重定向 ACL

Cisco WLC 上的重定向 ACL 还命名为 **ACL-WEBAUTH-REDIRECT**，以维护与交换机配置的一致性。此 ACL 定义如下所示。

图 4 - 无线局域网控制器上用于 Web 身份验证的 ACL



如果您将交换机重定向 ACL 与 WLC 重定向 ACL 相比较，则会看到差异。我们使用语句 **deny udp any any eq 53** 停止在交换机上重定向 DNS 流量，而在 WLC 上则对 DNS 流量使用允许操作。这是因为 WLC 上的重定向 ACL 只是常规无线 ACL。因此，ACL 规则对于诸如 DNS 和流向 ISE (10.1.100.3) 的流量等允许的流量具有相应的允许语句。任何其他流量都由隐式拒绝语句捕获，并且重定向到 ISE 中设置的重定向 URL。当 ISE 通过授权配置文件发送 VSA 时，将会调用此 ACL。

总之，

a. 在思科交换机和 Cisco WLC 上均必须提前配置重定向 ACL ACL-WEBAUTH-REDIRECT。

b. 重定向 ACL 使用 ISE 授权配置文件中定义的 VSA 进行调用。

c. 流量应重新定向到的 URL 在 ISE 授权配置文件中还指定为 VSA。

d. 在交换机上定义重定向 ACL 时，拒绝语句会免除对流量进行重定向，而允许语句会重定向指定的流量。

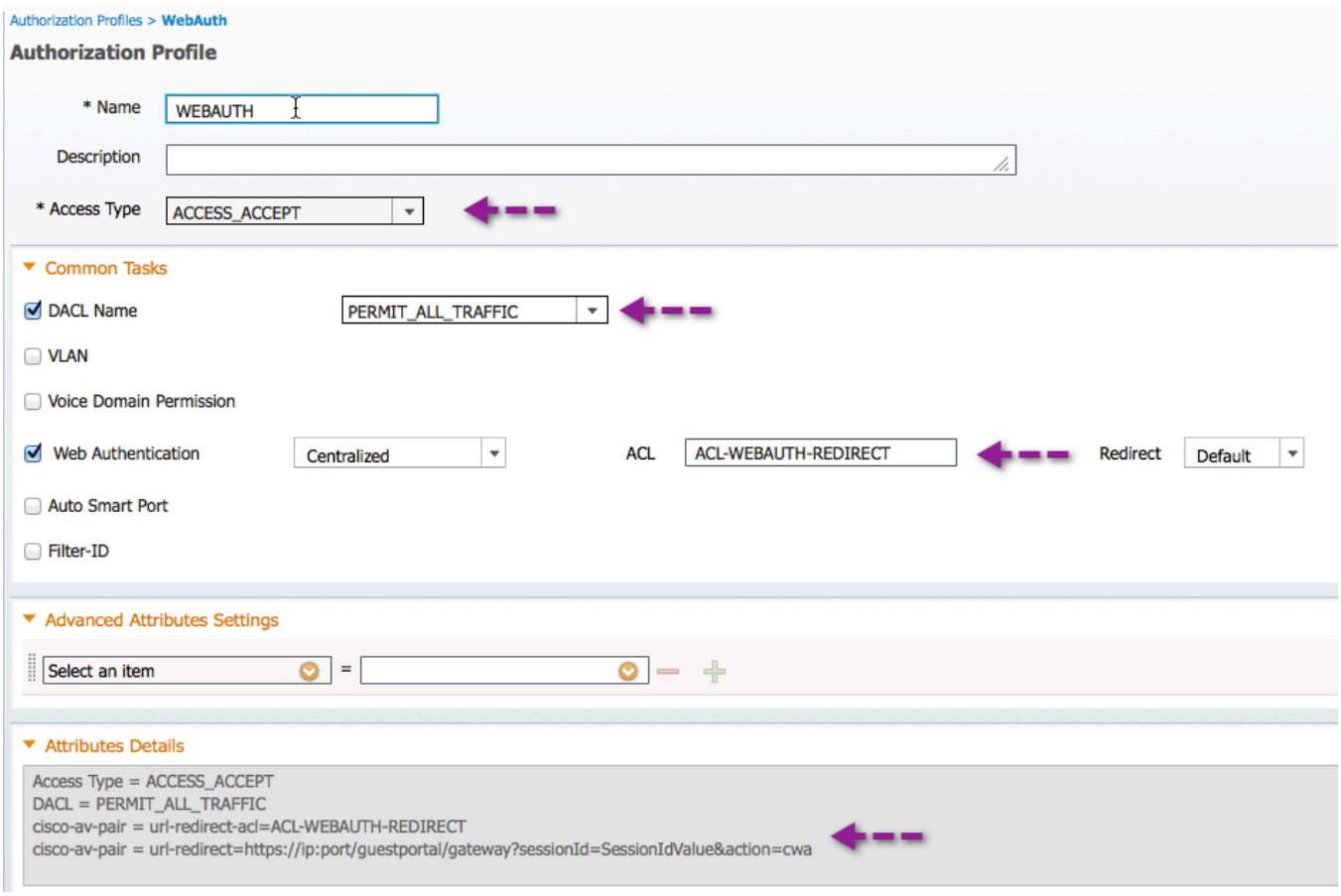
e. WLC 上的重定向 ACL 只是常规无线 ACL。允许语句会免除对流量进行重定向，而拒绝语句会重定向指定的流量。ACL 在末尾具有一个隐式拒绝语句。

f. 此外，ISE 授权策略还可以发送 DACL 来替换现有预身份验证交换机端口 ACL。

用于 CWA 的 Cisco ISE 授权配置文件

本节将说明如何在 Cisco ISE 授权策略中定义各种 ACL 和重定向 URL。根据“低影响”操作指南中的配置，WEBAUTH 的 ISE 授权配置文件应如下图所示。

图 5 - ISE 中定义的 WebAuth 身份验证配置文件



授权配置文件具有以下内容：

a. RADIUS access_accept

这向交换机端口表明身份验证成功。因此，交换机会打开端口并允许流量通过。

b. PERMIT_ALL_TRAFFIC DACL

这是可下载的交换机端口 ACL。此 ACL 将替换已在交换机端口上配置的预身份验证 ACL。

c. Web 身份验证参数

此处列出了三个不同的参数。首先，我们将 Web 身份验证方法设置为“集中式”。然后，提到需要应用什么 ACL。在交换机上，我们会调用重定向 ACL，在 WLC 上会调用无线 ACL。重定向字段指定重定向 URL。在这种情况下，我们即将使用默认 ISE 访客门户。

这是您更改为将 Web 身份验证用于状态评估、请求方配置和设备注册所需的同一组参数。

d. 属性详细信息

本节自动填充。它显示使用的各种供应商特定属性。请注意如何将 ACL-WEBAUTH-REDIRECT 列为 url-redirect-acl。url-redirect 值指定流量应重定向到的 URL。

附录 A：参考

TrustSec 系统：

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

- 对于 Cisco Catalyst 2900 系列交换机：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000 系列交换机：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000-X 系列交换机：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 4500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 6500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- 对于 Cisco ASR 1000 系列路由器：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html