

ISE客户占RADIUS/802.1x身份验证配置示例

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[背景信息](#)

[Configure](#)

[所有版本的配置注意事项](#)

[ISE 1.1.1的配置及以后](#)

[Related Information](#)

[Introduction](#)

本文描述如何配置所有基于RADIUS的认证的客户帐户，以及基于PORTAL的认证，在思科身份服务引擎(ISE)。

[Prerequisites](#)

[Requirements](#)

在本文的程序要求思科身份服务引擎(ISE)和IEEE 802.1x基础知识。

[Components Used](#)

本文的信息根据思科身份服务引擎(ISE)。

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

关于文件规则的信息，请参见[Cisco技术提示规则](#)。

[背景信息](#)

在本文描述的此功能不同地运作在ISE版本之间。

- 在ISE 1.1.1前：所有客户帐户在一个非激活状态坚持，当他们被创建时，并且他们没有被激活直到首次登录通过客户门户。使用RADIUS时，当在非激活状态，他们不能登陆。
- ISE 1.1.1及以后：在默认组创建的客户帐户(ActivatedGuest)是活跃的，在他们被创建之后。Cisco Bug ID [CSCuc76477](#) (仅限注册用户)运用于这些版本。如果使用，由于此问题，帐户没有创建以有效状态DefaultFirstLogin时间配置文件。为了解决此问题，请使用一个不同的默认或自定义时间配置文件。

Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

所有版本的配置注意事项

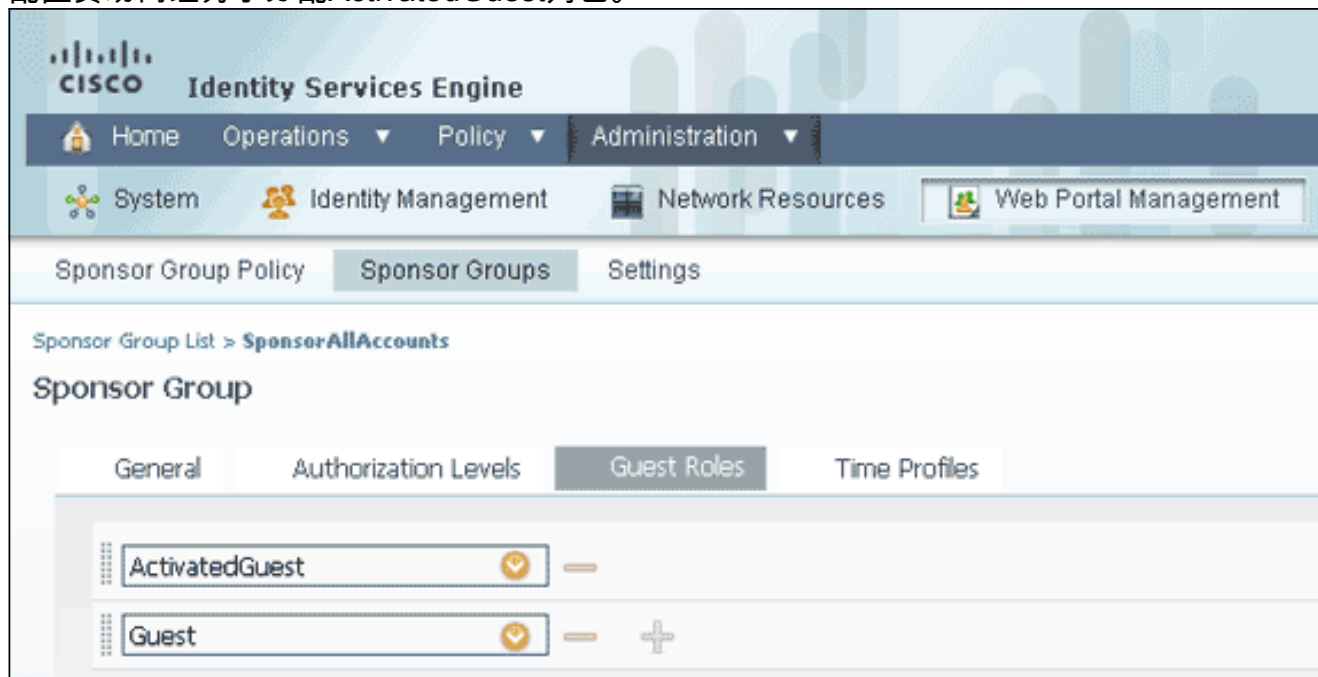
这些考虑适用于所有版本：

- 使用客户帐户的所有认证规则应该有内部用户作为来源。
- 这样顺序的所有授权规则在客户(在ISE1.1.1)前或被激活的客户(ISE 1.1.1应该配比及以后)。
- 赞助商门户和自己注册配置在正确的组应该安置客户帐户。对于ISE 1.1.1，正确的组必须是ActivatedGuest为了通过客户门户避免首次登录的需求。

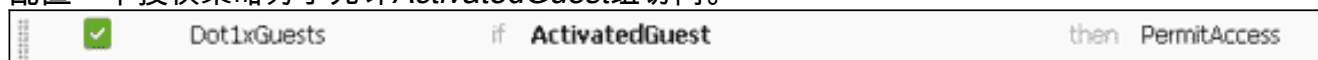
ISE 1.1.1的配置及以后

完成这些步骤为了配置ISE 1.1.1及以后：

1. 配置赞助商组为了分配ActivatedGuest角色。



2. 配置一个授权策略为了允许ActivatedGuest组访问。



赞助商用户应该当前能用ActivatedGuest角色创建客户。用户被创建这里应该能通过802.1x或支持内部身份存储的其他认证方法登录。在实际认证日志，您应该看到在此镜像显示的文本：

Identity Group:	ActivatedGuest
Allowed Protocol Selection Matched Rule:	Default
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users

Note: 身份组是正确的，并且身份存储是“内部用户”。

[Related Information](#)

- [Technical Support & Documentation - Cisco Systems](#)