ISE 2.0 ：ASA CLI TACACS+认证和Authorization命令配置示例

Contents

Introduction

本文描述如何用身份服务引擎(ISE) 2.0配置TACACS+认证和Authorization命令在Cisco可适应的安全工具(ASA)上及以后。ISE使用本地身份存储存储资源例如用户、组和终端。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- ASA防火墙是完全能操作的
- ASA和ISE之间的连接
- ISE服务器被引导

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco身份服务引擎2.0
- Cisco ASA Software Release 9.5(1)

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.

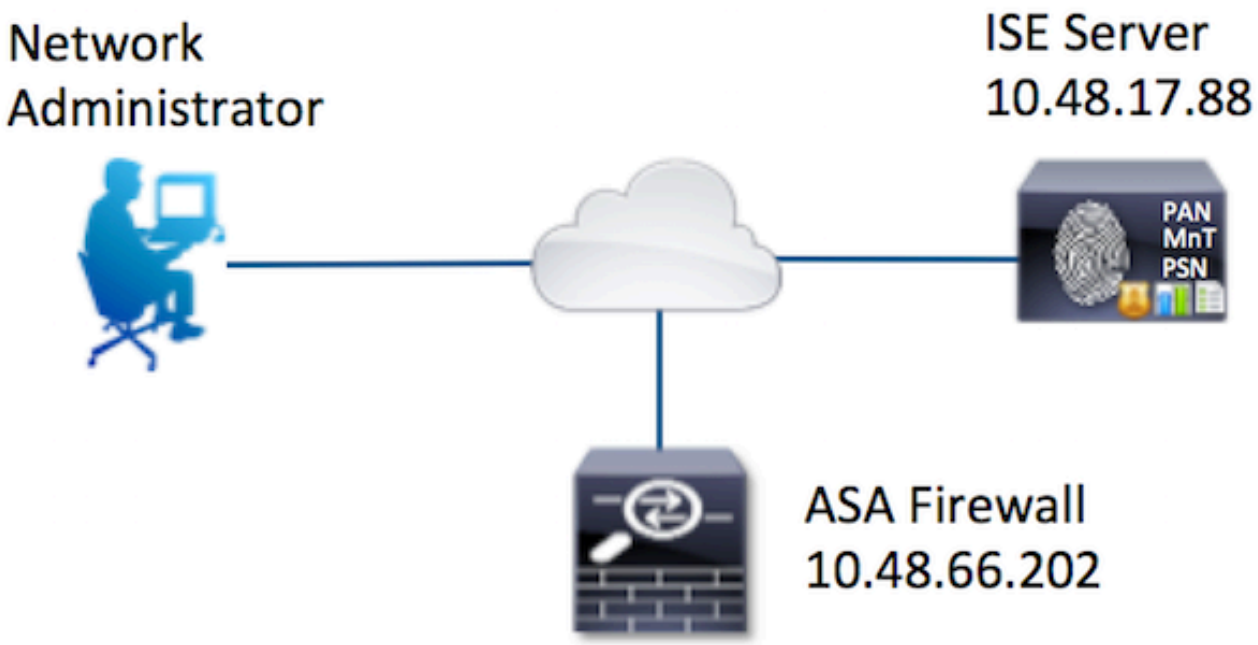
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

配置的AIM对：

- 通过内部身份存储验证SSH用户
- 认证SSH用户，因此它将被放置到privileged EXEC模式在登录以后
- 检查并且发送每个被执行的命令到验证的ISE

Network Diagram



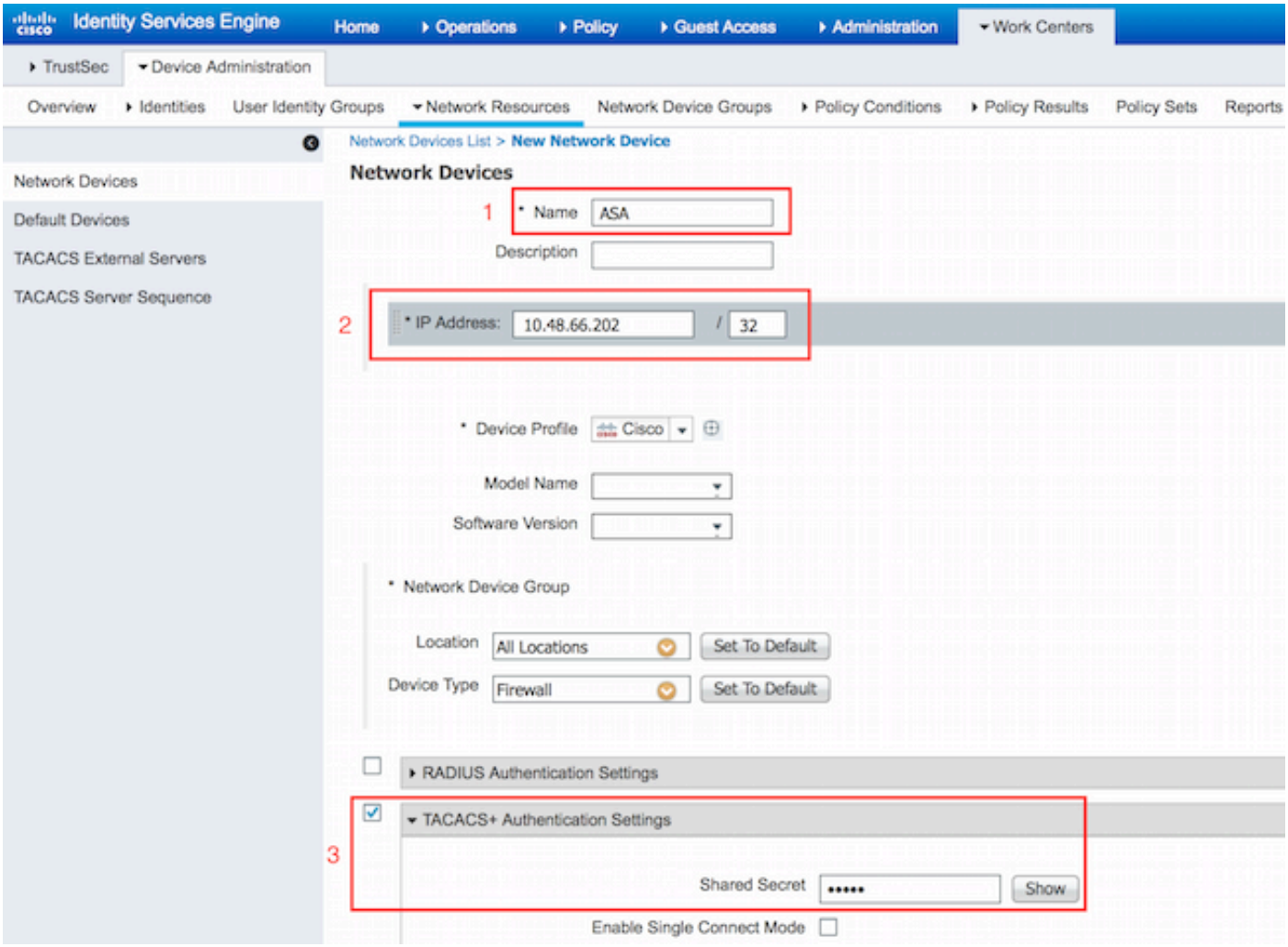
配置

配置认证和授权的ISE

两个用户被创建。用户**管理员**是**网络管理员**本地身份组的部分在ISE的。此用户有充分的CLI权限。用户**用户**是**网络维护小组**本地身份组的部分在ISE的。此用户允许执行只显示命令和ping。

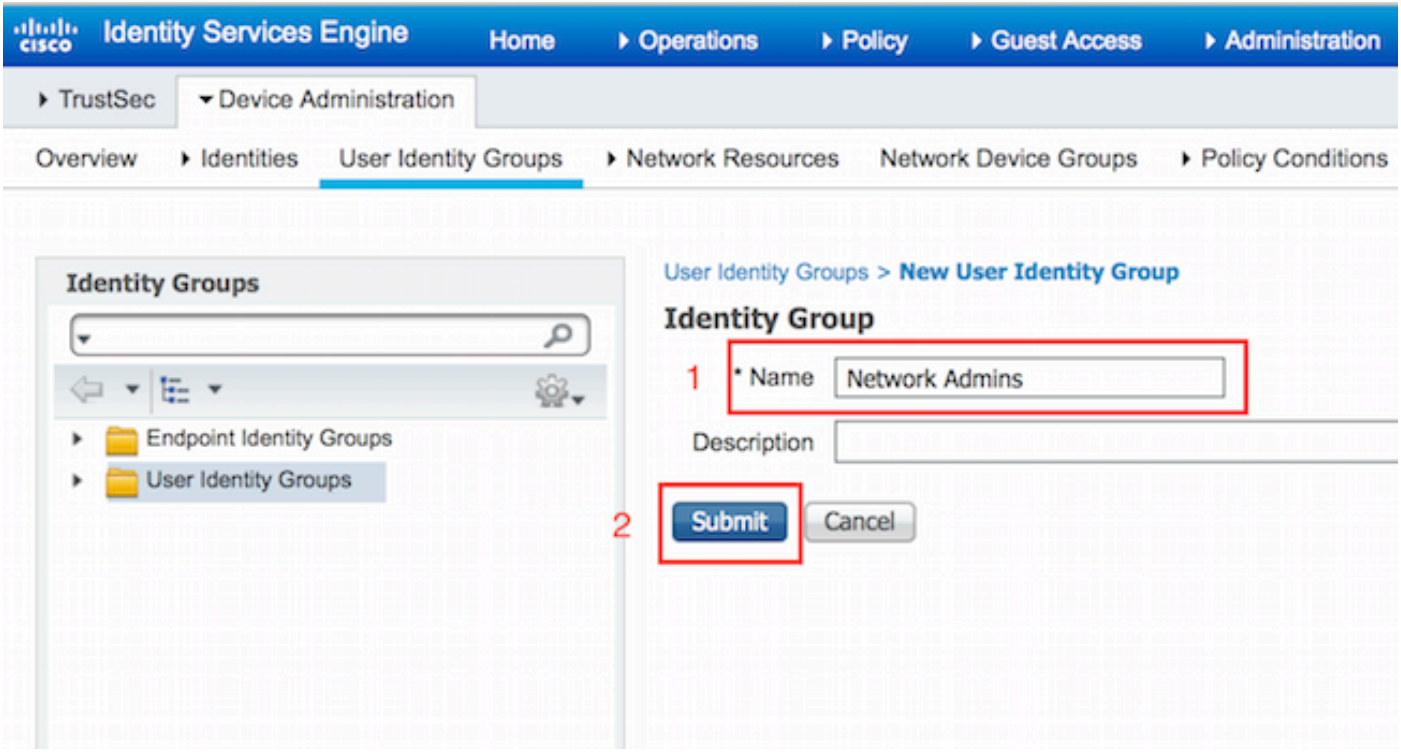
添加网络设备

连接到**工作区>设备Administration >网络资源>网络设备。**单击 **Add**。提供名字， IP地址，选择**Settings复选框的TACACS+认证**并且提供**被共享的密钥**。随意地设备类型/位置可以指定。



配置用户身份组

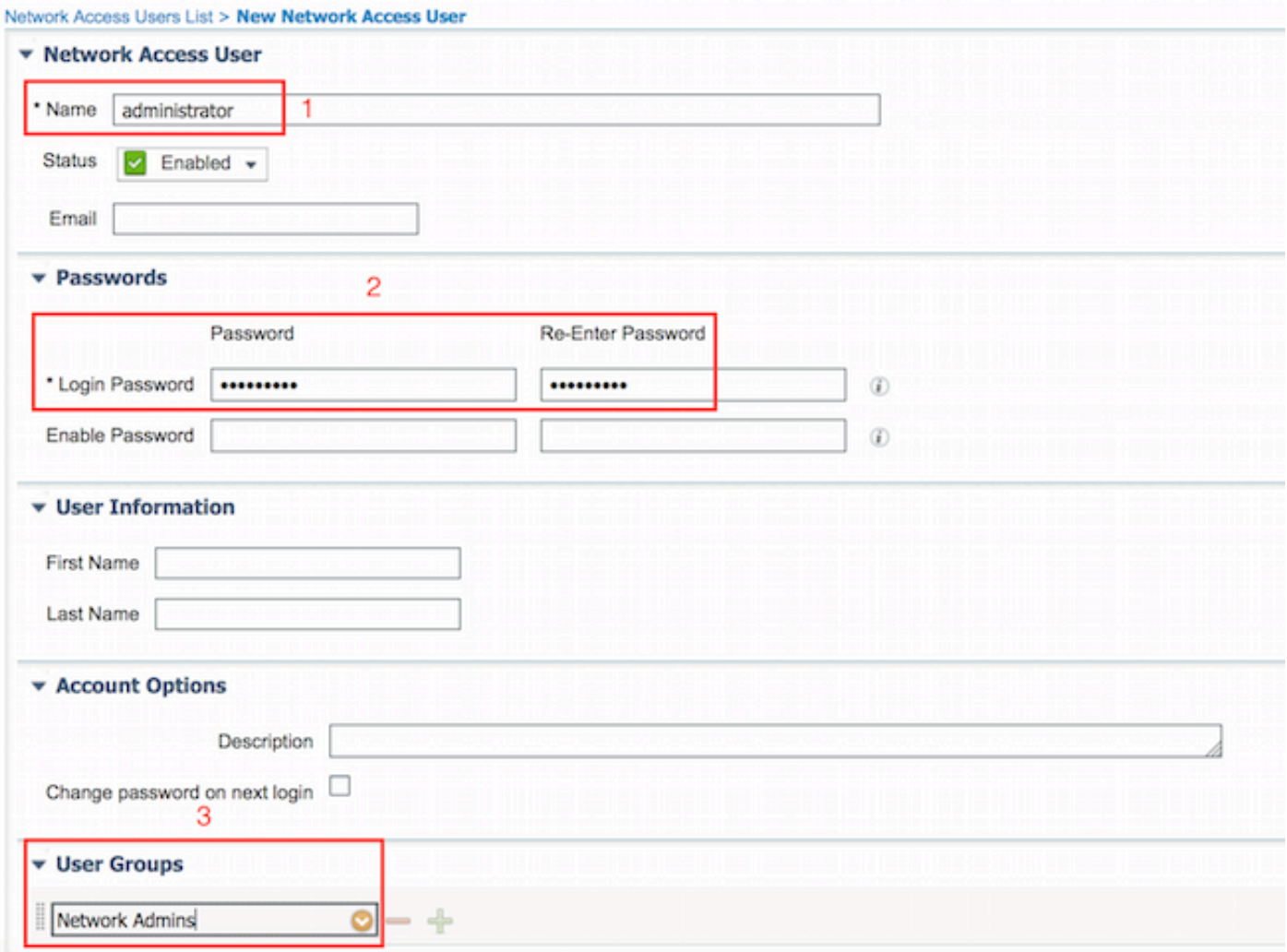
连接对**工作区>设备Administration >用户身份组。**单击 **Add**。提供名字并且点击**提交。**



重复同一个步骤对configure network**维护小组**用户身份组。

配置用户

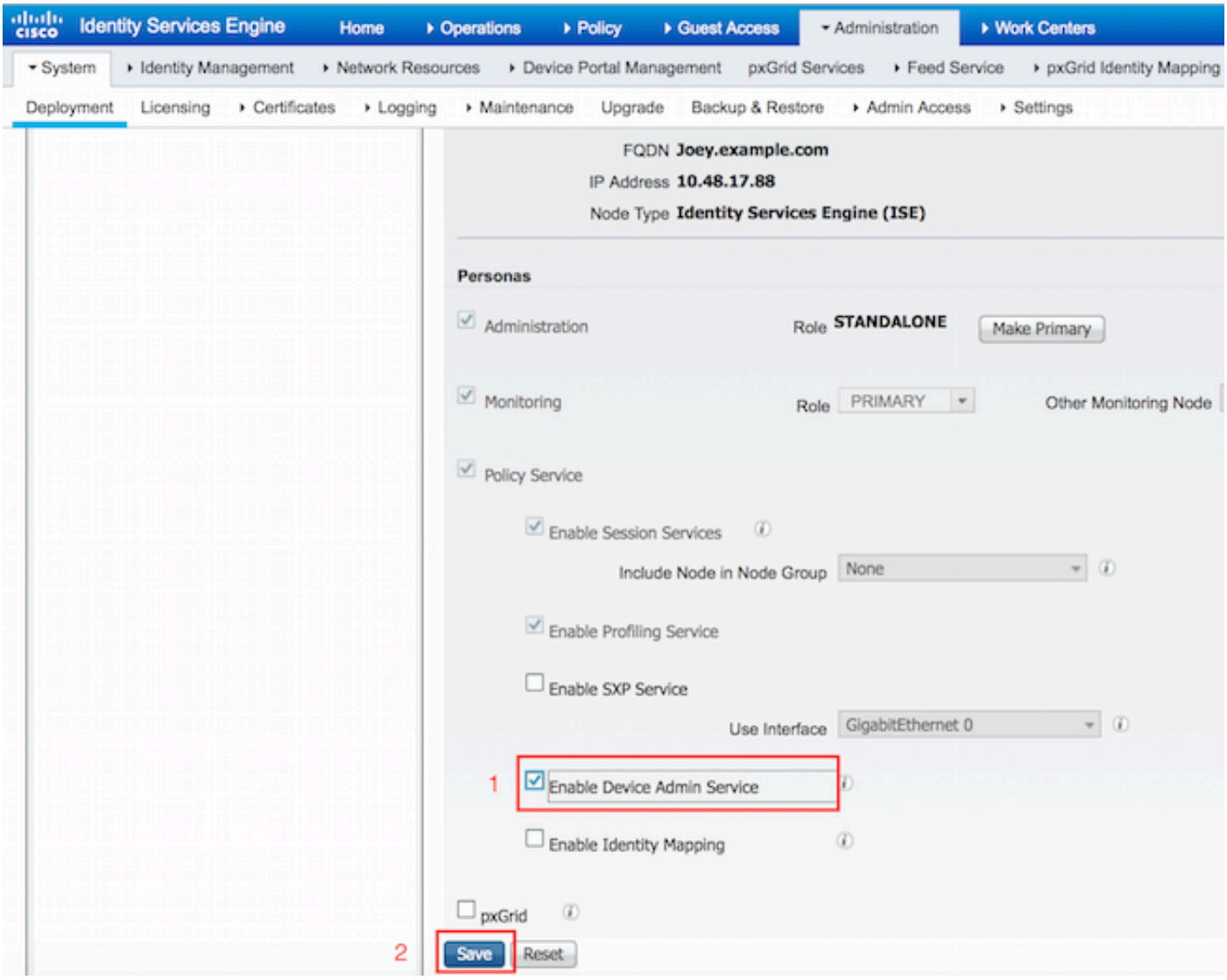
连接对**工作区>设备Administration >身份> Users。**单击 Add。提供名字，登录密码指定用户组并且点击**提交**。



重复步骤配置用户**用户**和分配**网络维护小组**用户身份组。

以启用设备Admin服务

连接对**管理>System >配置。**select要求了节点。选择**以启用设备Admin服务**复选框并且点击**“Save”。**

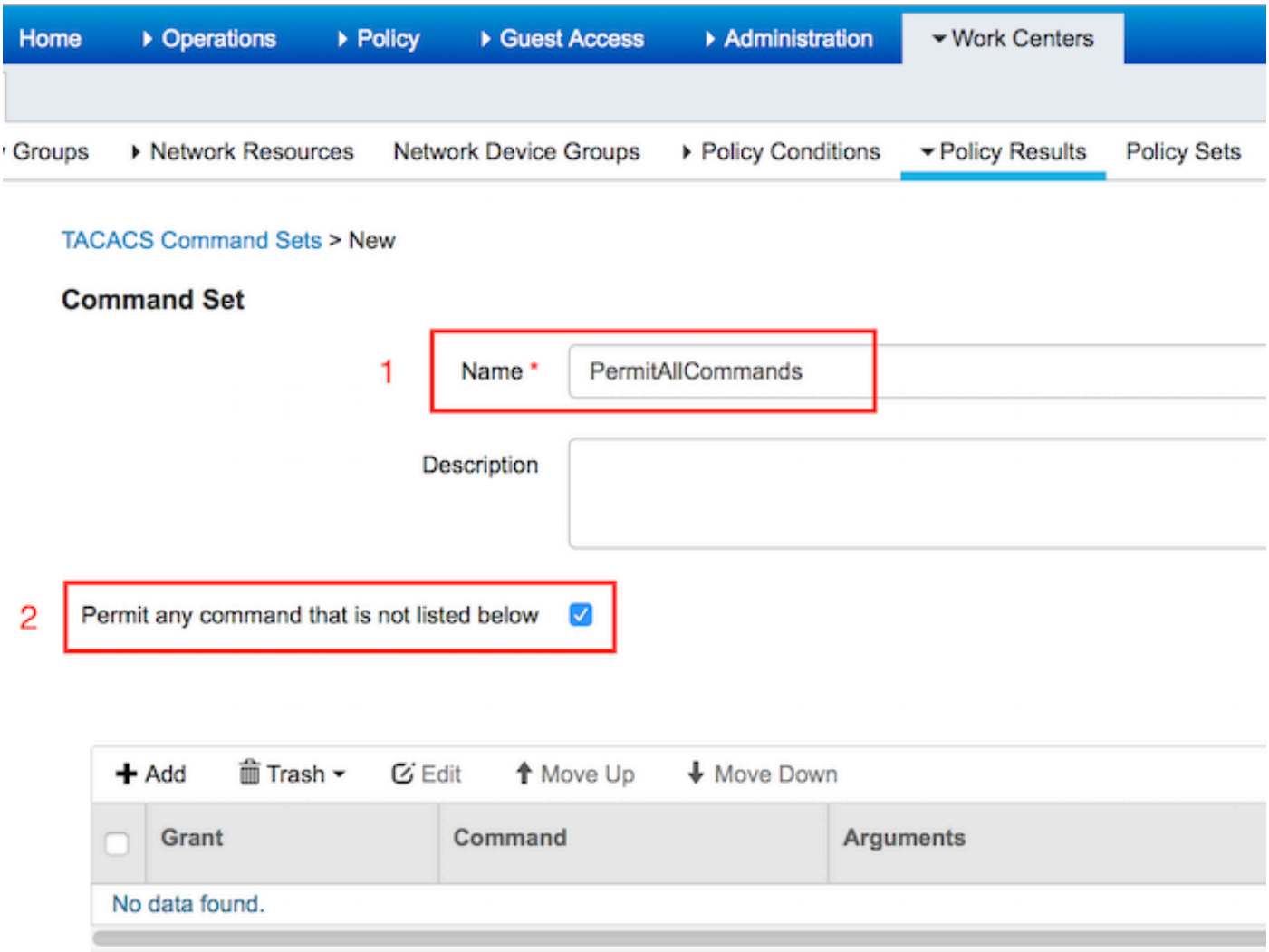


Note:对于TACACS您需要安排分开的许可证安装。

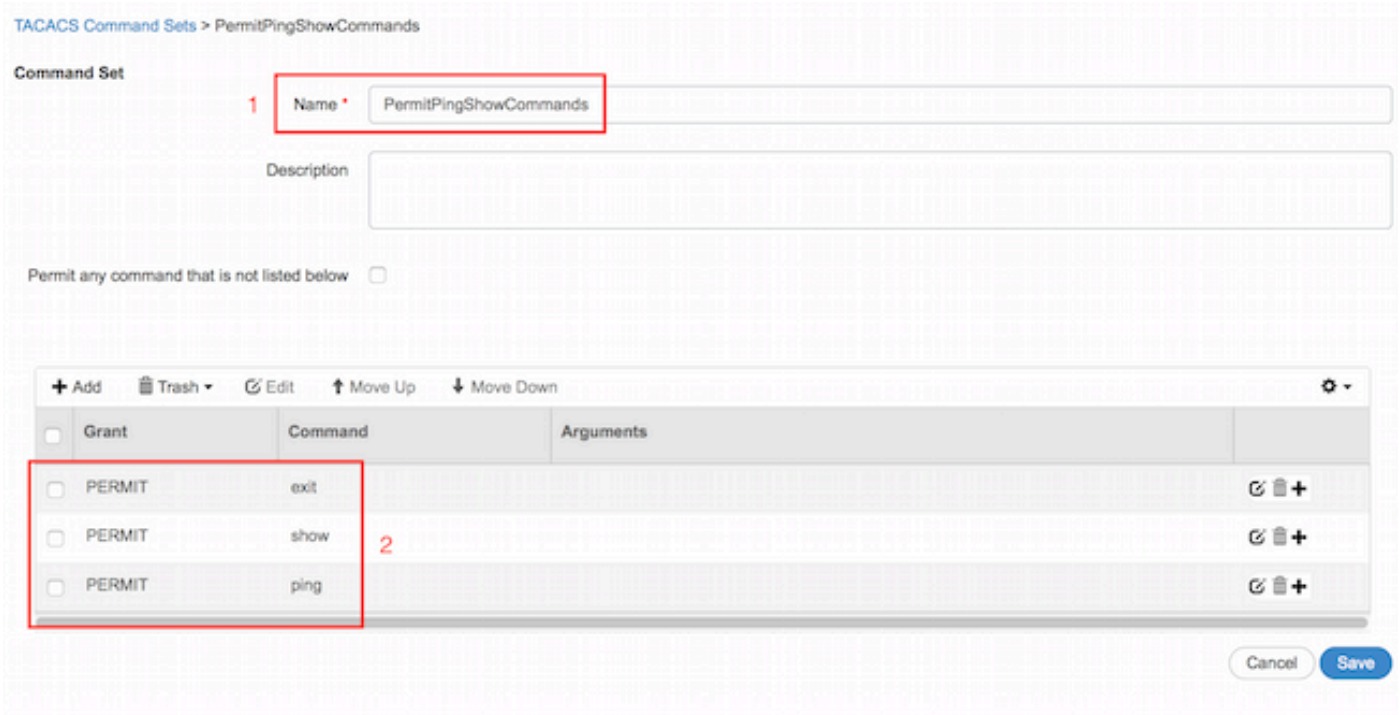
配置tacacs命令集

配置两命令集。提供所有on命令设备的**管理员用户的**第一**PermitAllCommands**。允许的**用户**用户的第二**PermitPingShowCommands**只显示和查验命令。

1. 连接对**工作区>设备管理>Policy结果> tacacs命令集。**单击 Add。提供名字 **PermitAllCommands**，选择**permit any命令不是列出的下面的**复选框并且点击**提交。**

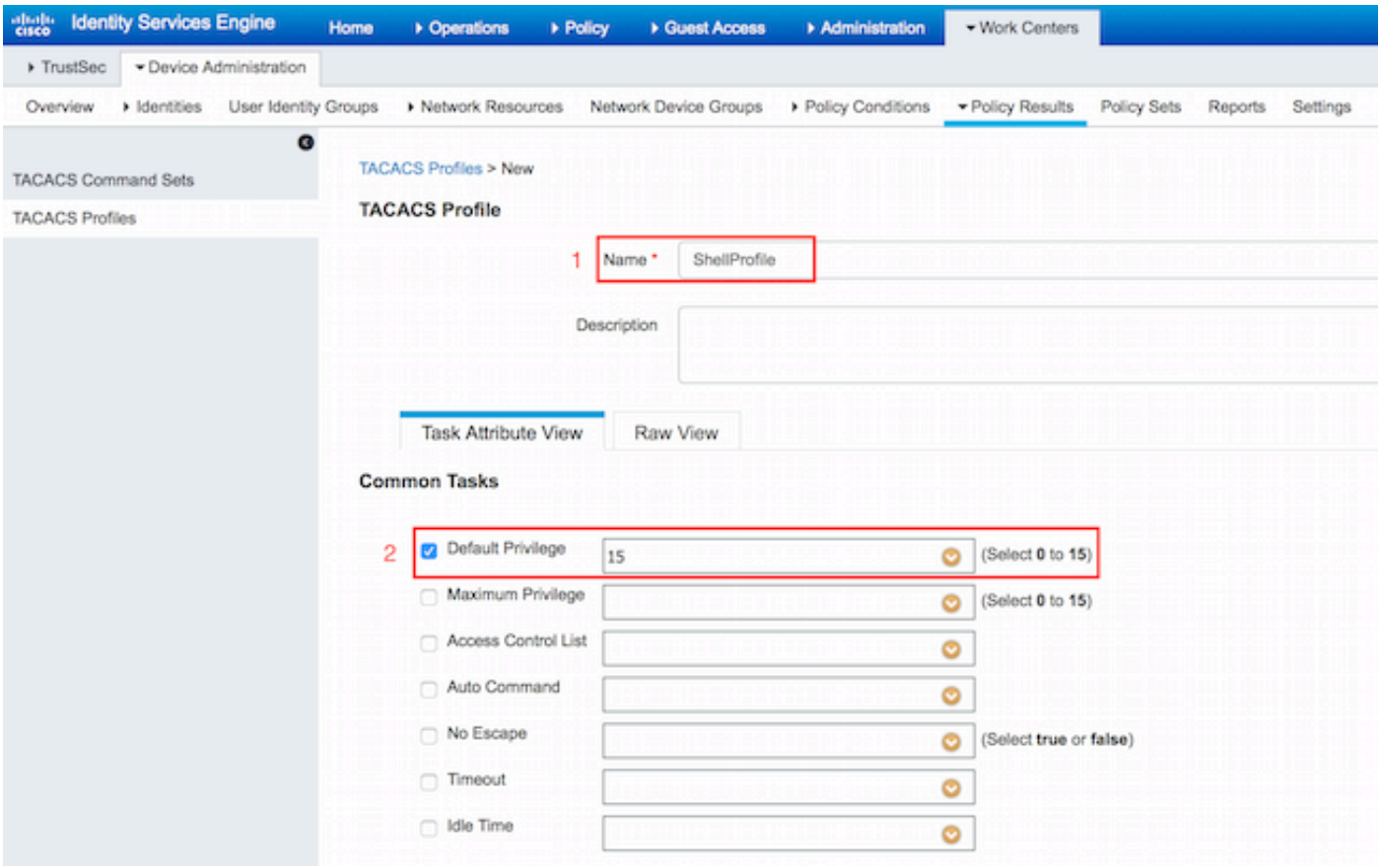


2. 连接对**工作区>设备管理>Policy结果> tacacs命令集。**单击 Add。提供名字 **PermitPingShowCommands**，点击**添加**，并且许可证**显示，连接**并且**退出**命令。默认情况下，如果参数被留下空白，所有参数是包括的。单击 **submit**。



配置TACACS配置文件

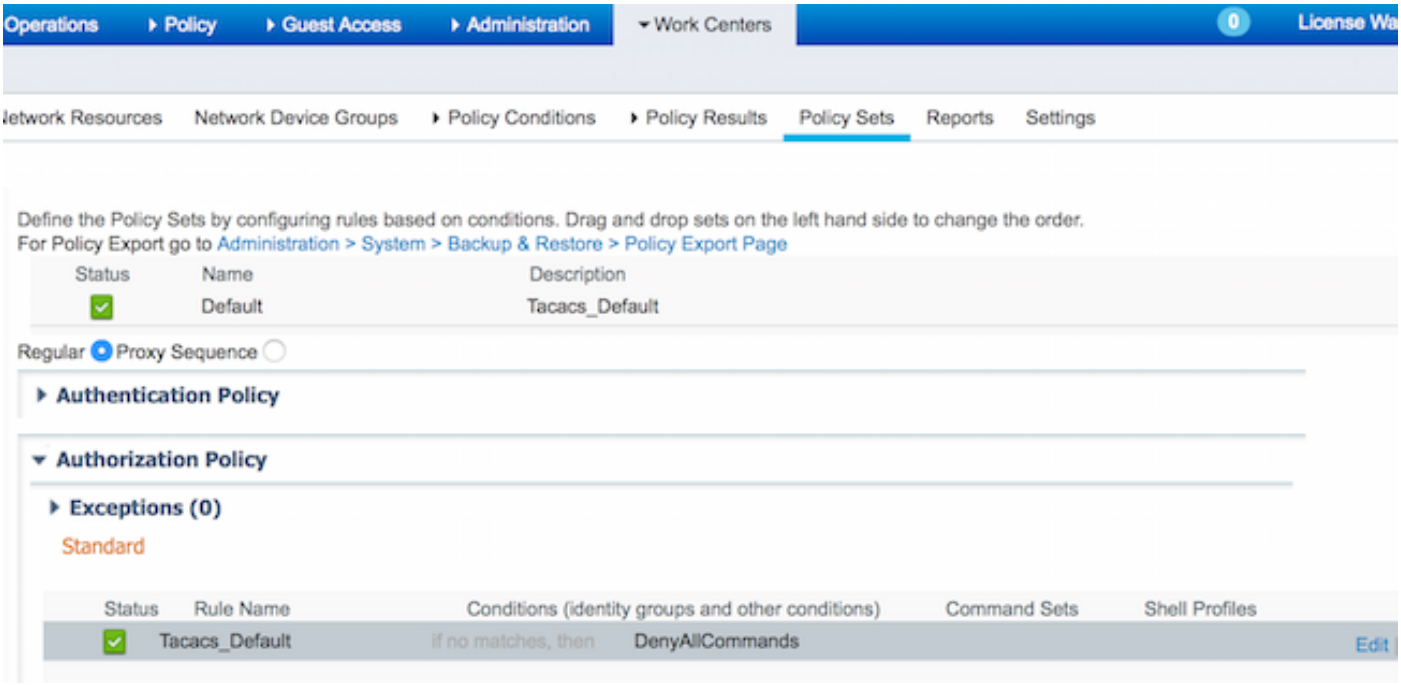
将配置单个TACACS配置文件。实际命令实施通过命令集将完成。连接对**工作区>设备管理>Policy结果> TACACS配置文件。**单击 **Add**。提供命名**ShellProfile**，选择**默认权限**复选框并且输入值为15。单击 **submit**。



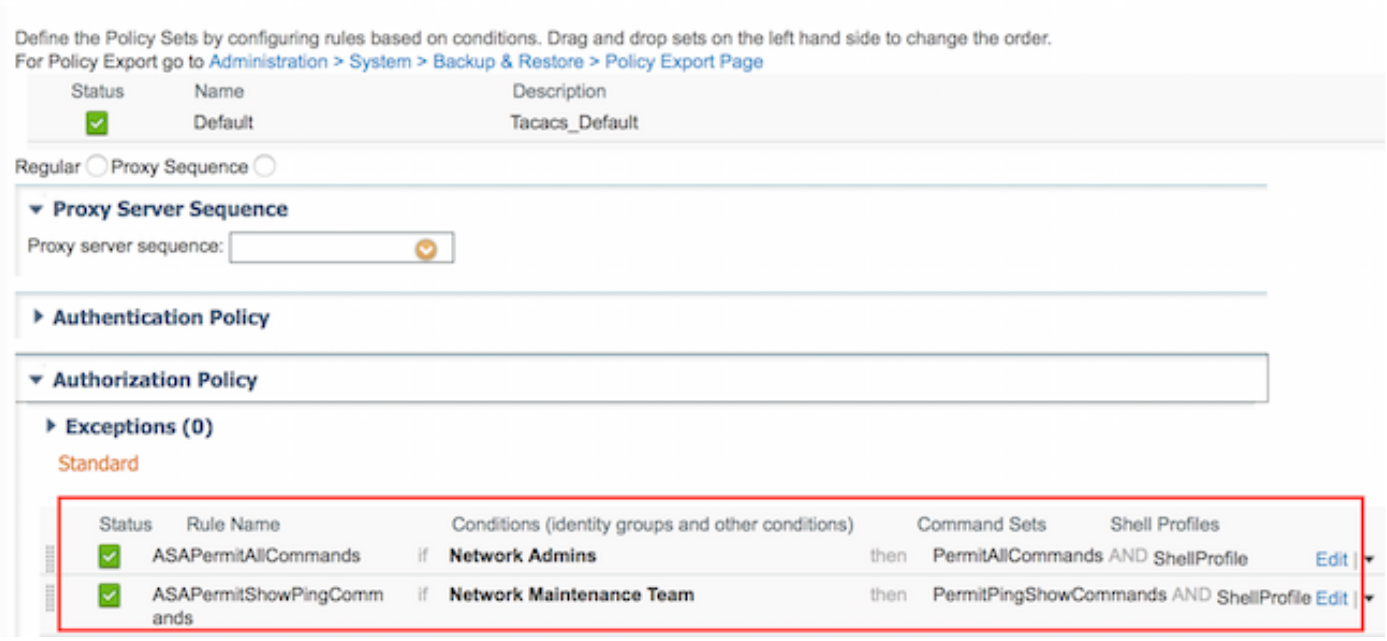
配置TACACS授权策略

默认情况下认证策略指向All_User_ID_Stores，包括本地存储，因此保持不变。

连接对**工作区>设备管理>Policy集>默认>授权策略> Edit >上面插入新规则。**



被配置的两个授权rulesare，第一个规则分配TACACS配置文件**ShellProfile**和set命令根据**网络**管理员用户身份组成员的**PermitAllCommands**。第二个规则分配TACACS配置文件**ShellProfile**和set命令根据**网络维护小组**用户身份组成员的**PermitPingShowCommands**。



配置认证和授权的Cisco ASA防火墙

1. 用退路的充分的权限创建一个本地用户用**username命令**如显示这里

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. 定义TACACS服务器ISE，指定接口、协议IP地址和**TACACS**键。

```
ciscoasa(config)# username cisco password cisco privilege 15
```

Note:服务器密钥在ISE服务器应该匹配那个定义了前。

3. 测试与测试的TACACS服务器可到达性**aaa命令**如显示。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

前面的命令的输出表示， TACACS服务器可及的，并且用户成功验证。

4. 配置SSH、exec授权和命令授权的认证如下所示。使用**AAA认证exec认证服务器自动enable (event)**您在privileged EXEC模式将自动地安置。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

> **Note**:用以上的命令，认证在ISE完成，用户被放置直接地到特权模式，并且authorization命令发生。

5. 允许嘘在mgmt接口。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Verify

Cisco ASA防火墙验证

1. 对ASA防火墙的SSH作为属于全部存取的用户身份组的**管理员。网络管理员**组被映射对**ShellProfile**和**PermitAllCommands** Set命令在ISE。设法运行所有命令保证全部存取。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

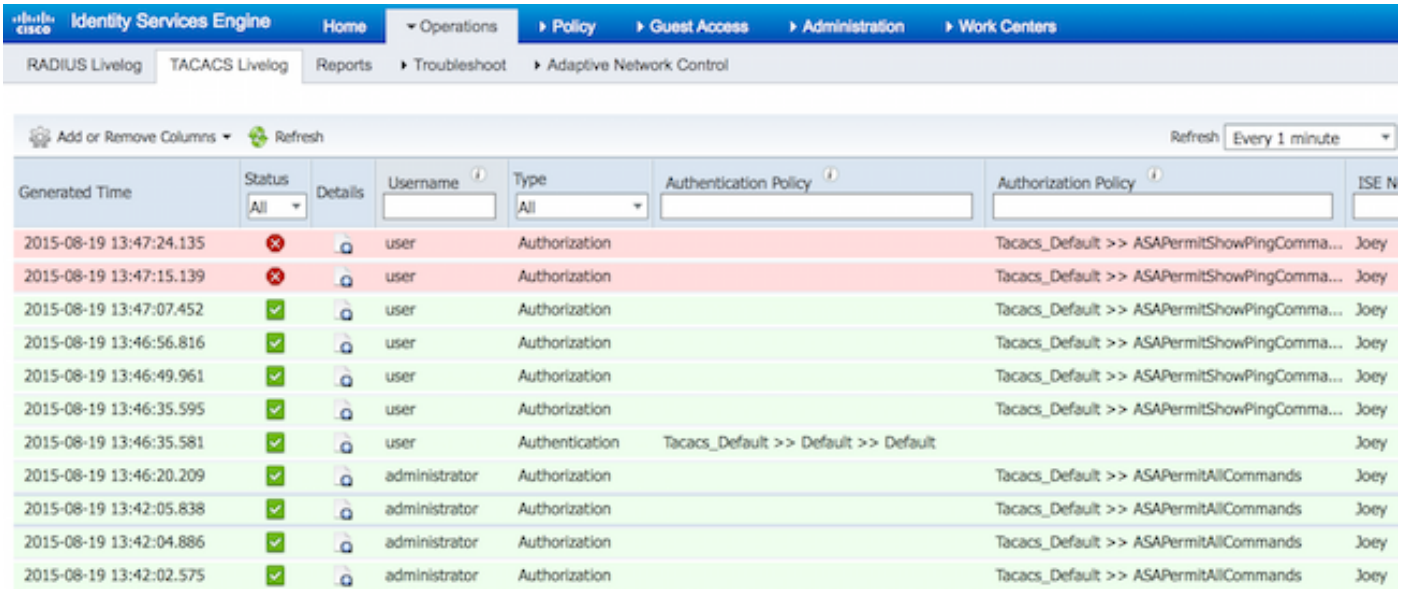
2. 对ASA防火墙的SSH作为属于有限享用用户身份组的**用户。网络维护**组被映射对**ShellProfile**和**PermitPingShowCommands** Set命令在ISE。设法运行所有命令保证只显示，并且可以发出查验命令。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
```

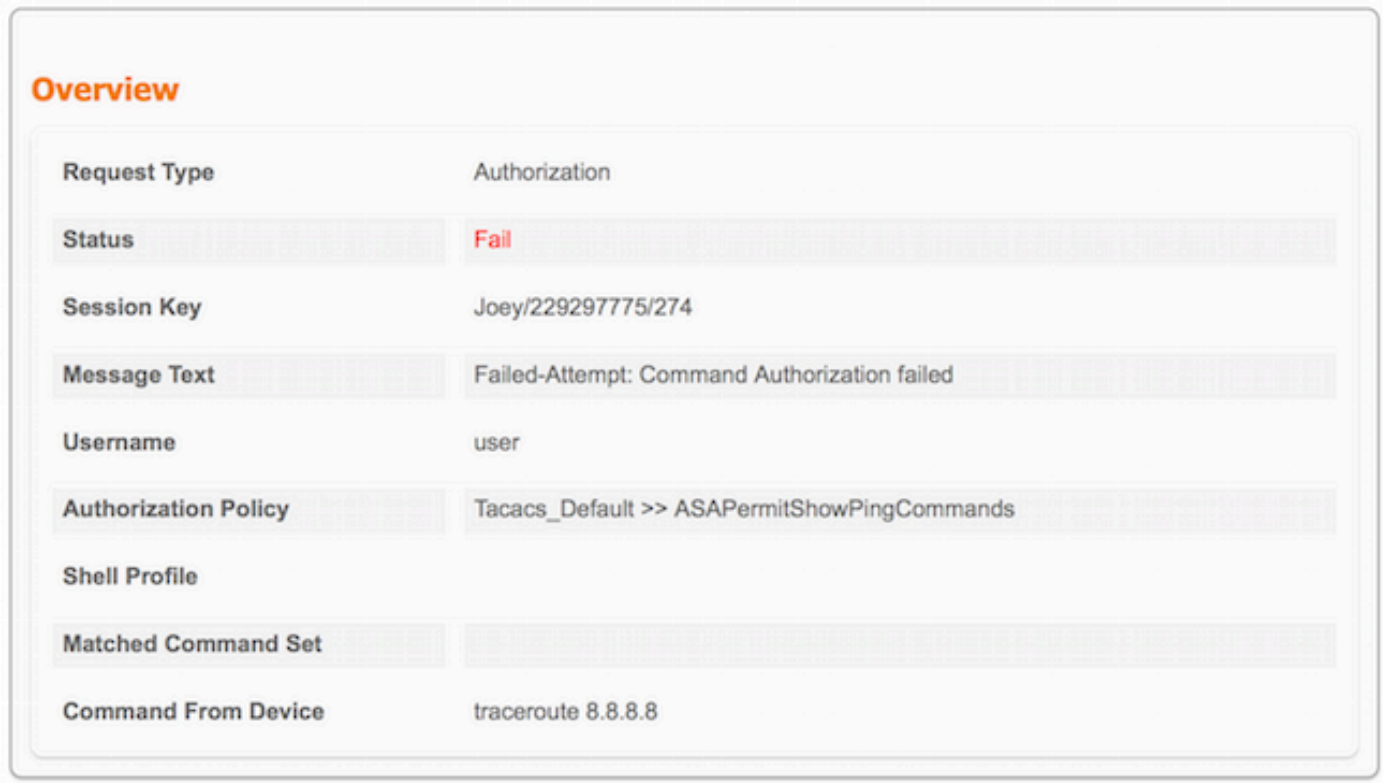
```
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

ISE 2.0验证

1. 连接对**操作> TACACS Livelog。**保证完成的尝试以上被看到。



2. 点击详细资料其中一个红色报告，及早被执行的失败的命令能被看到。



Troubleshoot

Error:失败尝试：出故障的Authorization命令

检查SelectedCommandSet属性验证期望的命令集由授权策略选择

Related Information

Technical Support & Documentation - Cisco Systems

ISE 2.0版本注释

ISE 2.0硬件安装指南

ISE 2.0升级指南

对ISE迁移工具指南的ACS

ISE 2.0激活目录集中指南

ISE 2.0引擎管理员指南