在ISE和ASAv之间配置TrustSec SXP

目录

简介

本文档介绍如何在ISE（身份服务引擎）和ASAv（虚拟自适应安全设备）之间配置SXP（安全组交换协议）连接。

SXP是TrustSec用于将IP到SGT的映射传播到TrustSec设备的SGT（安全组标记）交换协议。

SXP的开发目的是允许网络（包括不支持SGT内联标记的第三方设备或传统思科设备）具有TrustSec功能。SXP是对等协议，一台设备将用作扬声器，另一台将用作侦听器。SXP发言人负责发送IP-SGT绑定，而侦听程序负责收集这些绑定。SXP连接使用TCP端口64999作为底层传输协议，使用MD5来实现消息完整性/真实性。

SXP已在以下链接发布为IETF草案：

https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/

先决条件

要求

TrustSec兼容性列表：

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html

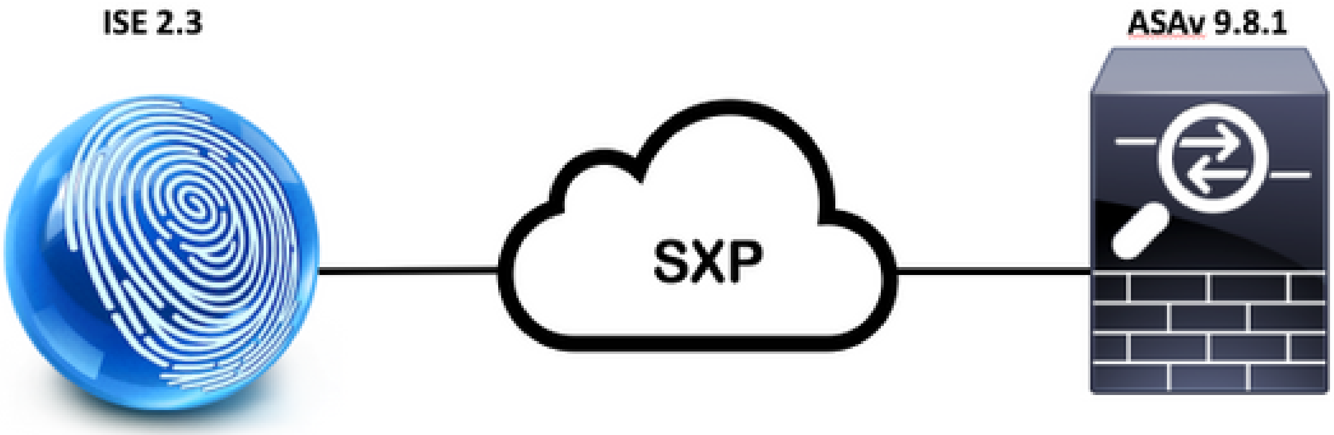
使用的组件

ISE 2.3

ASAv 9.8.1

ASDM 7.8.1.150

网络图



IP 地址

ISE:14.36.143.223

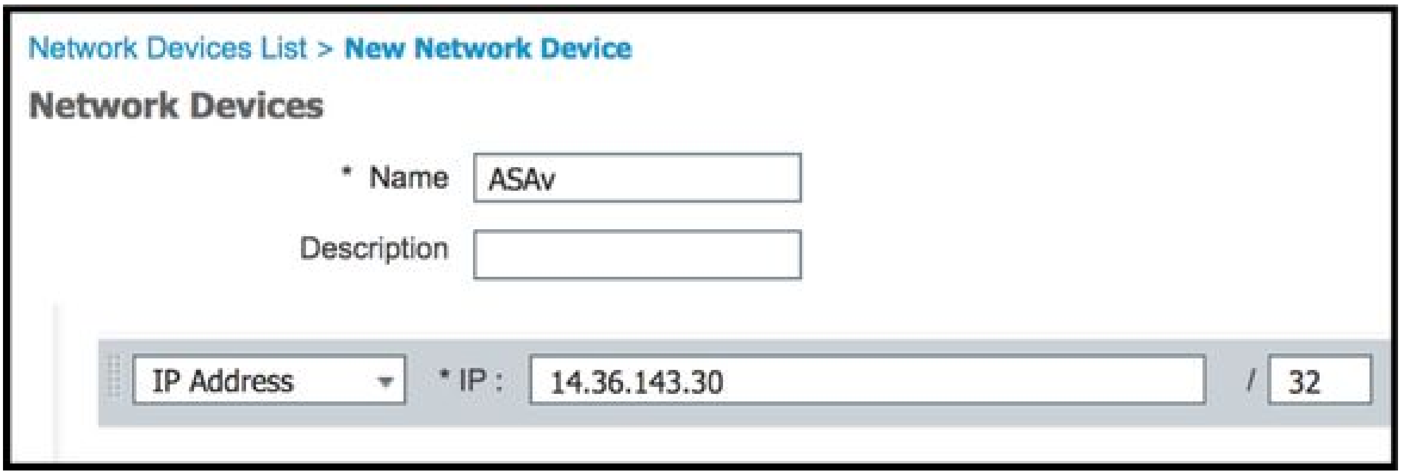
ASAv:14.36.143.30

初始配置

ISE网络设备

将ASA注册为网络设备

WorkCenters > TrutSec >组件>网络设备>添加



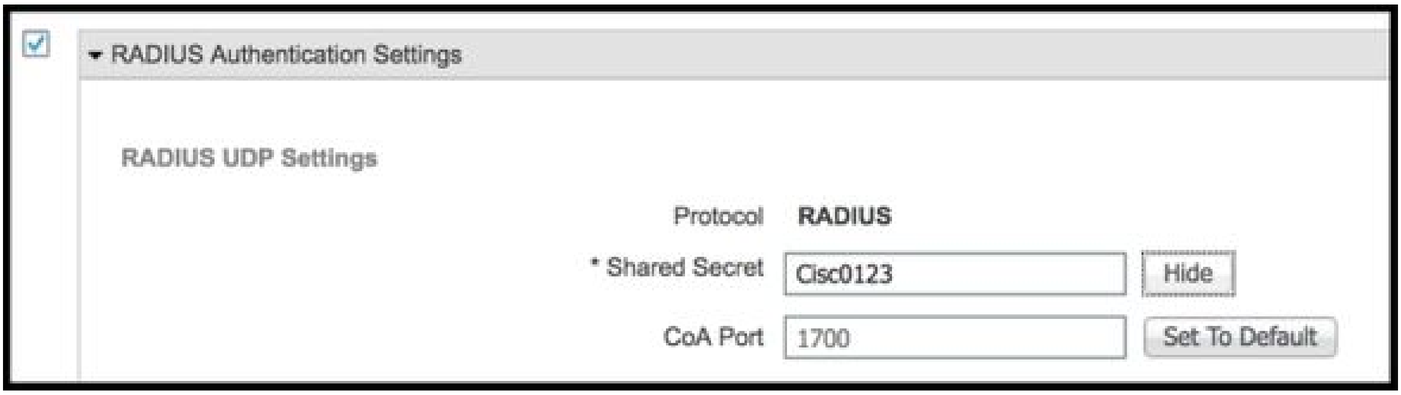
Network Devices List > New Network Device

Network Devices

* Name: ASAv

Description:

IP Address ▾ * IP : 14.36.143.30 / 32



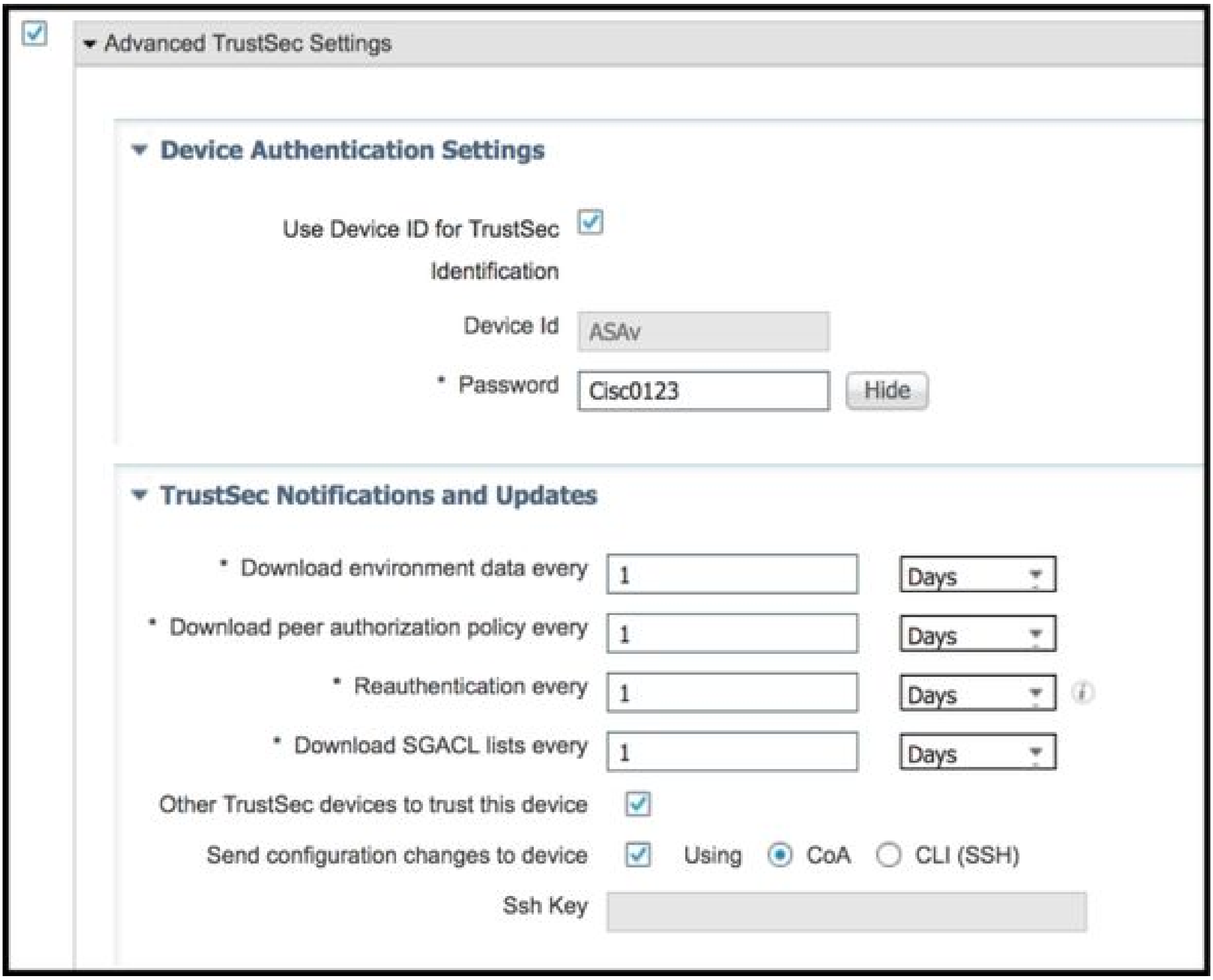
☑ ▾ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: Cisc0123

CoA Port: 1700



☑ ▾ Advanced TrustSec Settings

▾ **Device Authentication Settings**

Use Device ID for TrustSec Identification ☑

Device Id: ASAv

* Password: Cisc0123

▾ **TrustSec Notifications and Updates**

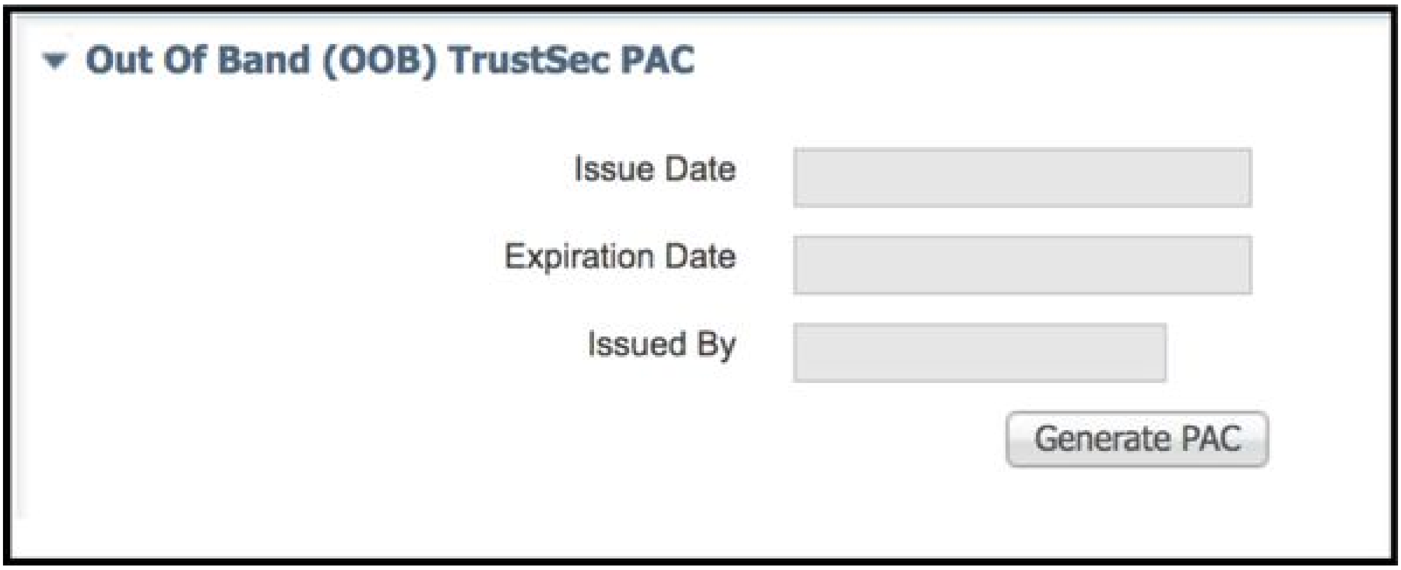
* Download environment data every	1	Days
* Download peer authorization policy every	1	Days
* Reauthentication every	1	Days
* Download SGACL lists every	1	Days

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

Ssh Key:

生成带外(OOB)PAC（受保护访问凭证）并下载

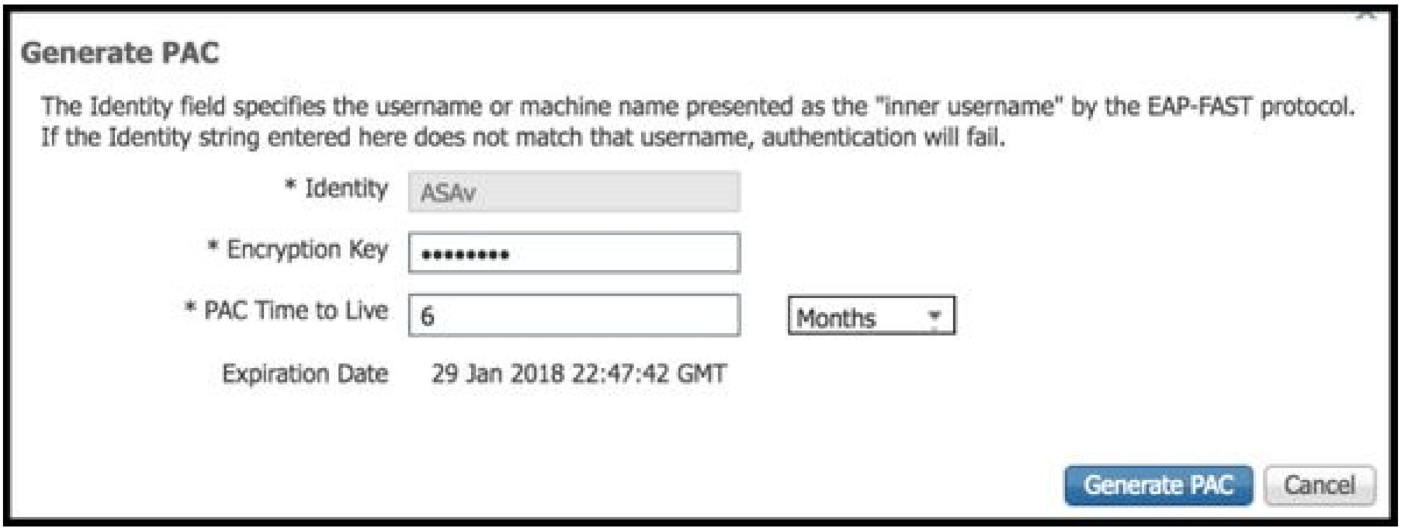


▾ **Out Of Band (OOB) TrustSec PAC**

Issue Date:

Expiration Date:

Issued By:



Generate PAC

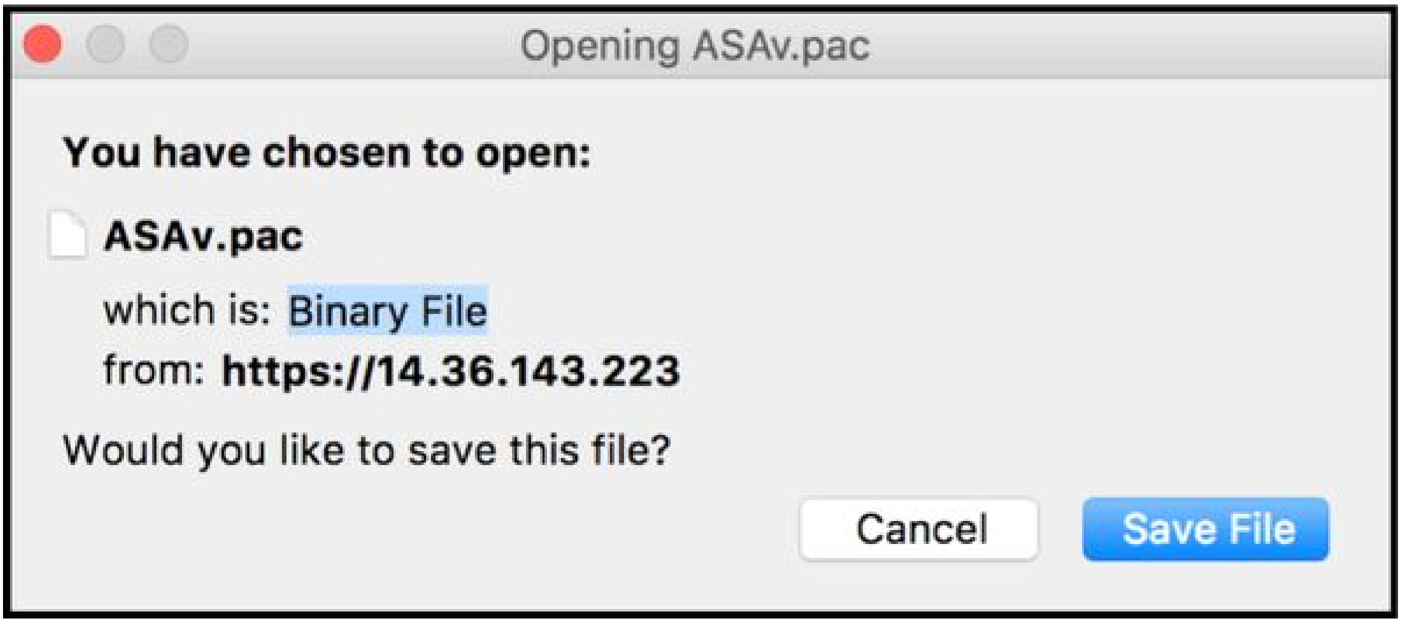
The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity: ASAv

* Encryption Key: •••••••••

* PAC Time to Live: 6 Months

Expiration Date: 29 Jan 2018 22:47:42 GMT



Opening ASAv.pac

You have chosen to open:

ASAv.pac

which is: Binary File

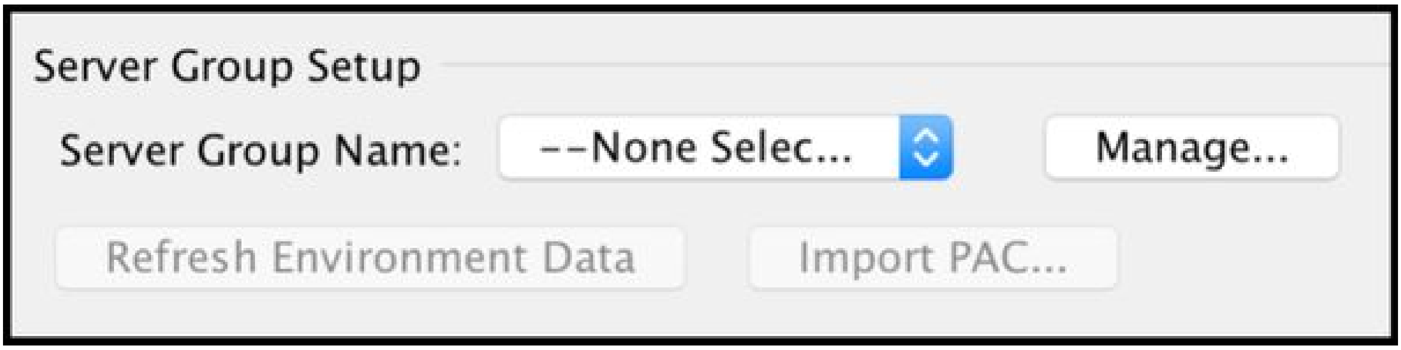
from: https://14.36.143.223

Would you like to save this file?

ASDM AAA服务器配置

创建AAA服务器组

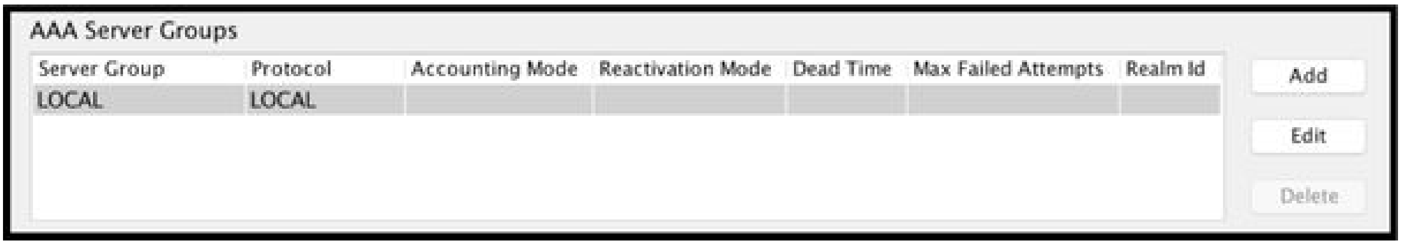
Configuration > Firewall > Identity by TrustSec > Server Group Setup > **Manage...**



Server Group Setup

Server Group Name: --None Selec...

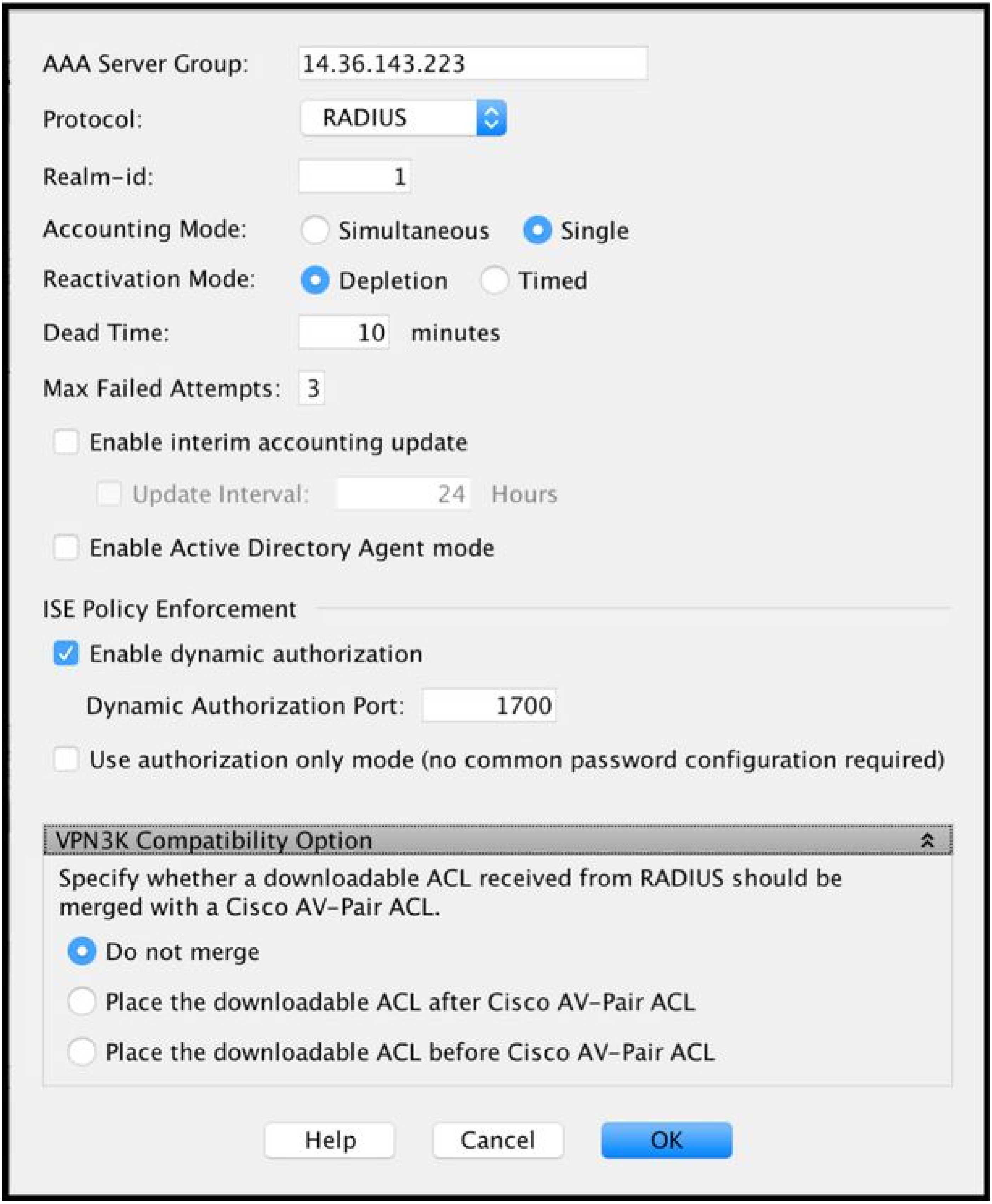
AAA服务器组>**添加**



AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Realm Id
LOCAL	LOCAL					

- AAA 服务器组:**<组名>**
- **启用动态授权**



AAA Server Group: 14.36.143.223

Protocol: RADIUS

Realm-id: 1

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

□ Enable interim accounting update

□ Update Interval: 24 Hours

□ Enable Active Directory Agent mode

ISE Policy Enforcement

☑ Enable dynamic authorization

Dynamic Authorization Port: 1700

□ Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Specify whether a downloadable ACL received from RADIUS should be merged with a Cisco AV-Pair ACL.

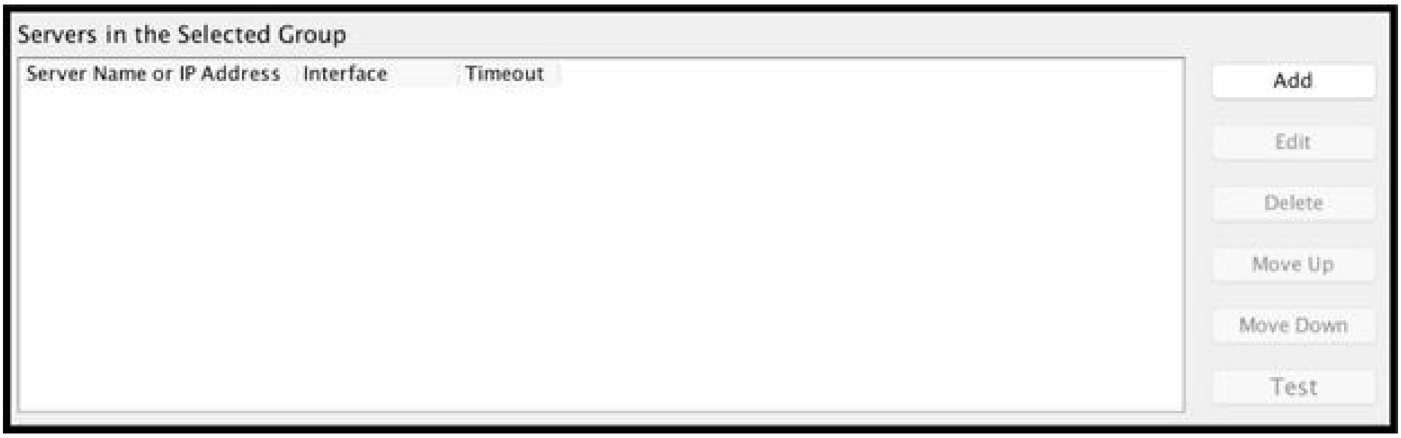
● Do not merge

○ Place the downloadable ACL after Cisco AV-Pair ACL

○ Place the downloadable ACL before Cisco AV-Pair ACL

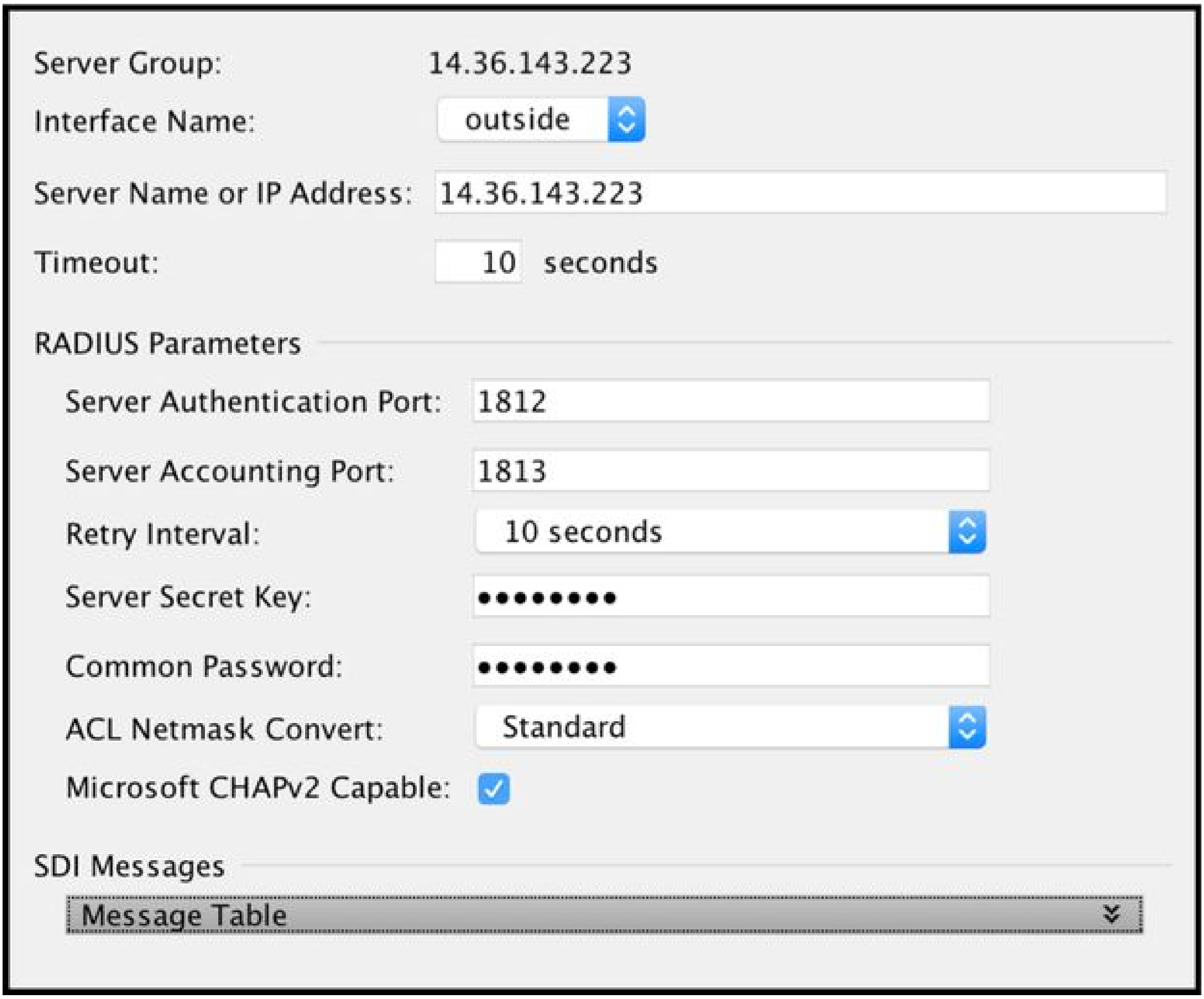
将服务器添加到服务器组

所选组>添加中的服务器


Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

- 服务器名称或IP地址：**<ISE IP地址>**
- 服务器身份验证端口：**1812**
- 服务器记帐端口：**1813**
- 服务器密钥：**Cisco0123**
- 常用密码：**Cisco0123**


Server Group: 14.36.143.223

Interface Name: outside

Server Name or IP Address: 14.36.143.223

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1812

Server Accounting Port: 1813

Retry Interval: 10 seconds

Server Secret Key: •••••••••

Common Password: •••••••••

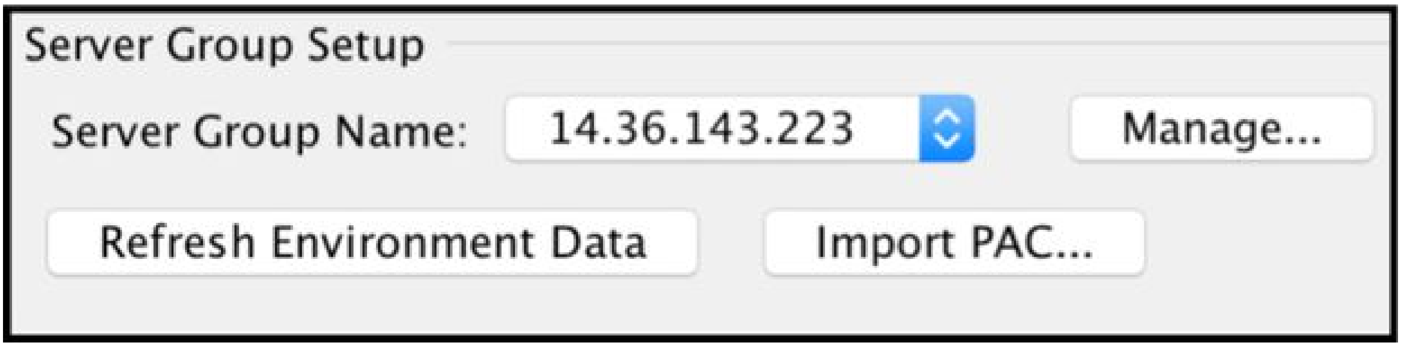
ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☑

SDI Messages

从ISE下载的导入PAC

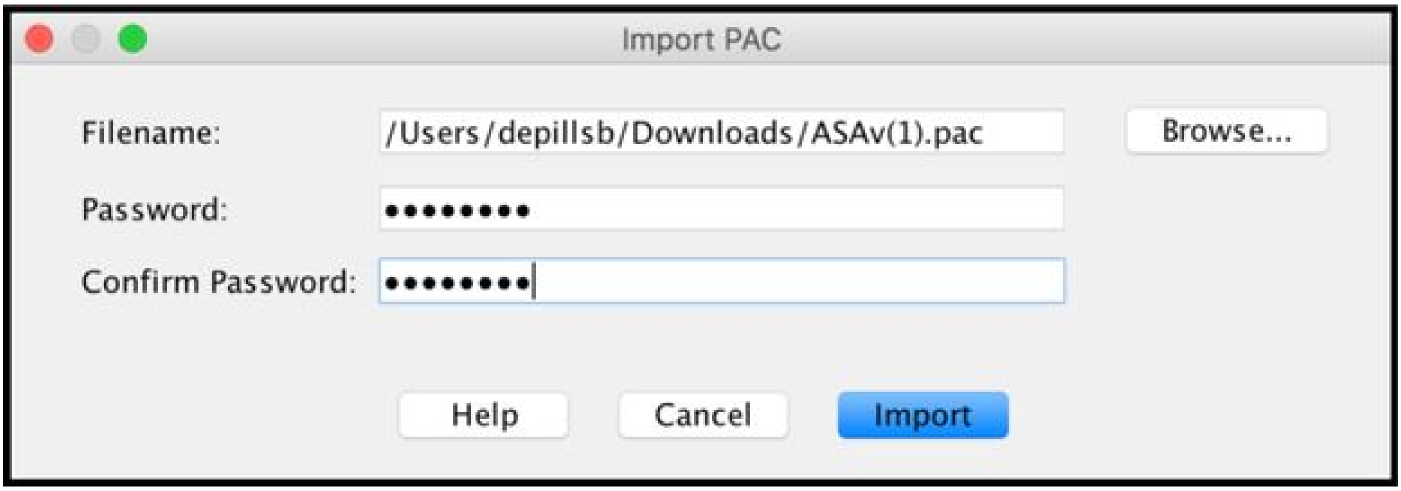
Configuration > Firewall > Identity by TrustSec > Server Group Setup > **Import PAC...**



Server Group Setup

Server Group Name: 14.36.143.223

- 密码：**Cisco0123**

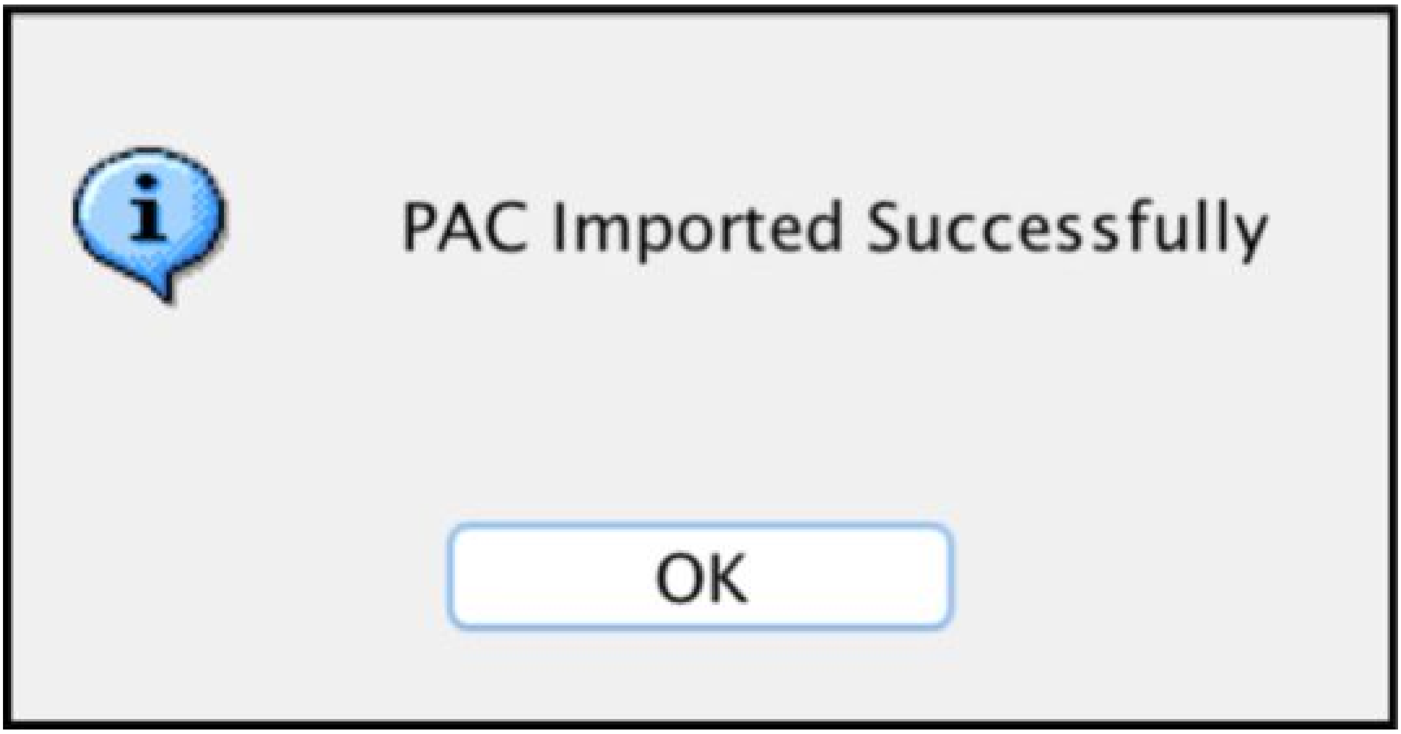


Import PAC

Filename: /Users/depillsb/Downloads/ASAv(1).pac

Password: •••••••••

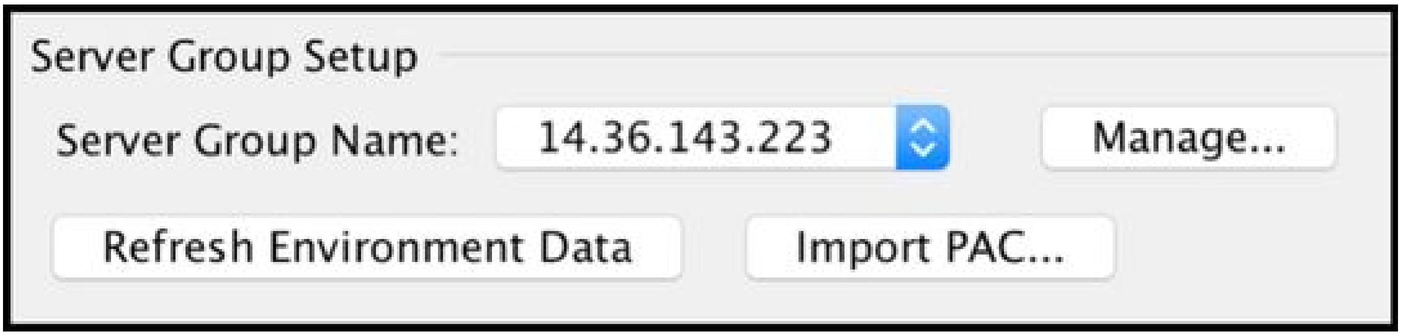
Confirm Password: •••••••••



PAC Imported Successfully

刷新环境数据

Configuration > Firewall > Identity by TrustSec > Server Group Setup > **Refresh Environment Data**



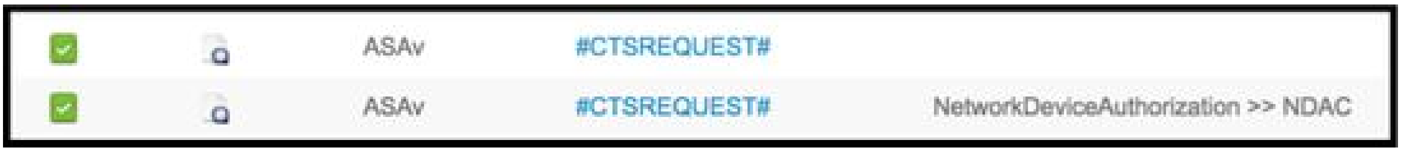
Server Group Setup

Server Group Name: 14.36.143.223

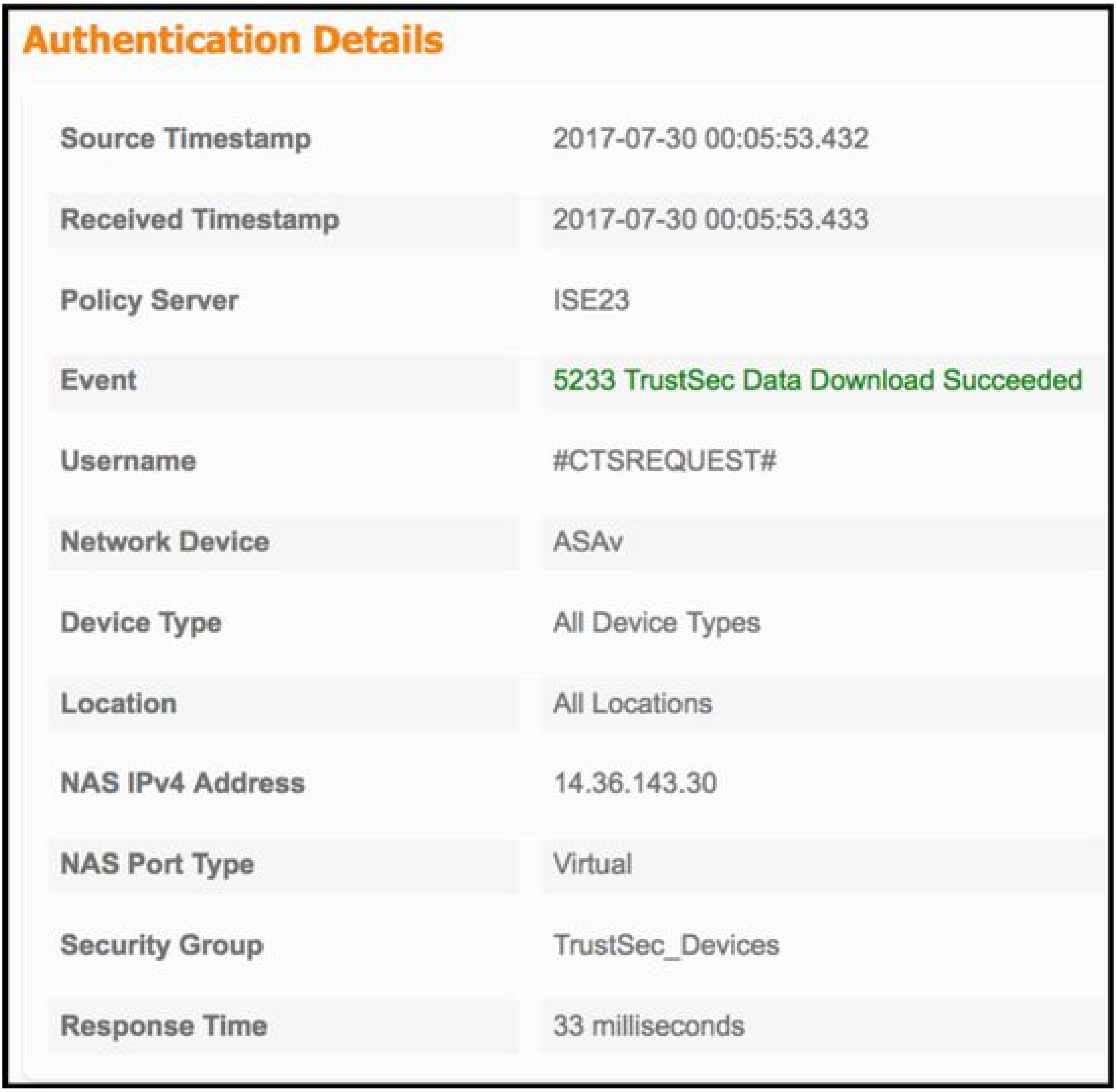
确认

ISE实时日志

操作> RADIUS >实时日志

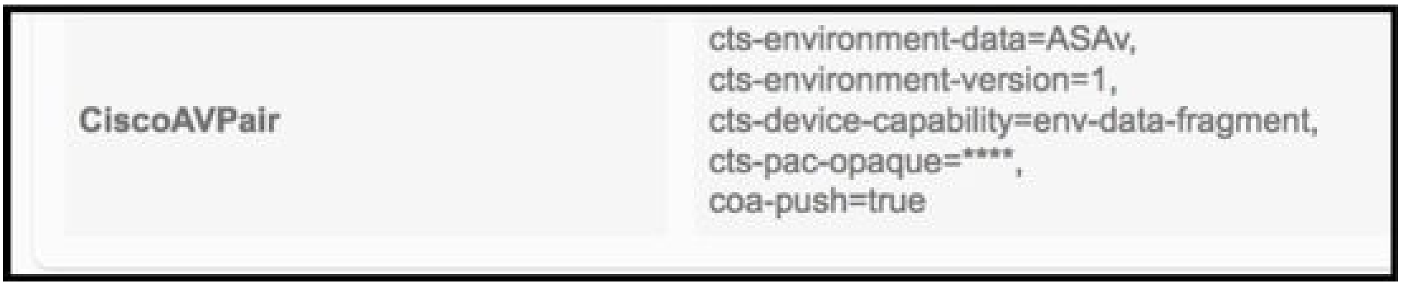


✓	🔍	ASAv	#CTSREQUEST#	
✓	🔍	ASAv	#CTSREQUEST#	NetworkDeviceAuthorization >> NDAC

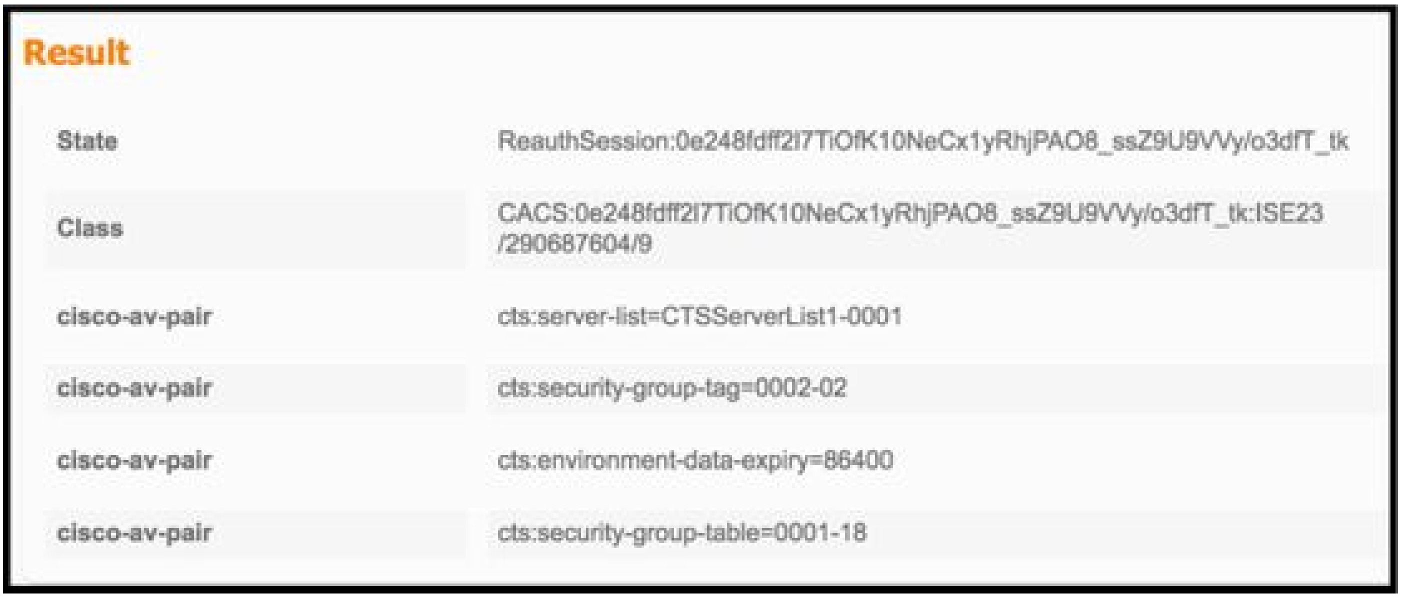


Authentication Details

Source Timestamp	2017-07-30 00:05:53.432
Received Timestamp	2017-07-30 00:05:53.433
Policy Server	ISE23
Event	5233 TrustSec Data Download Succeeded
Username	#CTSREQUEST#
Network Device	ASAv
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	14.36.143.30
NAS Port Type	Virtual
Security Group	TrustSec_Devices
Response Time	33 milliseconds

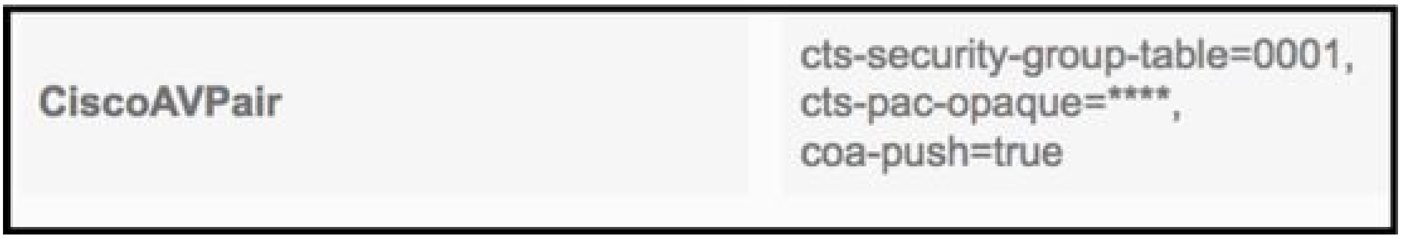


CiscoAVPair	cts-environment-data=ASAv,
	cts-environment-version=1,
	cts-device-capability=env-data-fragment,
	cts-pac-opaque=****,
	coa-push=true



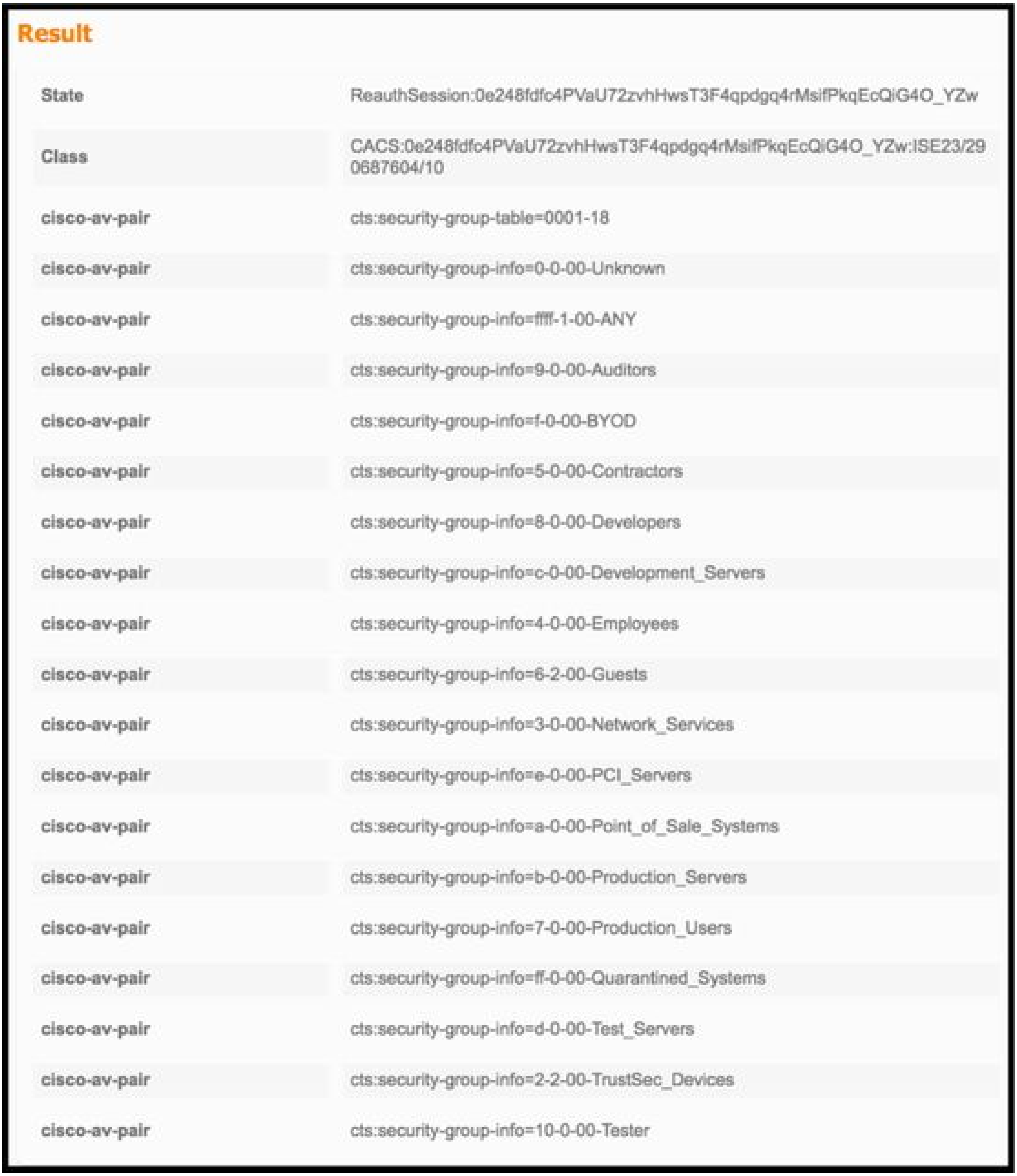
Result

State	ReauthSession:0e248fdff2l7TiOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dfT_tk
Class	CACS:0e248fdff2l7TiOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dfT_tk:ISE23 /290687604/9
cisco-av-pair	cts:server-list=CTSServerList1-0001
cisco-av-pair	cts:security-group-tag=0002-02
cisco-av-pair	cts:environment-data-expiry=86400
cisco-av-pair	cts:security-group-table=0001-18



CiscoAVPair	cts-security-group-table=0001,
	cts-pac-opaque=****,
	coa-push=true

工作中心> TrustSec >组件>安全组

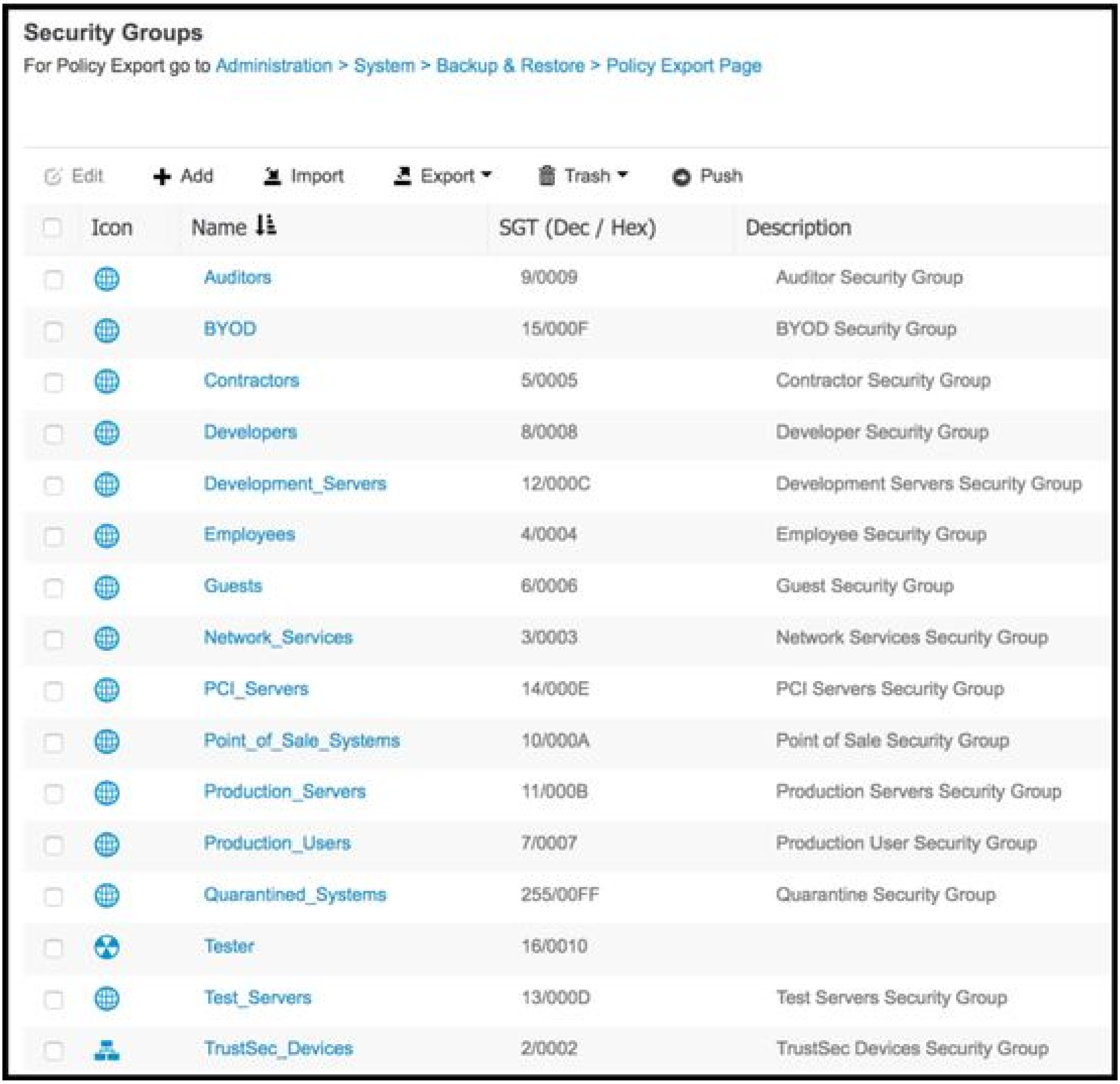


Result

State	ReauthSession:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw
Class	CACS:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw:ISE23/290687604/10
cisco-av-pair	cts:security-group-table=0001-18
cisco-av-pair	cts:security-group-info=0-0-00-Unknown
cisco-av-pair	cts:security-group-info=ffff-1-00-ANY
cisco-av-pair	cts:security-group-info=9-0-00-Auditors
cisco-av-pair	cts:security-group-info=f-0-00-BYOD
cisco-av-pair	cts:security-group-info=5-0-00-Contractors
cisco-av-pair	cts:security-group-info=8-0-00-Developers
cisco-av-pair	cts:security-group-info=c-0-00-Development_Servers
cisco-av-pair	cts:security-group-info=4-0-00-Employees
cisco-av-pair	cts:security-group-info=6-2-00-Guests
cisco-av-pair	cts:security-group-info=3-0-00-Network_Services
cisco-av-pair	cts:security-group-info=e-0-00-PCI_Servers
cisco-av-pair	cts:security-group-info=a-0-00-Point_of_Sale_Systems
cisco-av-pair	cts:security-group-info=b-0-00-Production_Servers
cisco-av-pair	cts:security-group-info=7-0-00-Production_Users
cisco-av-pair	cts:security-group-info=ff-0-00-Quarantined_Systems
cisco-av-pair	cts:security-group-info=d-0-00-Test_Servers
cisco-av-pair	cts:security-group-info=2-2-00-TrustSec_Devices
cisco-av-pair	cts:security-group-info=10-0-00-Tester

ISE安全组

工作中心> TrustSec >组件>安全**组**



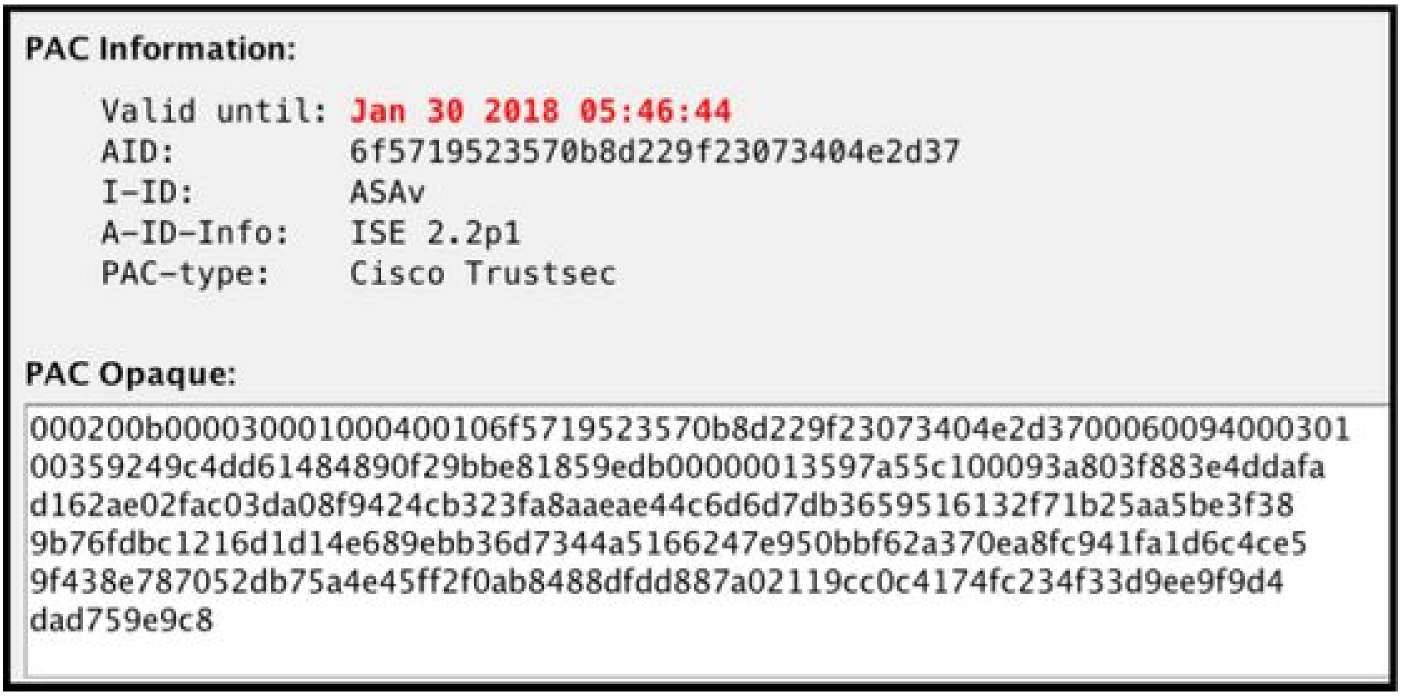
Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Icon	Name	SGT (Dec / Hex)	Description
□	🌐	Auditors	9/0009	Auditor Security Group
□	🌐	BYOD	15/000F	BYOD Security Group
□	🌐	Contractors	5/0005	Contractor Security Group
□	🌐	Developers	8/0008	Developer Security Group
□	🌐	Development_Servers	12/000C	Development Servers Security Group
□	🌐	Employees	4/0004	Employee Security Group
□	🌐	Guests	6/0006	Guest Security Group
□	🌐	Network_Services	3/0003	Network Services Security Group
□	🌐	PCI_Servers	14/000E	PCI Servers Security Group
□	🌐	Point_of_Sale_Systems	10/000A	Point of Sale Security Group
□	🌐	Production_Servers	11/000B	Production Servers Security Group
□	🌐	Production_Users	7/0007	Production User Security Group
□	🌐	Quarantined_Systems	255/00FF	Quarantine Security Group
□	☢	Tester	16/0010	
□	🌐	Test_Servers	13/000D	Test Servers Security Group
□	🖧	TrustSec_Devices	2/0002	TrustSec Devices Security Group

ASDM PAC

Monitoring > Properties > Identity by TrustSec > **PAC**



PAC Information:

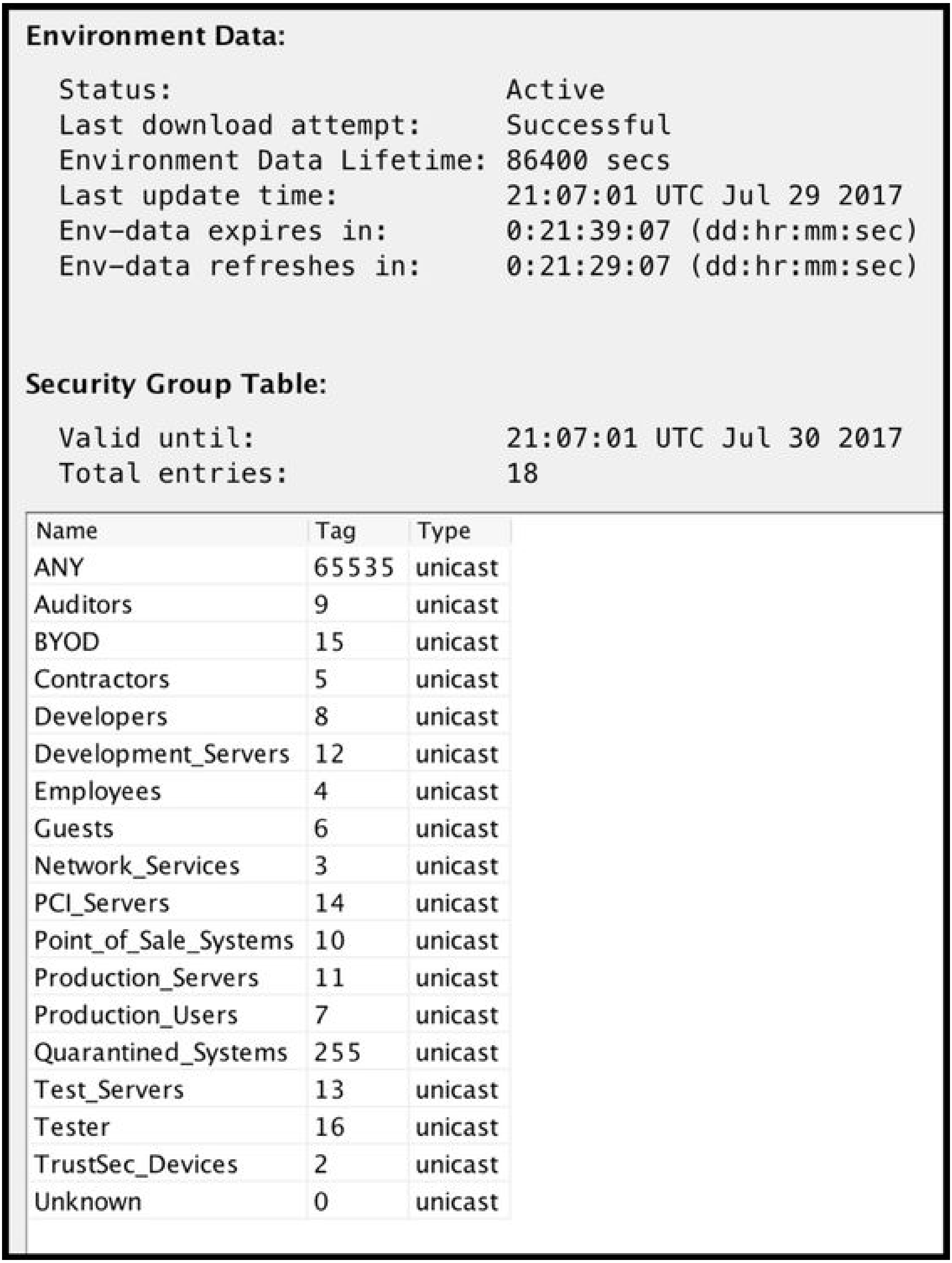
```
    Valid until: Jan 30 2018 05:46:44
    AID:         6f5719523570b8d229f23073404e2d37
    I-ID:        ASAv
    A-ID-Info:   ISE 2.2p1
    PAC-type:    Cisco Trustsec
```

PAC Opaque:

```
000200b00003000100040010 6f5719523570b8d229f23073404e2d3700060094000301
00359249c4dd61484890f29bbe81859edb00000013597a55c100093a803f883e4ddafa
d162ae02fac03da08f9424cb323fa8aaeae44c6d6d7db3659516132f71b25aa5be3f38
9b76fdbc1216d1d14e689ebb36d7344a5166247e950bbf62a370ea8fc941fa1d6c4ce5
9f438e787052db75a4e45ff2f0ab8488dfdd887a02119cc0c4174fc234f33d9ee9f9d4
dad759e9c8
```

ASDM环境数据和安全组

Monitoring > Properties > Identity by TrustSec > Environment **Data**



Environment Data:

```
  Status:                       Active
  Last download attempt:        Successful
  Environment Data Lifetime:    86400 secs
  Last update time:             21:07:01 UTC Jul 29 2017
  Env-data expires in:          0:21:39:07 (dd:hr:mm:sec)
  Env-data refreshes in:        0:21:29:07 (dd:hr:mm:sec)
```

Security Group Table:

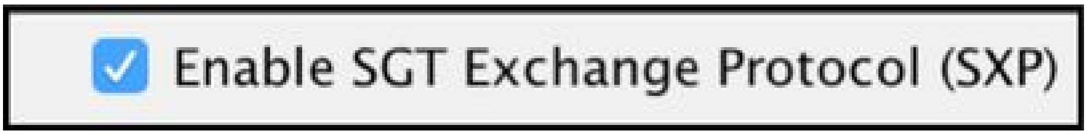
```
  Valid until:                  21:07:01 UTC Jul 30 2017
  Total entries:                18
```

Name	Tag	Type
ANY	65535	unicast
Auditors	9	unicast
BYOD	15	unicast
Contractors	5	unicast
Developers	8	unicast
Development_Servers	12	unicast
Employees	4	unicast
Guests	6	unicast
Network_Services	3	unicast
PCI_Servers	14	unicast
Point_of_Sale_Systems	10	unicast
Production_Servers	11	unicast
Production_Users	7	unicast
Quarantined_Systems	255	unicast
Test_Servers	13	unicast
Tester	16	unicast
TrustSec_Devices	2	unicast
Unknown	0	unicast

ASDM SXP配置

启用SXP

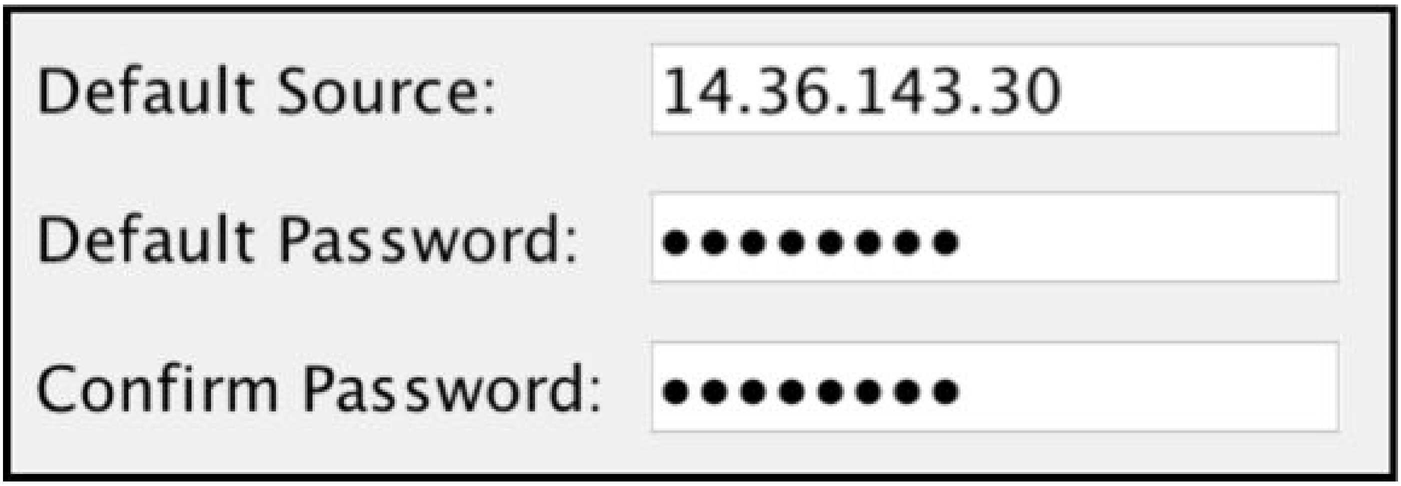
Configuration > Firewall > Identity by TrustSec > **Enable SGT Exchange Protocol(SXP)**



☑ Enable SGT Exchange Protocol (SXP)

设置默认SXP源IP地址和默认SXP密码

Configuration > Firewall > Identity by TrustSec > **Connection Peers**



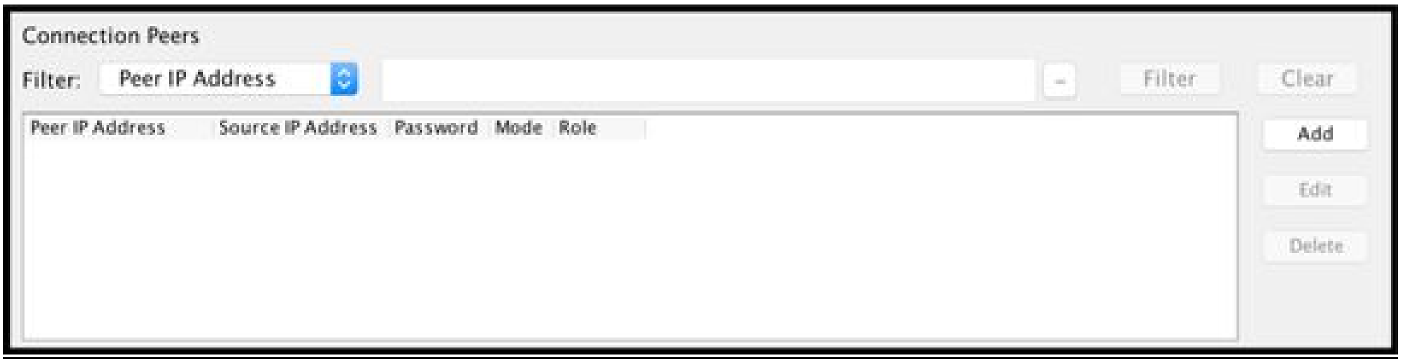
Default Source: 14.36.143.30

Default Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

添加SXP对等体

Configuration > Firewall > Identity by TrustSec > Connection Peers > **Add**

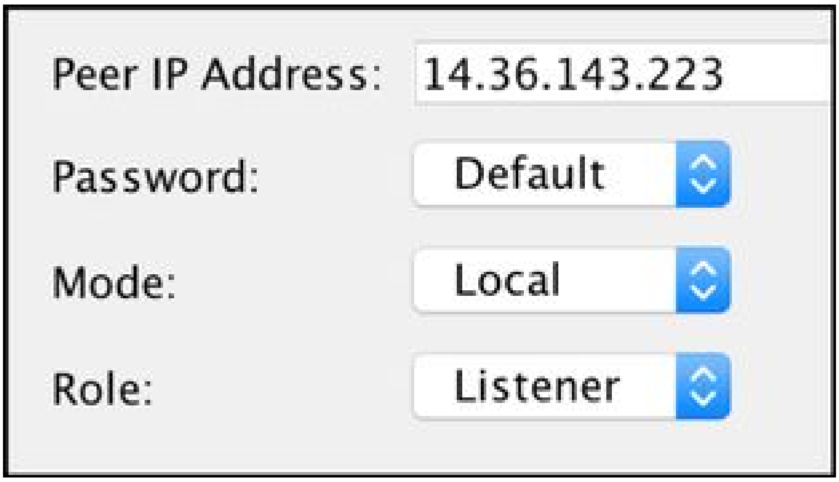


Connection Peers

Filter: Peer IP Address

Peer IP Address	Source IP Address	Password	Mode	Role

- 对等IP地址：**<ISE IP地址>**



Peer IP Address: 14.36.143.223

Password: Default

Mode: Local

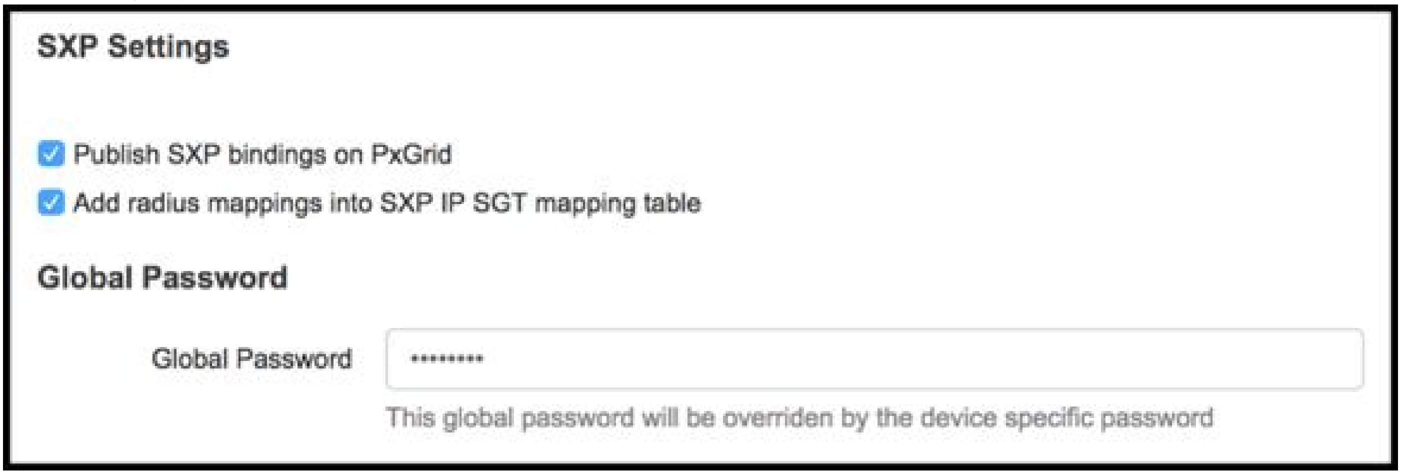
Role: Listener

ISE SXP配置

全局SXP密码设置

WorkCenters > TrustSec > Settings > **SXP Settings**

- 全局密码：**Cisco0123**



SXP Settings

☑ Publish SXP bindings on PxGrid

☑ Add radius mappings into SXP IP SGT mapping table

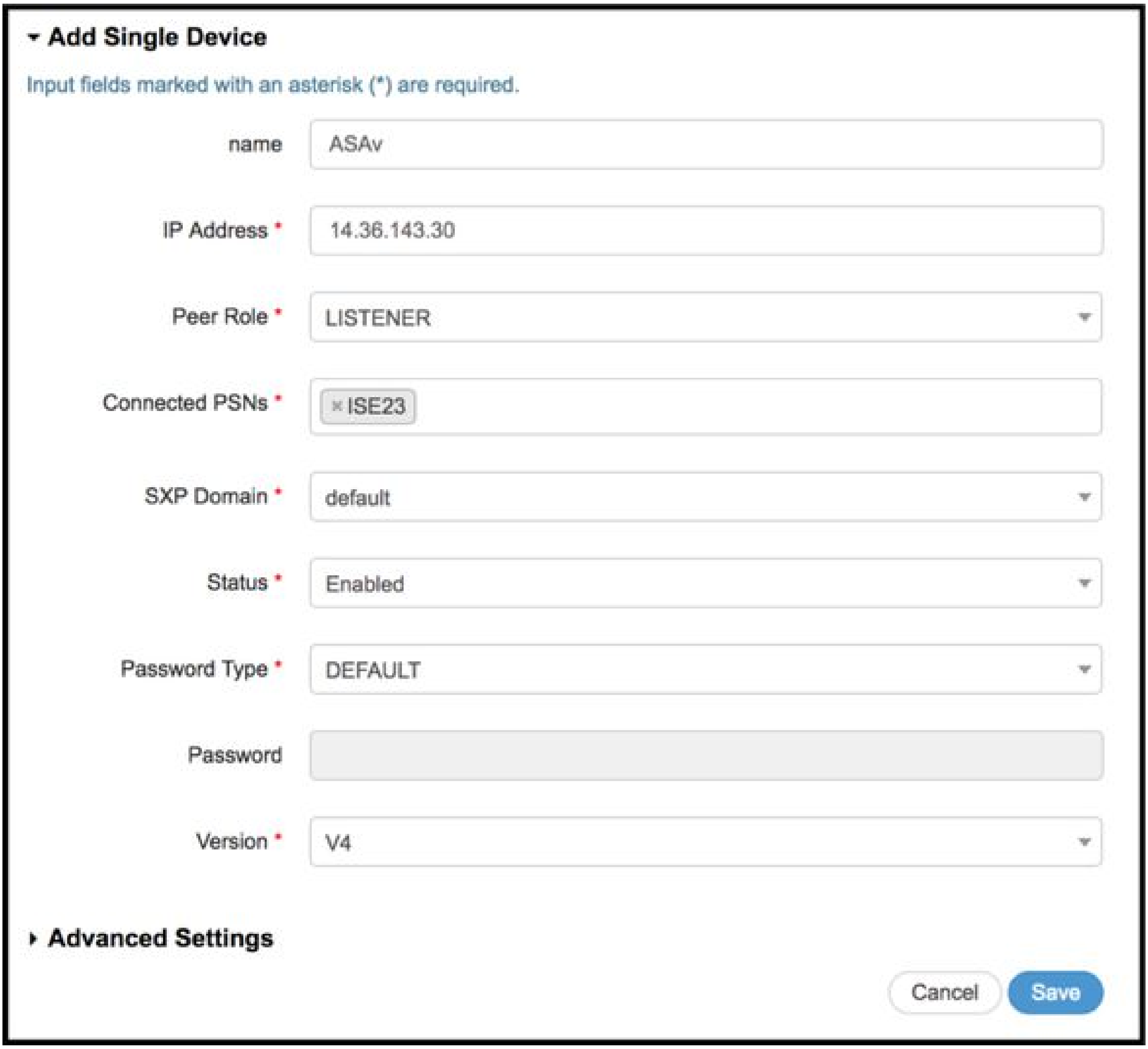
Global Password

Global Password: *********

This global password will be overriden by the device specific password

添加SXP设备

WorkCenters > TrustSec > SXP > SXP Devices > **Add**



▾ Add Single Device

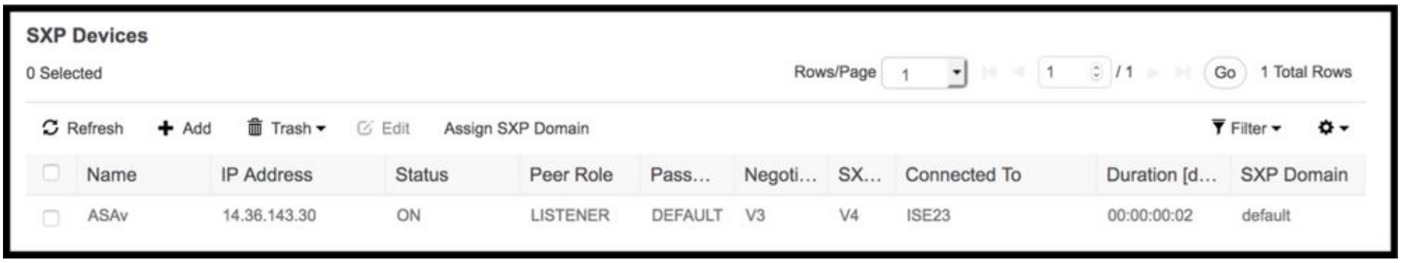
Input fields marked with an asterisk (*) are required.

name	ASAv
IP Address *	14.36.143.30
Peer Role *	LISTENER
Connected PSNs *	× ISE23
SXP Domain *	default
Status *	Enabled
Password Type *	DEFAULT
Password	
Version *	V4

SXP验证

ISE SXP验证

WorkCenters > TrustSec > SXP > **SXP Devices**



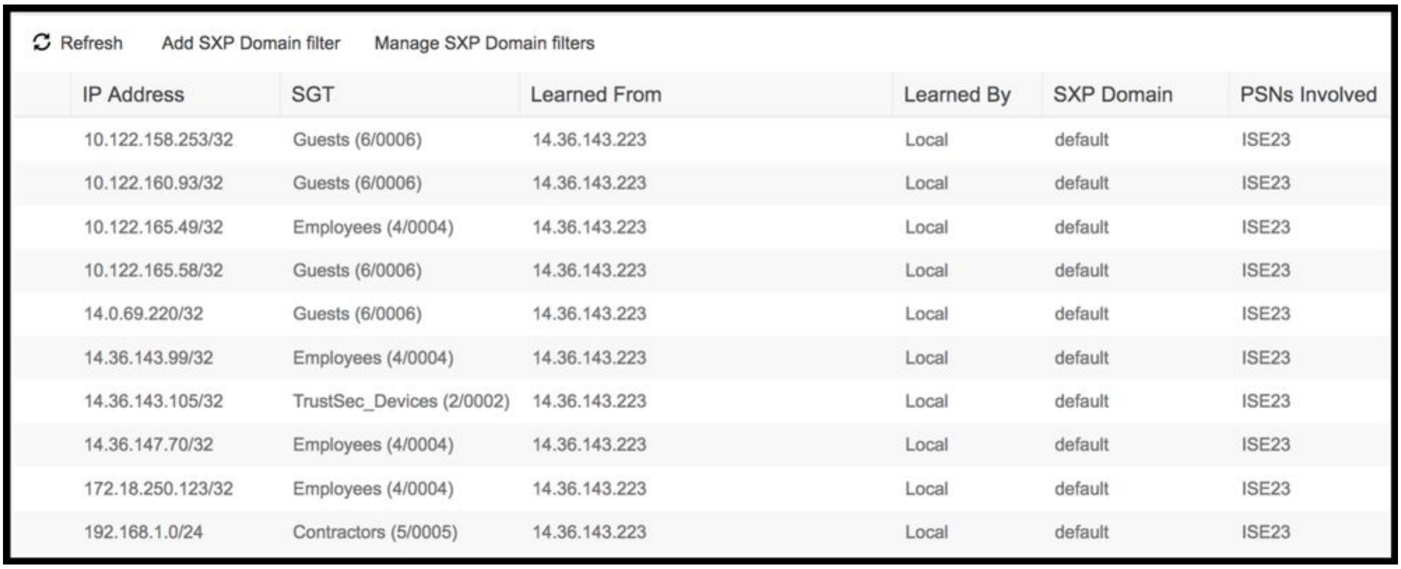
SXP Devices

0 Selected

□	Name	IP Address	Status	Peer Role	Pass...	Negoti...	SX...	Connected To	Duration [d...	SXP Domain
□	ASAv	14.36.143.30	ON	LISTENER	DEFAULT	V3	V4	ISE23	00:00:00:02	default

ISE SXP映射

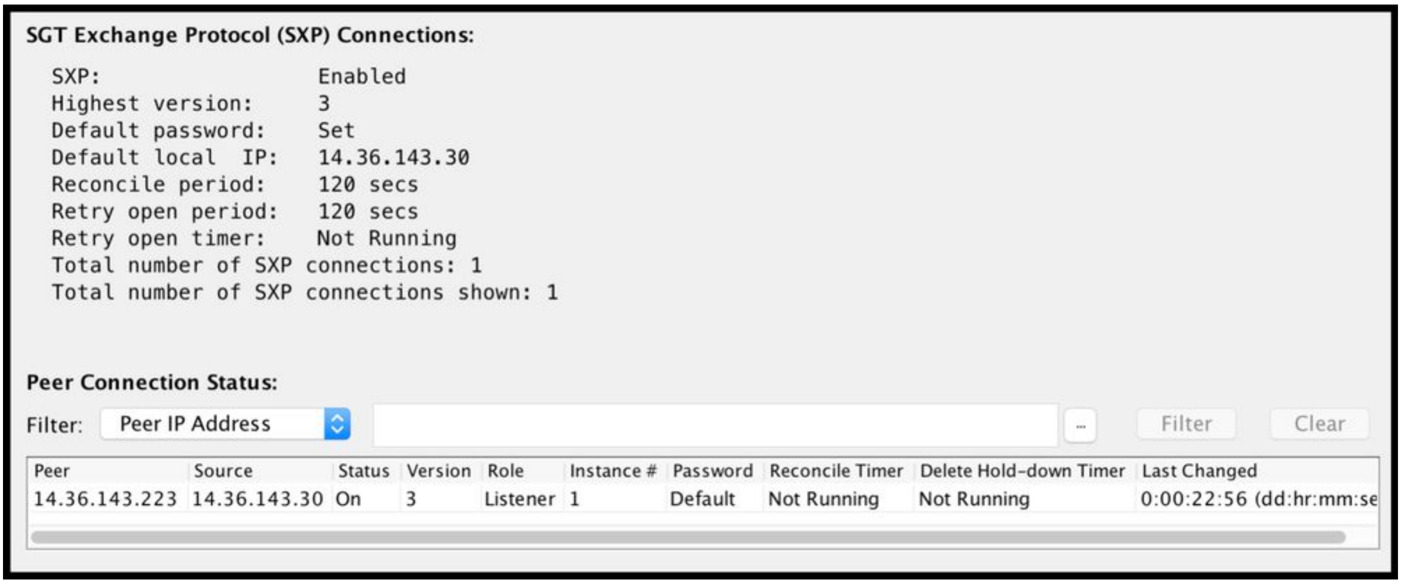
WorkCenters > TrustSec > SXP > **All SXP Mappings**



IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
10.122.158.253/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
10.122.160.93/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
10.122.165.49/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
10.122.165.58/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
14.0.69.220/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
14.36.143.99/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
14.36.143.105/32	TrustSec_Devices (2/0002)	14.36.143.223	Local	default	ISE23
14.36.147.70/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
172.18.250.123/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
192.168.1.0/24	Contractors (5/0005)	14.36.143.223	Local	default	ISE23

ASDM SXP验证

Monitoring > Properties > Identity by TrustSec > **SXP Connections**



SGT Exchange Protocol (SXP) Connections:

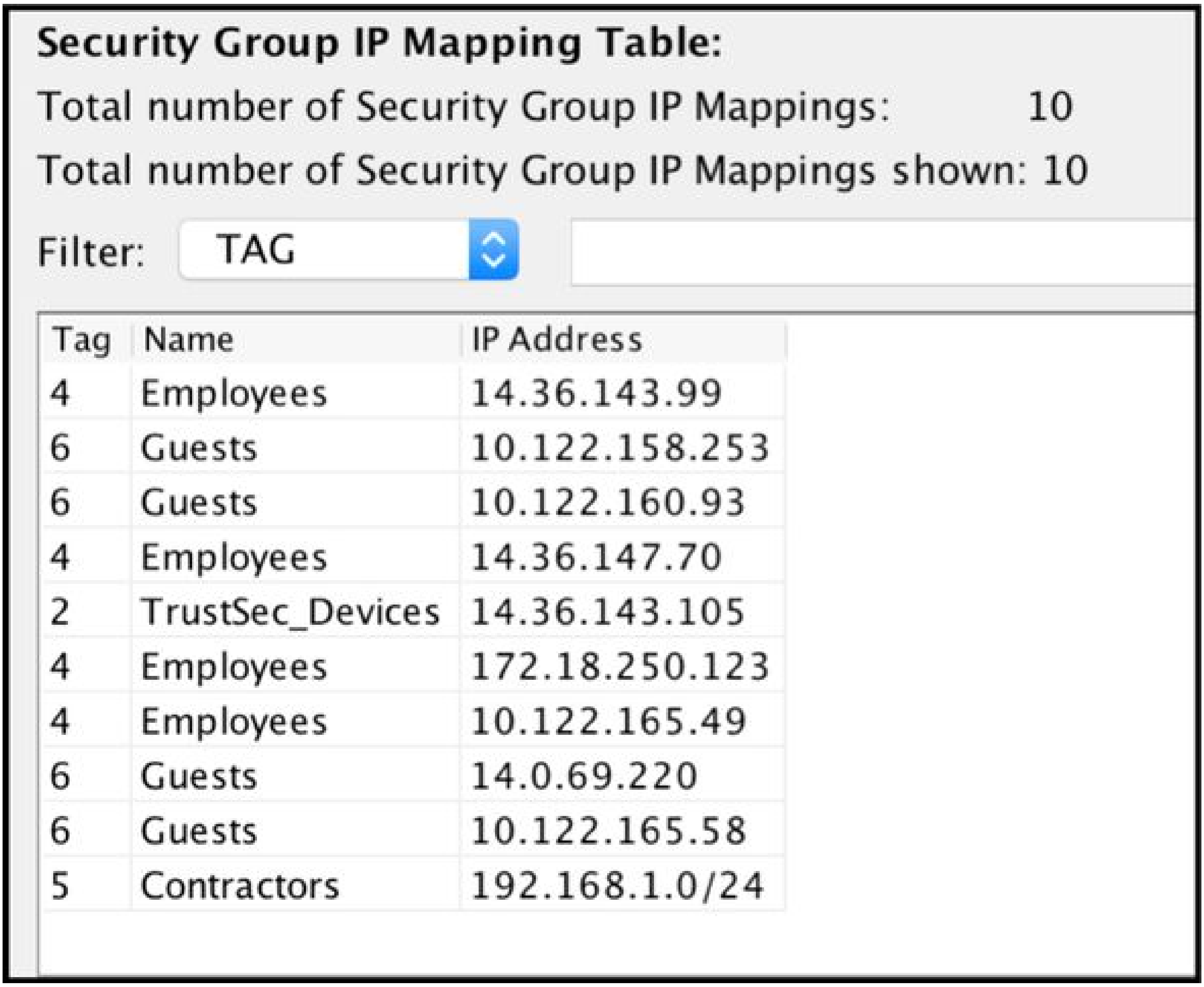
```
  SXP:                  Enabled
  Highest version:      3
  Default password:     Set
  Default local  IP:    14.36.143.30
  Reconcile period:     120 secs
  Retry open period:    120 secs
  Retry open timer:     Not Running
  Total number of SXP connections: 1
  Total number of SXP connections shown: 1
```

Peer Connection Status:

Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
14.36.143.223	14.36.143.30	On	3	Listener	1	Default	Not Running	Not Running	0:00:22:56 (dd:hr:mm:se

ASDM获知SXP IP到SGT的映射

Monitoring > Properties > Identity by TrustSec > **IP Mappings**



Security Group IP Mapping Table:

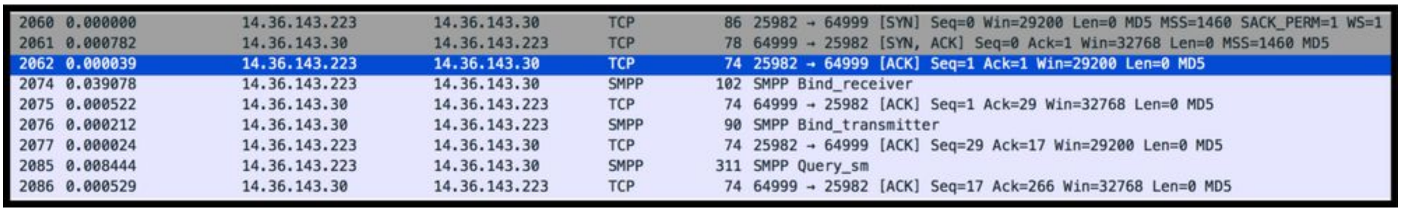
Total number of Security Group IP Mappings: 10

Total number of Security Group IP Mappings shown: 10

Filter: TAG

Tag	Name	IP Address
4	Employees	14.36.143.99
6	Guests	10.122.158.253
6	Guests	10.122.160.93
4	Employees	14.36.147.70
2	TrustSec_Devices	14.36.143.105
4	Employees	172.18.250.123
4	Employees	10.122.165.49
6	Guests	14.0.69.220
6	Guests	10.122.165.58
5	Contractors	192.168.1.0/24

在ISE上捕获数据包



```
2060 0.000000    14.36.143.223   14.36.143.30    TCP      86 25982 → 64999 [SYN] Seq=0 Win=29200 Len=0 MD5 MSS=1460 SACK_PERM=1 WS=1
2061 0.000782    14.36.143.30    14.36.143.223   TCP      78 64999 → 25982 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 MD5
2062 0.000039    14.36.143.223   14.36.143.30    TCP      74 25982 → 64999 [ACK] Seq=1 Ack=1 Win=29200 Len=0 MD5
2074 0.039078    14.36.143.223   14.36.143.30    SMPP    102 SMPP Bind_receiver
2075 0.000522    14.36.143.30    14.36.143.223   TCP      74 64999 → 25982 [ACK] Seq=1 Ack=29 Win=32768 Len=0 MD5
2076 0.000212    14.36.143.30    14.36.143.223   SMPP     90 SMPP Bind_transmitter
2077 0.000024    14.36.143.223   14.36.143.30    TCP      74 25982 → 64999 [ACK] Seq=29 Ack=17 Win=29200 Len=0 MD5
2085 0.008444    14.36.143.223   14.36.143.30    SMPP    311 SMPP Query_sm
2086 0.000529    14.36.143.30    14.36.143.223   TCP      74 64999 → 25982 [ACK] Seq=17 Ack=266 Win=32768 Len=0 MD5
```