Configurar o TrustSec SXP entre o ISE e o ASAv

Contents

Introduction

Este documento descreve como configurar uma conexão SXP (Security Group Exchange Protocol) entre o ISE (Identity Services Engine) e um ASAv (virtual Adaptive Security Appliance).

O SXP é o protocolo SGT (Security Group Tag) Exchange usado pelo TrustSec para propagar

mapeamentos de IP para SGT para dispositivos TrustSec. O SXP foi desenvolvido para permitir que as redes que incluem dispositivos de terceiros ou dispositivos antigos da Cisco que não suportam marcação em linha SGT tenham recursos TrustSec. O SXP é um protocolo de peering, um dispositivo atuará como um alto-falante e o outro como um ouvinte. O alto-falante do SXP é responsável por enviar as associações IP-SGT e o ouvinte é responsável por coletar essas associações. A conexão SXP usa a porta TCP 64999 como o protocolo de transporte subjacente e MD5 para integridade/autenticidade da mensagem.

O SXP foi publicado como um rascunho da IETF no link a seguir:

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

Prerequisites

Requirements

Matriz de compatibilidade TrustSec:

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

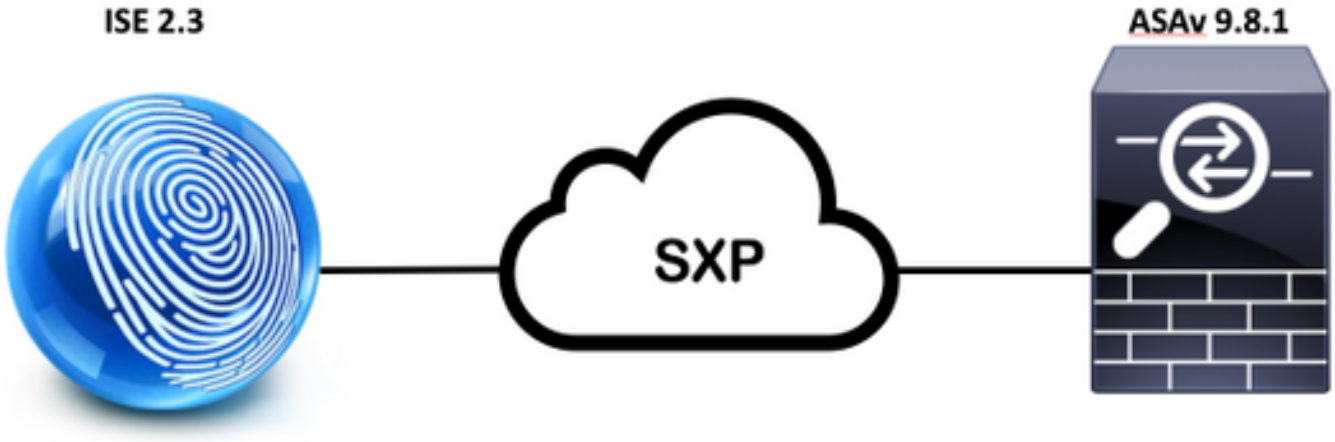
Componentes Utilizados

ISE 2.3

ASAv 9.8.1

ASDM 7.8.1.150

Diagrama de Rede



Endereços IP

ISE: 14.36.143.223

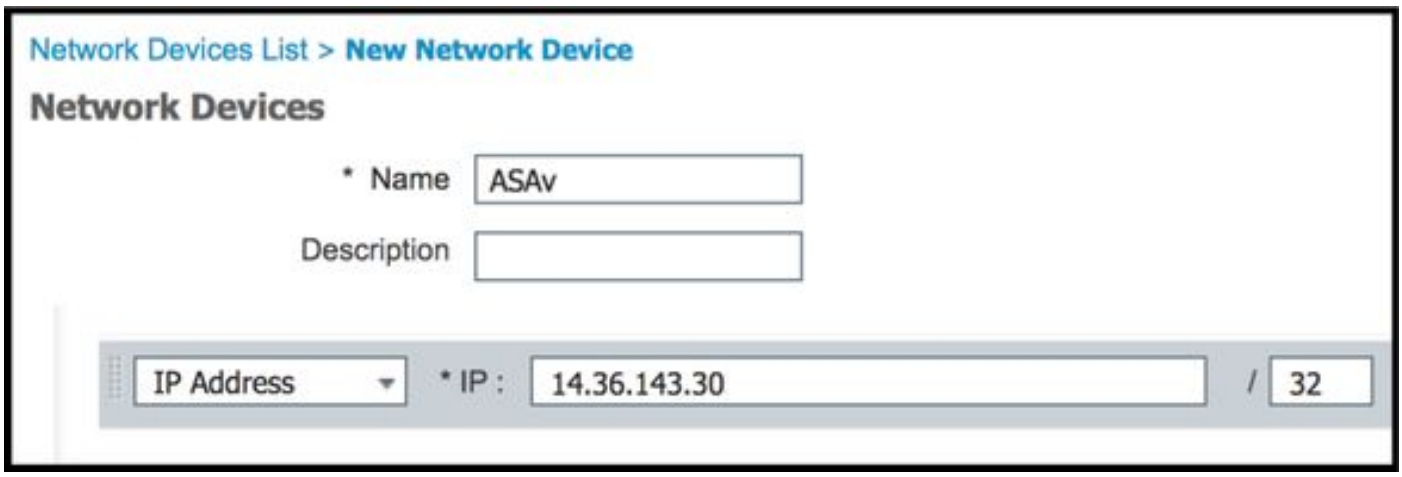
ASAv: 14.36.143.30

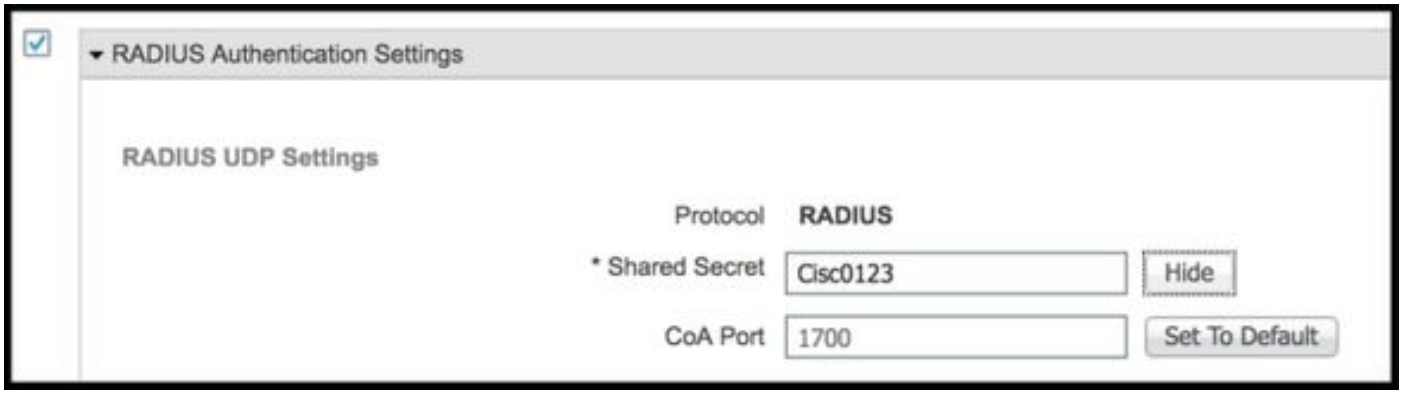
Configuração inicial

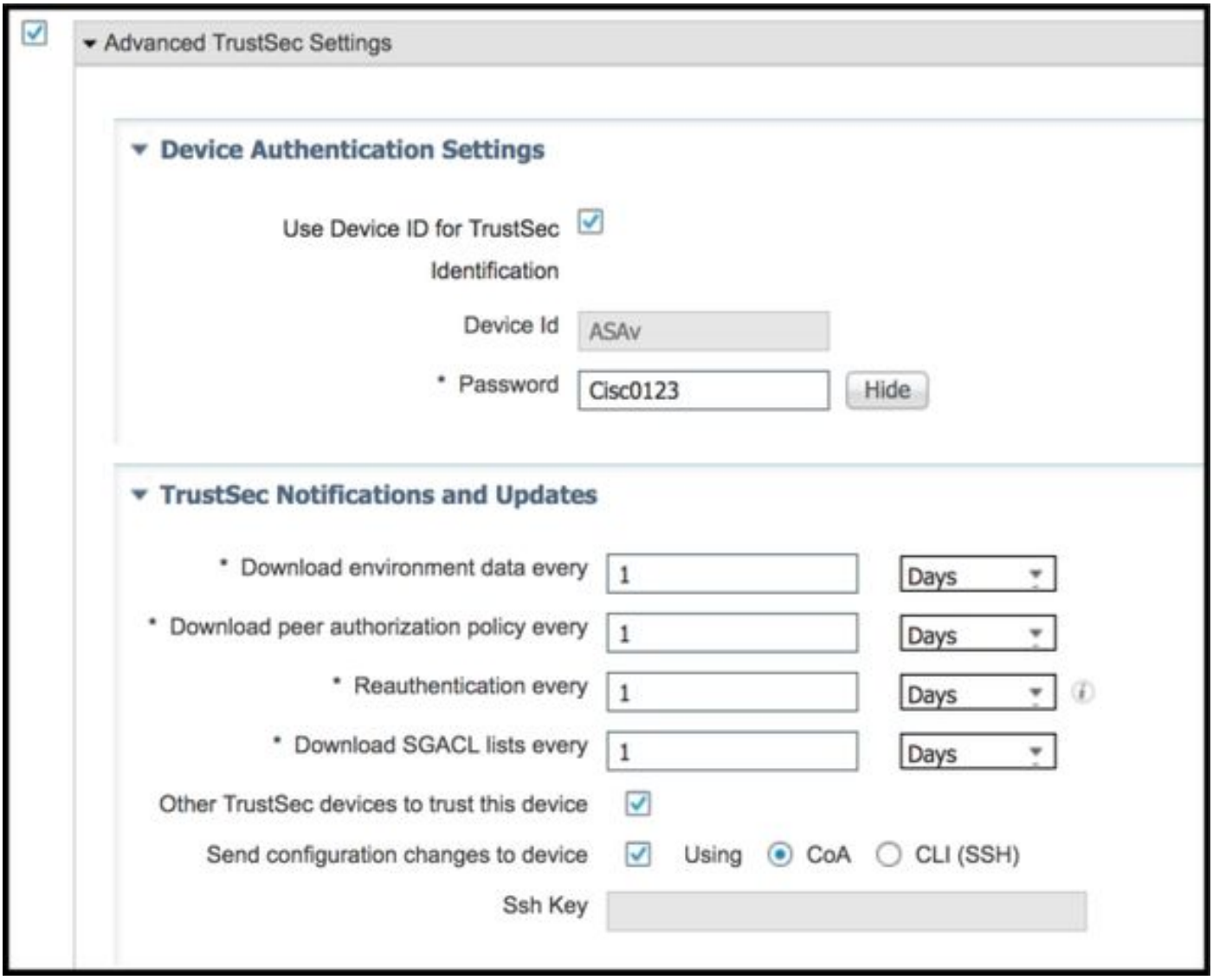
Dispositivo de rede ISE

Registrar o ASA como um dispositivo de rede

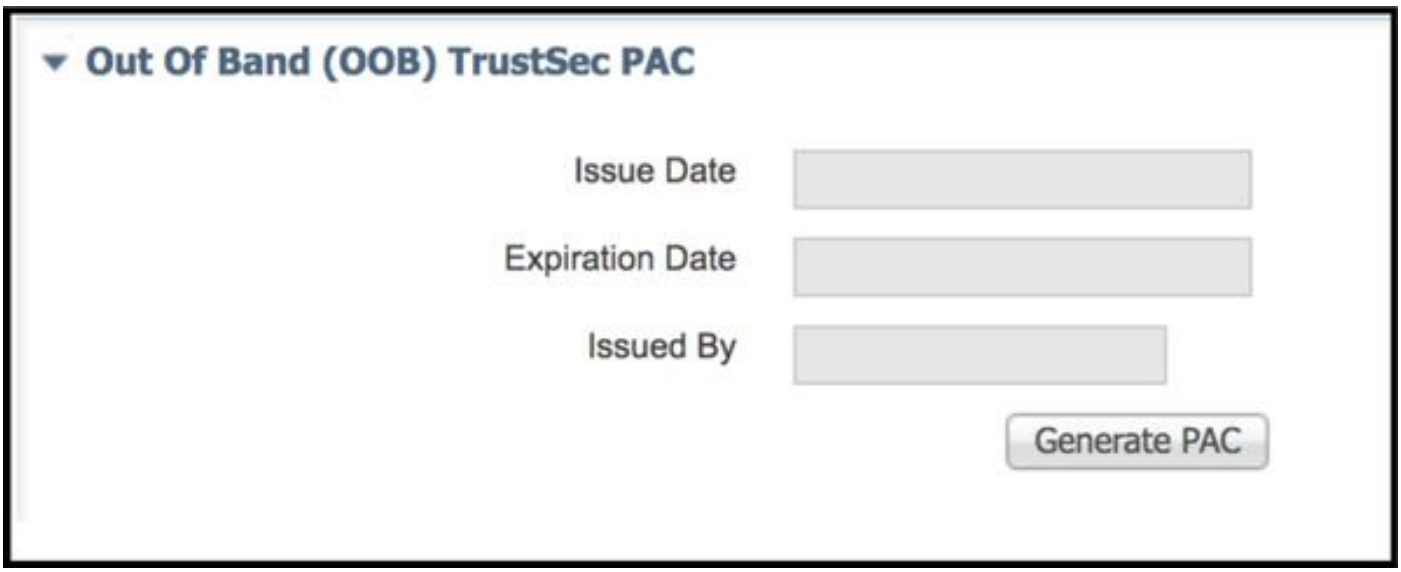
Centros de Trabalho > TrustSec > Componentes > Dispositivos de Rede > **Adicionar**

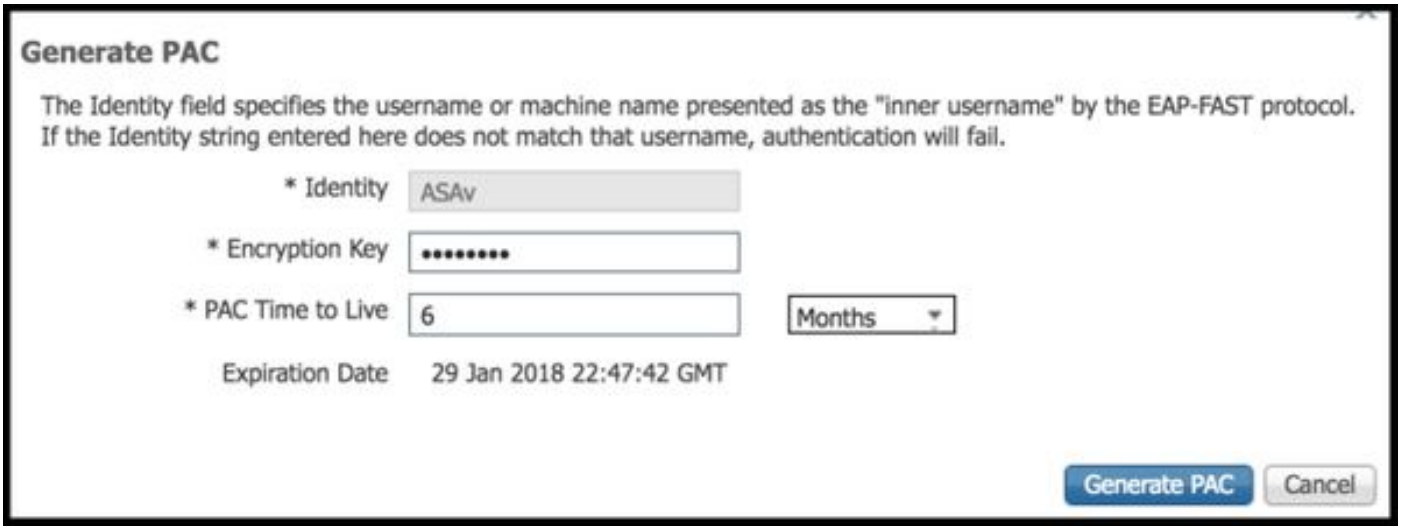


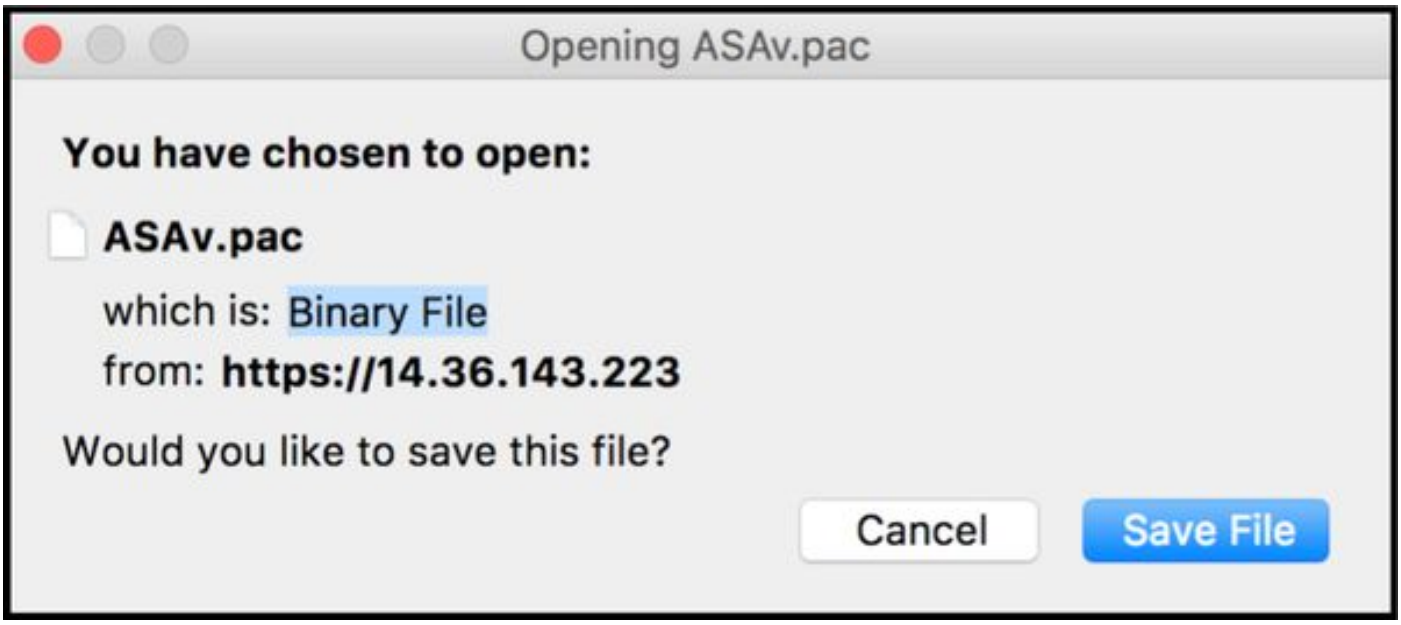




Gerar PAC fora da banda (OOB) (Credencial de Acesso Protegido) e transferir



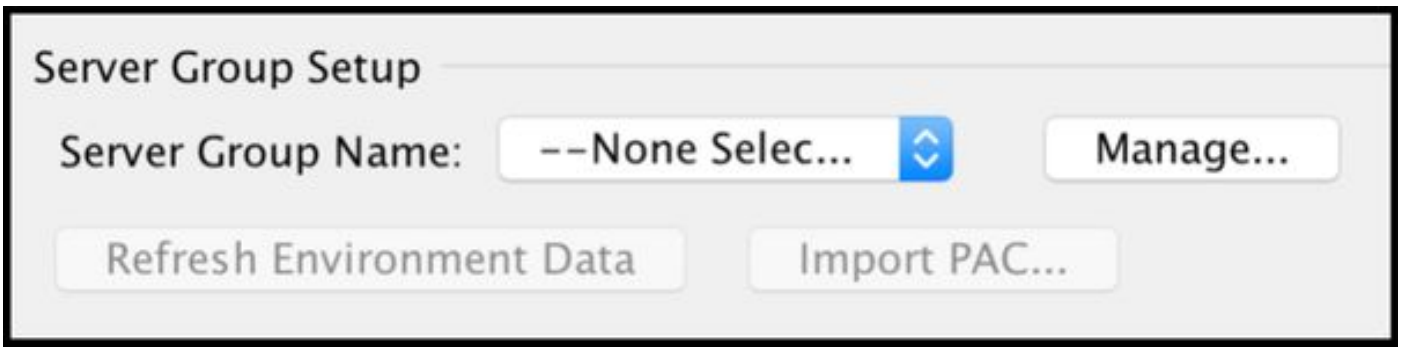




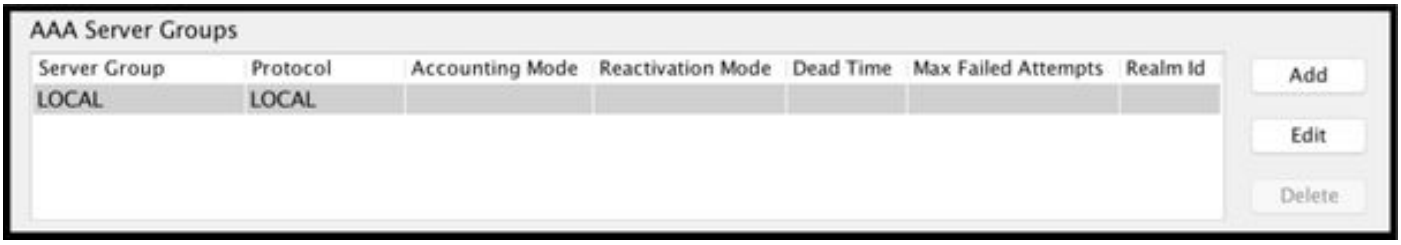
Configuração do servidor ASDM AAA

Criar grupo de servidores AAA

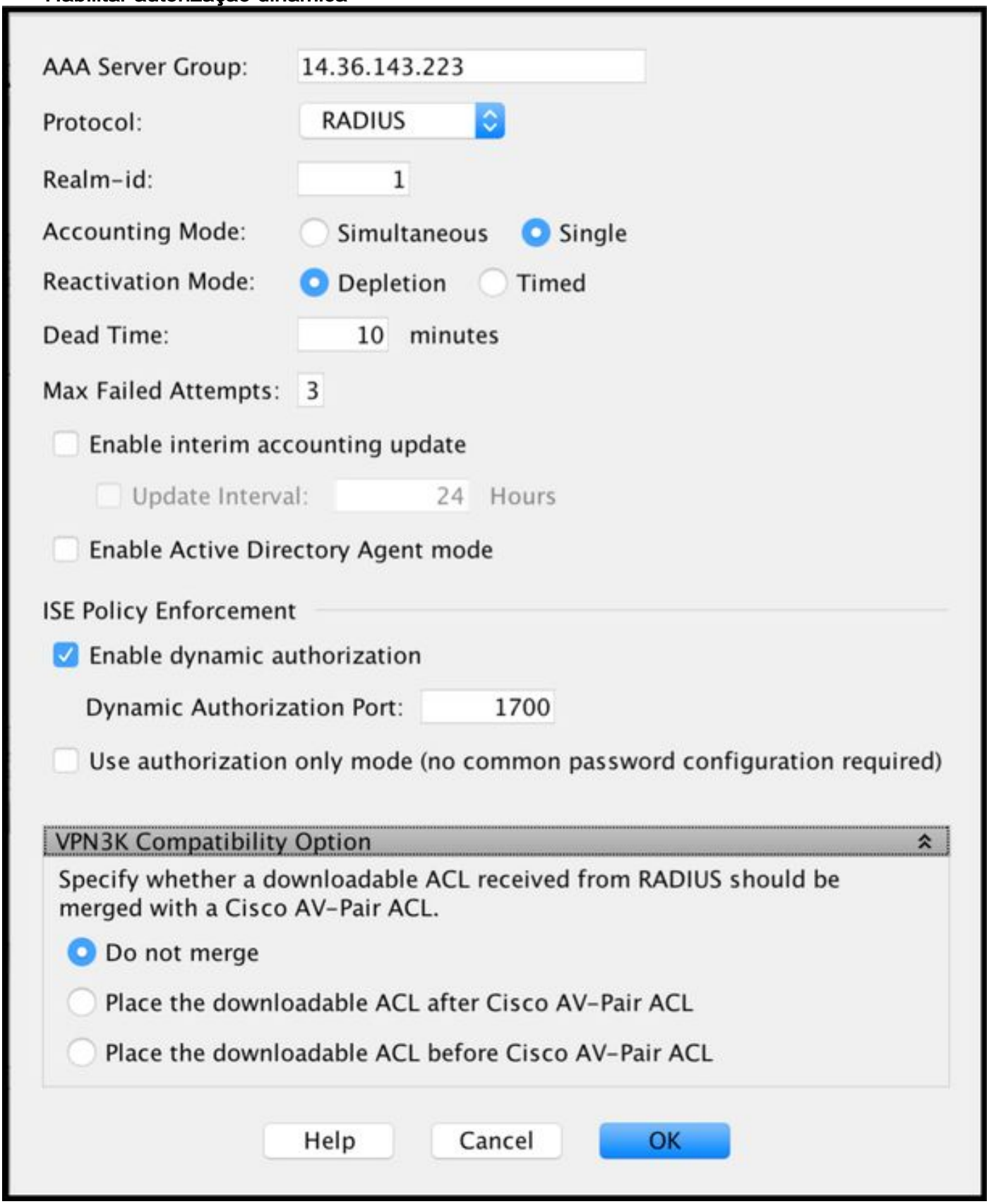
Configuração > Firewall > Identity by TrustSec > Server Group Setup > **Manage...**



Grupos de servidores AAA > **Adicionar**

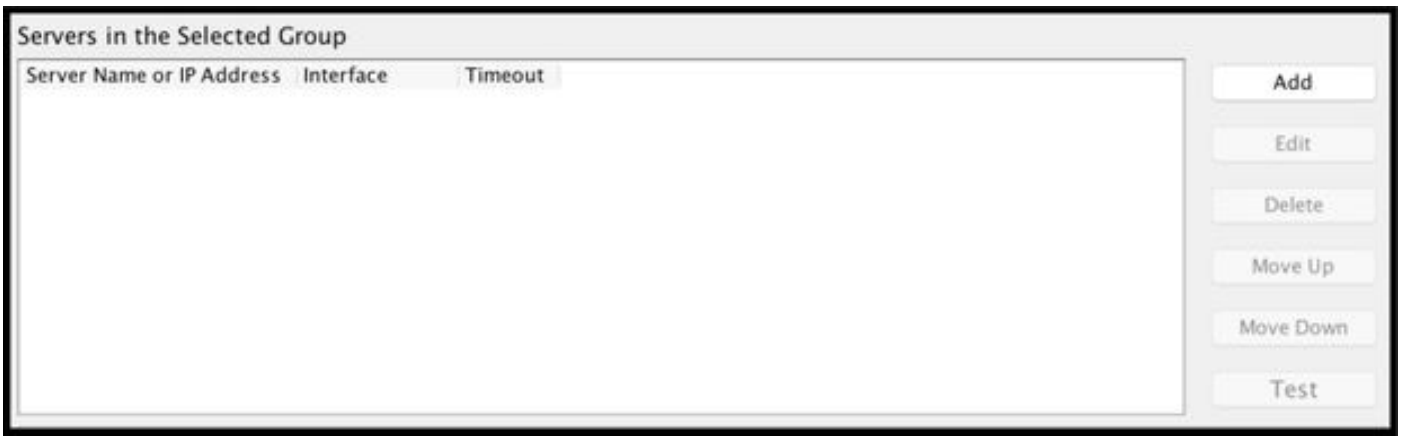


- Grupo de servidores AAA: **<Nome do grupo>**
- **Habilitar autorização dinâmica**

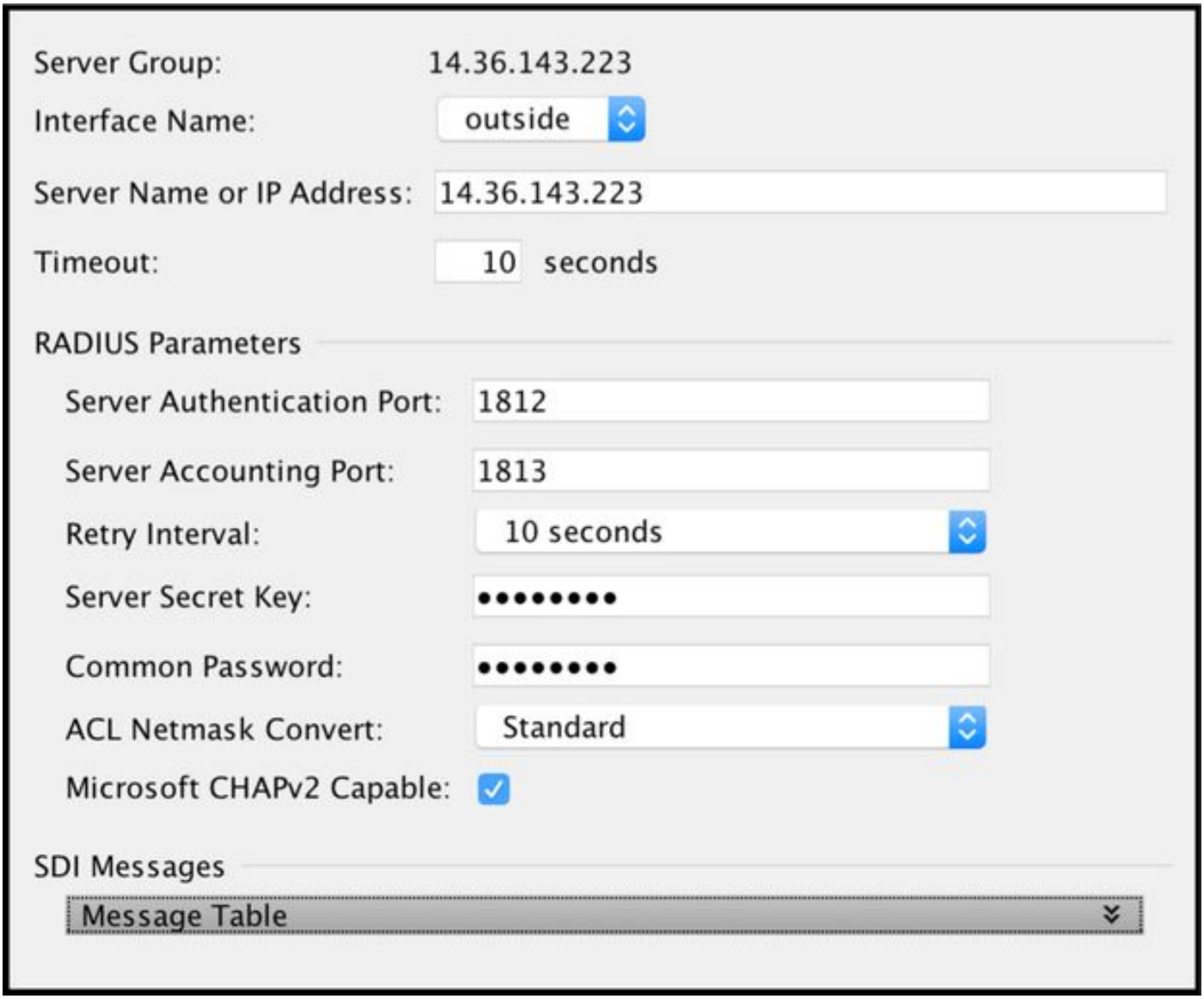


Adicionar servidor ao grupo de servidores

Servidores no Grupo Selecionado > **Adicionar**

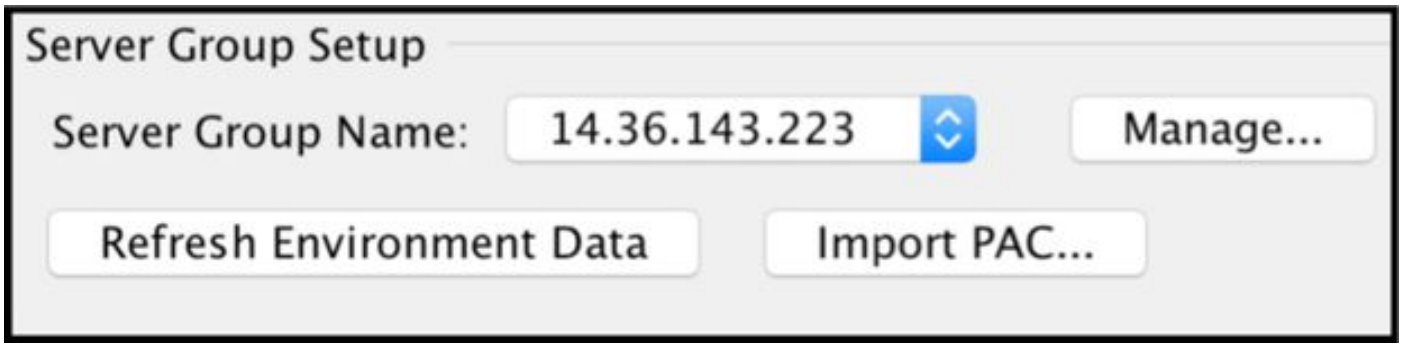


- Nome do servidor ou endereço IP: **<Endereço IP do ISE>**
- Porta de autenticação do servidor: **1812**
- Porta de relatório do servidor: **1813**
- Chave secreta do servidor: **Cisco0123**
- Senha comum: **Cisco0123**

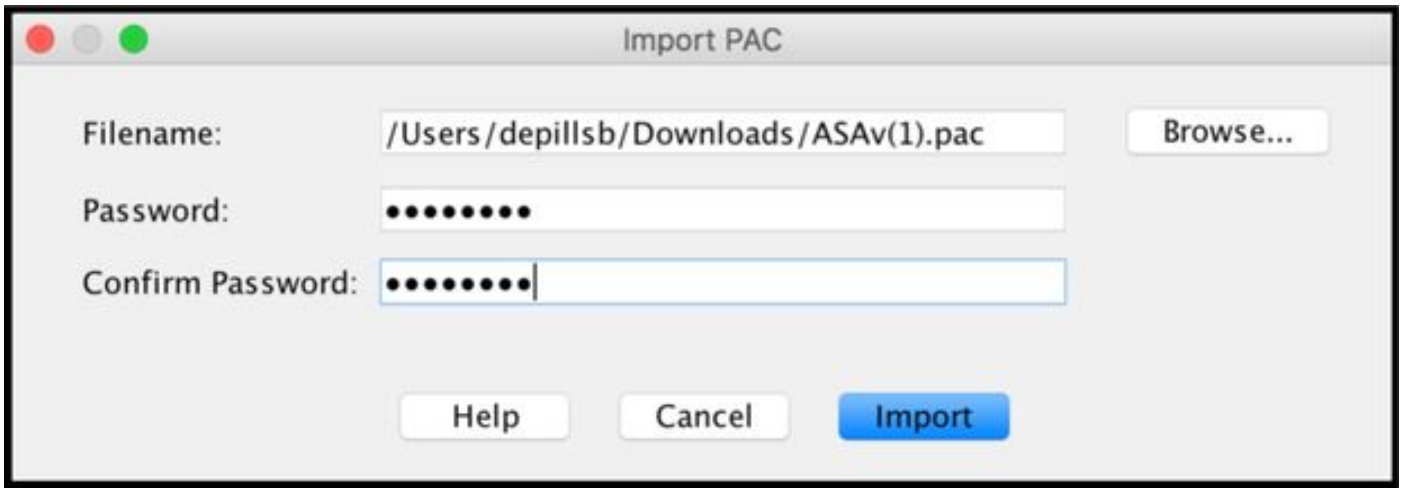


Importar PAC baixado do ISE

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



- Senha: **Cisco0123**



Atualizar dados do ambiente

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

Verificação

Logs ao vivo do ISE

Operações > RADIUS > **Logs ao vivo**

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

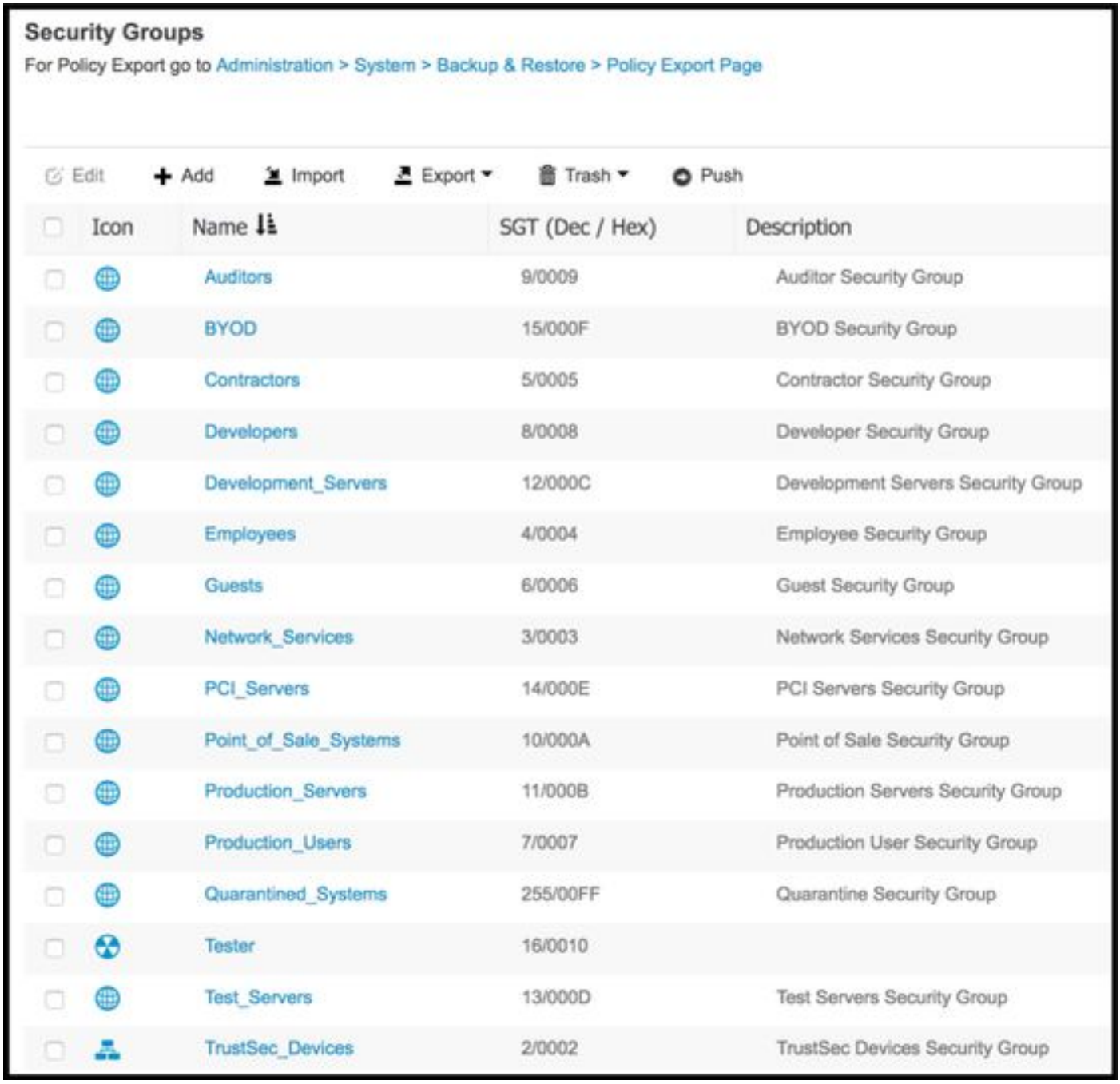
CiscoAVPair	cts-security-group-table=0001, cts-pac-opaque=****, coa-push=true

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

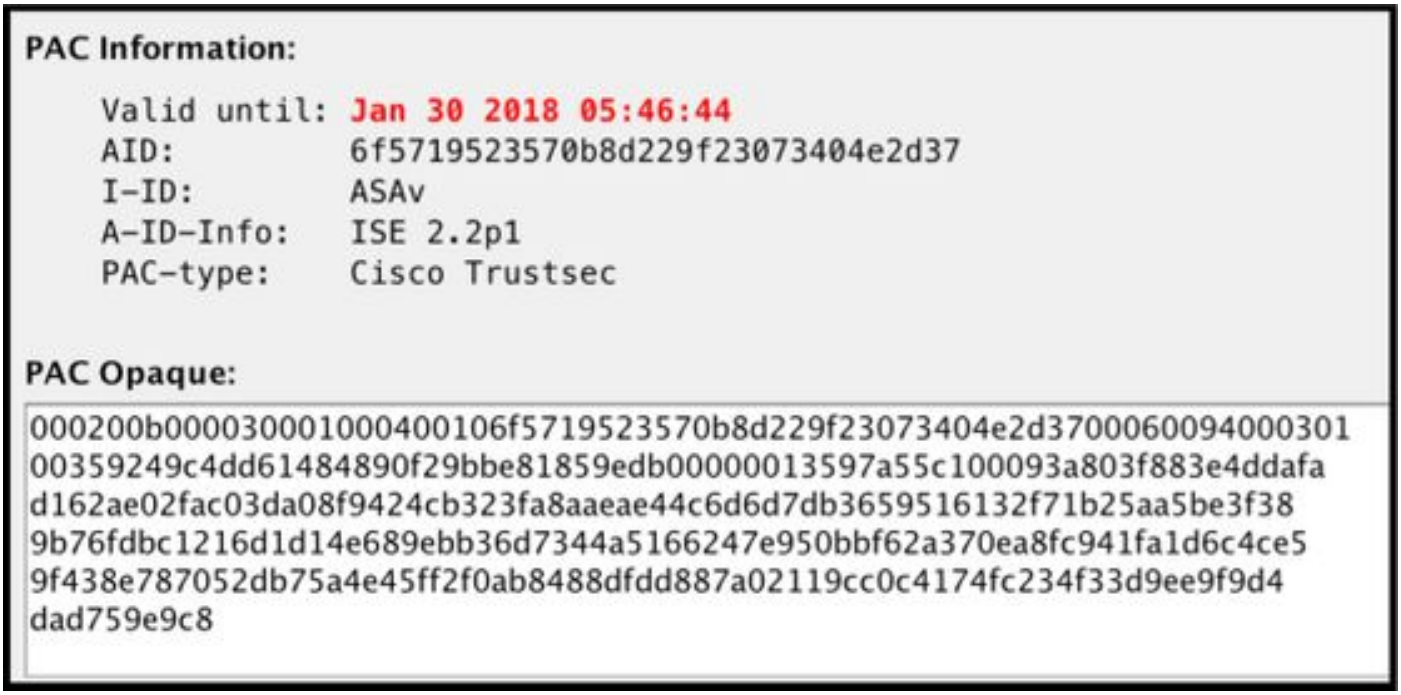
Grupos de segurança do ISE

Centros de Trabalho > TrustSec > Componentes > **Grupos de Segurança**



PAC de ASDM

Monitoramento > Propriedades > Identidade por TrustSec > **PAC**



Grupos de dados e segurança do ambiente ASDM

Monitoramento > Propriedades > Identidade por TrustSec > **Dados de ambiente**

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

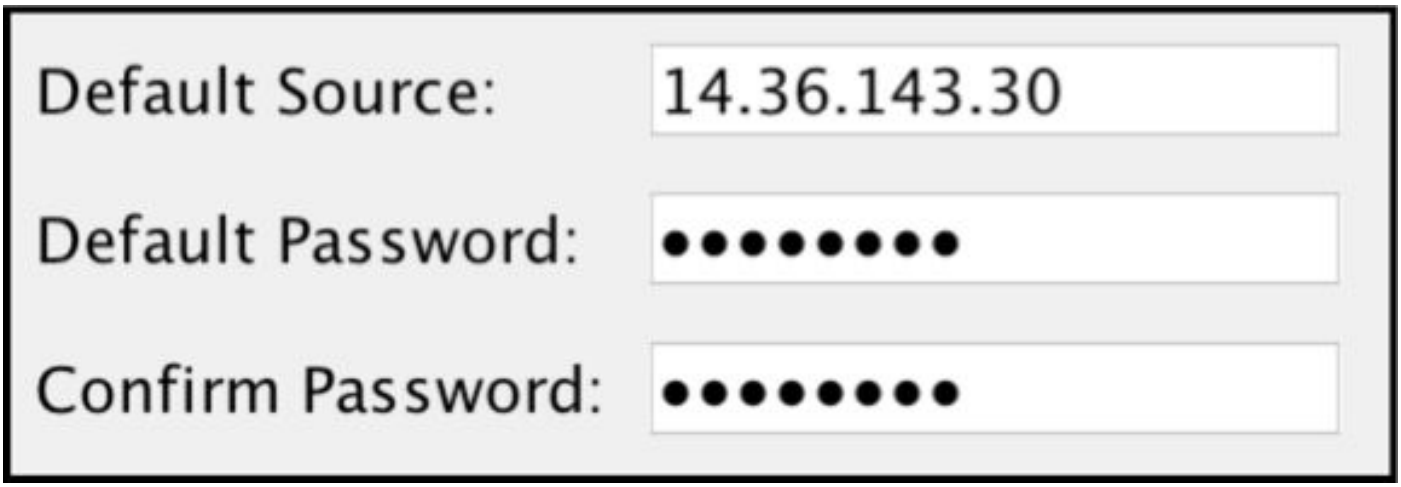
Configuração do ASDM SXP

Habilitar SXP

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

Definir o endereço IP de origem padrão do SXP e a senha padrão do SXP

Configuração > Firewall > Identity by TrustSec > **Connection Peers** (Configuração > Firewall > Identidade por TrustSec > **Peers de conexão)**



Adicionar par SXP

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

- Endereço IP do peer: **<Endereço IP do ISE>**

Configuração do ISE SXP

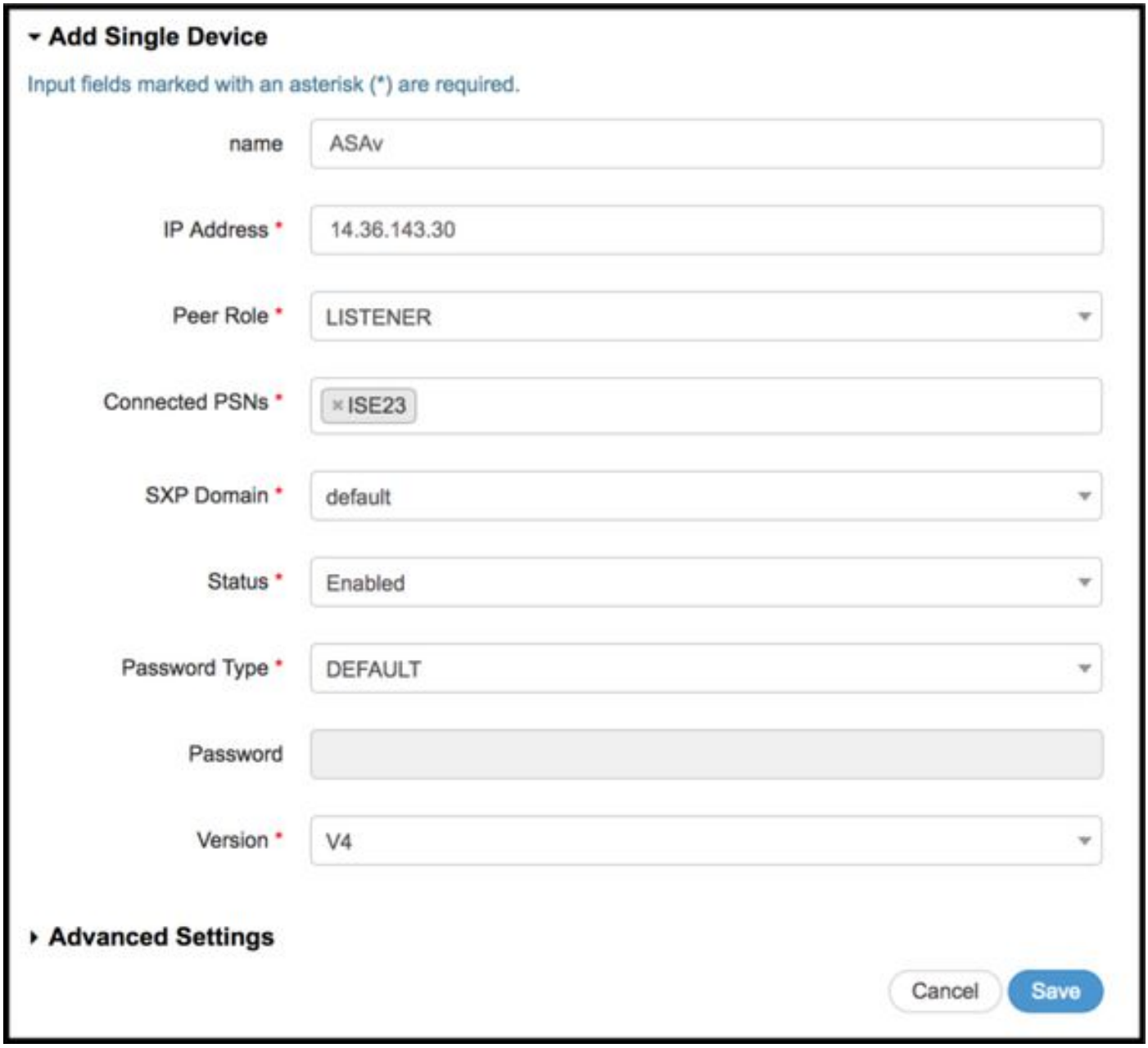
Configuração de senha do Global SXP

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

- Senha global: **Cisco0123**

Adicionar dispositivo SXP

WorkCenters > TrustSec > SXP > Dispositivos SXP > **Adicionar**



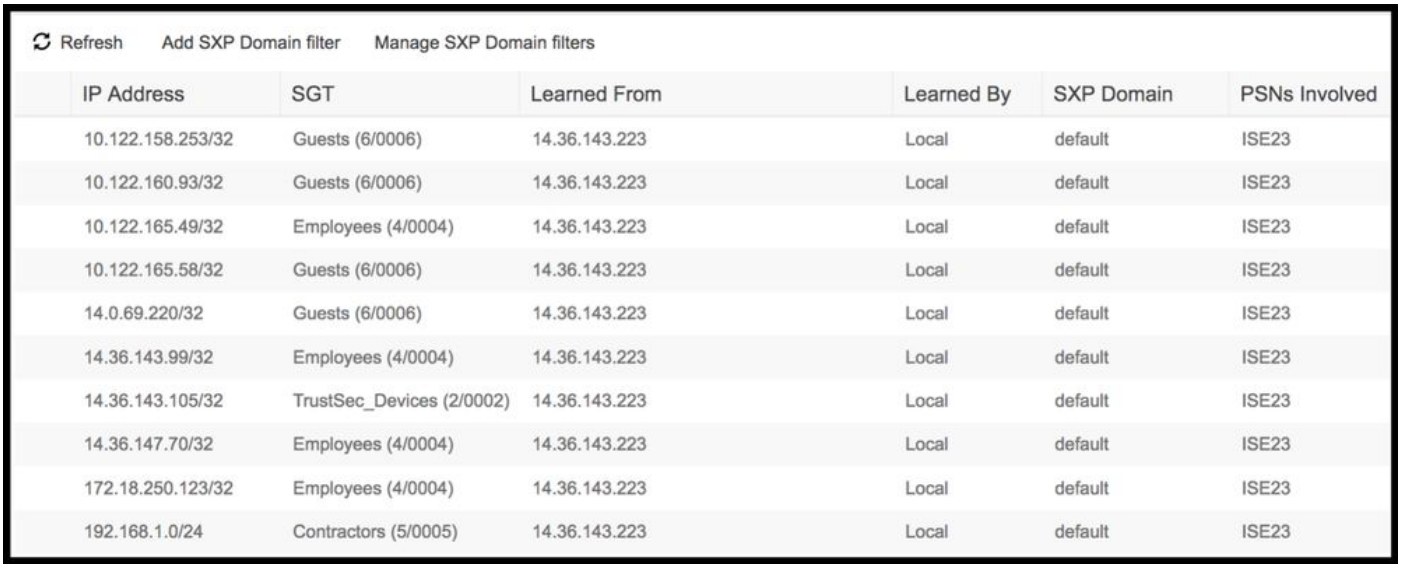
Verificação SXP

verificação de ISE SXP

WorkCenters > TrustSec > SXP > **Dispositivos SXP**

Mapeamentos ISE SXP

WorkCenters > TrustSec > SXP > **Todos os mapeamentos SXP**

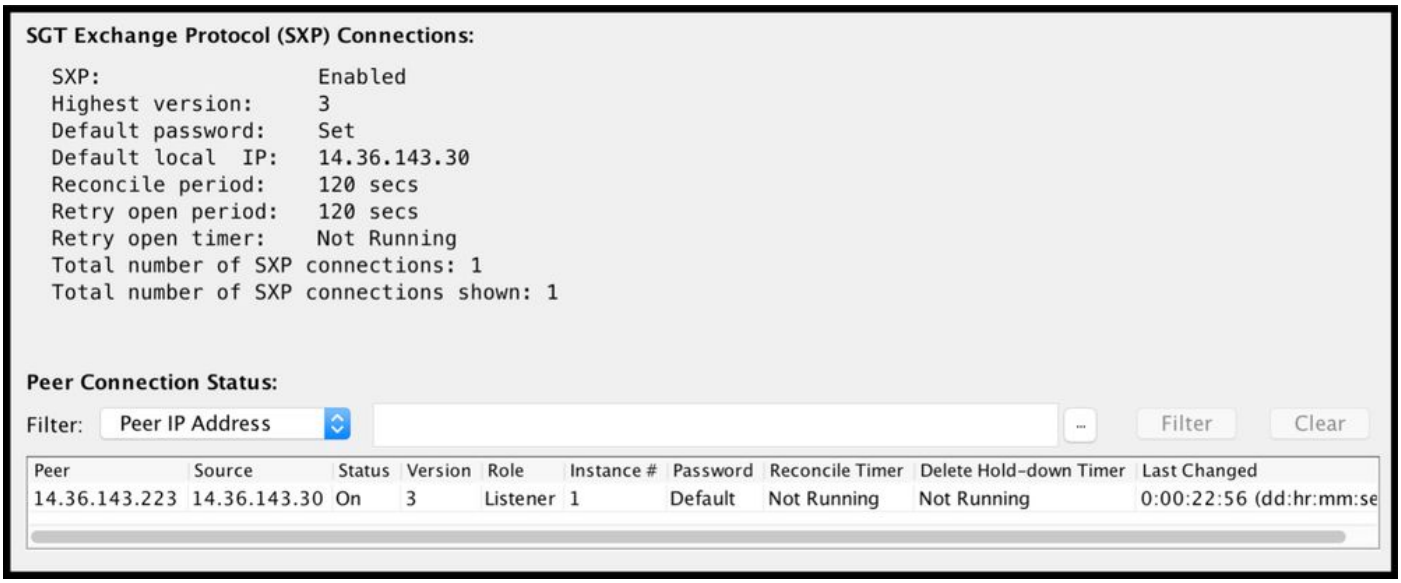


Refresh Add SXP Domain filter Manage SXP Domain filters

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

verificação ASDM SXP

Monitoramento > Propriedades > Identidade por TrustSec > **Conexões SXP**



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:

Filter: Peer IP Address ... Filter Clear

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

O ASDM aprendeu IP SXP para mapeamentos SGT

Monitoramento > Propriedades > Identidade por TrustSec > **Mapeamentos IP**

Security Group IP Mapping Table:

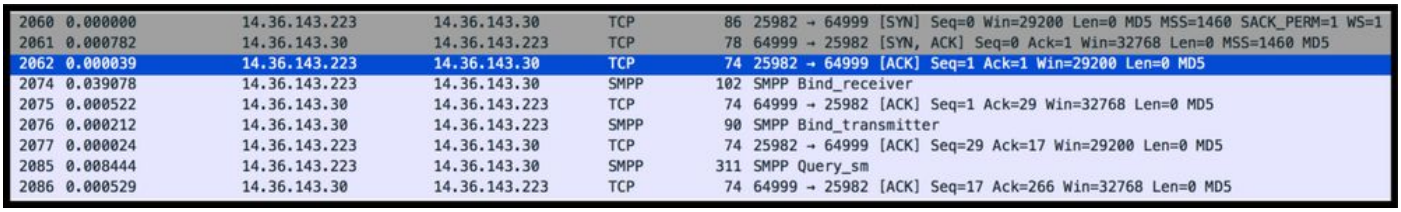
Total number of Security Group IP Mappings: 10

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

Captura de pacote tirada no ISE



```
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
```