Configurer TrustSec SXP entre ISE et ASAv

Contenu

Introduction

Ce document décrit comment configurer une connexion SXP (Security Group Exchange Protocol) entre ISE (Identity Services Engine) et ASAv (Virtual Adaptive Security Appliance).

SXP est le SGT (Security Group Tag) Exchange Protocol utilisé par TrustSec pour propager les mappages IP/SGT aux périphériques TrustSec. SXP a été développé pour permettre aux réseaux, y compris les périphériques tiers ou les périphériques Cisco existants qui ne prennent pas en charge le marquage en ligne SGT, d'avoir des fonctionnalités TrustSec. SXP est un protocole d’appairage, un périphérique agit en tant que haut-parleur et l’autre en tant qu’écouteur. Le haut-parleur SXP est responsable de l'envoi des liaisons IP-SGT et l'écouteur est responsable de la collecte de ces liaisons. La connexion SXP utilise le port TCP 64999 comme protocole de transport sous-jacent et MD5 pour l'intégrité/l'authenticité des messages.

SXP a été publié en tant que brouillon IETF à l'adresse suivante :

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

Conditions préalables

Conditions requises

Matrice de compatibilité TrustSec :

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

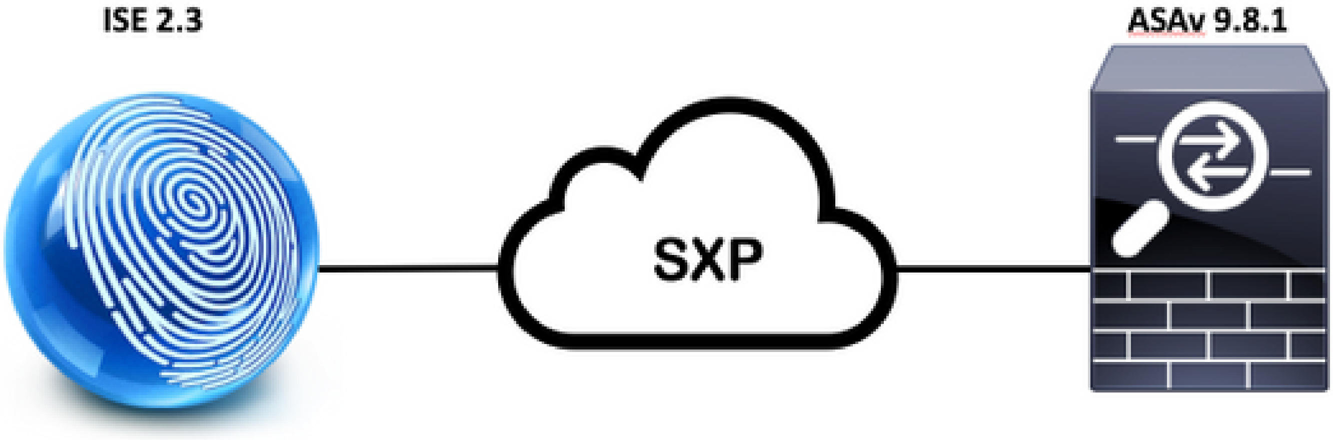
Components Used

ISE 2.3

ASAv 9.8.1

ASDM 7.8.1.150

Diagramme du réseau



Adresses IP

ISE: 14.36.143.223

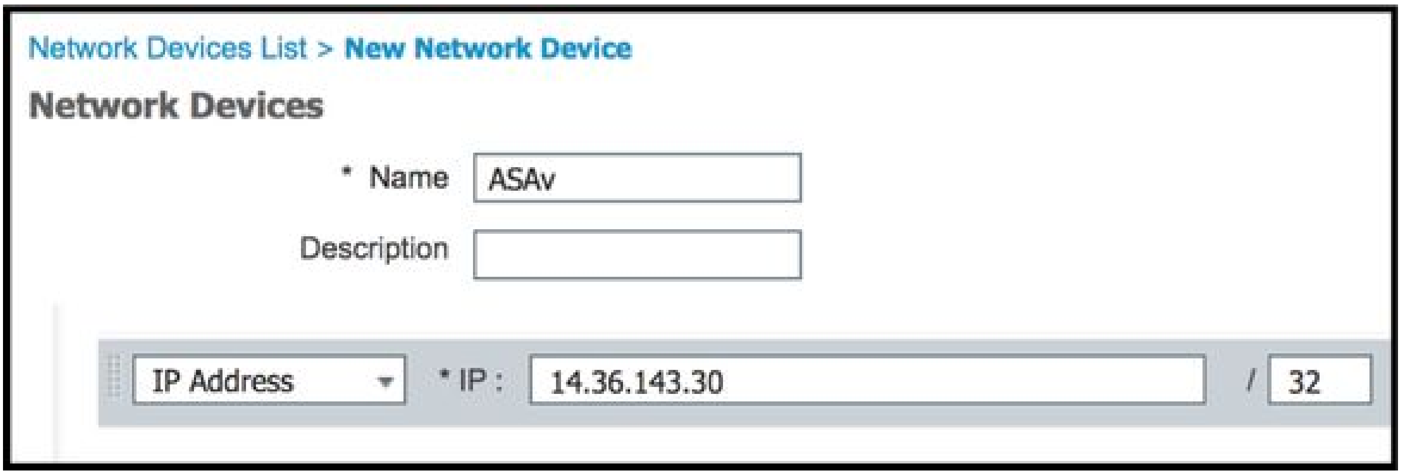
ASAv : 14.36.143.30

Configuration initiale

Périphérique réseau ISE

Enregistrer ASA comme périphérique réseau

WorkCenters > TrutSec > Components > Network Devices > **Add**



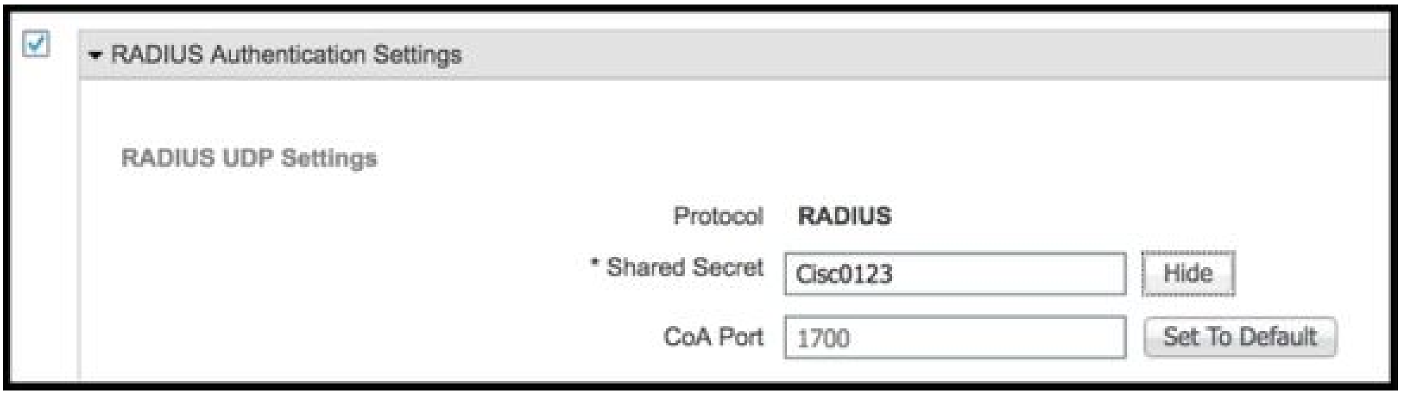
Network Devices List > New Network Device

Network Devices

* Name: ASAv

Description:

IP Address ▾ * IP : 14.36.143.30 / 32



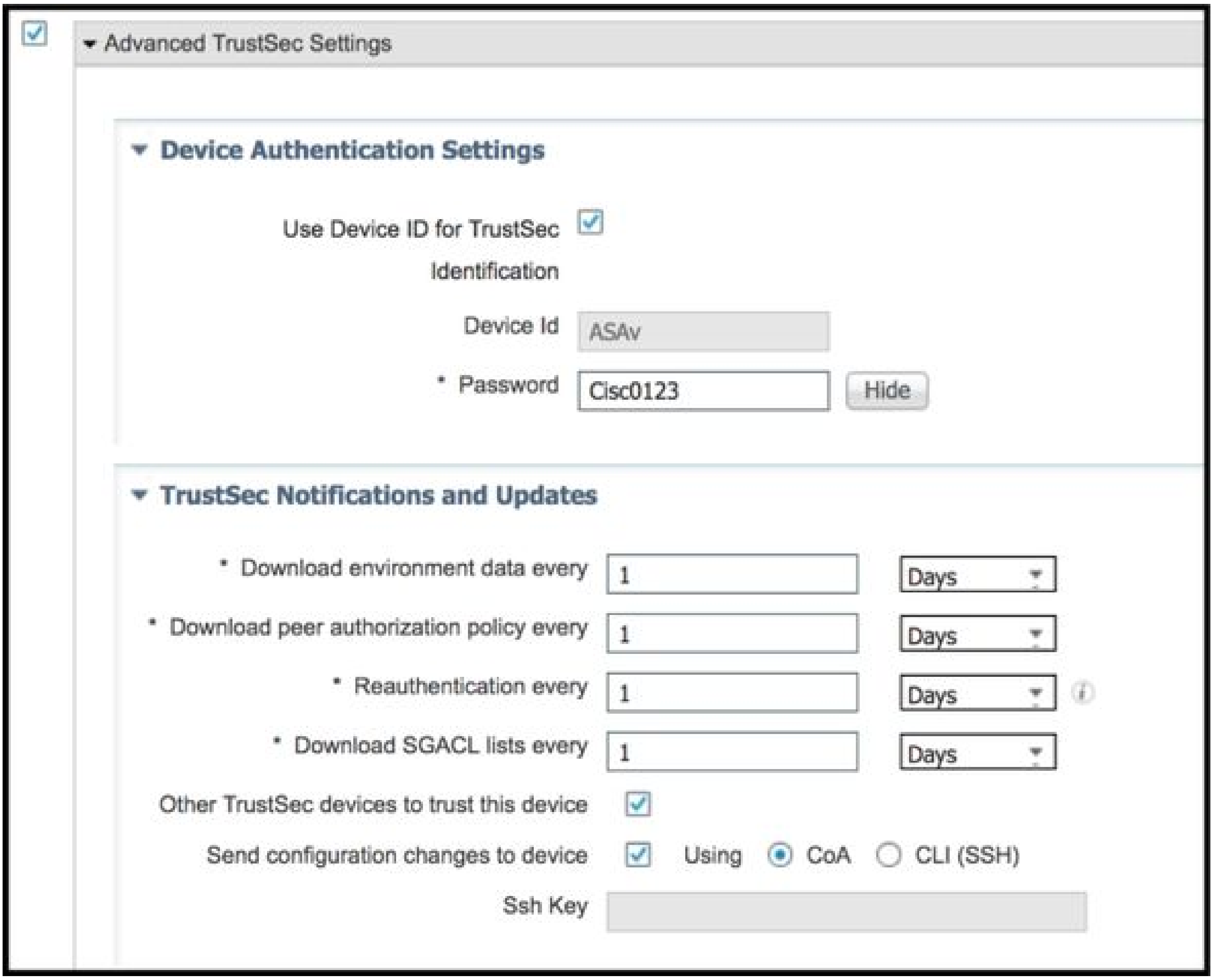
☑ ▾ RADIUS Authentication Settings

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 Hide

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

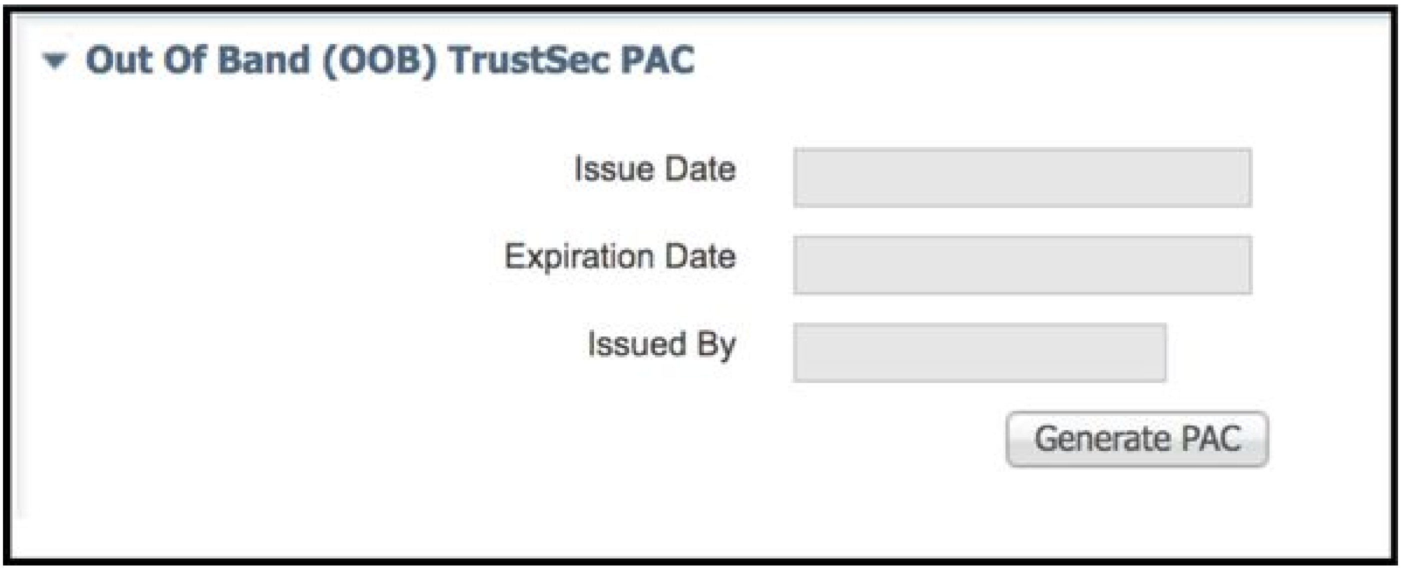
* Download SGACL lists every: 1 Days

Other TrustSec devices to trust this device ☑

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

Ssh Key:

Générer un PAC hors bande (OOB) (Protected Access Credential) et télécharger

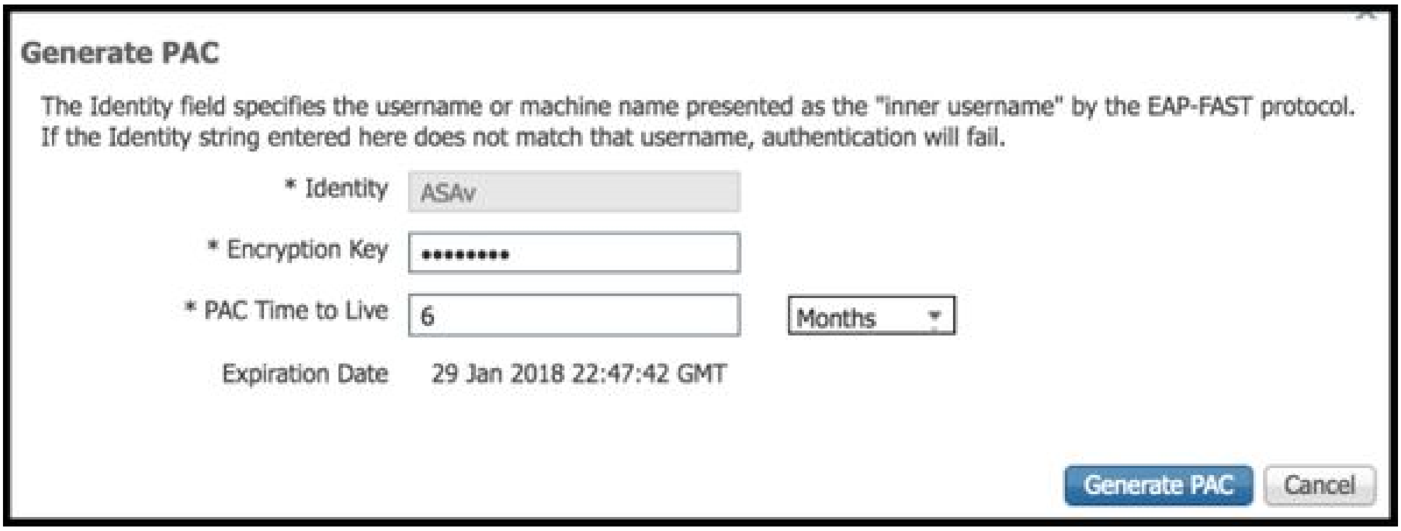


Out Of Band (OOB) TrustSec PAC

Issue Date:

Expiration Date:

Issued By:


Generate PAC

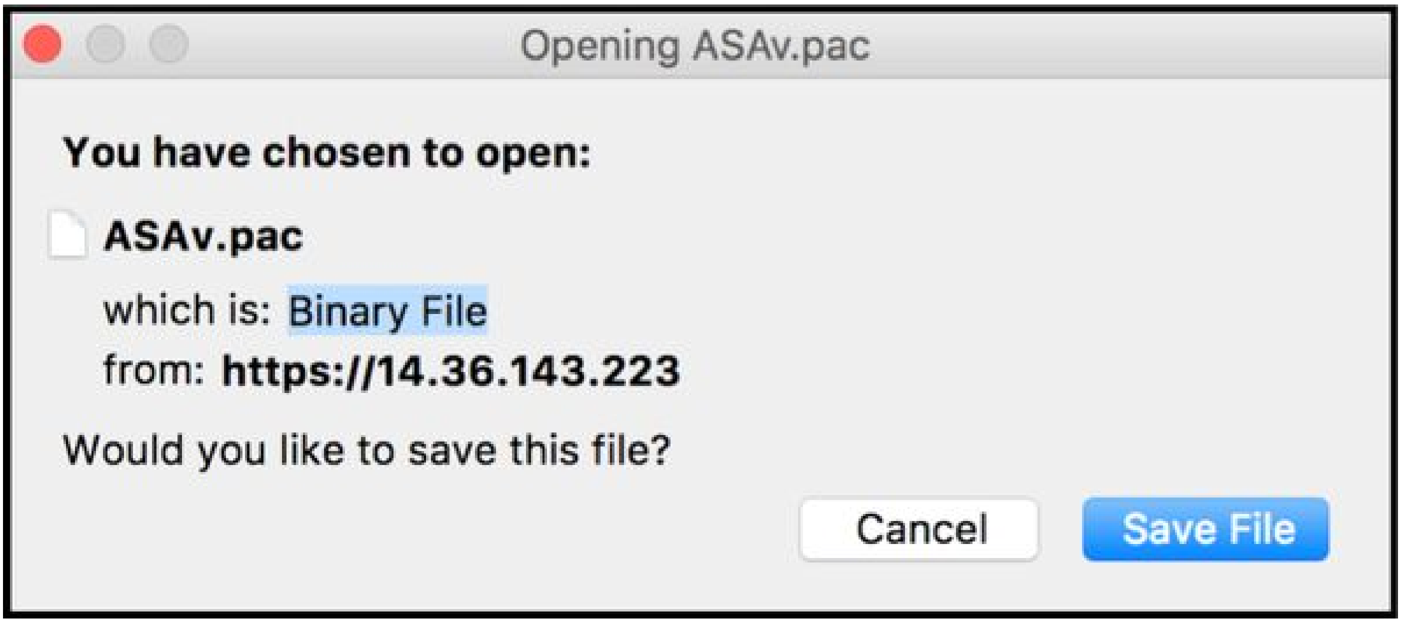
The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* 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

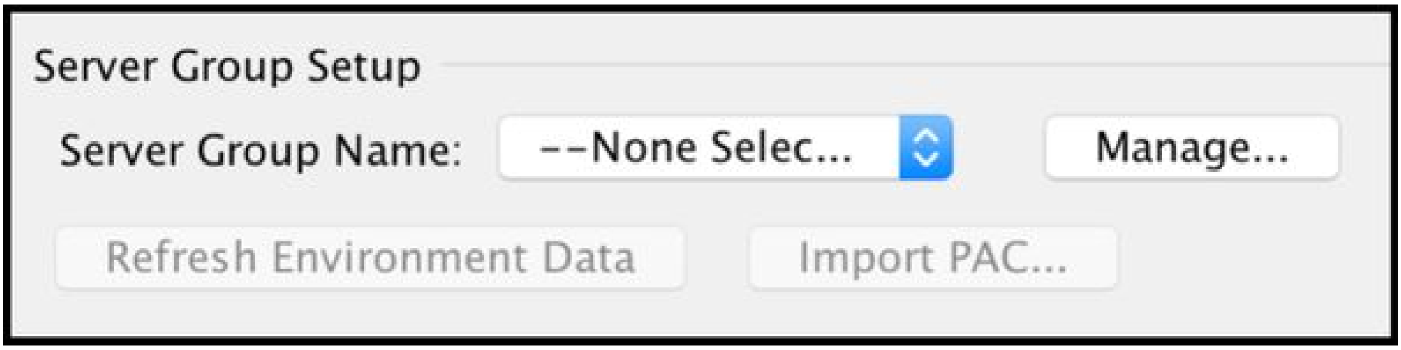
from: https://14.36.143.223

Would you like to save this file?

Configuration du serveur ASDM AAA

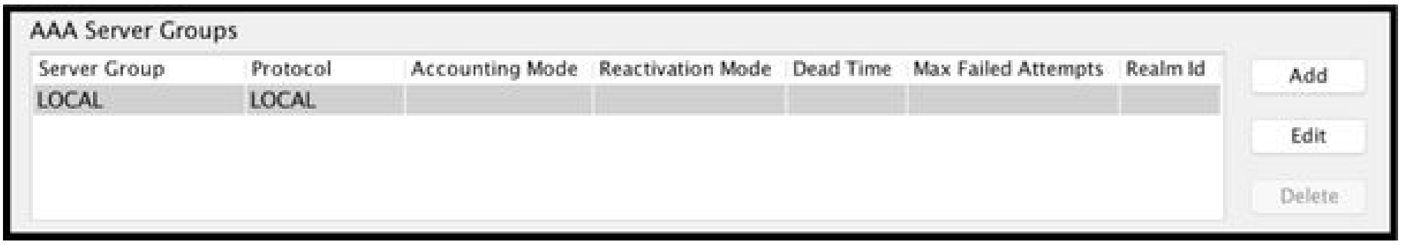
Créer un groupe de serveurs AAA

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


Server Group Setup

Server Group Name: --None Selec...

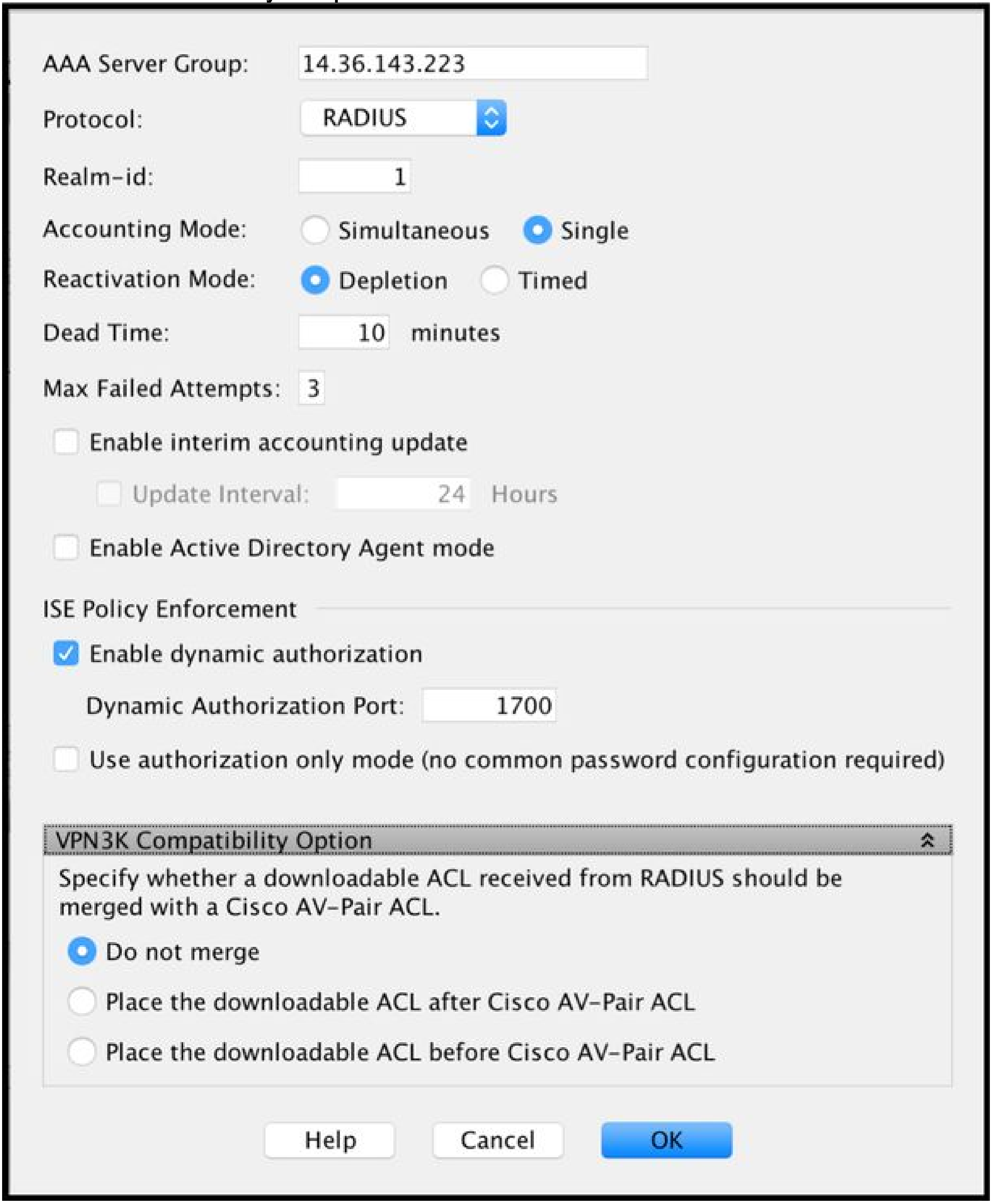
Groupes de serveurs AAA > **Ajouter**



AAA Server Groups

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

- Groupe de serveurs AAA : **<Nom du groupe>**
- **Activer l'autorisation dynamique**



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.

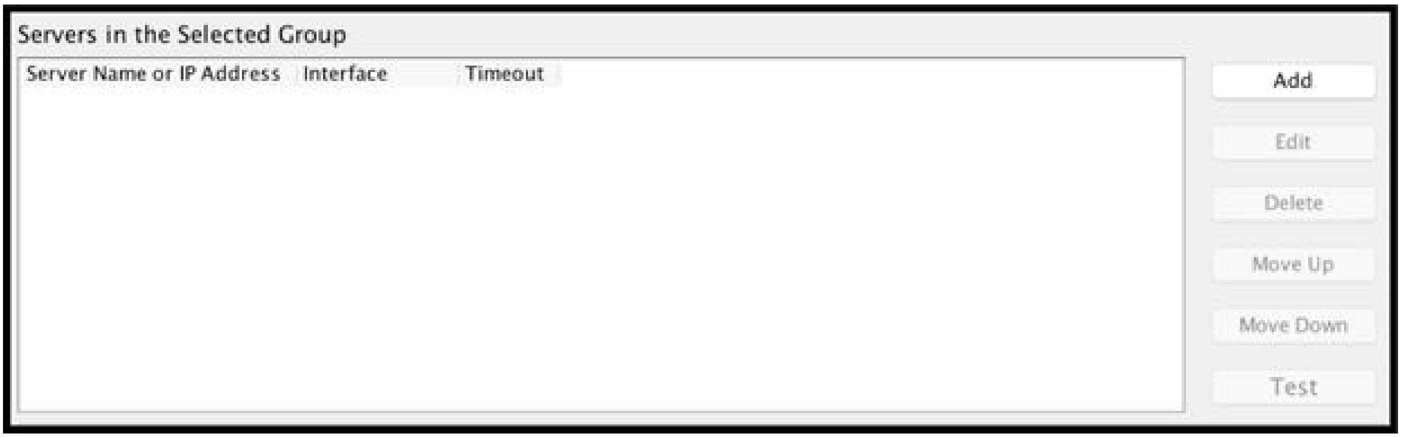
● Do not merge

○ Place the downloadable ACL after Cisco AV-Pair ACL

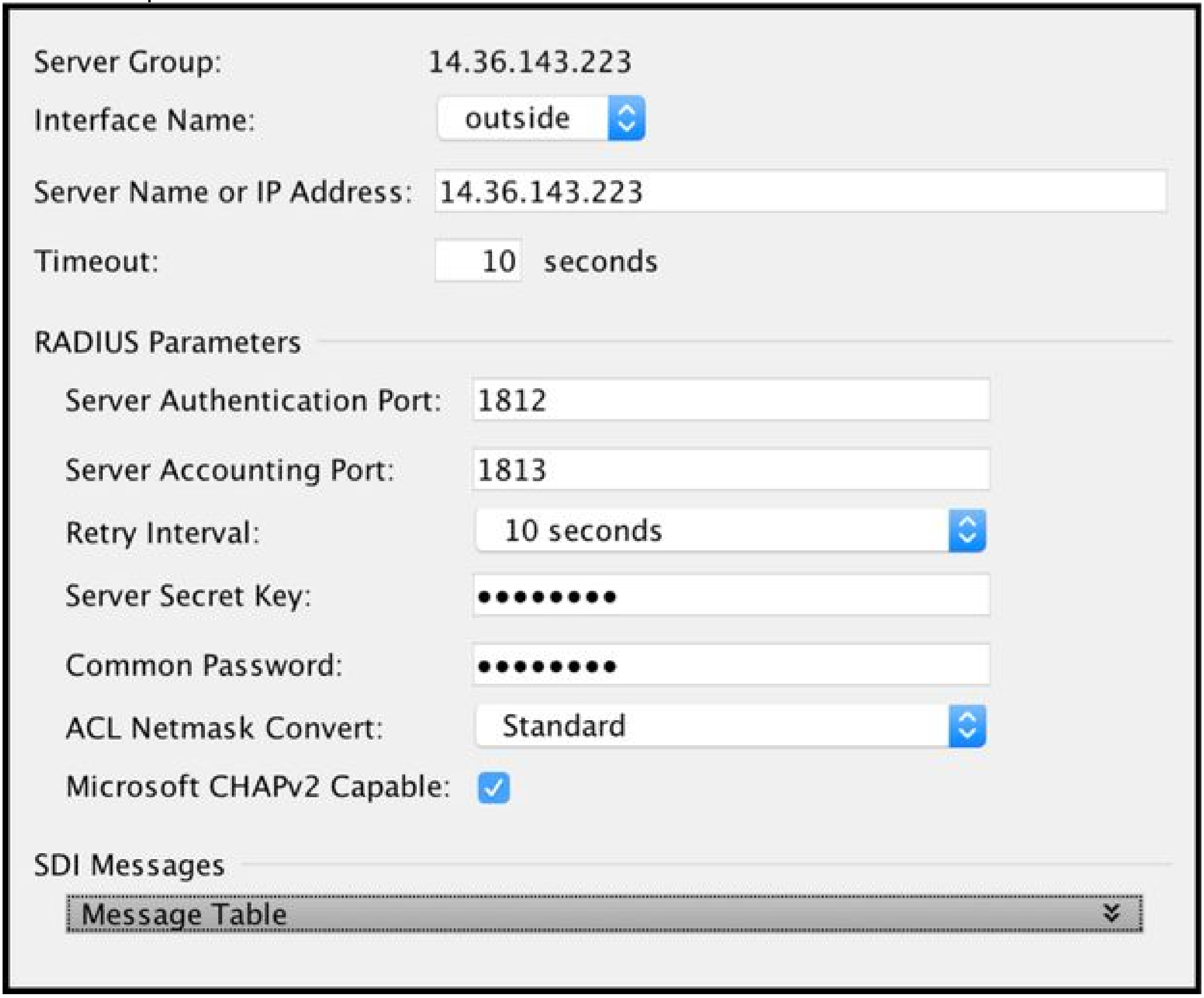
○ Place the downloadable ACL before Cisco AV-Pair ACL

Ajouter un serveur au groupe de serveurs

Serveurs du groupe sélectionné > **Ajouter**



- Nom du serveur ou adresse IP : **<Adresse IP ISE>**
- Port d'authentification du serveur : **1812**
- Port de comptabilité du serveur : **1813**
- Clé secrète du serveur : **Cisco0123**
- Mot de passe commun : **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: ●●●●●●●●●

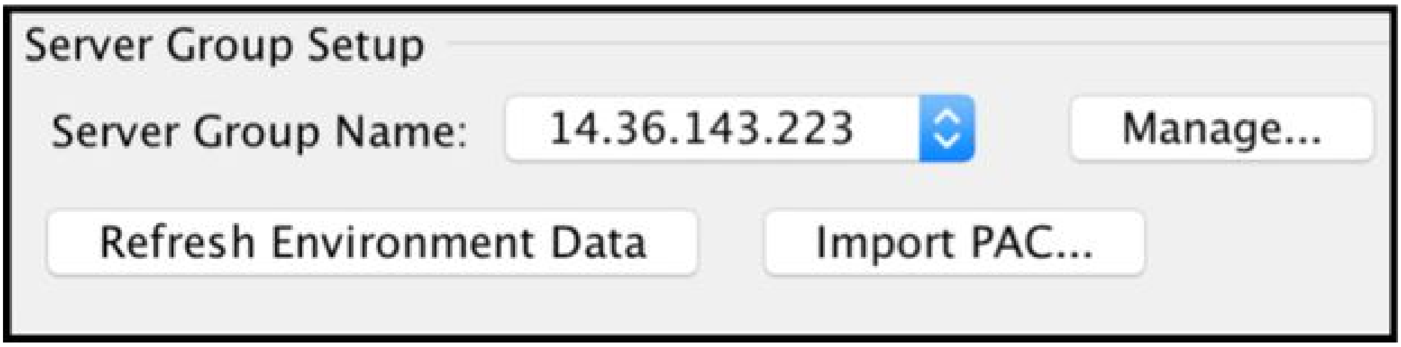
Common Password: ●●●●●●●●●

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☑

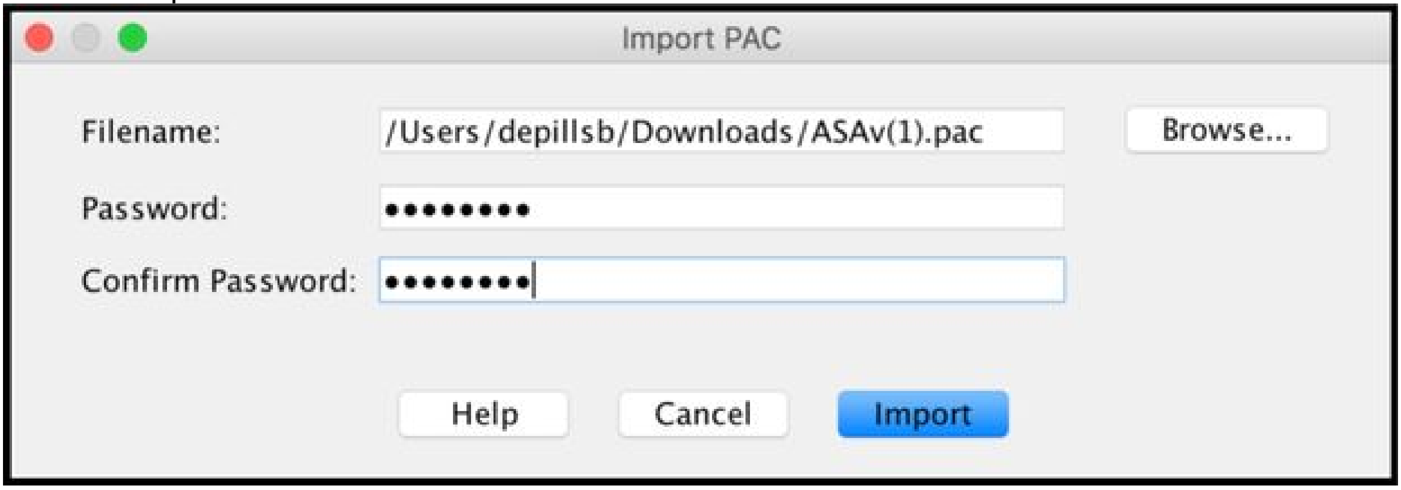
Importer un PAC téléchargé à partir de ISE

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


Server Group Setup

Server Group Name: 14.36.143.223

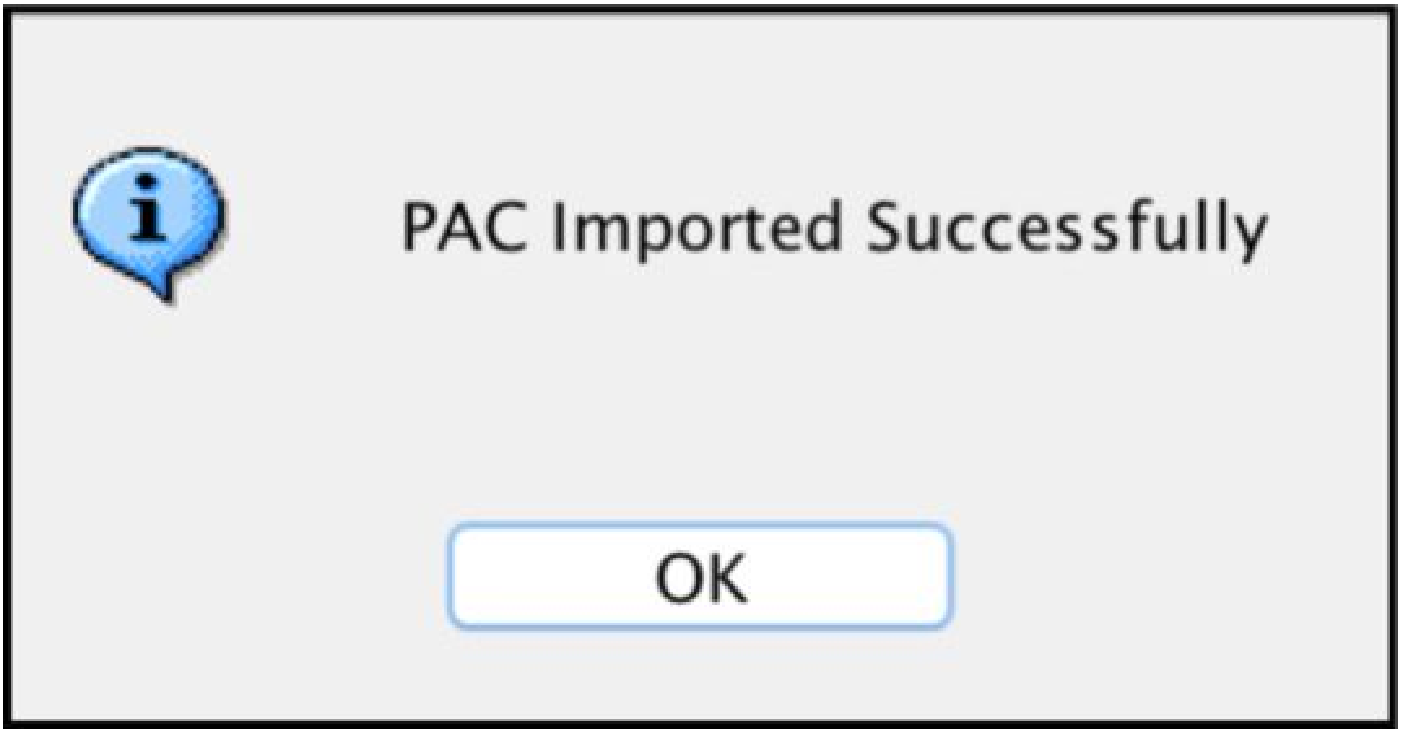
- Mot de passe : **Cisco0123**



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

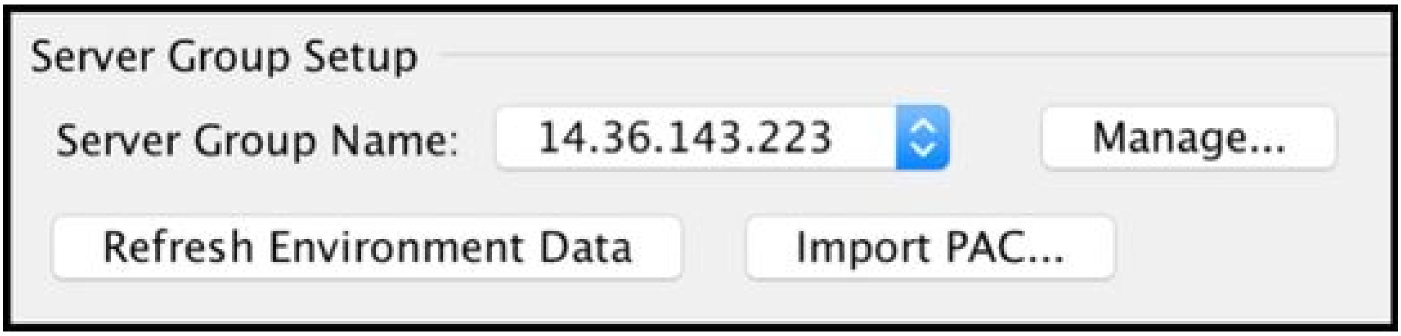
Password: •••••••••

Confirm Password: •••••••••


PAC Imported Successfully

Actualiser les données de l'environnement

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



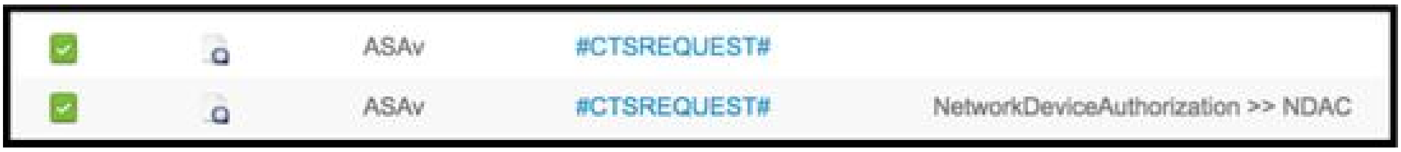
Server Group Setup

Server Group Name: 14.36.143.223

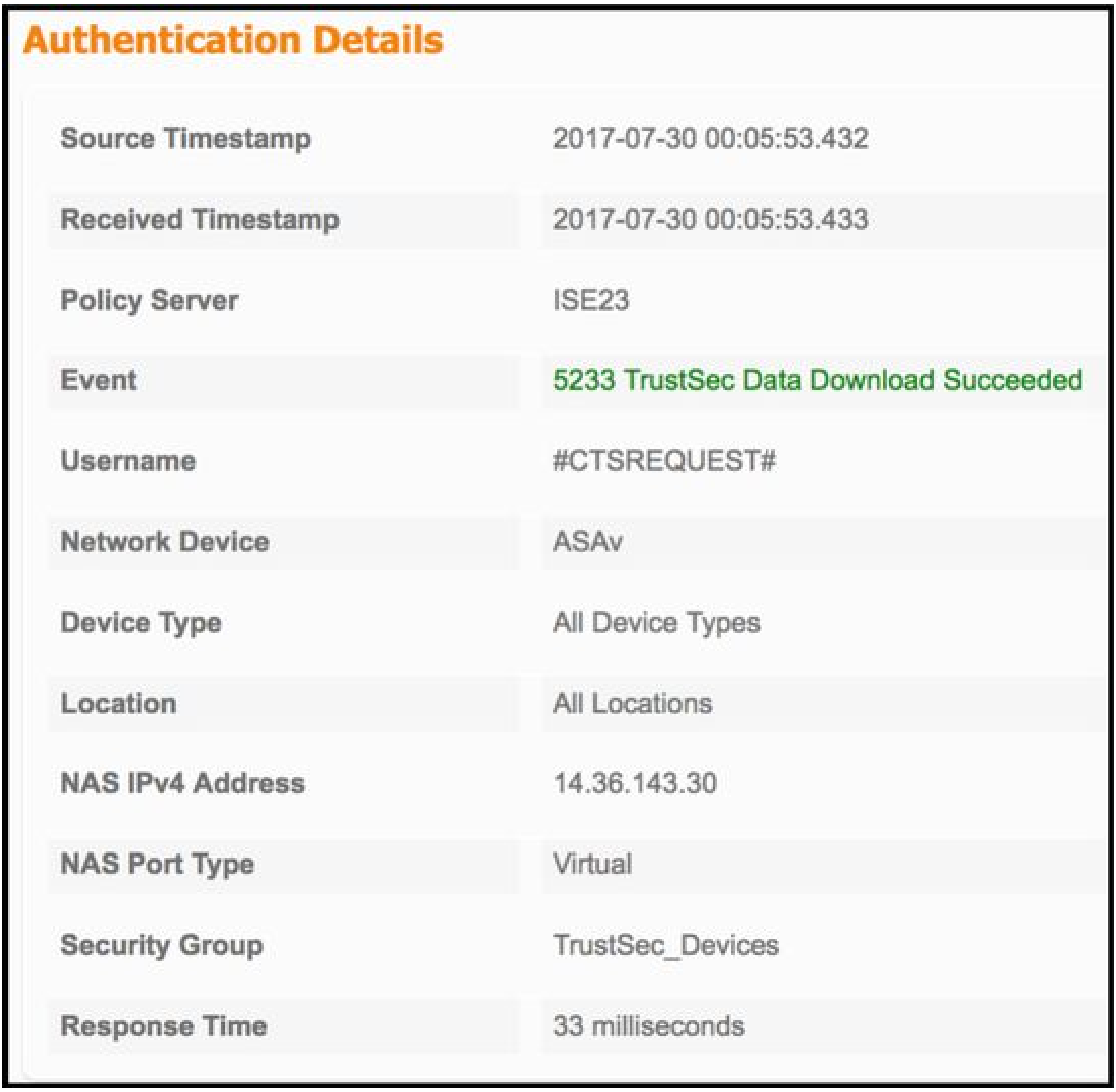
Vérification

Journaux en direct ISE

Opérations > RADIUS > **Journaux en direct**

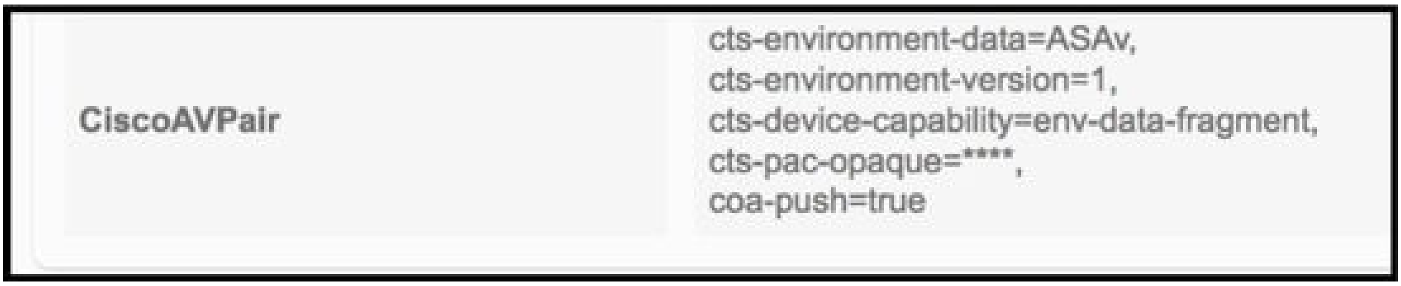


✓	🔍	ASAv	#CTSREQUEST#	
✓	🔍	ASAv	#CTSREQUEST#	NetworkDeviceAuthorization >> NDAC

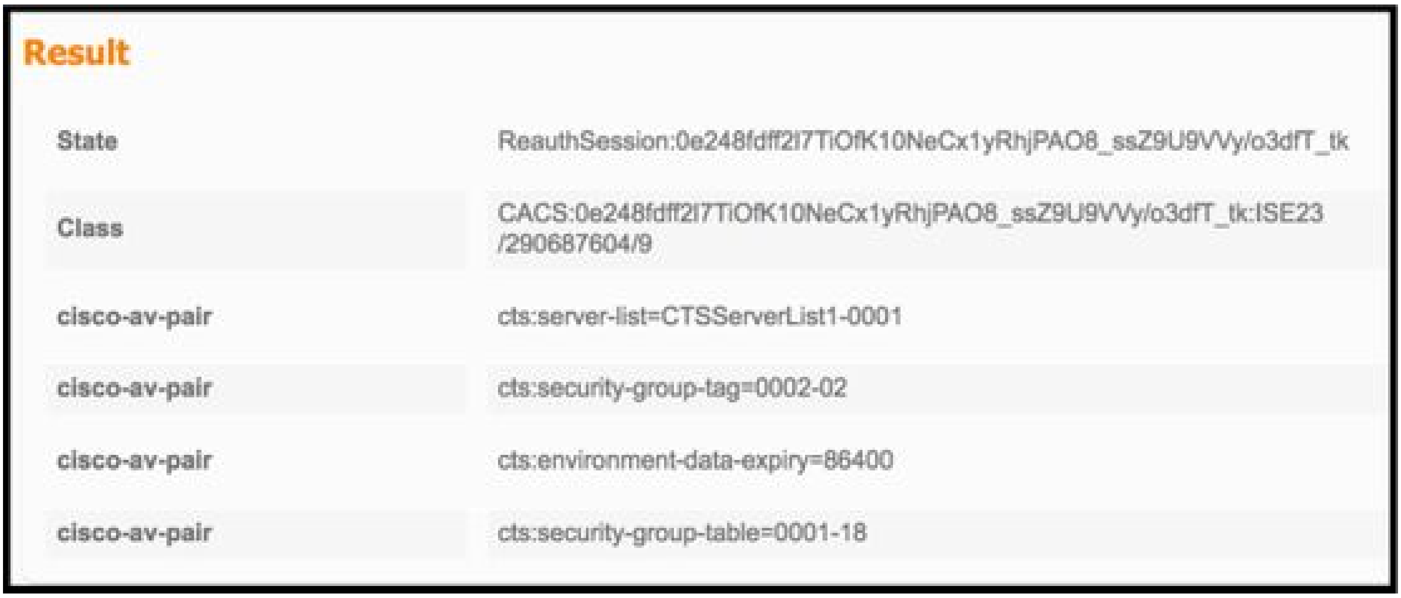


Authentication Details

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

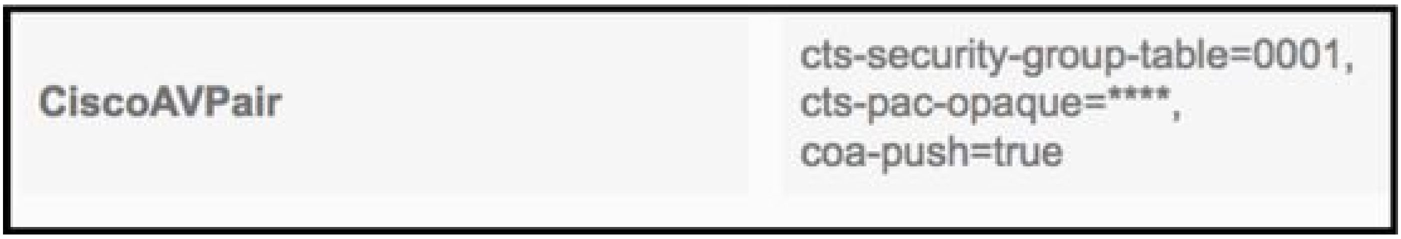


CiscoAVPair	cts-environment-data=ASAv,
	cts-environment-version=1,
	cts-device-capability=env-data-fragment,
	cts-pac-opaque=****,
	coa-push=true

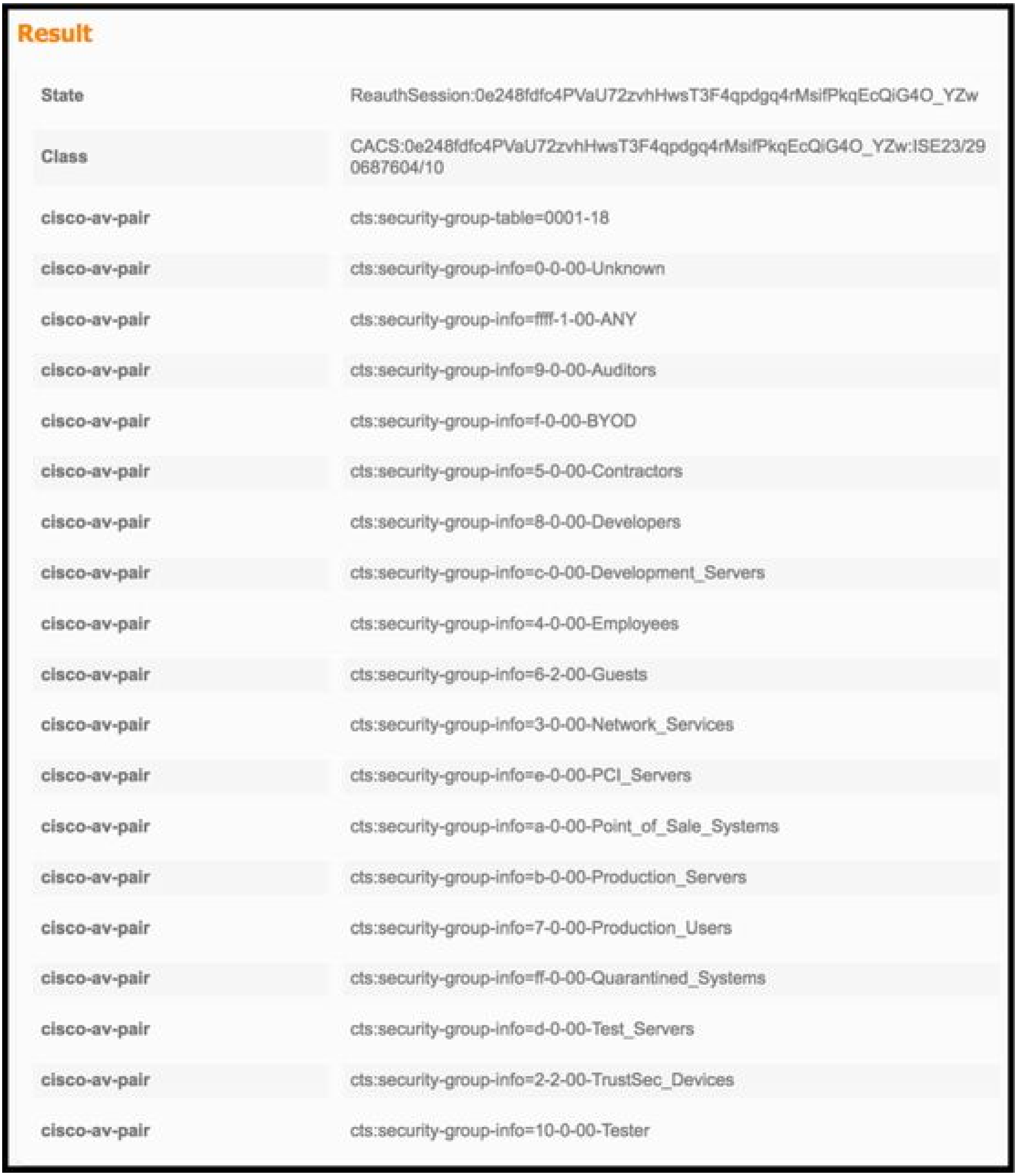


Result

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

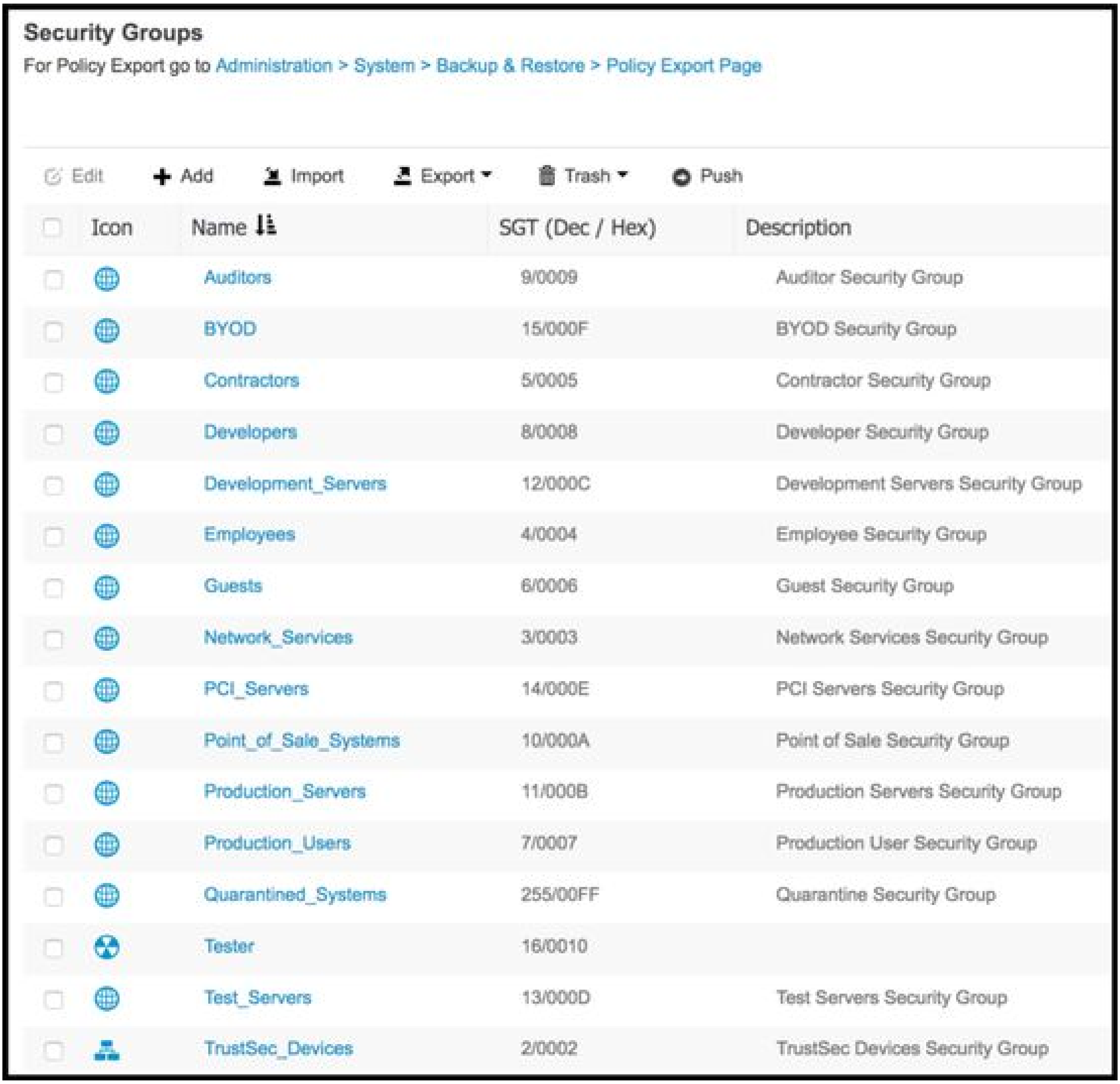


Result

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

Groupes de sécurité ISE

Centres de travail > TrustSec > Composants > **Groupes de sécurité**



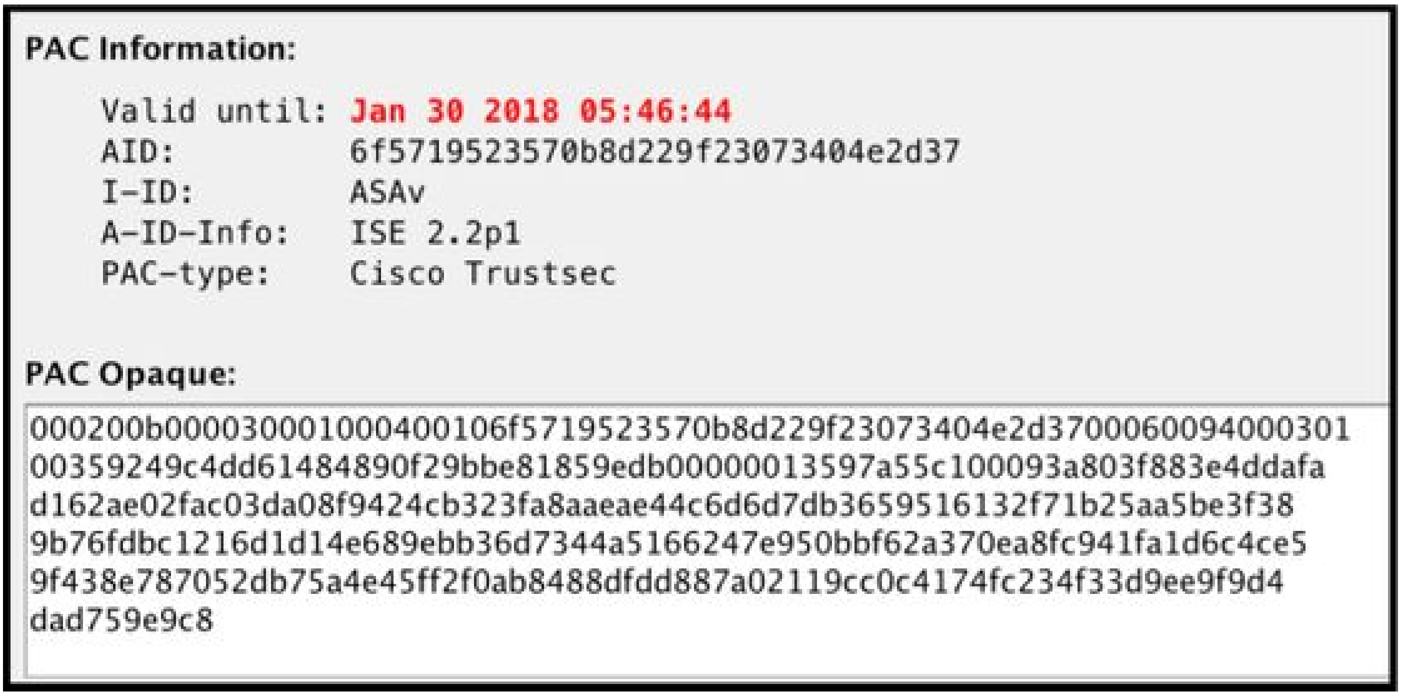
Security Groups

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

PAC ASDM

Surveillance > Propriétés > Identité par TrustSec > **PAC**



PAC Information:

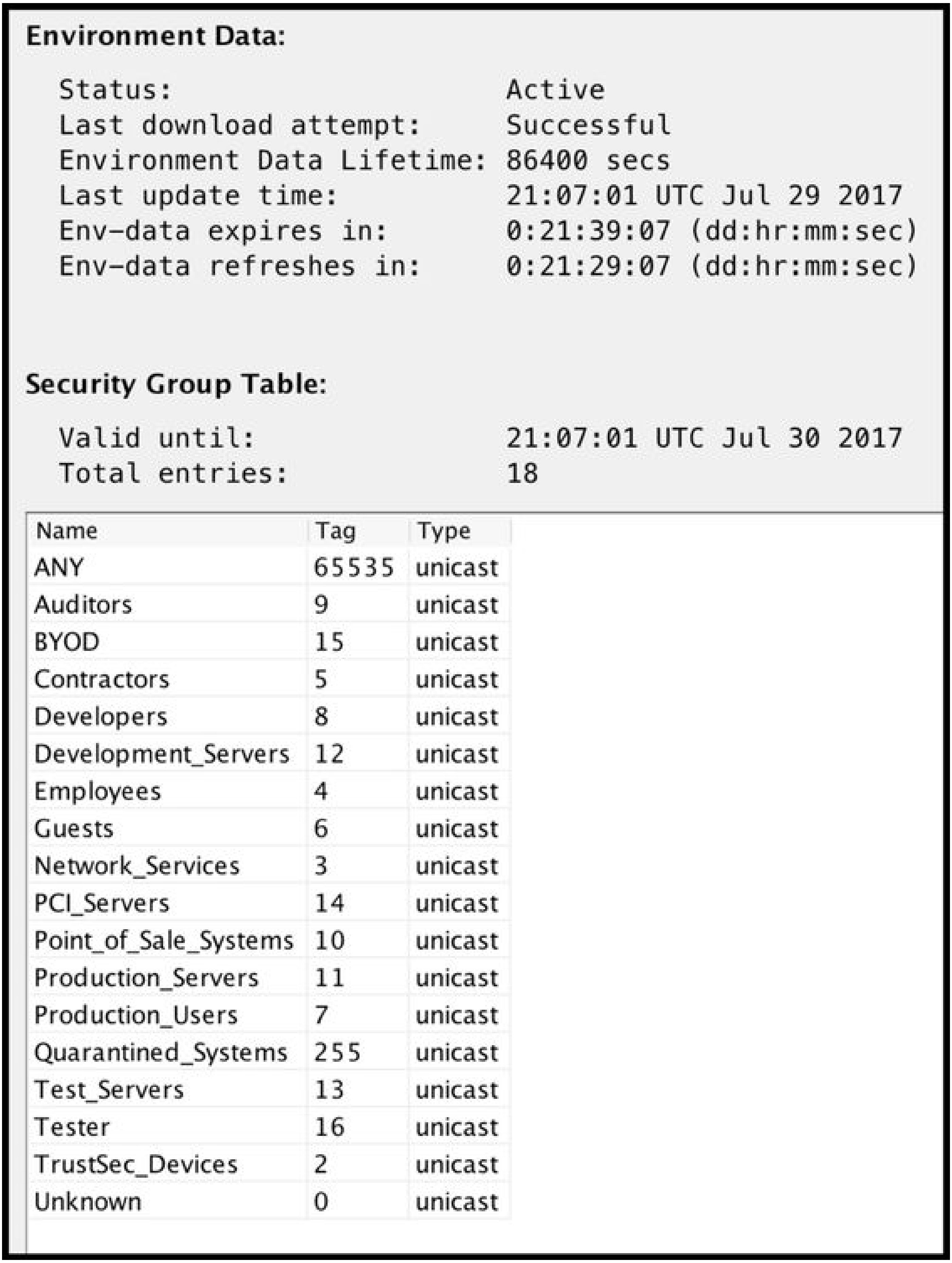
```
    Valid until: Jan 30 2018 05:46:44
    AID:         6f5719523570b8d229f23073404e2d37
    I-ID:        ASAv
    A-ID-Info:   ISE 2.2p1
    PAC-type:    Cisco Trustsec
```

PAC Opaque:

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

Groupes de données et de sécurité de l'environnement ASDM

Surveillance > Propriétés > Identité par TrustSec > **Données d'environnement**



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:

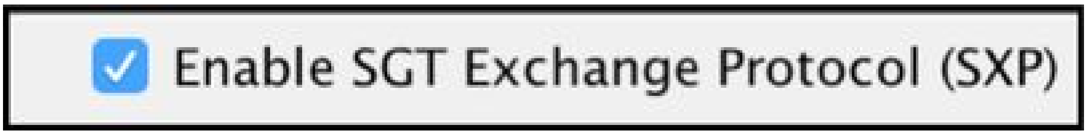
```
  Valid until:                   21:07:01 UTC Jul 30 2017
  Total entries:                 18
```

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

Configuration ASDM SXP

Activer SXP

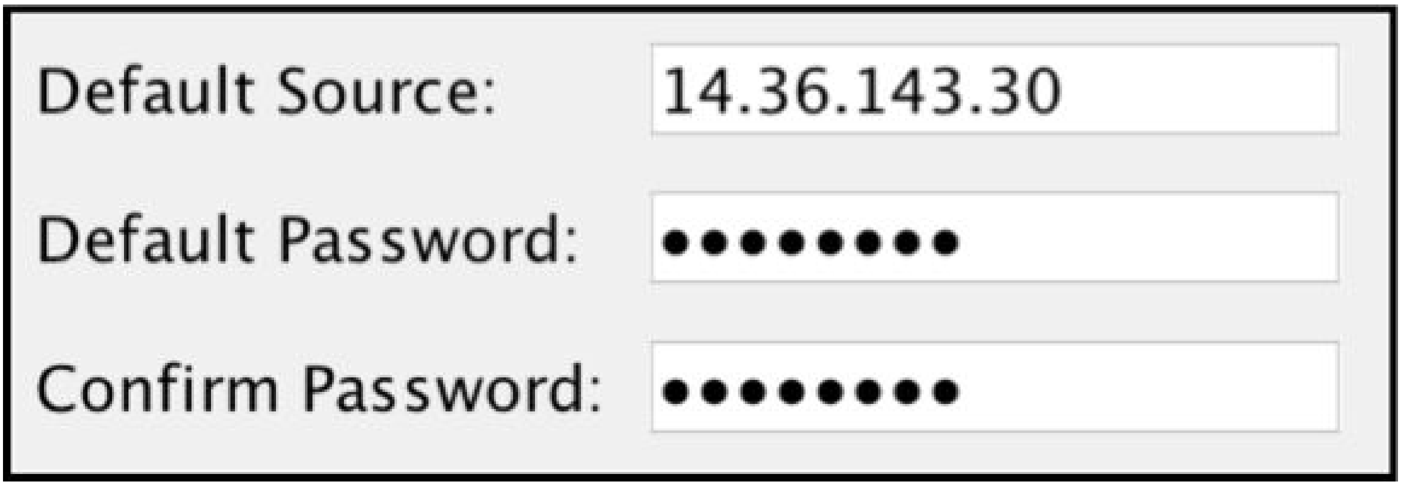
Configuration > Firewall > Identity by TrustSec > **Enable SGT Exchange Protocol (SXP)**



☑ Enable SGT Exchange Protocol (SXP)

Définir l'adresse IP source SXP par défaut et le mot de passe SXP par défaut

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



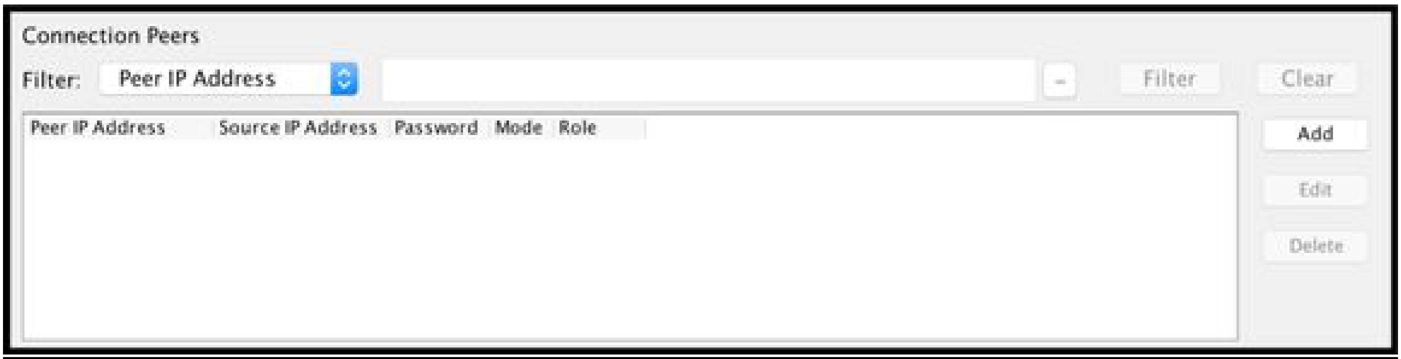
Default Source: 14.36.143.30

Default Password: •••••••••

Confirm Password: •••••••••

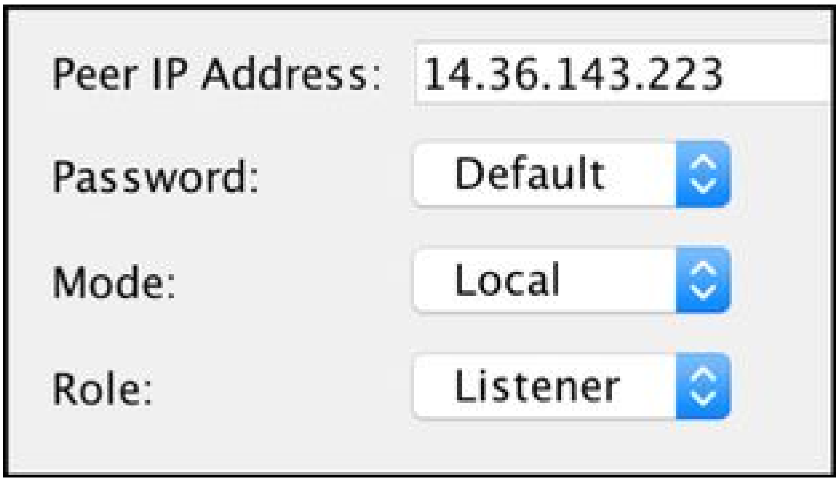
Ajouter un homologue SXP

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



Peer IP Address	Source IP Address	Password	Mode	Role

- Adresse IP de l'homologue : **<Adresse IP ISE>**



Peer IP Address: 14.36.143.223

Password: Default

Mode: Local

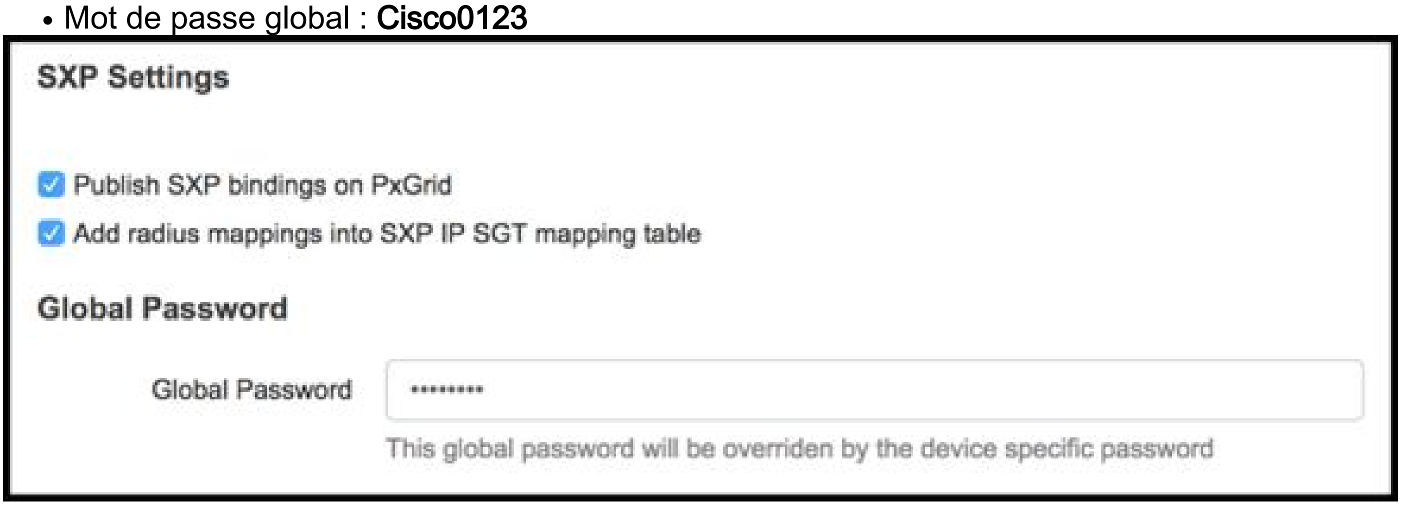
Role: Listener

Configuration ISE SXP

Paramètre de mot de passe SXP global

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

- Mot de passe global : **Cisco0123**



SXP Settings

☑ Publish SXP bindings on PxGrid

☑ Add radius mappings into SXP IP SGT mapping table

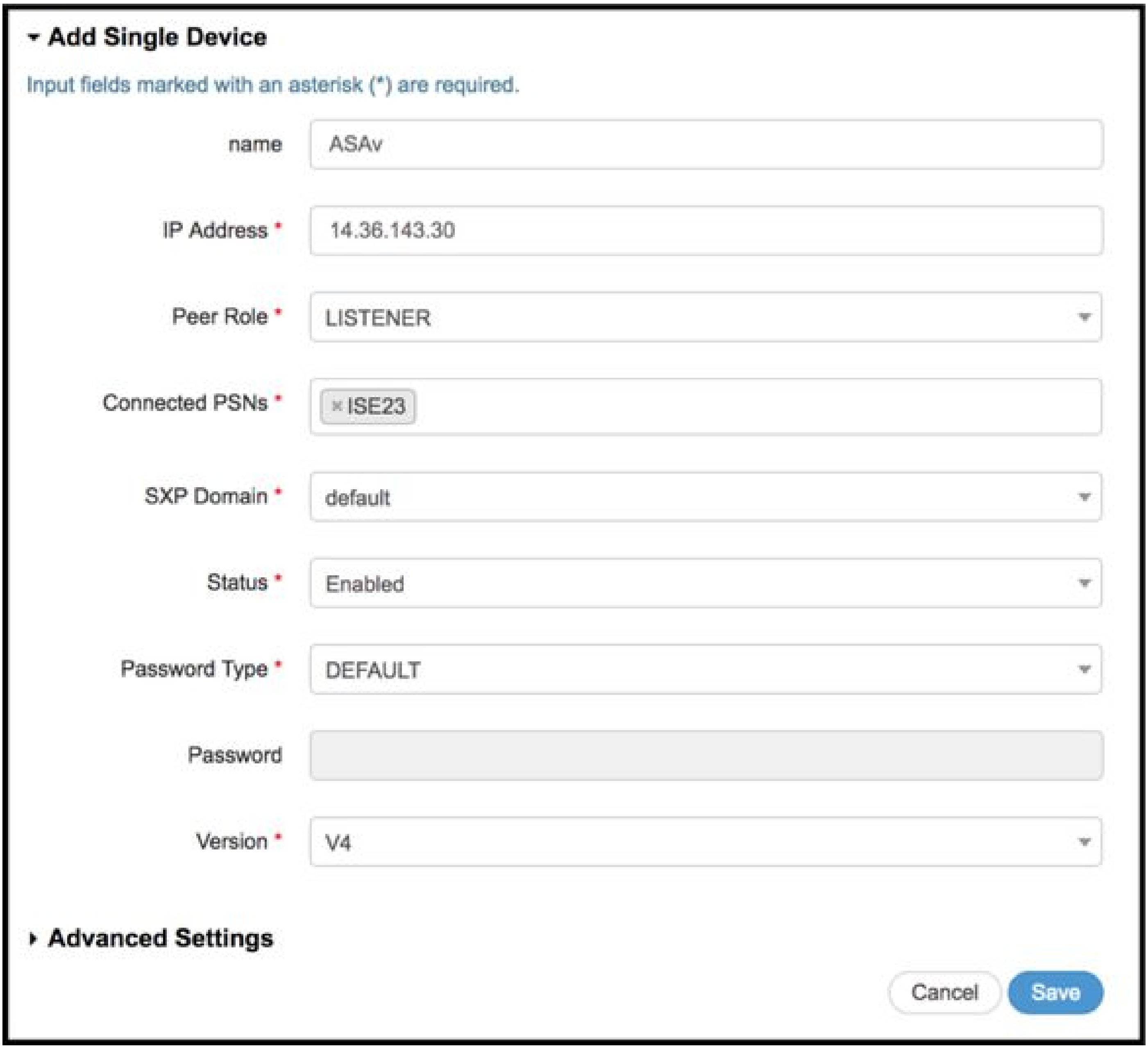
Global Password

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

This global password will be overriden by the device specific password

Ajouter un périphérique SXP

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



▾ **Add Single Device**

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

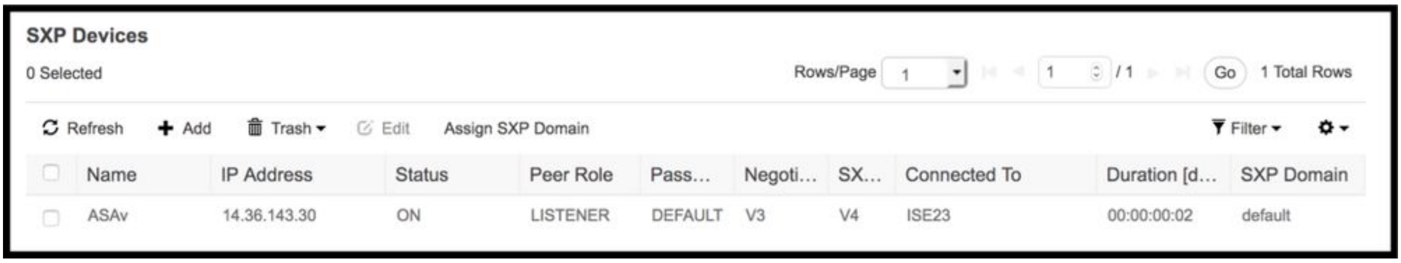
name	ASAv
IP Address *	14.36.143.30
Peer Role *	LISTENER
Connected PSNs *	× ISE23
SXP Domain *	default
Status *	Enabled
Password Type *	DEFAULT
Password	
Version *	V4

▸ **Advanced Settings**

Vérification SXP

Vérification ISE SXP

WorkCenters > TrustSec > SXP > **Périphériques SXP**



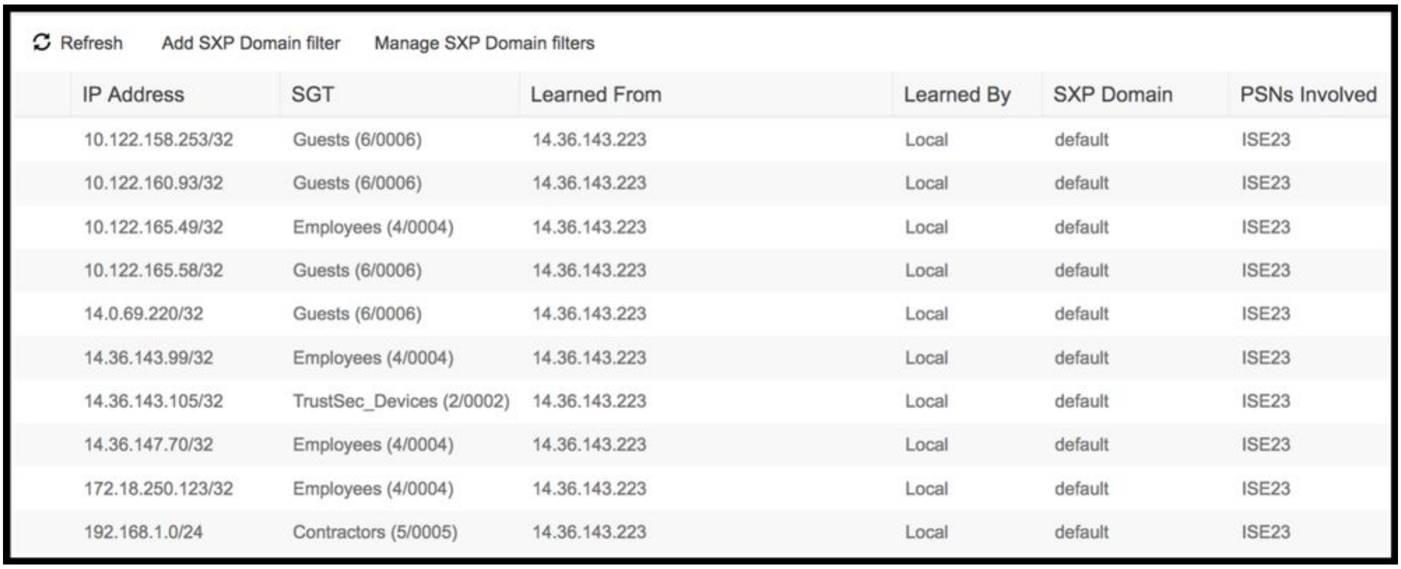
SXP Devices

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

Mappages ISE SXP

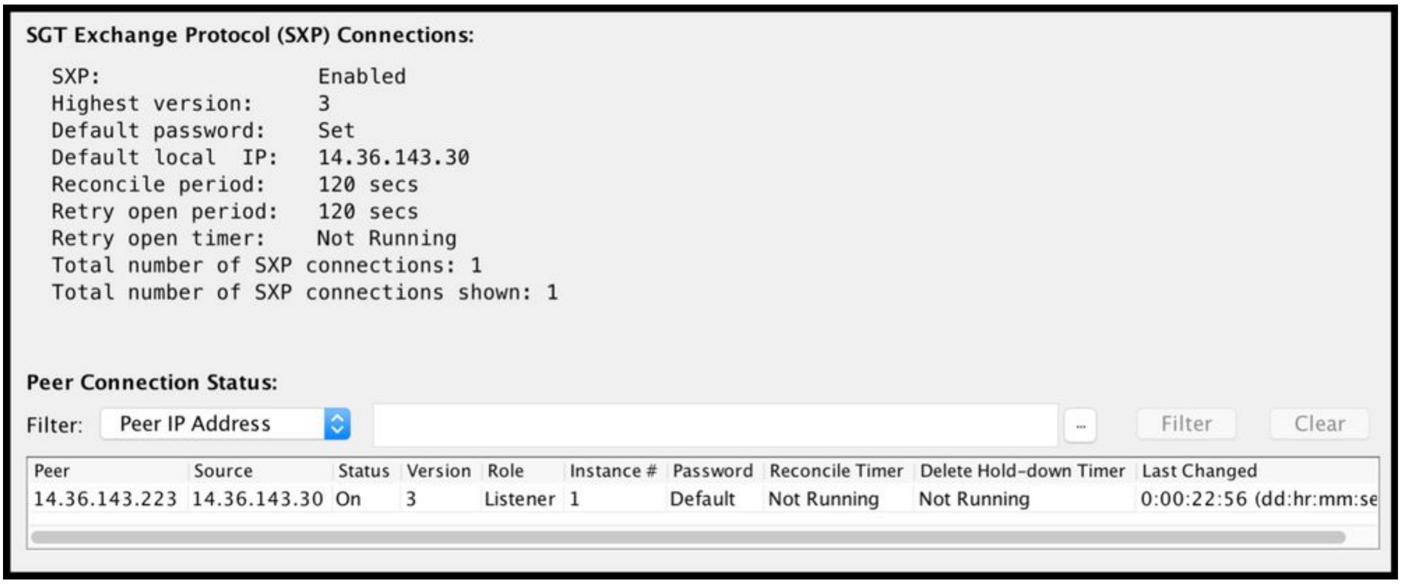
WorkCenters > TrustSec > SXP > **Tous les mappages SXP**



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

Vérification ASDM SXP

Surveillance > Propriétés > Identité par TrustSec > **Connexions 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
```

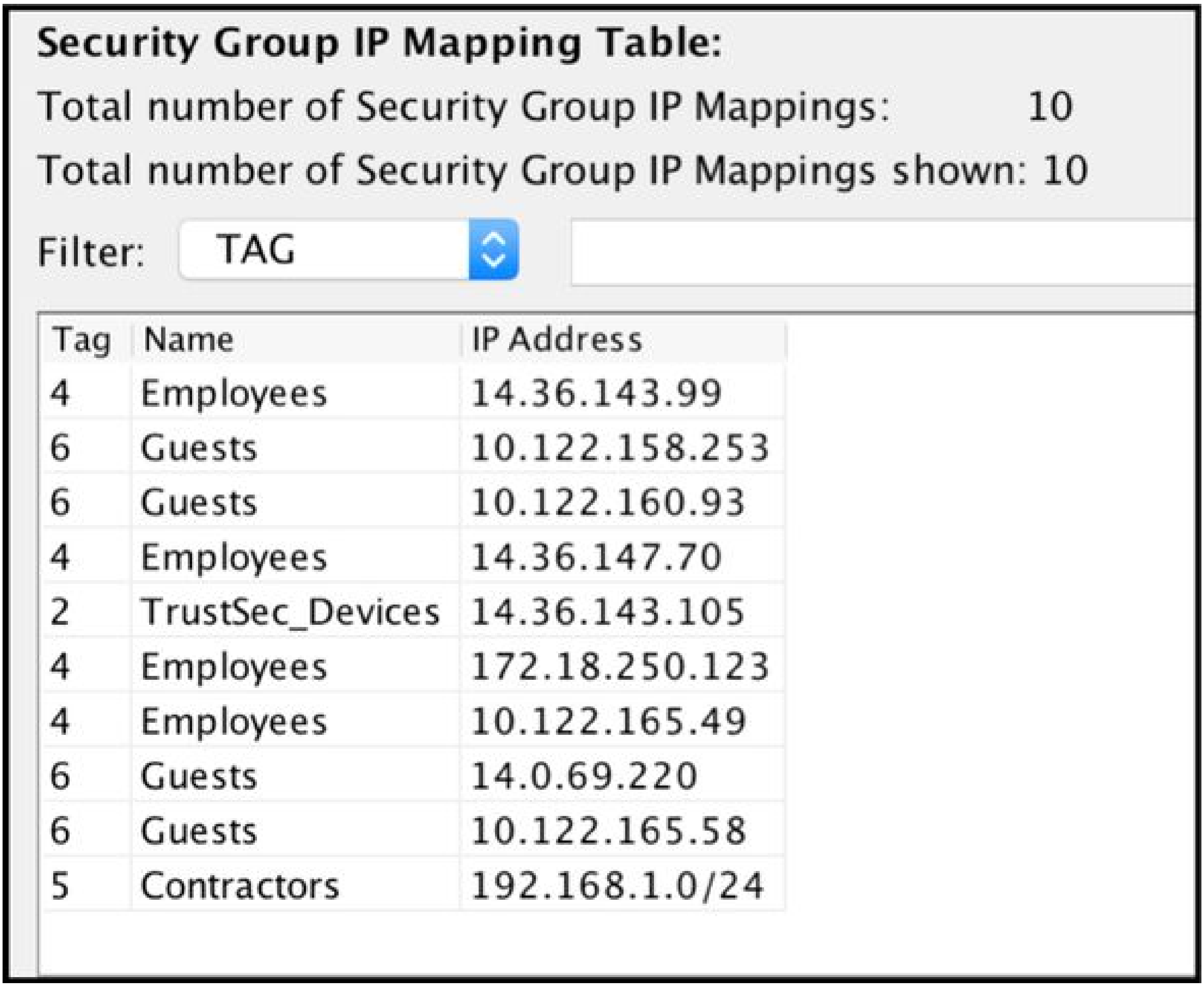
Peer Connection Status:

Filter: Peer IP Address

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 a appris les mappages IP SXP vers SGT

Surveillance > Propriétés > Identité par TrustSec > **Mappages IP**



Security Group IP Mapping Table:

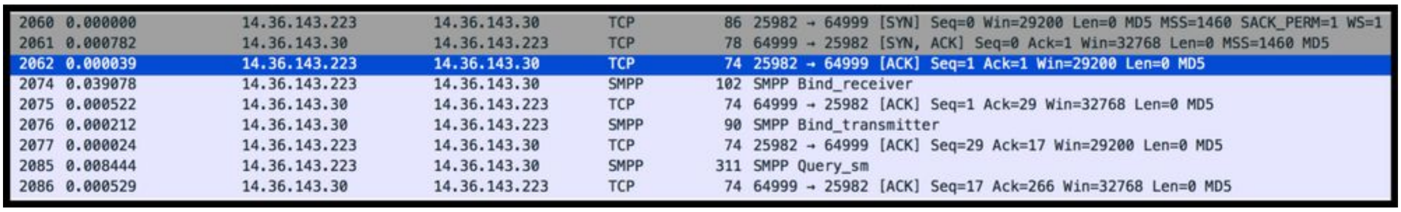
Total number of Security Group IP Mappings: 10

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

Capture de paquets sur 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
```