配置TrustSec NDAC种子和非种子设备

目录

简介
先决条件
使用的组件
网络图
IP 地址
ISE配置
添加网络设备
6500（种子）
3560X（非种子）
TrustSec安全组
网络设备授权策略
种子设备配置(6500)
确认
ISE实时日志
PAC调配
TrustSec数据下载
非种子设备配置(3560X)
确认
ISE实时日志
PAC调配
非种子身份验证
相互对等策略下载
TrustSec数据下载
接口验证

简介

本文档介绍在ISE（身份服务引擎）中使用trustsec时如何配置种子和非种子设备。

Trustsec使用NDAC（网络设备准入控制）对新设备进行身份验证，然后允许其加入trustsec域。这可以防止未授权设备参与信任sec信息交换。种子设备/身份验证器（在本例中为6500交换机）需要手动配置并使用RADIUS over IP连接到ISE。非种子设备/请求方（在本例中为3560X）没有与ISE的直接IP连接，需要种子设备注册并使用802.1X在网络上对其进行身份验证。一旦请求方（非种子设备）通过身份验证，ISE将调配PAC（受保护访问凭证）并下载服务器信息。PAC包含共享密钥和加密令牌，以在将来为ISE提供安全联系。

先决条件

ISE身份验证服务器

支持Trustsec的种子设备/身份验证器

支持Trustsec的非种子设备/请求方

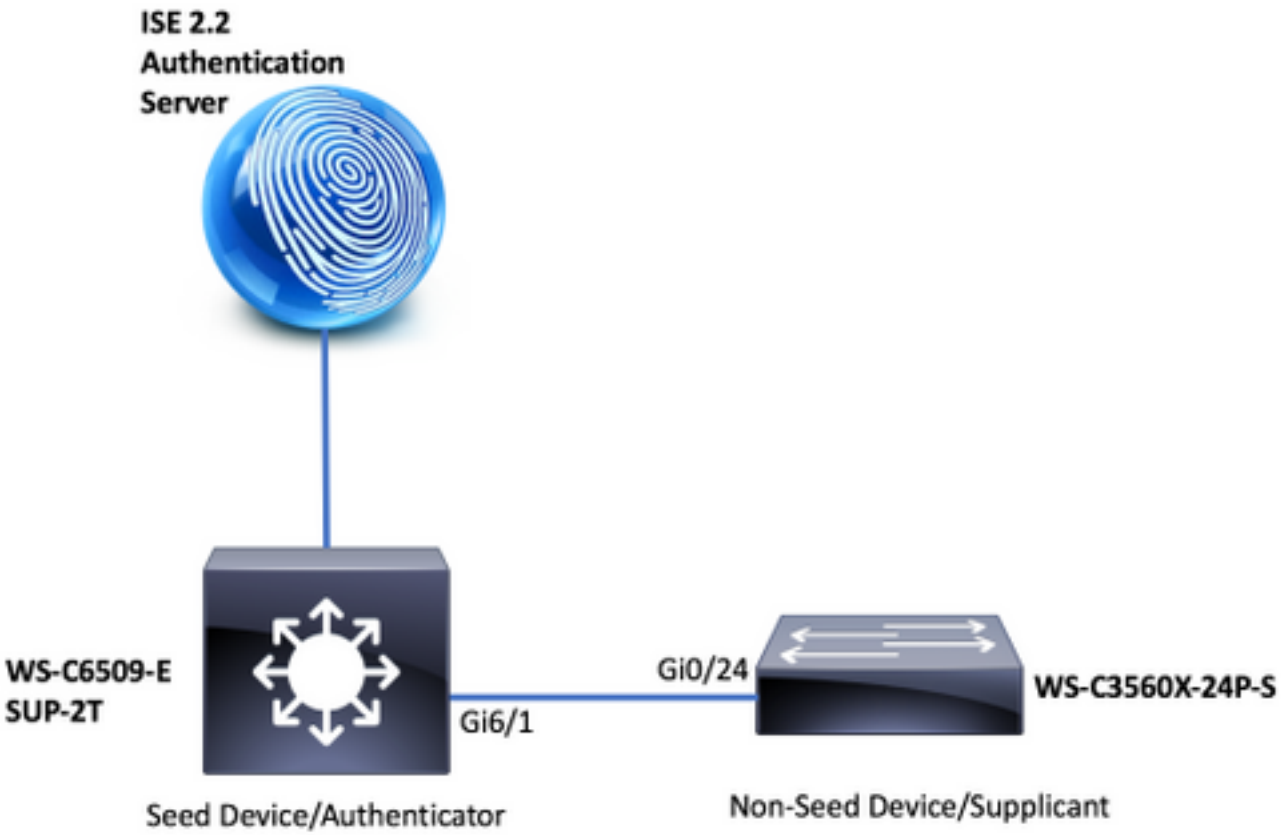
请参考最新的trustsec兼容性列表：

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

使用的组件

- ISE 2.2补丁2
- WS-C6509-E [VS-SUP2T-10G] s2t54-ipservicesk9-mz.SPA.152-1.SY3.bin
- WS-C3560X-24P-S c3560e-universalk9-mz.152-4.E4.bin

网络图



N

DAC拓扑

IP 地址

ISE:14.36.143.18

6509：10.122.165.35

3560X:10.122.160.118

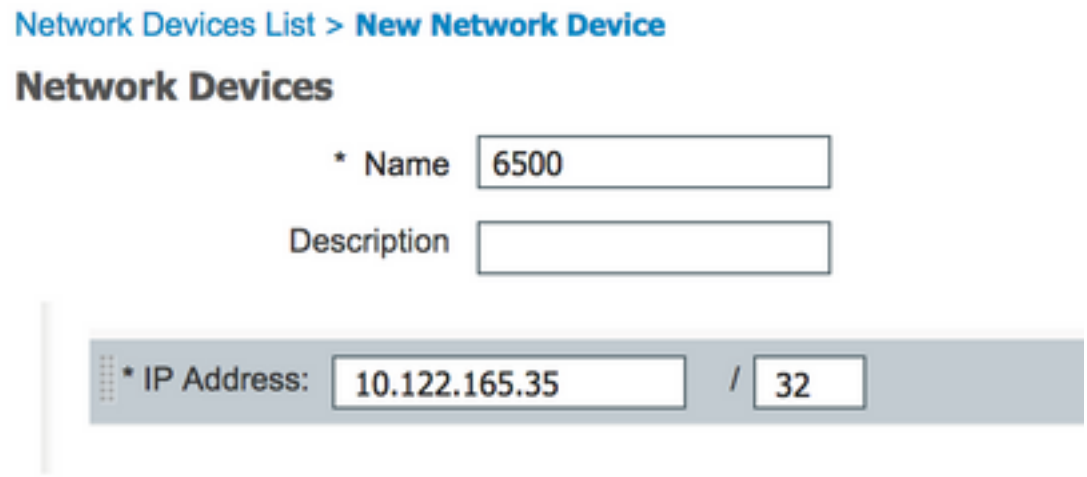
ISE配置

添加网络设备

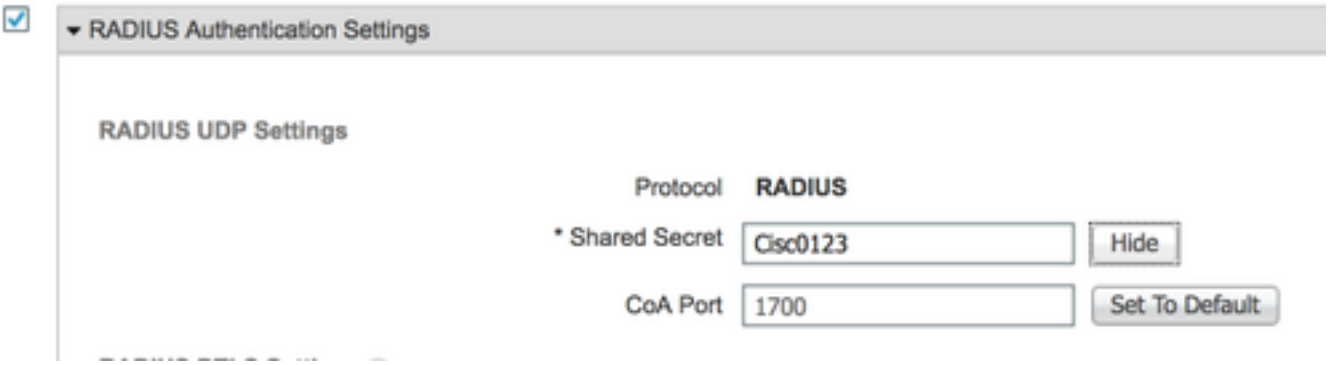
6500（种子）

WorkCenters > TrustSec > Components > Network Devices > Add

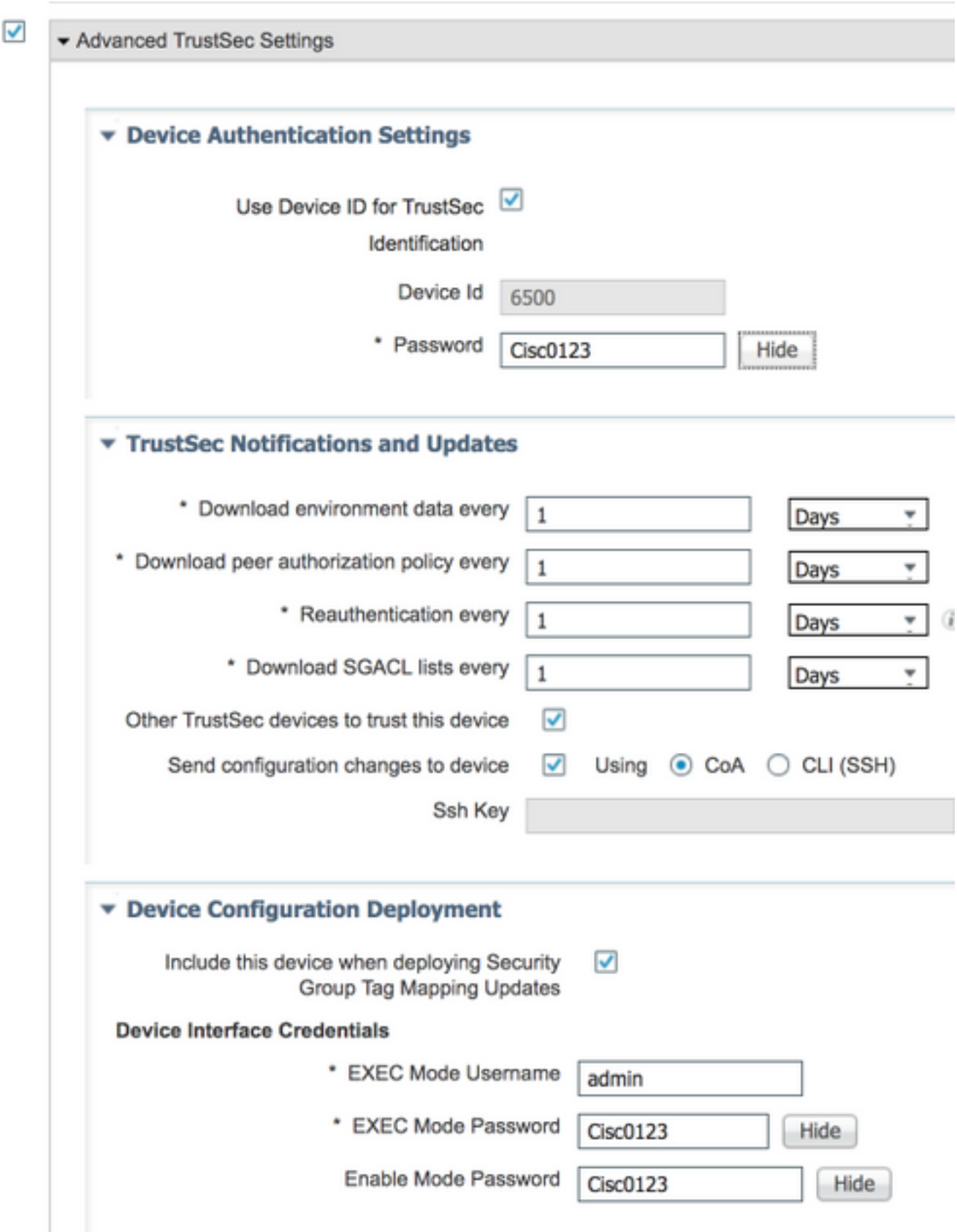
设备名称和IP地址



RADIUS共享密钥



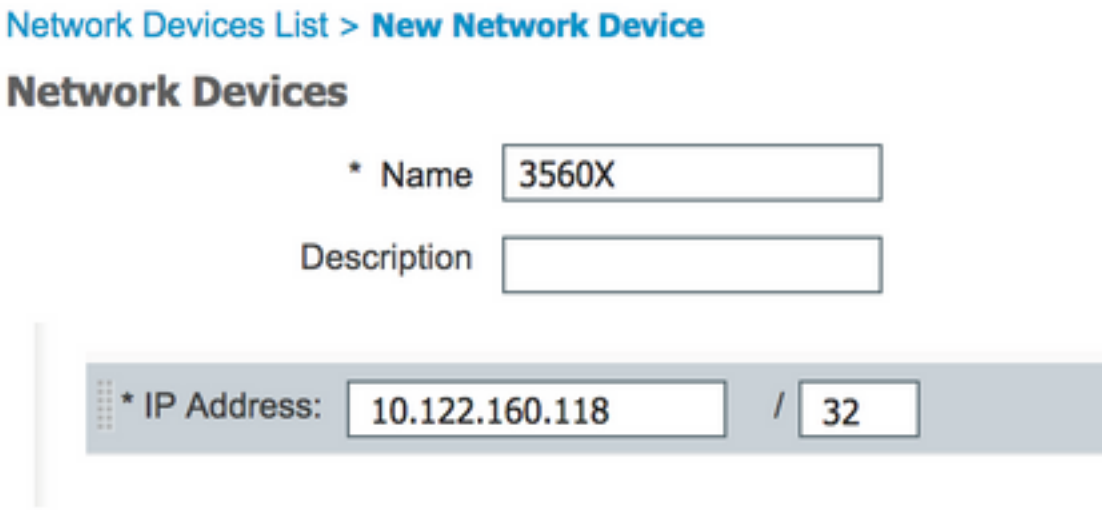
Trustsec凭证



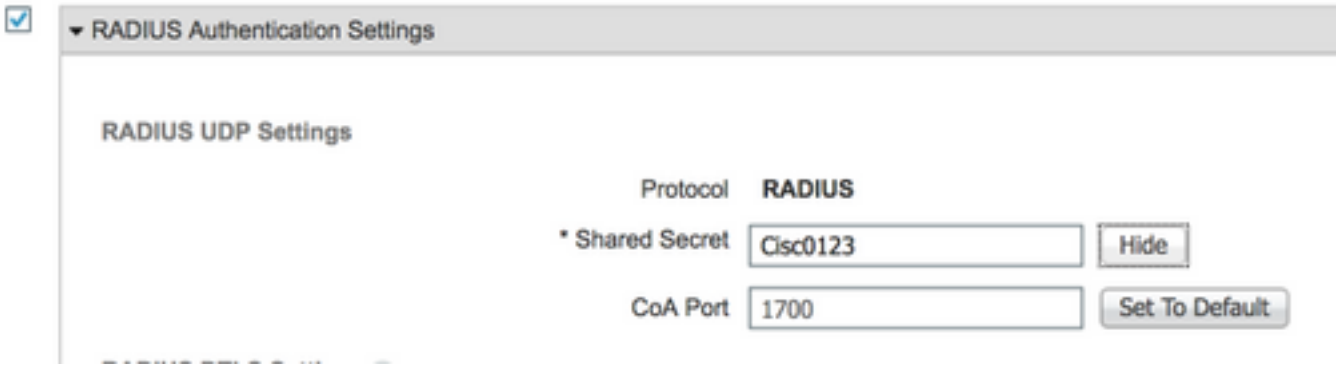
3560X（非种子）

WorkCenters > TrustSec > Components > Network Devices > Add

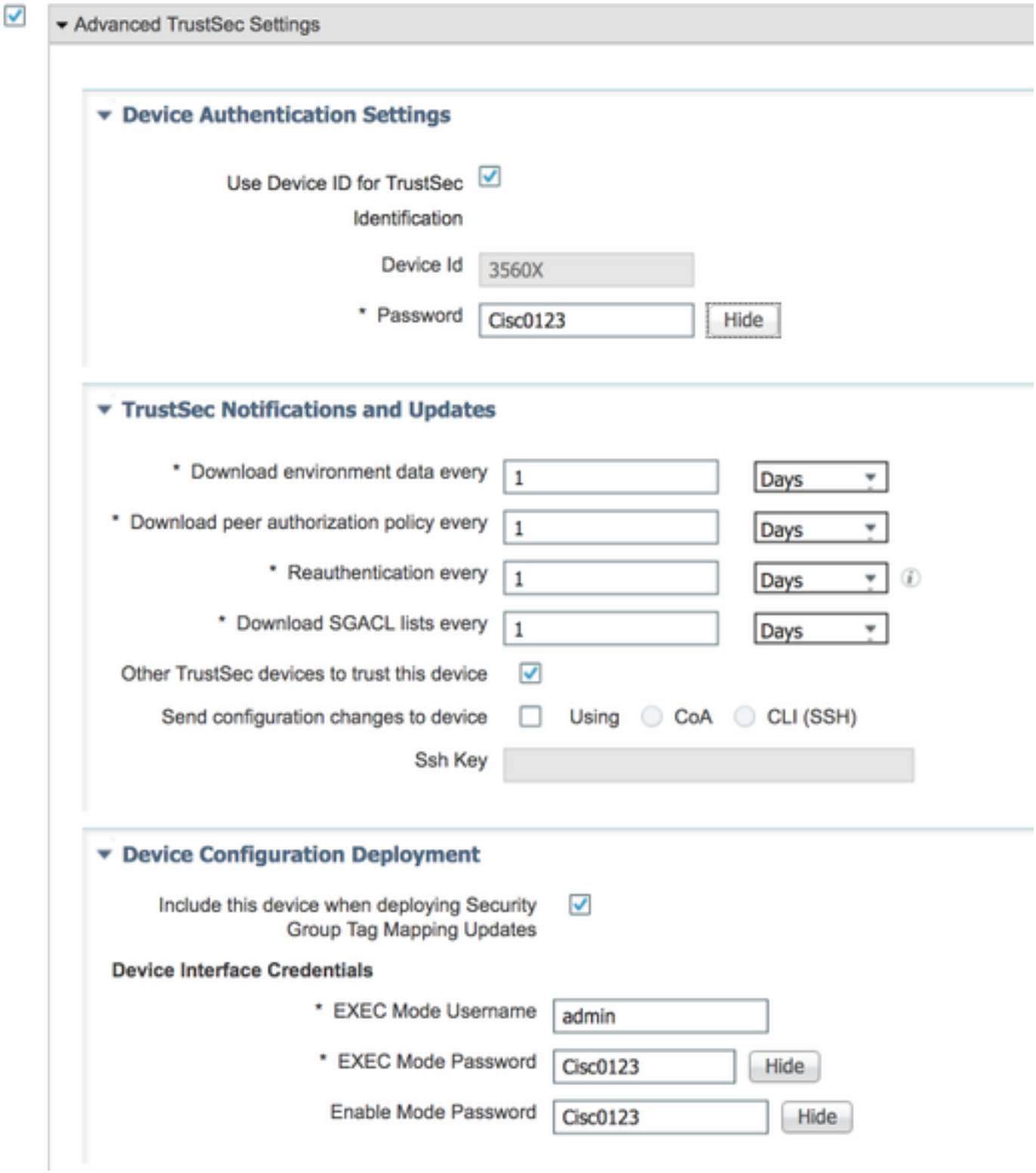
设备名称和IP地址



RADIUS共享密钥



Trustsec凭证



TrustSec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

Edit | Add | Import | Export | Delete | Push

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
	Test_Servers	13/000D	Test Servers Security Group
	TrustSec_Devices	2/0002	TrustSec Devices Security Group
	Unknown	0/0000	Unknown Security Group

网络设备授权策略

工作中心> TrustSec > TrustSec策略>网络设备授权

Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

	Rule Name	Conditions			Security Group
☑	NDAC	If	DEVICE:Device Type equals to Device Type#All Device Types	then	TrustSec_Devices
☑	Default Rule	If	no rules defined or no match	then	Unknown

种子设备配置(6500)

TrustSec Credentials

```
6500#cts credentials id 6500 password Cisc0123
```

AAA configuration

```
6500(config)#aaa new-model
6500(config)#aaa authentication dot1x default group radius
6500(config)#aaa accounting identity default start-stop group radius
6500(config)#aaa authorization network CTSlist group radius
6500(config)#cts authorization list CTSlist
```

Radius Server Configuration

```
6500(config)#radius server ISE
6500(config-radius-server)#address ipv4 14.36.143.18 auth-port 1812 acct-port 1813
6500(config-radius-server)#pac key Cisc0123
```

Recognize and use vendor-specific attributes

```
6500(config)#radius-server vsa send authentication
```

Enable Change of Authorization

```
6500(config)#aaa server radius dynamic-author
6500(config-locsvr-da-radius)#client 14.36.143.18 server-key Cisc0123
```

Enable 802.1X

```
6500(config)#dot1x system-auth-control
```

Switchport TrustSec Configuration

```
6500(config)#int gi6/1
6500(config-if)#switchport mode trunk
6500(config-if)#cts dot1x
6500(config-if-cts-dot1x)#sap mode-list null
6500(config-if-cts-dot1x)#propagate sgt
```

确认

PAC Download

```
6500#show cts pac
 AID: 6F5719523570B8D229F23073404E2D37
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: 6F5719523570B8D229F23073404E2D37
   I-ID: 6500
   A-ID-Info: ISE 2.2p1
   Credential Lifetime: 04:27:29 UTC Oct 26 2017
 PAC-Opaque:
000200B000030001000400106F5719523570B8D229F23073404E2D3700060094000301008010 62F6BE70E2CCB6B0D25B
FC81CB5D00000013597A55C100093A8059F0E1A3FAF83A2B7C8332479B7324C0FDC4CBAE9AE4AFD19C614A7DB13C9DBD
06798A344423897745F0F91F19489772E543ED205A9CD0F276A96C4505BF34CB75F132377FE770B77A3D822842DFE3A0
A858130612D08DD58965B09C352E33E74DB3F6B5C7E1F6EC8C30FF215A6FEB3EA7BBC95E
 Refresh timer is set for 12w5d
```

Environment Data

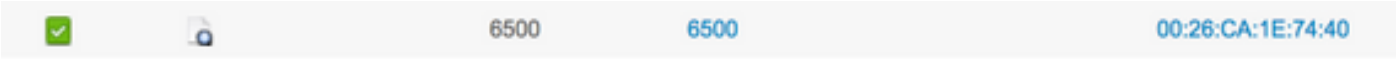
```
6500#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 14.36.143.18, port 1812, A-ID 6F5719523570B8D229F23073404E2D37
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
   0-fb:Unknown
   2-fb:TrustSec_Devices
   3-fb:Network_Services
   4-fb:Employees
   5-fb:Contractors
   6-fb:Guests
   7-fb:Production_Users
```

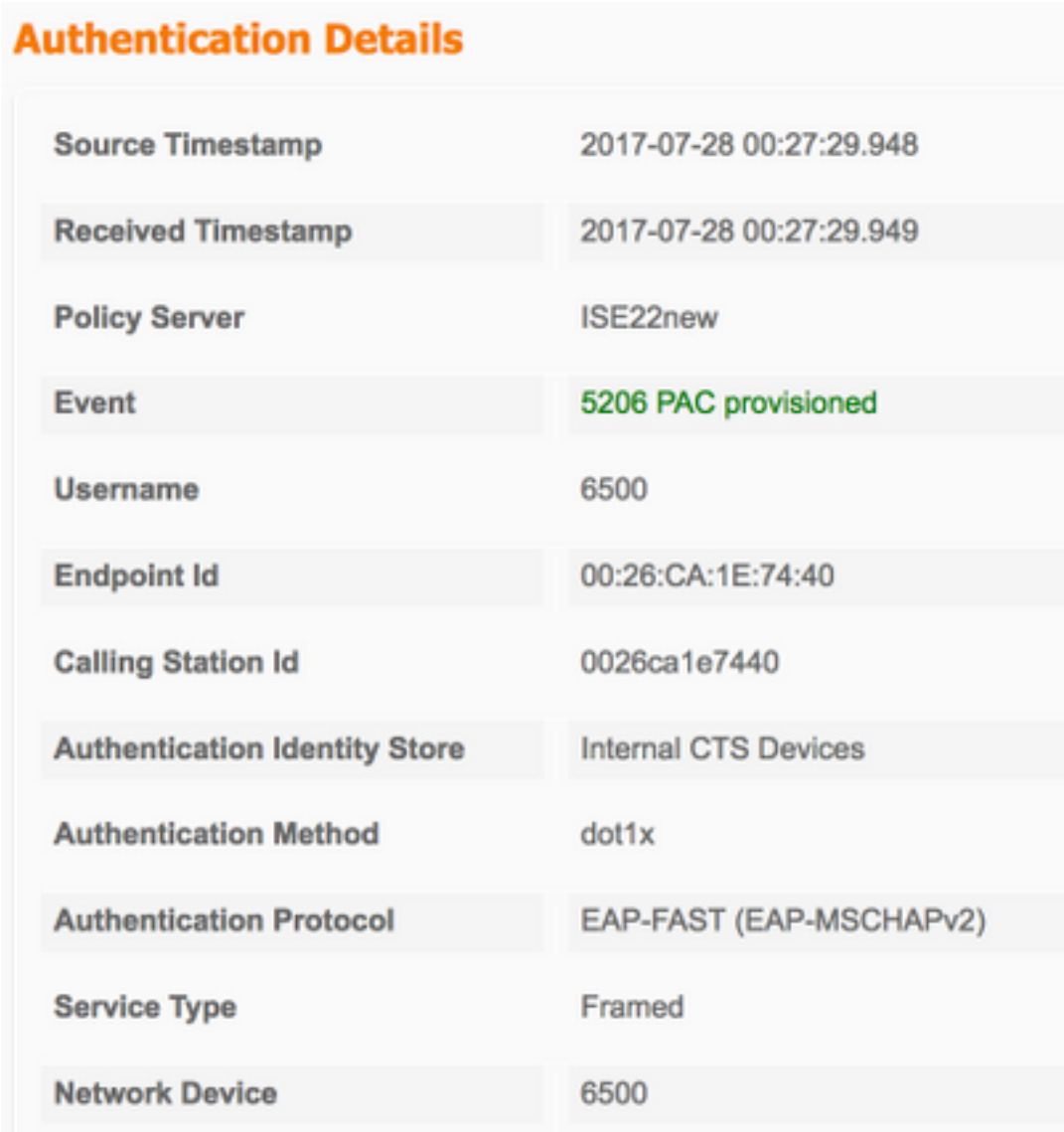
```
   8-fb:Developers
   9-fb:Auditors
   10-fb:Point_of_Sale_Systems
   11-fb:Production_Servers
   12-fb:Development_Servers
   13-fb:Test_Servers
   14-fb:PCI_Servers
   15-fb:BYOD
   255-fb:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 20:28:36 UTC Thu Jul 27 2017
Env-data expires in   0:23:47:05 (dd:hr:mm:sec)
Env-data refreshes in 0:23:47:05 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

ISE实时日志

操作> RADIUS >实时日志

PAC调配





CiscoAVPair	AAA:service-type=cts-pac-provisioning

TrustSec数据下载

☑		6500	#CTSREQUEST#		
☑		6500	#CTSREQUEST#		
☑		6500	#CTSREQUEST#		NetworkDeviceAuthorization >> NDAC

Authentication Details

Source Timestamp	2017-07-28 00:28:00.73
Received Timestamp	2017-07-28 00:28:00.731
Policy Server	ISE22new
Event	5233 TrustSec Data Download Succeeded
Username	#CTSREQUEST#
Service Type	Outbound
Network Device	6500
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.122.165.35
Security Group	TrustSec_Devices
Response Time	26 milliseconds

Other Attributes

ConfigVersionId	81
DestinationPort	1812
Protocol	Radius
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ISE22new/290042933/391
AuthorizationPolicyMatchedRule	NDAC
CPMSessionID	0e248f12uRp7Oyjg47Xw5P1a3ocsnKLGOWxUEIAEeOP9HaC6aEs
ISEPolicySetName	NetworkDeviceAuthorization
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	#CTSREQUEST#
Device IP Address	10.122.165.35
CiscoAVPair	cts-pac-opaque=****, cts-environment-data=6500, cts-device-capability=env-data-fragment

Result

State	ReauthSession:0e248f12uRp7Oyjg47Xw5P1a3ocsnKLGOWxUEIAEeOP9HaC6aEs
Class	CACS:0e248f12uRp7Oyjg47Xw5P1a3ocsnKLGOWxUEIAEeOP9HaC6aEs:ISE22new/290042933/391
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=0001-17

Result

Class	CACS:0e248f12uRp7Oyjg47Xw5P1a3ocsnKLGOWxUElAEeOP9HaC6aEs:ISE22new/290042933/392
cisco-av-pair	cts:server-list=CTSServerList1-0001
cisco-av-pair	cts:server=6f5719523570b8d229f23073404e2d37:14.36.143.18:1812

Result

Class	CACS:0e248f12uRp7Oyjg47Xw5P1a3ocsnKLGOWxUElAEeOP9HaC6aEs:ISE22new/290042933/393
cisco-av-pair	cts:security-group-table=0001-17
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

非种子设备配置(3560X)

TrustSec Credentials

```
3560X#cts credentials id 3560X password Cisc0123
```

AAA configuration

```
3560X(config)#aaa new-model
3560X(config)#aaa authentication dot1x default group radius
3560X(config)#aaa authorization network default group radius
3560X(config)#aaa accounting identity default start-stop group radius
```

Recognize and use vendor-specific attributes

```
3560X(config)#radius-server vsa send authentication
```

Enable Change of Authorization

```
3560X(config)#aaa server radius dynamic-author
3560X(config-locsvr-da-radius)#client 14.36.143.18 server-key Cisc0123
```

Enable 802.1X

```
3560X(config)#dot1x system-auth-control
```

Switchport TrustSec Configuration

```
3560X(config)#int gi0/24
3560X(config-if)#switchport trunk encapsulation dot1q
3560X(config-if)#switchport mode trunk
3560X(config-if)#cts dot1x
3560X(config-if-cts-dot1x)#sap mode-list null
3560X(config-if-cts-dot1x)#propagate sgt
```

确认

Pac Download

```
3560X#show cts pac
 AID: 6F5719523570B8D229F23073404E2D37
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: 6F5719523570B8D229F23073404E2D37
   I-ID: 3560X
   A-ID-Info: ISE 2.2p1
   Credential Lifetime: 05:32:57 UTC Oct 26 2017
 PAC-Opaque:
000200B000030001000400106F5719523570B8D229F23073404E2D3700060094000301009F9B0624C0A0C5D2AFDAAE89
C173D34300000013597A55C100093A8059F0E1A3FAF83A2B7C8332479B7324C0B224F18D8654C2DB14544B58296A0A97
C7B52EB1B7C0725776FE16F715094AC8A766E1F6D16A2A151B70632D6EAB34C5E1874409779FADA53F5892AD4ACC3533
B5A61F89D028C076D94B52744A328C23437306AF428162AC680742003C6BDDB207A08F57
 Refresh timer is set for 11y42w
```

Environment Data

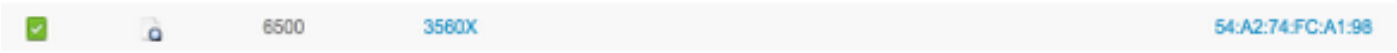
```
3560X#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 14.36.143.18, port 1812, A-ID 6F5719523570B8D229F23073404E2D37
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
   0-d1:Unknown
   2-d1:TrustSec_Devices
```

```
   3-d1:Network_Services
   4-d1:Employees
   5-d1:Contractors
   6-d1:Guests
   7-d1:Production_Users
   8-d1:Developers
   9-d1:Auditors
   10-d1:Point_of_Sale_Systems
   11-d1:Production_Servers
   12-d1:Development_Servers
   13-d1:Test_Servers
   14-d1:PCI_Servers
   15-d1:BYOD
   255-d1:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 02:41:21 UTC Mon Jan 2 2006
Env-data expires in   0:23:56:36 (dd:hr:mm:sec)
Env-data refreshes in 0:23:56:36 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

ISE实时日志

操作> RADIUS >实时日志

PAC调配



Authentication Details

Source Timestamp	2017-07-28 01:32:57.707
Received Timestamp	2017-07-28 01:32:57.708
Policy Server	ISE22new
Event	5206 PAC provisioned
Username	3560X
Endpoint Id	54:A2:74:FC:A1:98
Calling Station Id	54-A2-74-FC-A1-98
Authentication Identity Store	Internal CTS Devices
Audit Session Id	0A7AA5230000000100094C0F0
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	6500

CiscoAVPair	cts-pac-opaque=****, service-type=Framed, cts-capabilities=sap, audit-session-id=0A7AA5230000000100094C0F0, method=dot1x

非种子身份验证

	6500	3560X	NetworkDeviceAuthorization >> NDAC	54:A2:74:FC:A1:98

Overview

Event	5200 Authentication succeeded
Username	3560X
Endpoint Id	54:A2:74:FC:A1:98
Endpoint Profile	
Authorization Policy	NetworkDeviceAuthorization >> NDAC
Authorization Result	Permit Access

Result

User-Name	3560X
State	ReauthSession:0A7AA523000000110094D88C
Class	CACS:0A7AA523000000110094D88C:ISE22new/290042933/396
Session-Timeout	86400 milliseconds
EAP-Key-Name	2b:90:51:10:6d:f0:fd:04:12:07:b1:ea:37:dd:a8:e7:f1:d3:9f:59:49:eb:3b:6d:fe:f4:bb:7c:f9:f5:2c:df:b6:e8:55:7b:cc:84:7c:fa:3a:86:be:a6:c7:93:63:96:03:57:c5:a4:46:bb:e0:19:e9:be:95:b4:37:12:f2:db:ae
cisco-av-pair	cts:security-group-tag=0002-02
cisco-av-pair	cts:supplicant-cts-capabilities=sap
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****

相互对等策略下载

✓		3560X	#CTSDEVICE#-6500	NetworkDeviceAuthorization >> NDAC
✓		6500	#CTSDEVICE#-3560X	NetworkDeviceAuthorization >> NDAC

Overview

Event	5234 TrustSec Peer Policy Download Succeeded
Username	#CTSDEVICE#-3560X
Endpoint Id	
Endpoint Profile	
Authorization Policy	NetworkDeviceAuthorization >> NDAC
Authorization Result	

Result

State	ReauthSession:0e248f12oMzxY0d6l0OEZ/u3aFQs2AoZYPCddb7dJCSt7yoNIwg
Class	CACS:0e248f12oMzxY0d6l0OEZ/u3aFQs2AoZYPCddb7dJCSt7yoNIwg:ISE22new/290042933/397
cisco-av-pair	cts:trusted-device=true
cisco-av-pair	cts:security-group-tag=0002-02
cisco-av-pair	cts:authorization-expiry=86400

Overview

Event	5234 TrustSec Peer Policy Download Succeeded
Username	#CTSDEVICE#-6500
Endpoint Id	
Endpoint Profile	
Authorization Policy	NetworkDeviceAuthorization >> NDAC
Authorization Result	

Result

State	ReauthSession:0e248f122xsxXRQJut5/BzqahPizdpEcb22WZ6zPRPmu0Ms03Bo
Class	CACS:0e248f122xsxXRQJut5/BzqahPizdpEcb22WZ6zPRPmu0Ms03Bo:ISE22new/290042933/399
cisco-av-pair	cts:trusted-device=true
cisco-av-pair	cts:security-group-tag=0002-02
cisco-av-pair	cts:authorization-expiry=86400

TrustSec数据下载

☑		3560X	#CTSREQUEST#	
☑		3560X	#CTSREQUEST#	
☑		3560X	#CTSREQUEST#	NetworkDeviceAuthorization >> NDAC

Overview

Event	5233 TrustSec Data Download Succeeded
Username	#CTSREQUEST#
Endpoint Id	
Endpoint Profile	
Authorization Policy	NetworkDeviceAuthorization >> NDAC
Authorization Result	

Result

State	ReauthSession:0e248f12IVQjPrZ3n038zkt2xhOYWXRJhCAjw_hXw5UAJbMvsLY
Class	CACS:0e248f12IVQjPrZ3n038zkt2xhOYWXRJhCAjw_hXw5UAJbMvsLY:ISE22new/290042933/398
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=0001-17

Result

Class	CACS:0e248f12IVQjPrZ3n038zkt2xhOYWXRJhCAjw_hXw5UAJbMvsLY:ISE22new/290042933/400
cisco-av-pair	cts:server-list=CTSServerList1-0001
cisco-av-pair	cts:server=6f5719523570b8d229f23073404e2d37:14.36.143.18:1812

Result

Class	CACS:0e248f12IVQjPrZ3n038zkt2xhOYWXRJhCAjw_hXw5UAJbMvsLY:ISE22new/290042933/401
cisco-av-pair	cts:security-group-table=0001-17
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

接口验证

Seed (6500)

```
6500#show cts interface gi6/1
Global Dot1x feature is Enabled
Interface GigabitEthernet6/1:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:38:50.744
   Authentication Status:   SUCCEEDED
       Peer identity:       "3560X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Authenticator
   Authorization Status:    SUCCEEDED
```

```
        Peer SGT:            2:TrustSec_Devices
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
Dot1x Info for GigabitEthernet6/1
-----------------------------------
PAE                       = AUTHENTICATOR
```

Non-Seed (3560X)

```
3560X#show cts interface gi0/24
Global Dot1x feature is Enabled
Interface GigabitEthernet0/24:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Interface Active for 00:08:51.317
    Authentication Status:   SUCCEEDED
        Peer identity:       "6500"
        Peer's advertised capabilities: "sap"
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:TrustSec_Devices
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             2
Dot1x Info for GigabitEthernet0/24
-----------------------------------
PAE                       = SUPPLICANT
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。