

为Trustsec在ISE和NAD之间设置ISE 3.4无PAC身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[信息](#)

[配置](#)

[配置](#)

[交换机配置](#)

[ISE 配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍ISE和NAD客户端之间用于Trustsec环境数据下载的无建立(PAC)配置的初始设置。

先决条件

要求

- 熟悉Cisco TrustSec作为网络安全解决方案。
- 身份服务引擎(ISE)知识，用于管理网络安全。
- 基本了解可扩展身份验证协议(EAP)作为传输身份验证信息的框架。

使用的组件

身份服务引擎(ISE)版本3.4.x

Cisco IOS® 17.15.1或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

信息

在无PAC模式下，TrustSec策略更容易实施，因为它们不需要保护访问凭证(PAC)，而保护访问凭

证通常是在设备和身份服务引擎(ISE)之间进行安全通信所必需的。此方法尤其适用于具有多个ISE节点的环境。如果主节点脱机，设备可以自动切换到备份而无需重新建立其凭证，从而减少了中断。无PAC身份验证可简化流程，使其更具扩展性和用户友好性，并支持符合零信任原则的现代安全方法。

在此模式下，设备首先发送包含用户名和密码的请求。ISE通过建议安全会话进行响应。设置此会话后，ISE会提供安全通信所需的重要信息。这包括安全密钥以及服务器身份和计时等详细信息。此信息用于确保安全持续地访问必要的策略和数据。

配置

配置

交换机配置

在本文档中，使用Cisco C9300交换机配置无PAC身份验证的设置。任何运行17.15.1或更高版本的交换机都可以通过身份服务引擎(ISE)执行无PAC身份验证。

步骤 1：在交换机的配置终端下配置交换机上的RADIUS服务器和RADIUS组。

RADIUS 服务器:

```
radius server
```

```
address ipv4
```

```
auth-port 1812 acct-port 1813
```

```
key
```

Radius组：

```
aaa group server radius trustsec  
server name
```

步骤 2：将radius服务器组映射到cts authorization和dot1x，以使用无PAC进行身份验证。

CTS映射：

```
<#root>
  cts authorization list
  cts-mlist
    // cts-mlist is the name of the authorization list
```

Dot1x身份验证：

```
<#root>
  aaa authentication dot1x default group

  aaa authorization network
  cts-mlist
    group
```

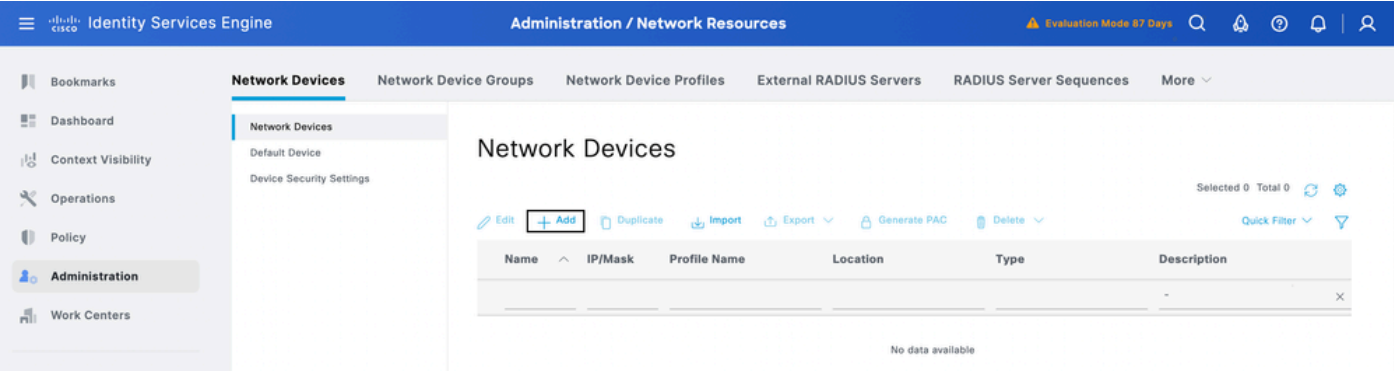
步骤 3：在交换机的enable模式下配置CTS-ID和密码

```
cts credentials id

    password
```

ISE 配置

1.在ISE上，在Administration > Network Resources > Network Devices > Network Devices下配置网络设备。单击add将交换机添加到ISE服务器。



- 2.在ISE的IP地址字段中添加NAD IP地址，以处理来自交换机的trustsec身份验证的RADIUS请求。
- 3.为NAD客户端启用Radius身份验证设置，并输入Radius共享密钥。
- 4.启用Advanced Trustsec Settings，并使用CTS-ID更新Device name，使用password字段更新命令中的密码(cts credentials id <CTS-ID> password <Password>)。

Network Devices List > Test

Network Devices

Name Description IP Address / 32Device Profile Model Name Software Version

Network Device Group

Location [Set To Default](#)IPSEC [Set To Default](#)Device Type [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol Shared Secret [Show](#)☐ Use Second Shared SecretSecond Shared Secret [Show](#)CoA Port [Set To Default](#)

RADIUS DTLS Settings

☐ DTLS RequiredShared Secret CoA Port [Set To Default](#)Issue CA of ISE Certificates for CoA DNS Name

General Settings

☐ Enable KeyWrapKey Encryption Key [Show](#)Message Authenticator Code Key [Show](#)

Key Input Format

☒ ASCII ☐ HEXADECIMAL☐ TACACS Authentication Settings☐ SNMP Settings☒ Advanced TrustSec Settings

Device Authentication Settings

☒ Use Device ID for TrustSec IdentificationDevice ID Password [Show](#)

HTTP REST API settings

☐ Enable HTTP REST APIUsername Password ☐ Support TrustSec Verification reports

TrustSec Notifications and Updates

Download environment data every DaysDownload peer authorization policy every DaysReauthentication every Days

on the switch , radius request is sent to ISE for authentication.(cts refresh environment-data on the switch , radius request is sent to ISE for authentication.)

Live Logs

Live Sessions

Misconfigured Supplicants

Misconfigured Network Devices

RADIUS Drops

Client Stopped Responding

Repeat Counter

0

0

11

0

0

Refresh

Never

Show

Latest 20 records

Within

Last 3 hours

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorizati...
Feb 23, 2025 08:16:12.0...	✓			#CTSREQUEST#			NetworkDeviceAuthorization	NetworkDevic
Feb 23, 2025 08:16:05.7...	✓			#CTSREQUEST#			NetworkDeviceAuthorization	NetworkDevic

Cisco ISE

Overview

Event5233 TrustSec Data Download Succeeded

Username#CTSREQUEST#

Endpoint Id90:77:EE:EC:78:80

Endpoint Profile

Authentication PolicyNetworkDeviceAuthorization

Authorization PolicyNetworkDeviceAuthorization >> Default

Authorization Result

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
12237	PAC-less request	0
11117	Generated a new session ID	1
15012	Selected Access Service	0
12238	Successfully processed PAC-less	0
15036	Evaluating Authorization Policy	0
15006	Matched Default Rule	6
11002	Returned RADIUS Access-Accept	3

Authentication Details

Source Timestamp2025-02-23 19:14:46.407

Received Timestamp2025-02-23 19:14:46.407

Policy Serverise341

Event5233 TrustSec Data Download Succeeded

Username#CTSREQUEST#

Endpoint Id90:77:EE:EC:78:80

Calling Station Id90:77:ee:ec:78:80

Authentication Methodwebauth

故障排除

要解决此问题，请在交换机上运行以下调试：

Debug Command:

```
debug cts environment-data all
debug cts env
debug cts aaa
debug radius
debug cts ifc events
```

```
debug cts authentication details
debug cts authorization all debug
```

调试代码段：

```
*Feb 23 14:48:14.974:CTS环境数据：强制环境数据刷新位掩码0x2
*Feb 23 14:48:14.974:CTS环境数据：download transport-type = CTS_TRANSPORT_IP_UDP
*Feb 23 14:48:14.974: cts_env_data完成：在状态env_data_complete期间，获取事件
0(env_data_request)
*Feb 23 14:48:14.974:@@ cts_env_data完成：env_data_complete -> env_data_waiting_rsp
*Feb 23 14:48:14.974:env_data_waiting_rsp_enter:state = WAITING_RESPONSE
*Feb 23 14:48:14.974:设备上存在安全密钥，请继续无数据包环境数据下载//从交换机启动无数据包
身份验证
*Feb 23 14:48:14.974:cts_aaa_is_fragmented:(CTS env-data SM)NOT-FRAG attr_q(0)
*Feb 23 14:48:14.974:env_data_request_action:state = WAITING_RESPONSE
*Feb 23 14:48:14.974:env_data_download_complete:
    状态(FALSE)，请求(x0),rec(x0)
*Feb 23 14:48:14.974: 状态(FALSE)、请求(x0)、rec(x0)、期望(x81)、
    wait_for_server_list(x85)、wait_for_multicast_SGT(xB5)、
    wait_for_SGName_mapping_tbl(x1485)、
    wait_for_SG-EPG_tbl(x18085)、wait_for_default_EPG_tbl(xC0085)、
    wait_for_default_SGT_tbl(x600085)、wait_for_default_SERVICE_ENTRY_tbl(xC000085)
*Feb 23 14:48:14.974:env_data_request_action:状态= WAITING_RESPONSE，已接收= 0x0请求=
0x0
*Feb 23 14:48:14.974:cts_env_data_aaa_req_setup :aaa_id = 15
*Feb 23 14:48:14.974:cts_aaa_req_setup:(CTS env-data SM)Private group appear DEAD，
attempt public group
*Feb 23 14:48:14.974:cts_aaa_attr_add:AAA请求(0x7AB57A6AA2C0)
*Feb 23 14:48:14.974: 用户名= #CTSREQUEST#
*Feb 23 14:48:14.974:AAA环境添加属性：(CTS env-data SM)attr ( 测试 )
```

*Feb 23 14:48:14.974: cts-environment-data =测试

*Feb 23 14:48:14.974:cts_aaa_attr_add:AAA请求(0x7AB57A6AA2C0)

*Feb 23 14:48:14.974:AAA环境添加属性 : (CTS env-data SM)attr(env-data-fragment)

*Feb 23 14:48:14.974: cts-device-capability = env-data-fragment

*Feb 23 14:48:14.974:cts_aaa_attr_add:AAA请求(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975:AAA环境添加属性 : (CTS env-data SM)attr (多服务器IP支持)

*Feb 23 14:48:14.975: cts-device-capability =多服务器 — ip-supported

*Feb 23 14:48:14.975:cts_aaa_attr_add:AAA请求(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975:AAA环境添加属性 : (CTS env-data SM)attr(wnlx)

*Feb 23 14:48:14.975: clid = wnlx

*Feb 23 14:48:14.975:cts_aaa_req_send:AAA请求(0x7AB57A6AA2C0)已成功发送到AAA。

*Feb 23 14:48:14.975:RADIUS/ENCODE(0000000F) : 源组件类型= CTS

*Feb 23 14:48:14.975:RADIUS(0000000F):配置NAS IP:0.0.0.0

*Feb 23 14:48:14.975:vrvid:[65535] ipv6表ID:[0]

*Feb 23 14:48:14.975:idb为空

*Feb 23 14:48:14.975:RADIUS(0000000F):配置NAS IPv6:::

*Feb 23 14:48:14.975:RADIUS/ENCODE(0000000F):acct_session_id:4003

*Feb 23 14:48:14.975:RADIUS(0000000F):发送

*Feb 23 14:48:14.975:RADIUS:无PAC模式，存在密钥

*Feb 23 14:48:14.975:RADIUS:已成功将CTS无数据包属性添加到RADIUS请求

*Feb 23 14:48:14.975:RADIUS/编码 : Radius-Server 10.127.196.169的最佳本地IP地址 10.127.196.234

*Feb 23 14:48:14.975:RADIUS:无PAC模式，存在密钥

*Feb 23 14:48:14.975:RADIUS(0000000F):将访问请求发送到来自交换机的10.127.196.169:1812 id 1645/11,len 249 // Radius访问请求

RADIUS: 身份验证器78 8A 70 5C E5 D3 DD F1 - B4 82 57 E2 1F 95 3B 92

*Feb 23 14:48:14.975:RADIUS: User-Name [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.975:RADIUS: 思科供应商[26] 33

*Feb 23 14:48:14.975:RADIUS: Cisco AVpair [1] 27 "cts-environment-data=test"

*Feb 23 14:48:14.975:RADIUS: 思科供应商[26] 47

*Feb 23 14:48:14.975:RADIUS: Cisco AVpair [1] 41 "cts-device-capability=env-data-fragment"

*Feb 23 14:48:14.975:RADIUS: 思科供应商[26] 58

*Feb 23 14:48:14.975:RADIUS: Cisco AVpair [1] 52 "cts-device-capability=multiple-server-ip-supported"

*Feb 23 14:48:14.975:RADIUS: User-Password [2] 18 *

*Feb 23 14:48:14.975:RADIUS: Calling-Station-Id [31] 8 "wnlx"

*Feb 23 14:48:14.975:RADIUS: Service-Type [6] 6 Outbound [5]

*Feb 23 14:48:14.975:RADIUS: NAS-IP-Address [4] 6 10.127.196.234

*Feb 23 14:48:14.975:RADIUS: 思科供应商[26] 39

*Feb 23 14:48:14.975:RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC Less cv-pair属性添加到ISE处理无平台身份验证数据包的请求

*Feb 23 14:48:14.975:RADIUS(0000000F):发送IPv4 Radius数据包

*Feb 23 14:48:14.975:RADIUS(0000000F):已启动5秒超时

*Feb 23 14:48:14.990:RADIUS:接收自id 1645/11 10.127.196.169:1812, Access-Accept , len 313。 //身份验证成功

RADIUS: 身份验证器92 4C 21 5C 99 28 64 8B - 23 06 4B 87 F6 FF 66 3C

*Feb 23 14:48:14.990:RADIUS: User-Name [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.990:RADIUS: 类[25] 78

RADIUS: 43 41 43 53 3A 30 61 37 66 63 34 61 39 54 37 68 [CACS:0a7fc4a9T7h]

RADIUS: 39 79 44 42 70 2F 7A 6A 64 66 66 56 49 55 74 4D [9yDBp/zjdffVIUtM]

RADIUS: 78 34 68 63 50 4C 4A 45 49 76 75 79 51 62 4C 70 [x4hcPLJElvuyQbLp]

RADIUS: 31 48 7A 35 50 45 39 38 3A 69 73 65 33 34 31 2F [1Hz5PE98:ise341/]

RADIUS: 35 32 39 36 36 39 30 32 31 2F 32 31 [529669021/21]

*Feb 23 14:48:14.990:RADIUS: 思科供应商[26] 39

*Feb 23 14:48:14.990:RADIUS: Cisco AVpair [1] 33"cts-pac-capability=cts-pac-less"

*Feb 23 14:48:14.990:RADIUS: 思科供应商[26] 43

*Feb 23 14:48:14.991:RADIUS: Cisco AVpair [1] 37 "cts:server-list=CTSServerList1-0001"

*Feb 23 14:48:14.991:RADIUS: 思科供应商[26] 38

*Feb 23 14:48:14.991:RADIUS: Cisco AVpair [1] 32 "cts:security-group-tag=0002-00"

*Feb 23 14:48:14.991:RADIUS: 思科供应商[26] 41

*Feb 23 14:48:14.991:RADIUS: Cisco AVpair [1] 35 "cts:environment-data-expiry=86400"

*Feb 23 14:48:14.991:RADIUS: 思科供应商[26] 40

*Feb 23 14:48:14.991:RADIUS: Cisco AVpair [1] 34 "cts:security-group-table=0001-17"

*Feb 23 14:48:14.991:RADIUS:无PAC模式，存在密钥

*Feb 23 14:48:14.991:RADIUS(0000000F):从1645/11号码收到

*Feb 23 14:48:14.991:cts_aaa_callback:(CTS env-data SM)AAA req(0x7AB57A6AA2C0)响应成功

*Feb 23 14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr (测试)

*Feb 23 14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr(env-data-fragment)

*Feb 23 14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr (多服务器IP支持)

*Feb 23 14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr(wnlx)

*Feb 23 14:48:14.991: AAA属性：未知类型(450)。

*Feb 23 14:48:14.991: AAA属性：未知类型(1324)。

*Feb 23 14:48:14.991: AAA属性：server-list = CTSServerList1-0001。

*Feb 23 14:48:14.991:已收到SLIST名称。将cts_is_slist_send_to_binos_req设置为FALSE

*Feb 23 14:48:14.991: AAA属性：security-group-tag = 0002-00。

*Feb 23 14:48:14.991: AAA属性：environment-data-expiry = 86400。

*Feb 23 14:48:14.991: AAA属性：security-group-table = 0001-17.CTS env-data:接收AAA属性。
//下载环境数据

CTS_AAA_SLIST

在1st Access-Accept中收到的slist name(CTSServerList1)

slist name(CTSServerList1)存在

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400。

CTS_AAA_SGT_NAME_LIST

表(0001)在第1次访问接受中收到

将表(0001)从已安装复制到已接收，因为没有任何更改。

新名称(0001),gen(17)

CTS_AAA_DATA_END

*Feb 23 14:48:14.991: cts_env_data WAITING_RESPONSE:在状态env_data_waiting_rsp期间，获取事件1(env_data_received)

*Feb 23 14:48:14.991:@@ cts_env_data WAITING_RESPONSE:env_data_waiting_rsp -> env_data_assessing

*Feb 23 14:48:14.991:env_data_assessing_enter:状态=正在评估

*Feb 23 14:48:14.991:cts_aaa_is_fragmented:(CTS env-data SM)NOT-FRAG attr_q(0)

*Feb 23 14:48:14.991:env_data_assessing_action:状态=正在评估

*Feb 23 14:48:14.991:env_data_download_complete:

状态(FALSE)，请求(x81),rec(xC87)

*Feb 23 14:48:14.991:期望与接收相同

*Feb 23 14:48:14.991: status(TRUE)、req(x81)、rec(xC87)、expect(x81)

wait_for_server_list(x85)、wait_for_multicast_SGT(xB5)、
wait_for_SGName_mapping_tbl(x1485)、

wait_for_SG-EPG_tbl(x18085)、wait_for_default_EPG_tbl(xC0085)、
wait_for_default_SGT_tbl(x600085)、wait_for_default_SERVICE_ENTRY_tbl(xC000085)

*Feb 23 14:48:14.991: cts_env_data评估：在状态env_data_assessing期间，获取事件4(env_data_complete)

*Feb 23 14:48:14.991:@@ cts_env_data正在评估：env_data_assessing -> env_data_complete

*Feb 23 14:48:14.991:env_data_complete_enter:状态=完成

*Feb 23 14:48:14.991:CTS-ifc-ev:env数据报告至核心，结果：成功

*Feb 23 14:48:14.991:env_data_install_action:状态= COMPLETE completed.types 0x0

*Feb 23 14:48:14.991:env_data_install_action:全新安装的sgt<->sgname表

*Feb 23 14:48:14.991:正在清理已安装的sg-epg列表

*Feb 23 14:48:14.991:正在清除已安装的默认epg列表

*Feb 23 14:48:14.991:env_data_install_action:mcast_sgt表已更新

*Feb 23 14:48:14.991:环境数据同步到备用状态2

*Feb 23 14:48:14.991:SLIST与上一次刷新相同。无需将其发送到BINOS

*Feb 23 14:48:14.991:CTS-sg-epg-events : 将default_sg 0设置为env data

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）。