Setup ISE 3.4 PAC-less Authentication between ISE and NAD for Trustsec

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Information

Configure

- Configurations
  - Switch Configuration
  - ISE Configuration

Verify

Troubleshoot

Introduction

The document describes the initial setup for PAC-less configuration between ISE and NAD clients for Trustsec environment data download.

Prerequisites

Requirements

- Familiarity with Cisco TrustSec as a network security solution.
- Knowledge of Identity Services Engine (ISE) for managing network security.
- Basic understanding of Extensible Authentication Protocol (EAP) as a framework for transporting authentication information.

Components Used

Identity Services Engine (ISE) Release 3.4.x

Cisco IOS® 17.15.1 or higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Information

In PAC-less mode, TrustSec policies are easier to implement because they do not require a Protected Access

Credential (PAC), which is usually needed for secure communication between devices and the Identity Services Engine (ISE). This approach is particularly beneficial in environments with multiple ISE nodes. If the primary node goes offline, devices can automatically switch to a backup without needing to re-establish their credentials, reducing interruptions. PAC-less authentication simplifies the process, making it more scalable and user-friendly, and supports modern security methods aligned with Zero Trust principles.

In this mode, devices start by sending a request that includes a username and password. The ISE responds by proposing a secure session. Once this session is set up, the ISE provides important information needed for secure communication. This includes a key for security and details like server identity and timing. This information is used to ensure secure and continuous access to necessary policies and data.

Configure

Configurations

Switch Configuration

In this document, the setup for PAC-less authentication is configured using the Cisco C9300 switch. Any switch running version 17.15.1 or higher can perform PAC-less authentication with the Identity Services Engine (ISE).

Step 1: Configure the Radius server and radius group on the switch under configuration terminal of the switch.

Radius server:

```
radius server <Server Name>
 address ipv4 <ISE Ip address> auth-port 1812 acct-port 1813
 key <Radius shared secret>
```

Radius Group:

```
aaa group server radius trustsec
 server name <Server Name>
```

Step 2: Map the radius server group to cts authorization and dot1x for authentication with PAC-less.

CTS Mapping:

<#root>

```
cts authorization list
```

cts-mlist

```
   // cts-mlist is the name of the authorization list
```

Dot1x authentication:

<#root>

```
aaa authentication dot1x default group <Server Name>
aaa authorization network
```

cts-mlist

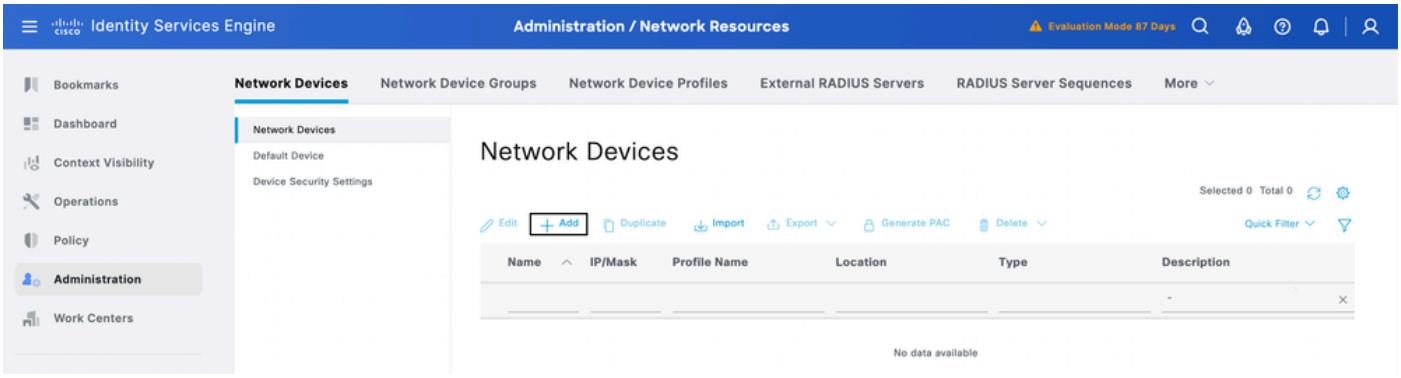
```
 group <Server Name>
```

Step 3: Configure the **CTS-ID** and **password** under the **enable mode** on the switch

```
cts credentials id <CTS-ID> password <Password>
```

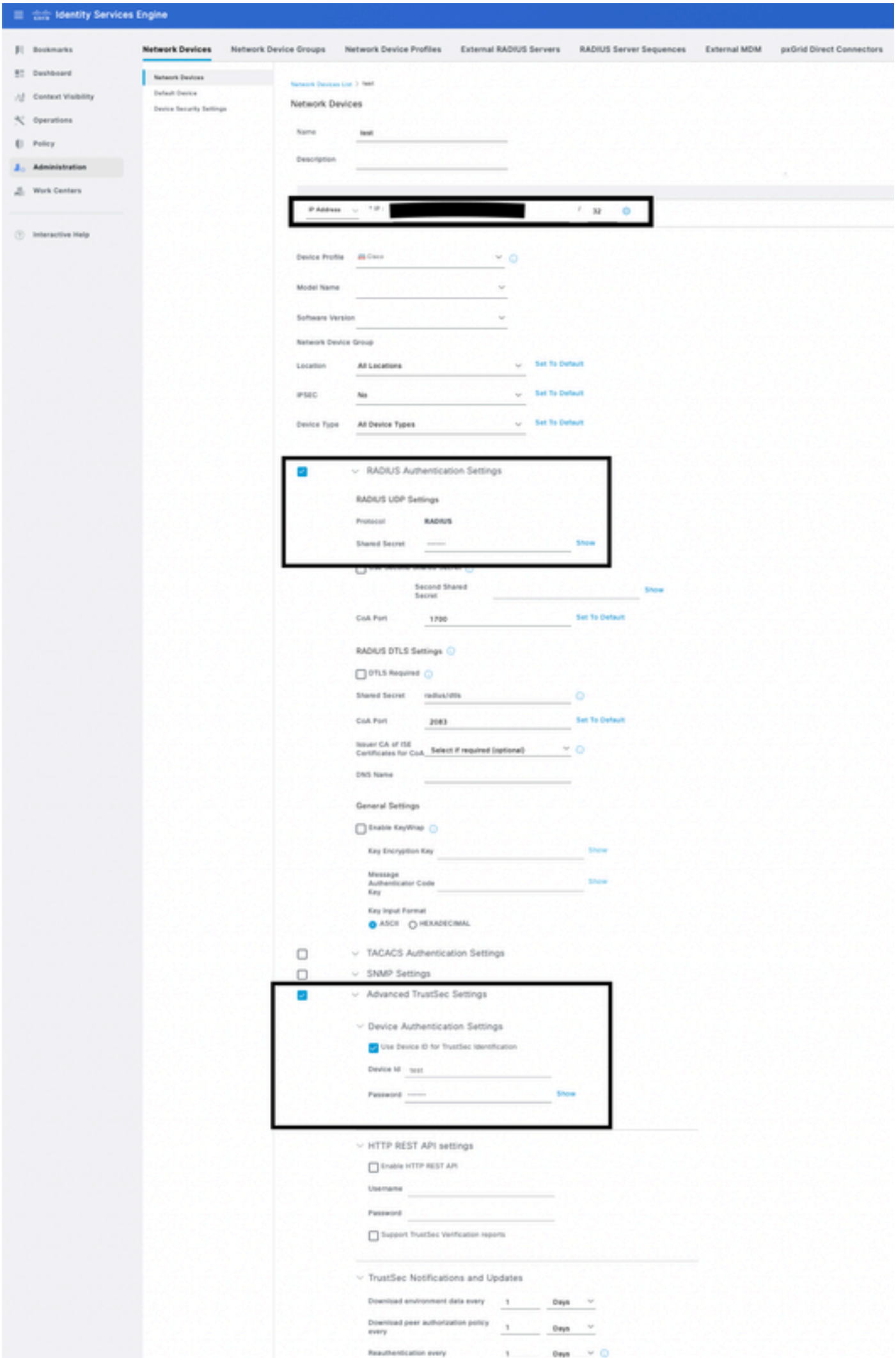
ISE Configuration

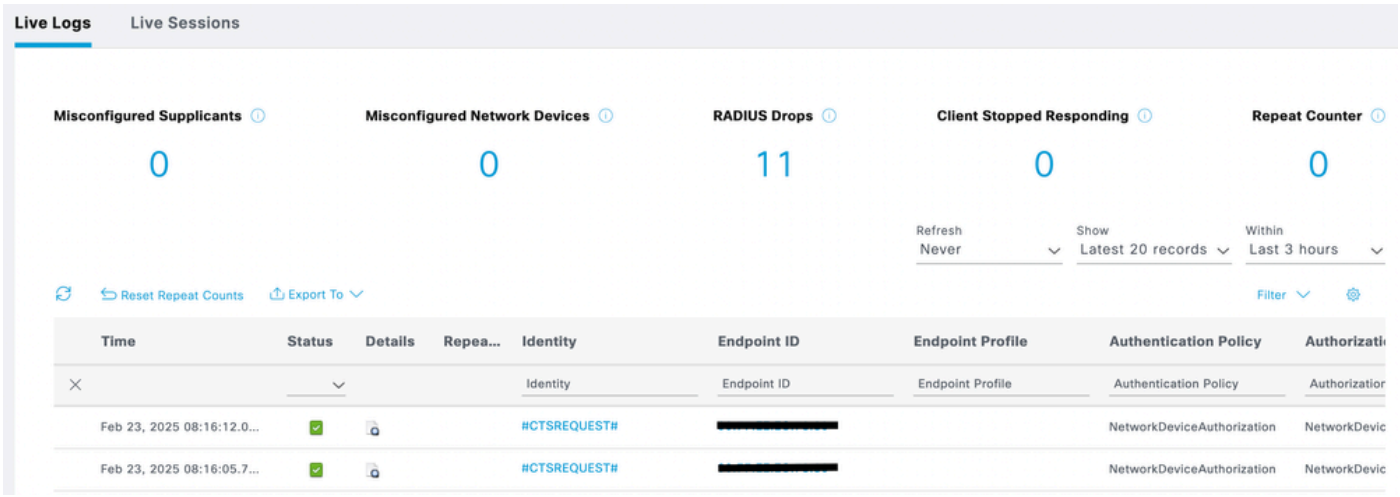
1. On ISE, configure the **network device** under **Administration > Network Resources > Network Devices > Network Devices**. Click **add** to add the switch to the ISE server.

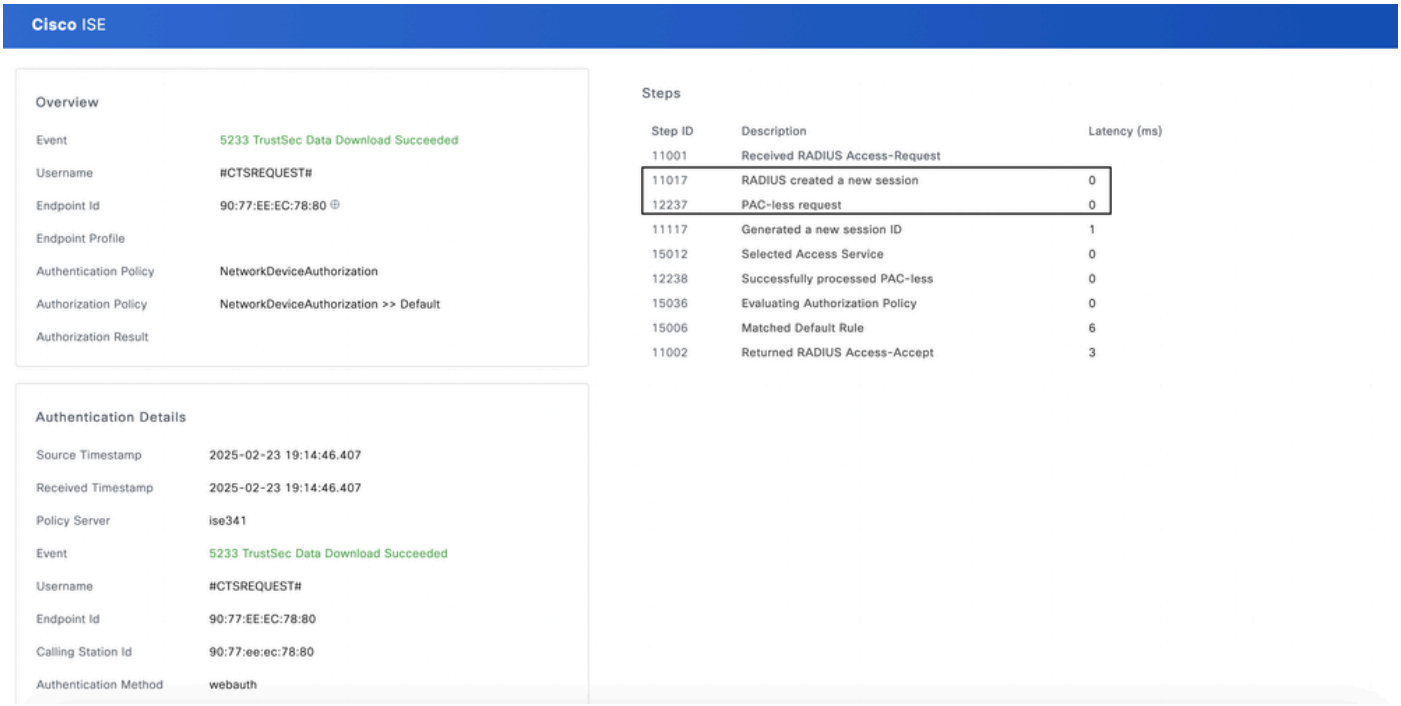


2. Add the **NAD IP address** in the ip address field for ISE to process the radius request for the trustsec authentication from the switch.
3. Enable **Radius Authenticaiton Settings** for the NAD client and enter the **Radius shared secret key**.

4. Enable **Advanced Trustsec Settings** and update the **Device name** with CTS-ID and the password field with the **password from the command** (cts credentials id <CTS-ID> password <Password>).


Identity Services Engine
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
pxGrid Direct Connectors
Network Devices
Default Device
Device Security Settings
Network Devices List > test
Network Devices
Name
test
Description
IP Address
[redacted]
32
Device Profile
Model Name
Software Version
Network Device Group
Location
All Locations
Set To Default
IPSEC
No
Set To Default
Device Type
All Device Types
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
Shared Secret
Show
Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
DNS Name
General Settings
Enable KeyWrap
Key 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 Identification
Device Id
test
Password
Show
HTTP REST API settings
Enable HTTP REST API
Username
Password
Support TrustSec Verification reports
TrustSec Notifications and Updates
Download environment data every
1
Days
Download peer authorization policy every
1
Days
Reauthentication every
1
Days





Troubleshoot

To Troubleshoot the issue, please run these debugs on the switch:

```
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
```

Debug Snippet:

*Feb 23 14:48:14.974: CTS env-data: Force environment-data refresh bitmask 0x2

*Feb 23 14:48:14.974: CTS env-data: download transport-type = CTS_TRANSPORT_IP_UDP

*Feb 23 14:48:14.974: cts_env_data COMPLETE: during state env_data_complete, got event 0(env_data_request)

*Feb 23 14:48:14.974: @@@ cts_env_data COMPLETE: 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: Secure Key is present on the device, proceed with pac-less env-data download // initiate the PAC-Less authententication from switch

*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:

status(FALSE), req(x0),rec(x0)

*Feb 23 14:48:14.974: status(FALSE), req(x0), rec(x0), 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 14:48:14.974: env_data_request_action: state = WAITING_RESPONSE, received = 0x0 request = 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 appears DEAD, attempt public group

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

*Feb 23 14:48:14.974: username = #CTSREQUEST#

*Feb 23 14:48:14.974: AAA Context Add Attribute: (CTS env-data SM)attr(test)

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

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

*Feb 23 14:48:14.974: AAA Context Add Attribute: (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 req(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975: AAA Context Add Attribute: (CTS env-data SM)attr(multiple-server-ip-supported)

*Feb 23 14:48:14.975: cts-device-capability = multiple-server-ip-supported

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

*Feb 23 14:48:14.975: AAA Context Add Attribute: (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 req(0x7AB57A6AA2C0) successfully sent to AAA.

*Feb 23 14:48:14.975: RADIUS/ENCODE(0000000F):Orig. component type = CTS

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

*Feb 23 14:48:14.975: vrfid: [65535] ipv6 tableid : [0]

*Feb 23 14:48:14.975: idb is NULL

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

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

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

*Feb 23 14:48:14.975: RADIUS: PAC less mode, secret is present

*Feb 23 14:48:14.975: RADIUS: Successfully added CTS pacless attribute to the radius request

*Feb 23 14:48:14.975: RADIUS/ENCODE: Best Local IP-Address 10.127.196.234 for Radius-Server 10.127.196.169

*Feb 23 14:48:14.975: RADIUS: PAC less mode, secret is present

*Feb 23 14:48:14.975: RADIUS(0000000F): Send Access-Request to 10.127.196.169:1812 id 1645/11, len 249 // Radius Access Request from the switch

RADIUS: authenticator 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: Vendor, Cisco [26] 33

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

*Feb 23 14:48:14.975: RADIUS: Vendor, Cisco [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: Vendor, Cisco [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: Vendor, Cisco   [26] 39

*Feb 23 14:48:14.975: RADIUS: Cisco AVpair   [1]   33 "cts-pac-capability=cts-pac-less"
  // CTS PAC Less cv-pair attribute add to the request for ISE to handle the packet for PAC-less authentication

*Feb 23 14:48:14.975: RADIUS(0000000F): Sending a IPv4 Radius Packet

*Feb 23 14:48:14.975: RADIUS(0000000F): Started 5 sec timeout

*Feb 23 14:48:14.990: RADIUS: Received from id 1645/11 10.127.196.169:1812, Access-Accept, len 313.
  // Authentication success

RADIUS: authenticator 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: Class   [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 [x4hcPLJEIvuyQbLp]

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: Vendor, Cisco   [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: Vendor, Cisco   [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: Vendor, Cisco   [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: Vendor, Cisco   [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: Vendor, Cisco   [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: PAC less mode, secret is present

*Feb 23 14:48:14.991: RADIUS(0000000F): Received from id 1645/11

*Feb 23 14:48:14.991: cts_aaa_callback: (CTS env-data SM)AAA req(0x7AB57A6AA2C0) response success

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

*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(multiple-server-ip-supported)

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

*Feb 23 14:48:14.991: AAA attr: Unknown type (450).

*Feb 23 14:48:14.991: AAA attr: Unknown type (1324).

*Feb 23 14:48:14.991: AAA attr: server-list = CTSServerList1-0001.

*Feb 23 14:48:14.991: Received SLIST name. Setting cts_is_slist_send_to_binos_req to FALSE

*Feb 23 14:48:14.991: AAA attr: security-group-tag = 0002-00.

*Feb 23 14:48:14.991: AAA attr: environment-data-expiry = 86400.

*Feb 23 14:48:14.991: AAA attr: security-group-table = 0001-17.CTS env-data: Receiving AAA attributes. // Downloading the environment data

CTS_AAA_SLIST

slist name(CTSServerList1) received in 1st Access-Accept

slist name(CTSServerList1) exists

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

table(0001) received in 1st Access-Accept

Copy table(0001) from installed to received because no change.

new name(0001), gen(17)

CTS_AAA_DATA_END

*Feb 23 14:48:14.991: cts_env_data WAITING_RESPONSE: during state env_data_waiting_rsp, got event 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: state = ASSESSING

*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: state = ASSESSING

*Feb 23 14:48:14.991: env_data_download_complete:

status(FALSE), req(x81),rec(xC87)

*Feb 23 14:48:14.991: Expect same as received

*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 ASSESSING: during state env_data_assessing, got event 4(env_data_complete)

*Feb 23 14:48:14.991: @@@ cts_env_data ASSESSING: env_data_assessing -> env_data_complete

*Feb 23 14:48:14.991: env_data_complete_enter: state = COMPLETE

*Feb 23 14:48:14.991: CTS-ifc-ev: env data reporting to core, result: Successful

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

*Feb 23 14:48:14.991: env_data_install_action: clean installed sgt<->sgname table

*Feb 23 14:48:14.991: Cleaning up installed sg-epg list

*Feb 23 14:48:14.991: Cleaning up installed default epg list

*Feb 23 14:48:14.991: env_data_install_action: mcast_sgt table updated

*Feb 23 14:48:14.991: Env data sync to standby status 2

*Feb 23 14:48:14.991: SLIST is the same as previous refresh. No need to send it to BINOS

*Feb 23 14:48:14.991: CTS-sg-epg-events:setting default_sg 0 to env data