

Configure RADIUS KeyWrap in ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[ISE](#)

[Switch](#)

[PC](#)

[Verify](#)

[Frequently Asked Questions](#)

[Reference](#)

Introduction

This document describes the procedure to configure RADIUS KeyWrap in Cisco ISE and Cisco Switch.

Prerequisites

- Knowledge of dot1x
- Knowledge of RADIUS protocol
- Knowledge of EAP

Components Used

- ISE 3.2
- Cisco C9300-24U with Software Version 17.09.04a
- Windows 10 PC

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.

Background Information

Key wrapping is a technique where one key value is encrypted using another key. The same mechanism is used in RADIUS to encrypt the key material. This material is usually produced as a by-product of an Extensible Authentication Protocol (EAP) authentication and returned in the Access-Accept message after a successful authentication. This feature is mandatory if ISE is running in FIPS mode.

This provides a protective layer that insulates the actual key material for safeguarding against potential attacks. The underlying key material essentially becomes virtually inaccessible to threat actors, even in cases of data interception. The main intention behind RADIUS key wrapping is to prevent the exposure of key

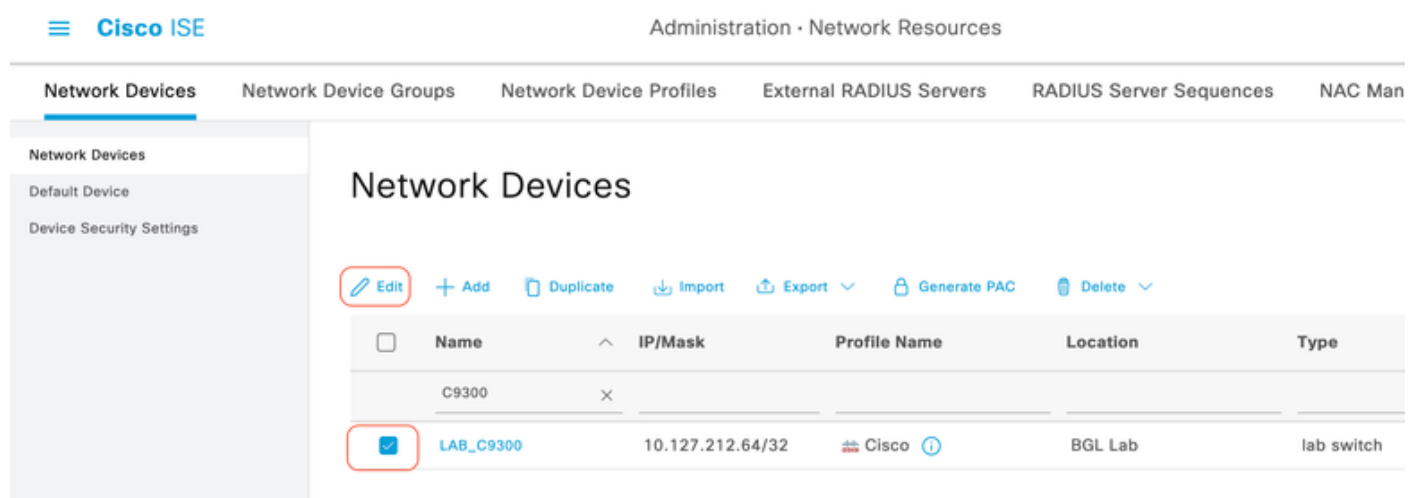
material that secure digital content, particularly in a large-scale enterprise-level network.

In ISE, the Key Encryption Key is used to encrypt the key materials with the AES encryption and the Message Authenticator Code Key separated from RADIUS shared secret key in order to generate Message authenticator Code.

Configure

ISE

Step 1: Navigate to **Administration > Network Resources > Network Devices**. Click the checkbox for the network device for which you want to configure RADIUS KeyWrap. Click **Edit** (if the Network Device is already added).



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes the Cisco ISE logo and the path "Administration > Network Resources". Below this, a horizontal menu lists various resource types: "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", "RADIUS Server Sequences", and "NAC Man". The "Network Devices" section is active, showing a sidebar with "Network Devices", "Default Device", and "Device Security Settings". The main content area is titled "Network Devices" and contains a toolbar with buttons: "Edit" (highlighted with a red box), "+ Add", "Duplicate", "Import", "Export", "Generate PAC", and "Delete". Below the toolbar is a table with columns: "Name", "IP/Mask", "Profile Name", "Location", and "Type". The table lists two devices: "C9300" and "LAB_C9300". The "LAB_C9300" row has its checkbox selected and is highlighted with a red box. The details for "LAB_C9300" are: IP/Mask: 10.127.212.64/32, Profile Name: Cisco, Location: BGL Lab, and Type: lab switch.

	Name	IP/Mask	Profile Name	Location	Type
☐	C9300	x			
☒	LAB_C9300	10.127.212.64/32	Cisco	BGL Lab	lab switch

Step 2 : Expand the **RADIUS Authentication Settings**. Click the **Enable KeyWrap** check box. Enter the **Key Encryption Key** and **Message Authenticator Code Key**. Click **Save**.

General Settings

☒ Enable KeyWrap ⓘ

Key Encryption Key

22AB0###CA#1b2b1

Hide

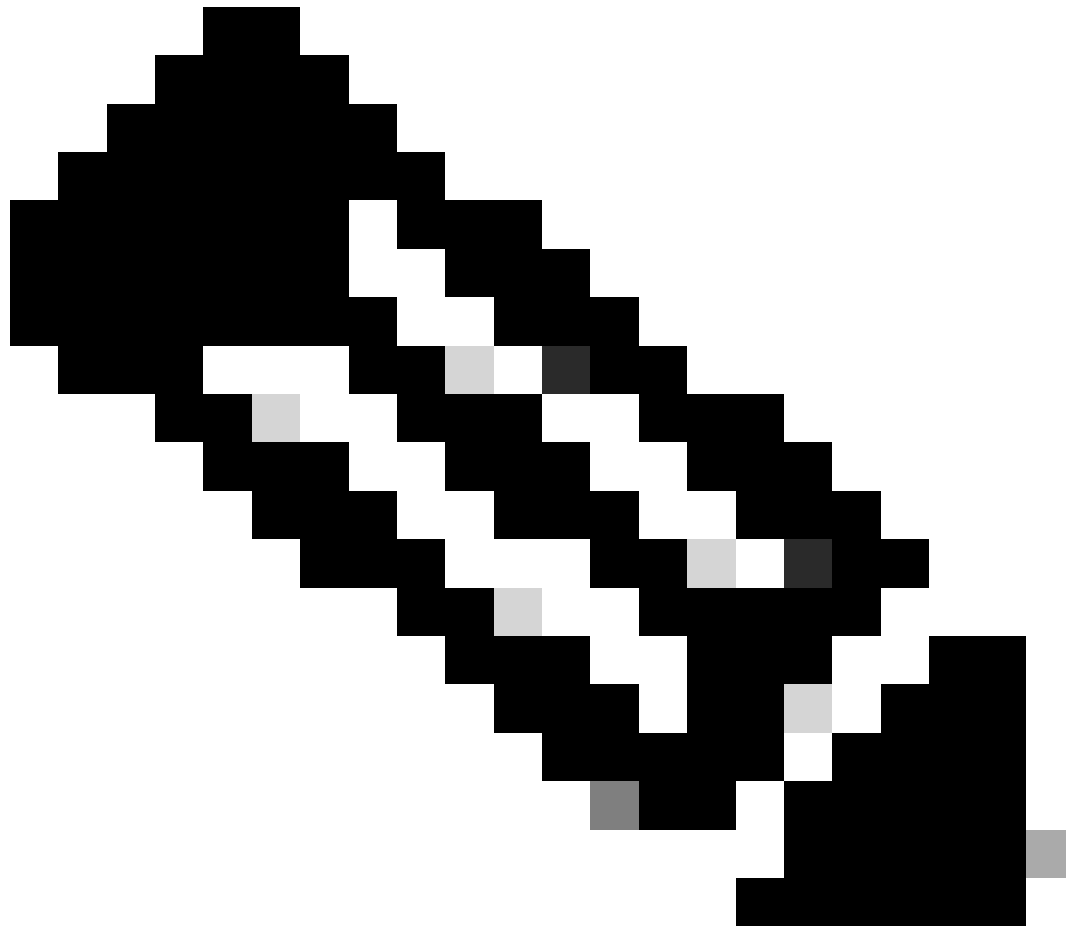
Message
Authenticator Code

12b1CcB202#2Cb1#bCa#

Hide

Key Input Format

☒ ASCII ☐ HEXADECIMAL



Note: Key Encryption Key and Message Authenticator Code Key must be different.

Switch

AAA configuration in Switch to enable the RADIUS KeyWrap feature.

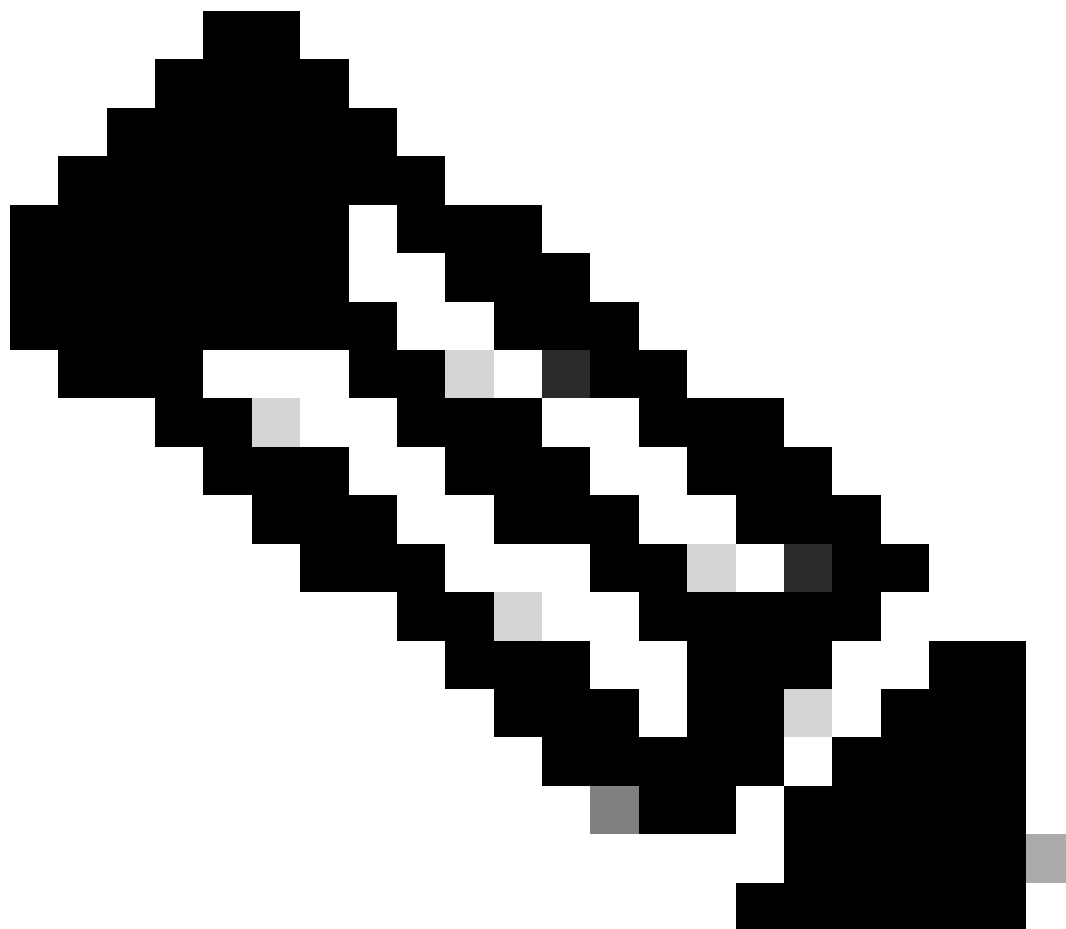
```
aaa authentication dot1x default group RADGRP
aaa authorization network default group RADGRP
aaa accounting dot1x default start-stop group RADGRP
```

```
radius server ISERAD
address ipv4 10.127.197.165 auth-port 1812 acct-port 1813
key-wrap encryption-key 0 22AB0###CA#1b2b1 message-auth-code-key 0 12b1CcB202#2Cb1#bCa# format ascii
key Iselab@123
```

```
aaa group server radius RADGRP
server name ISERAD
key-wrap enable
```

```
interface GigabitEthernet1/0/22
```

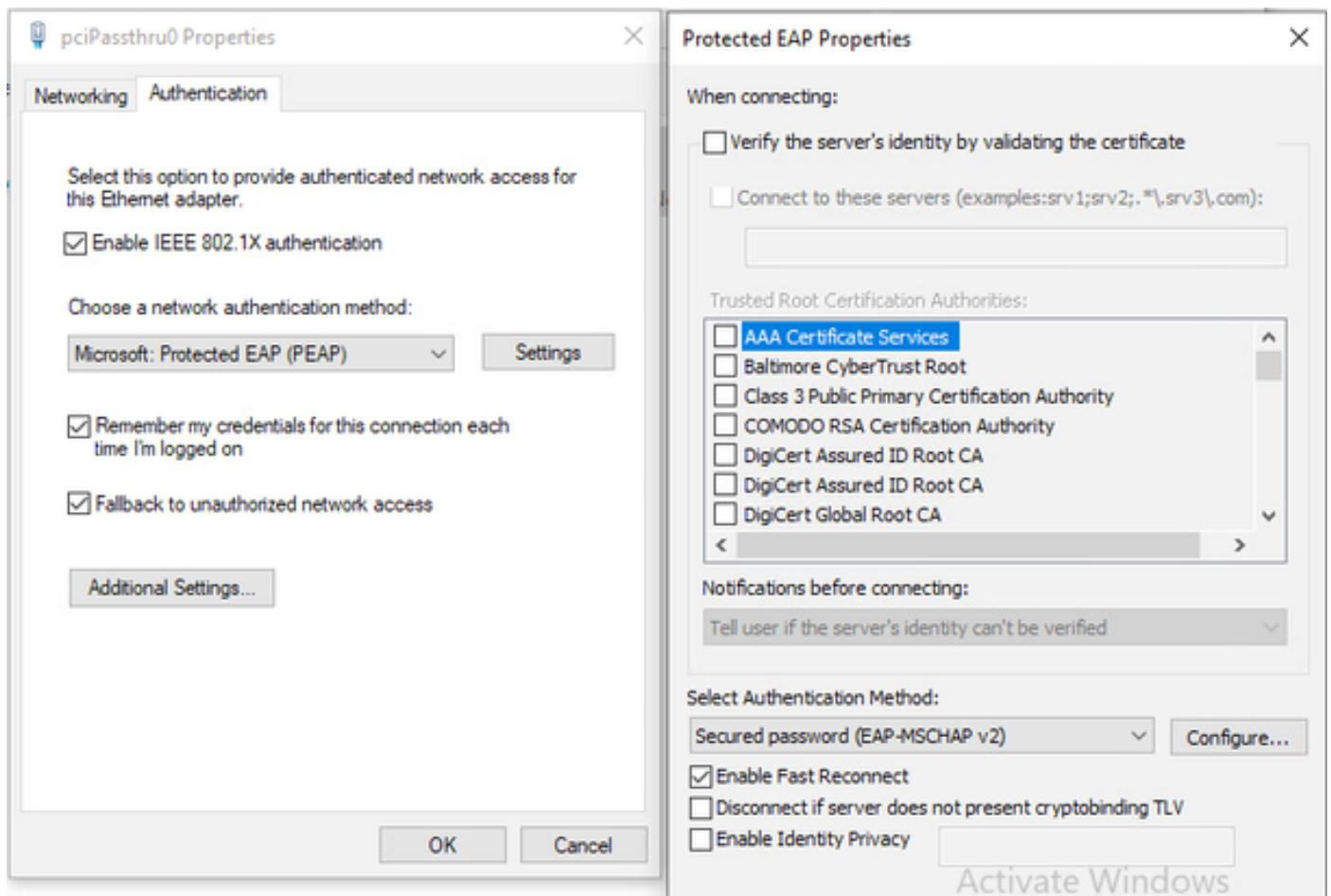
```
switchport access vlan 302
switchport mode access
device-tracking attach-policy IPDT
authentication host-mode multi-domain
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
end
```



Note: The encryption-key must be 16 characters long and message-auth-code and 20 characters long.

PC

Windows 10 Supplicant configured for PEAP-MSCHAPv2.



Verify

When the RADIUS KeyWrap feature is not enabled on Switch:

show radius server-group <SERVER GROUP NAME>

The command output must show **Keywrap enabled: FALSE**.

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: FALSE
```

In the packet capture, you can see that there no Cisco-AV-Pair attribute for app-key, random-nonce and separate message-authenticator-code. This indicates that RADIUS KeyWrap is disabled on the switch.

No.	Time	Source	Destination	Protocol	Length	Info
5	38	10.127.212.64	10.127.197.165	RADIUS	331	Access-Request id=149
> Frame 5: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) > Ethernet II, Src: Cisco_de:7e:79 (4c:ec:0f:de:7e:79), Dst: VMware_8b:9a:ba (00:50:56:8b:9a:ba) > Internet Protocol Version 4, Src: 10.127.212.64, Dst: 10.127.197.165 > User Datagram Protocol, Src Port: 58199, Dst Port: 1812 > RADIUS Protocol						
Code: Access-Request (1) Packet identifier: 0x95 (149) Length: 289 Authenticator: 890b5cfffdf737affa6b6f0c18d9925ee [The response to this request is in frame 6]						
Attribute Value Pairs > AVP: t=User-Name(1) l=10 val=sksarkar > AVP: t=Service-Type(6) l=6 val=Framed(2) > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9) > AVP: t=Framed-MTU(12) l=6 val=1468 > AVP: t=EAP-Message(79) l=15 Last Segment[1] > AVP: t=Message-Authenticator(80) l=18 val=79aca893d2933dee24cab4184c5674be > AVP: t=EAP-Key-Name(102) l=2 val= > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9) > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9) > AVP: t=Framed-IP-Address(8) l=6 val=10.127.212.216 > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9) > AVP: t=NAS-IP-Address(4) l=6 val=10.127.212.64 > AVP: t=NAS-Port-Id(87) l=23 val=GigabitEthernet1/0/22 > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15) > AVP: t=NAS-Port(5) l=6 val=50122 > AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DD-E7 > AVP: t=Called-Station-Id(30) l=19 val=50-F7-22-B2-D6-16						

In the ISE prrt-server.log, you can see that ISE only validates the integrity attribute which is the Message-Authenticator.

```
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
[8] Framed-IP-Address - value: [10.127.212.216]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[80] Message-Authenticator - value: [<88>/`f<f2>|<a1>><b3><18><06>(<ee>?<c3><c3>]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A0000002B9E06997E]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iiif-id=292332370] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
```

In the Access-Accept packet, you can see that the MS-MPPE-Send-key and MS-MPPE-Recv-Key are sent from the RADIUS Server to the Authenticator. MS-MPPE specifies the key material generated by the EAP methods which can be used to perform data encryption between peer and Authenticator. These 32-byte keys

are derived from the RADIUS shared secret, request authenticator, and a random salt.

No.	Time	Source	Destination	Protocol	Length	Info	Start	Type
28	38	10.127.197.165	10.127.212.64	RADIUS	333	Access-Accept id=160		

```

> Frame 28: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits)
> Ethernet II, Src: VMware_8b:9a:ba (00:50:56:8b:9a:ba), Dst: Cisco_de:7e:79 (4c:ec:0f:de:7e:79)
> Internet Protocol Version 4, Src: 10.127.197.165, Dst: 10.127.212.64
> User Datagram Protocol, Src Port: 1812, Dst Port: 58199
< RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xa0 (160)
  Length: 291
  Authenticator: 72c12c624ea2e3b85358b5746895bcf3
  [This is a response to a request in frame 27]
  [Time from request: 0.081826000 seconds]
  Attribute Value Pairs
    > AVP: t=User-Name(1) l=10 val=sksarkar
    > AVP: t=Class(25) l=54 val=434143533a3430443437463041303030303030323739353743364631383a6c616270616e...
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=54cc0cf47f9a996cf92c49960e7b0ea7
    > AVP: t=EAP-Key-Name(102) l=67 val=\031\040\000\000\t\036\000\006\035\01\00c\0\0\05CB?\u0012\036\0250\000es2F0M\005\024?\033\002\00\022!\00Ap\000\003
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
      Type: 26
      Length: 58
      Vendor ID: Microsoft (311)
      > VSA: t=MS-MPPE-Send-Key(16) l=52 val=afb8ce27f0f911330627544ee383e0fb8c6f721ae4fc86ea400e56a28f0026fa2949167d...
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
      Type: 26
      Length: 58
      Vendor ID: Microsoft (311)
      > VSA: t=MS-MPPE-Recv-Key(17) l=52 val=fabfda3156c55a1107b8e01264ee00da8a8efd91aecd419a46f7be5293494f9f8d7a2a1...

```

When the RADIUS KeyWrap feature is enabled on Switch and ISE:

show radius server-group <SERVER GROUP NAME>

The command output must shows **Keywrap enabled: TRUE**.

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: TRUE
```

In the packet capture, you can see that there is a Cisco-AV-Pair attribute for app-key (with no data), random-nonce and separate message-authenticator-code are present. This indicates to the RADIUS server that the Authenticator (Switch) supports the RADIUS KeyWrap and the server must use the same.

Time	Source	Destination	Protocol	Length	Info	Start	Type	Service-Type	Frame
1.0	10.127.212.64	10.127.197.165	RADIUS	512	Access-Request id=173		Identity		
					Cisco-AVPair: method=dot1x	0000	00 50 56 8b 9a ba 4c ec 0f de 7e 79 08 00 45 00	..PV...L...y..E..	
					AVP: t=Framed-IP-Address(8) l=6 val=10.127.212.216	0010	01 12 90 47 00 00 3d 11 3c 0d 0a 7f d4 40 0a 7f	...G...=<...@...	
					AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)	0020	05 c5 a5 e3 57 07 14 01 de 75 02 01 ad 01 d6 b2 74	...W...u...t...	
					Type: 26	0030	cc 01 6c b3 5c 17 27 c1 54 5c 9d eb ca a7 01 0a	...L...T... ..	
					Length: 31	0040	73 6b 73 61 72 6b 61 72 06 06 00 00 02 1a 1b	...sksarkar...	
					Vendor ID: ciscoSystems (9)	0050	00 00 00 09 01 15 73 65 72 76 69 63 65 2d 74 79	...r...se rvic...ty	
					VSA: t=Cisco-AVPair(1) l=25 val=client-ii-f-id=389191649	0060	70 65 3d 46 72 61 6d 65 64 0c 00 00 05 bc 4f	pe=Frame d...=0	
					Type: 1	0070	0f 02 01 00 0d 01 73 6b 73 61 72 6b 61 72 6e 02	...sk sarkarf...	
					Length: 25	0080	1a 31 00 00 00 09 01 2b 61 75 64 69 74 2d 73 65	..1...+ audit...se	
					Cisco-AVPair: client-ii-f-id=389191649	0090	73 73 69 6f 6e 2d 69 64 3d 34 30 44 34 37 46 30	ssion-id =40047F0	
					AVP: t=NAS-IP-Address(4) l=6 val=10.127.212.64	00a0	41 30 30 30 30 30 30 32 39 39 35 39 44 45 31 44	A0000002 99594DEID	
					AVP: t=NAS-Port-Id(87) l=23 val=GigabitEthernet1/0/22	00b0	39 1a 14 00 00 00 09 01 0e 6d 65 74 68 6f 64 3d	9...method=	
					AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)	00c0	64 6f 74 31 78 08 06 0a 7f d4 08 1a 1f 00 00 00	dot1x...	
					AVP: t=NAS-Port(5) l=6 val=50122	00d0	09 01 19 63 6c 69 65 6e 74 4d 69 69 66 2d 69 64	...clien t-ii-f-id	
					AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DD-E7	00e0	3d 33 38 39 31 39 31 36 34 39 04 06 0a 7f d4 00	=3891916 49...@...	
					AVP: t=Called-Station-Id(30) l=19 val=50-F7-22-82-D6-16	00f0	17 47 47 69 6f 61 62 69 74 45 74 68 65 72 6e 65	W Gigabit tEthere	
						0100	70 31 2f 30 2f 32 32 3d 06 00 00 00 0f 05 06 00	tl/0/22=	
						0110	00 c4 3c 1f 13 42 34 2d 39 36 2d 39 31 2d 32 36	...B4- 96-91-26	
						0120	2d 44 44 2d 45 37 1e 13 35 30 2d 46 37 2d 32 32	-DD-E7- 50-F7-22	
						0130	2d 42 32 2d 44 36 2d 31 36 1a 3c 00 00 00 00 00	-B2-06-1 6 < >	
						0140	36 72 61 64 69 35 73 3a 51 70 78 2d 6b 65 79 3d	radius: app-key=	
						0150	00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00		
						0160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
						0170	00 00 00 00 1a 3c 00 00 00 09 01 36 72 61 64	radius: <...brad	
						0180	69 75 73 3a 72 61 6e 64 6f 6d 62 6e 6f 6e 63 65	ius:rand om-nonce	
						0190	3d 10 9a 47 63 82 3f 2b 6a 47 e9 47 de 2b 3a 38	= GC 7+ j...+ 8	
						01a0	de 65 85 de da b8 3a 1f 0e fc 46 3c 99 31 06 40	- = GC 7+ j...+ 8	
						01b0	41 1a 4f 00 00 00 09 01 49 72 61 64 69 75 73 3a	A 0...radius: A	
						01c0	6d 65 73 73 61 67 65 2d 61 75 74 68 65 6e 74 69	message- authenti	
						01d0	63 61 74 6f 72 2d 63 6f 64 65 3d 00 00 00 00 00	cator-co de=...	
						01e0	00 00 00 00 00 00 00 00 00 00 00 27 c8 4e 5d	[N]	
						01f0	71 06 47 8c f9 c7 a5 d0 d7 2c ac e2 b9 f2 3b 1f	q G... ..,	

Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=1abpan02/530700707/539,Calling

[illegible]

```

24 0      10.127.197.165      10.127.212.64      RADIUS      482 Access-Accept id=184
> User Datagram Protocol, Src Port: 1812, Dst Port: 58199
> RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xb8 (184)
  Length: 440
  Authenticator: c1b1215db8612f588ebcf23383ca2d81
  [This is a response to a request in frame 231]
  [Time from request: 0.085991000 seconds]
  Attribute Value Pairs
    > AVP: t=User-Name(1) l=10 val=sksarkar
    > AVP: t=Class(25) l=54 val=434143533a3430434374630413030303030323939353944453144393a6c61627
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
    > AVP: t=EAP-Key-Name(102) l=67 val=031g0=0'0T0\0050\005\02300H13\0232\017\00000E0=0\t00\fb0y~
      Type: 102
      Length: 67
      EAP-Key-Name: \031g0=0'0T0\0050\005\02300H13\0232\017\00000E0=0\t00\fb0y~gW600P=0e0Ug\xnTlf
    > AVP: t=Vendor-Specific(26) l=144 vnd=ciscoSystems(9)
      Type: 26
      Length: 144
      Vendor ID: ciscoSystems (9)
      VSA: t=Cisco-AVPair(1) l=138 val=radius:app-key=00000000000000100000000000000000
        Type: 1
        Length: 138
        Cisco-AVPair: radius:app-key=
    > AVP: t=Vendor-Specific(26) l=60 vnd=ciscoSystems(9)
      Type: 26
      Length: 60
      Vendor ID: ciscoSystems (9)
      VSA: t=Cisco-AVPair(1) l=54 val=radius:random-nonce=Y001\02600q0F0*/ZczH0\0210\000b\0T0:
        Type: 1
        Length: 54
        Cisco-AVPair: radius:random-nonce=Y001\02600q0F0*/ZczH0\0210\000b\0T0:
    > AVP: t=Vendor-Specific(26) l=79 vnd=ciscoSystems(9)
      Type: 26
      Length: 79
      Vendor ID: ciscoSystems (9)
      VSA: t=Cisco-AVPair(1) l=73 val=radius:message-authenticator-code=000000000000000000000000
        Type: 1
        Length: 73
        Cisco-AVPair: radius:message-authenticator-code=

```

1) Does RADIUS KeyWarp need to be enabled on both Network device and ISE to make it work?

2) Does enabling KeyWrap increase the resource utilization on the ISE and Network device?

3) How much extra security does RADIUS KeyWrap provide?

Reference

- Cisco Vendor-Specific RADIUS Attributes for the Delivery of Keying Material