Configure RADIUS KeyWrap in ISE

Contents

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 use 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

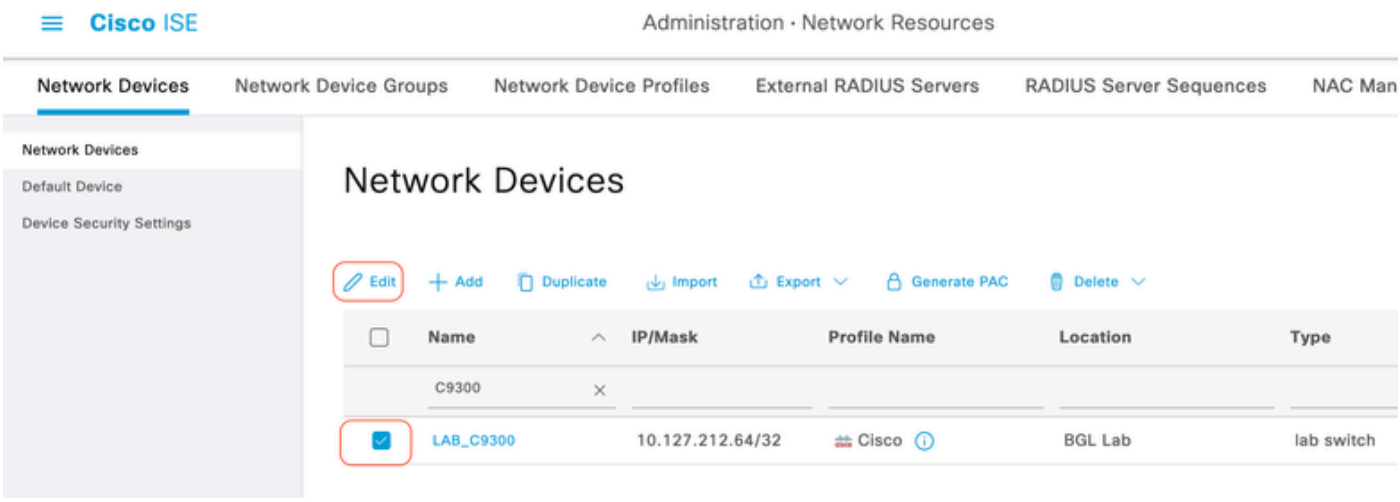
material that secure digital content, particularly in a large-scale enterprise-level network.

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).



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

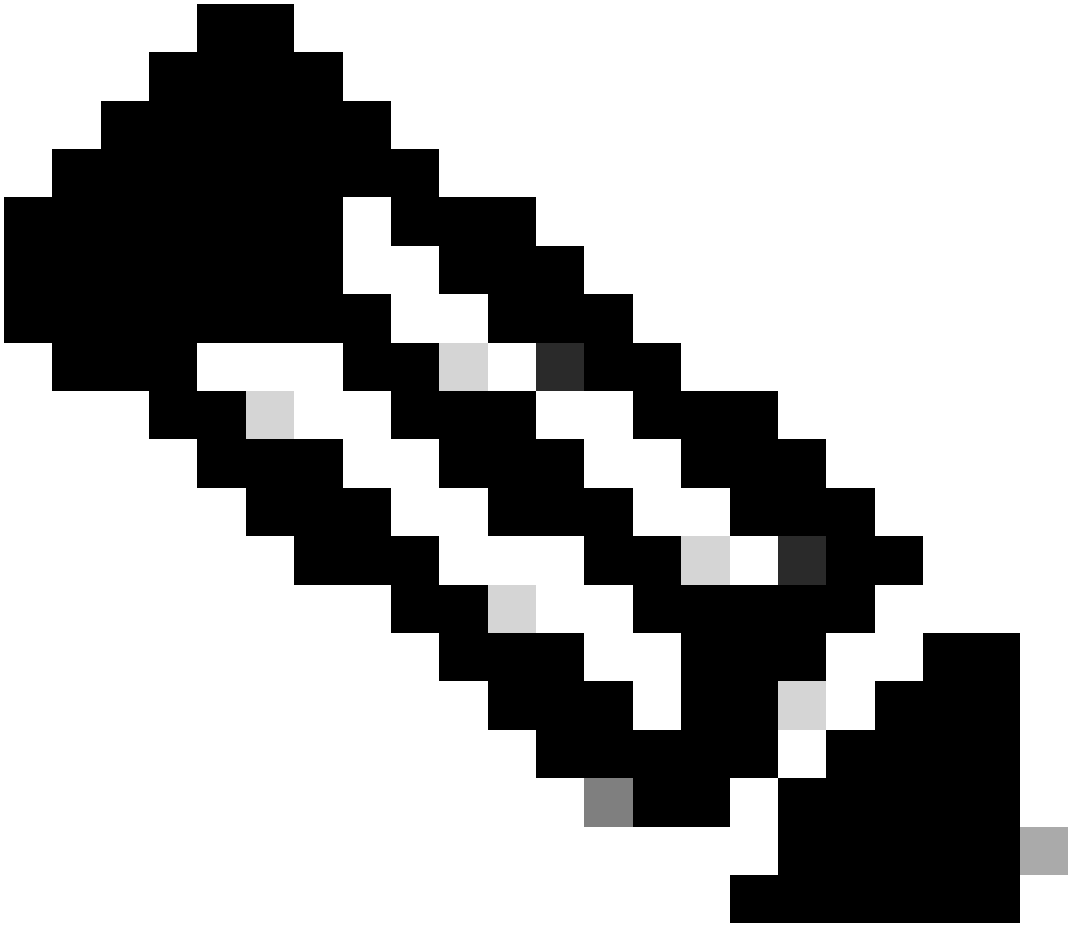
Enable KeyWrap

Key Encryption Key 22AB0###CA#1b2b1 Hide

Message Authenticator Code Key 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.

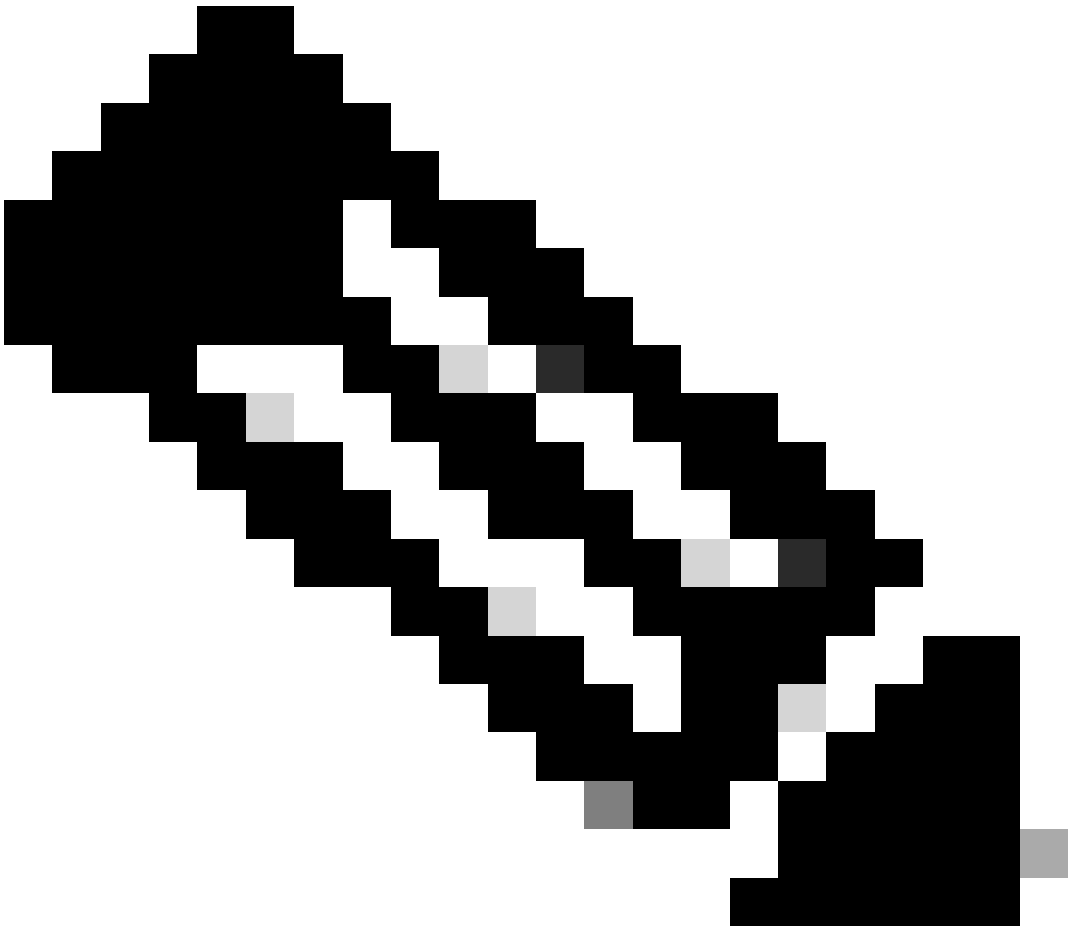
```
aaa authentication dot1x default group RADGRP
aaa authorization network default group RADGRP
aaa accounting dot1x default start-stop group RADGRP

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
```

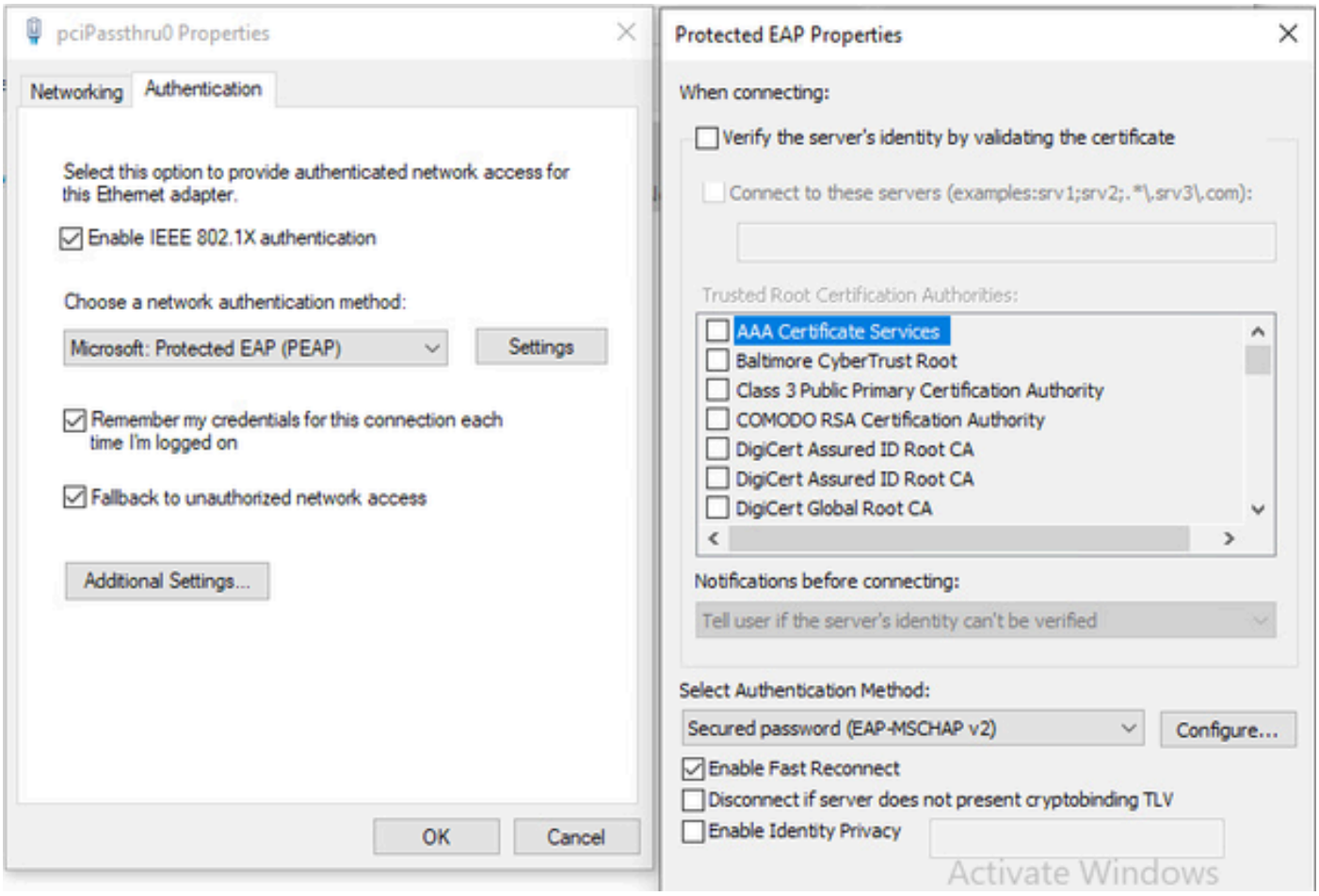
```
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



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

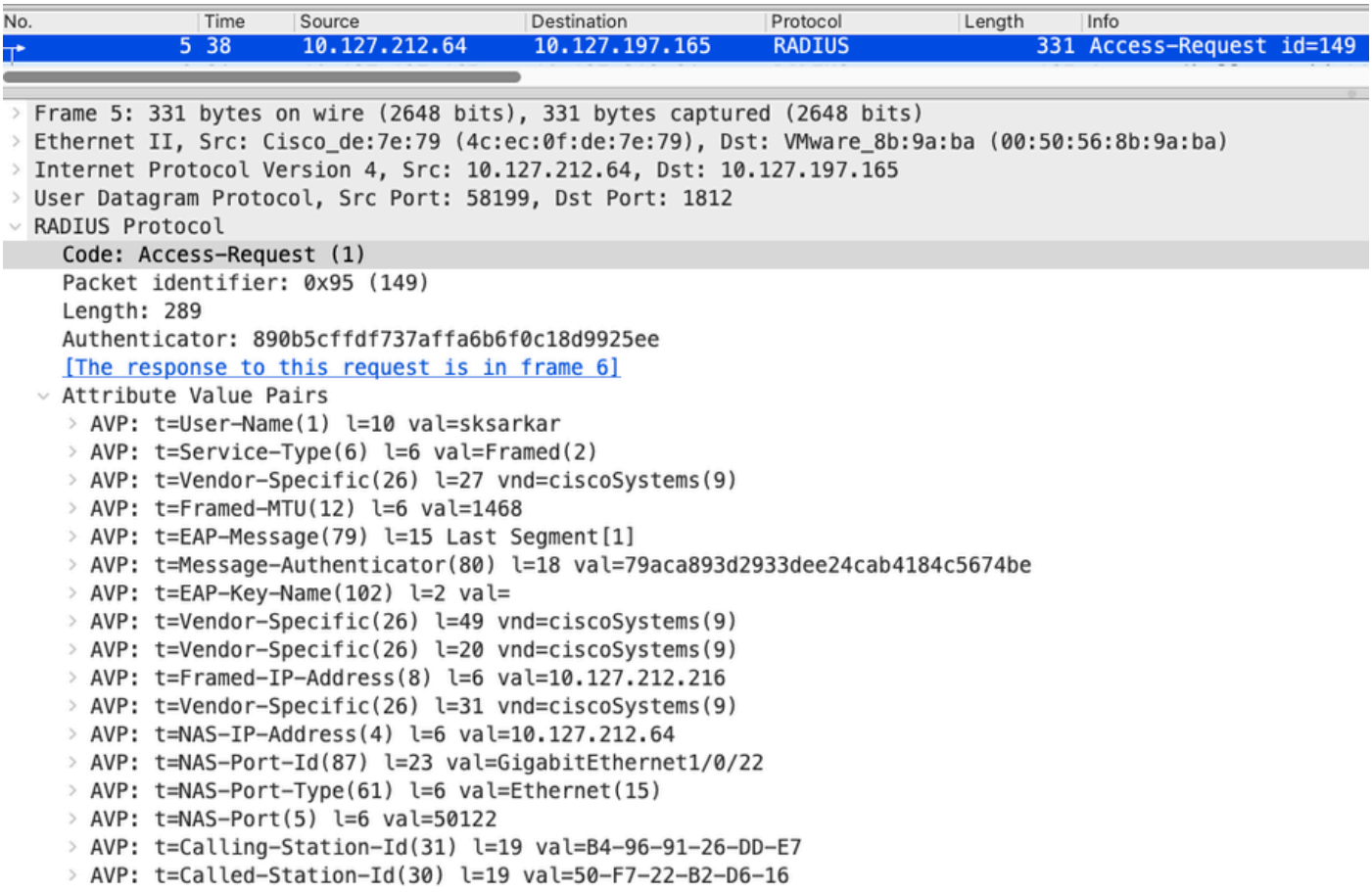
When the RADIUS KeyWrap feature is not enabled on Switch:

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.

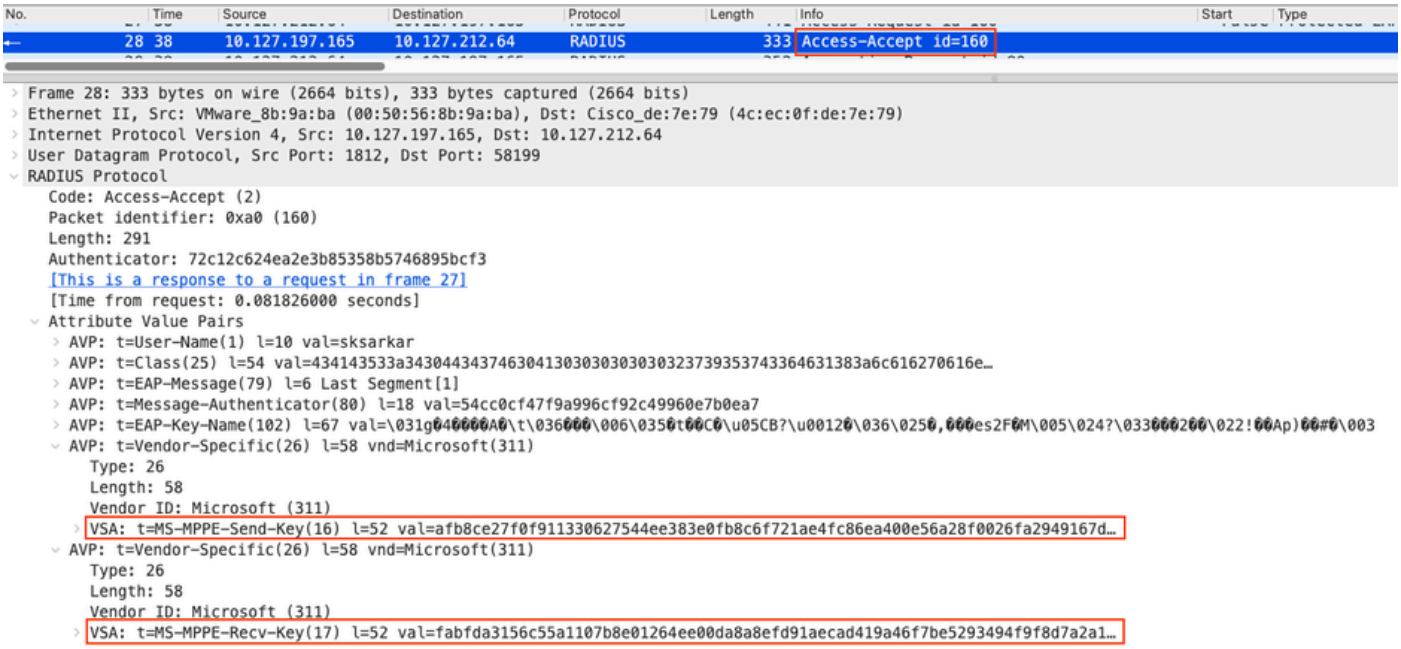


In the ISE prrt-server.log, you can see that ISE only validates the integrity attribute which is the Message-Authenticator.

```
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-iif-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.



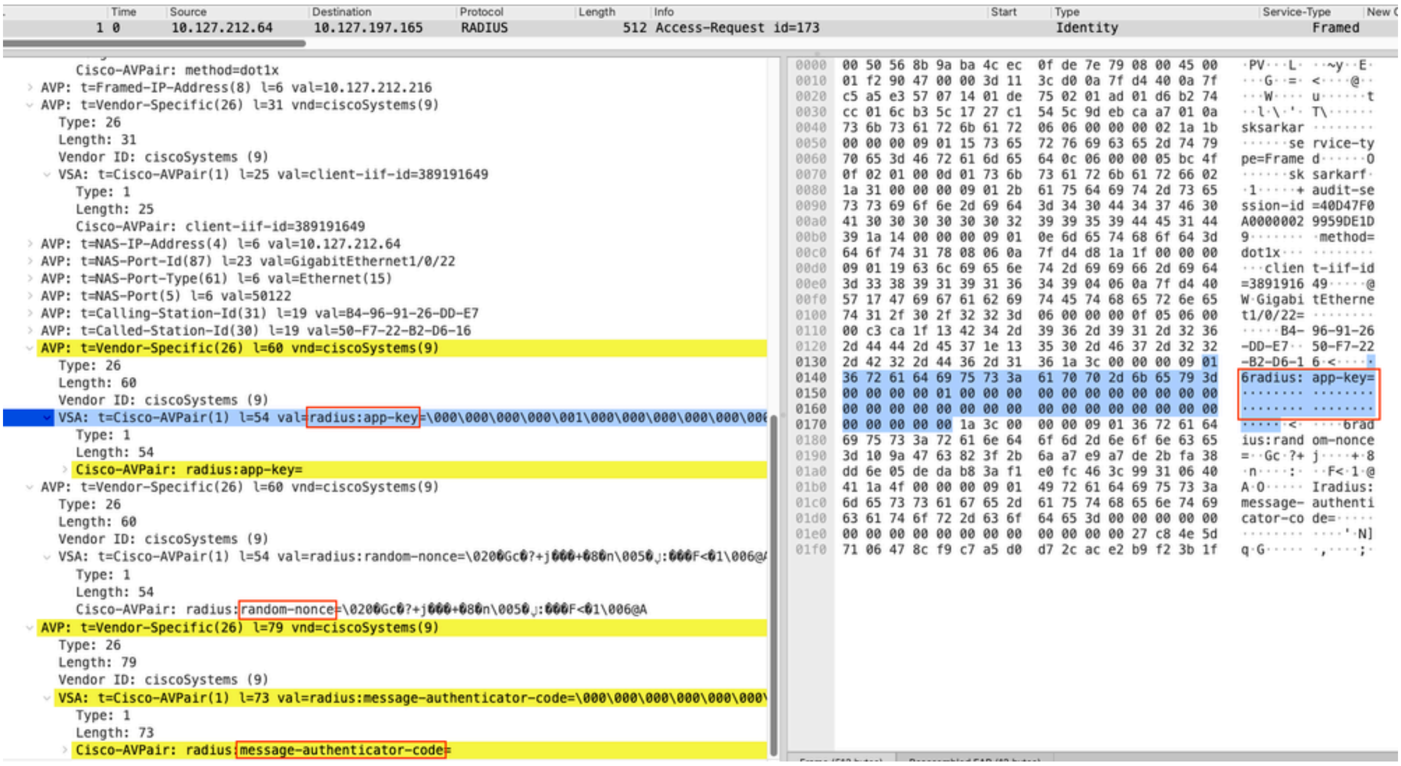
When the RADIUS KeyWrap feature is enabled on Switch and ISE:

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.

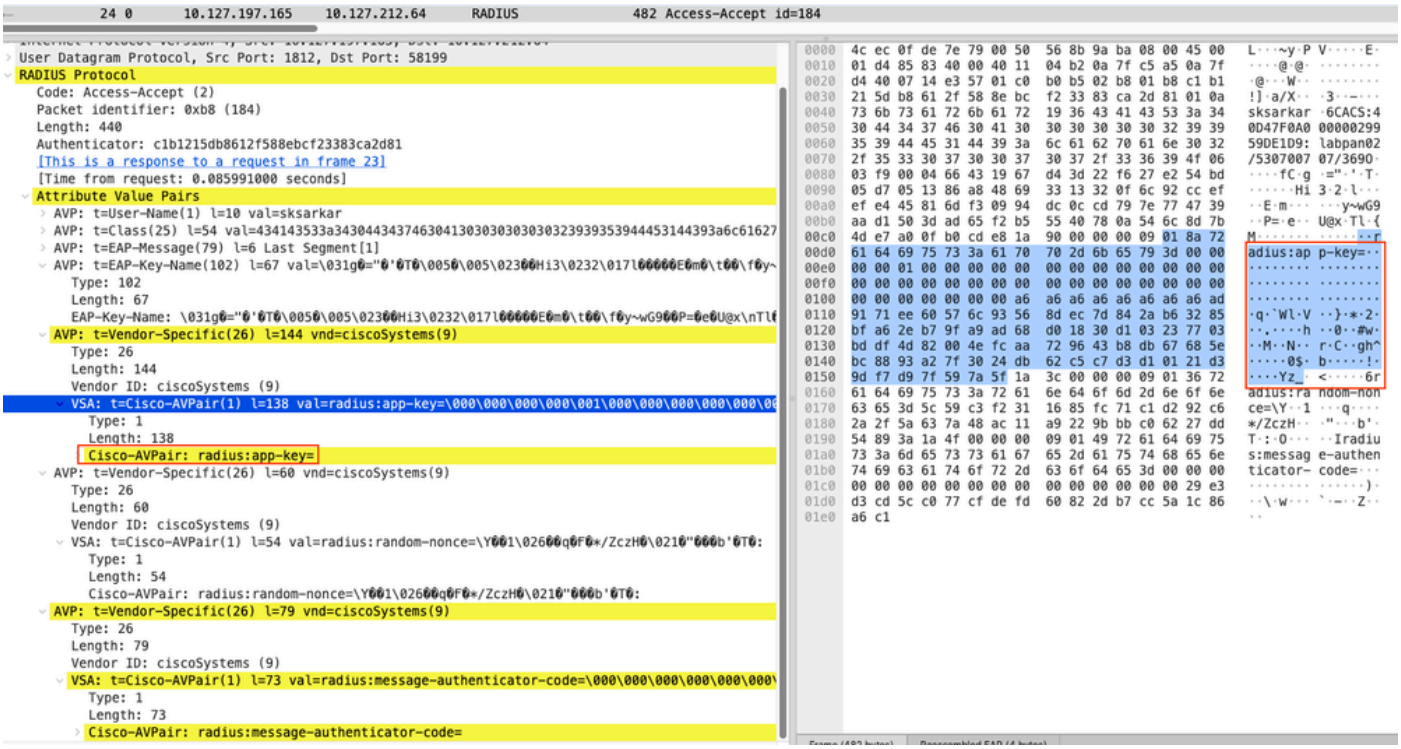


In the ISE prrt-server.log, you can see that ISE validates the attributes app-key, and that random-nonce and message-authenticator-code came in the ACCESS-REQUEST packet.

```
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,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]
[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]
[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=40D47F0A000000319E1CAEFD]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=293712201]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
```

In the Access-Accept packet, you can see that the encrypted key materials in the app-key attribute along with a random-nonce and message-authenticator-code. These attributes were designed to provide stronger

protection and more flexibility than the currently defined Vendor-Specific MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes.



Frequently Asked Questions

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

Yes, RADIUS KeyWrap needs to be enabled on both both Network device and ISE to make it work. Although, if you enable the KeyWrap only on the ISE but not on the Network Device, authentication still works. But, if you enabled it on Network Device but not in ISE, authentication fails.

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

No, there no significant increase in resource utilization on the ISE and Network device after enabling KeyWrap.

3) How much extra security does RADIUS KeyWrap provide?

As, the RADIUS itsself does not provides any encryption to its payload, KeyWrap provides extra security by encrypting the key materials. The level of security depends on which encryption algorithm is used to encrypt the key material. In ISE, AES is used to encrypt the key material.

Reference

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