

在ISE中配置RADIUS金鑰包

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[ISE](#)

[交換器](#)

[PC](#)

[驗證](#)

[常見問題](#)

[參考](#)

簡介

本文檔介紹在思科ISE和思科交換機中配置RADIUS金鑰包裝的過程。

必要條件

- Dot1x知識
- 瞭解RADIUS通訊協定
- EAP知識

採用元件

- ISE 3.2
- 思科C9300-24U與軟體版本17.09.04a
- Windows 10 PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

金鑰包裝技術使用另一個金鑰加密一個金鑰值。RADIUS中使用相同的機制來加密金鑰材料。此材料通常作為可擴充驗證通訊協定(EAP)驗證的副產品產生，並在成功驗證後返回到Access-Accept訊息。如果ISE在FIPS模式下運行，此功能是必需的。

這提供了一個保護層，該層將實際的關鍵材料隔離起來，以防範潛在的攻擊。即使是在資料攔截的情況下，威脅方實際上也無法訪問底層關鍵材料。RADIUS金鑰包裝的主要目的是防止安全數位內

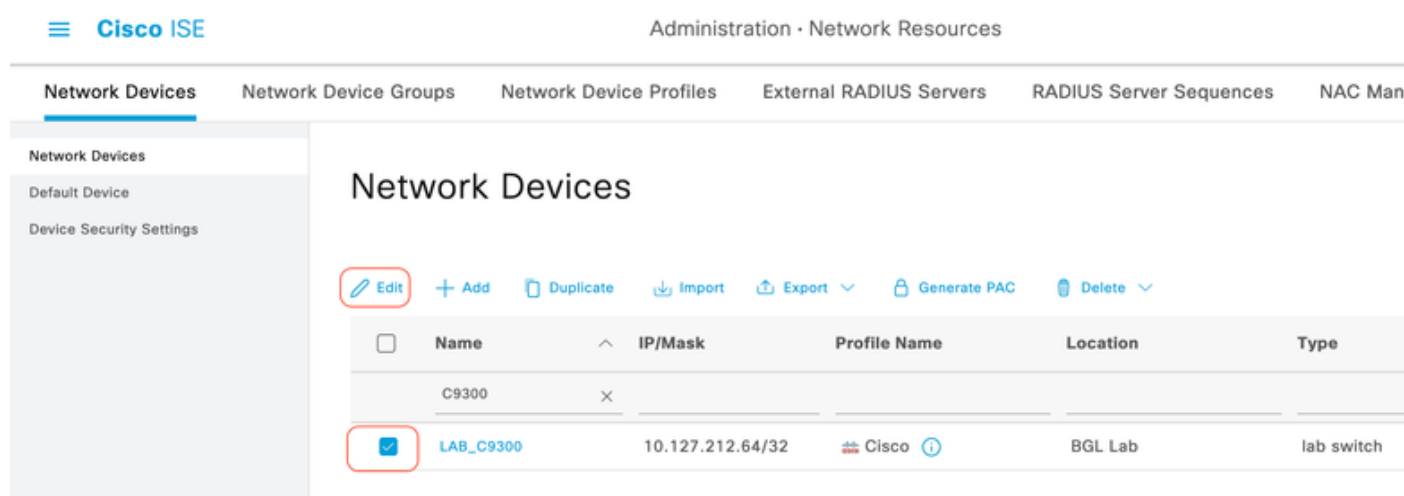
容的關鍵材料的曝光，特別是在大規模的企業級網路中。

在ISE中，金鑰加密金鑰用於使用AES加密和從RADIUS共用金鑰分離的消息驗證器代碼金鑰來加密金鑰材料，以便生成消息驗證器代碼。

設定

ISE

步驟 1:導覽至Administration > Network Resources > Network Devices。按一下要為其配置RADIUS KeyWrap的網路裝置的覈取方塊。按一下Edit (如果已新增網路裝置)。



The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > Network Resources. The left sidebar shows the 'Network Devices' menu. The main content area is titled 'Network Devices' and contains a table of devices. The 'Edit' button and the checkbox for the device 'LAB_C9300' are highlighted with red boxes.

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

步驟 2:展開RADIUS身份驗證設定。按一下Enable KeyWrap覈取方塊。輸入密鑰加密金鑰和消息驗證器代碼金鑰。按一下「Save」。

General Settings

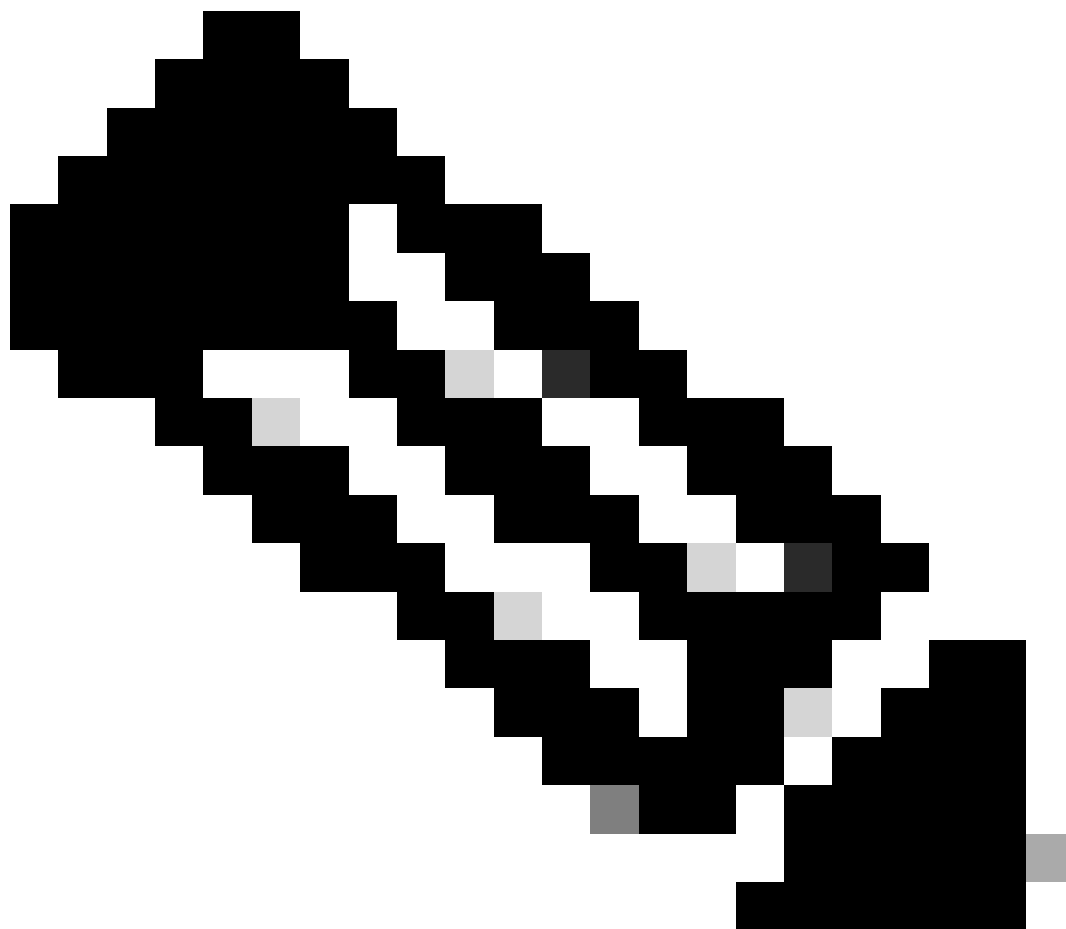
☒ Enable KeyWrap ⓘ

Key Encryption Key 22AB0###CA#1b2b1 [Hide](#)

Message
Authenticator Code 12b1CcB202#2Cb1#bCa# [Hide](#)
Key

Key Input Format

☒ ASCII ☐ HEXADECIMAL



注意：金鑰加密金鑰和消息驗證程式碼金鑰必須不同。

交換器

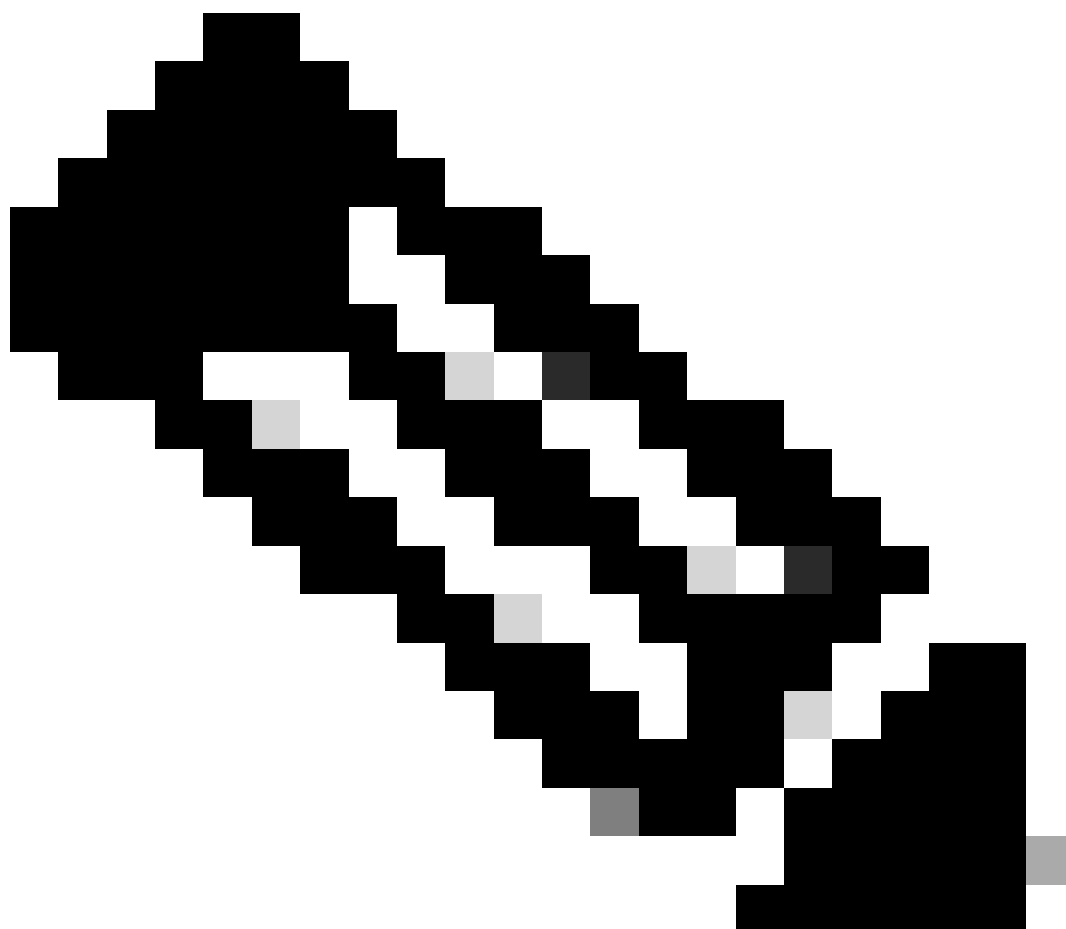
交換機中的AAA配置啟用RADIUS KeyWrap功能。

```
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
```

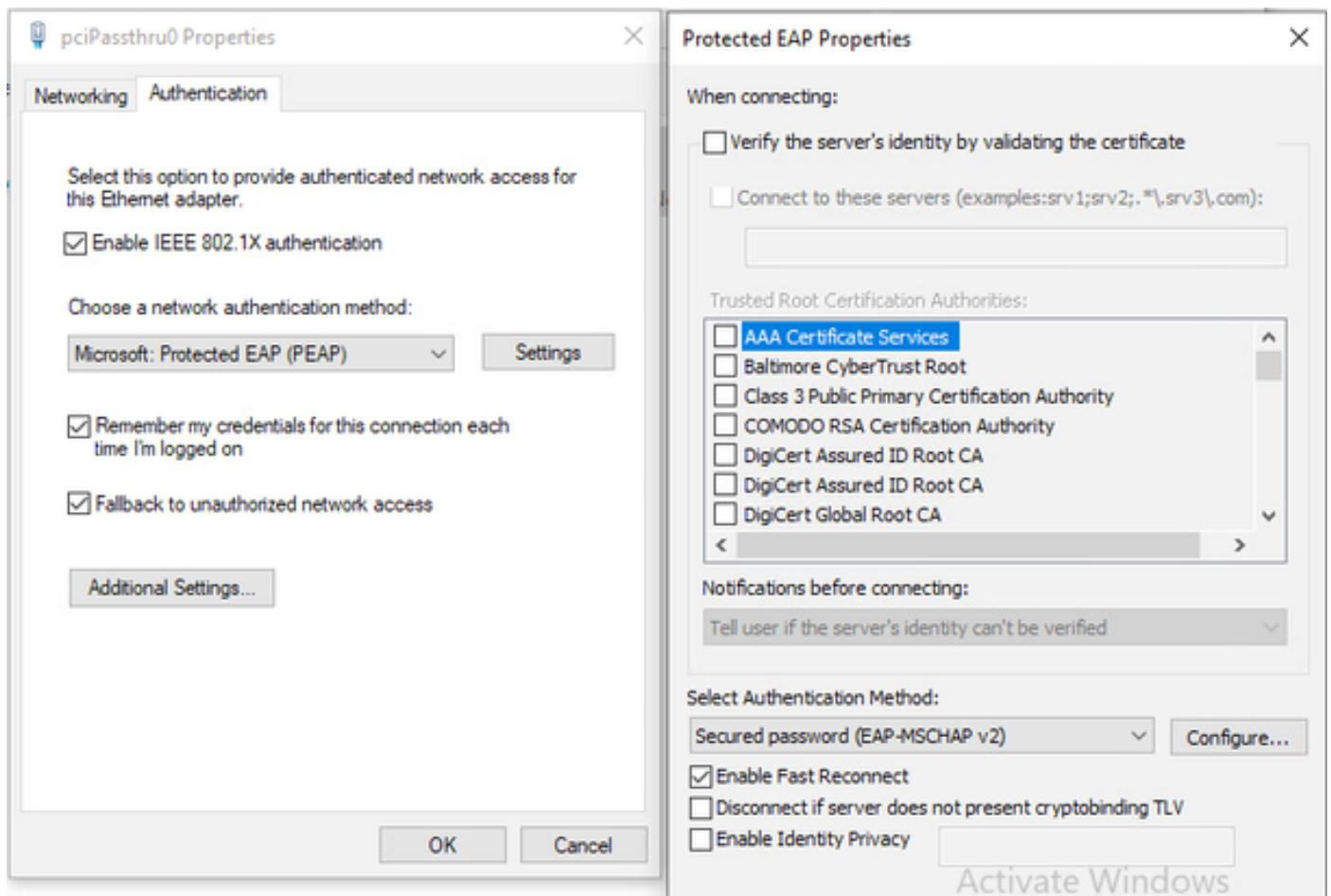
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



附註：Encryption-key的長度必須為16個字元和message-auth-code以及20個字元的長度。

PC

為PEAP-MSCHAPv2配置的Windows 10請求方。



驗證

在Switch：上未啟用RADIUS KeyWrap功能時：

show radius server-group <伺服器組名稱>

命令輸出必須顯示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
```

在資料包捕獲中，您可以看到app-key、random-nonce和separate message-authenticator-code沒有Cisco-AV-Pair屬性。這表示交換器上已停用RADIUS KeyWrap。

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: 890b5cffdf737affa6b6f0c18d9925ee [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						

在ISE prrt-server.log中，您可以看到ISE僅驗證完整性屬性，即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
```

|

>

<18><06>(

?

```

]
[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=1abpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=1abpan02/530700707/490,Calling

```

在Access-Accept資料包中，可以看到MS-MPPE-Send-key和MS-MPPE-Recv-Key從RADIUS伺服器傳送到身份驗證器。MS-MPPE指定EAP方法生成的金鑰材料，可用於在對等方和驗證方之間執行資料加密。這些32位元組的金鑰是從RADIUS共用金鑰、請求驗證器和隨機鹽派生的。

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=\031g040000A0\t\036000\006\0350t00C0\u05CB?\u00120\036\0250,000es2F0M\005\024?\033000200\022!00Ap)00#0\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=fabfda3156c55a1107b8e01264ee00da8a8efd91aecad419a46f7be5293494f9f8d7a2a1...								

當在交換機和ISE上啟用RADIUS金鑰包裝功能時：

show radius server-group <伺服器組名稱>

```
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
```

在資料包捕獲中，您可以看到app-key（無資料）、random-nonce和單獨的message-authenticator-code存在Cisco-AV-Pair屬性。這向RADIUS伺服器指出驗證器（交換器）支援RADIUS KeyWrap，但伺服器必須使用。

[illegible]

在ISE prrt-server.log中，您可以看到ISE驗證屬性app-key，並且random-nonce和message-authenticator-code出現在ACCESS-REQUEST資料包中。

```
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]
```

[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 23] [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=434143533a34304434374630413030303030303239393539444531444393a6c61627						
AVP: t=EAP-Message(79) l=6 Last Segment[1]						
AVP: t=EAP-Key-Name(102) l=67 val=\031g\0="0'0T0\0050\005\02306H13\0232\017L0000E0m\0t0\0fy~ Type: 102 Length: 67 EAP-Key-Name: \031g\0="0'0T0\0050\005\02306H13\0232\017L0000E0m\0t0\0fy~wG06P=0eUgx\nTLf						
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=\000\000\000\000\001\000\000\000\000\000\000 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'T0: Type: 1 Length: 54 Cisco-AVPair: radius:random-nonce=\Y001\02600q0F0*/ZczH0\0210"000b'T0:						
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=\000\000\000\000\000\000\000 Type: 1 Length: 73 Cisco-AVPair: radius:message-authenticator-code=						

不，啟用KeyWrap後，ISE和網路裝置的資源利用率沒有顯著提高。

3)RADIUS KeyWrap提供多少額外安全性？

因為RADIUS本身不向其負載提供任何加密，KeyWrap透過加密金鑰資料提供額外的安全性。安全級別取決於使用哪種加密演算法加密金鑰材料。在ISE中，AES用於加密金鑰材料。

參考

- [交付金鑰材料的思科供應商特定RADIUS屬性](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。