

Configurar KeyWrap RADIUS no ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[ISE](#)

[Switch](#)

[PC](#)

[Verificar](#)

[Perguntas mais freqüentes](#)

[Referência](#)

Introdução

Este documento descreve o procedimento para configurar RADIUS KeyWrap no Cisco ISE e no Cisco Switch.

Pré-requisitos

- Conhecimento de dot1x
- Conhecimento do protocolo RADIUS
- Conhecimento de EAP

Componentes Utilizados

- ISE 3.2
- Cisco C9300-24U com versão de software 17.09.04a
- PC com Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A quebra de chaves é uma técnica em que um valor de chave é criptografado usando outra chave. O mesmo mecanismo é usado no RADIUS para criptografar o material da chave. Esse material é geralmente produzido como um subproduto de uma autenticação EAP (Extensible

Authentication Protocol) e retornado na mensagem Access-Accept após uma autenticação bem-sucedida. Esse recurso será obrigatório se o ISE estiver sendo executado no modo FIPS.

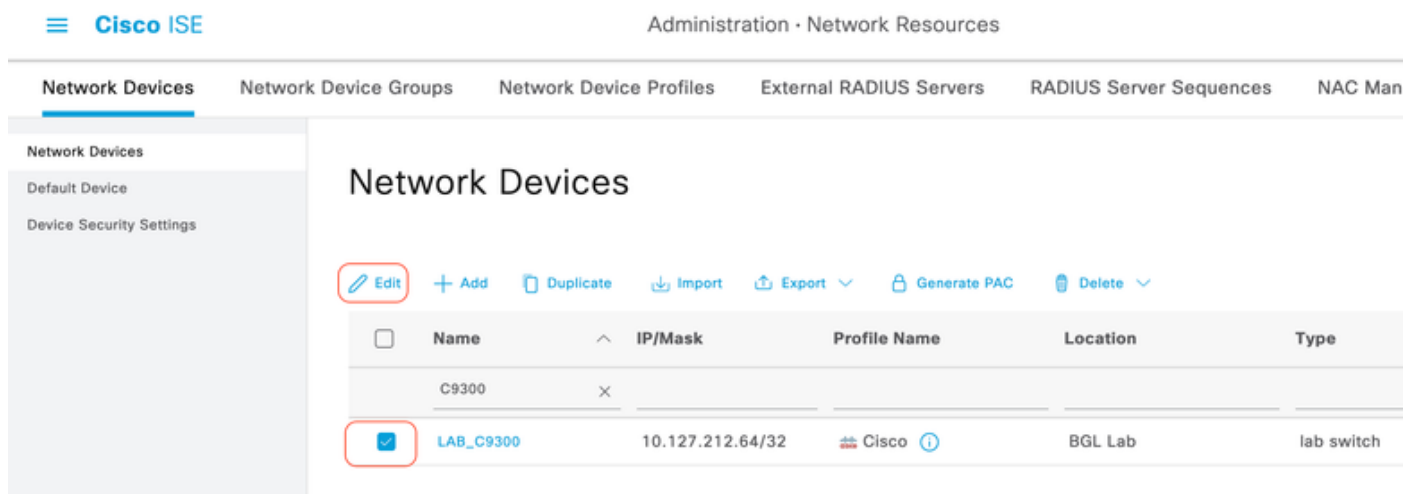
Isso fornece uma camada de proteção que isola o material-chave real para proteção contra ataques potenciais. O material essencial subjacente torna-se praticamente inacessível aos agentes de ameaças, mesmo em casos de interceptação de dados. A principal intenção por trás do encapsulamento de chaves RADIUS é evitar a exposição de materiais-chave que protegem o conteúdo digital, particularmente em uma rede de grande escala de nível empresarial.

No ISE, a chave de criptografia é usada para criptografar os materiais da chave com a criptografia AES e a chave do código do autenticador de mensagem separada da chave secreta compartilhada RADIUS para gerar o código do autenticador de mensagem.

Configurar

ISE

Passo 1: Navegue até Administração > Recursos de rede > Dispositivos de rede. Clique na caixa de seleção do dispositivo de rede para o qual você deseja configurar RADIUS KeyWrap. Clique em Editar (se o dispositivo de rede já tiver sido adicionado).



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration · Network Resources'. The main navigation tabs are 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'NAC Man'. The left sidebar shows 'Network Devices' with sub-items '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 has two rows: 'C9300' and 'LAB_C9300'. The 'LAB_C9300' row is selected, and its selection checkbox is highlighted with a red box. The 'LAB_C9300' row shows an IP/Mask of '10.127.212.64/32', a Profile Name of 'Cisco', a Location of 'BGL Lab', and a Type of 'lab switch'.

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

Passo 2: Expanda as Configurações de Autenticação RADIUS. Clique na caixa de seleção Enable KeyWrap. Insira a chave de criptografia de chave e a chave do código do autenticador de mensagem. Click Save.

General Settings

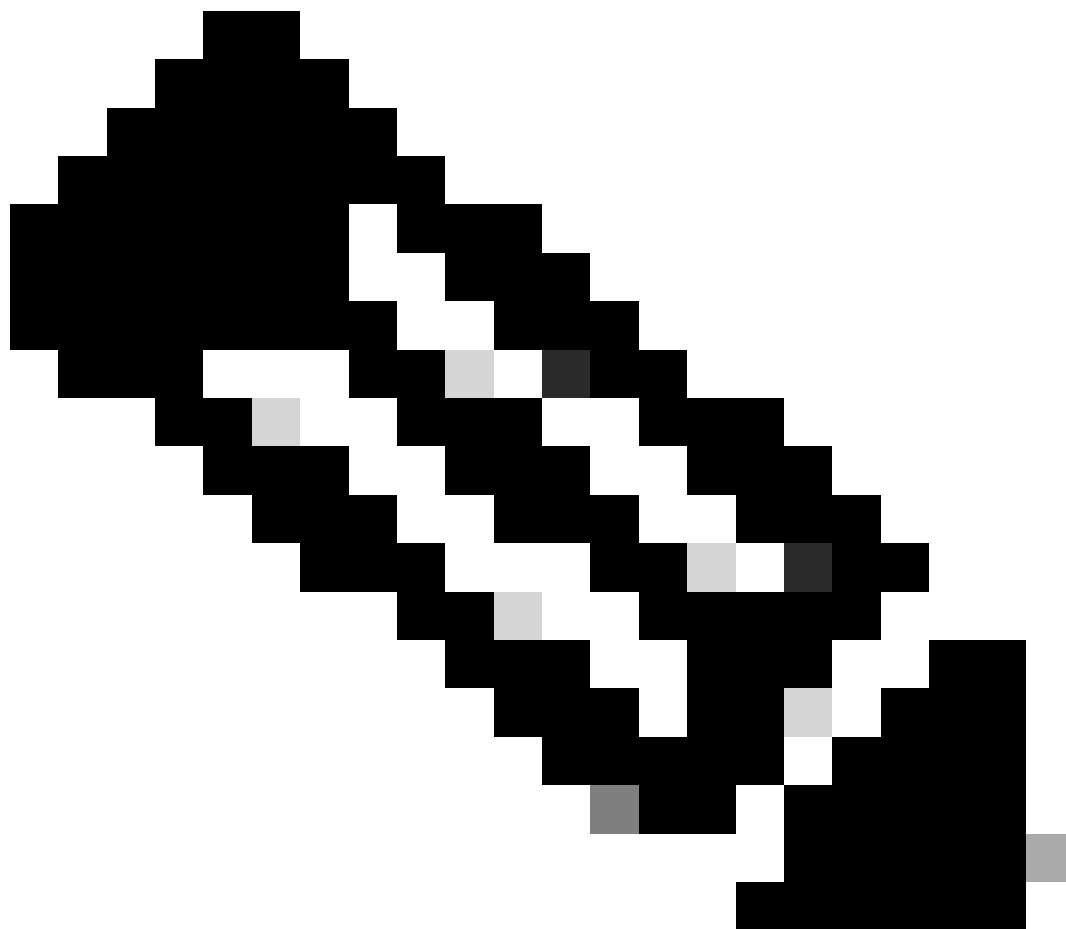
☒ Enable KeyWrap 

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

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

Key Input Format

☒ ASCII ☐ HEXADECIMAL



Observação: a Chave de Criptografia da Chave e a Chave do Código do Autenticador de Mensagem devem ser diferentes.

Switch

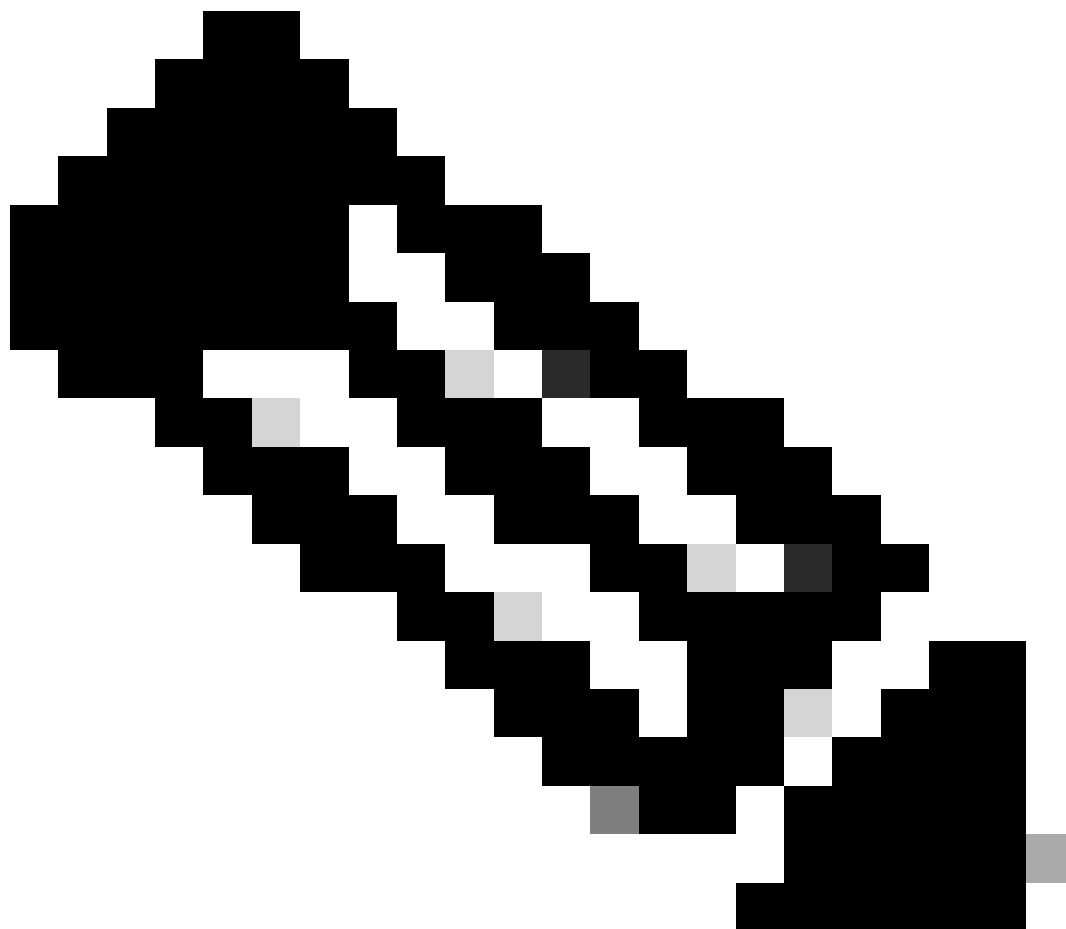
Configuração AAA no Switch para habilitar o recurso KeyWrap RADIUS.

```
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
```

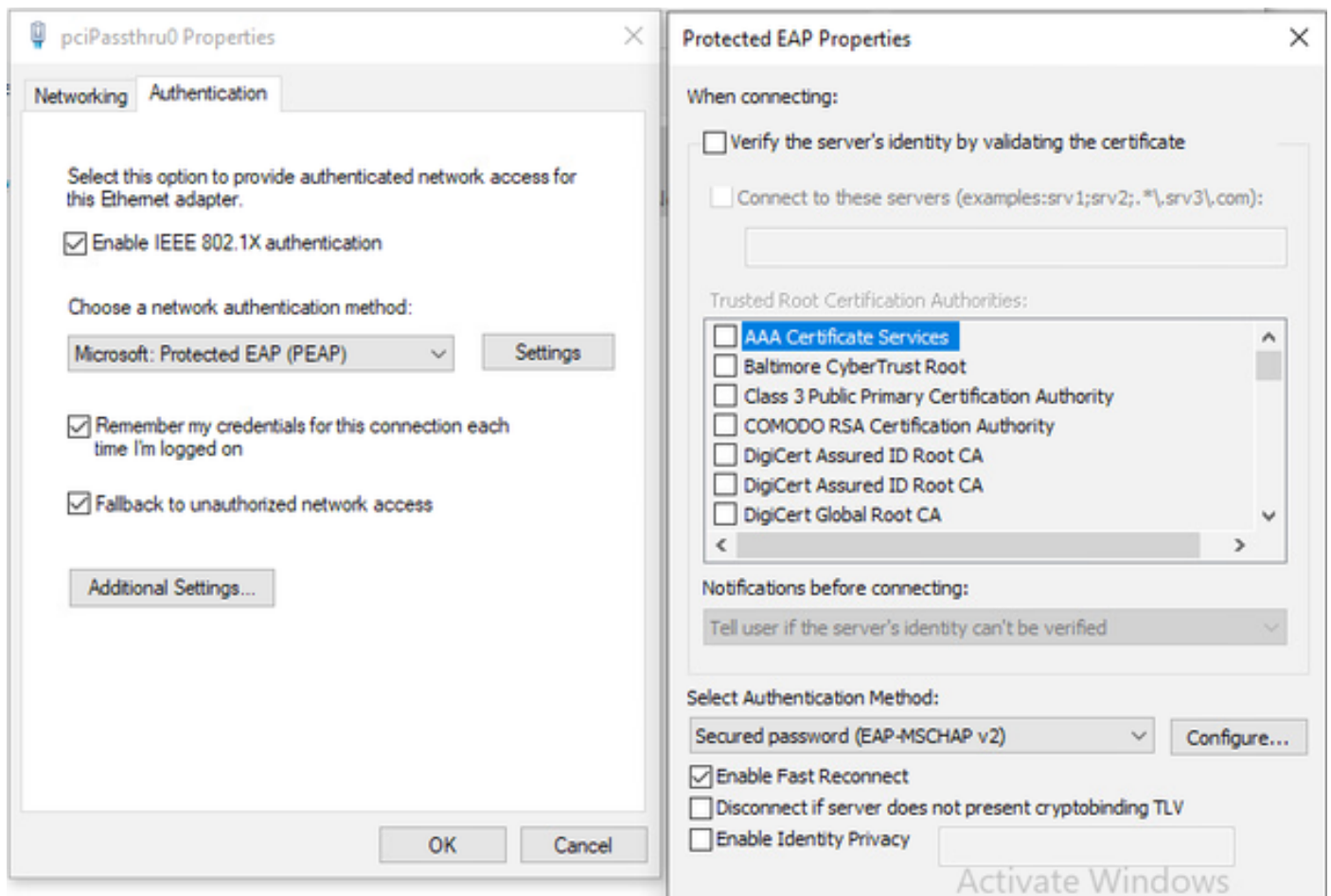
```
interface GigabitEthernet1/0/22
switchport access vlan 302
switchport mode access
device-tracking attach-policy IPDT
authentication host-mode multi-domain
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
end
```



Note: A chave de criptografia deve ter 16 caracteres e o código de autenticação de mensagem e 20 caracteres.

PC

Windows 10 Supplicant configurado para PEAP-MSCHAPv2.



Verificar

Quando o recurso KeyWrap do RADIUS não estiver habilitado no Switch:

show radius server-group <SERVER GROUP NAME>

A saída do comando deve mostrar Keywrap habilitado: FALSO.

```
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
```

Na captura de pacotes, você pode ver que não há atributo Cisco-AV-Pair para app-key, random-nonce e message-authenticator-code separado. Isso indica que RADIUS KeyWrap está desabilitado no 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: 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						

No arquivo prt-server.log do ISE, você pode ver que o ISE valida somente o atributo de integridade que é o Autenticador de mensagem.

```
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=labpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling

```

No pacote Access-Accept, você pode ver que a chave MS-MPPE-Send-key e a chave MS-MPPE-Recv-Key são enviadas do Servidor RADIUS para o Autenticador. O MS-MPPE especifica o material-chave gerado pelos métodos EAP que podem ser usados para executar a criptografia de dados entre o peer e o Authenticator. Essas chaves de 32 bytes são derivadas do segredo compartilhado RADIUS, do autenticador de solicitação e de um salt aleatório.

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_de7e: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=\031g00000000\t\036000\006\0350t00C0\005CB7\00120\036\0250\000es2F0M\005\0247\033000200\022!00Ap)0000\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...

```
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]
```

[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=434143533a3430443437463041303030303030323939353944453144393a6c61627
- AVP: t=EAP-Message(79) l=6 Last Segment(1)
- AVP: t=EAP-Key-Name(102) l=67 val=031g0="0'0T0'0050'005'02300H13'0232'017'06000E0m0't00'f0y~
 Type: 102
 Length: 67
 EAP-Key-Name: 031g0="0'0T0'0050'005'02300H13'0232'017'06000E0m0't00'f0y~wG900P=0e0Ux\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*/ZczH0'0210'0000'0T0:
 Type: 1
 Length: 54
 Cisco-AVPair: radius:random-nonce=\Y001\02600q0f0*/ZczH0'0210'0000'0T0:
- 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=\000\000\000\000\000\000\000
 Type: 1
 Length: 73
 Cisco-AVPair: radius:message-authenticator-code=

1) O RADIUS KeyWarp precisa ser habilitado no dispositivo de rede e no ISE para que funcione?

funcione. Embora, se você habilitar o KeyWrap somente no ISE, mas não no dispositivo de rede, a autenticação ainda funcionará. Mas, se você o habilitou no dispositivo de rede, mas não no ISE, a autenticação falhará.

2) A ativação do KeyWrap aumenta a utilização de recursos no ISE e no dispositivo de rede?

Não, não há aumento significativo na utilização de recursos no ISE e no dispositivo de rede após a habilitação de KeyWrap.

3) Quanto de segurança extra o RADIUS KeyWrap fornece?

Como o próprio RADIUS não fornece nenhuma criptografia para sua carga útil, o KeyWrap fornece segurança extra ao criptografar os materiais da chave. O nível de segurança depende do algoritmo de criptografia usado para criptografar o material da chave. No ISE, o AES é usado para criptografar o material da chave.

Referência

- [Atributos RADIUS específicos do fornecedor da Cisco para a entrega de material de chaveamento](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.