

مادختساب MACsec لوجملا فيضم ريفشت ISE و Cisco AnyConnect نيوكت لاثم

تايوتحملا

[عمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[نيوكتللا](#)

[تانايبللا رورم ةكرح قفدتو ةكبش لل يطيطختلا مسرلا](#)

[تاننيوكتللا](#)

[\(ISE\) ةيوهلا فشك تامدخ كرحم](#)

[ليدبت](#)

[AnyConnect NAM](#)

[ةحصلا نم ققحتلا](#)

[اهخالص او عاطخألا فاشكتسا](#)

[لمع ويرانيسرل عاطخألا ححصت](#)

[لشاف ويرانيسرل عاطخألا ححصت](#)

[مزحلا طاقتلا](#)

[802.1x و MacSec يعضو](#)

[ةلص تاذ تامولعم](#)

عمدقملا

طئاسولا ىلا لوصولا في مكحتلا ناما ريفشتل نيوكتلل الاثم دنتسملا اذه مدقي مادختسا متي. (لوجم) ةقداصمو (لاوجلل Cisco AnyConnect ناما) 802.1x لي مع نيپ (MACsec) ةسايسلاو ةقداصم لل مداخك Cisco نم (ISE) ةيوهلا تامدخ تاكرحم.

4500 و 3560X و 3750X Cisco تالوجم ىلع معديو 802.1AE راي عم في MACsec ديحوت متي مدختست يتلا ةيكلسلل تاكپشلل ربع طابتراللا ريفشت 802.1ae راي عم ددحي SUP7E. لوكوتورب عم هذه ريفشتلا حيتافم ىلع ضوافتللا متي. يدرتلل قاطنلا چراخ حيتافملا MKA. ةحجانلل 802.1x ةقداصم دعب همادختسا متي يذلا (MKA) MACsec حيتافم ةيقافتا IEEE 802. 1x-2010 في ريعام.

ىلا ةطقن نم ريفشت) لوجملاو رتويبمكلا نيپ طابتراللا ىلع طقف ةمزحلا ريفشت متي ربع اهللاسرالو لوجملا ةطساوب اهللابقتسا متي يتلا ةمزحلا ريفشت كفتي. (ةطقن لوجملا ريفشتب ىصوي، تالوجملا نيپ لاسرالا ريفشتل. ةرفشملا ريغ تالوصولا عم ضوافتلل (SAP) نامال نارثقا لوكوتورب مادختسا متي، ريفشتلا كذل ةبسنلاب Cisco. هتروط ريعاملل قباس حاتفم ةيقافتا لوكوتورب وه SAP. اهئاشن اذاعا و حيتافملا

ةيساسألا تابلطتملا

[تابلطتملا](#)

ةةللالتل عةضاولابل ةفرعم كلدل نوكتل نابل Cisco ةصوت

- 802.1x نةوكتل ةةساسا ةفرعم
- ءاتفم ةزافء ةءام نم لةكشتل ل ءةساساا ةفرعم
- ISE نةوكتل عم ةءءت

ةمدءتسملا تانوكملا

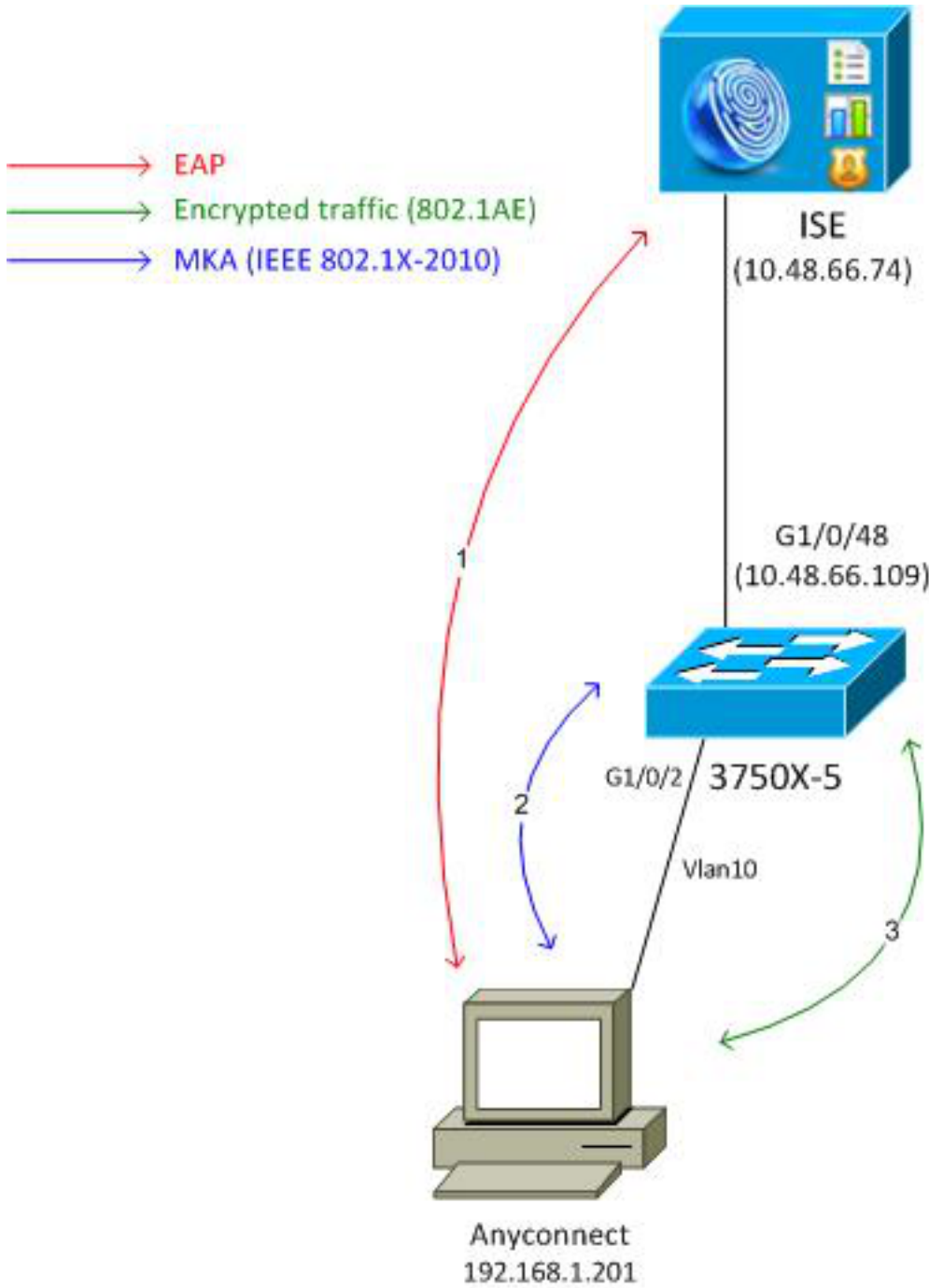
ةةللالتل ةةءامللا تانوكملا وءمءملا تاراءصلا لءل ءنلسملا اءه ةفراولا تامولعملل ءنلسملا

- Microsoft Windows XP و Microsoft Windows 7 لءءشلا ةمظنأ
- ءءءاللا تاراءصلا او 15.0 راءصلا، Cisco 3750X ءمءنرب
- ءءءاللا تاراءصلا او 1.1.4 راءصلا، Cisco ISE ءمءنرب
- راءصلا، (NAM) ةكءشللا لءل لوصولل رءءمءاءءلسماب Cisco AnyConnect Mobile Security ءءءاللا تاراءصلا او 3.1

ءصاءةةلمعم ةئب ةءوءوملا ةزهءاللا نم ءنلسملا اءه ةفراولا تامولعملل ءاشنلءمءل ءنلسملا اءل. ءوسمم نةوكتل ءنلسملا اءه ةمدءتسملا ةزهءاللا ءمءءءءب رملل لءمءءملا رءلءل كءمءف نم ءكأءف، ءرشابم كلءكءبش

نةوكتللا

تاناةلل رورم ءكءء قوءءءو ةكءبشللل ةطءءلل مسرلا



مداخ و ISE و قدصملا وه لوجملا 802.1x لمع ةسلج (AnyConnect NAM) بلاطلا أدبي 1. ةوطخلا ل قنك (EAPOL) لوكوتورب ربع ةسوتملا ةقداصملا لوكوتورب مادختسا متي. ةقداصملا ال ISE و لوجملا نبي EAP ل قن لوكوتوربك RADIUS مدختسي. لوجملا او بلاطلا نبي EAP ل ISE نم EAPOL حيتافم عاجرا بجي هنال ارظن، (MAB) MAC ةقداصم زواجت مادختسا نكمي (MKA) "MacSec" حاتفم ةيقافتا" لمع ةسلجل اهمادختساو.

2. ةوطخلا EAPOL مادختسا اب MKA ةسلج لوجملا أدبي، 802.1x لمع ةسلج لامتك دع ب. AES-ري فشتلا حيتافم قباطت، حيص لكشب بلاطملا نيوكت مت اذا. ل قن لوكوتوربك 128-ب-لثامتملا (Galois/دادعلا عضو) AES-GCM.

3. ةوطخلا (802.1ae ني مضا) لوجملا وهجوملا نبي ةيلالاتل مزجال عي مج ري فشت متي.

تانبيوكتلا

(ISE) ةيوهلا فشك تامدخ كرحم

ليوختال فيرعت فللم ءانثتسا عم 802.1x قودب ايجذومن ويرانيس ISE نيوكت نمضتي ريفشت تاسايس نمضتي دق يذلاو

حاتفم لخدأ. ءادأ ءكبشك حاتفملا تفضأ in order to ءادأ ءكبش > دروم ءكبش > ءرادإ ترتخأ (كرتشم رس) اقبس م كرتشملا RADIUS.

Network Devices List > 3750-5

Network Devices

* Name: 3750-5

Description:

* IP Address: 10.48.66.109 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations (Set To Default)

Device Type: All Device Types (Set To Default)

Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: [Masked Password] (Show)

(ISE) لىل ع ايلحم ني ددحملا ني مدختس ملل) ءيضا رتفالال ءق داصملا ءدعاق مادختسا نكمي

اي لحم "cisco" لمعتسملال تني ع in order to لمعتسم > ءرادإ ءي وه > ءرادإ ترتخأ

Identities

Network Access Users List > New Network Access User

Network Access User

* Name: cisco

Status: Enabled

Email:

Password

* Password: [Masked Password] (Need help with password policy ?)

* Re-Enter Password: [Masked Password]

رتخأ، لاثملا اذ ءي حضوم وه امك. ريفشت تاسايس ليوختال فيرعت فلم نمضتي دق ربت عي يذلا ل وحملا لىل ءعجرت ملام ISE تامولعم ضرع Policy > Results > Authorization Profile ت لكش نوكي ىقلتتي (10) مقر VLAN ل، اضيا. ايامزلا طابترالا ريفشت

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active, showing a search bar and a navigation tree on the left. The tree is expanded to 'Authorization Profiles'. The main content area shows the configuration for the 'MACSECprofile' authorization profile. The 'Name' field is 'MACSECprofile', and the 'Access Type' is 'ACCESS_ACCEPT'. The 'Service Template' checkbox is unchecked. Under 'Common Tasks', the 'MACSec Policy' checkbox is checked, and its value is set to 'must-secure'.

لا ثم لما اذ ع جري . لي وخت لا ءدع اق ي ف لي وخت لا في رت فلم م ادخت سال ضي وفت > ج ه رت خأ ع جري ISE ن ا ف ، 802.1x ل و ح م ل ا ح ج ن ا ذ ا . "cisco" م د خ ت س م ل ل ه ن ي و ك ت م ت ي ذ ل ا ف ي ر ت ل ا ف ل م ع ج ر ي C i s c o A V P a i r l i n k S e c - p o l i c y = m u s t - s e c u r e . م ا د خ ت س ا ب ل و ح م ل ا ل ا " ر ط ق ل ا ف ص ن ل و ب ق " ء ز ي م ا ض ي ا ل ش ف ي ، ء س ل ل ا ه ذ ه ل ش ف ء ل ا ح ي ف . M K A . ء س ل ج ء ب ي ل ع ل و ح م ل ا ء م س ل ل ا ه ذ ه م ع ر ت ل و ح م ل ا ي ل ع 802.1X ض ي و ف ت .

The screenshot displays the Cisco Identity Services Engine (ISE) web interface for configuring an Authorization Policy. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Authorization Policy' tab is active, showing a description: 'Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.' Below this, there is a dropdown menu for 'First Matched Rule Applies'. Under 'Exceptions (0)', there is a 'Standard' section. A table lists the policy rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Macsec	if Radius:User-Name EQUALS cisco	then MACSECprofile

لي د ب ت

(ح:ض و م ل ا ي و ل ع ل ا ء ج ل ا) 802. 1x ر ا ي ع م ب ء ي ج ذ و م ن ل ا ذ ف ا ن م ل ا ت ا د ا د ع ا ن م ض ت ت

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
aaa group server radius ISE
server name ISE
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet1/0/2
description windows7
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
```

```
radius server ISE
address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
timeout 5
retransmit 2
key cisco
```

على MACsec نيكتمت مت، اضي. ههاولا على اهقبيبطت و هيلحملا MKA هسايس اشنا متي ههاولا.

```
mka policy mka-policy
replay-protection window-size 5000
```

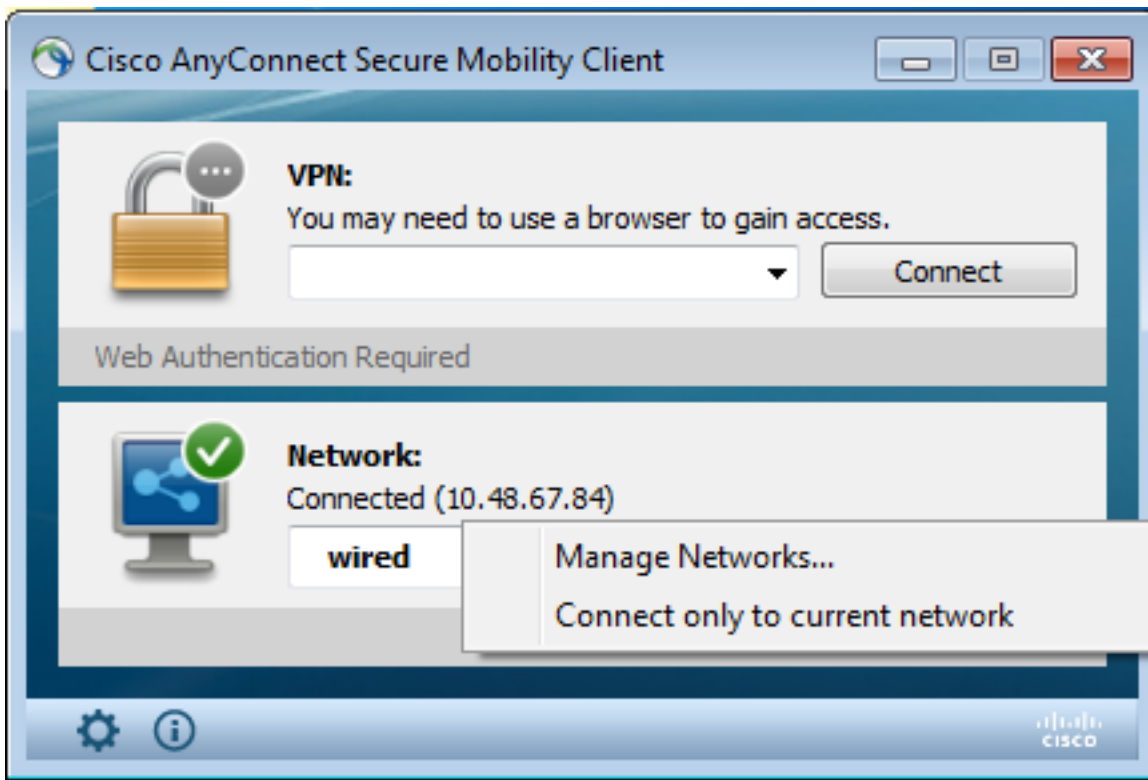
```
interface GigabitEthernet1/0/2
macsec
mka policy mka-policy
```

ISE. نم اهعفد نكمي ال يتلا هيلصفتلا تاداعلا نيوكتب كل ليلحملا MKA جهن حمسي هرايتخا هيلحملا MKA هسايس.

AnyConnect NAM

تاوطلال ضرعت Cisco ASA. ربع هعفد و اويودي 802.1x بلطم ل فيرعتلا فلم نيوكت نكمي تاوطلال ضرعت.

NAM: تاافيصوت هرادا لجا نم



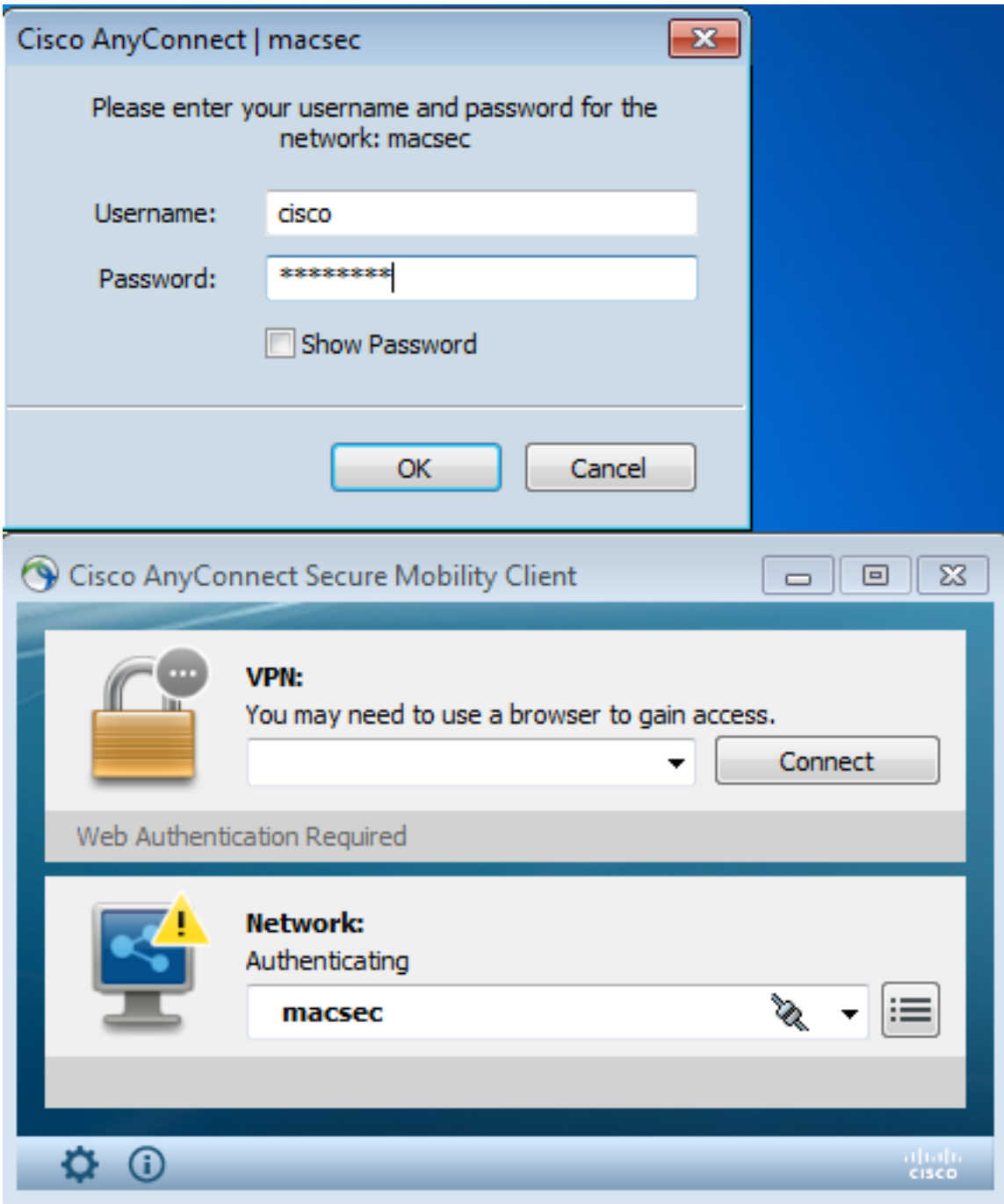
م تي 802.1x راي عمل ة بس ن ل اب MacSec. مادخت س اب دي ج 1x. 802.1x صي صخت فلم ة فاضا
 "Cisco" ه ني وكت مت ي ذل ا مدخت س م ل ا (PEAP) ي م ح م ل ا ع س و ت م ل ا ة ق د ا ص م ل ا ل و ك و ت و ر ب م ا د خ ت س ا
 ل ع ISE):



ة ح ص ل ل ا ن م ق ق ح ت ل ا

ح ح ص ل ل ك ش ب ن ي و ك ت ل ا ل م ع د ي ك ا ت ل م س ق ل ا ا ذ ه م د خ ت س ا

ة.حيص دامتعا تاناي ب EAP-PEAP ل اهنويوكت مت يتي ال AnyConnect NAM بلطتت



ةينامضلا لالحال نوكت نا يغبني .ضيوفتلاو لوحمالا لىل عمعلا ةسلج ةقداصم بجي
"ةنومضم":

```
bsns-3750-5#show authentication sessions interface g1/0/2
  Interface: GigabitEthernet1/0/2
  MAC Address: 0050.5699.36ce
  IP Address: 192.168.1.201
  User-Name: cisco
  Status: Authz Success
  Domain: DATA
  Security Policy: Must Secure
  Security Status: Secured
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: 10
```


Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A8000100000D56FD55B3BF
Acct Session ID: 0x00011CB4
Handle: 0x97000D57

Runnable methods list:

Method	State
dot1x	Authc Success

يُسمح لجهازنا بإدخال قفل عتية اميف لخصائص التالو حمال لى لى MACsec تايئاصح ارفوت
ذفان مال تايئاصح ارضي او، ةلسرر مال/ةملتس مال رورمال ةكرج (SCIs) ةنمال تاونق ل تافرع مو
ءاطخال او.

bsns-3750-5#show macsec interface g1/0/2

MACsec is enabled

Replay protect : enabled

Replay window : 5000

Include SCI : yes

Cipher : GCM-AES-128

Confidentiality Offset : 0

Capabilities

Max. Rx SA : 16

Max. Tx SA : 16

Validate Frames : strict

PN threshold notification support : Yes

Ciphers supported : GCM-AES-128

Transmit Secure Channels

SCI : BC166525A5020002

Elapsed time : 00:00:35

Current AN: 0 Previous AN: -

SC Statistics

Auth-only (0 / 0)

Encrypt (2788 / 0)

Receive Secure Channels

SCI : 0050569936CE0000

Elapsed time : 00:00:35

Current AN: 0 Previous AN: -

SC Statistics

Notvalid pkts 0 Invalid pkts 0

Valid pkts 76 Late pkts 0

Uncheck pkts 0 Delay pkts 0

Port Statistics

Ingress untag pkts 0 Ingress notag pkts 2441

Ingress badtag pkts 0 Ingress unknownSCI pkts 0

Ingress noSCI pkts 0 Unused pkts 0

Notusing pkts 0

Decrypt bytes 176153

Ingress miss pkts 2437

ةمزال تاءاصح او ريفش التالو مادختس لى لى تاءاصح ارفوت AnyConnect،

Network Access Manager

Configuration Statistics Message History

Subnet Mask (IPv4)	255.255.255.0
Default Gateway (IPv4)	192.168.1.10
Bytes	
Sent:	16567
Received:	5760
Frames	
Sent:	115
Received:	49
Security Information	
Configuration:	802.1X (MACsec)
Encryption:	GCM(Software)
EAP Method:	eapPeap(eapMschapv2)
Server:	ise2.test-cisco.com
Credential Type:	Username/Password

اهحال صاوا عااطخاا فاشكسا

اهحال صاوا نيوكتلا عااطخا فاشكسا ال اهمادختسا كنكمي تامولعم مسقلا اذه رفاوي

لمع وييرانيسل عااطخاا حيحصت

(حوضولل تاخرملا ضع ب فذ م ت) ل وحملا ل عااطخاا حيحصت نيكم تب مق

```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

ةباجتسا رخا نمضتت. EAPOL ربع ةددعتم EAP مزح لدابت متي، 802.1x لمع ةسلج عاشن ا دع ب RADIUS تامس ةدع اضيأ RADIUS-Accept لخاد ةلمحملا (EAP حاجن) ISE نم ةحجان

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS: EAP-Key-Name [102] 67 *
RADIUS: Vendor, Cisco [26] 34
RADIUS: Cisco AVpair [1] 28 "linksec-policy=must-secure"
RADIUS: Vendor, Microsoft [26] 58
RADIUS: MS-MPPE-Send-Key [16] 52 *
RADIUS: Vendor, Microsoft [26] 58
```

RADIUS: MS-MPPE-Recv-Key [17] 52 *

مادختس | لوجم لى لىع Linksec جهن ضر في MKA لمع ةس لىع EAP-Key-Name مادختس | متي تامس لى كلت نم ققحت لى اضيأ نك مي . (المتكم كلذ نكي مل اذا ضي وفت لى لى في) MACsec طاق لى لى مز في .

18	10.48.66.74	10.48.66.109	RADIUS	418	Access-Accept(2)	(id=40, l=376)
.....						
▶	AVP: l=7	t=User-Name(1):	cisco			
▶	AVP: l=40	t=State(24):	52656175746853657373696f6e3a43304138303030313030...			
▶	AVP: l=51	t=Class(25):	434143533a43304138303030313030303030443536464435...			
▶	AVP: l=6	t=Tunnel-Type(64)	Tag=0x01: VLAN(13)			
▶	AVP: l=6	t=Tunnel-Medium-Type(65)	Tag=0x01: IEEE-802(6)			
▶	AVP: l=6	t=EAP-Message(79)	Last Segment[1]			
▶	AVP: l=18	t=Message-Authenticator(80):	05fc3f0450d6b4f80564404551992972			
▶	AVP: l=5	t=Tunnel-Private-Group-Id(81)	Tag=0x01: 10			
▼	AVP: l=67	t=EAP-Key-Name(102):	\031R\315g\206\334\236\254\344:\333`jH\355(\353\343\ [Length: 65]			
		EAP-Key-Name:	\031R\315g\206\334\236\254\344:\333`jH\355(\353\343\255\004\362H\376\ ▼			
▶	AVP: l=34	t=Vendor-Specific(26)	v=ciscoSystems(9)			
▶	VSA: l=28	t=Cisco-AVPair(1):	linksec-policy=must-secure			
▶	AVP: l=58	t=Vendor-Specific(26)	v=Microsoft(311)			
▶	AVP: l=58	t=Vendor-Specific(26)	v=Microsoft(311)			

ةحجان ةقداصل

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on  
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client  
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

(تلسراً اضيأ نو كي ي قىل تي ي ا ي راي تخ | مق ر VLAN نم ض تي اذه) ةمس لى حات فم لى ق ب ط ي .

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID  
C0A8000100000D56FD55B3BF
```

ط ب ر EAPOL م ل ت س ي و ل س ر ي ا م د ن ع MKA ةس لى حات فم لى ا د ب ي م ث .

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,  
AuditSessionID C0A8000100000D56FD55B3BF, AuthMgr-Handle 97000D57
```

```
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
```

```
EAPOL pak dump Tx
```

```
EAPOL pak dump rx
```

```
dot1x-packet(Gi1/0/2): Received an EAPOL frame
```

```
dot1x-packet(Gi1/0/2): Received an MKA packet
```

ب ي قىل لى ا م ا ن ا ر ت ق ا ع م م ز ح ل ل ا د ب ت ل ة ن م ا ت ا ف ر ع م 4 ا ا ش ن ا د ب (RX).

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
```

```
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
```

```
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
```

```
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

ن ا ر ت ق ا ن م ا (tx) لى ت ف ض ا و ةس لى ح ل ا ت ه ت ن ا .

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
```

RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: **Process install TxSA** request66B4EEC for interface GigabitEthernet1/0/
ضيوفتال حاجنو "ني مات بجي" جهنللق باطمتتم.

%AUTHMGR-5-SUCCESS: **Authorization succeeded** for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
ةايحل دي قىل ع ني كراشمال عي مج نأ نامضل ني تي ناث لك MKA Hello مزح لدابت متي

dot1x-ev(Gi1/0/2): Received TX PDU (5) for the client 0x6E0001EC (0050.5699.36ce)
dot1x-packet(Gi1/0/2): MKA length: 0x0084 data: ^A
dot1x-ev(Gi1/0/2): Sending EAPOL packet to group PAE address
EAPOL pak dump Tx

لشاف ويراني سلءاطخال حي حصت

ةحجانل 802.1x ةقداصم دعب ريفشتلال ISE لبلطي و MKA لبلاطمالي نيوكت متي ال امدنع

RADIUS: Received from id 1645/224 10.48.66.74:1645, **Access-Accept**, len 342
%DOT1X-5-SUCCESS: **Authentication successful** for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: **Authentication result 'success' from 'dot1x'** for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
EAPOL مزح 5 لسري امدنع MKA ةسلج ادب لوحمال لواحي

%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D55FD4D7529, AuthMgr-Handle A4000D56
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx

ليوختلال في لشفيو وتقولاي هتني اريخأو

%MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) **Peer has stopped sending MKPDUs** for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) **MKA Session was stopped** by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: **Authorization failed or unapplied** for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
ضيوفتلال لشف نكل، ةقداصم الحاجن لىل 802.1x لمع ةسلج ريشت

```
bsns-3750-5#show authentication sessions int g1/0/2
      Interface: GigabitEthernet1/0/2
      MAC Address: 0050.5699.36ce
      IP Address: 192.168.1.201
```

```

User-Name: cisco
Status: Authz Failed
Domain: DATA
Security Policy: Must Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Idle timeout: N/A
Common Session ID: COA8000100000D55FD4D7529
Acct Session ID: 0x00011CA0
Handle: 0xA4000D56

```

Runnable methods list:

```

Method State
dot1x Authz Success

```

ت.انايبل رورم ة كرح رطح متيس.

مزحل طاق الت

لوكتورب يدص دودر/تابلط لاسرا متي 4 يعرف ال عقوم ال يلع رورم ال ة كرح طاق الت دنع
كانه نوكتيس، اهلابقتساو (ICMP) تنرتن ال ي ف مكحتل لئاسر

- 802.1ae ل ة زوجم (88e5) لوحم ال ال اه لاسرا متي ICMP يدصل ة رفشم تابلط 4
- اهرففت ك ف مت ICMP يدص يلع دودر 4 يقولت مت

لبقو مزحل لاسرا دنع libpcap لبق) Windows API ب AnyConnect لاصت اة ففك ببسب كلذو
(مزحل مالتسا دنع libpCAP):

No.	Source	Destination	Protocol	Length	Info
3	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
4	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=255
5	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
6	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=255
7	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
8	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=255
9	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
10	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=255

```

Frame 3: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Vmware_99:36:ce (00:50:56:99:36:ce), Dst: Cisco_25:a5:43 (bc:16:65:25:a5:43)
Data (92 bytes)
Data: 2c000000013c0050569936ce0000565d05c5dfa65d7345d3...
[Length: 92]

```

ةمس عم حتفم ال يلع رورم ة كرح 802.1ae و MKA قشن ي نأ ة ردق ال دناسي ال: ةظحالم
(EPC) طاق التا طبر رمطي و (نيتماعد ني ب ةحس ف) رسي للحم لوحي لثم.

802.1x و MacSec يعضو

ال MacSec ل 802.1x عاضوا عي مج معد متي ال

يلع صنت NDAC و MacSec ال ةم دقم: Cisco TrustSec 3.0 تاداشرا

- اذه ي ف. دحاولا فيضم ال عضو ي ف لم اك لكشب MACsec معددي: دحاولا فيضم ال عضو
ن. MACsec مادختسا ب هني ماتو دحاو IP و MAC ناو نع ة قداصم طقف نكمي، عصولا
يقولتي ة ياهن ة طقن نأ دعب اعانيم ال يلع نوكتي {upper}mac address فل تخم تفشك

- عانېملا ىلع تقولطا نوکي كاهتنا نمأ، قدصبي
- ىلع ءدحاو ءياهن ءطقن نوکت دق، عضولا اذه في (MDA) تالاجملا ءدعتم ءقداصملا عضو
في لمالكلاب موعدم MacSec. توصلال لاجم ىلع ىرخأ ءياهن ءطقن نوکت دقو تانايبلا لاجم
نيماأ متيسف، MACsec مادختسا ىلع نيترداق ءياهنلا يطقن تناك اذا. MDA عضو
ءدحاو ءياهن ءطقن تناك اذا. هب ءصاخلا ءلقتسملا MACsec لمع ءسلج لالخ نم امهنم لك
ءياهنلا ءطقن لسرت امنيب كلت ءياهنلا ءطقن نيماأ نكمي، MACsec ىلع ءرداق طقف
حسملال في تانايبلا رورم ءكرح ىرخألا
- نم ابيرقت دودحم ريغ ددع ءقداصم متت دق، عضولا اذه في: ءدعتملا ءقداصملا عضو
عضولا اذه في دمتعم ريغ MacSec. دحاو لوحم ذفنم ىلع ءياهنلا طاقن
- ءيخانلا نم انكمم عضولا اذه في MACsec مادختسا نوکي امنيب: فيضملا ددعتم عضولا
ءطقن ءقداصم متت، ءفيضملا ءزهجال ددعتم عضولا في. هب ىصوي ال، ءينقتلا
نم ءكبشلا ىلع ءيفاضا ءياهن طاقن ياب حامسلا متي م، ذفنملا ىلع لولأا ءياهنلا
ءكرح رم ت نل نكلو، لصتملا لولأا فيضملا عم MacSec لمعتس. لولأا ليوختلا لالخ
ءرفشم رورم ءكرح نوکت نل اهانال، لعفلال ىرخأ ءياهن ءطقن رورم.

ءلص تاذا تامولعم

- [Cisco TrustSec ل 3750 نيوكت ليلد](#)
- [Cisco TrustSec ل ASA 9.1 نيوكت ليلد](#)
- [MAC نامأ: ءيوهلا ىلا ءدنتسملا ءكبشلا تامدخ](#)
- [لاثم ليلكشت حاتفم 3750X sery ءزافح ءدام ىلع MACsec 802.1x عم TrustSec ءباحس](#)
- [ءاطخالا فاشكتسا ليلدو Catalyst 3750X Series Switch TrustSec و ASA نيوكت للاثم
اهحالصاو](#)
- [قيرطالا ءطيخو Cisco TrustSec رشن](#)
- [Cisco Systems - تادنتسملا و ينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا