# ISE مادختساب EAP-TLS ةقداصم نيوكت

### تايوتحملا

<u>قمدق مل ا</u>
<u>قيساسألاا تابلطتملا</u>
<u>تابلطتملاً</u>
<u>قمدختسملاً تانوكملاً</u>
<u>قيساساً تامول.عم</u>
<u>نېوكتل ا</u>
ل <u>ېمعلاو مداخلا تادامش ېلع لوصحلا</u>
<u>ISE نم قدامش عيقوت بلط ءاشنا .1 قوطخلا</u>
<u>ISE داريتس داريتس 2. قوطخل SE</u>
<u>قياەنلا قطقىنل لىمعلا قداەش ىلع لوصحلا .3 قوطخلا</u>
<u>قكېش ل ا قزمچأ</u>
<u>ISE يف ةكبشلا عال لوصولا زامج ةفاضا .4 ةوطخلا</u>
<u>ةس اي س لما رص ان ع</u>
<u>قېچراخلا قېوەل ردصم مادختسا .5 قوطخلا</u>
<u>ةداەشل،ا ةقداصم فيرعت فل.م ءاش.نا .6 قوطخل.ا</u>
<u>قيوما اردصم لسلست يا ا قفاضا .7 قوطخا ا</u>
<u>اەب جومسمل،ا تالبوكوتورپل،ا قمدخ دىدجت .8 قوطخليا</u>
<u>ضي،وفتا، ا في،رعت فا م ءاش،ا 9 ةوطخا، ا</u>
<u>تامأليا تاسايس</u>
<u>چەنالا قومچم ءاش،نا .10 قوطخلا</u>
<u>ققداصم ةسيايس ءاش،نا .11 ةوطخليا</u>
ل.ي.وختالا جەن ءاش، إ. 12 قوطخليا
<u>قحصلا نم ققحتلا</u>
<u>امحالصاو ءاطخألاا فاشكتسا</u>
<u>امحال صاف عاطخاًلاً فاشكت سال مَمِدخت سمل ا بِيل اسأل اف مَعِداشل ا تالكشمل ا</u>
<u>قل ص تاذ تامول عم</u>

# ةمدقملا

لباقلا ةقبطلا لقن لوكوتورب ةقداصم ميدقتل يلوألا نيوكتلا دنتسملا اذه فصي عم عسوتلل Cisco ISE.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- . تالاصتالا قفدت RADIUS و EAP ل يساسألا مەفلا
- اميف ةداهشلا علام المان المان المان المراح عم المان المان المان المان المان المان المان المان المان ا

لاصتالا قفدتب قلعتي.

- .MAC (MAB) ةقداصم زواجت نيب قورفلا مَهف •
- الماعلام حاتفملل ةيساسألا المين الما مهفلا (PKI).
- ىلع تاداەشلا ةرادإو (CA) قدصم عجرم نم ةعقوم تاداەش ىلع لوصحلا ةيفيكب ماملإ ةياەنلا (طاقن) ةطقن.
- ىلع (RADIUS) (AAA) ةبساحملاو ضيوفتلاو ةقداصملاب ةطبترملا تادادعإلا نيوكت (يكلسال وأ يكلس) ةكبشلا زاهج.
- مادختسالل (ةياهنلا قطقن ىلع) بلاطملا نيوكت RADIUS/802.1x.

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- رادصإلا، (ISE)، ةيوەلا تامدخ كرحم 3.x.
- CA مادختسإ وأ ةماع CA/ةيجراخ ةهج وأ Enterprise CA نوكي نأ نكمي) تاداهشّلا رادصإلّ <u>تاداهشلار ريفوت لخدم</u>.
- نم (يجراخ ةيوه ردصم) Windows Server، نم المدخ عم قفاوتي ثيح I<u>SE</u>.
- يَفُ مَكْحِ<u>ت مَدِح</u>وِ وَأَ (مَيَّكلس) لوحم نوكي نأْ نكُمي (NAD) مَكْبِشلا علام لوصولا زامجً 1802. 1x/AAA. لا اەنيوكت مت (يكلسال) (<u>WLC) مَيْكلساللا مَيْلَحِملاً مَكْبِشلا</u>
- نكمي يتلا ليمعلا نيوكُتُو (مدُختُسُملاً) قَيُوهُل ةرداصُلا تاداهشلاً قَياهنلاً قطقَن نكمملا نم .مدختسملا ةقداصم :RADIUS/802.1x ربع ةكبشلا ىلإ لوصولل اهتقداصم لائملا اذه يف ةمدختسم ريغ اهنكل ،زاهج ةداهش ىلع لوصحلا.

ً قئاثولاا عجارم عيمج دنتست ،ISE نم 3.1 رادصإلا مدختسي ليلدلاا اذه نأل ارظن :ةظحالم يف لماكلاب اموعدمو انكمم لثامملا/هسفن نيوكتلا نوكي ،كلذ عمو .رادصإلاا اذه ىلإ نم ةقباسلا تارادصإلاا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

# ةيساسأ تامولعم

ةددعتم تاهويرانيس ىلع هقيبطت نكمي يذلاا ISE نيوكت ىلع يسيئرلاا زيكرتلا بصنيو .يكلسال وأ يكلس ربع ةلصتم IP ةياهن ةطقن/فتاه عم (ىلع ارصح سيلو) ةقداصملا لثم

:(RADIUS) ةقداصم قفدت نم لحارملا هذه مهف مهملا نم ،ليلدلا اذه قاطنل

- يتلا (كلذ ىلا امو مدختسملاو زاهجلا) ةيئاەنلا ةيوەلا فيرعتب مق ةقداصملا اەتحص نم ققحتلاو ةكبشلا ىلا لوصولا بلطتت.
- ىلع اەحنم نكمي يتلا ةيئاەنلا ةيوەلا ىلإ لوصولا/تانوذألا ديدحت ضيوفتلا ةكبشلا.
- لوصولا قيقحت دعب ەبقعتو ةيئاەنلا ةيوەلا ةكبش طاشن نع غالبإلا ةبساحملا .ةكبشلا ىل

### نيوكتلا

### ليمعلاو مداخلا تاداهش ىلع لوصحلا

ISE نم ةداەش عيقوت بلط ءاشنإ .1 ةوطخلا

(مداخلاا) CA ىلإ ەلاسراو ISE نم (CSR) قداەش عيقوت بلط ءاشنإ يف ىلوألا ةوطخلا لثمت قداەشلا ەذە ميدقت نكمي .ماظن قداەشك ،ISE ىلإ قرداصلا قعقوملا قداەشلا ىلع لوصحلل (EAP-TLS) عسوتملا ققداصملا ققبط لقن لوكوتورب ققداصم ءانثأ ISE قطساوب مداخ قداەشك Management > Certificate Signing Requests. تحت Certificate Signing Requests. قوف تماي الالا Section 2000 (Cartificate Signing Requests. تحت المدختسم قام الالاي Section 2000) Requests (CSR) قوف مالا الالاي Section 2000) الالاي الالاي الالاي Section 2000) الالالاي Section 2000 الالالاي Section 2000) الالالاي Section 2000 (Cartificate Signing Requests. تحت الالالاي Section 2000) الالالاي Section 2000) الالالاي Section 2000 (Section 2000) الالالاي Section 2000) الالالاي Section 2000) الالالاي Section 2000 (Section 2000) (Sec

Certificate Signing Requests

Gener	ate Certificate Sig	gning Reque	ests (CSR)								
A Certific that authors	ate Signing Requests (C ority. Once a CSR is bour	SRs) must be s nd, it will be rem	ent to and signed by an external authority. Click "exp oved from this list.	ort" to download one	e or more CSRs so	that they may be sign	ned by an exte	nal authorit	ty. After a request has been signed, click "bind" to bind the request to the sign	1ed certificate issu	ied by
Q View	1 Export	Delete	Bind Certificate							All $\sim$	$\nabla$
	Friendly Name		Certificate Subject	Key Length	Portal gro	Timestamp		Host	i l		
No data	available										

تامادختسإ ةمئاقلا ەذە ددحت .ةفلتخم ةعسوم حاتفم تامادختسإ تاداەشلا عاونأ بلطتت ةداەش عون لكل ةبولطملا ةعسوملا حيتافملا:

ISE ةيوه تاداهش

- مداخلاو ليمعلا ةقداصم (pxGrid و Portal و EAP و ةرادإلا) ددعتملا مادختسالا •
- مداخلا ةقداصم Admin •
- مداخلا ةقداصم EAP ةقداصم •
- مداخلا ةقداصم (DTLS) تانايبلا لقن ةقبط ةقداصم •
- مداخلا ةقداصم ةباوبلا
- pxGrid مداخلاو ليمعلا ةقداصم
- SAML عيقوت ةداهش (SAML) نامألاا ديكأت زيمرت ةغل •
- امامت ةديدج ةلسارم ةداهش ءاشنإ وأ عيقوت ةداهش ءاشنإ ISE تالسارم ةمدخ •

ةدقع لك ربع تانايبلا خسنب ةصاخ ISE ةلسارم ةمدخ ماظن ةداهش نوكت ،يضارتفا لكشبو اهرادصإ متو ةدوجوم نوكتو ،دقعلا نيب ىرخألا تالاصتالاو دقعلا ليجستو رشنلا يف ISE هذه عم ءارجإ يأ مامتإ مزلي ال .(ISE ىلإ يلخاد) ISE (CA) ةداهشلل يلخادلا عجرملا مداخ ةطساوب .قداهشلا

ماظن ةداهش" مادختسإ متي الله فيرعتل "Admin ماظن ةداهش" مادختسإ متي نيب تالاصتالا ضعبلو ،(API) Admin مدختسم ةهجاوب ةنرتقملا (API) تاقيبطت ليلدب ةرشابم ءارجإلا اذه طبتري ال .ةرادإلا ماظن ةداهش عضوب مق ،ةرم لوأل ISE دادعإل .دقعلا اذه نيوكتلا.

ماظن ةداهشل ءارجإ ذختا ،(ةداهش ىلإ ةدنتسم ةقداصم) EAP-TLS ربع IEEE 802.1x ذيفنتل ءانثأ ليمعلا/ةياهنلا ةطقن ىلإ ةمدقملا مداخلا ةداهشك اهمادختسإ متي ثيح EAP ةقداصم قفدت EAP-TLS قان لخاد ةجيتان انيمأت متي كلذل ةجيتانو EAP-TLS قافدت يف CA (مداوخ) مداخ نوريدي نيذلا نيفظوملل اهئاطعإو EAP ةقداصم ماظن ةداهش ءاشنإل CA لبق نم ةعقوملا ةداهشلا يه ةيئاهان ا قجيتان ا عيقوتان (ماعل CA رفوم وأ) كتسسؤم تاوطخلا هذه عم ISE با نرتقتو CSR با طبتارت يتالا.

ىلع لوصحلاو CSR لامكإ لجأ نم تارايخلا هذه رتخأ ،(CSR) ةداهشلا عيقوت بلط جذومن يف اهتايوتحم:

- رتخأ ،اذه نيوكتلا لاثمل ،ةداهشلا مادختسا EAP Authentication.
- اضيأ كيلع بجي مث ،example.com، ،قداهشلا يف لدب فرح قرابع مادختسال ططخت تنك اذإ
   ليدبلا مسالا قداهش لقح وه عقوم لضفأ .رايتخالا قناخ Allow Wildcard Certificate نم ققحتلا
   مسالا قدامش لقح وه عقوم لضفأ .رايتخالا قناخ Allow Wildcard Certificate نم ققحتلا
   مسالا مسالا قدامش لقح وه عقوم لضفأ .رايتخالا قناخ مادختسالا مسالا قدامش لقح وه عقوم لضفاً .رايتخال القناح مالي المسالا المسالا المالي .
- نارقإ يف بغرت يتلا ISE دقع رتخأ ،ةداهشلا يف لدب فرح ةرابع عضو رتخت مل اذإ (عيقوتلا دعب) CA ب ةعقوملا ةداهشلا.

♦ لدبلا فرح ةرابع ىلع يوتحت يتلا CA لبق نم ةعقوملا ةداەشلا طبر دنع :ةظحالم دقعلا ىلع وأ) ISE ةدقع لك ىلع ةداەشلا عيزوت متي ،CSR لخاد ةددعتم دقعب ليغشت ةداعإ نإف ،كلذ عمو .تامدخلا ليغشت ةداعإ نكميو ،ISE رشن يف (ةددحملا ليغشت قداعإ قبقارم .قرم لك يف ةدحاو ةدقع ىلع ايئاقلت رصتقت تامدخلا

تاداهش لوقح كلذ لمشي .عوضوملا ديدحت لجأ نم جذومنلا لامكإ كيلع بجي ،كلذ دعب ةلودلاو ،(L) ةنيدملاو ،(O) ميظنتلاو ،(OU) ةيميظنتلا ةدحولاو ،(CN) كرتشملا مسالا (ST)، لابلام مسالات يتلا ةميقلا وه \$FQDN ريغتملا. (C). الجملا مسا لافتا الافتان الافتان الافتان الافتان الماكل الماك

- تامولعم يأ نيمضتل لوقحلا لامكإ اضيأ بجي (SAN) Subject Alternative Name (SAN) رمألا ضرعي لاخدإ ديدحت ىلإ جاتحت ،بلطتمك .ةقثلا ءاشنإل اهمادختسإ متيل ةبوغرمو ةبولطم عيقوت دعب ،ةداهشلا هذهب ةنرتقملا ISE (تادحو) ةدقعل FQDN ىلإ ريشي يذلا DNS .قداهشلا

ميقلا مادختسإ نم دكأت .لدب فرح ةرابع مادختسإ نودب لمتكم CSR جذومن ىلع لاثم اذه ةئيبلاب ةصاخلا ةيلعفلا:

### Usage



3. تاداەشلا نزخم ىلإ ،ةلماكلا CA ةلسلس نم ءزجك ،تاداەشلا عيمج داريتسإ درجمب لقتناو ISE ب ةصاخلا (GUI) ةيموسرلا مدختسملا ةمجاو ىلإ عجرا ،ISE يف اەب قوثوملا لاخدا ناكم ددح .Administration > System: Certificates > Certificate Management: Certificate Signing Requests ىل مث ،ةداەشلل رايتخالا ةناخ رقنا ،ةعقوملا ةداەشلا لثامي يذلا فولأم مسا تحت Bind Certificate.

Certificate Signing Requests

Generat	e Certificate Signing Requests	(CSR)							
A Certificate	Signing Requests (CSRs) must be sent to y. Once a CSR is bound, it will be removed	and signed by an external authority. Click "export" from this list.	to download one	or more CSRs so t	hat they may be signed by	an externa	al authority. After a request has been signed, click "bind" to bind the request to the signed c	ertificate iss	ued by
) View	1) 2)	nd Certificate						all $\sim$	$\nabla$
	Friendly Name 1)	Certificate Subject	Key Length	Portal gro	Timestamp	^	Host		
	ise#EAP Authentication	CN=ise. example.com ,O=E_	4096		Tue, 10 May 2022		ise		
	ise2#EAP Authentication	CN=ise2.example.com ,O=	4096		Tue, 10 May 2022		ise2		
	ise3#EAP Authentication	CN=ise3.example.com .O=_	4096		Tue, 10 May 2022		ise3		

CSR ب ةداەشلا طبر

لك يف CSR ةداەش لكب CA لبق نم ةعقوم ةدحاو ةداەش طبر ىلإ جاتحت :ةظحالم 🛇 رشنلا يف ىرخألاا ISE دقعل اەؤاشنإ مت ةيقبتم CSR تادحو ةيأ ررك .ةرم

مسا فيرعتب مقو ،عقوملا صيخرتلا فلم رتخاو Browse رقنا ،ةيلاتلا ةحفصلا يف تارييغتلا ظفحل لاسرا .صيخرتلا (تامادختسإ) مادختسا رتخاو ،بغرم فولأم.

#### Bind CA Signed Certificate

* Certificate File	Browse EXAMPLE_ISE.cer	
Friendly Name	EAP Authentication System Certificate	()
Validate Certificate Extensions	0	
Usage		
EAP Authentication: Use certificate	for EAP protocols that use SSL/TLS tunneling	

4. لقتنا .(ISE) ةيموسرلا مدختسملا ةمجاو ىلإ ةعقوملا ةدامشلا لقن متي ،تقولا اذه يف سفن ىلإ امنييعتو Administration > System: Certificates > Certificate Management: System Certificates ىلإ تامادختسإ وأ/و ىرخألا دقعلل ةيلمعلا سفن ررك .امل CSR ءاشنا مت يتلا ةدقعلا يرخألا صيخرتلا

ةياەنلا ةطقنل ليمعلا ةداەش ىلع لوصحلا .3 ةوطخلا

مادختسالل ليمع ةداهش ءاشنإل ةياهنلا ةطقن ىلع ةلثامم ةيلمع ربع لقنتلل بولطم وهو

CSR ب طبرلل ةداەش ديدحت

مدختسملا باسح ىلإ اەرادصاو ليمع ةداەش عيقوت كمزلي ،لاثملا ليبس ىلع EAP-TLS. مدختسملا باسح ىل ةداەش ىلع لوصحلا ةيفيك لوح لاثم ىلع روثعلا نكمي ISE. عم مدختسملا ةقداصم ءارجإل WLC مادختساب ەنيوكتو EAP-TLS مەف :يف Active Directory ةئيب نم ةياەنلا ةطقنل ليمع ISE مادختساب مايوكتو SeP-TLS مەف :ي

ةفلتخم نوكت دق ةيلمعلاا نأ ثيح ،ليغشتلا ةمظنأو ةياهنلا طاقنل ةددعتملا عاونألل ارظن قيحانلا نم اهسفن يه قماعلا ةيلمعلا نأ ريغ .قيفاضإ قلثمأ ميدقت متي ال ،عيشلا ضعب يف اهنيمضت متيل قلصلا تاذ تامولعملا قفاك ىلع يوتحي CSR ءاشنإب مق .قيميهافملا قيجراخ/ةماع ةكرش وأ ةئيبلا يف ايلخاد امداخ كلذ ناك عاوس ،CA لبق نم اهعيقوتو قداهشلا

(SAN) ليدبلا عوضوملا مساو (CN) عئاشلا مسالا ةداەش يلقح نإف ،كلذ ىلع ةوالع اضيأ يلمي اذەو .ةقداصملا قفدت ءانثأ اەيف اەمادختسا متيس يتلا ةيوەلا نانمضتي وأ ،مدختسملا وأ/و زاەجلا ةقداصم :ةيوەلاب قلعتي اميف EAP-TLS ل بلاطملا نيوكت ةيفيك يف طقف مدختسملا ةقداصم لاثملا اذە مدختسي .مدختسملا ةقداصم وأ ،زاەجلا ةقداصم يفاب

ةكبشلا ةزهجأ

ISE يف ةكبشلا ىلإ لوصولا زامج ةفاضإ .4 ةوطخلا

ISE يف هب ةياهن ةطقن ليصوت متي يذلا (NAD) "ةكبشلا ىلإ لوصولا زاهج" نيوكت مت امك لاصتا ءارجإ نكمي ىتح ISE، مادختسإ متي ISE، و NAD نيب .(زاهجلا لوؤسم) +RADIUS/TACACS لاصتا ءارجإ نكمي ىتح ةقثلا ضارغأل كرتشم رورم ةملك/رس.

ةفاضإ لجأ نم Administration > Network دىل لقتنا، (ISE)، كل لقتنا Administration > Network دىل لقتنا. Resources: Network Devices > Network Devices قوف رقناو Addl قوف رقناو.

E Cisco ISE	Administration - Network Resources	Q (0)	Ø 67
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services		
Network Devices Default Device Device Security Settings	Network Devices List 3 Satch   Name   * Name   Description     * Model Name     * Oracle Profile   Model Name   * Name   * Oracle Profile   Model Name   * Name   * Name   * Name   * Oracle Profile   Model Name   * Name   * Name   * Name   * Oracle Profile   Model Name   * Name <th></th> <th></th>		

ةكبشلا زاهج لاثم نيوكت

لوكوتورب نيوكت اضيأ ديرت ،"(ISE) ةيوهلا فيرعت تافلم ءاشنإ" ةزيم عم مادختسالل SNMPv2 وأ SNMPv2 وأ SNMPv2 و ان مسلل (انامأ رثكأ) تام الع تام العتسان بربع تام سلا عيمجتل SNM يلع ةياهنلا ةطقن ةقداصم يف ةنمضملا دادعإ ةيفيك يلاتلا لاثملا حضوي .ةمدختسملا ةياهنلا قطقن عون يلع ةقيقد تارارق ذاختال SNMP (v2c) :قرباسلا لي في العلا ال

* SNMP Version	2c 🗸	
* SNMP RO Commu	inity	• Show
SNMP Username		
Security Level	~	
Auth Protocol	~	
Auth Password		Show
Privacy Protocol	~	
Privacy Password		Show
* Polling Interval	28,800	seconds (Valid Range 600 to 86400 or zero)
Link Trap Query	<b>~</b>	
MAC Trap Query		

SNMPv2c نيوكت لااثم

رادصإلا، Cisco نم ةيوهلا تامدخ كرجم لوؤسم ليلد يف تامولعملا نم ديزم ىلع روثعلا نكمي ع<u>ف ةكبشلا ةزمجاً فيرعت</u> < نمآلا لوصولاا :لصفلا < 3.1

ةلصلا تاذ تادادعإلا عيمج نيوكت ىل قجاحب تنأف ،لعفلاب كلذب مقت مل اذإ ،تقولا اذه يف مادختساب ضيوفتلاو ةقداصملل NAD ىلع AAA ب

### ةسايسلا رصانع

اذه يف .ليوختلا جەن وأ ةقداصملا جەنب طابترالا ىلإ يەتنت رصانع يە تادادعإلا ەذە جەن يف ەنييعت متي مث جەنلا رصانع نم رصنع لك ءاشنإ لوألا ماقملا يف متي ،ليلدلا لامكإ متي ىتح اەقيبطت متي ال ةسايسلا نأ مەف مەملا نم .ليوختلا جەن وأ ةقداصملا حاجنب ليوختلا / ةقداصملا جەنب طبرلا.

ةيجراخلا ةيوەلا ردصم مادختسإ .5 ةوطخلا

وأ زامجلا) ةيئامنلا ةيوملا باسح دجاوتي ثيح ردصم ةطاسبب وه ةيجراخلا ةيوملا ردصم معدل ةداع Active Directory مدختسي .ISE ققداصم ةلحرم ءانثأ ممادختسإ متي يذلا (مدختسملا مدختسمل باسح لباقم مدختسملا ققداصم وأ/و رتويبمكلا باسح لباقم زامجلا ةقداصم نيزختب (قيلخادلا) ةيلخادلا ةيامنلا طاقن ردصم موقي ال .Active Directory يف يئامنلا .زامجلا ةقداصم عم ممادختسإ نكمي ال ،يلاتلابو ،فيضملا مسا/رتويبمكلا باسح

نكمي يتلا (ةقداصملا عون) تالوكوتوربلاو ISE عم ةموعدملا ةيوهلا رداصم انه حضوم وه امك ةيوه ردصم لك عم اهمادختسإ:

Protocol	I (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GT	C, PAP (plain text password)	Yes	Yes	Yes	Yes
MS-CHA MSCHA EAP-MS FAST, or LEAP	AP password hash: Pv1/v2 SCHAPv2 (as inner method of PEAP, EAP- r EAP-TTLS)	Yes	Yes	No	No
EAP-ME CHAP	05	Yes	No	No	No
EAP-TLS PEAP-TI (certifica Note	S LS ate retrieval) For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

تايوەلا نزخم تاردق

تامدخ كرحم لوؤسم ليلد يف ةسايسلا رصانع لوح تامولعملا نم ديزم ىلع روثعلا نكمي <u>تاسايسلا تاعومجم</u> < ةئزجتلا :لصفلا < 3.1 رادصإلا، Cisco نم ةيوهلا

ISE ىلإ Active Directory نامأ تاعومجم ةفاضإ

ةطقن ىلإ ةعومجملا ةفاضإ الوأ بجي ،ISE جەن يف Active Directory نامأ تاعومجم مادختسال

طبر Active Directory. رتخأ ، ISE أ قيموسرل مدختسمل قمجاو نم Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory.

دنتسملا اذه عجار ،Active Directory عم ISE 3.x جمدل تابلطتملاو تامولعملا نم ديزمل SE 3.x دنتسملا اذه عجار ، <u>حم Active Directory لماك</u>لاب :لماكلاب

ن العومجم قفاضإ ىلع ەسفن ءارجإلا قبطني :ةظحالم LDAP. ليثم ىل نامأ تاعومجم قفاضإ ىلع ەسفن ءارجإلا قبطني :قطحالم ISE، از مرفسرلا مرختسمل LDAP instance name > tab: Groups > Add > Select Groups From Directory.

ةداەشلا ةقداصم فيرعت فلم ءاشنإ .6 ةوطخلا

يف اەنم ةيوەلا ىلع روثعلا نكمي يتلا ةداەشلا ةمس رايتخال Identity From مادختسإ متي يە تارايخلا .نيعم لقح:

Subject - Common Name Subject Alternative Name Subject - Serial Number Subject Subject Alternative Name - Other Name Subject Alternative Name - EMail Subject Alternative Name - DNS

لام اذه، اليمعلا ةداهش نم (CN) عئاشلا مسالا لقح يف ةدوجوم ةيوهلا نوكت امدنع نيوكت لاثم اذه، (يرايتخا) ةيئانثلا ةنراقملا نيكمت عم:

E Cisco ISE		Administration - Identity Managemen	α	0.0	53 Ø
Identities Groups External Ide	ntity Sources Identity So	urce Sequences Settings			
External Identity Sources	Conficate Authentication Profiles Li Certificate Authentication	ut > Centrate_Protile 1 Profile			
Certificate Authentication F     Certificate Authentication F	* Namo	Certificate_Profile			
😤 AD1	Description				
ODBC RADIUS Token					
RSA SecurID SAML Id Providers	Identity Store	Al_AD_Join_Points V			
🗀 Social Login	Use Identity From	Contricate Attribute Subject - Common Name      V			
		Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)			
	Match Client Certificate Against Certificate In Identity Store ()	Nevor     Orky to resolve identity antiquity     Aways portorm binary comparison			
< >>			Save	Rese	ι

ةداەشلا ةقداصم فيرعت فلم

رادصإلا، Cisco نم ةيوهلا تامدخ كرجم لوؤسم ليلد يف تامولعملا نم ديزم ىلع روثعلا نكمي 3.1 > تاداهشلا مادختسال Cisco ISE تيوكت < Cisco ISE CA قمدخ < يساسألا دادعإلاا :لصفلا <u>قدنتسملا ققداصمل قداهش ققداصم فيرعت فلم ءاشنا</u> < ةيصخشلا قزهجألاا ققداصمل <u>TLS</u>.

ةيوەلا ردصم لسلست ىلا ةفاضا .7 ةوطخلا

ىلإ لقتنا. (ISE) ةيموسرلا مدختسملا ةمجاو نم ةيوملا ردصم لسلست ءاشنإ نكمي Administration > Identity Management. تحت Identity Source Sequences ، قوف رقنا

ردصم لسلست ىلإ ةداەشلا ةقداصم فيرعت فلم ةفاضإ يف ةيلاتلا ةوطخلا لثمتت ةعومجم عيمجت وأ Active Directory ل ةددعتم طبر طاقن نيمضت ىلع ةردقلا حنمي يذلا ةيوەلا جەنب طبترت كلذ دعب يتلاو ،ةبغرلا بسح ،اعم ةيجراخلا/ةيلخادلا ةيوەلا رداصم نم دومع use تحت ةقداصملا

روثعلا متي مل اذإ مث ،الوأ Active Directory لباقم ثحبلا ءارجإ انه حضوم وه امك لاثملا حيتي امئاد دكأت .ةددعتم ةيوه رداصمل .كلذ دعب LDAP مداخ نع ثحبلاب موقي هنإف ،مدختسملا ىلع ينعي اذهو .رايتخالا ةناخ ديدحت مت Treat as if the user was not found and proceed to the next store in the sequence نم منا منا مراجع ما مراجع الما من المراجع من مراج المراجع من مراجع من المراجع من المراجع من المراجع من المراجع من

Identities Groups External Identity Source Sequences	
Identity Source Sequence Identity_Sequence Identity_Sequence Identity_Sequence Description Certificate Based Authentication	
V Identity Source Sequence          * Name       Identity_Sequence         Description	
Certificate Based Authentication	
✓ Certificate Based Authentication	
Select Certificate Authentication Profile Certificate_Profile	
Authentication Search List A set of identity sources that will be accessed in sequence until first authentication succeeds Auxiliable	
Internal Endpoints All_AD_Join_Points Internal Users Guest Users	
ADI	
✓ Advanced Search List Settings If a selected identity store cannot be accessed for authentication	
<ul> <li>Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"</li> <li>Treat as if the user was not found and proceed to the next store in the sequence</li> </ul>	

ةيوەلا ردصم لسلست

ةقداصملا جەنب طقف ةداەشلا ةقداصم فيصوت طبر اضيأ كنكمي ،الإو.

اەب حومسملا تالوكوتوربلا ةمدخ ديدحت .8 ةوطخلا

ISE اهمعدي يتلا ةقداصملا تالوكوتورب/قرط الإ اهب حومسملا تالوكوتوربلا ةمدخ حيتت ال رصانع < ةسايس ىلإ لقتنا ،ISE GUI لا نم تلكش RADIUS. in order to ةقداصم ءانثأ ىلإ رصنعك طبري مث اهب حومسملا تالوكوتوربلا <ةقداصملا < جئاتنلا :ةسايسلا .ققداصملا ةسايس

.ISE ىلع MAB نيكمتب قلعتي ةيلمعلا فيضم ثحب < ةقداصملا زواجت :ةظحالم 🛇

ةطقن ىلع) بلاطملا ىلع ەنيوكتو ەمعد متي ام اەسفن يە تادادعإلا ەذە نوكت نأ بجي لشفي نأ نكميو عقوتم وە امك ةقداصملا لوكوتورب ىلع ضوافتلا متي ال ،الإو .(ةياەنلا ةقداصم لوكوتورب يأ نيكمتب ىصوي ،يقيقحلا ملاعلل ISE نيوكت يف RADIUS لاصتا وە امك ةقداصملاو ضوافتلا نم فلكملاو ISE نكمتي ىتح ةئيبلا يف ەمادختسا متي عقوتم

حومسملا لوكوتوربلا تامدخل ديدج ليثم ءاشنإ دنع (ةيوطملا) ةيضارتفالا ميقلا يه هذه

.ەب

💊 ربع ناقدصي انبلاطمو ISE نأل ارظن لـقألـا ىلع EAP-TLS نيكمت كـيلع بجي :ةظحالم اذه نيوكـتلا لـاثم يف EAP-TLS

Cotome Condet     Answerd Protocols     Answerd Protocols     Potting     Cotome     Answerd Protocols     National Protocols     Detailing     Answerd Protocols     Detailing     Detailing </th <th>E Cisco ISE</th> <th>Policy - Policy Elements</th> <th>Q © 58 @</th>	E Cisco ISE	Policy - Policy Elements	Q © 58 @
Automation of the provide state of the provide s	Dictionaries Conditions	Results	
Ausead Protection     Autonic Autonica     Autonica     Partine 1     Cater Provideo 1     Outonica     Outonica </th <th>Authentication ~</th> <th>Allowed Protocols Services List &gt; New Allowed Protocols Service</th> <th></th>	Authentication ~	Allowed Protocols Services List > New Allowed Protocols Service	
indication   indication <td>Allowed Protocols</td> <td>Allowed Protocols</td> <td></td>	Allowed Protocols	Allowed Protocols	
Image: Image	Authorization	Name Allowed_Protocols	
rung     Parke        cited Providening <b>Poter Other Deter De</b>	Brefiling >	Description	
Cited Providing     * Chrome Drococle     * Contraction Concocle     * Contraction Concle     <	Posture		
• And Wedd Protocols         • Process Hest Loway ①         • Process Hest Loway ②         • Process Hest Loway ②         • Process Hest Loway ③         • Process Hest Loway ③         • Process Hest Loway ③         • Process ●         • Process ● <t< td=""><td>Client Provisioning &gt;</td><td>- Allowed Desteads</td><td></td></t<>	Client Provisioning >	- Allowed Desteads	
		Authentication Bypass         Process Host Looking ()       MAB         Anow PAP/ASCB         Anow PAP/ASCB         Anow CHAP         Anow EAP-MDS         Anow Wask cohers for EAP ()         Anow Wask	ubmit Cancel

عفد ىلا EAP-TLS ةميق ىلع نيعملا لضفملا EAP لوكوتورب مادختسا يدؤي :ةظحالم ةطقنل IEEE 802.1x ببسم ىلا مدقي لوكوتورب لوأك EAP-TLS لوكوتورب بلط ىل ISE مظعم ىلع ابلاغ EAP-TLS ربع ةقداصملا يونت تنك اذا اديفم دادعإلا اذه نوكي .ةياهنلا ISE. عم اهتقداصم متت يتلا ةياهنلا طاقن

ضيوفتلا فيرعت فلم ءاشنإ .9 ةوطخلا

حنميو ليوختلا جەنب طبتري يذلاو ،ليوختلا فيرعت فلم وە ەۋاشنإ بولطم جەن رصنع رخآ ەذە نيوكتل ليوختلا جەنب طبترم ليوختلا فيرعت فلم .بولطملا لوصولا ىوتسم ادە نيوكتل اليوختلا جەنب طبترم ليوختلا فيرعت فلم . القيموسرلا مدختسملا قەجاو نم قەجاولا Add.

ىلإ ISE نم اەريرمت متي تامس ەنع جتني نيوكت ىلع ليوختلا فيرعت فلم يوتحي ىوتسملا قيقحتل تامسلا ەذە مادختسإ اەيف متي يتلاو ،ةنيعم RADIUS لمع ةسلجل .ةكبشلا ىلإ لوصولا نم بوغرملا

ىلإ لوصولا لوبق ريرمتب ةطاسبب موقي هنإف ،انه حضوم وه امكو ، راعشإلا ةمس ليصافت .ةيلوألا ةقداصملا دنع ةيفاضإ رصانع مادختسإ نكمي ،كلذ عمو امدنع NAD ىلإ ISE اهلسري يتلا تامسلا صخلم ىلع يوتحت يتلاو ،ةحفصلا لفسأ يف .نيعم ليوخت فيرعت فلم قباطت

=	Cieco	ISE
_	01300	1012

Dictionaries	Conditions	Results
Authentication	>	Authorization Profiles > New Authorization Profile Authorization Profile
Authorization	~	Autorization Frome
Authorization Pr	rofiles	* Name Basic_Access
Downloadable AC	ls	Description
Profiling	>	
Posture	>	* Access Type
<b>Client Provisioning</b>	, >	ACCESS_ACCEPT V
		Network Device Profile 🏥 Cisco 🗸 🕀
		Service Template
		Track Movement 🔲 🕢
		Agentiess Posture
		Passive Identity Tracking 🗌 🕜
		A Common Teolo
		<ul> <li>Common tasks</li> </ul>
		DACL Name
		PP6 DACL Name
		ACL (F(Rer-ID)
		ACL 8-46 (Fitter-10)
		V Advanced Attributes Settings
		V Attributes Details
		Access Type = ACCESS_ACCEPT
		Submit Cancel

جەنلا رصنع - ليوختلا فيرعت فلم

لوؤسم ليلد يف جەنلاو ISE ليوخت فيرعت فلم لوح تامولعملا نم ديزم ىلع روثعلا نكمي ISE ليوؤسم ليل مي اليل ليوخت في Cisco Identity Services، ل<u>ليوختلا</u> تا<u>سايس</u> < ةئزجتلا: لصفلا

### نامألا تاسايس

حتاب الحاية (ISE) قيموسرلا مدختسملا قمجاو نم ضيوفتلاو ققداصملا تاسايس ءاشنإ متي Policy Sets. تيبثت دنع ISE 3.x. نوكي الكشب رصانعلا هذه نيكمت متيو جهنلا قعومجم يوتحت .قيضارتفالا جهنلا قعومجم يهو ،قفرعم قدحاو جهن قعومجم امئاد كانه اقبسم قددحملا ءانثتسالاو ضيوفتلاو ققداصملا جهن دعاوق ىلع قيضارتفالا .قيضارتفالاو

تاسايسلا عيمجتب ISE لوؤسمل حمسي امم ،يمره لكشب جەنلا تاعومجم نيوكت متي دودح ال .ةقداصم بلط يف مادختسالل ةفلتخم تاعومجم ىلإ ،ضرغلا ثيح نم ،اعم ةلثامملا ةدحاو جەن ةعومجم مادختسإ نكمي ،وحنلا اذه ىلعو .ايلعف عيمجتلاو صيصختلا جەنل جەن ةعومجم مادختسإ نكمي امنيب قكبشلا ىل لوصولل ةيكلسال ةياەن ةطقن ةقداصمل قديرف ىرخأ ةقيرط يأل وأ ؛ةكبشلا ىلإ لوصولل ةيكلسلا ةياەنلا الاق الالال الارمال ىرخأ

ِ جەنلا اذە نمض ةدوجوملا تاسايسلاو تاسايسلا تاعومجم مييقتب Cisco ISE موقي نا نكمي

طورش عيمج مييقت متي امدنع الوأ ةنيعم تاسايس ةعومجم ةقباطمل لفسأ ىلإ ىلعأ نم تاسايس مييقتب اهساسأ ىلع ISE موقي يتلاو ،ةحيحص اهنأ ىلع قروكذملا ةعومجملا يلي امك تاسايسلا ةعومجم عم قفاوتي ام نمض ليوختلا تاسايسو ةقداصملا:

- تاسايسلا ةعومجم طورشو تاسايسلا ةعومجم مييقت .1
- ةقباطملا جەنلا ةعومجم نمض ةقداصملا جەن .2
- ةيلحملا تاءانثتسالا ليوختلا جەن .3
- ةماعلا تاءانثتسالا ضيوفتلا ةسايس .4
- ليوختلا جەن .5

تاسايس ةعومجم نمض ايلحم وأ جەنلا تاعومجم ةفاكل ماع لكشب جەنلا تاءانثتسإ دجوت عم لماعتت اەنأل ارظن ،ليوختلا جەن نم ءزجك ەذە جەنلا تاءانثتسإ عم لماعتلا متي .ةددم نيعم تقۇم ويرانيسل ةكبشلا ىلإ لوصولل اەحنم متي يتلا جئاتنلا وأ تانوذألا.

ةقداصم جەنب طبرلل ةسايسلاو نيوكتلا رصانع جمد ةيفيك يلاتلا مسقلا يطغي ربع ةياەن ةطقن ةقداصمل ISE ليوختو

جەنلا ةعومجم ءاشنإ .10 ةوطخلا

ريشت مدختسملا لبق نم ةفرعم ةدحاو ةدعاق نم نوكتت ةيمره ةيواح نع ةرابع جەنلا ةعومجم ىلا ةفاضإلاب ،ةكبشلا ىل لوصولل مداخلا لسلست وأ ەب حومسملا لوكوتوربلا ىل مادختساب اضيأ اەنيوكت مت يتلاو ،جەنلا تاءانثتساو ضيوفتلاو ققداصملا تاسايس مدختسملا لبق نم ةفرعم طورشلا ىلع ةمئاق دعاوق.

مث Policy > Policy Set ىلإ لقتنا ، (ISE) ةيموسرلا مدختسملا ةهجاو نم تاسايس ةعومجم ءاشنإل ةروصلا هذه يف حضوم وه امك ،ىرسيلا ايلعلا ةيوازلا يف (+) دئاز ةنوقيأ رقنا.

E Cisco ISE	Policy • Policy Sets	২ ৩	50	٢
Policy Sets	Reset Reset Policyset Hitcounts		Save	
Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits	Action	s Vie	w
Q Search				

ةديدج جەن ةعومجم ةفاضإ

متيو اقبسم ەنيوكت مت يذلا اذه جەنلا رصنع جمد/طبرب جەنلا ةعومجم موقت نأ نكمي ققداصم بلط يف اەتقباطم متيس يتلا جەنلا ةعومجم ديدحتل ەمادختسإ Request):

اهب حومسملا تالوكوتوربلا تامدخ :طبرلا

=	Cis	sco IS	E				Policy - Policy Sets					(	Q ()	50	0
Po	licy S	iets							Reset	Reset Policy:	set Hitc	ounts		Save	
<sup>1)</sup> [	● s	tatus Search	Policy Set Name	Description	Con	ditions			Allowed Protocol	s / Server Sequ	ence	Hits	Actions	s Vier	w )
		o <sup>2</sup>	EAP-TLS Example		AND	3) E	Radius Service-Type EQUALS Framed Network Access Protocol EQUALS RADIUS	4)	Allowed_Protoco	Ns 🙁	-+	0	٨	,	
		•	Default	Default policy set					Default Network	Access 🙁 🕚		0	٥	>	
											R	Reset		Save	

اهب حومسملا تالوكوتوربلا ةمئاقو جەنلا ةعومجم طورش فيرعت

تسلج يف رەظت نأ اەنأش نم ةنيعم ميقو تامس لاثملا اذە مدختسي ADIUS ضرفل RADIUS تسلي الاف مدختسي RADIUS. 802.1x لوكوتورب ضرف ةداعإل رركتم نوكي نأ لمتحملا نم ەنأ مغر ،(framed قمس) RADIUS قربطنت يتلا طقف ةديرفلا RADIUS تسلج تامس مدختسأ ،جئاتنلا لضفأ ىلع لوصحلل 802.1x وأ يكلسلا 802.1x ب قصاخلا وأ ةكبشلا ةزهجأ تاعومجم لثم ،ةبولطملا ةهجولا ىلع يكلساللا 802.1x و يكلساللا

ليلد يف ISE ب ةصاخلاا تاسايسلا تاعومجم لوح تامولعملا نم ديزم ىلع روثعلا نكمي ،<u>تاسايسلا تاعومجم</u> < ةئزجتلاا :لصفلا < 3.1 رادصإلا، Cisco Identity Services لوؤسم، <u>ضيوفتلا تاسايس ماسقا</u>و ،<u>ققداصملا تاسايس</u>.

ةقداصم ةسايس ءاشنإ .11 ةوطخلا

اەنيوكت مت يتلا ەذە جەنلا رصانع عيمجت/طبرب ةقداصملا جەن موقي ،جەنلا ةعومجم لخاد ةقداصم ةدعاق ةقباطم بجي ىتم ديدحتل طورشلا عم اەمادختسإ متيل اقبسم.

· .ةيوەلا ردصم لسلست وأ ةداەشلا ةقداصم فيرعت فلم :طبرلا.

•	1) Status	Rule Name	Cond	litions			Use		Hits	Actions
0	Search	2) EAP-TLS	AND	3) 2 OR	Network Access-EapAuthentication EQUALS EAP-TLS	4)	Identity_Sequence	× 20	0	\$
	0	Default					If Process fail DROP DenyAccess	Si	0	\$

ةقداصملا ةسايس ةدعاق لاثم

V Authentication Policy (2)

ليوختلا جەن ءاشنإ .12 ةوطخلا

اەنيوكت مت يتلا ەذە جەنلا رصانع عيمجت/طبرب "ليوختلا جەن" موقي ،"جەنلا ةعومجم" لخاد انە لاثملاو .ليوختلا ةدعاق ةقباطم بجي ىتم ديدحتل طورشلا عم اەمادختسإ متيل اقبسم Active يف لاجملا يمدختسم نامأ ةعومجم ىلإ ريشت طورشلا نأل ارظن مدختسملا ةقداصم وە Directory.

ليوختلا فيرعت فلم :طبرلا

> Authorization Policy - Local Exceptions						
> Authorization Policy - Global Exceptions						
$\sim$ Authorization Policy (2)						
1)		Results				
Status Rule Name	Conditions	Profiles	Security Groups		Hits Acti	ions
Q Search						
2) Basic Permit Access	AND     Retwork Access AuthenticationStatus EQUALS AuthenticationPlassed     AD     Retwork Access AuthenticationStatus EQUALS AuthenticationPlassed     AD     Retwork Access AuthenticationStatus EQUALS AuthenticationPlassed     Ad	Basic_Access ×	→ + Select from list	~+	• {ĝ	\$
Oefault		DenyAccess ×	V + Select from list	~+	•	₽
					5)	
				Reset	Sa	we

ليوختلا ةسايس ةدعاق لاثم

ليثم نم ةعومجملاا ةفاضإ بجي ،(LDAP وأ LDAP نم لثم) ةيجراخ ةعومجم ةفاضإل المداخلال مداخلا مداخلا ISE: Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups. مدخ ص نم Directory [AD Join Point Name] > Groups. مدخ ص نم Directory ومجملا لك نع ثحبلل مسالا حشرم مدخ تساو Directory [ كار مسال الحشرم مدخ تساو الالحميان المواجع الم

■ Cisco ISE			Administration • Identity Management
Identities Groups External Iden	ntity Sources	Identity Source Sequences	Settings
External Identity Sources	Connection	Allowed Domains PassiveID	1) Groups Attributes Advanced Settings
> 🗀 Certificate Authentication F	C Edit + Ad	dd 🔨 📋 Delete Group Update	SID Values
Active Directory	s	ielect Groups From Directory 3)	∧ SID
👻 AD1		dd Group	<omitted as="" be="" intentionally="" sid="" unique="" value="" would=""></omitted>
> 🛅 LDAP			

ليلدلا نم ةعومجم ةفاضاٍ بجي ،ISE جەن يف ةيجراخ تاعومجم مادختسال

### Select Directory Groups

This dialog is used to select groups from the Directory.

Domain	example.com				
Name Filter	*domain users*	SID * Filter		Type ALL Filter	
	Retrieve Groups 1 Groups Retrie	eved.			
	Name	^	Group SID		Group Type
	example.com /Users/Domain Use	ers	<omitted inte<="" sid="" th=""><th>entionally&gt;</th><th>GLOBAL</th></omitted>	entionally>	GLOBAL

Cancel	ок

Active Directory لائم - يجراخلا ليلدلا نمض ثحبلا

رقنلا سنت ال .ISE لخاد جەنلا مادختسإ كنكمي ،ةعومجم لك راوجب رايتخالا ةناخ ديدحت دعب تارييغتلا ظفحل ظفح وأ/و قفاوم قوف.

# ةحصلا نم ققحتلا

جيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

نيوكتلا ودبي ،جەنلا ةعومجم طبرب جەنلاو ماعلا نيوكتلا رصانع عيمج موقت نأ درجمب ربع مدختسملا ةقداصمل ةروصلا ەذەل اەباشم

sco ISE		Policy - Policy Sets		Q	0 24
Sets→ EAP-TLS Example			Reset Reset Policyse	t Hitcounts	Sav
tus Policy Set Name De	scription Conditions		Allowed Protoc	ols / Server Se	quence
Search					
EAP-TLS Example	AND L Radius Service-Type EQUALS Framed Network Access Protocol EQUALS RADIUS		Allowed_Prot	ocols 🤇	<u>a ~</u> +
hentication Policy (2)					
Status Rule Name	Conditions		Use	Hit	ts Action
Q Search					
	Network Access EspAuthentication EQUALS EAP-TLS		Identity_Sequence  Options  If Auth fail  PE INCY	<u>8</u> ~	
EAP-TLS	AND OR Wred_M02.1X Wredess_802.1X		If User not found REJECT If Process fail DROP		ø
			DenyAccess	<u>a</u> ~	
Default			Options     If Auth fail     REJECT     If User not found	<u> </u>	¢
			REJECT If Process fail DROP	03 ~ 03 ~	
uthorization Policy - Local Exceptions uthorization Policy - Global Exception	i de la constante de				
uthorization Policy (2)					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups		lits Act
Q Search					
Basic Permit Access	AND & Network Access AuthenticationStatus EQUALS AuthenticationPassed A ADI-EnternalGroups EQUALS example.com/Users/Domain Users	Basic_Access ×	~+ Select from list	~+	• {ĝ

اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي تامولعم مسقلا اذه رفوي.

ىلع روثعلا نكميو .ةقداصملا رابتخال ةياەنلا ةطقن ليصوتب مق ،نيوكتلا لامتكا دعب راتخن .ISE رادصإلاب ةصاخلا (GUI) ةيموسرلا مدختسملا ةەجاو يف جئاتنلا Live Logs، دام وه امك ،قروصلا ەذە يف حضوم وه امك

طاشن/تالواحمل (زاهجلا لوؤسم) +TACACS و RADIUS ل ةيح تالجس رفوتت ،ةيعوتلل اذه ةيؤر يف بغرت تنك اذإ .ةيضاملا ةئاملا تالجسللو ةيضاملا ةعاس 24 ىتح ةقداصملا هجو ىلعو ،ريراقتلا مادختسإ كيلعف ،ينمزلا راطإلا اذه دعب ريراقتلا تانايب نم عونلا ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications.

≡ Cisco ISE				Operations -	RADIUS					0.0.20
Live Logs Live Sessions										
Misconfigured Supplicants 🕕		lisconfigured Network Devic	:es ()	RJ	ADIUS Drops 🕕	Client	Stopped Respondin			Repeat Counter 🕢
0	0 0				0		0			0
Ø Refresh 🕁 Reset Repeat Counts 🖒 Export To ∨								Refresh Novor	Show Latest 20 reco	✓ Within ↓ Last 3 hours ↓ ✓ Filter ↓ ♦
Time Status	Details Repeat	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Posture St Server	Mdm Serve
×	<u>×</u> *									
May 10, 2022 09:35:15.460 PM	<b>0</b> 0	employee1	00.00.AA.11.22.33	EAP-TLS Example >> EAP-TLS	EAP-TLS Example >> Basic Permit Access	Basic_Access			ise3	
May 10, 2022 09:35:15.460 PM	0	employee1	00.00.AA:11:22:33	$EAP\text{-}TLS\;Example \mapsto EAP\text{-}TLS$	EAP-TLS Example >> Basic Permit Access	Basic_Access	Switch		ise3	
Last Updated: Twe May 10 2022 21:37:03 GMT-0	500 (Central Daylight Time)									Records Shown:2

ةرشابملا تالجسلا < RADIUS نم جارخإ لاثم

يت الجس يف RADIUS قسلج نع تامولعم دجت نأ عقوتت ،ISE يف قرشابملا RADIUS تالجس يف قفدت ءانثأ ظحالملا كولسلا صيخشتل ىرخأ قديفم تامولعمو ،قسلجلا تامس نمضتت ضرعل لمعلا قسلجل قيليصفتلا ضرعلا ققيرط حتفل زمرلا details قوف رقنا .ققداصملا .وذه ققداصملا قلواحمب قصاخلا قلصلا تاذ تامولعملاو لمعلا قسلج تامس

لاثمل .ةحيحصلا تاسايسلا قباطت نم دكأتلا مەملا نم ،اەحالصإو ءاطخألا فاشكتسال وه امك ،عقوتم وه امك ةبولطملا ضيوفتلاو ةقداصملا تاسايس قباطت متي ،اذه نيوكتلا ةروصلا يف حضوم:

Authentication Policy	EAP-TLS Example >> EAP-TLS
Authorization Policy	EAP-TLS Example >> Basic Permit Access
Authorization Result	Basic_Access

ةقداصملا نأ نم ققحتلل تامسلا هذه نم ققحتلا متي ،ةيليصفتلا ضرعلا ةقيرط يف اذه نيوكتلا لاثم نم ءزجك ميمصت لكل عقوتملا وحنلا ىلع فرصتت

ثدح •

- ال مأ ةحجان ةقداصملا تناك اذإ ام ىلع اذه يوتحي 🗉
- . جاجنب 5200 ةقداصم تمت :ةميقلا نوكت لمعلا ويرانيس يف 🗉
- Username
  - ∍ اەميدقت مت يتلا ليمعلا ةداەش نم اەبحس مت يتلا ةيئاەنلا ةيوەلا لمشي اذەو يلإ ISE.
  - اليجست مت يذلا مدختسملاب صاخلا مدختسملا مسا وه اذه ،لمعلا ويرانيس يف (ققباسلا ةروصلا نم 1 فظوملا يأ) ةياهنلا ةطقن ىلإ هلوخد.
- ةياەنلا ةطقن فرعم

  - َ ربع لاصتالا نكي مل ام ةياهنلا ةطقنل MAC ناونع اذه حبصي ،لمع ويرانيس يف قياهنلا ةطقنل IP ناونع نوكي نأ نكمي ةلاحلا هذه يف ،VPN

- ةقداصملا جەن
  - َةسلج تامس ىلإ ادانتسا ةددحملا لمعلا ةسلجل قباطتملا ةقداصملا جەن راەظا جەنلا طورش قباطت يتلا لمعلا.
  - اەنيوكت مت امك ةعقوتملا ةقداصملا ةسايس وه اذه ،لمعلا ويرانيس يف 🗉
  - طورشلاب اەتنراقم دنع ةعقوتملا ةسايسلا نأ ينعي اذەف ،ىرخأ ةسايس تيأر اذإ مق ،ةلاحلا ەذە يف .ةحيحص ةسايسك اەمييقت متي مل ةسايسلا يف ةدوجوملا ةفلتخم طورش ىلع يوتحت ةسايس لك نأ نم دكأتو لمعلا ةسلج تامس ةعجارمب .ةسايس لكل ةديرف نكلو
- ليوختلا ةسايس
  - ة المات المات المات المعلام المعلام المعلام المعلام الت المات المات المعال المعلام المعلى المعلى المعلى المعل ا جەنل المورش قب اط ت ي ت ل المعل.
  - اهنيوكت مت امك ةعقوتملا ليوختلا ةسايس وه اذه ،لمعلا ويرانيس يف 🗉
  - طورشلاب اەتنراقم دنع ةعقوتملا ةسايسلا نأ ينعت اەنإف ،ىرخأ ةسايس تيأر اذإ مق ،ةلاحلا ەذە يف .ةحيحص اەنأ ىلع اەمييقت متي مل ،ةسايسلا يف ةدوجوملا ةفلتخم طورش ىلع يوتحت ةسايس لك نأ نم دكأتو ةسلجلا تامس ةعجارمب .ةسايس لكل ةديرف اەنكلو
- دامتعالا ةجيتن
  - مت يذلا ليوختلا فيرعت فلم اذه ضرعي ،قباطتملا ليوختلا جەن ىلإ ادانتسا ةددحملا لمعلا ةسلج يف ەمادختسإ.
  - َ ، ةسايسلا يف اەنيوكت مت يتلا ةميقلا سفن ەذە نوكت ،لمعلا ويرانيس يف ليوختلا فيرعت فلم نيوكت نم دكأتلاو قيقدتلا ضارغأل ةعجارملا ديجلا نم حيحصلا
- جەنلا مداخ
  - اهتكراشم مت يتلا (PSN) ISE قسايس ةمدخ ةدقعل فيضملا مسا كلذ نمضتيو · ةقداصملا ةلواحم يف.
  - يلوألاا PSN ةدقع ىلإ لقتنت يتلا تاقداصملا الإ ىرت ال ،لمعلا ويرانيس يف ديق PSN نكي مل ام ،(ةفاحلا زاهج مساب اضيأ فورعملا) NAD ىلع اهنيوكت مت امك اذإ وأ عقوتملا نم ىلعأ لوصو نمز ببسب لثم ،لشفلا زواجت ثدح اذإ وأ ليغشتلا .ةقداصم ةلهم تثدح
- ةقداصٍملا بولسأ
  - ِ ،لااثملا اذهل .ةددحملا لمعلا ةسلج يف همادختساٍ مت يذلا ةقداصملا بولسأ ضرع، قائمة عليه علي قميقلا عرت dot1x.
  - َ تيأر اذإ .dot1x ةميقلا ىرت ،اذه نيوكتلا لاثم ىلإ ادانتسا ،لمع ويرانيس يف قلواحم مدع وأ dot1x لشف كلذ ينعي دقف ،ىرخأ ةميق.
- ةقداصملا<mark>ً</mark> لوكوتورب
  - َ ليبس ىلع .ةددحملا لمعلا ةسلج يف همادختسا مت يذلا ةقداصملا بولسأ ضرع قئيه ىلع ةميقلا ىرت ،لاثملا EAP-TLS.
  - اەنأ ىلع امئاد ةميقلا ىرت ،اذە نيوكتلا لاثم ىلإ ادانتسا ،لمع ويرانيس يف EAP-TLS حاجنب اضوافتي مل SE و سمتلملا نإف ،ىرخأ ةميق تيأر اذإ
- ەكبشلا زاەج •

- مساب اضيأ فورعملا) NAD ل ،ISE يف ەنيوكت مت امك ،ةكبشلا زاەج مسا رەظي ∘ ISE. و ةياەنلا ةطقن نيب ةقداصملا ةلواحم يف لومشملا (ةفاحلا زاەج
- مدختسم ةهجاو يف مسالا اذه ءاطعإ امئاد متي ،لمعلا ويرانيس يف
   System: Network Devices. ب صاخلا IP ناونع مادختسإ متي ،نيوكتلا اذه ىلإ ادانتسا
   NAD (من تعاج يذلا ةكبشلا زاهج ديدحتل (قفاحلا زاهج مساب اضيأ فورعملا)
   NAD ناونع مادة العامي المالية الم

فاشكتسال ةعجارملل ةنكمملا ةسلجلا تامس لك نم ةلماك ةمئاق هذه نأ كلذ ينعي ال ىصوي .ققحتلل ةديفم ىرخأ تامس كانه نأ امب ،ىرخأ ةيؤر ضارغأل وأ اهحالصاو ءاطخألا ىرت نأ كنكمي .تامولعملا ةفاك ىلع فرعتلا ءدبل لمعلا ةسلج تامس ةفاك ةعجارمب هب ماق يذلا كولسلا وأ تايلمعلا رهظي يذلا ،مسقلا تاوطخ نمض نميألا بناجلا نيمضت ISE.

اهحالصإو ءاطخألا فاشكتسال ةمدختسملا بيلاسألاو ةعئاشلا تالكشملا

،اەحالصإو تالكشملا فاشكتسأ حئاصنو ةعئاشلا تالكشملا ضعب ةمئاقلا ەذە نمضتت، دشرمك اذه مدختسأ ،كلذ نم الدبو .ةلماك ةمئاق نوكت نأ لاوحألا نم لاح يأب اەب دصقي الو ISE. ةكراشم دنع اەحالصإو لكاشملا فاشكتسال ةصاخلا كتاينقت ريوطتب مقو

ريغ ىرخأ ةقداصم ةلواحم يأ وأ (5400 ةقداصم تلشف) ةقداصملا لشف هجاوت :ةلكشملا ةحجان.

- تامولعم يطعي يذلا ليصافتلا زمر قوف رقنا ،ةقداصملا يف لشف ةهجاوم ةلاح يف ببسلاو لشفلا ببس لمشي اذهو .ةذختملا تاوطخلاو ةقداصملا لشف ببس لوح لمتحملا يرذجلا.
- تامولعملا ىلع رفوتي ISE نإف ،ةقداصملا ةجيتن نأشب رارقلا ذختي ISE نأل ارظنو ةقداصملا ةلواحم حاجن مدع ببس مەفل ةمزاللا.

ةروجەملا EAP لمع ةسلج" لشفلا ببس رەظيو حاجنب ةقداصملا لمتكت ال :ةلكشملا الالات ISE". يلإ ةباجتسالا نع 5411 لومم فقوت" وأ "ةديدج تأدبو 5440 ةياەنلا ةطقنل

- نأ امب .تيقوتلا ءاهتنا لبق RADIUS لاصتا لامتكا مدع ىلإ اذه لشفلا ببس ريشي متي يتلا ةلهملا نم ققحتلا ىلإ جاتحت كنإف ،NAD و ةياهنلا ةطقن نيب عقي EAP ل.لقألا ىلع ناوث سمخ ةدمل اهنييعت نم دكأتلاو NAD ىلع اهمادختسإ.
- ناوث سمخب اەتدايز نسحتسملا نمف ،ةلكشملا ەذە لحل ةيفاك ناوث سمخ نكت مل اذا .ةلكشملا ەذە لحي بولسألا اذە نأ نم ققحتلل طبضلا ةداعاو تارم عضب
- ةقداصملا ةجلاعم نامضب ىصويف ،ةقباسلا تاوطخلا نم ةلكشملا لح متي مل اذا كولسلا ىل يلمجإلا كولسلا ريشي الو ،ةحيحصلاو اهسفن ISE PSN ةدقع ةطساوب (دقع) ةدقع ISE PSN و NAD نيب يداعلا نم ىلعأ لاقتنا نمز لثم ،يعيبطلا ريغ.
- لالخ نم ليمعلا ةداهش لسرت ةياهنلا ةطقن تناك اذإ امم ققحتلل ةديج ةركف اهنأ امك تاداهش) ةياهنلا ةطقنل نكمي ال مث ،ليمعلا ةداهش ISE ملتسي مل اذإ مزحلا طاقتلا داريتساب مق ،ةحيحص ةميقلا نأ دجو اذإ .ISE EAP ةقداصم ةداهشب قوثولا (مدختسملا

عجرملا = رذجلا قدصملا عجرملا) ةحيحصلا تاداهشلا نزاخم يف قدصملا عجرملا ةلسلس (هب قوثوملا طيسولا CA = طيسولا CA | هب قوثوملا رذجلا قدصملا).

حيحصلا ليوختلا جهن وأ/و ةقداصملا قباطت ال اهنكلو ،ةحجان ةقداصملا :ةلكشملا.

- ، ،ةحيحصلا ليوختلا وأ/و ةقداصملا دعاوق قباطي ال ەنكلو ،احجان ةقداصم بلط تەجاو اذا ةقيقد ةمدختسملا طورشلا نأ نم دكأتلل ةسلجلا تامس ةعجارم نسحتسملا نمف RADIUS. قسلج يف ةدوجومو
- (عضولاا تاسايس ءانثتساب) لفسأ ىلإ ىلعأ نم جەن نم تاسايسلا ەذە ISE ميقيو. بولطملا جەنلا لفسأ وأ ىلعأ ەتقباطم مت يذلا جەنلا ناك اذإ ام ديدحت الوأ كيلع بجي جەن نع لقتسم لكشبو الوأ ةقداصملا ةسايس مييقت متي .ەتقباطم متيل ةقداصم ريرمت متي ،حيحص لكشب ةقداصملا ةسايس قوباطم ةلاح يف .ليوختلا ."تاوطخلا" ىمسملا رسيألا مسقلا تحت ةقداصملا ليصافت يف 22037
- عومجم نأ ينعي اذهف ،ةقباطملا ةسايسلا نم ىلعأ ةبولطملا ةسايسلا تناك اذإ لك عجاري وه .حيحص هنأ ىلع همييقت متي مل ةبولطملا ةسايسلا يف طورشلا أطخ دجوي الو دوجوم وه تنمض in order to ةسلجلا يفو ةلاحلا يف ميقلاو صئاصخلا يئالمإ
- ىرخأ ةسايس نأ ينعي اذهف ،ققباطملا ةسايسلا نم لقأ ةبولطملا ةسايسلا تناك اذإ طورشلا ميق نأ كلذ ينعي دق .قبولطملا ةسايسلا نم الدب اهتقباطم تمت (ىلعأ) جەنلا بيترت نأ وأ ،رخآ جەن يف اەراركت مت دق طورشلا نأ وأ ،يفاك لكشب ةددحم تسيل ءدبب ىصوي ،ةبوعص رثكأ اەحالصإو ءاطخألا فاشكتسأ حبصي امنيبو .حيحص ريغ ىلع دعاسي اذەو .ةبولطملا ةسايسلا قباطت مدع ببس ديدحتل تاسايسلا ةعجارم .قيلاتلا قاردرا يف اەذاختا يف اەراركا يف اوراد

ةميقلا ةقداصملا ءانثأ مدختسملا مدختسملا مدختسملا مسا وأ ةيوهلا نكت مل :ةلكشملا ةعقوتملا.

- ال حجرألاا ىلع ISE نإف ،ليمعلاا ةداەش لسرت ةياەنلاا ةطقن تناك اذإ ،كلذ ثدحي امدنع ەمييقت متي يذلاو ،"ةداەشلا ةقداصم بلاق" يف حيحصلا ةداەشلا لقح مدختسي .ةقداصملا ةلحرم ءانثأ
- نامضو مدختسملا مسا/ةيوەلل بولطملا لقحلا عقوم ديدحتل ليمعلا قداەش عجار : ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).

عجرم ببسب EAP-TLS 12514 SSL/TLS كاصتا ببس لشف عم ةقداصملا حجنت ال :ةلكشملا ليمعلا تاداهش ةلسلس يف فورعم ريغ قدصم.

• ريغ CA ةلسلس يف ةداەش ىلع يوتحت ليمعلا ةداەش تناك اذإ كلذ ثدحي نأ نكمي ISE: Administration > System: Certificates > Trusted Certificates.

- كا ةلسلس ىلع (ةياەنلا ةطقن ىلع) ليمعلا ةداەش يوتحت امدنع كلذ ثدحي ام ةداعو قوداصمل ISE ىلع ةعقوملا CA تاداەشلا ةلسلس نع فلتخت EAP.
- ليمع الحمي ال المي المي الحمي ا المي المي المي الحمي ال

اهب قوثوم نوكتل (ةيئاهنلا ةيوهلا ةداهش سيلو) CA ةلسلس داريتسإ :Firefox ل بيو مداخل.

### ةلص تاذ تامولعم

- <u>مېۋرتلاو تېپثتلا</u> ةل<u>دأ</u> < Identity Services Engine ةيوەلا تامدخ كرحم
- <u>نيوكتلا ةلدأ</u> < Identity Services Engine ةيوهلا تامدخ كرحم
- Cisco Identity Services Engine > <u>قفاوتلا تامولعم</u>
- < نمآلا لوصولا: لصفلا < 3.1 رادصإلا، Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد</li>
   < نمآلا لوصولا: لصفلا < 3.1 رادصإلا، Cisco التحمي </li>
- <u>تاعومجم</u> < ةئزجتلا :لصفلا < 3.1 رادصإلا ،Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد <u>تاسايسلا</u>
- <u>تاسايس</u> < ةئزجتلا: :لصفلا < 3.1 رادصإلا، Cisco نم ةيوەلا تامدخ كرحم لوؤسم ليلد <u>ققداصملا</u>
- <u>تاسايس</u> < ةئزجتلا: :لصفلا < 3.1 رادصإلا، Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد <u>ليوختلا</u>
- Cisco Identity Services Engine (<u>لماكت</u> < نيوكتلا ةلدأ < Cisco Cisco) نم ةيوهلا تامدخ كرحم <u>Active Directory عم Cisco ISE 2.x</u>
- ةمدخ < ةئزجتلا :لصفلا < 3.1 رادصإلا ،Cisco نم ةيوەلا تامدخ كرحم لوؤسم ليلد <u>ةكبشلا ىل نيمدختسملا لوصو</u> < ةكبشلا ىل لوصولا
- <u>قرادا</u> < يساسأ دادعإ :لصفلا < 3.1 رادصإلااً ،Cisco، نَّمَ ةيوەلاً تامدخ كرحّم لوؤسم ليّيلد <u>قرادا</u> < <u>Cisco ISE</u> <u>يف تاداەشلا</u>
- يساسألاا دادعإلاا :لصفلاا < 3.1 رادصإلاا ،Cisco نم ةيوهلاا تامدخ كرحم لوؤسم ليلد قمدخ Gisco ISE CA تيوكت < Cisco ISE مدخ الا مادختسال Cisco ISE مادخ ت<u>وكت < TLS كارا دنتست ققداصمل قداهشلاا ققداصم فيرعت فلم عاشنا</u> <
- Cisco Identity Services Engine (و نيوكتلا ةلثمأ < Cisco Identity Services Engine) تامدخ كرحم TechNotes > قدامش دادم قباوب نيوكت < ISE 2.0</li>
- Cisco Identity Services Engine (و نيوكتلا ةلثمأ < Cisco) نم ةيوهلا تامدخ كرحم ISE يف <u>ةيجراخ ةمج لبق نم CA نم قعقوم ةدامش تيبثت</u> < TechNotes
- مەف < ةينف تاظحالمو نيوكت ةلثمأ < (WLAN) ةيكلسال ةيلحم ةكبش <u>ISE و WLC مادختساب ەنيوكتو</u>
- Cisco Systems تادنتسملاو ينقتلا معدلا

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما