يف مكحتلا تادحو عم EAP-FAST ةقداصم تامدخ كرحمو ةيكلساللا ةيلحملا ةكبشلا ةيوهلا

تايوتحملا

<u>ةمدقملا</u> <u>ةىساسألا تابلطتملا</u> <u>تابلطتملا</u> ةمدختسملا تانوكملا <u>تاحالطصالا</u> <u>ةيساساً تامولعم</u> <u>يمحملا لوصولا تاغوسم</u> <u>يمحملا لوصولا تاغوسم ريفوت عاضواً</u> نىوكترا <u>ةكبشلل ىطىطختاا مسراا</u> <u>تانيوكتلا</u> <u>EAP-FAST ةقداصمل ةيكلساللا ةيلحملا ةكبشلا يف مكحتاا رصنع نيوكت</u> <u>لالخ نم RADIUS ةقداصمل (WLC) ةيكلس اللاا ةيلحملا ةكبش لاا يف مكحتايا رصنع نيوكت</u> يجراخ RADIUS مداخ EAP-FAST ةق داص مل WLAN ةكتش نى وكت EAP-FAST ةقداصمل RADIUS مداخ نىوكت EAP-FAST ءالمع ةقداصمل مدختسم تانايب ةدعاق ءاش<u>نا</u> <u>مداخ يلام AAA ليمعك (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتاا رصنع ةفاضا</u> RADIUS <u>قاطنلا لخاد لوهجم PAC دادما مادختساب RADIUS مداخ يلع EAP-FAST ققداصم نيوكت</u> <u>مىلع قدصملا قاطنلا لخاد PAC دادما عم RADIUS مداخ ىلع EAP-FAST ققداصم نىوكت</u> <u>قحصلا نم ققحتلا</u> <u>NAM فيرعت فلم نيوكت</u> .EAP-FAST ةقداصم مادختسات SSID ت لاصتالا ريتخا <u>ISE ةقداصم تالجس</u> لِماكلا EAP-FAST قِفَدَت عَلَّع WLC بِنَاج ءَاطَخاً حَيَّحَصَتِ اهحالصاو ءاطخألا فاشكتسا

ەمدقملا

(WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا ةدحو نيوكت ةيفيك دنتسملا اذه حرشي نمآلا يقفنلا لاصتالا ةقداصم ربع ةنرم ةقداصم - (EAP) عسوتملا ةقداصملا لوكوتوربل (ISE) ةيوهلا تامدخ كرحم اذه نيوكتلا لاثم مدختسي .يجراخ RADIUS مداخ مادختساب (FAST) مداخ RADIUS مداخك

اهيلع قدصملا (PAC) يمحملا لوصولا تاغوسمل ISE نيوكت ةيفيك ىلع دنتسملا اذه زكري نييكلساللا ءالمعلا ىلإ (يئاقلتلا) قاطنلا لخاد ةلوهجملاو.

ةيساسألا تابلطتملا

تابلطتملا

نيوكتلا اذه ءارجإ لواحت نأ لبق ةيلاتلا تابلطتملا ءافيتسا نم دكأت:

- Cisco WLCs و Lightweight (LAPs) عضولاا يف لوصولا طاقن نيوكتب ةيساسأ ةفرعم •
- CAPWAP لوكوتوربب ةيساساً ةفرعم •
- Cisco ISE لِثم ،يجراخلا RADIUS مداخ نيوكت ةيفيك ةفرغم •
- ةينورتكلإلاا لوصولاً طاقنل ماعلاً راطإلاب ةقلعتملاً ةيفيظولاً فراعملاً •
- تاداهشلا ةفرعمو ،EAP-GTC و MS-CHAPv2 لَتْم ،نامألاا تالوكُوتُوربب ةيساسأ ةفُرغم قيمقرلا

ةمدختسملا تانوكملا

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

• Cisco 5520 Series WLC رادصإلاا ،تباثلا جمانربلا لغشي يذلا 8.8.111.0cisco 4800 sery APAnyConnect NAM.Cisco Secure ISE، الدصإلاا دم 2.3.0.298 قلسلس لوحم 15.2(4)E1 رادصإلاا لغشي يذل

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 ،ةرشابم كتكبش.

تاحالطصالا

<u>تاحالطصا لوح تامولعملا نم ديزم ىلع لوصحلل ةينقتلا Cisco تاحيملت تاحالطصا عجار</u> <u>تادنتسملا</u>.

ةيساسأ تامولعم

لوكوتورب EAP-FAST ون الله ماع لكشب هيلإ لوصولاا نكمي IEEE 802.1X EAP لوكوتورب عون رشن نوديريو ةيوق رورم ةملك ةسايس ضرف نوعيطتسي ال نيذلاا ءالمعلاا معدل Cisco المعن مقرر تاداهش بلطتي ال 802.1X EAP.

لوكوتورب EAP تاكرح ريفشتب موقت يتلا مداخلا-ليمعلا نامأ ةينب وه EAP-FAST لوكوتورب ةيوق رارسأ ىلإ EAP-FAST قفن ءاشنإ دنتسي .(TLS) لقنلا ىوتسم نامأ قفن مادختساب يتلا ،(PACs) يمحملا لوصولا تاغوسم ةيوقلا رارسألا هذه ىمستو .نيمدختسملل ةديرف ISE. لطقف فورعم يسيئر حاتفم مادختساب ISE اودلوي

:لحارم ثالث يف EAP-FAST ثدحي

، رفص ةلحرملا EAP-FAST **(يئاقلتلا يمحملا لوصولا غوسم دادما قلحرم) رفص ةلحرملا •** مدختسملل EAP-FAST ليمع ريفوتل قفنلاب ةنمؤم ةليسو يه ةيرايتخالا ةلحرملا ريفوت نا .ةكبشلا ىلإ لوصولا بلطي يذلا مدختسملل يمحم لوصو غوسم عم يئاهنلا قلحرملا نم ديحولا ضرغلا وه يئاهنلا مدختسملا ليمعل (PAC) يمحم لوصو غوسم يف مكحتلا مئاوق ريفوت اضيا نكمي هنال ةيرايتخإ رفص ةلحرملا دعت :قظحالم.رفص عجار.رفص ةلحرملا مادختسإ نم الدب عالمعلل ايودي (PAC) ذفنملاب قصاحات ليصافت ىلع لوصحلل دنتسملا اذه يف <u>PAC ديوزت عاضوا</u> مسق.

- يئاەنلا مدختسملا ليمعلاو ISE نم لك موقي ،ىلوألا ةلحرملا يف—**ىلوألا ةلحرملا** ةصاخلا يمحملا لوصولا تاغوسم دامتعا تانايب ىلإ ادانتسا TLS قفن ءاشنإب ريفوت مت دق يئاەنلا مدختسملا ليمع نوكي نأ ةلحرملا ەذە بلطتت .مدختسملاب غوسم دنتسي نأو ،ةكبشلا ىل لوصولا لواحي يذلا مدختسملل يمحم لوصو غوسم ةكبش ةمدخ يأ نيكمت متي ال .ەتيحالص ەتنت مل يسيئر حاتفم ىلإ يمحملا لوصول ول
- نمآ لكشب مدختسملا ةقداصم تاغوسم ررمت ،ةيناثلا ةلحرملا يف -**ةيناثلا ةلحرملا** مت يذلا RADIUS ىلإ TLS قفن لخاد EAP-FAST ب ةموعدم ةيلخاد EAP ةقيرط مادختساب و RADIUS. EAP-GTC مداخو ليمعلا نيب PAC يمحملا لوصولا غوسم مادختساب هؤاشنإ EAP-FAST ل ةموعدم ىرخأ EAP عاونأ دجوت ال .ةيلخاد EAP قرطك ةموعدم PAC و TLS

.تامولعملا نم ديزم يلع لوصحلل <u>EAP-FAST لمع ةيفيك</u> عجار

يمحملا لوصولا تاغوسم

ISE نكمت ةيوق ةكرتشم ارارسأ (PAC) ذفنملاب ةصاخلا لوصولا يف مكحتلا مئاوق دعت TLS قفن ءاشنإو ضعبلا امهضعب ةقداصم نم EAP-FAST يئاهن مدختسم ليمعو يمحم لوصو تاغوسم ءاشنإب ISE موقي EAP-FAST نم ةيناثلا ةلحرملا يف مادختسالل (PAC) مردختسمل مساو طشنلا يسيئرلا حاتفملا مادختساب (PAC)

يلي ام ەطرشلا نوئش سلجم مضي:

- PAC-Key— مداخلا الاي المعالية على المعالية على المعالية المعالية المعالية المعالية المعالية المعالية المعالية .
- درتسي .مداخلا ىلإ ەريرمتو ەتانايب نيزختب ليمعلا موقي متعم لقح—**متعم PAC** ليمعلا عم ةلدابتملا ةقداصملل ليمعلا ةيوەو PAC حاتفم مداخلا.
- PAC-Info نيزخت نم ليمعلاا نيكمتل لقألا ىلع مداخلا فرعم نمضتي—PAC-Info تفريم نمضتي تاغوسم ةيحالص ءاهتنا تقو لثم ىرخأ تامولعم نمضتت ،يرايتخإ لكشبو .اتقؤم يمحملا لوصولا

يمحملا لوصولا تاغوسم ريفوت عاضوأ

ةيرايتخإ ةلحرم يه رفص ةلحرملا نإف ،اقباس ركذ امكو.

:يمحم لوصو غوسم مادختساب ام ليمع طبضل نيرايخ EAP-FAST مدقي

(قاطنلا لخاد PAC دادمإ وأ ،EAP-FAST Phase 0) ايئاقلت PAC دادمإ •

(قاطنلا جراخ) ايودي PAC دادمإ •

(PAC) يمحم لوصو غوسم **قاطنلا لخاد/يئاقلتلا (PAC) يمحملا لوصولا غوسم ريفوت** لسري لوصولا غوسم ريفوت بلطتي ال .نمآ ةكبش لاصتا ربع يئاهنلا مدختسملا ليمع ىلإ ديدج نيوكت ةطيرش ،ISE لوؤسم نم وأ ةكبشلا مدختسم نم لخدت يأ يئاقلتلا (PAC) يمحملا ISE يئاقلتلا معدل يئاهنلا مدختسمل اليمعو ISE

رادصإ ثدحأ معدي EAP-FAST يمحملا لوصولا غوسم دادمإ نيوكتل نيفلتخم نيرايخ EAP-FAST رادصإ ثدحأ معدي قاطنلا لخاد:

قاطنلا لخاد لفغملا يمحملا لوصولا غوسم دادمإ •

قاطنلا لخاد اهيلع قدصملا (PAC) يمحملا لوصولا تاغوسم دادمإ •

ةيفيكو قاطنلا لخاد يمحملا لوصولا تاغوسم دادمإ قرط دنتسملا اذه شقاني **:ةظحالم** اهنيوكت. تافلم ءاشنإل ISE لوؤسم دوجو **يوديلا/قاطنلا جراخ يمحملا لوصولا غوسم ريفوت** بلطتي ةكبشلا يمدختسم ىلع كلذ دعب اهعيزوت بجي يتلاو ،(PAC) يمحملا لوصولا تاغوسم تافلم مادختساب يئاهنلا مدختسملا ءالمع نيوكت نيمدختسملا ىلع بجي .قبطنملا مهب ةصاخلا (PAC) يمحملا لوصولا تاغوسم.

نيوكتلا

ةكبشلل يطيطختلا مسرلا



تانيوكتلا

ةيكلساللاا ةيلحملاا ةكبشلا يف مكحتلا رصنع نيوكت ققداصمل EAP-FAST

:EAP-FAST ةقداصمل WLC لا تلكش steps in order to اذه تزجنأ

- انم RADIUS ةقداصمل (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت .1 يجراخ RADIUS مداخ لالخ
- EAP-FAST ةقداصمل WLAN ةكبش نيوكت .2

يجراخ RADIUS مداخ لالخ نم RADIUS ةقداصمل (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت

تانايب هيجوت ةداعإل (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت مزلي تاغوسم نم يجراخلا RADIUS مداخ ققحتي مث .يجراخ RADIUS مداخ ىلإ مدختسملا دامتعا نييكلساللاا ءالمعلا ىلإ لوصولا رفويو EAP-FAST مادختساب مدختسملا.

:RADIUS يجراخ مداخل WLC لا تلكش steps in order to اذه تمتأ

- ل حان ةيوه ةحص RADIUS لا ضرعي نأ gui مكحت زاهجلا نم **RADIUS ةقداصم**و **نيمأت** ترتخأ .1 مداخ ديدحتل **ديدج** قوف رقنا مث .ةحفص
- 2. **قديدج** ةحفص **< RADIUS ققداصم مداوخ** ىلع RADIUS مداخ تاملعم فيرعتب مق قلاحذفنملا مقركرتشم رسRADIUS مداخل IP ناونع:يلي ام تاملعملا هذه نمضتتو IP ناونعب ISE مداخ دنتسمل اذه مدختسيمداخلا 10.48.39.128.

| cisco | MONITOR WLANS CONTROLLER | R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK |
|--|---|---|
| Security | RADIUS Authentication Serve | ers > New |
| AAA General RADIUS Authentication Accounting | Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format | 2 ¢ 10.48.39.128 (ASCII ¢) |
| Auth Cached Users Fallback | Shared Secret | |
| DNS Downloaded AVP | Confirm Shared Secret | |
| ► TACACS+ | Apply Cisco ISE Default settings | |
| Local Net Users | Apply Cisco ACA Default settings | |
| MAC Filtering Disabled Clients | Key Wrap | (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |
| User Login Policies AP Policies | Port Number | 1812 |
| Password Policies | Server Status | |
| Local EAP | Support for CoA | |
| Advanced EAP | Server Timeout | S seconds |
| Priority Order | Network User | |
| Certificate | Management | |
| Access Control Lists | Tunnel Provy | |
| Wireless Protection Policies | PAC Provisioning | |
| Web Auth | IPSec | Enable |
| TrustSec | Cisco ACA | Enable |
| Local Policies | | |
| Umbrella | | |
| Advanced | | |

.**قيٻطت** رقنا .3

ةكبش نيوكتب مق ،كلذ دعب WLAN تكبش نيوكتب مق ،كلذ دعب مت يذلا WLAN مسا .ةيكيمانيد ةهجاول اهصيصختو EAP-FAST ققداصمل ةيكلساللاا نام اذه نيعي .**عيرس EAP** وه لاثملا اذه يف هنيوكت.

ةلصلا تاذ اهتاملعمو WLAN **عيرس eap لا** تلكش steps in order to اذه تمتأ

- ەذە درست.ةحفص WLANs تضرع in order to مكحت زاەجلا نم gui لا نم WLANs تقطقط .1 مكحتلا ةدحو ىلع ةدوجوملا WLAN تاكبش ةحفصلا.
- 2. ديدج WLAN تقلخ in order to ديدج تقطقط.

| ւվովո cisco | MONITOR WLAI | Ns <u>C</u> ONTROLLER | WIRELESS | SECURITY | MANAGEMENT | C <u>O</u> MMANDS | HELP <u>F</u> | EEDBACK | | |
|----------------|-----------------|-----------------------|-----------------|----------------|------------|-------------------|---------------|------------|----------------------|--|
| WLANs | WLANs | | | | | | | | | |
| VLANs WLANs | Current Filter: | None | [Change Filter] | [Clear Filter] | | | | | Create New 🗘 Go | |
| Advanced | WLAN ID Typ | e Profile Na | ame | | WLAN SSID | | Adn | nin Status | Security Policies | |
| | 1 WL | AN test | | | test | | Enal | bled | [WPA2][Auth(802.1X)] | |
| | 2 WL | AN AndroidAP | | | AndroidAP | | Enal | bled | [WPA2][Auth(PSK)] | |

ىلع WLAN فرعمو فيرعتلا فلم مساو EAP_FAST WLAN SSID مسا نيوكتب مق .3 ق**يبطت** قوف رقنا ،كلذ دعب .ةديدج ةحفص < WLAN تاكبش.

| cisco | MONITOR WLANS | CONTROLLER WIRELESS | SECURITY MANAGEMENT | COMMANDS HELP | FEEDBACK | Save Configuration Fing Logout |
|----------------------|------------------------------------|--|---------------------|---------------|----------|------------------------------------|
| WLANs | WLANs > New | | | | | < Back |
| WLANs WLANs Advanced | Type Profile Name SSID ID | WLAN \$ eap_fast eap_fast 3 \$ | | | | |

- هذه يف .رهظي ديدج WLAN ل ةحفص **ريرحت < WLAN** لا ،ديدج WLAN تنأ قلخي نإ ام .4 كلذ نمضتيو .هذه WLAN ةكبشب ةصاخ ةفلتخم تاملعم ديدحت كنكمي ،ةحفصلا مداوخو ،ةماعلا تاسايسلا
- ةكبش نيكمتل **ةماع تاسايس** بيوبتلا ةمالع نمض **لوؤسملا ةلاح** رايتخالاا ةناخ ددح .5 ةناخ ددح ،اهب ةصاخلا ةرانملا تاراطإ يف SSID ثبت نأ لوصولا ةطقنل تدرأ اذإ WLAN. **ثب** رايتخالاا SSID.

| Security QoS Policy-Mapping Advanced Profile Name eap_fast Type WLAN SSID eap_fast Status Image: Comparison of the security of the security tab will appear after Radio Policy All Interface/Interface Group(G) vlan1477 |
|--|
| Profile Name eap_fast Type WLAN SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after Radio Policy All Interface/Interface Group(G) vlan1477 \$ |
| Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after Radio Policy All Interface/Interface Group(G) vian1477 + |
| Interface/Interface Group(G) vlan1477 + |
| |
| Multicast Vlan Feature 🔲 Enabled |
| Broadcast SSID 🗹 Enabled |
| NAS-ID none |

6. ددجو WPA/WPA2 تالماعم رتخأ **2 ةقبطلا<- نامألا -- ريرحت -- WLAN** تال AKM. ل AKM ل dot1x ددجو dot1x تالماعم رتخأ نكمي .هذه WLAN قكبشل 2 ةقبطك WPA2/AES + dot1x نيمأت لاثملا اذه مدختسي WLAN. قكبش تابلطتم ىلإ ادانتسا ىرخألاا تاملعملا ليدعت

| ANs > E | dit 'eap_fa | ast' | | | | |
|------------|-----------------------|------------|------------|-----------|---------|---------|
| eneral | Security | QoS | Policy-Map | ping Adva | nced | |
| Layer 2 | Layer 3 | AAA Ser | vers | | | |
| Layer 2 | Security ⁶ | WPA+WPA2 | \$ | | | |
| Fast Trans | ition | Dicab | | | | |
| Protected | Management | Frame | | | | |
| PMF | | Disabl | ed 🗘 | | | |
| NPA+WP4 | A2 Parameter | S | | | | |
| WPA Po | licy | | | | | |
| WPA2 P | olicy | | - | | | |
| WPA2 E | ncryption | AES | 🗆 ТКІР | CCMP256 | GCMP128 | GCMP256 |
| OSEN P | olicy | | | | | |
| Authentica | ation Key Man | agement 19 | 1 | | | |
| 802.1X | | Enable | | | | |
| ССКМ | | Enable | | | | |
| PSK | | Enable | | | | |
| ET 000 | 1V 🗆 E | nabla | | | | |

تحت . تم بسانملا RADIUS مداخ رتخأ "AAA مداوخ <**- (نامأ) Security - (ريرحت) WLAN -> Edit** مداوخ تحت . مداوخ تحت ةلدسنملا ةمئاقلا

| eneral | Security | QoS | Policy- | Mapping | Advanced | | |
|---|--|--|---------|--|----------|--|--------------|
| ayer 2 | Layer 3 | | Servers | | | | |
| ADIUS Serv RADIUS Se | vers erver Overwi | rite interfa | ce Enal | bled | | LAN | |
| Apply Cisco | o ISE Defaul | t Settings | Enal | Accounting | Servers | | ΓΔΡ Ρ |
| Apply Cisco | Authentica | t Settings Ition Serv | Enal | Accounting | Servers | | EAP P |
| Apply Cisco Server 1 | Authentica | t Settings Ition Serv 39.128, Po | ers | Accounting Contemporation Contempora | Servers | \$ | EAP P Ena |
| Apply Cisco Server 1 Server 2 | Authentica Contempt for the second se | t Settings Ition Serv 39.128, Po | Enal | Accounting Contemporation Contempora | Servers | ¢ | EAP P Ena |
| Apply Cisco Server 1 Server 2 Server 3 | Authentica Contempt for the second se | t Settings Ition Serv 39.128, Po | Enat | Accounting Contact Enabled None None None | Servers | < | EAP P Ena |
| Apply Cisco Server 1 Server 2 Server 3 Server 4 | Authentica Contraction Authentica Contraction Authentica Contraction Authentica Contraction None None None | t Settings ntion Serv 39.128, Po | Enal | Accounting Contempose | Servers | < | EAP P Ena |
| Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 | Authentica Contraction Authentica Contraction Authentica Contraction Authentica Contraction None None None None | t Settings ntion Serv 39.128, Po | Enal | Accounting Carbon Enabled None None None None None None None | Servers | | EAP P Ena |
| Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6 | Authentica Contraction Authentica Contraction Authentica Contraction None None None None None None | t Settings ntion Serv 39.128, Po | Enal | Accounting Contemporation Accounting Contemporation Accounting Contemporation None None None None None None None No | Servers | | EAP P Ena |

مكحتلا ةدحو ىلع ەنيوكت مزلي يذلا ديحولا EAP دادعإ وه اذه **:ةظحالم.قبطي** ةقطقط .8 مداخ ىلع متت نأ جاتحت EAP-FAST ب ةصاخلا ىرخألاا تانيوكتلا لك .EAP ةقداصمل RADIUS .ةقداصملا ىلإ نوجاتحي نيذلا ءالمعلاو

EAP-FAST ةقداصمل RADIUS مداخ نيوكت

:EAP-FAST ةقداصمل لدان RADIUS لا تلكش steps in order to اذه تزجنأ

- EAP-FAST ءالمع ةقداصمل مدختسم تانايب ةدعاق ءاشنإ .1
- مداخ ىلِ AAA ليمعك (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع ةفاضاٍ .2 RADIUS
- قاطنلا لخاد لوهجم PAC دادمإ مادختساب RADIUS مداخ ىلع EAP-FAST ةقداصم نيوكت .3
- هيلع قدصملا قاطنلا لخاد PAC دادمإ عم RADIUS مداخ يلع EAP-FAST ةقداصم نيوكت .4

EAP-FAST ءالمع ةقداصمل مدختسم تانايب ةدعاق ءاشنإ

eap_fast> ك EAP-FAST ليمعل رورملا ةملكو مدختسملا مسا نيوكتب لاثملا اذه موقي يلاوتلا ىلع <*EAP-FAST*

1. يف ISE Web Admin، <mark>تومدختس</mark>ملا المجاو لقنت "iSE Web Admin يف التو**مدختسملا -- قيوهلا قرادإ -- قرادإ** تحت مدختسمل . **"ةفاضإ" زمر** طغضاو

| dentity Services | s Engine | Home Conte | ext Visibility | Operations | Policy | Administration | + Work Cer | iters | | | |
|---------------------------|-----------------|--------------------------------------|-------------------|---------------|---------------|----------------|---------------|-----------------|---------------|----------------------|-------|
| ► System - Identity N | lanagement | Network Resource | s + Device Porta | al Management | pxGrid Servio | es 🕨 Feed | Service + Thr | eat Centric NAC | | | |
| ▼Identities Groups | External Identi | ty Sources Identity | y Source Sequence | s FSettings | | | | | | | |
| | 0 | | | | | | | | | | |
| Users | | Network Acce | ss Users | | | | | | | | |
| Latest Manual Network Sca | an Results | / Edit 🕂 Add | 🔀 Change Statu | is 🕞 Import | Export 👻 | XDelete | Duplicate | | | | |
| | | Status | Name | - | Description | | First Name | Last Name | Email Address | User Identity Groups | Admin |
| | | | | | | | | | No c | data available | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

ليجست رورم ةملك"و "مسالا - ەۋاشنإ متيل مدختسملل ةبولطملا جذامنلا ةئبعتب مق .2 كنكمي ،ىرخأ ةيحان نم]؛ةلدسنملا ةمئاقلا نم **"نيمدختسملا قعومجم"** ددحو "**لوخدلا** [مدختسملا باسحل ىرخأ تامولعم ةئبعت ىلع طغضا

| diala Iden | tity Services | s Engine | Home ► Co | ontext Visibility | ▸ Operations | ▶ Policy | - Administra | ation 🔹 🕨 | Work Center | 8 | | | |
|----------------------------|-----------------------------------|--------------------|-----------------------------|---------------------|-------------------|------------|---------------|-------------|----------------------------|-------------------|---|----|--|
| System | - Identity N | lanagement | Network Resource | rces + Device | Portal Management | pxGrid S | Services + F | eed Service | Threat | Centric NAC | | | |
| ▼ Identities | Groups | External Ident | ity Sources Ider | ntity Source Sequ | ences + Settings | | | | | | | | |
| | | G | Network Acces | es lleare list > No | ew Network Access | liser | | | | | | | |
| Users | | | Network | Access User | | | | | | | | | |
| Latest Manua | Network Sc | an Results | * Name | eap_fast | | | | | | | | | |
| | | | Status | Enabled • | | | | | | | | | |
| | | | Email | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | ▼ Passwo | ords | | | | | | | | | |
| | | | Password | Type: Intern | al Users | * | | | | | | | |
| | | | | Passwo | brd | | Re-Enter Pass | word | | | _ | | |
| | | | * Login Pa | assword ••••• | ••• | | ••••• | | | Generate Password | ١ | | |
| | | | Enable Pa | assword | | | | | | Generate Password | | | |
| | | | ▼ User In | nformation | | | | | | | | | |
| | | | First Nam | e Test user | | | | | | | | | |
| | | | Last Nam | e Test user | | 7 | | | | | | | |
| | | | | | | | | | | | | | |
| | | | Accourt | nt Options | | | | | | | | | |
| | | | | Descri | iption | | | | | | | // | |
| | | | Change p | assword on next | login 🗆 | | | | | | | | |
| | | | ▼ Accourt | nt Disable Polic | cy. | | | | | | | | |
| | | | Disa | ible account if dat | te exceeds 2019-0 | 04-23 | | (yyyy-mr | m-dd) | | | | |
| | | | - | | | | | | | | | | |
| | | | ▼ User G | roups | | | | | | | | | |
| | | | Employe | e | ○ | | | | | | | | |
| | | | Submit | Cancel | | | | | | | | | |
| | | | | | | | | | | | | | |
| تہ اِن | ا ءاش | تسمر | مدخ. | | | | | | | | | | |
| System | Identity Mana | agement I Ne | twork Resources | Device Portal Ma | anagement pxGrid | Services + | Feed Service | Threat Ce | entric NAC | | | | |
| Identities | Groups Ex | ternal Identity So | urces Identity So | urce Sequences | Settings | | | | | | | | |

| • Gyatem • Identity Management | Network Resources | · Device Fortal Ma | hagement pxond dervice | | Bat Contric 14AC | | | |
|---|-------------------|--------------------|---------------------------------|------------------------|------------------|---------------|----------------------|-------|
| Identities Groups External Identity | Sources Identity | Source Sequences | Settings | | | | | |
| Q | | | | | | | | |
| Users | Network Acces | s Users | | | | | | |
| Latest Manual Network Scan Results | 🕖 Edit 🛛 🕂 Add | 🔀 Change Status 👻 | 🕞 Import 🛛 🚯 Export 👻 | 🗙 Delete 👻 🕒 Duplicate | | | | |
| | Status | Name | Description | First Name | Last Name | Email Address | User Identity Groups | Admin |
| | 🗌 🛛 Enabled | 🧕 eap_fast | \oplus | Test user | Test user | | Employee | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

اليمعك (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع ةفاضا AAA ليمعك (WLC) ميكلساللا علي AAA ليمعك إل

ACS: مداخ ىلع AAA ليمعك مكحتلا ةدجو فيرعتل ةيلاتلا تاوطخلا لمكأ

ا بيولاا ةرادا مدختسم ةهجاو يف .1 ISE، **قزمجأ <- ةكبشلا دراوم <- ةراداٍ**" نمض لقتنا . **ةفاضاٍ" زمر** طغضاو **"ةكبشلا**".

| diale Identity Services Engine | Home Contex | t Visibility | -Administration + Work Centers | | |
|------------------------------------|---------------------|---|--------------------------------------|-----------------------------|-------------------|
| System Identity Management | - Network Resources | Device Portal Management pxGrid | Services + Feed Service + Threat Cer | ntric NAC | |
| Network Devices Network Device | Groups Network Dev | ice Profiles External RADIUS Servers | RADIUS Server Sequences NAC Manag | ers External MDM + Location | n Services |
| G | | | | | |
| Network Devices | Network Devic | ces | | | |
| Default Device | | | | | |
| Device Security Settings | / Edi 🕂 Add | Duplicate 💽 Import 💽 Export | Generate PAC X Delete | | |
| | Name | IP/Mask Profile Name | Location | Туре | Description |
| | | | | | No data available |
| | | | | | |

رورملا ةملك نيوكتو "**IP**"و ،"**مسالا** - زاهجلا ةفاضإل ةبولطملا جذامنلا ةئبعتب مق .2 يف ،قباسلا مسقلا يف WLC ىلع اهنيوكتب انمق امك ،اهسفن ةكرتشملا ةيرسلا ،عقوملا لثم زاهجلل ىرخأ تامولعم ةئبعت كنكمي هنأ رايخ] "**كرتشم رس** جذومن .[كلذ ىلإ امو ،ةعومجملاو ىلع طغضا

| dentity Services Engine | Home Context Visibility Operations Policy Administration Work Centers |
|--------------------------------|--|
| System Identity Management | Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC |
| Network Devices Network Device | Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services |
| 0 | |
| Network Devices | Network Devices List > New Network Device |
| Default Device | * Name WILCES20 |
| Device Security Settings | Description |
| | |
| | IP Address + IP: 10.48.71.20 / 32 |
| | |
| | IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected |
| | |
| | * Device Profile 🔐 Cisco 💌 🕀 |
| | Model Name 🔍 👻 |
| | Software Version |
| | 1 Nakurdi Davlas Caura |
| | - Metwork Pealoe Group |
| | Location LAB Set To Default |
| | IPSEC Is IPSEC Device O Set To Default |
| | Device Type WLC-lab 🛇 Set To Default |
| | |
| | ✓ RADIUS Authentication Settings |
| | |
| | RADIUS UDP Settings |
| | Protocol RADIUS |
| | Shared Secret Show |
| | CoA Port 1700 Set To Default |
| | RADIUS DTLS Settings () |
| | DTLS Required |
| | Shared Secret radius/dtls (7) |
| | CoA Port 2083 Set To Default |
| | Issuer CA of ISE Certificates for CoA Select if required (optional) * |
| | DNS Name |

ا الما المات المات المات المات المات المات المات المات المات 3. (ISE. (NAD) المات المات 3. المات المات المات ال



لخاد لوهجم PAC دادمإ مادختساب RADIUS مداخ ىلع EAP-FAST ةقداصم نيوكت قاطنلا

اPKI ةينب رفوت مدع ةلاح يف قرطلا نم عونلا اذه مادختسإ يف ءرملا بغري ،ماع لكشبو هب ةصاخلا رشنلا ةيلمع يف ةيساسألاا.

تمت يذلا (Diffie-HellmanKey (ADHP ةيقافتإ لوكوتورب قفن لخاد ةقيرطلا هذه لمعت مداخ ةقداصمب ريظنلا موقي نأ لبق هتقداصم

لخاد فورعم ريغ يمحم لوصو تاغوسم ريفوتب حامسلا" نيكمت ىلإ جاتحن ،ةقيرطلا هذه معدل امب حومسملا ةقداصملا تالوكوتورب نمض ISE ىلع "قاطنلاا

| cisco Identity Services Engine | Home Context Visibility Operations Policy Administration Work Centers |
|--------------------------------------|---|
| Policy Sets Profiling Posture C | lient Provisioning - Policy Elements |
| Dictionaries → Conditions → Result | ts |
| 0 | ✓ Allow EAP-FAST |
| ▼ Authentication | |
| Allowed Protocols | - EAP-FAST Inner Methods |
| Authorization | |
| ▶ Profiling | |
| | |
| ▶ Posture | Allow Password Change Retries 3 (Valid Range 0 to 3) |
| Client Provisioning | |
| | Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy |
| | Use PACs O Don't Use PACs |
| | Tunnel PAC Time To Live 90 Days * |
| | Proactive PAC update will occur after 90 % of PAC Time To Live has expired |
| | Allow Anonymous In-Band PAC Provisioning |
| | Allow Authenticated In-Band PAC Provisioning |
| | Server Returns Access Accept After Authenticated Provisioning |
| | Accept Client Certificate For Provisioning |
| | Allow Machine Authentication |
| | Machine PAC Time To Live 1 Weeks * |
| | Enable Stateless Session Resume |
| | Authorization PAC Time To Live 1 (1) |
| | Enable EAP Chaining |

لثم ،رورملا ةملك عون ىلع ةقداصم ءارجاب تحمس دق كنأ نم دكأت **:ةظحالم** EAP-MS-CHAPv2 لثم ،رورملا ةملك عون ىلع ققداصم ءارجاب تحمس دق كنأ نم دكأت الل لل

قاطنلا لخاد لفغملا ريفوتلا.

قاطنلا لخاد PAC دادمإ عم RADIUS مداخ ىلع EAP-FAST ةقداصم نيوكت ميلع قدصملا

مت يتلا مداخلا ةداهش ىلإ ادانتسا TLS قفن ءاشنإ مت .ةيصوتلاو انامأ رثكألا رايخلا وه اذه .(يضارتفالا) ISE لبق نم Clean ةداهش ةحص نم ققحتلا متو بلاطلا لبق نم اهنم ققحتلا

اددحم نوكي دق ەنأ نم مغرلا ىلع ،مداخلاو ليمعلل ةيساسأ PKI ةينب دوجو رايخلا اذه بلطتي نيبناجلا الك ىلع ەيطخت مت وأ طقف مداخلا بناج ىلع.

:قاطنلا لخاد ەتقداصم متت يذلا دادمإلل نايفاضإ نارايخ كانە ،ISE يف

- ريفوت دعب ،ةداع "ةقداصملاب **ديوزتلا دعب "لوصولا لوبق" عاجراب مداخلا موقي"** 1. ةداعإب لسرملا ىلع امغرم لوصولا ضفر لاسرا بجي ،(PAC) يمحملا لوصولا تاغوسم ريفوت نأل ارظنف ،كلذ عمو .(PAC) يمحملا لوصولا تاغوسم مادختساب ةقداصملا قباجتسالا اننكميف ،هتقداصم تمت يذلا TLS قفن يف متي يمحملا لوصولا تاغوسم يف) .ىندألا دحلا ىلإ ةقداصملا تقو ليلقتل Access-Accept مادختساب يروف لكشب .(مداخلا بناج ىلعو Itas ىلع اهب قوثوم تاداهش كيدل نأ نم دكأت قلاحل اهذه لثم
- 2. قيساسألاا PKI ةينب ريفوت يف عرملا بغري مل اذا "دادمإلل ليمعلاا ةداهش لوبق" امم ،رايخلا اذه نيكمتب مقف ،SE ىلع طقف اهب قوثوم ةداهش هيدل ناكو ليمعلاا ةزهجأل مداخلا بناج يلع ليمعلا ةداهش ةحص نم ققحتلا يطختب حمسي.

| cisco Identity Services Engine | Home Context Visibility Operations Policy Administration Work Centers |
|------------------------------------|--|
| Policy Sets Profiling Posture C | ient Provisioning - Policy Elements |
| Dictionaries + Conditions - Result | S |
| 0 | ✓ Allow EAP-FAST |
| ▼Authentication | |
| Allowed Protocols | EAP-FAST Inner Methods |
| Authorization | |
| ▶ Profiling | |
| | |
| ▶ Posture | |
| Client Provisioning | Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Use PACs O Don't Use PACs Tunnel PAC Time To Live 90 Days * Proactive PAC update will occur after 90 % of PAC Time To Live has expired Allow Anonymous In-Band PAC Provisioning |
| | Allow Authenticated In-Band PAC Provisioning Server Returns Access Accept After Authenticated Provisioning Accept Client Certificate For Provisioning Allow Machine Authentication Machine PAC Time To Live <u>1</u> Weeks * Enable Stateless Session Resume Authorization PAC Time To Live <u>1</u> Hours * (I) |

لاثملا ،نييكلساللا نيمدختسملل ةطيسب ةقداصم تاسايس ةعومجم ISE يف ددحن امك ةقداصملا قفدت ةقباطمو ،ةقداصملا عونو عقوملاو ظفح ةملعم زامج عون مادختسا وه يلاتلا ةيلخادلا مدختسملا تانايب ةدعاق لباقم امتحص نم ققحتلا متيس يتلا.

|--|

ةحصلا نم ققحتلا

تاغوسم دادعا قفدتو (NAM) ةكبشلا ىل لوصولا ةرادا نيوكت تادادعا لاثملا اذه رهظيس قلباقملا WLC ءاطخاً حيحصت عم قاطنلا لخاد اهيلع قدصملا (PAC) يمحملا لوصولا.

NAM فيرعت فلم نيوكت

ةسلج ةقداصمل AnyConnect NAM فيرعت فلم نيوكتل ةيلااتلا تاوطخلاب مايقلا مزلي مادختساب ISE لباقم مدختسملا لمع BAP-FAST:

| Authentication Policy Profile: Untitled | |
|--|------------------------------|
| Allow Association Modes | Allowed Authentication Modes |
| Select All (Personal) | Select All Outer |
| Open (no encryption) | EAP-FAST |
| Open (Static WEP) | EAP-GTC |
| Shared (WEP) | EAP-TLS |
| WPA Personal TKIP | EAP-TLS |
| WPA Personal AES | EAP-TTLS |
| WPA2 Personal TKIP | EAP-MD5 EAP-MSCHAPV |
| WPA2 Personal AES | MSCHAP (legacy) |
| Select All (Enterprise) | LEAP |
| Open (Dynamic (802.1X) WEP) | |
| WPA Enterprise TKIP | EAP-MSCHAPv2 |
| WPA Enterprise AES | EAP-TLS |
| WPA2 Enterprise TKIP | Allowed Wired Security |
| WPA2 Enterprise AES | Select All |
| | Open (no encryption) |
| | 2 802. 1x only |
| CCKM Enterprise AES | ☑ 802. 1x with MacSec |

:ديدج ةكبش فيرعت فلم **"ةفاضإ**" .3

| | | lager | | | |
|--|-----------------------------|---|--------|--------|---|
| Help | | | | | |
| Network Access Manager | Networks Profile: Untitl | ed | | | |
| Networks | Network | | | | ŕ |
| and the second s | Name | Media Type | Group* | | |
| | wired | Wired | Global | Add | |
| | | | | Edit | |
| | | | | Cultin | |
| | | | | Delete | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | * A network in gro | up 'Global' is a member of <i>all</i> gro | oups. | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

ةكبش عونك يكلساللا "**مسا** فيصوتلا نيوكتلا مسق ددحي "**طئاسولا عون** تحت .4 مسا ددحيو كب صاخلا طئاسولا

| Networks Name: eap_fast Group Membership In group: Local networks In all groups (Global) In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): eap_fast Hidden Network Corporate Network | Med Securi | ia Typ ^ ity Lev |
|---|---------------|---------------------|
| Association Timeout 5 seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds Next Cancel < | | × |

نارتقالا عضو ددحو "ةكبشلا ةقداصم" ددح "**نامألا ىوتسم** نيوكت بيوبتلا ةمالع تحت . هنأ ىلع WPA2 Enterprise (AES)

| vork Access Manager Client Policy Authentication Policy | Networks Profile:ility Client | Network Access Manager\system\cont | figuration.xml | |
|---|---|--|----------------|---------------|
| Networks | Security Level | | | Media Type |
| Network Groups | Open Network | | | Security Leve |
| | Open networks hav | e no security, and are open to anybody within range. T | 'his is | Connection Ty |
| | the least secure typ | e of network. | | |
| | O Shared Key Networ | k | | |
| | Shared Key Networ | ks use a shared key to encrypt data between end statio | ins and | |
| | network access poir | nts. This medium security level is suitable for | | |
| | small/home offices. | | | |
| | Authenticating Network | vork | | |
| | Authenticating netv | orks provide the highest level of security and are perfec | ct for | |
| | enterprise level pet | and a state ware and a state of a second state of the second state | | |
| | enterprise iever net | works. Authentication networks require radius servers, | and | |
| | other network infra | works. Authentication networks require radius servers, structure. | and | |
| | other network infra | works. Authentication networks require radius servers, structure. | and | |
| | other network infra - 802. 1X Settings - authPeriod (sec.) | structure. | and | |
| | 802. 1X Settings authPeriod (sec.) | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) -Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) MPA2 Enterprise (AES) | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) -Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 3 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 | |
| | 802. 1X Settings authPeriod (sec.) heldPeriod (sec.) Association Mode | 30 startPeriod (sec.) 60 maxStart | and 30 | |

ةيلاتلا بيوبتلا ةمالع تحت كلذل ،مدختسملا عون ةقداصم مدختسن ،لاثملا اذه يف .6 **مدختسملا لاصتا** ددح "**لاصتالا عون**

| AnyConnect Profile Editor | - Network Access Manager — | C | | × |
|---------------------------|--|---------------------------|--|------------------------------|
| File Help | | | | |
| Network Access Manager | Networks Profile:ility Client\Network Access Manager\system\configuration.xml | | | |
| Network Groups | Network Connection Type Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. Image: Section Should be used when a machine connection is not needed. A user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in. Next Cancel | M See Con U C | ledia T curity i nectio Jser Ai ireden | ype A .eve ith ials |
| | Help | | | |

اهب حومسم ةقداصم ةقيرطك EAP-FAST ددح "**مدختسملا ةقداصم** بيوبتلا ةمالع تحت .7 يف اهب قوثوم تاداهش مدختسن ال اننأل ارظن ،مداخلا ةداهش نم ققحتلا ليطعتب مقو لاثملا اذه.

| letwork Access Manager Client Policy Authentication Policy | Networks Profile:ility Client\Netw | vork Access Manager\system\configuration | on.xml |
|--|--|--|--------------------------|
| Networks | EAP Methods | | Media Type |
| | ◯ EAP-TLS | ○ PEAP | Security Leve |
| | O FAR-TTI S | ■ EARLEAST | Connection Ty |
| | CLAPPITES | CAPT AST | Oser Auto Credentials |
| | ◯ LEAP | | Credendus |
| | Extend user connection I | beyond log off | |
| | EAP-FAST Settings | | |
| | Validate Server Identity | | |
| | Enable Fast Reconnect | | |
| | Disable when using a | a Smart Card | |
| | <u> </u> | | |
| | Inner Methods based on Credent | tials Source | |
| | Authenticate using a Pas | ssword | |
| | EAP-MSCHAPv2 | EAP-GTC | |
| | If using PACs, allow | unauthenticated PAC provisioning | |
| | O Authenticate using a Cer | rtificate | |
| | When requested ser | nd the client certificate in the clear | |
| | Only send client cert | tificates inside the tunnel | |
| | Send client certificat | te using EAP-TLS in the tunnel | |
| | Authenticate using a Tok | ken and EAP-GTC | |
| | | | |
| | V OSCIACS | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Ne | Cancel | |

ىلع ةتبثم اهب قوثوم ةداهش كيدل نأ نم دكأت ،يقيقحلا جاتنإلا ةئيب يف **:ةظحالم** ISE تادادعإ يف انكمم مداخلا ةداهش ةحص نم ققحتلا رايخ قبأو حامسلا ،(PAC) يمحملا لوصولا تاغوسم مادختسا ةلاح يف" رايخلا ديدحت بجي :ةظحالم لوصو غوسم ديوزت ةلاح يف طقف "هيلع قدصملا ريغ يمحملا لوصولا تاغوسم دادمإب محم

سفن مادختسإ يف كتبغر ةلاح يف SSO ك امإ مدختسملا دامتعا تانايب فيرعتب مق .8 يف "دامتعالا تانايبب ةبلاطم" ددح وأ ،لوخدلا ليجستل ةمدختسملا دامتعالا تانايب مق وأ ،ةكبشلاب لاصتالا ءانثأ مدختسملا نم دامتعا تانايب بلط ديرت تنك اذإ ام ةلاح ةبلاطمب موقن ،لاثملا اذه يف .اذه لوصولا عونل ةتباثلا دامتعالا تانايب مدختسملا .

| ÷. | AnyConnect Profile Editor - Network Access | Manager |
|----|--|---------|

| User Identity | | Media Type |
|--------------------------------|----------------|---------------|
| Unprotected Identity Pattern: | anonymous | Security Leve |
| | | Connection Ty |
| Protected Identity Pattern: | [username] | User Auth |
| | | Credentials |
| User Credentials | | |
| 🔾 Use Single Sign On Credentia | ls | |
| Prompt for Credentials | | |
| O Remember Forever | | |
| Remember while Use | r is Logged On | |
| O Never Remember | | |
| O Use Static Credentials | | |
| Password | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Dana | Canaal | |
| Done | Cancel | |

.ةلصلا يذ NAM دلجم نمض نوكملا فيرعتلا فلم ظفح .9

EAP-FAST ةقداصم مادختساب SSID ب لاصتالا ربتخا

AnyConnect ةكبش ةمئاق نم صاخلا فيرعتلا فلم ددح .1

| S Cisco AnyCo | onnect Secure Mobility Client | | _ | | × | |
|---------------|---|---|---|---------|----|--|
| | VPN: Verify your network connection. | ~ | | Connect | | |
| No Network Co | onnectivity | | | | | |
| | Network: Authenticating | | | | | |
| _ | eap_fast | | 8 | atl 🗸 | := | |
| | eap_fast | | | illin 🖰 | | |
| | | | | الله 🖻 | _ | |
| | (Shanna) | | | att | | |
| | | | | a 🛛 | | |
| | | | | ≜II | | |
| | | | _ | llır. 🖰 | | |

- ةقداصملل نيبولطملا رورملا ةملكو مدختسملا مسا لاخدإ .2
- (يتاذ عيقوت) مداخلاً قداهش لوبق .3





| 🕙 Cisco AnyC | onnect Secure Mobility Client | _ | | × |
|---------------|---|-------|---------------|---|
| | VPN: Network error. Unable to lookup host | names | s. Connect | |
| Limited Acces | s - DNS Failure | | | |
| | Network: Connected (192.168.77.34) eap_fast | A | all 🗸 : | = |
| | | | | |

ISE ةقداصم تالجس

تحت PAC و EAP-FAST دادمإ قفدت رەظت يتلاا ISE ةقداصم تالجس ىلع عالطالا نكمي ليصافتلا نم ديزمب اەيف ثحبلا نكميو ،"**(ةيح تالجس) RADIUS -> Live Log <- تايلمع** زمرلا مادختساب

ضفر نكلو ،ةقداصم ةقيرطك EAP-TLS حرتقي ISE ناكو ةقداصملا ةيلمع ليمعلا أدب .1 لك اهيلع قفتا يتلا ةقيرطلا يه هذه تناكو ،كلذ نم الدب EAP-FAST حرتقاو ليمعلا و ليمعلا نم

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 11507 Extracted EAP-Response/Identity

12500 Prepared EAP-Request proposing EAP-TLS with challenge

- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session

12101 Extracted EAP-Response/NAK requesting to use EAP-FAST instead

- 12100 Prepared EAP-Request proposing EAP-FAST with challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

متو PAC لدابتل ةيمحم ةئيب ريفوتل مداخلاو ليمعلا نيب TLS ةحفاصم عدب مت .2 حاجنب اهل|مك|.

| 12800 | Extracted first TLS record; TLS handshake started |
|-------|---|
| 12805 | Extracted TLS ClientHello message |
| 12806 | Prepared TLS ServerHello message |
| 12807 | Prepared TLS Certificate message |
| 12808 | Prepared TLS ServerKeyExchange message |
| 12810 | Prepared TLS ServerDone message |
| 12811 | Extracted TLS Certificate message containing client certificate |
| 12105 | Prepared EAP-Request with another EAP-FAST challenge |
| 11006 | Returned RADIUS Access-Challenge |
| 11001 | Received RADIUS Access-Request |
| 11018 | RADIUS is re-using an existing session |
| 12104 | Extracted EAP-Response containing EAP-FAST challenge-response |
| 12105 | Prepared EAP-Request with another EAP-FAST challenge |
| 11006 | Returned RADIUS Access-Challenge |
| 11001 | Received RADIUS Access-Request (112) Step latency=13317 ms) |
| 11018 | RADIUS is re-using an existing session |
| 12104 | Extracted EAP-Response containing EAP-FAST challenge-response |
| 12812 | Extracted TLS ClientKeyExchange message |
| 12813 | Extracted TLS CertificateVerify message |
| 12804 | Extracted TLS Finished message |
| 12801 | Prepared TLS ChangeCipherSpec message |
| 12002 | Propered TLO Finished message |
| 12816 | TLS handshake succeeded |

3. ةطساوب حاجنب مدختسملا دامتعا تانايب نم ققحتلاو ةيلخادلا ةقداصملا عدب مت (رورملا ةملك / مدختسملا مسا ىلإ ةدنتسملا ةقداصملا) MS-CHAPv2 مادختساب

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