ةيجراخ ةەج نم CA نم ةعقوم ةداەش تيبثت ISE يف

تايوتحملا

ەمدقملا

كرحم يف (CA) يجراخ قدصم عجرم لـبـق نـم ةعقوم ةداهش تـيبـثت ةيفـيك دنتسملا اذه حضوي فيرعت تـامدخ Cisco (ISE).

ةيساسألا تابلطتملا

تابلطتملا

.يساسألاا ماعلا حاتفملل ةيساسألاا ةينبلاب ةفرعم كيدل نوكت نأب Cisco يصوت

ةمدختسملا تانوكملا

نم 3.0 رادصإلاا ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست Cisco Identity Services Engine (ISE). تارادصإلاا ىلع هسفن نيوكتلا قبطني

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

،Admin و ،لخدمو ،EAP ةقداصم) يئاهنلا ةداهشلا رود نع رظنلا ضغب اهسفن يه ةيلمعلا هذه

و pxGrid).

نيوكتلا

.(CSR) ةداەشلا عيقوت بلط ءاشنإ .1 ةوطخلا

ءاشنإ قوف رقناو تاداەشلا عيقوت تابلط < تاداەش < ةرادإلا ىلإ لقتنا ،CSR ءاشنإل تاداەشلا عيقوت تابلط (CSR).

Certificate Management \checkmark System Certificates	Certificate Signing Requests	
Trusted Certificates	Generate Certificate Signing Requests (CSR)	
OCSP Client Profile	A Certificate Signing Requests (CSRs) must be sent to and signed by an external autho	rity. Click '
Certificate Signing Requests	request has been signed, click "bind" to bind the request to the signed certificate issued	by that au
Certificate Periodic Check Se	Q View ሰ Export 💼 Delete Bind Certificate	
Certificate Authority >	Friendly Name Certificate S	ubject

- مت اذإ .ةلدسنملا ةمئاقلا نم همادختسإ متيس يذلا رودلا ددح ،"مادختسالا" مسق نمض .1 ءاشنإ درجمب .مادختسالا ددعتم ديدحت كنكمي ،ةددعتملا راودألل ةداهشلا مادختسإ رمألا مزل اذإ راودألا رييغت نكمي ،ةداهشلا
- الهل ةداهشلا ءاشنإ نكمي يتلا ةدقعلا ددح .2
- . (دلبلاو ةيالولا، ،ةنيدملا، ،ةمظنملا، ،ةيميظنتلا، قدحولا) ةجاحلا بسح تامولعملا ألما. 3

مساب ايئاقلت ةدقعلا ميمعتب (CN) عئاشلا مسالا لقحب صاخلا ISE موقي :ةظحالم 🔍 لماكلاب لەؤملا لاجملا (FQDN).

لدبلا فرحا:

- لدبلا فرح تاداهشب حامسلا عبرم نم ققحتف ،لدب فرح ةداهش ءاشنإ وه فدهلا ناك اذا.
- عوضوملل CN لقح يف * زمرلا نوكي الأ بجي EAP ةقداصمل مدختست ةداهشلا تناك اذإ يلومم نإ ثيح Mindows يافري يافرم ن
- ة تحفاصم لشفت نأ نكمي ،بلاطملا ىلع مداخلا ةيوه ةحص نم ققحتلا ليطعت دنع ىتح• SSL لقح يف * نوكي امدنع SSL
- مادختسإ نكمي مث نمو ،CN لقح يف ماع FQDN مادختسإ نكمي ،كلذ نم الدبو «domain.com مسا لقح يف (SAN) عوضوملل ليدبلا مسالا DNS.

ةداەشلل CN يف (*) لدبلا فرح ةفاضإ (CA) تاداەشلا عجارم ضعبل نكمي :ةظحالم 🛇 صاخ بلط ميدقت مزلي ،ويرانيسلا اذه يفو .CSR يف ادوجوم نكي مل اذا يتح أيئاقلت .ءارجإلا اذه عنمل

:يدرفلا مداخلا ةداەشل CSR لاثم

Usage

Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for
			example, one certificate each for Guest Portals,
Allow Wildcard Certificates	i		LAF, and picind).
Node(s)			
Generate CSR's for these Nodes:			
Node	CSR Friendly Name		
Jabtomar30	abtomar30#Multi-Use		
Subject			
Common Name (CN) \$FQDN\$		<u>(</u>)	
Organizational Unit (OU) Cisco TAC		<u>(</u>)	
Organization (O) Cisco		<u>(</u>)	
City (L) Bangalore			
State (ST) Karnataka			
Country (C)			
Subject Alternative Name (SAN)			
IP Address	~ 10.106.120.87		- + 0
* Key type			
RSA	~ (i)		

:Wildcard CSR لاثم

sage			~
Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended
			practice. Rather, you should obtain individual certificates specifically for each service (for
Allow Wildcard Cartificates			example, one certificate each for Guest Portals, EAP, and pxGrid).
ubiect			
Common Name (CN)			
Mycluster.mydomain,com		(i)	
Organizational Unit (OU)			
Cisco TAC		<u>(</u>)	
Organization (O)		~	
Cisco		(i) 	
City (L)			
Bangalore			
State (ST)			
Karnataka			
Country (C)			
IN			
Subject Alternative Name (SAN)			
IP Address	✓ 10.106.120.87		- +
DNS Name	*.mydomain.com		- + 0
* Key type			
RSA	~ (i)		

نيزختلا ةقطنم ةكبش لقح ىلإ رشن (دقع) ةدقعل IP ناونع لك ةفاضإ نكمي :ةظحالم IP نيزختلا ةقطنم تكبش لقح الم IP.

لا صرعي ،هريدصت درجمب .اهريدصت رايخ عم ةقثبنم ةذفان ISE ضرعي ،CSR ءاشنإ درجمب عيقوتلل قدصملا عجرملا يلإ فلملا اذه.

~



Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen



ةديدج تاداەش ةلسلس داريتسإ .2 ةوطخلا.

ام .(طيسولا/رذجلا) ةلماكلا تاداەشلا ةلسلس عم عقوملا مداخلا ةداەش صيخرتلا ةئيە عجرت الامداخ يلا تاداەشلا دروتست نأ انە تاوطخلاب مق ،تملتسا نا ISE:

- ىلإ لقتنا ،قدصملا عجرملا نم ةمدقم ةطيسو تاداەش (وأ) و رذج تاداەش يأ داريتسال .1 اەب قوثوم تاداەش < تاداەش < قرادإ.
- رايتخالاا تاناخ راتخيو ةطيسولا ةداهشلا وأ/و رذجلا راتخي كلذ دعبو داريتسإ ةقطقط .2 لسري نأ تقبط امك ةلصلا تاذ.
- .ةداەشلا عيقوت تابلط < تاداەش < ةرادإ ىلإ لقتنا ،مداخلا ةداەش داريتسال .3
- . طبرلا ةداەش ىلع رقناو اقبسم ەؤاشنإ مت يذلI CSR ددح
- ەۋاشنإ مت يذلا صاخلا حاتڧملاب ةداەشلا طبرب ISE ماقو ديدجلا ةداەشلا عقوم ددح .5 تانايبلا ةدعاق يڧ ەنيزختو.
- 💊 امداخ تامدخ ليغشت ةداعإ متت ،ةداهشلا هذهل "لوؤسملا رود" ديدحت مت اذإ :ةظحالم. ةددحملا.
- اذإو رشنلل ةيساسألا ةرادإلا ةدقع صخت اهداريتسإ مت يتلا ةداهشلا تناك اذإ :ريذحت دقعلا ةفاك ىلع ةدوجوملا تامدخلا ليغشت ةداعإ متي ذئدنعف ،اددحم "لوؤسملا" رود ناك لمعلا نع فقوت تقو ثودح نسحتسملا نمو كلذ ثودح عقوتملا نم .ىرخألا ولت ةدحاو .طاشنلاا اذه ذيفنتل

ةحصلا نم ققحتلا

ةديدجلا ةداەشلا نأ نم ققحتلا كنكمي ،ةداەشلا داريتسإ ءانثأ لوؤسملا رود ديدحت مت اذإ ضرعتسملا قثي نأ بجي .ضرعتسملا يف ةرادإلا ةحفص ليمحت قيرط نع اەناكم يف ضرعتسملا ناك اذاو حيحص لكشب ةلسلسلا ءاشنإ مت املاط ةديدجلا لوؤسملا ةداەشب .تاداەشلا ةلسلس يف قثي

eral Details Certification Path	
Certification path abtomar-WIN-231PNBS4IPH-CA abtomar30.abtomar.local	cisco
	Identity Services Engine
	Intuitive network security
	Username
View Certificate	
rtificate status: nis certificate is OK.	Password
	Login
ОК	
	 English 日本語

© 2020 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE of View third-party licenses and notices

دوجو نم ققحت صيخرتلا راسم تحتو ضرعتسملا يف نيمأتلا زمر ددح ،ققحتلا نم ديزمل ةلسلسلا ريرمت ىلع ارشابم ارشؤم سيل اذه .زاهجلاب اهتقث نمو ةلماكلا ةلسلسلا ةداهشب ةقثلا هنكمي ضرعتسملل رشؤم هنكلو مداخلا لبق نم حيحص لكشب ةلماكلا ماخلا يلحملا ةقثلاا نزخم ىلإ ادانتسا مداخلا

اهحالصإو ءاطخألا فاشكتسا

dot1x ةقداصم ءانثأ ISE Local Server ةداهشب بلاطلا قثي ال

.SSL ةحفاصم ةيلمع ءانثأ ةلماكلا تاداهشلا ةلسلسب رمي ISE نأ نم ققحت

متي مداخلا ةيوه نم ققحتلاو (PEAP يأ) مداخ ةداهش بلطتت يتلا EAP بيلاسأ مادختسإ دنع ةدوجوملا تاداهشلا مادختساب تاداهشلا ةلسلس ةحص نم بلطلا مدقم ققحتي ،اهديدحت ، SSL ةحفاصم ةيلمع نم عزجك .ةقداصملا ةيلمع نم عزجك يلحملا ةقثلا نزخم يف هيدل نكمتي نل .هتلسلس يف ةدوجوم ةطسوتم (وأ)و رذج تاداهش يأ كلذكو هتداهش ISE مدقي ريرمت نم ققحتلل .ةلماك ريغ ةلسلسلا تناك اذإ مداخلا ةيوه نم ققحتلا نم بلاطملا :ةيلاتلا تاوطخلا ذيفنت كنكمي ،ليمعلا ىلإ ىرخأ ةرم تاداهشلا ةلسلس

- ا ح تايلمعلا ىلإ لقتنا ،ةقداصملا ءانثأ (ISE (TCPDump نم طاقتلا طاقتلا لجأ نم 1. غيرفت < ةماع تاودأ < صيخشتلا تاودأ
- 2. يف ssl.handshake.certificates حشرم قيبطتب مقو طاقتلالا حتف/ليزنتب مق لوصول ايدحت يلع روثعل و Wireshark
- 3. -EAP < ةميقلاا جاوزأ صئاصخ < RADIUS لوكوتورب ديدمت ىلإ لقتنا ،ەديدحت درجمب ةنمآلا ليصوتلا ذخآم ةقبط < عسوتملا ةقداصملا لوكوتورب < ريخألاا عطقملا ةلاسر تاداەش < ةداەش <.

طاقتلالا يف تاداەشلا ةلسلس.

Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
0 0 🛋	■ 点 目 日 第 部 久 キ キ @ 茶	🛓 🗐 🕞 🔍 Q Q Q 🖻	👪 🗹 🥵 🐝 😫 -		
Filter:	ssLhandshake.certificates	Expression	Clear Apply	Save	
No.	Time	Source	Destination	Protocol Length Info	
334	13:59:41.137274	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done	
857	13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS 1178 Access-Challenge(11) (id=198, 1=1136)	
860	13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=199, l=1132)	
862	13:59:53.213715	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=200, 1=1132)	
864	13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS 301 Access-Challenge(11) (id=201, 1=259)	
1265	14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done	
+				TI	
20 AV5 8 AV7 8 E	<pre>:: 1=235 t=EAP-Message(79) Segm :: 1=255 t=EAP-Message(79) Last AP fragment xtensible Authentication Protoc Code: Request (1) Id: 41 Length: 1012 Type: Protected EAP (EAP-PEAP) EAP-TLS Flags: 0xc0 EAP-TLS Flags: 0xc0 EAP-TLS Fragments (3141 byt Secure Sockets Layer w TLSv1 Record Layer: Handshakk Content Type: Handshake (22 Version: TLS 1.0 (0x0301) Length: 3048</pre>	ent[3] Segment[4] (25) es): #857(1002), #860 e Protocol: Server He e Protocol: Certificat)	(1002), #862(1002 17¤ te), #864(135)]	
	 Handshake Protocol: Certifi Handshake Type: Certifical Length: 3044 Certificates Length: 3041 Certificates (3041 bytes) Certificate Length: 1656 Certificate (id-at-comme Certificate Length: 1379 Certificate (id-at-comme Certificate (id-at-comme Certificate (id-at-comme Certificate (id-at-comme TLSv1 Record Layer: Handshake 	cate te (11) Name-TORISE20A.rtpa: Name-rtpaaa-ca,dc=rt e Protocol: Server He	<mark>ta.net,id-at-</mark> orga paaa,dc=net) 10 Done	rizationalUnitName=RTPAAA,id-at-organizationName=CISCO,id-at-localityName	-R1

نم ققحتو اەب قوثوم تاداەش < تاداەش < ISE ةرادإ ىلإ لقتنا ،ةلماك ريغ ةلسلسلا تناك اذإ ققحتلا بجيف ،حاجنب تاداەشلا ةلسلس ريرمت مت اذإ .رذجلا (وأ)و ةطيسولا تاداەشلا دوجو انە ةحضوملا ةقيرطلا مادختساب اەسفن ةلسلسلسل ايمحالص نم.

فرعم ةقباطم ل|لخ نم ةقثل| ةلسلس نم ققحتو (يرذجو طسوتم ،مداخ) ةداهش لك حتفا يف ةيلاتلا ةداهشلل (AKI) ةطلسلا حاتفم فرعم عم ةداهش لكل (SKI) عوضوملا حاتفم ةلسلسلا.

تاداەش ةلسلس ىلع لاثم.

Certificate 26	Certificate 25	Certificate 26
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show All>	Show <ai></ai>	Show <al></al>
Field Value *	Field Value ^	Field Value ^
Public key RSA (2048 8its)	CA Version V0.0	Public key RSA (4096 Bits)
ESubject Key Identifier da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6	Subject Key Identifier fe 34 ca 8d 22 9b 6e d7 a6 86 11 cl 18 1.	Key Usage Digital Signature, Certificate Signing, Off-I
Enhanced Key Usage Server Authentication (1.3.6.1.5.5.7.3.1)	Certificate Templat SubCA	Subject Key Ident 52 2e e5 2c 38 29 d6 da 81 19 11 70 74 00
Subject Alternative IP Address=14.36.157.21	Authority Key Identif KeyID=52 2e e5 2c 38 29 d6 da 81 19 11	CA Version V0.0
a Authority Key Identi KeyID=fe 34 ca 8d 22 9b 6e d7 a6 86 11	CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Basic Constraints Subject Type=CA, Path Length Constraint= :::
CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Authority Informatio [1] Authority Info Access: Access Method	Thumbprint algori sha1
Authority Informati [1] Authority Info Access: Access Method +	Key Usage Digital Signature, Certificate Signing, Off-L +	Thumbprint cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6 👻
₹F	₹	< III >
V3	Y3	A3
Edit Properties Copy to File Learn more about <u>certificate details</u>	Edit Properties Copy to File	Edit Properties Copy to File
OK	οκ	ок

ءانثأ ISE مداخ ةداەش ضڧرت ةياەنلا ةطقن نكلو ةحيحص ISE ةداەش ةلسلس ةقداصملا

ال بولطملا ناكو SSL ةحفاصم ءانثأ هب ةصاخلا ةلماكلا تاداهشلا ةلسلس مدقي ISE ناك اذا (وأ)و رذجلا تاداهشلا نأ نم ققحتلا يه ةيلاتلا ةوطخلا نإف ،تاداهشلا قلسلس ضفري لازي ليمعلاب صاخلا يلحملا ةقثلا نزخم يف ةدوجوم ةطيسولا تاداهشلا.

نامج نم كلذ نم ققحتلل Windows، قيان القتنا Mindows، قيان الالعام قاد الم المال المال المال المال المال المال ال مدختسمل الباسح امإ ددح .ةفاضإ ىلع رقناو تاداهشلا ددح ،رفوتمل الميفاضإل التاودأل ادومع نم مث (زامجلا وأ مدختسملا) مدختسمل المقداصمل عون للسح ىلع رتويلمكل للالباسح وأ يل صاخل قفاوم ىل عرقنا

تاداەشلا عجارمو اەب قوثوملا رذجلا ةقداصم عجارم ددح ،مكحتلا ةدحو ضرع ةقيرط تحت يلحملا قوثوملا نزخملا يف طسوتملاو رذجلا ةداەشلا دوجو نم ققحتلل ةطيسولا.

ile Action View Favorites Window Help → 2 □ □ 0 → 2 □					
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name
Gertificates - Current User Personal Trusted Root Certification Authorities Certificates	AddTrust External CA Root Baltimore CyberTrust Root Ccrtum CA Ccisco Root CA 2048	AddTrust External CA Root Baltimore CyberTrust Root Certum CA Cisco Root CA 2048	5/30/2020 5/12/2025 6/11/2027 5/14/2029	Server Authenti Server Authenti Server Authenti <all></all>	USERTrust Baltimore Cybe Certum <none></none>
Enterprise Trust Intermediate Certification Authorities Certificate Revocation List Certificates	Cisco Root CA M1 Class 2 Primary CA Class 3 Public Primary Ce	Cisco Root CA M1 Class 2 Primary CA Class 3 Public Primary Certi	11/18/2033 7/6/2019 8/1/2028	<all> Secure Email, S Secure Email, C</all>	<none> CertPlus Class 2 VeriSign Class 3</none>
Active Directory User Object Directory User Object Trusted Publishers Other States Third-Party Root Certification Authorities	COMODO RSA Certificati Copyright (c) 1997 Micro DigiCert Assured ID Root	COMODO RSA Certificatio Copyright (c) 1997 Microso DigiCert Assured ID Root C DigiCert Global Root CA	1/18/2038 12/30/1999 11/9/2031 11/9/2031	Server Authenti Time Stamping Server Authenti Server Authenti	COMODO Microsoft Time DigiCert DigiCert
Trusted People Other People Gertificate Enrollment Requests Smart Card Trusted Roots	DigiCert High Assurance DST Root CA X3 DST Root CA X3 DST Root CA X3 DST Root Certification	DigiCert High Assurance E DST Root CA X3 DST Root CA X3 Entrust Root Certification	11/9/2031 9/30/2021 9/30/2021 11/27/2026	Server Authenti Secure Email, S <all> Server Authenti</all>	DigiCert DST Root CA X3 <none> Fotost</none>

ديدحت ءاغلإب مق ،مداخلا ةيوه نم ققحتلا يف ةلكشم هذه نأ نم ققحتلل ةلەس ةقيرط .ىرخأ ةرم ەرابتخاو بولطملا فيرعتلا فلم نيوكت نمض مداخلا ةداەش ةحص نم ققحتلا

Connection Security	When connecting:
Security type: WPA2-Enterprise	Connect to these servers:
Encryption type: AES -	Trusted Root Certification Authorities:
	AddTrust External CA Root
	Baltimore CyberTrust Root
Choose a network authentication method:	Certum CA
Microsoft: Protected EAP (PEAP)	Cisco Root CA 2048
- Jourga	Cisco Root CA M1
Remember my credentials for this connection each	Class 2 Primary CA
time I'm logged on	Class 3 Public Primary Certification Authority
	COMODO DOL CUMPLICA Automatic

ةلص تاذ تامولعم

- <u>كالاراد المارية المارية المارية المراجع المراجع المارية ا</u>
- <u>العَزْنِتِلَاؤِ عِنْفَلاً مِعْدَل</u>ا

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