BYOD ل ISE SCEP معد نيوكت

تايوتحملا

<u>ةمدق مل ا</u> <u>ةيساسألا تابلطتملا</u> تا<u>بلطتملا</u> ةمدختسملا تانوكملا <u>ةيساساً تامولعم</u> <u>ةربتخملا CA/NDES رشن تاەوىرانىس</u> <u>ةلقتسملا رشنا تايلمع</u> <u>ةعزوماا رشناا تايامع</u> <u>Microsoft ل ةماه تاحالصا</u> <u>ةماەلا BYOD تالوكوتوربو ذفانم</u> نىوكترا <u>SCEP ليجست يدحت رورم ةملك تابلطتم ليطعت</u> <u>ةفورعملا ISE دقع ىل SCEP لىجست دىيقت</u> <u>IIS يف URL ناونع لوط ديدمت</u> <u>ةداەش لا بلاق ىلع قماع قرظن</u> <u>ةداەشلا بلاق نىوكت</u> <u>ةداەشلا بلاق لجس نيوكت</u> <u>SCEP لىكوك ISE نىوكت</u> <u>ةحصلا نم ققحتلا</u> <u>اهحالصاو ءاطخاُلا فاشكتسا</u> <u>ةماعلا اهحالصاو ءاطخألا فاشكتساً تاظحالم</u> <u>لىمعلا بناج نم لىجستلا</u> <u>ISE لىجست</u> <u>اهحالصاو ءاطخالا فاشكټساو NDES لوخد ليجست</u> <u>ةلص تاذ تامول عم</u>

ەمدقملا

ةكبش ةزهجأ ليجست ةمدخ نيوكتل اهمادختسإ متي يتلا تاوطخلا دنتسملا اذه فصي Microsoft (NDES) طيسبلا ةداهشلا ليجست لوكوتوربو (SCEP) طيسبلا تامدخ يلع فرعتلا كرم يلع (BYOD) كب

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ثدحأ رادصإ وأ 1.1.1 رادصإلI SE •
- ليغشتال Microsoft Windows Server 2008 R2 ليغ

- ليغشتا Microsoft Windows Server 2012 Standard
- تاداەشلاو (PKI) ماعلا حاتڧملل ةيساسُألا ةينُبلا •

ةمدختسملا تانوكملا

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

- ثدحأ رادصإ وأ 1.1.1 رادصإلI SE •
- Windows Server 2008 R2 SP1 و KB2483564 ةلجاعلا تاحالصإلا تيبثت عم KB2483564 و
- ليغشتلا ماظن Windows Server 2012 Standard

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

عجرا .Cisco BYOD ب صاخ ليلدك Microsoft تاداەش تامدخب ةقلعتملا تامولعملا ريفوت متي قمدخو Microsoft TechNet قداەش ةئيەل ةبسنلاب ةقيقحلل يئاەن ردصمك Microsoft TechNet ىلإ SCEP. ب قطبترملا مداخلا تانيوكتو (NDES) قكبشلا قزەجأ ليجست

ةيساسأ تامولعم

نيمدختسملاا ةردق يف Cisco نم هب ISE نيكمت مت يذلاا BYOD ذيفنت ايازم ىدحإ لثمتت ةينقت ىلع يرادإلاا ءبعلاا ليزي اذهو .ةيتاذلاا ةمدخلاا زامج ليجست ءارجإ ىلع نييئاهنلاا رهوج نمكي .ةكبشلا ىلع ةزهجألاا نيكمتو ةقداصملا دامتعا تانايب عيزوت لجأ نم تامولعملا قبولطملا تاداهشلا عيزوتل ىعست يتلاو ،ةكبشلا يقلتم ديوزت ةيلمع يف BYOD لح تاداهش عجرم نيوكت نكمي ،بلطتملا اذه ةيبلت لجأ نم .فظوملا اهكلمي يتلا ةزهجألاا ىلع Microsoft (CA ماد جيل مي قاد الالالي عن الالالي قال مي الالي المات المالي ال

ليهست لجأ نم (VPN) ةيرهاظلا ةصاخلا ةكبشلا تائيب يف تاونسل SCEP مادختسإ مت فئاظو نيكمت بلطتي .دعب نع لوصولا تاهجومو ءالمعلا ىلع اهعيزوتو قداهشلا ليجست اضيأ متي ،NDES رود تيبثت ءانثأ .NDES تيبثت Windows 2008 R2 مداخ ىلع SCEP تابلط ءاهنإل IIS مادختسإ متي .ISE جهن قدقعو CA نيب HTTPS SCEP وأطلال ليجست تاباجتساو

ةيلمع يف .وضع مداخ ىلع ەتيبثت نكمي وأ ،يلاح قدصم عجرم ىلع NDES رود تيبثت نكمي ،قدصم عجرم ةمدخ نمضتي يلاح قدصم عجرم ىلع NDES ةمدخ تيبثت متي ،ةلقتسم رشن قمدخ تيبثت متي ،ةعزوم رشن ةيلمع يف .تاداەشلا ةطلسل بيولا ليجست قمدخ ،ايرايتخاو وأ رذج CA ب لاصتالا لجأ نم عزوملا NDES مداخ نيوكت متي ،كلذ دعبو .وضع مداخ ىلع NDES اذه يف ةحضوملا لجسلا تاليدعت ءارجا متي ،ويرانيسلا اذه يف .قفدتل يعرف رذج عجرملا ىلع تاداەشلا دجوت ثيح ،صصخملا بلاقل مادختساب ميولا ليعمس قرم مداخ على عرف رزج

ةربتخملا CA/NDES رشن تاەويرانيس

يف اهرابتخإ مت يتلا CA/NDES رشن تاهويرانيس ىلع ةرصتخم ةماع ةرظن مسقلا اذه مدقي مداوخلا تانيوكتب ةصاخلا ةقيقحلل يئاهن ردصمك Microsoft TechNet ىلإ عجرا Cisco. ربتخم و SCEP ب ةطبترملا

ةلقتسملا رشنلا تايلمع

لقتسم زاهج رشن عئاشلا نم ،(PoC) ميهافملا ةحص تابثإ ويرانيس يف ISE مادختسإ دنع

ل كراب ماظنب لمعي Windows 2008 وأ Windows 2008 ل لاجملاب ماظنب لمعي Active Directory ليغشتلا ماظنب لمعي Active Directory (AD) مداخو رذجلا قدصملا عجرمل ل



- Domain Controller
- AD
- Root CA
- NDES

ةعزوملا رشنلا تايلمع

تامدخلاا ةيؤر رثكأ عئاشلا نمف ،ةيلاحل Microsoft AD/PKI جاتنا ةئيب يف ISE جمد متي امدنع تايلمعل نيەويرانيس Cisco تربتخا .ةفلتخملا 2012 وأ Windows 2008 مداوخ ربع ةعزوملا .ةعزوملا رشنلا

ةعزوملا رشنلا تايلمعل هرابتخإ مت يذلا لوألا ويرانيسلا ةروصلا هذه حضوت



ةعزوملا رشنلا تايلمعل ربتخملا يناثلا ويرانيسلا ةروصلا هذه حضوت



- NOULCH

Microsoft ل ةماه تاحالصإ

هذه ىلع يوتحي Windows 2008 R2 NDES مداخ نأ نم دكأت ،BYOD ل BYOD معد نيوكت لبق نم قلجاعلا تاحالصإلا Microsoft نم قلجاعلا تاحالصإلا

- م<u>ت ةداەشلا تناك اذا Windows Server 2008 R2 يف SCEP ةداەشل ديدجتلا بلط لشفي</u> قولمع معدي ال NDES نأل ةلكشملا هذه ثدحت - <u>NDES مادختساب اهترادا</u> SCEP م
- فسسؤملل قدصملا عجرملا ليغشت قداعا دعب تاداهشلا تابلط لاسراب NDES موقت ال قمدخ ىلع رذعتي :**ثادحألا ضراع** يف قلاسرلا هذه رهظت - Windows Server 2008 R2 يف رفوتم ريغ RPC مداخ .(0x800706ba) قداهشلا بلط لاسرا قكبشلا قزهجأ ليجست.

نيوكت دنع :**ريذحت** Microsoft CA، عيقوت ةيمزراوخ معدي ال ISE نأ مەف مەملا نم Microsoft CA، عيقوت تيوكت دنع PSS. مدختست ىتح Cisco قسايس نيوكتب Cisco كيصوت sha1WithRSAEncryption كيلذ نم الدب sha256WithRSAEncryption

ةماەلا BYOD تالوكوتوربو ذفانم

:ةماەلا اەتالوكوتوربو BYOD ذفانمب ةمئاق يلي اميف

- و Windows ليغشتلا ةمظنأ) Cisco ISE نم تيبثتلا جلاعم :8909 دادعإ Windows دادمإ Macintosh (OS))
- TCP: نم جلاعملا تيبثت Google Play (Android) نم جل
- ليمعلا ديوزت ةيلمع :8905 لوكوتورب دادعإ :(TCP) لاسرإلا يف مكحتالا لوكوتورب •
- A ىلإ 443 زارط SCEP لوكوتورب ليكو :TCP لوكوتورب وأ 80 رايعم :TCP لوكوتورب SCEP RA) لوكوتوربب صاخلا URL ناونع نيوكت ىلإ ادانتسا)

ليوليد علام عجرا ،ةبولطملا تالوكوتوربلاو ذفانملاب ةمئاق ثدحاً علع لوصحلل :**ةظحالم** <u>قزمجالا تيبثت</u> ISE 1.2.

نيوكتلا

.ISE ىلع BYOD ل SCEP و NDES معد نيوكتل مسقلاا اذه مدختسأ

SCEP ليجست يدحت رورم ةملك تابلطتم ليطعت

ةيكيمانيد يدحت رورم ةملك (Microsoft SCEP (MSCEP ذيفنت مدختسي ،يضارتفا لكشب نيوكتلا تابلطتم دوجو عم .ةداهشلا ليجست ةيلمع لللخ ةياهنلا طاقنو ءالمعلا ةقداصمل لوؤسمل بيوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو ىلإ ضارعتسالا كيلع بجي ،هذه عزجك هذه رورملا ةملك نيمضت بجي .بلطلا دنع رورم ةملك ءاشنإل NDES مداخ ىلع MSCEP ليجستلا بلط نم

ةيتاذلا ةمدخلا لح نم ضرغلا فلاخت يدحتلا رورم ةملك تابلطتم نإف ،BYOD رشن يف مداخ ىلع اذه ليجستلا حاتفم ليدعت بجي ،بلطتملا اذه ةلازإل .مدختسملل

- . ثحبلا طيرش يف **regedit** لخدأو **ءدب** ىلع رقنا.
- 2. دريفشتلا < Microsoft < جماربلا < HKEY_LOCAL_MACHINE < رتويبمكلا ىل كا ك. مرورملا ةملكضرف < MSCEP.
- .(1 يه ةيضارتفالاا ةميقلاا) 0 ىلع EnforcementPassword ةميق نييعت نم دكأت .3

🔐 Registry Editor					
File Edit View Favorites Help					
CatDBTempFiles		Name	Туре	Data	
😟 - 🄑 CertificateTemplateCache		ab (Default)	REG_SZ	(value not set)	
😟 🍌 Defaults		20 EnforcePassword	REG_DWORD	0x00000000 (0)	
B- MSCEP					
CAType					
CertsInMYStore					
EnforcePassword					
PasswordVDir					
🕀 🕌 OID					
😟 🔐 Protect		1			

ةفورعملا ISE دقع ىلإ SCEP ليجست دييقت

ةمئاق ىلع SCEP تالاصتإ ديءقت لضفملا نم نوكي دق ،رشنلا تاهويرانيس ضعب يف لاجملا دويقو IPv4 ناونع ةزيم مادختساب كلذ قيقحت نكميو .ةفورعملا ISE دقع نم ةددحم يف IIS:

1. بيو عقوم ىلإ لقتناو IIS بيو عقوم ىل



حامسلا ةفاضا تاءارجا مدختساً **.لاجملا دويقو IPv4 ناونع < نامألا** قوف اجودزم ارقن رقنا .2 ادانتسا هدييقت وأ بيولا ىوتحم ىلإ لوصولاب حامسلل **لاخدالا ضفر ةفاضاو لاخدالاب ةزيملا تادادعا ريرحت** ءارجالا مدختساً .تالاجملا ءامساً وأ ISE ةدقعل IPv4 نيوانع ىلإ نيددحم ريغ ءالمعل ةيضارتفا لوصو ةدعاق ديدحتل.

IPv4 Address and Domain Restrictions		Actions		
		Add Allow Entry		
se this feature	e to restrict or grant ac	cess to Web content bas	sed on IPv4 addresses or domain names. Set the	Add Deny Entry
strictions in o	rder of priority.			× Remove
Group by: No	Grouping 🔹			Edit Feature Settings.
4ode ≜	Requestor	Entry Type		Revent To Johanited
low	10.1.2.3	Local		View Ordered List
				Help
				Online Help
	Edit IP and	Domain Restrictions	s Settings 🔗 🗙	
	Access fo	r unspecified clients:		
	Deny			
	Enabi	e domain name restriction	ns	
		ОК	Cancel	

IIS يف URL ناونع لوط ديدمت

هذه بنجتل .IIS بيو مداخل ةبسنلاب ادج ةليوط URL نيوانع ءاشنإب ISE موقي نأ نكمملا نم نم رمأ اذه تلخد .لوطأ URL نيوانعب حامسلل يضارتفالIIS نيوكت ليدعت نكمي ،ةلكشملا لدان NDES ل %systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/ security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost

تلخد .ةياەنلا ةطقنو ISE نيوكتل اقفو مالعتسالا ةلسلس مجح فلتخي دق :**قظحالم** يراداٍ زايتما عم CLI لدان NDES لا نم رمأ اذه.

Administrator: Command Prompt Microsoft Windows [Version 6.0.6001] Copyright (c) 2006 Microsoft Corporation. All rights reserved. C:\Users\Administrator>%systemroot%\system32\inetsrv\appcmd.exe set config /sect ion:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"81 92" /commit:apphost Applied configuration changes to section "system.webServer/security/requestFiltering" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT T/APPHOST" C:\Users\Administrator>_

ةداەشلا بلاق ىلع ةماع ةرظن

قيبطتل ةمدختسملا بلاوقلا نم رثكأ وأ دحاو نيوكت Microsoft CA يلوؤسمل نكمي ديدحت يف جهنلا هذه دعاست .تاداهشلا نم ةكرتشم ةعومجم ىلع قيبطتلا تاسايس يف قيبطتلا جهن ميق دجوت .ةنرتقملا حيتافملاو ةداهشلا اهل مدختست يتلا ةفيظولا لقح يف ميقلا ليلحتب قدصملا موقي .ةداهشلل (EKU) عسوملا حاتفملا مادختسإ لقح نمضتتو .ةدوصقملا ةفيظولل ليمعلا نم ةمدقملا قداهشلا مادختسا قيناكما نامضل UNI IPSec قلي المادختسال في المعرب قراصم امادختسا رثكألا تامادختسالا ضعب قراصم امادختس ميان تامين القريف المادختسا في المعرب وما الحيا تعاملا مادختسا وما المعرب

يذلا بيو مداخ نيوكت متي ،نمآ يكنب بيو عقوم ىلإ ضارعتسالا دنع ،لاثملا ليبس ىلع بلط مداخلا ىقلتي امدنع .مداخلا ةقداصمل قيبطت جەن ىلع يوتحت ةداەشب بلطلا جلاعي المقونلا .ةقداصملل لصتملا بيو ضرعتسم ىلإ مداخلا ةقداصم ةداەش لسري ەنإف ،HTTPS نإف ،ISE ب قلعتي اميف .ليمعلا ىل مداخلا نم ەاجتالا يداخا لدابت وە اذە نأ يە انە ةمەملا (GUI) قيموسرلا مدختسملا قەجاو ىلإ لوصولا وە مداخلا ةقداصم ةداەشل عئاشلا مادختسالا عقوتي الو لصتمل صرعتسمل ىل اەنيوكت مت يتلا قداصم قداەش لسري . عقوتي الو لصتمل مداخا مادختس الىل اەنيوكت مت يتلا مادختسال

ةقدام مل الضفيف ، EAP-TLS مدختست يتلا BYOD لثم تامدخب رمألا قلعتي امدنع مدختسملا بلاق ايوتحي نأ بجي ،اذه ماجتإلا يئانث تاداهشلا لدابت نيكمتل .ةلدابتملا مداخ ةداهش بلاق يفوتسي .مداخلا ةقدام مل ىندأ قيبطت جهن ىلع ISE ةيوه ةداهش ءاشنإل قياهنلا ةطقن تاداهش ءاشنإب موقي يذلا ةداهشلا بلاق يوتحي نأ بجي .بلطتملا اذه بيولا اذإ .بلطتملا اذه مدختسمل قداهش بلاق يفوتسي .ليمعلا ةقداممل ىندأ قيبطت جهن ىلع الإ .بلطتمل اذه مدختسمل الماه موقي يذل المال يفوت يليم على المال من الجي .بلطتمل الذه بيولا بلاقل يوتحي نأ بجي في القلي يوكت من المال المال المال المام الما مال المات مال المال من المال الذه مدختسمل المالية موقي يذل المال المالي المال المالي المال المالي المال المالي المال المال المال المال المالي المالي المالي المال المال المال المال المال المالي ا

كنكمي وأ ،نيييضارتفالاا مدختسملاا بلاوقو Microsoft CA Web Server مادختسإ ةداعإ كنكمي ىلإ ادانتسا .دنتسملا اذه يف ةددحملا قيلمعلا مادختساب هؤاشنإو ديدج بلاق خسن ةجتانلا ةيفرطلا ةطقنلاو ISE تاداهشو CA نيوكت طيطخت بجي ،هذه ةداهشلا تابلطتم جاتنا قئيب يف اهتيبثت دنع اهيف بوغرم ريغ نيوكت تارييغت يأ ليلقتل قيانعب.

User Properties	? ×	Web Server Properties	? ×
General Request Handing Subject Name Extensions Security To view an extension description, select an extension. Extensions included in this template: Certificate Template Name Enhanced Kay Usage & Key Usage		General Request Handing Subject Name Extensions Security To view an extension description, select an extension. Extensions included in this template: Certificate Template Name Enhanced Key Usage Key Usage	
Description of Enhanced Key Usage: Encrypting File System Secure Email Client Authentication	×	Description of Enhanced Key Usage: Server Authentication	4
OK Cancel Apply Help	,	OK Cancel Apply He	dp

ةداەشلا بلاق نيوكت

يف عساو قاطن ىلع SCEP لوكوتورب مدختسي ،ةمدقملا يف كلذ ىلإ ةراشإلاا تمت امكو نيوكتب NDES رود تيبثت موقي ،كلذل ةجيتنو .IPSec لوكوتورب ربع VPN تاكبش تائيب ىدحإ نإف ،ببسلا اذهلو .SCEP ل **(لاصتا نود بلطلا) IPSec** بلاق مادختسال ايئاقلت مداخلا قيبطتلا جهنب ديدج بلاق ءاشنإ يه BYOD ل BYOD تانايب عجرم دادعإ يف ىلوألا تاوطخلا سفن ىلع Certified Authority و NDES تامدخ عيمجت متي ،ةلقتسم رشن ةيلمع يف .حيصلا قيلمع يف .مداخلا سفن علي قبولطملا لي ال يسل اتالي دعتو بلاوقلان ي مادخ ديدجت متي ،كلذ عمو ،NDES مداخلا وي ال يولي اليون ال اليون ديدجت متي ،كلذ عمو ،NDES مداخ على لي الي اليون الي اليول الي اليون ديدم القل اليون اليون اليون اليون اليون اليون ديدم اليون ديدم اليون اليون

ةداەشلا بلاق نيوكتل ةيلاتلا تاوطخلا لمكأ

- ا. **لوؤسمك** CA مداخ ىلإ لوخدلا ليجستب مق.
- . **قدصم عجرم < ةيرادإ تاودأ < ءدب** ىلع رقنا.
- اذه يوتحي .**تاداهشلا بلاوق** دلجم ددحو قدصملا عجرملا مداخ ليصافت عيسوتب مق .3 ايلاح اهنيكمت مت يتلا بلاوقلاب ةمئاق ىلع دلجملا.
- . **ةرادا** رتخاو **تاداەشلا بلاوق** دلجملا ىلع نميألا سواملا رزب رقنا ،تاداەشلا بلاوق ةرادال .4
- .ةطشنلا ريغ بلاوقلا نم ددع ضرع متي ،**تاداهشلا بلاوق مكحت ةدحو** يف .5
- دوجوم بلاق قوف نميألا سواملا رزب رقنا ،SCEP عم مادختسالل ديدج بلاق نيوكتل .6 **بلاقل راركت** رتخاو ،**مدختسملا** لثم ،لعفلاب.
- يف CA ليغشت ماظنل ىندألاا دحلا ىلع ءانب ،Windows 2008 وأ Windows 2003 رتخأ .7

.ةئيبلا

- 8. نةيحالصلا ةرتفو ،ISE-BYOD لثم ،ضرع مسا ةفاضإب مق ،**ماع** بيوبتلا ةمالع يف قيقدت نودب ىرخألا تارايخلا لك كرتأ. تاداهشلا ةيحالص ةرتف يواست وأ نم لقأ بلاقلا ةيحالص ةرتف نوكت نأ بجي :**قظحالم** ةطيسولا تاداهشلاو قدصملا رذجلا.
- . **بلطلا يف ديروتلا** ديدحت نم دكأتو ،**عوضوملا مسا** بيوبتلا ةمالع ىلع رقنا. 9
- رادصإلا تاسايس كرتب Cisco يصوت .**رادصإلا تابلطتم** بيوبتلا ةمالع قوف رقنا .10 ةي جذومن ةيمره CA ةئيب يف ةغراف.
- . **ريرحت** مث ،**قيبطتاا جەن**و **تاقحلماا** بيوبتالا ةمالع قوف رقنا.
- .OK قوف رقناو .قيبطت جەنك **ليمعلا ةقداصم** ةفاضإ نم دكأتو ،**ةفاضإ** قوف رقنا .12
- يف ددحملا SCEP ةمدخ باسح نأ نم دكأت .**...فضأ** مث ،**نامألا** بيوبتلا ةمالع قوف رقنا .13 قمدخ تيبثت . .**قفاوم** قوف رقنا مث ،بلاقلاب لماك مكحت هل NDES ةمدخ تيبثت
- .ق**يدصتلاا عجرمب** ةصاخلاا **GUI** ةەجاو ىلا عجرا.
- <mark>ةداەشلا بلاق < ديدج</mark> ىلإ لقتنا .**تاداەشلا بلاوق** ليلد ىلع نميألا سواملا رزب رقنا .15 .**ەرادص|** دارملا.
- .ق**فاوم** قوف رقنا مث ،اقبسم ەنيوكت مت يذلا **ISE-BYOD** بلاق ددح .16

رمألا مادختساب رماوألاا رطس ةهجاو ربع بلاقلا نيكمت كنكمي ،كلذ نم الدب :**ةظحالم** certutil -SetCAtemplates+ISE-BYOD. قنكمملا تاداهشلا بلاوق ةمئاق يف نآلاا ISE-BYOD بلاق جاردإ بجي.

ةداەشلا بلاق لجس نيوكت

ةداەشلا بلاق لجس حيتافم نيوكتل ةيلاتلا تاوطخلا لمكأ

- .NDES مداخب لاصتالا .1
- . ثحبالا طيرش يف **regedit** لخدأو **ءدب** ىلع رقنا.
- 3. <mark>(ج م اربل ح Microsoft > KEY_LOCAL_MACHINE > (د يوف ش ت ل ا ح Microsoft > (د يوف ش ت ل ا ح ا ح م اربل ا ح Microsoft > MSCEP.</mark>
- 4. و SignatureTemplate و GeneralPurposeTemplate حيتافم رييغتب مق اقبسم مؤاشنإ مت يذلا ISE-BYOD بلاق ىلإ **(لاصتا نود بلط) IPSec ن**م.
- .لجسلا دادعإ قيبطتل NDES مداخ ليغشت دعأ .5

💣 Registry Editor					
File Edit View Favorites Help					
		Name	Туре	Data	
		ab (Default)	REG_SZ	(value not set)	
САТуре		ab EncryptionTemplate	REG_SZ	ISE-BYOD	
CertsInMYStore		ab GeneralPurposeT	REG_SZ	ISE-BYOD	
EnforcePassword		ab SignatureTemplate	REG_SZ	ISE-BYOD	
PasswordVDir					
🖽 🛄 OID					
Dratact		1			

SCEP ليكوك ISE نيوكت

متي ،كلذ نم الدبو .يفلخلا NDES مداخب ةرشابم ةياهنلا ةطقن لصتت ال ،BYOD رشن يف .ةياهنلا طاقن نع ةباينلاب NDES مداخب لصتتو SCEP ليكوك ISE ةسايس ةدقع نيوكت طباور معدل NDES مداخ ىلع IIS ليثم نيوكت نكمي .ISE عم ةرشابم ةياهنلا طاقن لصتت HTTP وأ/و HTTPS ل قيرهاظلا ةلدألل HTTPS وأ/و

:SCEP ليكوك ISE نيوكتل ةيلااتلا تاوطخلا لمكأ

- ا. لوؤسملا دامتعا تانايب مادختساب **(ISE) ةيموسرلا مدختسملا ةەجاو** ىلإ لوخدلا لجس.
- . SCEP CA تا**فيصوت** مث ،**تاداەش ،ةرادإ** ىلع رقنا .2
- .(Add**) ةفاضإ** قوف رقنا .3
- .فصولاو مداخلا مسا لخدأ .4
- 5. الماكلاب لهؤملال لاجملا مسا وأ IP مادختساب SCEP مداخل URL ناونع لخداً (FQDN) لماكلاب لهؤمل. (لااثملا ليبس يلع ،<u>/http://10.10.10/certsrv/mscep)</u>).
- ةباجتساٍ ةقثبنم ةلااسر روهظ ىلاٍ حجانلا لاصتالا يدؤي .**لاصتالا رابتخاٍ** ىلع رقنا .6 ةحجان مداخ.
- .ليكشتلا تقبط in order to **ظفح** ةقطقط .7
- 8. **مداخ ةداەش ليزنت نم دكأت**و <mark>تاداەش نزخم</mark>و <mark>تاداەش</mark>و <mark>ةرادإ</mark> قوف رقنا ،ققحتلل .NDES RA **مداخ ةداەش ليئاقل**ت ISE.

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ اًيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال مسقلا اذه مدختسا.

ةماعلا اهحالصإو ءاطخألا فاشكتسأ تاظحالم

نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي يتلا ةمهملا تاظحالملاب ةمئاق يلي اميف اهحالصاو:

- طاقن ديدحت يف ةدعاسملل ةيقطنم قيرط طاقن ىلإ BYOD ةكبش ططخم ميسقتب مق CA. و NDES و ISE ةياهنلا طاقن نيب راسملا لوط ىلع كاسمالاو ءاطخألاا حيحصت
- .عئاشلا (NTP) ةكبشلا تقو لوكوتورب تقو ردصم يف CA و ISE ةدقع ةكراشم نم دكأت •
- NTP تارايخ مادختساب ايئاقلت تقولا نييعت ىلع ةرداق ةياەنلا طاقن نوكت نأ بجي TP تارايخ مادختساب ايئاقلت DHCP.
- .ISE ةدقعل FQDN لح ىلع ارداق ليمعلاب صاخلا DNS مداخ نوكي نأ بجي •
- . NDES مداخو ISE نيب هاجتإلا يئانث لكشب TCP 443 وأ/و NDES ب حامسلا مت هنأ دكأت •
- نم نسحملا ليجستلا ببسب Windows ليغشتلا ماظنب لمعي زامج عم رابتخالاب مق Apple ةدعاسملا ةادألا عم Apple نم iDevice زامج مدختساً ،يرايتخإ لكشبو .ليمعلا بناج iPhone Configuration Utility ليمعلا بناج نم مكحتلا تادحو تالجس ةبقارمل
- ocogle وأ Google مدختساو ،ليجستلا ءاطخأل لجس قيبطت NDES مداخو CA لا تبقار أطخ اذه تثحب order to
- نيب مزحلا طاقتلاا تايلمع ليهست لجأ نم SCEP ل HTTP مدختساً ،رابتخالاً قلحرم لاوط ISE و NDES و CA.
- ةكرح ةبقارمو ،(ISE (PSN ةسايس ةمدخ ةدقع ىلع TCP غيرفتل ةدعاسملا ةادألا مدختسأ **تاودألا < صيخشتلا تاودأ < تايلمعلا** نمض اذه دجويو .NDES مداخ ىلإو نم تانايبلا رورم **ةماعلا**.
- حاتفم ىلع نيتماعد نيب ةحسف تلمعتسا وأ ،لدان NDES و CA لا ىلع Wireshark تبكر مايسو SCEP تا لا نمو ىلإ رورم ةكرح SCEP ضبق ىلع in order to ،طيسو
- تاداەش ةقداصمل ISE جەن ةدقع ىلع ةبسانملا CA تاداەش ةلسلس تيبثت نم دكأت ليمعلا.
- المعلا الله المعالية المالي ا مامضنال المالي عان المالي ا
- .ةحيحصلا EKU تامس دوجو نم دكأتو ةيفرطلا ةطقنلاو ISE ةيوه تاداهش ةنياعمب مق •
- اليعمل (GUI) ةيموسرلا مدختسملا ةهجاو يف ةرشابملا ةقداصملا تالجس بقار ضيوفتلاو ةقداصملا قافخإل. ريغ EKU ناك اذإ ليمعلا تاداهشل لدابت ةئيهتب نيبلاطملا ضعب موقي ال :**قظحالم** لشف تالاح نوكت ال دق ،كلذل .مداخلا ةقداصمل EKU ب ةدوزم ليمع ةداهش لثم ،حيحص ISE.
- يعرف وأ يرذج قدصم عجرم صيصخت متيس ،ةعزوم رشن ةيلمع يف NDES تيبثت دنع مداخ لسري .ةمدخلا تيبثت يف رتويبمكلا مسا وأ قدصملا عجرملا مسا ةطساوب دعب نع ةداهش ليجست ةيلمع تلشف اذإ .اذه فدهلا CA مداخ ىلإ ةداهشلا ليجست تابلط NDES

مداخ (PCAP) مزحلا روص رهظت دقف ،قياهنلا أطخ ISE. مسا نم الدب رتويبمكلا مسا رايخ ددحو NDES ةمدخ تيبثت دعأ ،ةلكشملا هذه لحل قدصملا عجرملا.

- ماظن موقي ال .ةحوللاا ىلع ةزهجألاا بيكرت دعب SCEP CA ةلسلس يف تارييغتلا بنجت اقبسم تبثملا BYOD فيرعت فلم ثيدحتب ،Apple iOS لثم ،Endpoint OS ليغشتلا ةلازاو ،ةياهنلا ةطقن نم يلاحلا فيرعتلا فلم فذح بجي ،اذه iOS لاثم يف .ايئاقلت .ىرخأ ةرم مامضنالا ذيفنت نكمي ىتح ،ISE تانايب ةدعاق نم ةياهنلاا ةطقن

ليمعلا بناج نم ليجستلا

ليجستلا ءاطخأ فاشكتسال اهمادختسإ متي يتلا ةديفملا تاينقتلاب ةمئاق يلي اميف اهحالصاو ليمعلا بناج نم:

• تاقيبطتل ليمعلا بناج نم تالجسلا ضرعل log ːtempː/\spwProfileLog.txt. تاقيبطتل ليمعل ابناج فرعت Microsoft Windows.

او Microsoft Windows ةياهن ةطقن نيب لاصتالل WinHTTP مادختسإ متي :**قظحالم** ISE. ءاطخألاا زومرب ةمئاق ىلع لوصحلل Microsoft Windows يف <u>أطخلا لئاسر</u> ةلاقم عجار.

- تاقيبطتل ليمعلا بناج نم تالجسلا ضرعل sdcards/downloads/spw.log/ رمألا لخدأ Android.
- المع نع ثحباو ،مكحتلا ةدحو قيبطت مدختسأ ، Mac OSX كلإ ةبسنلاب ه SPW.
- . لئاسرلا ضرعل <u>Apple 2.0 نوكم</u> مدختسأ ،Apple iOS ليغشتلا ماظنل ةبسنلاب •

ISE ليجست

لجس ISE لا تدهاش steps in order to اذه تمتأ

- ISE ةسايس ةدقع ددحو ،**ءاطخألا حيحصت لجس نيوكت < ليجست < ةرادإ** ىلإ لقتنا .1 .ةبسانملا
- . ةجاحلا بسح ،عبتتلا وأ ءاطخألا حيحصت ىل**ِ ميدقتلاو لِيمعلا** تالجس نييعتب مق .2
- ل.ثم ،ثحبلا ليەستل ةلصلا تاذ ةيساسألا تامولعملا قيثوتو ةلكشملا جاتنإ ةداعإ .3 مدختسملاو ،MAC، IP

- 4. ةبسانملا ISE ةدقع ددجو ،**ليزنتلا تالجس < تايلمعلا** ىلإ لقتنا.
- 5. قامسملاا تالجسلا ليزنتب مق ،**ءاطخألا حيحصت تالجس** بيوبتلا ةمالع يف بتكملا حطس <u>يل</u>إ.
- الجسلا تافلم ليلحتل <u>++ Notepad</u> لثم ،يكذ ررحم مدختسأ .6
- . يضارتفالا يوتسملا يل لجسلا تايوتسم دعاً ،ةلكشملا لزع دنع.

اهحالصإو ءاطخألا فاشكتساو NDES لوخد ليجست

<u>قكبشلا ةزەجأ ليجست ةمدخ ءاطخأ فاشكتساً :AD CS</u> ةلاقم ىلإ عجرا ،تامولعملا نم ديزمل يف <u>امحالصاو</u> Windows Server.

ةلص تاذ تامولعم

- <u>تاداەشلا عجرم مداخ نيوكت BYOD لولح ليلد</u> •
- Windows 2008 R2 يف NDES دلع ةماع ةرظن •
- <u>MSCEP ريرقت</u>
- <u>SSL معدل NDES مداخ نيُوكت</u> •
- EAP-TLS عم PEAP وأ EAP-TLS مادختسإ دُنع قداهشلاً تَابِلُطُتم •
- <u>تادنتسملاو ينقتلا معدلا</u> •

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