Issuing certificates with Microsoft Certificate Authority for use on FortiGate units

This article describes how to use a "stand-alone" Microsoft Certificate Authority (CA) to issue certificates for use on FortiGate units. Once the certificates have been installed on the FortiGate units, they can be used to establish an IPSec VPN tunnel between units.

Microsoft CA Installation on Windows 2003 Server

There are two types of CA installations:

- "Enterprise" for Active Directory domain services. Some certificates are stored in AD.
- "Standalone" as a standard/generic type CA (this will be used for issuing FortiGate certificates).

To install the CA, go to Add/Remove Programs > Add/Remove Windows Components > Certificate Services.

CA Type Select the type of CA y	ou want to set up.			R
C Enterprise root CA				
C Enterprise subordina	ate CA			
Stand-alone root CA				
C Stand-alone subord	inate CA			
Description of CA type The most trusted CA i	e n a CA hierarchy.			
L				
			·	
Use custom setting:	s to generate the key p	pair and CA cert	tificate	
П Цse custom setting:	s to generate the key p	pair and CA cert	uhcate	
☐ <u>U</u> se custom setting:	to generate the key p	pair and CA cert	incate	

<u>C</u> ommon name for this C/	A:
rootca	
Distinguished name suffi	с.
DC=deka-corp,DC=com	
Preview of distinguished	name:
CN=rootca,DC=deka-co	rp,DC=com
⊻alidity period:	Expiration date:
Second se	10 111 10000 11 15 111

If IIS is installed, then a web based interface will be available to manage certificates upon installing the CA. Otherwise it is managed through a Microsoft Management Console (MMC).

Managing the installed CA service with MMC and the 'Certificate Authority' snap-in module.

🚡 Console1 - [Console Root\Certific	ation Authority (Local)\rootca]	_ 8 ×
📸 Eile Action View Favorites	<u>W</u> indow <u>H</u> elp	_ 8 ×
	• •	
Console Root	Name	
E 📷 Certificates - Current User	Revoked Certificates	
Trusted Root Certification Aut Enterprise Trust	Pending Requests	
🗄 🧰 Intermediate Certification Aut		
Active Directory User Object Trusted Publishers		
Ontrusted Certificates		
Third-Party Root Certification Trusted People		
🗄 📄 Certificate Enrollment Reques		
Revoked Certificates		
Pending Requests		
Failed Requests		
2		

Exporting FortiGate certificate requests

In this example, two FortiGate units will use certificates to setup an IPSec VPN between them. The example below demonstrates the procedure performed on one FortiGate unit only. A similar procedure will have to be performed for the second unit.

Generate a certificate request (i.e. a public key), to be signed by a CA. Enter an identifier for this certificate request. Here, the gateway's public IP address was used.

	re. 60			P Q ‡ 🖬 🕯
Durture	Local Certificates	CA Certificates		
System				
Router		Gene	erate Certificate Signing Request	
Firewall		Certification Name	gw1	
User		Subject Information		
- VPN		ID Type	Host IP	
IPSEC		IP	62.212.107.74	
PPTP		LL	· · · · · · · · · · · · · · · · · · ·	
L2TP		Optional Information		
centincates		Organization Unit		
IPS		Organization		
Anti-Virus		Locality(City)		
Web Filter		State/Province		
Spam Filter		Country		
Log&Report		e-mail		
		Кеу Туре	RSA	
		Key Size	2048 Bit 💌	
			OK Cancel	
C FORTINET				NETWORK PROTECTION

Certificate Request output example (filename is "gw1.csr"):

----BEGIN CERTIFICATE REQUEST----

MIICXDCCAUQCAQAwGTEXMBUGA1UEAxMONjIuMjEyLjEwOC4xODEwggEiMA0GCSqG SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7AAlidX3rsEXEiQ2BKM/cIz1bWj3ZSQx1 HtDRzsvpgrAeWlcJvLG9wN10Ym3d+oyZoB+m6eMoWSeO9KNsjl1tyweIOwZDkdUY P56Wt+SH/cIRAKB447kBhFBlkfFu4bpR39Ta7dusfLPMKoRbXOsWFOvaAu3eJ4k5 3qSbYf26AEvlCMQsXBazXydgiWQgswaPgPxL3afJ7vuDFaC6Zh2Qr7m2RACG0BRj uLWVnymRMIkUTIXxmxBWymnx2PslFomm5HBJZ128uvLAA5gwYMdS10fbiVRT+653 1jgha3X4ansWcFLKVDXDQkb0VDSLkYPM2GWeHt06gvkOcpoYD4xrAgMBAAEwDQYJ KoZIhvcNAQEEBQADggEBAD2BfMsuG6fqYsPNxhf+R5WbKSV0C+Y/WPe524XM6SfW vMt2jmj7YHFV7I/xpG/liyQx+x2X9pISkwECbfGYBLuewPNshD1rxB0hzlKioMF3 2KZfSvVb+DFzSLGfSF+/TYvidWOlmiIsgovibVc7oW3u2eXywhtWjHUHgQP3rL7p fPuDff3zB/Ejx8T1X4DaC4Cl+DbPuCiwt0XmO5sAVOAfLRbyvOV/IrJhoIN0r2HI 2kDH+xfqJAJmb4bDERFJUjRMX4gKTdYVEs2LaEvOIkPffw4iSs2hVtvgdfWMWnH1 Ko+FaHdxLkv6POdSUYw9RUJyT9wB2U16/pqHky2tLLA=

----END CERTIFICATE REQUEST----

Submit the FortiGate unit's certificate request to the Microsoft CA for signing. During this procedure, the FortiGate unit's public key will be signed with the CA's private key.

Image: Second Second Image: Second Sec	🚡 Console1 - [Console Root\Certificat	on Authority (Local)\rootca]	
Image: Control of Control Control Control of Control Contro	📸 Eile Action View Favorites Wir	dow <u>H</u> elp	X
A 11 Ges Bord Cartificates - Current User Bord Cartificates Cartificates - Current User Bord Cartificates Feeding Requests Failed Requests Failed Pacificates Failed Pacificate Failed Pacificates Failed Pacif	⇔ → 🗈 🖬 😭 🛱 😫	► ■	
Certification Certification Stort Service Stort S	Console Root	ame Revoked Certificates Issued Certificates Pending Requests Failed Requests	
Yjew Stop Service New Window from Here Submit new request New Iaskpad View Back up CA Refresh Restore CA Export List Renew CA Certificate Properties Help	Outrusted Certificates Outrusted Certificates Outrusted People Outrusted People Outrusted People Outrusted Enrollment Reques Outrusted Enrollment Reques Outrusted Enrollment Reques Outrusted People OutrustedPeople Ou	Start Service	
Refresh Export List Properties Help	View New <u>Window from Here</u>	Stop Service Submit <u>new request</u> Back up CA	
Properties Help	Refresh Export List	Restore CA Renew CA Certificate	
	Properties		
	Help		
		_	

View the Pending Requests, and Issue (sign) the certificate request.



Once Issued, the certificate needs to be exported from the CA database, and imported back into the FortiGate unit.



-

Cancel

View menu, click Add/Remove Columns.

Columns that contain binary data:	
Binary Certificate	

Export options:

- O View formatted text version of data
- Save binary data to a file

0K

Save jn: 🔂 🛅 shared		-	🗕 🖻 🛗	•
Image: Constraint of the second constraints Image: Constraint of the second	ord-bug T-cfg -cfgs *_workshop_v2.7.txt -edition-serial-number.txt sr igned.cer		 clientoverri clientoverri clientoverri clientoverri confall confall-fgté dante-1.1. debug.log default.htm dhcp-3.0pl dhcpd.conf dhcpd.conf dhcp-over- dhcp-relay 	deip-test.log deip-test.tcp deip-test_B290 deip-test_B290 50-dhcp.tar.gz 14.tar.gz n 1-9.i386.rpm : ipsec-fgt2.80b -debug.txt
File name:	dw1 cer		-	Save
Au Network Save as type	All Files (*.*)		-	Cancel

Each certificate (i.e. a signed certificate request), needs to be imported back into the respective FortiGate units. In the example below, the above-signed "gw1.csr" file (which becomes a "gw1.cer" file), gets imported back into the FortiGate unit.

	FortiGr	are. 60						
111	WEB CONFIG		and the second se					ALL
	System Router	Local Certificates Generate	CA Certificates					
Ľ		Name		Subject		Status		
	Firewall	gw1				PENDIN	G	Ì 📴
	User							
-	VPN							
	IPSEC							
	PPTP							
	L2TP							
	Certificates							
	IPS							
	Anti-Virus							
	Web Filter							
	Spam Filter							
	Log&Report							
	FORTINET				Up 3 Days 0 Hours	REAL TIME	NETWORK	PROTECTION

Upload Local Certificate	
Upload File: \\.host\Shared Folders\shared\gw1.cer Brows	e
OK Cancel	

Generate	Import	
Name	Subject	Status

Note: Clicking on the certificate .cer file (on a different PC that does not have the root certificate installed) opens the following dialog box:

Certificate	? ×
General Details Certification Path Image: Certificate Information Windows does not have enough information to verify this certificate.	This message is due to the fact that the Root certificate is not installed.
Issued to: 62.212.107.74	-
Issued by: rootca Valid from 11/10/2004 to 11/10/2005	
Install Certificate	OK

rtificate					?
General Details	Certification F	ath			
Show: <a>All>		<u> </u>	·		
Field		Value			
Version		V3			
Serial numb	er	61FC C3(65 0000 000	0 0002	
📃 Signature a	lgorithm	sha1RSA			
EIssuer		rootca, d	leka-corp, c	om	
Valid from		Monday,	October 11	, 200 <mark>4</mark> 16	
Valid to		Tuesday	October 1	1, 2005 1	
Subject		62.212.1	07.74		
		R5A (204	ið Bits)		_
3082 010A	0282 0101	. 00F3 761	DE 76E2	C4C8	
48DF F1AD	DC50 78BB	5 5107 БА. 7 1Е5А 1D	97 DA66	5131	
5B1C 7B83	FEE5 CE2C	287C 26	2C FE22	6F30	
76CC F0A2	02F3 4F12 0754 3602	2 050C C6	5F 4FD8 83 F460	4980 CAE3	-
36F1 5999	3AFC D699	CF55 93	F5 3E8F	032D	
8CBC 25B5	CA96 4E40	E9F0 BD	D8 CE4B	1E7F	-1
14ABC 6845	9025 1266	BAC3 D5	55 FB/3	657B	<u> </u>
		Edit Properti	es,.,	Copy to File.]
				0	ж

The CA's certificate (i.e. the CA's self-signed public key), must now be imported into each Fortigate device. To export the root certificate, select it in the MMC Certification Authority (Local) snap-in, and right-click its Properties.

Viewing the installed root certificate on the CA host, using a mmc snap-in:

🚡 Console1 - [Console Root\Certificates - C	urrent User\Trusted Root Certificatio	on Authorities\Certificates]			_ 8	N X
📸 Eile Action Yiew Favorites Window	Help				_ 8	1×1
	ş -					
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	
🖻 🐻 Certificates - Current User	EFESTE, Public Notary Certs	FESTE, Public Notary Certs	1/1/2020	Secure Email, Server	FESTE, Public Notary	
🕀 🧰 Personal	FESTE, Verified Certs	FESTE, Verified Certs	1/1/2020	Secure Email, Server	FESTE, Verified Certs	
Trusted Root Certification Authorities	🔛 First Data Digital Certificates Inc	First Data Digital Certificates Inc. Ce	7/3/2019	Server Authenticatio	First Data Digital Cer	
	FNMT Clase 2 CA	FNMT Clase 2 CA	3/18/2019	Secure Email, Server	Fabrica Nacional de	
Enterprise Trust	🔤 GlobalSign Root CA	GlobalSign Root CA	1/28/2014	Secure Email, Server	GlobalSign Root CA	
Intermediate Certification Authorities	GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/14/2018	Secure Email, Client	GTE CyberTrust Glob	
Active Directory User Object	GTE CyberTrust Root	GTE CyberTrust Root	4/4/2004	Secure Email, Client	GTE CyberTrust Root	
	GTE CyberTrust Root	GTE CyberTrust Root	2/24/2006	Secure Email, Client	GTE CyberTrust Root	
Third-Party Root Certification Authoritie	Http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server	ValiCert Class 1 Polic	
F Trusted People	Http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server	ValiCert Class 3 Polic	
🗄 🧰 Certificate Enrollment Requests	http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server	ValiCert Class 2 Polic	
🖻 💼 Certification Authority (Local)	IPS SERVIDORES	IPS SERVIDORES	12/30/2009	Secure Email, Server	IPS SERVIDORES	
🖻 👩 rootca	Microsoft Authenticode(tm) Root	Microsoft Authenticode(tm) Root Au	1/1/2000	Secure Email, Code S	Microsoft Authentico	
Revoked Certificates	🔛 Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<all></all>	Microsoft Root Auth	
🛅 Issued Certificates	Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/10/2021	<all></all>	Microsoft Root Certif	
- 🧰 Pending Requests	NetLock Expressz (Class C) Tanusi	NetLock Expressz (Class C) Tanusitv	2/20/2019	Server Authenticatio	NetLock Expressz (Cl	
Failed Requests	🖭 NetLock Kozjegyzoi (Class A) Tanu	NetLock Kozjegyzoi (Class A) Tanusit	2/20/2019	Server Authenticatio	NetLock Kozjegyzoi (
	🔤 NetLock Uzleti (Class B) Tanusitva	NetLock Uzleti (Class B) Tanusitvany	2/20/2019	Server Authenticatio	NetLock Uzleti (Class	ŝ.
	NO LIABILITY ACCEPTED, (c)97 V	NO LIABILITY ACCEPTED, (c)97 Veri	1/8/2004	Time Stamping	VeriSign Time Stampi	
	PTT Post Root CA	PTT Post Root CA	6/26/2019	Secure Email, Server	KeyMail PTT Post Ro	
	rootca	rootca	10/11/2009	<a >	<none></none>	
	🔤 Saunalahden Serveri CA	Saunalahden Serveri CA	6/26/2019	Secure Email, Server	Saunalahden Serveri	
	🖼 Saunalahden Serveri CA	Saunalahden Serveri CA	6/26/2019	Secure Email, Server	Saunalahden Serveri	
	Secure Server Certification Authority	Secure Server Certification Authority	1/8/2010	Server Authentication	VeriSign/RSA Secure	
	SecureNet CA Class A	SecureNet CA Class A	10/16/2009	Secure Email, Server	SecureNet CA Class A	
	SecureNet CA Class B	SecureNet CA Class B	10/16/2009	Secure Email, Server	SecureNet CA Class B	
	SecureNet CA Root	SecureNet CA Root	10/16/2010	Secure Email, Server	SecureNet CA Root	
	SecureNet CA SGC Root	SecureNet CA SGC Root	10/16/2009	Secure Email, Server	SecureNet CA SGC R	
	SecureSign RootCA1	SecureSign RootCA1	9/15/2020	Secure Email, Server	Japan Certification S	
	SecureSign RootCA2	SecureSign RootCA2	9/15/2020	Secure Email, Server	Japan Certification S	
	SecureSign RootCA3	SecureSign RootCA3	9/15/2020	Secure Email, Server	Japan Certification S	
	SERVICIOS DE CERTIFICACION	SERVICIOS DE CERTIFICACION - A	3/9/2009	Secure Email, Server	SERVICIOS DE CERT	
	SIA Secure Client CA	SIA Secure Client CA	7/9/2019	Secure Email, Server	Societa Interbancari	
	SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server	Societa Interbancari	
	TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	-
4 I I I	4			1	1	

Certificate	e Managers Rest	trictions	Au	diting	Security
General	Policy Module	Exit Mod	lule	Extensions	Storage
Certificatio	n authority (CA)				
Name:	rool	tca			
<u>C</u> A certific	ates:				
Certificate	e #O				
			(<u>V</u> iew Ce	ertificate
			(<u>V</u> iew Ce	ertificate
- Cryptograf	ohic settings		(<u>V</u> iew Ce	ertificate
- Cryptograp CSP:	ohic settings Mic	rosoft Strong	Cryptog	⊻iew Ce Iraphic Provide	ertificate
Cryptograp CSP:	ohic settings Mic	rosoft Strong	(Cryptog	⊻iew Ce graphic Provide	ertificate
Cryptograp CSP: Hash algo	ohic settings Mic rithm: SH/	rosoft Strong A-1	C ryptog	View Ce graphic Provide	ertificate
Cryptograp CSP: Hash algo	ohic settings Mic rithm: SH/	rosoft Strong A-1	C ryptog	⊻iew Ce graphic Provide	ertificate



Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
DER encoded binary X.509 (.CER)	
C Bage-64 encoded X.509 (.CER)	
◯ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
${igsaclimits}$ Include all certificates in the certification path if possible	
C Personal Information Exchange - PKC5 #12 (.PFX)	
${igsaclimits}$ Indyde all certificates in the certification path if possible	
🔲 Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
\square Delete the private key if the export is successful	
\square Delete the private key if the export is successful	
	Canad

This now needs to be imported into each Fortigate.

Local Certificates	CA Certificates	
	Upload CA Certificate	
	Upload File \\.host\Shared Folders\shared\rootcert.cer Browse	
	OV Cancel	
	UK Caricer	

cal Certificates <u>CA C</u>	ertificates	
Import		
Name	Subject	
CA_Cert_1	/DC=com/DC=deka-corp/CN=rootca	💼 🤬 📴

The FortiGate units are ready to use certificates to setup an IPSec tunnel between them. For further details, see the *FortiGate VPN Guide* and *Administration Guide* as well as as the following Fortinet Knowledge Center articles:

- http://kc.forticare.com/default.asp?id=422&Lang=1
- http://kc.forticare.com/default.asp?id=730&Lang=1

Note: Viewing (clicking on) the Root CA .cer file on a PC that has not generated the certificate, will result in the following message:

🕎 Certificate II	nformation
This CA Root certifi install this certifica Authorities store.	cate is not trusted. To enable trust, te in the Trusted Root Certification
Issued to: roo	otca
Issued by: roo	otca
Valid from 11/	10/2004 to 11/10/2009

Once installed, it will present the following:

🚞 Certifica	te Inforn	nation			
This certificate	is intend	led to:			
•Ensures th •Proves you •Ensures so •Protects so •Protects e •Allows dat	e identity ir identity ftware car oftware fro mail messa a to be sign	of a remote to a remote me from so om alteratio ages ned with th	e computer e computer ftware publi on after pub e current tir	sher ication ne	
Issued to:	rootca				
Issued by:	rootca				
¥alid from	11/10/20)04 to 11;	10/2009		

Note: Re-viewing the gw1.cer on the PC with the root CA certificate installed, results in a proper verification and recognition of the certificate:

licate		
neral Details Certificati	ion Path	
Certificate Infe	ormation	
This certificate is inte	ended to:	
•Ensures the identi	ity of a remote computer	
 Ensures software 	came from software publisher	
 Protects software 	e from alteration after publication	
 Protects e-mail me Allows data to be 	essages signed with the current time	-
	12.107.74	
Issued by: roote	a	
Valid from 11/10)/2004 to 11/10/2005	
	Toctall Cartificate	r Statemen
		a proteinein
		1022

