Forefront UAG mit DirectAccess

CA installieren oder existierende verwenden





Weitere Informationen zur Public Key-Infrastruktur

< Zurück Weiter > Installieren Abbrechen

Gültigkeitsdauer Zertifikatdatenbank Webserver (IIS) Rollendienste Bestätigung Status Ergebnisse

UAG Setup



Forefront UAG Setu	up Wizard
1. Welcome	Welcome to the Forefront UAG Setup Wizard
 Agreement 	
3. Select 3. Location	This wizard guides you through the UAG Installation process.
4. Install	It is strongly recommended you exit all programs before running Setup.
5. Finish	
	< Back Next > Cancel
	Concer

Forefront UAG Setup) Wizard
1. Welcome	
2. Sign 2. Agreement	Select Installation Location
3. Select J. Location	Install UAG in the following location.
4. Install	C:\Program Files\Microsoft Forefront Unified Access G
5. Finish	
	< Back Next > Cancel

Forefront UAG Set	up Wizard
1. Welcome	
2. Sign 2. Agreement	Installing Forefront UAG
3. Select Location	Installing Forefront UAG may take some time. Please wait
4. Install	Progress: Installing Roles and Features15%
5. Finish	
	< Back Next > Cancel

Forefront UAG Setu	up Wizard
1. Welcome	
2. Sign 2. Agreement	You have successfully completed the Forefront UAG Setup Wizard
3. Select Location	The server must be restarted .
4. Install	Restart now C Restart later
5. Finish	
	< Back Next > Cancel

NIS und Malware Update aktiviert

Not P & Advanced and P Second P Advanced P Advanced P Second P Advanced P Second P Sec		1.000	/					
	🕻 📦 🗔 📋 RDP 🗸 Administratio	n *						
iei allo Aradol ? Norder Forder The Management Gateway 2010 Proved Forder 11% (Geberroot) Proved Forder 11% (Geberroot)	Forefront TMG							
Intrusch Fordert Kinds Hangaren Kateway 200 Fordert Mickelsen Molice Kateway 200 Fordert Mickelsen Mickelsen Mickelsen Mickelsen Kateway 200 Fordert Mickelsen Mickelse	atei Aktion Ansicht ?							
http://www.income.com/com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/come.com/com/come.com/come.com/come.com/com/come.com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/come.com/com/com/come.com/com/com/come.com/com/com/com/come.com/com/com/	• 🔿 🖄 📅 📓 🐨	🦸 🤿						
Kelated	Horsont Fordrort Threat Manageme Fordrort Kineta (desbarvico)) Dathbaad Monoring Ferwall Policy Ferwall Policy Ferwall Policy Ferwall Policy Fermion Prevention System Remote Access Policy (VPN) Fermion Prevention System System System Logis Reports Databashooting Troubleshooting	Cefinition Updates Group by: Crone> Protection Mechanism Makeres Inspection System Network Inspection System	tervay 2010 Sarve changes and update the configurat Sarve Changes in Configuration Sarve Changes in Configuration Sarve Configuration Existing class co	on, dok Apply.	e new cread polety	rson [Licerson 0.0 ⊘ Erp 0.0 ⊘ Hev	e Status Ires on 27.08,2010 er Expites	Iask Refresh Refresh Attora Ptedun Definitior Config Conf

WFP Filter Konflikt Meldung kann ignoriert werden

http://blogs.technet.com/yuridiogenes/archive/2010/02/16/wfp-filter-conflict-detectedalert-after-installing-forefront-tmg-2010.aspx

UAG Update 1 installieren

😽 Microsoft F	prefront Unified Access Gateway Setup		
Installing	Microsoft Forefront UAG Update 1		
Please v This ma	vait while the Setup Wizard installs Microsoft F / take several minutes.	orefront UAG Update 1.	
Status:	Computing space requirements		_
,	Ç,		
	Back	Next	ancel

Fehlermeldung bei der Installation

Name *		Änderungsdatum T	ур	
i 開Microsoft Forefront Unified Access Gateway Setur	Dieser Ordner ist leer.			
The installer has insufficient privileges to access to directory: C:\Program Files\Microsoft Forefront U Access Gateway\von\Von\tor\languages. The installation cannot continue. Log on as administra- contact your system administrator.	this Jnified IX ator or Wicrosoft Forefront Uni	ified Access Gateway Set	tup	
Cancel Cancel	Installing Microsoft	Forefront UAG Update	1	
子 ForefrontUAG_KB981323_ENU 29.04.2011 29.04.2011 29.04.2011	0 11:57 Please wait while the This may take severa	Setup Wizard installs Microso I minutes.	oft Forefront UAG Update 1.	
Sie verfügen momentan nicht über die B des Zugriffs auf diesen Ordner.	Status: Copying ner	w files		_
Klicken Sie auf "Fortsetzen", um dauerhaft Zug Ordner zu erhalten.	riff auf diese		•	
Fortsetzen	Abbrechen			Fernster
		Bad	k Next C	ancel
	I			

📕 Eigenschaften von languages		
Allgemein Freigabe Sicherheit Vorg	ängerversior	en Anpassen
Objektname: C:\Program Files\Micro	osoft Forefrom	nt Unified Acces
Gruppen- oder Benutzernamen:		
SYSTEM		
METZWERKDIENST		
Administratoren (B BSSC Contractor A	anen-Admin: dministratore	sj n)
, Klicken Sie auf "Bearbeiten", um die Berechtigungen zu ändern.		Bearbeiten
Berechtigungen für "SYSTEM"	Zulassen	Verweigern
Vollzugriff	~	<u> </u>
Ändern	~	
Lesen, Ausführen	~	
Ordnerinhalt anzeigen	~	
Lesen	~	-
Schreiben	~	<u> </u>
Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.	e	Erweitert
Weitere Informationen über Zugriffssteu	ierung und B	erechtigungen
ОК	Abbrechen	Obernehmen

Besitz uebernehmen fuer den SYSTEM Account

Erweiterte Sicherheitseinstellungen für "Monitor"
Berechtigungen Überwachung Besitzer Effektive Berechtigungen
Sie können die Besitzrechte für dieses Objekt übernehmen oder zuweisen, wenn Sie über die erforderlichen Berechtigungen oder Privilegien verfügen.
Objektname: C:\Program Files\Microsoft Forefront Unified Access Gateway\von\Monitor
Aktueller Besitzer:
SYSTEM
Besitzer ändern nach:
Name Administratoren (D grote (grote@####################################
Bearbeiten
Weitere Informationen über Besitz von Objekten
OK Abbrechen Übernehmen





Report Server Konfiguration

Reporting Services Configuration Mana	ger: D* Think D\ISARS	_ 🗆 🗵
Microsoft SQL Server 2008 Reporting Services Config	uration Manager	
Connect Conne	E-mail Settings To use report server e-mail, specify an existing SMTP server and an e-mail account that can send e-mail from that server. SMTP Settings To edit, change the fields and click the Apply button. Sender Address: UAG-Report® Gurrent SMTP Delivery Method: Use SMTP server SMTP Server: Results	
0	Apply	Exit

Grundkonfig



Adapter name	Internal	External	Unassigned
BAD		×	
GOOD	_ ~		
SSL Network Tunneling			V
Adapter name: GOOD IP DHCP enabled: No IP address: 10.80,16.79 Subnet mask: 255.255.252.0 Default gateway: DNS DHCP enabled: No DNS server(s): 10.80,16.80 Static route: No			

pecify how network adapters a odify the network adapter set	are connected t tings.	o your netw	ork, and
Adapter name	Internal	External	Unassigned
BAD		×	
GOOD	×		
SSL Network Tunneling			V
Adapter name: BAD P DHCP enabled: No P address: 212.212.10.2 Subnet mask: 255.255.255.0 Default gateway: 212.212.10.	240		



Single Server

Server Management Wizard 🛛 🗙
Select Configuration
Specify whether this is a single Forefront UAG server, or configure it as an array member.
C Array member
Forefront UAG array members must belong to a domain.
< Zurück Weiter > Abbrechen



🛱 Activate Configuration			×
💮 Activate Configuration	1		
The system is being at Enter a password and	tivated for the first time. choose a directory to store the backup configuration files.		
Password:	•••••		
Confirm password:	••••••		
Backups directory:	C:\ProgramData\Microsoft\UAG\AutoBackups	Browse	
		Weiter	Abbrechen

Ö Ac	tivate Configuration 🛛 🛛 🗙	1
G	🔅 Activate Configuration	
	You must activate the configuration to apply your changes. If you select to back up the configuration, current settings (prior to activation) will be saved.	
	Back up configuratio	
	Activation might take several minutes.	
	Activate > Abbrechen	

Activate Configuration	
Activate Configuration	
Activation completed successfully	
The Forefront UAG configuration was saved, and the configuration was activated successfully. Synchronizing ch might take a few minutes.	nges
Fertig	stellen

Sorefront Unified Access G	Forefront Unified Access Gateway Activation Monitor								
Refresh 🔝 Options	Refresh 🗈 Options								
UAG Array Members	Severity	Message Activation is in progress since 13:22:06							
	•		Þ						

	_	
G Array Members	Severity	Message
UAG	State	Validating configuration settings.
	State	Starting activation.
	Information	Configuring NLB settings.
	Information	NLB settings were configured successfully.
	Information	Configuring the firewall.
	Debugging	Allowing incoming TCP connection for port: 50002'.
	Debugging	Allowing outgoing TCP connection for '10.80.16.79:50002'.
	Debugging	Allowing outgoing TCP connection for '212.212.10.2:50002'.
	Debugging	Allowing outgoing TCP connection for '212.212.10.3:50002'.
	Information	The firewall was configured successfully.
	Information	Configuring SSL Network Tunneling (SSTP).
	Information	The SSL Network Tunneling (SSTP) settings were configured successfully.
	Information	The Network Connector service was stopped successfully.
	Information	Activating Network Connector.
	State	Writing the configuration files.
	Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Reporter.xml].
	Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Repository.xml].
	Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Role.xml].
	Debugging	Writing the machine [UAG] [10.80.16.79] to the High Availability file.
	Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\Monitor\HAxml].
	State	Configuring Web sites.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Site.xml] was written successfully.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Acl.xml] was written successfully.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Policy.xml] was written successfully.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Resources.xml] was written successfully.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WFLB.xml] was written successfully.
	Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\common\conf\nap.xml] was written successfully.
	Debugging	The portal container [%s] was written successfully.
	Debugging	Writing the Trace parameter [high_water] [100].
	Debugging	Writing the Trace parameter [low_water] [50].
	Debugging	Writing the Trace parameter [instances_kept] [3].
	State	Writing the configuration to the registry.
	Debugging	Modifying the following registry settings: SOFTWARE\WhaleCom\e-Gap\Von\UrlFilter\WhIFiltSecureRemote\EncryptionIV to [BD
	Debugging	Modifying the following registry settings: SYSTEM/CurrentControlSet/Control/SecurityProviders/SCHANNEL/Ciphers/RC4 128/12
	Debugging	Modifying the following registry settings: 'SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 1
	Debugging	Modifying the following registry settings: 'SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/12
	Debugging	Modifying the following registry settings: 'SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128
	Debugging	Modifying the following registry settings: 'SYSTEM/CurrentControlSet/Control/SecurityProviders/SCHANNEL/Cinhers/DES 56/56/
	Debugging	Modifying the following projects actings: "SYSTEMIC whet Control Sci Control Society Deviders SCI ANNEL Control DCA 40(12)

Corefront TMG								×
File Action View H	File Action View Help							
🗢 🄿 🖄 📊 🛛	🗊 🖻 💺 😭	' 🗙 📀 📀 🌒	i 🔁 🧐 🖆	👷 🖻 🖻 🔮				
Microsoft Forefront T	Microsoft"	ont						Firewall Policy
Dashboard	Threat N	Anagement Ga	teway 2010					Enterprise
Monitoring	(i) Click have to	learn about the Cu	stomer Experien	co Improvement P	roara m			
Web Access F	Click liere to	learn about the cu	stomer Experience	te improvement P	rogram.			
😕 E-Mail Policy	All Firewall Pol							Toolbox Tasks Help
Remote Acce	Search	٩	Examples					
System	Order 🔶	Name	Action	Protocols	From / Listener	То	Condition 🔺	Firewall Policy Tasks
Logs & Repor	1 8	PublishingRule::C	Allow	ublishingRul	👍 Local Host	👍 Internal	🐣 All User:	Publish Exchange Web
Troubleshoot	🥂 9	PublishingRule::C	Allow	🖳 PublishingRul	👍 Local Host	👍 Internal	🐣 All User:	Client Access
_	🥂 10	PublishingRule::C	Allow	🖳 PublishingRul	👍 Local Host	👍 Internal	📇 All User:	Publish Mail Servers
	11	PublishingRule::C	Allow	🖳 PublishingRul	👍 Local Host	👍 Internal	🐣 All User:	Publish SharePoint Sites
	🥂 12	PublishingRule::C	Allow	🖳 PublishingRul	👍 Local Host	👍 Internal	🐣 All User:	Publish Non-Web Server
	13	PublishingRule::M	Allow	👰 PublishingRul	👍 Local Host	📃 PublishingRul	🐣 All User:	Protocols
	14	PublishingRule::M	Allow	🖳 PublishingRul	👍 Local Host	📕 PublishingRul	🐣 All User:	Create Access Rule
	15	PublishingRule::M	Allow	🖳 PublishingRul	👍 Local Host	📕 PublishingRul	🐣 All User:	Configure VoIP
	16	PublishingRule::M	Allow	🖳 PublishingRul	👍 Internal	👍 Local Host	🐣 All User:	Configure Client Access
	17	PublishingRule::A	🚫 Deny	퉳 All Outbound				Policy Editing Tasks
	🖃 📝 18	DirectAccess Allo	Allow	DNS Server	💐 Anywhere (IP	. 💐 DirectAccess	🐣 All User:	Edit Selected Rule
	🖃 📝 19	DirectAccess Allo	Allow	K Forefront TM	💐 Anywhere (IP	. 👍 Internal	🐣 All User:	Delete Selected Rules Move Selected Rules Up
	20	DirectAccess Prer	Allow	👰 HTTPS	👍 Local Host	👍 Internal	🐣 All User:	Disable Selected Rules
	🥂 21	ALL	🥝 Allow	💐 All Outbound	👍 Local Host	👍 Internal	🖀 All User:	
	💽 Last	Default rule	🚫 Deny		🛓 All Networks (. 🔹 All Networks (. 🐣 All User:	Related Tasks
								Go To Traffic Simulator
	4							Settings
								· · · · · · · · · · · · · · · · · · ·

Event Logging zum Exchange Server

🗟 Event Logging	×
General Built-In RAD	IUS Syslog Mail
Enable SMTP re	porting
IP address/host:	192.16
Port:	25
From:	UAG-Report@
To:	
Subject:	Mail From System Administrator
User:	
Password:	•••••
Confirm password:	••••••
	OK Abbrechen

Konfig speichern und aktivieren

5	1icrosoft For	efront Unif	ied Access Gateway
File	View Admin	Message:	s Help
	<u>N</u> ew	۲.	
	<u>S</u> ave	Ctrl+S	
Ö	Activate	Ctrl+G	cess Gateway
e	Import		
Ð	Export		Í
2	Reload Config	uration	
0	E⊻it		

Zertifikate

http://technet.microsoft.com/en-us/library/ee406213.aspx

Autoenrollment fuer Computer Zertifikate



Assistent für automatische Zertifikatanfor	derung X
Zertifikatvorlage Beim nächsten Anmelden des Computers, ausgewählte Vorlage zur Verfügung gestel	wird ein Zertifikat basierend auf die 🛛 🦪
Eine Zertifikatvorlage besteht aus einem S an Computer herausgegeben werden. Wä Zertifikatvorlagen:	atz vordefinierter Eigenschaften für Zertifikate, die hlen Sie eine Vorlage aus der Liste aus.
Name	Beabsichtigte Zwecke
Computer	Clientauthentifizierung, Serverauthentifizieru
Domänencontroller	Clientauthentifizierung, Serverauthentifizieru
IPSec	IP-Sicherheits-IKE, dazwischenliegend
Registrierungs-Agent (Computer)	Zertifikatanforderungs-Agent
•1 bs	
	<zurück weiter=""> Abbrechen</zurück>

IP-HTTPS Zertifikat

The IP-HTTPS certificate for the Forefront UAG DirectAccess server must have the following properties:

In the Subject field, either an Internet Protocol version 4 (IPv4) address of the Internet interface of the DirectAccess server or the fully qualified domain name (FQDN) of the IP-HTTPS uniform resource locator (URL).

For the Enhanced Key Usage field, the Server Authentication object identifier (OID). For the CRL Distribution Points field, a certificate revocation list (CRL) distribution point that is accessible by DirectAccess clients that are connected to the Internet. The IP-HTTPS certificate must have a private key.

The IP-HTTPS certificate must be imported directly into the personal store.

Zertifikate auf dem UAG Server anfordern

http://blogs.technet.com/edgeaccessblog/archive/2010/04/22/deep-dive-into-uagdirectaccess-certificate-enrollment.aspx

Template Berechtigungen

🙀 Active Directory-Standorte und -Dienste						
Datei Aktion Ansicht ?						
🗢 🔿 🖄 📷 🗙 🖬 🖻 🖦 🚺 🖬 🗼	2					
Real Active Directory-Standorte und -Dienste [TRAINER	Name	Тур	Beschreibung			
🖃 🧰 Sites	Administrator	Zertifikatsvorlage				
🕀 🚞 Subnets	🖳 CA	Zertifikatsvorlage				
Inter-Site Transports	🖳 CAExchange	Zertifikatsvorlage				
P IP	CEPEncryption	Zertifikatsvorlage				
	🖳 ClientAuth	Zertifikatsvorlage	Eigenschaften v	on WebServer		? ×
🕀 🔡 Hehlen	CodeSigning	Zertifikatsvorlage		f		
E Services	CrossCA	Zertifikatsvorlage	Allgemein	Anforderungsverar	beitung An	tragstellemame
MsmqServices	CTLSigning	Zertifikatsvorlage	Erweiterunger	n Sicherheit	Objekt	Attribut-Editor
NetServices	DirectoryEma	Zertifikatsvorlage	Gruppen-oder	Benutzemamen:		
Public Rey Services	DomainContr	Zertifikatsvorlage	A thortifi	iata Parutzar		
	DomainContr	Zertifikatsvorlage	Se Demineraliz	Admine (TRAINER) Dee	ainen Admine)	
Certificate Templates	🗵 EFS	Zertifikatsvorlage	da Domanen	Admins (TRAINER (DOI	Omeniantinas Admin	
E Certification authorities	EFSRecovery	Zertifikatsvorlage			Organisations-Admir	15)
Findment Services	EnrollmentAg	Zertifikatsvorlage		NIVER (UAGS)		
🗉 🧮 KRA	EnrollmentAg	Zertifikatsvorlage				
🗄 🧰 OID	ExchangeUser	Zertifikatsvorlage				
🕀 🚞 RRAS	ExchangeUs	Zertifikatsvorlage	,		L	
🕀 🚞 Windows NT	IPSECInterm	Zertifikatsvorlage			Hinzufügen	Entfernen
	IPSECInterm	Zertifikatsvorlage	Development	6- "UAC"		
	🗷 KerberosAut	Zertifikatsvorlage	Berechtigunger	itur UAG	Zulassen	Verweigem
	KeyRecovery	Zertifikatsvorlage	Vollzugriff			
	🗷 Machine	Zertifikatsvorlage	Lesen			
	A MachineEnrol	Zertifikatsvorlage	Schreiben			
	OCSPRespon	Zertifikatsvorlage	Begistrieren			- E - I II
	OfflineRouter	Zertifikatsvorlage			-	
	RASAndIASS	Zertifikatsvorlage				
	SmartcardLo	Zertifikatsvorlage				
	SmartcardUser	Zertifikatsvorlage	Klicken Sie auf	"Erweitert", um spezielle	e	Enweitert
	🖳 SubCA	Zertifikatsvorlage	Weiters	tionen üher 7.milleter		
	🖳 User	Zertifikatsvorlage	vveiteré informa	auorien über Zugnftssteu	lerung und berechti	gungen
	🕍 UserSignature	Zertifikatsvorlage				
	🚇 WebServer	Zertifikatsvorlage		OK Abbrech	en Übernehme	n Hilfe
	Workstation	Zertifikatsvorlage				
	-					

Firewallregel auf TMG Server fuer RPC Zertifikatanforderung

7 19	TMG: Zugriff auf PKI Server	Allow	💹 All Outbound 🚜 Local Host	💻 visaserve01 💒 All Users	Array
Saving Co	nfiguration Changes				
0	The changes were saved to the Configu configuration status to verify that chan members.	ration Storage. Che ges were applied to	ck OK all array		
	Existing client connections will be reeval configuration Client connections not ma will be dropped	luated according to t atching the newly en	he new forced policy		
	More about policy enforcement				
Descrip	tion of configuration change:				
Marc (http:// directa	Frote: Zugriffsregel fuer PKI Zugriff /blogs.technet.com/edgeaccessblog/archi access-certificate-enrollment.aspx	ve/2010/04/22/deep	-dive-into-uag-		

Strict RPC Checking ausschalten



Neues Zertifikat am UAG Server fuer DirectAccess anfordern

atei Aktion Ansicht Favoriten	Fenster ?					
) 🖄 📅 📋 🙆 😹 🚺	ī					
nsolenstamm	Ausgestellt für 🗠	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Aktionen	
Zertifikate (Lokaler Computer)	Default Web Site	Default Web Site	01.01.3999	Serverauthentifizierung	Zertifikate	
Zertifikate	WM5vc-DE5BSRV600	WM5vc-DESBSRV600	26.04.2020	Serverauthentifizierung	Weitere Aktionen	
Vertrauenswürdige Stammzertifiz						
Organisationsvertrauen						
📔 Zwischenzertifizierungsstellen						
Vertrauenswürdige Herausgeber						
Nicht vertrauenswurdige zertifik						
Vertrauenswürdige Personen						
Remote Desktop						
🦳 Smartcard vertrauenswürdige St						
📔 Vertrauenswürdige Geräte						
		1				

Zertifikatregistrierungsrichtlinie au	swählen	
Mithilfe der Zertifikatregistrierungsrichtlin registriert werden. Die Zertifikatregistrier	ie können Zertifikate basierend auf ungsrichtlinie ist möglicherweise ber	vordefinierten Zertifikatvorlagen reits für Sie konfiguriert.
Vom Administrator konfiguriert		
Active Directory-Registrierungsrichtlini	9	
Yon Ihnen konfiguriert		Neue hinzufüge
	\searrow	

Request Certificates	of certificates. Select the certificates you want to reques	st. and then dick Enroll.
Active Directory Enrollm	ent Policy	
Computer	i STATUS: Available	Details 🛞
Web Server	$\dot{\psi}$ STATUS: Available uired to enroll for this certificate. Click here to configure s	Details®
Show all templates		

Common Name und SAN angeben

Certificat	e Proper	ties				×
General	Subject	Extensions	Private Key	Certification	Authority	
The subj enter infi in a certi Subject o The user	ect of a ce ormation a ficate. of certifica or compu	ertificate is the bout the type te ter that is reco	e user or comp es of subject r eiving the cer	buter to which hame and altern tificate	the certificate is issued native name values tha	. You can It can be used
Subject r	name:				CN=UAG.TRAINER	.DE
Commo	n name	•]	Add >		
Value:			<	Remove		
Alternati	ve name:					
Type:		_	1		UAG.TRAINER.DE	
IDNS		•	1			
				Add >		
			<	Remove		
Learn mo	re about s	subject name				
				ОК	Cancel	Apply



Private Key Exportable

Certificate Properties	×
🔥 Subject General Extensions Private Key Certification Authority	
Cryptographic Service Provider	۲
Key options Set the key length and export options for the private key. Key size: 2048	®
 Make private key exportable Allow private key to be archived 	
Strong private key protection	
Кеу туре	۲
Key permissions	۲
Learn more about <u>private key</u>	
OK Cancel	Apply

e Certificate Enrollment		
💂 Certificate Enrollment		
Certificate Installation Results	;	
The following certificates have beer	n enrolled and installed on this computer.	
Active Directory Enrollm	ent Policy	
Web Server	STATUS: Succeeded	Details®
		Finish

Eigenschaften

Certificate	×
General Details Certification Path	1
	<u> </u>
Show: <all></all>	•
Field	Value
Valid from	Montag, 31. Mai 2010 20:51:26
Valid to	Mittwoch, 30. Mai 2012 20:51:26
Subject	UAG.TRAINER.DE
Public key	RSA (2048 Bits)
Certificate Template Name	WebServer
Enhanced Key Usage	Server Authentication (1.3.6
🛐 Subject Key Identifier	ca 21 57 3b 63 e0 3b 48 59 37
Subject Alternative Name	DNS Name=UAG.TRAINER.DE
DNS Name=UAG.TRAINER.DE	
E	dit Properties Copy to File
Learn more about certificate details	
	ОК

ISATAP Host Eintrag erstellen

Eigenschaften von ISATAP	? ×
Host (A) Sicherheit	
Host (bei Nichtangabe wird übergeordnete Domäne verwendet):	
ISATAP	
Vollqualifizierter Domänenname:	
ISATAP.trainer.intem	
IP-Adresse:	
10.80.16.79	
🕅 Entsprechenden Zeigereintrag (PTR) aktualisieren	
Eintrag löschen, sobald er verfällt	
Zeitstempel des Eintrags:	
Gültinkeitedauer (TTL): 0 :1 :0 :0 (TTTTT-HH MM	ss)
	55)
OK Abbrechen Übern	ehmen

ISATAP aus der DNS GlobalQueryBlocklist entfernen



DirectAccess einrichten

AD Gruppe fuer den DA Zugriff angeben

UAG DirectAccess Client Configuration	×
UAG DirectAccess Client Configuration	
Select the security groups of client computers that will be enabled for UAG DirectAccess configuration.	
Add Remove	
Learn more Finish	Cancel

Interne IP v4 Adresse angeben und erste oeffentliche Ipv4 IP

a UAG DirectAccess Server Config	uration	×	
UAG DirectAcces	s Server Configuration		
Connectivity Managing DirectAccess Services Authentication Options	To set up the UAG DirectAccess server, assign IP addresses to the Internet-facing and internal networks.		
	Internet-facing	Internal	
	First Internet-facing IPv4 address:	Internal IPv4 address used when ISATAP is deployed on the UAG DirectAccess server:	
	212.212.10.2	10.80.16.79	
	Second Internet-facing IPv4 address: 212.212.10.3	Internal IPv6 address:	
	ISATAP IPv6 transition technologies will be DNS name "ISATAP" with "10.80.16.79" on th these domains. In addition ensure that ISAT DNS servers.	enabled on the UAG DirectAccess server. Register the E DNS in all domains to enable IPv6 connectivity on AP is not blocked in the <u>Global Query Block List</u> on all	
Learn more		< Back Next > Finish Cancel	

arver Configuration of the server and the server an	juration X
UAG DirectAcces	s Server Configuration
Connectivity Managing DirectAccess Services Authentication Options	NAT64 and DNS64 enable DirectAccess clients to access IPv4-only resources, and are required by UAG DirectAccess. You can use either the UAG DirectAccess NAT64 and DNS64, or deploy external NAT64 and DNS64. Select whether to use UAG DirectAccess NAT64 and DNS64: If Enable UAG DirectAccess NAT64 Enable UAG DirectAccess DNS64
Learn more	< Back Next > Finish Cancel

Root CA Certificate angeben

Das IP-HTTPS Zertifikat angeben. Ein Computerzertifikat muss ebenfalls vorhanden sein und auf den CN des internen FQDN des DA Server ausgestellt sein

au UAG DirectAccess Server Config	uration	X
UAG DirectAccess	s Server Configuration	
Connectivity Managing DirectAccess Services Authentication Options	UAG DirectAccess uses certificates to help secure the connection between remote clients and the internal network. Browse and select a root or intermediate certificate that verifies certificates sent by DirectAccess clients. CUSE root certificate DC=intern, DC=trainer, CN=RootCA Browse_ Select the certificate that authenticates the UAG DirectAccess server to a client connecting using IP-HTTPS. CN=UAG.TRAINER.DE Browse_ To The IP-HTTPS certificate should be copied to all members of a UAG DirectAccess array. Edit IPSec corptography settings Accept connections only from: Computers that log on using a PKI smart card Computers that comply withyour organization's NAP policy.	
Learn more	< Back Next > Finish	Cancel

FQDN des internen NLS Server angeben

💐 Infrastructure Server Configura	ition	X
Infrastructure Ser	ver Configuration	
Network Location Server DNS Suffixes Management Servers and DCs	An internal network location server helps a client computer to determine whether it is connected to the Internet or to the internal network.	
	Enter the HTTPS URL of the network location server. https:// trainer-dc.trainer.intern/ Validate Example: insideoutside.corp.contoso.com	
	It is recommended that you use a high availability network location server. If the HTTPS URL is unavailable, client connectivity may be disrupted.	
	Validation successful. The URL https://trainer-dc.trainer.intern/ is reachable.	
Learn more	< Back Next > Finish	Cancel

Interne DNS Namensraeume angeben

ar Infrastructure Server Configura	ation			X
Infrastructure Ser	ver C	onfiguration		
Network Location Server				
DNS Suffixes	Enter	the name suffixes and IP addresses o	f internal DNS servers used to resolve DNS suffix queries.	
Management Servers and DCs		Name Suffix	IP address of DNS Server	
Frankgement Servers and Ses		*.trainer.intern	[DNS64]	
		trainer-dc.trainer.intern	[Excluded]	
	*	Double-click here to add		
	Select	a local name resolution option:		
	00	nly use local name resolution if the n	ame does not exist in DNS (most restrictive)	
	€ Ea ur	II back to local name resolution if th areachable when the client computer	e name does not exist in DNS or the DNS servers are is on a private network (recommended)	
	⊙ Fa	JI back to local name resolution for a	any kind of DNS resolution error (least secure)	
Learn more			< <u>B</u> ack <u>N</u> ext > <u>F</u> inish	Cancel

Infrastruktur Server Zusammenfassung

aria Infrastructure Server Configura	tion	×
Infrastructure Ser	ver Configuration	
Network Location Server DNS Suffixes Management Servers and DCs	List all internal servers that are required to manage and authenticate DirectAccess clients.	
	C Discoverable groups were last refreshed on Sunday, April 25, 2010 6:43 PM.	
Learn more	< Back Next > Finish Cancel	

End to Egde Aut. Und Verschluesselung

Application Server Configuration	×
Application Server Configuration	
By default, traffic between DirectAccess clients and the UAG DirectAccess server You can also enable authentication and encryption between clients and specifie	r is authenticated and encrypted (end-to-edge). ed applications servers (end-to-end).
Select an authentication and encryption model: Require end-to-edge authentication and encryption Require end-to-end authentication and encryption to specified applications Edit IPSec cryptography settings Select the security groups that contain the servers that require end-to-end authentication	hentication and Add Remove
Learn more_	Finish Cancel

Zusammenfassung der Konfiguration



Policy wird erstellt

DirectAccess Policy Configuration
Policy Configuration Log:
done. Executing Activate Windows Firewall public profile
Executing Activate Windows Firewall private profile done.
Executing Set the ICMP exemption done.
Executing Set MainMode Phase1CryptoSet(mmkeylifetime) done.
Executing Set MainMode Phase1CryptoSet(mmsecmethods) done.
done.
done. Executing Set UAG DirectAccess Gateway - Clients Access Enabling Humler
done. Executing Export local policy to file
done. Executing Import from export-file to domain gpo=trainer.intern\UAG Dire
OK Cancel

Powershell Skript

<pre>File Edit Format View Help # UAGDA Group Policy Configuration Script. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Generated on Monday, 31 May 2010 19:24 UTC. # Runtime variables Param(parameter (Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera parameter (Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera for an static variables # Static variables f (-not \$[UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}] { \$[UAGDA_ACCESS_ENABLING_ADDRESSES_ALL]="2" if (-not \$[UAGDA_CERT_TMPE]) { \$[UAGDA_CERT_TMPE]] { \$[UAGDA_CERT_TMPE]] { \$[UAGDA_CERT_TMPE]] { \$[UAGDA_CERT_TMPE]] { \$[UAGDA_CERT_TMPE]] { \$[UAGDA_DTE_ACCESS]="2002:d4d4:a03"; f (-not \$[UAGDA_DTE_ACCESS]] { \$[UAGDA_DTE_ACCESS]="2002:d4d4:a02"; d1 (-not \$[UAGDA_DTE_CORP]] { \$[UAGDA_DTE_ACCESS]="2002:d4d4:a02"; d1 (-not \$[UAGDA_IPHTTPS_URL]] { \$[UAGDA_DTE_CORP]="2002:d4d4:a02"; d1 (-not \$[UAGDA_IPHTTPS_URL]] { \$[UAGDA_IPTTPS_URL]="https://lreIIME]="fomin, osess"; f (-not \$[UAGDA_IPHEC_M_SECMETHODS]] { \$[UAGDA_IPSEC_MM_SECMETHODS]="esp:shal26-noi f (-not \$[UAGDA_IPSEC_MM_SECMETHODS]] { \$[UAGDA_IPSEC_MM_SECMETHODS]="esp:shal26-noi f (-not \$[UAGDA_NESI_IDNSPROBECONTENT]] { \$[UAGDA_IPSEC_MM_SECMETHODS]="esp:shal26-noi f (-not \$[UAGDA_NESI_IDNSPROBECONTENT]] { \$[UAGDA_NESI_IDNSPROBECONTENT]="::::::::::::::::::::::::::::::::::::</pre>	UAGDirectAccess_GroupPolicy.ps1 - Notepad	_ 🗆 ×
<pre># UAGDA Group Policy Configuration script. # Generated on Monday, 31 May 2010 19:24 UTC. # Generator Version 4.0.0.0 # Runtime variables Param([parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera [parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera } static variables if (-not \${UAGDA_CCERT_MACHINE_AUTH}) { \${UAGDA_CCESS_ENABLING_ADDRESSES_ALL}="2' (-not \${UAGDA_CCERT_MACHINE_AUTH}) { \${UAGDA_CCERT_MACHINE_AUTH}="Dc=intern, DC=trainer, CN if (-not \${UAGDA_CCERT_MACHINE_AUTH}) { \${UAGDA_CCERT_MACHINE_AUTH}="CD_intern, DC=trainer, CN if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CTE_TONC}" } if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CTE_TONC}" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_CTE_TONC}" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_DTE_ACCESS}="2002:d4d4:a03::d4d4:a03" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_DTE_ACCESS}="2002:d4d4:a02::d4d4:a03" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_DTE_ACCESS}="2002:d4d4:a02::d4d4:a03" } if (-not \${UAGDA_IPSEC_EZE_QM_SECMETHODS}) { \${UAGDA_IPSEC_MM_YPUBLIC_IP}="212.212.10.2" } if (-not \${UAGDA_IPSEC_EQM_SECMETHODS}) { \${UAGDA_IPSEC_MM_YPUBLIC_IP}="212.212.10.2" } if (-not \${UAGDA_IPSEC_EMM_SECMETHODS}) { \${UAGDA_IPSEC_MM_YPUBLIC_IP}="212.212.10.2" } if (-not \${UAGDA_IPSEC_MM_KEYLIFETIME}} { \${UAGDA_IPSEC_MM_SECMETHODS}="dmgroup2:aes128-sha25} if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="dmgroup2:aes128-sha25} if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_IPSEC_MM_SECMETHODS}="dmgroup2:aes128-sha25} if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_IPSEC_MM_SECMETHODS}="dmgroup2:aes128-sha25} if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_IPSEC_MM_SECMETHODS}="dmgroup2:aes128-sha25} if (-not \${UAGDA_ND_ND_NDRNOBECONTENT}) { \${UAGDA_NCSI_DNSPROBEDCSTNTT}=":::1" } if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_NCSI_DNSPROBEDCST="=2002:d4d4:a02:8000::::49,2i (-not \${UAGDA_ND_UCV_APPSERV}) { \${UAGDA_ND_UCV_APPSERV}=MAG DirectAccess: cherconscripte</pre>	File Edit Format View Help	
<pre># Runtime variables Param([parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera [parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(sepera) # Static variables if (-not \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}) { \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}="2' if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CERT_MACHINE_AUTH}="DC=intern, DC=trainer, CN if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CERT_TYPE}="root" } if (-not \${UAGDA_DTE_ACCESS}} { \${UAGDA_DTE_ACCESS}="2'002:ddd4:a03::ddd4:a03" } if (-not \${UAGDA_DTE_ACCESS}} { \${UAGDA_DTE_ACCESS}="2'002:ddd4:a02::ddd4:a03" } if (-not \${UAGDA_DTE_CORP}) { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::ddd4:a03" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::ddd4:a03" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::ddd4:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::ddd4:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::dd4:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:ddd4:a02::dd4:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'02:dd44:a02:" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'002:dd44:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'02:dd44:a02" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'02:dd44:a02:" } if (-not \${UAGDA_DTE_CORP}] { \${UAGDA_DTE_CORP}="2'02:dd44:a02" } if (-not \${UAGDA_DTESC_MM_KEYLIFETIME}] { \${UAGDA_DTESC_MM_SECMETHODS}="2'02:dd44:a02" } if (-not \${UAGDA_DTESC_MM_SECMETHODS}] { \${UAGDA_DTESC_MM_SECMETHODS}="2'02:dd44:a02:" } if (-not \${UAGDA_NCSI_DNSPROBECONTENT}] { \${UAGDA_NCSI_DNSPROBEONTENT}="::1" } if (-not \${UAGDA_NCSI_DNSPROBECMOTTENT}] { \${UAGDA_NCSI_DNSPROBEONTNT="1" } if (-not \${UAGDA_NCSI_DNSPROBECMOTTENT}] { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess: corpConnee if (-not \${UAGDA_NCSI_DNSPROBEHOST}] { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess: corpConnee if (-not \${UAGDA_NCSI_DNSPROBEHOST}] { \${UAGDA_NID_ADDRESS}="2002:dd44:</pre>	<pre># UAGDA Group Policy Configuration Script. # Generated on Monday, 31 May 2010 19:24 UTC. # Generator Version 4.0.0.0</pre>	▲ _
<pre>[parameter(Mandatory=SFalse, ValueFromPipeline=Strue, HelpMessage="Additional domains(sepera [parameter(Mandatory=SFalse, ValueFromPipeline=Strue, HelpMessage="Additional domains(sepera # Static variables if (-not \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}) { \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}="20 if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CERT_MACHINE_AUTH}="DC=intern, DC=trainer, CN- if (-not \${UAGDA_CENTTONS_FALLBACK}) { \${UAGDA_CERT_MACHINE_AUTH}="DC=intern, DC=trainer, CN- if (-not \${UAGDA_CLIENTDNS_FALLBACK}) { \${UAGDA_CERT_TYPE}="root" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_CERT_TYPE}="2002:ddd4:a03::dd4d:a03" } if (-not \${UAGDA_DTE_CORP}) { \${UAGDA_DTE_CORP}="2002:dd4d:a02::dd4d:a02" } if (-not \${UAGDA_DTE_CORP}) { \${UAGDA_DTE_CORP}="2002:dd4d:a02::dd4d:a02" } if (-not \${UAGDA_GATEWAY_PUBLIC_IP}} { \${UAGDA_GATEWAY_PUBLIC_IP}="212.212.10.2" } if (-not \${UAGDA_TPSEC_E2E_QM_SECMETHODS}) { \${UAGDA_IPFTFS_URL}="https://uag.trainer.de:443/IPHTTPS" } if (-not \${UAGDA_IPSEC_E2E_QM_SECMETHODS}) { \${UAGDA_IPSEC_MM_KEYLIFETIME}="60min,0sess" } if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="dhgroup2:aes128-sha25 if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_NCSI_DNSPROBECONTENT}="::1" } if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess-corpConne if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess: corpConne if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_NCI_SI_STTEPREFIXES}"2002:dd4d:a02:8000::/49,20 if (-not \${UAGDA_NCI_APPSER}) { \${UAGDA_NCI_SI_STTEPREFIXES}"2002:dd4d:a02:8000::/49,20 if (-not \${UAGDA_ND_URL}) { \${UAGDA_NDLURL}="https://trainer-dc.trainer.intern/" } if (-not \${UAGDA_NDLURL}) { \${UAGDA_NDLURL}="https://trainer-dc.trainer.intern/" } if (-not \${UAGDA_POLICY_CIIENT}) { \${UAGDA_POLICY_APPSERY}="UAG DirectAccess: Daserver{f7b} if (-not \${UAGDA_POLICY_GATEWAY}) { \${UAGDA_POLICY_APPSERY}="UAG DirectAccess: Daserver{f7b} if (-not \${UAGDA_POLICY_GATEWAY}) { \${UAGDA_POLICY_APPSERY}="UAG DirectAcce</pre>	# Runtime variables Param(
<pre># static variables if (-not \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}) { \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}="2" if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CERT_MACHINE_AUTH}="DC=intern, DC=trainer, CN if (-not \${UAGDA_CERT_TYPE}) { \${UAGDA_CERT_TYPE}="root" } if (-not \${UAGDA_CLENTDNS_FALLBACK}) { \${UAGDA_CERT_TYPE}="root" } if (-not \${UAGDA_DTE_ACCESS}] { \${UAGDA_DTE_ACCESS}="2002:ddd4:a03::ddd4:a03" } if (-not \${UAGDA_DTE_CORP}) { \${UAGDA_DTE_CCRP}="2002:ddd4:a02::ddd4:a02" } if (-not \${UAGDA_IPHTPS_URL}) { \${UAGDA_DTE_CORP}="2002:ddd4:a02::ddd4:a02" } if (-not \${UAGDA_IPHTPS_URL}) { \${UAGDA_IPTEYS_URL}="https://uag.trainer.de:443/IPHTTPS" } if (-not \${UAGDA_IPSEC_E2E_QM_SECMETHODS}) { \${UAGDA_IPSEC_E2E_QM_SECMETHODS}="esp:sha256-noi if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="esp:sha256-noi if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="esp:sha256-noi if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="esp:sha1-aes192+60min- if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_SECMETHODS}="esp:sha1-aes192+60min- if (-not \${UAGDA_NCSI_DNSPROBECONTENT}) { \${UAGDA_NCSI_DNSPROBENOST}="UAGDirectAccess-corpConne- if (-not \${UAGDA_NCSI_DNSPROBENOST}) { \${UAGDA_NID_ADDRESS}="2002:ddd4:a02:8000::/49,20 if (-not \${UAGDA_NID_ADDRESS}} { \${UAGDA_NID_ADDRESS}="2002:ddd4:a02:8000::/49,20 if (-not \${UAGDA_NID_ADDRESS}} { \${UAGDA_NID_ADDRESS}="UAGD irectAccess: corpConne- if (-not \${UAGDA_NID_URL}) { \${UAGDA_NID_URL}="https://trainer-dc.trainer.intern/" } if (-not \${UAGDA_POLICY_APPSERV}) { \${UAGDA_POLICY_APPSERV}="UAG DirectAccess: corpServer[f7b] if (-not \${UAGDA_POLICY_CATEWAY}) { \${UAGDA_POLICY_APPSERV}="UAG DirectAccess: Daserver[ab99] if (-not \${UAGDA_PREFIX_CORP_EXCLUSION}} { \${UAGDA_PREFIX_CORP_EXCLUSION}="::-2002:ddd4:a02:8100 if (-not \${UAGDA_PREFIX_CORP}} { \${UAGDA_PREFIX_CORP}="UAGD DirectAccess: Daserver[ab99] if (-not \${UAGDA_PREFIX_CORP}} { \${UAGDA_PREFIX_ORP}="UAGD DirectAccess: Daserver[ab99] if (-not \${UAGDA_PREFIX_CORP}}</pre>	parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains([parameter(Mandatory=\$False, ValueFromPipeline=\$true, HelpMessage="Additional domains(}	sepera sepera
	<pre># Static variables if (-not \${UAGDA_ACCESS_ENABLING_ADDRESSES_ALL}) { \${UAGDA_ACCESS_ENABLING_ADDRESSES_/ if (-not \${UAGDA_CERT_MACHINE_AUTH}) { \${UAGDA_CERT_MACHINE_AUTH}="DC=intern, DC=train if (-not \${UAGDA_CERT_TYPE}) { \${UAGDA_CERT_TYPE}="root" } if (-not \${UAGDA_CLIENTDNS_FALLBACK}) { \${UAGDA_CLIENTDNS_FALLBACK}="2" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_DTE_ACCESS}="2002:d4d4:a03::d4d4:a03" } if (-not \${UAGDA_DTE_ACCESS}) { \${UAGDA_DTE_CORP}="2002:d4d4:a02::d4d4:a03" } if (-not \${UAGDA_GATEWAY_PUBLIC_IP}) { \${UAGDA_DTE_CORP}="2002:d4d4:a02::d4d4:a03" } if (-not \${UAGDA_IPHTTPS_URL}) { \${UAGDA_IPHTTPS_URL}="Inttps://uag.trainer.de:443/IPH1 if (-not \${UAGDA_IPSEC_E2E_QM_SECMETHODS}) { \${UAGDA_IPSEC_MM_KEYLIFETIME}="60min_0ses" if (-not \${UAGDA_IPSEC_MM_KEYLIFETIME}} { \${UAGDA_IPSEC_MM_KEYLIFETIME}="60min_0ses" if (-not \${UAGDA_IPSEC_MM_SECMETHODS}) { \${UAGDA_IPSEC_MM_KEYLIFETIME}="60min_0ses" if (-not \${UAGDA_NCSI_DNSPROBECONTENT}} { \${UAGDA_NCSI_DNSPROBECONTENT}="::1" } if (-not \${UAGDA_NCSI_DNSPROBEHOST}) { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess-con if (-not \${UAGDA_NCSI_DNSPROBEHOST}) { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDirectAccess: CAPSEN' if (-not \${UAGDA_NCSI_DNSPROBEHOST}) { \${UAGDA_NCSI_DNSPROBEHOST}="UAGDIrectAccess: CAPSEN' if (-not \${UAGDA_NID_ADDRESS} { \${UAGDA_NID_ADDRESS}="2002:d4d4:a02:8000::5efe:10.80 if (-not \${UAGDA_NID_ADDRESS} { \${UAGDA_NID_ADDRESS}="2002:d4d4:a02:8000::5efe:10.80 if (-not \${UAGDA_NID_URL}) { \${UAGDA_NID_URL}="https://trainer-dc.trainer.intern/" } if (-not \${UAGDA_NID_URL}) { \${UAGDA_POLICY_CATEWAY}="UAG DirectAccess: CAPSEN' if (-not \${UAGDA_POLICY_CATEWAY}} { \${UAGDA_POLICY_CATEWAY}="UAG DirectAccess: CAPSEN' if (-not \${UAGDA_PREFIX_CORP_EXCLUSION} { \${UAGDA_PREFIX_CORP_EXCLUSION}="::-2002:d4d4: if (-not \${UAGDA_PREFIX_CORP_EXCLUSION} { \${UAGDA_PREFIX_CORP_EXCLUSIN}="::-2002:d4d4:a02: if (-not \${UAGDA_PREFIX_CORP}} { \${UAGDA_PREFIX_CORP_EXCLUSIN}="::-2002:d4d4:a02: if (-not \${UAGDA_PREFIX_CORP}] { \${UAGDA_PREFIX_CORP}="2002:d4d4:a02:8000::/49" } if (-not \${</pre>	TPS" } 1256-noi }-sha25i 2-60min pConnei :/49,2i).16.80 /er {f7b 91980e er {ab99 14:a02: a02:810i p,DC=ii ,DC=ii

Konfiguration aktivieren

🗘 Activate Configuration	×
Activate Configuration	
You must activate the configuration to apply your changes. If you select to back up the configuration, current settings (prior to activation) will be saved.	
Reack up configuration before performing this activation	
Activation might take several minutes.	
Ensure that the group policy has been updated on all of the array nodes	
Activate > Cancel	

Sperrlisten Verteilungspunkt und AIA Verteilungspunkt Publishing entfernen

Eigenschaften von RootCA
Speicherung Zertifikatverwaltungen Registrierungs-Agents Überwachung Wiederherstellungs-Agents Sicherheit Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen
Erweiten ug daswanien: Sperfisten-Verteilungspunkt Geben Sie Ständorte um von das Dander eine Zerunkarsperfiste erhalten können.
C:Windows\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix> dap:///CN<<catruncatedname><crlnamesuffix>,CN<<servershortnar http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><deltac< td=""></deltac<></crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname></crlnamesuffix></caname>
Hinzufügen Entfernen
In alle Sperifisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll
In Sperifisten einbeziehen. Wird z. Suche von Deltasperifisten verwender In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Etasperifisten an diesem Ott veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen
OK Abbrechen Übernehmen Hilfe

IP Konfiguration pruefen

Administrator: Command Prompt <u> – – ×</u> Tunnel adapter 6T04 Adapter: ٠ Connection-specific DNS Suffix Microsoft 6to4 Adapter 00-00-00-00-00-00-00-E0
 DNS Servers
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 :
 <th Tunnel adapter Teredo Tunneling Pseudo-Interface: Connection-specific DNS Suffix Microsoft Teredo Tunneling Adapter 00-00-00-00-00-00-00-E0 -No Yes fe80::8000:f227:2b2b:f5fd%27(Preferred) : Disabled Tunnel adapter isatap.trainer.intern: . : trainer.intern . : Microsoft ISATAP Adapter . : 00-00-00-00-00-00-00-E0 Connection-specific DNS Suffix 2002:d4d4:a02:8000:0:5efe:10.80.16.79(Pre ferred) NetBIOS over Tcpip. : Disabled Tunnel adapter isatap.{655D76D0-5179-4B8C-9234-28C27947E5FC}: Connection-specific DNS Suffix Microsoft ISATAP Adapter #2 00-00-00-00-00-00-00-E0 No Yes : fe80::200:5efe:212.212.10.2%29(Preferred) Link-local IPv6 Address : fe80::200:5efe:212.212.10.3%29(Preferred) Default Gateway fec0:0:0:ffff::1×1 fec0:0:0:ffff::2×1 fec0:0:0:ffff::3×1 DNS Servers NetBIOS over Topip. Disabled

DNS Eintraege pruefen

🊊 DNS-Manager					
Datei Aktion Ansicht ?					
🗢 🔿 🗡 📅 🔀 🖬 😣	🛛 🖬 🕴 🗐 🛍				
DNS	Name 🔺	Тур	Daten	Zeitstempel	
TRAINER-DC	(identisch mit übergeordnetem Ordner)	Autoritätsursprung (SOA)	[135], trainer-dc.trainer.int	Static	
🕀 🚞 Zwischengespeicherte Look	(identisch mit übergeordnetem Ordner)	Namenserver (NS)	trainer-dc.trainer.intern.	Static	
E Forward-Lookupzonen	🗐 (identisch mit übergeordnetem Ordner)	Host (A)	10.80.16.80	31.05.2010 07:00:00	
	(identisch mit übergeordnetem Ordner)	IPv6 Host (AAAA)	2002:d4d4:0a02:8000:0000	31.05.2010 22:00:00	
	📳 _msdcs				
🖽 📴 _msacs	🚞 _sites				
E sites	🚊 _tcp				
	🚞 _udp				
DomainDnsZones	DomainDnsZones				
ForestDnsZones	ForestDnsZones				
\pm 🧮 marcimarc	ISATAP	Host (A)	10.80.16.79	Static	
🛨 🧮 Reverse-Lookupzonen	i marcimarc				
🕀 📔 Bedingte Weiterleitungen	trainer-dc	Host (A)	10.80.16.80	Static	
표 💼 Globale Protokolle	UAG	Host (A)	10.80.16.79	31.05.2010 21:00:00	
	UAG	IPv6 Host (AAAA)	2002:d4d4:0a02:8000:0000	31.05.2010 21:00:00	
	UAGDirectAccess-corpConnectivityHost	IPv6 Host (AAAA)	0000:0000:0000:0000:0000	31.05.2010 21:00:00	
	win7Client	IPv6 Host (AAAA)	2002:c009:c82d:0000:0000	14.05.2010 11:00:00	
	1				

Group Polices

🛃 Gruppenrichtlinienverwaltung				_ 8
🔣 Datei Aktion Ansicht Fenster ?				_ 8
🗢 🔿 🔁 🖬 🗎 🙆 📔 🖬				
Image: Standard States Gesamstruktur: trainer.intern Image: Standard States Default Domain Policy Image: Standard States Image: Standard States Image: Standard States Concentration States Image: Standard States Image: Standard States Image: Standard	Gruppenrichtlinienobjekte in Inhalt Delegierung	trainer.intern	WMI-Filter Keine Keine Keine Keine	Geändert 25.04.201 13.02.201 31.05.201 31.05.201 31.05.201



Client

Computer Zertifikat anfordern



Ausgestellt auf den internen FQDN

🚡 Konsole1 - [Konsolenstan	nm\Zertifikate (Lokaler Computer)\Eig	ene Zertifikate\Zertifikate]		- • •
🚟 Datei Aktion Ansich	t Favoriten Fenster ?			_ 8 ×
🗢 🄿 🖄 🖬 🔏 🐁	🗙 🗉 😖 👔 🗊			
Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablau	Aktionen
Zertifikate (Lokaler C)	🙀 win7Client.trainer.intern	RootCA	31.05.	Zertifikate 🔺
Eigene Zertifikat				Weitere Aktionen 🕨
Vertrauenswürdi				win7Client.trainer.in 🔺
 Organisationsve Zwischenzertifizi 				Weitere Aktionen 🕨
Vertrauenswürdi				
Nicht vertrauens				
Drittanbieter-Sta				
Vertrauenswurdt				
Smartcard vertra				
4	< III		P.	
Der Speicher "Eigene Zertifika	te" enthält 1 Zertifikat.			

HOSTS Datei fuer Demoumgebung auf dem Windows 7 Ultimate oder EE Client patchen



Test



Success



NRPT pruefen



Win7 Client DNS Konfig

🖁 DNS-Manager							
Datei Aktion Ansicht ?							
🗢 🔿 🙋 📅 🔀 🖬 🙆							
DNS	Name 🔺	Тур	Daten	Zeitstempel			
 DNS TRAINER-DC Zwischengespeicherte Look Forward-Lookupzonen geneticstrainer.intern geneticstrai	Name (dentisch mit übergeordnetem Ordner) (identisch mit übergeordnetem Ordnetem O	Typ Autoritätsursprung (SOA) Namenserver (NS) Host (A) IPv6 Host (AAAA) Host (A) IPv6 Host (AAAA) Host (A) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	Daten [139], trainer-dc. trainer.int trainer-dc. trainer.intern. 10.80.16.80 2002:d4d4:0a02:8000:0000 10.80.16.79 10.80.16.80 2002:d4d4:0a02:8000:0000 10.80.16.79 20.80.16.79 2002:d4d4:0a02:8000:0000 10.80.16.79	Zeitstempel Static Static 31.05.2010 07:00:00 31.05.2010 22:00:00 Static Static Static Static 31.05.2010 21:00:00 31.05.2010 21:00:00 31.05.2010 21:00:00			
	win7Client win7Client	IPv6 Host (AAAA) IPv6 Host (AAAA)	2001:0000:d4d4:0a02:2897 2002:d4d4:0a51:0000:0000	31.05.2010 22:00:00 31.05.2010 22:00:00			

Logging auf TMG Seite beim Client Verbindungsaufbau

31.05.2010 22:54:41	212.212.10.81	212.212.10.3	0	IPv6 Over IPv4 T Initiate	
				_	
•					
Initiated Connection				UAG 31.05.2010 22:54:4	
Log type: Firewall serv	ice				
Status: The operation completed successfully.					
Rule: [System] Direct Access mode: Allow IPv6 transition technologies traffic to Local Host					
Source: External (212.	212.10.81)				
Destination: Local Hos	st (212.212.10.3)				
Protocol: IPv6 Over IP	v4 Tunnel				
Additional information	1				