# Migration Forefront Client Security (FCS) zu Forefront Endpoint Protection 2010 (FEP)

IST Zustand:

- 1 FCS Server mit WSUS und MOM
- 1 SQL Server 2005 fuer die FCS/MOM Datenbanken

SOLL Zustand:

- 1 FEP Server mit WSUS und SCCM
- 1 SQL Server 2008 fuer die FEP/SCCM Datenbanken

Offizielle Anleitung zur Migration von FCS zu FEP: <u>http://technet.microsoft.com/en-us/library/gg477033.aspx</u> Weitere Informationen zu FEP: <u>http://www.it-training-grote.de/download/FEP2010.pdf</u>

### Windows Server Installation / Konfiguration

Windows Server 2008 R2 installieren / patchen / Hardware und System requirements fuer FEP: <u>http://www.microsoft.com/forefront/endpoint-protection/en/us/system-requirements.aspx</u>

### WSUS installieren

hlen	
Wähen Sie für die Installation auf dem Server eine oder mehrere Roll         tolen:         Active Directory Lightweight Directory Services         Active Directory-Pomänendienste         Active Directory-Webundlienste         Active Directory-Vebundlienste         Active Directory-Vebundlienste         Active Directory-Vebundlienste         Active Directory-Vebundlienste         Dateidienste         Dateidienste         Directory und Dokumentdienste         Fasserver         Diruck- und Dokumentdienste         Remotedesktopdienste         Webserver (II5)         Windows-Bereitstellungsdienste         Weitere Informationen zu Serverrollen         Veitere Informationen zu Serverrollen	en aus. Beschreibung: Mit Windows Server Ubdate Services (WSUS) Konnen Netzwerkadministratoren die zu installierenden Microsoft-Updates angeben, separates Gruppen von Computern für verschiedene Sätze von Updates erstellen und Berichte über die Kompatibilitätsstufen der Computer nut über die zu installierenden Updates abrufen.
	Wahlen Sie für die Installation auf dem Server eine oder mehrere Roll         Kollen:         Active Directory-Uightweight Directory Services         Active Directory-Rochteverwalkungsdienste         Active Directory-Rochteverwalkungsdienste         Active Directory-Zertifikatdienste         Active Directory-Zertifikatdienste         Active Directory-Zertifikatdienste         DHCP-Server         DHCS-Server         Hyper-V         Netwerkrichtlinien- und Zugriffsdienste         Remotedesktopdienste         Webserver (115)         Windows-Bereitstellungsdienste         Wetere Informationen zu Serverrollen         Vettere Informationen zu Serverrollen         Zurück       Weiter

WSUS nach Vorgaben konfigurieren

Produkte und Klassifizierungen auswaehlen

Produkte und Klassifizierungen 🛛 🛛 🗙
Produkte Klassifizierungen
Sie können die Produkte angeben, deren Updates synchronisiert werden sollen.
Produkte:
Expression Media V1     Expression Web 3     Forefront     Forefront Client Security     Forefront code named Stirling Beta version     Forefront Endpoint Protection 2010     Forefront Protection Category     Forefront Server Security Category     Forefront Threat Management Gateway, Definition U     Forefront TMG     Forefront TMG     Threat Management Gateway Definition Updates for     HPC Park
Alle Produkte, einschließlich künftig hinzugefügter Produkte.
OK Abbrechen Übernehmen

Automatische Genehmigungen konfigurieren

Automatische Genehmigungen	×
Updateregeln Erweitert	
Sie können Regeln festlegen, um neue Updates automatisch zu Gog genehmigen, wenn sie synchronisiert werden.	
Neue Regel Bearbeiten 🗙 Löschen Regel ausführen	
Regeleigenschaften (zur Bearbeitung auf die unterstrichenen Werte klicken)	
Update für <b>Example</b> genehmigen	
OK Abbrechen Übernehmen	

Datenbank auf den zentralen SQL Server Cluster legen

WSUS Migration (wenn der FCS Server auch WSUS Server war) http://www.it-training-grote.de/download/WSUS3migration.pdf

### **SCCM** Installation

Vor der Installation das Computerkonto des SCCM Servers in die lokale Gruppe der Aministratoren auf dem MS SQL Server aufgenommen werden

OK, der ein oder andere Fehler

icrosoft System Center Configuration Manag	jer 2007 <b>S</b> P2		
Prüfung der Voraussetzungen für die Install	ation		
Es wird überprüft, ob Installationsprobleme verligge		workspidan and words	an datailliarta
Informationen angezeigt, wie die Probleme gelöst w	erden können.	vornanden sind, werde	en decamerce
Ergebnis der Voraussetzungsprüfung:			
Voraussetzung	Status	System	Standorttyp 🔺
1 Schemaerweiterungen	Warnung		Primärer Standort
🐼 Microsoft Remote Differential Compression-Bi	. Fehler		Primärer Standort
🛕 SQL Server-Sicherheitsmodus	Warnung	SKYLLUND	SQL Server
🔕 BITS installiert	Fehler		Verwaltungspunkl
🔕 BITS aktiviert	Fehler		Verwaltungspunki
🔕 WebDAV ist installiert.	Fehler		Verwaltungspunki 🖕
· · · ·			
Die Voraussetzungsprüfung wurde abgeschlossen.			
5QL Server-Sicherheitsmodus			
Der angegebene SQL Server-Name ist für die SQL-	Authentifizierung:	sicherheit konfiguriert. I	Es wird empfohlen, SQL
Configuration Manager-Setup fortsetzen.	ows-Auchendinzien	ungssicherneit umzukohr	nguneren, bevor bie das
Aktuellste Voraussetzungsinformationen anzeigen			Pröfung durchföhren
		Installation starten	Abbrechen

#### Besser

Microsoft System Center Configuration Mana	ger 2007 SP2		×	
Prüfung der Voraussetzungen für die Installation Es wird überprüft, ob Installationsprobleme vorliegen. Wenn Probleme vorhanden sind, werden detaillierte Informationen angezeigt, wie die Probleme gelöst werden können.				
Ergebnis der Voraussetzungsprüfung:				
Voraussetzung	Status	System	Standorttyp	
⚠ Schemaerweiterungen ⚠ SQL Server-Sicherheitsmodus	Warnung Warnung	salition Gillion	Primärer Standort SQL Server	
Die Voraussetzungsprüfung wurde abgeschlossen.				
Doppelklicken Sie auf ein beliebiges Element, um o identifizieren Sie das Problem mithilfe der Protoko	letaillierte Informat Ildatei "ConfigMgrP	tionen zur Lösung des Prol rereq.log".	blems anzuzeigen, oder	
Aktuellste Voraussetzungsinformationen anzeigen			Prüfung durchführen	
		Installation starten	Abbrechen	

#### SCCM 2007 R2 installieren

### SCCM 2007 R3 installieren



### Hotfix installieren

🙀 Software Updat	e for ConfigMgr 2007 SP2 (KB977384)-Setup 🛛 🗙
Installation So (KB977384)	iftware Update for ConfigMgr 2007 5P2
Warten Sie, SP2 (KB9773	während der Setup-Assistent Software Update for ConfigMgr 2007 84) installiert. Dies kann einige Minuten dauern.
Status:	
	< Zurück Weiter > Abbrechen
Installation von	KB977384
Γ	Microsoft*
	System Center
	configuration manager 2007
Dieser Hotfix er Systems Center	nthält eine Patchdatei (MSP) für die Software des erweiterten r Configuration Manager Client.
Möchten Sie je erzeugen?	tzt ein Paket und ein Programm zur Bereitstellung des Patches
💿 Ja, ein Pak	et und ein Programm jetzt erzeugen.
🔿 Nein, späte	r erzeugen.
	Abbrechen

### FEP 2010 Installation

### Erweiterte Topologie installieren

🔠 Microsoft Forefront En	dpoint Protection 2010-Server-Setup
<i>I</i>	Installationsoptionen
Microsoft Forefront Endpoint Protection 2010	<ul> <li>Wählen Sie die Installationsoption aus:</li> <li>Basistopologie Installiert die Microsoft Forefront Endpoint Protection 2010-Datenbank, Standortservererweiterung, Konsolenerweiterung, Berichtskomponenten und Berichtsdatenbanken auf Basis der aktuellen Bereitstellung des Konfigurations-Managers.</li> <li>Basistopologie mit Remoteberichtsdatenbank Installiert die Basistopologie und ermöglicht die Installation der Berichtsdatenbank auf einem anderen Computer.</li> <li>Erweiterte Topologie Ermöglicht eine benutzerdefinierte Installation.</li> <li>Nur Konsolenerweiterung des Konfigurations-Managers für FEP 2010 installieren Installiert die Forefront Endpoint Protection 2010-Erweiterung für die Konfigurations-Manager-Konsole.</li> </ul>
Microsoft Forefront En	<zurück weiter=""> Abbrechen  Idpoint Protection 2010-Server-Setup  Erweiterte Topologie</zurück>
Microsoft Forefront Endpoint Protection 2010	<ul> <li>Wählen Sie die zu installierenden Forefront Endpoint Protection 2010-Optionen aus. Weitere Informationen zu den einzelnen Optionen finden Sie unter <u>Bereitstellungshandbuch</u>.</li> <li>✓ FEP 2010-Erweiterung für Konfigurations-Manager-Standortserver Installiert Microsoft Forefront Endpoint Protection 2010-Erweiterungen für den Konfigurations-Manager-Standort (FEP 2010-Sammlungen, Pakete und Baselines der gewünschten Konfigurationsverwaltung). Das Setup für diese Erweiterung muss auf dem Konfigurations-Manager-Standortserver ausgeführt werden.</li> <li>✓ FEP 2010-Berichterstellung und -Warnungen Installiert Microsoft Forefront Endpoint Protection 2010-Berichterstellung und -Warnungen. Der Setup-Assistent für diese Funktion installiert den Forefront Endpoint Protection 2010-Überwachungsdienst lokal.</li> <li>✓ Konfigurations-Manager-Konsolenerweiterung für FEP 2010 Installiert die Microsoft Forefront Endpoint Protection 2010-Erweiterung für die Konfigurations-Manager-Konsole.</li> </ul>
	< Zurück Weiter > Abbrechen

### Neue Datenbank auf SQL Server

🔂 Microsoft Forefront End	point Protection 2010-Server-Setup		×
Y.	Forefront Endpoint Protection 2010-S	erverdatenbankkonfiguratio	n
Microsoft Forefront Endpoint Protection 2010	Verwenden Sie für die Microsoft Forefront Endpo Konfiguration: Computer mit der Konfigurations-Manager-Datenbank: Konfigurations-Manager-Datenbankinstanz: Name der Forefront Endpoint Protection 2010-Datenbank:	int Protection 2010-Datenbank die MSSQLSERVER FEPDB	folgende
		7 mint 1 Mature	Akkeesken

Berichterstellungskonfiguration

	Microsoft Englociet Englociet	nguration
Microsoft	Computer:	
Forefront	Instanz:	MSSQLSERVER
Endpoint	Datenbankname:	FEPDW
Protection		Vorhandene Datenbank wiederverwenden
2010	Die folgenden Informationen werder Konto wird vom Berichtsserver zum verwendet.	i zum Konfigurieren des Kontos zur Berichterstellungsausführung verwendet. Dieses Zugreifen auf die Microsoft Forefront Endpoint Protection 2010-Berichtsdatenbank
	Konto zur Berichtserstellungsa	ausführung für SQL Reporting Services:
	Konto zur Berichtserstellungsa URL:	ausführung für SQL Reporting Services: http://sectional/ReportServer
	Konto zur Berichtserstellungsa URL: Benutzername (Domäne\Benutzer):	Ausführung für SQL Reporting Services: http://services/ReportServer
	Konto zur Berichtserstellungsz URL: Benutzername (Domäne\Benutzer): Kennwort:	ausführung für SQL Reporting Services:       http://second/ReportServer
	Konto zur Berichtserstellungsa URL: Benutzername (Domäne\Benutzer): Kennwort:	Ausführung für SQL Reporting Services:       http://sectors/reportServer         Internet Services:
	Konto zur Berichtserstellungsa URL: Benutzername (Domäne\Benutzer): Kennwort:	susführung für SQL Reporting Services:         http://susful/ReportServer         Image: susful report Server         Image: susful report

Falls sich die Reporting Services nicht auf einem Windows Server 2008 x64 installieren lassen, koennte das hieran liegen: <u>http://support.microsoft.com/kb/894435/en-us</u>

😌 Microsoft Forefront Er	ndpoint Protection 2010-Server-Setup
1	Optionen für Updates und Benutzerfreundlichkeit
Microsoft	Warnung: Diese Optionen wirken sich auf die beim Setup installierten Serverfunktionen aus. Sie werden in den Standardrichtlinien gespeichert, die vom Microsoft Forefront Endpoint Protection 2010-Client verwendet werden, der als Teil der Berichterstellungsfunktion installiert oder auf Endpunktcomputern bereitgestellt wird.
Forefront	Updates
Endpoint	Microsoft Update verwenden, um meine Produkte auf dem neuesten Stand zu halten
Protection 2010	Microsoft Update bietet wichtige Updates (wie z. B. Sicherheitsupdates) für Windows und andere Microsoft-Produkte, einschließlich Microsoft Forefront Endpoint Protection 2010. Mit "Automatische Updates" werden Updates automatisch zur Verfügung gestellt. Sie können die Updates jedoch auch selbst über die Microsoft Update-Website ausführen. <u>Weitere Informationen</u>
	Nöchten Sie am Programm zur Verbesserung der Kundenzufriedenheit teilnehmen?
	Das Programm sammelt Informationen zu Computerhardware und zur Verwendungsweise von Microsoft Forefront Endpoint Protection 2010, ohne Sie dabei zu unterbrechen. Dadurch kann Microsoft ermitteln, welche Funktionen verbessett werden sollten. Die gesammelten Informationen werden nicht dazu genutzt, Sie zu identifizieren oder Kontakt zu Ihnen aufzunehmen.
	O Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen
ADBACK V	O Ich möchte dem Programm jetzt nicht beitreten.
ABDEN.	Online weitere Informationen zum Programm lesen
ALL AND AND A	Datenschutzbestimmungen lesen
AV AN AND	-
AAAA	<zurück weiter=""> Abbrechen</zurück>

### Installationspfad

🔂 Microsoft Forefront End	dpoint Protection	2010-Server-Setup			×
	Installatio	onsverzeichnis			
Microsoft Forefront Endpoint Protection	Produktdateie Navigieren Si <mark>CNProgram Fi</mark> Erforderlicher	n werden im folgenden St e zum gewünschten Speic les\Microsoft Forefront Speicherplatz:	ammordner installiert: herort, wenn Sie den Stammordne	r ändern möchten.	urchsuchen
2010	Volume	Kapazität	Verfügbar	Erforderlich	
	Klicken Sie au	uf ''Weiter'', um mit dem Pr	üfen der Voraussetzungen zu beg	innen.	
			< Zurü	ck Weiter >	Abbrechen

	Aktion	Status	Details
crosoft	S Hardwareanforderungen werden überprüft	Erfolgreich	
refront	Strorderliche Komponente ".NET Framework 3.5 SP1" wird überprüft	Fehler	Weitere
	🔇 Erforderliche Komponente "SQL Server"	Fehler	Weitere
apoint	🔇 SQL Analysis Services-Version überprüfen	Fehler	Weitere
otection	Services werden üb	Erfolgreich	
10	Konfigurations-Manager-Version wird überprüft	Erfolgreich	
10	🖉 Konfigurations-Manager-Gebietsschema überprüfen	Erfolgreich	
	🖉 🥝 Berechtigungen für den Konfigurations-Manager-Standortserver wer	Erfolgreich	
	Konfigurations-Manager-Clientkomponenten werden überprüft	Erfolgreich	
	🐼 Voraussetzung der Configuration Manager-Konsole überprüfen	Fehler	Weitere
	Es wird überprüft, ob ein Neustart nicht erforderlich ist.	Erfolgreich	

Alle Fehler behoben, dann kann das Setup starten

	Aktion	Status	Details	
icrosoft	Microsoft Forefront Endpoint Protection 2010	Wird ausgef		
prefront	Microsoft Forefront Endpoint Protection 2010	Nicht gestar		
docint	Microsoft Forefront Endpoint Protection 2010	Nicht gestar		
αροιπτ	Microsoft Forefront Endpoint Protection 2010	Nicht gestar		
otection				
10				

### Schema fuer SCCM erweitern

#### http://technet.microsoft.com/en-us/library/bb680432.aspx



### SCCM fuer AD Connection Objekt einstellen



### SCCM Sitegrenzen konfigurieren



Ziel soll es sein, den SCCM/FEP Client basierend auf Active Directory Computergruppen zu verteilen, wie das bei FCS der Fall ist.

Active Directory Sicherheitsgruppenermittlung aktivieren

Eigenschaften von Active Directory-Sich	erheitsgruppe	nermittlung 🔀
Allgemein Abfragezeitplan		
Active Directory-Sicherheitsgrupp	enermittlung	,
Active Directory-Sicherheitsgruppener	nittlung aktiviere	n
Active Directory-Container:	-	* 密 🗙
Definierter Name	Rekursiv	Gruppe
LDAP:/	Ja	Ausgeschlo.
LDAP://E	Ja	Ausgeschlo.
LDAP://	Ja	Ausgeschlo.
LDAP://Participarties/	Ja	Ausgeschlo.
OK Abbrechen	Übernehmen	Hilfe

### Danach tauchen die Gruppen in der SCCM Konsole auf

🔠 Datei Aktion Ansicht Fenster ?					
🗢 🔿 🔰 🖬 🛛 🖬					
🙀 System Center Configuration Manager 🗾	Alle Active Directory-Sicherheitsgrup	pen Filteransicht, 14	von 506 Elemente	en werden angezeigt	
🖃 🔤 Standortdatenbank (Standorsson) Verbund)		<u> </u>			
🖃 🤤 Standortverwaltung	Suchen nach: fcs 💌	in Alle Spalten	▼ Suc	the starten	Löschen
🖃 🍓 🖋 🗰 erbund		, .			
🖃 🔜 Standorteinstellungen					
Adressen	Name	Ressourcentyp	Domäne	Standortcode	Client
i Grenzen		Benutzergruppe	aluno		Nein
Clientagents	No. 10 August 10	Benutzergruppe	-		Nein
Clientinstallationsmethoden	2 And Antiperior States of the	Benutzergruppe			Nein
Komponentenkonfiguration	🥂 🥂 👬 🖓 🖓 🖓	Benutzergruppe	42		Nein
🕀 📑 Zertifikate	🧖 💏 💏 👘 🖓 👘 🖓 👘 🖓	Benutzeraruppe			Nein
Konten		Benutzerarunne	and the second s		Nein
Ermittlungsmethoden	Martin Contraction Contraction	Benutzergruppe	dekine and		Nein
4 Absender		Benutzergruppe			Nein
		Benutzergruppe	. Latin Children		Nein
Statusfilterregeln	m and a state of the state of t	Benutzergruppe	dalah menteka		Nein
Statusübersicht		Denutzergruppe	delaine ann		Nein
		Denutzergruppe			Nein
Computerverwaltung		Benutzergruppe	1999 B		Nein
E 🚰 Sammlungen		Benutzergruppe			Nein
Alle Active Directory-Sicherheitsgruppen	S CONTRACTOR OF	Benutzergruppe			Nein
🕀 🚅 Alle Benutzer					
at Alle Benutzergruppen					

#### Client Pushinstallation konfigurieren



#### Standortsystemkomponenten



Rollen	Тур
🗄 ConfigMgr-Komponentenserver	Server
🗓 ConfigMgr-Verteilungspunkt	Server
🗒 ConfigMgr-Verwaltungspunkt	Server
🗄 ConfigMgr-Serverlocatorpunkt	Server
🗄 ConfigMgr-Standortserver	Server
🗒 ConfigMgr-Standortsystem	Server

Als naechstes muss eine neue Collection (Sammlung) basierend auf den Gruppenmitgliedschaften erstellt werden

Sammlungserstellungs-Assis	stent 🗙
Mitgliedschaftsreg	eln
Allgemein	
Mitgliedschaftsregeln	Sammlungsmitgliedschaftsregeln bestimmen, welche Ressourcen beim Aktualisieren in die Sammlung einbezogen werden. Eine Mitgliedschaftsregel kann eine direkte Zuweisung oder eine Abfrage sein.
Ankündigungen	
Sicherheit	,
Status	Mitgliedschaftsregeln:
Bestätigung	Regel Typ Begrenzen auf
	Diese Sammlung entsprechend einem Zeitplan aktualisieren
	Alle 1 Tag(e), beginnend am 04.02.2011 08:10 Zeitplan Zeitplan
	< Zurück Weiter > Fertig stellen Abbrechen

### Abfragebasierte Sammlung erstellen

Abfrageregeleigenschaften		×
Allgemein		
Kame:	FEP-CLIENTS	
	Abfrageanweisung importieren	
Ressourcenklasse:	Systemressourcen           Abfrageanweisung bearbeiten	
Sammlungsbegrenzung —		
Alle Sammlungen		
C Auf Sammlung begren	zen:	
	Durchsuchen	
	OK Abbrechen Hilfe	

### Abfrageanweisung definieren

FEP-Clients Abfrageanweisungseigenschaften	×
Abfragesprache	
Sie können die Abfrageanweisung direkt in WQL bearbeiten	
Abfrageanweisung:	
select SMS_K_SYSTEM.Name from SMS_R_System where SMS_R_System.SystemGroupName = ""	
Abfrageentwurf anzeigen OK Abbrechen Hilfe	

Sammlungsmitgliedschaft aktualisieren

FEP-CLI	ENTS	×
Â	Die Mitgliedschaft dieser Sammlung wird aktualisiert. Falls diese Sammlung untergeordnete Sammlungen enthält, können Sie auch deren Mitgliedschaft aktualisieren.	
🗖 Mit	gliedschaft untergeordneter Sammlungen aktualisieren	
	OK Abbrechen	

F5 druecken nicht vergessen und Achtung: Wenn neue Windows Gruppen fuer FEP-Clients erstellt werden, im SCCM die Ermittlung der Gruppen manuell anstarten



**Client Deployment** 

Jetzt kann der SCCM Client deployed werden

Rechtsklick auf die Collection und Client deployen

Clientpushinstallations-Assis	itent 🗙
Clientpushinstallat	ions-Assistent
Willkommen Installationsoption Fertig stellen	Installationsoptionen Geben Sie die Optionen für die Clientpushinstallation von ConfigMgr an. Installationsoptionen: Geben Sie die Clientinstallationsoptionen an, die zur Installation eines ConfigMgr-Clients in einer Sammlung, einer Abfrage oder auf einem Computer verwendet werden. Domänencontroller einbeziehen Vur Clients innerhalb der Grenzen dieses Standorts einbeziehen Untersammlungen einschließen Immer installieren (vorhandenen Client reparieren oder aktualisieren)
	< Zurück Weiter > Fertig stellen Abbrechen

Auf dem Client startet dann das CCM Setup

👰 Wine	🕎 Windows Task-Manager							
Datei (	Optionen	Ansicht	?					
Anwen	Anwendungen Prozesse Dienste Leistung Netzwerk Benutzer							
Abl	bildname			Benutze	CPU	Arbeitssp	Beschreibung	
Cor	mExec.ex	e *32		SYSTEM	00	2.644 K	CCM Executive	

### SCCM Dienste

🖏 Jillancaru	V CIVVAILEL LICIT		Manuell	LONGICI DICHSU
🎑 SMS Agent Host	Provides chan	Gestartet	Automat	Lokales System
🎑 SMS Task Sequence Agent	SMS client ag		Manuell	Lokales System

### CCM Setup Verzeichnisse

📕 ccmsetup							
🕞 🖓 🗸 Computer	<ul> <li>System (C:) ▼ Windows ▼ comsetup ▼</li> </ul>	· 🗸 🔂	comsetup durchsuchen	2			
Organisieren 👻 🛛 In Bibliothe	k aufnehmen 👻 Freigeben für 👻 N	Neuer Ordner		= 🔹 🛄 😢			
🚖 Favoriten	Name *	Änderungsdatum	Тур	Größe			
📃 Desktop	🔑 {7AA8A59A-2053-4C7E-ABB2-6E9	0017DF4425} 16.03.2011 07:57	Dateiordner				
Downloads	💷 ccmsetup	18.09.2009 05:00	Anwendung	597 KB			
🔛 Zuletzt besucht	📋 ccmsetup	16.03.2011 07:59	Textdokument	107 KB			
🚍 Bibliotheken	📋 client.msi	16.03.2011 07:59	Textdokument	6.657 KB			
	A MobileClient.tcf	16.03.2011 07:55	TCF-Datei	2 KB			
SCCM Symbole							
Angekündigte Programme ausführe (32-Bit)	Anmeldeinformationsverwaltung	Anzeige	Automatische Wiederg	abe			
8enutzerkonten	Center für erleichterte Bedienung	Configuration Manager (32-Bit)	Datum und Uhrzeit				
Energieoptionen	Farbverwaltung	Geräte und Drucker	Geräte-Manager				
Infobereichsymbole	Internetoptionen	iSCSI-Initiator	🧷 Maus				
Netzwerk- und Freigabecente	r Vidneroptionen	Problembehandlung	Programmdownloadmo (32-Bit)	nitor			
Programme und Funktionen	Region und Sprache	RemoteApp- und Desktopverbindungen	Remotesteuerung (32-	Bit)			
Schriftarten	Software Explorers	Sound	Standardprogramme				
🙀 System	Taskleiste und Startmenü	astatur Tastatur	🦚 Telefon und Modem				
Text-in-Sprache	Verwaltung	VM VMware Tools	Wartungscenter				
Windows CardSpace	Windows Update	Windows-Firewall					
SCCM Logdateien auf einem 64 Bit System							
G 🕞 🗸 🕻 🔹 Computer 🔹 System (C	:) • Windows • SysWOW64 • CCM • Logs		<ul> <li>✓</li> </ul>	Logs durch			
Organisieren 🔻 In Bibliothek aufnehmer	n 🔻 Freigeben für 🔻 Neuer Ordner						
🚖 Favoriten	Name ^	Änderungsdatum Typ	Größe				

Organisieren ▼ In Bibliothek autnehmen ▼ Freigeben für ▼ Neuer Ordner									
☆ Favoriten	Name *	Änderungsdatum	Тур	Größe					
📃 Desktop	CAS	17.03.2011 13:10	Textdokument	4 KB					
Downloads	CcmExec	17.03.2011 14:12	Textdokument	116 KB					
🕍 Zuletzt besucht	CertificateMaintenance	17.03.2011 14:00	Textdokument	4 KB					
🦰 Bibliotheken	CIAgent	17.03.2011 10:01	Textdokument	2 KB					
Ellder	ClientIDManagerStartup	17.03.2011 10:00	Textdokument	115 KB					
Dokumente	ClientLocation	17.03.2011 14:12	Textdokument	23 KB					
🌙 Musik	ContentTransferManager	17.03.2011 13:08	Textdokument	4 KB					
📑 Videos	DataTransferService	17.03.2011 14:08	Textdokument	59 KB					
	DCMAgent	17.03.2011 10:01	Textdokument	1 KB					
Computer	execmgr	17.03.2011 13:10	Textdokument	10 KB					
DB (D:)	FileSystemFile	17.03.2011 10:56	Textdokument	94 KB					
Translog (E:)	InternetProxy	17.03.2011 10:00	Textdokument	1 KB					
Tracklogs (F:)	InventoryAgent	17.03.2011 10:57	Textdokument	56 KB					

## Forefront Endpoint Policy erstellen

🖃 📷 Standortsysteme	Richtlinien 8 Elemente gefunden	Aktionen
		Richtlinien 🔺
E Computerverwaltung	Suchen nach: I In Alle Spatten I Suche starten Loschen	Neue Richtlinie
🖃 🚅 Sammlungen		🚰 Richtlinien importieren
Alle Benutzer	Name Beschreidung Rangroige	1 Richtlinienrangfolge bearbeiten
Alle Benutzergruppen	HydMediaCluster 7	😵 Feedback erteilen
<ul> <li>Alle Geräte mit Windows Mobile Pocket PC</li> </ul>	2003 6	Ansicht 🕨
🗉 🗿 Alle Geräte mit Windows Mobile Pocket PO	5.0 Exchange 4	Neues Fenster hier öffnen
<ul> <li>It alle Geräte mit Windows Mobile Smartpho</li> <li>Alle Geräte mit Windows Mobile Smartpho</li> </ul>	ne 5.0 Clients 3	G Aktualisieren
🗈 🚅 Alle Systeme	Default Server Policy     Diese Richtlinie definiert die Standardeinstellungen für Fo 2     Default Deckton Policy     Mit dieser Richtlinie werden die Standardeinstellungen für 1 (Niedrinste)	Hilfe
🗉 🚽 Alle Windows 2000 Server-Systeme		
Image: Alle Windows Server 2003-Systeme     Image: Alle Windows Server-Systeme		
🗉 🚽 Alle Windows Workstation- oder Professio	onal-System /	
Image: Alle Windows XP-Systeme     Alle Windows-Mobilgeräte		
FEP-CLIENTS		
FEP-ExchangeServer		
FEP-HydMediaCluster		
h Konflikt stehende Datensätze		
Softwareverteilung     Softwareupdates		
🗉 👔 Betriebssystembereitstellung		
Asset Intelligence     Asset antelligence     Asset antelligence		
🗉 📃 Berichterstellung		
E Transitionen Er Statistikken in Statistikken Er Statistik		
🗉 👔 Verwaltung mobiler Geräte		
Richtlinien		
4		
Assistent für neue Richtlinien	×	
Allgemein		
Allgemein Dieser	Assistent unterstützt Sie beim Erstellen einer Forefront Endpoint Protection-Richtlinie, die Sie	
Richtlinientyp zum S	chutz von Computern bereitstellen können.	
Zusammenfassung Richtli	nienname:	
Status	seu and	
Bestätigung		
Besch	reibung:	
	v	
	< Zuruck Weiter > Fertig stellen Abbrechen	

### Vorlage auswaehlen



### Richtlinie anpassen

Eigenschaften von File-Serve	r	×
Allgemein AntiMalware Upda	ates   Windows-Firewall	1
Geplante Scans Standardaktionen Echtzeitschutz Ausgeschlossene Dateien um Ausgeschlossene Drozesse Erweitert Außerkraftsetzungen Microsoft SpyNet	<ul> <li>Art und Zeit des Scans planen</li> <li>Scanart: Wöchentlicher Schnellscan</li> <li>Wöchentlicher Scan:</li> <li>Tag: Samstag</li> <li>Uhrzeit: 02:00</li> <li>Vor dem Starten eines Scans überprüfen, ob Definitionsupdates verfügbar sind</li> <li>Nur scannen, wenn der Computer nicht verwendet wird</li> <li>Startzeiten für geplante Scans zufällig festlegen (innerhalb von 30 Minuten vor oder nach der geplanten Zeit)</li> <li>Beim Neustart Scan erzwingen, wenn mindestens zwei geplante Scans nicht stattgefunden haben</li> <li>Prozessorauslastung während Scans auf folgenden Prozentwert begrenzen:</li> <li>30%</li> <li>Benutzern an Endpunktcomputern die Konfiguration von Prozessorauslastungshöchstwerten für Scans ermöglichen</li> <li>Steuerung durch den Benutzer von geplanten Scans:</li> <li>Vollzugriff: aktivieren, deaktivieren, Scantyp festlegen und planen</li> </ul>	
×		
	OK Abbrechen Übernehme	en

### Richtlinie zuweisen

Richtlinie zuweisen Klicken Sie auf "Hinzufügen" Richtlinie anwenden möchte	', um die einzelnen S≀ n. Klicken Sie anschli	ammlungen auszu eßend auf "OK",	wählen, auf die	× Sie diese	Jng
Sammlungsname	Standortcode	Untergeordnete Sammlungen einschließen	Н	inzufügen Entfernen	itlinie definiert die S Richtlinie werden d
	Sammlung	g durchsuchen			
geServer ingen ver ande Datensätze ung ss pereitstellung ce	Sammlun 	gen: Alle unbekannten Alle Windows 2000 Alle Windows 2000 Alle Windows Serv Alle Windows Wor Alle Windows Wor Alle Windows XP-3 Alle Windows-Mob FEP-CLIENTS FEP-ExchangeSer FEP-Fileserver FEP-Sammlungen	Computer D Professional- D Server-Syste ver-Systeme kstation- oder Systeme illgeräte ver	Systeme eme eme Professional-Sys	teme
ng g rünschter Konfigurationen	Sammlun	g:	FEP-Fileserve	r	
iler Geräte			ОК	Abbrechen	Hilfe

### Pakete verteilen

	Assistent zur Verteilung von	Software an Sammlunge	n	×
	Paket	Paket auswählen		×
	Willkommen Paket Programm ankündigen Programm auswählen	KB977384 - Adva Microsoft Corpor Microsoft Corpor Microsoft Corpor	anced Client Hotfix - GLG ation FEP - Deployment 1.0 ation FEP - Operations 1.0 ation FEP - Policies 1.0	- /erteilen aus.
ı.	Zusammenfassung			
	Status			
1	Bestätigung			
•			51 500005	
ł		Paket-ID:		Durchsuchen
		Quellversion:	12 (17.03.2011 13:09:52)	
i		Zeit der letzten Aktual.:	17.03.2011 13:10:01	
I.		Kommentar:	Mit diesem Paket konnen Sie die Verteilung von Microsoft Forefront Endpoint	
1			Protection 2010 verwalten.	
		[	OK Abbrechen Hilfe	
:			< Zurück Weiter >	Fertig stellen Abbrechen

Assistent zur Verteilung von S	oftware an Sammlungen	×
Programm auswähle	n	
Willkommen Paket Verteilungspunkte	Wählen Sie das Programm aus, das Mitgliedern einer Sammlung angekündigt werden soll.	
Ankündigungsname Untergeordnete Ankündi Ankündigungsplan Programm zuweisen Zusammenfassung Status Bestätigung	Paket: FEP - Deployment Programme: Name Beschreibung Install Installiert Microsoft Forefront Endpoint Prot Uninstall Entfernt Microsoft Forefront Endpoint Prote	-
ај <u>ј</u> рј	<pre>&lt; Zurück Weiter &gt; Fertig stellen Abbre</pre>	chen

### Paket zuweisen

Assistent zur Verteilung von S	oftware an Sammlungen	× • • • • • • • • • • • • • • • • • • •							
Programm zuweisen									
Willkommen Paket	Geben Sie an, ob das Prog	gramm zugewiesen werden soll.							
verteilungspunkte Programm auswählen Ankündigungsname Untergeordnete Ankündi	Durch das Zuweisen eines Programms wird das Programm erforderlich. Ein zugewiesenes Programm wird automatisch ausgeführt, falls es noch nicht auf dem Client ausgeführt wurde. Soll dieses Programm nach einem angegebenen Zeitpunkt (Datum/Uhrzeit) zugewiesen werden?								
Ankündigungsplan Programm zuweisen	O Nein, das Programm nicht zuweisen.								
Zusammenfassung	is say as rrogramm	conoson.							
Status	Verfügbar nach:	15:00:12 17.03.2011							
Bestätigung	Zuweisen nach:	17.03.2011 💌 15:00							
	Läuft ab nach:								
	🔲 Wake-On-LAN akti	vieren							
	🔲 Beim Ausführen de	s Programms Wartungsfenster ignorieren							
	Systemneustart außerhalb des Wartungsfensters zulassen								
<pre></pre>		< Zurück Weiter > Fertig stellen Abbrechen							

Ggfs. Uebernahme der Custom FCS Einstellungen in den Policies

tlinie bearbeiten	
gemein Schutz Erweitert Außerkraftsetzungen Berichterst	ellung
Malwaredefinitionsupdates	
☑ ⊻or dem Starten eines Scans auf Updates prüfen	
☑ In festgelegtem Intervall auf Updates prüfen (Stunden):	
🔽 🔟 enn WSUS nicht verfügbar ist, bei Microsoft Update auf	Updates prüfen
Datenschutzbestimmungen	
Malwarescapoptionen	
Archivdateien scannen	🗖 Dateien in Quarantäne löschen:
- Houristik zum Erkonnon uprdächtiger Dataion	Linghon nach (Tagan): 00
Heulistik zum Erkennen verdachtiger bigtelen	Euschen nach (Lagen). 30 🔄
Ausschlüsse aus Malwarescans	
Datei- und Ordnerpfade:	E <u>r</u> weiterungen:
D:\Programme\BBES	n Iadm 🔺 Hinzufügen
Nnttrs_cmp°.*	admi
Registry.pol	
w:\	.edb
	jdb 🗾
Clientoptionen	
Benutzer können alle Client	Nur Administratoren können Client
Security-Agenteneinstellungen und -Meldungen	Security-Agenteneinstellungen ändern
O Benutzer können nur ein Taskleistensymbol und	Benutzern das Hinzufügen von Ausschlüssen und
Statusmeldungen anzeigen	Eingabeaufforderung anzeigen, wenn nicht klassifizierte
	Software erkannt wird
	OK Abbrechen Hilfe

### **FEP Reporting**

#### FEP Statistiken aktualisieren



Die Statistik fuellt sich mit Leben. Schon auf fast 6 Servern/Clients FEP ausgerollt ©

Dashboard - Aktualisiert: 17.03.2011 12:58	
Operative Statistiken	
Clientbereitstellungsstatus Als Ziel festgelegt von FEP: 6 von 3091	Sicherheitsstatus       Computer         Infiziert       0         Neustart erforderlich       0         Vollständiger Scan erforderlich       0         Aktuelle Schadsoftwareaktivität       0         Definitionsstatus       Computer         Älter als 1 Woche       0         Bis zu 7 Tage alt       0         Aktuell       3
Schutzstatus Computer	Richtlinienverteilungsstatus Computer
😵 Schutzdienst deaktiviert 🗕	😵 Fehler 🗕
🚯 Keine Meldung 🕴 👤	🚯 Ausstehend 🕴 🤱
📀 Ordnungsgemäß 🗕	Verteilt 2

Zusammenfassungsreport eines Servers / Clients

🔗 Report Viewer - Windows Internet Explorer	_ 8
🚱 🕙 🖉 http:// 💭 http:// DeportServer/Pages/ReportWewer.aspx?/Forefront%20Endpoint%20Protection 🛥 AntiMalware/Computer%20Details%20Repo	💌 🍫 🗙 🔎 Bing 🖉
Favoriten	
Report Viewer	🏠 🔹 🔊 🕤 🚔 🔹 Seite 🗸 Sicherheit 🔹 Extras 🗸 🌀
Sammlung: Alle Desktop-PCs und Server Merchtszeitspanne: Mo	nat Bericht anzeigen
Startdatum (nur 17.02.2011 Enddatum (nur 17. benutzerdefinierte Berichtszeitspanne): Berichtszeitspanne):	03.2011
Computername: Jocal	
Id d I von 1 ▶ ▶ 100%	tieren 😰 🎒
Forefront Endpoint Protection	
Computerdetailbericht	
Sammlung: Alle Desktop-PC's und Berichtszeitspanne: Monat Generiert am: 17.03.2011 12:33.43 Server	
Startdatum: 17.02.2011 00:00 Enddatum: 17.03.2011 12:33	ür alle Datums- und Zeitangaben wird die pordinierte Wettzeit verwendet.
Computerdetails	
Computername (	
Domäne	
Betriebssystem Microsoft Windows NT Server 6.1	
Schutzetatue	
Schutzstatus	
Letzte Aktualisierung: Keine Informationen verfügbar	
Corofront Endnoint Protection Oliont Installiont	

### FEP Scans und Updates manuell ausfuehren

	SRV	System		STAND .		Ja	Gen
Ļ	SRV	Client installieren			-	Ja	Gen
2	SR۷	Verteilen	•			Ja	Gen
	SRV	Start	►			Nein	Nich
	SRV	Letzte PXE-Ankündigung löschen				Ja	Gen
	AEK	Genehmigen				Nein	Nich
	SRV	Blockieren		-		Nein	Nich
	SR۷	Sammlungsmitgliedschaft verwalten	►		-	Ja	Gen
	SR۷	Out-of-Band-Verwaltung	►		( <b>1)</b>	Nein	Nich
Ľ	SRV	FEP-Vorgänge	•	Update der A	ntiMalware-Defin	nitionen ausführen	h
	SR۷	FEP-Computerdetailbericht ausführen		Schnellscan a	usführen		h
	MSC	Löschen		Vollständigen	Scan ausführen		h
	SRV	Aktualisieren	-		-	Nein	Nich
	MIC	AKCOMISICICIT		- 🗰 -	-	Nein	Nich
2	F12	Eigenschaften			-	Nein	Nich
2	MIC	Hilfe		45998	<b></b>	Nein	Nich
	VMG				6005	Nein	Nich

#### Microsoft Forefront Endpoint Protection 2010

×

OK



FEP Vorgang "Update der AntiMalware-Definitionen ausführen" wurde geplant.

Die Ankündigung "Update der AntiMalware-Definitionen um 17.03.2011 12:20:42 (UTC) ausführen" wurde für die folgende Sammlung erstellt: "Update der AntiMalware-Definitionen um 17.03.2011 12:20:42 (UTC)".

] 🚅 Alle Active Directory-Sicherheitsgruppen		Name	Ressourcentyp	Domäne	Standortcode	Client	Genehmigt
Alle Benutzer		M YNC	System			Ja	Genehmigt
Alle Benutzergruppen							
Alle Desktop-PCs und Server							
Alle Geräte mit Windows Mobile Pocket PC 2003							
Alle Geräte mit Windows Mobile Pocket PC 5.0							
Alle Geräte mit Windows Mobile Smartphone 2003							
Alle Geräte mit Windows Mobile Smartphone 5.0							
Alle Systeme							
Alle unbekannten Computer							
Alle Windows 2000 Professional-Systeme							
Alle Windows 2000 Server-Systeme							
Alle Windows Server 2003-Systeme							
Alle Windows Server-Systeme							
Alle Windows Workstation- oder Professional-Sys	teme						
lle Windows XP-Systeme							
e Windows-Mobilgeräte							
P-CLIENTS							
P-ExchangeServer							
P-Fileserver							
EP-HydMediaCluster							
EP-Orbis-Server							
EP-Sammlungen							
💑 Bereitstellungsstatus							
🐴 Definitionsstatus							
🚪 Richtlinienverteilungsstatus							
Schutzstatus							
🐴 Sicherheitsstatus							
🚪 Vorgänge							
Schnellscan um 17.03.2011 12:32:46 (UT Schnellscan um 17.03.2011 13:36:50 (UT)	C)						
🗉 才 Update der AntiMalware-Definitionen um	17.C						
🕀 🗃 Vollständiger Scan um 17.03.2011 12:21	08 (						

Fuer jeden manuellen FEP Vorgang werden entsprechende Advertisements erstellt



### Warnungsbenachrichtigung einrichten

E-Mail-Einstellungen	×
E-Mail-Warnungsbenachrichtigung	
<u>S</u> MTP-Server (FQDN):	Port:
Service States Incal	25 📑
Authentifizierungsmethode: O Anonym	
<ul> <li>Windows-integriert</li> </ul>	
E-Mail-Absenderadresse:	
<b>Hereit State</b> Incal	
Testen und schließen OK	Abbrechen

Eigenschaften von Warnungen beim Erkennen von Schadsoftware	x
Warnung bei Erkennung neuer Schadsoftware	
Von Forefront Endpoint Protection kann eine Warnung ausgelöst werden, wenn Schadsoftware auf einem Computer erkannt wird, der Mitglied der angegebenen Sammlung oder der dazugehörigen untergeordneten Sammlungen ist. Übergeordnete Sammlung eingeben:	
FEP-Sammlungen Durchsuchen	
Er <u>k</u> ennungsstufe auswählen:	
Hoch: Malware wurde erkannt	
<ul> <li>Eine Warnung wird generiert, wenn Schadsoftware erkannt wird, unabhängig davon, ob die Schadsoftware entfernt wurde.</li> </ul>	
Wenn eine warnung ausgelost wird, eine E-Mail an die rolgenden Empränger senden:         E-Mail-Adresse         Entfernen	
OK Abbrechen Übernehmen	- 1

#### FCS deinstallieren

Nach der erfolgreichen FEP Einfuehrung, muessen als erstes die FCS Policies und damit die Gruppenrichtlinien entfernt werden. Der FCS / MOM Client wurde bereits waehrend der FEP/SCCM Client Installation automatisch entfernt

FCS Policies entfernen

🚺 Microsoft Forefront	Client Security			
Datei Aktion Ansicht	t <u>?</u>			
← → 🗈 🖬 🔮				
				Forefront Client Security Management Console
Dashboard	Richtlinienverwaltung			
Richtlinien				
🗋 Neu 📝 Bearbeiter	en 🗈 Kopieren 📗 Bereits	tellen Bereitstellung zurü	cknehmen 🗙 Löschen	Berichte anzeigen
Name 🔶	Zuletzt geändert	Geändert von	Zuletzt bereitgestellt	Bereitgestellt für
Clients-Richtlinie	16.03.2011 09:30	<b>des m</b> administrator	16.03.2011 09:33	Clients
BExchange-Server	25.01.2010 07:31	ministrator	22.04.2010 13:46	A CONTRACT OF A CO
🔓 File-Server	08.06.2010 14:22	<b>Contractor</b> Manual Antipation	08.06.2010 14:30	A CONTRACTOR OF
🔓 GLG	08.06.2010 12:47	administrator	15.03.2011 12:48	
🚡 HydMedia-Cluster	08.06.2010 12:48	administrator	08.06.2010 12:49	
눩 Orbis-Server	08.06.2010 14:22	dministrator	08.06.2010 14:30	
Μ	licrosoft Forefront Client 5 Durch das Zurücknehmen dr Wenn Sie einige (und nicht a Möchten Sie die Bereitstellur	Security ar Bereitstellung wird die Lis Ille) Ziele zur Richtlinie hinz g wirklich zurücknehmen?	te der Ziele aus dieser Rich	ntinie und die Richtlinie aus der Gruppenrichtlinie entfernt. erren möchten, klicken Sie auf "Abbrechen" und dann auf "Bereitstellen". Bereitstellung zurücknehmen Abbrechen

### FCS Deinstallation

5oftware			_ 🗆
5	Zurzeit installierte Programme: 🔲 Up <u>d</u> ates anzeigen Sortie	ren nach: Name	•
Programme ändern oder entfernen	😽 Microsoft .NET Framework 3.5 Language Pack SP1 - DEU	Größe:	37,94 MB
	🔀 Microsoft .NET Framework 3.5 SP1	Größe:	28,72 MB
- <b>1</b>	Microsoft Forefront Client Security Collection Server	Größe:	<u>0,82 MB</u>
<u>N</u> eue Programme	Klicken Sie hier, um Supportinformationen zu erhalten.	Verwendet:	<u>selten</u>
hinzufügen		Zuletzt verwendet am:	27.07.2009
6	Klicken Sie auf "Entfernen", um dieses Programm von dem Computer zu entfernen	l.	Entfernen
Windows-	Microsoft Forefront Client Security Data Warehouse Server	Größe:	0,40 MB
mponenten inzufügen/	Microsoft Forefront Client Security Installation Tool	Größe:	1,23 MB
entfernen	Microsoft Forefront Client Security Management Server	Größe:	13,85 MB
	Microsoft Forefront Client Security State Assessment Service	Größe:	1,56 MB -
	Microsoft Forefront Client Security-Antimalwaredienst	Größe:	8,80 MB
	Microsoft Forefront Client Security-Update-Assistent	Größe:	0,22 MB
	ទីខ្លុ Microsoft Gruppenrichtlinien-Verwaltungskonsole mit SP1	Größe:	6,30 MB
	S Microsoft Office 2003 Web Components	Größe:	30,66 MB
	🧭 Microsoft Operations Manager 2005	Größe:	186,00 MB
	🧭 Microsoft Operations Manager 2005 Forefront Evaluation Patch	Größe:	3,84 MB
	🧭 Microsoft Operations Manager 2005-Berichterstattung	Größe:	4,13 MB
	🕮 Microsoft Report Viewer Redistributable 2005	Cräßer	75 74 MD