

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

IST Zustand:

- 1 FCS Server mit WSUS und MOM
- 1 SQL Server 2008 Cluster fuer die FCS/MOM Datenbanken

SOLL Zustand:

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

Offizielle Anleitung zur Migration von FCS zu FEP:

<http://technet.microsoft.com/en-us/library/gg477033.aspx>

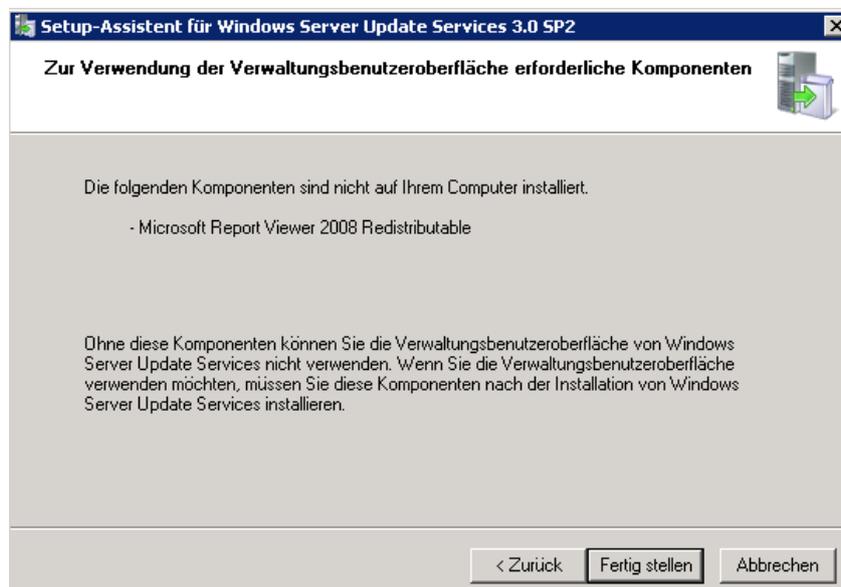
Weitere Informationen zu FEP:

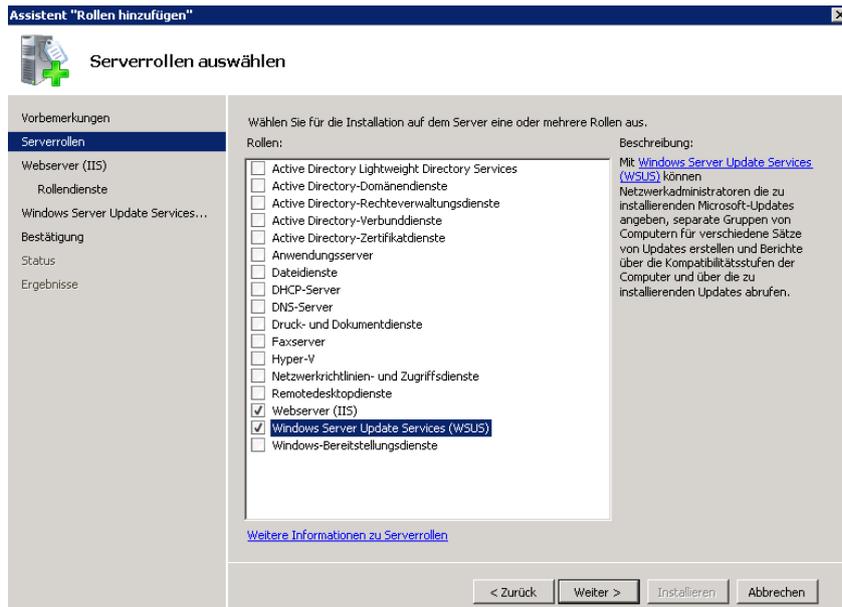
<http://www.it-training-grote.de/download/FEP2010.pdf>

Windows Server Installation / Konfiguration

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

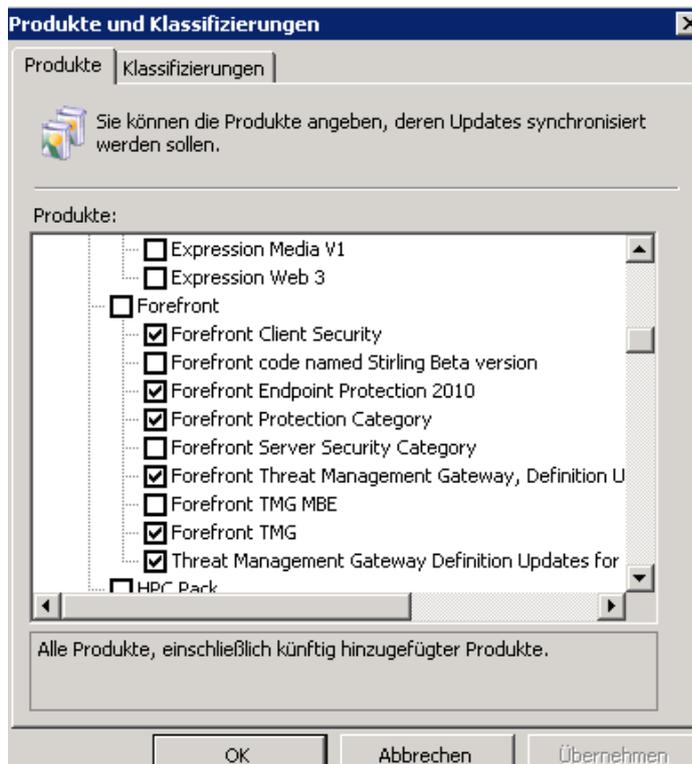
WSUS installieren oder nur die Verwaltungskonsole



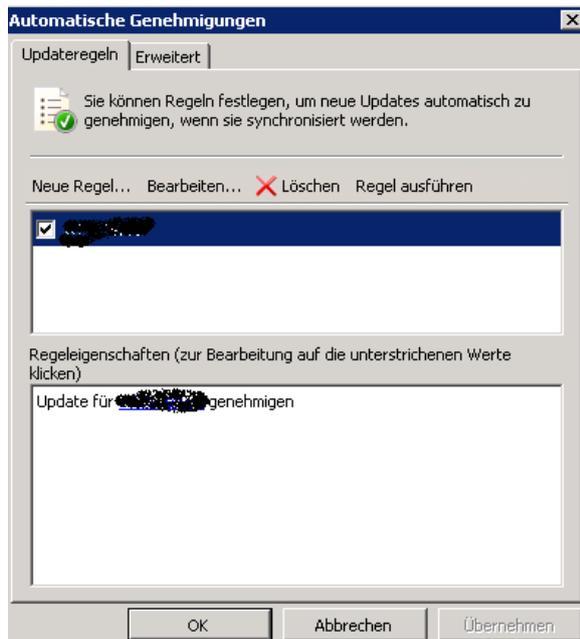


WSUS nach Vorgaben konfigurieren

Produkte und Klassifizierungen auswahlen



Automatische Genehmigungen konfigurieren

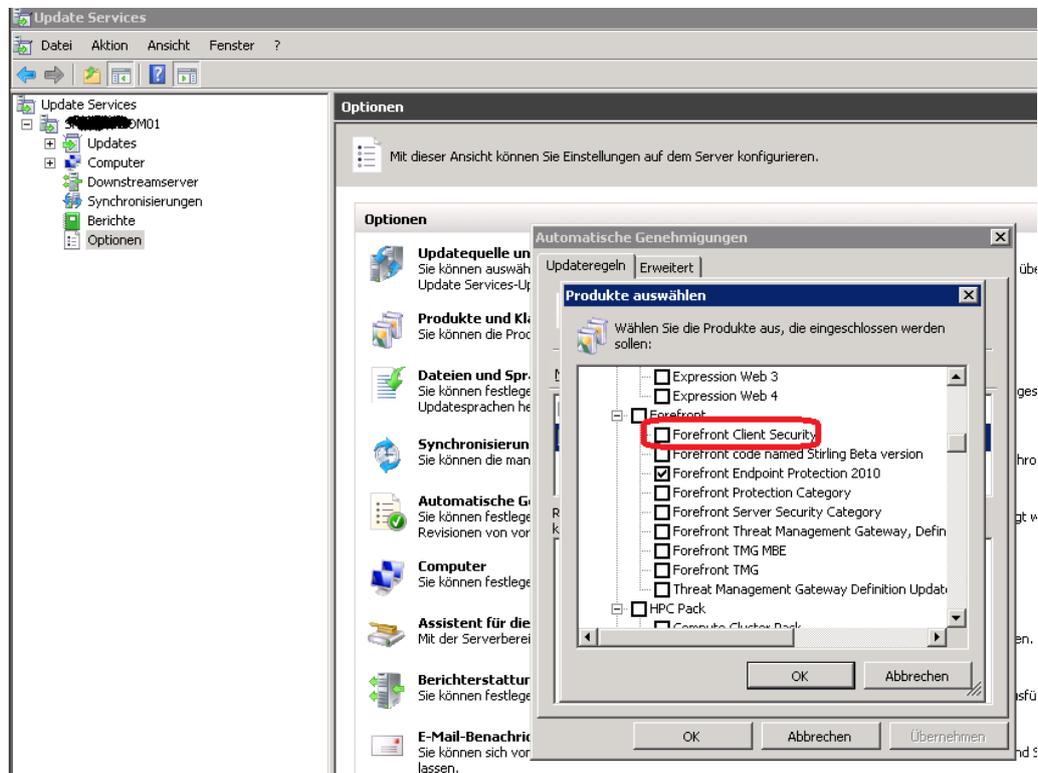


Datenbank auf den zentralen SQL Server Cluster legen

WSUS Migration (wenn der FCS Server auch WSUS Server war)

<http://www.it-training-grote.de/download/WSUS3migration.pdf>

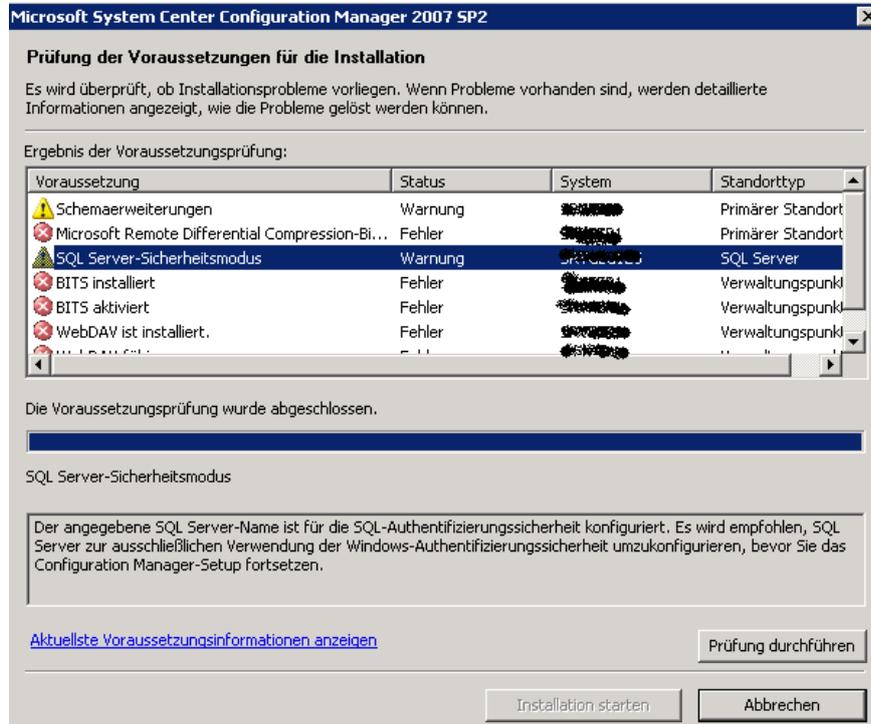
Vorhandene FCS Updates unapproven



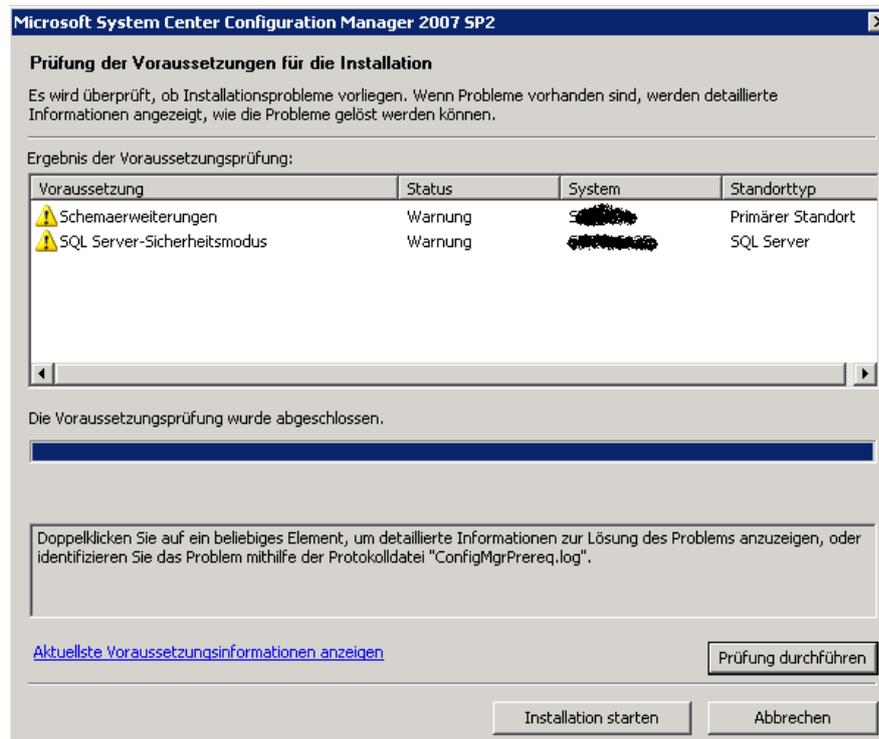
SCCM Installation

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

OK, der ein oder andere Fehler



Besser



Schema fuer SCCM erweitern

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

Ausfuehrung auf dem Schema Master

```
Administrator: C:\Windows\system32\cmd.exe
Volumeseriennummer: 38D8-BBB6

Verzeichnis von C:\Temp

16.05.2011 11:43 <DIR>          .
16.05.2011 11:43 <DIR>          ..
07.02.2011 15:22             362.272 AdConfigPack.exe
16.01.2009 01:00             201.064 EXTADSCH.EXE
                2 Datei(en),          563.336 Bytes
                2 Verzeichnis(se), 21.072.281.600 Bytes frei

C:\Temp>EXTADSCH.EXE

Microsoft System Center Configuration Manager v4.00 (Build 6487)
Copyright (C) 2005 Microsoft Corp.

Successfully extended the Active Directory schema.

Please refer to the SMS documentation for instructions on the manual configurati
on of access rights in active directory which may still need to be performed. <
Although the AD schema has now be extended, AD must be configured to allow each
SMS Site security rights to publish in each of their domains.>

C:\Temp>
```

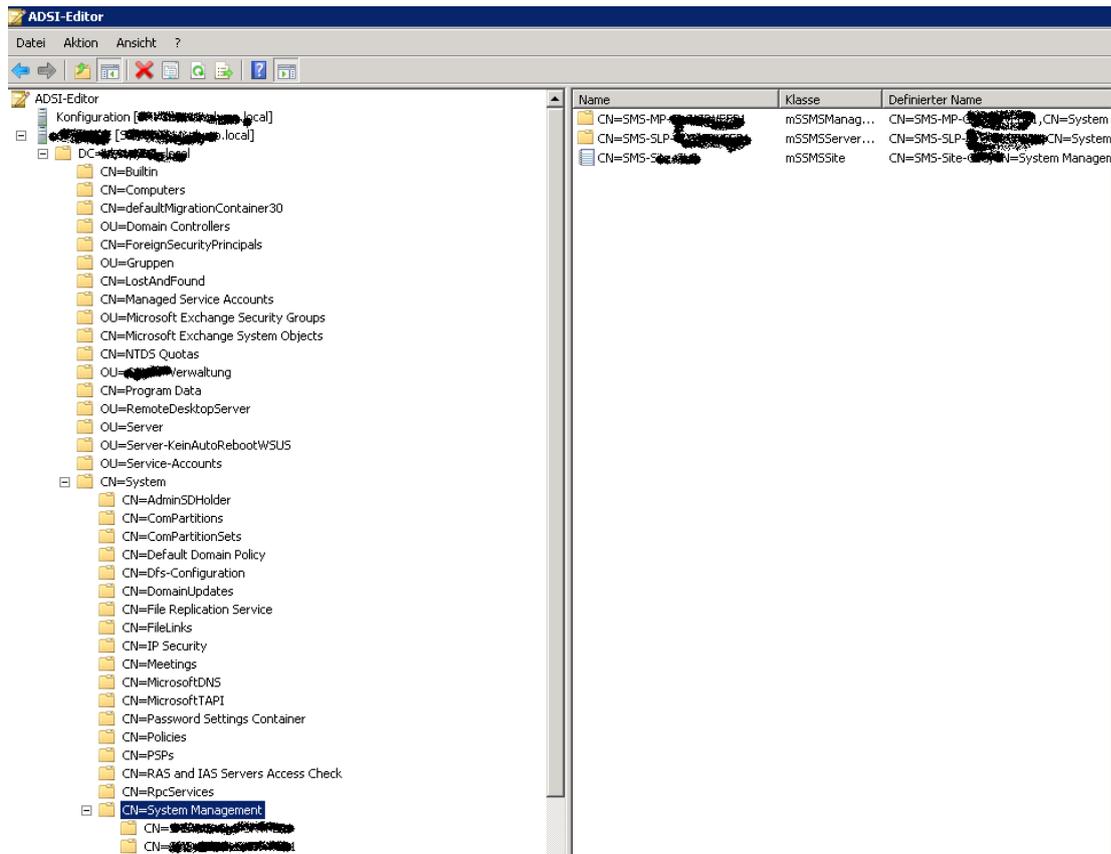
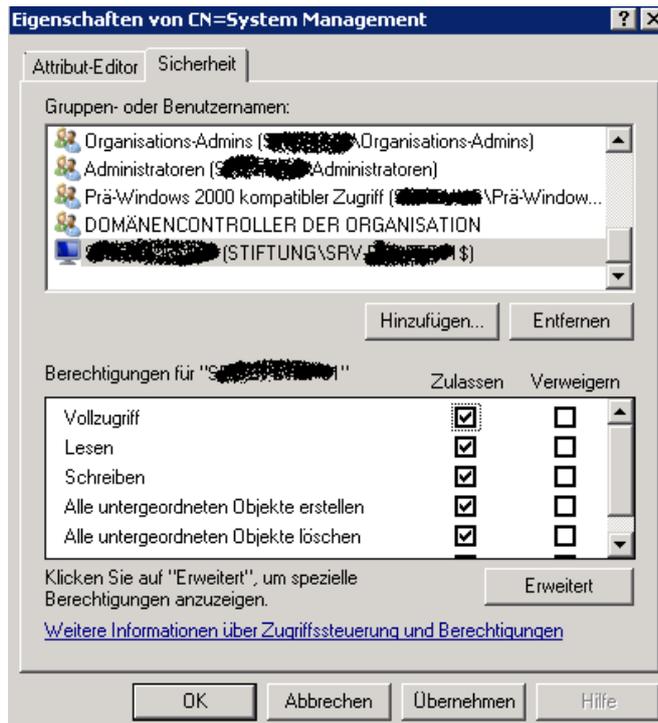
Mit ADSIEDIT anlegen

The screenshot shows the ADSI Edit tool. On the left, a tree view displays the Active Directory structure, with 'CN=System' expanded to show various system containers. On the right, the 'Objekt erstellen' (Create Object) dialog box is open. It contains the following information:

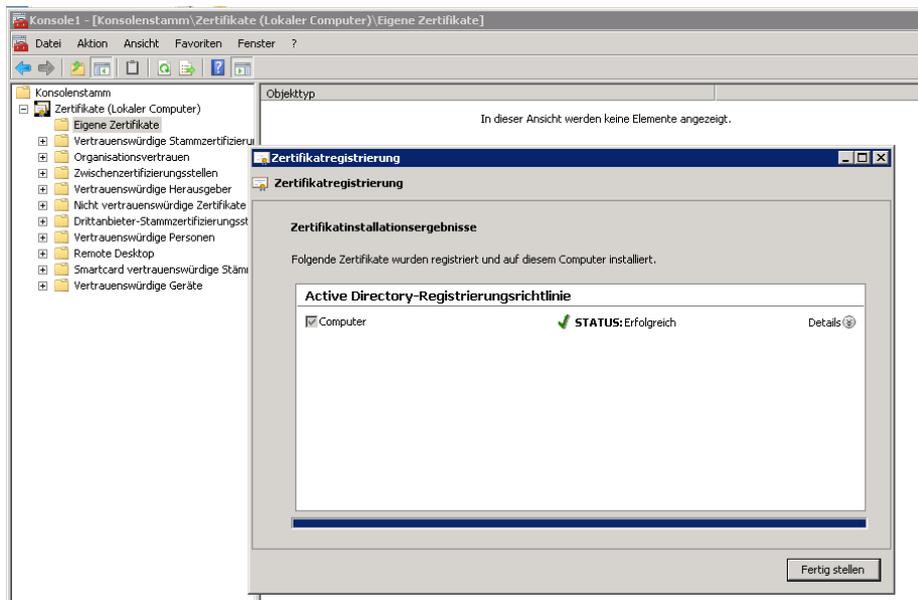
- Attribut: cn
- Syntax: Unicode-Zeichenfolge
- Beschreibung: Common-Name
- Wert: System Management

At the bottom of the dialog, there are four buttons: '< Zurück', 'Weiter >', 'Abbrechen', and 'Hilfe'.

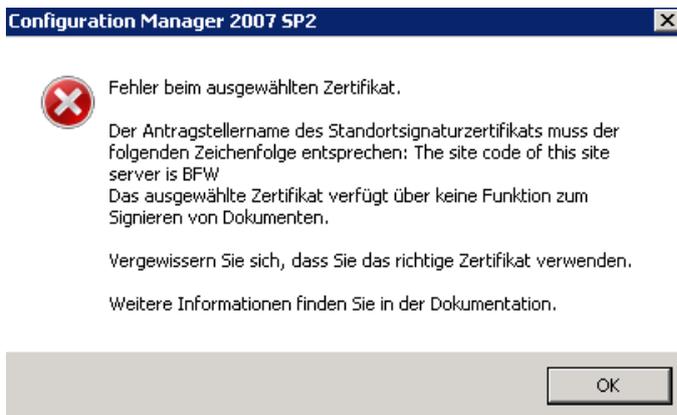
Container fuer den FEP(SCCM) Computer Account berechtigen



Computerzertifikat fuer den nativen SCCM Modus



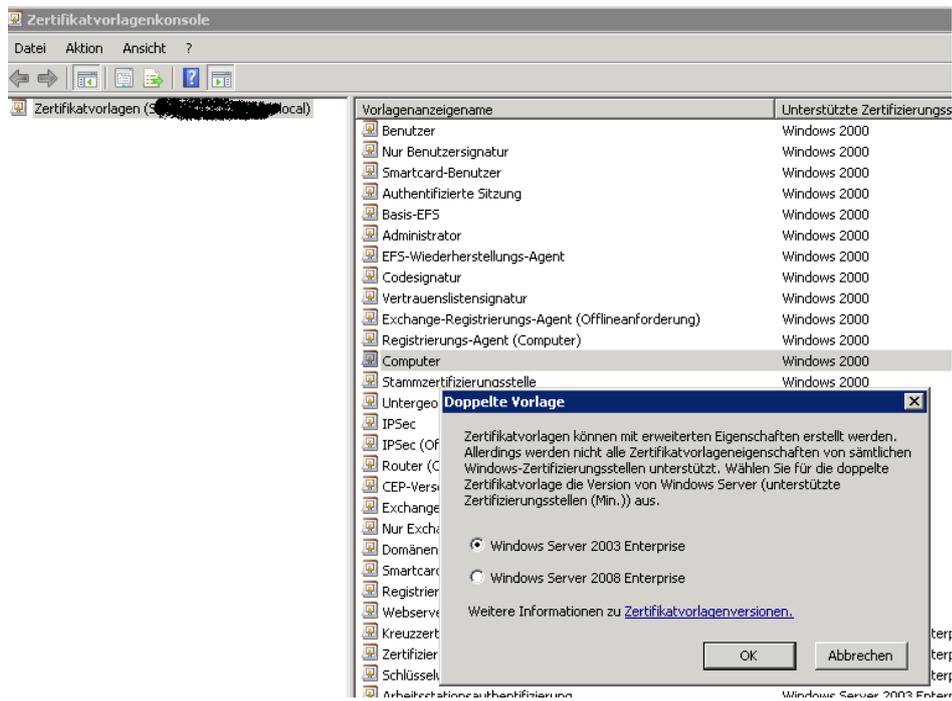
Nicht ausreichend



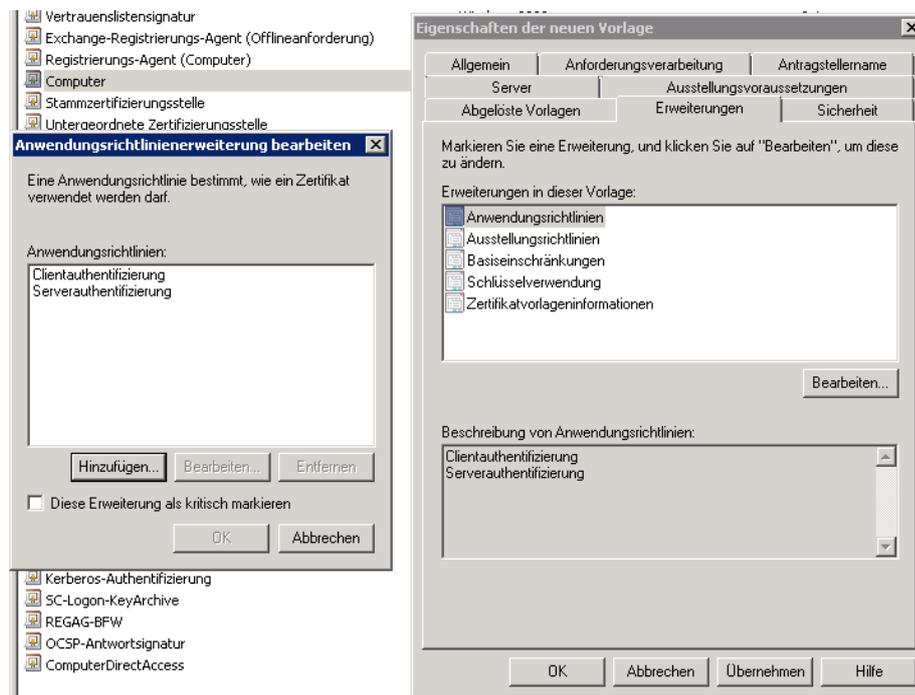
Quelle:

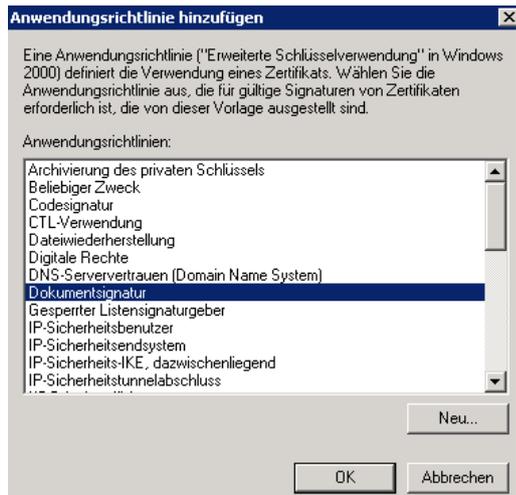
<http://technet.microsoft.com/en-us/library/bb680733.aspx>

Neues Zertifikatvorlagen Template erstellen

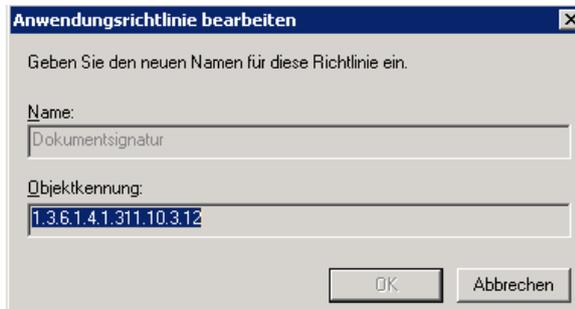


EKU hinzufügen

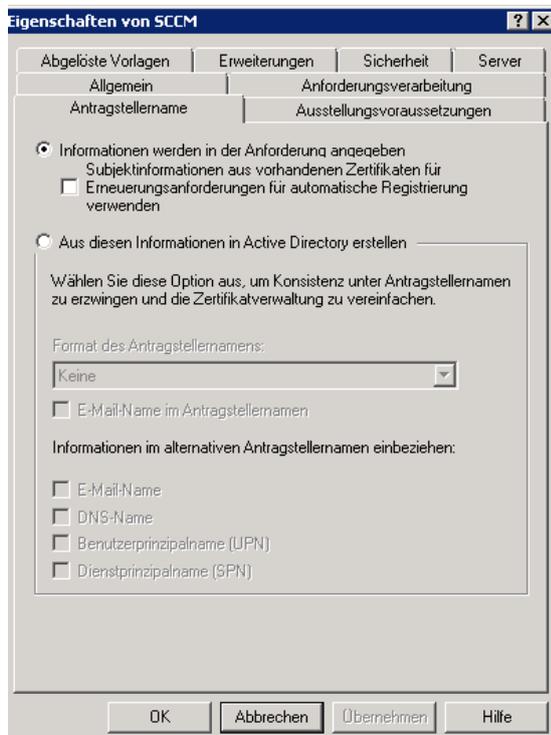




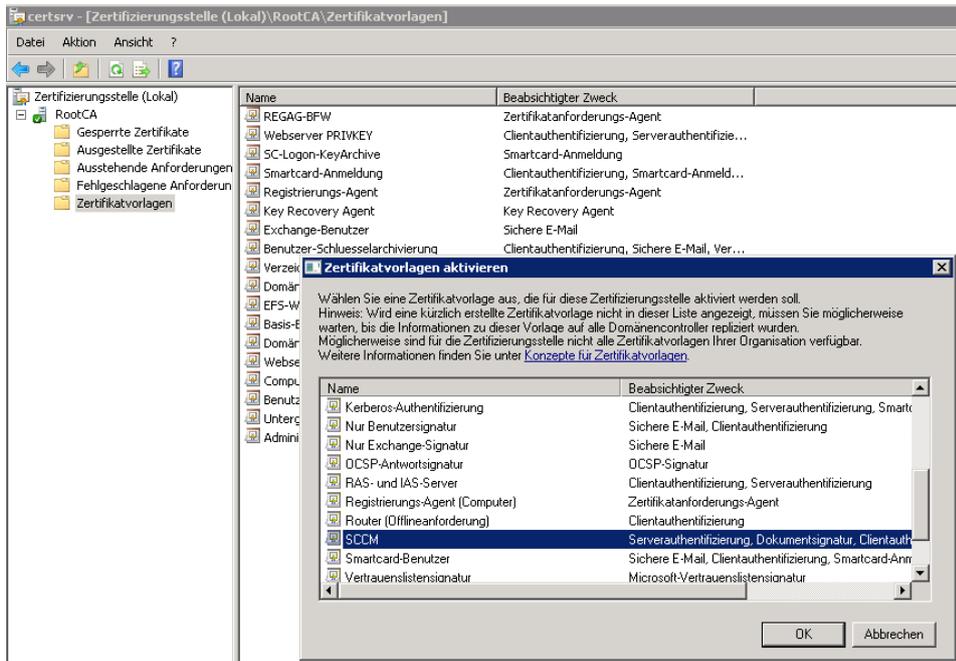
Richtig:



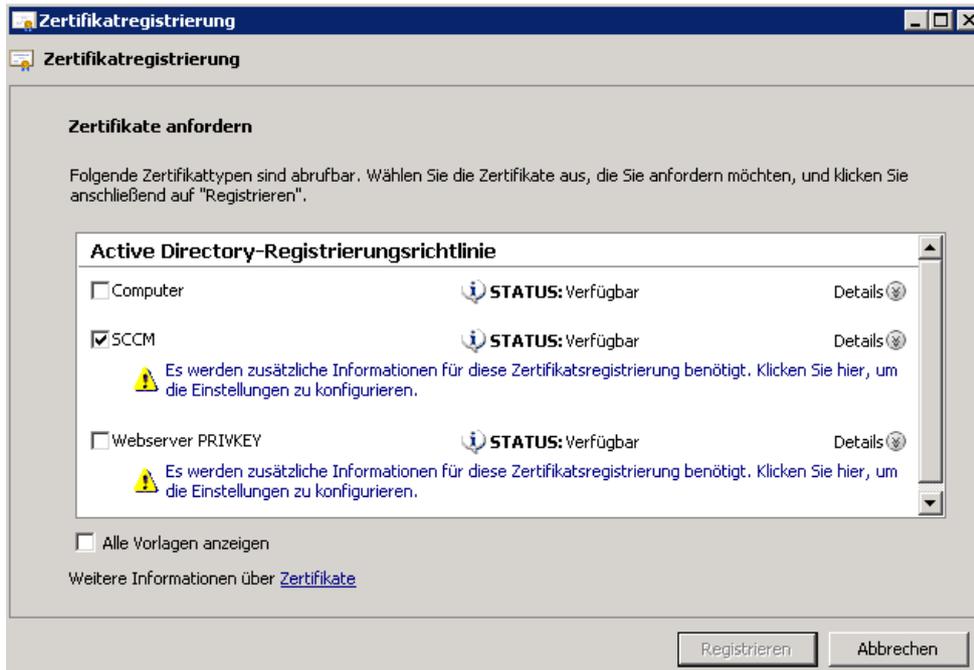
Informationen ueber den Antragsteller waehrend der Zertifikatgenerierung eingeben

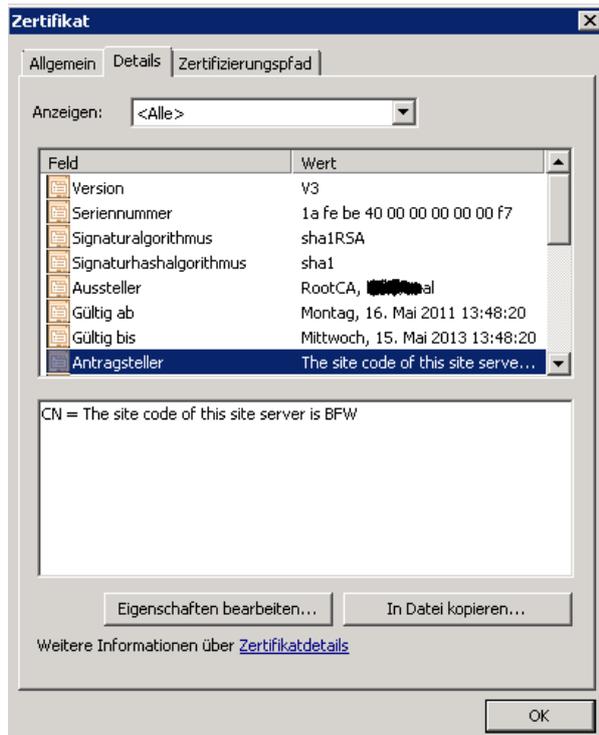
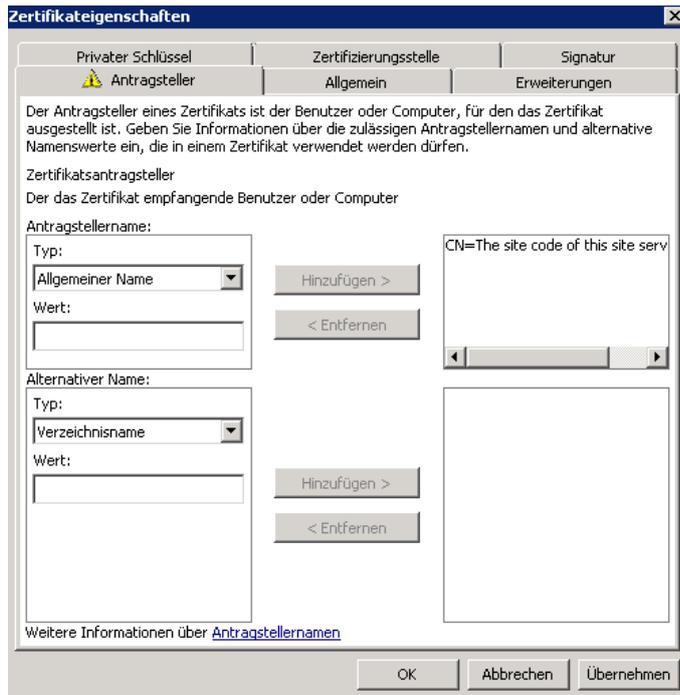


Zertifikatvorlage aktivieren



Neues Zertifikat basierend auf der neuen Vorlage anfordern

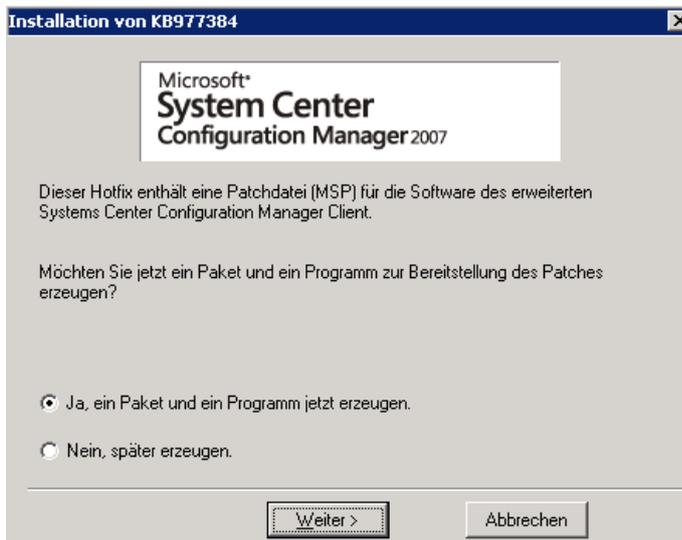
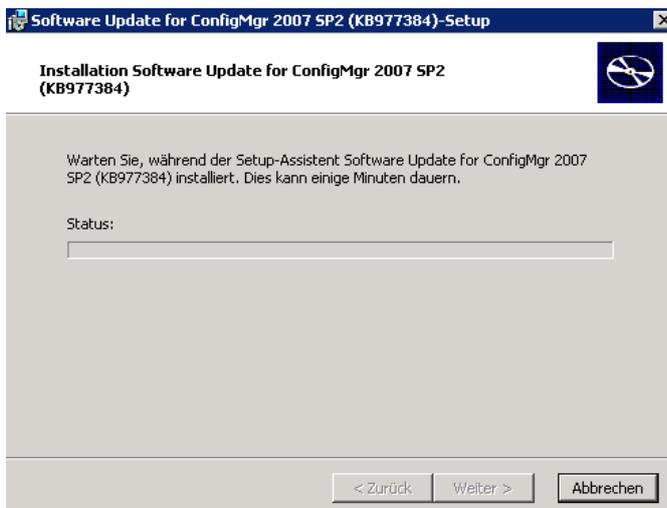




SCCM 2007 R3 installieren

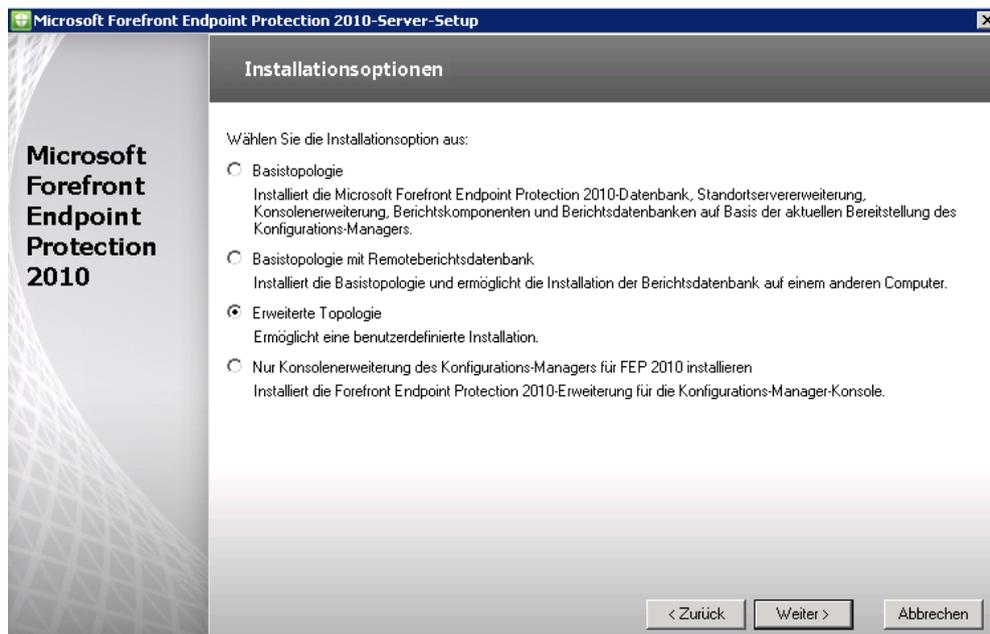


Hotfix installieren



FEP 2010 Installation

Erweiterte Topologie installieren



Neue Datenbank auf SQL Server

Microsoft Forefront Endpoint Protection 2010-Server-Setup

Forefront Endpoint Protection 2010-Serverdatenbankkonfiguration

Verwenden Sie für die Microsoft Forefront Endpoint Protection 2010-Datenbank die folgende Konfiguration:

Computer mit der Konfigurations-Manager-Datenbank: [REDACTED]

Konfigurations-Manager-Datenbankinstanz: MSSQLSERVER

Name der Forefront Endpoint Protection 2010-Datenbank: FEPOB

< Zurück Weiter > Abbrechen

Berichterstellungskonfiguration

Microsoft Forefront Endpoint Protection 2010-Server-Setup

Berichterstellungskonfiguration

Microsoft Forefront Endpoint Protection 2010-Berichtsdatenbankeinstellungen:

Computer: [REDACTED]

Instanz: MSSQLSERVER

Datenbankname: FEPOB

Vorhandene Datenbank wiederverwenden

Die folgenden Informationen werden zum Konfigurieren des Kontos zur Berichterstellungsausführung verwendet. Dieses Konto wird vom Berichtsserver zum Zugreifen auf die Microsoft Forefront Endpoint Protection 2010-Berichtsdatenbank verwendet.

Konto zur Berichterstellungsausführung für SQL Reporting Services:

URL: http://[REDACTED]/ReportServer

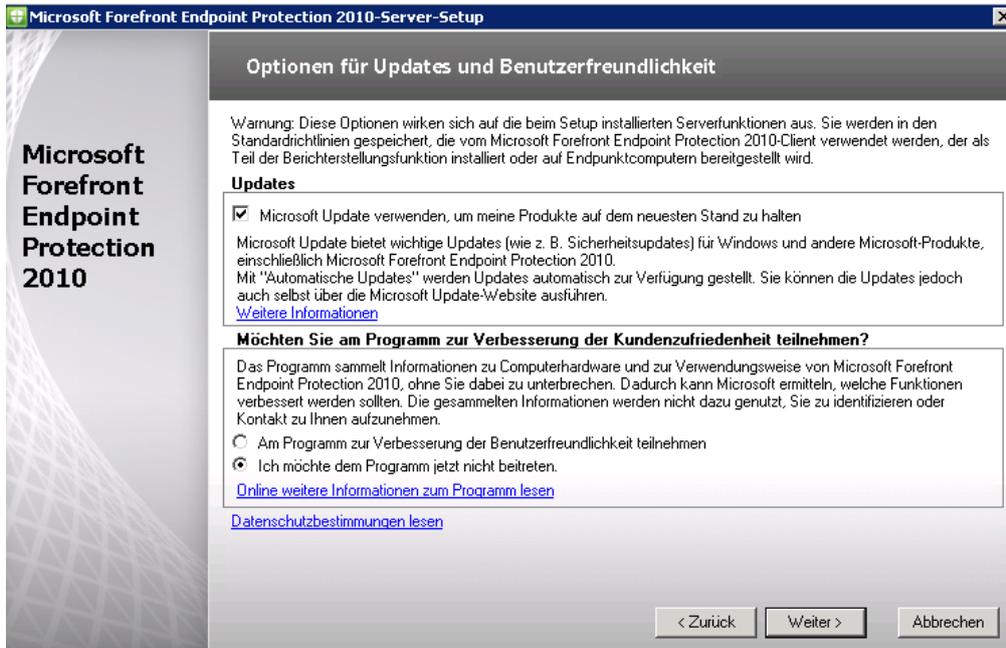
Benutzername (Domäne\Benutzer): [REDACTED]\Administrator

Kennwort: [REDACTED]

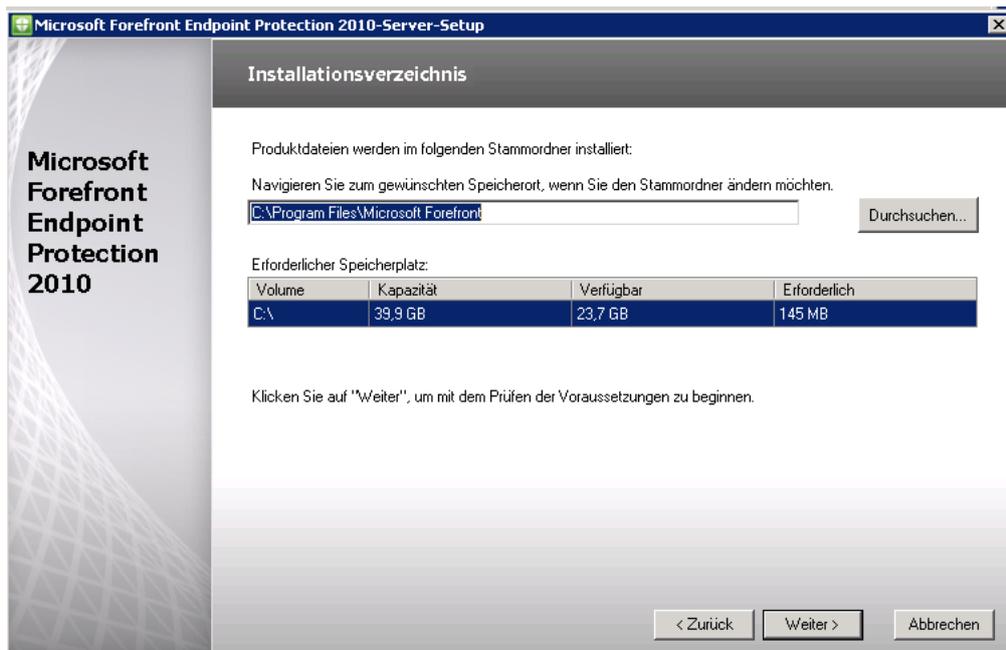
< Zurück Weiter > Abbrechen

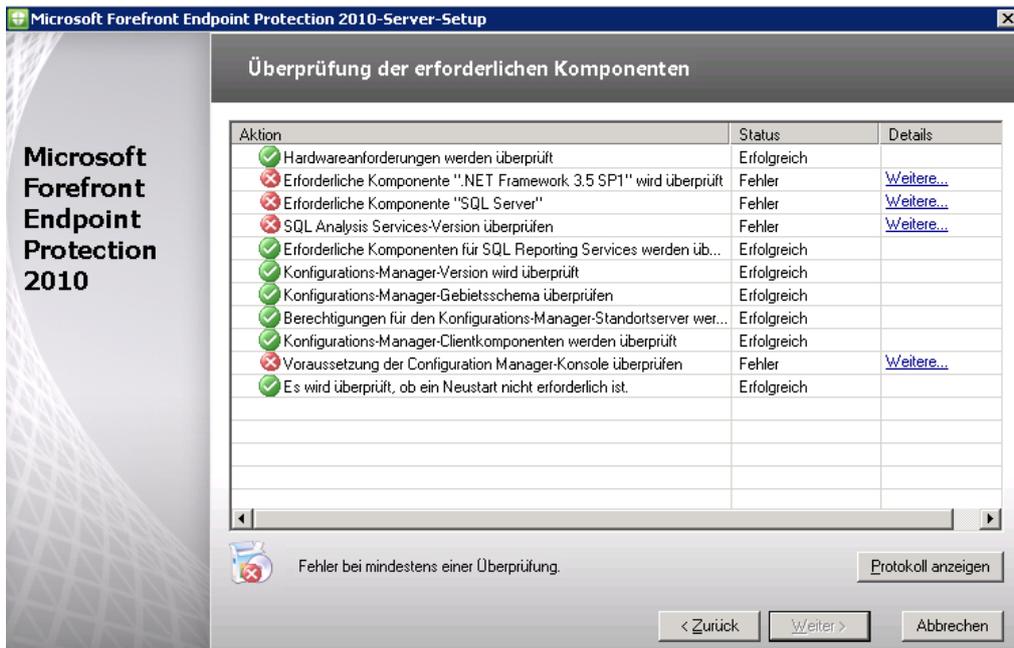
Falls sich die Reporting Services nicht auf einem Windows Server 2008 x64 installieren lassen, könnte das hieran liegen:

<http://support.microsoft.com/kb/894435/en-us>

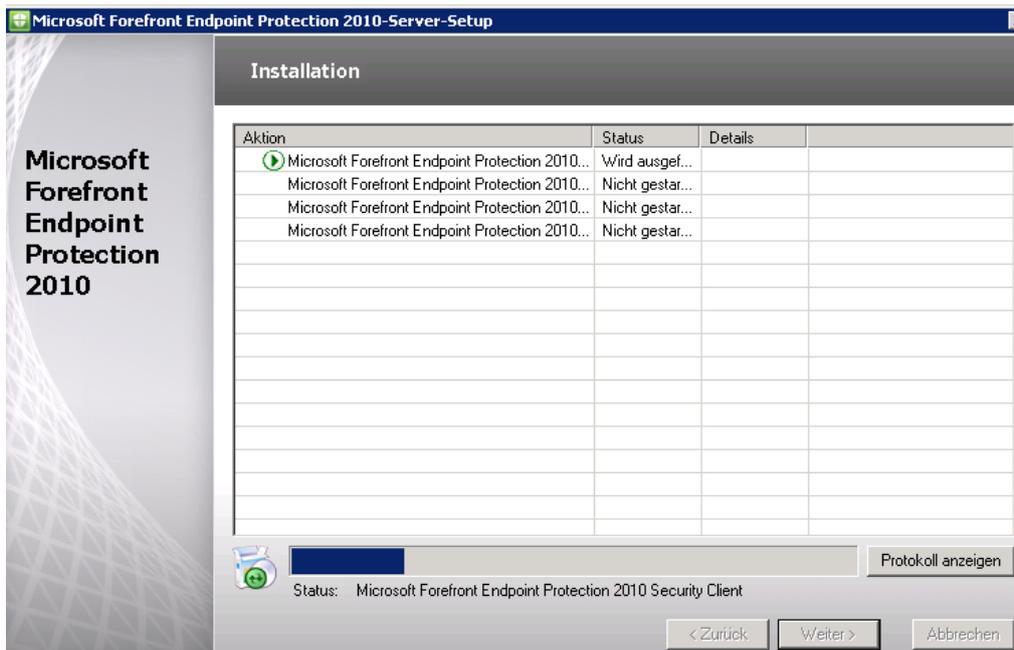


Installationspfad

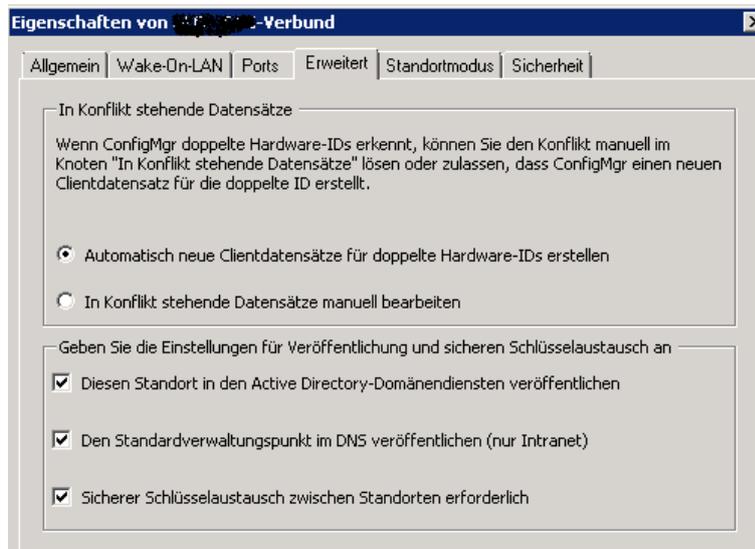




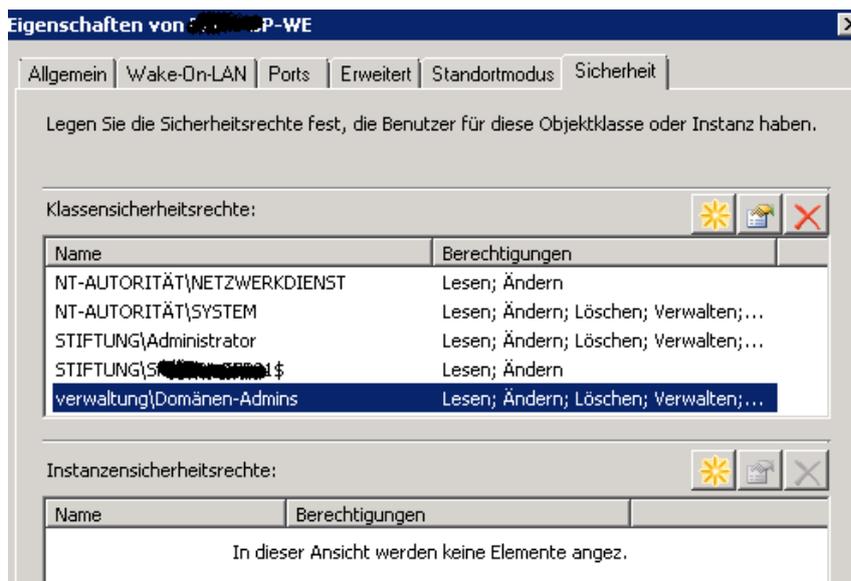
Alle Fehler behoben, dann kann das Setup starten



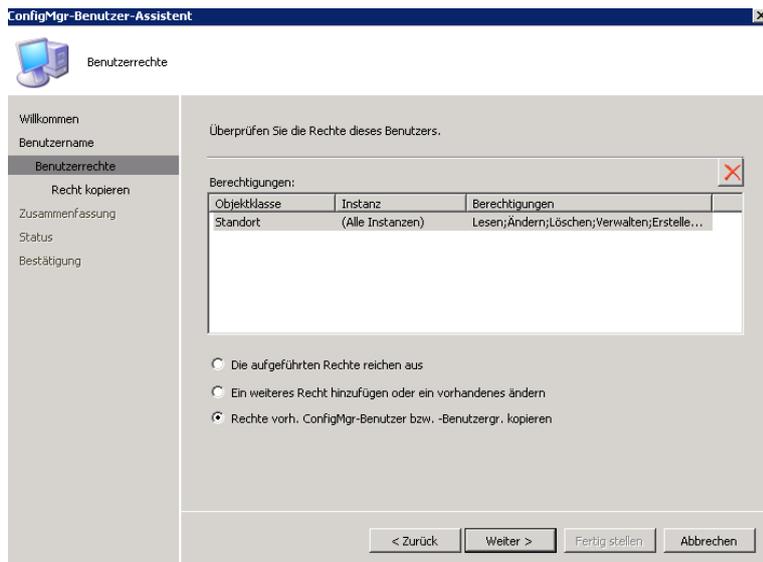
SCCM fuer AD Connection Objekt einstellen



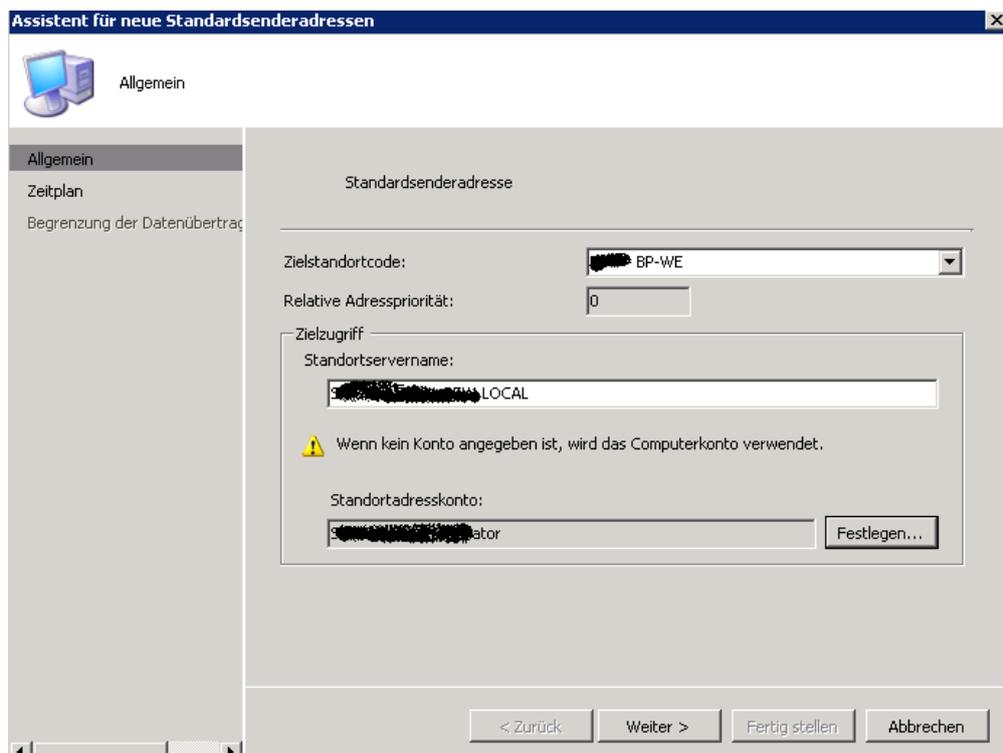
Sicherheitsberechtigungen fuer SCCM Verwaltung aendern



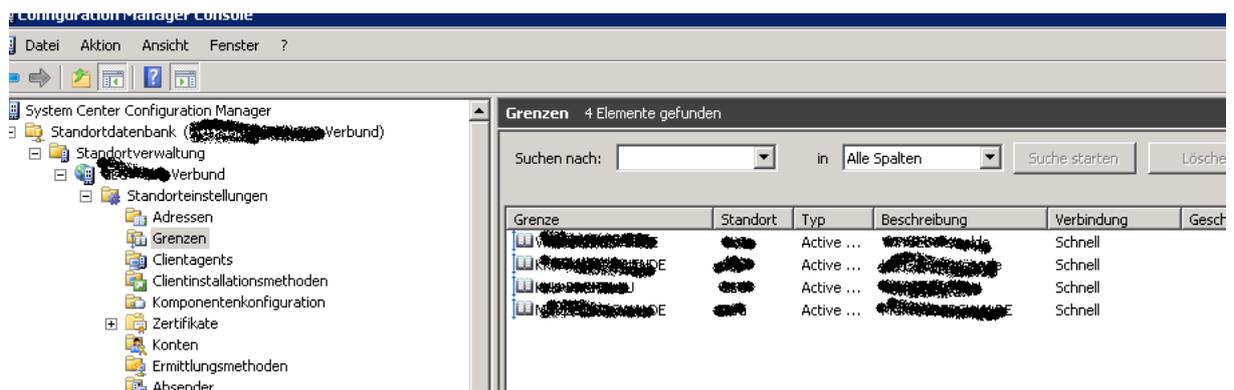
SCCM Berechtigungen eines bestehenden Benutzers uebernehmen



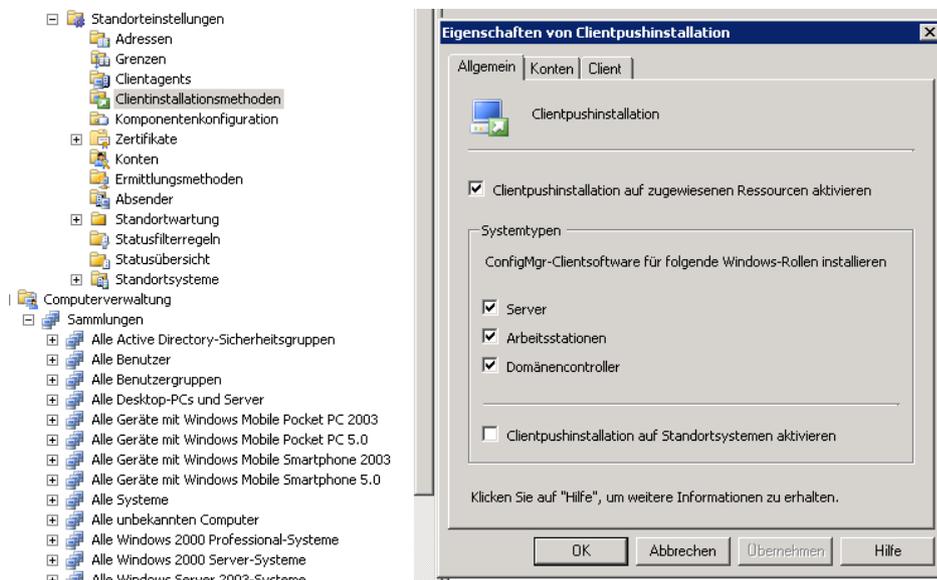
Standardsenderadresse festlegen



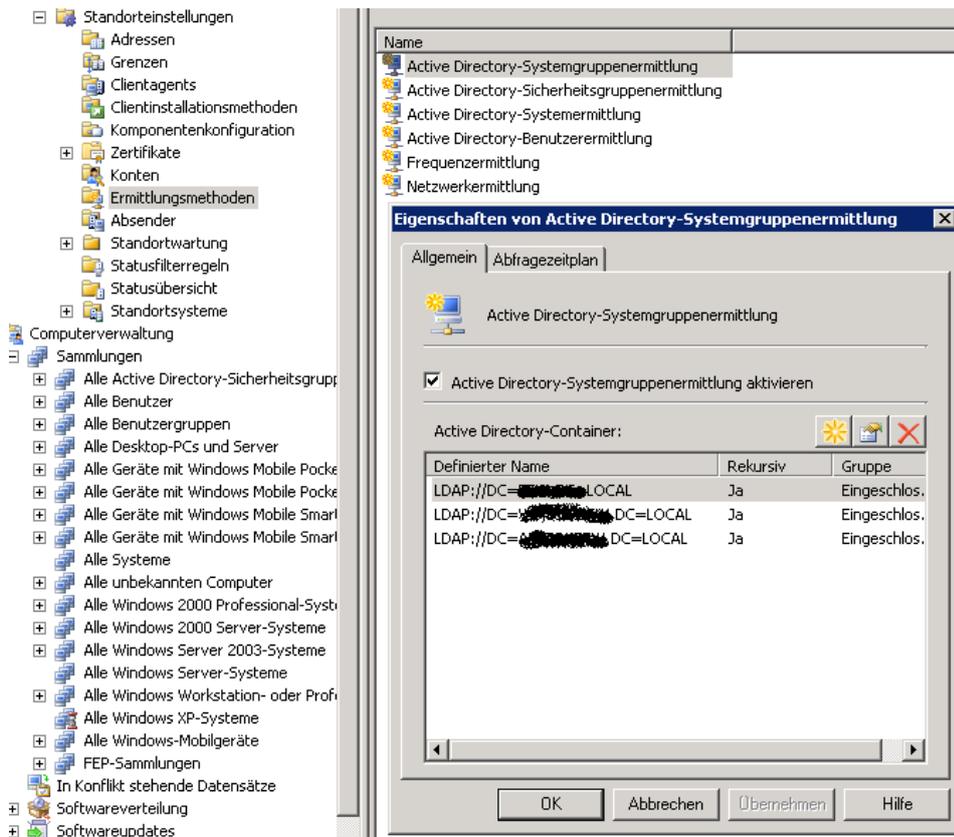
SCCM Sitegrenzen konfigurieren



Client Pushinstallation konfigurieren



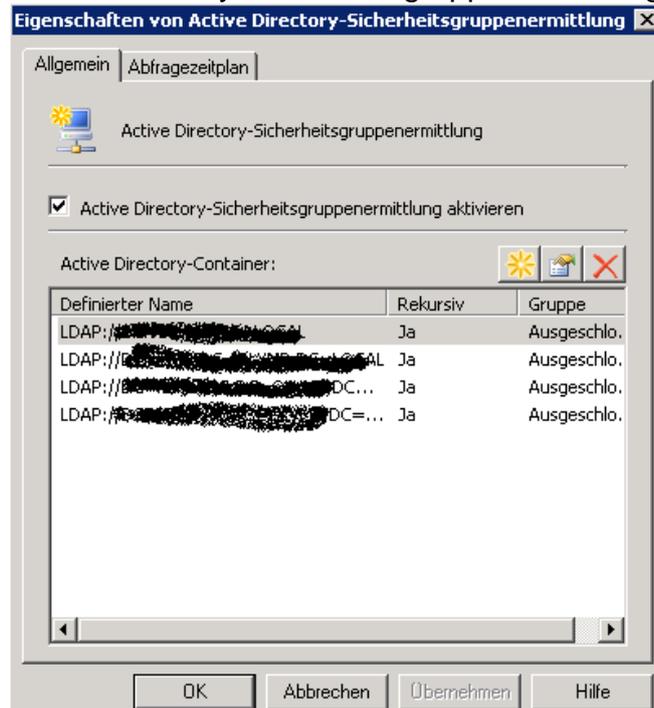
Ermittlungsmethoden konfigurieren



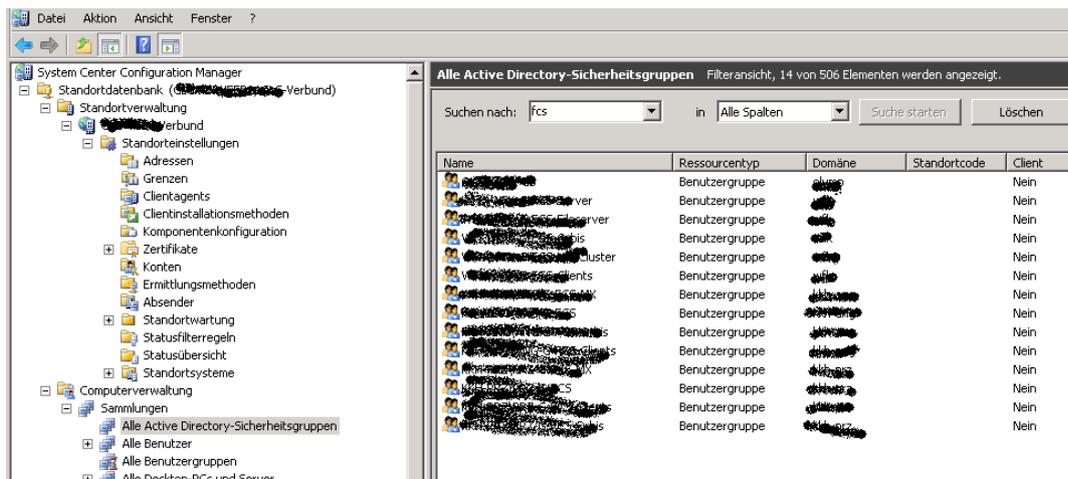
Ggfs. Delta Ermittlung aktivieren

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

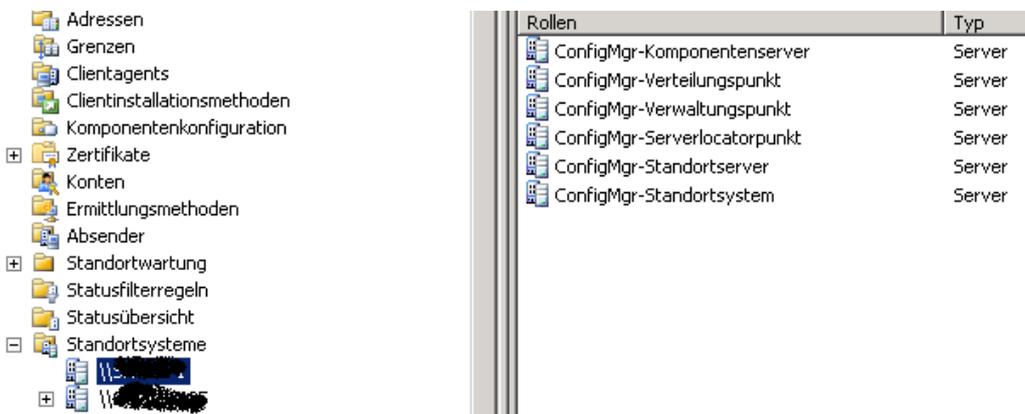
Active Directory Sicherheitsgruppenermittlung aktivieren



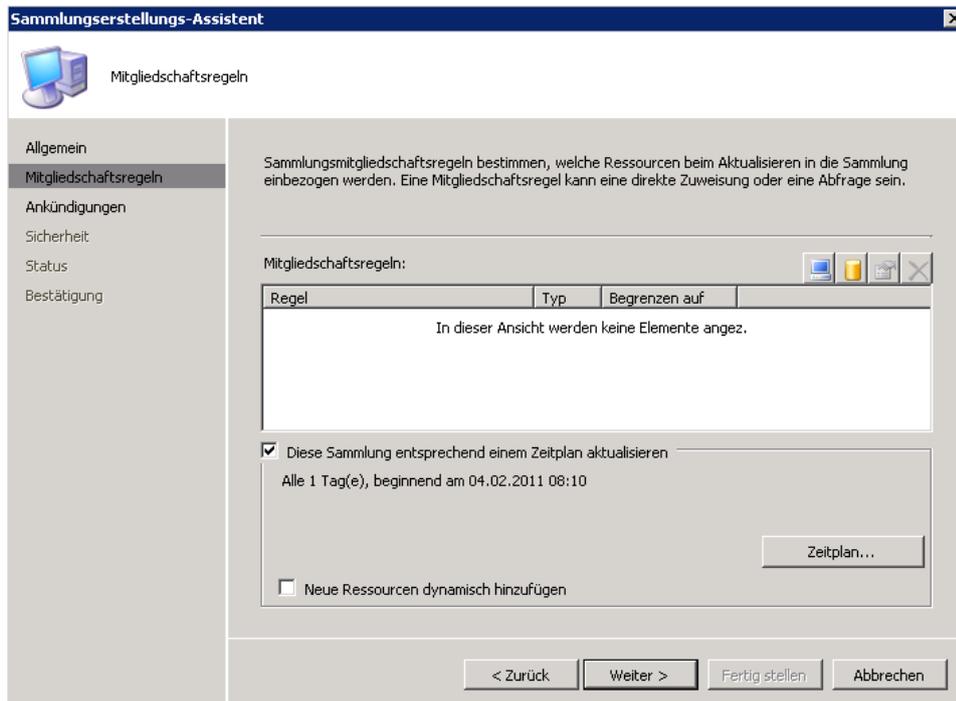
Danach tauchen die Gruppen in der SCCM Konsole auf



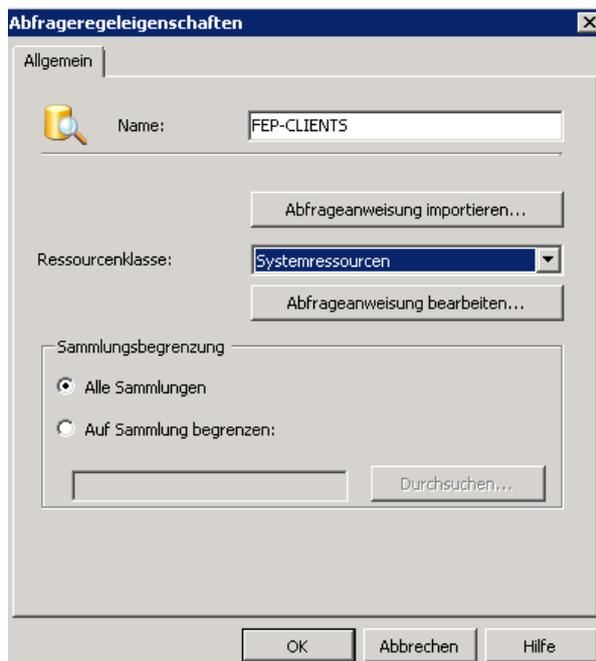
Standortsystemkomponenten

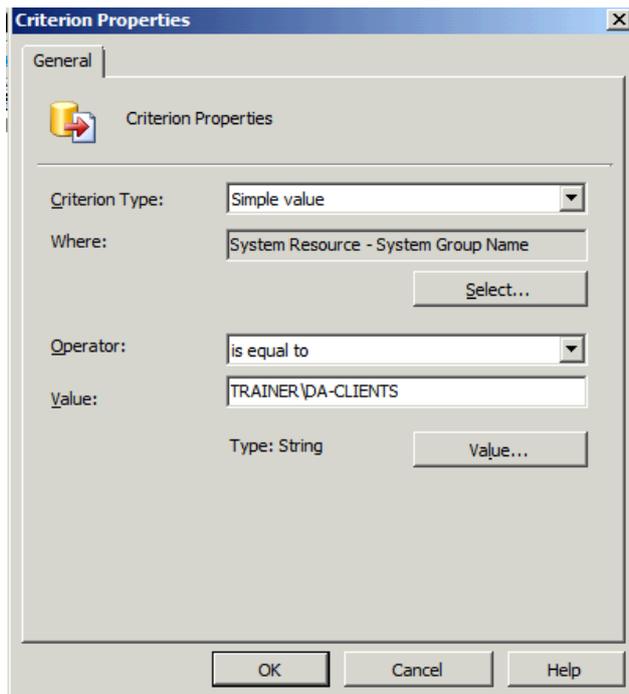


Als naechstes muss eine neue Collection (Sammlung) basierend auf den Gruppenmitgliedschaften erstellt werden

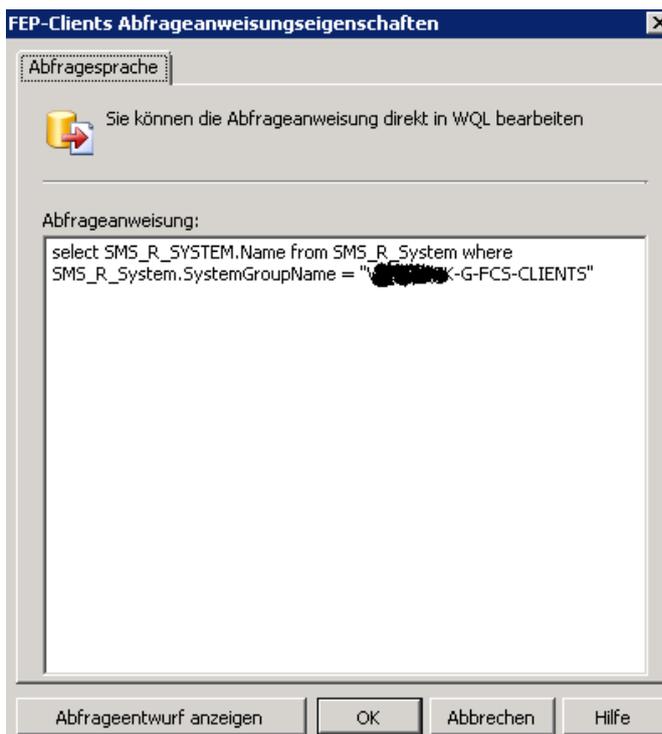


Abfragebasierte Sammlung erstellen

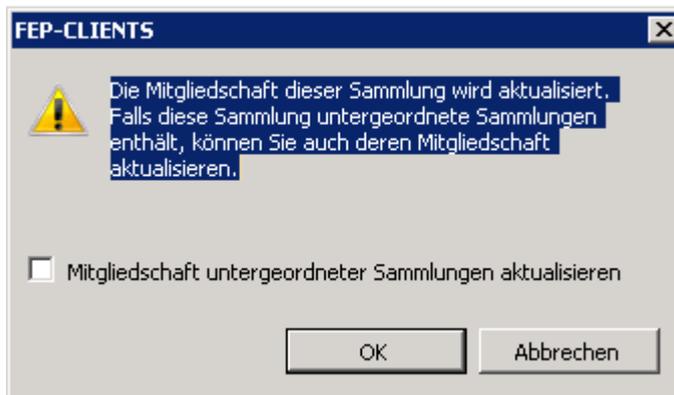




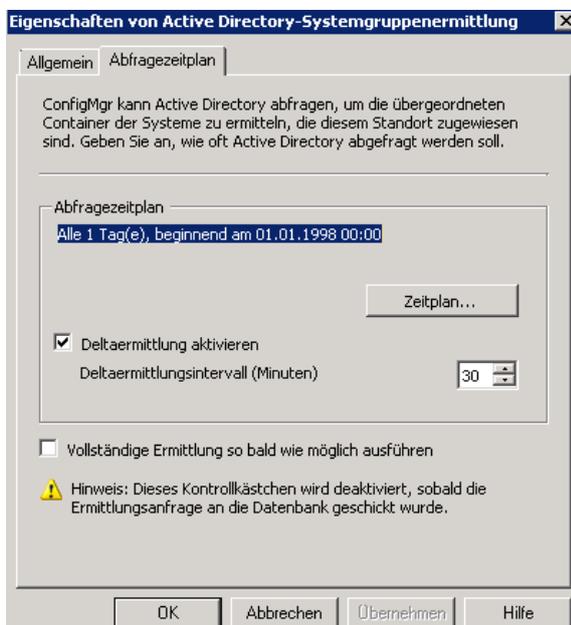
Abfrageanweisung definieren



Sammlungsmemberschaft aktualisieren



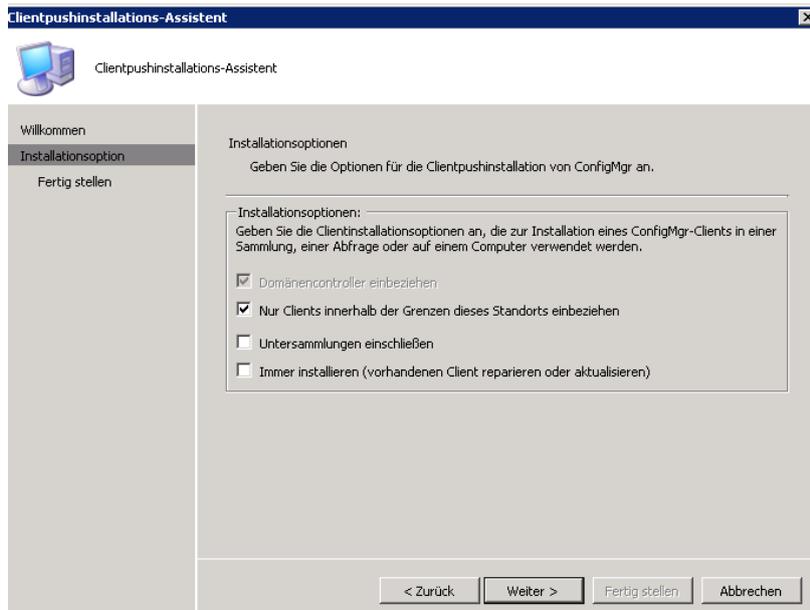
F5 druecken nicht vergessen und Achtung: Wenn neue Windows Gruppen fuer FEP-Clients erstellt werden, im SCCM die Ermittlung der Gruppen manuell anstarten



Client Deployment

Jetzt kann der SCCM Client deployed werden

Rechtsklick auf die Collection und Client deployen



Auf dem Client startet dann das CCM Setup

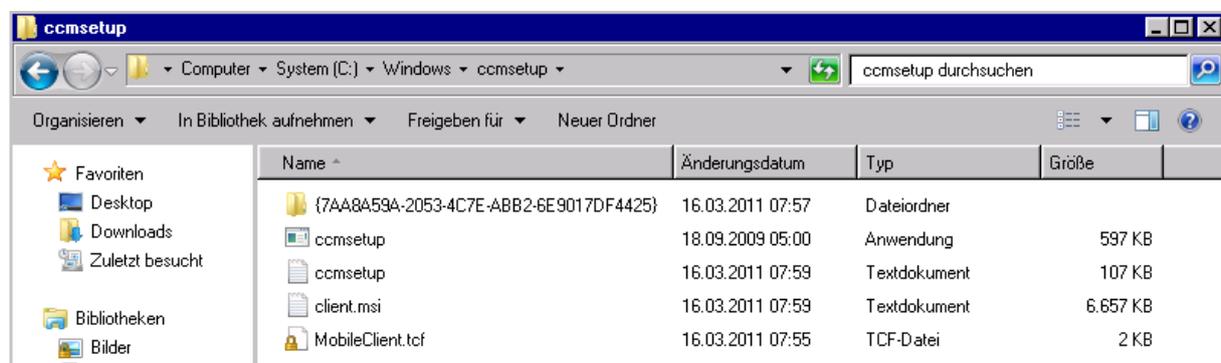


SCCM Dienste

SmartCard	Verwaltet von...	Status	Starttyp	Ort
SMS Agent Host	Provides chan...	Gestartet	Automat...	Lokales System
SMS Task Sequence Agent	SMS client ag...		Manuell	Lokales System

CCM Setup Verzeichnisse

C:\windows\ccmsetup auf 64 Bit Maschinen, c:\windows\system32\ccmsetup auf 32 Bit Maschinen



SCCM Symbole



SCCM Logdateien auf einem 64 Bit System

The screenshot shows a Windows Explorer window titled 'Logs' with the address bar set to 'Computer > System (C:) > Windows > SysWOW64 > CCM > Logs'. The left sidebar shows the 'System (C:)' drive selected. The main pane displays a list of log files with columns for Name, Änderungsdatum, Typ, and Größe.

Name	Änderungsdatum	Typ	Größe
CAS	17.03.2011 13:10	Textdokument	4 KB
CcmExec	17.03.2011 14:12	Textdokument	116 KB
CertificateMaintenance	17.03.2011 14:00	Textdokument	4 KB
CIAgent	17.03.2011 10:01	Textdokument	2 KB
ClientIDManagerStartup	17.03.2011 10:00	Textdokument	115 KB
ClientLocation	17.03.2011 14:12	Textdokument	23 KB
ContentTransferManager	17.03.2011 13:08	Textdokument	4 KB
DataTransferService	17.03.2011 14:08	Textdokument	59 KB
DCMAgent	17.03.2011 10:01	Textdokument	1 KB
execmgr	17.03.2011 13:10	Textdokument	10 KB
FileSystemFile	17.03.2011 10:56	Textdokument	94 KB
InternetProxy	17.03.2011 10:00	Textdokument	1 KB
InventoryAgent	17.03.2011 10:57	Textdokument	56 KB

Manuelle Verteilung des SCCM und FEP Clients

SCCM Client:

CCMSetup.exe /mp:Servername.domaene.tld /logon SMSSITECODE=XYZ

FEP Client:

FEPINSTALL.exe /S /Q

Hier noch was zum Lesen:

<http://technet.microsoft.com/en-us/library/bb680980.aspx>

<http://technet.microsoft.com/en-us/library/gg412485.aspx>

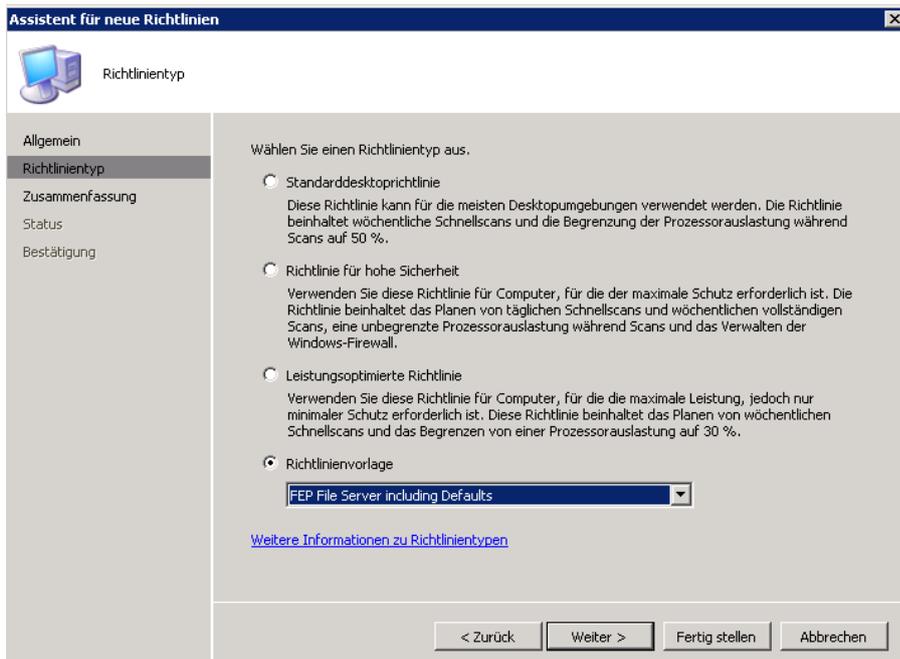
Forefront Endpoint Policy erstellen

The screenshot shows the Group Policy console with the 'Richtlinien' folder selected. The list of policies is as follows:

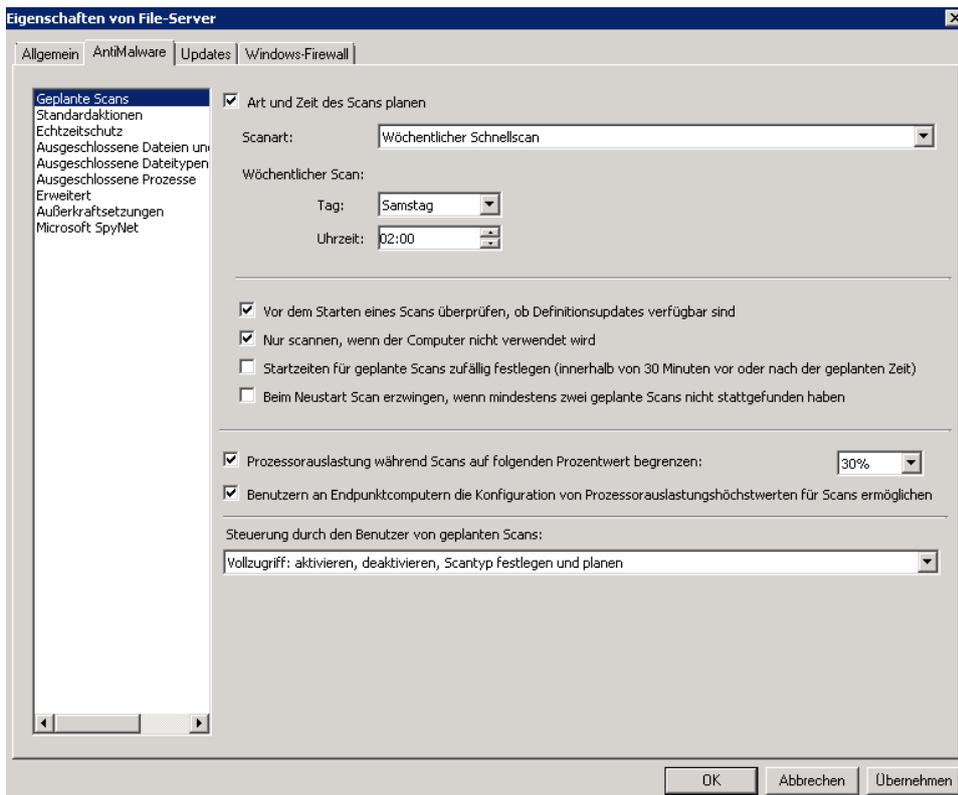
Name	Beschreibung	Rangfolge
Orbis-Server		8 (Höchste)
HydMediaCluster		7
File-Server		6
Exchange		5
Clients		4
Default Server Policy	Diese Richtlinie definiert die Standardeinstellungen für Fo...	2
Default Desktop Policy	Mit dieser Richtlinie werden die Standardeinstellungen für...	1 (Niedrigste)

The 'Assistent für neue Richtlinien' dialog box is shown with the 'Allgemein' tab selected. The 'Richtliniename' field contains 'File-Server' and the 'Beschreibung' field is empty. The navigation buttons at the bottom are '< Zurück', 'Weiter >', 'Fertig stellen', and 'Abbrechen'.

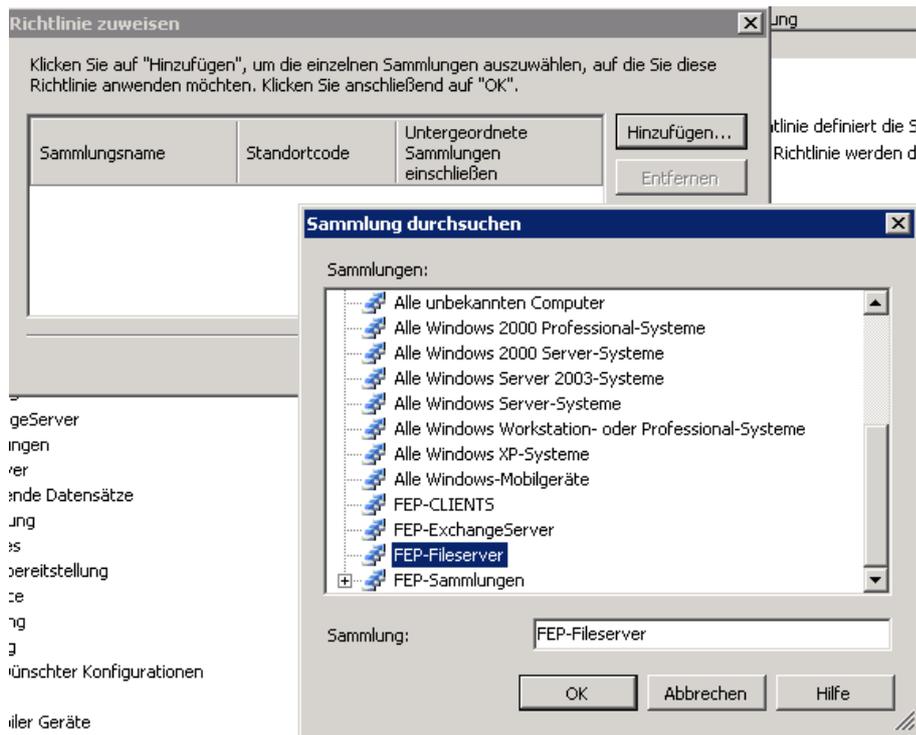
Vorlage auswahlen



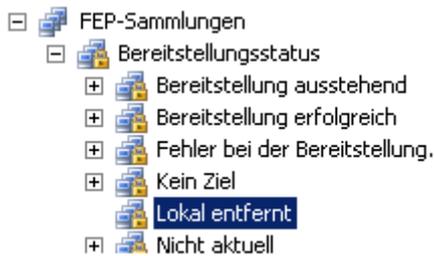
Richtlinie anpassen



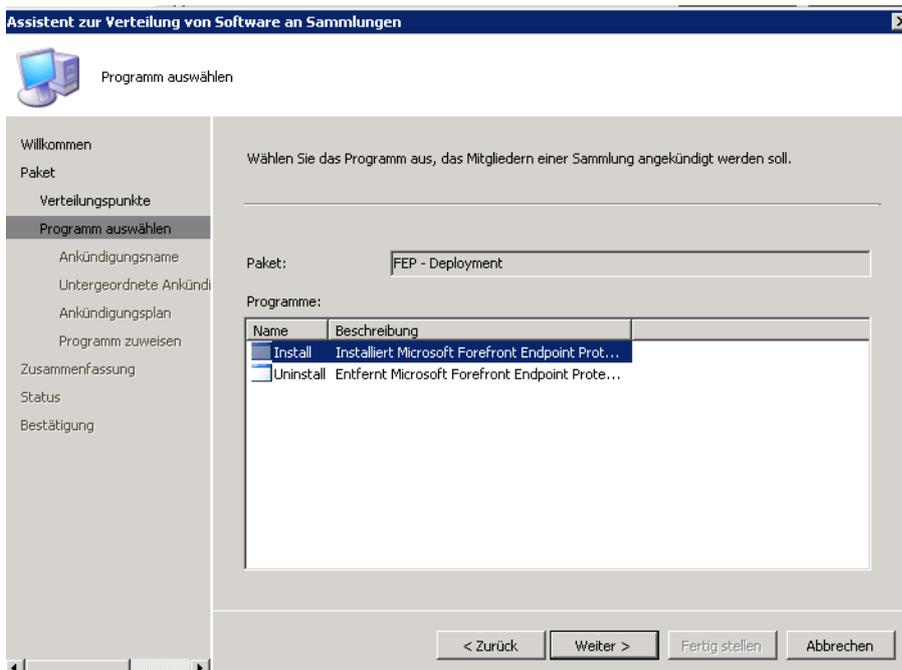
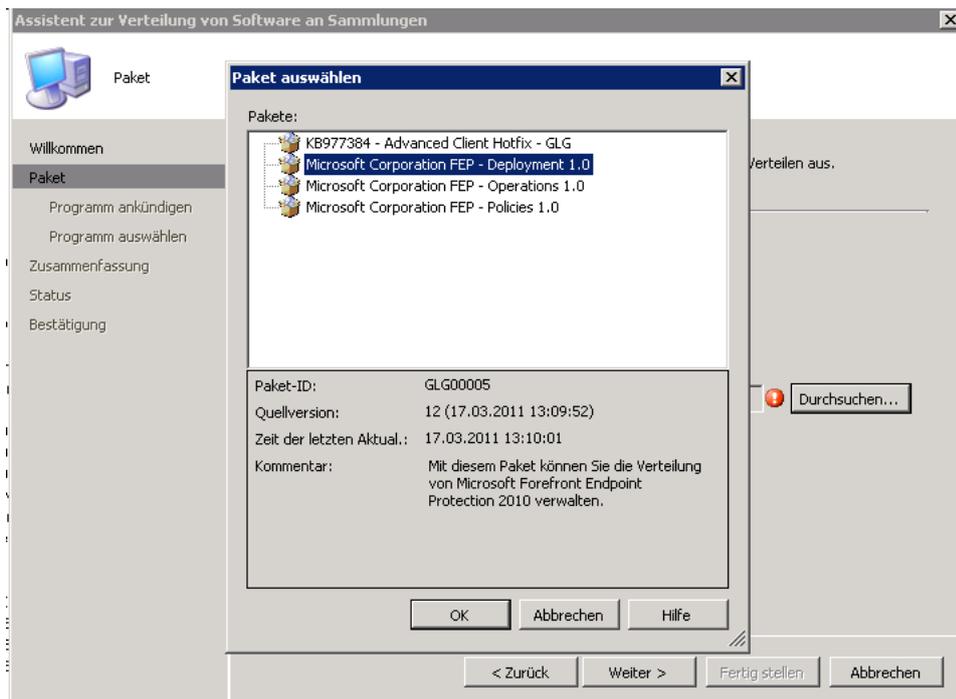
Richtlinie zuweisen



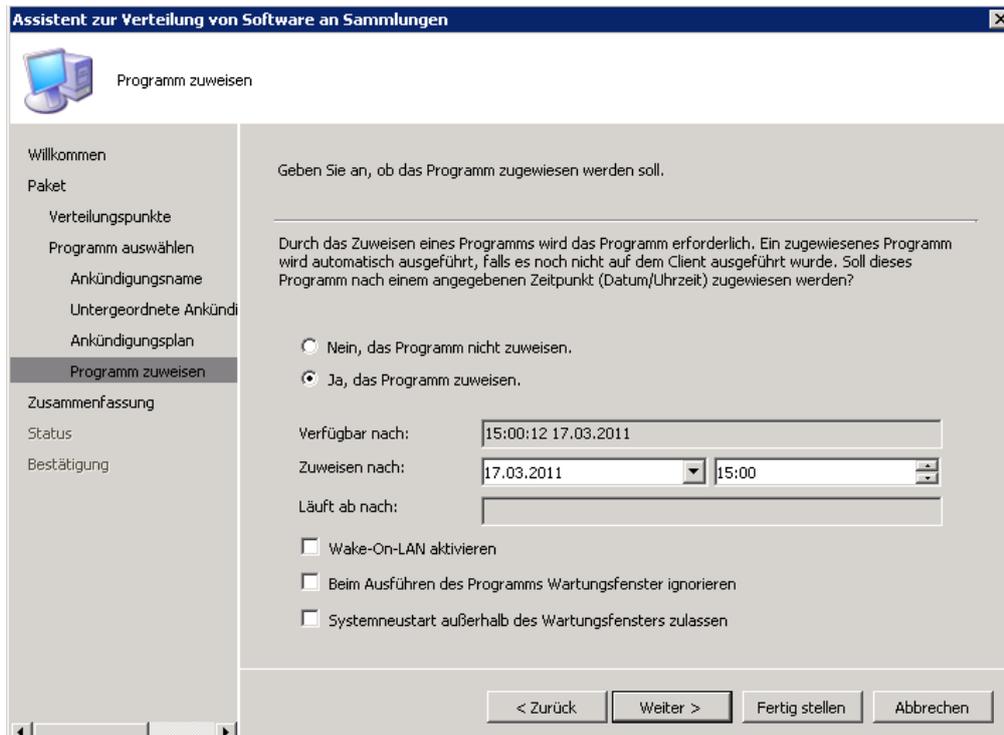
Aus Sicherheitsgründen sollte man die FEP Policy auch der FEP Collection „Lokal entfernt“ zuweisen, falls ein Admin den Client manuell deinstalliert



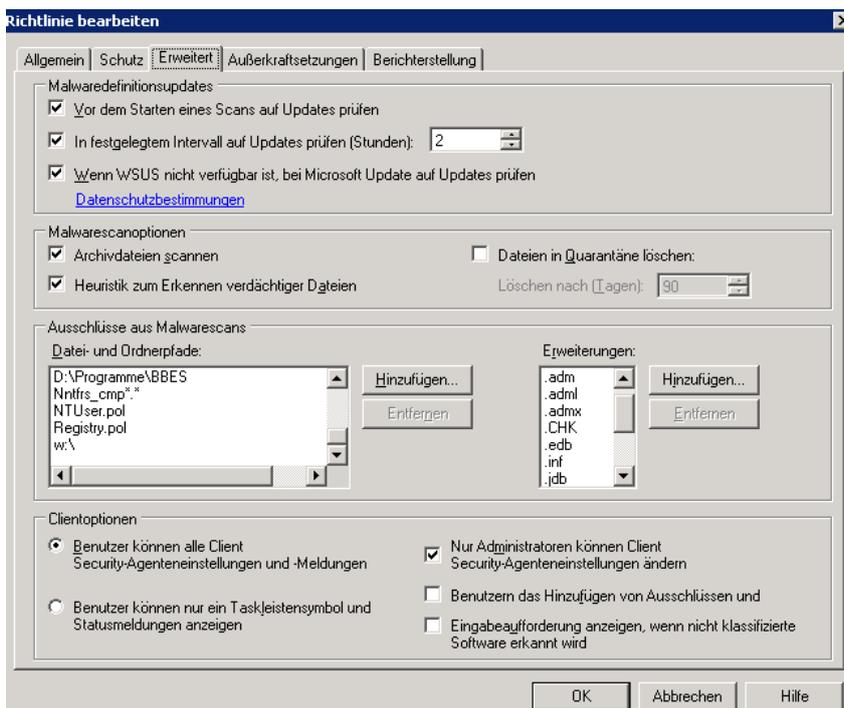
Pakete verteilen



Paket zuweisen

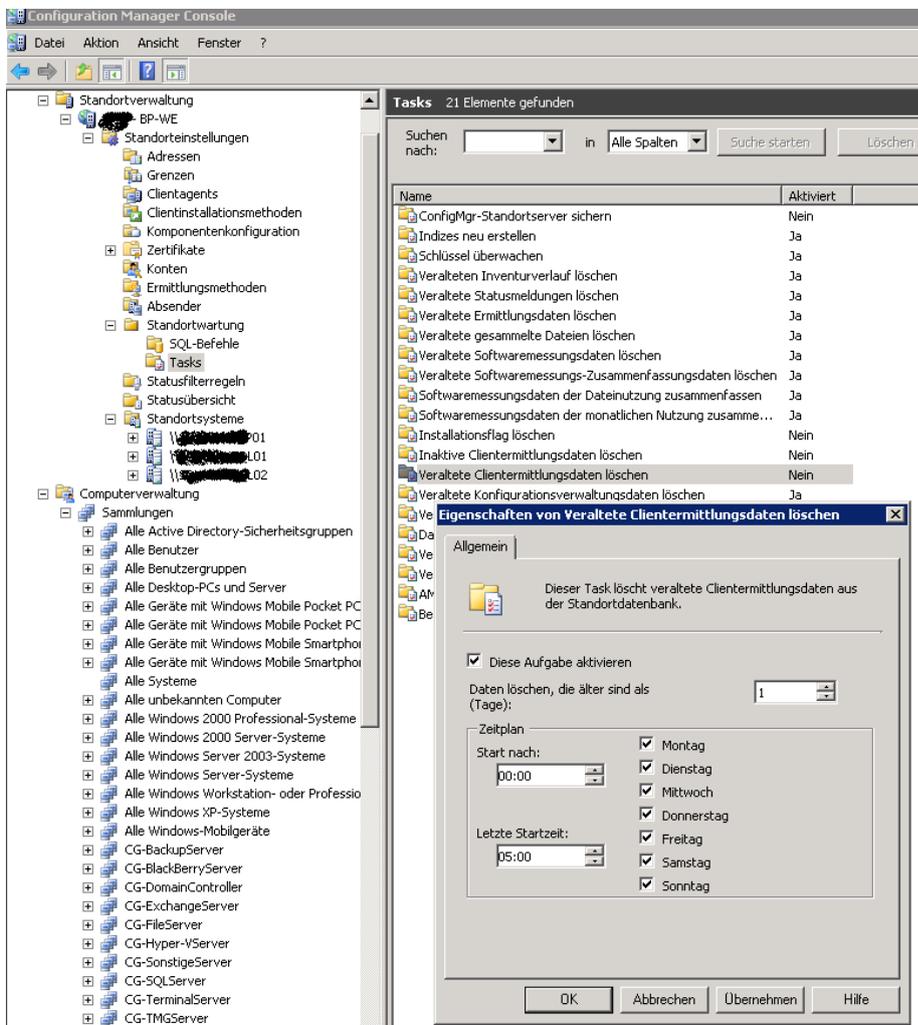
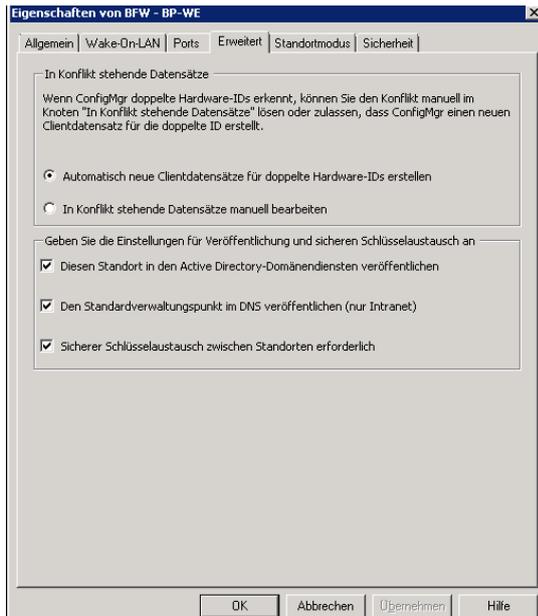


Ggfs. Uebernahme der Custom FCS Einstellungen in den Policies



Veraltete Clientdaten loeschen

Sollte durch eine Neubespilung des Clients der SCCM Client doppelt in der SCCM Verwaltung auftauchen, kann dieser manuell oder automatisch geloescht werden.



FEP Reporting

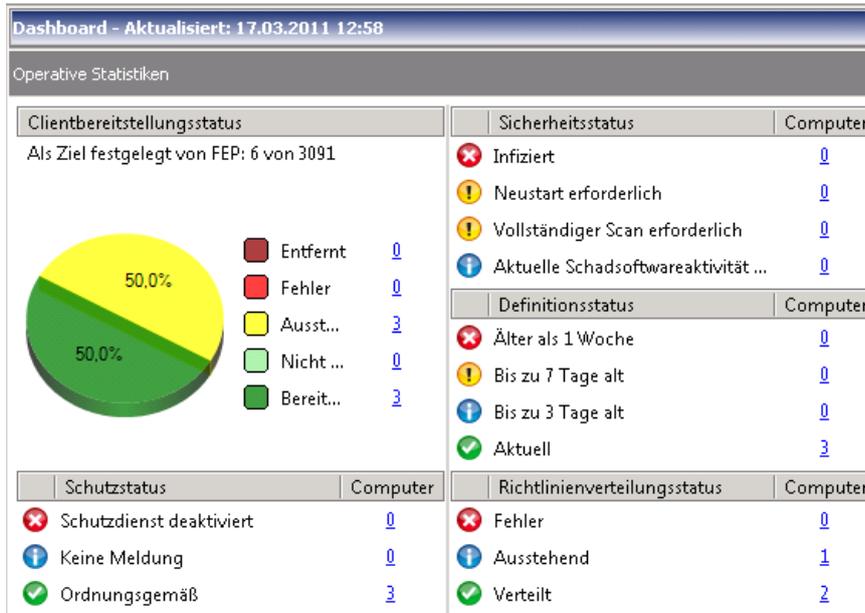
FEP Statistiken aktualisieren

The screenshot displays the Microsoft Forefront Endpoint Protection 2010 console. The main window is titled "Forefront Endpoint Protection" and contains a dashboard with the following sections:

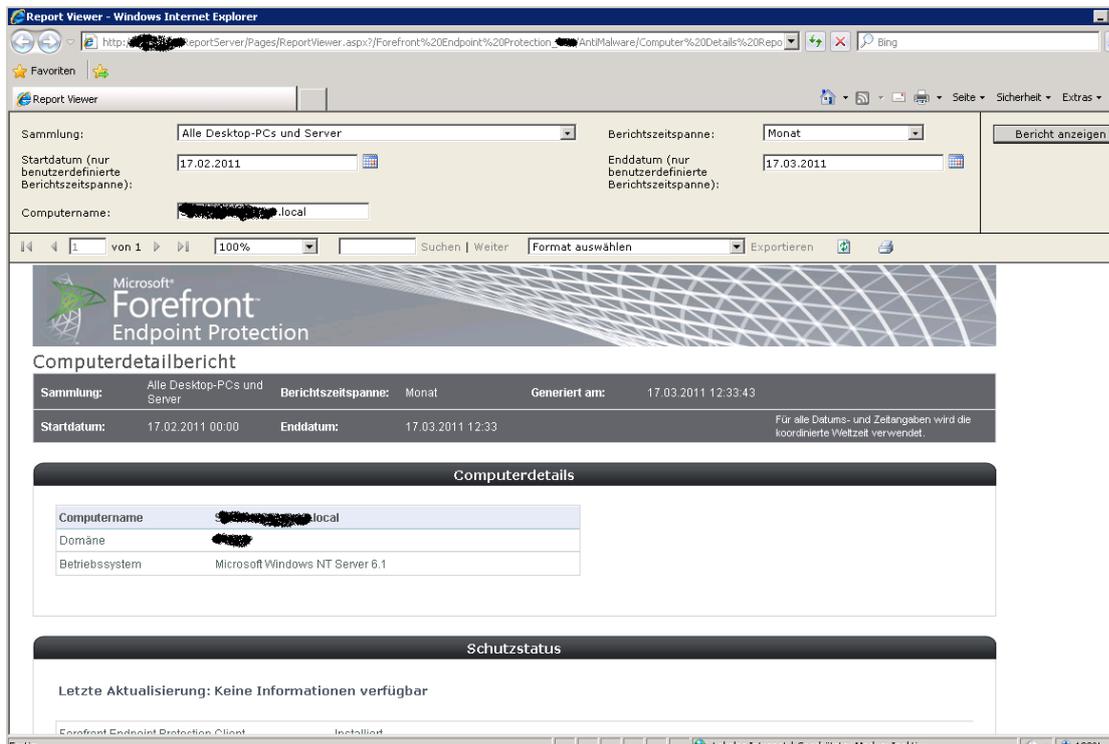
- Operative Statistiken:**
 - Clientbereitstellungszustand:** Als Ziel festgelegt von FEP: 3 von 3091. A pie chart shows 100.0% completion.
 - Sicherheitsstatus:**
 - Infiziert: 0
 - Neustart erforderlich: 0
 - Vollständiger Scan: 0
 - Aktuelle Schadsoft: 0
 - Definitionsstatus:**
 - Älter als 1 Woche: 0
 - Bis zu 7 Tage alt: 0
 - Bis zu 3 Tage alt: 3
 - Aktuell: 3
- Schutzstatus:**
 - Schutzdienst deaktiviert: 0
 - Keine Meldung: 0
- Richtlinienverteilung:**
 - Fehler: 0
 - Ausstehend: 0

An update notification dialog box is overlaid on the console, titled "Microsoft Forefront Endpoint Protection 2010". The text in the dialog reads: "Die Mitgliedschaft der FEP-Sammlungen wird aktualisiert. Dieses Update kann einige Zeit in Anspruch nehmen. Bis die Sammlungen vollständig aktualisiert sind, können in der angezeigten Betriebsstatistik Abweichungen auftreten. Sie müssen nach dem Update möglicherweise die Anzeige aktualisieren, damit die richtigen Daten angezeigt werden." The dialog has "OK" and "Abbrechen" buttons.

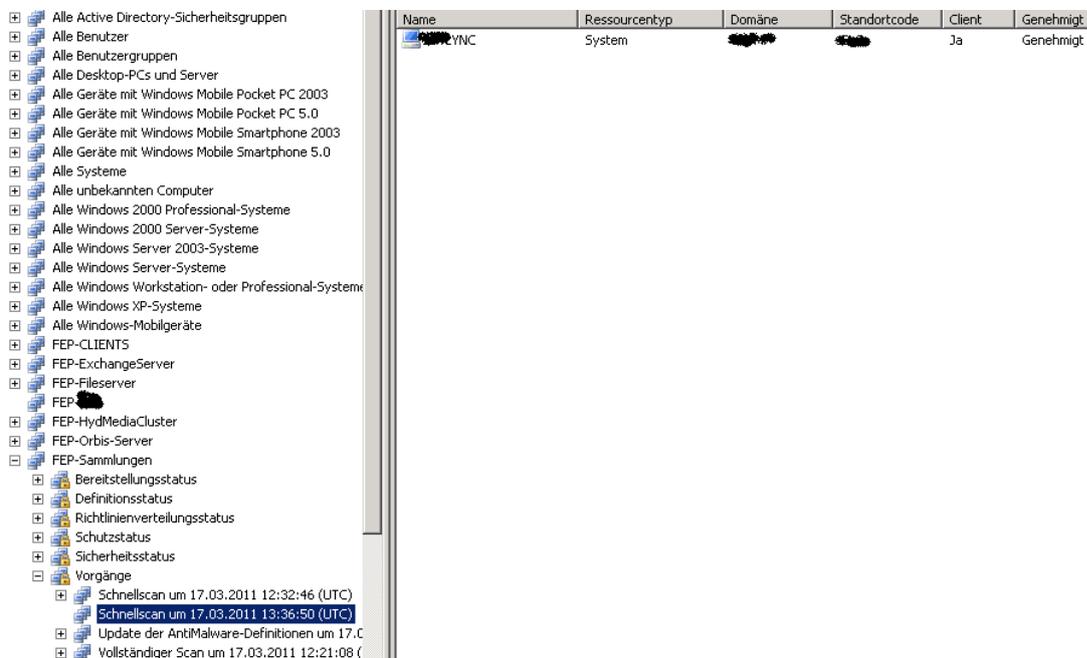
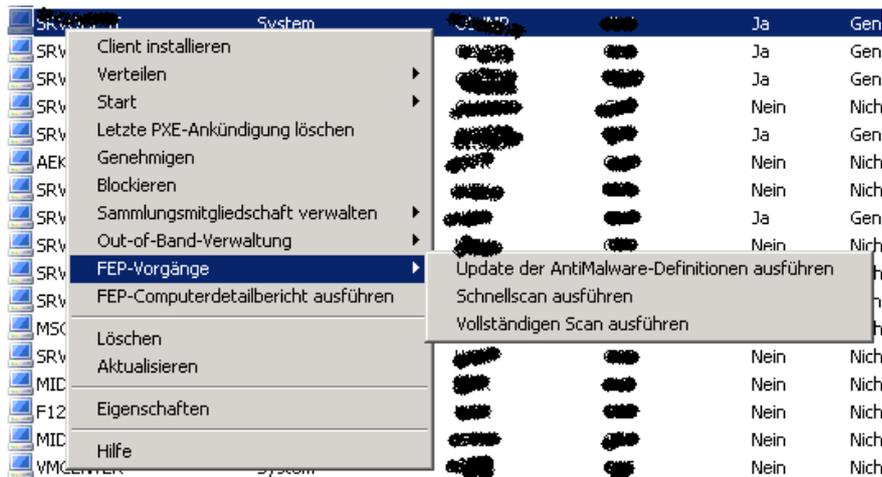
Die Statistik füllt sich mit Leben. Schon auf fast 6 Servern/Clients FEP ausgerollt 😊



Zusammenfassungsreport eines Servers / Clients



FEP Scans und Updates manuell ausführen



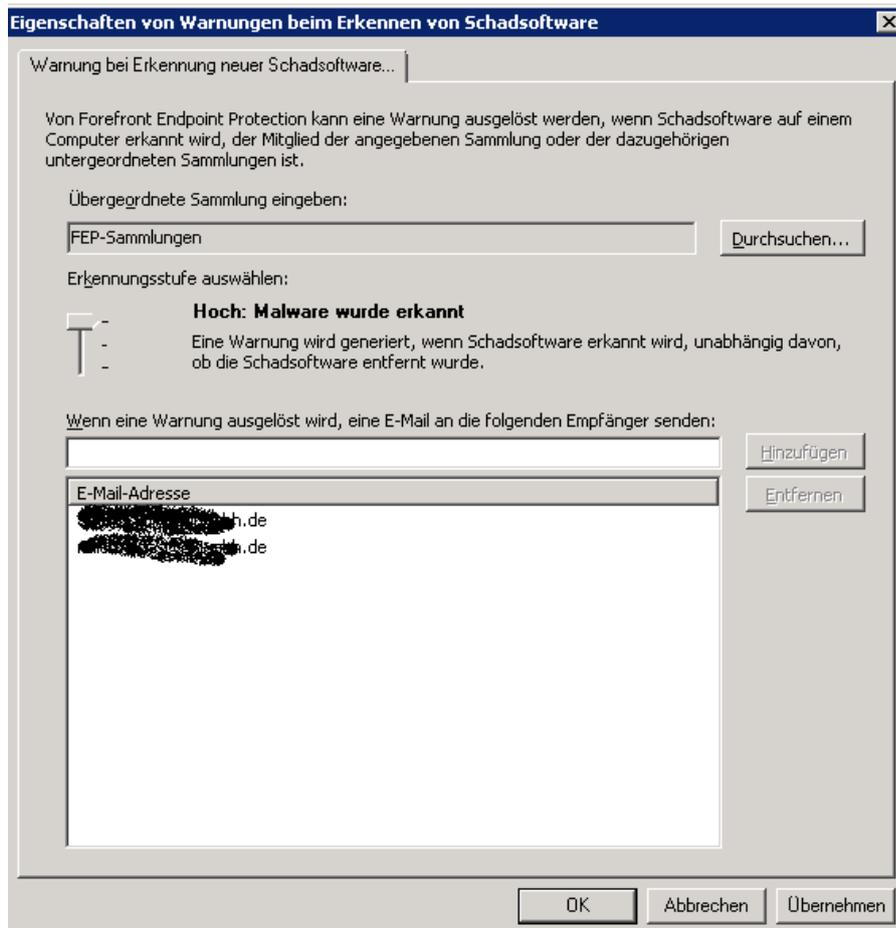
Fuer jeden manuellen FEP Vorgang werden entsprechende Advertisements erstellt

The screenshot shows the Windows System Center console. On the left is a tree view of the environment, including 'Alle Windows-Mobilgeräte', 'FEP-CLIENTS', 'FEP-ExchangeServer', 'FEP-Fileserver', 'FEP-HydMediaCluster', 'FEP-Orbis-Server', 'FEP-Sammlungen', 'Bereitstellungsstatus', 'Definitionsstatus', 'Richtlinienverteilungsstatus', 'Schutzstatus', 'Sicherheitsstatus', 'Aktuelle Schadssoftwareaktivität', 'Infiziert', 'Neustart erforderlich', 'Vollständiger Scan erforderlich', 'Vorgänge', 'In Konflikt stehende Datensätze', 'Softwareverteilung', 'Pakete', 'Ankündigungen', 'FEP-Richtlinien', and 'FEP-Vorgänge'. On the right is a list of scan events:

<input type="checkbox"/>	Schnellscan um 17.03.2011 12:32:46 (UTC)	Microsoft Corporation F...	Quick Scan	Schnellscan um 17.03.2011 12:32:46 (UTC)	1
<input type="checkbox"/>	Schnellscan um 17.03.2011 13:36:50 (UTC)	Microsoft Corporation F...	Quick Scan	Schnellscan um 17.03.2011 13:36:50 (UTC)	1
<input type="checkbox"/>	Schnellscan um 17.03.2011 13:41:01 (UTC)	Microsoft Corporation F...	Quick Scan	Schnellscan um 17.03.2011 13:41:01 (UTC)	1
<input type="checkbox"/>	Update der AntiMalware-Definitionen um 17.03.2011 12:21:08 (UTC)	Microsoft Corporation F...	Update Definitions	Update der AntiMalware-Definitionen um 17.03.2011 12:21:08 (UTC)	1
<input type="checkbox"/>	Vollständiger Scan um 17.03.2011 12:21:08 (UTC)	Microsoft Corporation F...	Full Scan	Vollständiger Scan um 17.03.2011 12:21:08 (UTC)	1

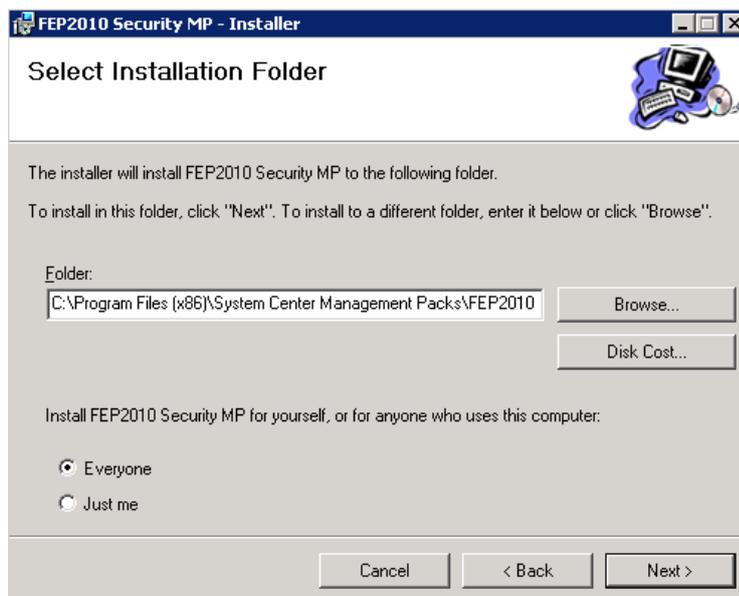
Warnungsbenachrichtigung einrichten

The screenshot shows the 'E-Mail-Einstellungen' dialog box. The 'E-Mail-Warnungsbenachrichtigung' checkbox is checked. The 'SMTP-Server (FQDN):' field contains '[REDACTED].local' and the 'Port:' field contains '25'. The 'Authentifizierungsmethode:' section has 'Anonym' unselected and 'Windows-integriert' selected. The 'E-Mail-Absenderadresse:' field contains '[REDACTED].local'. At the bottom are buttons for 'Testen und schließen...', 'OK', and 'Abbrechen'.



SCOM – FEP Integration

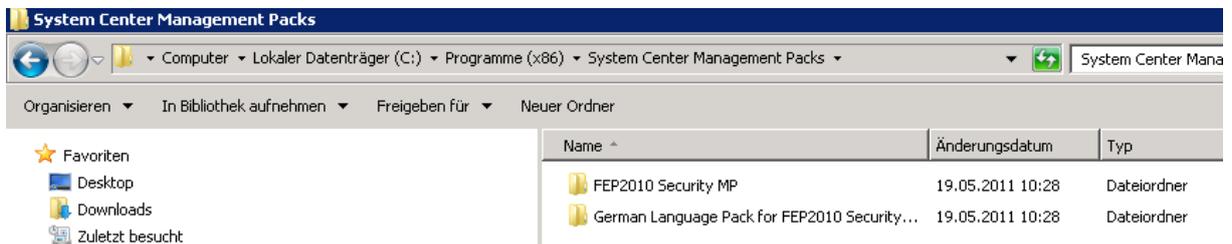
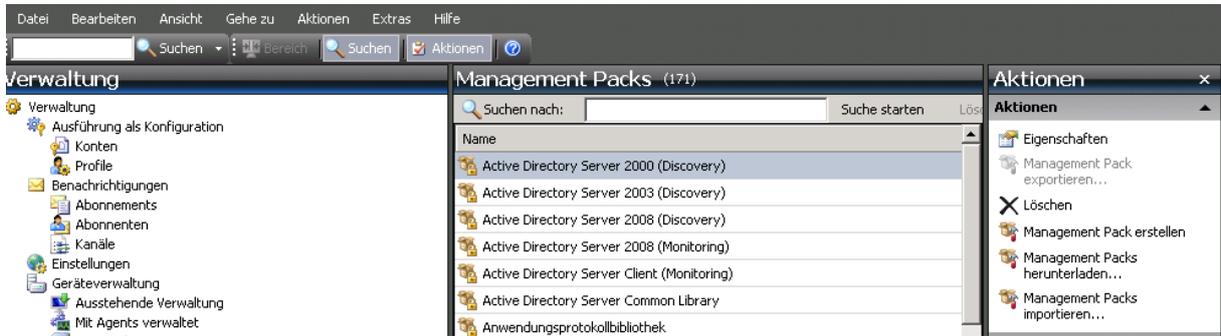
SCOM Management Pack fuer FEP installieren



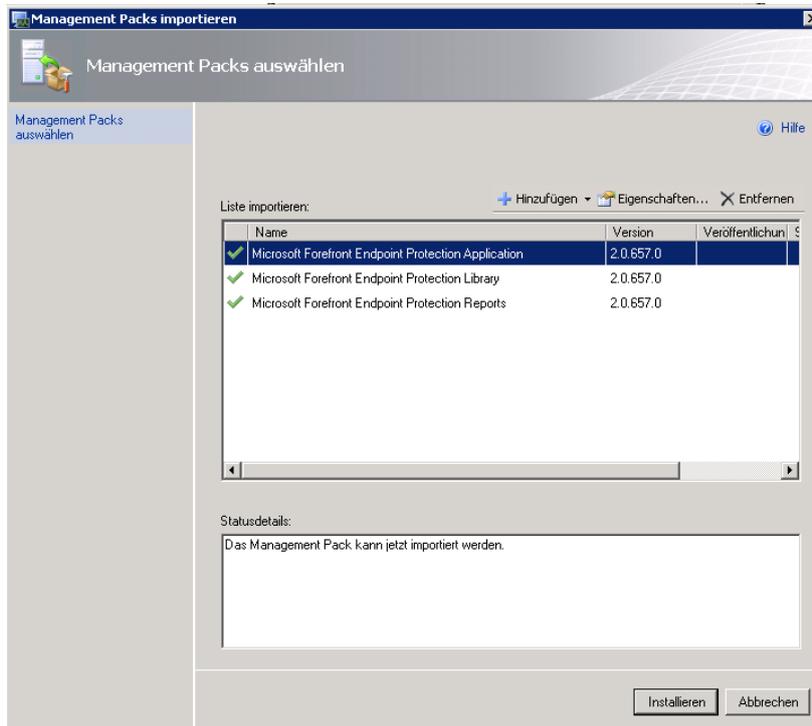
Language Pack fuer FEP installieren

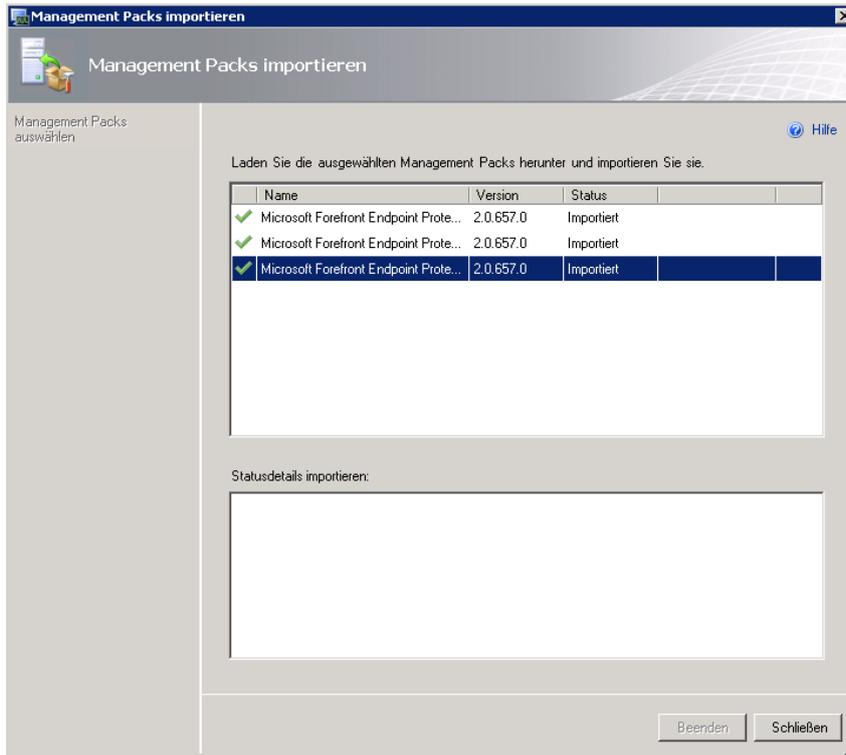
SCOM Operationskonsole starten

Management Pack importieren

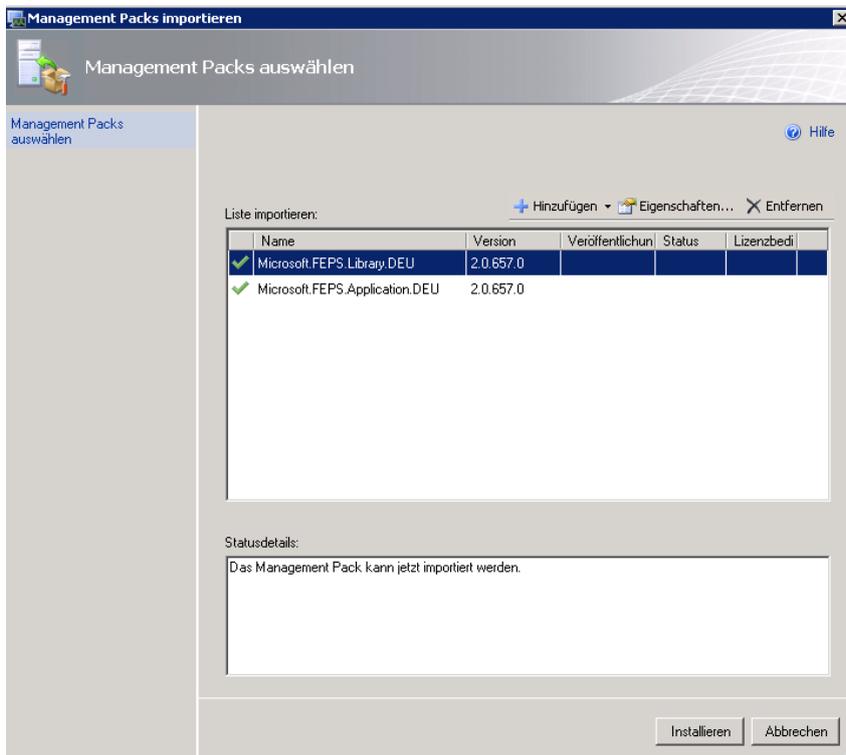


Alle drei MPs importieren





MP Language Pack importieren



FEP Monitoring

The screenshot shows the 'System Center Operations Manager 2007 R2' interface. The left pane displays a tree view under 'Überwachung' with 'Forefront Endpoint Protection' expanded. The right pane, titled 'Aktive Warnungen (15)', lists the following warnings:

- Schweregrad: Kritisch (2)**
 - SRV-...502...: Keine Definitionen vorhanden
 - SRV-...502...: AntiMalware-Modulfehler
- Schweregrad: Warnung (1)**
 - SRV-...502...: Echtzeitschutz deaktiviert
- Schweregrad: Informationen (12)**
 - SRV-...01...: Forefront Endpoint Protection-Client
 - SRV-...01...: Forefront Endpoint Protection-Client
 - SRV-...01...: Forefront Endpoint Protection-Client
 - SRV-...50...: Forefront Endpoint Protection-Client
 - SRV-...01...: Forefront Endpoint Protection-Client

Berichte

The screenshot shows a 'Computerlistenbericht' (Computer List Report) for 'Forefront Endpoint Protection'. The report is generated on 19.05.2011 13:24:53, covering the period from 12.05.2011 00:00 to 19.05.2011 13:24. It displays a table with 381 entries (showing 100).

Computername	Schutzstatus	Sicherheitsstatus	Definitionsversion	Erste Erkennung	Letzte Erkennung	Letzter gesendeter Status
...	Der Client ist nicht bereitgestellt.	Nicht aktualisiert.				19.05.2011 00:00
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 08:51
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 08:36
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 08:54
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 08:51
...	Der Client ist nicht bereitgestellt.	Nicht aktualisiert.				19.05.2011 00:00
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:28
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:31
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 08:59
...	Der Client ist nicht bereitgestellt.	Nicht aktualisiert.				19.05.2011 00:00
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:40
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:35
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:38
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:27
...	Echtzeitschutz aktiviert	Bereinigen	1.105.32.0			19.05.2011 09:52
...	Der Client ist nicht bereitgestellt.	Nicht aktualisiert.				19.05.2011 00:00

Administrationskonsole auf Admin PCs installieren

Microsoft System Center Configuration Manager 2007 SP2

Verfügbare Setupoptionen

Beim Setup wurden die verfügbaren Installationsoptionen basierend auf dem installierten Betriebssystem und den vorhandenen Systems Management Server 2003-Installationen oder Configuration Manager-Installationen aktiviert.

Es wurde auf diesem Computer keine Installation eines primären Standortservers, sekundären Standortservers, Standortsystems oder einer Configuration Manager-Konsole gefunden.

Auf diesem Computer können Sie keine primären oder sekundären Standortserverkomponenten installieren, da dies kein Server in einer Windows-Domäne ist.

Configuration Manager-Standortserver installieren

Vorhandene Configuration Manager- oder SMS 2003-Installation aktualisieren

Administratorkonsole installieren bzw. aktualisieren

Standortwartung durchführen oder diesen Standort zurücksetzen

Configuration Manager-Standortserver deinstallieren

< Zurück Weiter > Abbrechen

Microsoft System Center Configuration Manager 2007 SP2

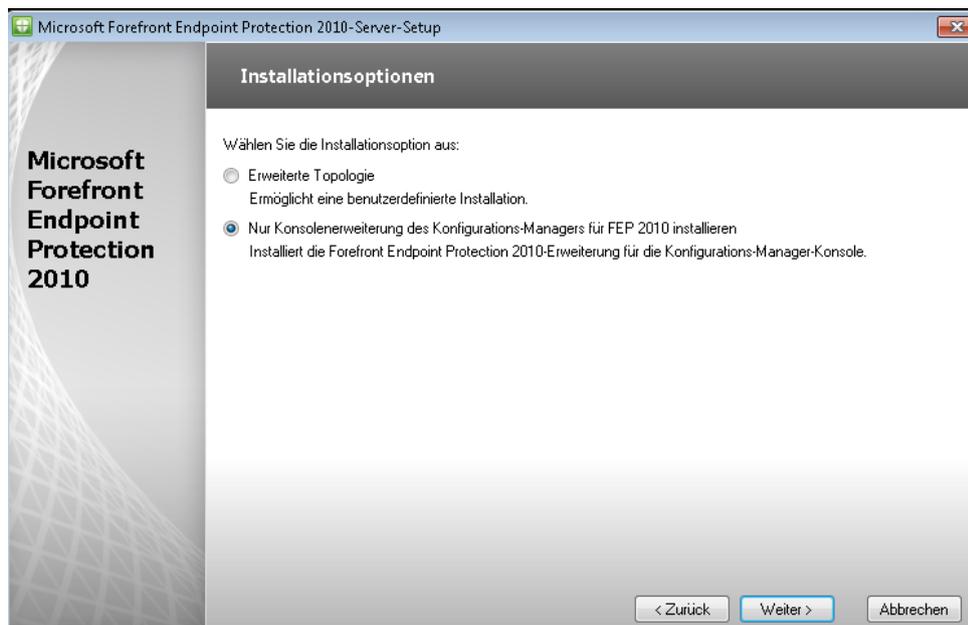
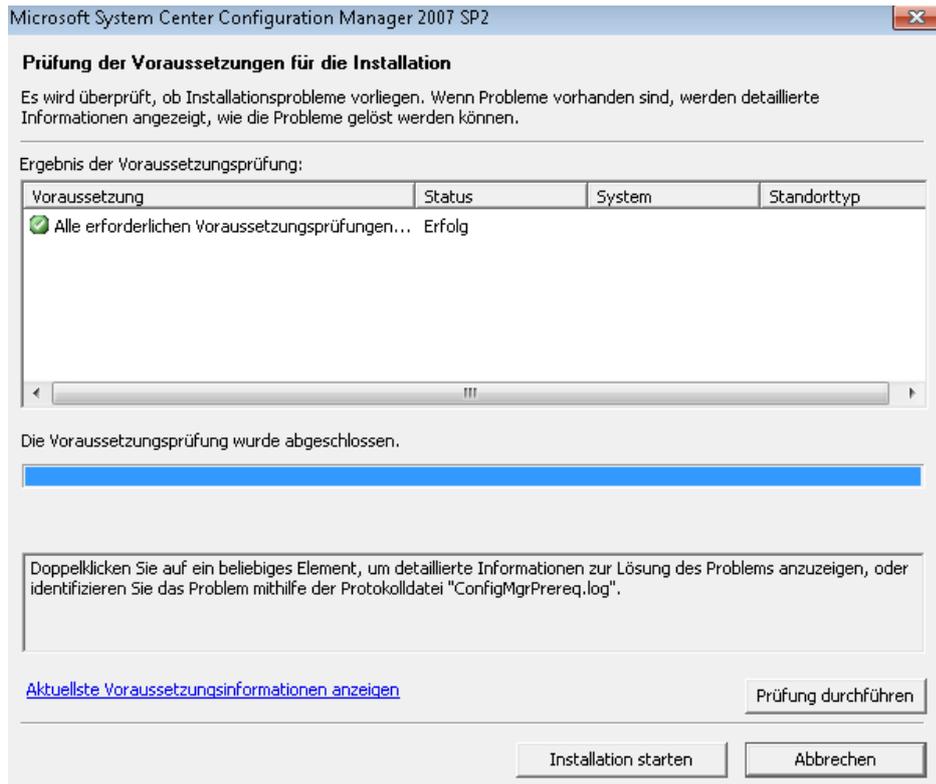
Standortserver

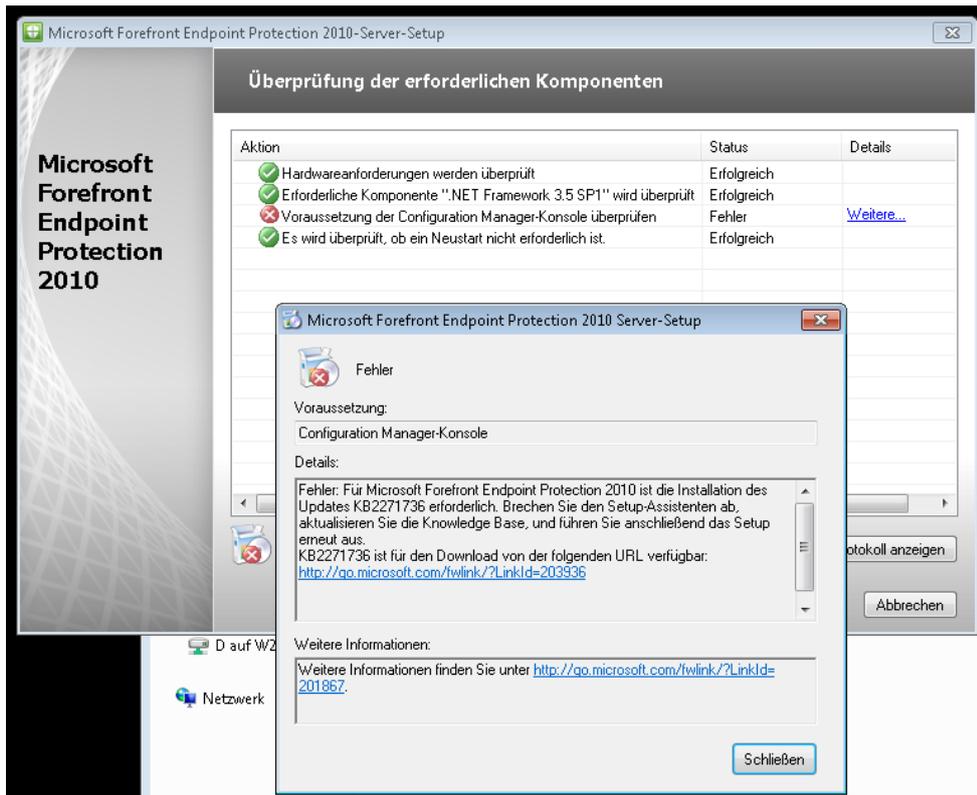
Geben Sie einen ConfigMgr-Standortservernamen ein.

Geben Sie den Namen des Servers ein, mit dem die Configuration Manager-Konsole beim ersten Starten dieses Programms eine Verbindung herstellen soll.

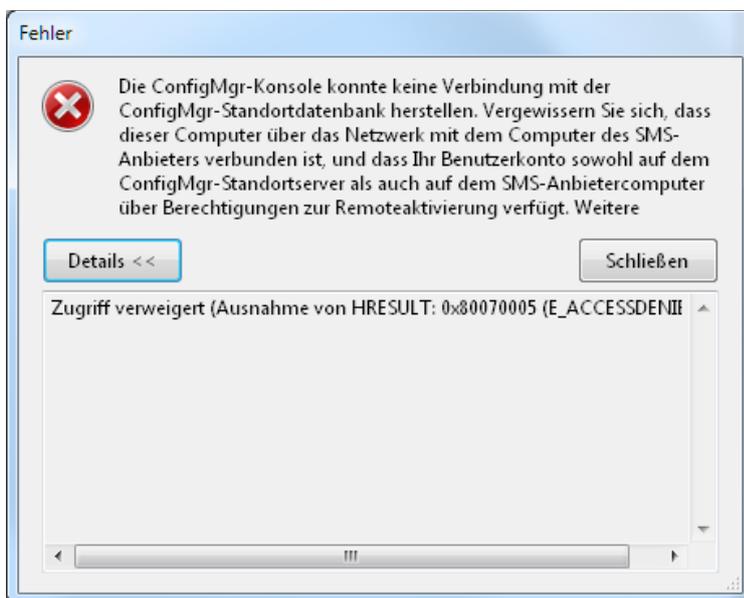
Servername:

< Zurück Weiter > Abbrechen





Fehlermeldung beim Aufruf der Konsole



Loesung:

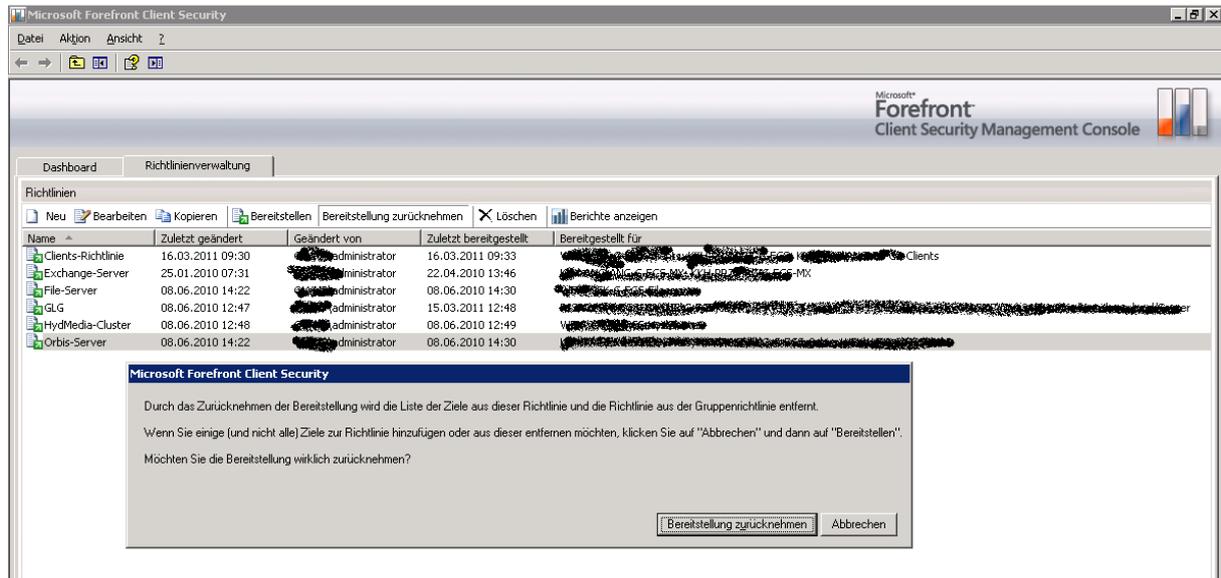
<http://technet.microsoft.com/de-de/library/bb932213.aspx>

DCOM Berechtigungen fuer Remoteausfuehrung fuer die SCCM Accounts setzen, welche die Remotekonsole aufrufen duerfen.

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



FCS Deinstallation

