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:

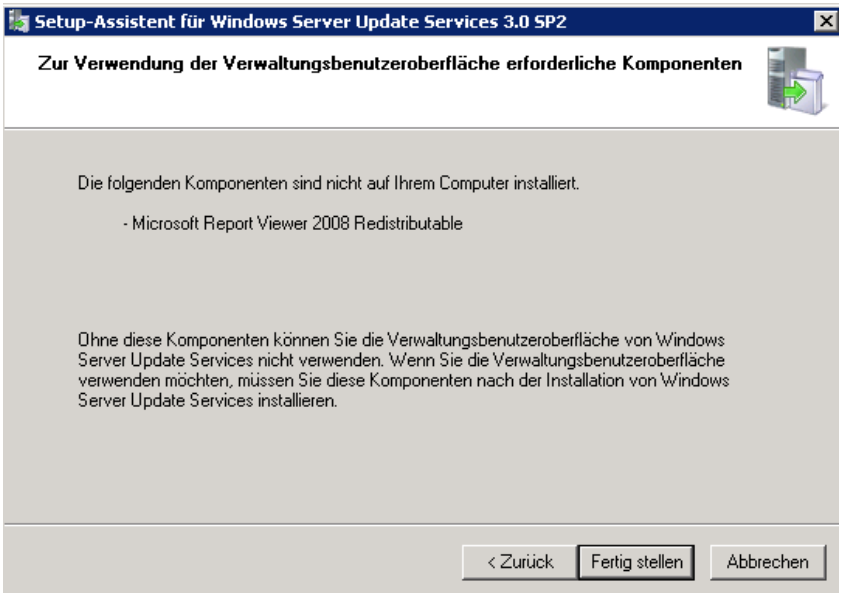
1 FEP Server mit SCCM
1 WSUS Server
1 SQL Server 2008 Cluster fuer die FEP/SCCM Datenbanken

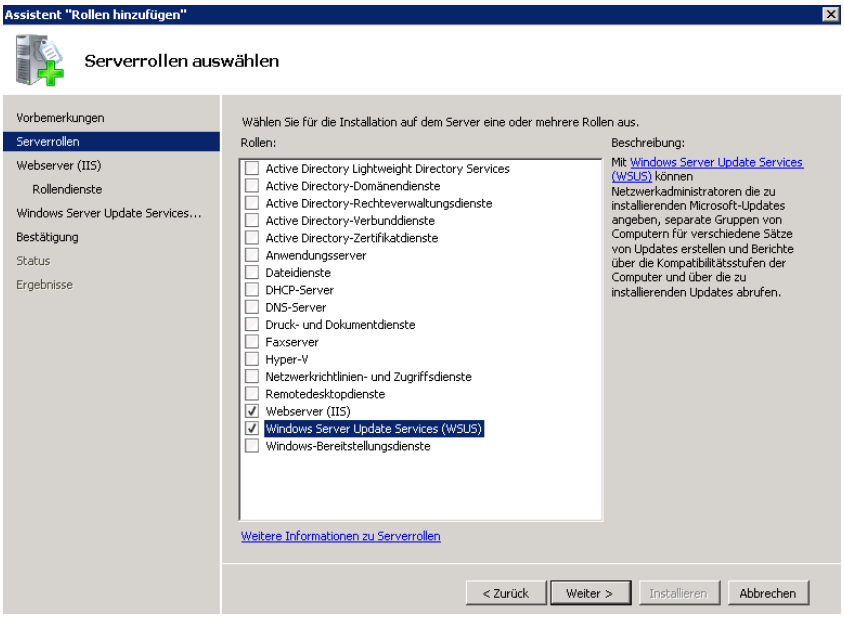
Offizielle Anleitung zur Migration von FCS zu FEP:
http://technet.microsoft.com/en-us/library/gg477033.aspx
Weitere Informationen zu FEP:
http://www.it-training-grote.de/download/FEP2010.pdf

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

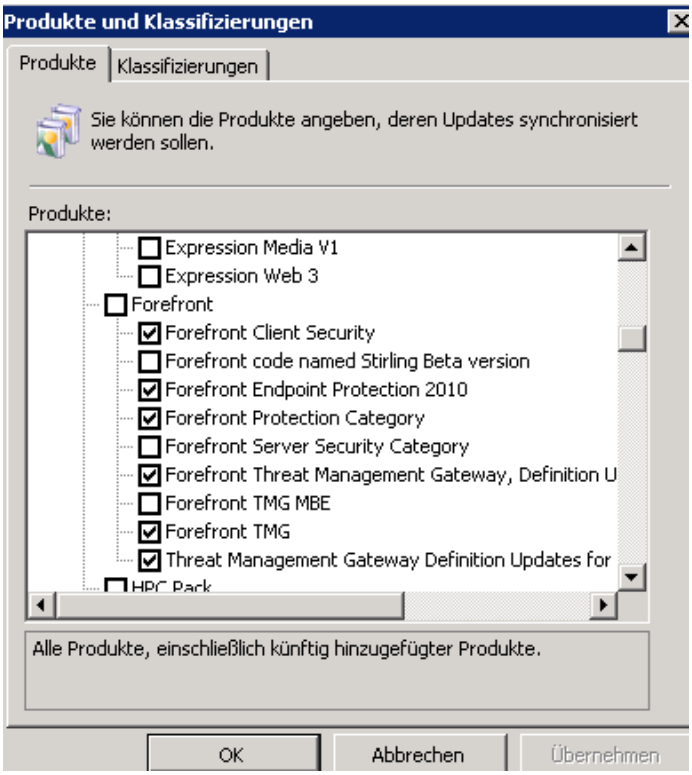
WSUS installieren oder nur die Verwaltungskonsole



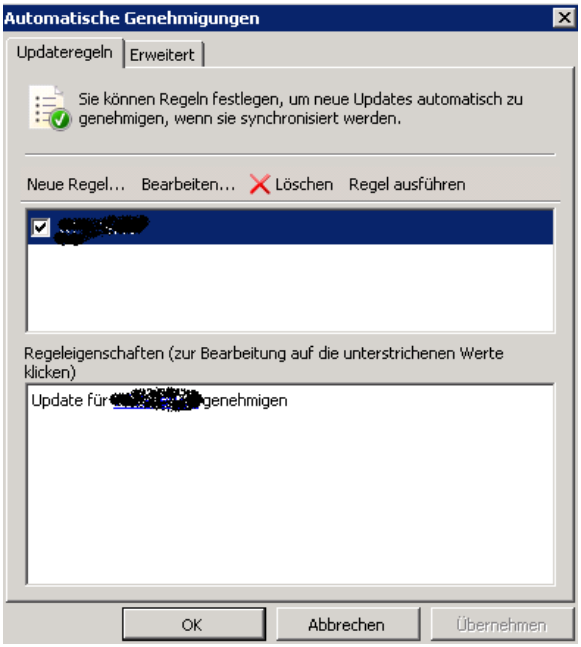


WSUS nach Vorgaben konfigurieren

Produkte und Klassifizierungen auswaehlen



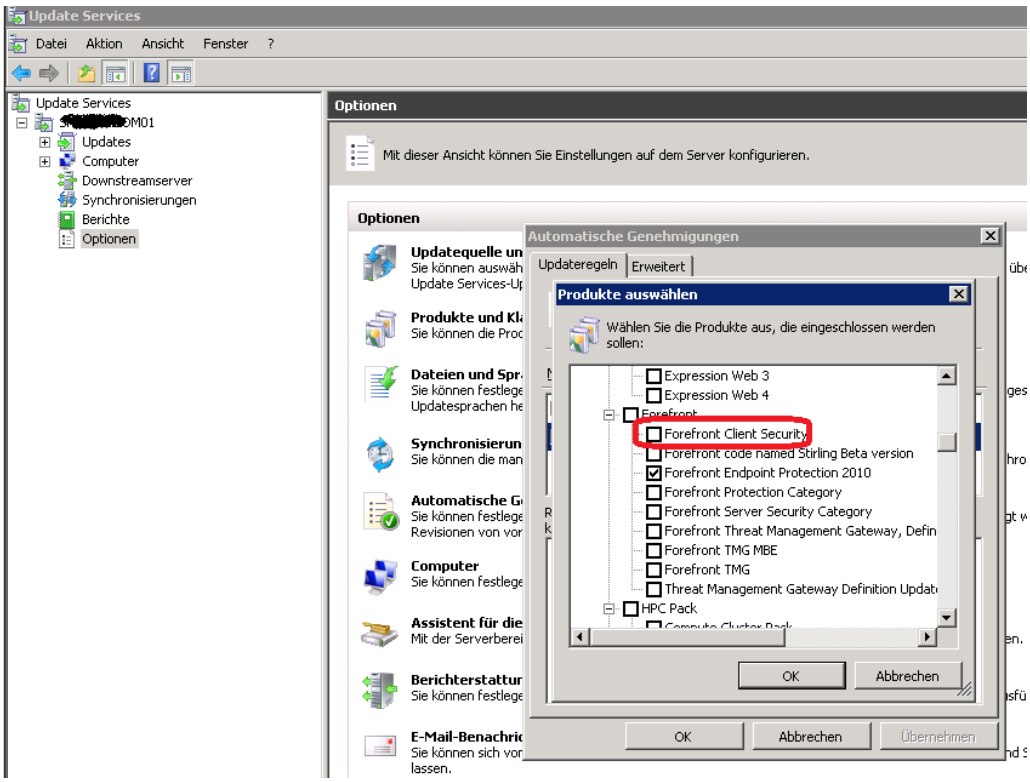
Automatische Genehmigungen konfigurieren



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

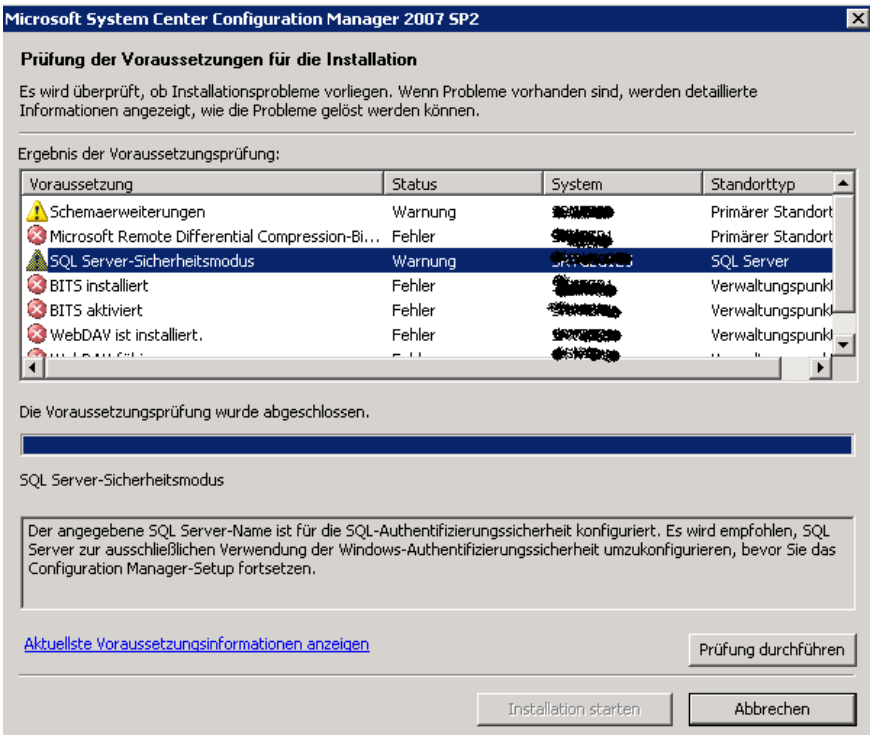
Vorhandene FCS Updates unapproven



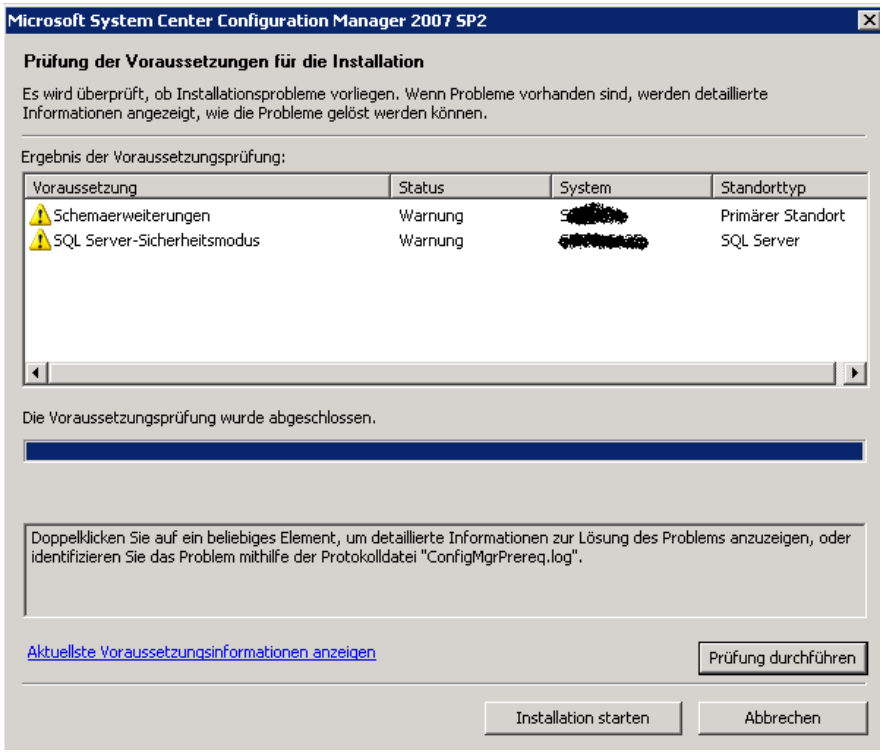
SCCM Installation

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

OK, der ein oder andere Fehler



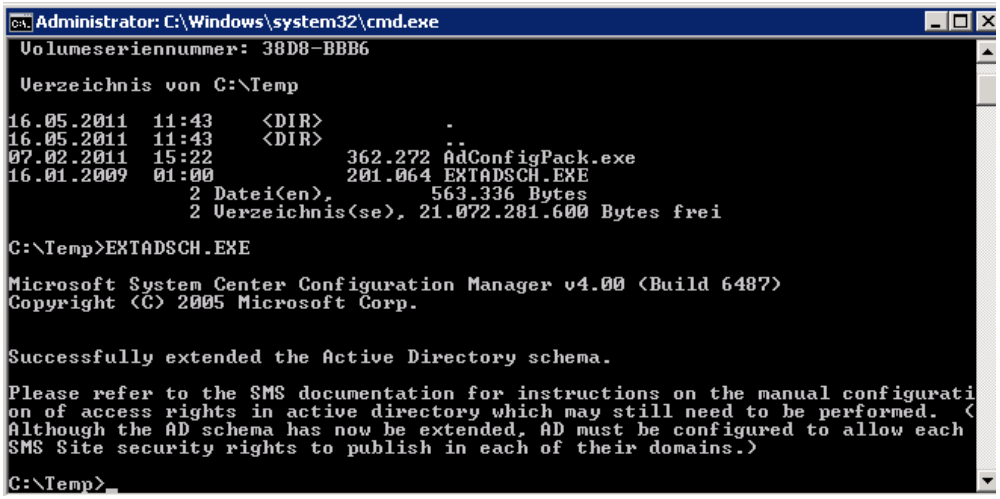
Besser



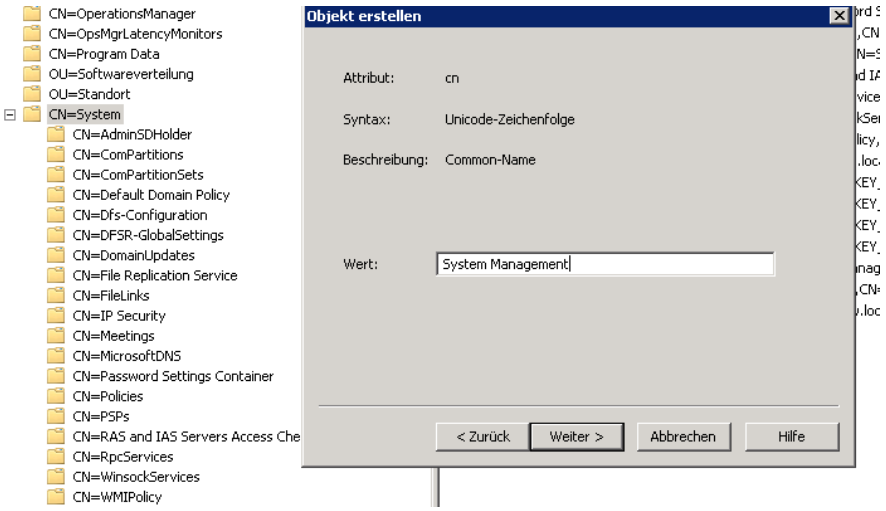
Schema fuer SCCM erweitern

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

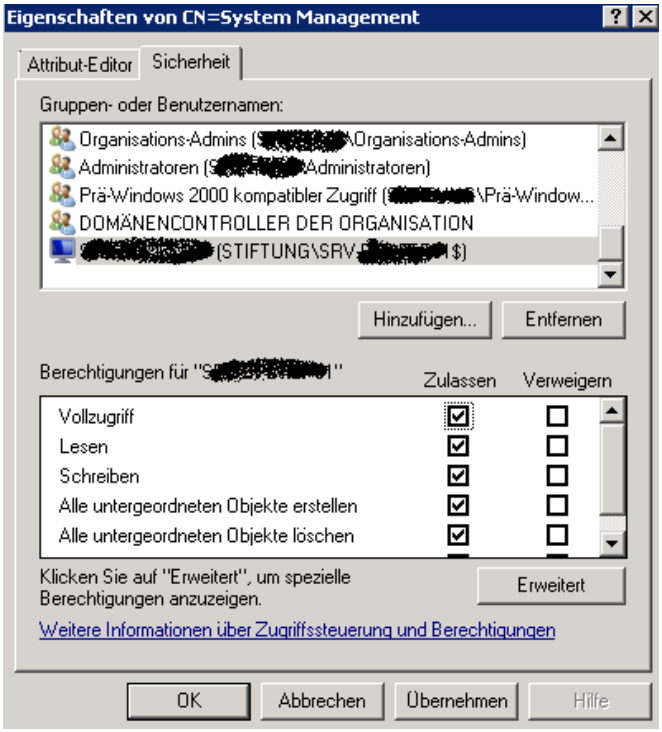
Ausfuehrung auf dem Schema Master

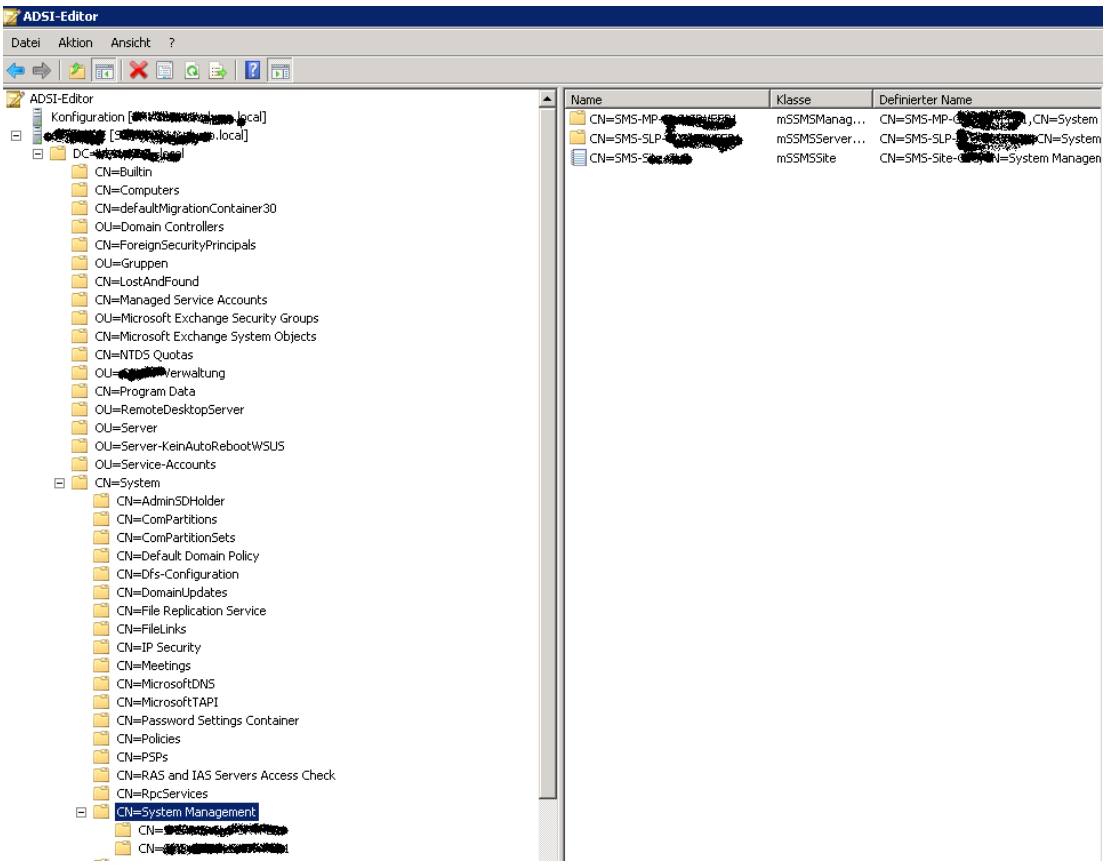


Mit ADSIEDIT anlegen

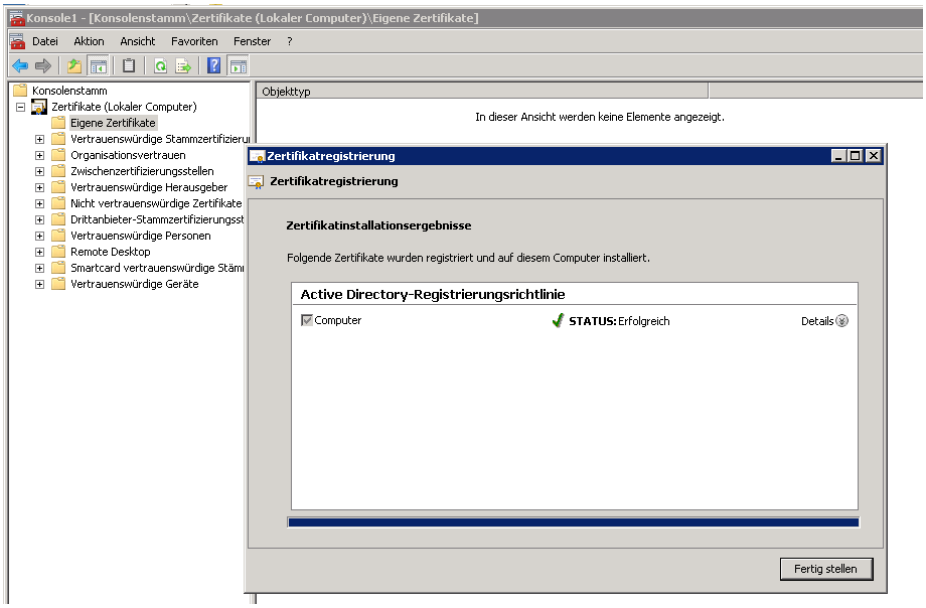


Container fuer den FEP(SCCM) Computer Account berechtigen

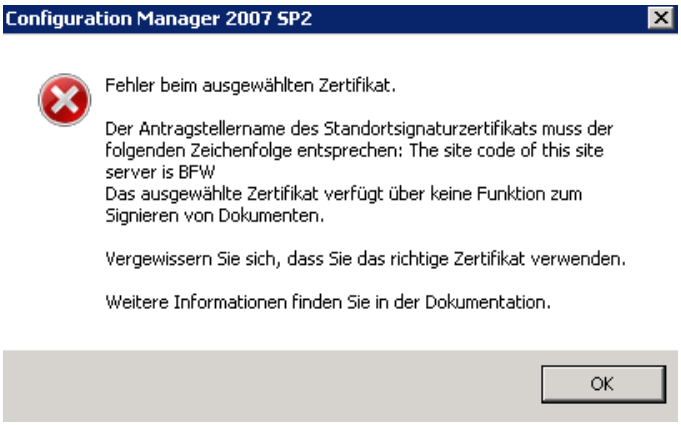




Computerzertifikat fuer den nativen SCCM Modus

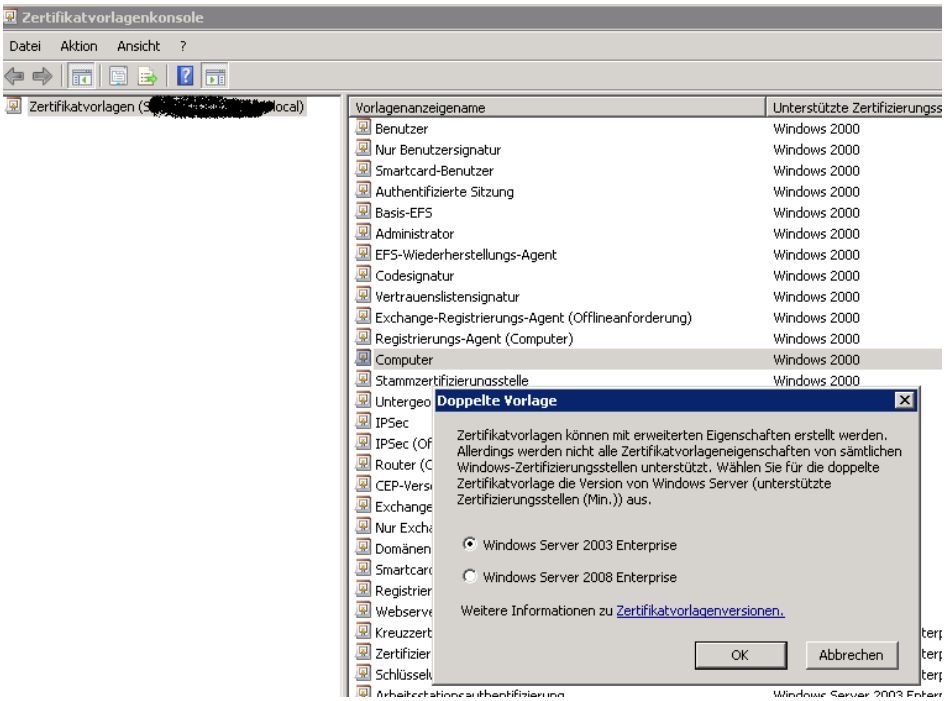


Nicht ausreichend

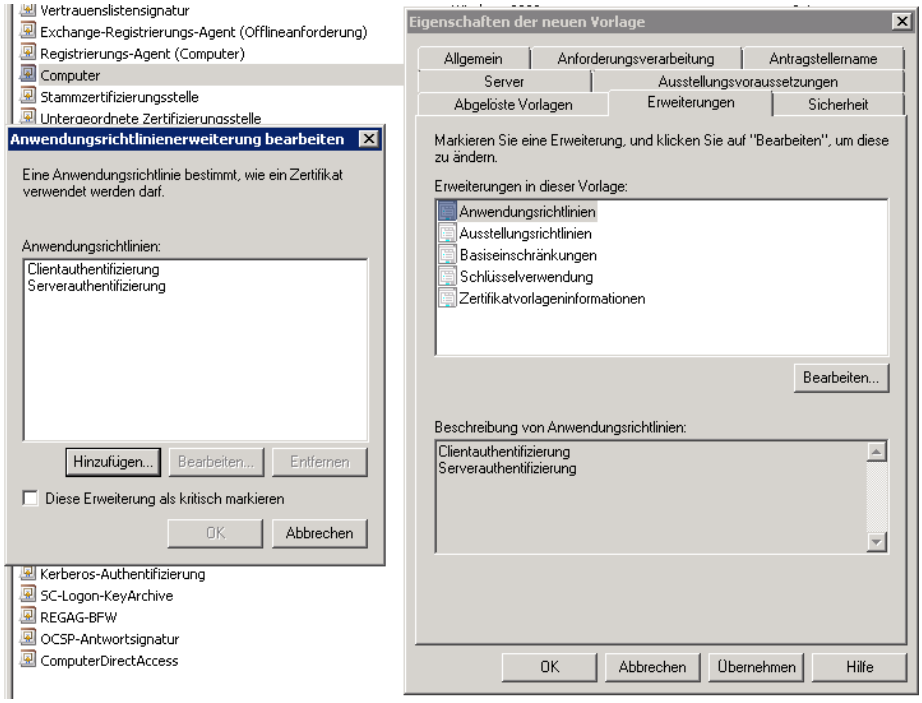


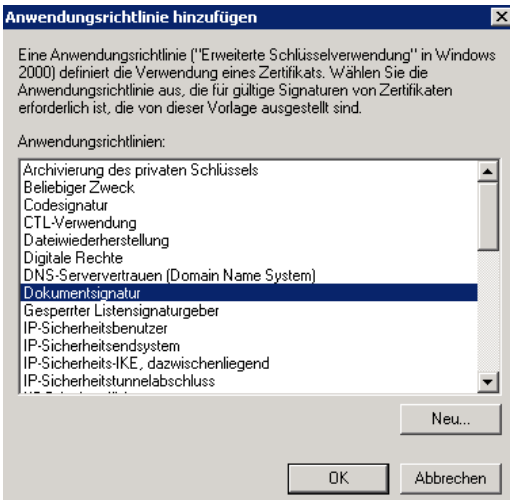
Quelle:
http://technet.microsoft.com/en-us/library/bb680733.aspx

Neues Zertifikatvorlagen Template erstellen

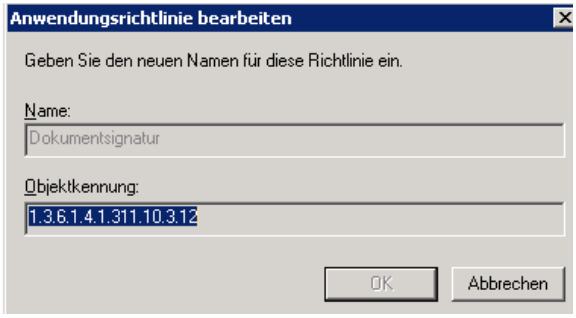


EKU hinzufuegen

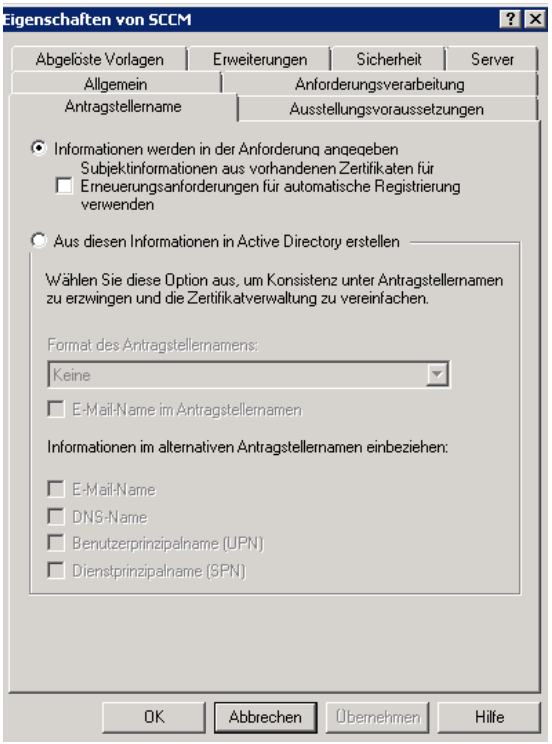




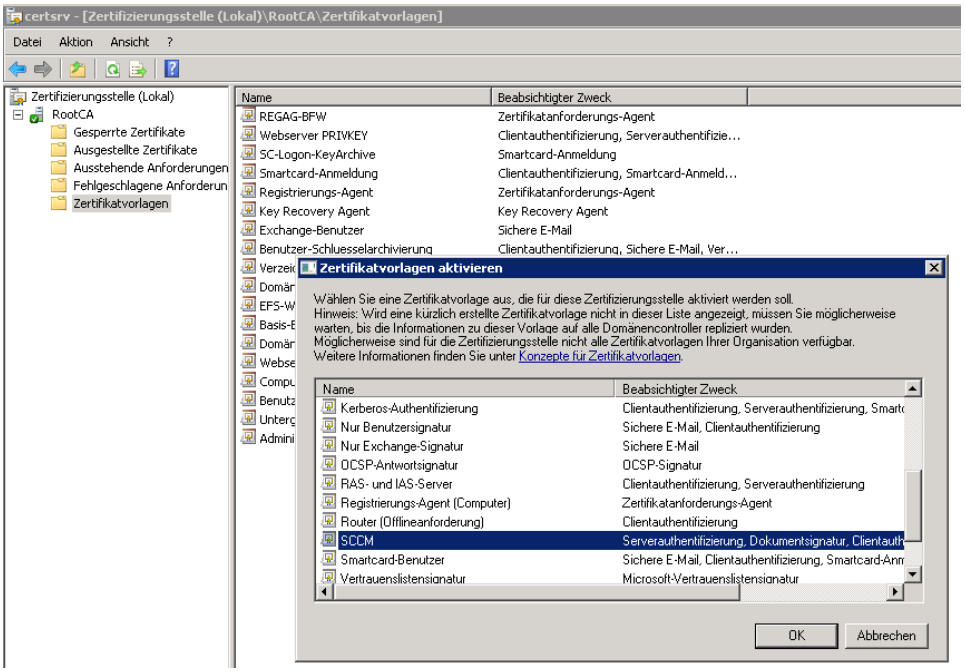
Richtig:



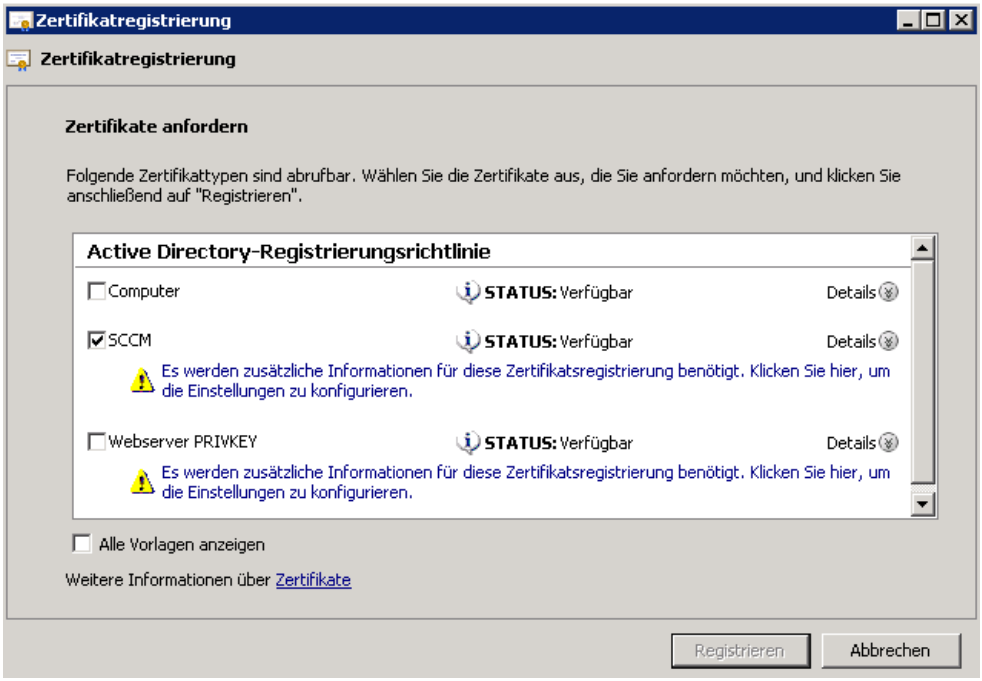
Informationen ueber den Antragsteller waehrend der Zertifikatgenerierung eingeben

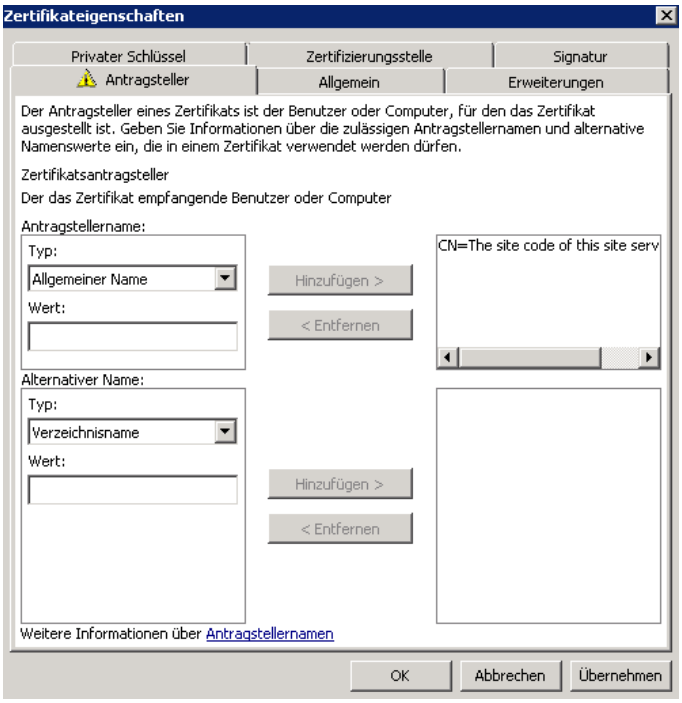


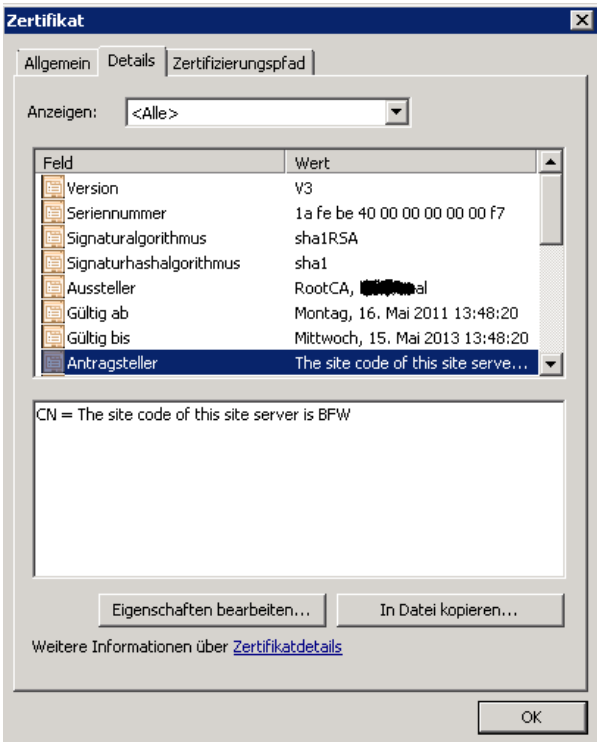
Zertifikatvorlage aktivieren

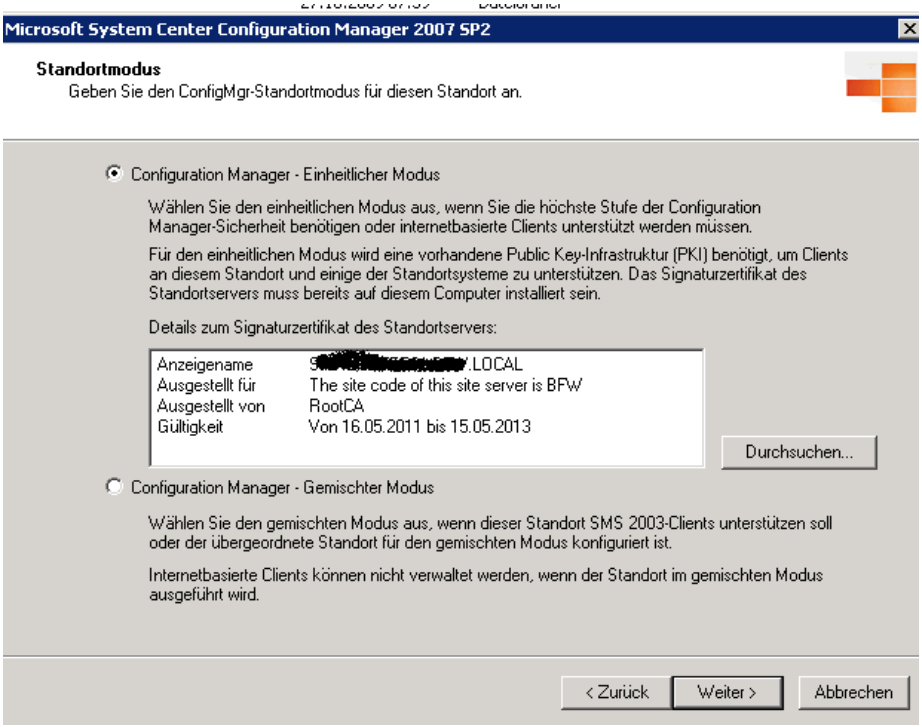


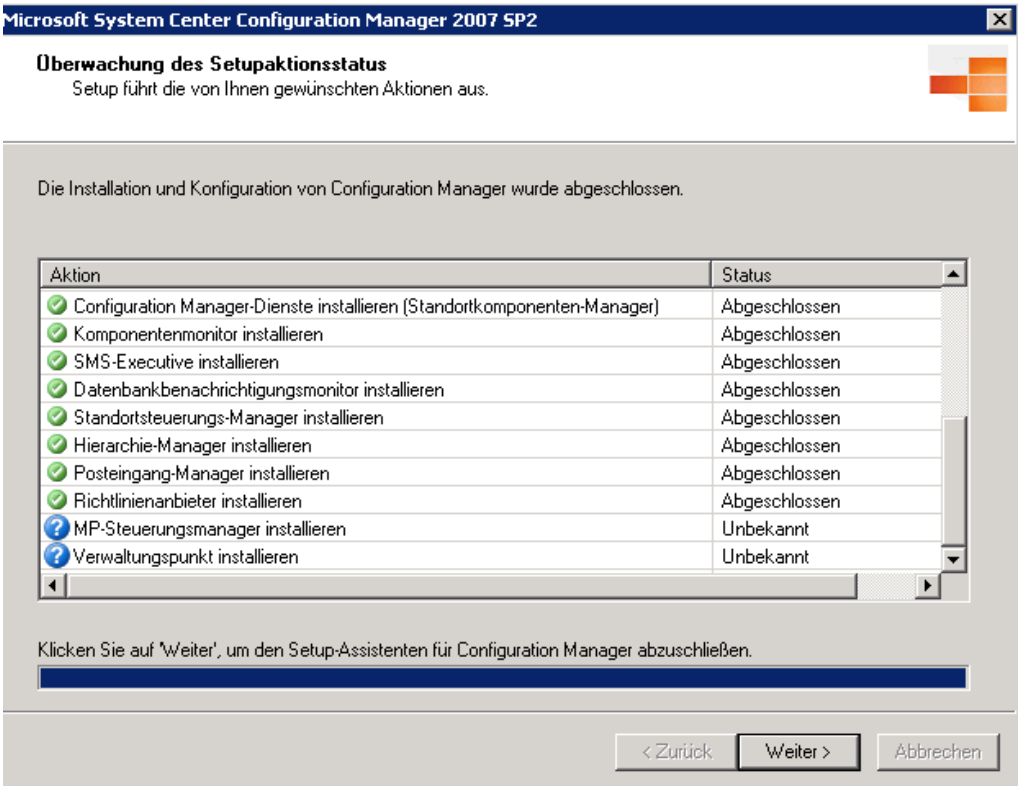
Neues Zertifikat basierend auf der neuen Vorlage anfordern




Zertifikateigenschaften
Privater Schlüssel
Zertifizierungsstelle
Signatur
Antragsteller
Allgemein
Erweiterungen
Der Antragsteller eines Zertifikats ist der Benutzer oder Computer, für den das Zertifikat ausgestellt ist. Geben Sie Informationen über die zulässigen Antragstellernamen und alternative Namenswerte ein, die in einem Zertifikat verwendet werden dürfen.
Zertifikatsantragsteller
Der das Zertifikat empfangende Benutzer oder Computer
Antragstellername:
Typ:
Allgemeiner Name
Wert:
Hinzufügen >
< Entfernen
CN=The site code of this site serv
Alternativer Name:
Typ:
Verzeichnisname
Wert:
Hinzufügen >
< Entfernen
Weitere Informationen über Antragstellernamen
OK
Abbrechen
Übernehmen


Zertifikat
Allgemein
Details
Zertifizierungspfad
Anzeigen:
<Alle>
Feld
Wert
Version
V3
Seriennummer
1a fe be 40 00 00 00 00 00 f7
Signaturalgorithmus
sha1RSA
Signaturhashalgorithmus
sha1
Aussteller
RootCA, [redacted]al
Gültig ab
Montag, 16. Mai 2011 13:48:20
Gültig bis
Mittwoch, 15. Mai 2013 13:48:20
Antragsteller
The site code of this site serve...
CN = The site code of this site server is BFW
Eigenschaften bearbeiten...
In Datei kopieren...
Weitere Informationen über Zertifikatdetails
OK

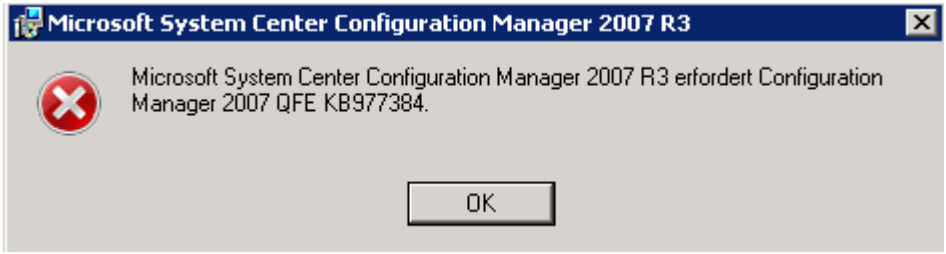




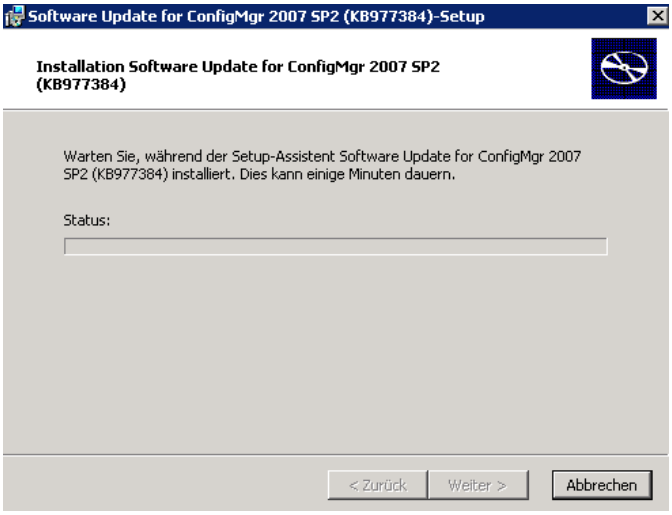
Wenn der MP-Steuerungsmanager und der Verwaltungspunkt mit Status Unbekannt angezeigt werden, koennte das an einer fehlenden korrekten WebDAV Einstellung liegen:
http://blogs.southworks.net/aortega/2009/09/16/deploy-sccm-2007-sp2-rc-on-windows-server-2008-r2/

SCCM 2007 R2 installieren

SCCM 2007 R3 installieren

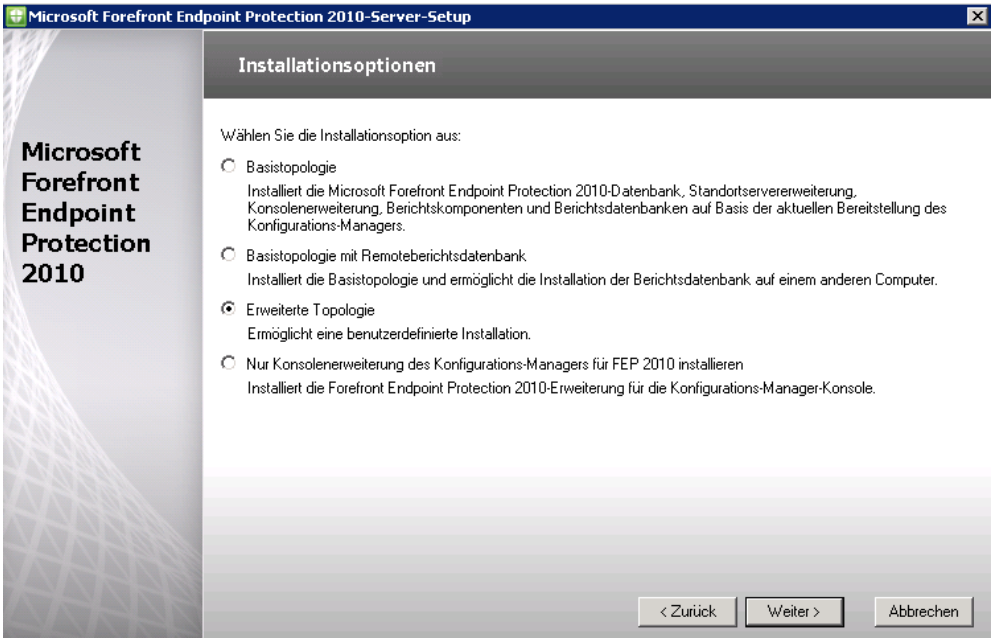


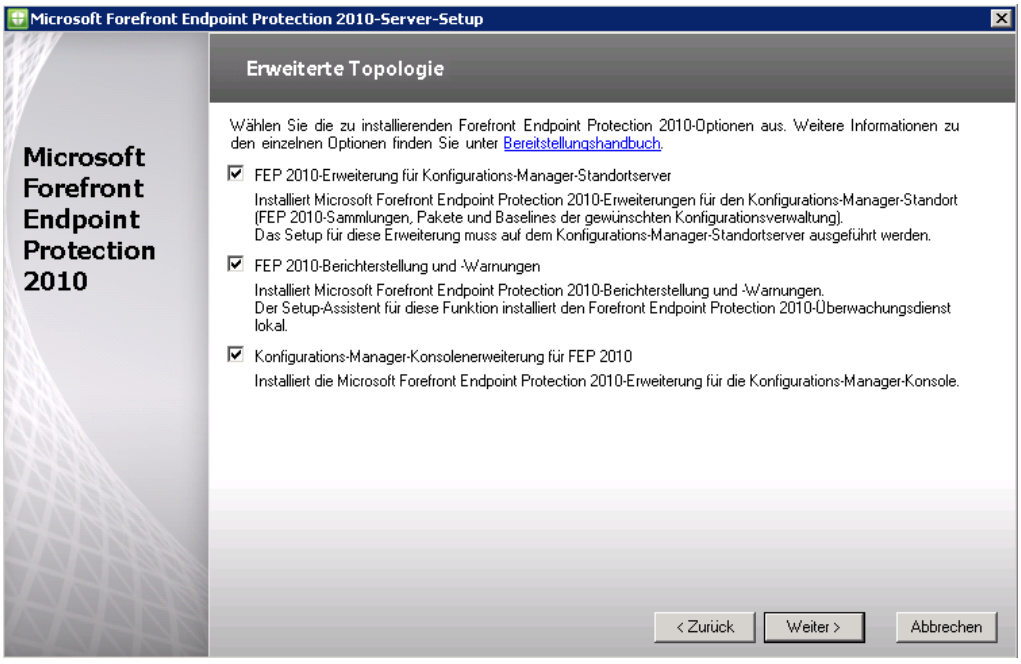
Hotfix installieren



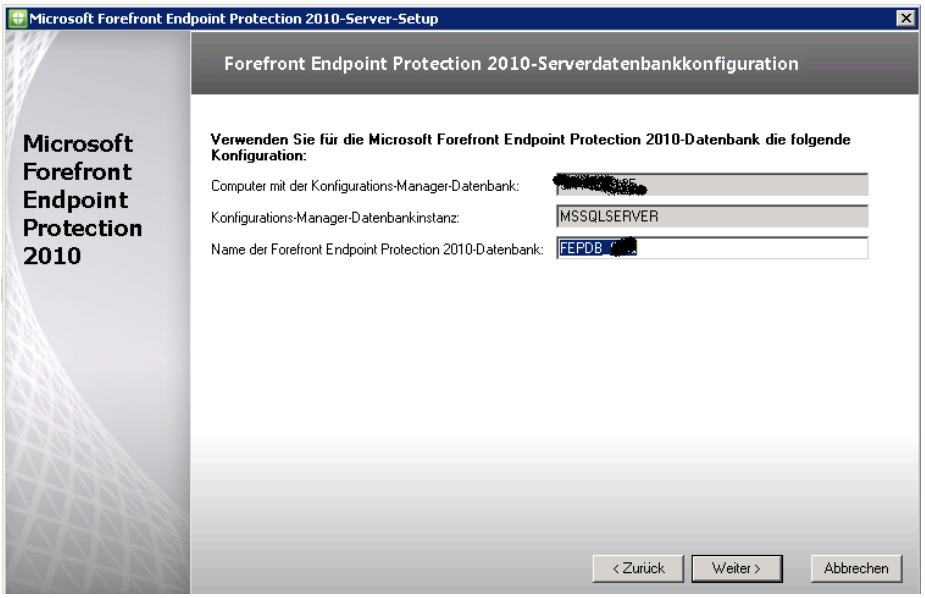
FEP 2010 Installation

Erweiterte Topologie installieren

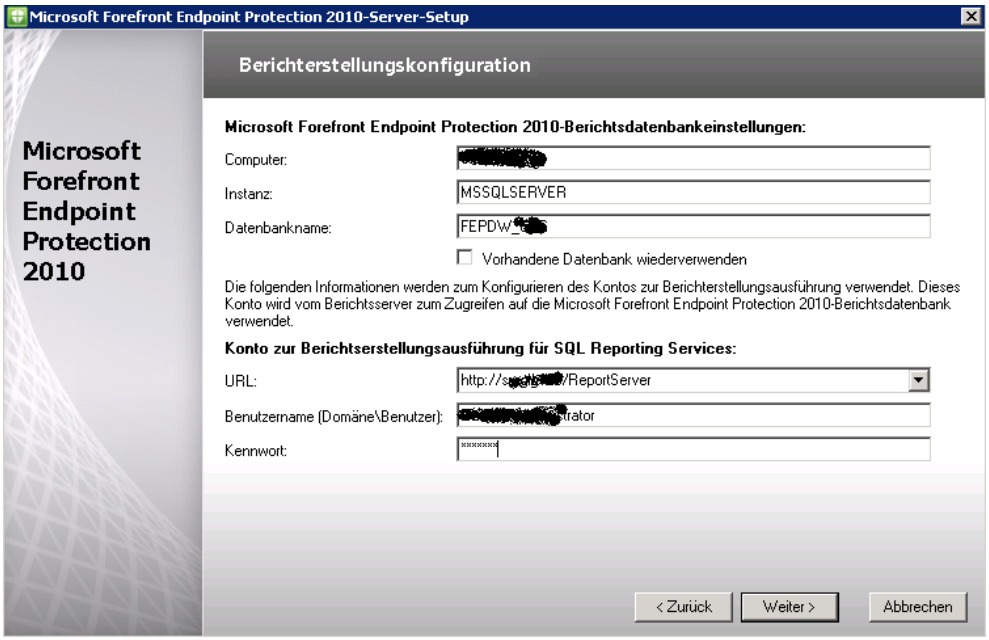




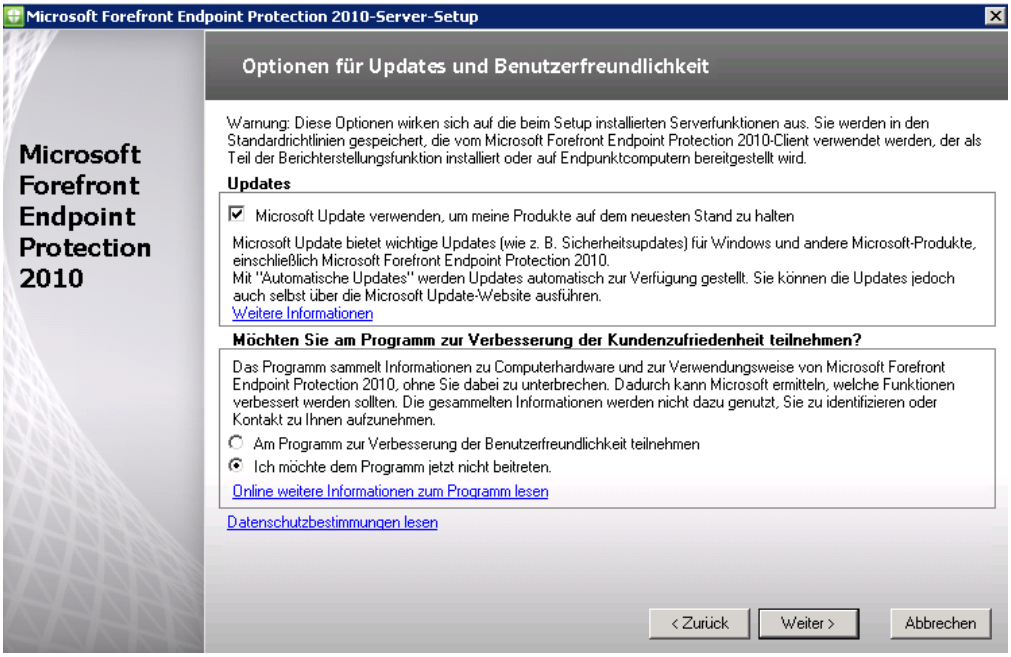
Neue Datenbank auf SQL Server



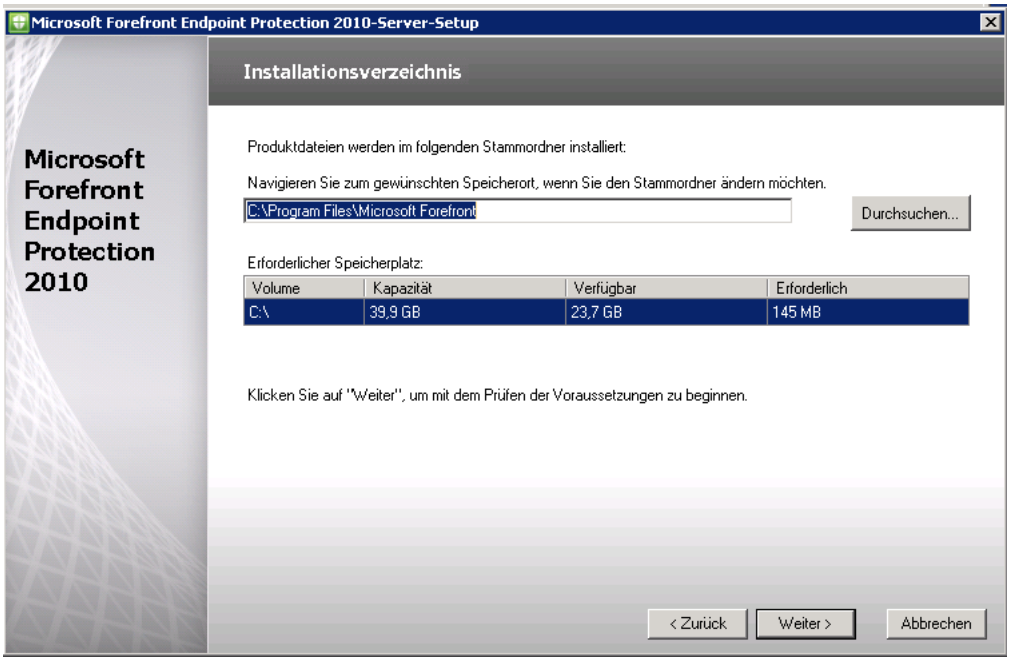
Berichterstellungskonfiguration

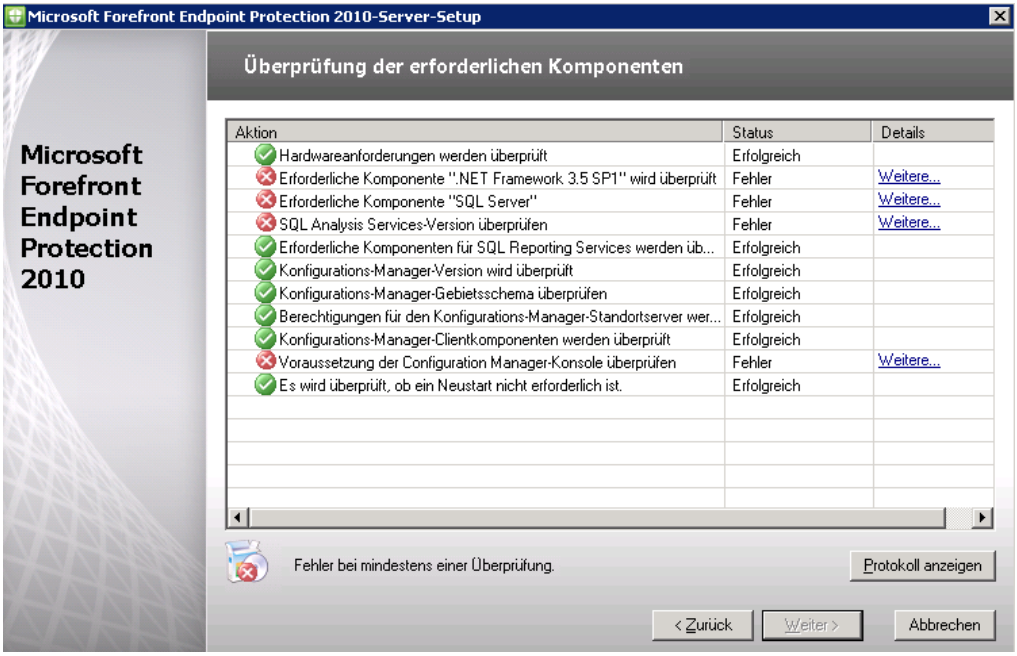


Falls sich die Reporting Services nicht auf einem Windows Server 2008 x64 installieren lassen, koennte das hieran liegen:
http://support.microsoft.com/kb/894435/en-us

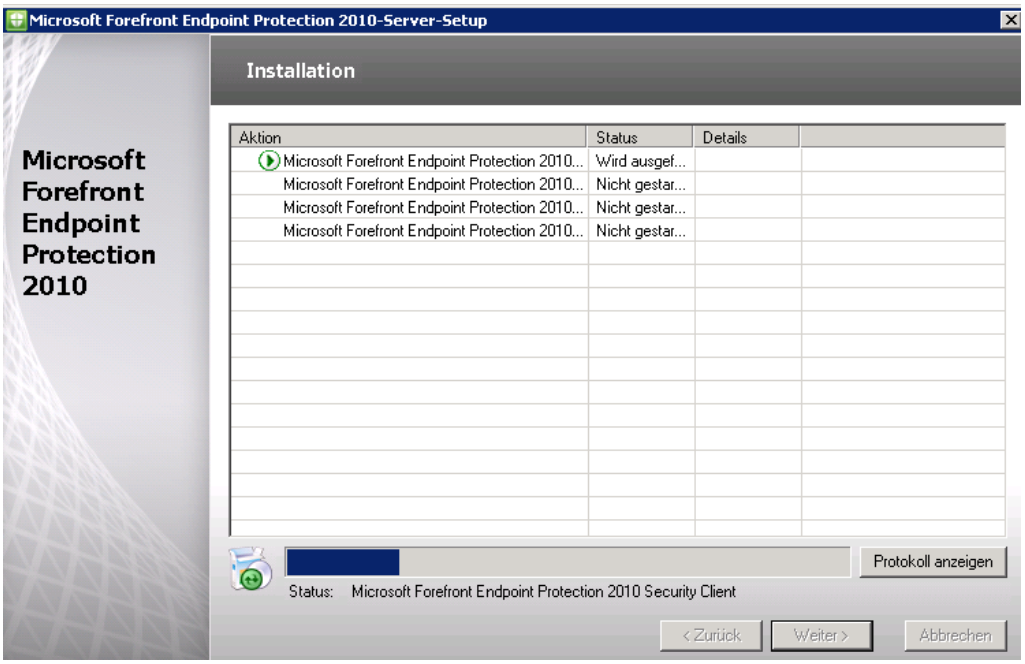


Installationspfad

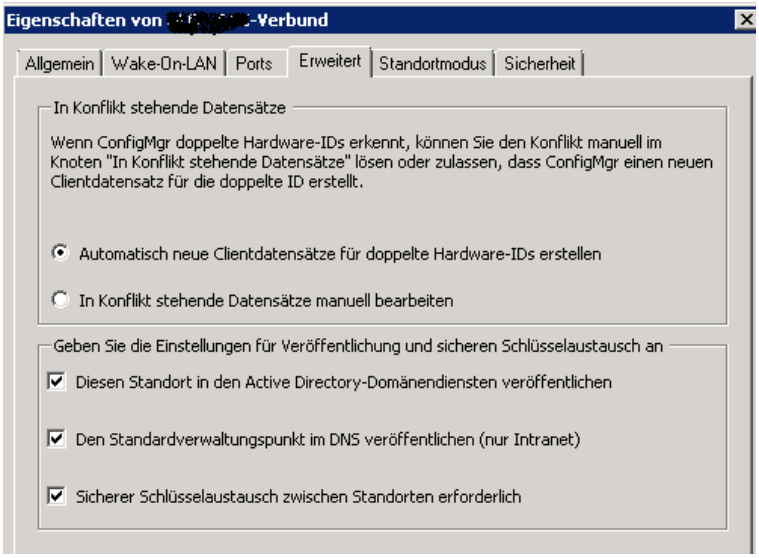




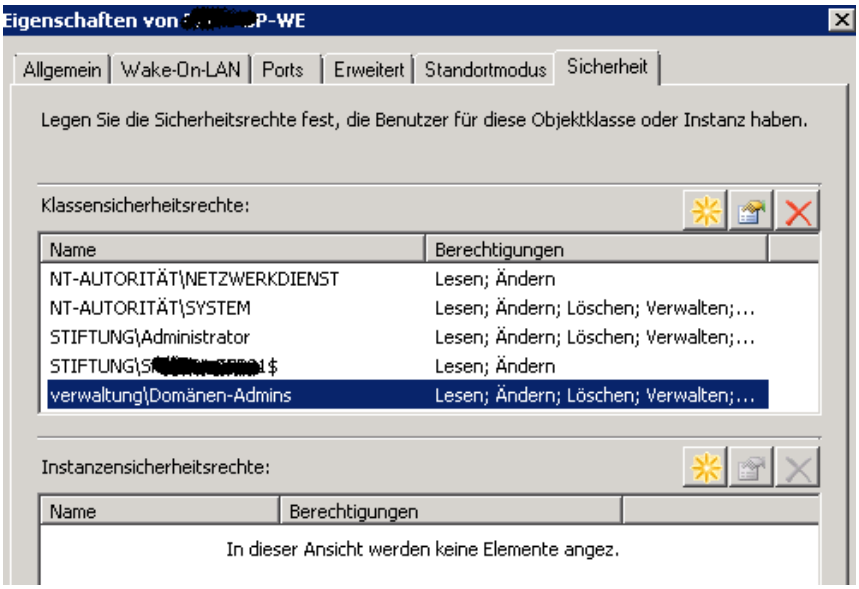
Alle Fehler behoben, dann kann das Setup starten



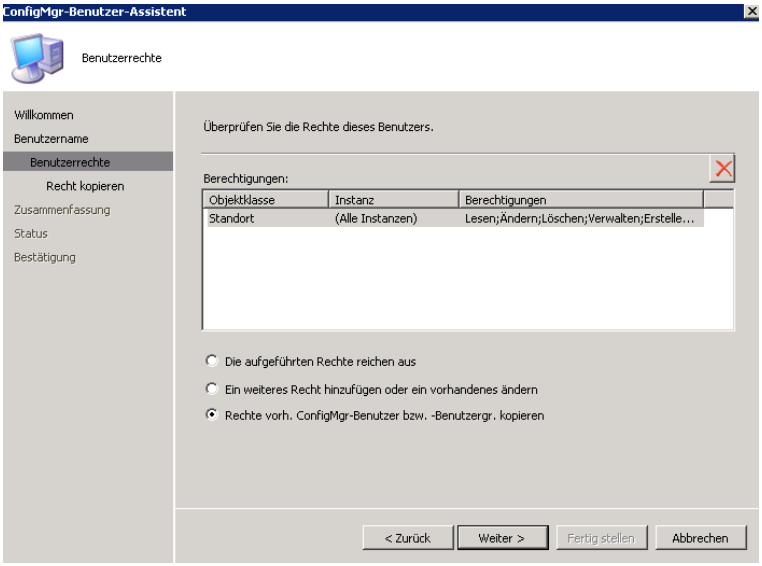
SCCM fuer AD Connection Objekt einstellen



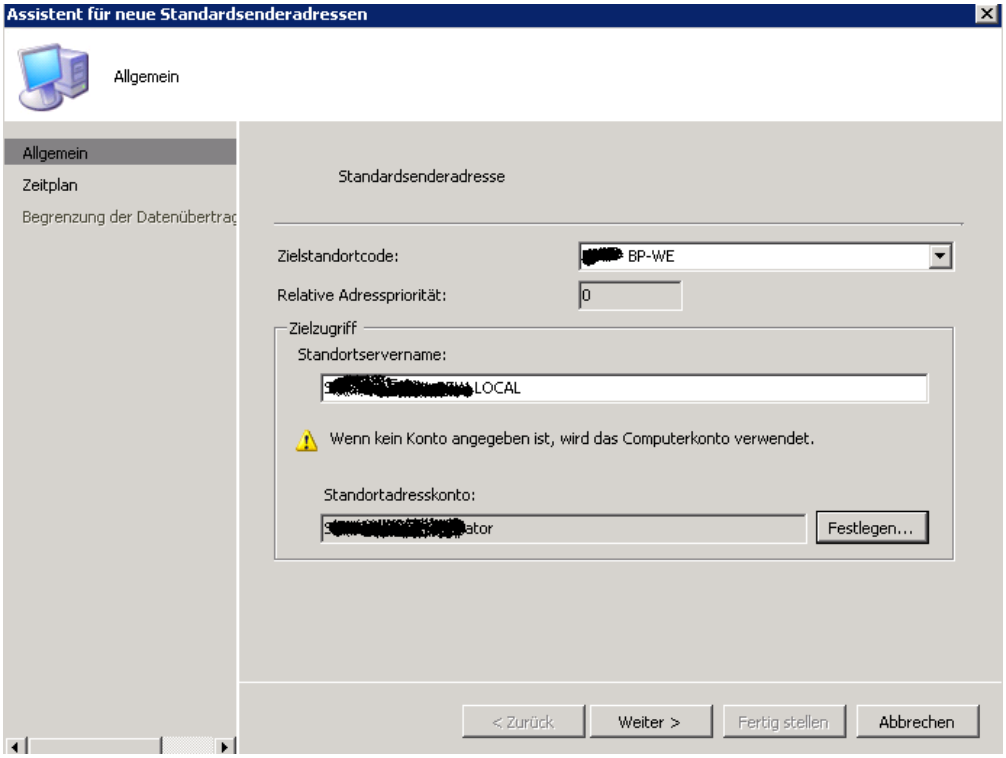
Sicherheitsberechtigungen fuer SCCM Verwaltung aendern



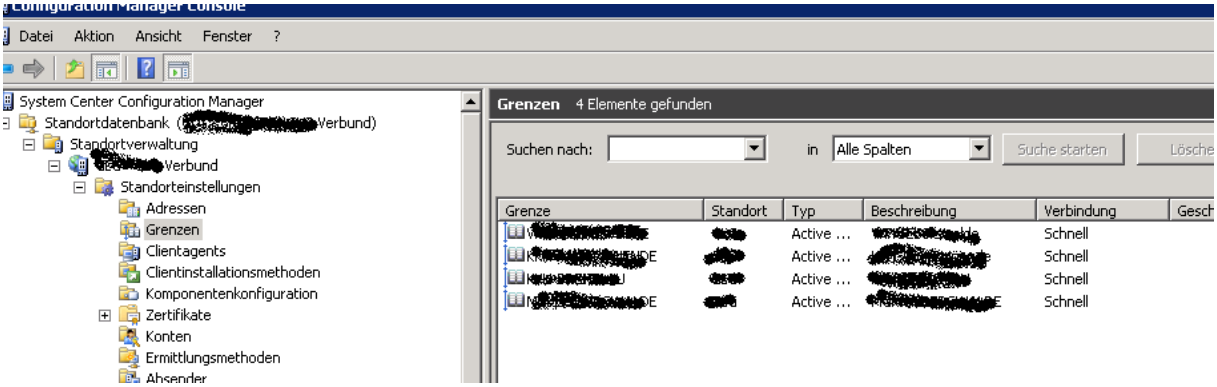
SCCM Berechtigungen eines bestehenden Benutzers uebernehmen



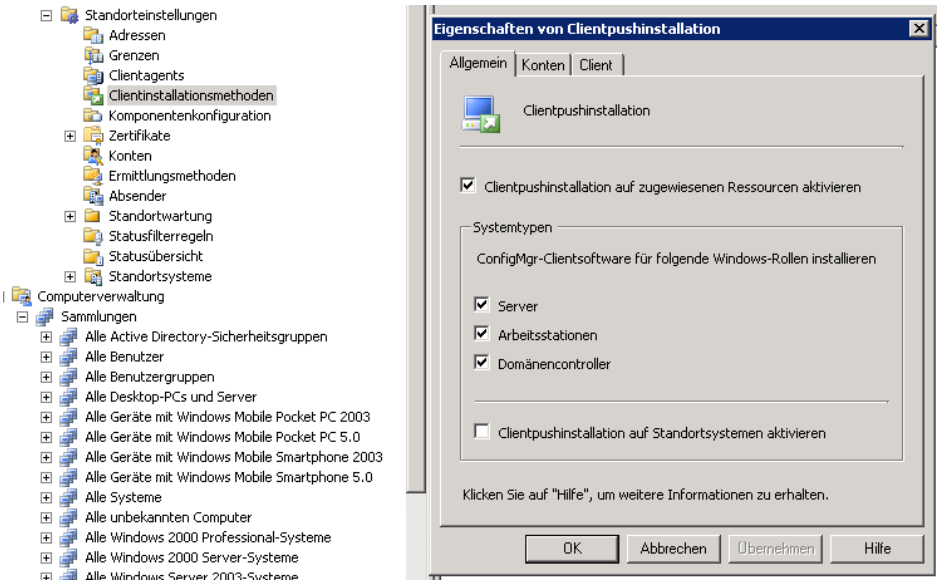
Standardsenderadresse festlegen



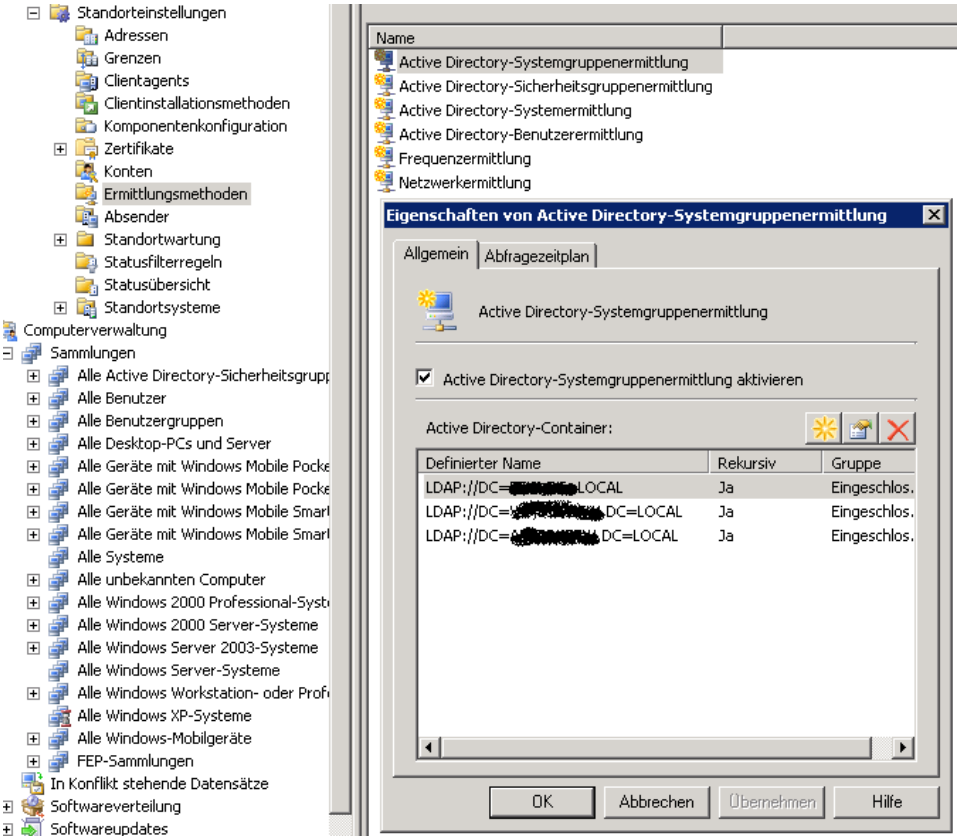
SCCM Sitegrenzen konfigurieren



Client Pushinstallation konfigurieren



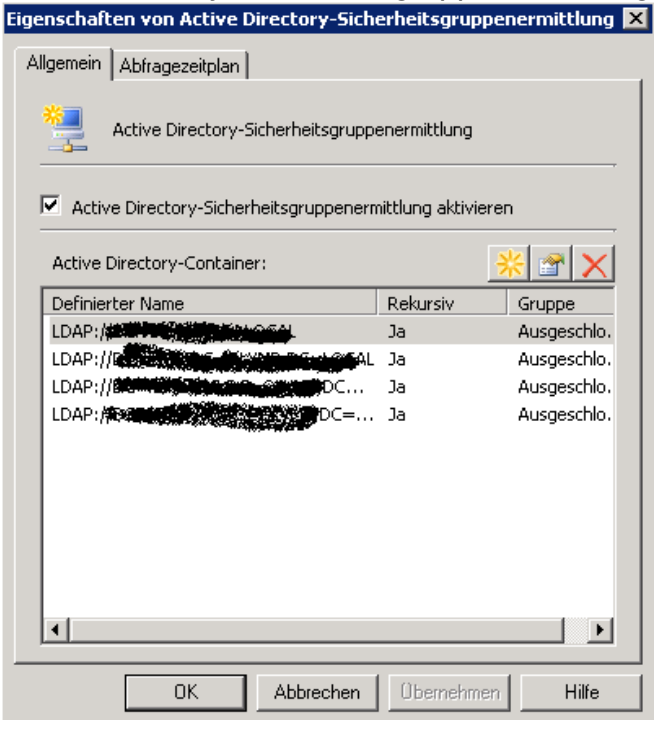
Ermittlungsmethoden konfigurieren



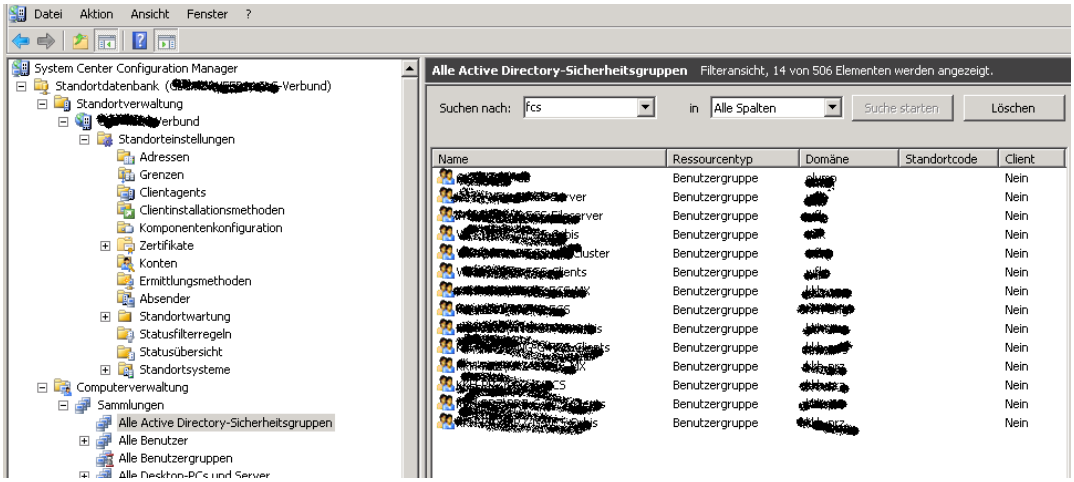
Ggfs. Delta Ermittlung aktivieren

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

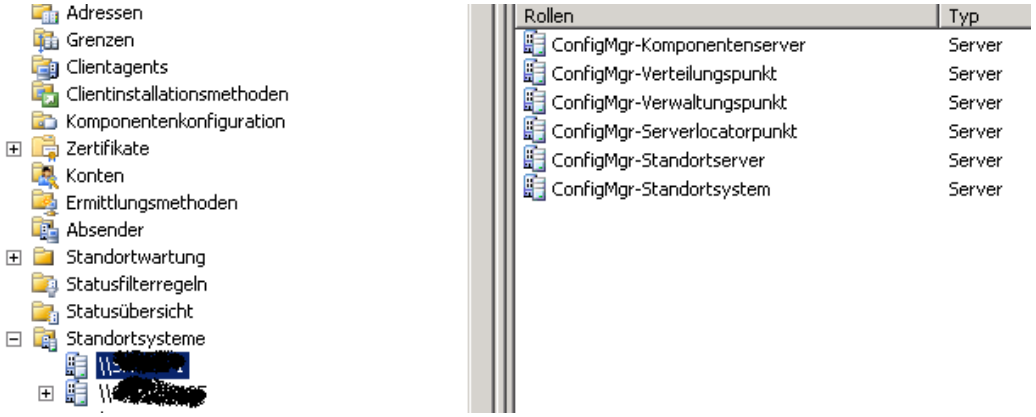
Active Directory Sicherheitsgruppenermittlung aktivieren



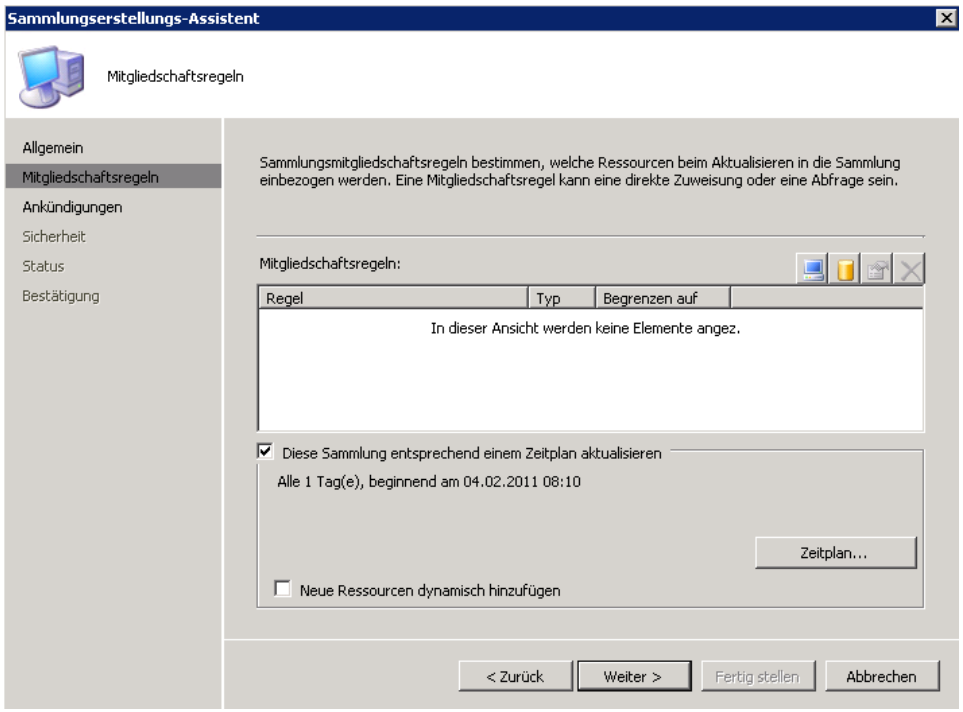
Danach tauchen die Gruppen in der SCCM Konsole auf



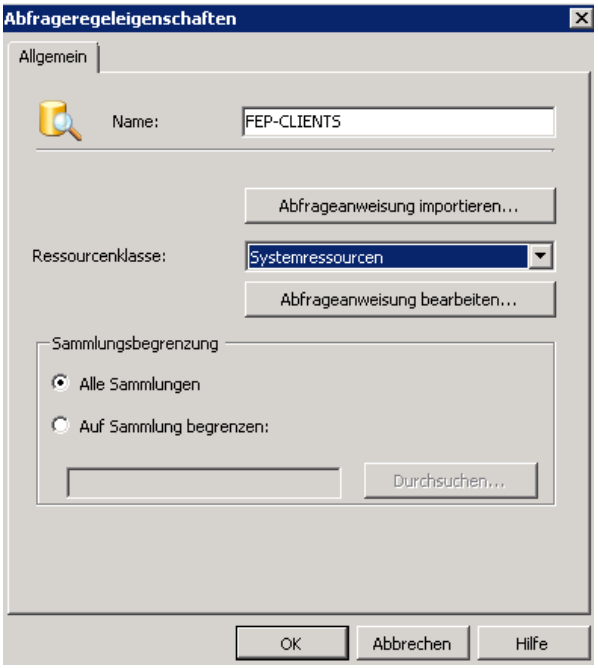
Standortsystemkomponenten

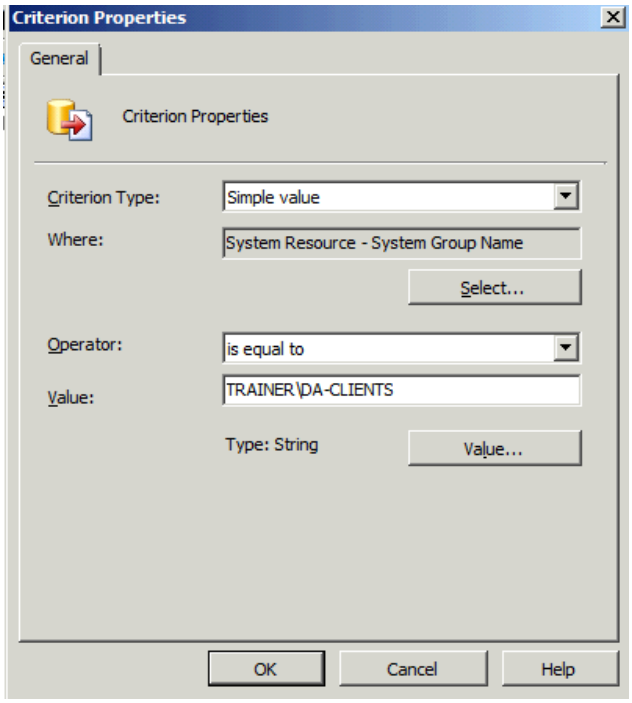


Als naechstes muss eine neue Collection (Sammlung) basierend auf den Gruppenmitgliedschaften erstellt werden

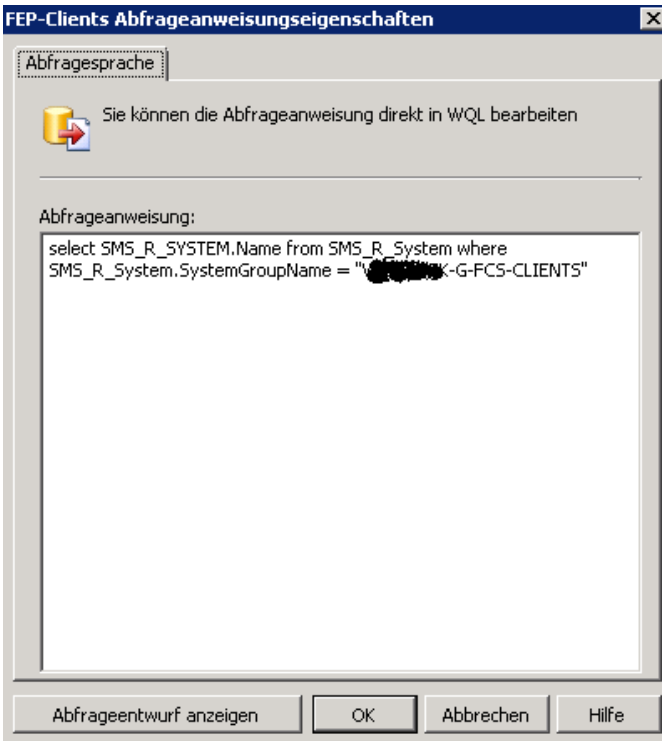


Abfragebasierte Sammlung erstellen

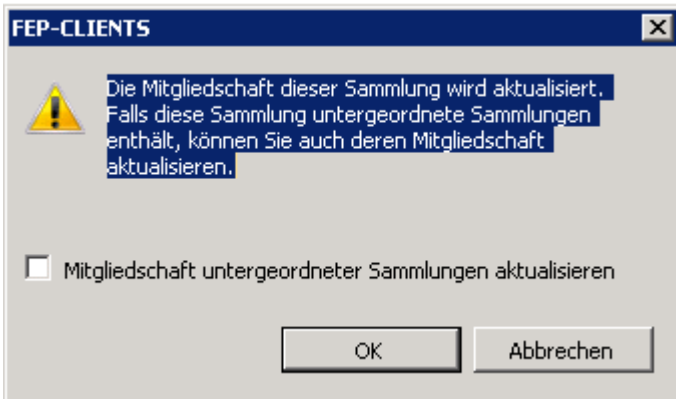




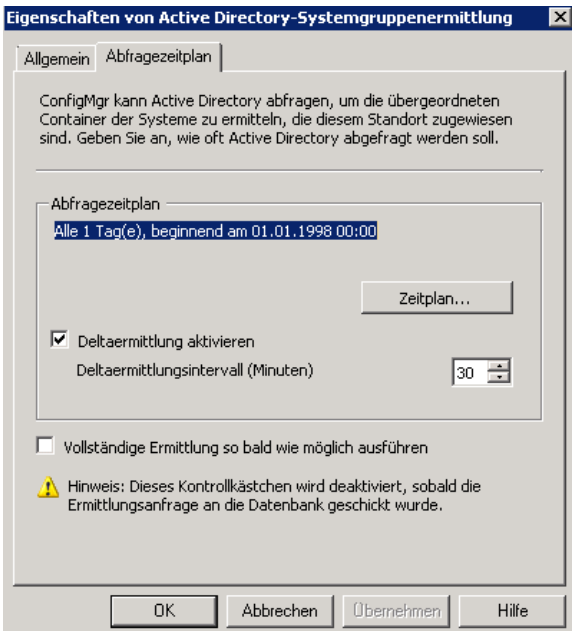
Abfrageanweisung definieren



Sammlungsmitgliedschaft aktualisieren



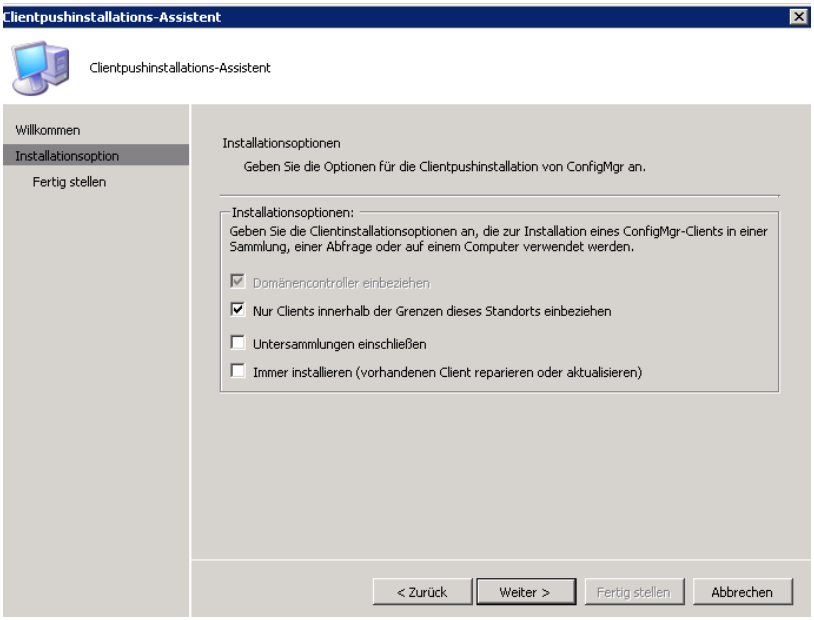
F5 druecken nicht vergessen und Achtung: Wenn neue Windows Gruppen fuer FEP-Clients erstellt werden, im SCCM die Ermittlung der Gruppen manuell anstarten



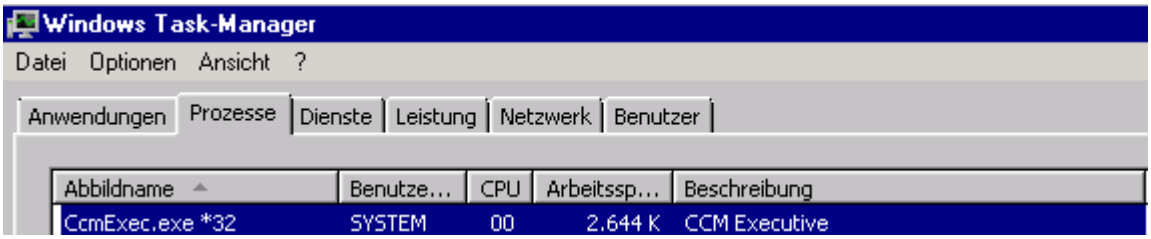
Client Deployment

Jetzt kann der SCCM Client deployed werden

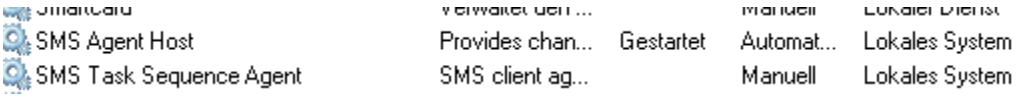
Rechtsklick auf die Collection und Client deployen



Auf dem Client startet dann das CCM Setup

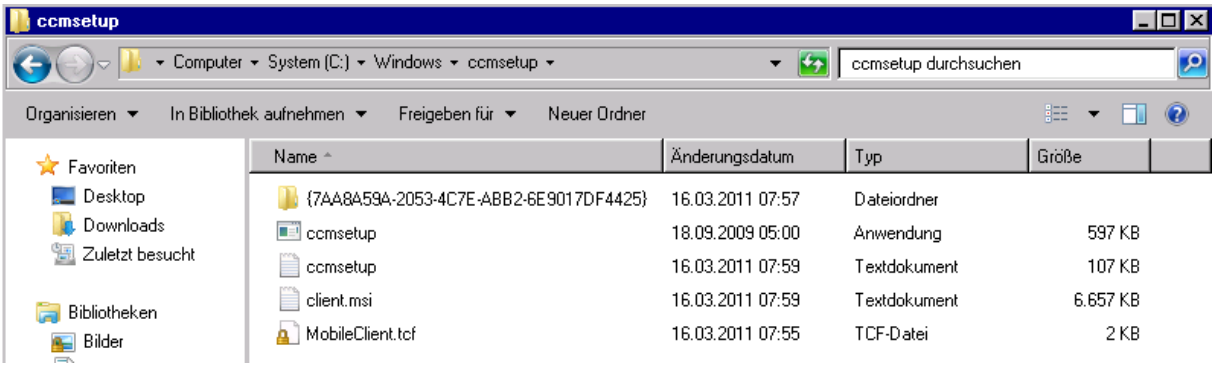


SCCM Dienste



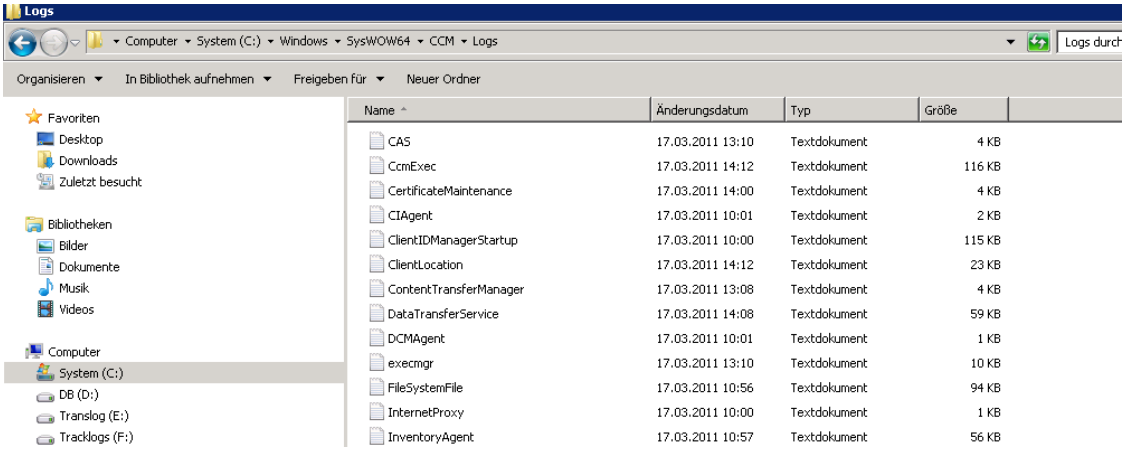
CCM Setup Verzeichnisse

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



SCCM Symbole

SCCM Logdateien auf einem 64 Bit System

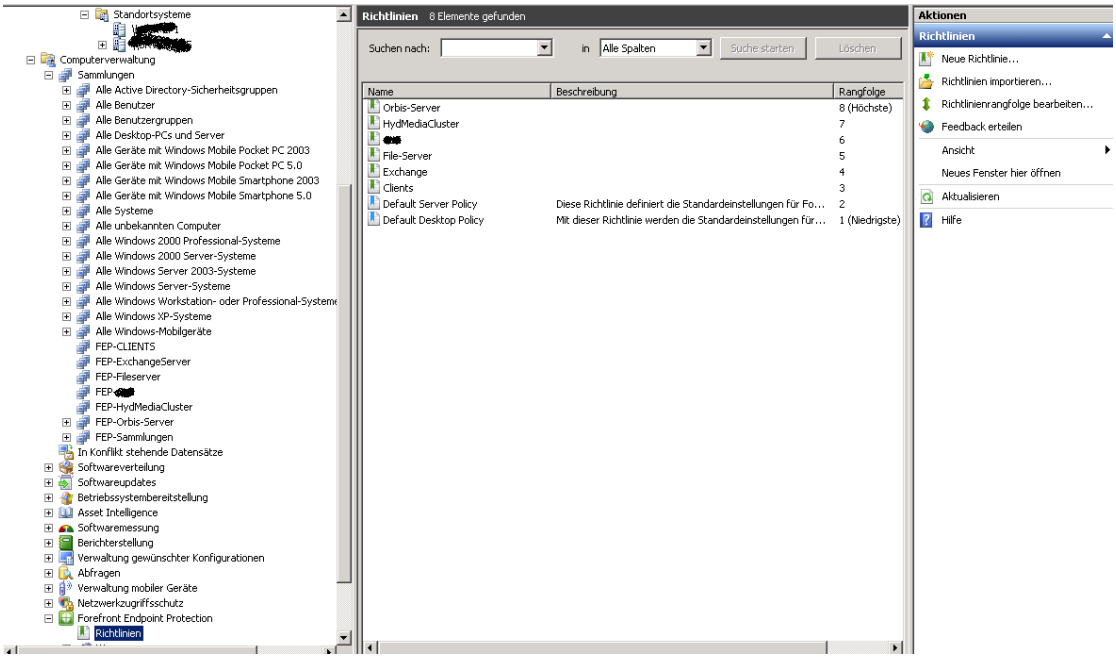


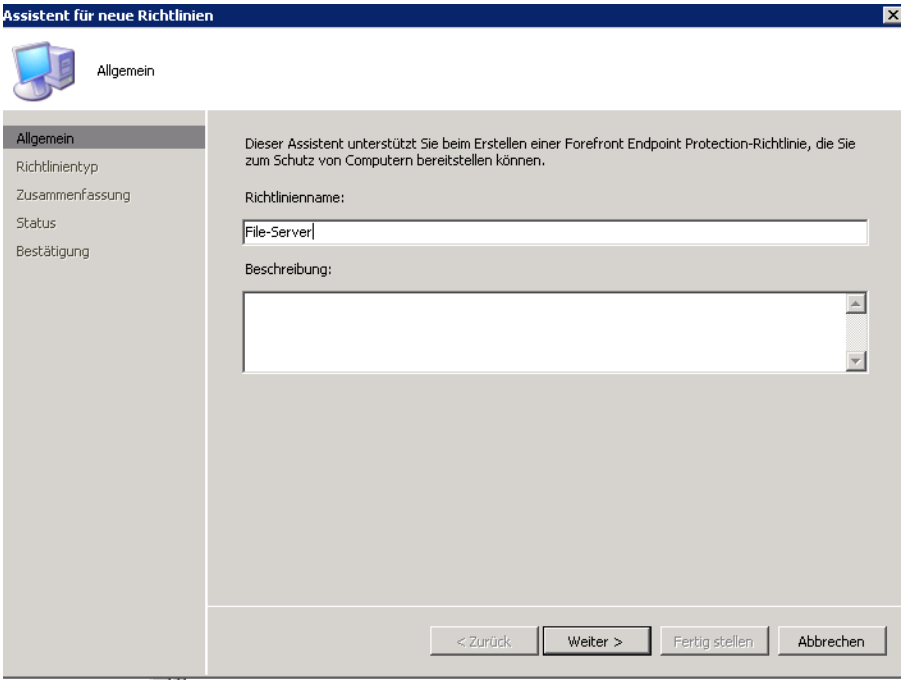
Manuelle Verteilung des SCCM und FEP Clients

SCCM Client:
CCMSetup.exe /mp:Servername.domaene.tld /logon SMSSITECODE=XYZ
FEP Client:
FEPINSTALL.exe /S /Q

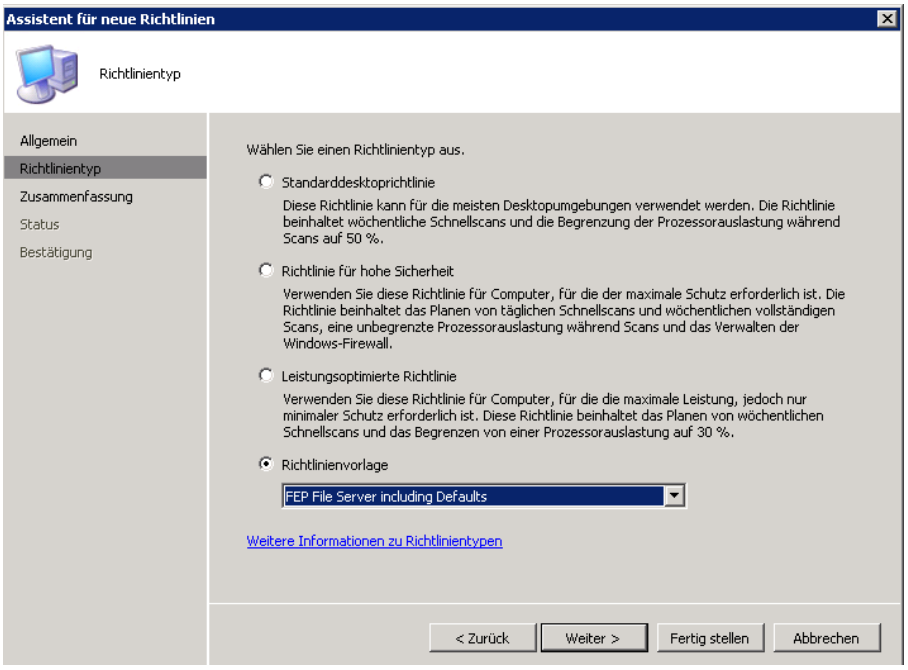
Hier noch was zum Lesen:
http://technet.microsoft.com/en-us/library/bb680980.aspx
http://technet.microsoft.com/en-us/library/gg412485.aspx

Forefront Endpoint Policy erstellen

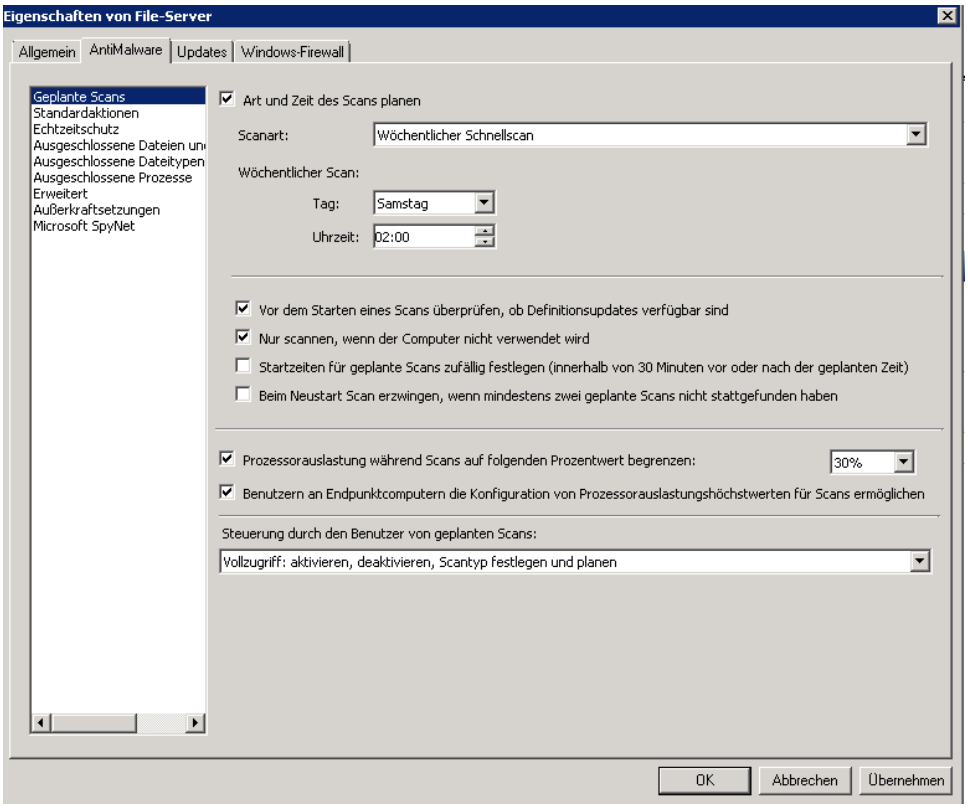




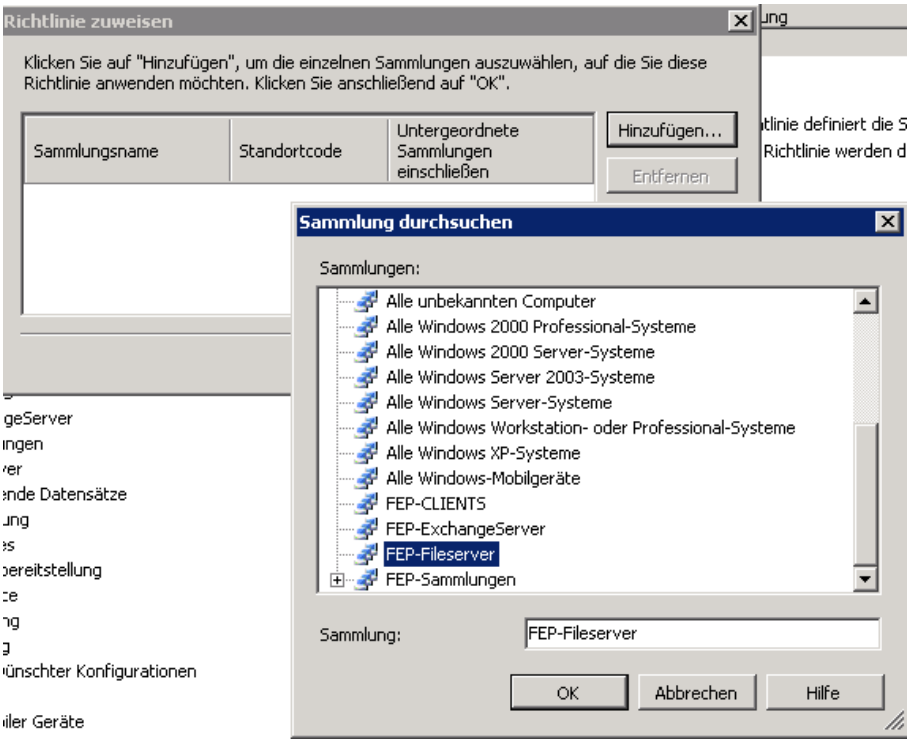
Vorlage auswaehlen



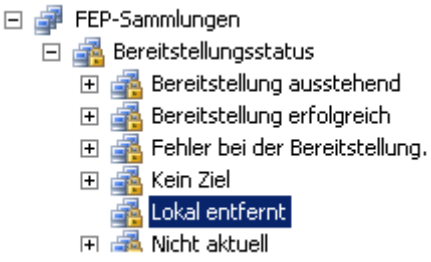
Richtlinie anpassen



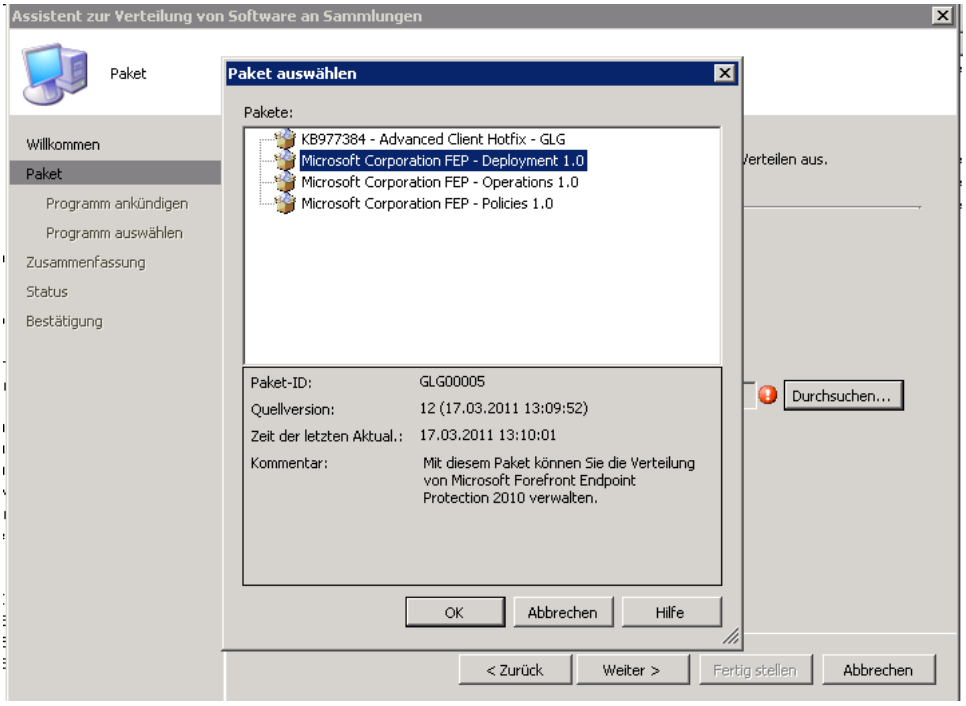
Richtlinie zuweisen

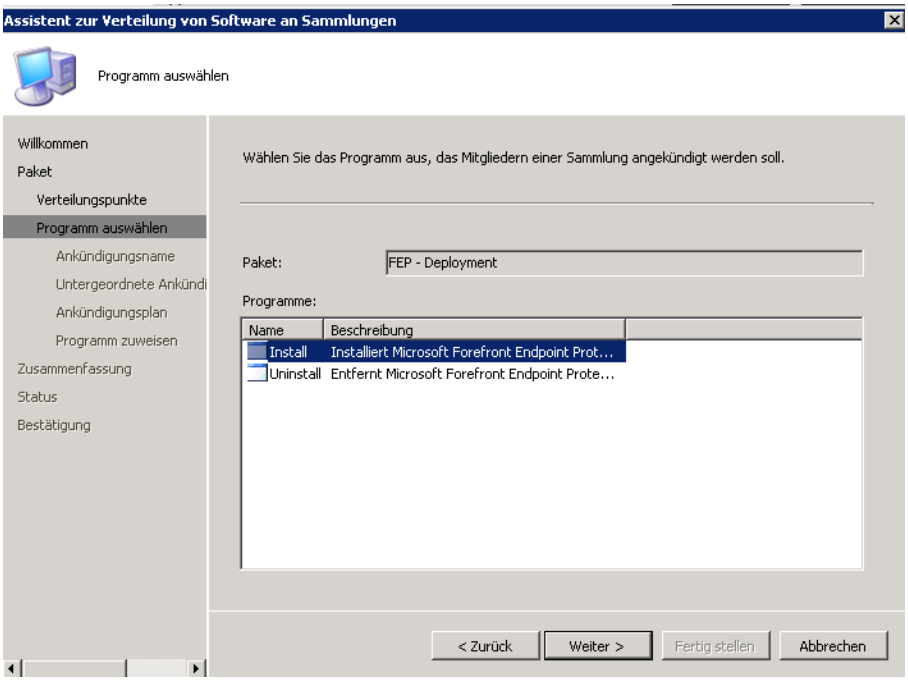


Aus Sicherheitsgruenden sollte man die FEP Policy auch der FEP Collection „Lokal entfernt“ zuweisen, falls ein Admin den Client manuell deinstalliert

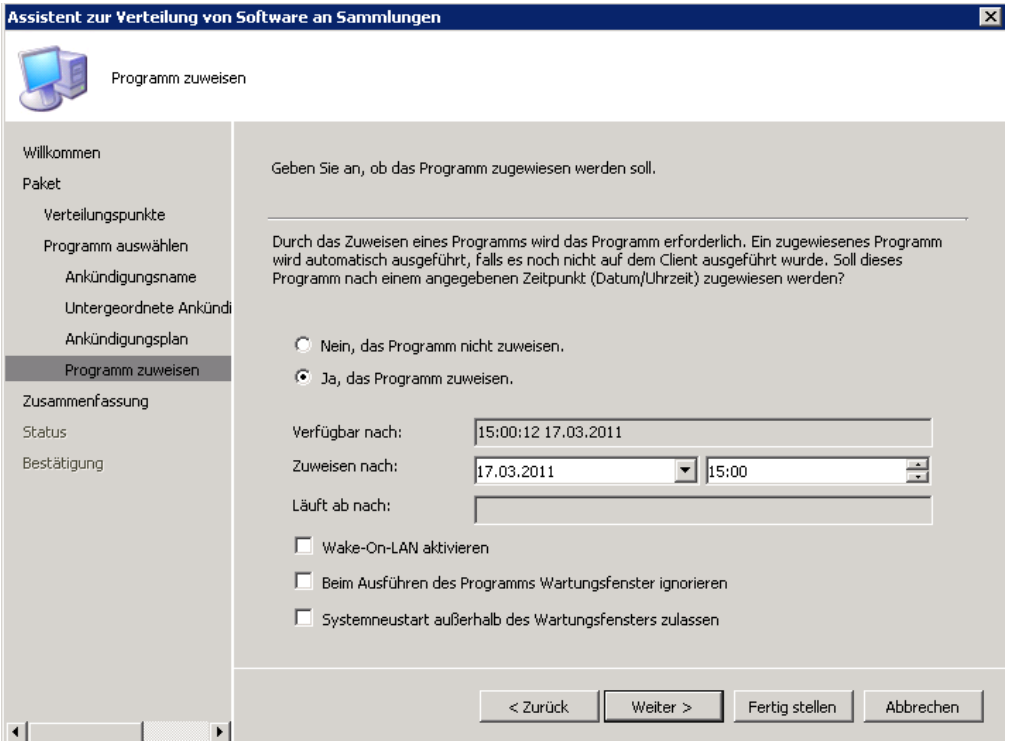


Pakete verteilen

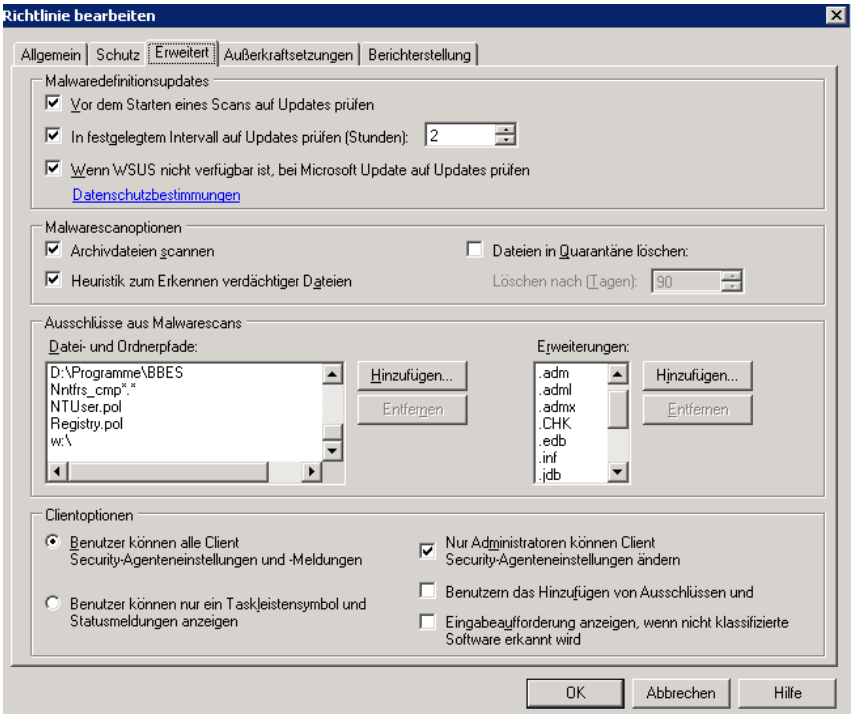




Paket zuweisen

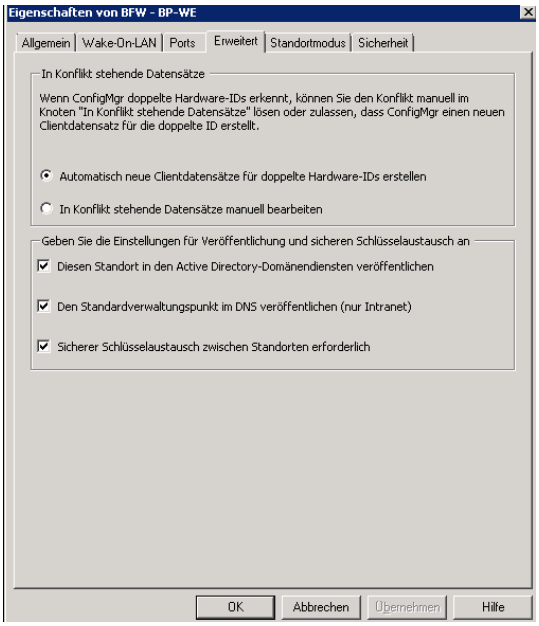


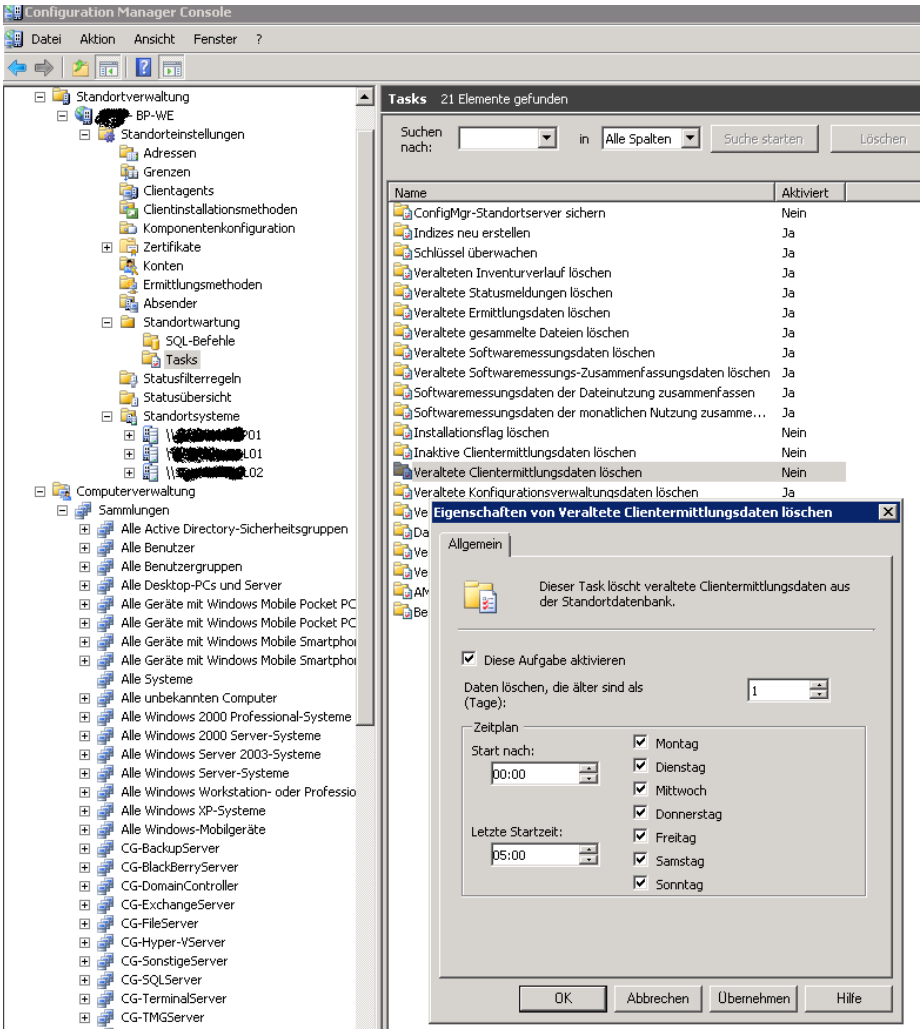
Ggfs. Uebernahme der Custom FCS Einstellungen in den Policies



Veraltete Clientdaten loeschen

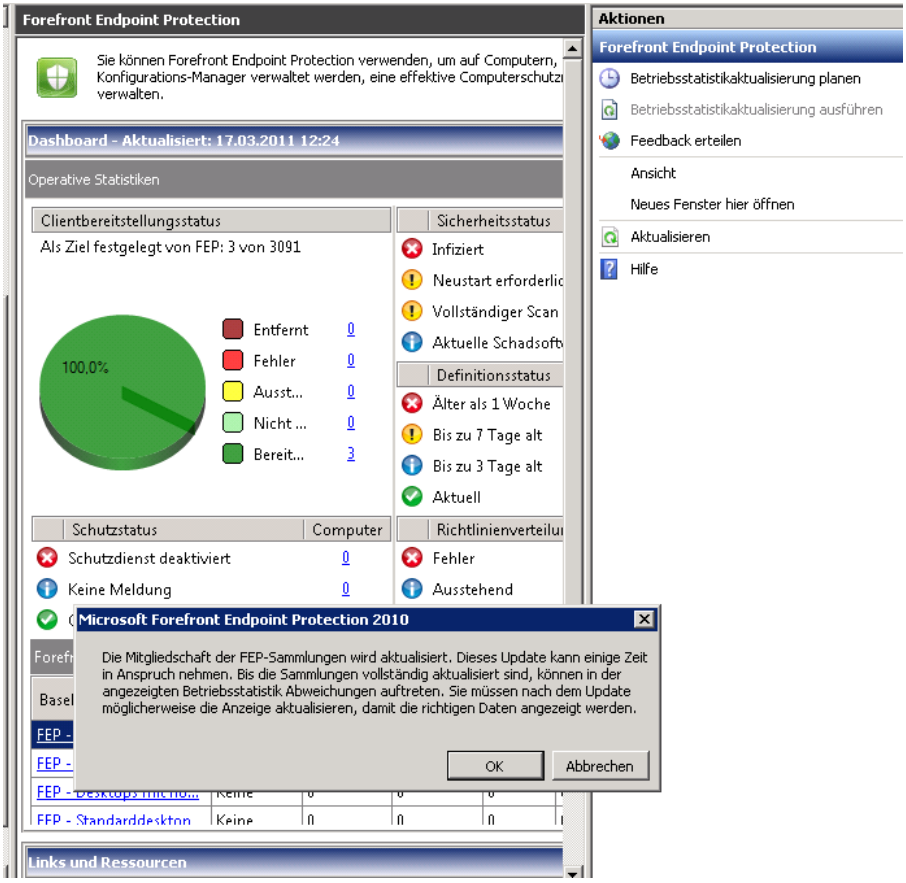
Sollte durch eine Neubespielung des Clients der SCCM Client doppelt in der SCCM Verwaltung auftauchen, kann dieser manuell oder automatisch geloescht werden.


Eigenschaften von BFW - BP-WE
Allgemein
Wake-On-LAN
Ports
Erweitert
Standortmodus
Sicherheit
In Konflikt stehende Datensätze
Wenn ConfigMgr doppelte Hardware-IDs erkennt, können Sie den Konflikt manuell im Knoten "In Konflikt stehende Datensätze" lösen oder zulassen, dass ConfigMgr einen neuen Clientdatensatz für die doppelte ID erstellt.
Automatisch neue Clientdatensätze für doppelte Hardware-IDs erstellen
In Konflikt stehende Datensätze manuell bearbeiten
Geben Sie die Einstellungen für Veröffentlichung und sicheren Schlüsselaustausch an
Diesen Standort in den Active Directory-Domänendiensten veröffentlichen
Den Standardverwaltungspunkt im DNS veröffentlichen (nur Intranet)
Sicherer Schlüsselaustausch zwischen Standorten erforderlich
OK
Abbrechen
Übernehmen
Hilfe

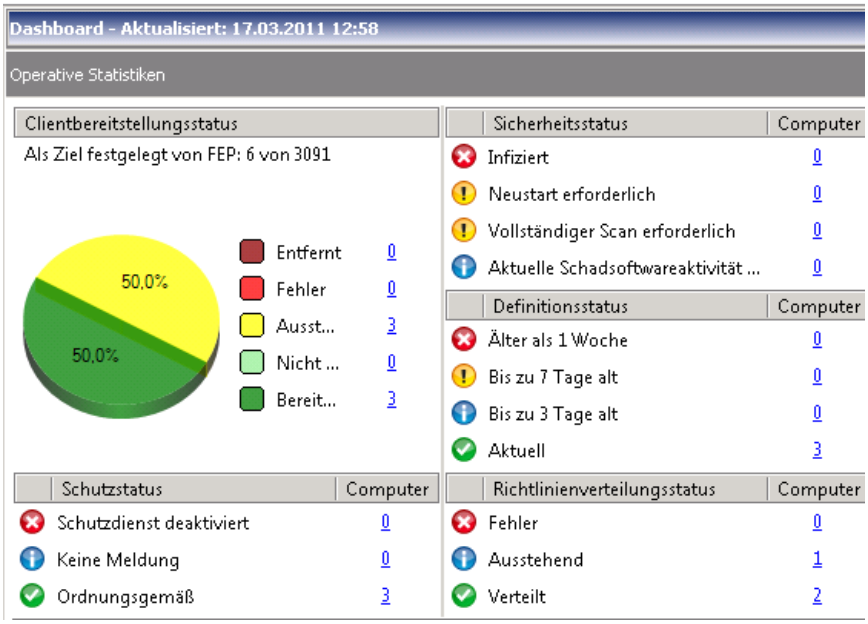

Configuration Manager Console
Datei
Aktion
Ansicht
Fenster
?
Standortverwaltung
BP-WE
Standorteinstellungen
Adressen
Grenzen
Clientagents
Clientinstallationsmethoden
Komponentenkonfiguration
Zertifikate
Konten
Ermittlungsmethoden
Absender
Standortwartung
SQL-Befehle
Tasks
Statusfilterregeln
Statusübersicht
Standortsysteme
Computerverwaltung
Sammlungen
Alle Active Directory-Sicherheitsgruppen
Alle Benutzer
Alle Benutzergruppen
Alle Desktop-PCs und Server
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 XP-Systeme
Alle Windows-Mobilgeräte
CG-BackupServer
CG-BlackBerryServer
CG-DomainController
CG-ExchangeServer
CG-FileServer
CG-Hyper-VServer
CG-SonstigeServer
CG-SQLServer
CG-TerminalServer
CG-TMGServer
Tasks 21 Elemente gefunden
Suchen nach:
in
Alle Spalten
Suche starten
Löschen
Name
Aktiviert
ConfigMgr-Standortserver sichern Nein
Indizes neu erstellen Ja
Schlüssel überwachen Ja
Veralteten Inventurverlauf löschen Ja
Veraltete Statusmeldungen löschen Ja
Veraltete Ermittlungsdaten löschen Ja
Veraltete gesammelte Dateien löschen Ja
Veraltete Softwaremessungsdaten löschen Ja
Veraltete Softwaremessungs-Zusammenfassungsdaten löschen Ja
Softwaremessungsdaten der Dateinutzung zusammenfassen Ja
Softwaremessungsdaten der monatlichen Nutzung zusamme... Ja
Installationsflag löschen Nein
Inaktive Clientermittlungsdaten löschen Nein
Veraltete Clientermittlungsdaten löschen Nein
Veraltete Konfigurationsverwaltungsdaten löschen Ja
Eigenschaften von Veraltete Clientermittlungsdaten löschen
Allgemein
Dieser Task löscht veraltete Clientermittlungsdaten aus der Standortdatenbank.
Diese Aufgabe aktivieren
Daten löschen, die älter sind als (Tage):
1
Zeitplan
Start nach:
00:00
Letzte Startzeit:
05:00
Montag
Dienstag
Mittwoch
Donnerstag
Freitag
Samstag
Sonntag
OK
Abbrechen
Übernehmen
Hilfe

FEP Reporting

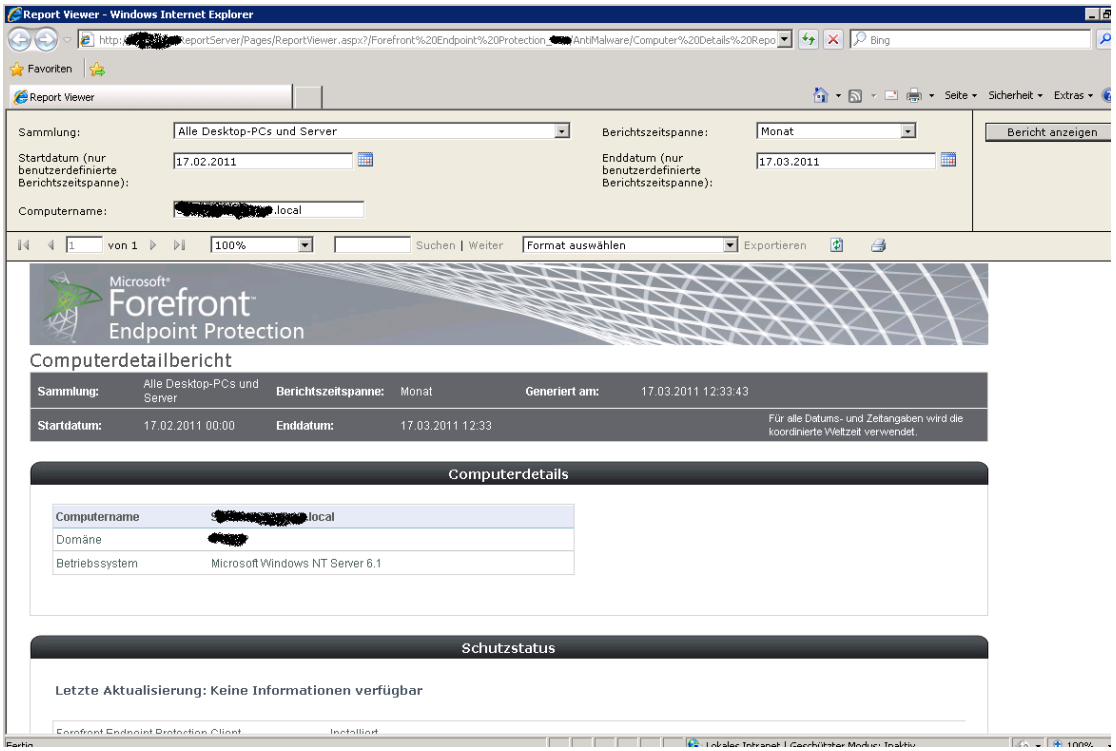
FEP Statistiken aktualisieren



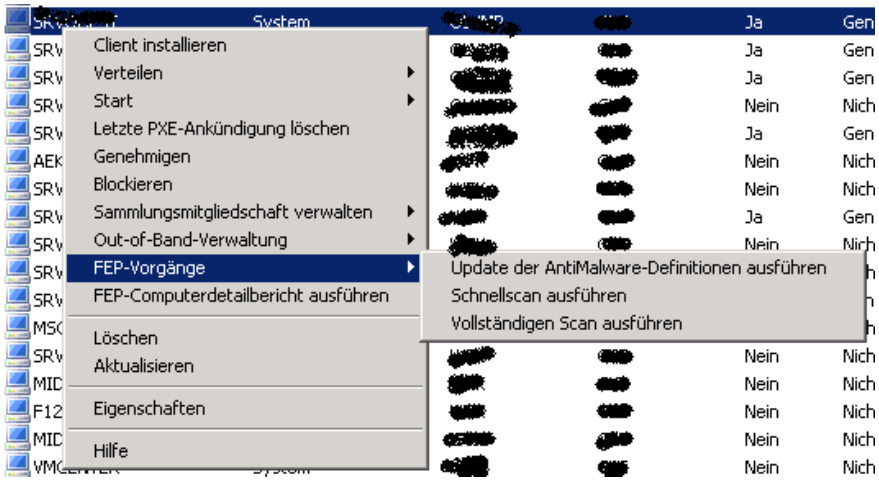
Die Statistik fuellt sich mit Leben. Schon auf fast 6 Servern/Clients FEP ausgerollt ☺

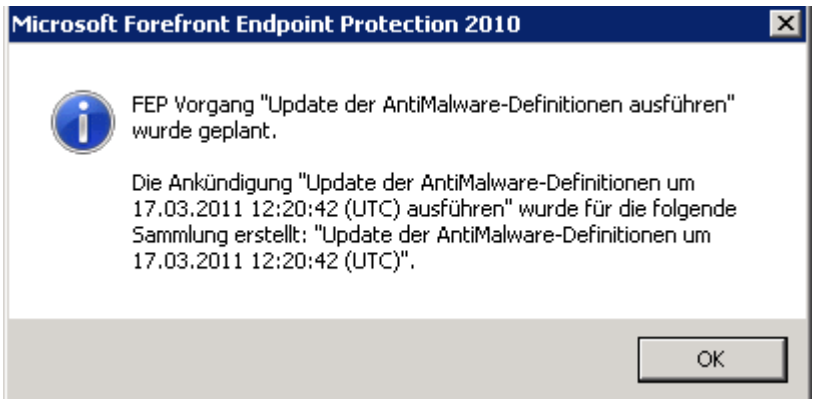


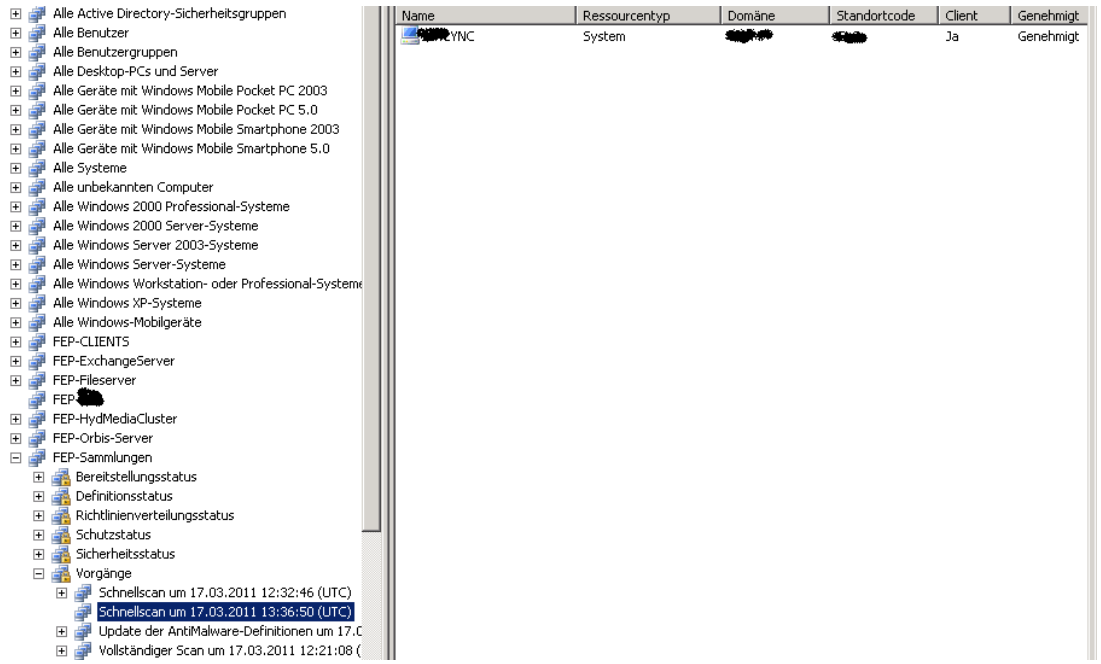
Zusammenfassungsreport eines Servers / Clients



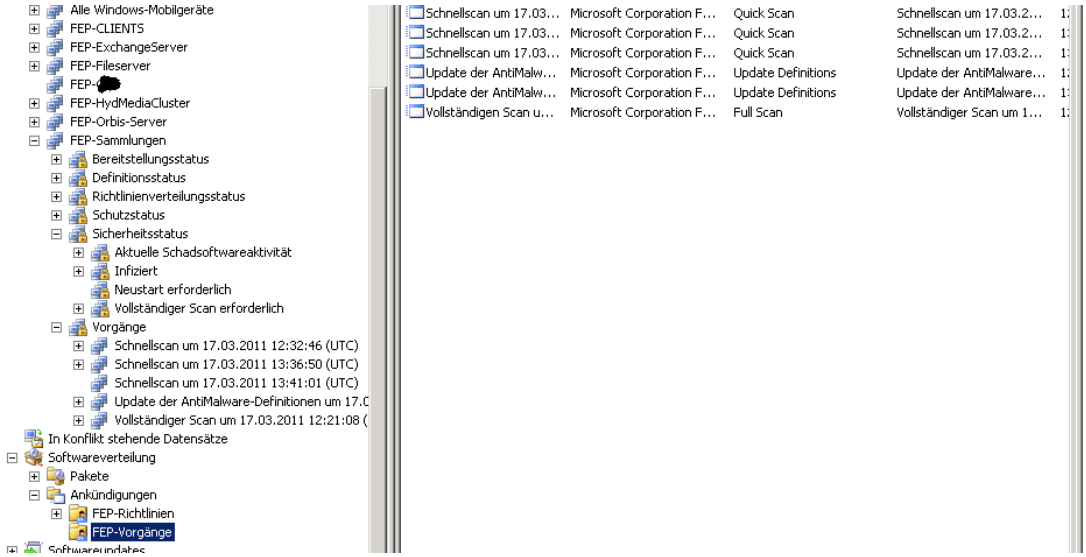
FEP Scans und Updates manuell ausfuehren



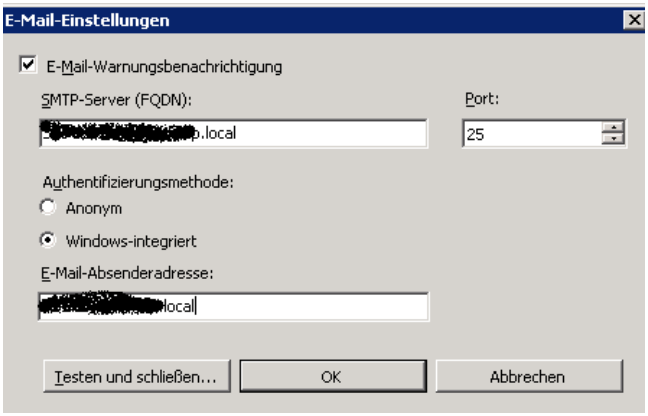


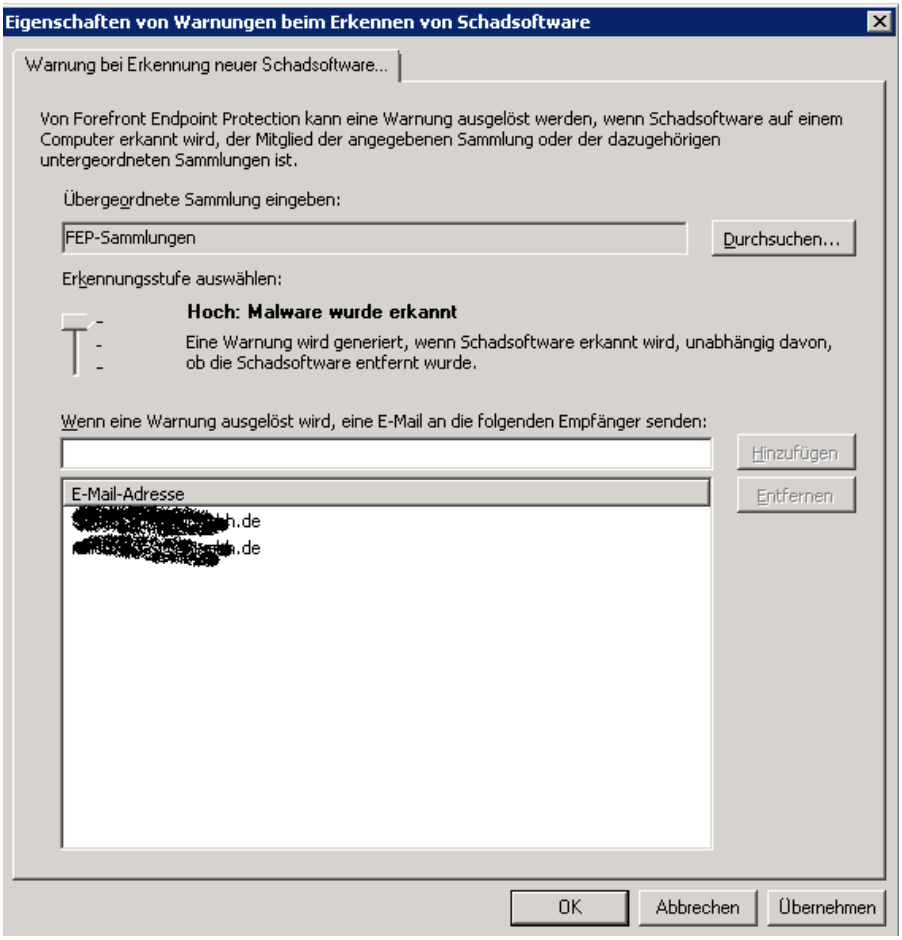


Fuer jeden manuellen FEP Vorgang werden entsprechende Advertisements erstellt



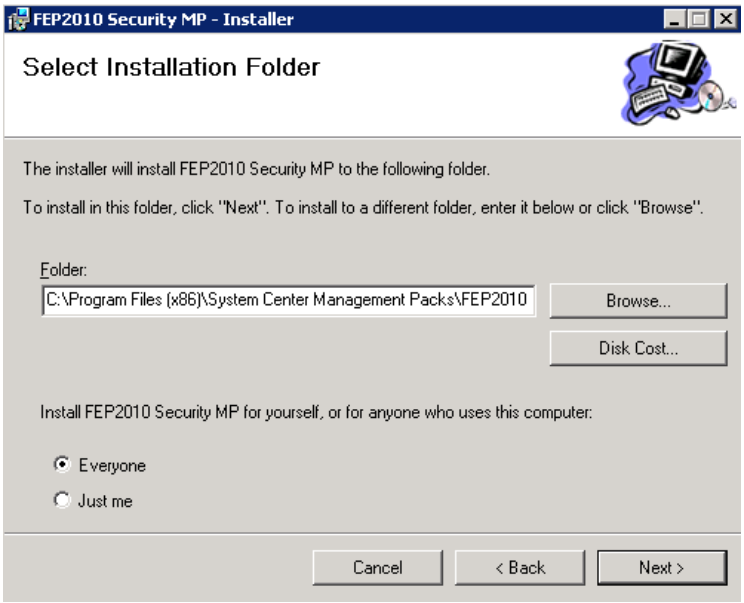
Warnungsbenachrichtigung einrichten





SCOM – FEP Integration

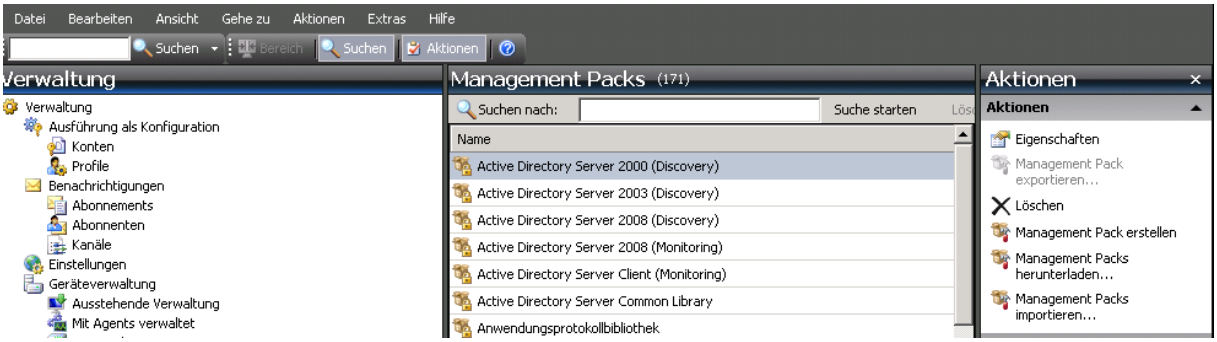
SCOM Management Pack fuer FEP installieren

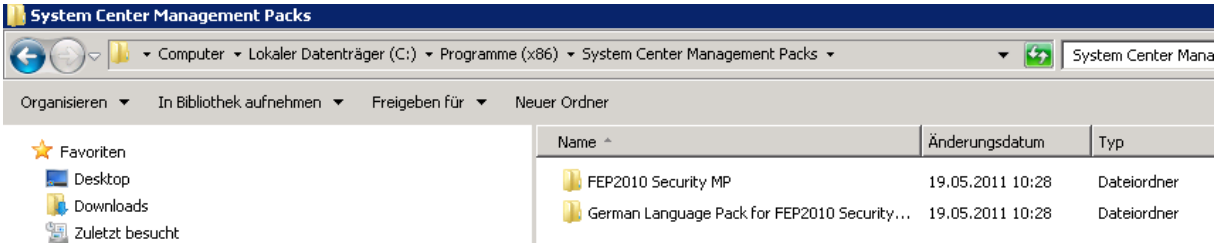


Language Pack fuer FEP installieren

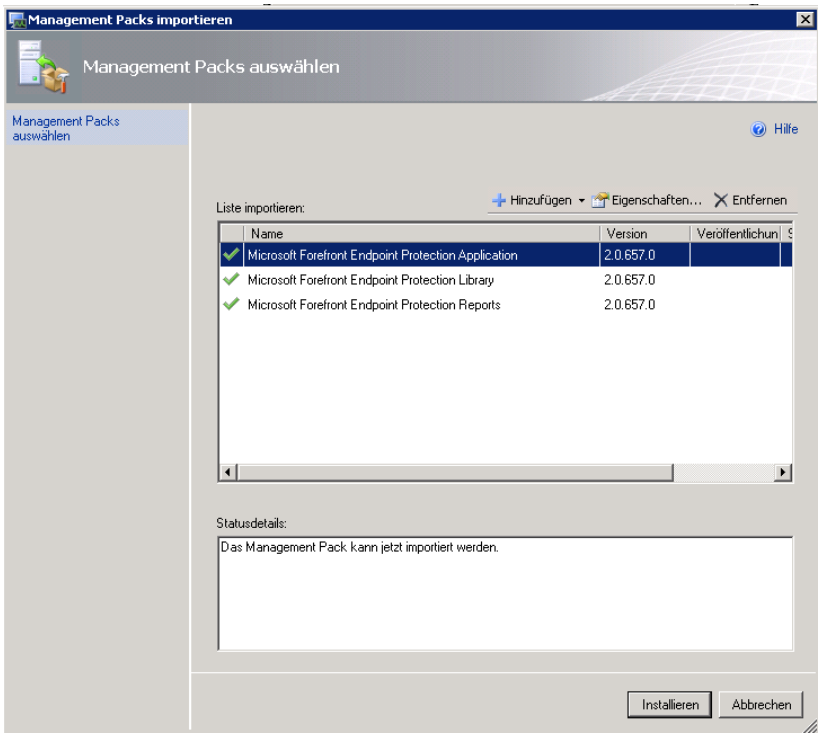
SCOM Operationskonsole starten

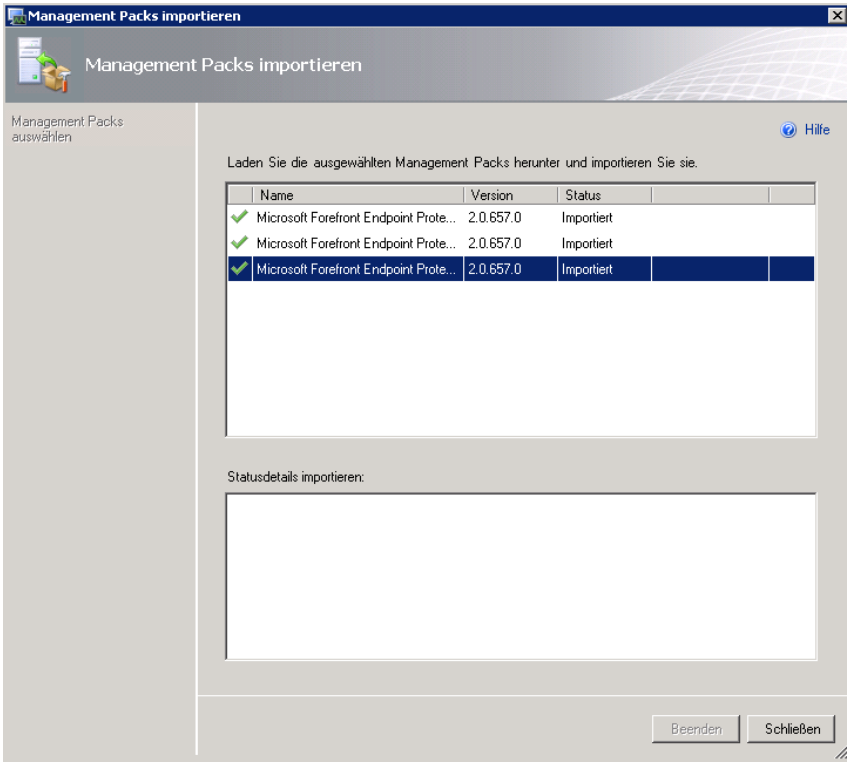
Management Pack importieren



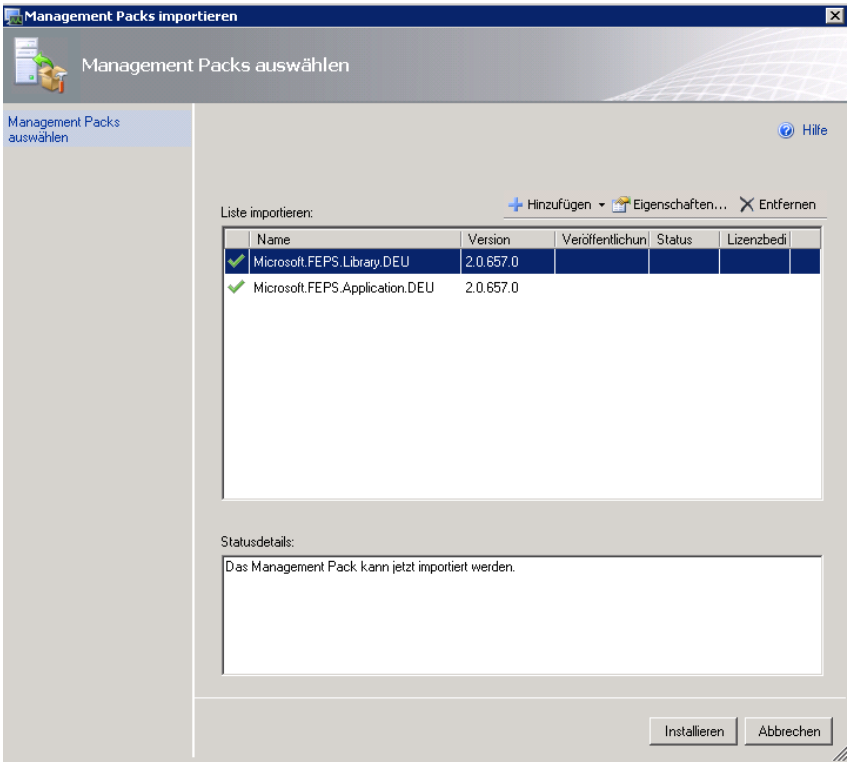


Alle drei MPs importieren

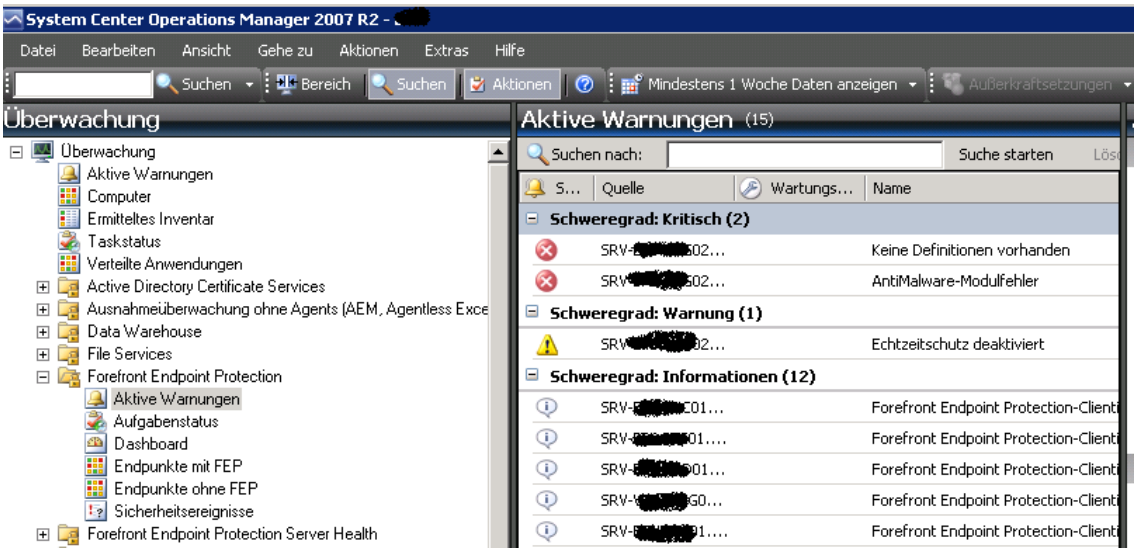




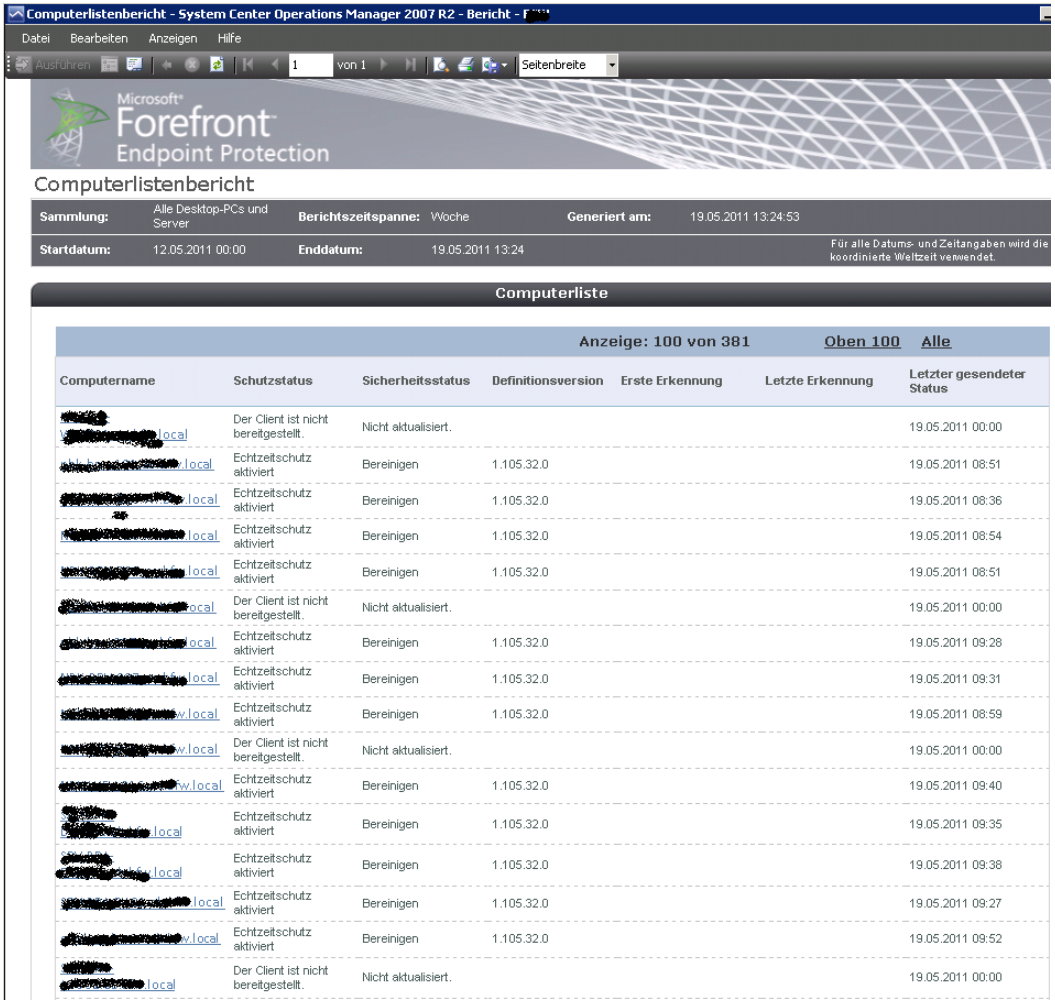
MP Language Pack importieren



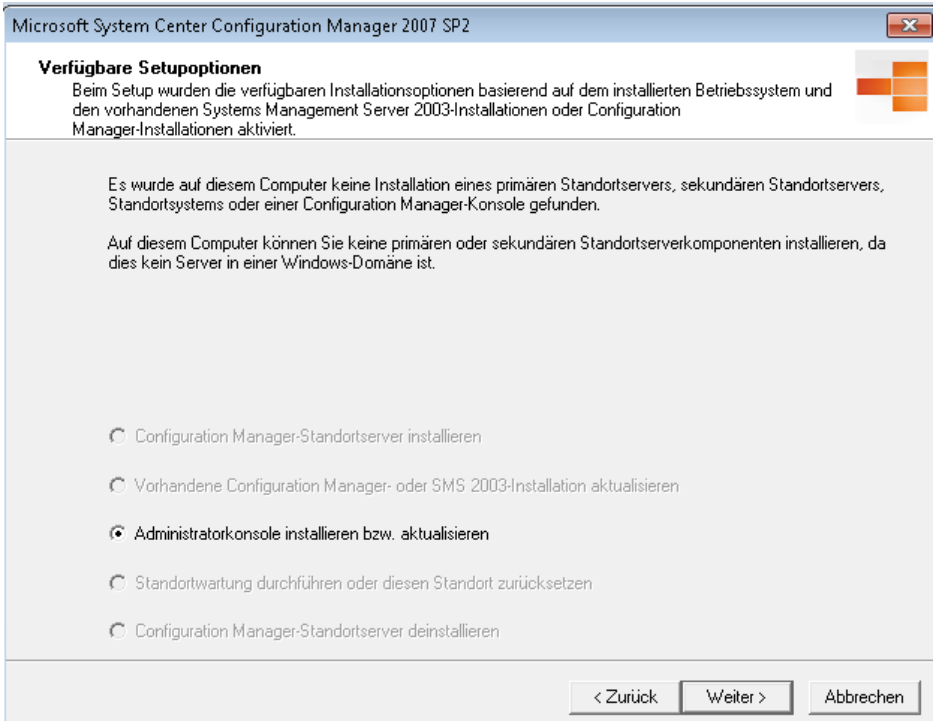
FEP Monitoring

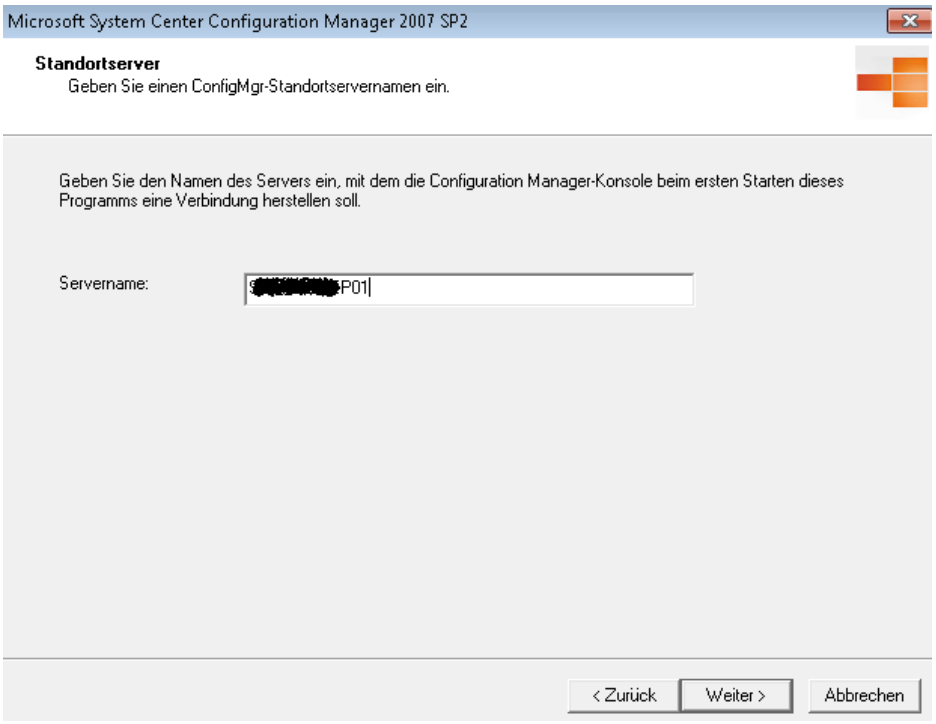


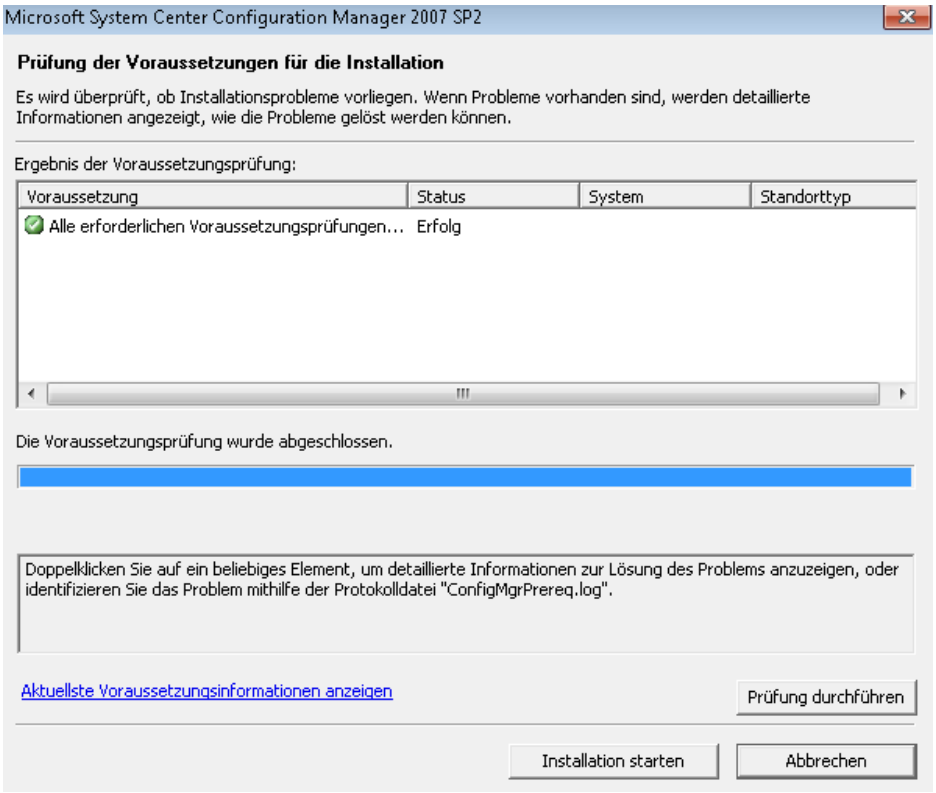
Berichte

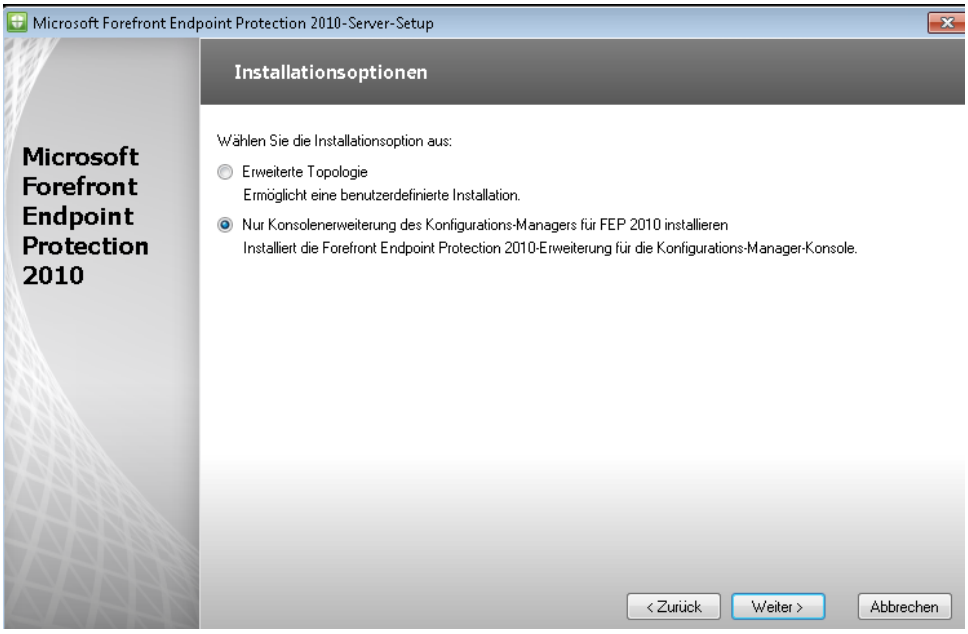


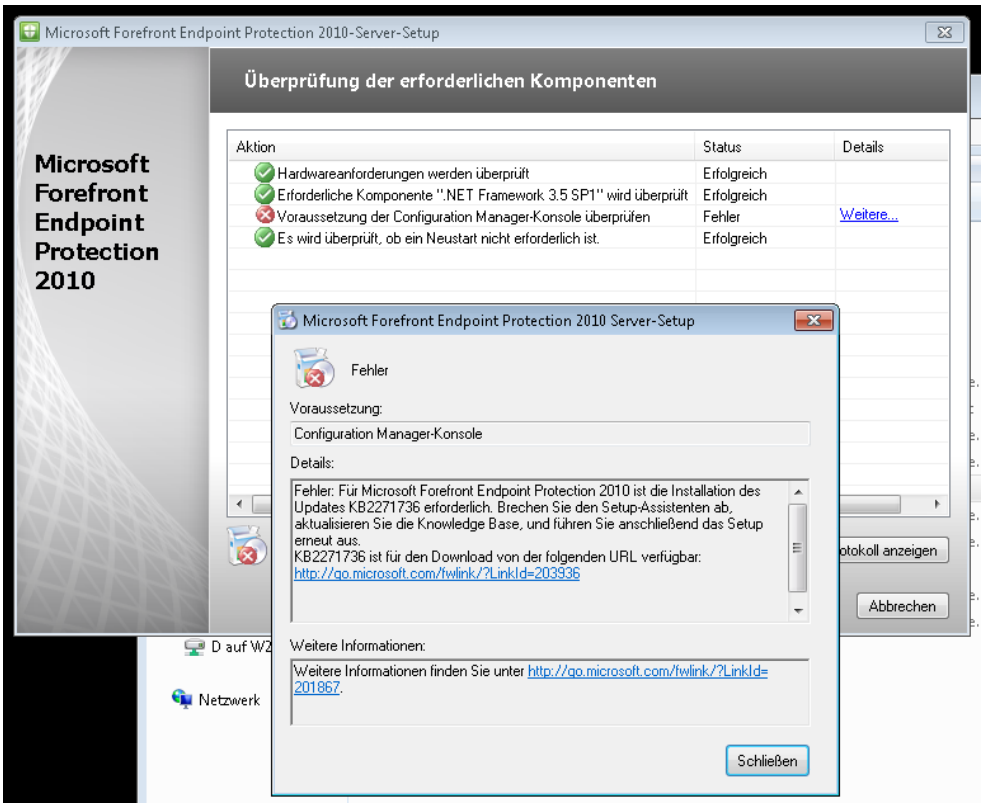
Administrationskonsole auf Admin PCs installieren



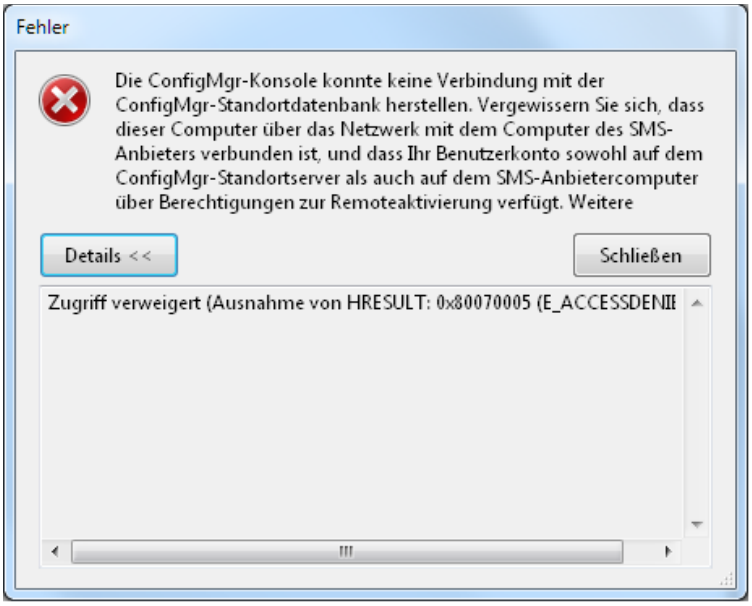



Microsoft System Center Configuration Manager 2007 SP2
Prüfung der Voraussetzungen für die Installation
Es wird überprüft, ob Installationsprobleme vorliegen. Wenn Probleme vorhanden sind, werden detaillierte Informationen angezeigt, wie die Probleme gelöst werden können.
Ergebnis der Voraussetzungsprüfung:
Voraussetzung
Status
System
Standorttyp
Alle erforderlichen Voraussetzungsprüfungen...
Erfolg
Die Voraussetzungsprüfung wurde abgeschlossen.
Doppelklicken Sie auf ein beliebiges Element, um detaillierte Informationen zur Lösung des Problems anzuzeigen, oder identifizieren Sie das Problem mithilfe der Protokolldatei "ConfigMgrPrereq.log".
Aktuellste Voraussetzungsinformationen anzeigen
Prüfung durchführen
Installation starten
Abbrechen


Microsoft Forefront Endpoint Protection 2010-Server-Setup
Installationsoptionen
Microsoft Forefront Endpoint Protection 2010
Wählen Sie die Installationsoption aus:
Erweiterte Topologie
Ermöglicht eine benutzerdefinierte Installation.
Nur Konsolenerweiterung des Konfigurations-Managers für FEP 2010 installieren
Installiert die Forefront Endpoint Protection 2010-Erweiterung für die Konfigurations-Manager-Konsole.
< Zurück
Weiter >
Abbrechen



Fehlermeldung beim Aufruf der Konsole

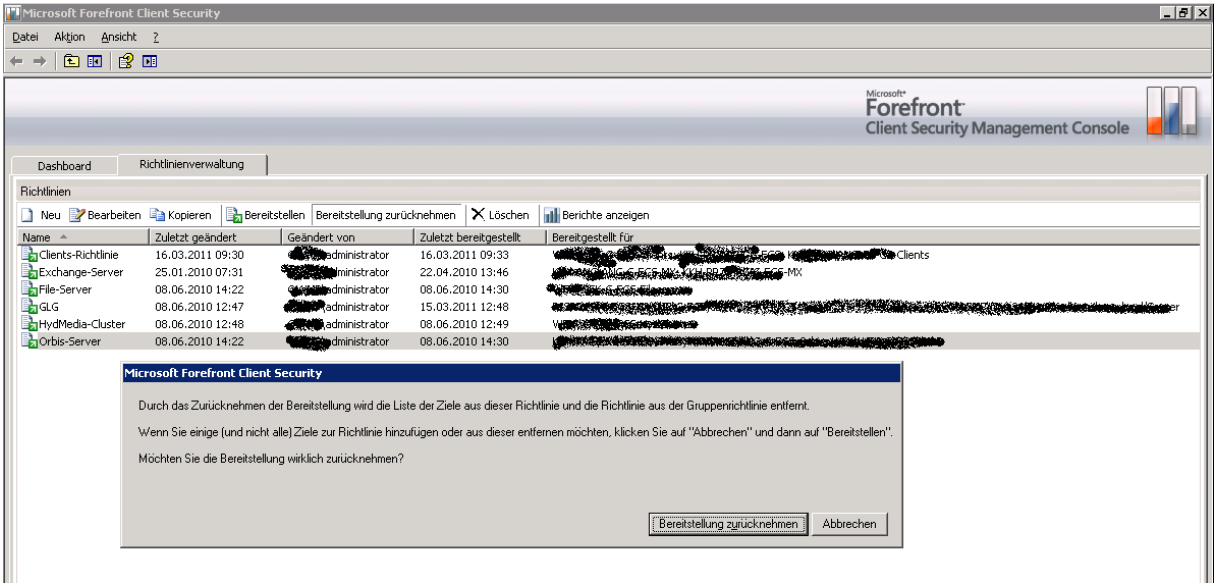


Loesung:
http://technet.microsoft.com/de-de/library/bb932213.aspx
DCOM Berechtigungen fuer Remoteausfuehrung fuer die SCCM Accounts setzen, welche die Remotekonsole aufrufen duerfen.

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