

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:

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

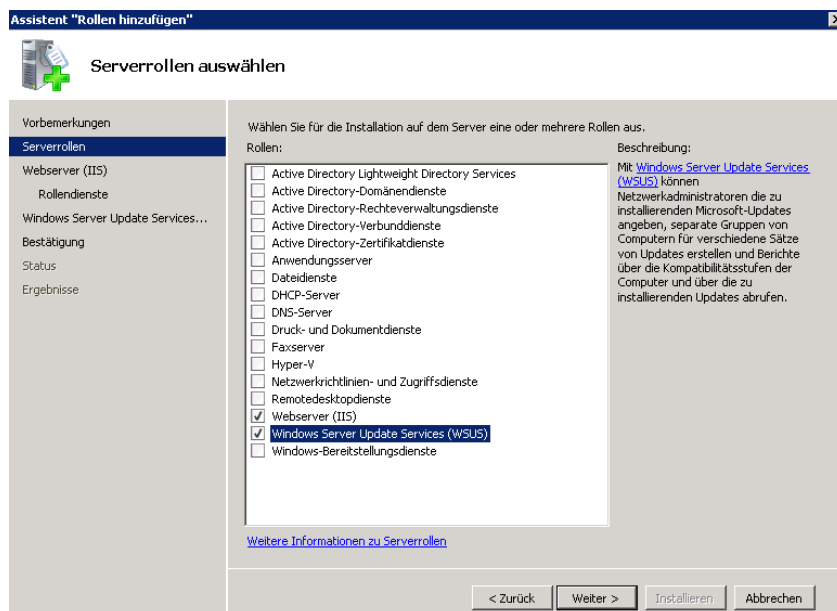
Weitere Informationen zu FEP:

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

Windows Server Installation / Konfiguration

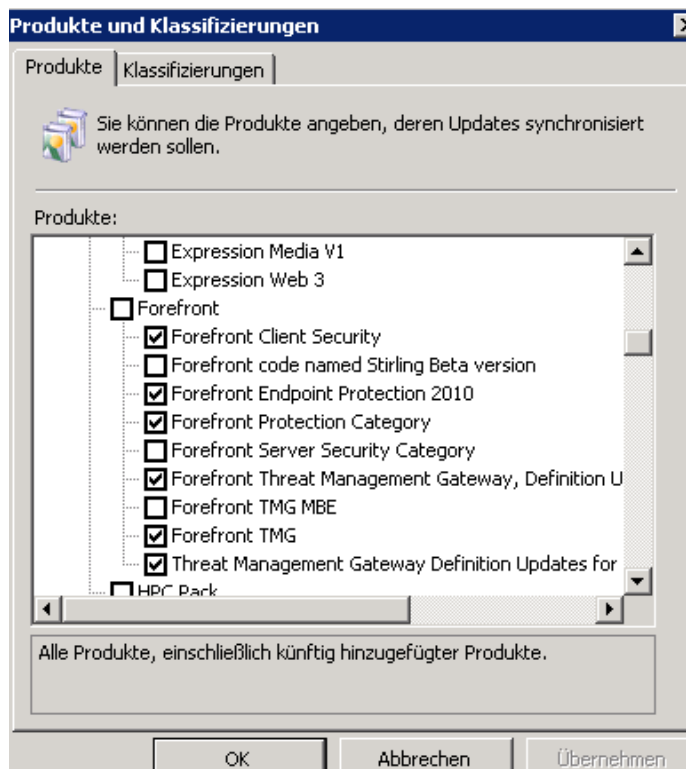
Windows Server 2008 R2 installieren / patchen / Hardware und System requirements fuer FEP: <http://www.microsoft.com/forefront/endpoint-protection/en/us/system-requirements.aspx>

WSUS installieren

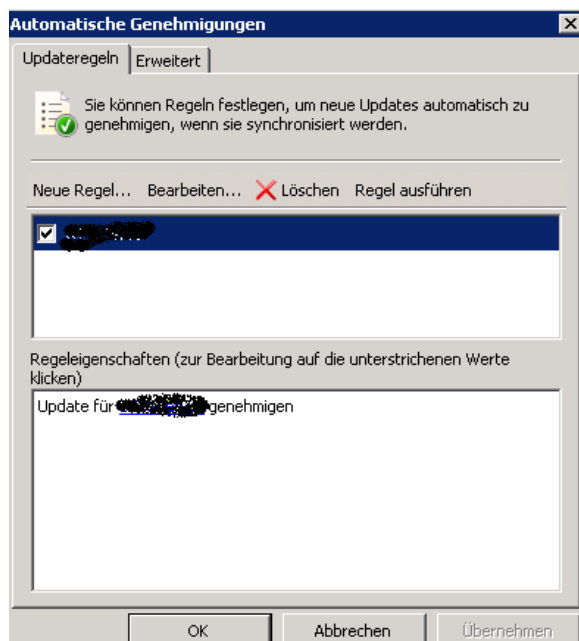


WSUS nach Vorgaben konfigurieren

Produkte und Klassifizierungen auswaehlen



Automatische Genehmigungen konfigurieren



Datenbank auf den zentralen SQL Server Cluster legen

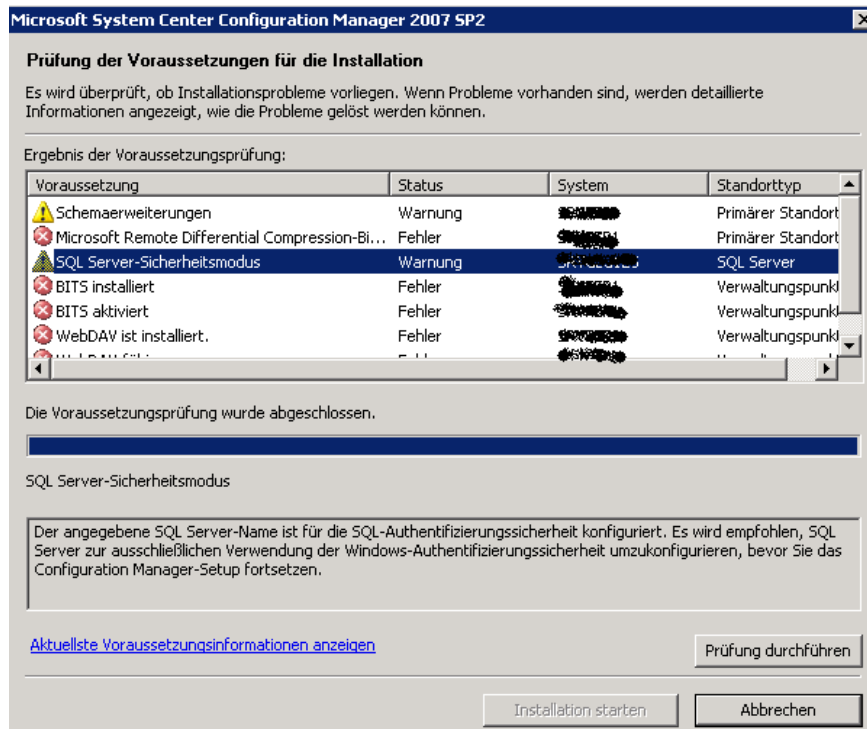
WSUS Migration (wenn der FCS Server auch WSUS Server war)

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

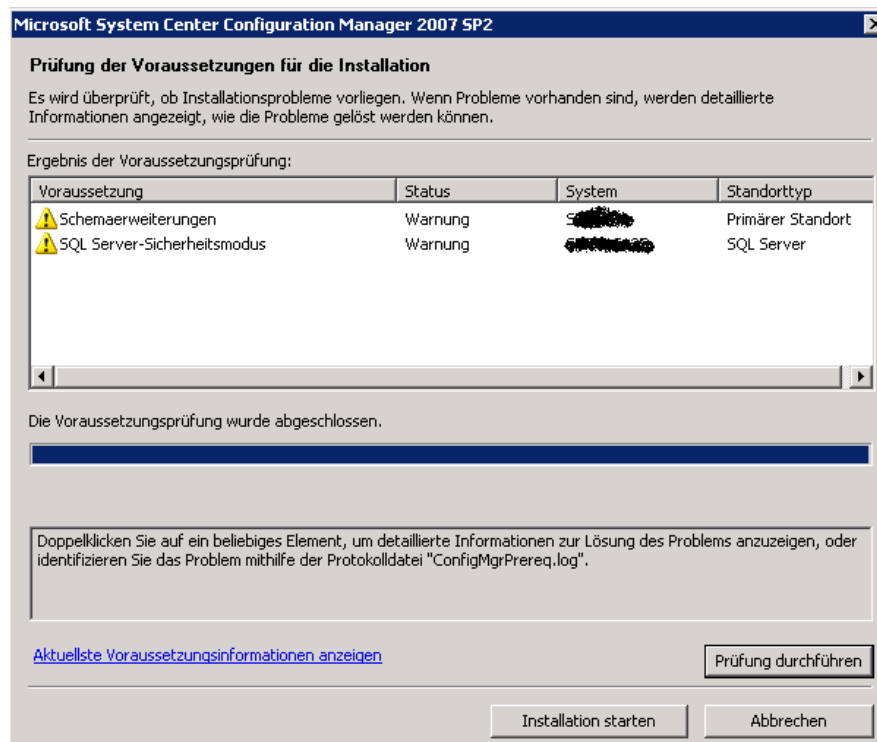
SCCM Installation

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

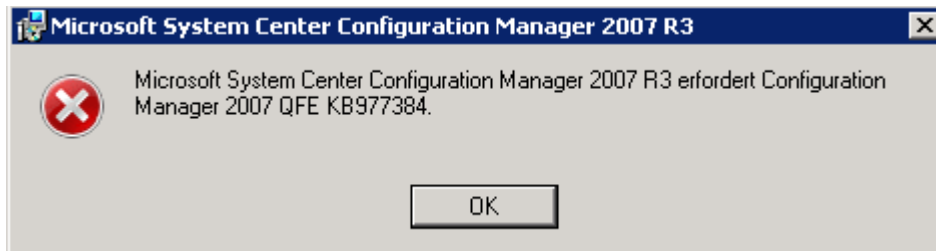


Besser

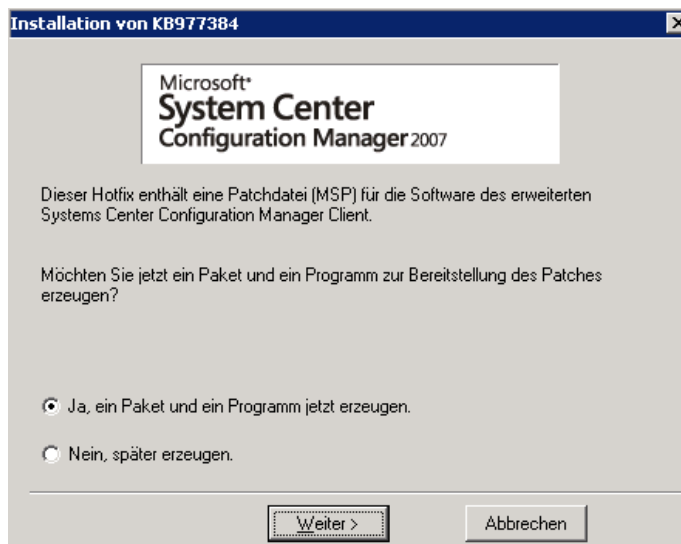
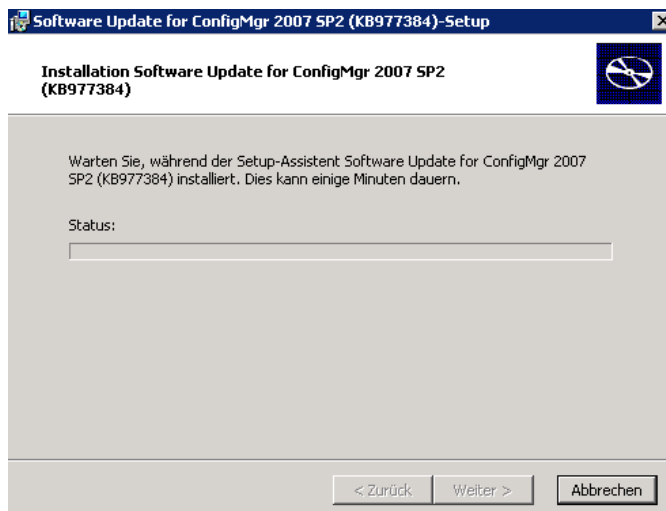


SCCM 2007 R2 installieren

SCCM 2007 R3 installieren

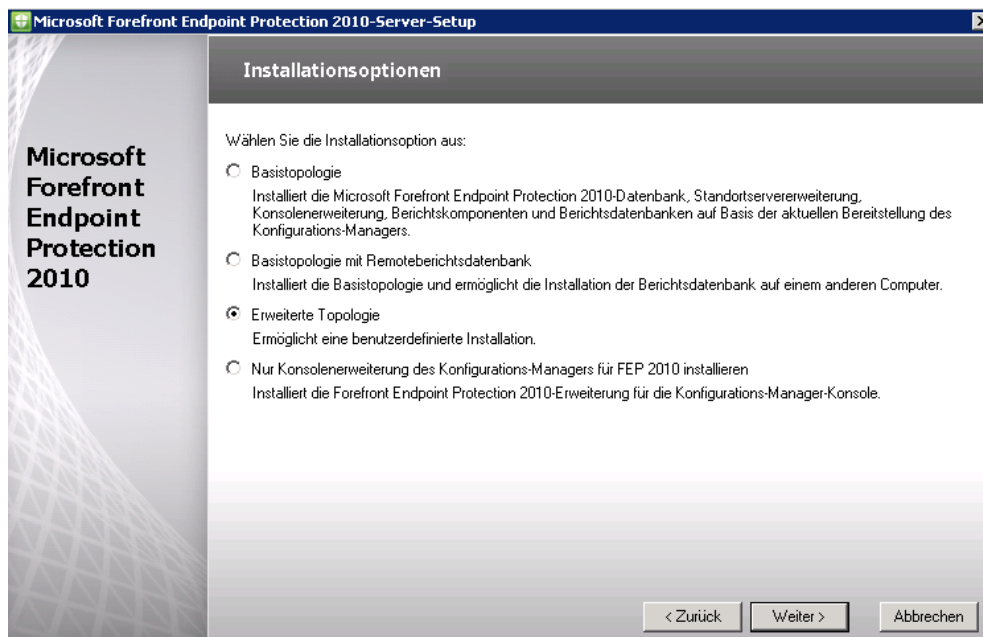


Hotfix installieren

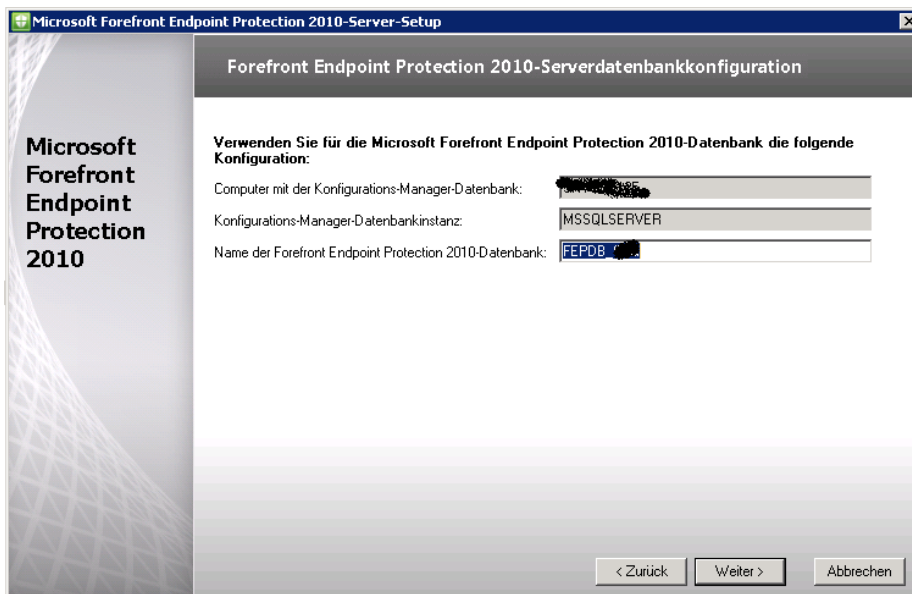


FEP 2010 Installation

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:

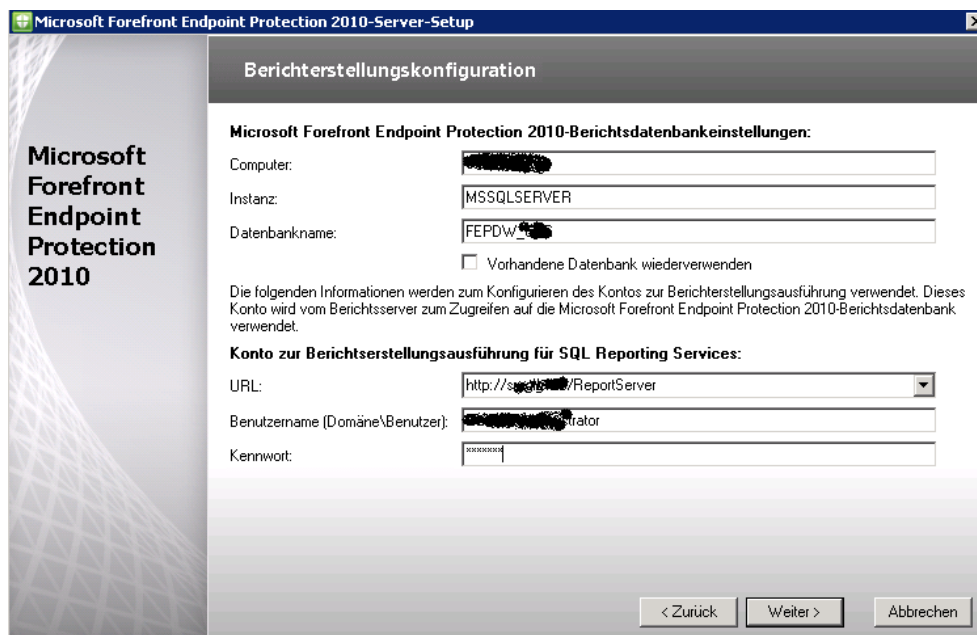
Computer mit der Konfigurations-Manager-Datenbank: [REDACTED]

Konfigurations-Manager-Datenbankinstanz: MSSQLSERVER

Name der Forefront Endpoint Protection 2010-Datenbank: FEPOB [REDACTED]

< Zurück Weiter > Abbrechen

Berichterstellungskonfiguration



Microsoft Forefront Endpoint Protection 2010-Server-Setup

Berichterstellungskonfiguration

Microsoft Forefront Endpoint Protection 2010-Berichtsdatenbankeinstellungen:

Computer: [REDACTED]

Instanz: MSSQLSERVER

Datenbankname: FEPOB [REDACTED]

☐ 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

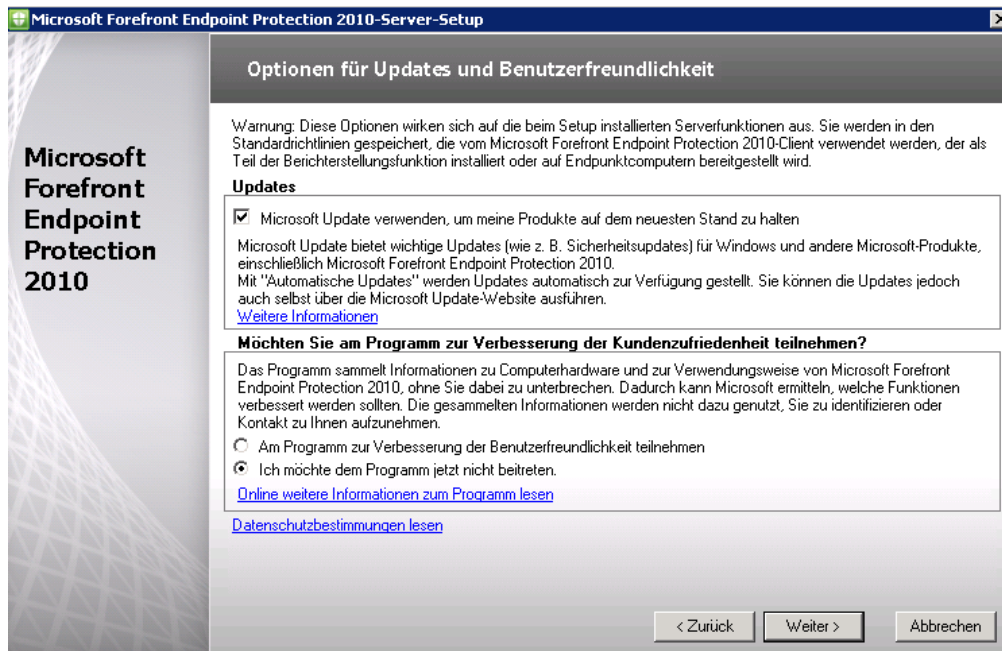
Benutzername (Domäne\Benutzer): [REDACTED]\Administrator

Kennwort: [REDACTED]

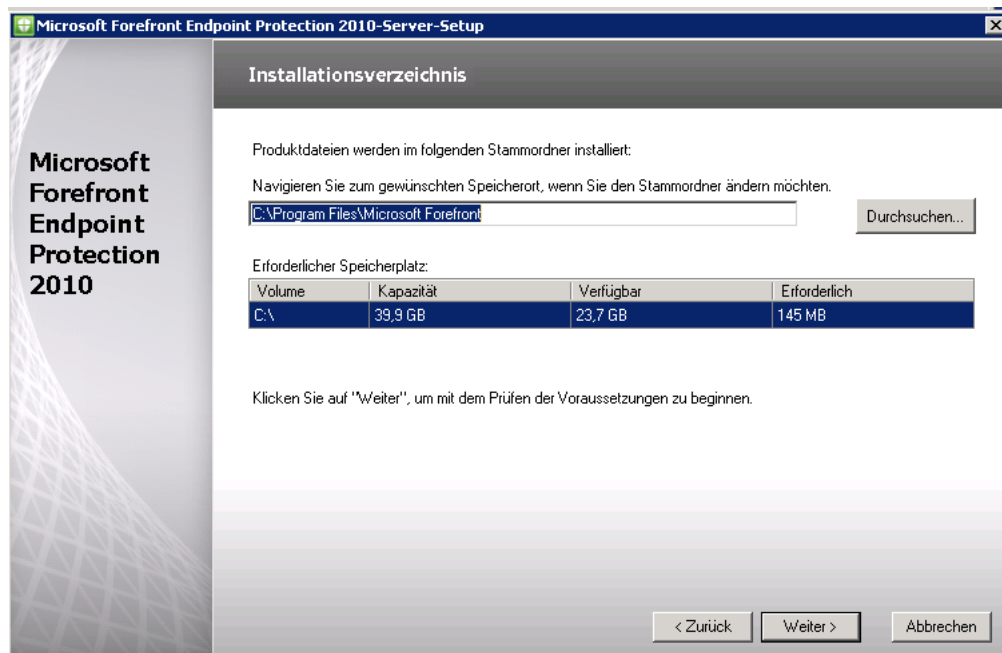
< Zurück Weiter > Abbrechen

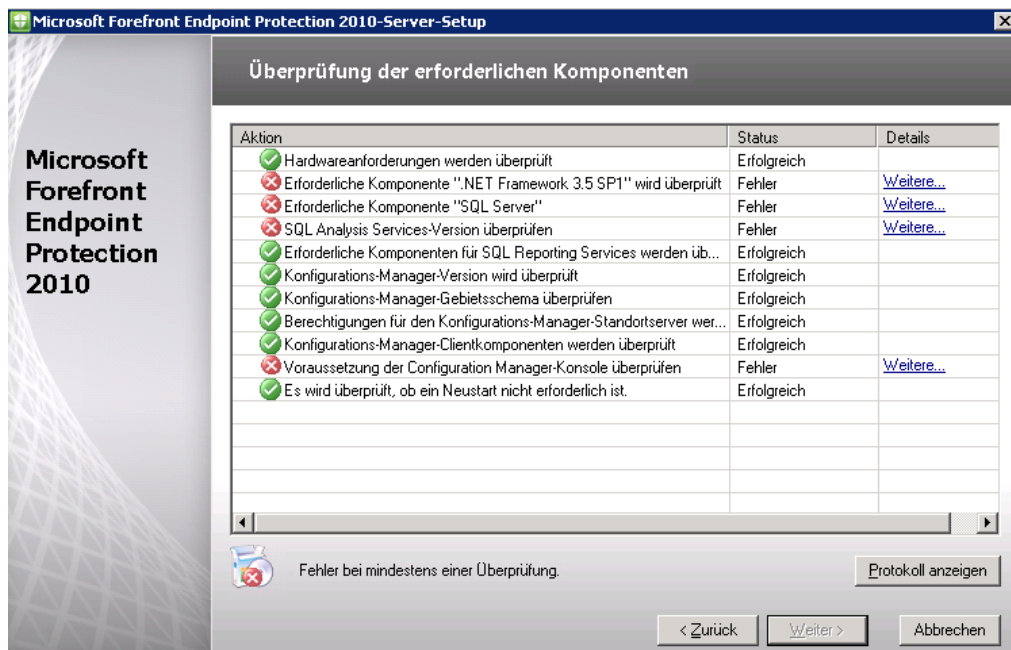
Falls sich die Reporting Services nicht auf einem Windows Server 2008 x64 installieren lassen, könnte das hieran liegen:

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

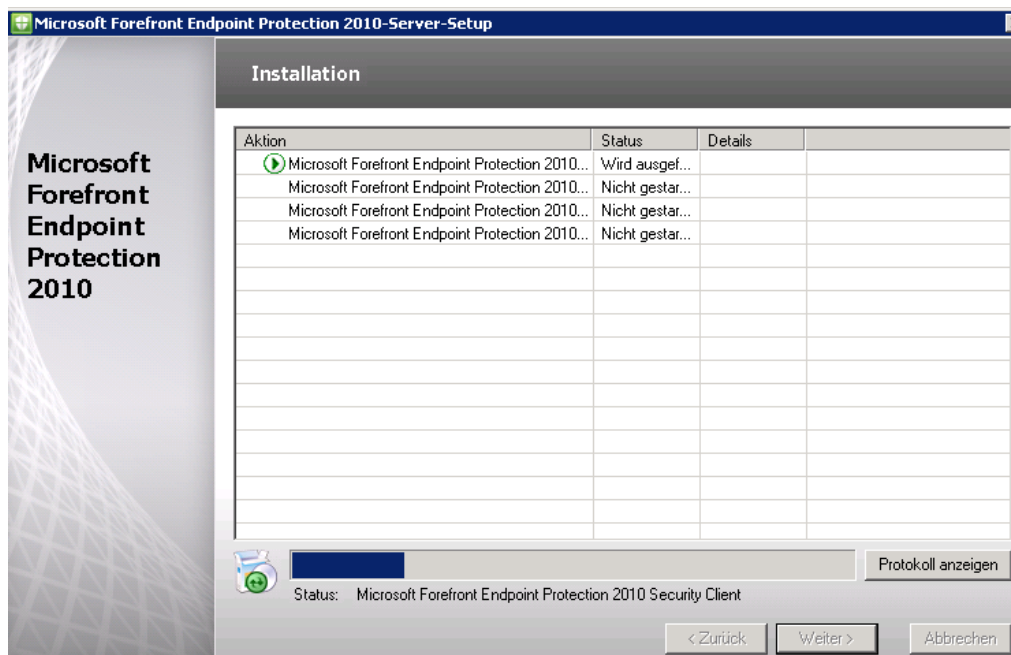


Installationspfad



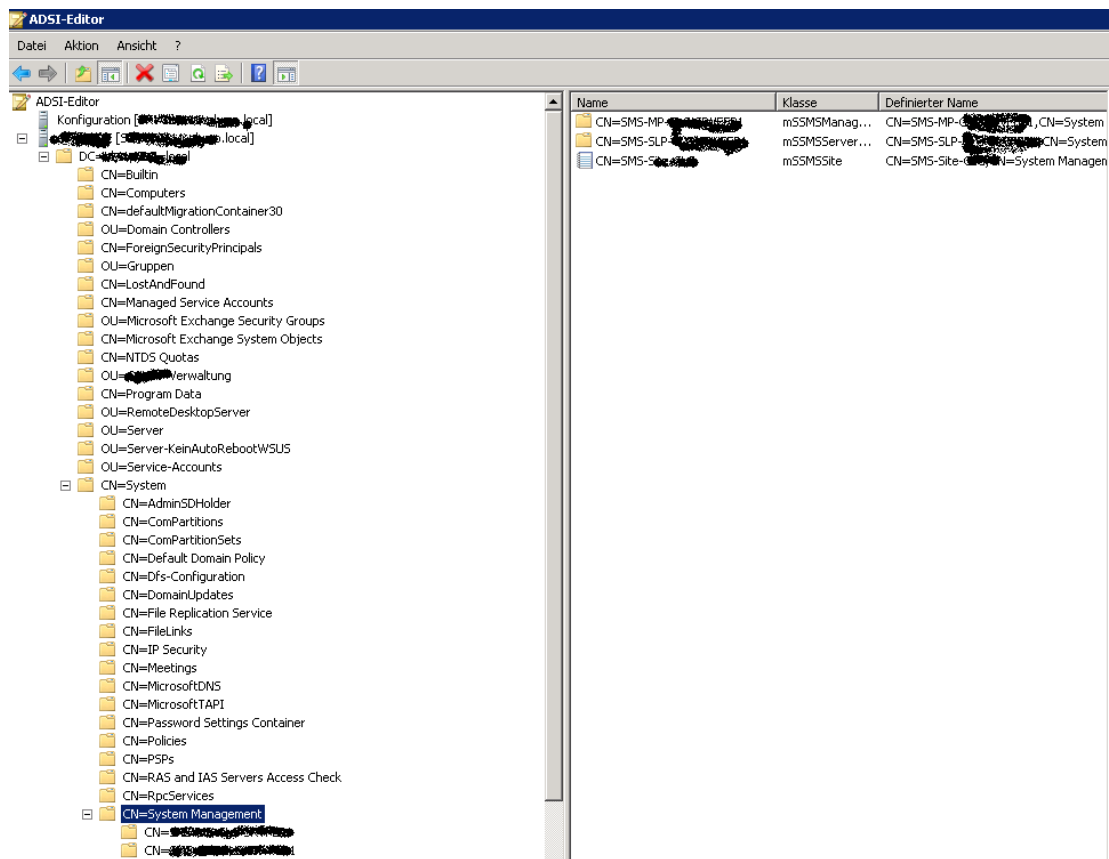


Alle Fehler behoben, dann kann das Setup starten

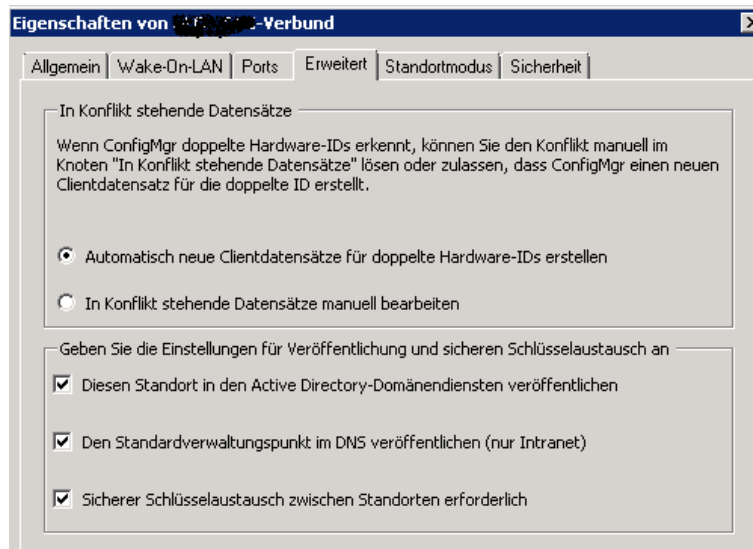


Schema fuer SCCM erweitern

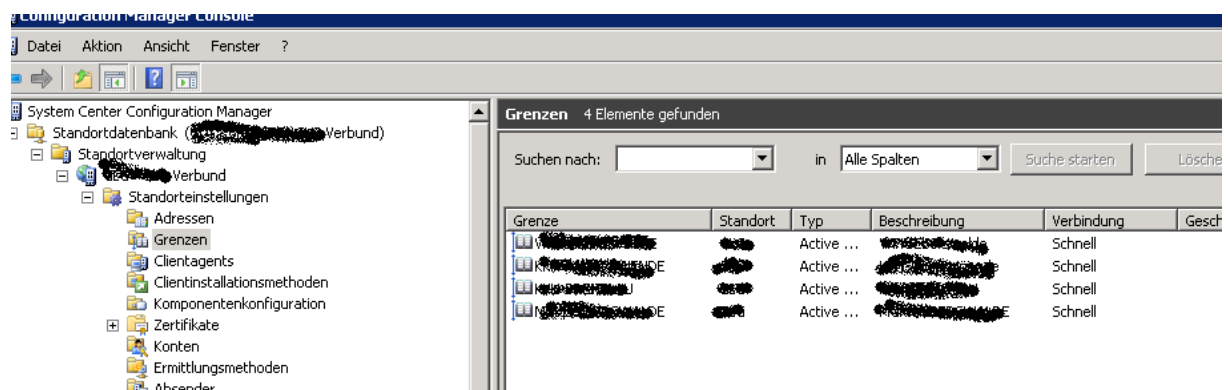
<http://technet.microsoft.com/en-us/library/bb680432.aspx>



SCCM fuer AD Connection Objekt einstellen

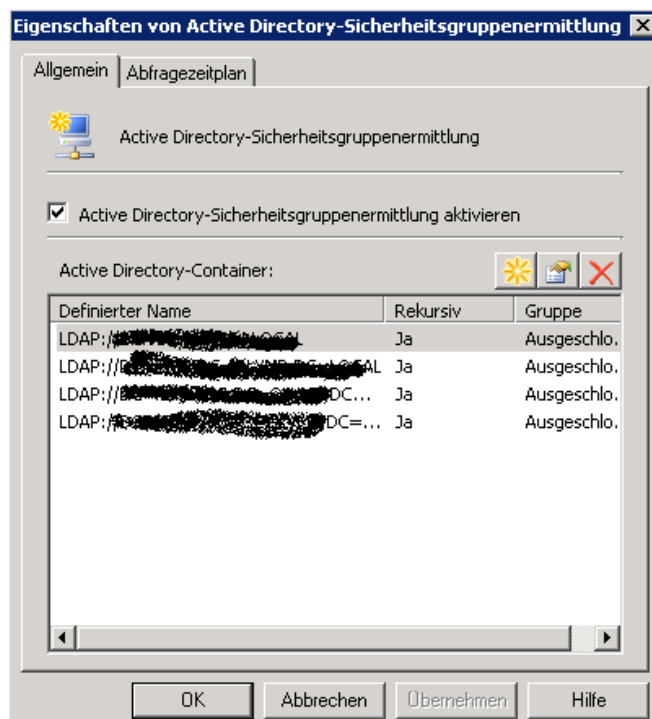


SCCM Sitegrenzen konfigurieren

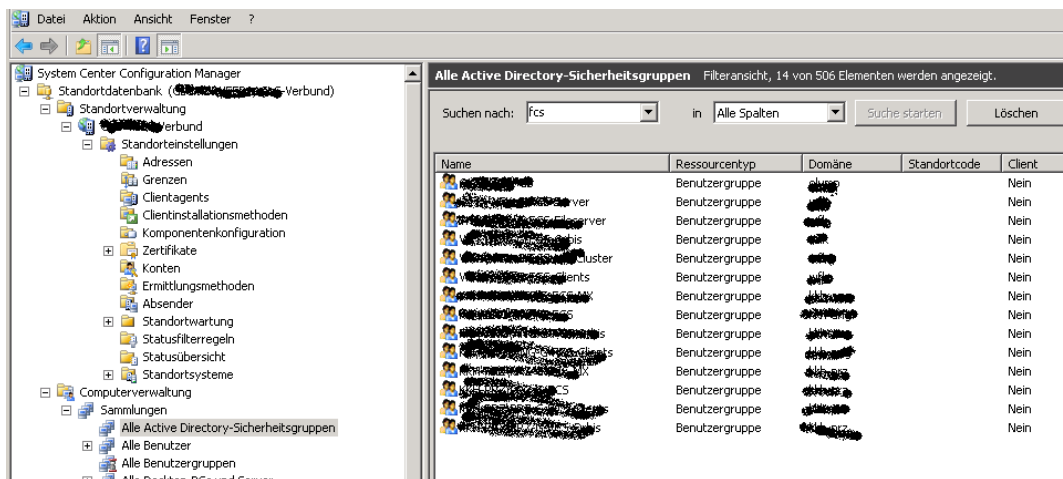


Ziel soll es sein, den SCCM/FEP Client basierend auf Active Directory Computergruppen zu verteilen, wie das bei FCS der Fall ist.

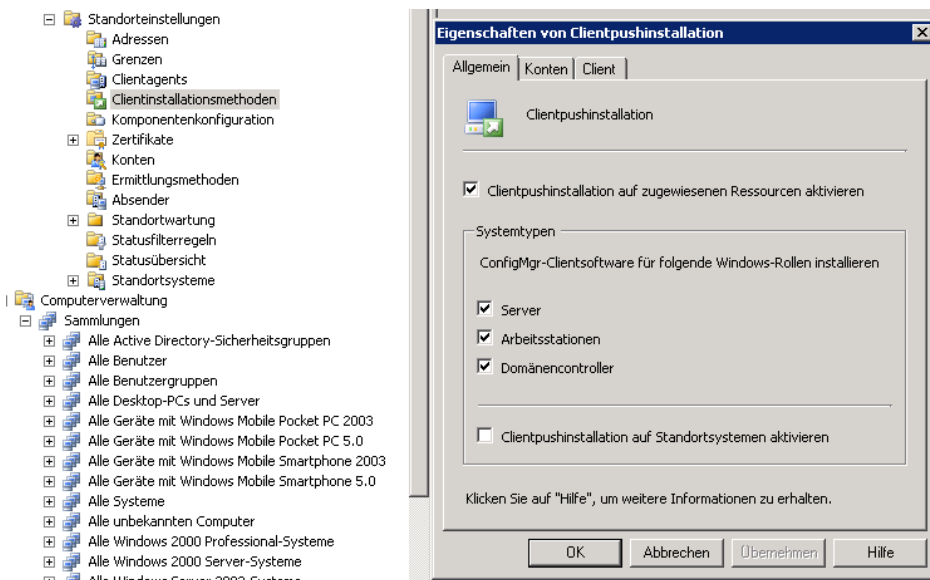
Active Directory Sicherheitsgruppenermittlung aktivieren



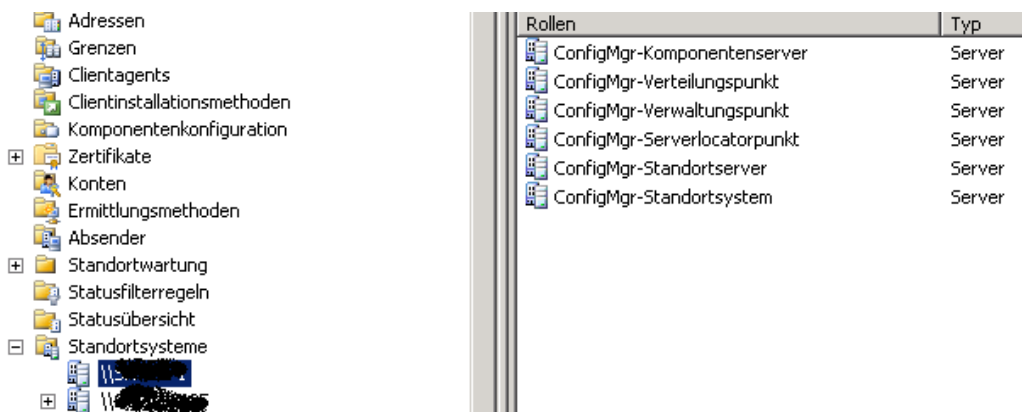
Danach tauchen die Gruppen in der SCCM Konsole auf



Client Pushinstallation konfigurieren



Standortsystemkomponenten



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

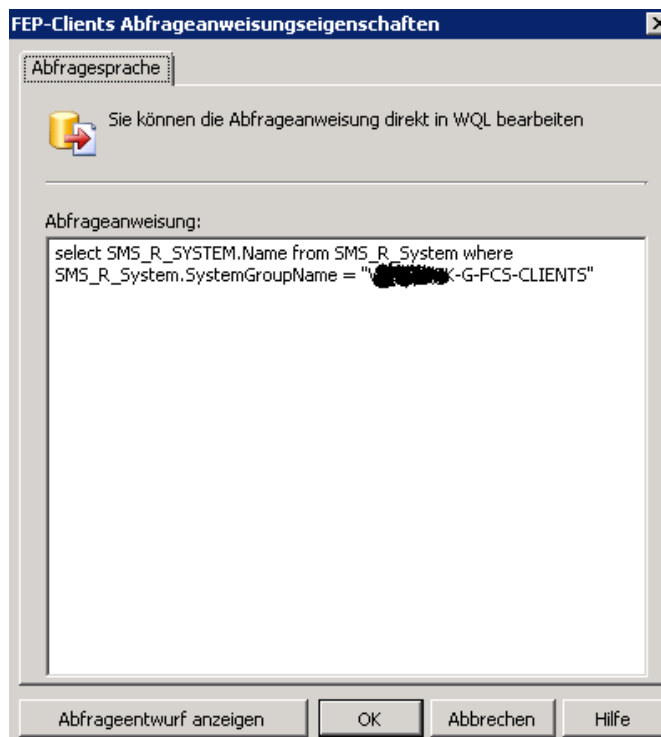
The screenshot shows the 'Sammlungserstellungs-Assistent' window. The left sidebar has tabs: Allgemein, Mitgliedschaftsregeln (selected), Ankündigungen, Sicherheit, Status, and Bestätigung. The main area has a title bar 'Mitgliedschaftsregeln' and a description: 'Samplingsmitgliedschaftsregeln bestimmen, welche Ressourcen beim Aktualisieren in die Sammlung einbezogen werden. Eine Mitgliedschaftsregel kann eine direkte Zuweisung oder eine Abfrage sein.' Below this is a table with columns 'Regel', 'Typ', and 'Begrenzen auf'. The table is empty, with a message 'In dieser Ansicht werden keine Elemente angez.' (No elements are displayed in this view). Below the table are two checkboxes: 'Diese Sammlung entsprechend einem Zeitplan aktualisieren' (checked) and 'Neue Ressourcen dynamisch hinzufügen' (unchecked). The checked checkbox has a sub-label 'Alle 1 Tag(e), beginnend am 04.02.2011 08:10' and a 'Zeitplan...' button. At the bottom are buttons: '< Zurück', 'Weiter >', 'Fertig stellen', and 'Abbrechen'.

Regel	Typ	Begrenzen auf
In dieser Ansicht werden keine Elemente angez.		

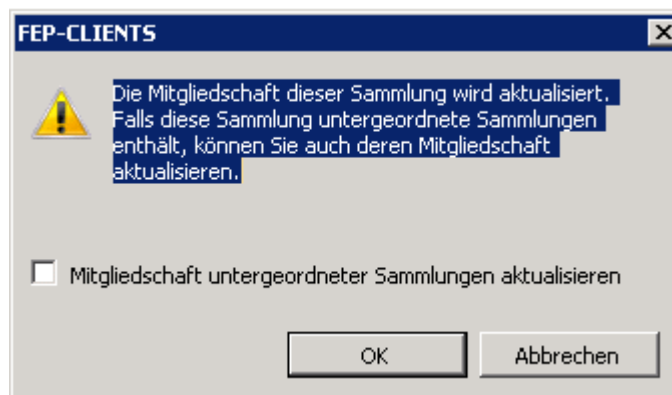
Abfragebasierte Sammlung erstellen

The screenshot shows the 'Abfrageregeleigenschaften' window. The left sidebar has a tab 'Allgemein'. The main area has a 'Name:' field with the value 'FEP-CLIENTS'. Below it is a button 'Abfrageanweisung importieren...'. Then is a 'Ressourcenklasse:' dropdown menu with 'Systemressourcen' selected. Below it is a button 'Abfrageanweisung bearbeiten...'. Then is a section 'Sammlungsbegrenzung' with two radio buttons: 'Alle Sammlungen' (selected) and 'Auf Sammlung begrenzen:'. Below the second radio button is a text input field and a 'Durchsuchen...' button. At the bottom are buttons: 'OK', 'Abbrechen', and 'Hilfe'.

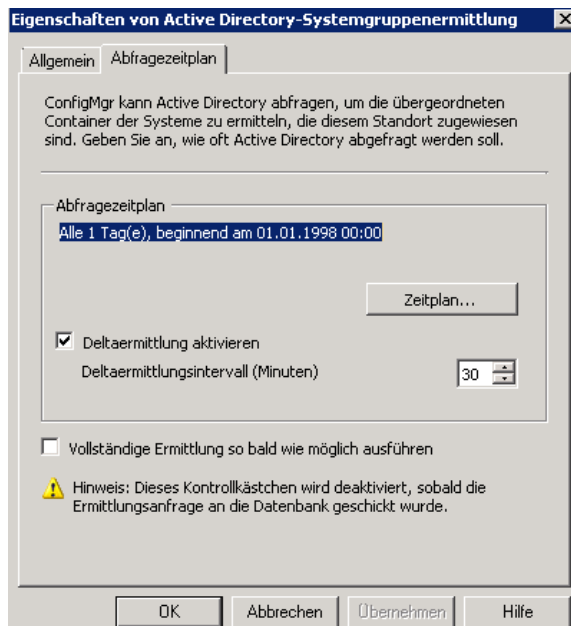
Abfrageanweisung definieren



Sammlungsmitgliedschaft aktualisieren



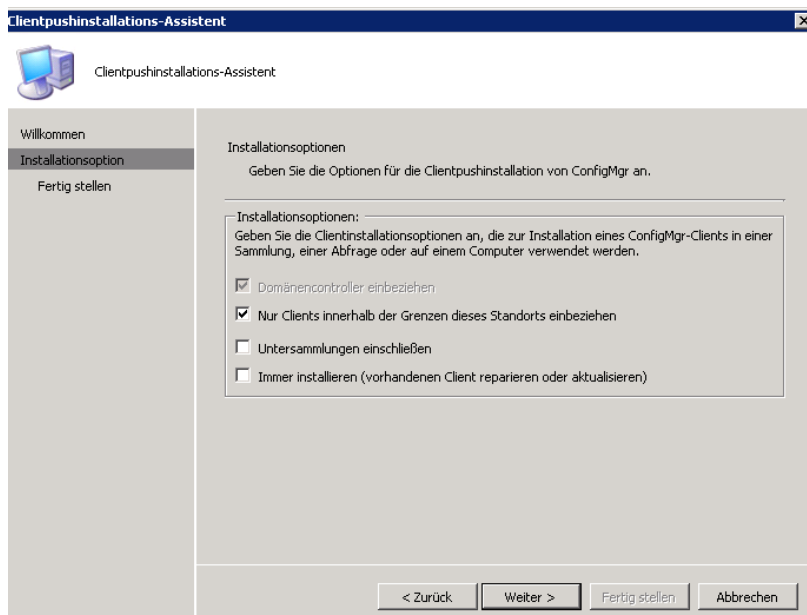
F5 druecken nicht vergessen und Achtung: Wenn neue Windows Gruppen fuer FEP-Clients erstellt werden, im SCCM die Ermittlung der Gruppen manuell anstarten



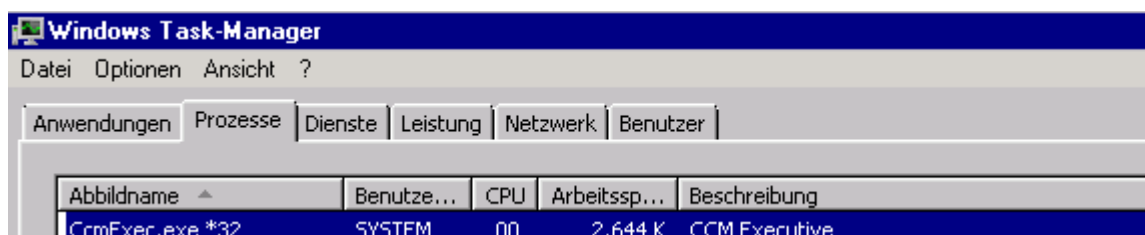
Client Deployment

Jetzt kann der SCCM Client deployed werden

Rechtsklick auf die Collection und Client deployen



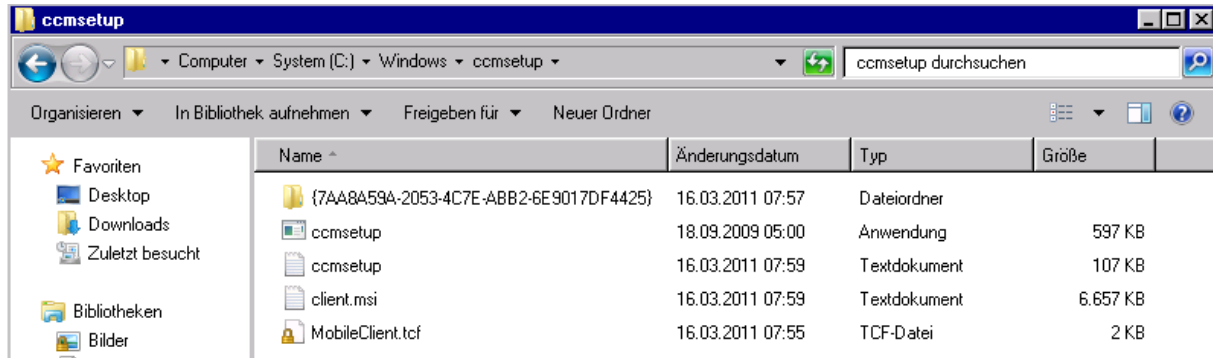
Auf dem Client startet dann das CCM Setup



SCCM Dienste

Smartcard	Verwaltet von...	Status	Modus	Lokales Dienst
SMS Agent Host	Provides chan...	Gestartet	Automat...	Lokales System
SMS Task Sequence Agent	SMS client ag...		Manuell	Lokales System

CCM Setup Verzeichnisse

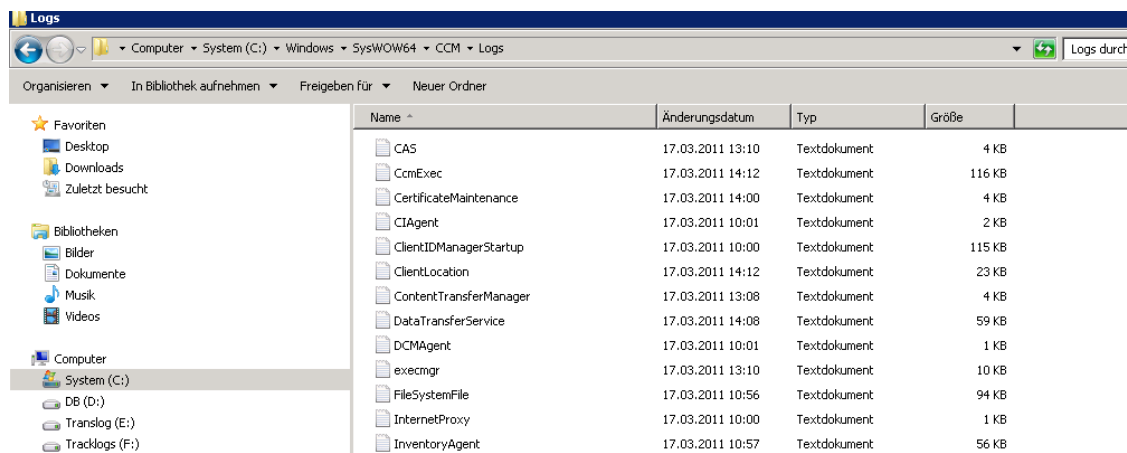


Name	Änderungsdatum	Typ	Größe
{7AA8A59A-2053-4C7E-ABB2-6E9017DF4425}	16.03.2011 07:57	Dateiordner	
ccmsetup	18.09.2009 05:00	Anwendung	597 KB
ccmsetup	16.03.2011 07:59	Textdokument	107 KB
client.msi	16.03.2011 07:59	Textdokument	6.657 KB
MobileClient.tcf	16.03.2011 07:55	TCF-Datei	2 KB

SCCM Symbole



SCCM Logdateien auf einem 64 Bit System



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

Forefront Endpoint Policy erstellen

The screenshot shows the Microsoft Management Console (MMC) interface. On the left is the 'Standardsysteme' (Standard Systems) console tree, which includes various system categories like 'Computerverwaltung' (Computer Management), 'Sammlungen' (Collections), and 'Softwareverteilung' (Software Distribution). The 'Richtlinien' (Policies) console pane is selected, displaying a list of policies. The list has three columns: 'Name', 'Beschreibung', and 'Rangfolge' (Priority). The policies listed are:

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)

On the right side of the console pane, there is an 'Aktionen' (Actions) pane with the following options:

- Neue Richtlinie...
- Richtlinien importieren...
- Richtlinienangabe bearbeiten...
- Feedback erstellen
- Ansicht
- Neues Fenster hier öffnen
- Aktualisieren
- Hilfe

Assistent für neue Richtlinien

The 'Assistent für neue Richtlinien' (New Policy Wizard) dialog box is shown. It has a title bar with the text 'Assistent für neue Richtlinien'. The main area is titled 'Allgemein' (General). Below the title, there is a description: 'Dieser Assistent unterstützt Sie beim Erstellen einer Forefront Endpoint Protection-Richtlinie, die Sie zum Schutz von Computern bereitstellen können.' (This assistant supports you in creating a Forefront Endpoint Protection policy that you can use to protect your computers.)

The wizard has a left sidebar with the following options:

- Allgemein (selected)
- Richtlinientyp
- Zusammenfassung
- Status
- Bestätigung

The main area contains the following fields:


Richtliniennamen:

Beschreibung:

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

Vorlage auswählen

Assistent für neue Richtlinien

 Richtlinientyp

Allgemein
Richtlinientyp
Zusammenfassung
Status
Bestätigung

Wählen Sie einen Richtlinientyp aus.

☐ Standarddesktoprichtlinie
Diese Richtlinie kann für die meisten Desktopumgebungen verwendet werden. Die Richtlinie beinhaltet wöchentliche Schnellscans und die Begrenzung der Prozessorauslastung während Scans auf 50 %.

☐ Richtlinie für hohe Sicherheit
Verwenden Sie diese Richtlinie für Computer, für die der maximale Schutz erforderlich ist. Die Richtlinie beinhaltet das Planen von täglichen Schnellscans und wöchentlichen vollständigen Scans, eine unbegrenzte Prozessorauslastung während Scans und das Verwalten der Windows-Firewall.

☐ Leistungsoptimierte Richtlinie
Verwenden Sie diese Richtlinie für Computer, für die die maximale Leistung, jedoch nur minimaler Schutz erforderlich ist. Diese Richtlinie beinhaltet das Planen von wöchentlichen Schnellscans und das Begrenzen von einer Prozessorauslastung auf 30 %.

☒ Richtlinienvorlage

FEP File Server including Defaults

[Weitere Informationen zu Richtlinientypen](#)

< Zurück Weiter > Fertig stellen Abbrechen

Richtlinie anpassen

Eigenschaften von File-Server

Allgemein AntiMalware Updates Windows-Firewall

Geplante Scans
Standardaktionen
Echtzeitschutz
Ausgeschlossene Dateien und
Ausgeschlossene Dateitypen
Ausgeschlossene Prozesse
Erweitert
Außerkräftsetzungen
Microsoft SpyNet

☒ Art und Zeit des Scans planen

Scanart:

Wöchentlicher Schnellscan

Wöchentlicher Scan:
Tag:

Samstag

Uhrzeit:

02:00

☒ Vor dem Starten eines Scans überprüfen, ob Definitionsupdates verfügbar sind

☒ Nur scannen, wenn der Computer nicht verwendet wird

☐ Startzeiten für geplante Scans zufällig festlegen (innerhalb von 30 Minuten vor oder nach der geplanten Zeit)

☐ Beim Neustart Scan erzwingen, wenn mindestens zwei geplante Scans nicht stattgefunden haben

☒ Prozessorauslastung während Scans auf folgenden Prozentwert begrenzen:

30%

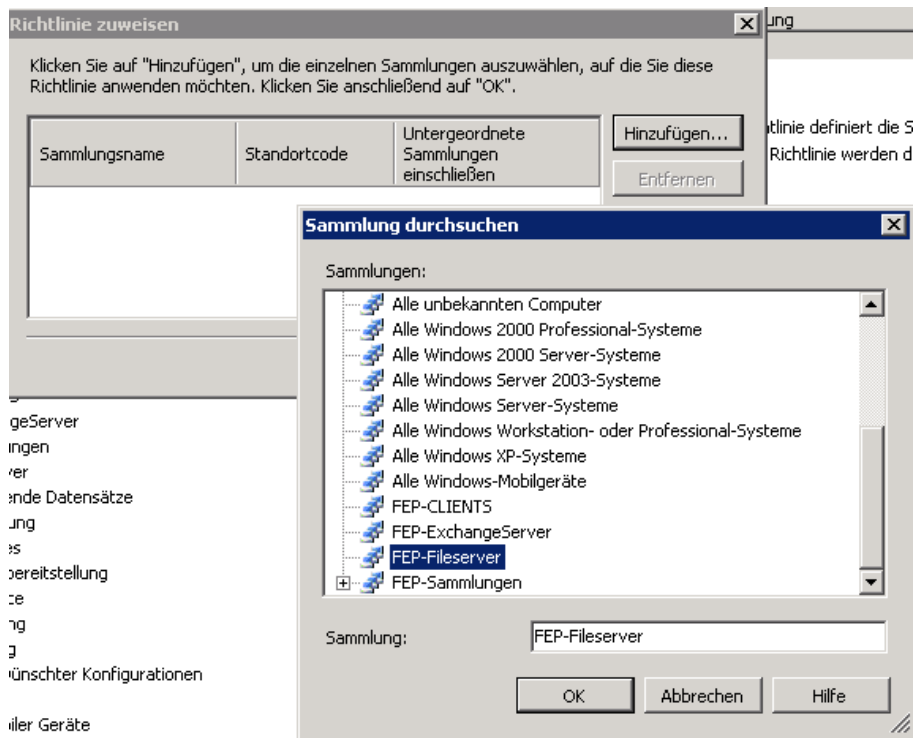
☒ Benutzern an Endpunktcomputern die Konfiguration von Prozessorauslastungshöchstwerten für Scans ermöglichen

Steuerung durch den Benutzer von geplanten Scans:

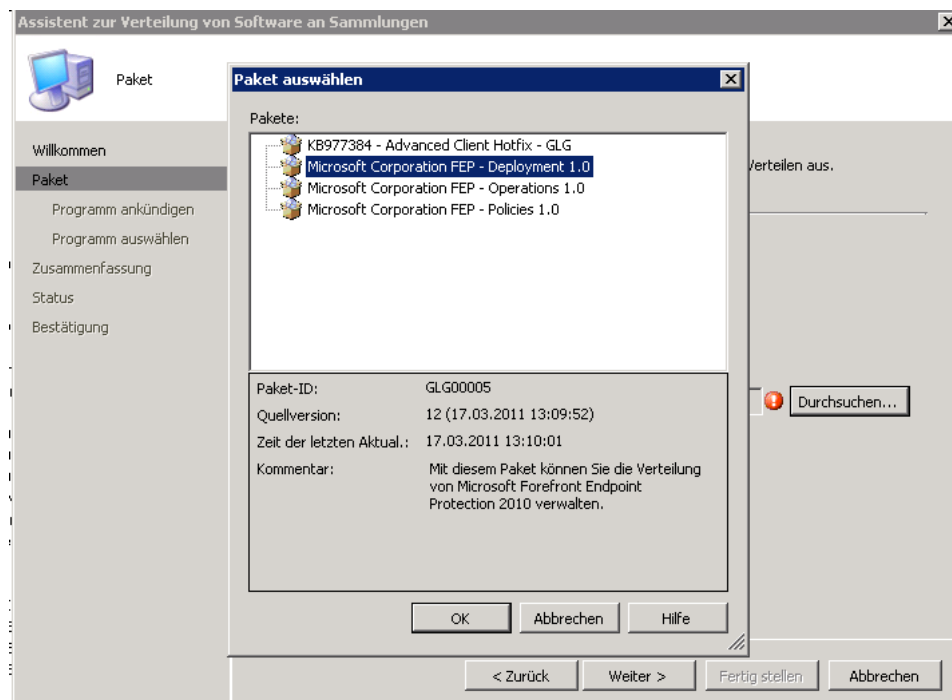
Vollzugriff: aktivieren, deaktivieren, Scantyp festlegen und planen

OK Abbrechen Übernehmen


Richtlinie zuweisen



Pakete verteilen



Assistent zur Verteilung von Software an Sammlungen

 Programm auswählen

Willkommen
Paket
Verteilungspunkte
Programm auswählen
Ankündigungsname
Untergeordnete Ankündi
Ankündigungsplan
Programm zuweisen
Zusammenfassung
Status
Bestätigung

Wählen Sie das Programm aus, das Mitgliedern einer Sammlung angekündigt werden soll.

Paket: FEP - Deployment


Programme:

Name	Beschreibung
Install	Installiert Microsoft Forefront Endpoint Prot...
Uninstall	Entfernt Microsoft Forefront Endpoint Prote...

< Zurück Weiter > Fertig stellen Abbrechen

Paket zuweisen

Assistent zur Verteilung von Software an Sammlungen

 Programm zuweisen

Willkommen
Paket
Verteilungspunkte
Programm auswählen
Ankündigungsname
Untergeordnete Ankündi
Ankündigungsplan
Programm zuweisen
Zusammenfassung
Status
Bestätigung

Geben Sie an, ob das Programm zugewiesen werden soll.

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?

☐ Nein, das Programm nicht zuweisen.
☒ Ja, das Programm zuweisen.

Verfügbar nach: 15:00:12 17.03.2011

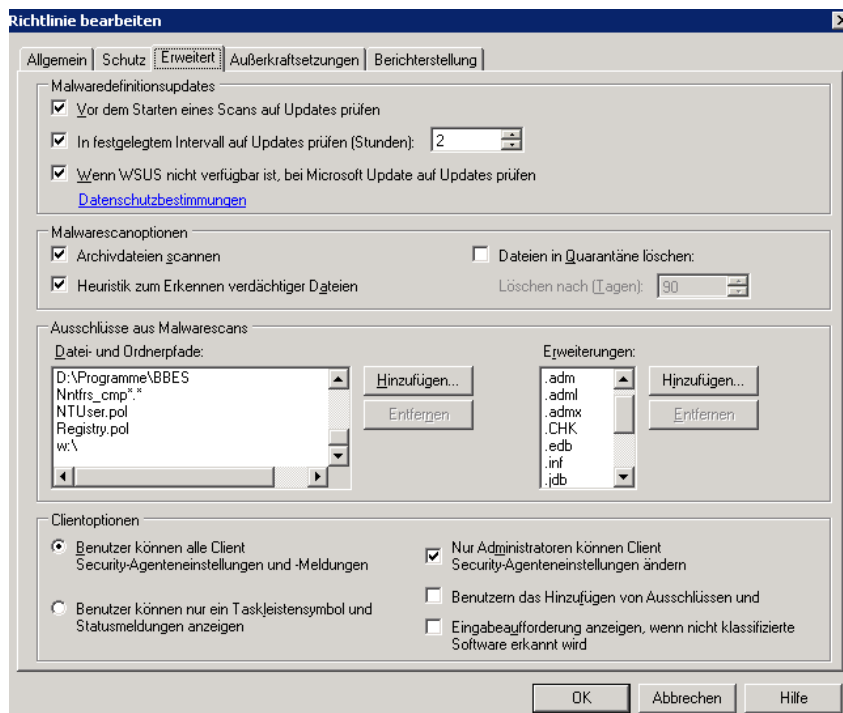
Zuweisen nach: 17.03.2011 15:00

Läuft ab nach:

☐ Wake-On-LAN aktivieren
☐ Beim Ausführen des Programms Wartungsfenster ignorieren
☐ Systemneustart außerhalb des Wartungsfensters zulassen

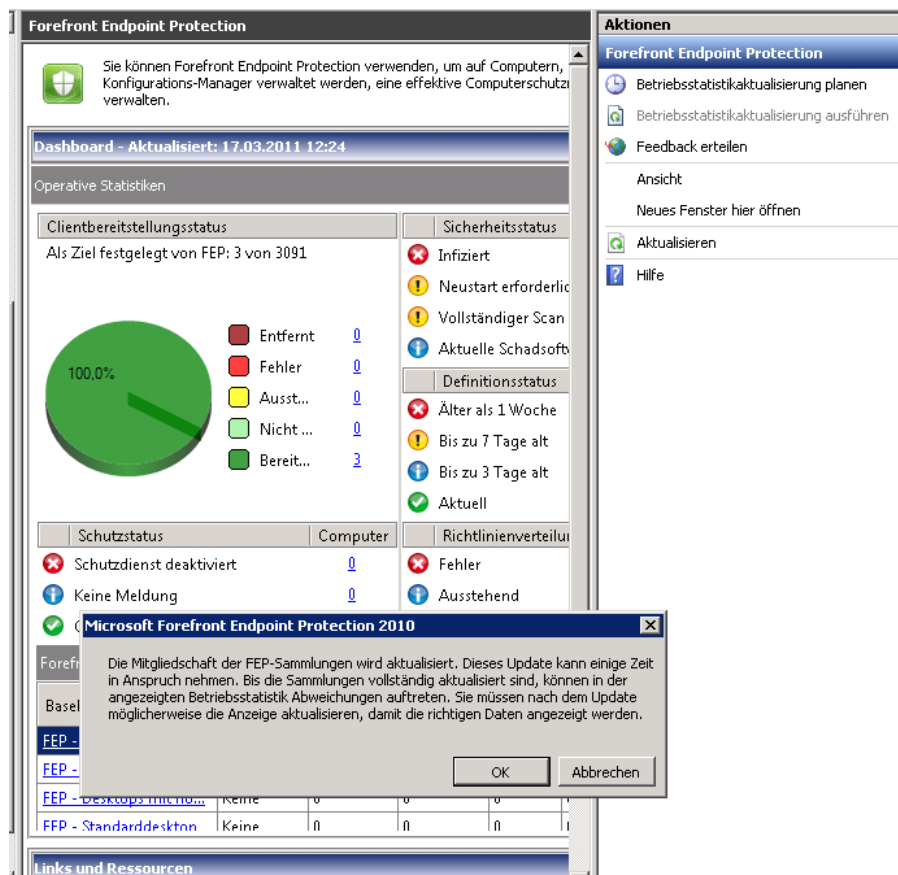
< Zurück Weiter > Fertig stellen Abbrechen

Ggfs. Uebernahme der Custom FCS Einstellungen in den Policies

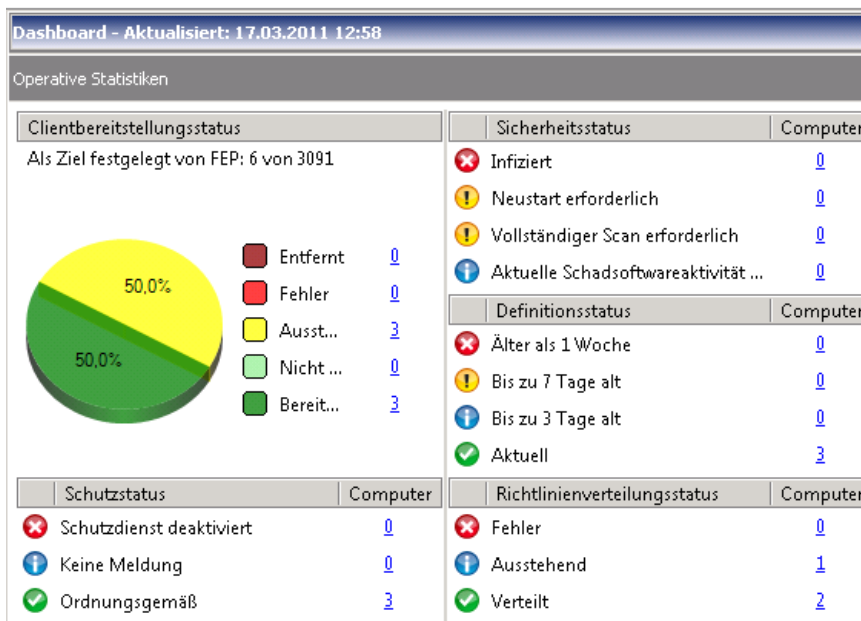


FEP Reporting

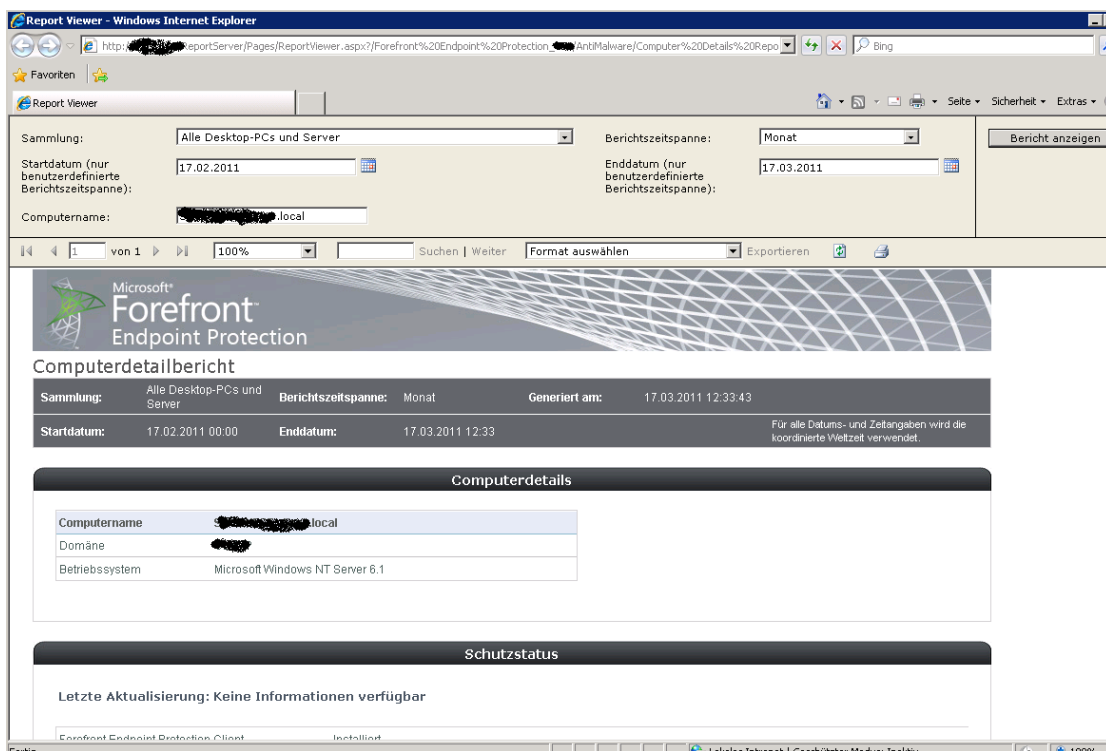
FEP Statistiken aktualisieren



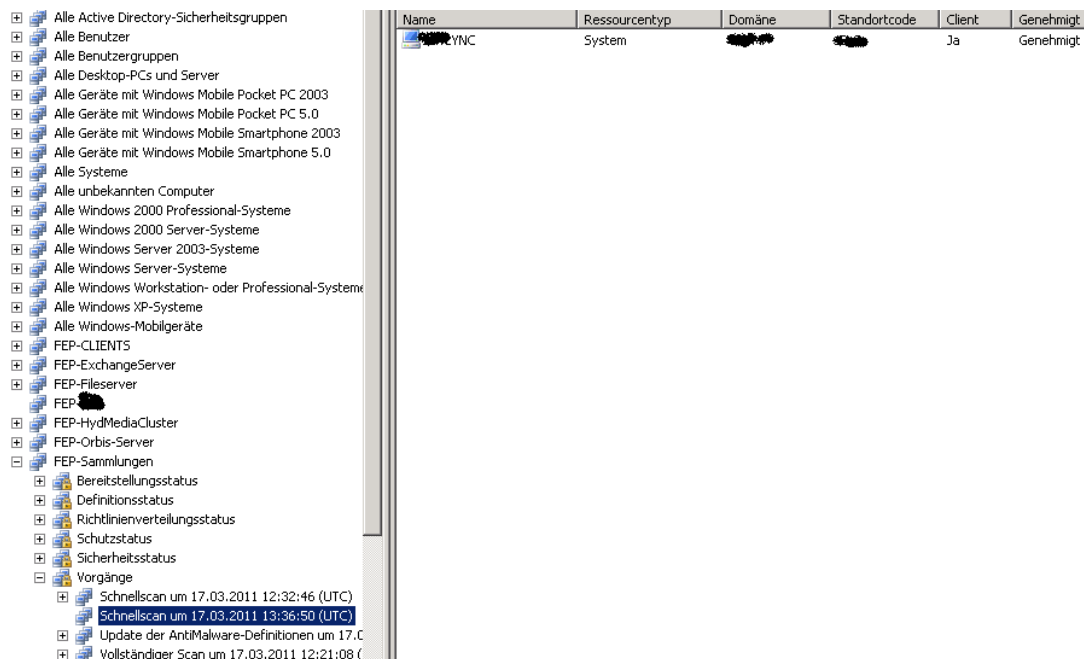
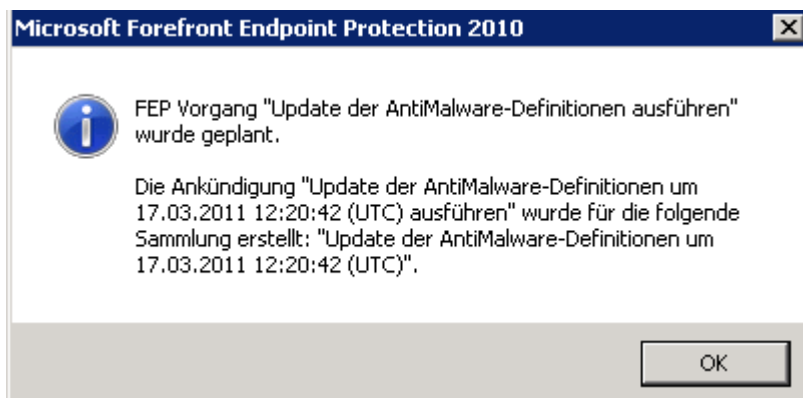
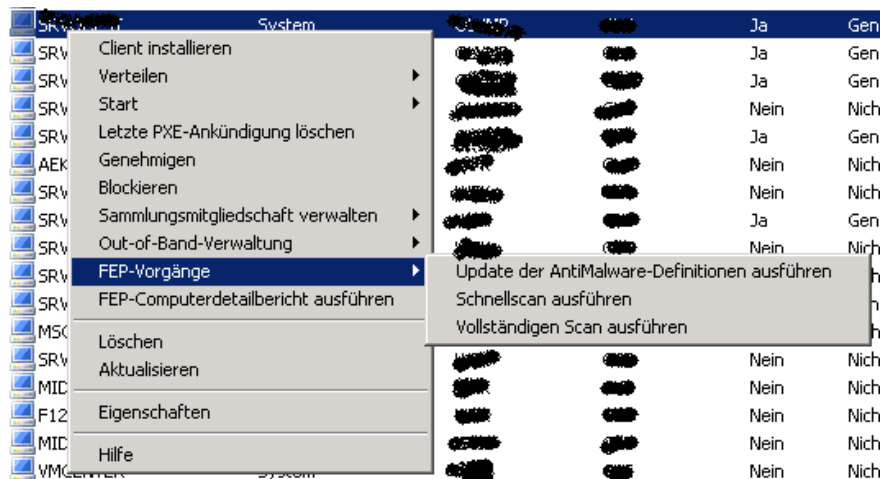
Die Statistik füllt sich mit Leben. Schon auf fast 6 Servern/Clients FEP ausgerollt ☺



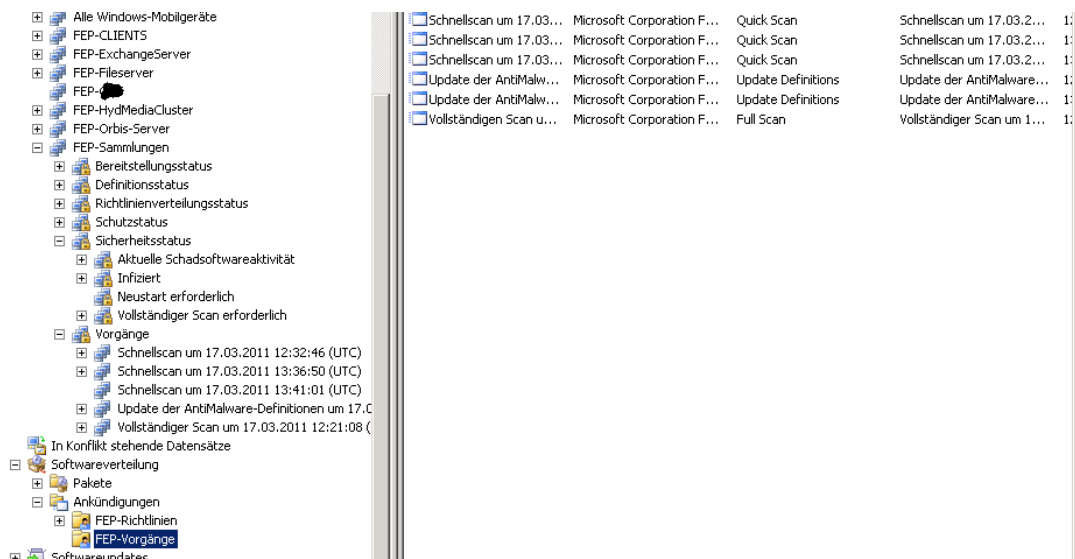
Zusammenfassungsreport eines Servers / Clients



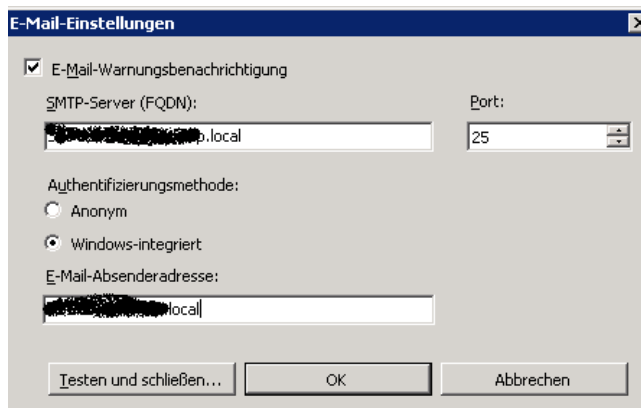
FEP Scans und Updates manuell ausfuehren

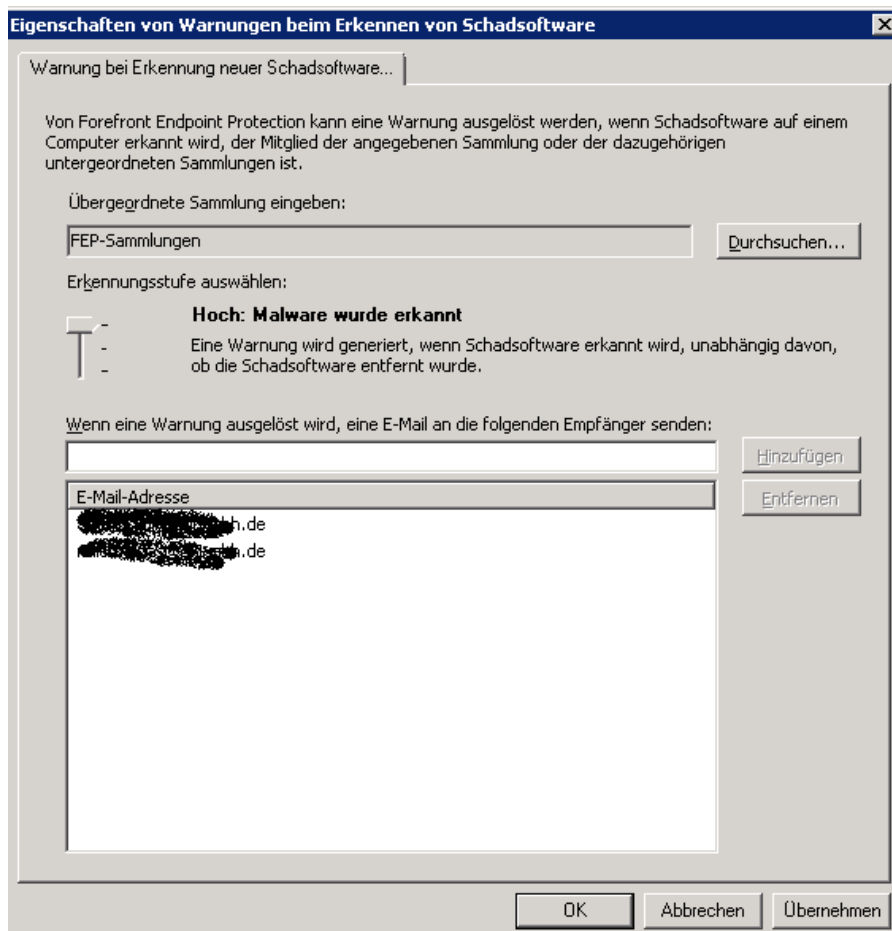


Fuer jeden manuellen FEP Vorgang werden entsprechende Advertisements erstellt



Warnungsbenachrichtigung einrichten

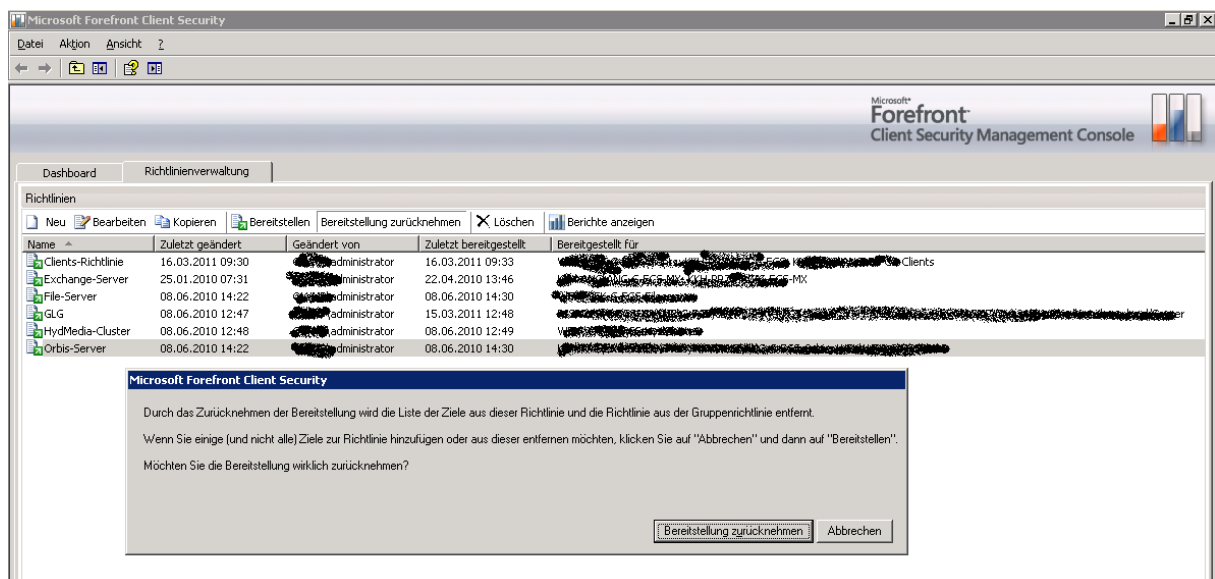




FCS deinstallieren

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

