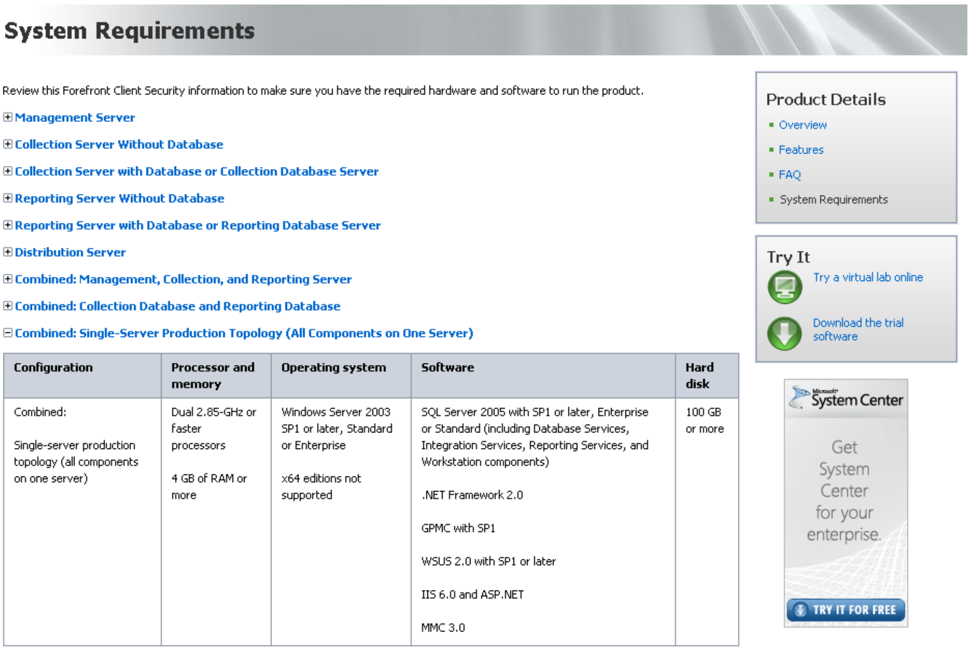
# Installation Microsoft Forefront Client Security

## Systemanforderungen



**System Requirements**

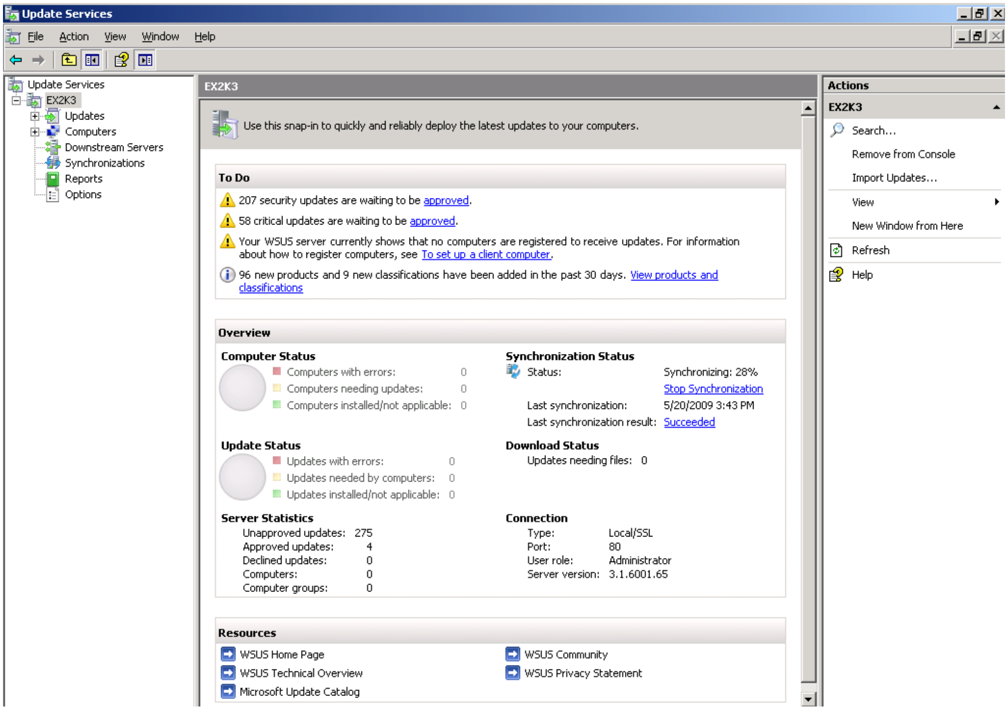
Review this Forefront Client Security information to make sure you have the required hardware and software to run the product.

- ⊞ Management Server
- ⊞ Collection Server Without Database
- ⊞ Collection Server with Database or Collection Database Server
- ⊞ Reporting Server Without Database
- ⊞ Reporting Server with Database or Reporting Database Server
- ⊞ Distribution Server
- ⊞ Combined: Management, Collection, and Reporting Server
- ⊞ Combined: Collection Database and Reporting Database
- ⊟ Combined: Single-Server Production Topology (All Components on One Server)

| Configuration | Processor and memory | Operating system | Software | Hard disk |
|---|---|---|---|---|
| Combined:<br>Single-server production topology (all components on one server) | Dual 2.85-GHz or faster processors<br>4 GB of RAM or more | Windows Server 2003 SP1 or later, Standard or Enterprise<br>x64 editions not supported | SQL Server 2005 with SP1 or later, Enterprise or Standard (including Database Services, Integration Services, Reporting Services, and Workstation components)<br>.NET Framework 2.0<br>GPMC with SP1<br>WSUS 2.0 with SP1 or later<br>IIS 6.0 and ASP.NET<br>MMC 3.0 | 100 GB or more |

# Installation

## Erst mal WSUS und syncen



EX2K3

Use this snap-in to quickly and reliably deploy the latest updates to your computers.

**To Do**

207 security updates are waiting to be approved.

58 critical updates are waiting to be approved.

Your WSUS server currently shows that no computers are registered to receive updates. For information about how to register computers, see To set up a client computer.

96 new products and 9 new classifications have been added in the past 30 days. View products and classifications

**Overview**

**Computer Status**

```
Computers with errors:              0
Computers needing updates:          0
Computers installed/not applicable: 0
```

**Synchronization Status**

```
Status:                        Synchronizing: 28%
                               Stop Synchronization
Last synchronization:          5/20/2009 3:43 PM
Last synchronization result:   Succeeded
```

**Update Status**

```
Updates with errors:              0
Updates needed by computers:      0
Updates installed/not applicable: 0
```

**Download Status**

```
Updates needing files:   0
```

**Server Statistics**

```
Unapproved updates:   275
Approved updates:       4
Declined updates:       0
Computers:              0
Computer groups:        0
```

**Connection**

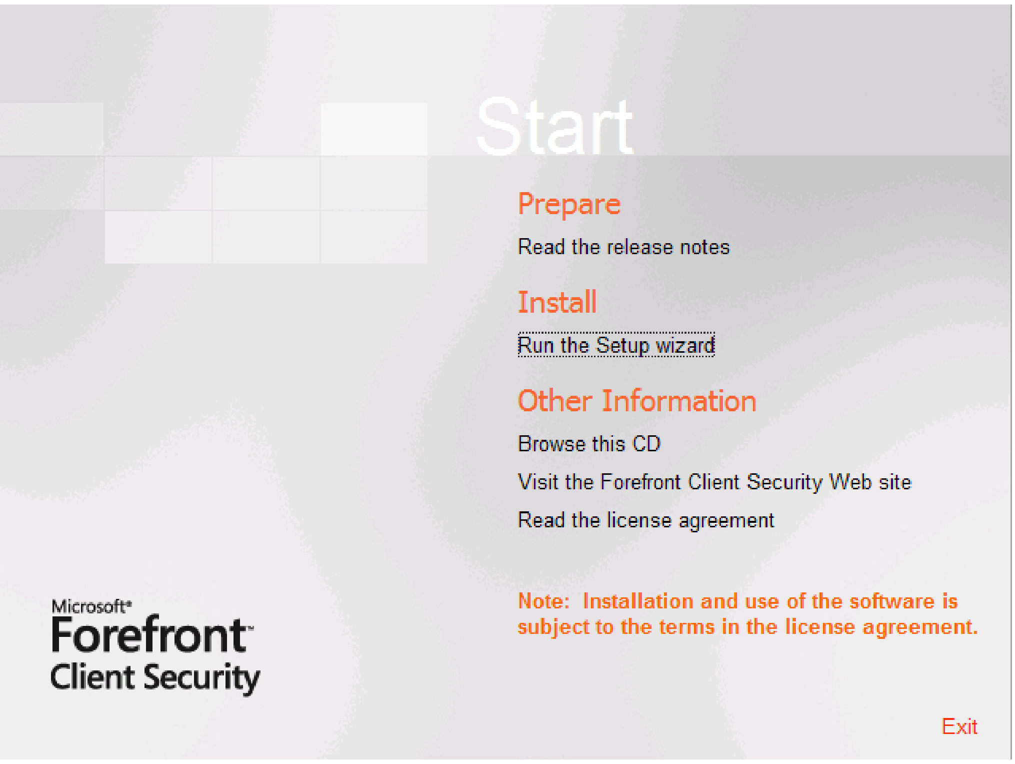
```
Type:            Local/SSL
Port:            80
User role:       Administrator
Server version:  3.1.6001.65
```

**Resources**

- WSUS Home Page
- WSUS Technical Overview
- Microsoft Update Catalog
- WSUS Community
- WSUS Privacy Statement

## Dann MS SQL Server 2005 mit SP2

Dann geht es wirklich los



Start

Prepare

Read the release notes

Install

Run the Setup wizard

Other Information

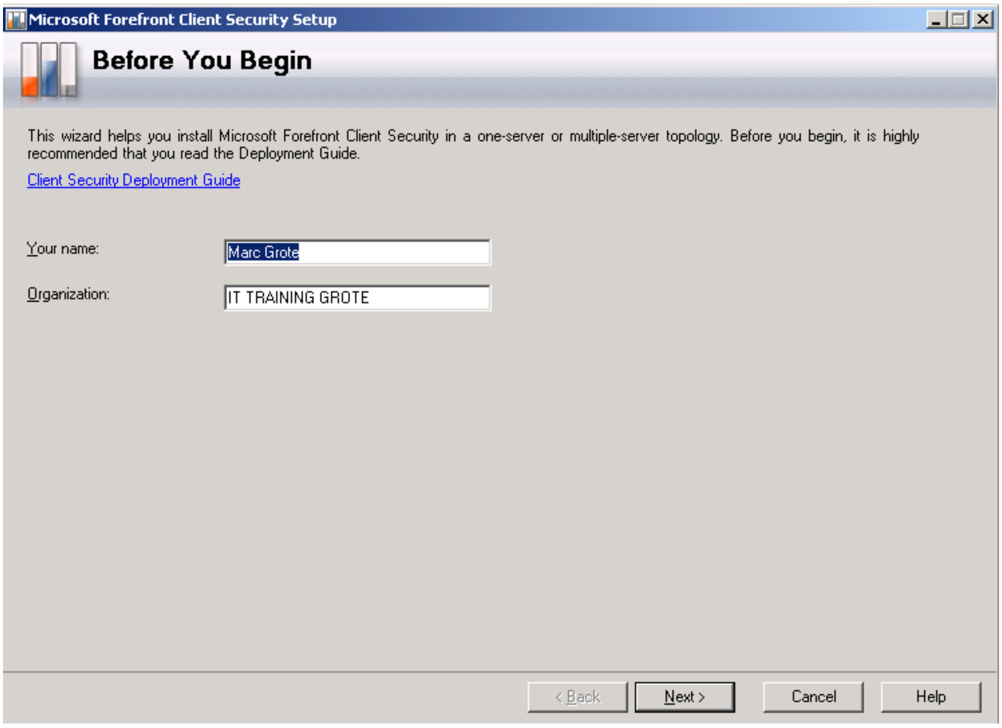
Browse this CD

Visit the Forefront Client Security Web site

Read the license agreement

Note: Installation and use of the software is subject to the terms in the license agreement.

identifizierung



Microsoft Forefront Client Security Setup

Before You Begin

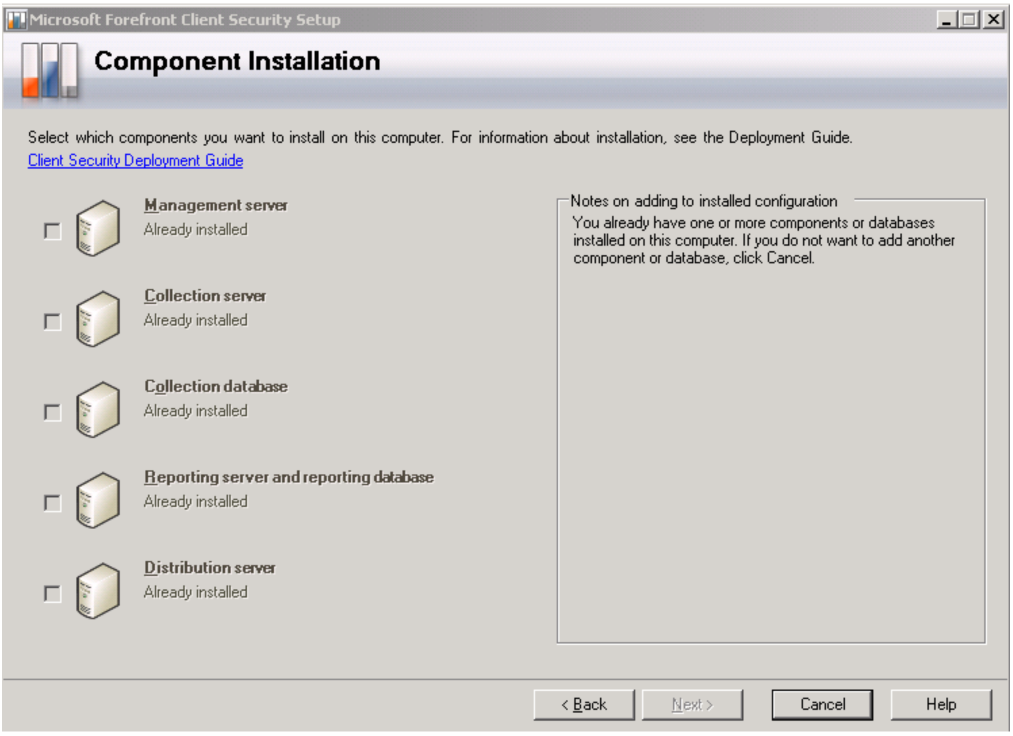
This wizard helps you install Microsoft Forefront Client Security in a one-server or multiple-server topology. Before you begin, it is highly recommended that you read the Deployment Guide.

Client Security Deployment Guide

Your name: Marc Grote

Organization: IT TRAINING GROTE

Komponenten


Microsoft Forefront Client Security Setup

Component Installation

Select which components you want to install on this computer. For information about installation, see the Deployment Guide.
Client Security Deployment Guide

□ Management server
Already installed

□ Collection server
Already installed

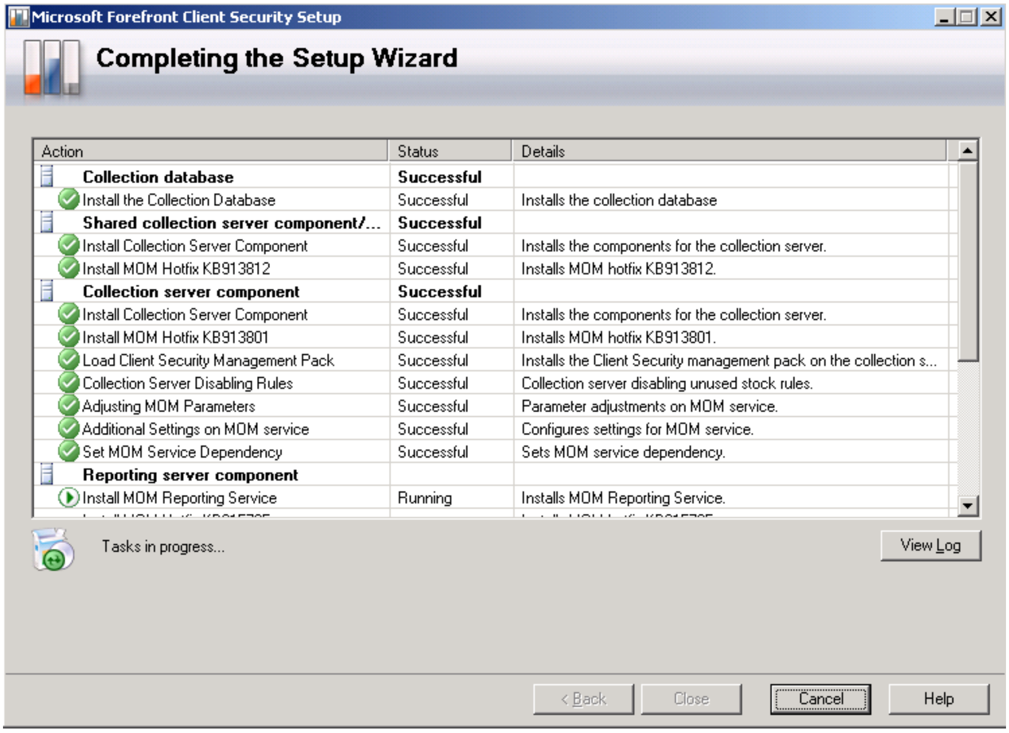
□ Collection database
Already installed

□ Reporting server and reporting database
Already installed

□ Distribution server
Already installed

Notes on adding to installed configuration
You already have one or more components or databases installed on this computer. If you do not want to add another component or database, click Cancel.

Was ne Liste

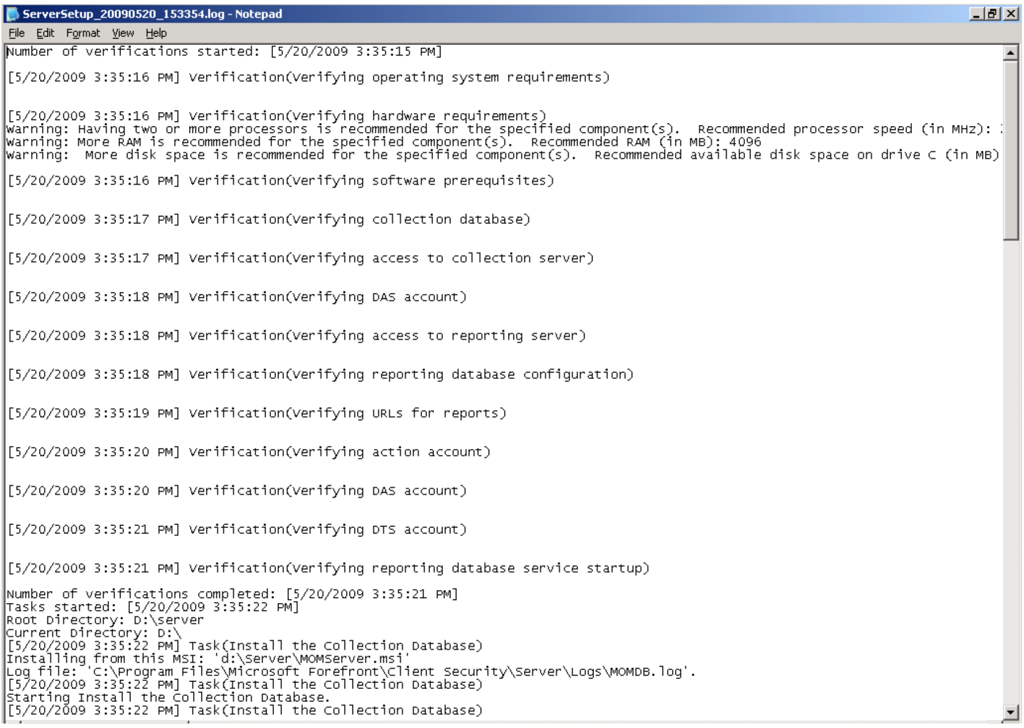

Microsoft Forefront Client Security Setup

Completing the Setup Wizard

| Action | Status | Details |
|---|---|---|
| **Collection database** | **Successful** | |
| ✓ Install the Collection Database | Successful | Installs the collection database |
| **Shared collection server component/...** | **Successful** | |
| ✓ Install Collection Server Component | Successful | Installs the components for the collection server. |
| ✓ Install MOM Hotfix KB913812 | Successful | Installs MOM hotfix KB913812. |
| **Collection server component** | **Successful** | |
| ✓ Install Collection Server Component | Successful | Installs the components for the collection server. |
| ✓ Install MOM Hotfix KB913801 | Successful | Installs MOM hotfix KB913801. |
| ✓ Load Client Security Management Pack | Successful | Installs the Client Security management pack on the collection s... |
| ✓ Collection Server Disabling Rules | Successful | Collection server disabling unused stock rules. |
| ✓ Adjusting MOM Parameters | Successful | Parameter adjustments on MOM service. |
| ✓ Additional Settings on MOM service | Successful | Configures settings for MOM service. |
| ✓ Set MOM Service Dependency | Successful | Sets MOM service dependency. |
| **Reporting server component** | | |
| ▶ Install MOM Reporting Service | Running | Installs MOM Reporting Service. |

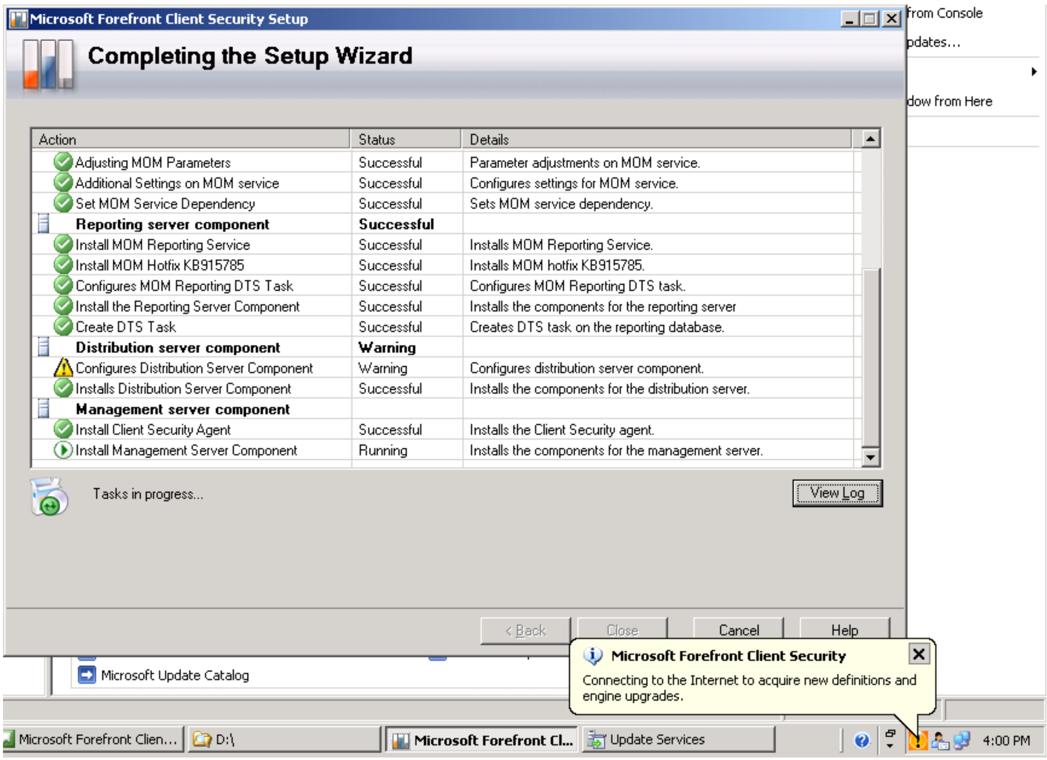
Tasks in progress...

## Setup Log


ServerSetup_20090520_153354.log - Notepad
File Edit Format View Help

```
Number of verifications started: [5/20/2009 3:35:15 PM]

[5/20/2009 3:35:16 PM] Verification(Verifying operating system requirements)


[5/20/2009 3:35:16 PM] Verification(Verifying hardware requirements)
Warning: Having two or more processors is recommended for the specified component(s).  Recommended processor speed (in MHz): 
Warning: More RAM is recommended for the specified component(s).  Recommended RAM (in MB): 4096
Warning:  More disk space is recommended for the specified component(s).  Recommended available disk space on drive C (in MB)

[5/20/2009 3:35:16 PM] Verification(Verifying software prerequisites)


[5/20/2009 3:35:17 PM] Verification(Verifying collection database)


[5/20/2009 3:35:17 PM] Verification(Verifying access to collection server)


[5/20/2009 3:35:18 PM] Verification(Verifying DAS account)


[5/20/2009 3:35:18 PM] Verification(Verifying access to reporting server)


[5/20/2009 3:35:18 PM] Verification(Verifying reporting database configuration)


[5/20/2009 3:35:19 PM] Verification(Verifying URLs for reports)


[5/20/2009 3:35:20 PM] Verification(Verifying action account)


[5/20/2009 3:35:20 PM] Verification(Verifying DAS account)


[5/20/2009 3:35:21 PM] Verification(Verifying DTS account)


[5/20/2009 3:35:21 PM] Verification(Verifying reporting database service startup)

Number of verifications completed: [5/20/2009 3:35:21 PM]
Tasks started: [5/20/2009 3:35:22 PM]
Root Directory: D:\server
Current Directory: D:\
[5/20/2009 3:35:22 PM] Task(Install the Collection Database)
Installing from this MSI: 'd:\Server\MOMServer.msi'
Log file: 'C:\Program Files\Microsoft Forefront\Client Security\Server\Logs\MOMDB.log'.
[5/20/2009 3:35:22 PM] Task(Install the Collection Database)
Starting Install the Collection Database.
[5/20/2009 3:35:22 PM] Task(Install the Collection Database)
```

## WSUS war noch nicht in sync



Completing the Setup Wizard

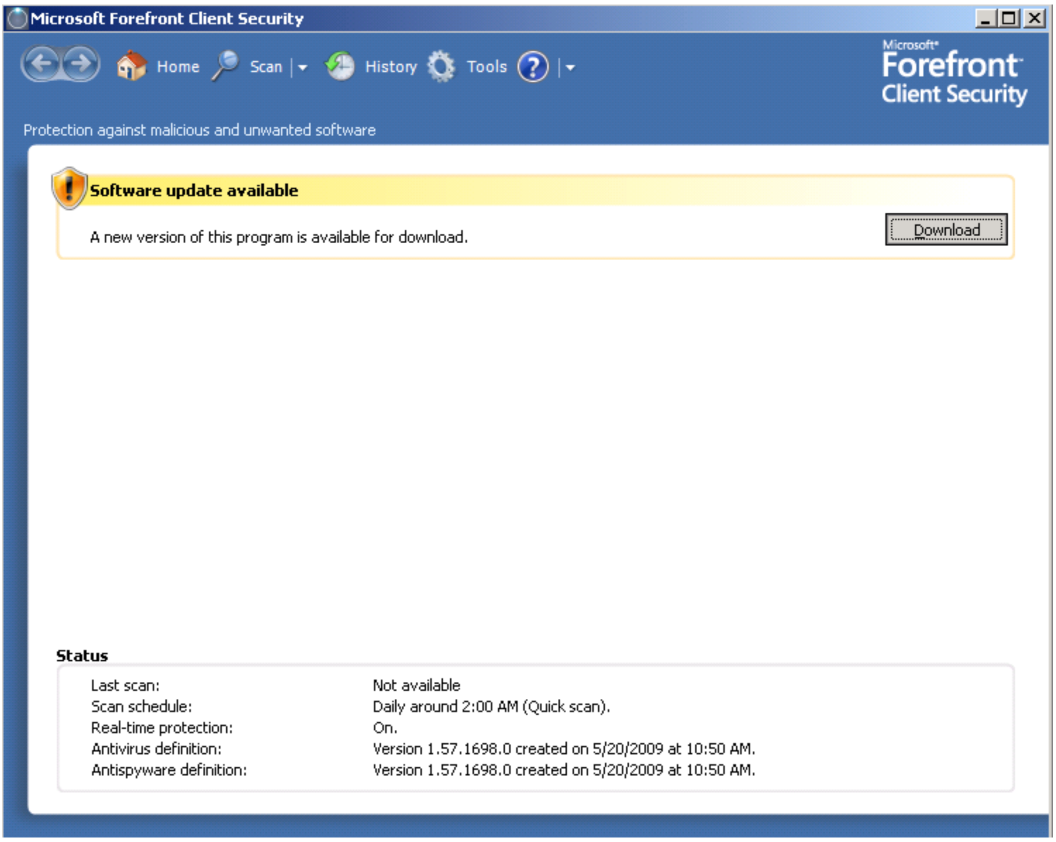
| Action | Status | Details |
|---|---|---|
| ✓ Adjusting MOM Parameters | Successful | Parameter adjustments on MOM service. |
| ✓ Additional Settings on MOM service | Successful | Configures settings for MOM service. |
| ✓ Set MOM Service Dependency | Successful | Sets MOM service dependency. |
| **Reporting server component** | **Successful** | |
| ✓ Install MOM Reporting Service | Successful | Installs MOM Reporting Service. |
| ✓ Install MOM Hotfix KB915785 | Successful | Installs MOM hotfix KB915785. |
| ✓ Configures MOM Reporting DTS Task | Successful | Configures MOM Reporting DTS task. |
| ✓ Install the Reporting Server Component | Successful | Installs the components for the reporting server |
| ✓ Create DTS Task | Successful | Creates DTS task on the reporting database. |
| **Distribution server component** | **Warning** | |
| ⚠ Configures Distribution Server Component | Warning | Configures distribution server component. |
| ✓ Installs Distribution Server Component | Successful | Installs the components for the distribution server. |
| **Management server component** | | |
| ✓ Install Client Security Agent | Successful | Installs the Client Security agent. |
| ▶ Install Management Server Component | Running | Installs the components for the management server. |

Tasks in progress...

Microsoft Forefront Client Security

Connecting to the Internet to acquire new definitions and engine upgrades.

## Updates verfuegbar


Microsoft Forefront Client Security
Home
Scan
History
Tools
Microsoft®
Forefront
Client Security
Protection against malicious and unwanted software
Download

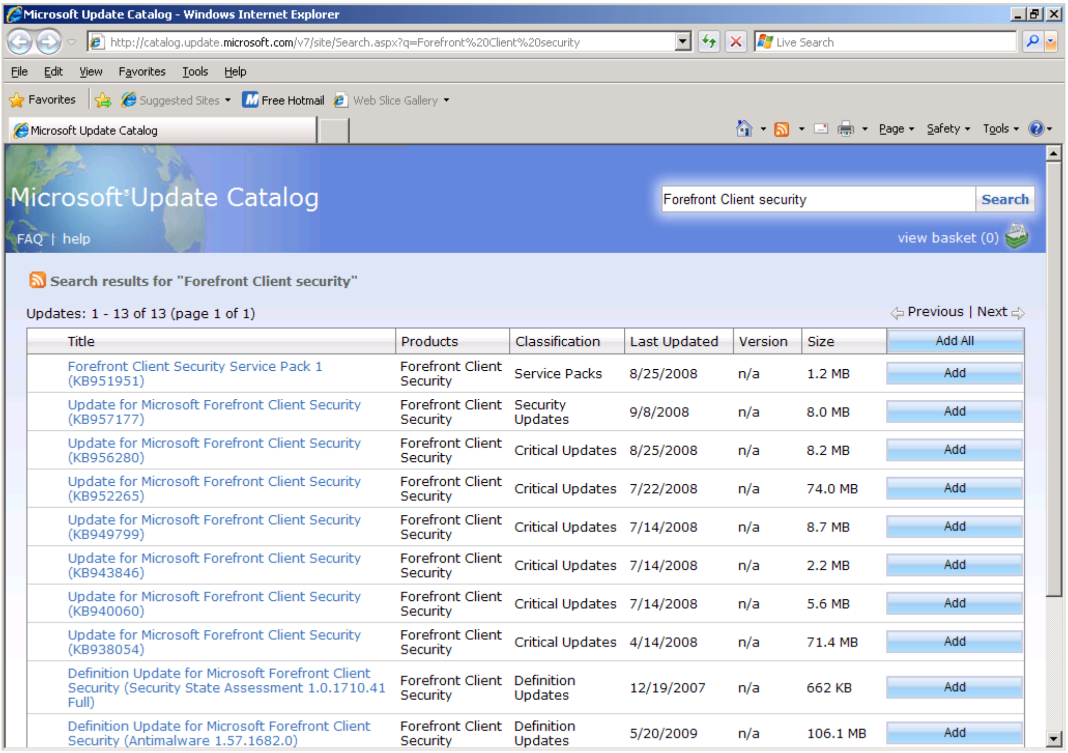
**Software update available**

A new version of this program is available for download.

**Status**

| | |
|---|---|
| Last scan: | Not available |
| Scan schedule: | Daily around 2:00 AM (Quick scan). |
| Real-time protection: | On. |
| Antivirus definition: | Version 1.57.1698.0 created on 5/20/2009 at 10:50 AM. |
| Antispyware definition: | Version 1.57.1698.0 created on 5/20/2009 at 10:50 AM. |

## Da gibt es doch was



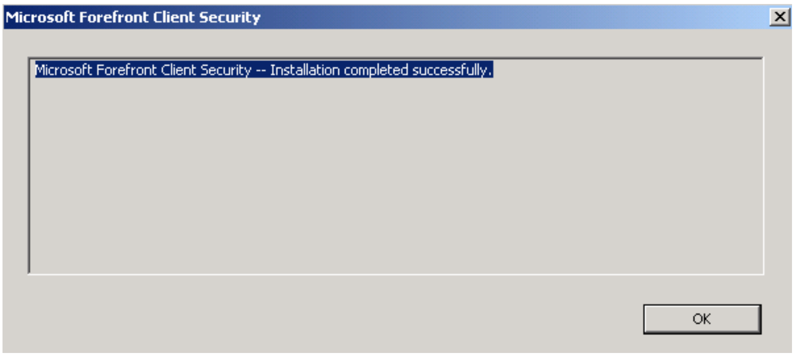
**Search results for "Forefront Client security"**

Updates: 1 - 13 of 13 (page 1 of 1)

Previous | Next

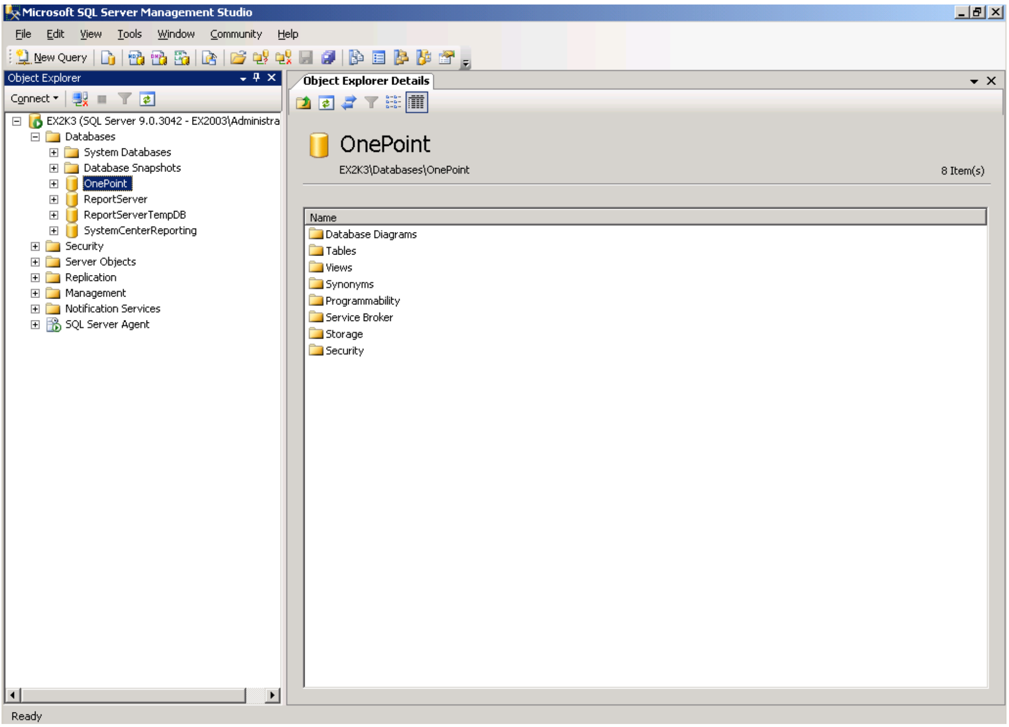
| Title | Products | Classification | Last Updated | Version | Size | Add All |
|---|---|---|---|---|---|---|
| Forefront Client Security Service Pack 1 (KB951951) | Forefront Client Security | Service Packs | 8/25/2008 | n/a | 1.2 MB | Add |
| Update for Microsoft Forefront Client Security (KB957177) | Forefront Client Security | Security Updates | 9/8/2008 | n/a | 8.0 MB | Add |
| Update for Microsoft Forefront Client Security (KB956280) | Forefront Client Security | Critical Updates | 8/25/2008 | n/a | 8.2 MB | Add |
| Update for Microsoft Forefront Client Security (KB952265) | Forefront Client Security | Critical Updates | 7/22/2008 | n/a | 74.0 MB | Add |
| Update for Microsoft Forefront Client Security (KB949799) | Forefront Client Security | Critical Updates | 7/14/2008 | n/a | 8.7 MB | Add |
| Update for Microsoft Forefront Client Security (KB943846) | Forefront Client Security | Critical Updates | 7/14/2008 | n/a | 2.2 MB | Add |
| Update for Microsoft Forefront Client Security (KB940060) | Forefront Client Security | Critical Updates | 7/14/2008 | n/a | 5.6 MB | Add |
| Update for Microsoft Forefront Client Security (KB938054) | Forefront Client Security | Critical Updates | 4/14/2008 | n/a | 71.4 MB | Add |
| Definition Update for Microsoft Forefront Client Security (Security State Assessment 1.0.1710.41 Full) | Forefront Client Security | Definition Updates | 12/19/2007 | n/a | 662 KB | Add |
| Definition Update for Microsoft Forefront Client Security (Antimalware 1.57.1682.0) | Forefront Client Security | Definition Updates | 5/20/2009 | n/a | 106.1 MB | Add |

Erfolgreich

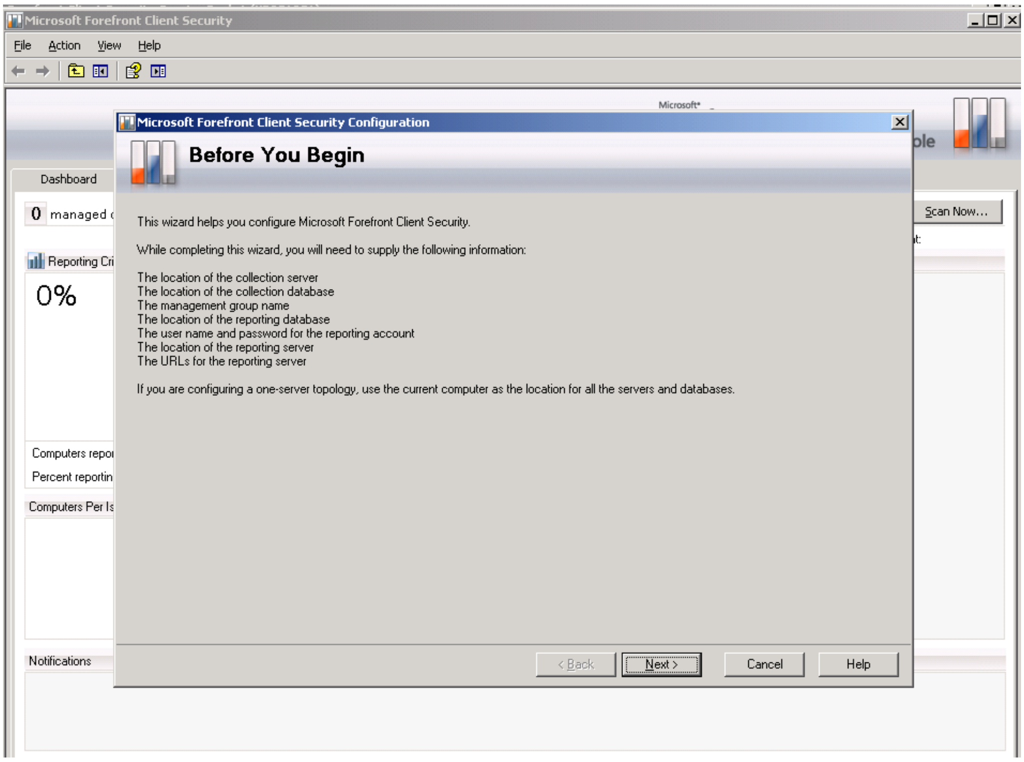


Microsoft Forefront Client Security -- Installation completed successfully.

Die FCS Installation legt eine "Onepoint" Datenbank an



## Configuration beenden



Microsoft Forefront Client Security Configuration

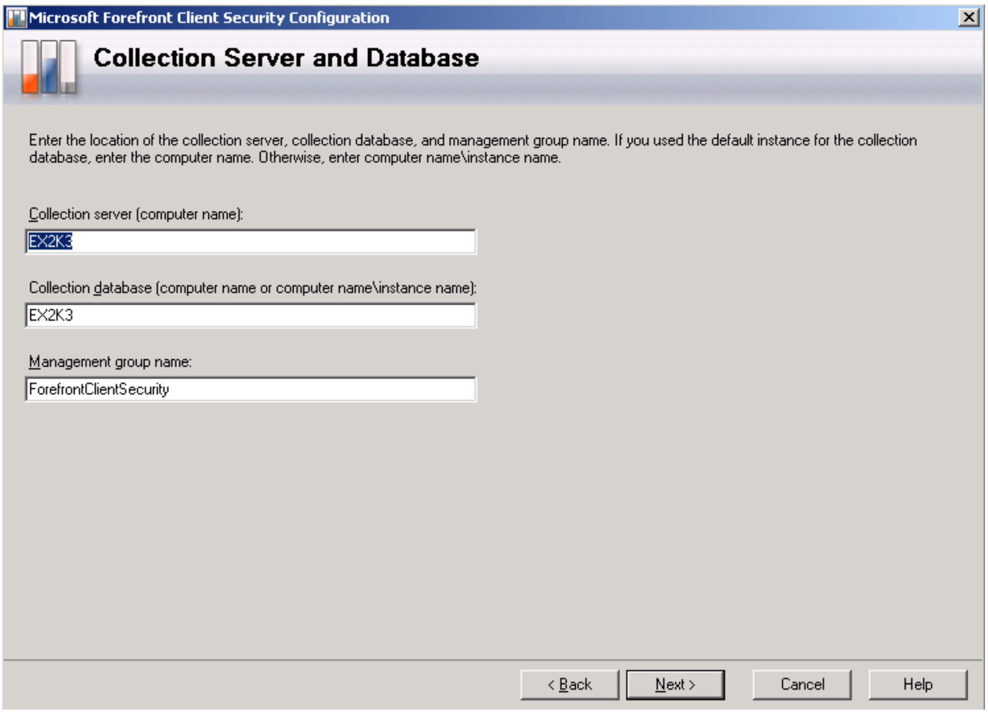
Before You Begin

This wizard helps you configure Microsoft Forefront Client Security.

While completing this wizard, you will need to supply the following information:

The location of the collection server
The location of the collection database
The management group name
The location of the reporting database
The user name and password for the reporting account
The location of the reporting server
The URLs for the reporting server

If you are configuring a one-server topology, use the current computer as the location for all the servers and databases.



Microsoft Forefront Client Security Configuration

Collection Server and Database

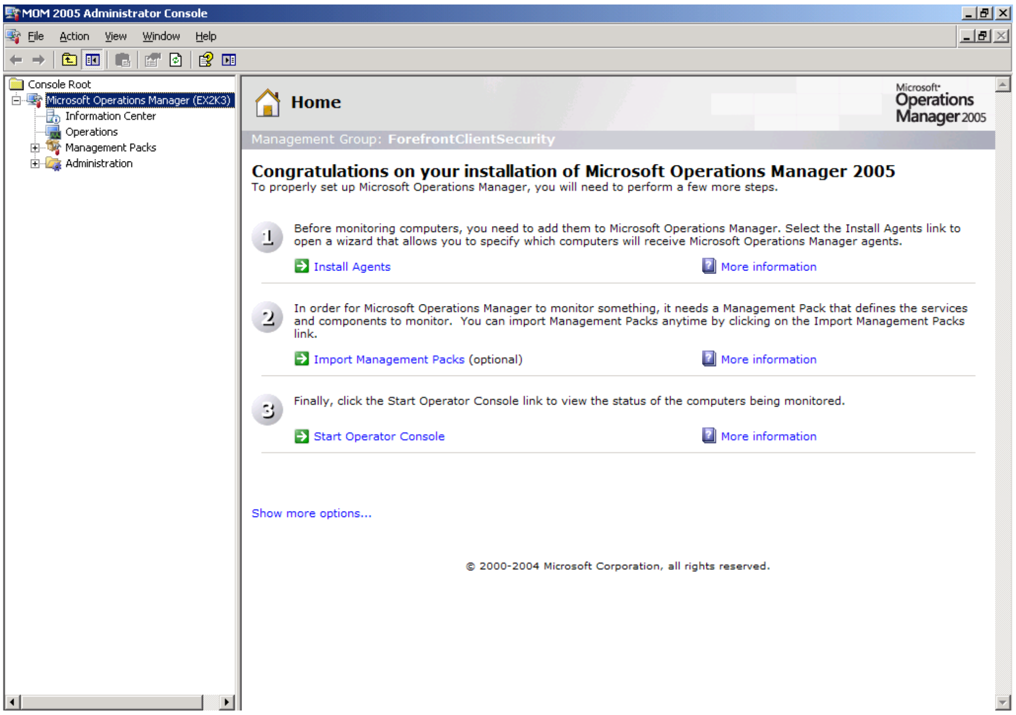
Enter the location of the collection server, collection database, and management group name. If you used the default instance for the collection database, enter the computer name. Otherwise, enter computer name\instance name.

Collection server (computer name): EX2K3

Collection database (computer name or computer name\instance name): EX2K3

Management group name: ForefrontClientSecurity

## FCS installiert eine MOM Management Group


MOM 2005 Administrator Console
File Action View Window Help
Console Root
Microsoft Operations Manager (EX2K3)
Information Center
Operations
Management Packs
Administration
Home
Microsoft Operations Manager 2005

Management Group: ForefrontClientSecurity

**Congratulations on your installation of Microsoft Operations Manager 2005**

To properly set up Microsoft Operations Manager, you will need to perform a few more steps.

1. Before monitoring computers, you need to add them to Microsoft Operations Manager. Select the Install Agents link to open a wizard that allows you to specify which computers will receive Microsoft Operations Manager agents.

   Install Agents — More information

2. In order for Microsoft Operations Manager to monitor something, it needs a Management Pack that defines the services and components to monitor. You can import Management Packs anytime by clicking on the Import Management Packs link.

   Import Management Packs (optional) — More information

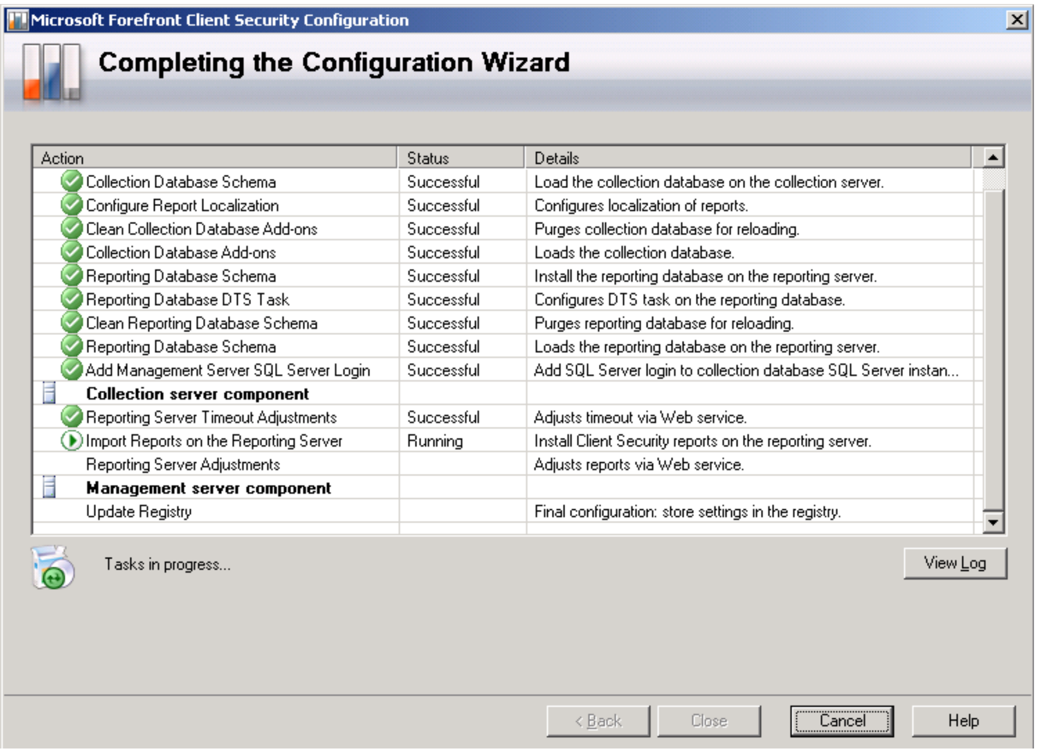
3. Finally, click the Start Operator Console link to view the status of the computers being monitored.

   Start Operator Console — More information

Show more options...

© 2000-2004 Microsoft Corporation, all rights reserved.

## Abschlusskonfiguration des Assistenten

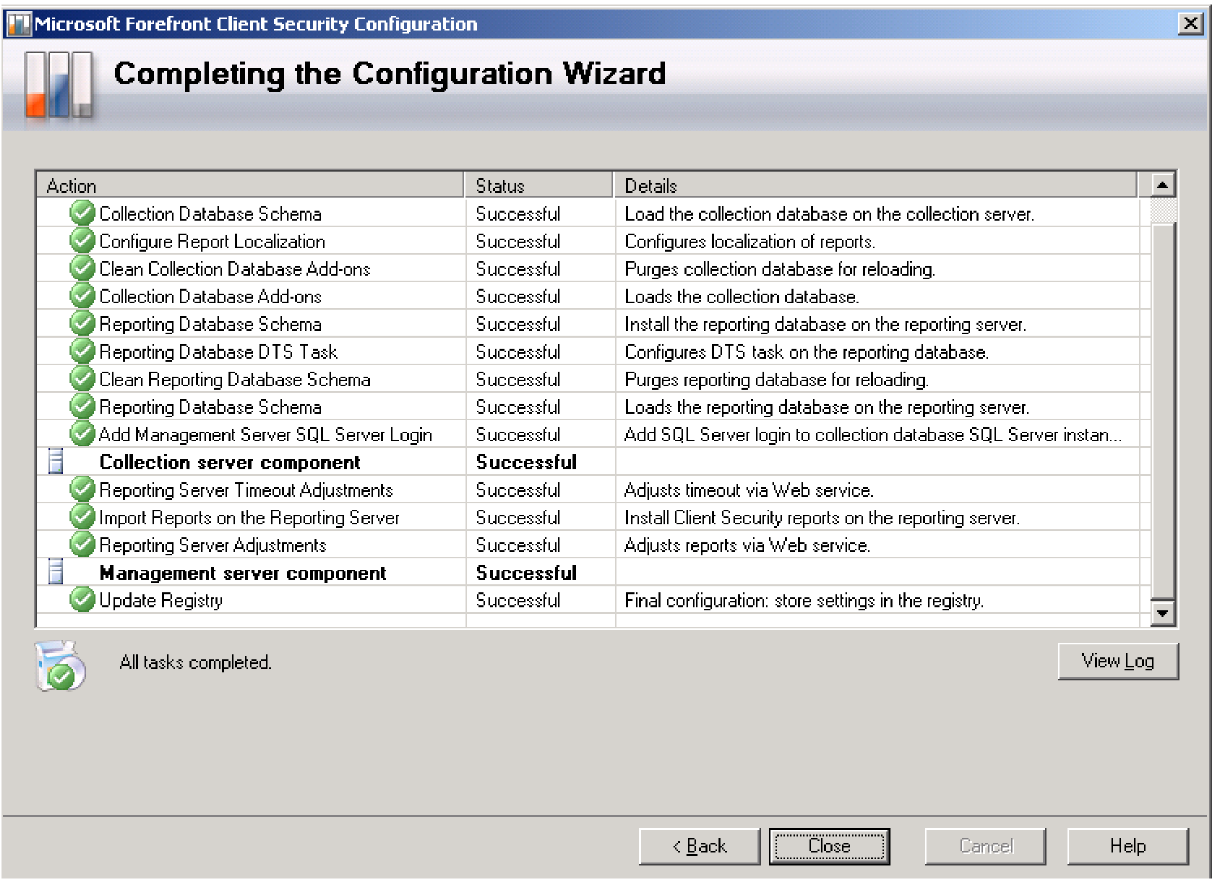


**Completing the Configuration Wizard**

| Action | Status | Details |
|---|---|---|
| Collection Database Schema | Successful | Load the collection database on the collection server. |
| Configure Report Localization | Successful | Configures localization of reports. |
| Clean Collection Database Add-ons | Successful | Purges collection database for reloading. |
| Collection Database Add-ons | Successful | Loads the collection database. |
| Reporting Database Schema | Successful | Install the reporting database on the reporting server. |
| Reporting Database DTS Task | Successful | Configures DTS task on the reporting database. |
| Clean Reporting Database Schema | Successful | Purges reporting database for reloading. |
| Reporting Database Schema | Successful | Loads the reporting database on the reporting server. |
| Add Management Server SQL Server Login | Successful | Add SQL Server login to collection database SQL Server instan... |
| **Collection server component** | | |
| Reporting Server Timeout Adjustments | Successful | Adjusts timeout via Web service. |
| Import Reports on the Reporting Server | Running | Install Client Security reports on the reporting server. |
| Reporting Server Adjustments | | Adjusts reports via Web service. |
| **Management server component** | | |
| Update Registry | | Final configuration: store settings in the registry. |

Tasks in progress...

Alles prima

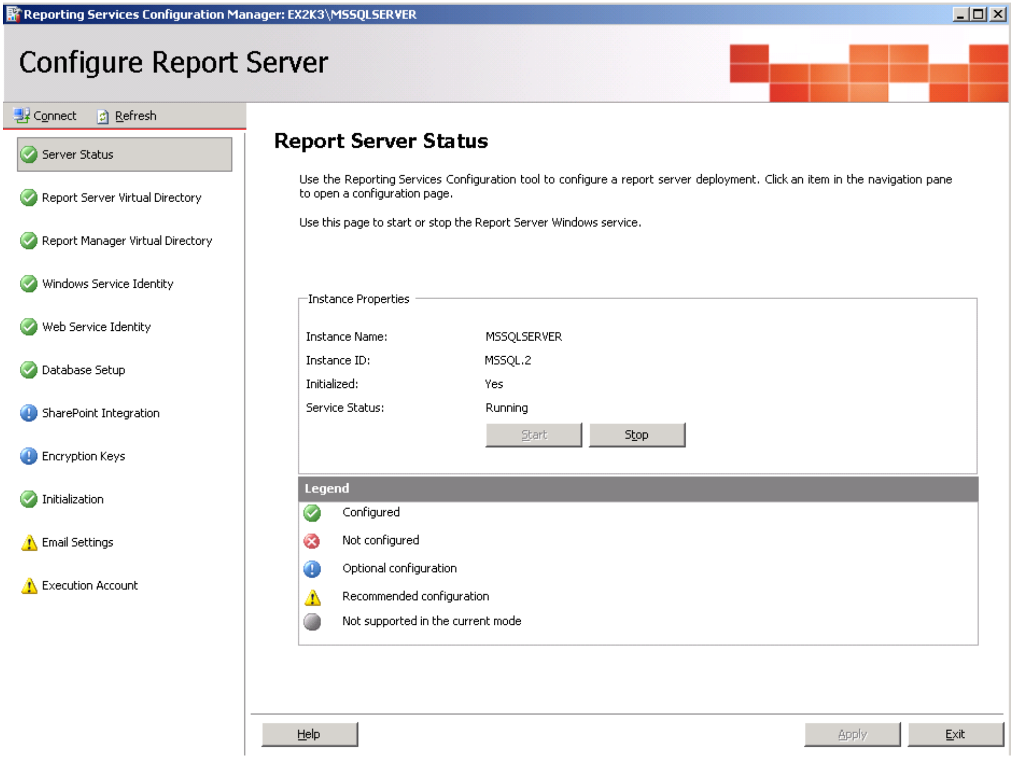


Completing the Configuration Wizard

| Action | Status | Details |
|---|---|---|
| ✓ Collection Database Schema | Successful | Load the collection database on the collection server. |
| ✓ Configure Report Localization | Successful | Configures localization of reports. |
| ✓ Clean Collection Database Add-ons | Successful | Purges collection database for reloading. |
| ✓ Collection Database Add-ons | Successful | Loads the collection database. |
| ✓ Reporting Database Schema | Successful | Install the reporting database on the reporting server. |
| ✓ Reporting Database DTS Task | Successful | Configures DTS task on the reporting database. |
| ✓ Clean Reporting Database Schema | Successful | Purges reporting database for reloading. |
| ✓ Reporting Database Schema | Successful | Loads the reporting database on the reporting server. |
| ✓ Add Management Server SQL Server Login | Successful | Add SQL Server login to collection database SQL Server instan... |
| **Collection server component** | **Successful** | |
| ✓ Reporting Server Timeout Adjustments | Successful | Adjusts timeout via Web service. |
| ✓ Import Reports on the Reporting Server | Successful | Install Client Security reports on the reporting server. |
| ✓ Reporting Server Adjustments | Successful | Adjusts reports via Web service. |
| **Management server component** | **Successful** | |
| ✓ Update Registry | Successful | Final configuration: store settings in the registry. |

All tasks completed.

Alles Roger beim Report Server?



Configure Report Server

**Report Server Status**

Use the Reporting Services Configuration tool to configure a report server deployment. Click an item in the navigation pane to open a configuration page.

Use this page to start or stop the Report Server Windows service.

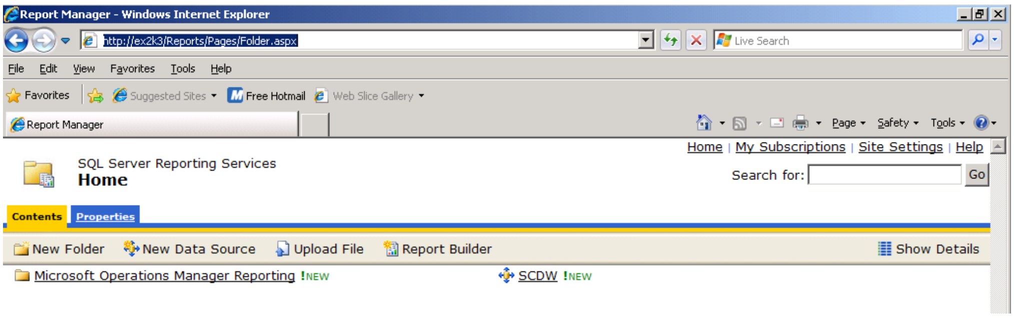
Instance Properties

| | |
|---|---|
| Instance Name: | MSSQLSERVER |
| Instance ID: | MSSQL.2 |
| Initialized: | Yes |
| Service Status: | Running |

Legend

| | |
|---|---|
| ✓ | Configured |
| ✗ | Not configured |
| ! | Optional configuration |
| ⚠ | Recommended configuration |
| ● | Not supported in the current mode |

juup



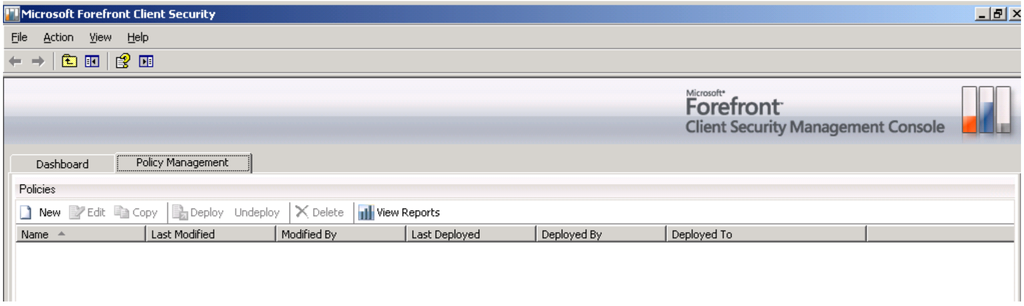
http://ex2k3/Reports/Pages/Folder.aspx

SQL Server Reporting Services
Home

Microsoft Operations Manager Reporting !NEW

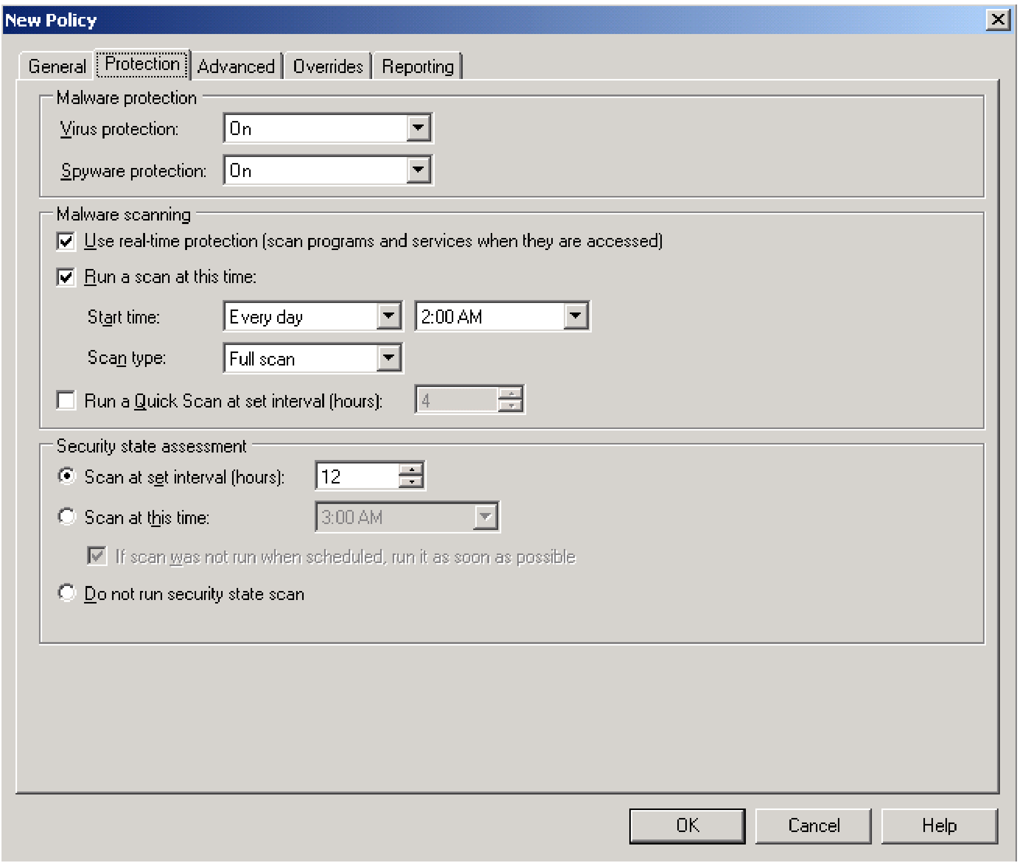
SCDW !NEW

Neue FCS Richtlinie



| Name | Last Modified | Modified By | Last Deployed | Deployed By | Deployed To |
|---|---|---|---|---|---|

Was soll denn alles drin sein?



Malware protection

Virus protection: On

Spyware protection: On

Malware scanning

☑ Use real-time protection (scan programs and services when they are accessed)

☑ Run a scan at this time:

Start time: Every day 2:00 AM

Scan type: Full scan

☐ Run a Quick Scan at set interval (hours): 4

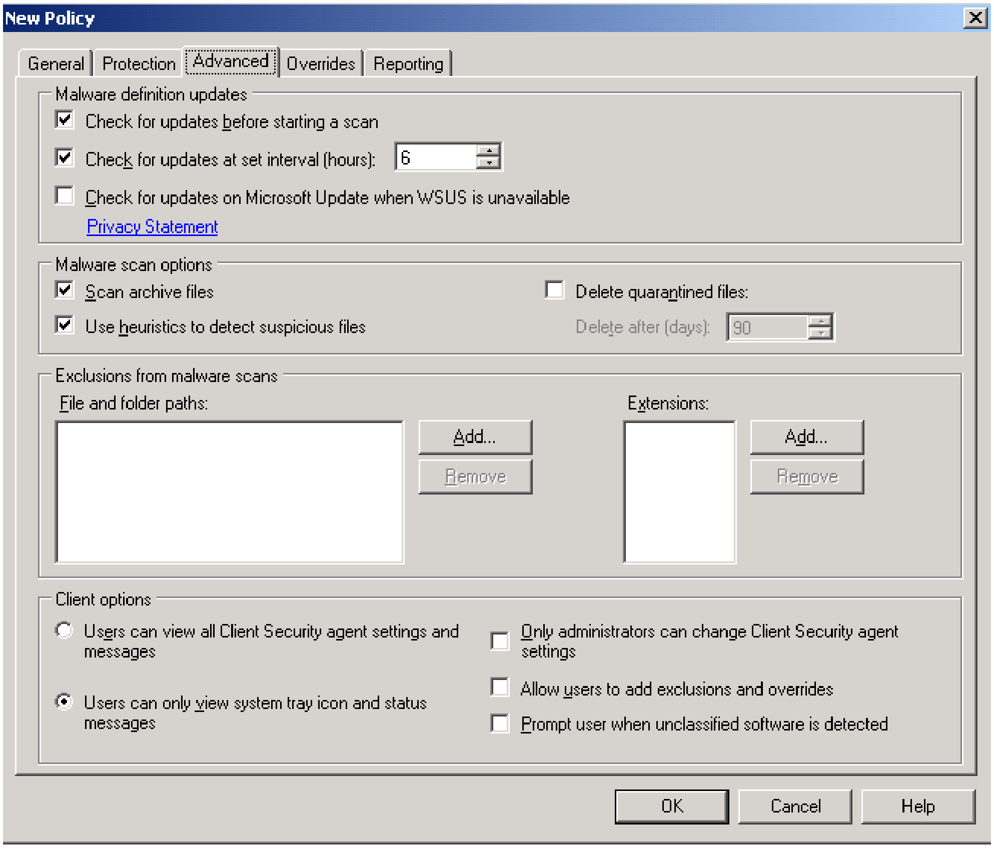
Security state assessment

● Scan at set interval (hours): 12

○ Scan at this time: 3:00 AM

☑ If scan was not run when scheduled, run it as soon as possible

○ Do not run security state scan



New Policy

General | Protection | Advanced | Overrides | Reporting

Malware definition updates

☑ Check for updates before starting a scan

☑ Check for updates at set interval (hours): 6

□ Check for updates on Microsoft Update when WSUS is unavailable

Privacy Statement

Malware scan options

☑ Scan archive files

☑ Use heuristics to detect suspicious files

□ Delete quarantined files:

Delete after (days): 90

Exclusions from malware scans

File and folder paths: Add... Remove

Extensions: Add... Remove

Client options

○ Users can view all Client Security agent settings and messages

● Users can only view system tray icon and status messages

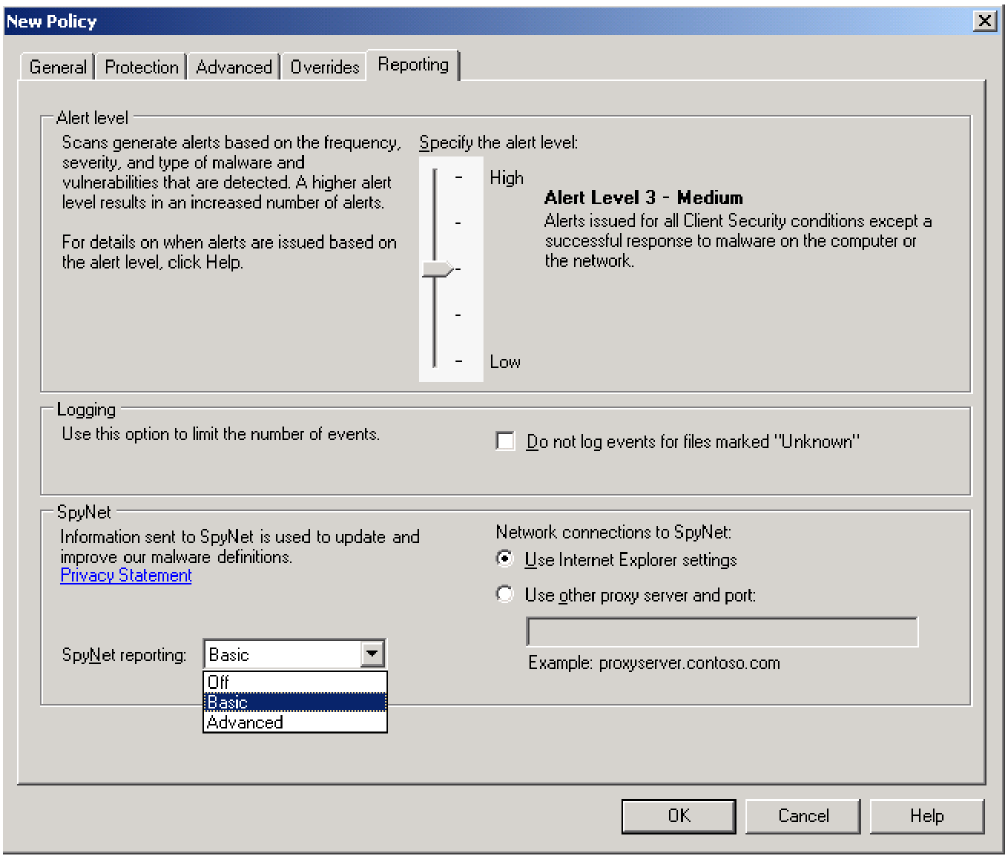
□ Only administrators can change Client Security agent settings

□ Allow users to add exclusions and overrides

□ Prompt user when unclassified software is detected

OK | Cancel | Help

## Reporting ohne Ende



New Policy

General | Protection | Advanced | Overrides | Reporting

Alert level

Scans generate alerts based on the frequency, severity, and type of malware and vulnerabilities that are detected. A higher alert level results in an increased number of alerts.

For details on when alerts are issued based on the alert level, click Help.

Specify the alert level:

**Alert Level 3 - Medium**

Alerts issued for all Client Security conditions except a successful response to malware on the computer or the network.

Logging

Use this option to limit the number of events.

□ Do not log events for files marked "Unknown"

SpyNet

Information sent to SpyNet is used to update and improve our malware definitions.

Privacy Statement

SpyNet reporting: Basic

Network connections to SpyNet:

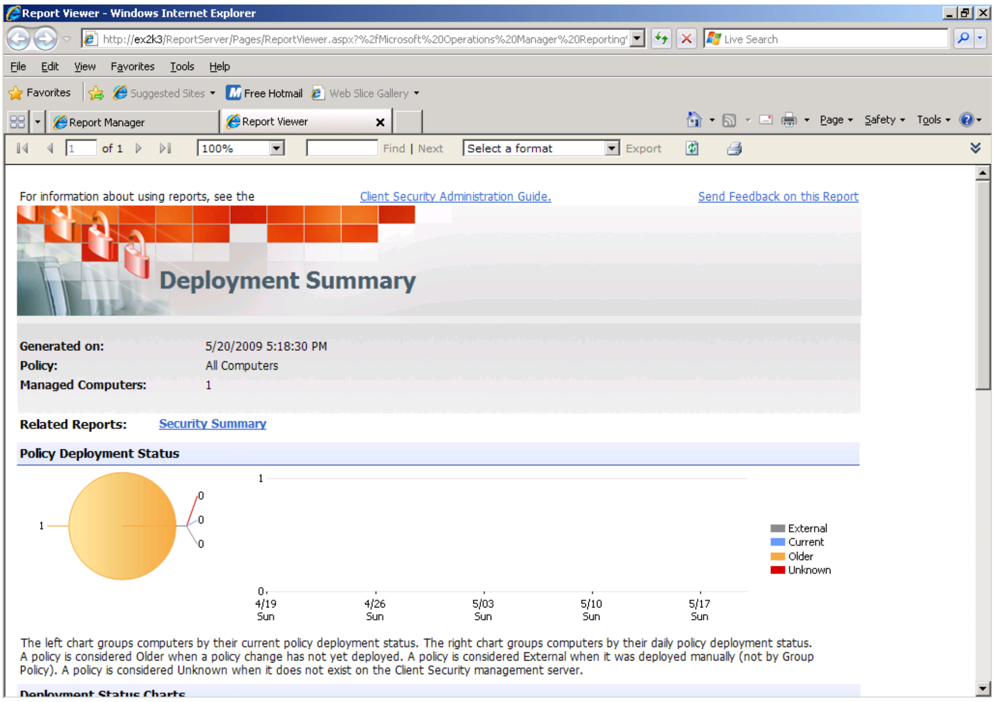
● Use Internet Explorer settings

○ Use other proxy server and port:

Example: proxyserver.contoso.com

OK | Cancel | Help

# View Reports



For information about using reports, see the Client Security Administration Guide. Send Feedback on this Report

**Generated on:** 5/20/2009 5:18:30 PM
**Policy:** All Computers
**Managed Computers:** 1

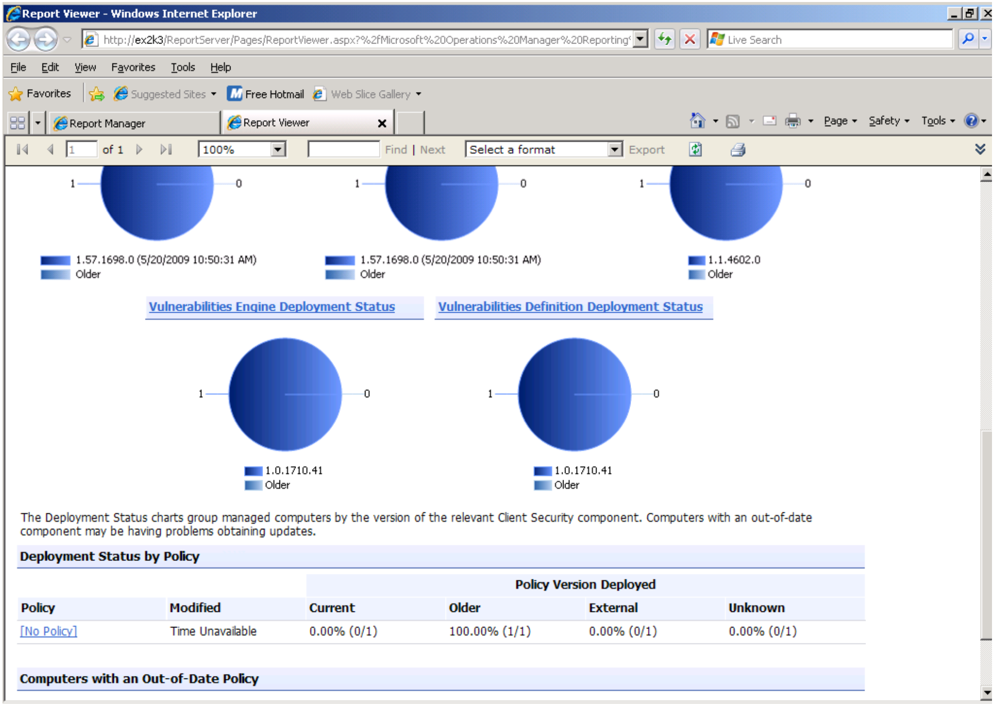
**Related Reports:** Security Summary

**Policy Deployment Status**

The left chart groups computers by their current policy deployment status. The right chart groups computers by their daily policy deployment status. A policy is considered Older when a policy change has not yet deployed. A policy is considered External when it was deployed manually (not by Group Policy). A policy is considered Unknown when it does not exist on the Client Security management server.

**Deployment Status Charts**

# Reports, Reports, Reports


Report Viewer - Windows Internet Explorer
http://ex2k3/ReportServer/Pages/ReportViewer.aspx?%2fMicrosoft%20Operations%20Manager%20Reporting
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Report Manager
Report Viewer
Page Safety Tools
1 of 1
100%
Find | Next
Select a format
Export
1
0
1.57.1698.0 (5/20/2009 10:50:31 AM)
Older
1
0
1.57.1698.0 (5/20/2009 10:50:31 AM)
Older
1
0
1.1.4602.0
Older
1
0
1.0.1710.41
Older
1
0
1.0.1710.41
Older

Vulnerabilities Engine Deployment Status    Vulnerabilities Definition Deployment Status

The Deployment Status charts group managed computers by the version of the relevant Client Security component. Computers with an out-of-date component may be having problems obtaining updates.

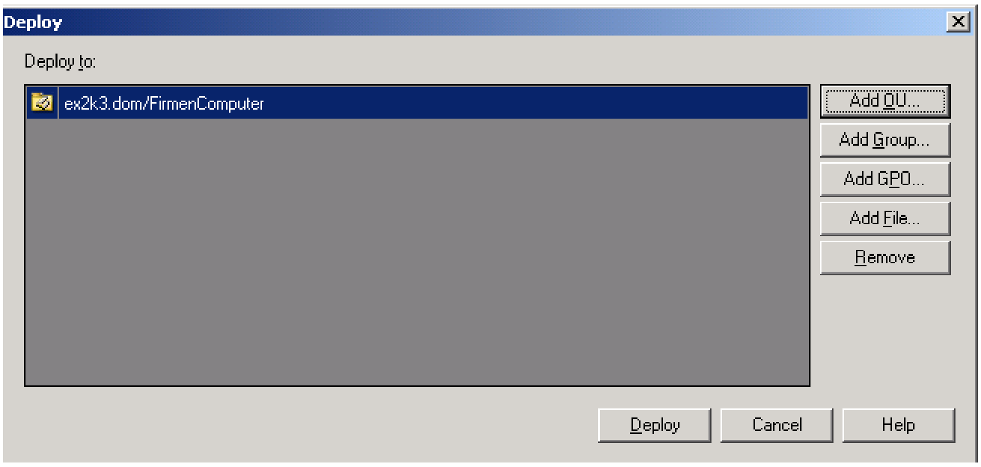
**Deployment Status by Policy**

| | | Policy Version Deployed | | | |
|---|---|---|---|---|---|
| **Policy** | **Modified** | **Current** | **Older** | **External** | **Unknown** |
| [No Policy] | Time Unavailable | 0.00% (0/1) | 100.00% (1/1) | 0.00% (0/1) | 0.00% (0/1) |

**Computers with an Out-of-Date Policy**

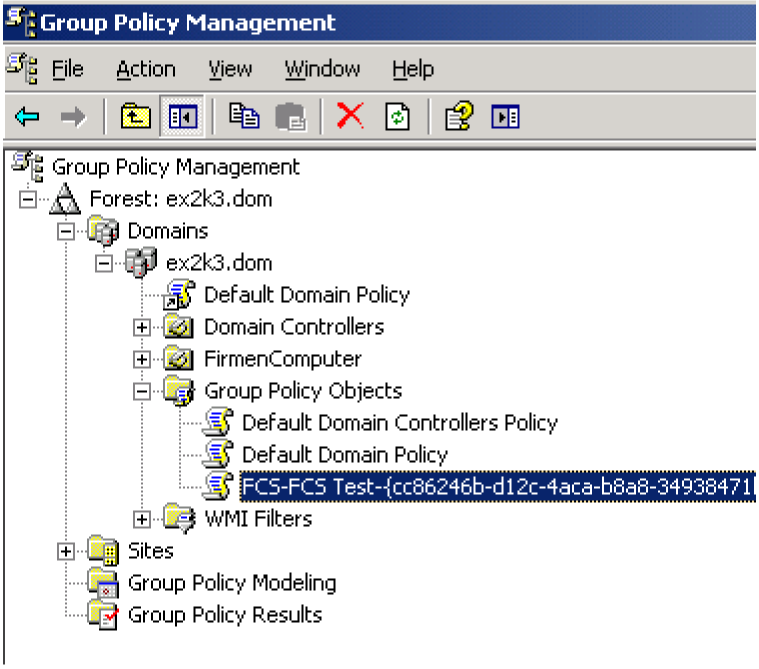
Wie bekomme ich nun einen Client in die FCS Console?

Deploy .....



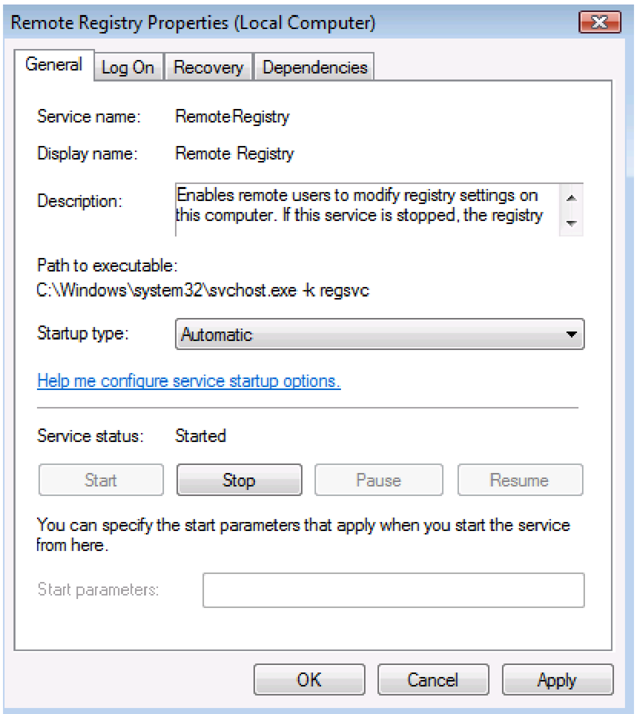
ex2k3.dom/FirmenComputer

oder / und per GPO



Group Policy Management
Forest: ex2k3.dom
Domains
ex2k3.dom
Default Domain Policy
Domain Controllers
FirmenComputer
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
FCS-FCS Test-{cc86246b-d12c-4aca-b8a8-34938471
WMI Filters
Sites
Group Policy Modeling
Group Policy Results

Verteilung schlaegt fehl, weil der Remote Registry Dienst nicht laeuft



Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry

Path to executable:
C:\Windows\system32\svchost.exe -k regsvc

Startup type: Automatic

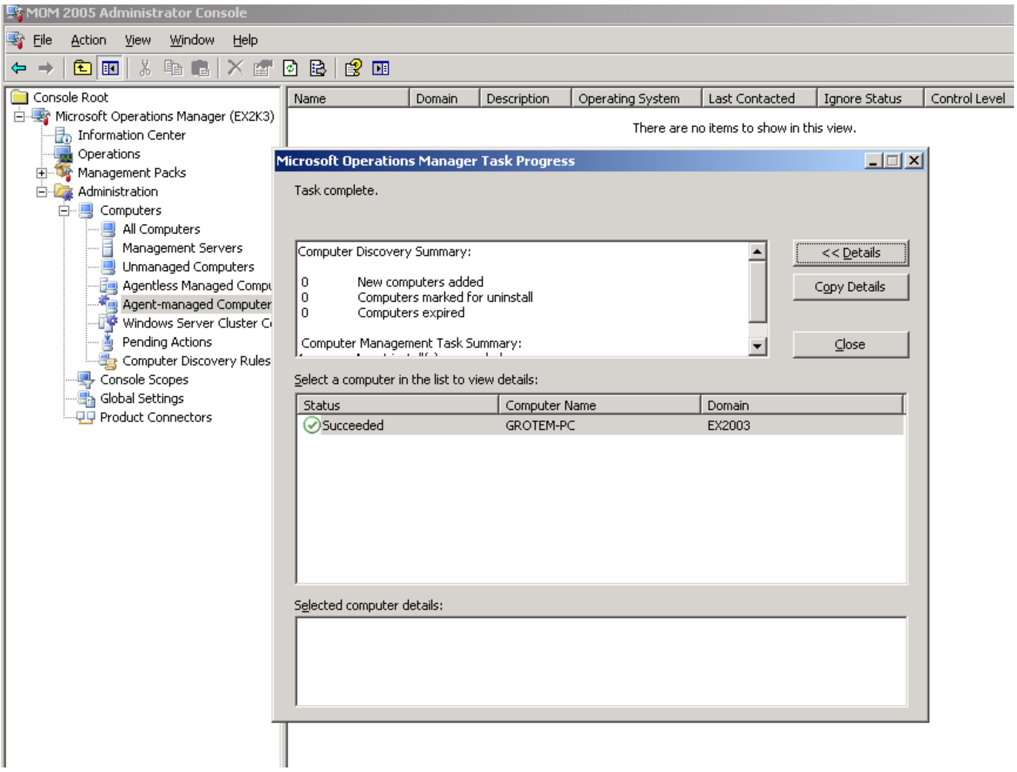
Help me configure service startup options.

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Jetzt passiert was



There are no items to show in this view.

Task complete.

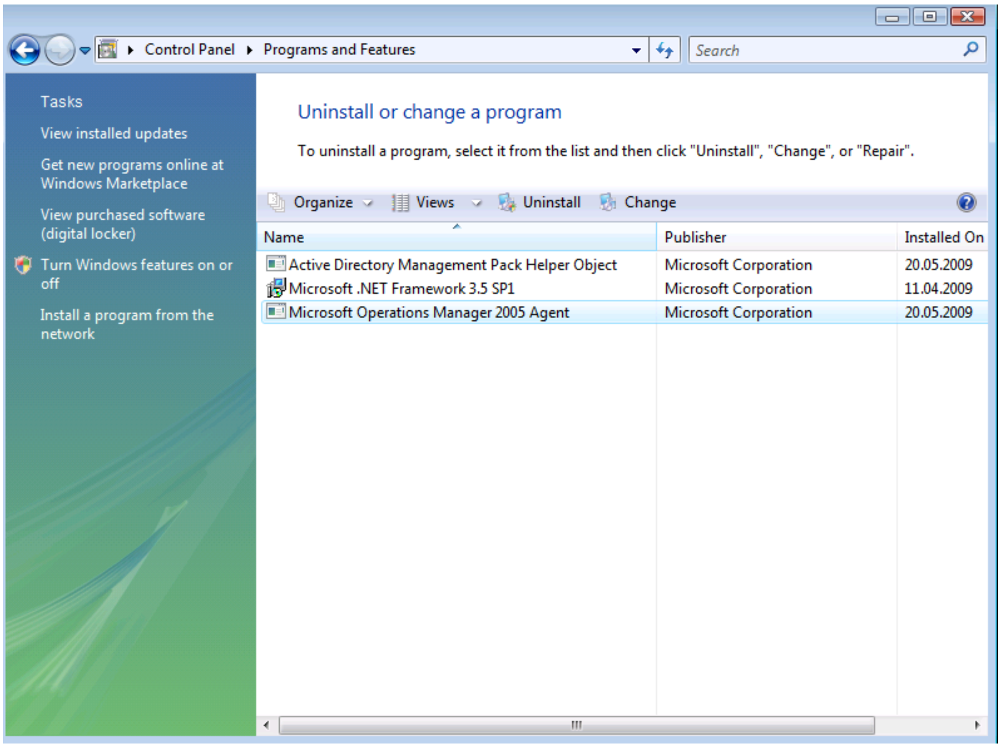
```
Computer Discovery Summary:

0        New computers added
0        Computers marked for uninstall
0        Computers expired

Computer Management Task Summary:
```

Select a computer in the list to view details:

| Status | Computer Name | Domain |
|---|---|---|
| ✓ Succeeded | GROTEM-PC | EX2003 |

Selected computer details:

druff ist der Agent

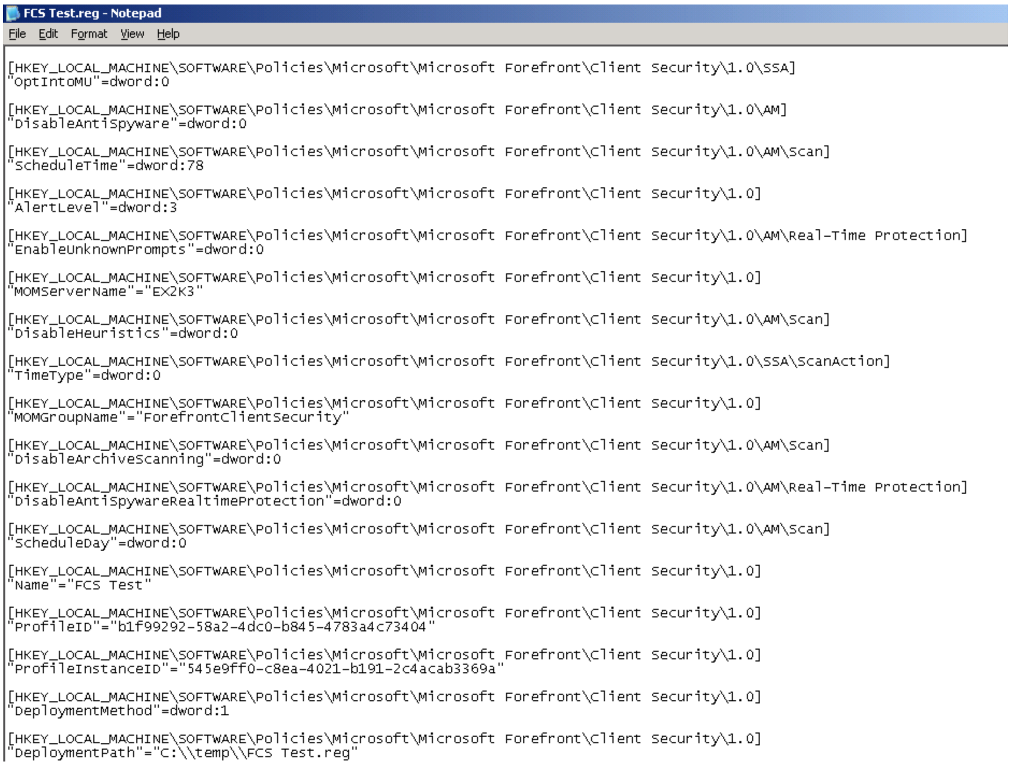

Control Panel
Programs and Features
Search
Tasks
View installed updates
Get new programs online at Windows Marketplace
View purchased software (digital locker)
Turn Windows features on or off
Install a program from the network
Organize
Views
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

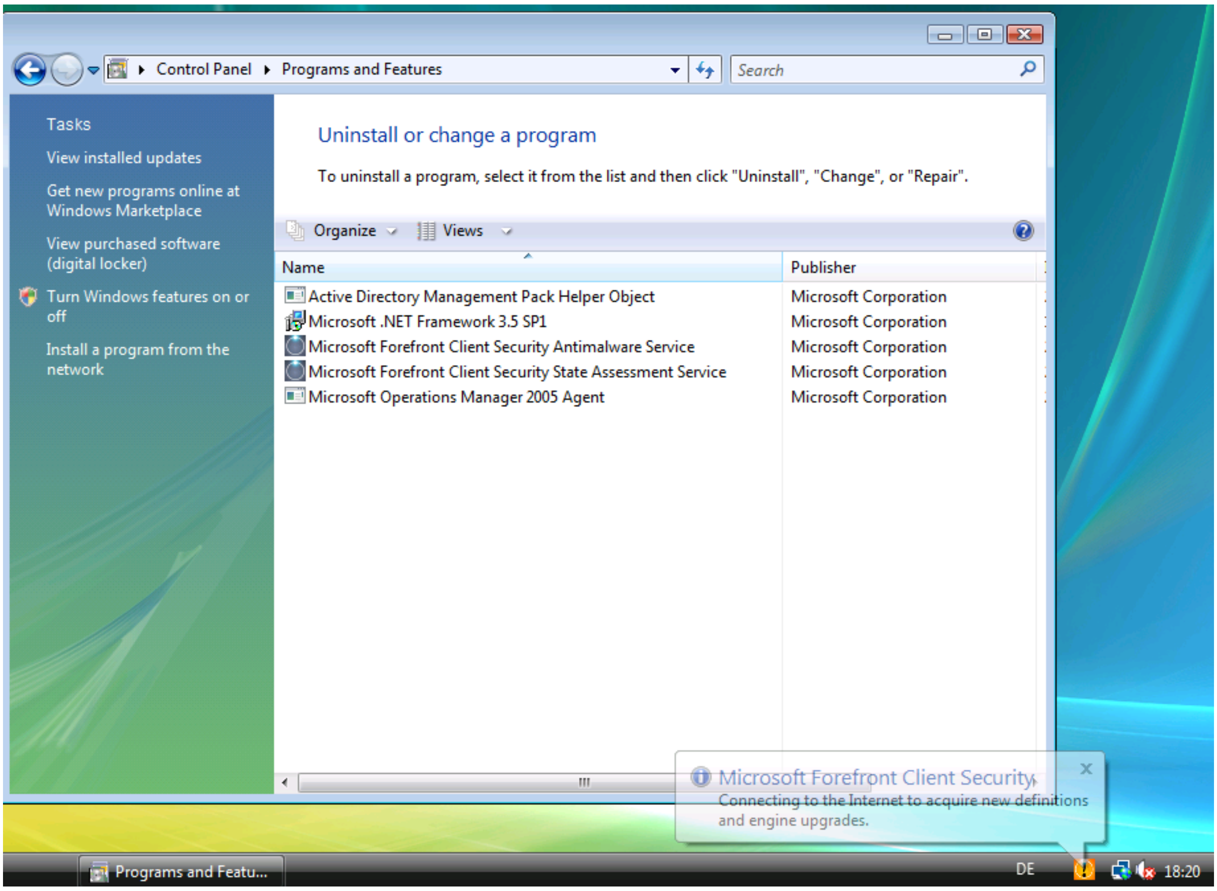
| Name | Publisher | Installed On |
|---|---|---|
| Active Directory Management Pack Helper Object | Microsoft Corporation | 20.05.2009 |
| Microsoft .NET Framework 3.5 SP1 | Microsoft Corporation | 11.04.2009 |
| Microsoft Operations Manager 2005 Agent | Microsoft Corporation | 20.05.2009 |

Deploy per REG-Datei



```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\SSA]
"OptIntoMU"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM]
"DisableAntiSpyware"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Scan]
"ScheduleTime"=dword:78

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"AlertLevel"=dword:3

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Real-Time Protection]
"EnableUnknownPrompts"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"MOMServerName"="EX2K3"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Scan]
"DisableHeuristics"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\SSA\ScanAction]
"TimeType"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"MOMGroupName"="ForefrontClientSecurity"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Scan]
"DisableArchiveScanning"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Real-Time Protection]
"DisableAntiSpywareRealtimeProtection"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0\AM\Scan]
"ScheduleDay"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"Name"="FCS Test"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"ProfileID"="b1f99292-58a2-4dc0-b845-4783a4c73404"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"ProfileInstanceID"="545e9ff0-c8ea-4021-b191-2c4acab3369a"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"DeploymentMethod"=dword:1

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Forefront\Client Security\1.0]
"DeploymentPath"="C:\\temp\\FCS Test.reg"
```

da isser



Control Panel ▸ Programs and Features
Search
Tasks
View installed updates
Get new programs online at Windows Marketplace
View purchased software (digital locker)
Turn Windows features on or off
Install a program from the network
Organize
Views
Programs and Featu...
DE
18:20

Uninstall or change a program

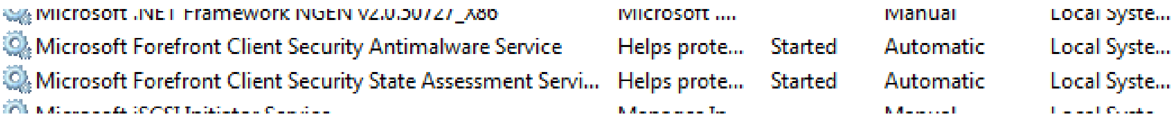
To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

| Name | Publisher |
|---|---|
| Active Directory Management Pack Helper Object | Microsoft Corporation |
| Microsoft .NET Framework 3.5 SP1 | Microsoft Corporation |
| Microsoft Forefront Client Security Antimalware Service | Microsoft Corporation |
| Microsoft Forefront Client Security State Assessment Service | Microsoft Corporation |
| Microsoft Operations Manager 2005 Agent | Microsoft Corporation |

Microsoft Forefront Client Security

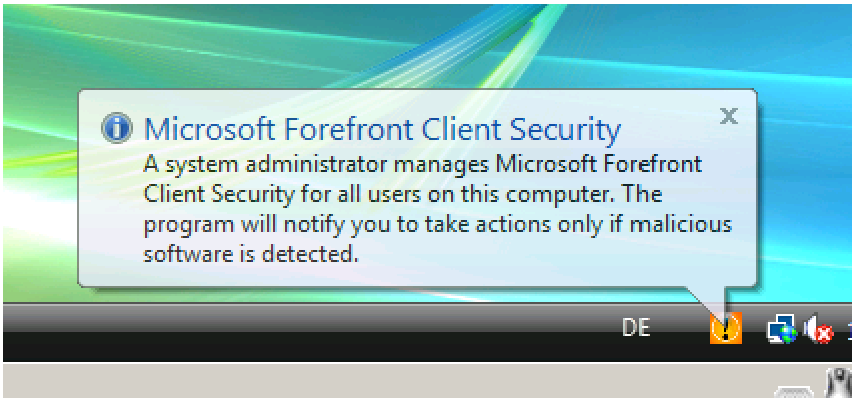
Connecting to the Internet to acquire new definitions and engine upgrades.

zwei neue Dienste auf dem Client



| | | | | |
|---|---|---|---|---|
| Microsoft .NET Framework NGEN v2.0.50727_X86 | Microsoft .... | | Manual | Local Syste... |
| Microsoft Forefront Client Security Antimalware Service | Helps prote... | Started | Automatic | Local Syste... |
| Microsoft Forefront Client Security State Assessment Servi... | Helps prote... | Started | Automatic | Local Syste... |
| Microsoft iSCSI Initiator Service | Manages In... | | Manual | Local Syste... |

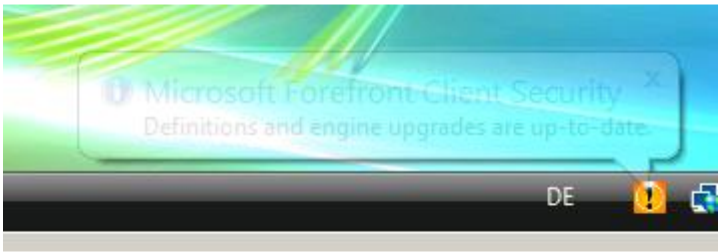
Zentrale Konfiguration



Microsoft Forefront Client Security

A system administrator manages Microsoft Forefront Client Security for all users on this computer. The program will notify you to take actions only if malicious software is detected.

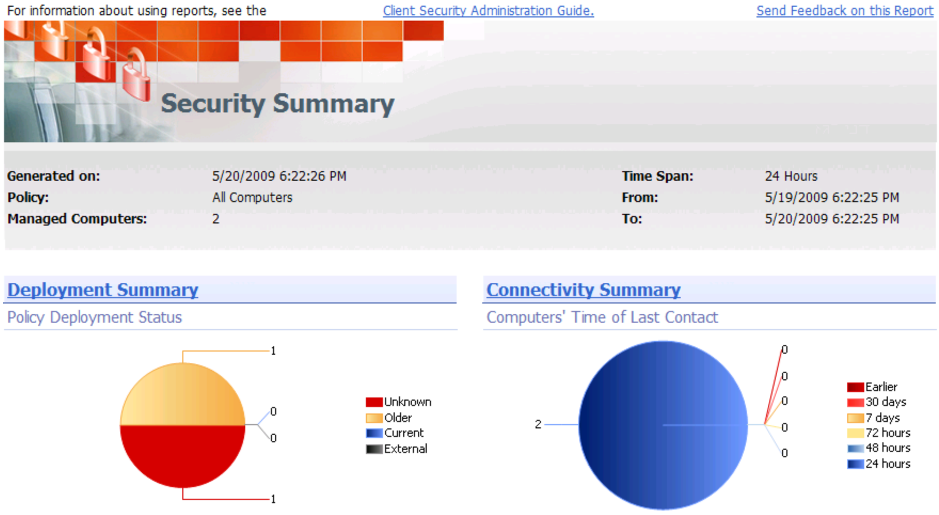
## Updates sind da



Microsoft Forefront Client Security

Definitions and engine upgrades are up-to-date

## FCS Console Summary



For information about using reports, see the Client Security Administration Guide. Send Feedback on this Report

Security Summary

| | | | |
|---|---|---|---|
| **Generated on:** | 5/20/2009 6:22:26 PM | **Time Span:** | 24 Hours |
| **Policy:** | All Computers | **From:** | 5/19/2009 6:22:25 PM |
| **Managed Computers:** | 2 | **To:** | 5/20/2009 6:22:25 PM |

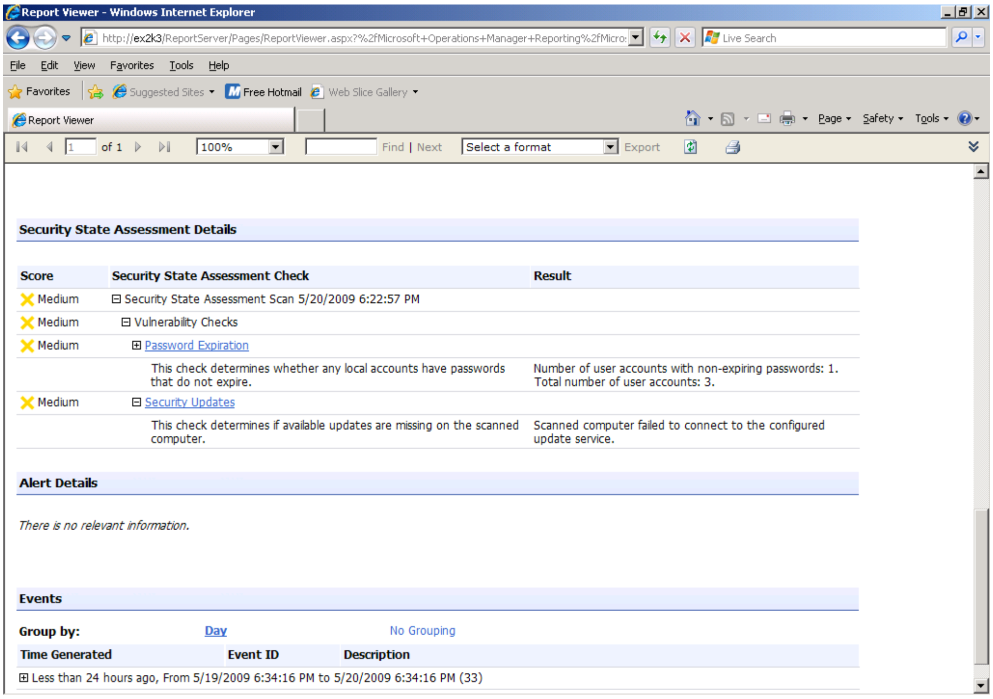
**Deployment Summary**

Policy Deployment Status

**Connectivity Summary**

Computers' Time of Last Contact

## Security Check des Clients



Report Viewer - Windows Internet Explorer
http://ex2k3/ReportServer/Pages/ReportViewer.aspx?%2fMicrosoft+Operations+Manager+Reporting%2fMicro
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Report Viewer
Page
Safety
Tools
1 of 1
100%
Find | Next
Select a format
Export

**Security State Assessment Details**

| Score | Security State Assessment Check | Result |
|---|---|---|
| ✗ Medium | ⊟ Security State Assessment Scan 5/20/2009 6:22:57 PM | |
| ✗ Medium | ⊟ Vulnerability Checks | |
| ✗ Medium | ⊞ Password Expiration | |
| | This check determines whether any local accounts have passwords that do not expire. | Number of user accounts with non-expiring passwords: 1. Total number of user accounts: 3. |
| ✗ Medium | ⊟ Security Updates | |
| | This check determines if available updates are missing on the scanned computer. | Scanned computer failed to connect to the configured update service. |

**Alert Details**

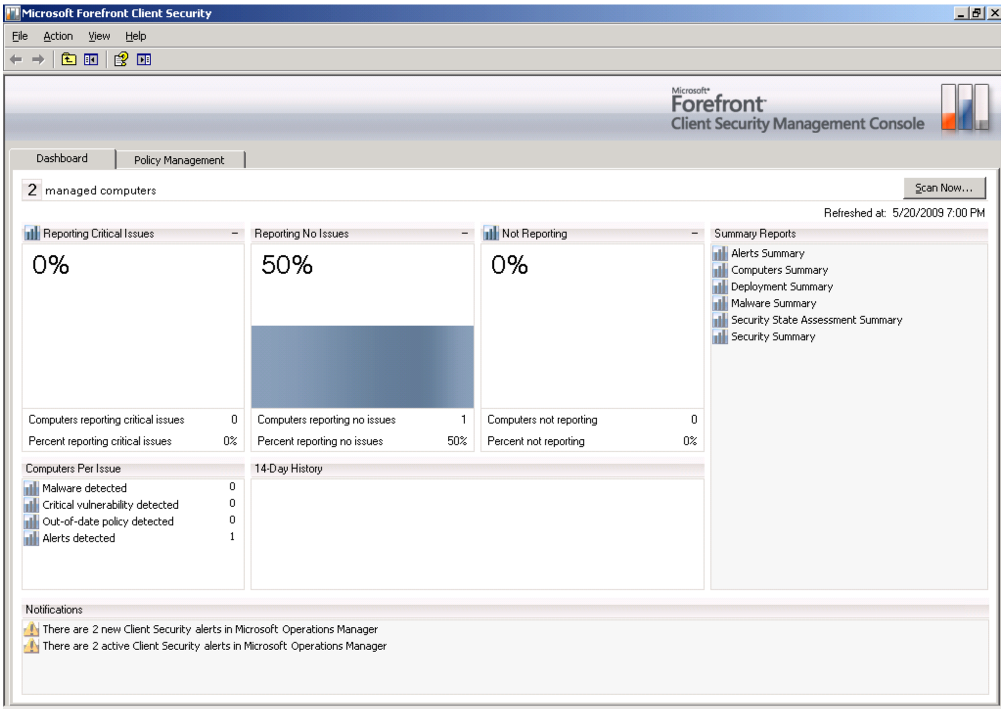
*There is no relevant information.*

**Events**

**Group by:** Day No Grouping

| Time Generated | Event ID | Description |
|---|---|---|
| ⊞ Less than 24 hours ago, From 5/19/2009 6:34:16 PM to 5/20/2009 6:34:16 PM (33) | | |

## Gesamtuebersicht aller Clients


Microsoft Forefront Client Security
File Action View Help
Microsoft® Forefront Client Security Management Console
Dashboard
Policy Management
Scan Now...

2 managed computers

Refreshed at: 5/20/2009 7:00 PM

| Reporting Critical Issues | | Reporting No Issues | | Not Reporting | |
|---|---|---|---|---|---|
| 0% | | 50% | | 0% | |
| Computers reporting critical issues | 0 | Computers reporting no issues | 1 | Computers not reporting | 0 |
| Percent reporting critical issues | 0% | Percent reporting no issues | 50% | Percent not reporting | 0% |

Summary Reports

- Alerts Summary
- Computers Summary
- Deployment Summary
- Malware Summary
- Security State Assessment Summary
- Security Summary

| Computers Per Issue | |
|---|---|
| Malware detected | 0 |
| Critical vulnerability detected | 0 |
| Out-of-date policy detected | 0 |
| Alerts detected | 1 |

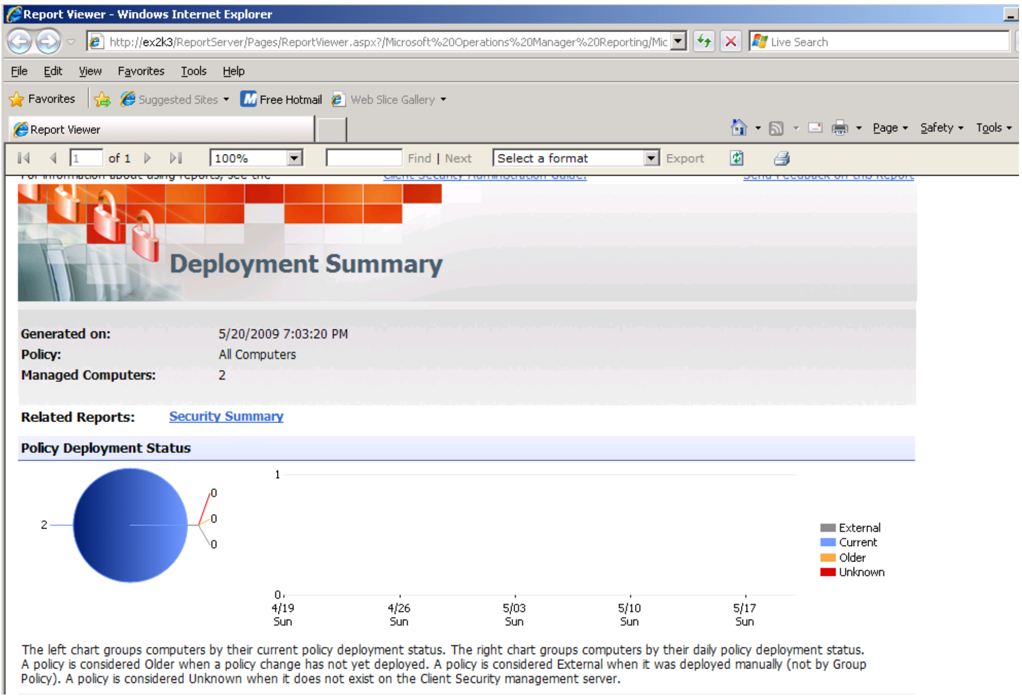
14-Day History

Notifications

There are 2 new Client Security alerts in Microsoft Operations Manager

There are 2 active Client Security alerts in Microsoft Operations Manager

## Jetzt sehen die Reports auch sauberer aus



Deployment Summary

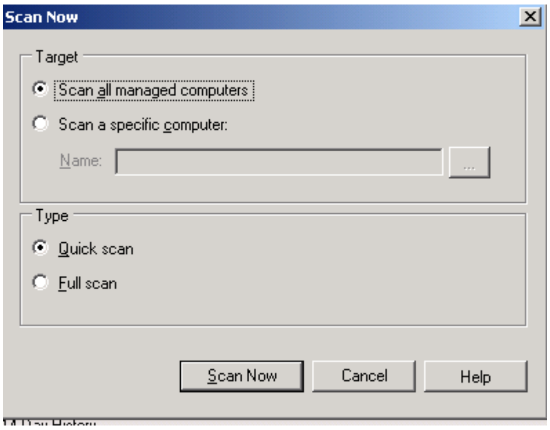
| | |
|---|---|
| **Generated on:** | 5/20/2009 7:03:20 PM |
| **Policy:** | All Computers |
| **Managed Computers:** | 2 |

**Related Reports:** Security Summary

**Policy Deployment Status**

The left chart groups computers by their current policy deployment status. The right chart groups computers by their daily policy deployment status. A policy is considered Older when a policy change has not yet deployed. A policy is considered External when it was deployed manually (not by Group Policy). A policy is considered Unknown when it does not exist on the Client Security management server.

Manueller Scan von Client Computern



● Scan all managed computers

○ Scan a specific computer:

Name:

● Quick scan

○ Full scan

... danach ist ein Scan in Progress