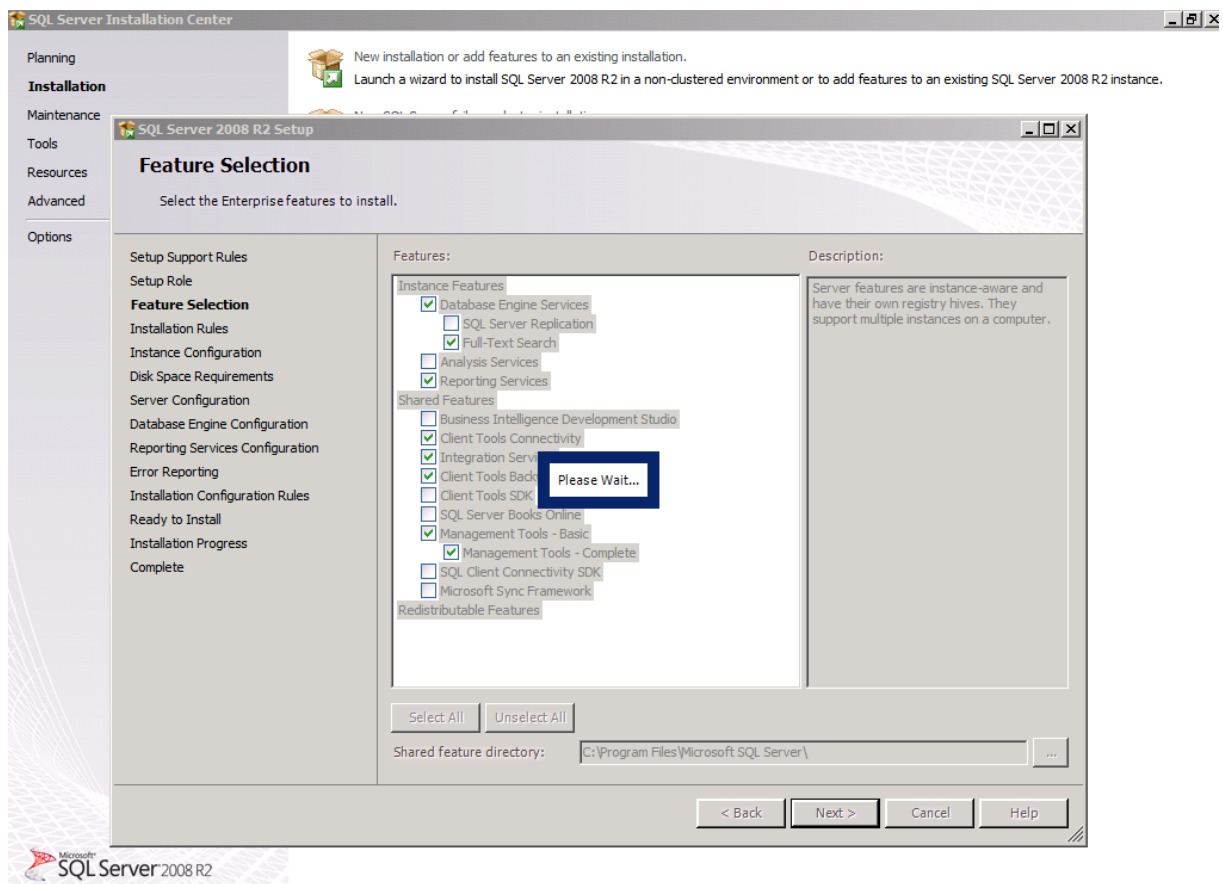


Forefront Endpoint Protection 2010 Installation und Konfiguration



SQL Server 2008 R2 Setup

Server Configuration

Specify the service accounts and collation configuration.

Setup Support Rules
 Setup Role
 Feature Selection
 Installation Rules
 Instance Configuration
 Disk Space Requirements
Server Configuration
 Database Engine Configuration
 Reporting Services Configuration
 Error Reporting
 Installation Configuration Rules
 Ready to Install
 Installation Progress
 Complete

Service Accounts | Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	TRAINER\administrator	••••••••	Manual
SQL Server Database Engine	TRAINER\administrator	••••••••	Automatic
SQL Server Reporting Services	TRAINER\administrator	••••••••	Automatic
SQL Server Integration Services 10.0	TRAINER\administrator	••••••~•	Automatic
SQL Full-text Filter Daemon Launcher	NT AUTHORITY\LOCAL S...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL S...		Disabled

Use the same account for all SQL Server services

< Back Next > Cancel Help

SQL Server 2008 R2 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Setup Support Rules
 Setup Role
 Feature Selection
 Installation Rules
 Instance Configuration
 Disk Space Requirements
 Server Configuration
Database Engine Configuration
 Reporting Services Configuration
 Error Reporting
 Installation Configuration Rules
 Ready to Install
 Installation Progress
 Complete

Account Provisioning | Data Directories | FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

☒ Windows authentication mode
☐ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

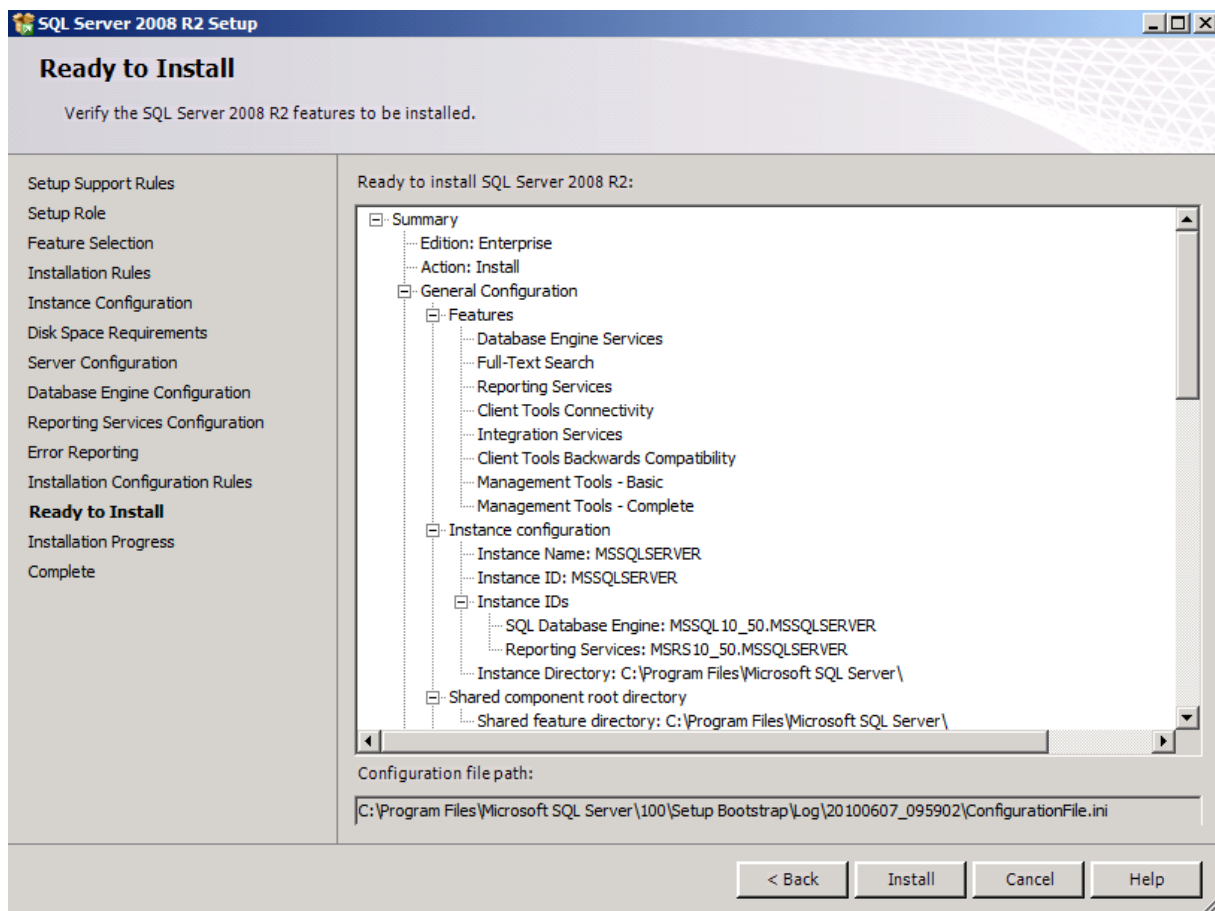
Confirm password:

Specify SQL Server administrators

TRAINER\administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

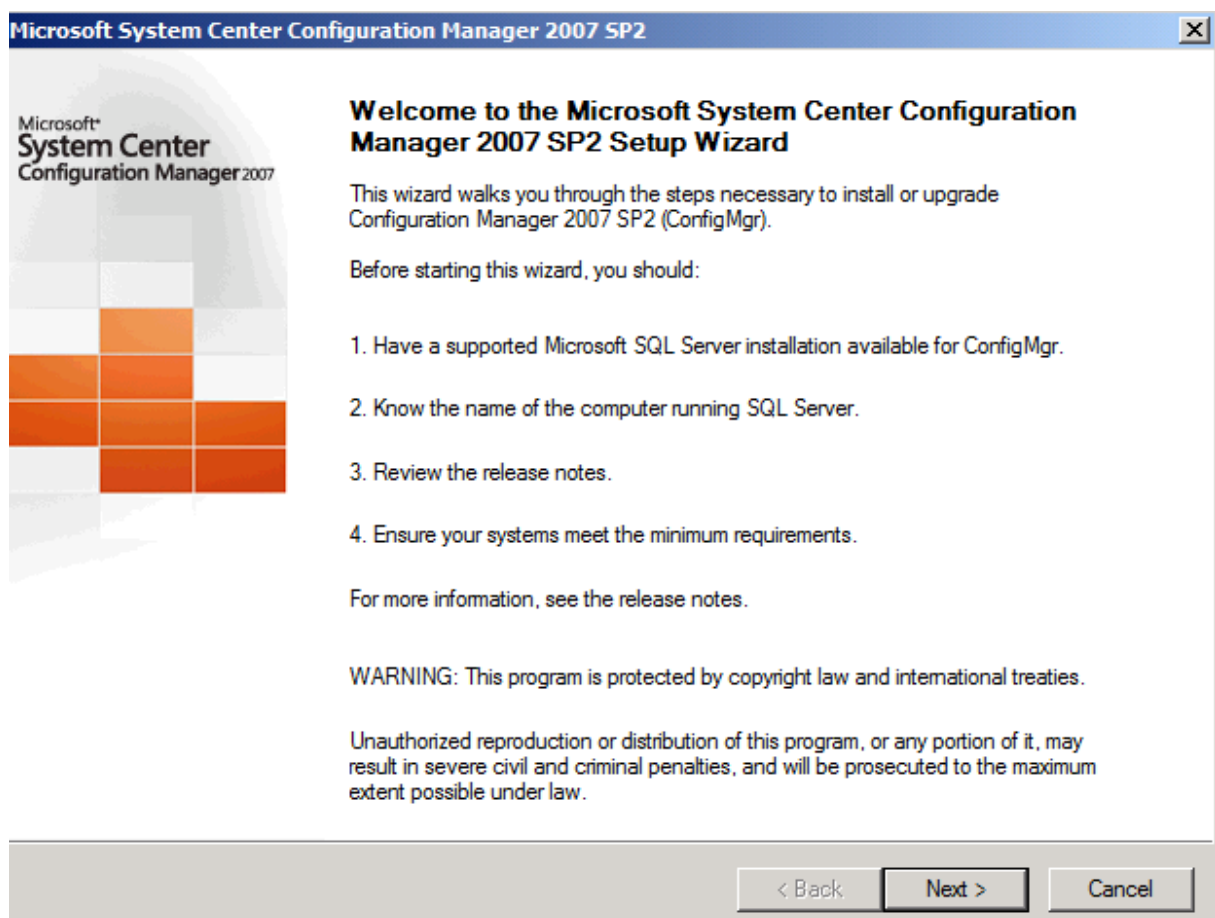
< Back Next > Cancel Help



WSUS Installation



SCCM Installation



Available Setup Options

Setup has enabled available installation options based on the installed operating system and any existing Systems Management Server 2003 or Configuration Manager installations.



Setup has not detected an existing installation of a primary site server, secondary site server, site system, or Configuration Manager console on this computer.

- ☒ Install a Configuration Manager site server
- ☐ Upgrade an existing Configuration Manager or SMS 2003 installation
- ☐ Install or upgrade an administrator console
- ☐ Perform site maintenance or reset this Site
- ☐ Uninstall a Configuration Manager site server

< Back

Next >

Cancel

Site Type

Specify the type of site you would like to install.



☒ Primary site

A primary site stores data for itself and for all of its child sites in a SQL Server database.

Primary sites are used to administer Configuration Manager hierarchies. Secondary sites must be children of the primary sites, and Configuration Manager clients must be assigned to primary sites.

☐ Secondary site

A secondary site must be attached to and managed from a primary site. A secondary site has no SQL Server database and forwards all Configuration Manager client information to the parent site's database.

Secondary sites are useful to control bandwidth across slow network connections but cannot have child sites and cannot be converted to primary sites.

For more information, see the Configuration Manager 2007 SP2 planning documentation.

< Back

Next >

Cancel

**Site Settings**

Please enter your Configuration Manager site code and site name.



The site code will be used to uniquely identify this Configuration Manager site in your hierarchy.

Enter a 3-character site code containing letters, numbers, or a combination of the two. The site code and site name cannot be changed after installation and must be unique throughout your Configuration Manager hierarchy.

Site code:

Example: XYZ

The site name is a friendly name identifier for this site.

Site name:

Example: Contoso Headquarters Site

< Back

Next >

Cancel

**Site Mode**

Specify the ConfigMgr site mode for this site.



☐ Configuration Manager Native Mode

Select native mode if you need the highest level of Configuration Manager security or must support Internet-based clients.

Native mode requires an existing public key infrastructure (PKI) to support clients in this site and some of the site systems. The site server signing certificate must already be installed on this computer.

Site server signing certificate details:

Browse...

☒ Configuration Manager Mixed Mode

Select mixed mode if this site will support SMS 2003 clients, or has a parent site configured for mixed mode.

Internet-based clients cannot be managed if the site is operating in mixed mode.

< Back

Next >

Cancel

**Client Agent Selection**

Configuration Manager can enable client agents for you after setup completes.



Select the client agents to enable with default settings.

Client agents can be modified by using the Configuration Manager console after setup is completed.

- | | |
|---|--|
| <input checked="" type="checkbox"/> Software inventory | <input checked="" type="checkbox"/> Software updates |
| <input checked="" type="checkbox"/> Hardware inventory | <input checked="" type="checkbox"/> Software metering |
| <input checked="" type="checkbox"/> Advertised programs | <input checked="" type="checkbox"/> Desired configuration management |
| <input type="checkbox"/> Network Access Protection | <input checked="" type="checkbox"/> Remote tools |

Refer to the Configuration Manager 2007 SP2 documentation for more information about client agents.

< Back

Next >

Cancel



Database Server

Specify the Microsoft SQL Server information for your installation.



Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.

SQL Server Computer

Specify the computer name, SQL Server instance, and database name:

SQL Server and instance, if applicable:

Examples: Server1, Server2\InstanceName

ConfigMgr site database:

Example: SMS_XYZ

< Back

Next >

Cancel



SMS Provider Settings

Specify the SMS Provider settings for your Configuration Manager site.



The SMS Provider is used by the Configuration Manager console to communicate with the site database.

Enter the appropriate installation location for the provider:

FEP

The provider cannot be installed on a clustered SQL server.

< Back

Next >

Cancel

Management point

Specify the server to be used as your ConfigMgr management point.



Configuration Manager uses the management point to communicate with all clients for this site.

- ☒ Install a management point

Management point computer fully qualified domain name (FQDN) on the intranet:

Example: MPServer1.contoso.com

- ☐ Do not install a management point

A management point can be installed later using the Configuration Manager console.

< Back

Next >

Cancel

**Port Settings**

Specify the TCP port that clients will use to communicate with ConfigMgr site systems.



The settings you configure will be used by all site roles for client to server communication.
If you selected ConfigMgr mixed mode, you cannot configure HTTPS settings.

HTTP settings

☒ Use default port (80)

☐ Use custom port:

HTTPS settings

☐ Use default port (443)

☐ Use custom port:

You can change these settings after installation by using the Configuration Manager console.

< Back

Next >

Cancel

**Updated Prerequisite Components**

Specify whether to download updated components or install from an alternate path



If your computer is connected to the Internet, Setup can check for updated prerequisite components and download them automatically to a path you specify.

Setup will install the latest version of the prerequisites if they are available.

- ☒ Check for updates and download newer versions to an alternate path
- ☐ The latest updates have already been downloaded to an alternate path

To ensure the highest level of functionality and compatibility, you should download the latest available components.

< Back

Next >

Cancel

Microsoft System Center Configuration Manager 2007 SP2



Updated Prerequisite Component Path

Specify the alternate path for Setup to store or access updated components.



Enter the alternate path that Setup should search for prerequisite components. If you choose to check for new updates, Setup will download any updated versions to the alternate path.

Note: You can use the same alternate path to install multiple sites. Always verify that the alternate path contains the most recent updates.

Alternate path:

C:\SCCM-Update

Browse...

Example: \\servername\sharename, C:\downloads

< Back

Next >

Cancel

Downloading updates

Please wait while Configuration Manager downloads updated components...

Downloading file 2 of 88: msrdcoob_ia64.exe



Cancel

Microsoft System Center Configuration Manager 2007 SP2

Settings Summary

Configuration Manager will be installed with the following settings:

Setup Component	Component Details
Setup Type	Primary site installation
Site Code	FEP
Site Name	FEP-Site
ConfigMgr Security Mode	Mixed
Product Key	PYHYP-WXB3B-B2CCM-V9DX9-VDY8T
Installation Directory	C:\Program Files\Microsoft Configuration Manager
External File Folder	C:\SCCM-Update
SQL Server	FEP
ConfigMgr Database Name	SMS_FEP
SMS Provider	FEP
Management Point	FEP
ConfigMgr Agents	Software inventory
	Hardware inventory
	Advertised programs
	Software updates
	Software metering

To change the settings click Back. To apply these settings and launch the installation prerequisite check, click Next. After the installation prerequisite check has begun, you cannot change these settings.

< Back Next > Cancel

FEP Setup

Microsoft Forefront Endpoint Protection 2010 Server Setup

Welcome to Forefront Endpoint Protection 2010 Setup Wizard

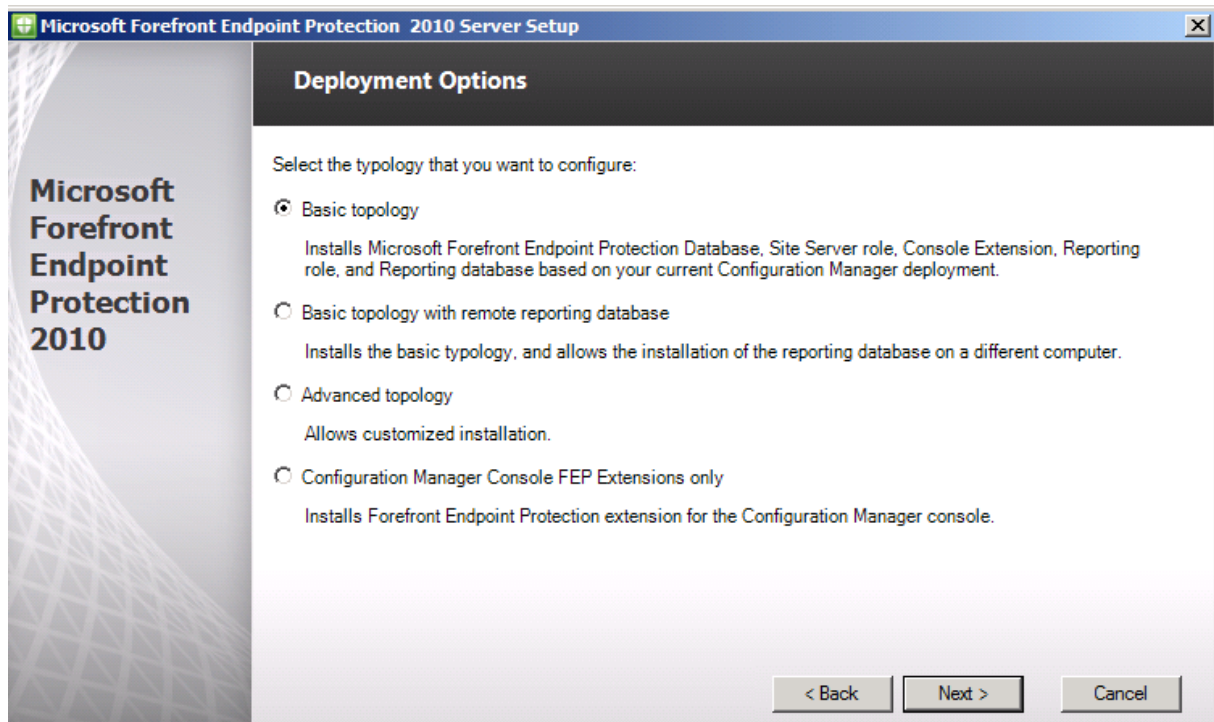
This wizard walks you through the steps necessary to install Microsoft Forefront Endpoint Protection 2010. Before you proceed, you should read the [Forefront Endpoint Protection Installation Guide](#) and then read the [Microsoft Forefront Protection Privacy Statement](#).

Name:

Organization:

Next > Cancel

All in One



The screenshot shows the 'Deployment Options' window of the Microsoft Forefront Endpoint Protection 2010 Server Setup. The window has a blue title bar and a sidebar on the left with the product name. The main area contains a list of deployment options with radio buttons. The 'Basic topology' option is selected. Below the options are three buttons: '< Back', 'Next >', and 'Cancel'.

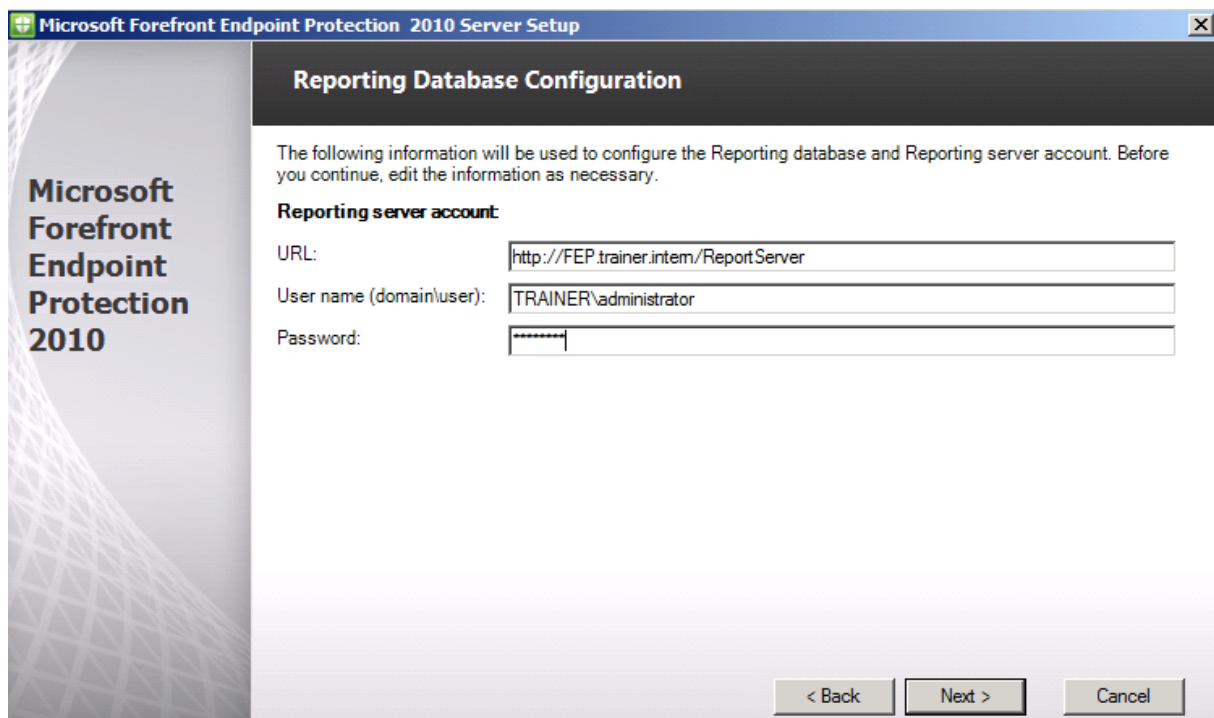
Microsoft Forefront Endpoint Protection 2010

Deployment Options

Select the typology that you want to configure:

- ☒ **Basic topology**
Installs Microsoft Forefront Endpoint Protection Database, Site Server role, Console Extension, Reporting role, and Reporting database based on your current Configuration Manager deployment.
- ☐ **Basic topology with remote reporting database**
Installs the basic typology, and allows the installation of the reporting database on a different computer.
- ☐ **Advanced topology**
Allows customized installation.
- ☐ **Configuration Manager Console FEP Extensions only**
Installs Forefront Endpoint Protection extension for the Configuration Manager console.

< Back Next > Cancel



The screenshot shows the 'Reporting Database Configuration' window of the Microsoft Forefront Endpoint Protection 2010 Server Setup. The window has a blue title bar and a sidebar on the left with the product name. The main area contains instructions for configuring the reporting database and server account. Below the instructions are three input fields for 'URL', 'User name (domain/user)', and 'Password'. The 'URL' field contains 'http://FEP.trainer.intern/ReportServer', the 'User name' field contains 'TRAINER\administrator', and the 'Password' field contains a masked password. Below the input fields are three buttons: '< Back', 'Next >', and 'Cancel'.

Microsoft Forefront Endpoint Protection 2010

Reporting Database Configuration

The following information will be used to configure the Reporting database and Reporting server account. Before you continue, edit the information as necessary.

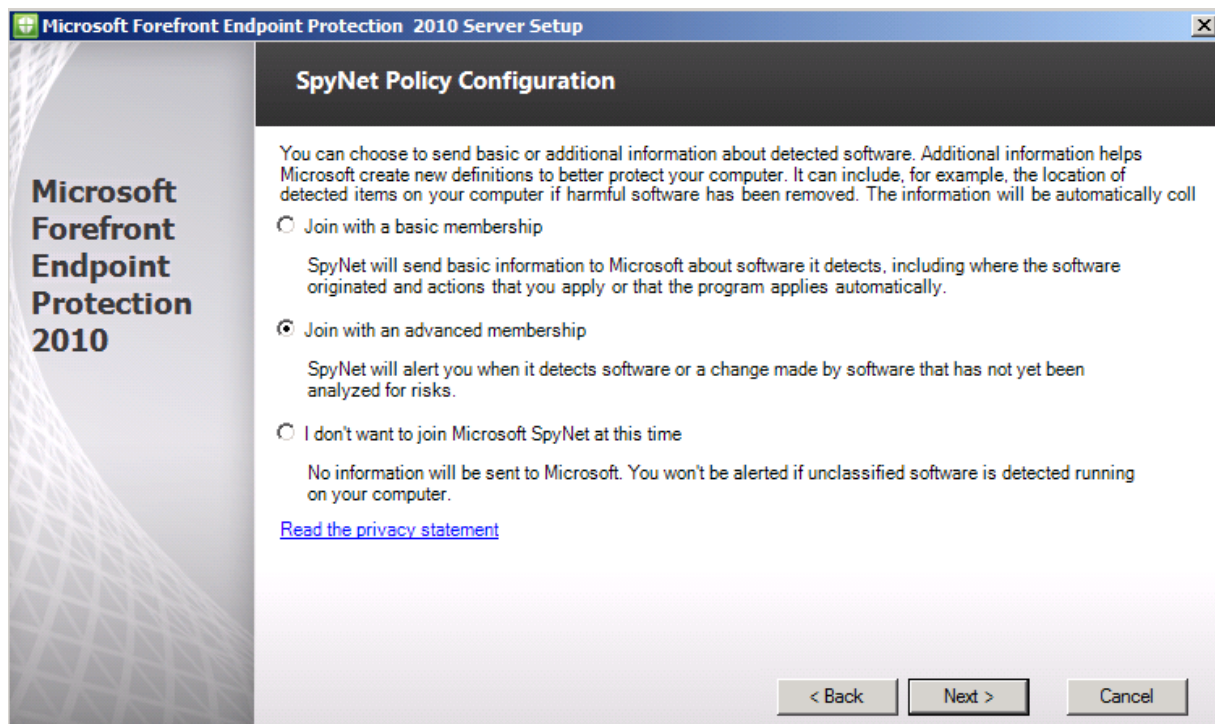
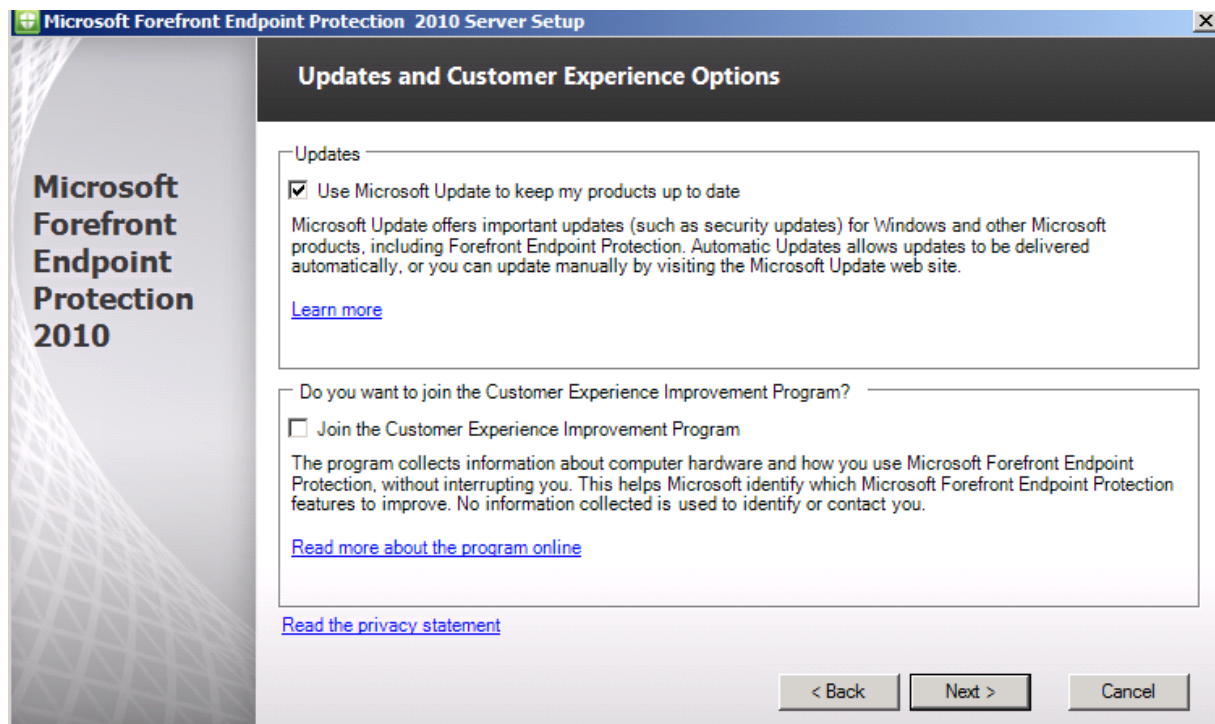
Reporting server account:

URL:

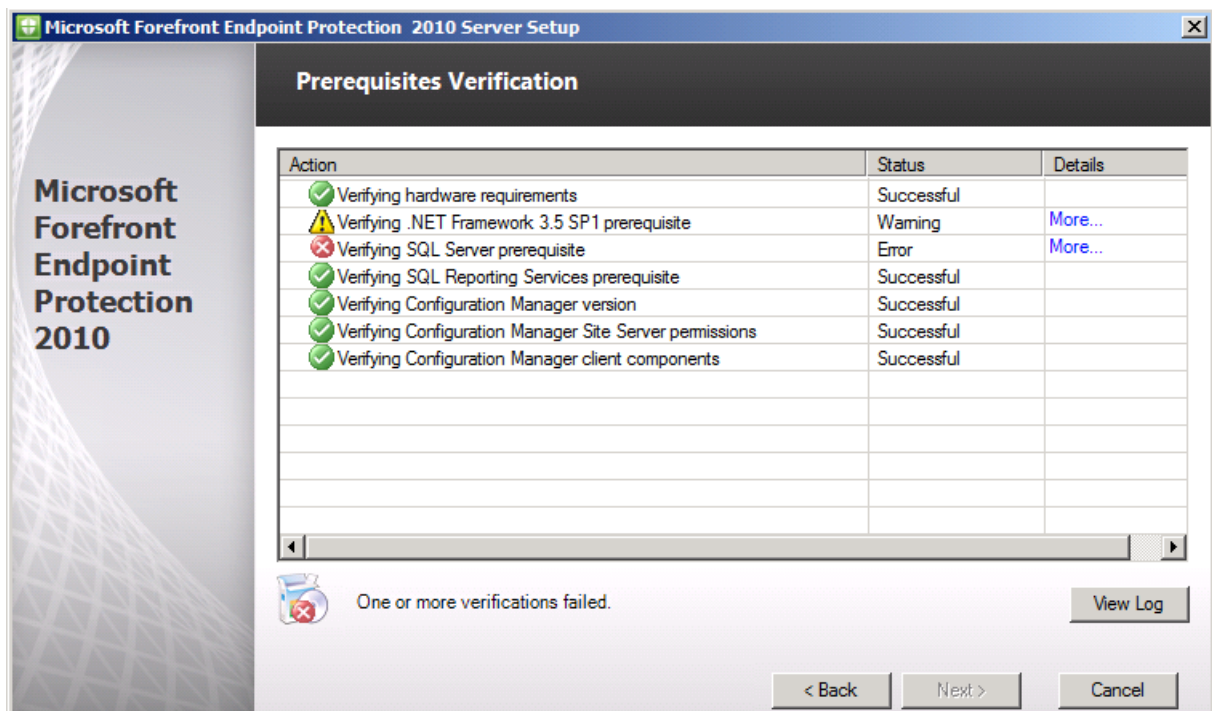
User name (domain/user):

Password:

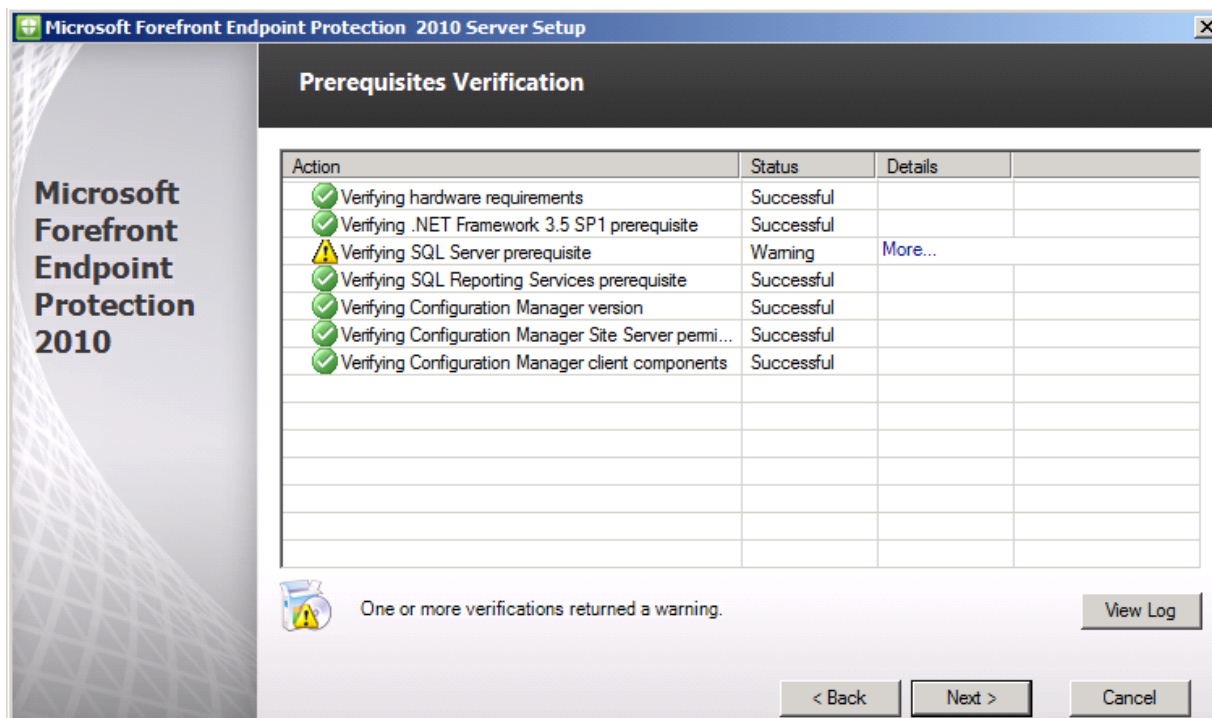
< Back Next > Cancel



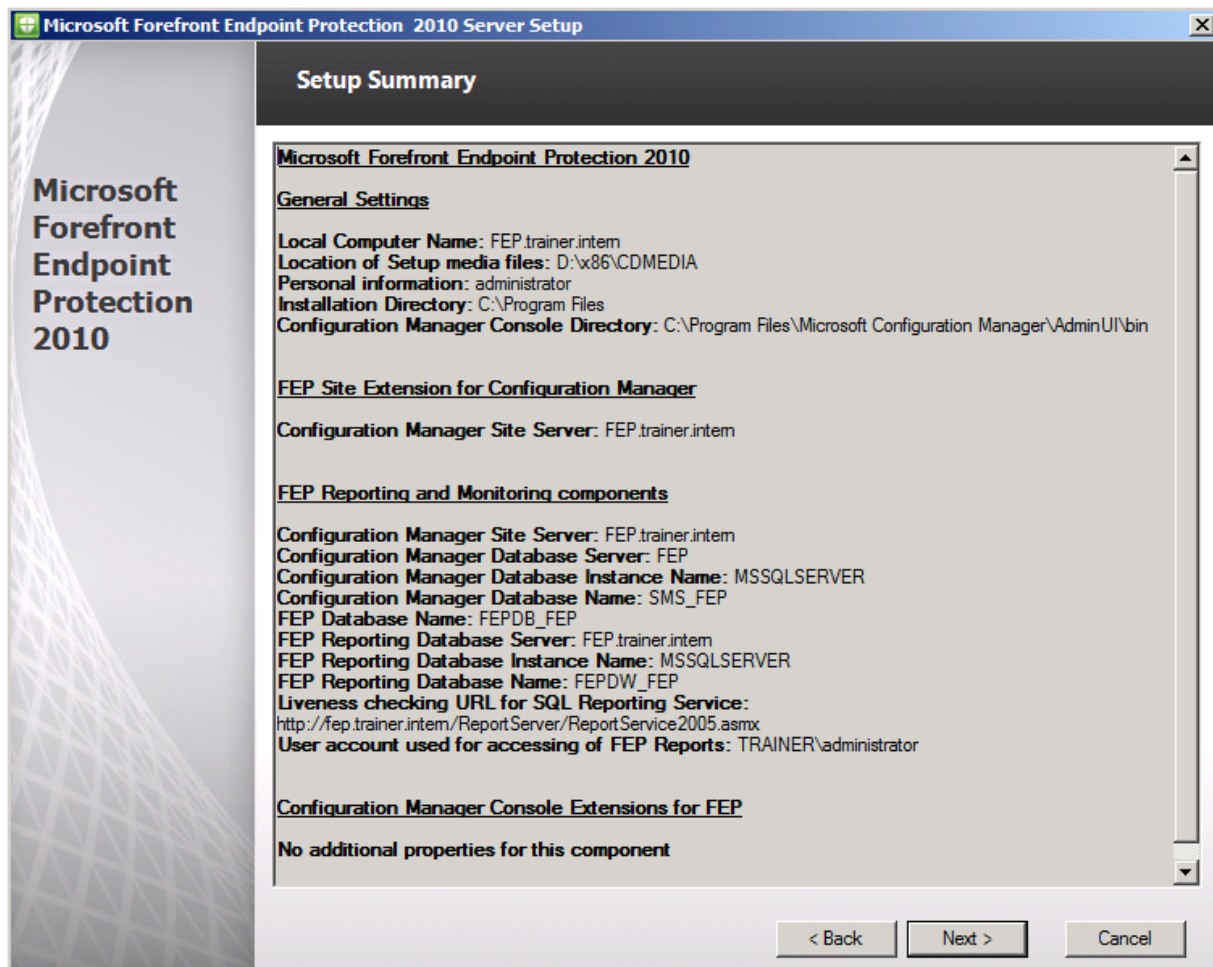
OK, SQL Server Agent muss auf Startart automatisch gestellt werden und gestartet sein, sowie ein ADWS ein Hotfix fehlt



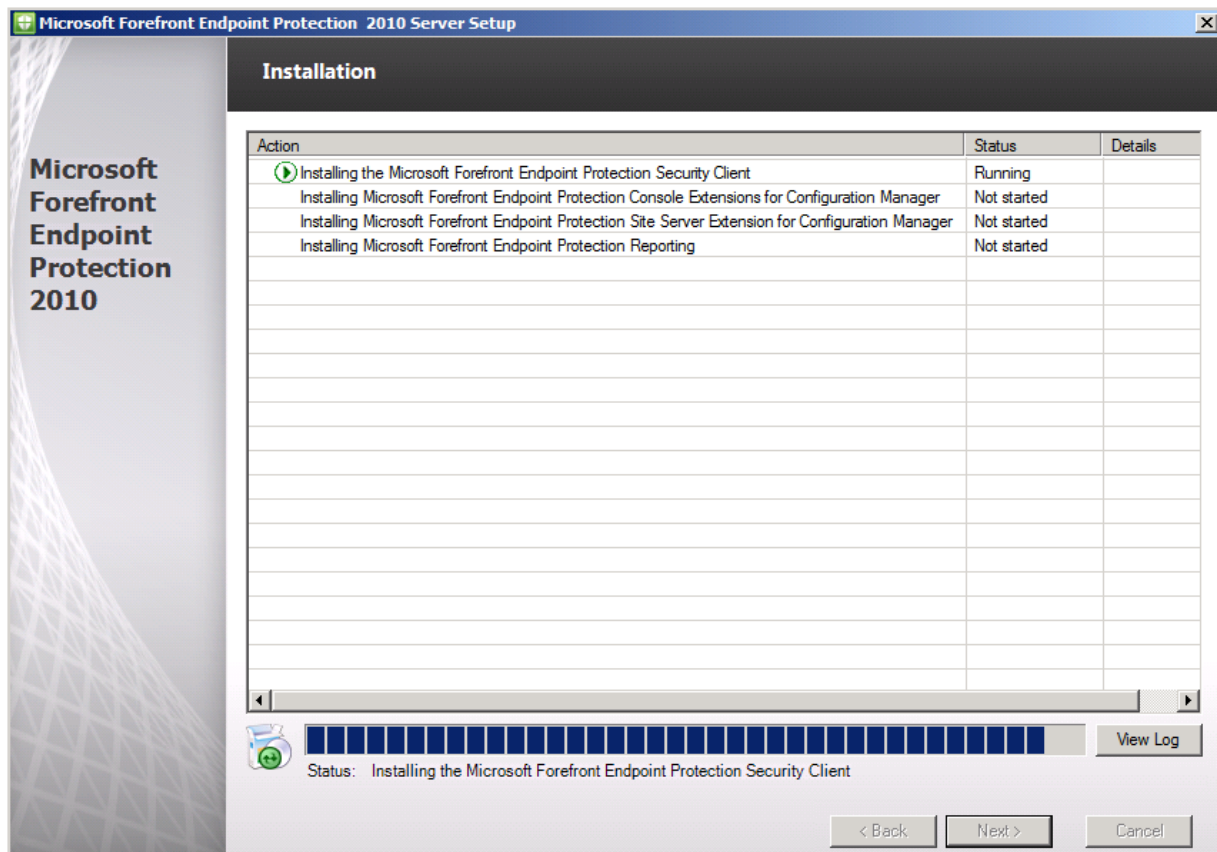
Schon besser



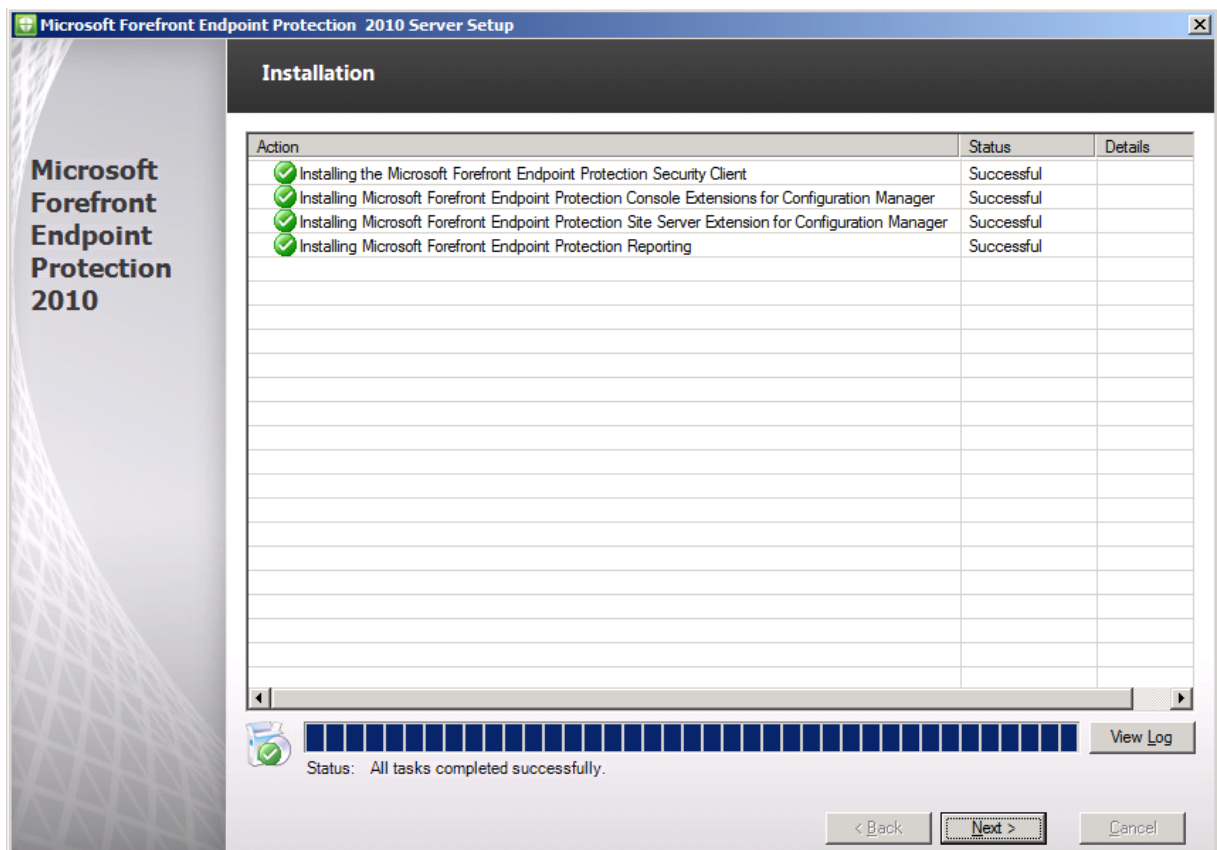
Zusammenfassung



Ab dafuer



Alles erfolgreich



FEP Konfiguration

SCCM Konfig

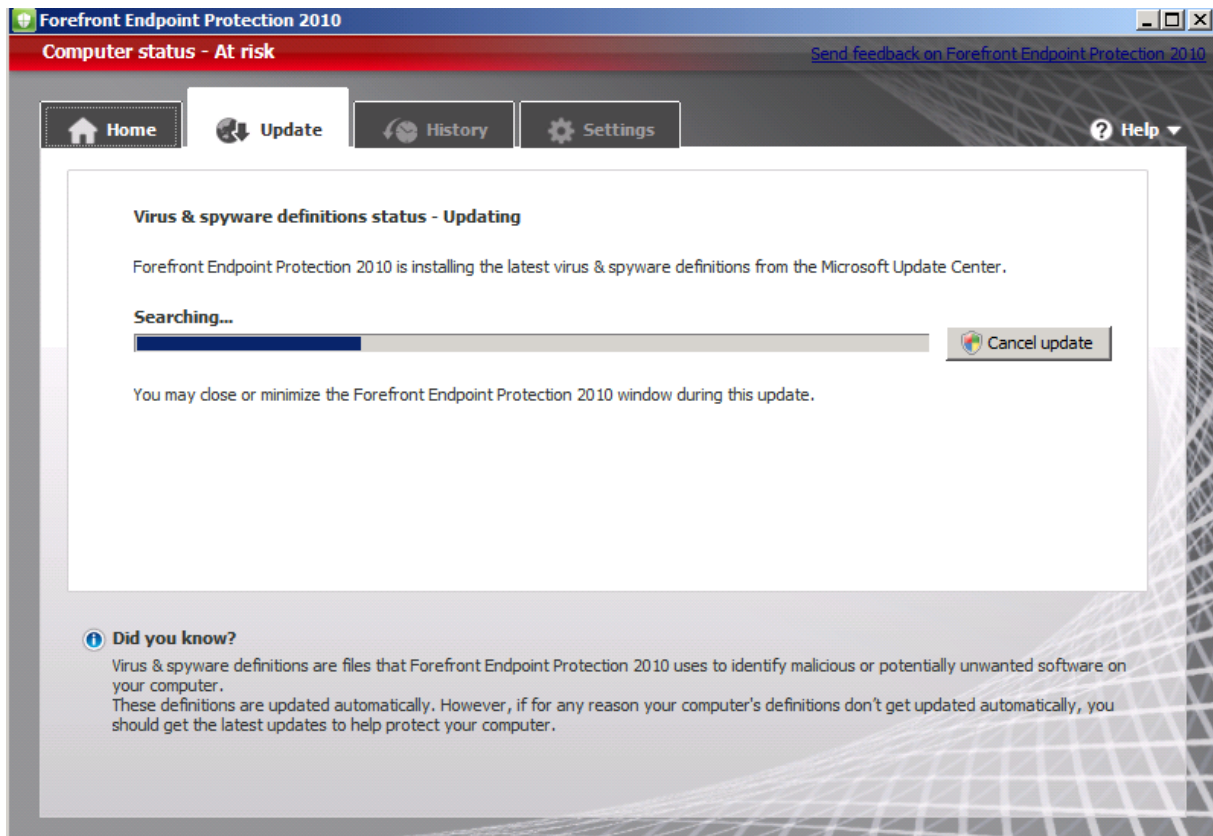
The screenshot displays the Configuration Manager Console with the Forefront Endpoint Protection (FEP) dashboard. The left-hand navigation pane shows the hierarchy: System Center Configuration Manager > Site Database (FEP - FEP, FEP-Site) > Computer Management > Forefront Endpoint Protection. The main pane shows the FEP dashboard with the following sections:

- Dashboard - Updated: 07.06.2010 14:17**
- Operational Statistics**
- Clients Deployment Status**
 - Not targeted by FEP: 1
 - Targeted by FEP: 0
- Antimalware Activity Status**
 - Active malware: 0
 - Reboot is required: 0
 - Full scan is required: 0
 - Malware cleaned (Last 24 hours): 0
- Definition Status**
 - Older than 1 week: 0
 - Up to 7 days old: 0
 - Up to 3 days old: 0
 - Up to date: 0
- Policy Distribution Status**
 - Policy failed to deploy: 0
 - Distribution in progress: 0
 - Policy deployed: 0
- Legend**
 - Failed to deploy cli... (Red square)
 - Deployment pending (Yellow square)
 - Client deployed (Green square)
- Forefront Endpoint Protection Baselines**

Baseline	Severity	Assigned	Non-Comp	Complia	Failed	Compliance Level
	None	0	0	0	0	0,00%
	None	0	0	0	0	0,00%
	None	0	0	0	0	0,00%
	None	0	0	0	0	0,00%

The right-hand pane shows the **Actions** menu for Forefront Endpoint Protection, including options like Update FEP collec..., Give Feedback, View, New Window from..., Refresh, and Help.

FEP Client Update



Reports

Antimalware Summary Report - Berichts-Viewer - Windows Internet Explorer

http://fep.trainer.intern/ReportServer/Pages/ReportViewer.aspx?/Forefront%20Endpoint%20Protection/Antimalware/Antimal

Antimalware Summary Report - Berichts-Viewer

Collection: Client deployed Report Time Span: Week Bericht anzeigen

Start Date (Custom Report Span Only): 31.05.2010 End Date (Custom Report Span Only): 07.06.2010

1 von 1 100% Suchen | Weiter

Microsoft Forefront Endpoint Protection

Antimalware Summary Report

Collection:	Report Time Span:	Generated On:
Client deployed	Week	6/7/2010 12:22:27 PM

Start Date:	End Date:	
5/31/2010 12:00 AM	6/7/2010 12:59 PM	All dates and times are UTC

Antimalware Deployment and Health

Current Antimalware Protection Coverage

Status

- Antimalware is not installed
- Antimalware Disabled
- Real-time Protection Disabled
- Real-time Protection Enabled

Antimalware Protection Breakdown - Week

Fehler: Der Unterbericht konnte nicht angezeigt werden.

Current Antimalware Signature Version

Antimalware Signature Breakdown - Week

Default FEP Policy

The screenshot displays the Configuration Manager Console interface. On the left is a navigation pane with a tree view containing categories like Site Database, Computer Management, Software Updates, and Policies. The 'Policies' category is selected. The main pane is titled 'Policies 1 items found' and contains a table with one entry: 'Default FEP Policy'. Below this table are tabs for 'General', 'Antimalware', 'Updates', and 'Host Firewall'. The 'Updates' tab is active, showing settings for 'Scheduled Scans'. On the right side of the console is an 'Actions' pane with options like 'New Policy', 'Policy Precedence...', and 'Give Feedback'. Below these are specific actions for the 'Default FEP Policy', such as 'Duplicate Policy', 'Refresh', 'Properties', and 'Help'. A 'Description' section at the bottom right explains that this is a system read-only policy for desktop computers.

Configuration Manager Console

File Action View Window Help

System Center Configuration Manager

- Site Database (FEP - FEP, FEP-Site)
- Site Management
- Computer Management
- Collections
- Conflicting Records
- Software Distribution
- Software Updates
- Operating System Deployment
- Asset Intelligence
- Software Metering
- Reporting
- Desired Configuration Management
- Queries
- Mobile Device Management
- Network Access Protection
- Forefront Endpoint Protection
- Policies
- Alerts
- Reports
- System Status
- Security Rights
- Tools

Policies 1 items found

Look for: [] in All Columns Find Now Clear

Name	Description	Precedence
Default FEP Policy	System read-only policy that contains the recommended ...	1 (Lowest)

Actions

Policies

- New Policy
- Policy Precedence...
- Give Feedback
- View
- New Window from...
- Refresh
- Help

Default FEP Policy

- Duplicate Policy
- Refresh
- Properties
- Help

Description

System read-only policy that contains the recommended settings for most desktop computers and associated with the FEP Deployed Clients Collection.

Updates

Scheduled Scans

- Real-time Protection
- Threat Handling
- Exclude Files and Locations
- Exclude File Types
- Excluded processes
- Overrides
- Advanced Settings

☒ Run a scheduled scan

Select the frequency of scheduled scans.

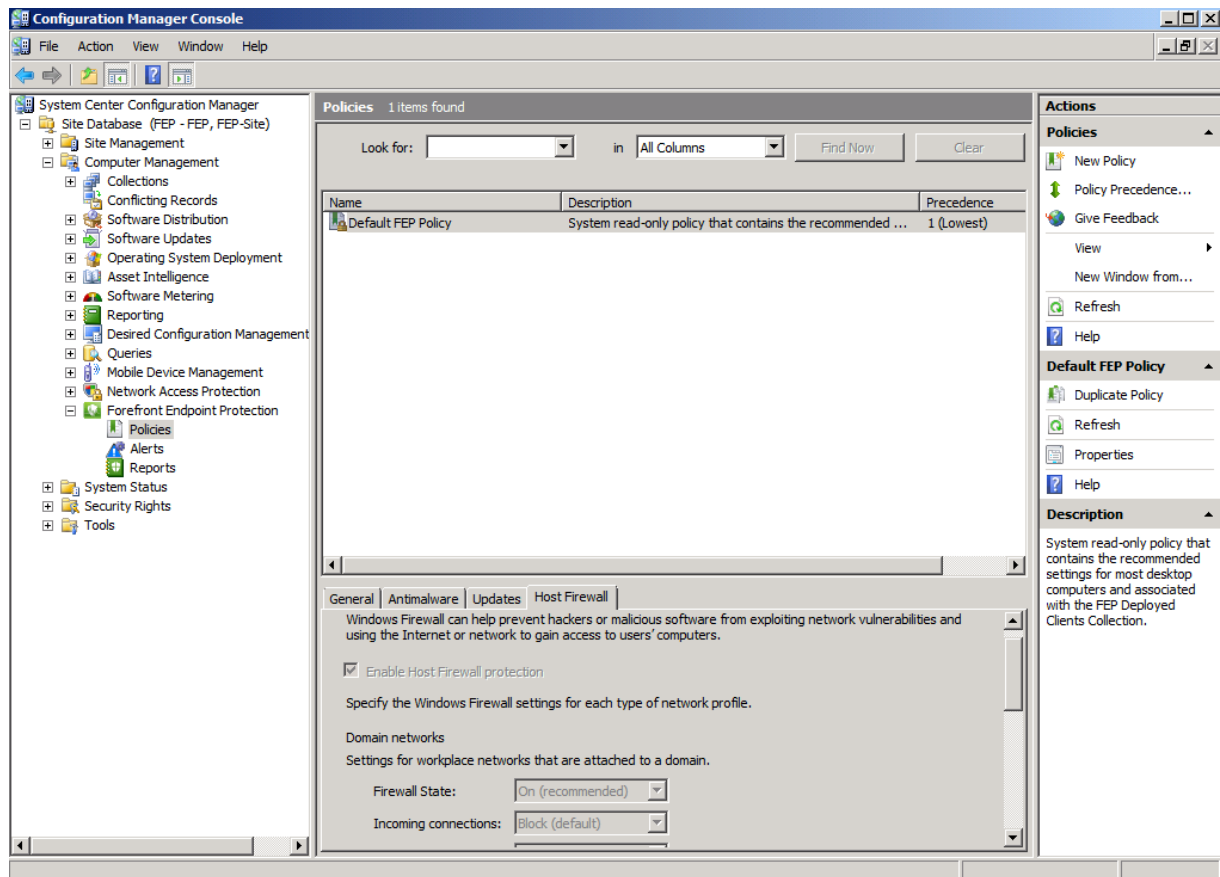
Scan frequency: Weekly quick scan

Daily scan at: 01:00

Weekly scan every:

Day: Sunday

Hour: 22:00



Neue FEP Policy

New Policy Wizard



Policy Type

General

Policy Type

Scheduled scan

Scan Exclusions

Updates

Client Computer Options

Summary

Progress

Confirmation

Select the policy type that is most appropriate.

- ☒ Standard desktop policy
Use for most enterprise desktop environments. This policy includes antimalware and Windows Firewall.
- ☐ High-security policy
Use for computers that require maximum protection. This policy includes antimalware and Windows Firewall.
- ☐ Performance-optimized policy
Use when performance is a concern and computers require minimal security protection.

< Previous

Next >

Finish

Cancel

New Policy Wizard



Scheduled scan

General

Policy Type

Scheduled scan

Scan Exclusions

Updates

Client Computer Options

Summary

Progress

Confirmation

Select the frequency of scheduled scans.

Scan frequency: Weekly quick scan

Daily scan at: 01:00

Weekly scan every:

Day: Sunday

Hour: 22:00

Quick scan checks only the areas that malicious software is most likely to infect. Full scan checks all the files and all running programs. Full scan can take more than an hour.

< Previous

Next >

Finish

Cancel

New Policy Wizard



Scan Exclusions

General

Policy Type

Scheduled scan

Scan Exclusions

Updates

Client Computer Options

Summary

Progress

Confirmation

You can exclude certain files or folders from scans. Exclusions can help speed up the scan, but may leave computers at higher risk.

Do not scan the specified files and folders:

Add

Name

c:\temp

Remove


< Previous

Next >

Finish

Cancel

New Policy Wizard

 Updates

General
Policy Type
Scheduled scan
Scan Exclusions
Updates
Client Computer Options
Summary
Progress
Confirmation

Select the locations where client computers can get updates.

☒ Enable updates from Configuration Manager

☒ Enable updates from Microsoft Update (MU)

☐ Get signature updates from the following file share location:


< Previous

Next >

Finish

Cancel

New Policy Wizard

 Client Computer Options

General
Policy Type
Scheduled scan
Scan Exclusions
Updates
Client Computer Options
Summary
Progress
Confirmation

Configure what options are available to end users.

Allow end users to change configuration of:
☐ Real-time protection
☐ Scheduled scan time

☐ Show client notifications on detected malware

< Previous

Next >

Finish

Cancel

New Policy Wizard



Summary

General

Policy Type

Scheduled scan

Scan Exclusions

Updates

Client Computer Options

Summary

Progress

Confirmation

Review the settings for this new Forefront Endpoint Protection policy.

Details:

General policy information:

- Name: FEP-test

Antimalware policy settings:

- Real-time protection: incoming and outgoing files
- Scheduled scan: quick scan every Sunday at 22:00
- CPU limit: 50% load
- Excluded paths: c:\temp

Windows Firewall

- On

Update antimalware definitions from the following sources:

- Configuration Manager
- Microsoft Update

End user configuration:

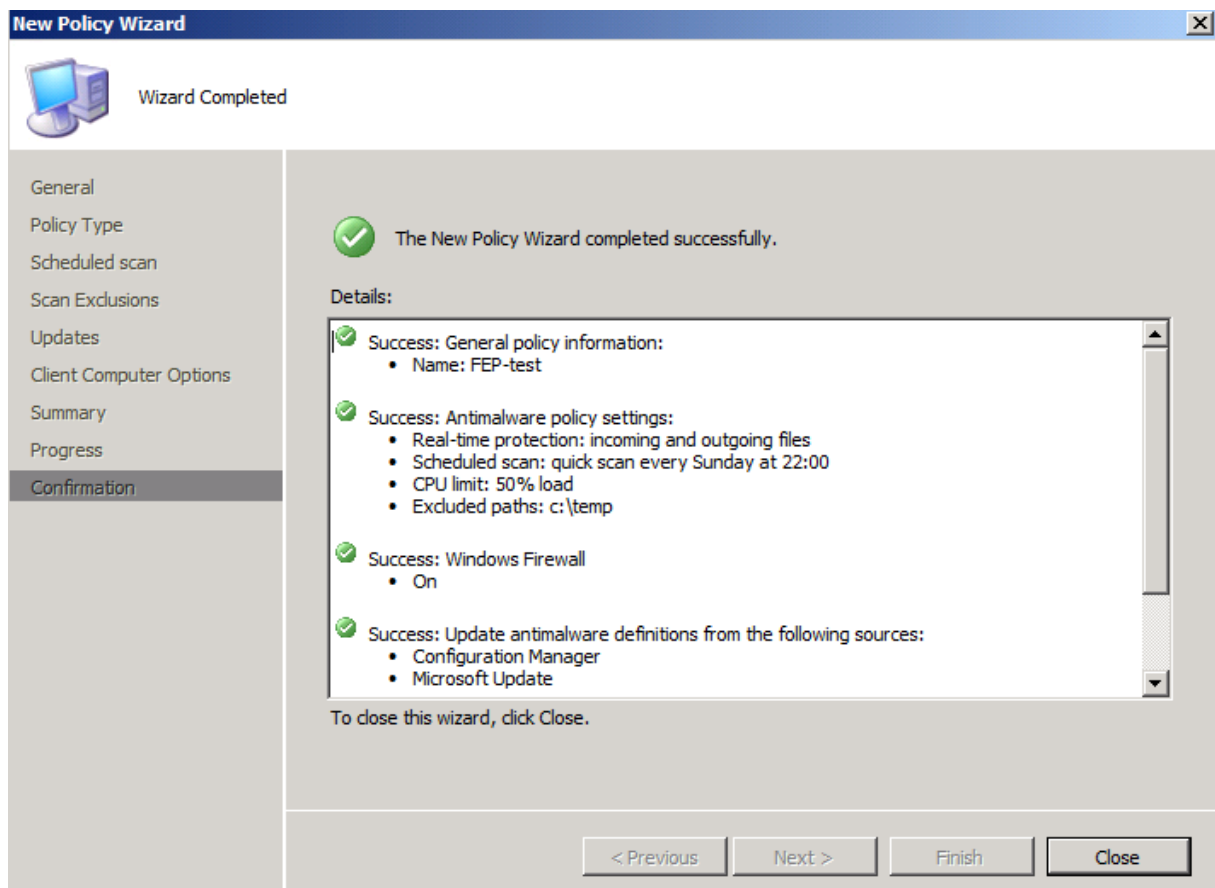
To change these settings, click Previous. To apply the settings, click Next.

< Previous

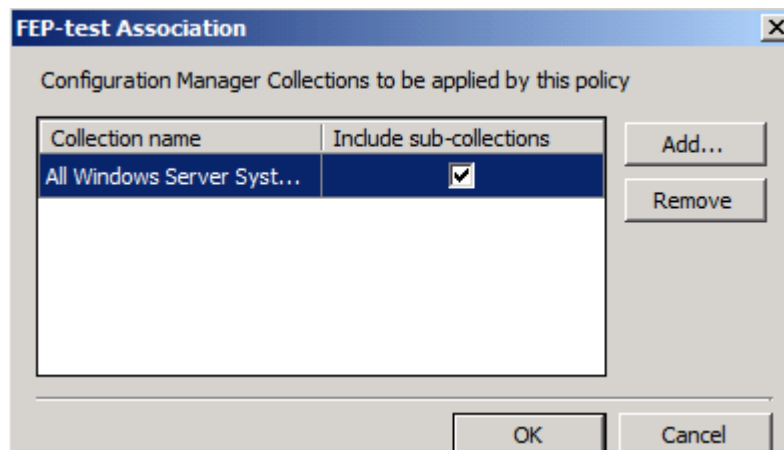
Next >

Finish

Cancel



Policy assignen



FEP-test Properties [X]

General | **Antimalware** | Updates | Host Firewall

Configure protection from viruses and spyware.

☒ Enable antimalware protection

Scheduled Scans
Real-time Protection
Threat Handling
Exclude Files and Locations
Exclude File Types
Excluded processes
Overrides
Advanced Settings

☒ Run a scheduled scan
Select the frequency of scheduled scans.
Scan frequency: Weekly quick scan
Daily scan at: 01:00
Weekly scan every:
Day: Sunday
Hour: 22:00
☐ Allow users to change scan time
☒ Scan only when computer is idle
☒ Randomize scheduled scan start times (within 30 minutes from scheduled time)
☐ Force a scan after a second missed scan upon reboot
☒ Scan archived files
☒ Limit CPU usage during scan to the following percentage: 50%
☐ Allow users to enable, disable and configure processor usage

OK Cancel Apply

FEP-test Properties

GeneralAntimalwareUpdatesHost Firewall

Configure protection from viruses and spyware.

☒ Enable antimalware protection

Scheduled ScansReal-time ProtectionThreat HandlingExclde Files and LocationsExclde File TypesExcluded processesOverridesAdvanced Settings

Configure advanced options.

☐ Scan network drives when running a full scan☐ Scan removable storage devices such as USB flash drives☐ Create a system restore point before cleaning computers☒ Use behavior monitoring☐ Delete quarantined files after: 14 days

Quarantining a potential threat disables it and leaves it in this state until the user decides what to do with it. Use this option to specify after how many days to delete quarantined files from users' computers.

OKCancelApply

FEP-test Properties [X]

General | Antimalware | **Updates** | Host Firewall

You can configure where, when, and how Forefront Endpoint Protection checks for the latest virus and spyware definitions.

Update definitions:

☒ Every 3 hours [v]
☐ Daily at 00:00 [v]

☒ Check for definition updates before starting a scan
☒ Force a definition update after updates have failed for: 1 day [v]

Customize the source for getting the latest virus and spyware definition updates for user's computers:

☒ Enable updates from Configuration Manager
☒ Enable updates from Microsoft Updates (MU)
☐ Enable updates from the following file shares

Specify, in order of preference, file shares:

Name
There are no items to show in this view.

OK Cancel Apply

FEP-test Properties [X]

General | Antimalware | Updates | **Host Firewall**

Windows Firewall can help prevent hackers or malicious software from exploiting network vulnerabilities and using the Internet or network to gain access to users' computers.

☒ Enable Host Firewall protection

Specify the Windows Firewall settings for each type of network profile.

Domain networks
Settings for workplace networks that are attached to a domain.

Firewall State: On (recommended) ▼

Incoming connections: Block (default) ▼

Display a notification: Yes ▼

Private networks
Settings for networks at home or work where the user knows and trusts the people and devices on the network (this is the "Standard" profile for Windows XP computers)

Firewall State: On (recommended) ▼

Incoming connections: Block (default) ▼

Display a notification: Yes ▼

Public networks
Settings for networks in public places such as airports or coffee shops. This profile applies only to Windows Vista and Windows 7 computers and will be ignored on Windows XP computers.

Firewall State: On (recommended) ▼

Incoming connections: Block (default) ▼

Display a notification: Yes ▼

OK Cancel Apply

Display a notification: Yes ▼

e-mail settings

E-Mail Settings

☒ Send e-mail notification

SMTP Server: Port:

Choose the authentication method used when validating your e-mail account:

☒ Anonymous

☐ Service credentials

E-mail from address:

Malware detection Properties

Alerts properties

Malware Detection

Forefront Endpoint Protection can send an alert when malware is detected on a computer that is a member of a specified collection. For example, you can configure FEP to alert you when malware is detected on sensitive computers.

☒ Enable malware detection alerts

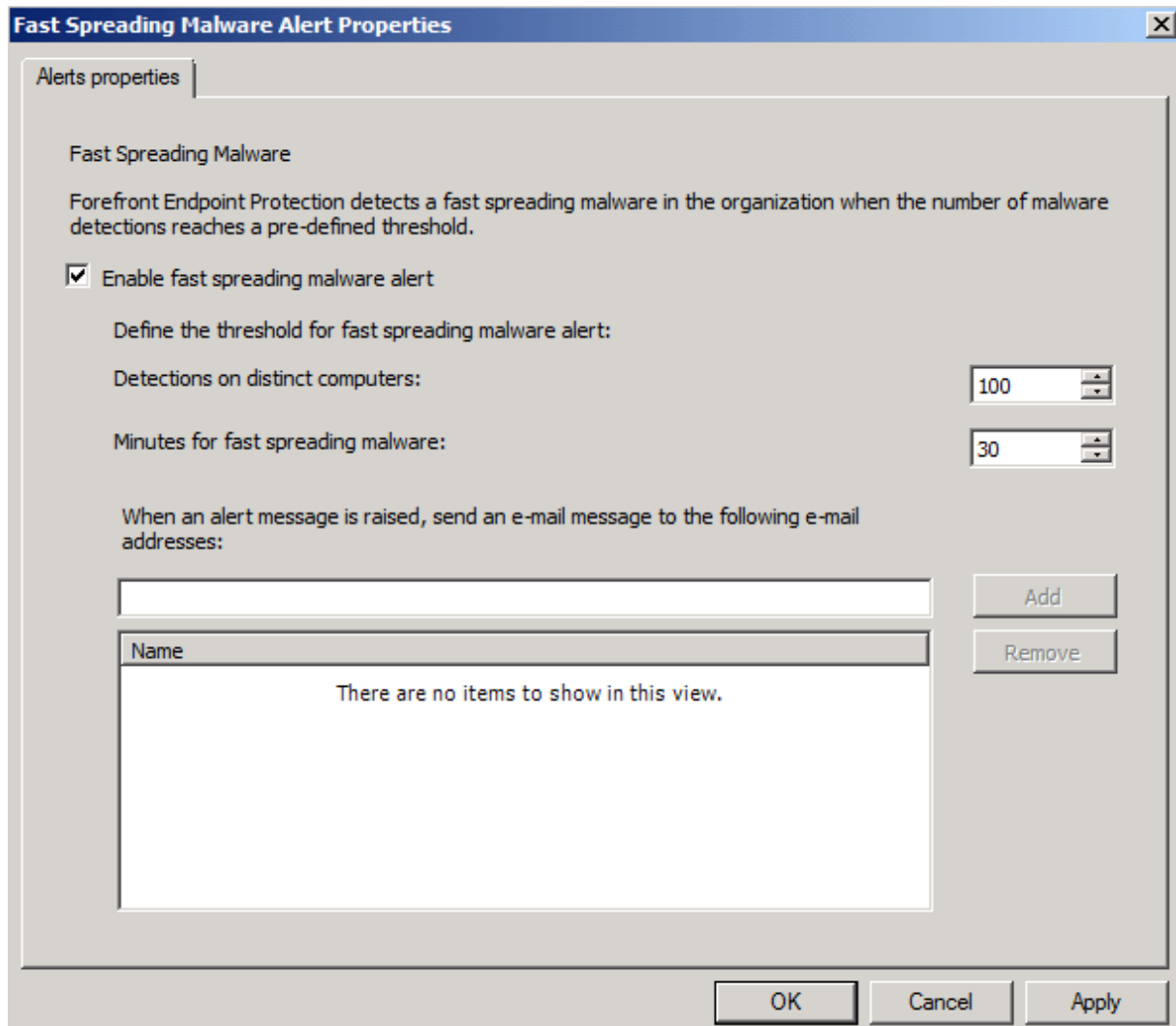
Select a parent collection to monitor for malware detections:

Select the detection level to monitor:

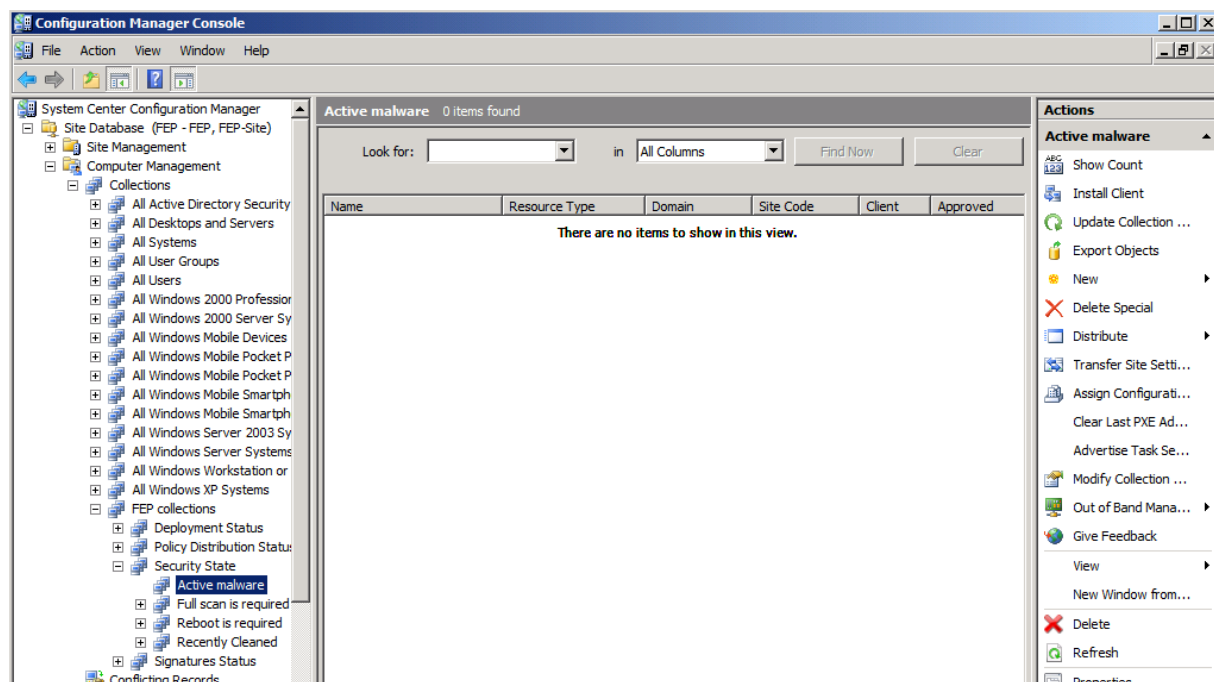
☐ **Low: Failed to clean**
Malware is detected and cleaning fails

When an alert message is raised, send an e-mail message to the following e-mail addresses:

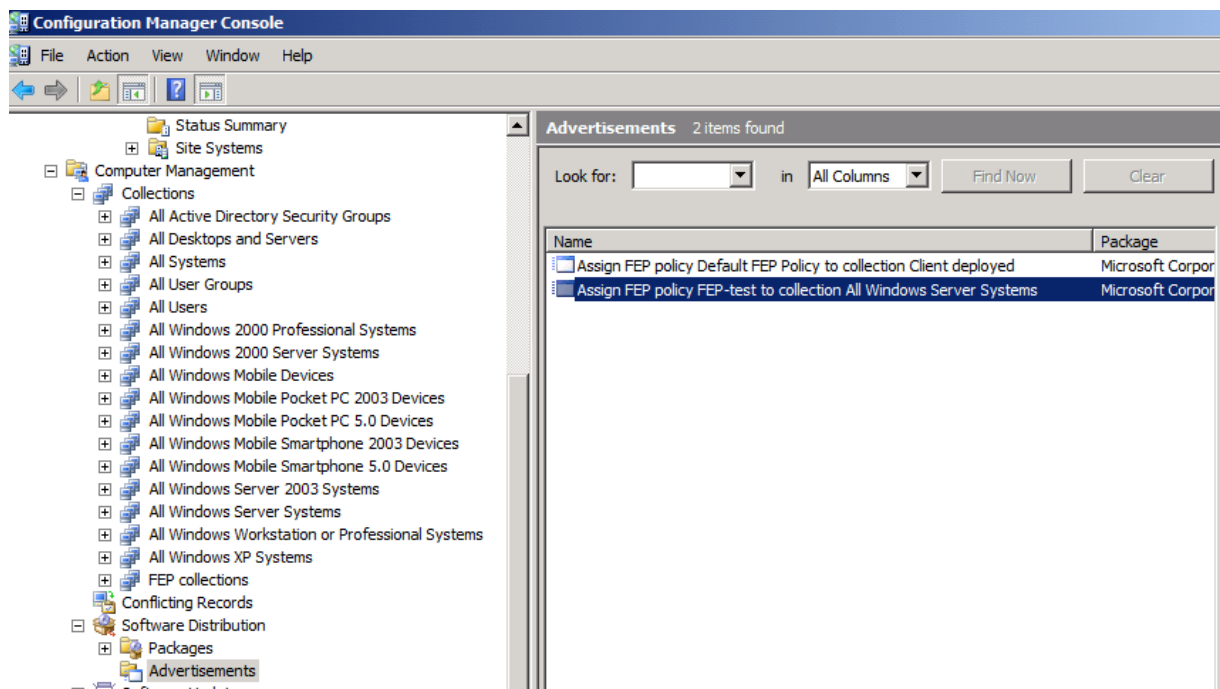
Name
There are no items to show in this view.



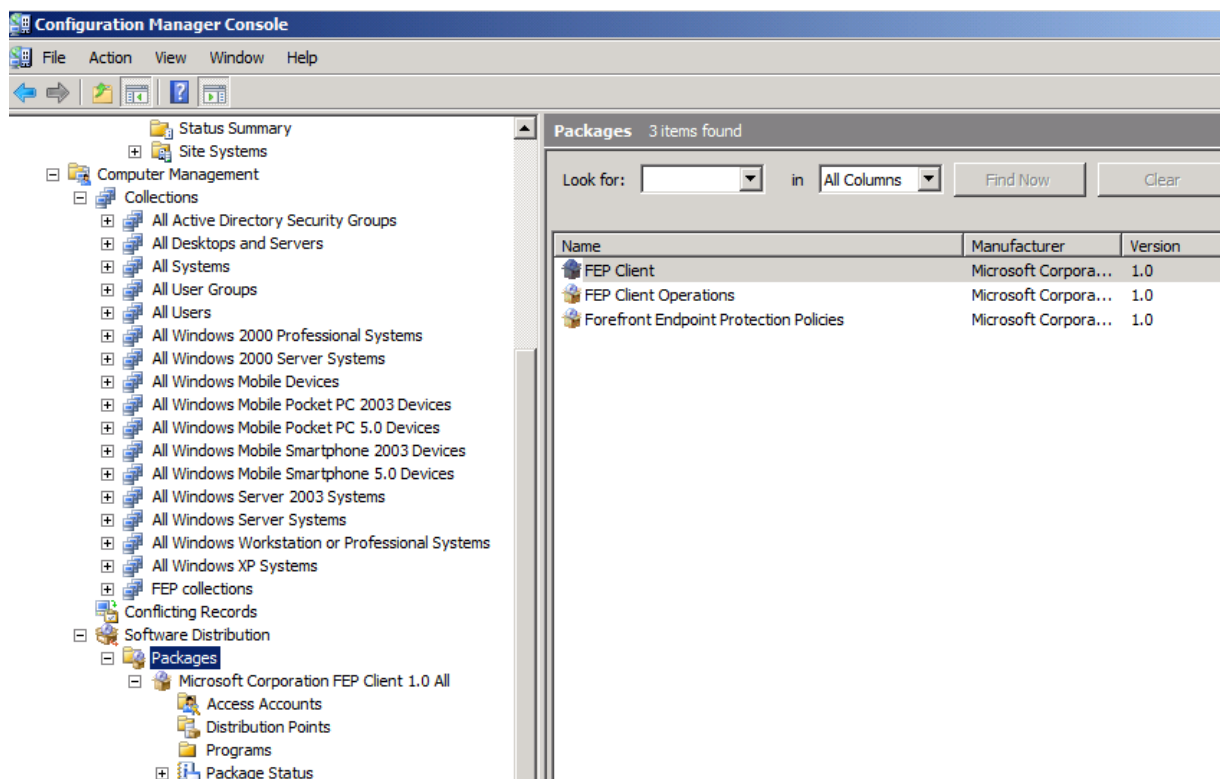
FEP collections



FEP Policy advertisement



FEP Packages



Install Properties

Windows Installer

MOM Maintenance Mode

General

Requirements

Environment

Advanced

Name:

Install

Your use of software deployed by ConfigMgr may be subject to license terms. You should review any applicable license terms prior to deploying software.

Comment:

Install Microsoft Forefront Endpoint Protection 2010 with competitor's product removal, SQM Off, and SpyNet advanced registration

Command line:

vbs "%FEPIInstall.exe /s /q /

Browse...

Start in:

Run:

Hidden

After running:

No action required

Category:

OK

Cancel

Apply

Help