

Microsoft Forefront "Stirling" - Forefront Stirling - Ueberblick und Konfiguration

In diesem Artikel zeige ich kurz den Funktionsumfang von Forefront Stirling.

Erster Artikel Forefront Stirling im Ueberblick:

<http://www.it-training-grote.de/download/stirling-b2-1.pdf>

Artikel zu Forefront Security fuer Exchange

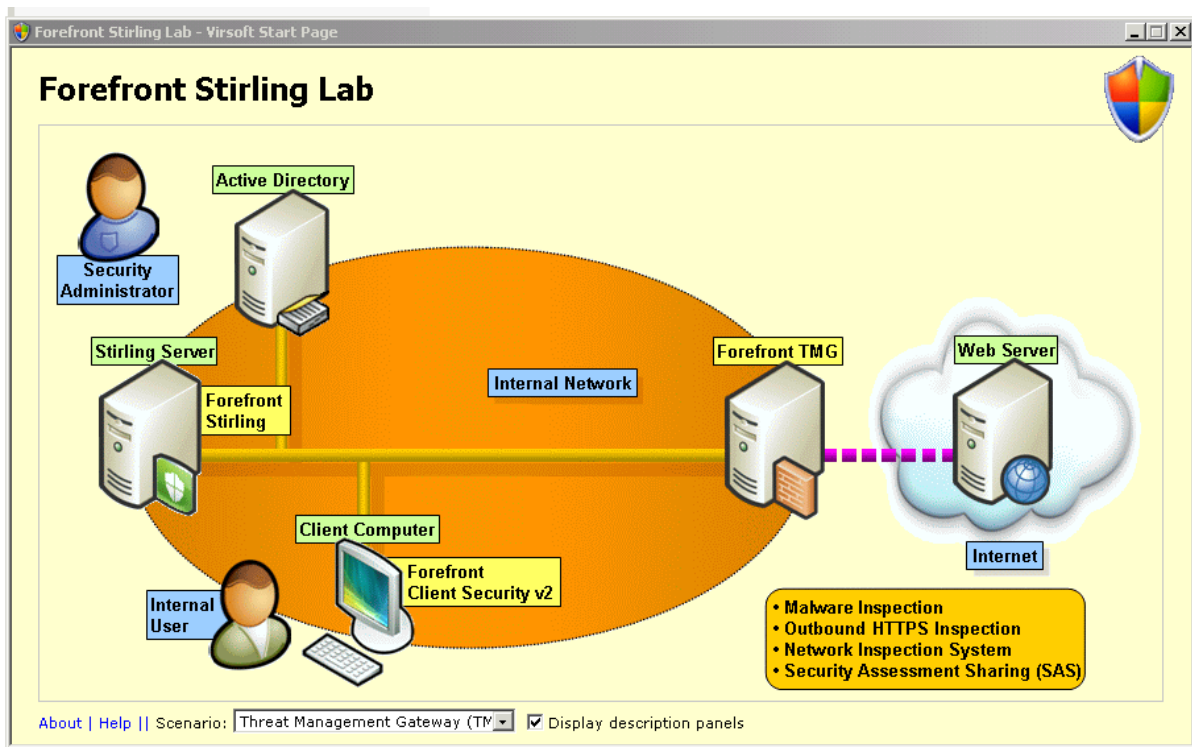
<http://www.it-training-grote.de/download/stirling-b2-2.pdf>

Artikel zu Forefront Client Security

<http://www.it-training-grote.de/download/stirling-b2-3.pdf>

Ich nutze wieder die herunterladbare VHD-Testumgebung von Microsoft.

Alles im Ueberblick



Was enthalten die Downloads

- . Denver
 - Domain Controller
 - Roles: DHCP server, DNS server, NPS server
 - WSUS 3.0 SP1
- . Stirling
 - System Center Operations Manager (SCOM) 2007 R2 (build 6407 - beta 1)
 - SQL Server 2005 SP3
 - Forefront Stirling (build 1677 - beta 2)
 - Outlook 2007
- . Venice
 - Forefront Client Security (build 1677 - beta 2)
 - NAP agent

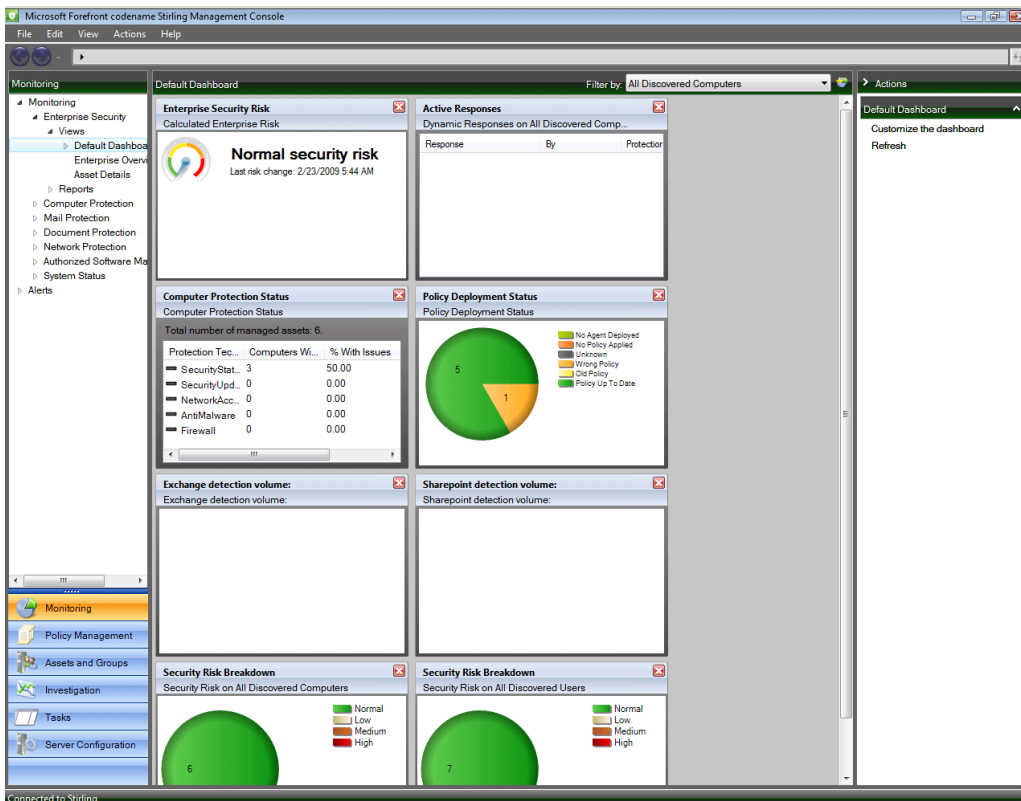
- Outlook 2007
- . Madrid
 - Exchange Server 2007 SP1 (Mailbox/Client Access/Hub Transport roles)
 - Forefront for Exchange (build 243 - beta 2)
- . Sydney
 - Windows SharePoint Services (WSS) 3.0 SP1
 - Forefront for SharePoint (build 243 - beta 2)
- . Toronto
 - Exchange Server 2007 SP1 (Edge Transport role)
 - Threat Management Gateway (build 7264 - beta 2)

Stirling Konsole

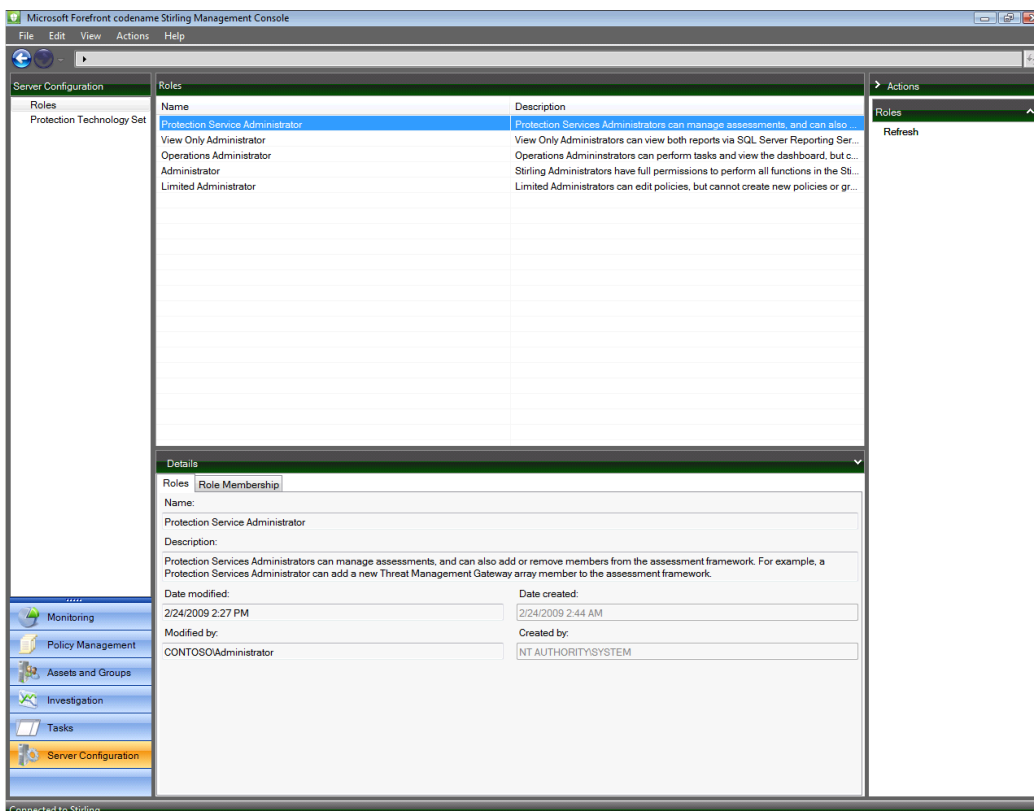
Beim Starten von Stirling verbindet sich die Konsole mit dem Remote MS SQL Server 2005.



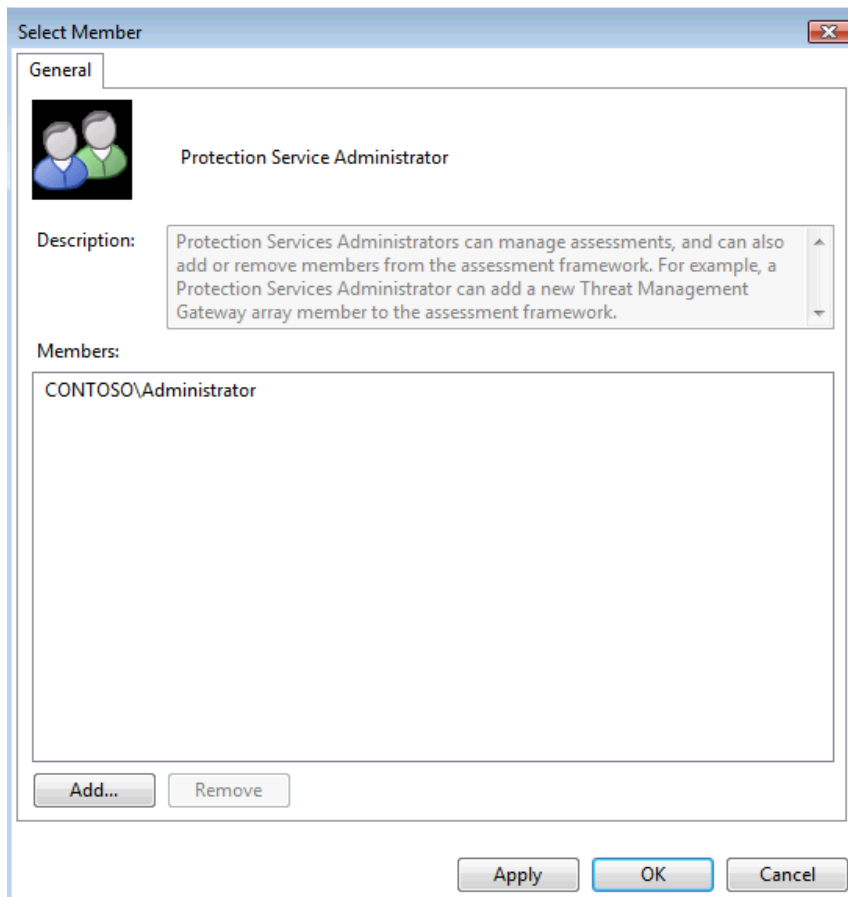
In der Stirling Konsole erhaelt man einen Ueberblick ueber die wichtigsten Komponenten und den moeglichen Konfigurationsparametern.



In der Server Konfiguration koennen die einzelnen Stirling Rollen eingerichtet und entsprechenden Benutzern und Gruppen zugeordnet werden.



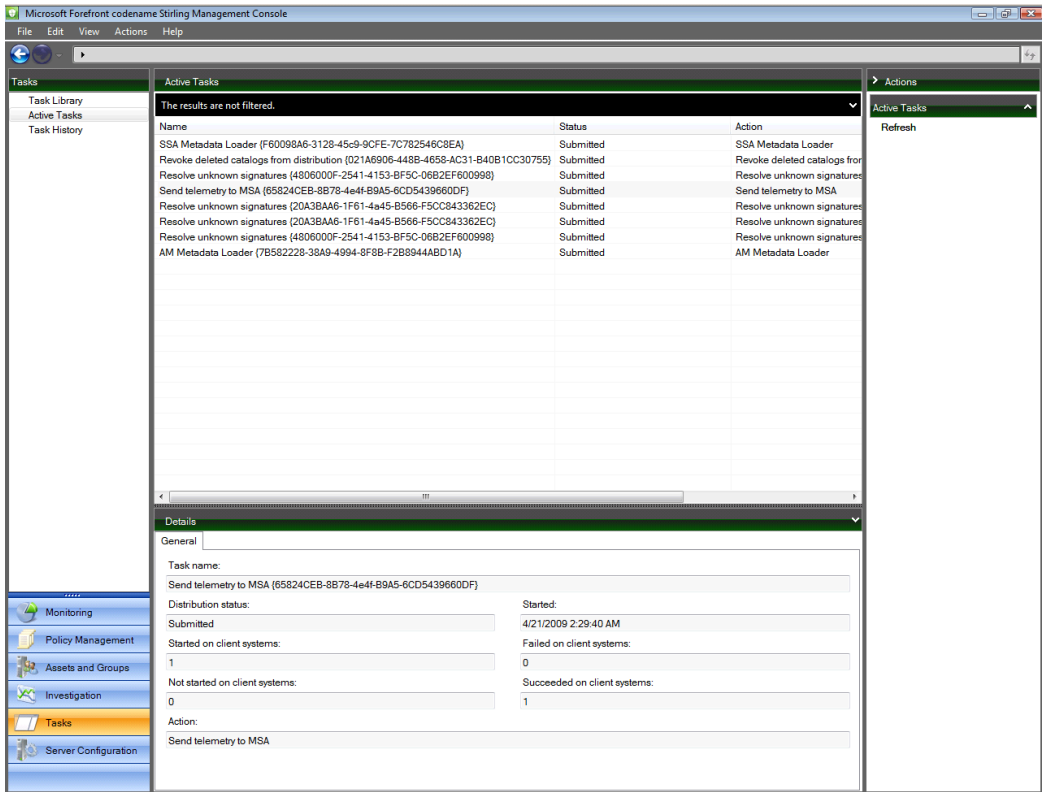
Neue Benutzer und Gruppen koennen hinzugefuegt werden.



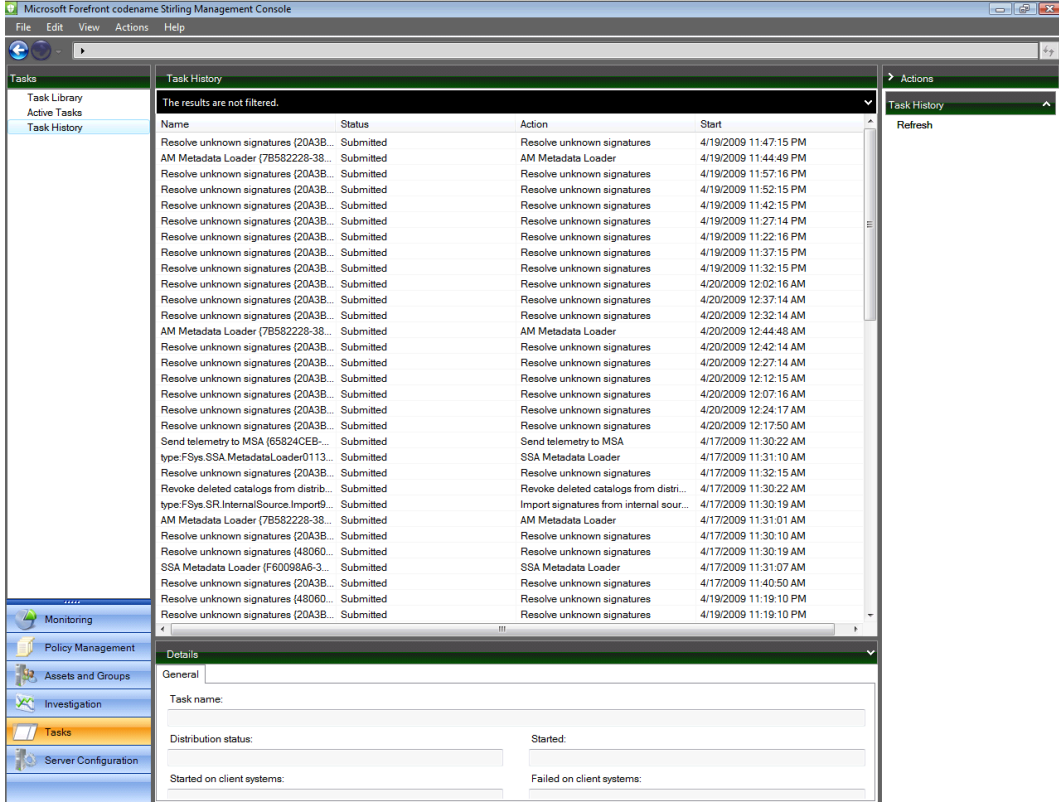
Forefront Stirling bietet eine Reihe von Schutztechnologien fuer einzelne Produkte oder Funktionen von Microsoft.

| Microsoft Forefront codename Stirling Management Console | | | | |
|--|--------------------------------|-----------------------------|----------------------|-----------------------|
| File Edit View Actions Help | | | | |
| Server Configuration | | | | |
| Roles | Protection Technology Set | | | |
| Protection Technology Set | Name | Type | Modified On | Owner |
| | Stirling SharePoint Protection | SharePoint Protection | 2/23/2009 1:44:27 PM | |
| | Stirling NAP Protection | Network Access Protection | 2/23/2009 1:44:27 PM | |
| | Stirling TMG Protection | Threat Management Gateway | 2/24/2009 2:27:08 PM | CONTOSO\Administrator |
| | Stirling Mail Protection | Mail Protection | 2/23/2009 1:44:27 PM | |
| | Stirling Core Protection | Stirling Core | 2/23/2009 1:44:27 PM | |
| | Stirling Client Protection | Client Protection | 2/23/2009 1:44:27 PM | |
| | Stirling AD Protection | Active Directory Protection | 2/24/2009 4:05:08 PM | |

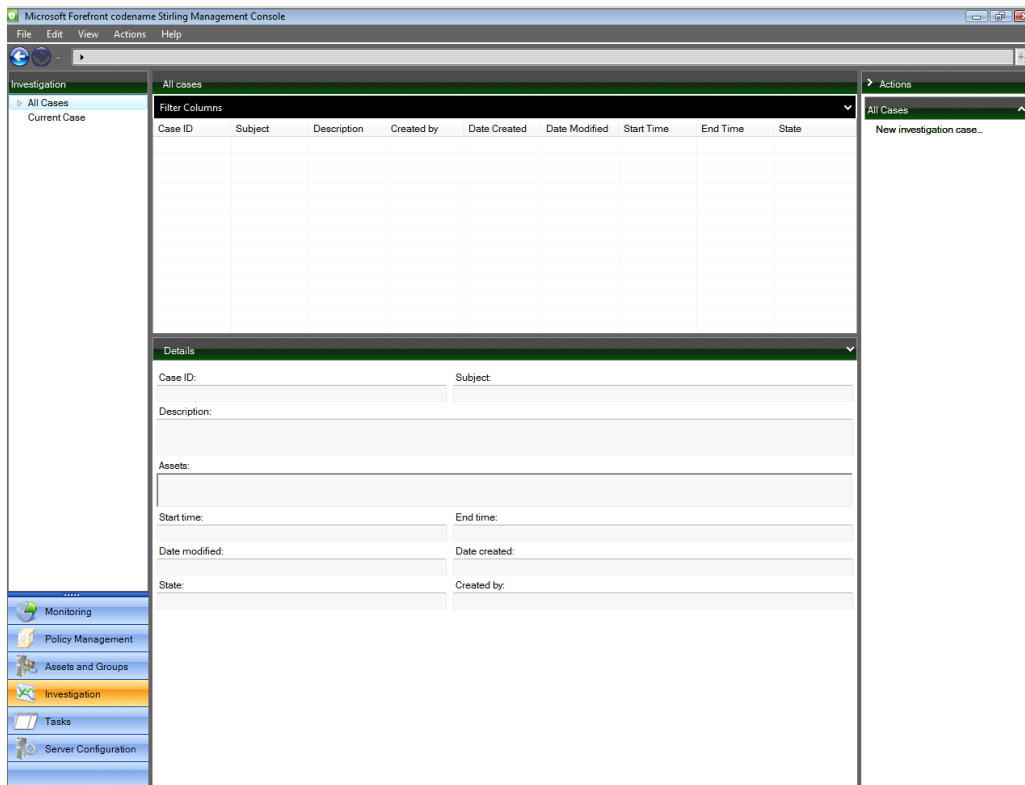
Verschiedene Tasks koennen mit Stirling eingerichtet werden



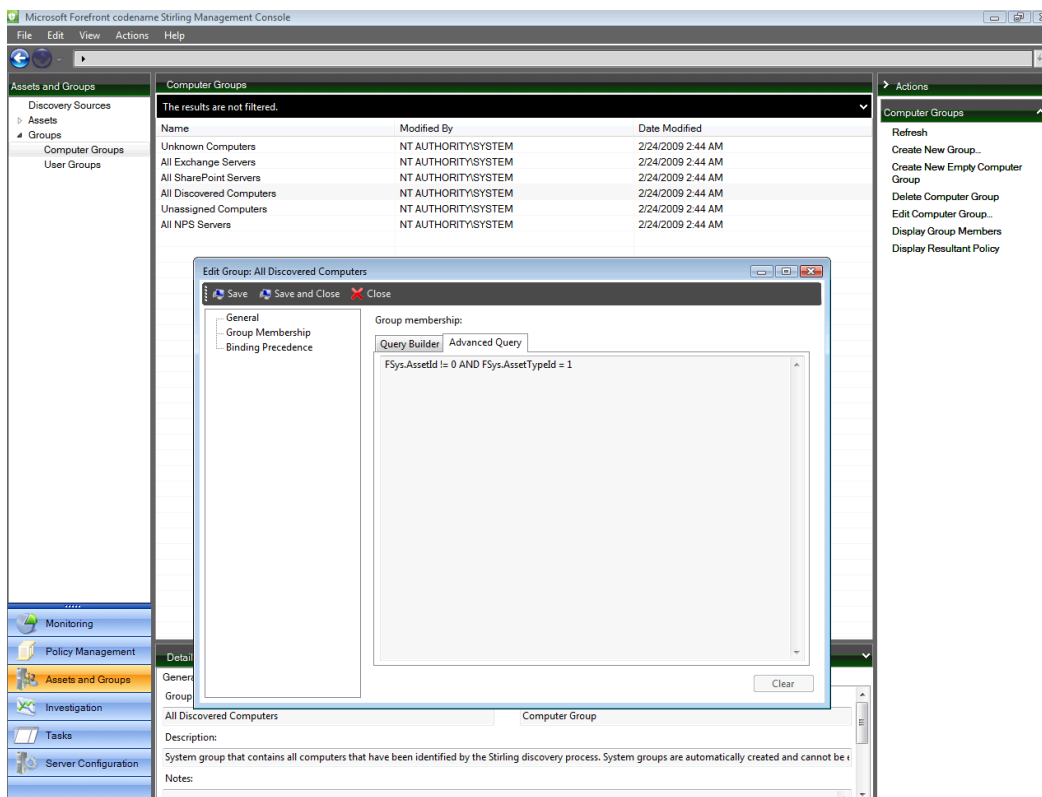
Uebersicht ueber die Stirling Tasks



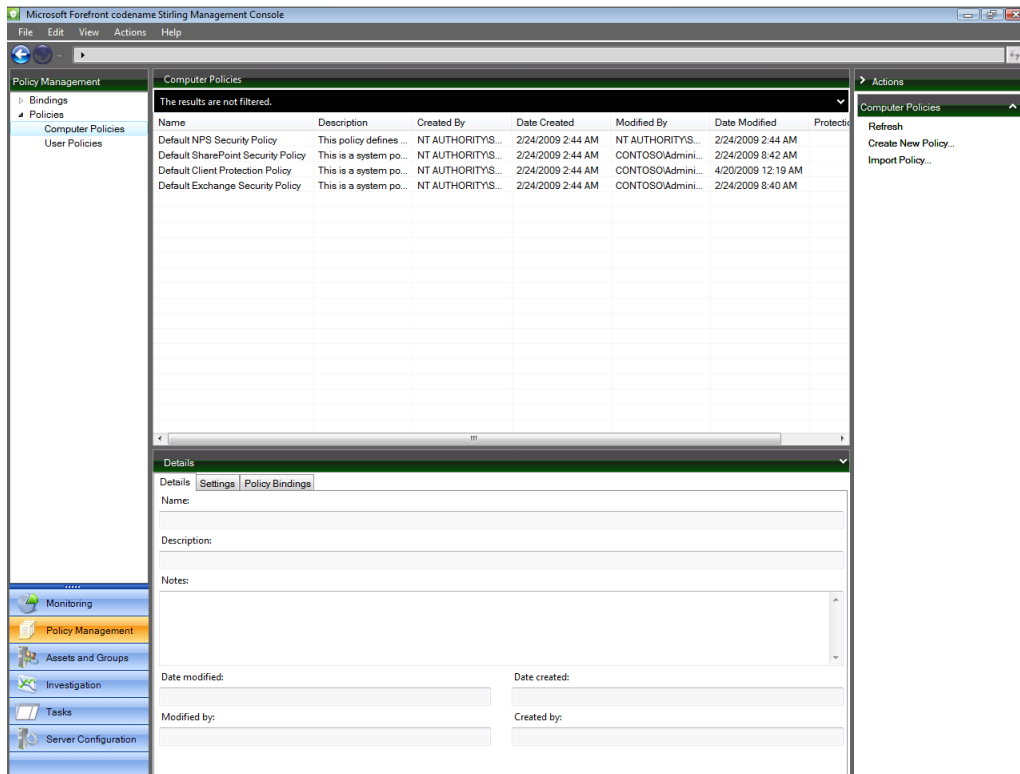
Stirling bietet eine Konsole zum Ueberblick ueber aktuelle Sicherheitsprobleme, welche von Stirling gefunden wurden.



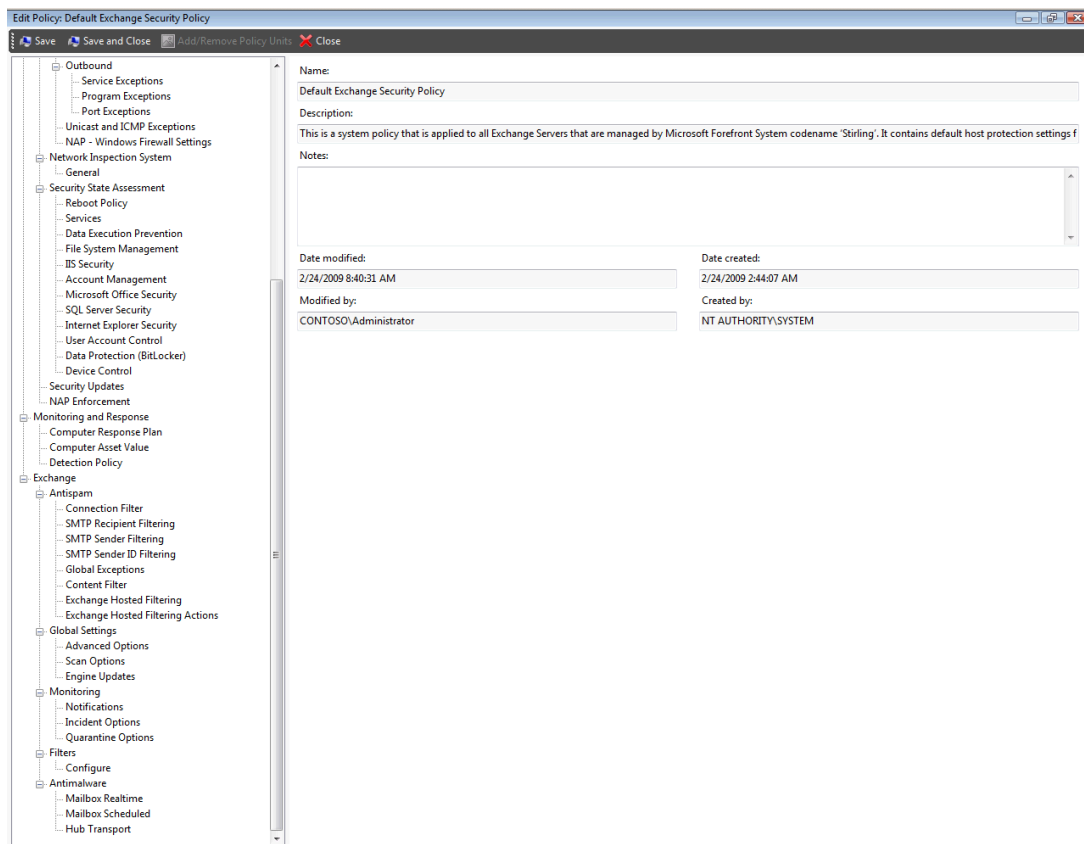
Bestimmte Windows Versionen, Server Rollen und Funktionen koennen zu Gruppen, sogenannten Computer und Benutzer Gruppen zusammengefasst werden.



Es gibt eine Reihe von vordefinierten Policies, welche angepasst werden koennen. es koennen aber auch neue Richtlinien erstellt werden.



Die Liste der konfigurierbaren Richtlinien in Stirling ist lang.



Stirling bietet auch ein umfassendes Alerting System, mit welchem Administratoren sich ueber verschiedene Zustaeude informieren lassen koennen.

Microsoft Forefront codename Stirling Management Console

File Edit View Actions Help

Monitoring

- Monitoring
 - Enterprise Security
 - Views
 - Default Dashboard
 - Enterprise Overview
 - Asset Details
 - Reports
 - Computer Protection
 - Mail Protection
 - Document Protection
 - Network Protection
 - Authorized Software Management
 - System Status
 - Alerts
 - Active Alerts
 - Security Alerts
 - Health Alerts
 - Operational Alerts
 - Notification Rules
 - Configure System Alerts

Configure System Alerts

| Alert Name | Alert Status |
|---|--------------|
| Stirling Agent managed machine is connecting to more than one Stirling... | Enabled |
| System Center Operations Manager 2007 agent queue is full | Enabled |
| System Center Operations Manager connection failed | Enabled |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Actions

Configure System Alerts

Refresh

Details

General

Name:

Status:

Description:

- Monitoring
- Policy Management
- Assets and Groups
- Investigation
- Tasks
- Server Configuration