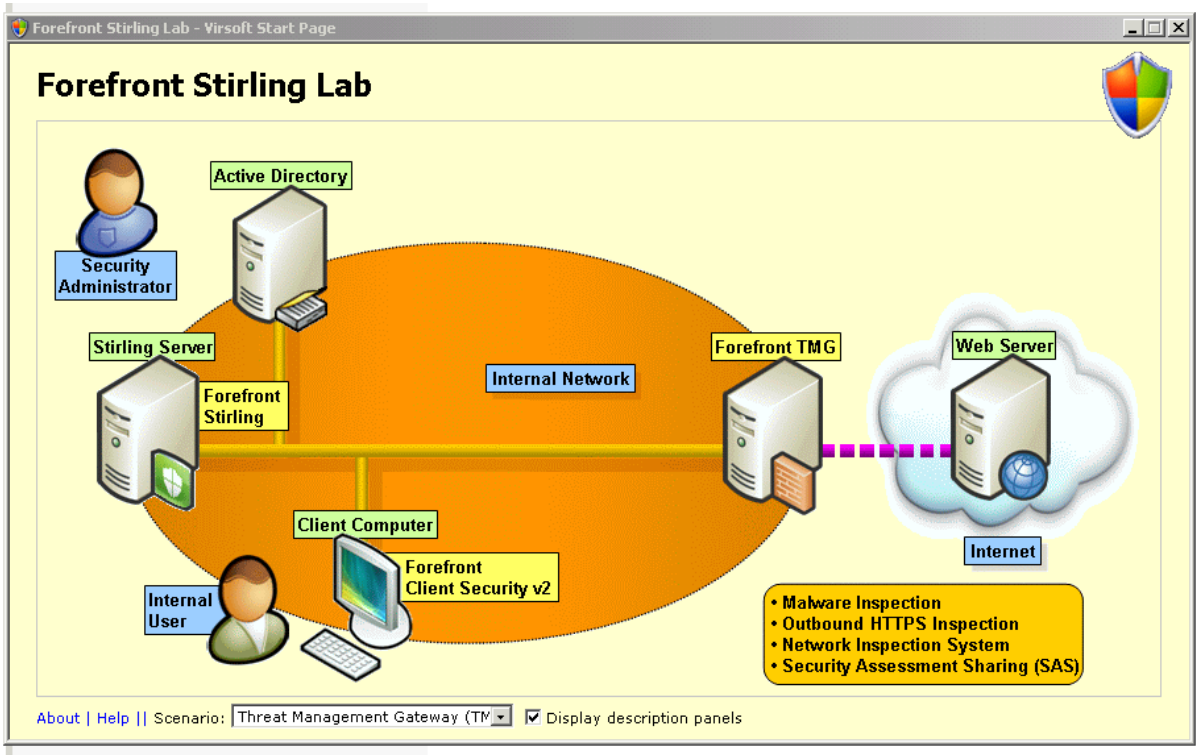
**Microsoft Forefront "Stirling" - Forefront Client Security - Ueberblick und Konfiguration**

In diesem Artikel zeige ich kurz den Funktionsumfang von Forefront Client Security und die Integration in 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

Ich nutze wieder die herunterladbare VHD-Testumgebung von Microsoft.

**Alles im Ueberblick**



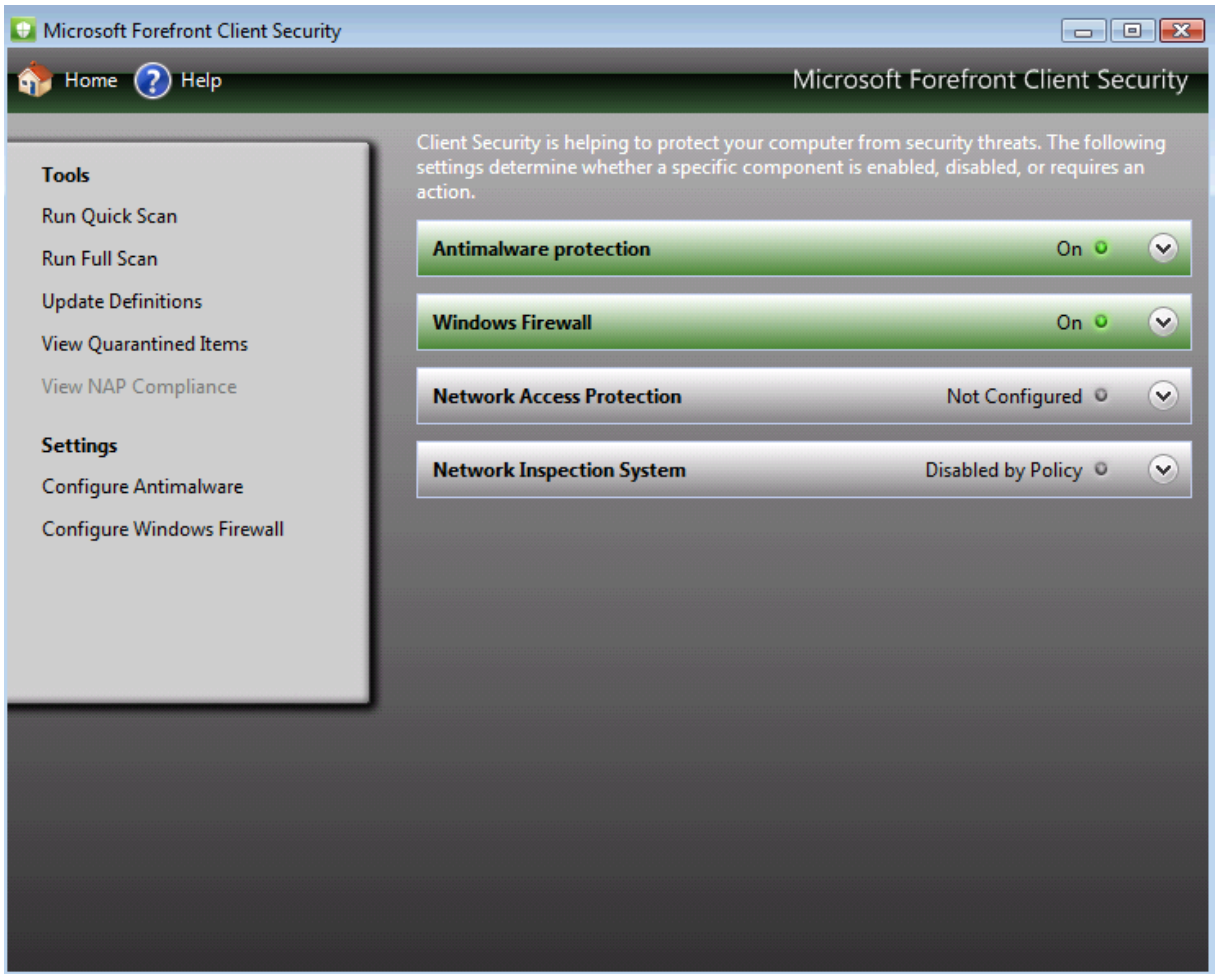

**Was enthalten die Downloads**

. 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

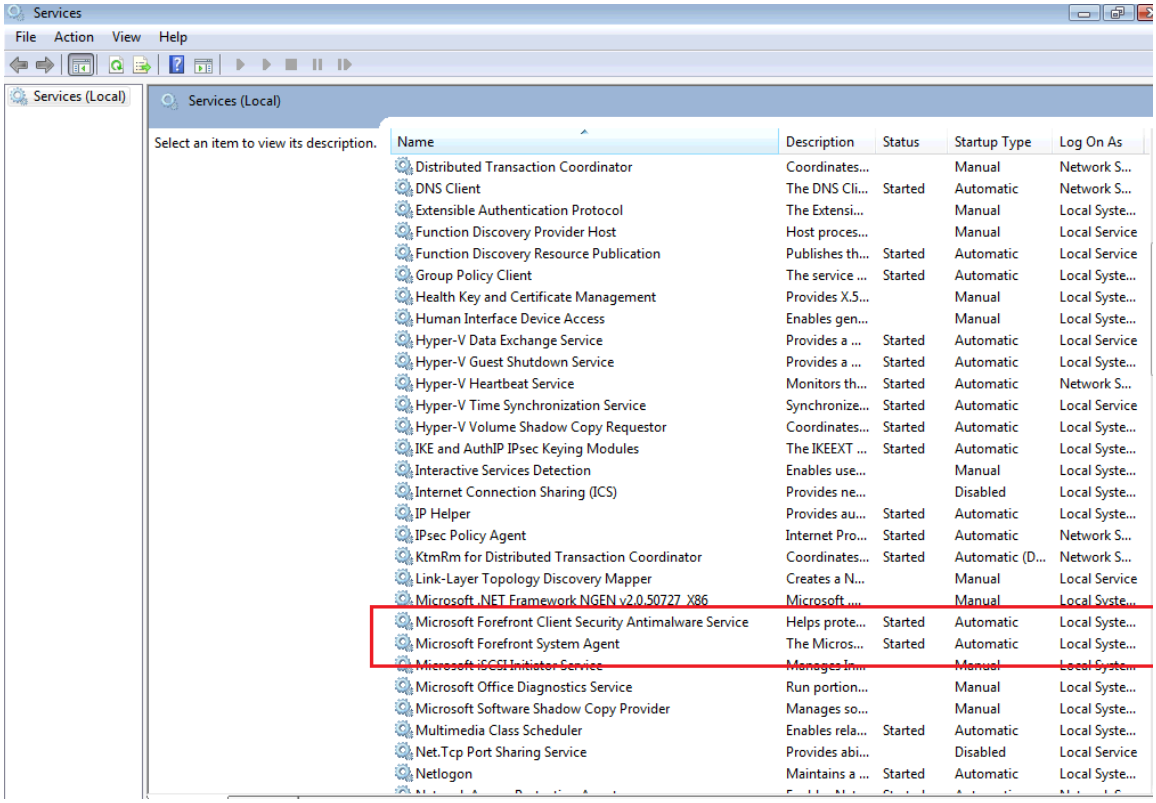
. Madrid
  - Exchange Server 2007 SP1 (Mailbox/Client Access/Hub Transport roles)
  - Forefront for Exchange (build 243 - beta 2)
. Sydney
  - Windows SharePoint Services (WSS) 3.0 SP1
  - Forefront for SharePoint (build 243 - beta 2)
. Toronto
  - Exchange Server 2007 SP1 (Edge Transport role)
  - Threat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

**Client Einstellungen**

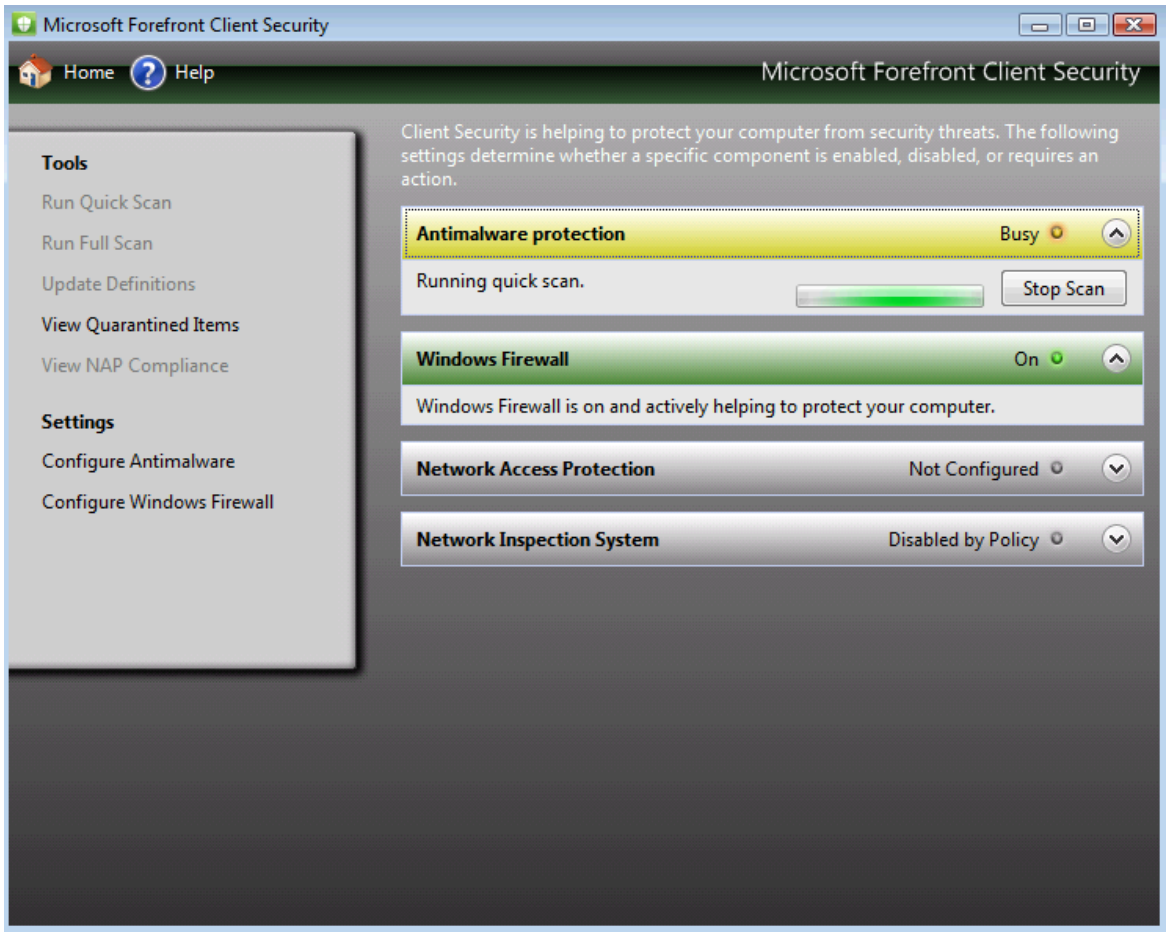
Bei der Installation von FCS = Forefront Client Security wird eine Verwaltungskonsole installiert. Die Einrichtung von FCS kann manuell oder ueber zentrale Richtlinien von Forefront Stirling.



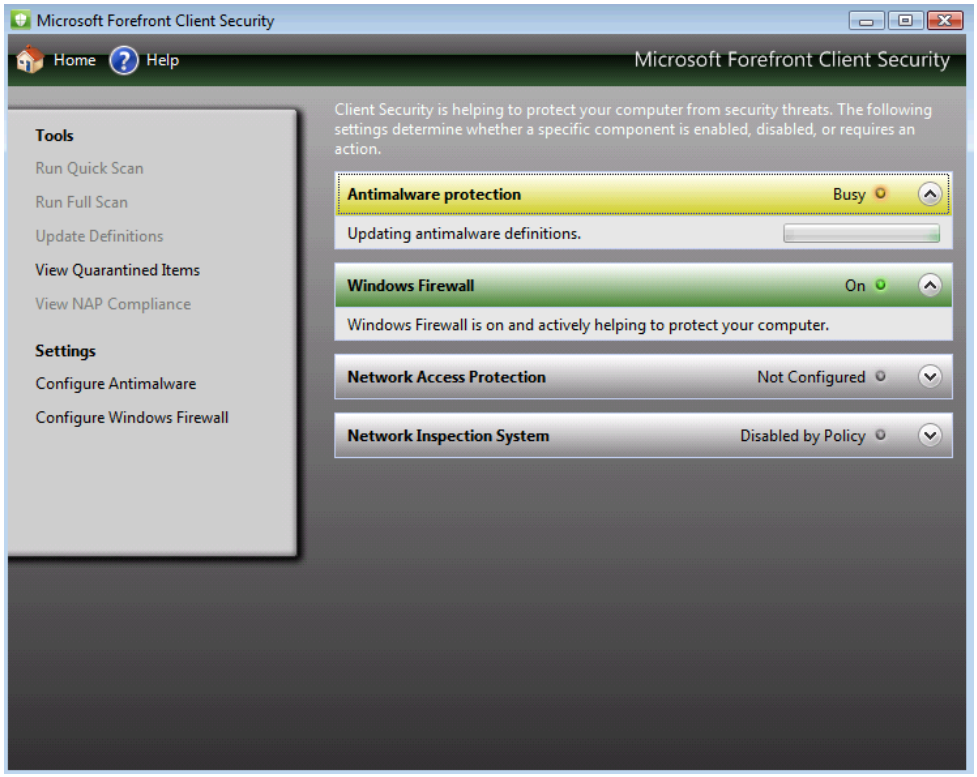
Auf der Client Seite werden verschiedene Forefront Dienste installiert.



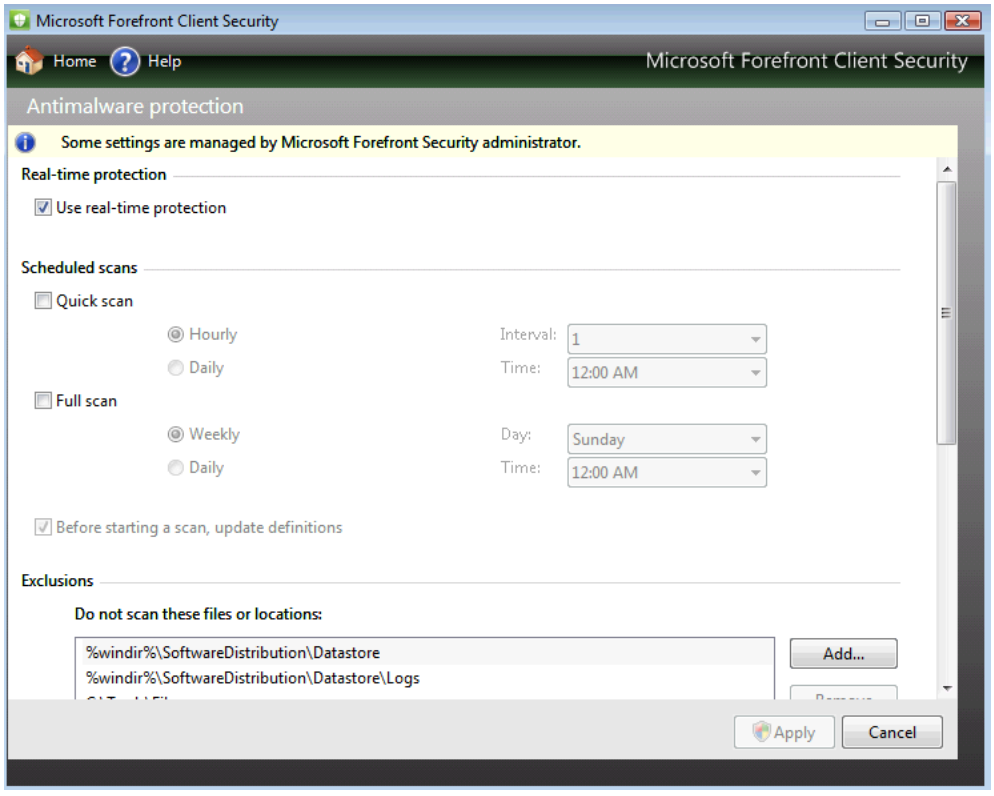

Ein Antimalware Scan kann ggfs. manuell ausgefuehrt werden.



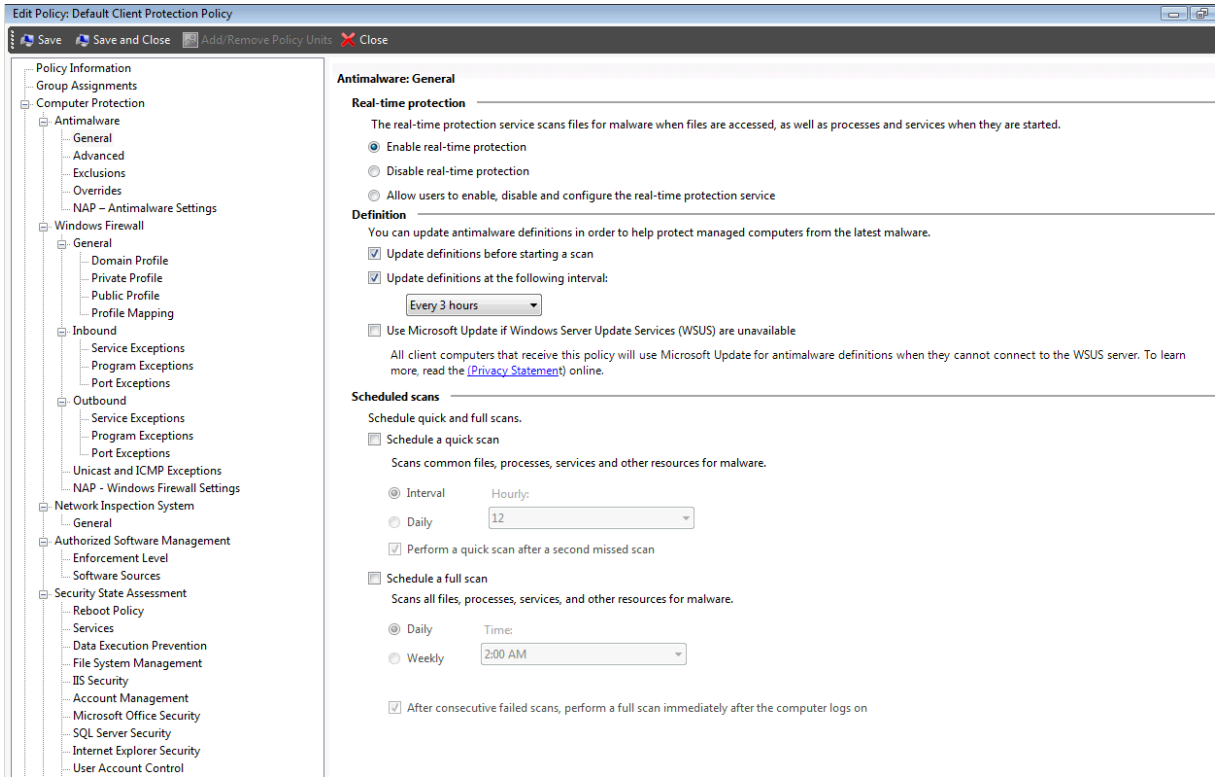
Antimalware Definitions koennen manuell oder zentral geladen werden



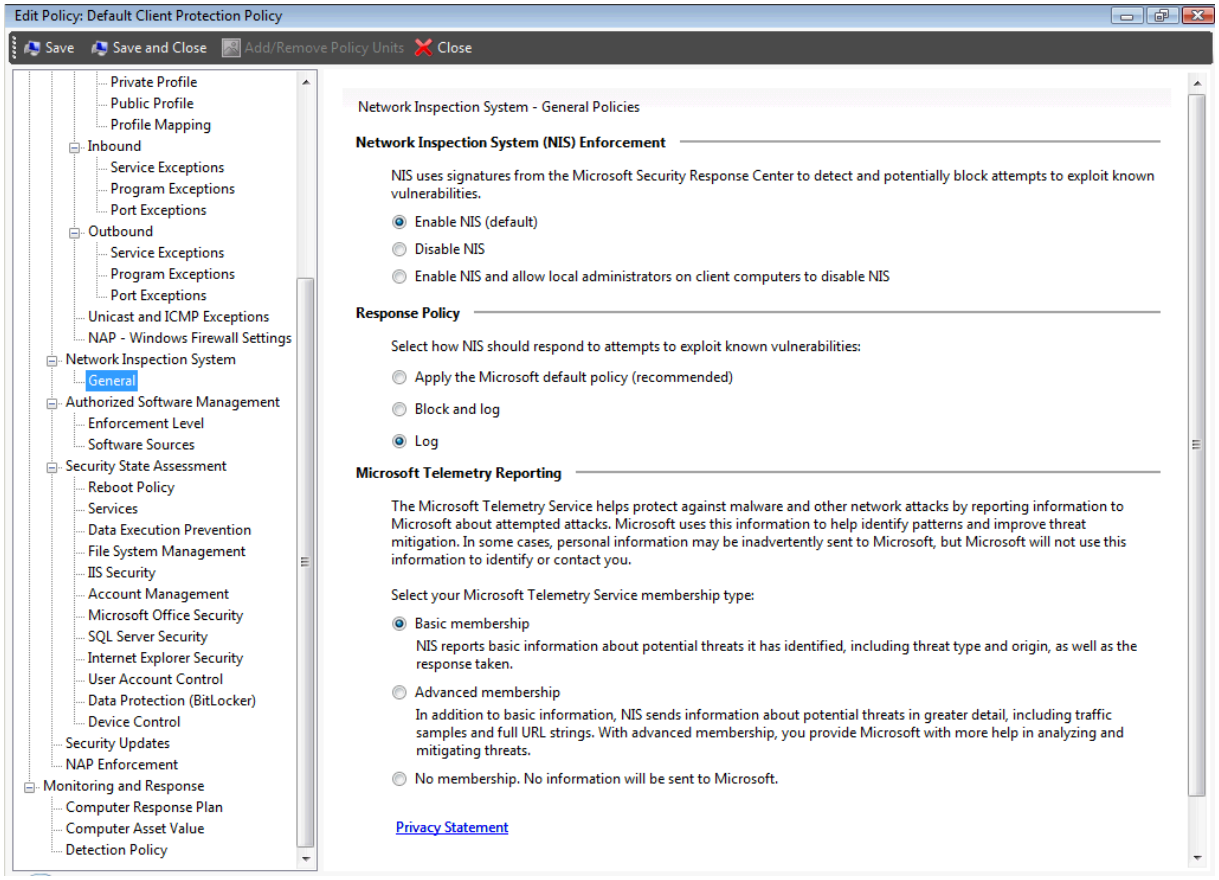

Die Realtime Protection kann vom Endbenutzer ausgeschaltet werden, wenn das nicht per Stirling Policy unterbunden wird.



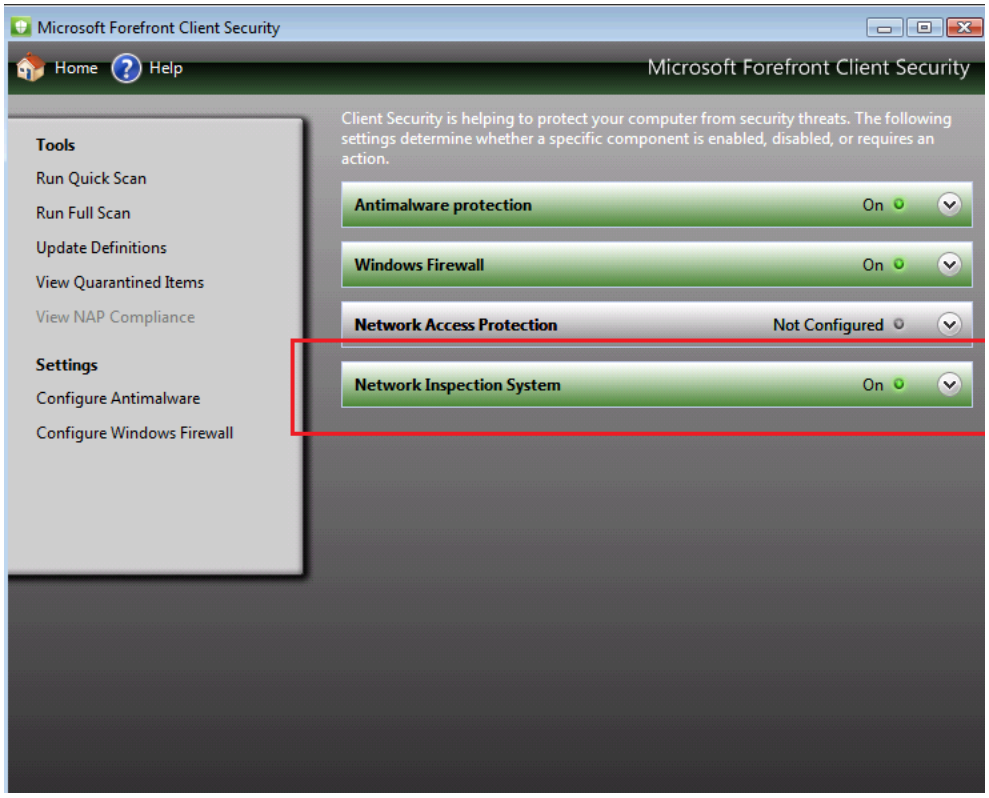
Realtime Protection Settings in Forefront Stirling



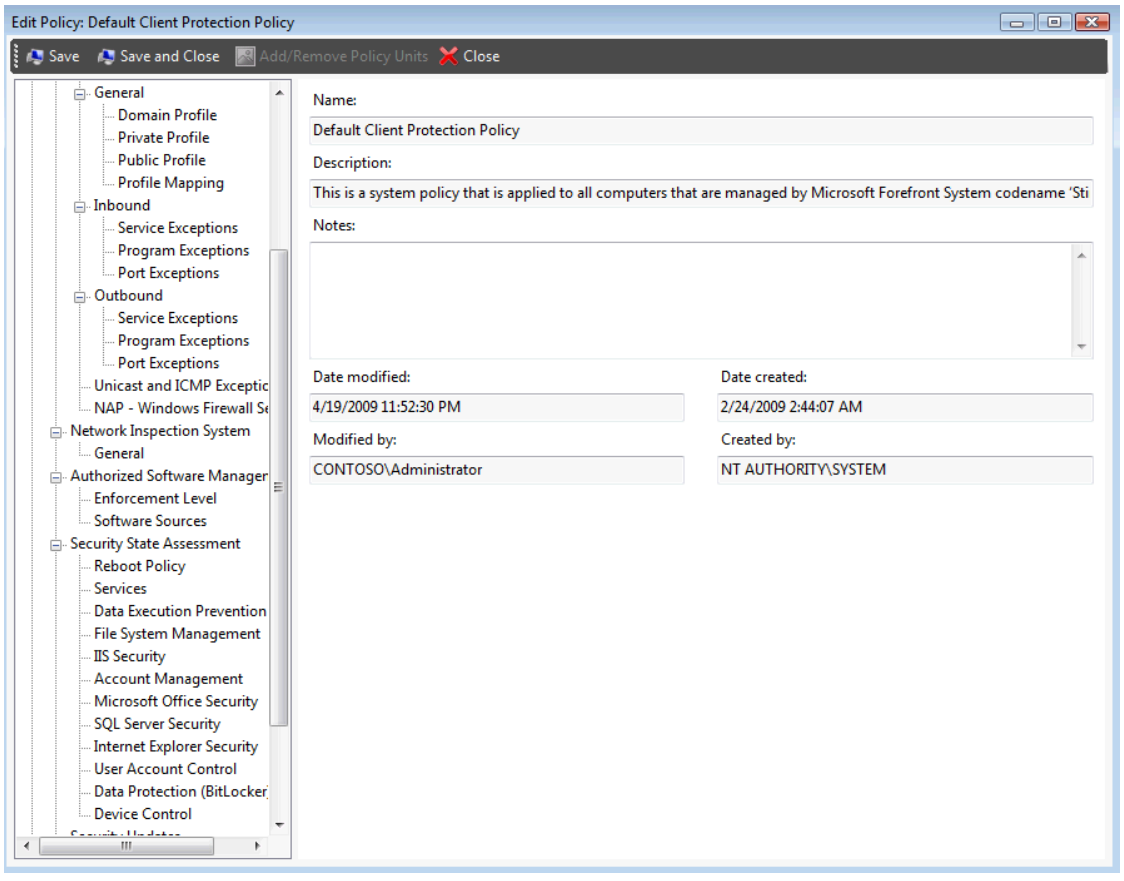

Per Stirling Policy koennen Funktionen wie NIS aktiviert werden.



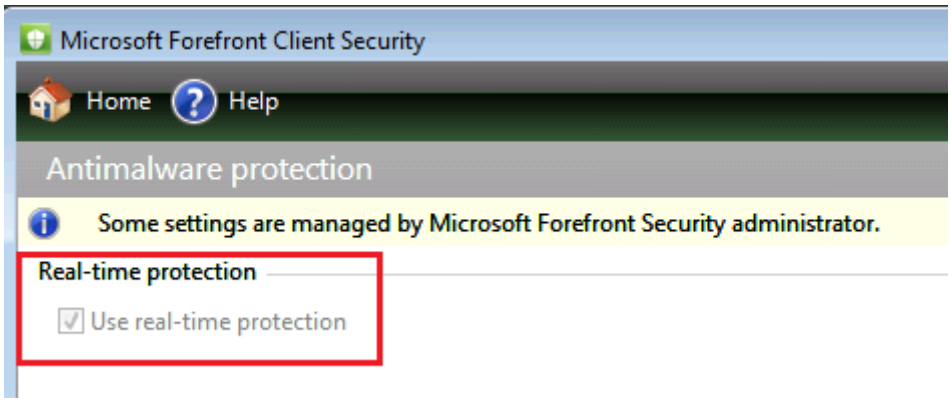
Nach kurzer Zeit ist die Client Konfiguration aktualisiert worden und NIS ist aktiv.



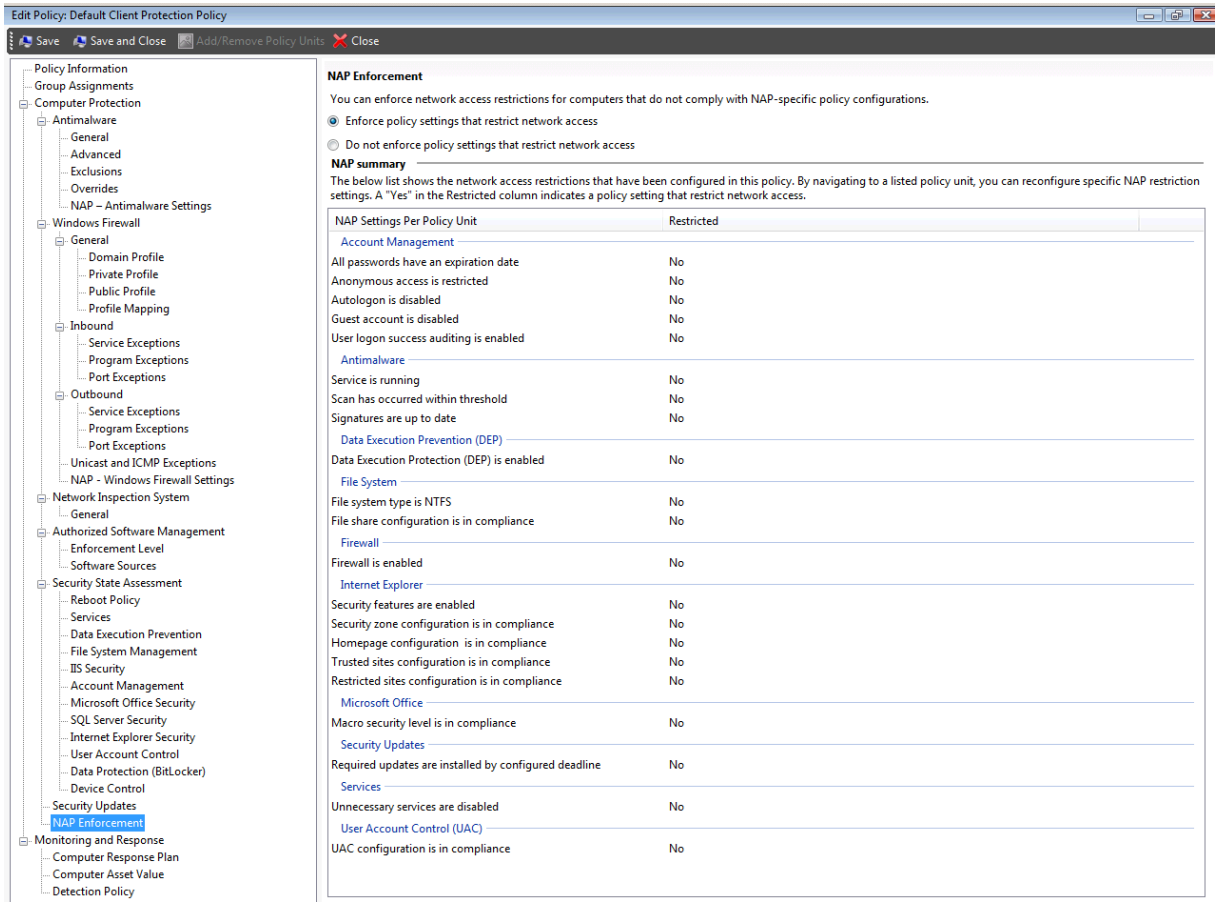

Mit Hilfe von Forefront Stirling kann eine Vielzahl von Einstellungen zentral vorgenommen werden.



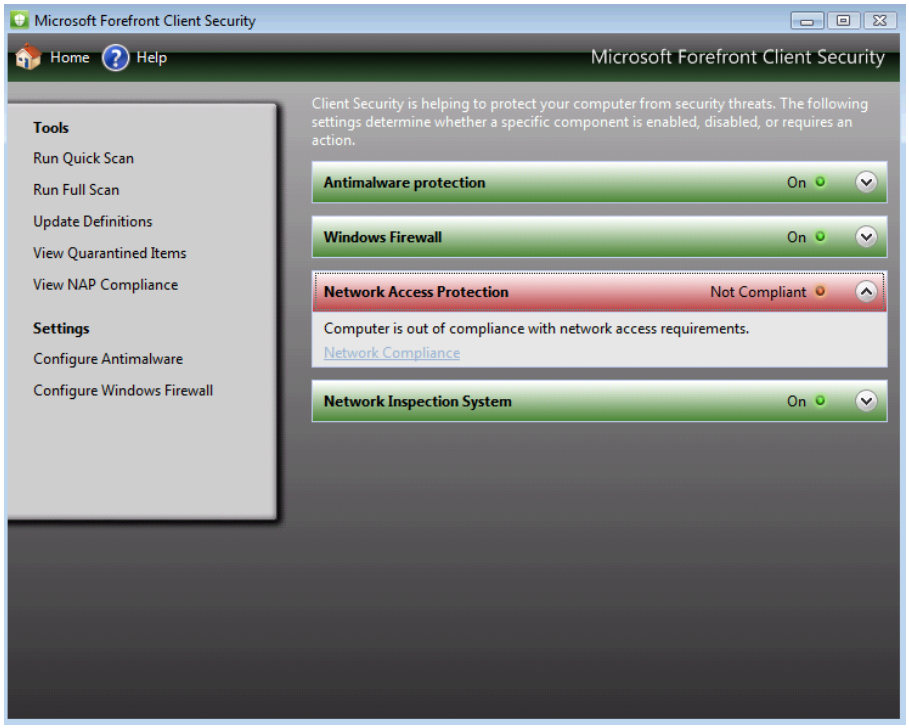
Die Realtime Protection ist jetzt durch eine zentrale Richtlinie aktiviert worden und kann vom Endbenutzer nicht mehr deaktiviert werden.




Desweiteren koennen mit Hilfe der Stirling Konsole zentrale NAP-Einstellungen fuer die Clients vorgenommen werden.



Nach kurzer Zeit ist das NAP Enforcement auf dem Client aktiv.




Die Forefront Stirling Konsole bietet umfangreiche Reportings wie in der folgenden Abbildung die Summary der Antimalware Konfigurationen zu sehen ist.