

ISA Server 2004 – VPN Quarantine Control - Von Marc Grote

**Die Informationen in diesem Artikel beziehen sich auf:
Microsoft ISA Server 2004**

Einleitung

Dieser Artikel ist als Ergänzung für den folgenden Artikel zu sehen: [VPN mit PPTP](#) und beschreibt die Einrichtung des ISA Server 2004 VPN Quarantine Control Features.

Was ist VPN Quarantine Control?

Bei dem VPN Quarantine Control Feature handelt es sich um ein neues Feature des ISA Server 2004 mit der Möglichkeit, VPN Clients erst dann Zugriff auf interne Netzwerkressourcen zu gewähren, wenn der Client vorher vom Administrator festgelegte Anforderungen erfüllt. Solche vom Administrator festgelegte Anforderungen könnten z. B. sein:

- ? Einsatz eines aktuellen Virenscanners
- ? Aktivierte Windows Firewall
- ? Verwendung der aktuellsten Windows Updates

Bemerkung:

Das VPN Quarantine Control Feature existiert bereits seit der Einführung von Windows 2003.

Bestandteile des VPN Quarantine Control Feature

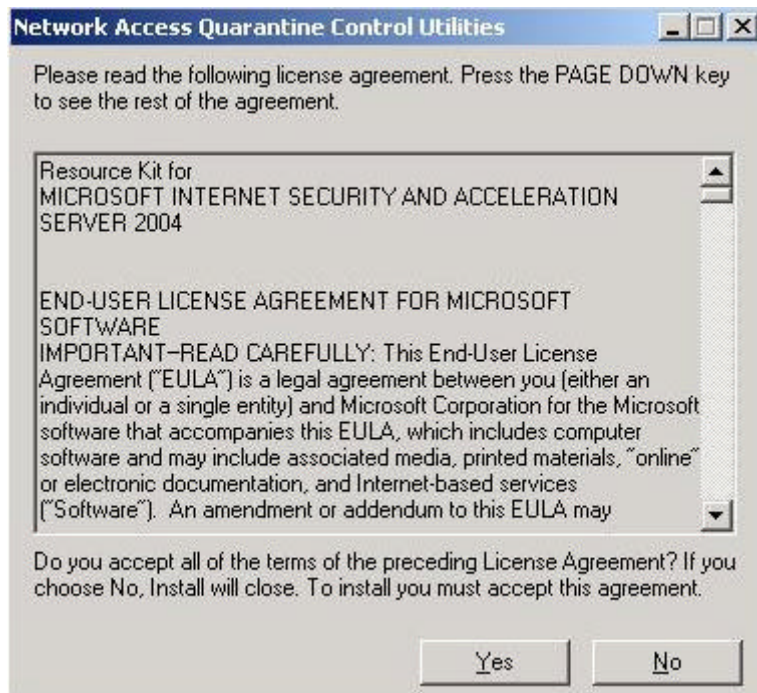
- ? RQS.EXE – Remote Quarantine Server (Bestandteil des Windows 2003 Resource Kits) auf dem ISA Server 2004
- ? RQC.EXE – Remote Quarantine Client (Bestandteil des Windows 2003 Resource Kits) auf den VPN Clients
- ? Connection Manager Administration Profile aus dem Connection Manager Administration Kit (CMAK)
- ? ConfigureRQSForISA.VBS zur Konfiguration der notwendigen ISA Server 2004 Komponenten

Remote Access Quarantine Control Tool

Die benötigten Quarantine Control Tools sind Bestandteil des Windows 2003 Resource Kits. Sie müssen das Windows 2003 Resource Kit auf dem ISA Server 2004 installieren. Sie erhalten das Windows 2003 Resource Kit [hier](#):

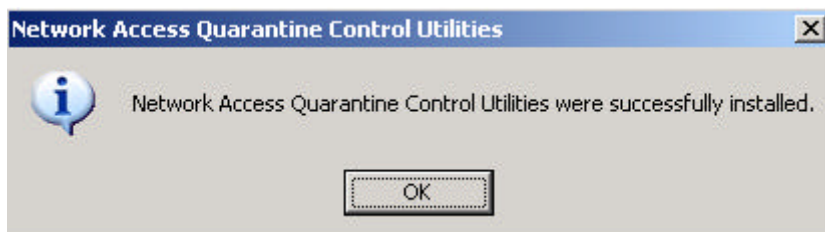
Nach Installation des Windows 2003 Resource Kits müssen Sie ein Update der RQS Komponenten installieren. Sie finden das Tool [hier](#):

Nach dem Download des Tools erfolgt die Installation:



Bemerkung:

RQS.EXE ist Bestandteil des Windows 2003 Resource Kits. Es existiert allerdings eine aktuelle Version, welche Sie auf alle Fälle verwenden sollten. Nachdem Sie die Tools installiert haben, führen Sie das Skript ConfigureRQSForISA.vbs aus, um den ISA Server 2004 als RQS Listener Komponente vorzubereiten.



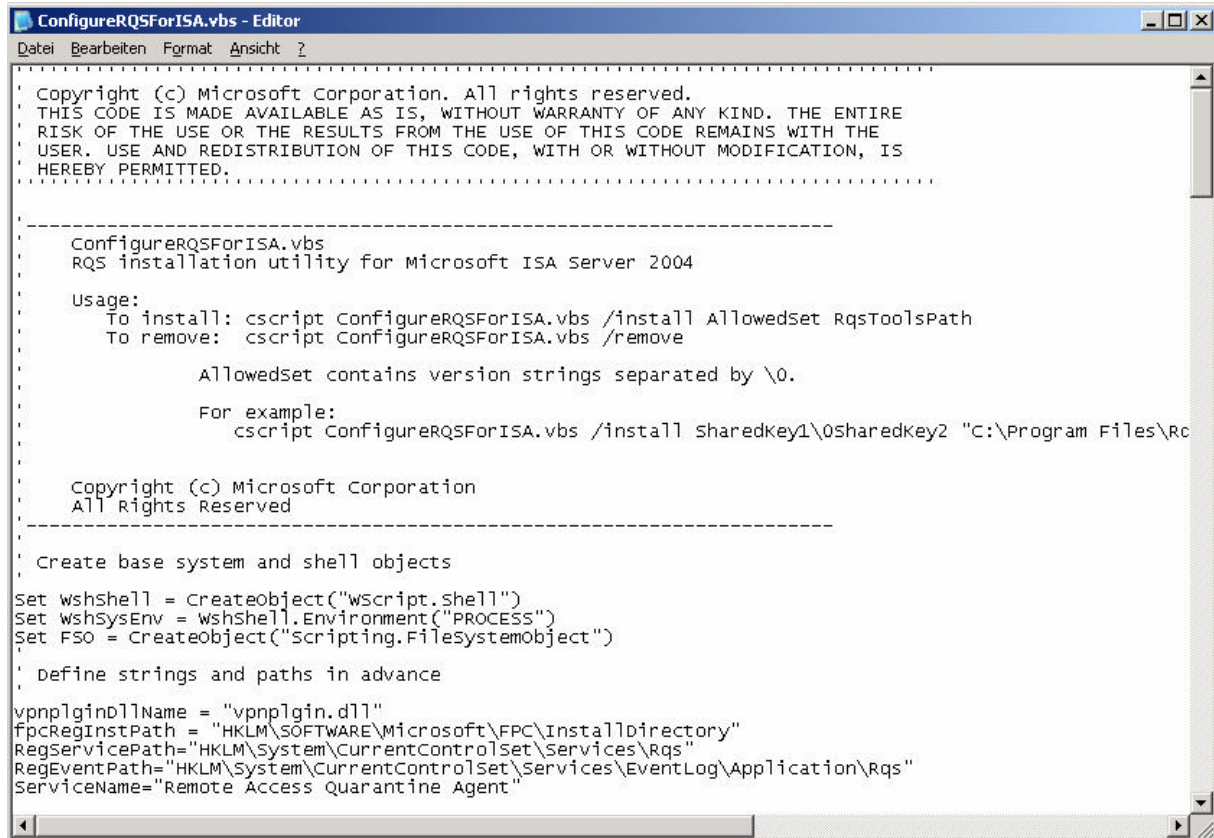
Als nächstes müssen Sie das Skript ConfigureRQSForISA.VBS ausführen.

Dieses Skript führt folgende Aufgaben durch:

- ? Erstellt eine RQS Protokolldefinition (TCP Port 7250)
- ? Erstellt einen RQS Dienst auf dem ISA (Network Quarantine Service (keine Dependencies))
- ? Erstellt folgenden Registry Key: HKEY_LOCAL_MACHINE\System\Current ControlSet\Services\Rqs
- ? Erstellt einen Registry Key, damit RQS Ereignisse korrekt in der Ereignisanzeige dargestellt werden
- ? Erstellt eine Firewallregel:
 - VON: „Quarantine VPN“ und „VPN Client Netzwerke“
 - ZU: „Local Host Network“
 - PROTOKOLL: RQS

- ERLAUBEN: Alle Benutzer
- ? Der RQS Dienst startet, wenn die Regel aktiviert wird. Der Starttyp ist *Automatisch*

Auszug aus dem Skript:



```
ConfigureRQSForISA.vbs - Editor
Datei Bearbeiten Format Ansicht ?

Copyright (c) Microsoft Corporation. All rights reserved.
THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE ENTIRE
RISK OF THE USE OR THE RESULTS FROM THE USE OF THIS CODE REMAINS WITH THE
USER. USE AND REDISTRIBUTION OF THIS CODE, WITH OR WITHOUT MODIFICATION, IS
HEREBY PERMITTED.

-----
ConfigureRQSForISA.vbs
RQS installation utility for Microsoft ISA Server 2004

Usage:
To install: cscript ConfigureRQSForISA.vbs /install AllowedSet RqsToolsPath
To remove:  cscript ConfigureRQSForISA.vbs /remove

        Allowedset contains version strings separated by \0.

        For example:
        cscript ConfigureRQSForISA.vbs /install SharedKey1\0SharedKey2 "C:\Program Files\Rc

Copyright (c) Microsoft Corporation
All Rights Reserved

-----

Create base system and shell objects
Set wshshell = Createobject("wscript.shell")
Set wshSysEnv = wshshell.Environment("PROCESS")
Set FSO = Createobject("Scripting.FileSystemObject")

Define strings and paths in advance

vpnplogin.dllName = "vpnplogin.dll"
fpcRegInstPath = "HKLM\SOFTWARE\Microsoft\FPC\InstallDirectory"
RegServicePath="HKLM\System\CurrentControlSet\Services\Rqs"
RegEventPath="HKLM\System\CurrentControlSet\Services\EventLog\Application\Rqs"
ServiceName="Remote Access Quarantine Agent"
```

Wie lautet die Syntax zur Installation des RQS Skriptes für Quarantine Control?

```
cscript ConfigureRQSForISA.vbs /install AllowedSet RqsToolsPath
```

AllowedSet ist ein Version String, welcher von der RQC Komponente angegeben werden muss, um sich beim RQS Listener zu identifizieren. Verwenden Sie "\0" um mehrfache Versions Strings zu trennen.

ToolsPath ist der Pfad zu den RQS Tools ohne Angabe des Dateinamen

Beispiel:

```
cscript ConfigureRQSForISA.vbs /install SharedKey1 "C:\RQS"
```

Bemerkung:

Das Skript ConfigureRQSForISA.vbs setzt voraus, dass sich die Dateien SC.EXE und REG.EXE im Windows System Pfad befinden. Das ist bei Windows 2003 der Fall, aber nicht bei Windows 2000.

```

C:\>cd c:\rqs
C:\rqs>cscript configurerqsforsisa.ubs /install sharedkey1 c:\rqs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Registering RQS as Service...
[SC] CreateService SUCCESS

[SC] ChangeServiceConfig2 SUCCESS

[SC] ChangeServiceConfig2 SUCCESS

Adding the allowed version strings under HKLM\System\CurrentControlSet\Services\Rqs...
Setting entries for the event log messages...
Looking for ISA installation path...
Setting RQS Authenticator value under HKLM\System\CurrentControlSet\Services\Rqs...
Updating firewall policy...
Adding RQS protocol definition...
Creating RQS access rule:
- from Quarantined UPN clients and UPN Clients
- to local host
- protocol = RQS
Starting the RQS service...
The script successfully installed RQS for ISA Server 2004.

```

Erstellter RQS Dienst auf dem ISA Server 2004

| Name | Beschreibung | Status | Ort |
|----------------------|--|-------------|--------------|
| NetMeeting-Remote... | Ermöglicht einem autorisierten Benutzer an einem anderen Computer auf diesen Computer mit NetMeeting über ... | Deaktiviert | Lokales Syst |
| Network News Tran... | Transportiert Netzwerkbotschaften über das Netzwerk | Deaktiviert | Lokales Syst |
| Network Quarantin... | This service can be used to implement a Quarantined VPN Clients network for a Routing and Remote Access Server | Gestart... | Automat... |
| Netzwerk-DDE-Dienst | Ermöglicht Netzwerktransport und Sicherheit für den dynamischen Datenaustausch (DDE) von Programmen, die ... | Deaktiviert | Lokales Syst |
| Netzwerk-DDE-Serv... | Verwaltet DDE-Netzwerkfreigaben (Dynamic Data Exchange=Dynamischer Datenaustausch). Wenn dieser Dien... | Deaktiviert | Lokales Syst |

Erstellte Firewall Regel für RQS

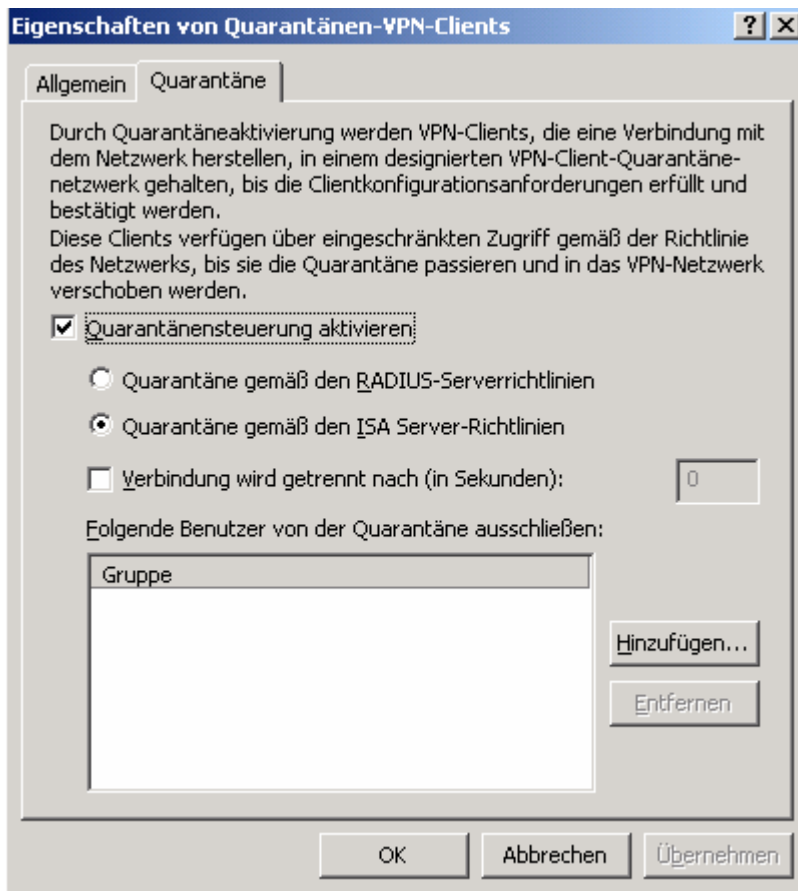
| R... | Name | Aktion | Protokolle | Von / Listener | Nach | Bedingung |
|------|--------------------|----------|------------|--|--------------|---------------|
| 1 | Network Quarant... | Zulassen | RQS | Quarantänen-VPN-Clients VPN-Clients | Lokaler Host | Alle Benutzer |

Aktivieren des Quarantine Control Features auf dem ISA Server 2004

Starten Sie die ISA Verwaltungskonsole und navigieren Sie zu *Konfiguration – Netzwerke* – und wählen im Reiter *Netzwerke* die *Quarantänen-VPN-Clients* aus. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontext Menü *Eigenschaften* aus.

Im Reiter *Quarantäne* können Sie dann die *Quarantänensteuerung aktivieren*.

Wählen Sie *Quarantäne gemäß den ISA Server-Richtlinien*.

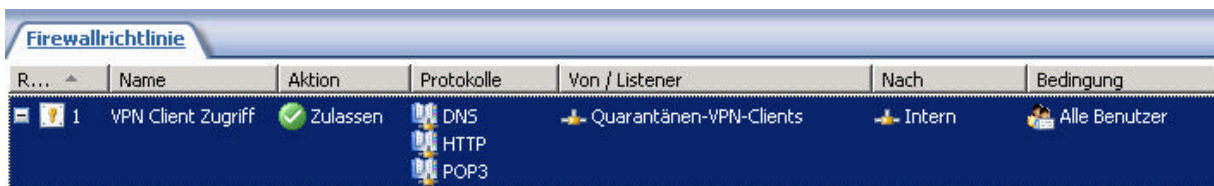


Bemerkung:

Wenn Sie *Quarantäne gemäß den RADIUS Server-Richtlinien* wählen, muss der ISA Server Mitglied einer Domäne sein. Es sind dann noch weitere Schritte erforderlich.

Erstellen einer Firewall Policy für die VPN Clients

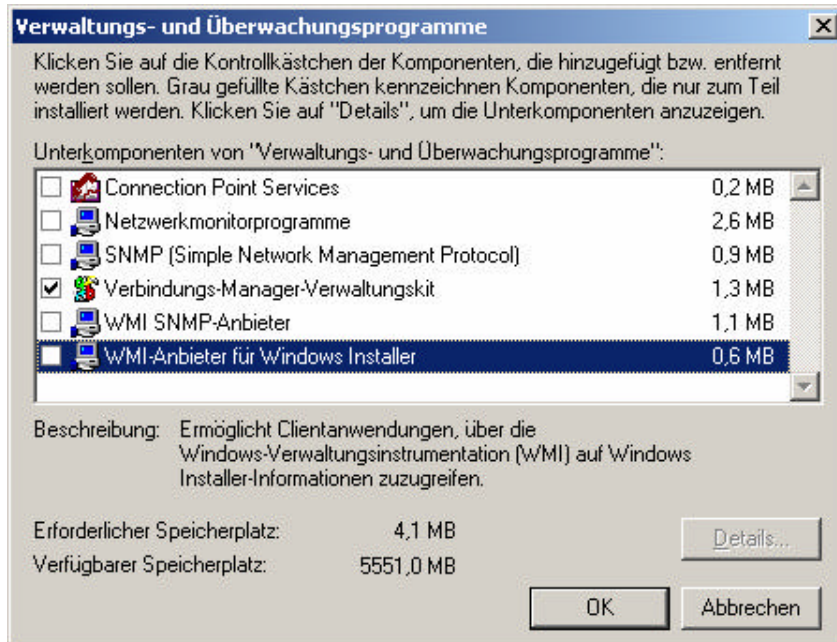
Damit die Quarantined VPN Clients Zugriff auf interne Netzwerkressourcen erhalten, müssen Sie eine entsprechende Firewall Policy erstellen. Die Grafik zeigt ein Beispiel:



Details zur Konfiguration von Firewall Policies erhalten Sie [hier](#).

Verbindungs-Manager Profil

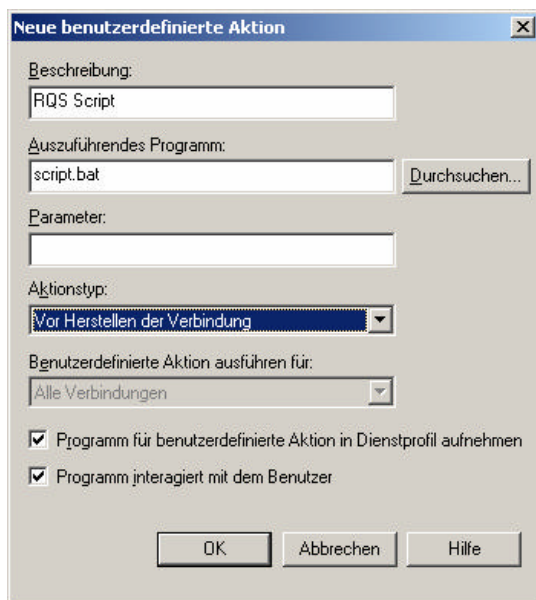
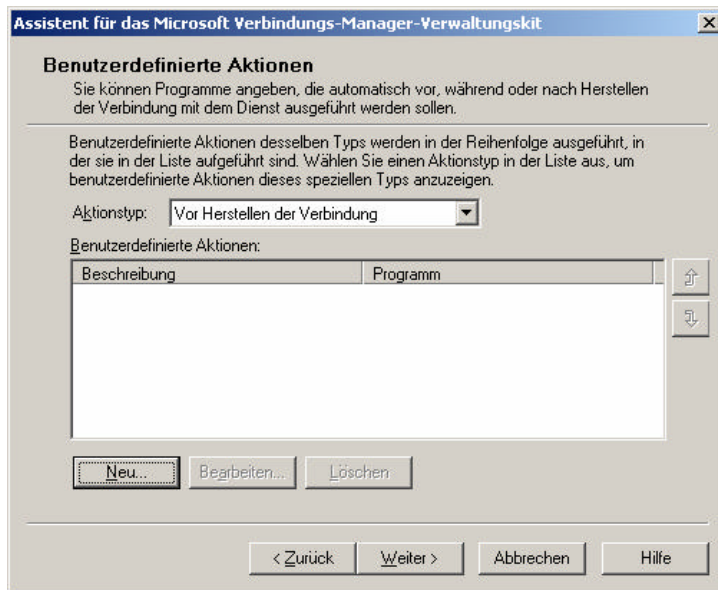
Erstellen Sie mit Hilfe des Verbindungs-Manager Verwaltungskits auf dem ISA Server 2004 ein Connection Manager Profile, mit dessen Hilfe ein VPN Client die Verbindung zum VPN Server aufbauen kann. Bestandteil des CM Profiles ist auch das Quarantine Control Skript.



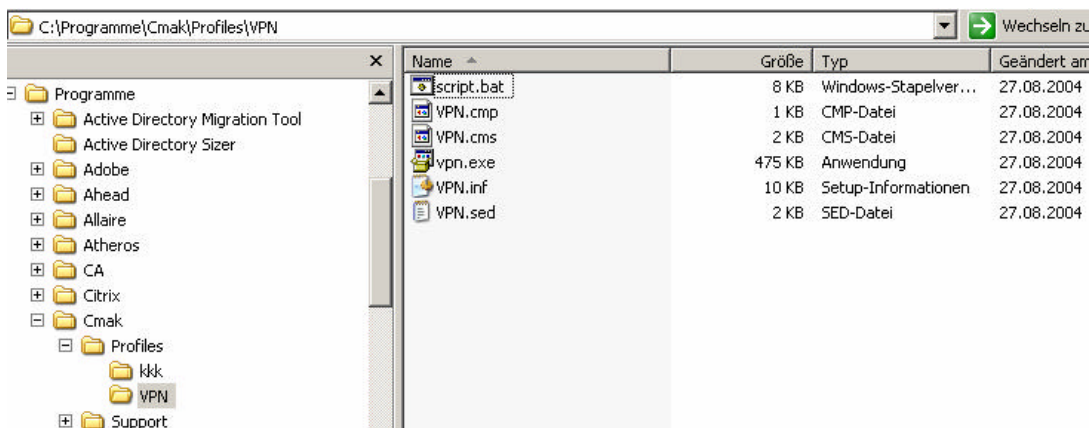
Ich beschreibe in diesem Artikel nicht jeden Schritt zur Konfiguration eines CM Profiles. Für weitere Informationen klicken Sie [hier](#).



Sie müssen das Script (in diesem Beispiel SCRIPT.BAT) als Aktionstyp *Vor Herstellen der Verbindung* ausführen.



CMAK erstellt ein komplettes Profil anhand Ihrer Angaben und packt das ganze in eine .EXE Datei, welche Sie nur noch auf dem VPN Client ausführen müssen.



Nach erfolgreicher Installation des CMAK Profiles, existiert ein neuer Eintrag in den Netzwerkverbindungen des Clients.

Verbindungs-Manager



Quarantine Script

Das Quarantine Script kann eine ausführbare Datei (.EXE), Skript (.VBS) oder eine Batchdatei (.CMD oder .BAT) sein.

Nachdem im Script alle Anforderungen des VPN Clients abgefragt worden sind, erfolgt der Aufruf von RQC.EXE mit folgenden Parametern:

```
rqc ConnName TunnelConnName TCPPort Domain UserName ScriptVersion
```

ConnName: Der Name der Remote Access Verbindung. Kann mit %DialRasEntry% abgefragt werden!

TunnelConnName: Der Name der Tunnel Verbindung auf dem Host. Kann mit %TunnelRasEntry% abgefragt werden.

TCPPort: Die Port Nummer der RQS Komponente. Default = 7250

Domain Die Domäne des zu verbindenden Benutzers. Kann mit %Domain% abgefragt werden.

UserName: Der Name des Benutzers welcher die Verbindung aufbaut. Kann mit %UserName% abgefragt werden.

ScriptVersion: Ein text String welcher die Script Version beinhaltet. Sie können alle Textstrings außer /0 verwenden, weil diese vom RQS verwendet werden um mehrfache Strings zu trennen.

Die Erstellung des Quarantine VPN Scriptes ist die schwerste Angelegenheit. Hier hat Microsoft noch einiges erheblich zu verbessern. Die Konkurrenz bietet hier wesentlich komfortablere Konfigurationsmöglichkeiten.

Es ist eine permanente Anpassung des Scriptes notwendig, um es an die sich fast täglich ändernden Sicherheitsbedrohungen anzupassen.

Bemerkung:

Mit Windows 2003 SP1 soll es eine GUI zur Konfiguration des Quarantine Control Features geben. Bei meinen bisherigen Test mit der Beta Version von Windows 2003 SP1 konnte ich dieses Programm nicht finden.

Sie können als Einstieg das Beispielskript aus dem Windows 2003 Quarantine Access Control [Artikel](#) verwenden. Ich habe das Skript in diesem Artikel etwas angepasst. Das Skript kann jedoch nicht für ein reales Quarantine Control Script verwendet werden, zumal es sich bei diesem Beispielskript nur um ein Gerüst ohne wirkliche Funktion handelt.

Derzeit existieren noch keine frei verfügbaren Beispielskripte auf den Webseiten von Microsoft. Es bleibt zu hoffen, das Microsoft in Zukunft einige Beispielskripte veröffentlicht.

Die Syntax lautet:

```
script.bat %DialRasEntry% %TunnelRasEntry% %Domain% %UserName%
```

Aus %DialRasEntry% wird %1
Aus %TunnelRasEntry% wird %2
Aus %Domain% %3
Aus %UserName% wird %4

```
@echo off
echo RAS Connection = %1
echo Tunnel Connection = %2
echo Domain = %3
echo User Name = %4
set MYSTATUS=
REM
REM Netzwerk Poliy Check
REM
REM Überprüft ob ICF aktiviert ist
REM Setzt ICFCHECK auf 1 (pass).
REM Setzt ICFCHECK auf 2 (fail).
REM Prüft auf installierten Virenchecker
REM Setzt VIRCHECK auf 1 (pass).
REM Setzt VIRCHECK auf 2 (fail).
REM Basierend auf den Ergebnissen wird Rqc.exe ausgeführt
REM
if "%ICFCHECK%" == "2" goto :TESTFAIL
if "%VIRCHECK%" == "2" goto :TESTFAIL
rqc.exe %1 %2 7250 %3 %4 Version1
REM %1 = %DialRasEntry%
REM %2 = %TunnelRasEntry%
REM 7250 ist der TCP Port auf welchem Rqs.exe einen Listener setzt
REM %3 = %Domain%
REM %4 = %UserName%
REM Version1 ist die Versionsnummer des Scripts
REM
REM Statusausgabe
REM
if "%ERRORLEVEL%" == "0" (
    set MYERRMSG=Success!
) else if "%ERRORLEVEL%" == "1" (
    set MYERRMSG=Kein Zugriff möglich. Quarantine Control ist evtl. deaktiviert
) else if "%ERRORLEVEL%" == "2" (
    set MYERRMSG=Zugriff verweigert. Installieren Sie das CMAK Profile aus dem
Unternehmensnetz.
) else (
    set MYERRMSG=Unbekannter Fehler, der Client bleibt im Quarantine Mode)
echo %MYERRMSG%
goto :EOF
:TESTFAIL
echo
echo Der Computer erfüllt nicht die Anforderungen der Security Policy der Firma IT TRAINING
echo GROTE. Wenden Sie sich an Ihren Administrator um die Mängel zu beheben und so Zugriff auf
echo Firmenressourcen zu erhalten
:EOF
```

Zusammenfassung:

Welche Schritte werden bei der Verwendung des Quarantine Control Features von ISA 2004 durchgeführt

- ? Der Benutzer der Quarantine Remote Access Clients verwendet das installierte Quarantine CM Profil um sich zum ISA 2004 Server zu connecten
- ? Der Client leitet die Authentifizierungsanfrage an den ISA Server
- ? Der ISA Server validiert die Authentifizierungsdaten und prüft die Remote Access Policy ob diese die Quarantine Policy matched.
- ? Die Verbindung wird mit Quarantine Restriktionen akzeptiert und der Client erhält eine IP Adresse und wird im " Quarantined VPN Clients" Netzwerk geparkt
- ? Der Quarantined Client kann dem ISA Server nur mitteilen, ob das Skript erfolgreich ausgeführt wurde
- ? Das CM Profile führt das Quarantine Skript als sogenannte „Post Connect“ Aktion durch
- ? Das Quarantine Skript wird ausgeführt und überprüft ob der Remote Access Client den Netzwerk Richtlinien entspricht. Wenn alle Tests bestanden wurden, führt das Skript RQC.EXE aus (mit dem Text String, welcher im CM Profil angegeben wurde)
- ? RQC.EXE sendet eine Notifikation an den ISA Server das das Skript erfolgreich ausgeführt wurde.
- ? Die Notifikation wird von der RQS Listener Komponente empfangen (es wird nur Traffic über den RQS Port 7250 erlaubt)
- ? Die Listener Komponente überprüft den Skript Version String in der Notification Message und schickt eine Bestätigung zurück.
- ? Wenn das Skript validiert wurde, ruft die Listener Komponente die MprAdminConnectionRemoveQuarantine() API auf, welche den ISA Server dazu veranlasst, den Client aus dem „Quarantined VPN Clients network“ in das „VPN Clients Network“ verschiebt.
- ? Die Listener Komponente erstellt ein Ereignis in die Ereignisanzeige (System)