Forefront UAG Endpoint Access Policies

Eine der Staerken von Forefront UAG ist die Durchsetzung der sogenannten Endpunktrichtlinientreue. Mit Hilfe der Endpunktrichtlinientreue koennen Forefront UAG Administratoren diverse Sicherheitseinstellungen auf Clients, welche auf UAG zugreifen sollen erzwingen, um so einen sicheren Zugriff auf Unternehmensdaten / -Anwendungen zu ermoeglichen.

Forefront UAG stellt eine Reihe von Forefront UAG Endpoint Access Policies zur Verfuegung, welche auf Ebene des Forefront UAG Portals und auf Ebene der einzelnen veroeffentlichten Applikationen innerhalb des Portals eingerichtet werden koennen.

Eine Forefront UAG Endpoint Access Policies kann auf Basis von zwei Eigenschaften erstellt werden:

- Betriebssytemspezifische Einstellungen
- Einstellungen anhand von Expressions

Betriebssytemspezifische Einstellungen

Diese Einstellungen legen den Fokus auf die verwendeten Betriebssysteme und stellen Richtlinien fuer Windows, Linux und Mac OS zur Verfuegung

Einstellungen anhand von Expressions

Bei Expressions handelt es sich um Bedingungen basierend auf Variablen, Vbscript oder eine Kombination von beidem. Expressions koennen immer dann verwendet werden, wenn keine Betriebssystemspezifischen Einstellungen vorliegen und verwendet werden koennen.

Auf Trunk (Portal) Ebene koennen zwei Typen von Session Policies konfiguriert werden:

- Session Access Policy
- Privileged Endpoint Policy

Session Access Policy

Die Session Access Policy definiert die Bedingungen welche erfuellt sein muessen, damit ein Endgeraet Zugriff auf Unternehmensanwendungen erhalten kann.

Privileged Endpoint Policy

Definiert die Bedingungen, welche erfuellt sein muessen, um aus einem Endpoint einen privilegierten Endpoint zu machen, um weitere Privilegien innerhalb der Session zu erhalten.

Application Endpoint Policies

Application Endpoint Policies regeln die Privilegien und Voraussetzungen eines Endpoint Clients fuer den Zugriff auf spezifische Applikationen innerhalb des Trunks. Auch hier stehen wieder eine Reihe von Policies zur Verfuegung:

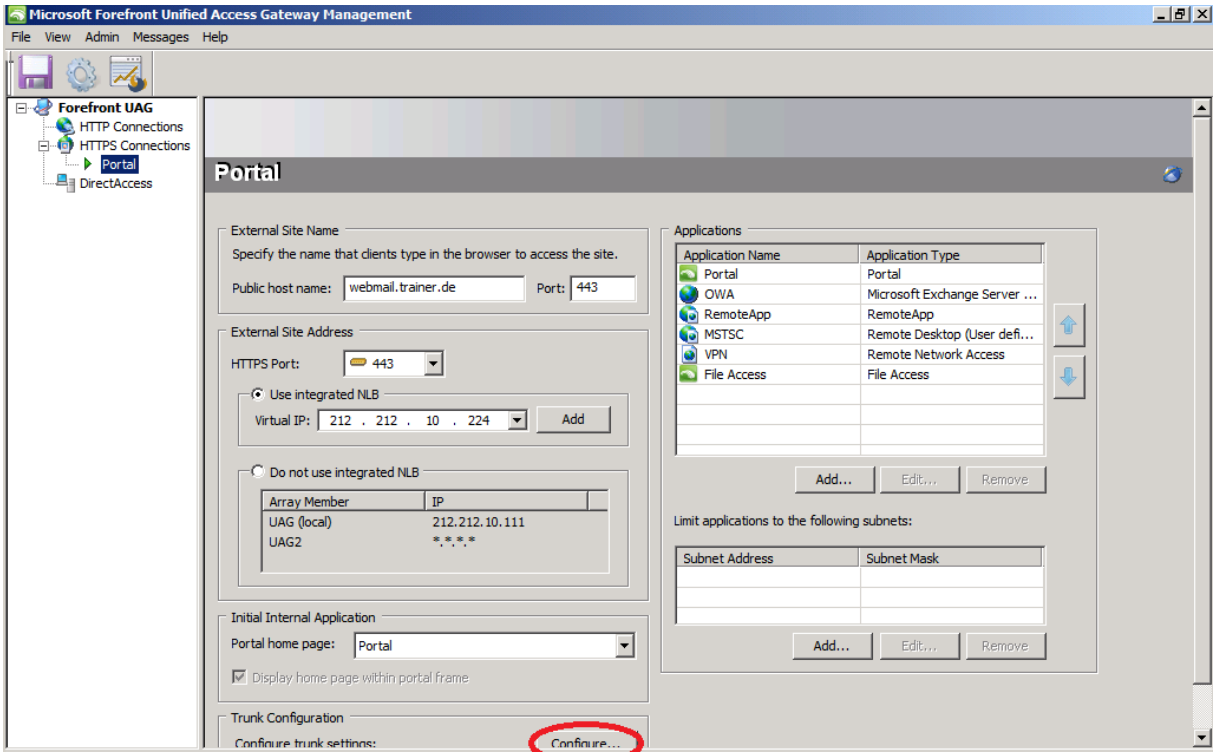
- Access Policies welche den Zugriff auf Applikationen regeln
- Download Policies welche regeln, was ein Endpoint herunterladen darf
- Upload Policies welche regeln, was ein Client heraufladen darf
- Restricted Zone Policies welche regeln, wie der Zugriff auf Webapplikationen mit Zonenmodellen geregelt werden kann
- Printer, Clipboard und Drive Redirection Policies fuer RemoteApps der Remotedesktopdienste

Weitere Informationen:

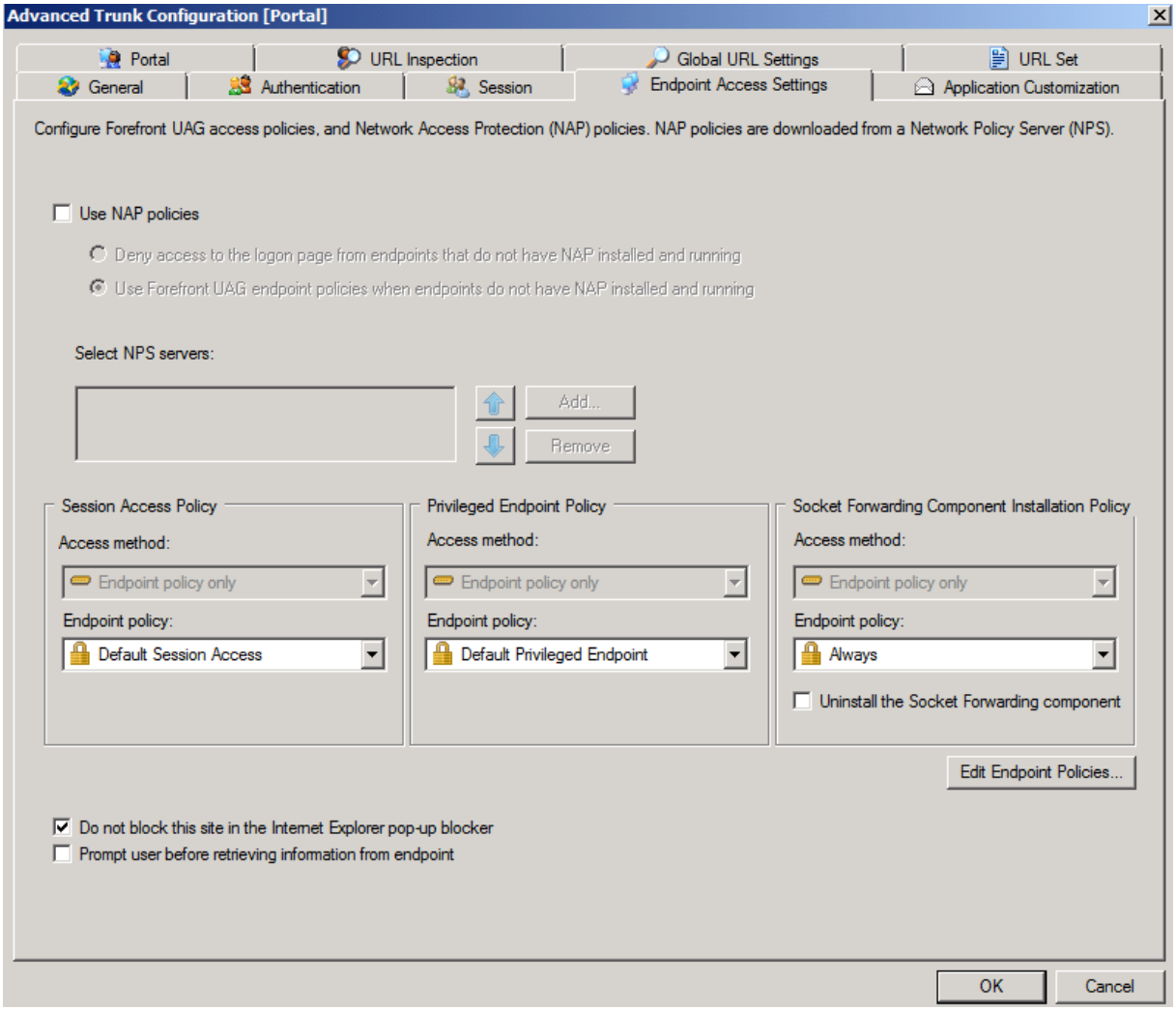
http://technet.microsoft.com/en-us/library/dd897093.aspx
Forefront Unified Access Gateway (UAG) Content Series - Client Endpoint Component Guides
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9CBBC75E-2C21-440F-B7DC-000CE4774C2B&amp%3Bdisplaylang=en

Forefront UAG Endpoint Access Polices auf Portal (Trunk) Ebene

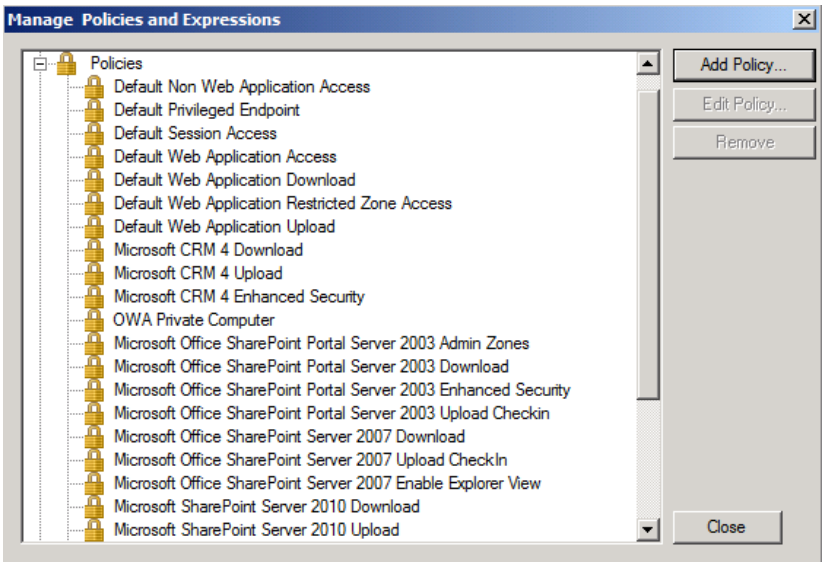
Zur Konfiguration der Endpoint Access Policies auf Trunkebene wird die UAG Verwaltungskonsole gestartet und zum jeweiligen Portal (Trunk) navigiert.



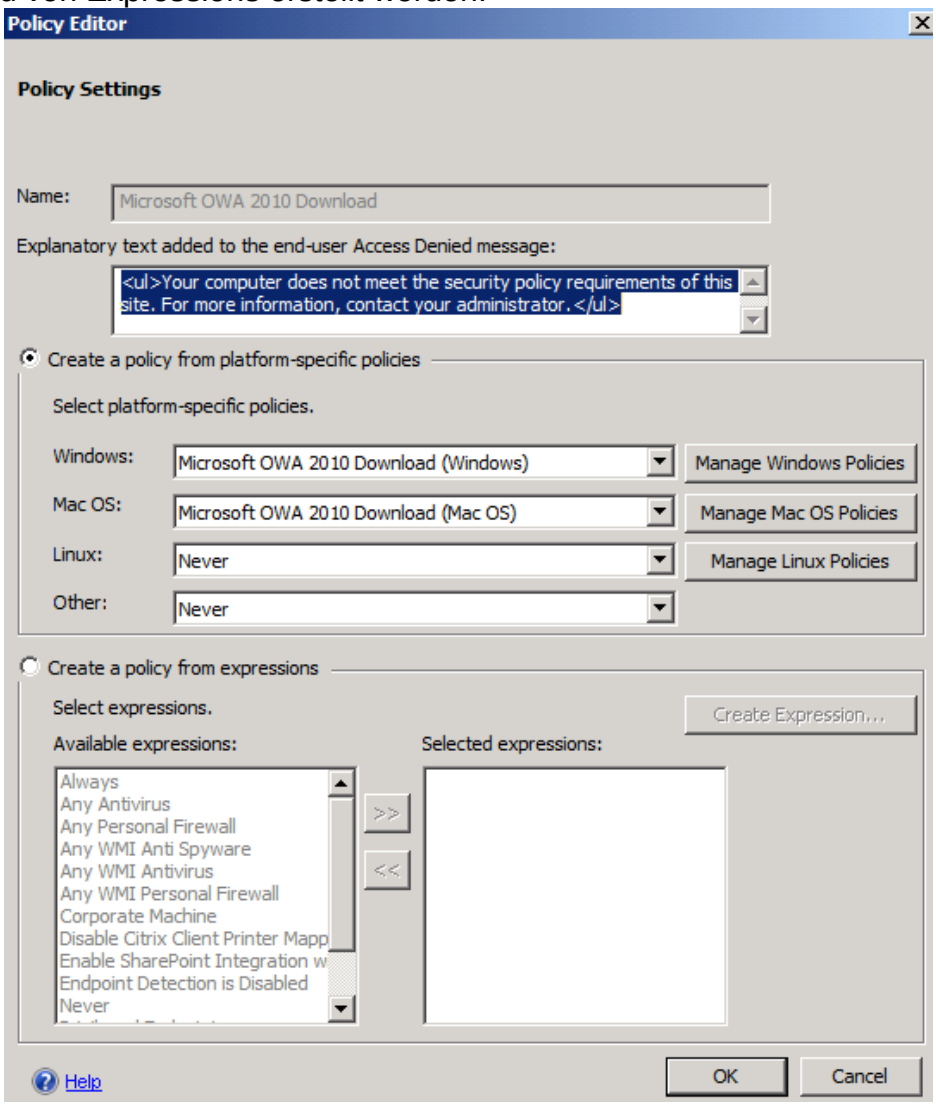
Auf der Registerkarte Endpoint Access Settings koennen dann unterschiedliche Endpoint Access Polices eingerichtet werden, welche im spaeteren Verlauf dieses Artikels noch erlaeutert werden.



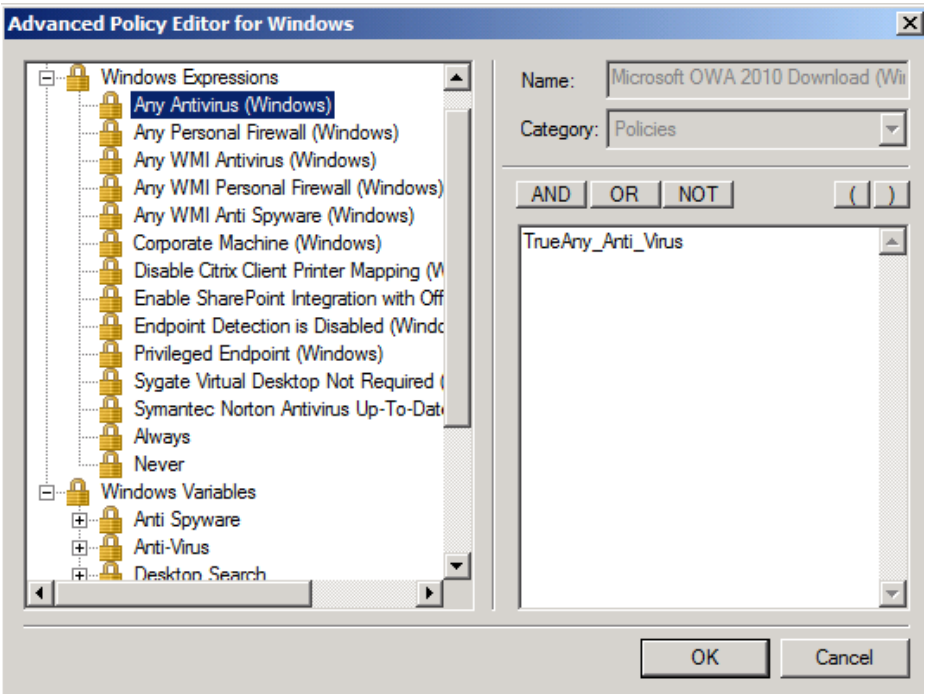
Es stehen eine Reihe von vordefinierten Richtlinien und Expressions zur Verfuegung, welche modifiziert werden koennen, aber auch neue Policies erstellt werden koennen.



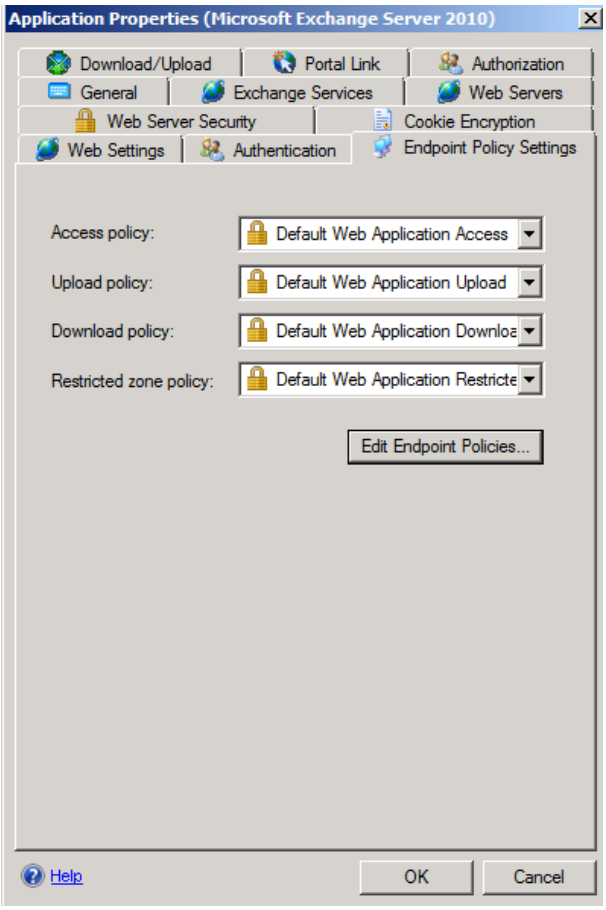
Wie bereits weiter oben in diesem Artikel erwaehnt, koennen betriebssystemspezifische Policies erstellt und genutzt werden, aber auch Policies anhand von Expressions erstellt werden.



Expressions und Policies koennen mit AND OR oder NOT Bedingungen kombiniert und ausgeschlossen werden und so auf die Firmenbeduerfnisse angepasst werden.



Auf Ebene der einzelnen Appliaktionen innerhalb des Portals koennen dann, wie weiter oben in diesem Artikel erwaehnt, unterschiedliche Einstellungen fuer den Upload / Download und den Zugriff auf die Applikationen ueberhaupt geregelt werden.



Forefront UAG Endpoint Access Policies auf Client Seite

Fuer die Durchsetzung der Forefront UAG Endpoint Access Policies muessen auf dem Endgeraet einzelne Komponenten installiert werden, welche mit dem Forefront UAG und dem Endgeraet interagieren.

Je nach verwendetem Betriebssystem und Berechtigungen auf dem Endgeraet koennen die benoetigten Komponenten als ActiveX Control, Java Applet, MSI Paket Online oder Offline installiert werden. An Komponenten steht zur Verfuegung:

Forefront UAG Endpoint Component Manager

Downloads, installs, manages, and removes all the Forefront UAG endpoint components. There are two versions of this component: ActiveX and Java Applet.

Forefront UAG Endpoint Session Cleanup

There are two versions of this component: ActiveX and Java Applet.

Forefront UAG Endpoint Detection

There are two versions of this component: ActiveX and Java Applet. For more information, see About the Endpoint Detection component.

Non-Web tunneling

Several components are used to provide SSL tunneling capabilities.

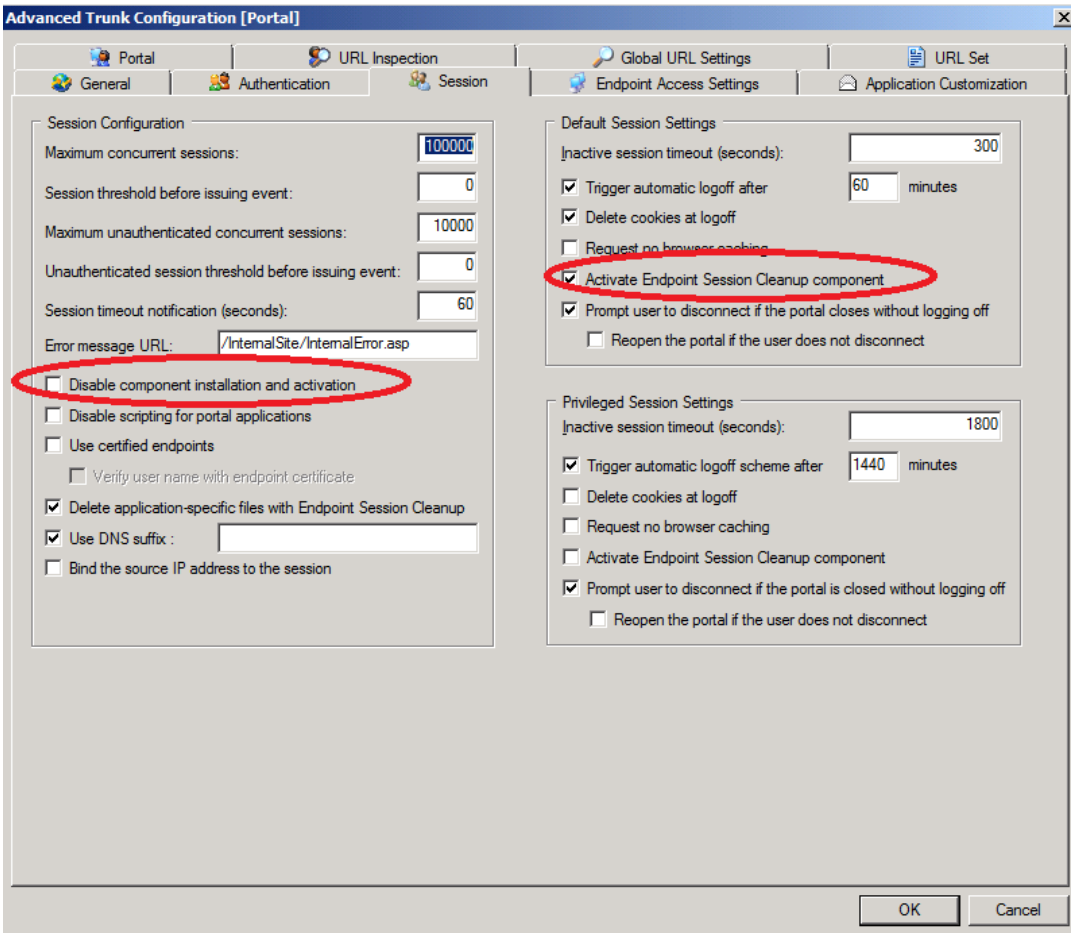
The SSL tunneling components are:

- Forefront UAG SSL Application Tunneling—There are two versions of this component: ActiveX and Java Applet
- Forefront UAG Socket Forwarding
- Forefront UAG SSL Network Tunneling

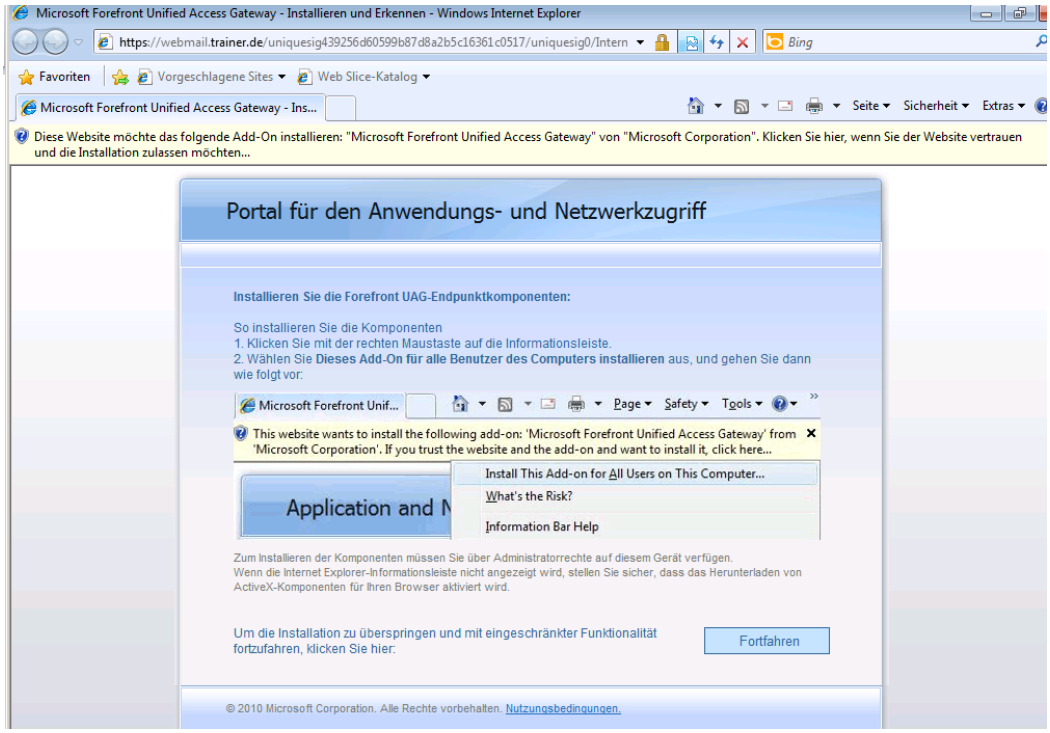
Socket Forwarding Helper—Used for support purposes.

Bei dem ersten Kontakt eines Clients mit dem Forefront UAG Server werden die Forefront UAG-Endpunktkomponenten auf dem Client installiert. Dazu werden lokale Administratorrechte auf dem Endgeraet benoetigt.

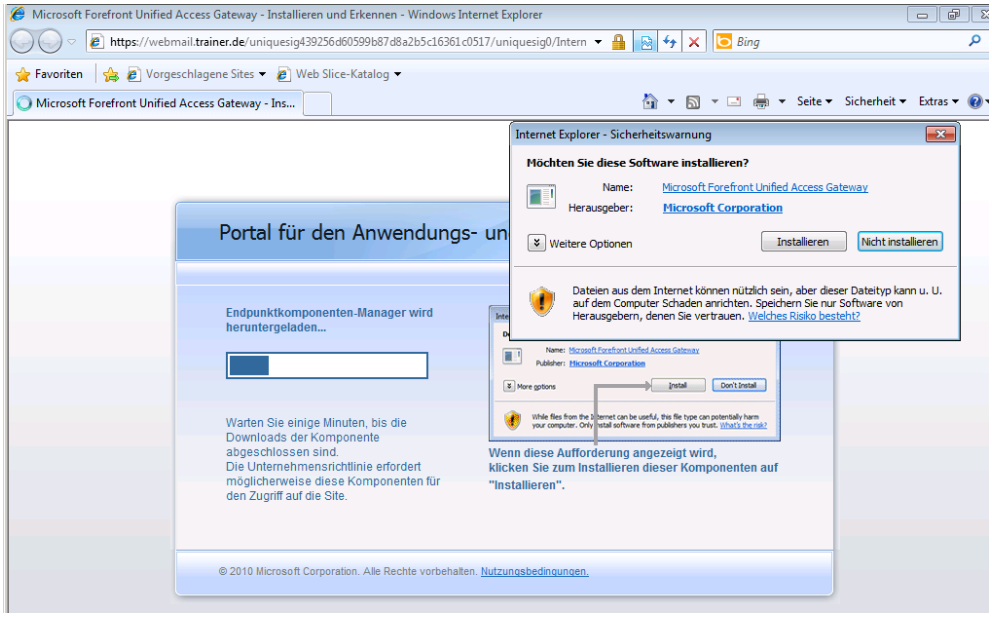
Die Installation der Komponenten beim Aufruf der Portal Webseite ist automatisch aktiviert und kann in den Portaleigenschaften modifiziert werden:



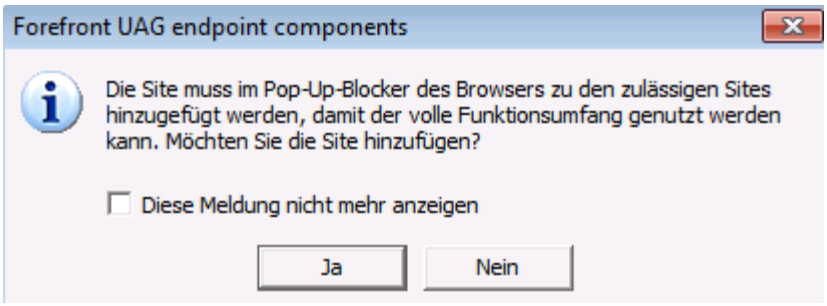
Beim ersten Aufruf des Portals wird dann zur Installation der UAG-Endpunktkomponenten aufgefordert:



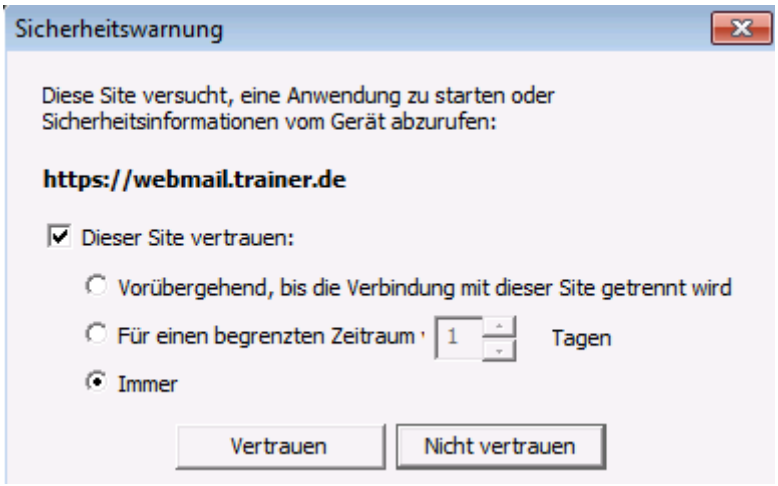
Die Installation der Endpoint Komponenten nimmt einige Zeit in Anspruch, einige Popupdialoge muessen bestaetigt werden.



Ja, raus aus dem Popup Blocker

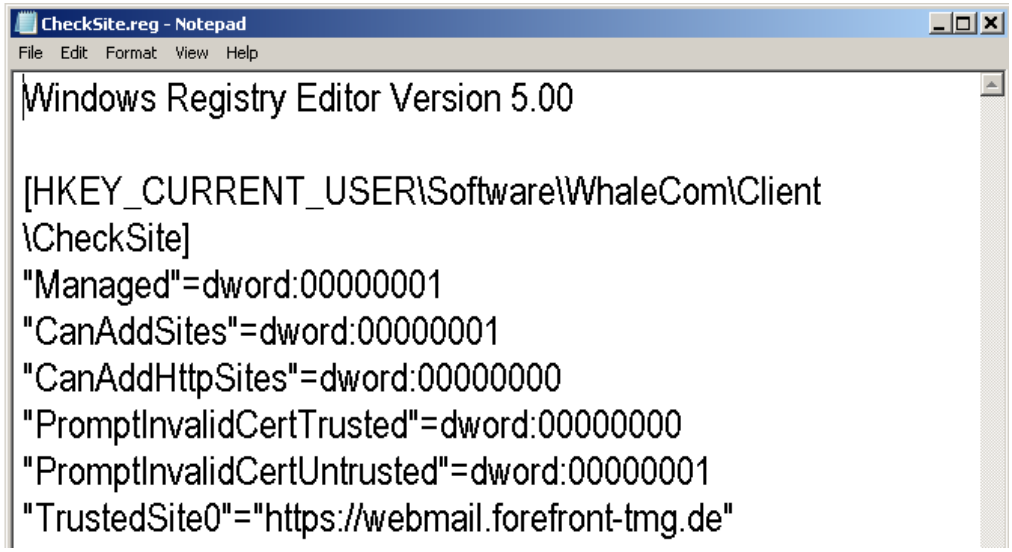


Ja, immer vertrauen.



Reghacks

Karsten Hentrup hat einige UAG RegHacks erstellt, um die oben gezeigten Meldungen zu elemnieren. Hier sind sie:



popup.reg - Notepad

File Edit Format View Help

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer
\New Windows\Allow]
"webmail.forefront-tmg.de"=hex:
```

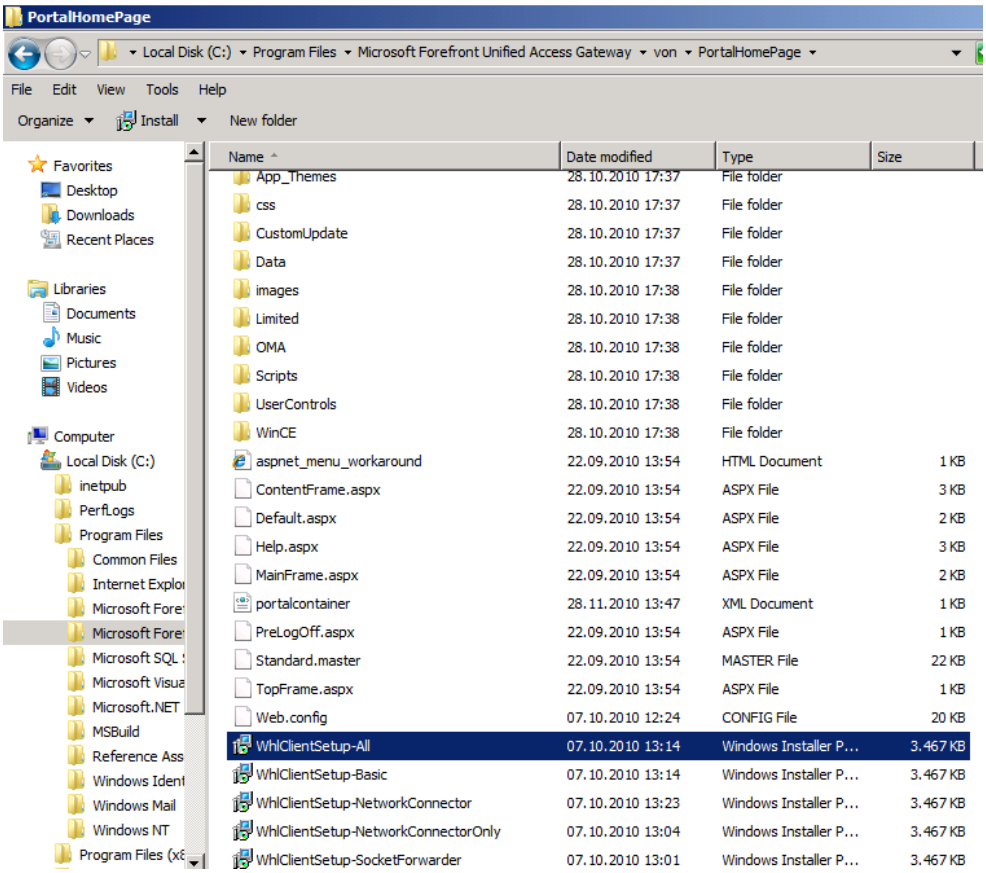
xp-firewall.reg - Notepad

File Edit Format View Help

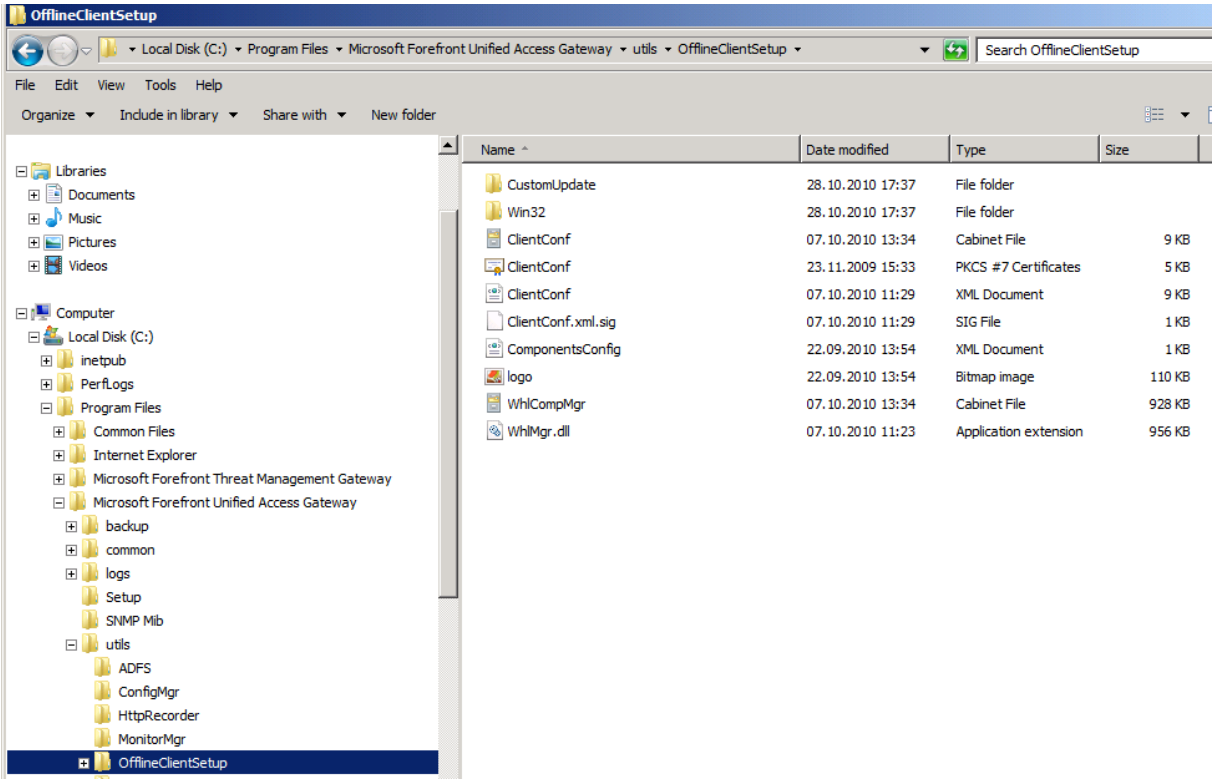
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\SharedAccess\Parameters\FirewallPolicy
\StandardProfile\AuthorizedApplications\List]
"C:\\Programme\\Microsoft Forefront UAG\\Endpoint
Components\\3.1.0\\WhlClnt3.exe"="C:\\Programme\\Microsoft
Forefront UAG\\Endpoint Components\\3.1.0\
\WhlClnt3.exe:*:Enabled:SSL Application Tunneling"
```

Die Endpoint Components liegen als MSI File im Dateisystem des UAG Server vor:



Ein Offline Client Setup ist verfuegbar:



Aktivierung des Offline Installers

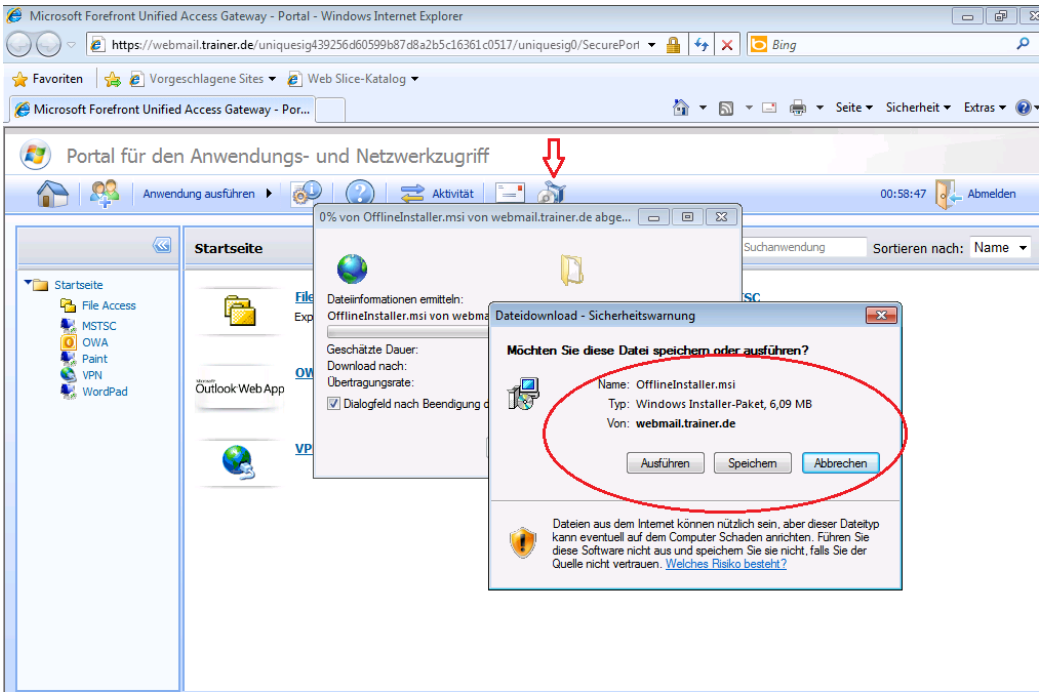
http://technet.microsoft.com/en-us/library/ee861162.aspx

1.On the Forefront UAG server, open the folder Microsoft Forefront Unified Access Gateway\von\PortalHomePage\Data\SiteMap\Toolbar, and copy the web.sitemap file to the ...\PortalHomePage\Data\SiteMap\Toolbar\CustomUpdate folder.
2.In the CustomUpdate folder, open the web.sitemap file, and locate the line <!--<siteMapNode url="~/OfflineInstaller.msi?type=Basic".
3.Remove the comment from the start of the line.
Copy Code <siteMapNode url="~/OfflineInstaller.msi?type=Basic"
title="$Resources:Resource, 114"
description="$Resources:Resource, 114"
imageUrl="~/images/ToolBar/offlineInstallation.gif"
DisplayMode="OnlyImage"
target="_blank" />4.Set the OfflineInstaller type:

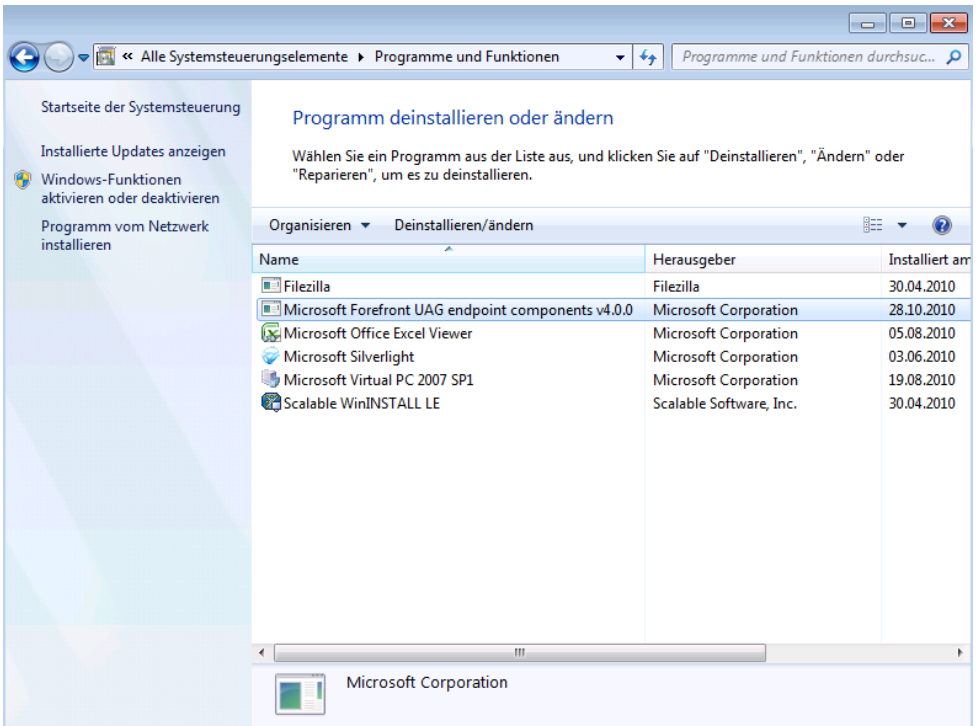
Basic—Installs the basic components: Endpoint Session Cleanup, Client Trace Utility, Endpoint Detection, SSL Application Tunneling ActiveX component.
NetworkConnector—Installs the basic components and the SSL Network Tunneling (Network Connector) component.
NetworkConnectorOnly—Installs only the SSL Network Tunneling (Network Connector) component, without the basic components.
SocketForwarder—Installs the basic components and the Socket Forwarding component.
All—Installs all endpoint components: basic components, SSL Network Tunneling (Network Connector) component, and Socket Forwarding component.

```
<!-- Copy the file to the CustomUpdate folder and uncomment the next siteMapNode to add a button to the toolba
<!--<siteMapNode url="~/OfflineInstaller.msi?type=Basic"
        title="$Resources:Resource, 114"
        description="$Resources:Resource, 114"
        imageUrl="~/images/ToolBar/offlineInstallation.gif"
        DisplayMode="OnlyImage"
        target="_blank" /> -->
```

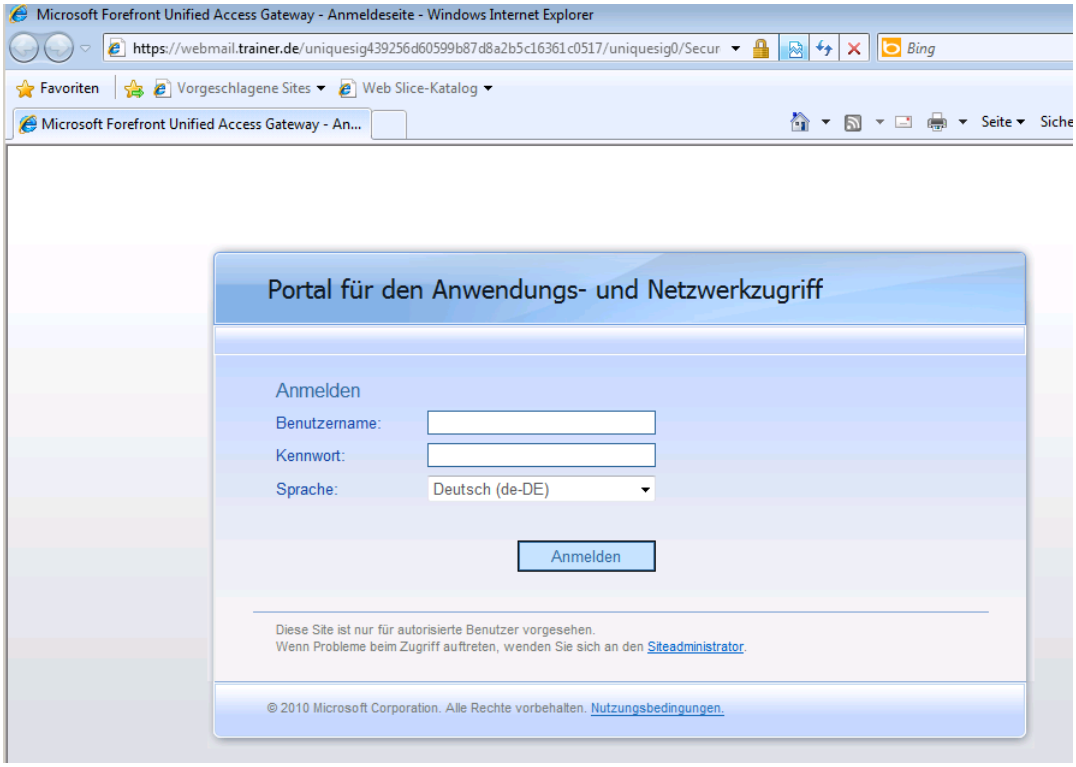
Ergebnis des Patchen



Die installierten Endpoint Komponenten koennen ueber die Systemsteuerung des Clients wieder deinstalliert werden:



Dann ist der Portalaufruf endlich moeglich

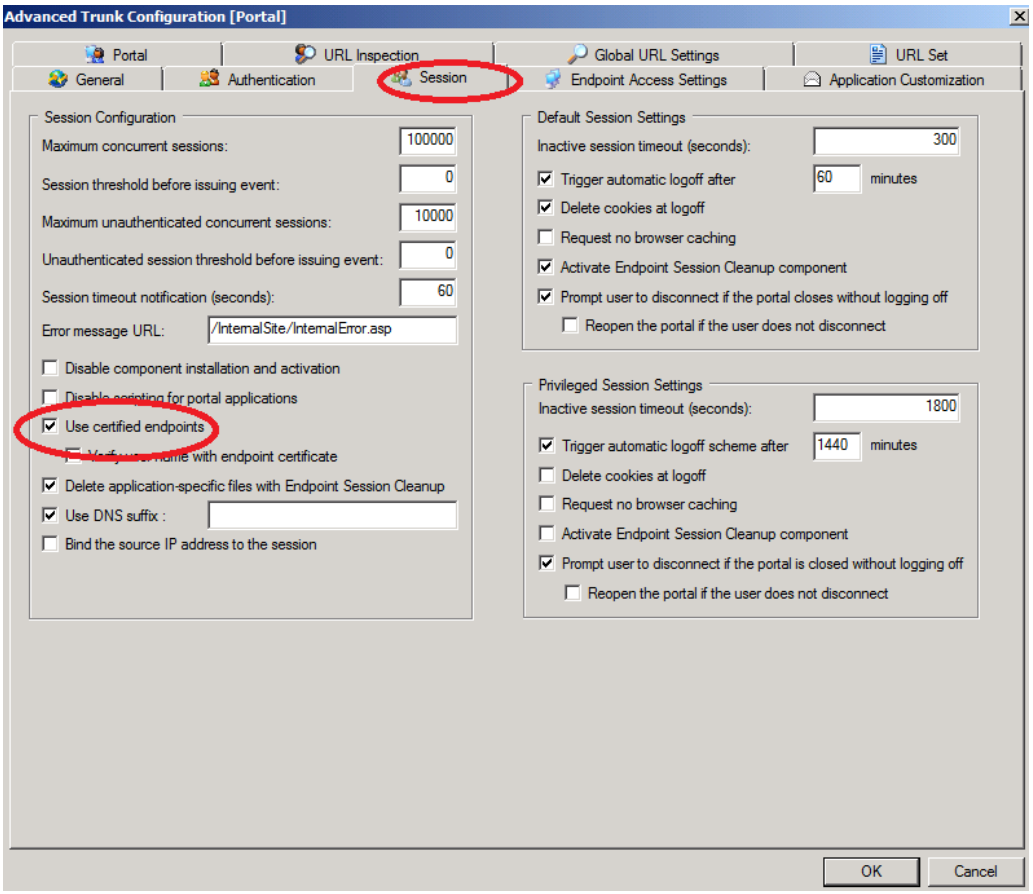


Client Informationen, im Portalzugriff auswaehlbar.

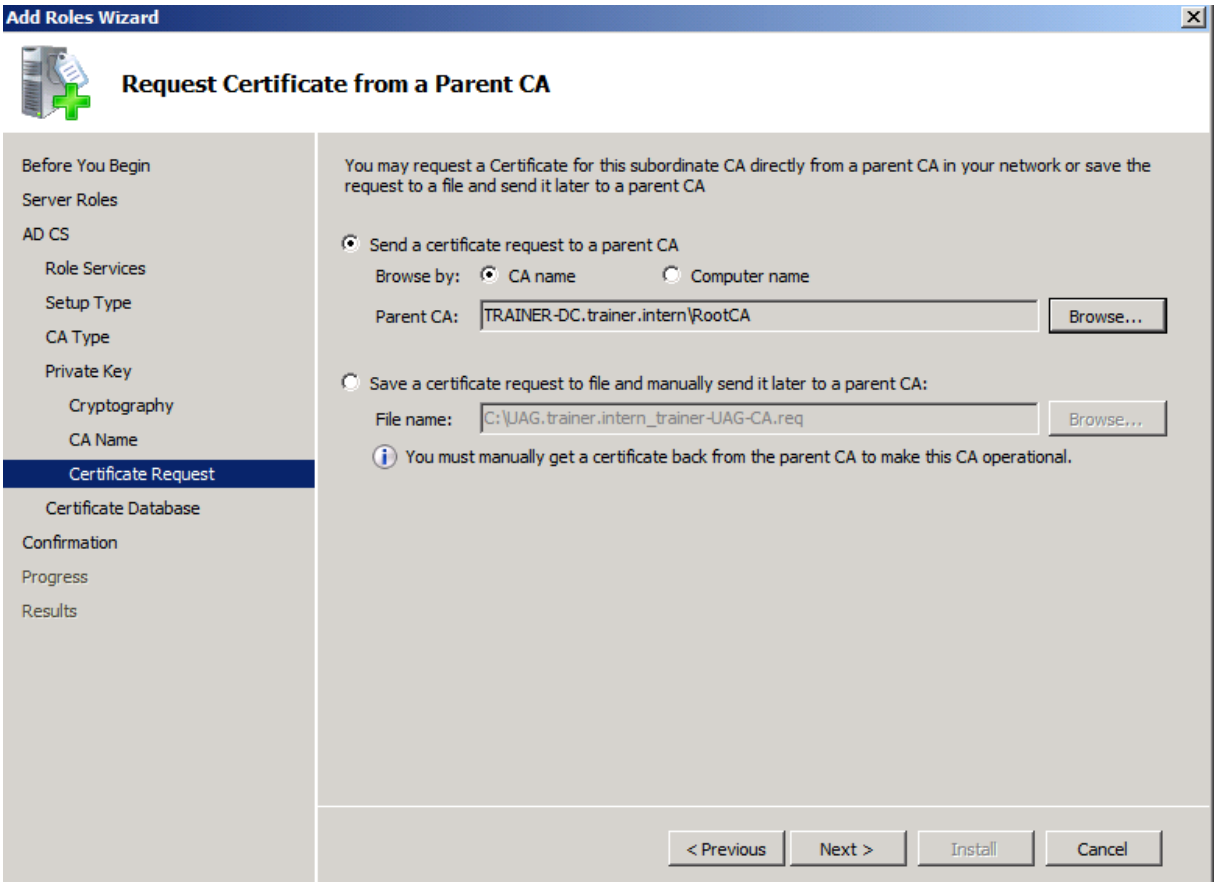
Privilegierter Endpoint

Wie wird aus einem nicht priviligierten Endpoint ein privilegierter Endpoint?
Ein zertifizierter Endpoint im Forefront UAG Jargon ist ein Endgeraet mit einem Zertifikat (Vorlage Computerzertifikat), welches von einer internen Zertifizierungsstelle ausgestellt wurde.

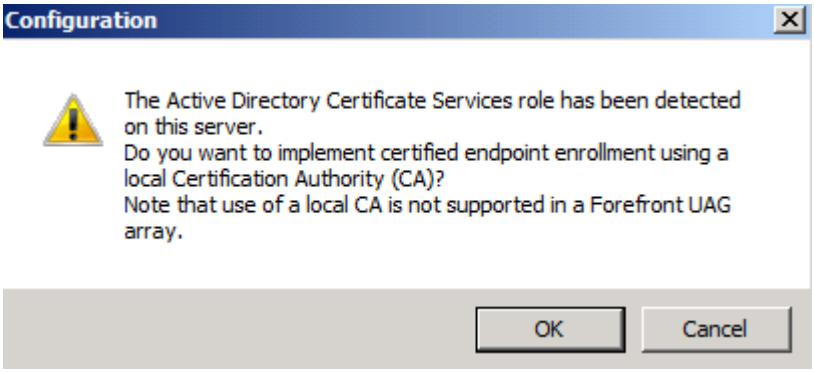
In den Trunk-Einstellungen kann auf der Registerkarte die Einstellung fuer privilegierte Endpoints aktiviert werden.



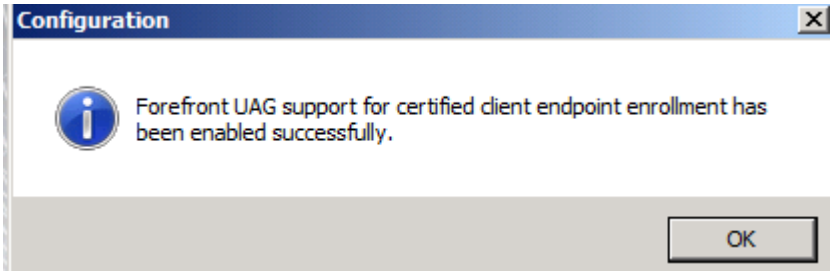
Achtung: Fuer die Privileged Endpoint Features MUSS eine CA installiert werden, eine Standalone CA geht nicht und wenn die CA lokal auf dem UAG installiert werden soll und UAG im Array betrieben wird. Wenn UAG im Array betrieben wird, kann die Certified Endpoint Enrollment Application nicht genutzt werden! :-(



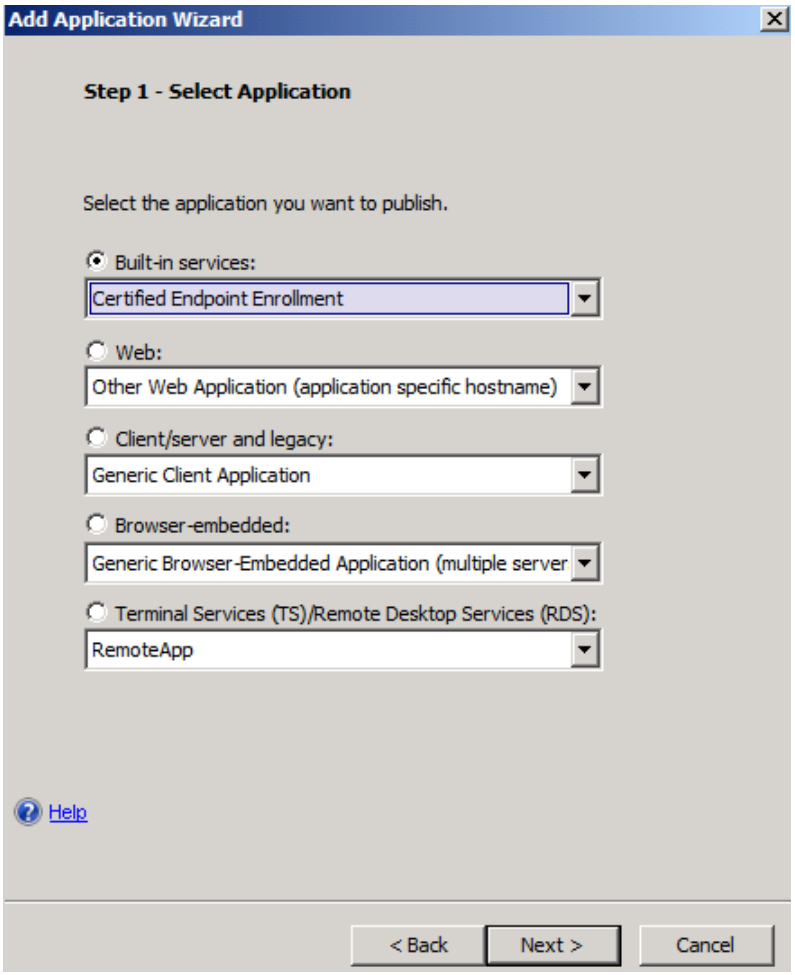
Aha, welche Firmenmgebungen das wohl nutzen (werden).



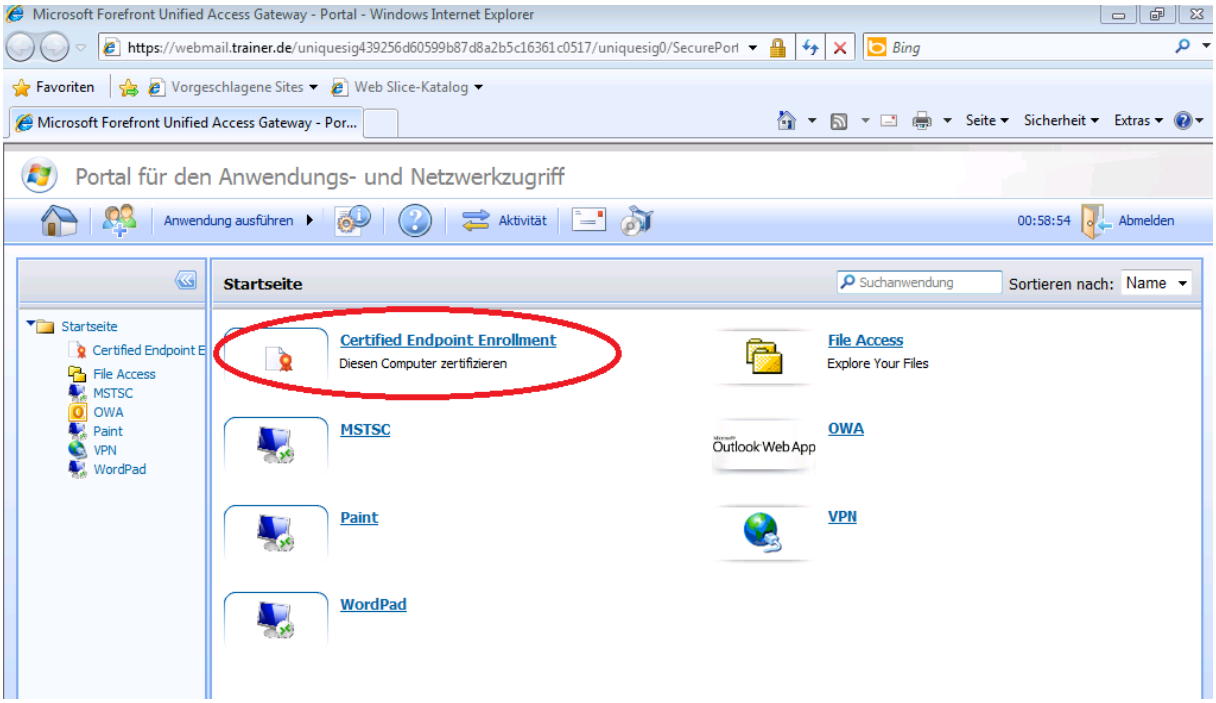
Prima



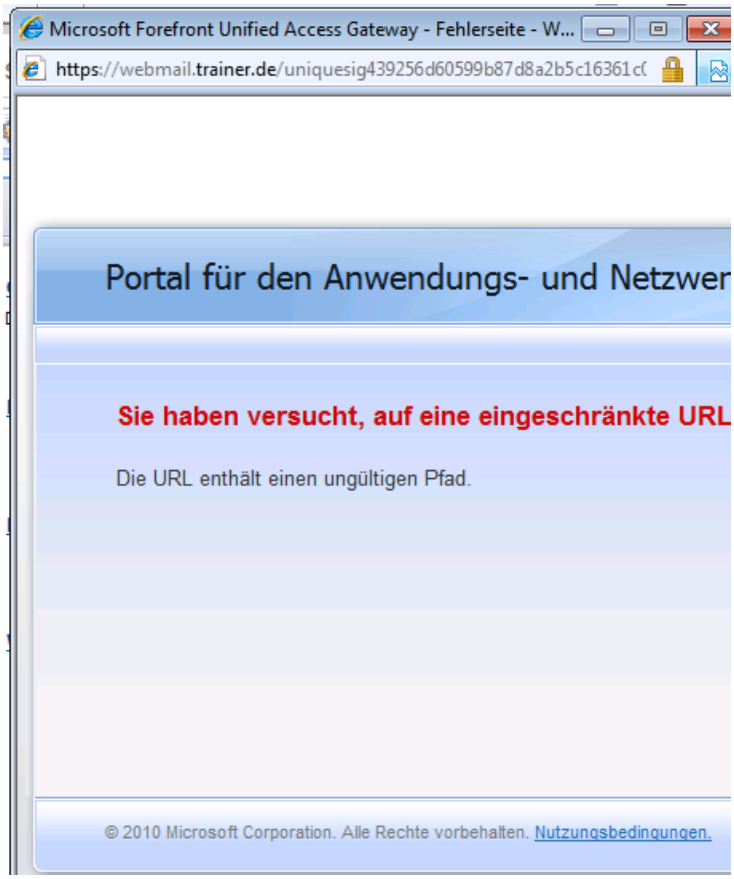
Certified Endpoint Enrollment in der UAG MMC unter den Built-In Services auswaehlen



Zertifizieren wir mal den Computer



Fehlermeldung ☹



Warning	12/02/2010 12:29:32	67	URL Path Not Allowed	Security	portal (S)	UAG	A request from source IP addr 212.212.10.120, user marcim portal; Secure=1 for applicatio Desktop Services of type TerminalServicesGateway fail URL /certifiedendpointenrollm type=0&Site=Portal contains a The rule applied is Default rul GET.

Hotfix:
http://support.microsoft.com/kb/981506/en-us

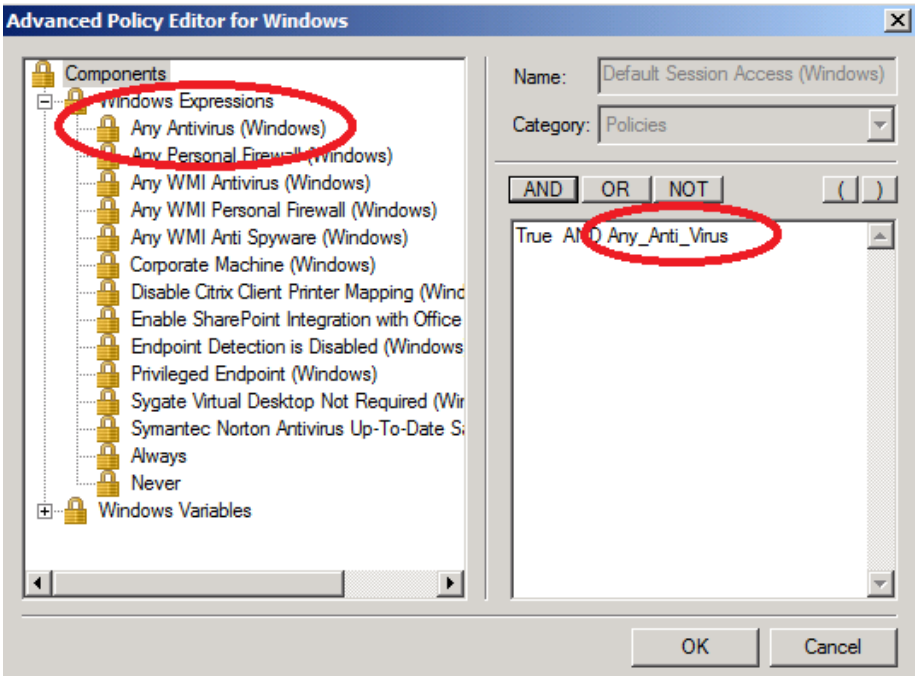
Der Benutzer muss auf den „Submit“ Button klicken und das Zertifikat „installieren“ . Das Computerzertifikat wird jetzt im Zertifikatspeicher installiert. Danach kann das Endgeraet als privilegierter Endpoint fungieren (wenn denn die Privileged Endpoint Policies mitspielen) ☺

Was ein zertifiziertes Geraet ist, muss ich noch herausfinden ☺

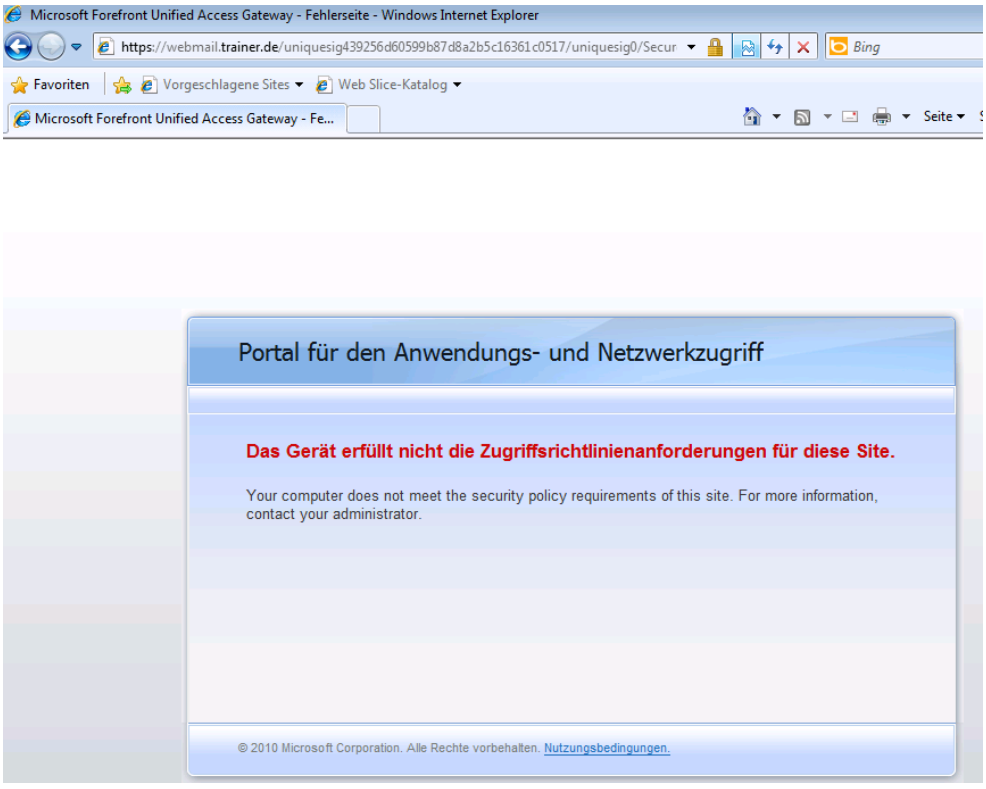
Bemerkung: Auch ohne das Zertifikat Enrollment von UAG kann ein Client ein privilegiertes Endgeraet sein, wenn ein entsprechendes Computerzertifikat der internen CA installiert ist!

Anpassung der Endpoint Access Polies

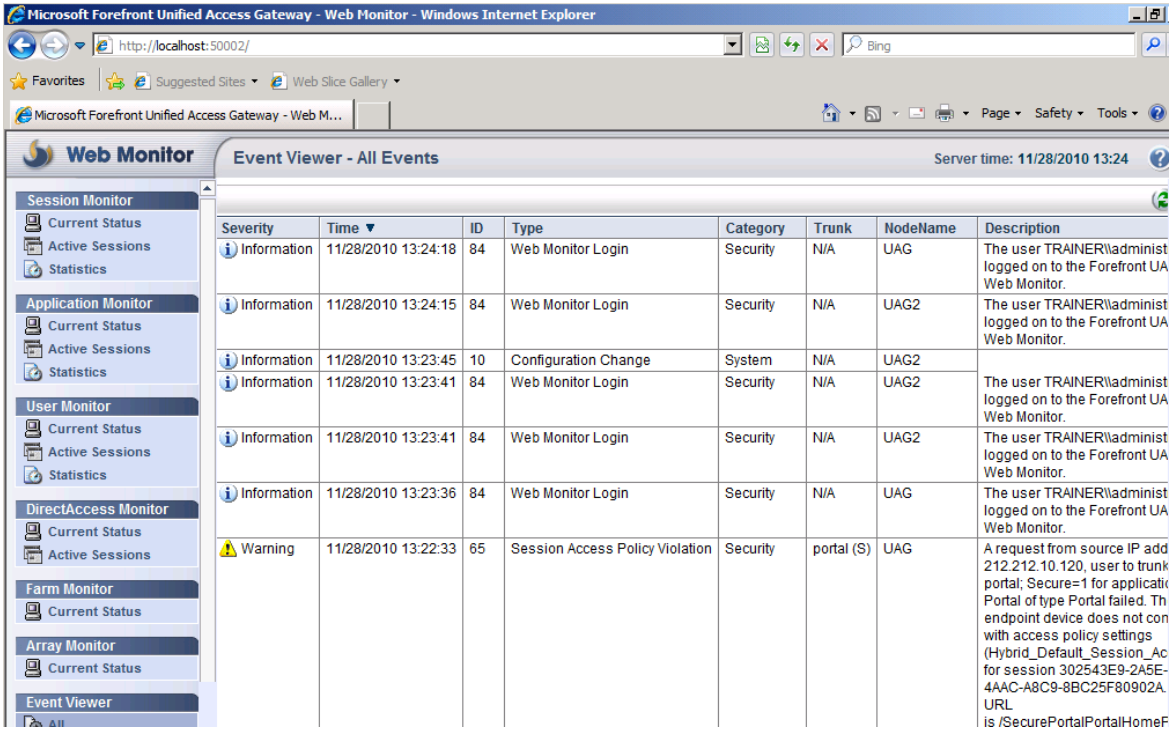
In diesem Beispiel aendern wir die Endpoint Access Policy dahingehend, dass auch noch eine beliebige Antivirus-Anwendung auf dem Endgeraet installiert sein muss. Da das bei dem Client in diesem Fall nicht der Fall ist, ist die Nutzung des Portals nicht moeglich.



Nach Speicherung und Aktivierung der UAG Policies kann das Endgeraet nicht mehr auf das UAG Portal zugreifen.

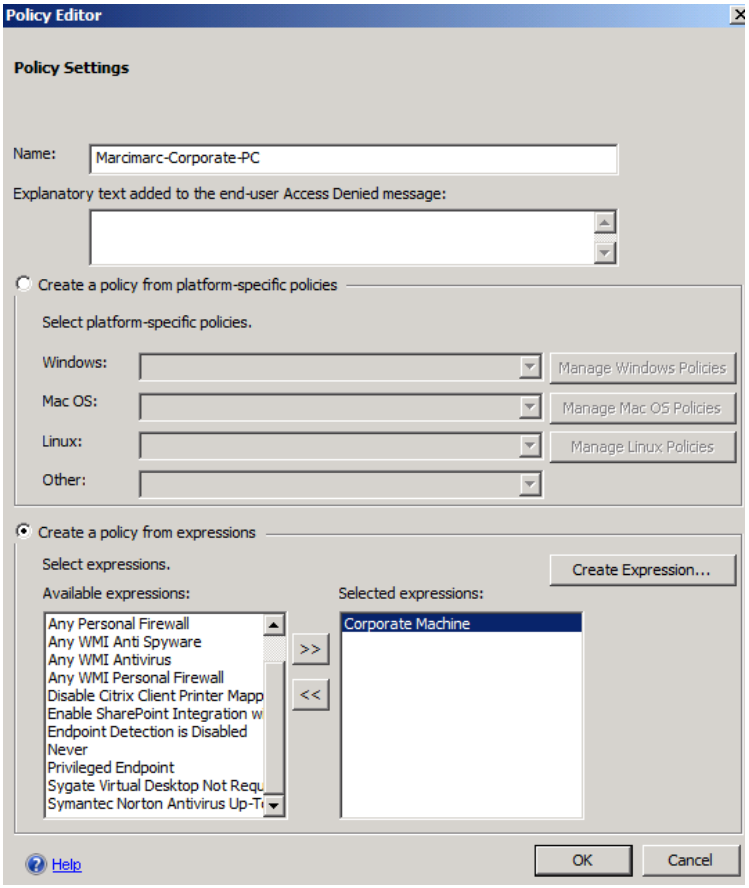


Der verweigerte Zugriff auf das Portal kann im Forefront UAG Webmonitor ueberwacht werden.

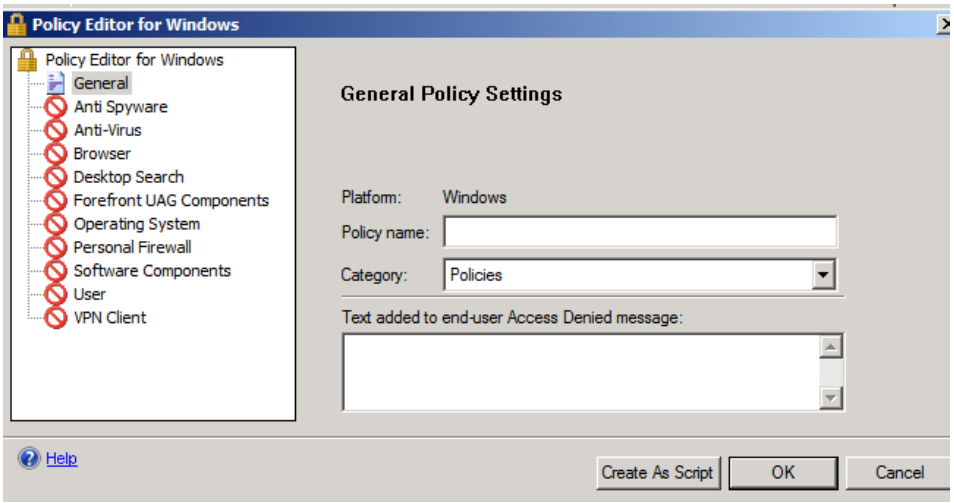


Erstellung eigener Forefront UAG Endpoint Access Policies

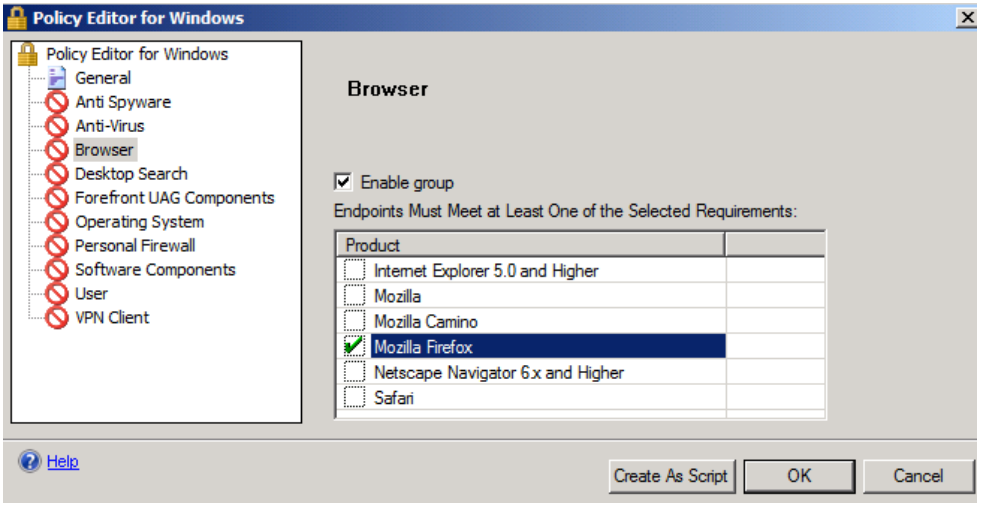
Wem die Standard Forefront UAG Richtlinien nicht ausreichen, kann eigene Policies erstellen, um diese auf die Beduerfnisse der Firma anzupassen. Neue Policies koennen fuer die jeweilige Betriebssystemplattform oder anhand von Expressions, erstellt werden.



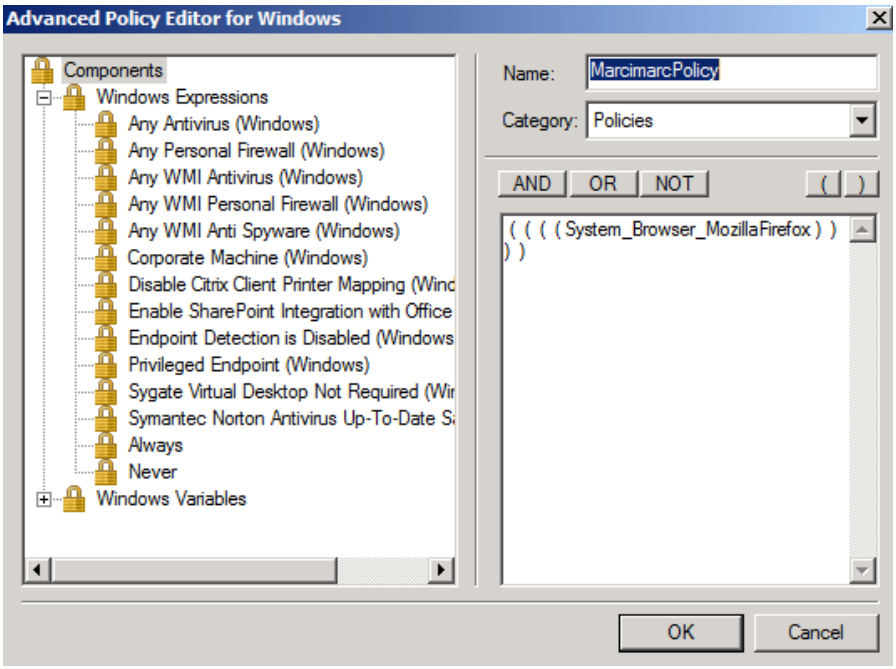
Mit dem Policy Editor fuer Windows koennen eigene Policies erstellt und konfiguriert werden und nach belieben Policies erstellt werden, um Zugriffe von Clients zu steuern.



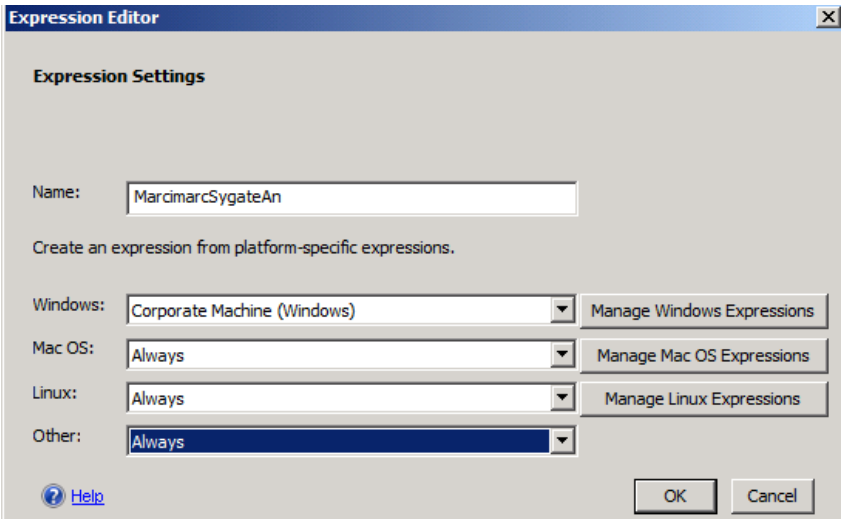
Nach Erstellung der entsprechenden Policy muss diese aktiviert werden (die Gruppe aktiviert werden).

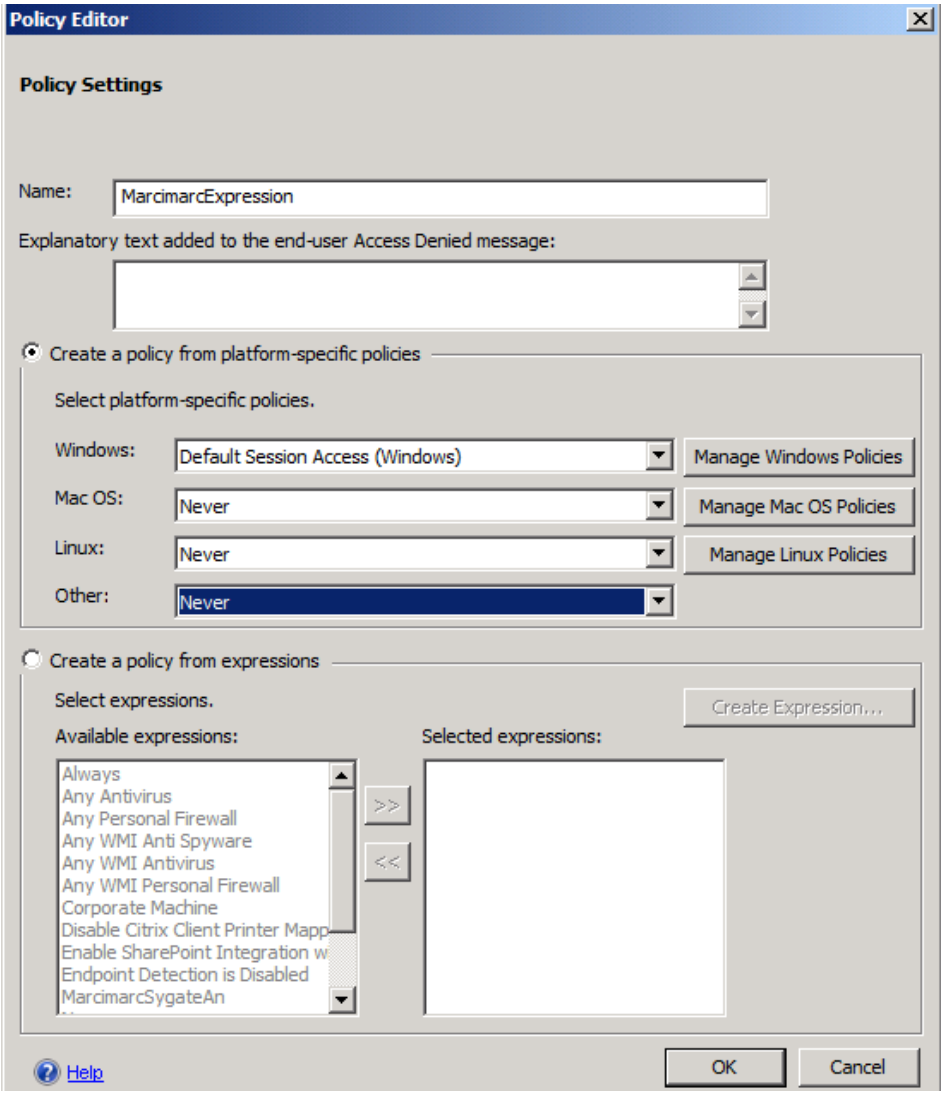


Das Ergebnis des Policy Editors ist dann die folgende Policy, wo zum Beispiel nur Mozilla Firefox als zulaessiger Browser verwendet werden darf.

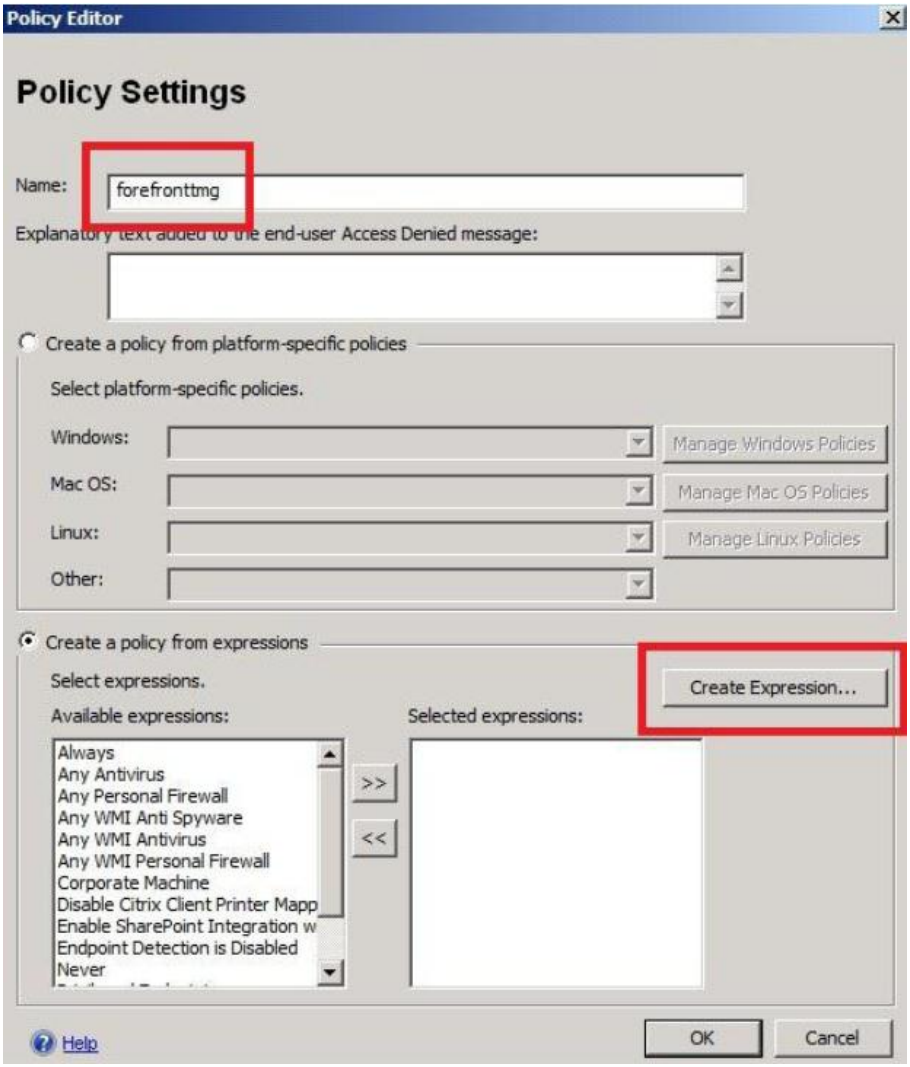


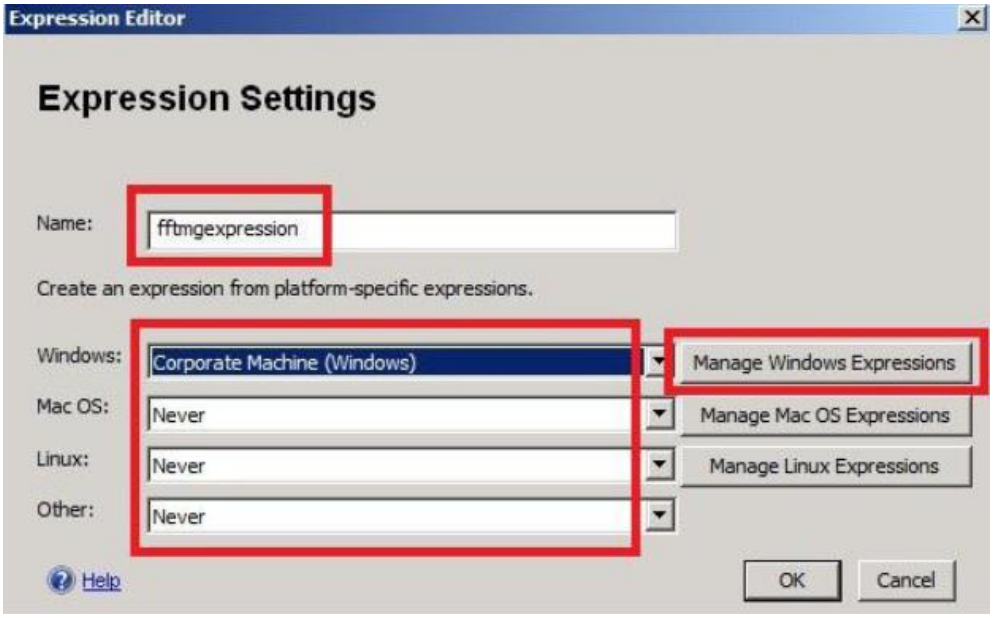
Es koennen auch eigene Expressions erstellt werden und diese dann in den Policies aktiviert werden.

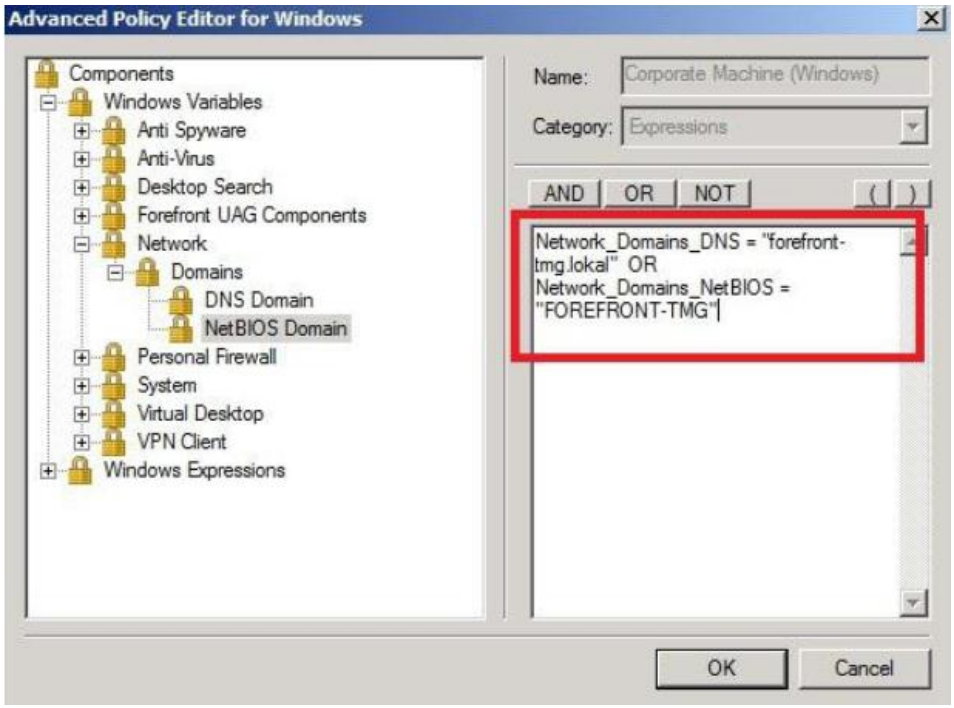


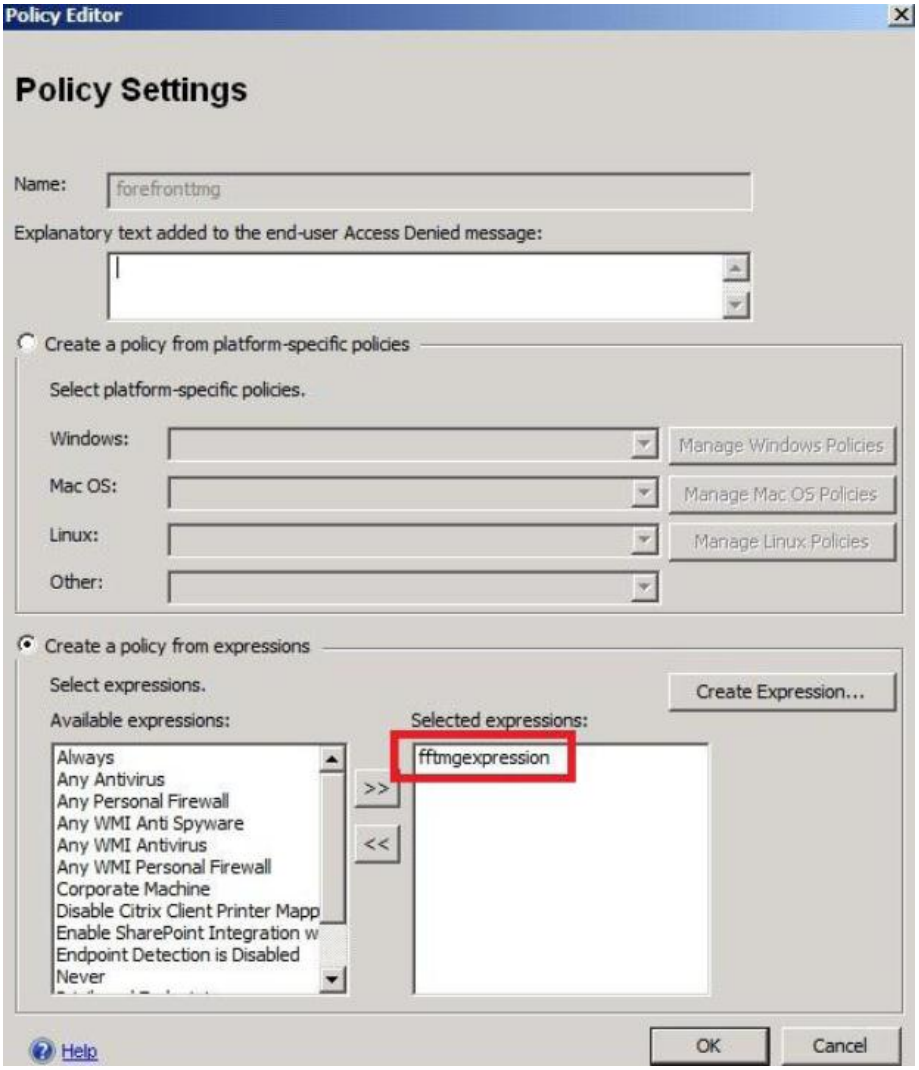


Mein Kollege und Freund Karsten Hentrup hat auch mal eine Policy gebaut, wo der Corporate Client abgefragt wird und nur Clients mit Domaenenmitgliedschaft Zugriff erhalten.






Advanced Policy Editor for Windows
Components
Windows Variables
Anti Spyware
Anti-Virus
Desktop Search
Forefront UAG Components
Network
Domains
DNS Domain
NetBIOS Domain
Personal Firewall
System
Virtual Desktop
VPN Client
Windows Expressions
Name:
Corporate Machine (Windows)
Category:
Expressions
AND
OR
NOT
( )
Network_Domains_DNS = "forefront-tmg.lokal" OR Network_Domains_NetBIOS = "FOREFRONT-TMG"
OK
Cancel


Policy Editor
Policy Settings
Name:
forefronttmg
Explanatory text added to the end-user Access Denied message:
Create a policy from platform-specific policies
Select platform-specific policies.
Windows:
Manage Windows Policies
Mac OS:
Manage Mac OS Policies
Linux:
Manage Linux Policies
Other:
Create a policy from expressions
Select expressions.
Create Expression...
Available expressions:
Selected expressions:
Always
Any Antivirus
Any Personal Firewall
Any WMI Anti Spyware
Any WMI Antivirus
Any WMI Personal Firewall
Corporate Machine
Disable Citrix Client Printer Mapp
Enable SharePoint Integration w
Endpoint Detection is Disabled
Never
fftmgexpression
>>
<<
Help
OK
Cancel

Ergebnis


Portal für den Anwendungs- und Netzwerkzugriff
Anwendung ausführen
Aktivität
00:59:55
Abmelden
Startseite
Suchanwendung
Sortieren nach:
Name
Startseite
AssAssAllWiePlAn
Axtschänsch
Intranet
Schöne Filez hier!
Sharepoint
AssAssAllWiePlAn
Outlook Web App
Axtschänsch
Intranet
Schöne Filez hier!
Explore Your Files
Sharepoint
SharePoint Server 2010