

Forefront UAG Endpoint Access Policies

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

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

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

- Betriebssystemspezifische Einstellungen
- Einstellungen anhand von Expressions

Betriebssystemspezifische Einstellungen

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

Einstellungen anhand von Expressions

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

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

- Session Access Policy
- Privileged Endpoint Policy

Session Access Policy

Die Session Access Policy definiert die Bedingungen welche erfüllt sein müssen, damit ein Endgerät Zugriff auf Unternehmensanwendungen erhalten kann.

Privileged Endpoint Policy

Definiert die Bedingungen, welche erfüllt sein müssen, 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&%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.

The screenshot displays the Microsoft Forefront Unified Access Gateway Management console. The main window is titled "Portal" and contains several configuration sections:

- External Site Name:** Specifies the name that clients type in the browser to access the site. Public host name: Port:
- External Site Address:** HTTPS Port: Virtual IP: Add
- Do not use integrated NLB:** Array Member | IP
UAG (local) | 212.212.10.111
UAG2 | *.*.*.*
- Initial Internal Application:** Portal home page: Display home page within portal frame
- Trunk Configuration:** Configure trunk settings:

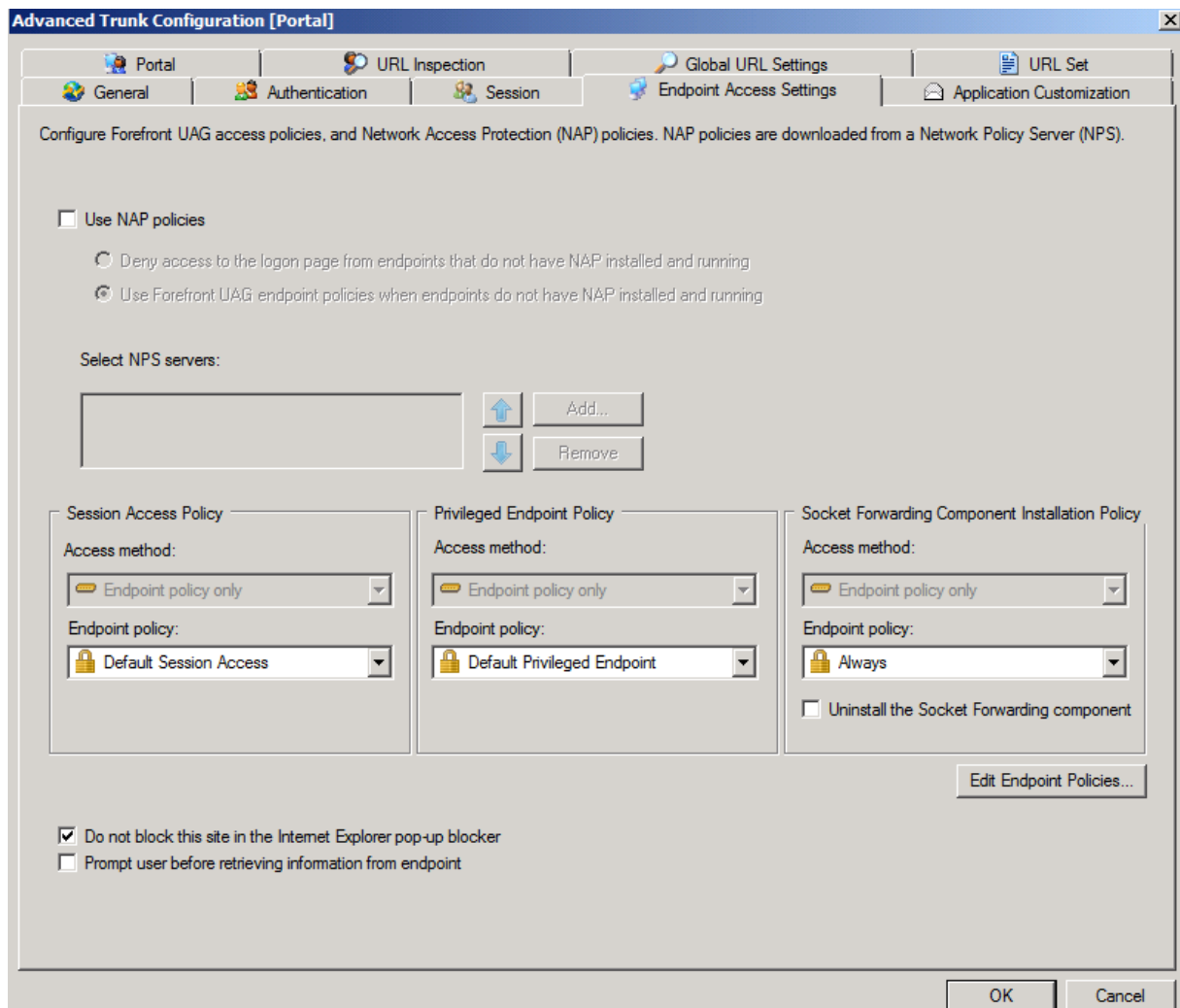
The right-hand side of the console shows a table of Applications:

Application Name	Application Type
Portal	Portal
OWA	Microsoft Exchange Server ...
RemoteApp	RemoteApp
MSTSC	Remote Desktop (User defi...
VPN	Remote Network Access
File Access	File Access

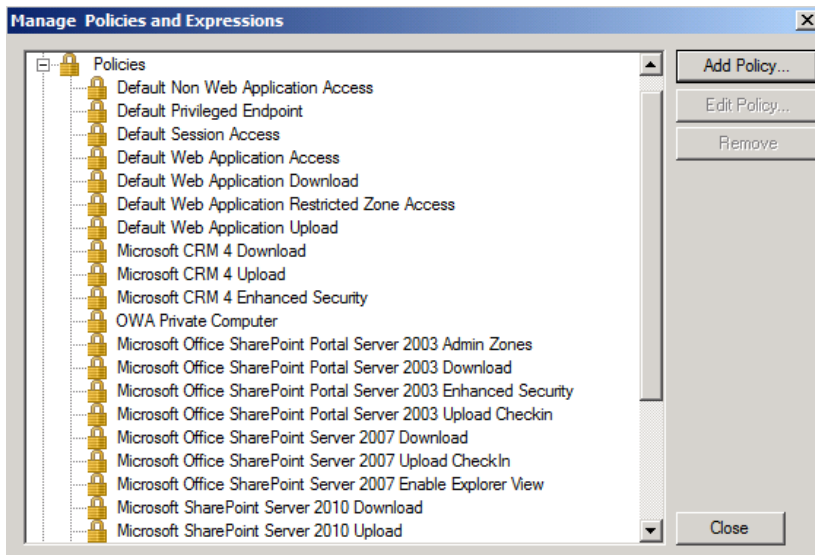
Below the Applications table are buttons for "Add...", "Edit...", and "Remove".

At the bottom, there is a section for "Limit applications to the following subnets:" with a table for Subnet Address and Subnet Mask, and buttons for "Add...", "Edit...", and "Remove".

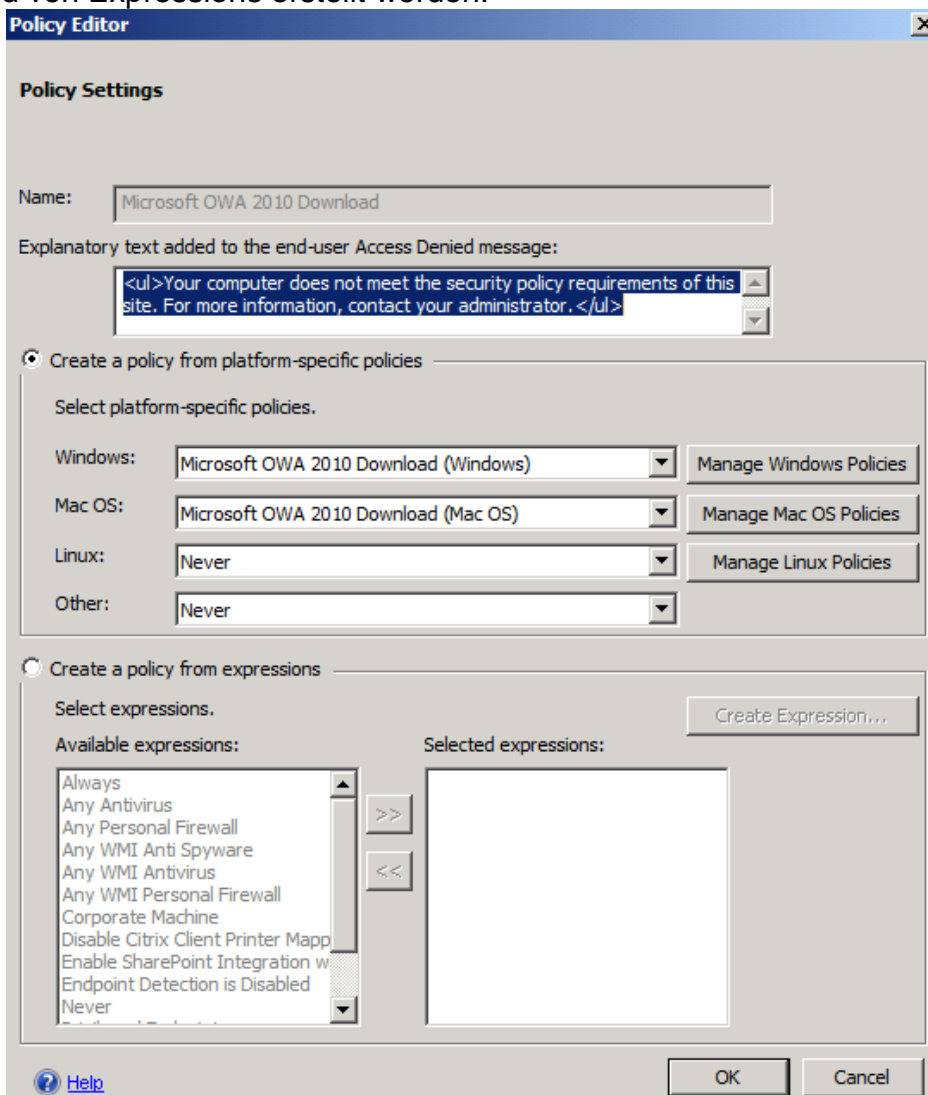
Auf der Registerkarte Endpoint Access Settings koennen dann unterschiedliche Endpoint Access Polices eingerichtet werden, welche im spaeteren Verlauf dieses Artikels noch erlaeutert werden.



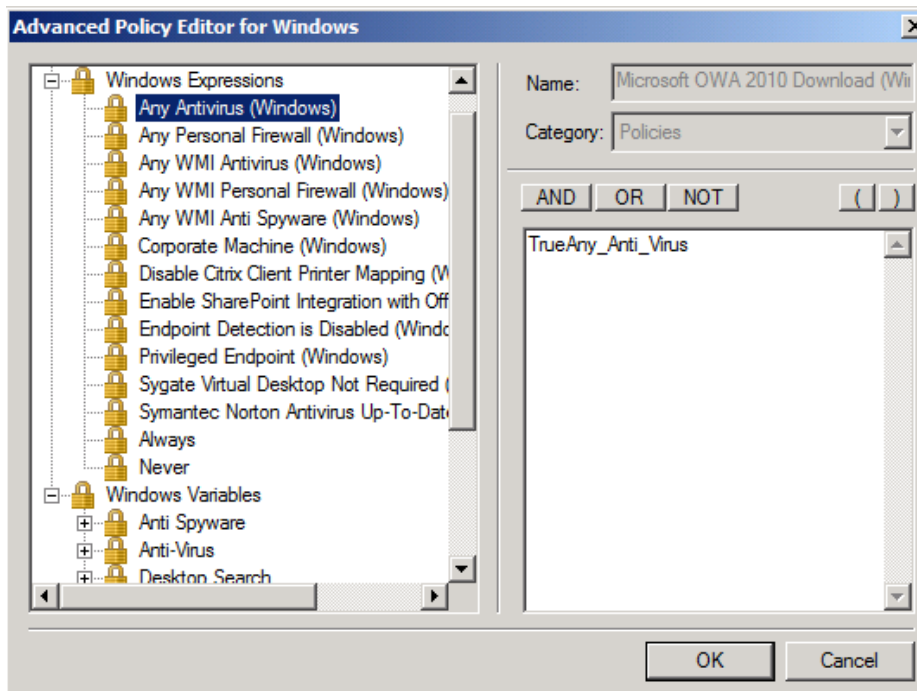
Es stehen eine Reihe von vordefinierten Richtlinien und Expressions zur Verfuegung, welche modifiziert werden koennen, aber auch neue Policies erstellt werden koennen.



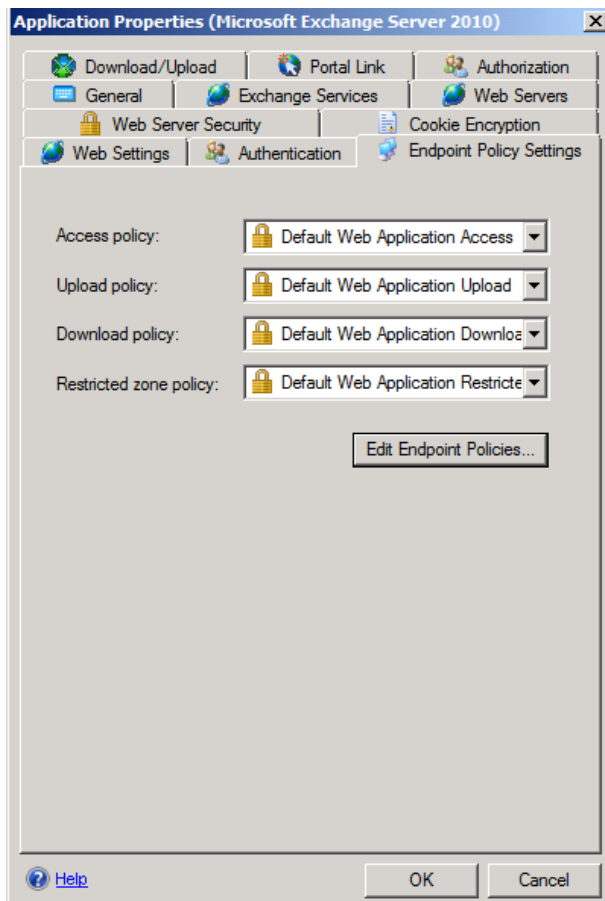
Wie bereits weiter oben in diesem Artikel erwahnt, koennen betriebssystemspezifische Policies erstellt und genutzt werden, aber auch Policies anhand von Expressions erstellt werden.



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 Applikationen innerhalb des Portals koennen dann, wie weiter oben in diesem Artikel erwaeht, 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.

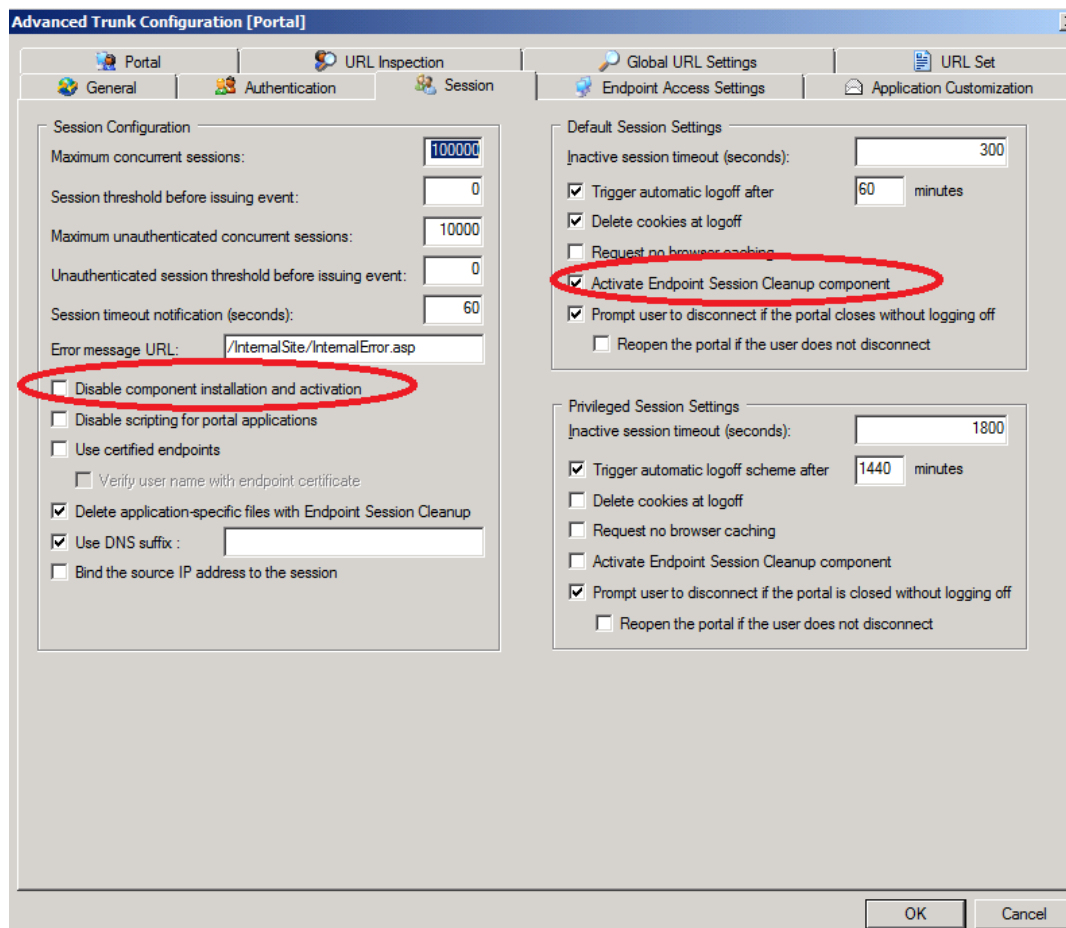
The SSL tunneling components are:

- 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

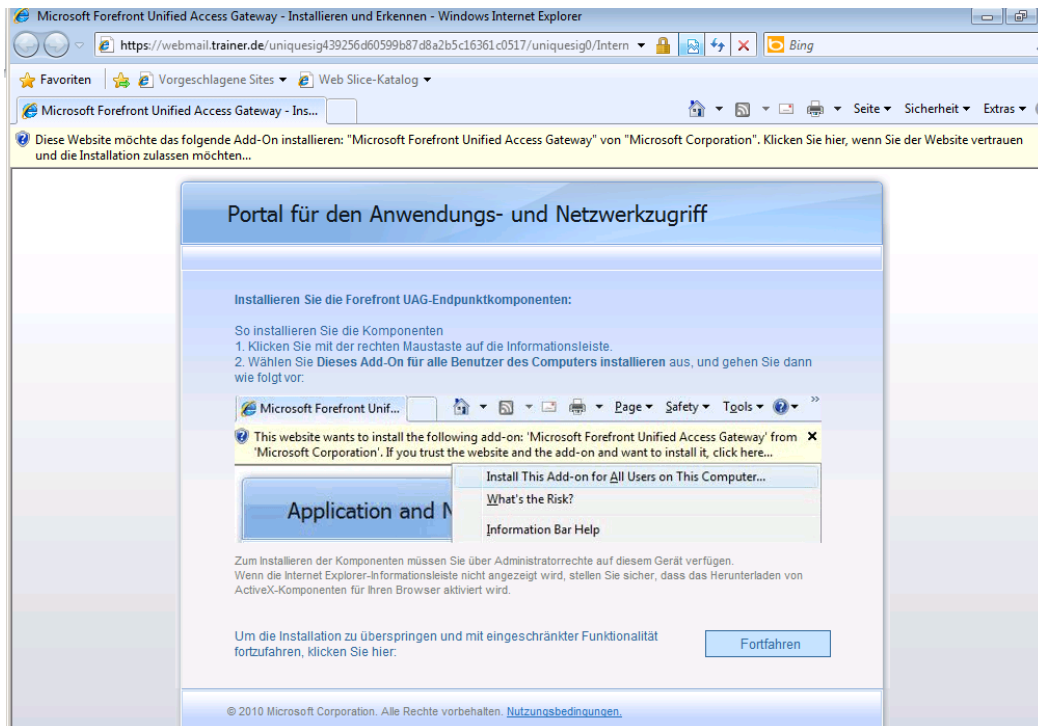
Socket Forwarding Helper—Used for support purposes.

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

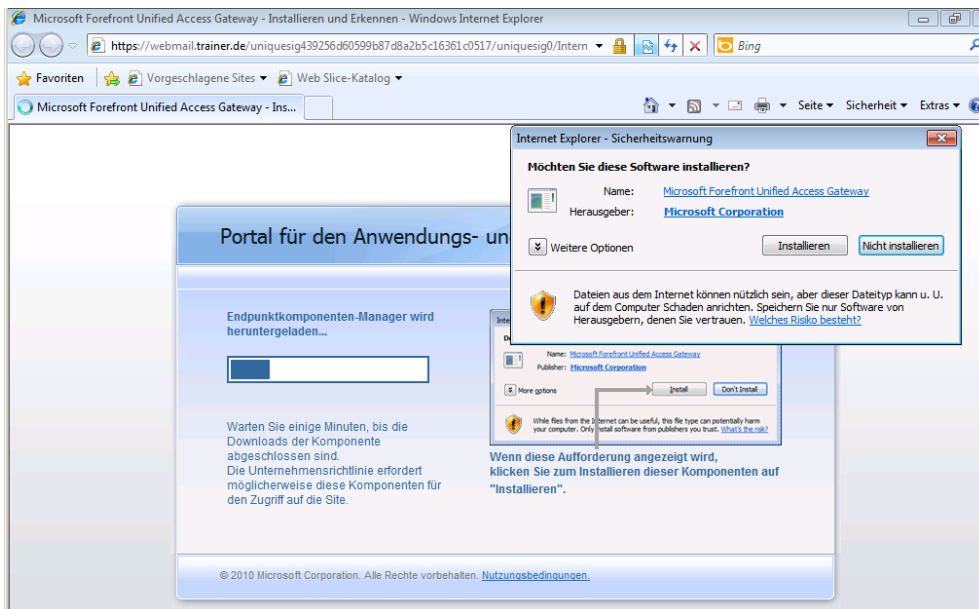
Die Installation der Komponenten beim Aufruf der Portal Webseite ist automatisch aktiviert und kann in den Portaleigenschaften modifiziert werden:



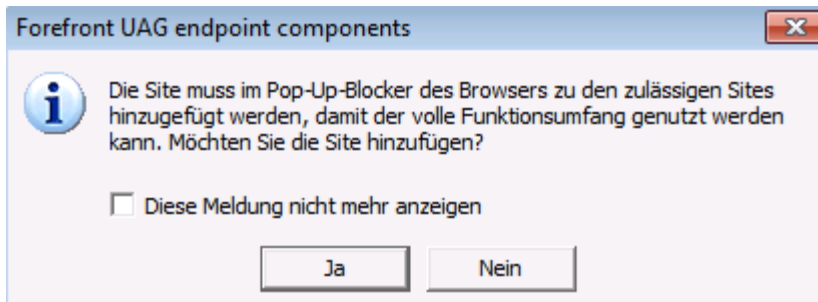
Beim ersten Aufruf des Portals wird dann zur Installation der UAG-Endpunktkomponenten aufgefordert:



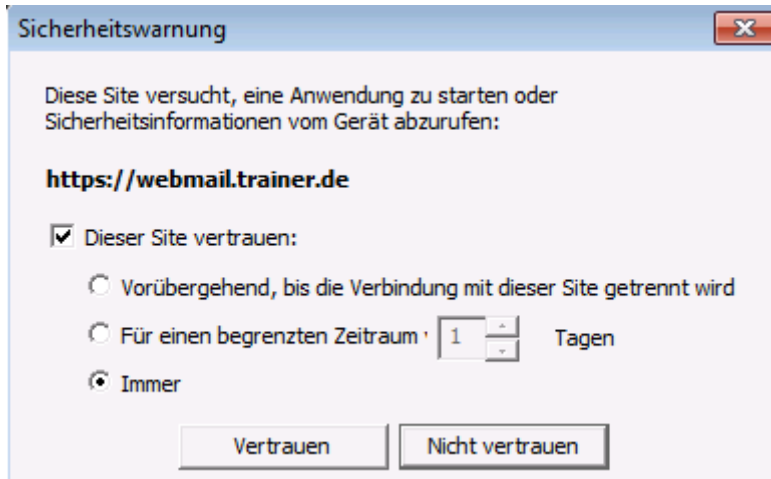
Die Installation der Endpoint Komponenten nimmt einige Zeit in Anspruch, einige Popupdialoge muessen bestaetigt werden.



Ja, raus aus dem Popup Blocker



Ja, immer vertrauen.



Reg hacks

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

```
CheckSite.reg - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\WhaleCom\Client
\CheckSite]
"Managed"=dword:00000001
"CanAddSites"=dword:00000001
"CanAddHttpSites"=dword:00000000
"PromptInvalidCertTrusted"=dword:00000000
"PromptInvalidCertUntrusted"=dword:00000001
"TrustedSite0"="https://webmail.forefront-tmg.de"
```

```
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

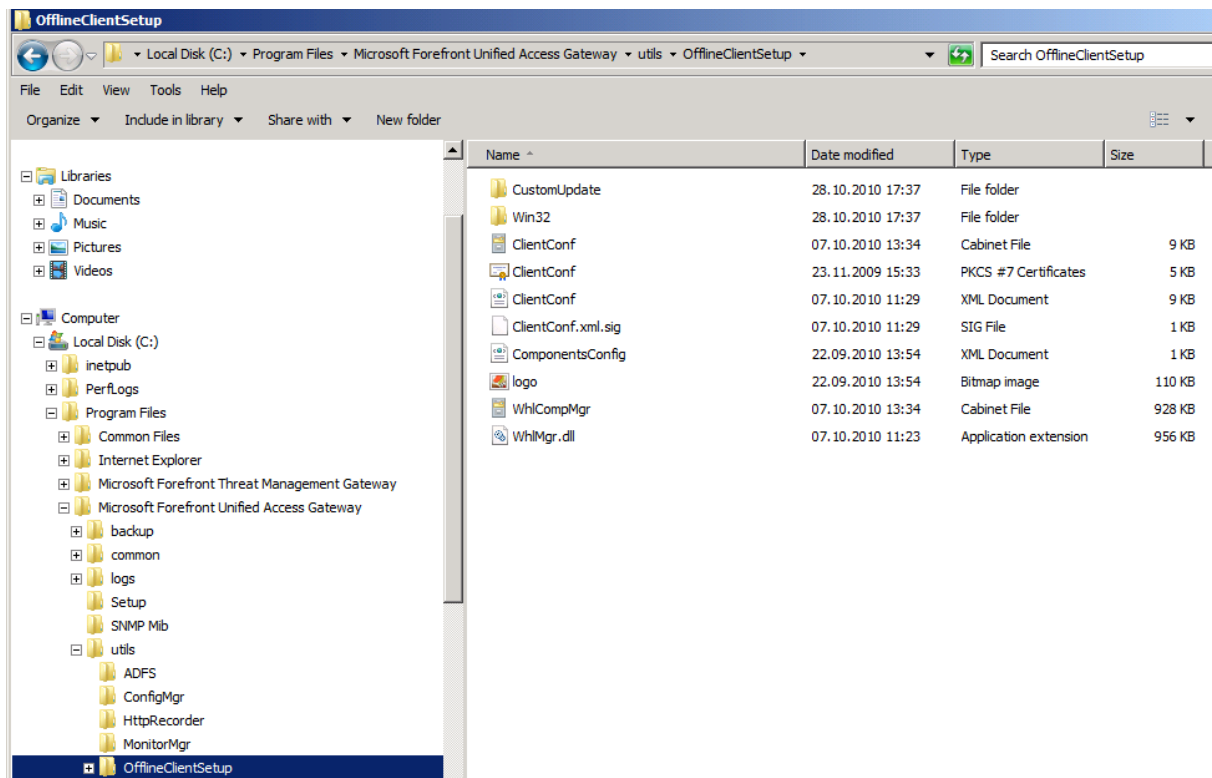
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\SharedAccess\Parameters\FirewallPolicy
\StandardProfile\AuthorizedApplications\List]
"C:\\Programme\\Microsoft Forefront UAG\\Endpoint
Components\\3.1.0\\WhlCInt3.exe"="C:\\Programme\\Microsoft
Forefront UAG\\Endpoint Components\\3.1.0\\
WhlCInt3.exe*:Enabled:SSL Application Tunneling"
```

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

Name	Date modified	Type	Size
App_Themes	28.10.2010 17:37	File folder	
css	28.10.2010 17:37	File folder	
CustomUpdate	28.10.2010 17:37	File folder	
Data	28.10.2010 17:37	File folder	
images	28.10.2010 17:38	File folder	
Limited	28.10.2010 17:38	File folder	
OMA	28.10.2010 17:38	File folder	
Scripts	28.10.2010 17:38	File folder	
UserControls	28.10.2010 17:38	File folder	
WinCE	28.10.2010 17:38	File folder	
aspnet_menu_workaround	22.09.2010 13:54	HTML Document	1 KB
ContentFrame.aspx	22.09.2010 13:54	ASPX File	3 KB
Default.aspx	22.09.2010 13:54	ASPX File	2 KB
Help.aspx	22.09.2010 13:54	ASPX File	3 KB
MainFrame.aspx	22.09.2010 13:54	ASPX File	2 KB
portalcontainer	28.11.2010 13:47	XML Document	1 KB
PreLogOff.aspx	22.09.2010 13:54	ASPX File	1 KB
Standard.master	22.09.2010 13:54	MASTER File	22 KB
TopFrame.aspx	22.09.2010 13:54	ASPX File	1 KB
Web.config	07.10.2010 12:24	CONFIG File	20 KB
WhlClientSetup-All	07.10.2010 13:14	Windows Installer P...	3.467 KB
WhlClientSetup-Basic	07.10.2010 13:14	Windows Installer P...	3.467 KB
WhlClientSetup-NetworkConnector	07.10.2010 13:23	Windows Installer P...	3.467 KB
WhlClientSetup-NetworkConnectorOnly	07.10.2010 13:04	Windows Installer P...	3.467 KB
WhlClientSetup-SocketForwarder	07.10.2010 13:01	Windows Installer P...	3.467 KB

Ein Offline Client Setup ist verfügbar:



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.

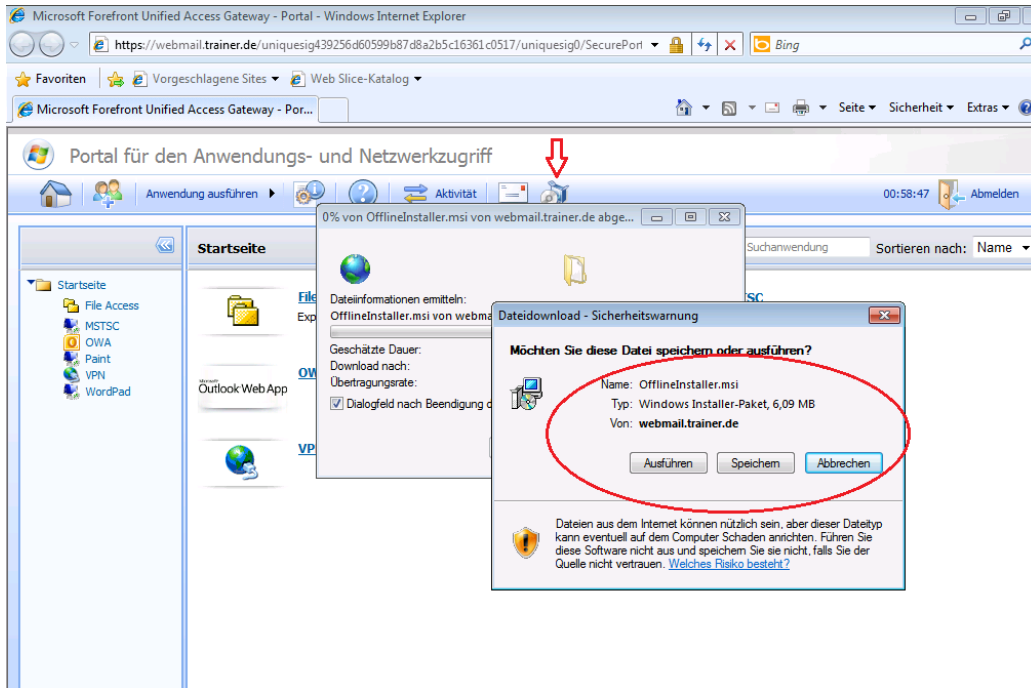
All—Installs all endpoint components: basic components, SSL Network Tunneling (Network Connector) component, and Socket Forwarding component.

```

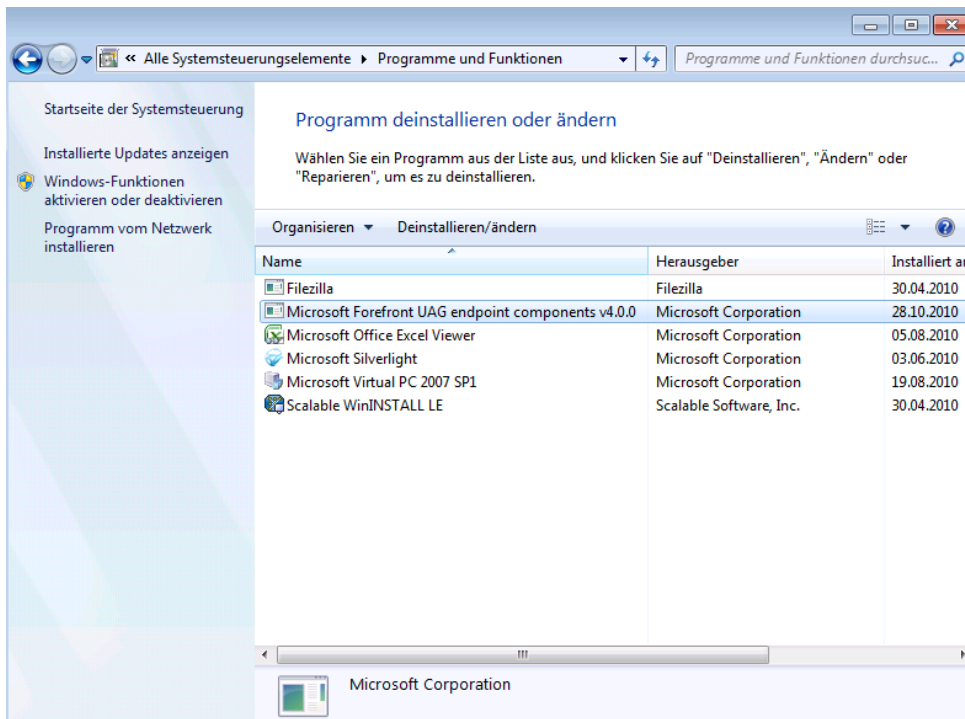
<!-- Copy the file to the Customupdate folder and uncomment the next siteMapNode to add a button to the toolba
<!--<siteMapNode url="/offlineInstaller.msi?type=Basic"
      title="$Resources:Resource, 114"
      description="$Resources:Resource, 114"
      imageUrl="/~/images/ToolBar/offlineInstallation.gif"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

```

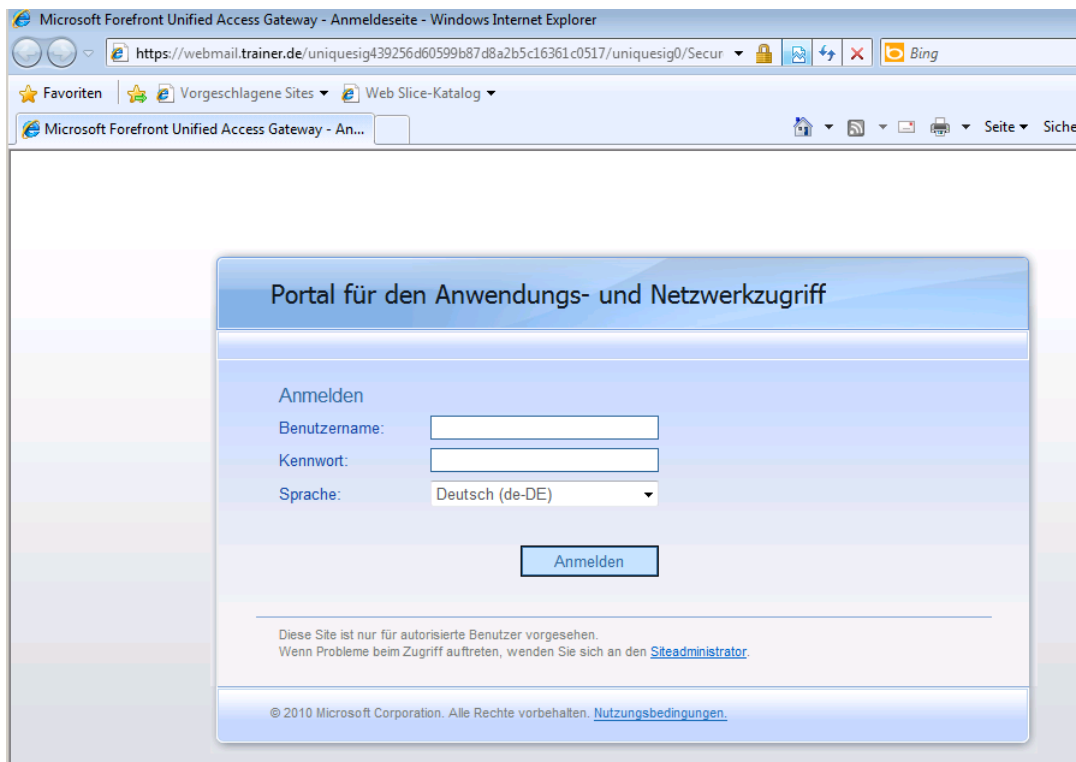
Ergebnis des Patchen



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



Dann ist der Portalaufruf endlich moeglich



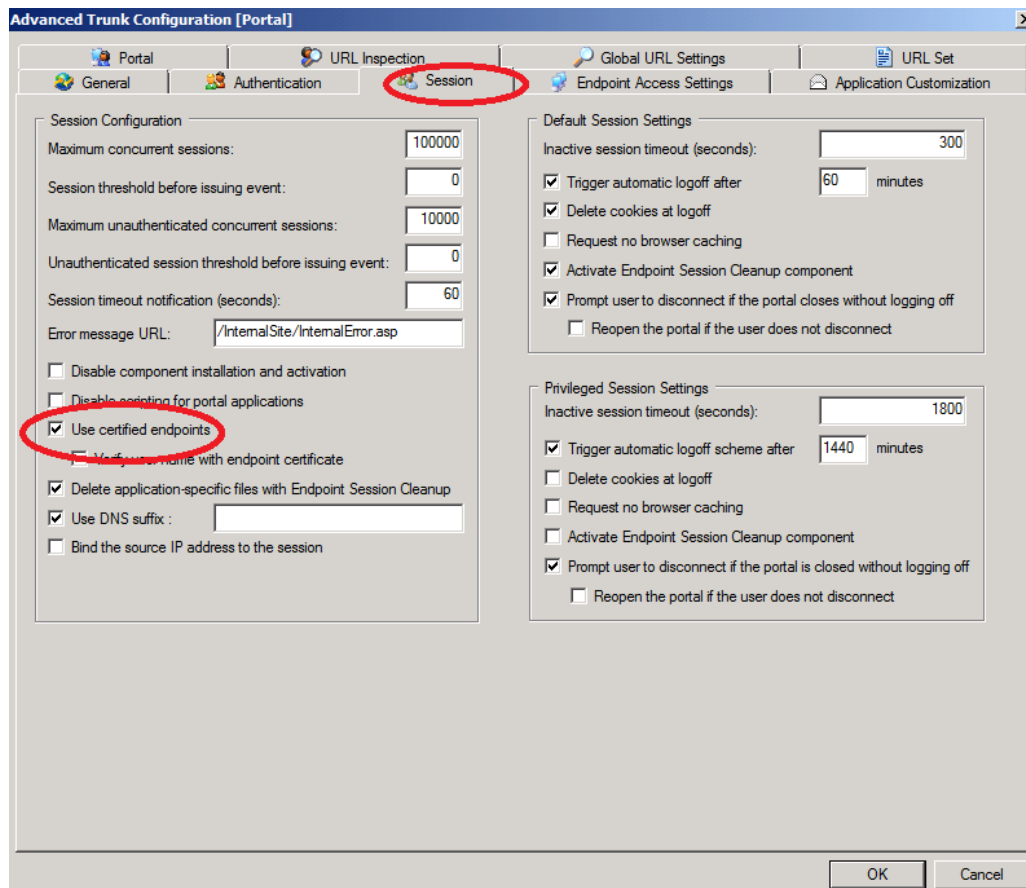
Client Informationen, im Portalzugriff auswaehlbbar.



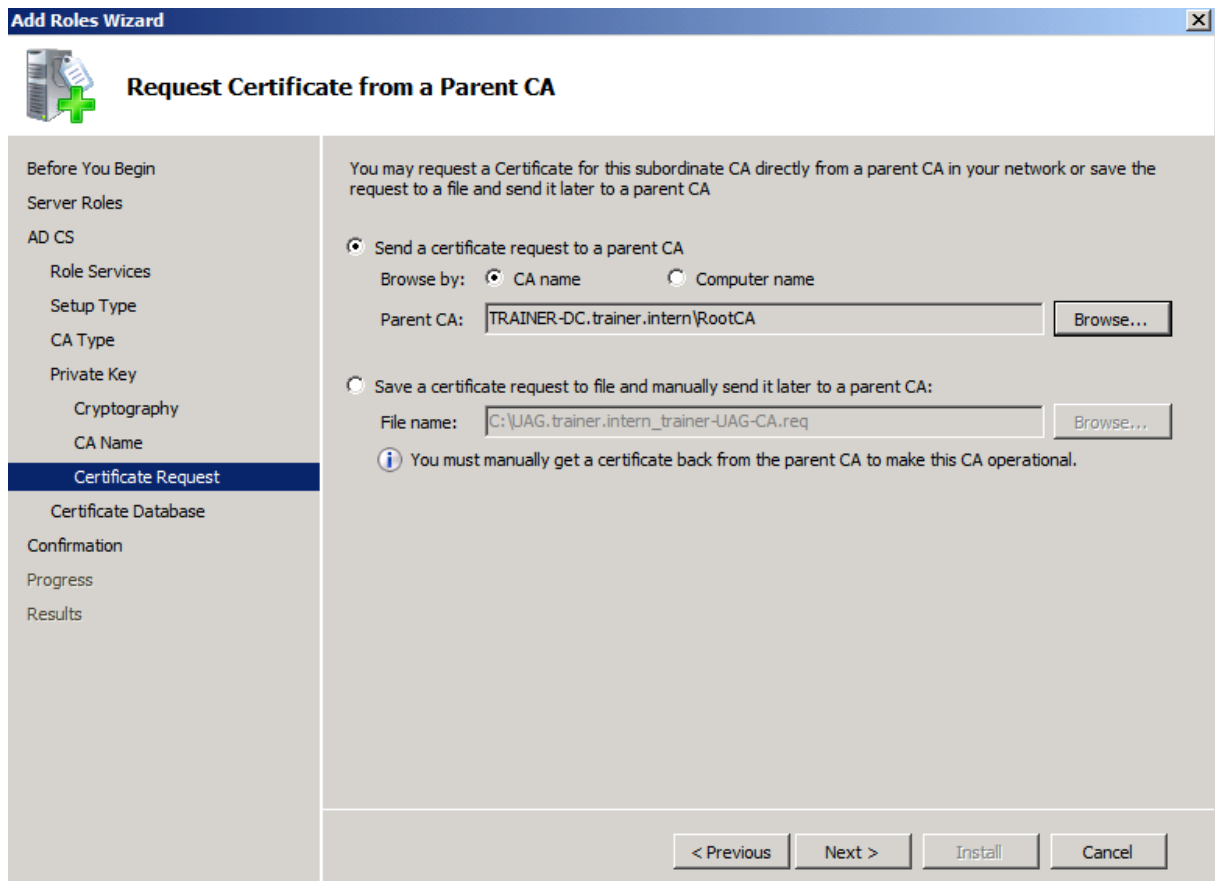
Privilegierter Endpoint

Wie wird aus einem nicht privilegierten 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.

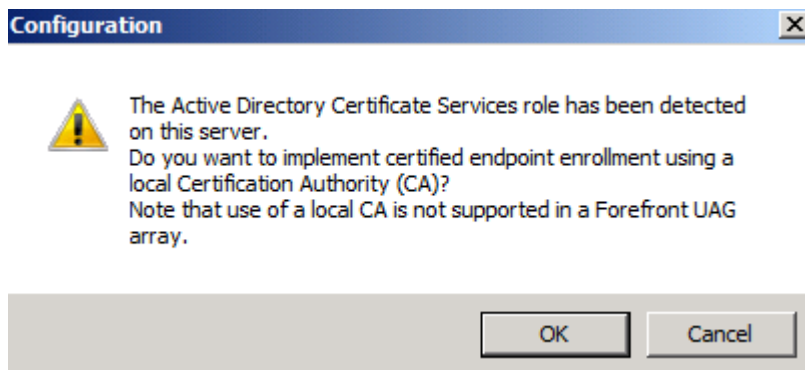
In den Trunk-Einstellungen kann auf der Registerkarte die Einstellung fuer privilegierte Endpoints aktiviert werden.



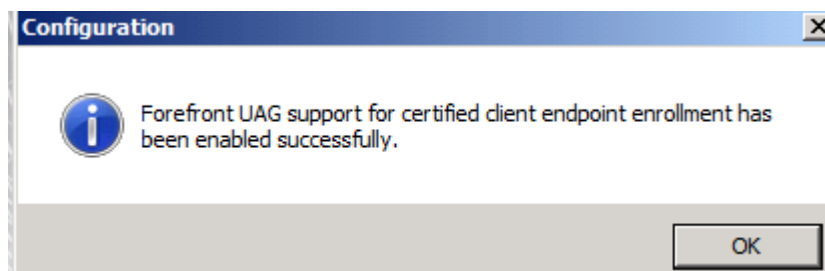
Achtung: Fuer die Privileged Endpoint Features MUSS eine CA installiert werden, eine Standalone CA geht nicht und wenn die CA lokal auf dem UAG installiert werden soll und UAG im Array betrieben wird. Wenn UAG im Array betrieben wird, kann die Certified Endpoint Enrollment Application nicht genutzt werden!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



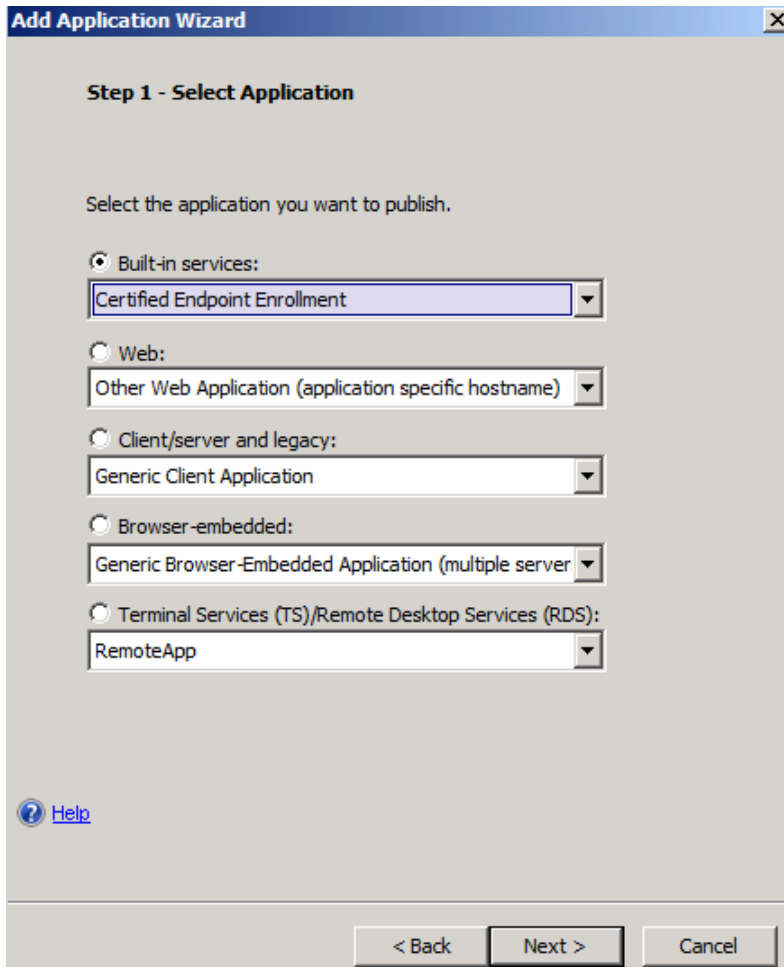
Aha, welche Firmenumgebungen das wohl nutzen (werden).



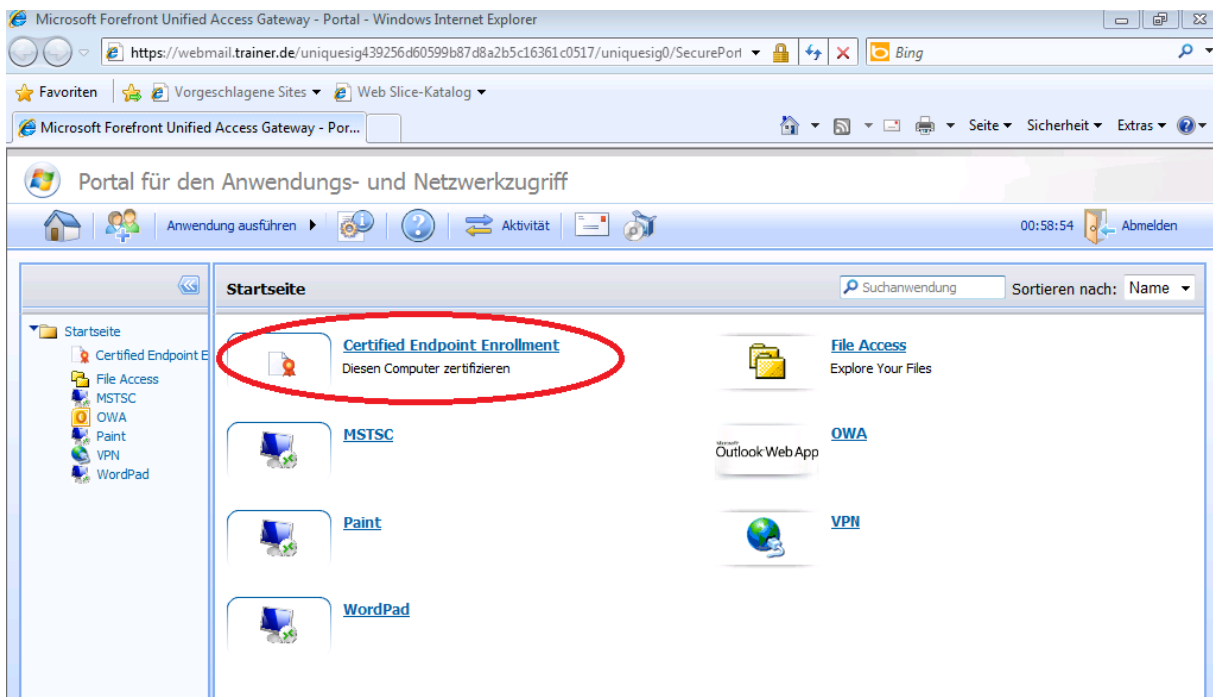
Prima



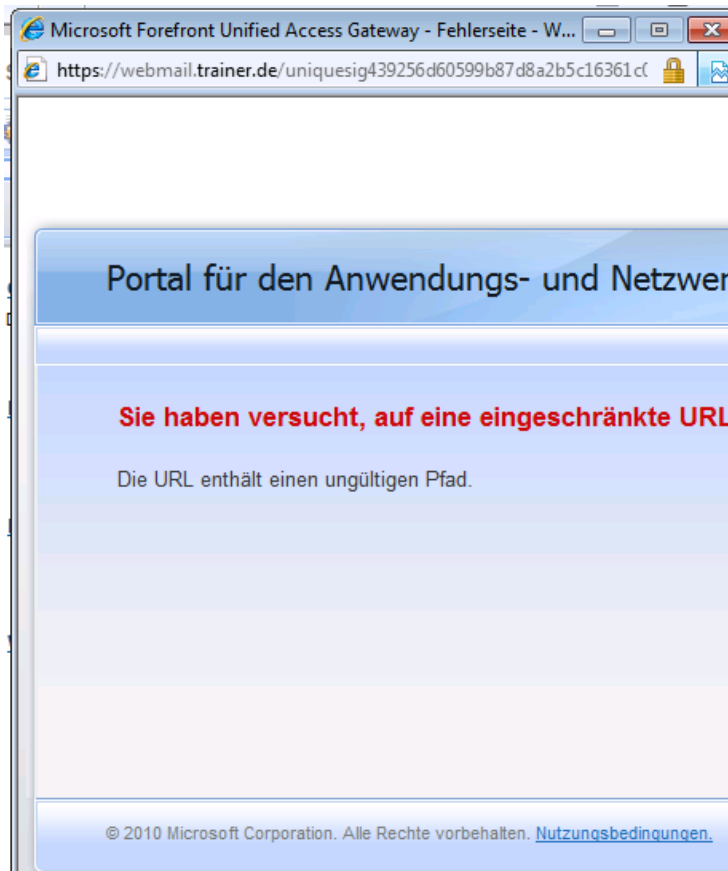
Certified Endpoint Enrollment in der UAG MMC unter den Built-In Services auswaehlen



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 rule 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) ☺

Portal für den Anwendungs- und Netzwerkzugriff

Forefront UAG-Endpunktcomponenten

Endpunktcomponenten-Manager	
Endpunkterkennung (ActiveX)	✓ (4.0.1575.10000)
SSL-Anwendungstunneling	✗
Socketweiterleitung	
SSL-Netzwerk-tunneling	
Endpunktsitzungs-bereinigung (ActiveX)	✓ (4.0.1575.10000)
Antivirensoftware	Keine kompatible Antivirensoftware gefunden.
Persönliche Firewall	Win7 (Version nicht erkannt)
Betriebssystem	Windows 7 Professional 6.01.7600, 32-Bit-Version
Browserversion	Internet Explorer 7
Benutzer-Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Sun JRE-Version	Nicht erkannt
Domäne	TRAINER
Zertifiziertes Gerät	
Privilegiertes Gerät	✓

Melden Sie sich zum Aktualisieren der Seite zunächst ab und dann erneut an.

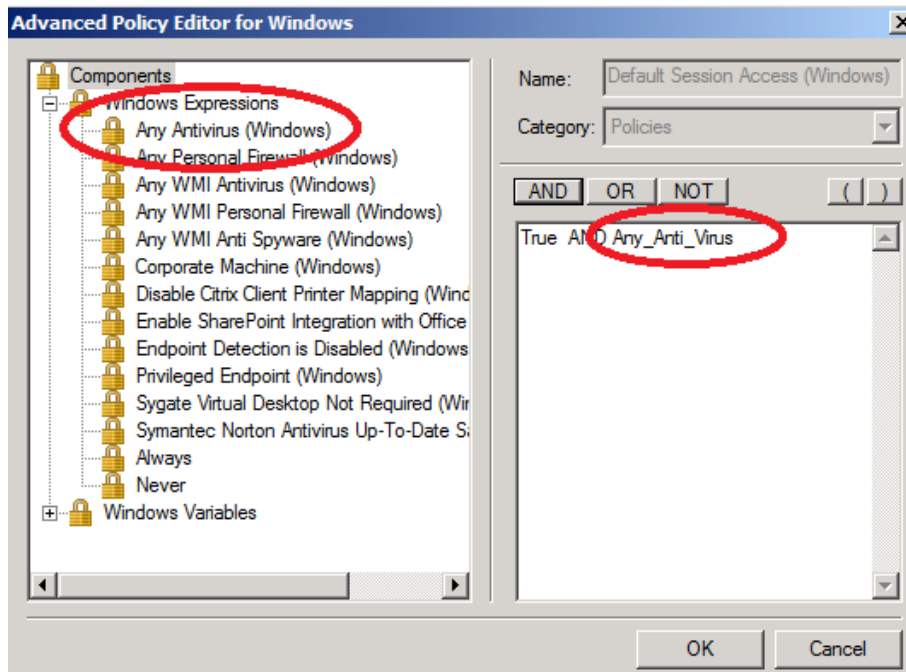
© 2010 Microsoft Corporation. Alle Rechte vorbehalten. [Nutzungsbedingungen](#).

Was ein zertifiziertes Geræet ist, muss ich noch herausfinden ☺

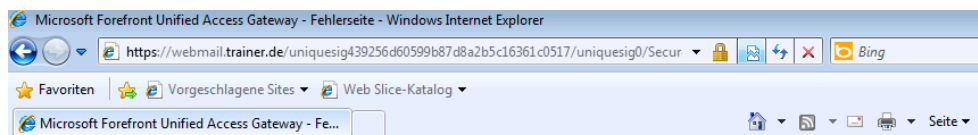
Bemerkung: Auch ohne das Zertifikat Enrollment von UAG kann ein Client ein privilegiertes Endgeræet sein, wenn ein entsprechendes Computerzertifikat der internen CA installiert ist!

Anpassung der Endpoint Access Policies

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



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



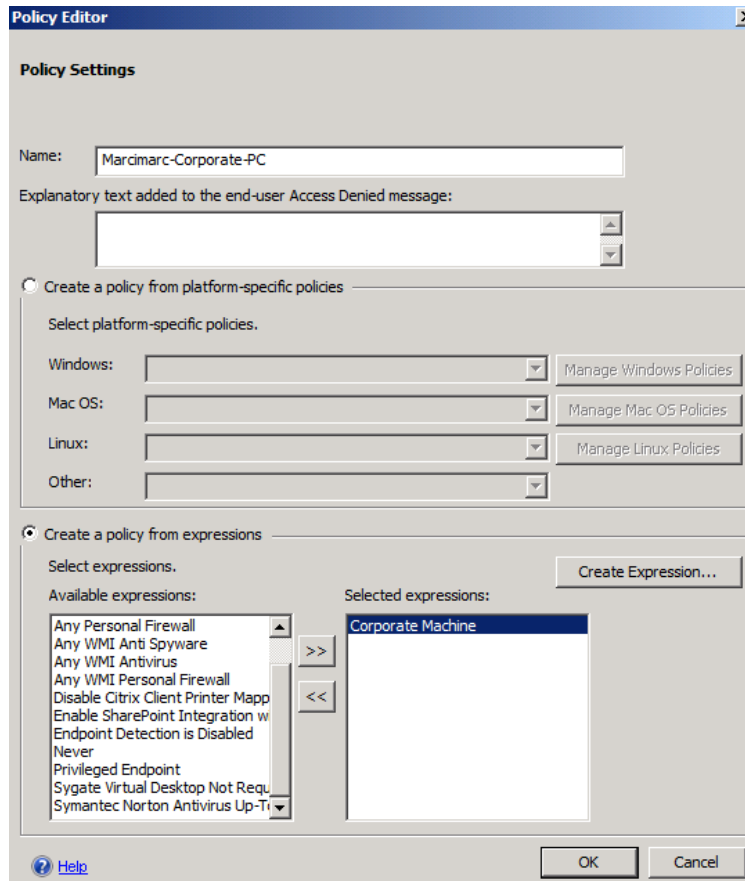
Der verweigerte Zugriff auf das Portal kann im Forefront UAG Webmonitor ueberwacht werden.

The screenshot shows the Microsoft Forefront Unified Access Gateway - Web Monitor interface. The main area displays an 'Event Viewer - All Events' table. The table has columns for Severity, Time, ID, Type, Category, Trunk, NodeName, and Description. The events include several 'Web Monitor Login' entries and one 'Session Access Policy Violation' warning.

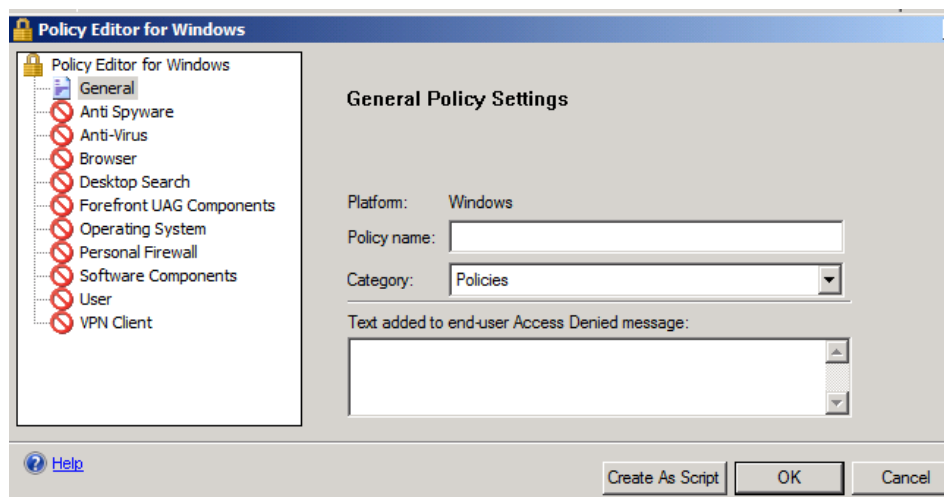
Severity	Time	ID	Type	Category	Trunk	NodeName	Description
Information	11/28/2010 13:24:18	84	Web Monitor Login	Security	N/A	UAG	The user TRAINER\ladministr logged on to the Forefront UA Web Monitor.
Information	11/28/2010 13:24:15	84	Web Monitor Login	Security	N/A	UAG2	The user TRAINER\ladministr logged on to the Forefront UA Web Monitor.
Information	11/28/2010 13:23:45	10	Configuration Change	System	N/A	UAG2	
Information	11/28/2010 13:23:41	84	Web Monitor Login	Security	N/A	UAG2	The user TRAINER\ladministr logged on to the Forefront UA Web Monitor.
Information	11/28/2010 13:23:41	84	Web Monitor Login	Security	N/A	UAG2	The user TRAINER\ladministr logged on to the Forefront UA Web Monitor.
Information	11/28/2010 13:23:36	84	Web Monitor Login	Security	N/A	UAG	The user TRAINER\ladministr logged on to the Forefront UA Web Monitor.
Warning	11/28/2010 13:22:33	65	Session Access Policy Violation	Security	portal (S)	UAG	A request from source IP add 212.212.10.120, user to trunk portal; Secure=1 for applicati Portal of type Portal failed. Th endpoint device does not con with access policy settings (Hybrid_Default_Session_Ac for session 302543E9-2A5E-4AAC-A8C9-8BC25F80902A. URL is /SecurePortalPortalHomeF

Erstellung eigener Forefront UAG Endpoint Access Policies

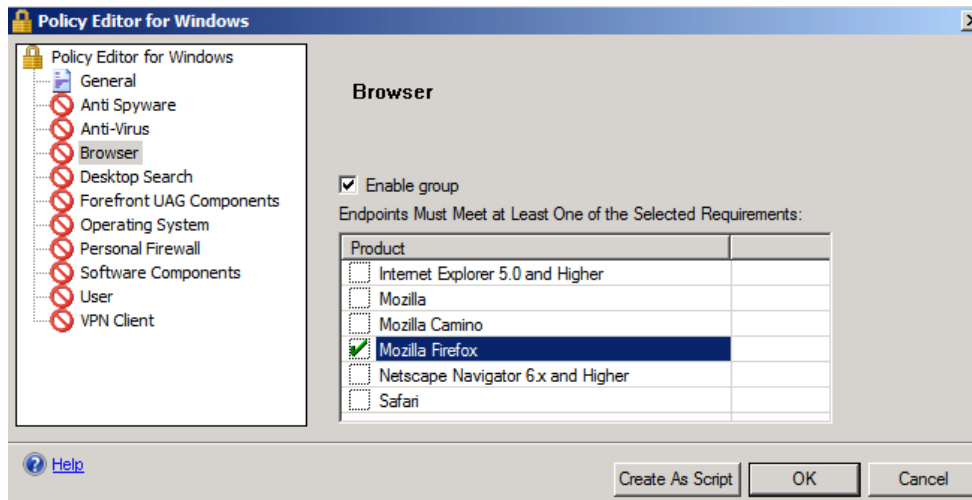
Wem die Standard Forefront UAG Richtlinien nicht ausreichen, kann eigene Policies erstellen, um diese auf die Beduerfnisse der Firma anzupassen. Neue Policies koennen fuer die jeweilige Betriebssystemplattform oder anhand von Expressions, erstellt werden.



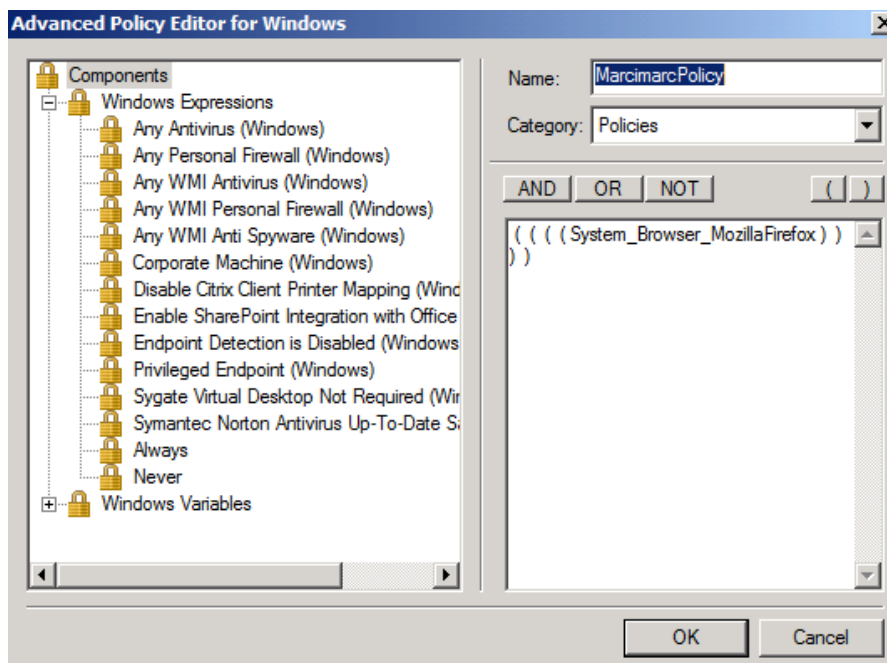
Mit dem Policy Editor fuer Windows koennen eigene Policies erstellt und konfiguriert werden und nach beliebigen Policies erstellt werden, um Zugriffe von Clients zu steuern.



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.

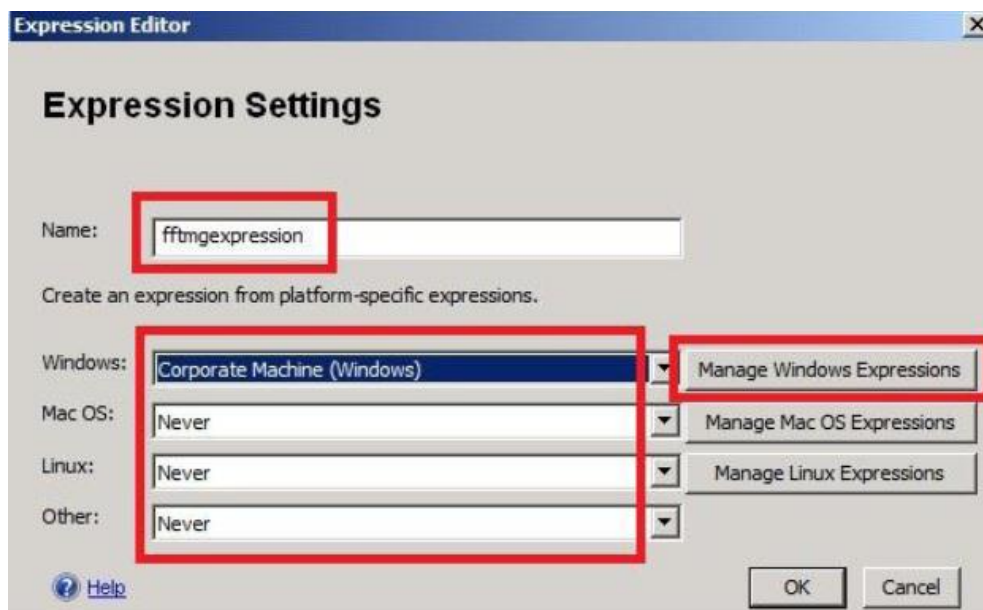
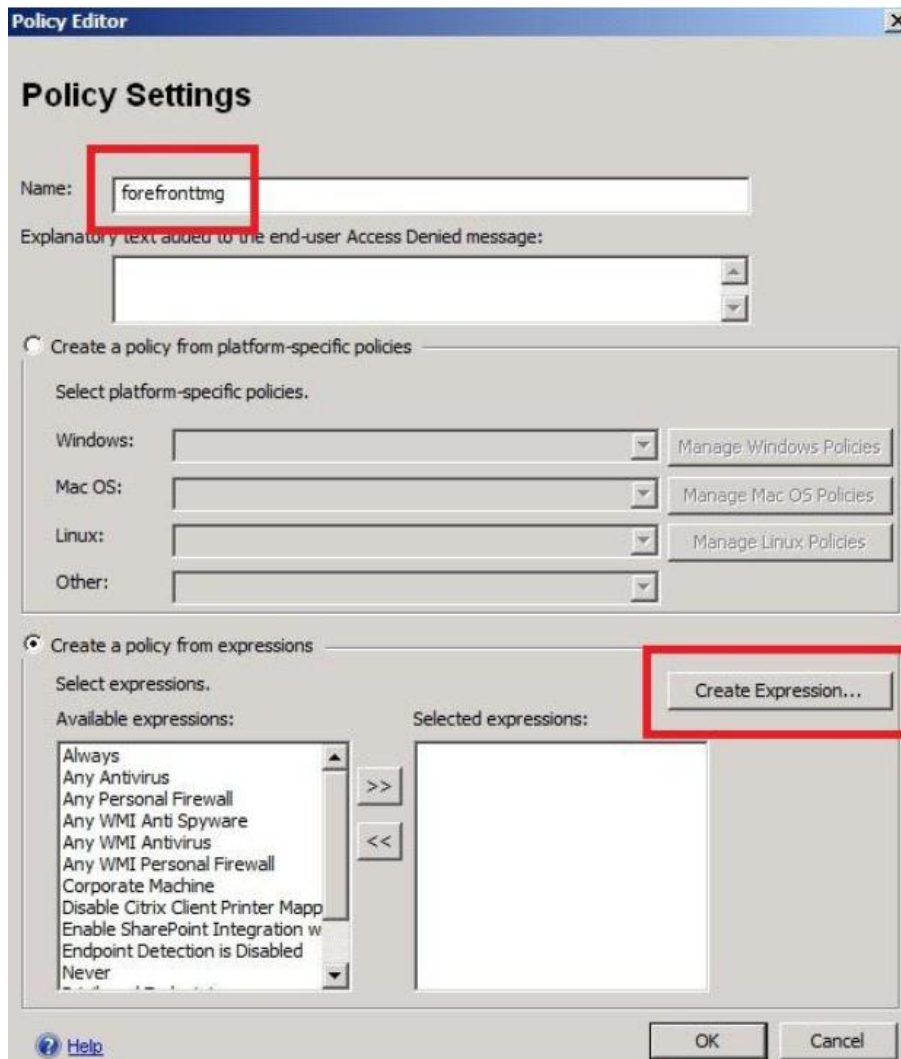


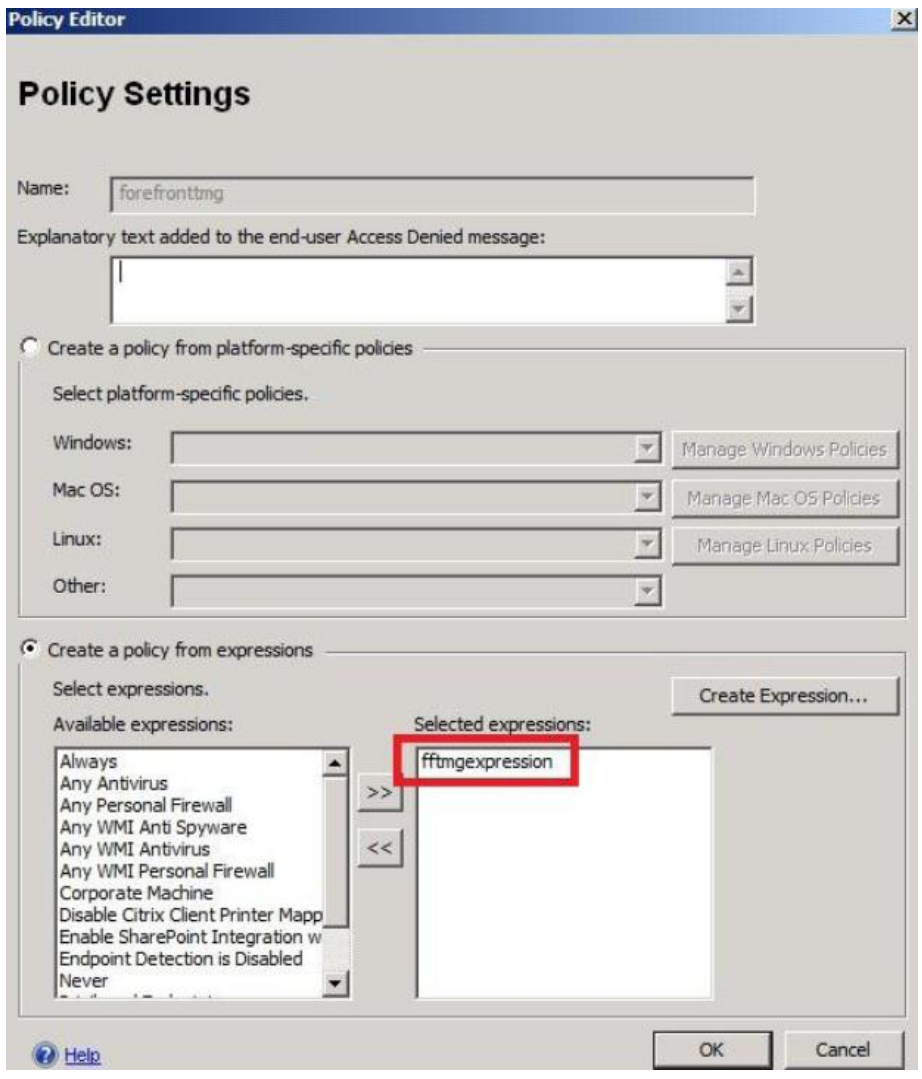
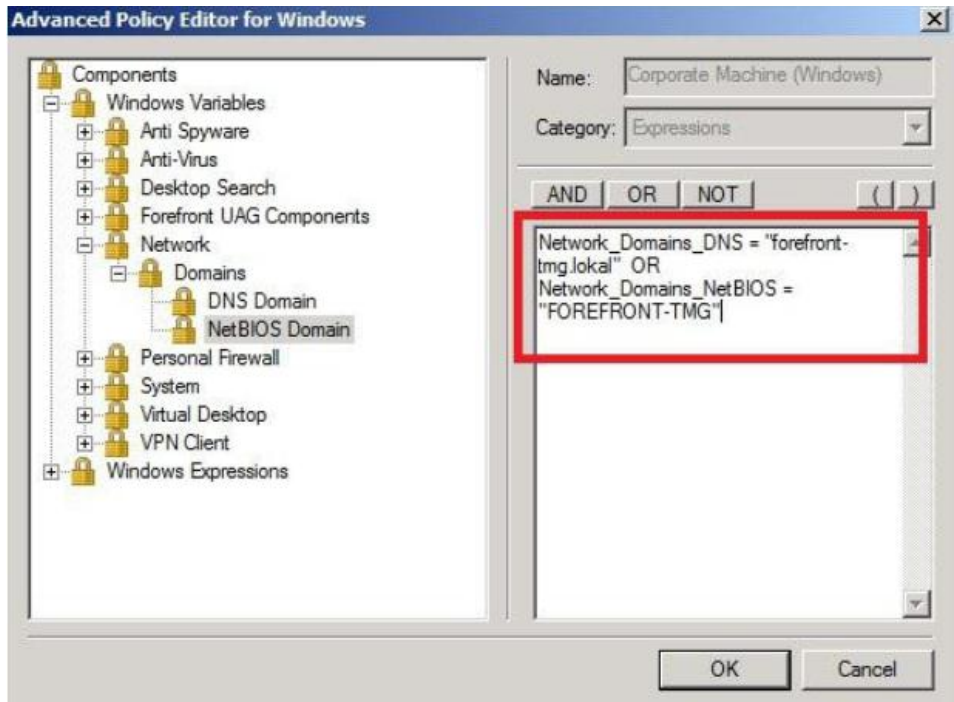
Es koennen auch eigene Expressions erstellt werden und diese dann in den Policies aktiviert werden.

The **Expression Editor** dialog box is shown. It has a title bar with a close button. The main area is titled **Expression Settings**. There is a text field for **Name:** containing "MarcimarcSygateAn". Below it is the instruction "Create an expression from platform-specific expressions." There are four rows of platform-specific settings: **Windows:** "Corporate Machine (Windows)" with a **Manage Windows Expressions** button; **Mac OS:** "Always" with a **Manage Mac OS Expressions** button; **Linux:** "Always" with a **Manage Linux Expressions** button; and **Other:** "Always". At the bottom left is a **Help** link, and at the bottom right are **OK** and **Cancel** buttons.

The **Policy Editor** dialog box is shown. It has a title bar with a close button. The main area is titled **Policy Settings**. There is a text field for **Name:** containing "MarcimarcExpression". Below it is a text area for **Explanatory text added to the end-user Access Denied message:**. There are two radio buttons: **Create a policy from platform-specific policies** (which is selected) and **Create a policy from expressions**. Under the first radio button, there is the instruction "Select platform-specific policies." and four rows of platform-specific settings: **Windows:** "Default Session Access (Windows)" with a **Manage Windows Policies** button; **Mac OS:** "Never" with a **Manage Mac OS Policies** button; **Linux:** "Never" with a **Manage Linux Policies** button; and **Other:** "Never". Under the second radio button, there is the instruction "Select expressions." and a **Create Expression...** button. Below this are two list boxes: **Available expressions:** containing a list of expressions including "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", and "MarcimarcSygateAn"; and **Selected expressions:** which is currently empty. Between the list boxes are **>>** and **<<** buttons. At the bottom left is a **Help** link, and at the bottom right are **OK** and **Cancel** buttons.

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.





Ergebnis

The image shows a screenshot of a SharePoint portal interface. At the top, the title bar reads "Portal für den Anwendungs- und Netzwerkzugriff". Below this is a navigation bar with icons for "Anwendung ausführen", "Aktivität", and a clock showing "00:59:55" with an "Abmelden" button. The main content area is titled "Startseite" and features a search bar labeled "Suchanwendung" and a sort dropdown menu set to "Name". On the left, a sidebar lists navigation options: "Startseite", "AssAssAllWiePIAn", "Abtschansch", "Intranet", "Schöne Filez hier!", and "Sharepoint". The main area contains several tiles: "AssAssAllWiePIAn" (highlighted with a red box), "Abtschansch" (with a "Outlook Web App" sub-label), "Intranet", "Schöne Filez hier!" (with "Explore Your Files" sub-label), and "Sharepoint" (with "SharePoint Server 2010" sub-label).