Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront UAG – Explaining and configuring Forefront UAG endpoint policies

Abstract

In this article I will show you how to enhance the security for clients who wants to access a Forefront UAG Server with the help of Forefront UAG endpoint access policies and Forefront UAG endpoint components installed on the client machines.

Let's begin

In a previous article published at www.isaserver.org I showed you how to create a portal trunk in Forefront UAG to publish internal applications like Microsoft SharePoint. In this article I will show you how it is possible to extend the security for clients who want to access the Forefront UAG Server with the help of Endpoint access policies. A Forefront UAG administrator can use a number of predefined endpoint access policies which checks a client who tries to access the Forefront UAG Server if for example an antivirus application is installed, the Windows Firewall is enabled or the client is a corporate machine. If the predefined endpoint access policies are not sufficient it is possible to create your own endpoint access policies.

It is possible to create Forefront UAG endpoint access policies at the portal trunk level and at the application level in the portal.

Forefront UAG Endpoint access policies at portal level

To use endpoint access policies at the portal level navigate to the properties of the portal trunk and click the Endpoint Access Settings tab. There are a number of possible endpoint access settings:

- Session Access Policy
- Privileged Endpoint Policy
- Socket Forwarding Component Installation Policy

The Session Access Policy is used to control which clients are allowed to access the Forefront UAG portal before they can logon to the portal.
The Privileged Endpoint Policy is used for privileged clients who must provide a certificate in addition to the endpoint access policies. I will give you more information about privileged endpoints later in this article.
The Socket Forwarding Component Installation Policy is used to control the requirements for clients which must use the UAG socket components for additional interaction with the Forefront UAG Server and the client.

If you don’t want to use endpoint access policies it is possible to configure Forefront UAG to use NAP (Network Access Protection).

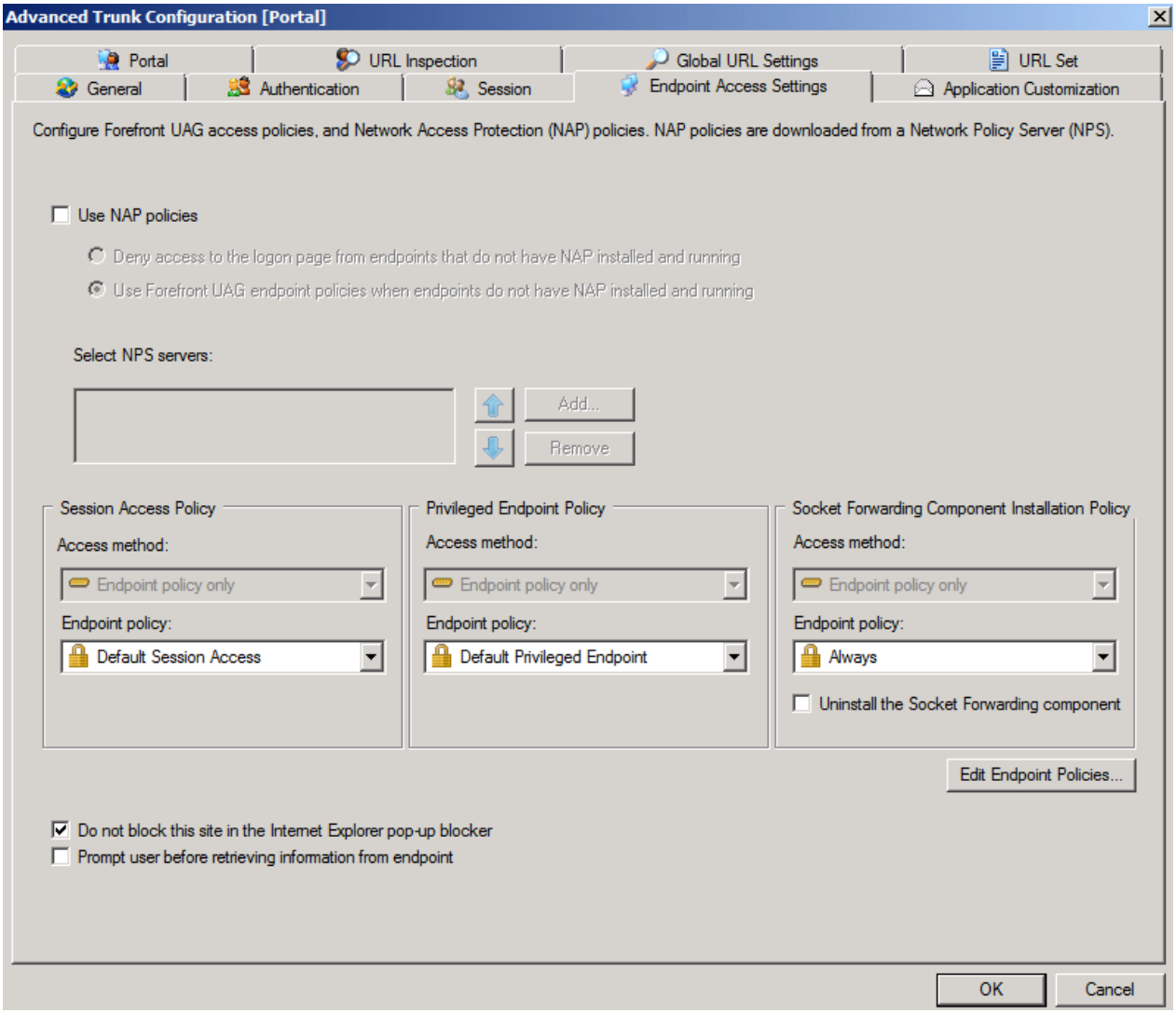

Figure 1: Endpoint access settings at portal level

It is possible to edit the predefined endpoint access policies. Click Edit Endpoint Policies and you will see a list of predefined endpoint access policies. Forefront UAG endpoint policies can be platform specific. You can use policies for Windows clients, Mac OS and Linux.

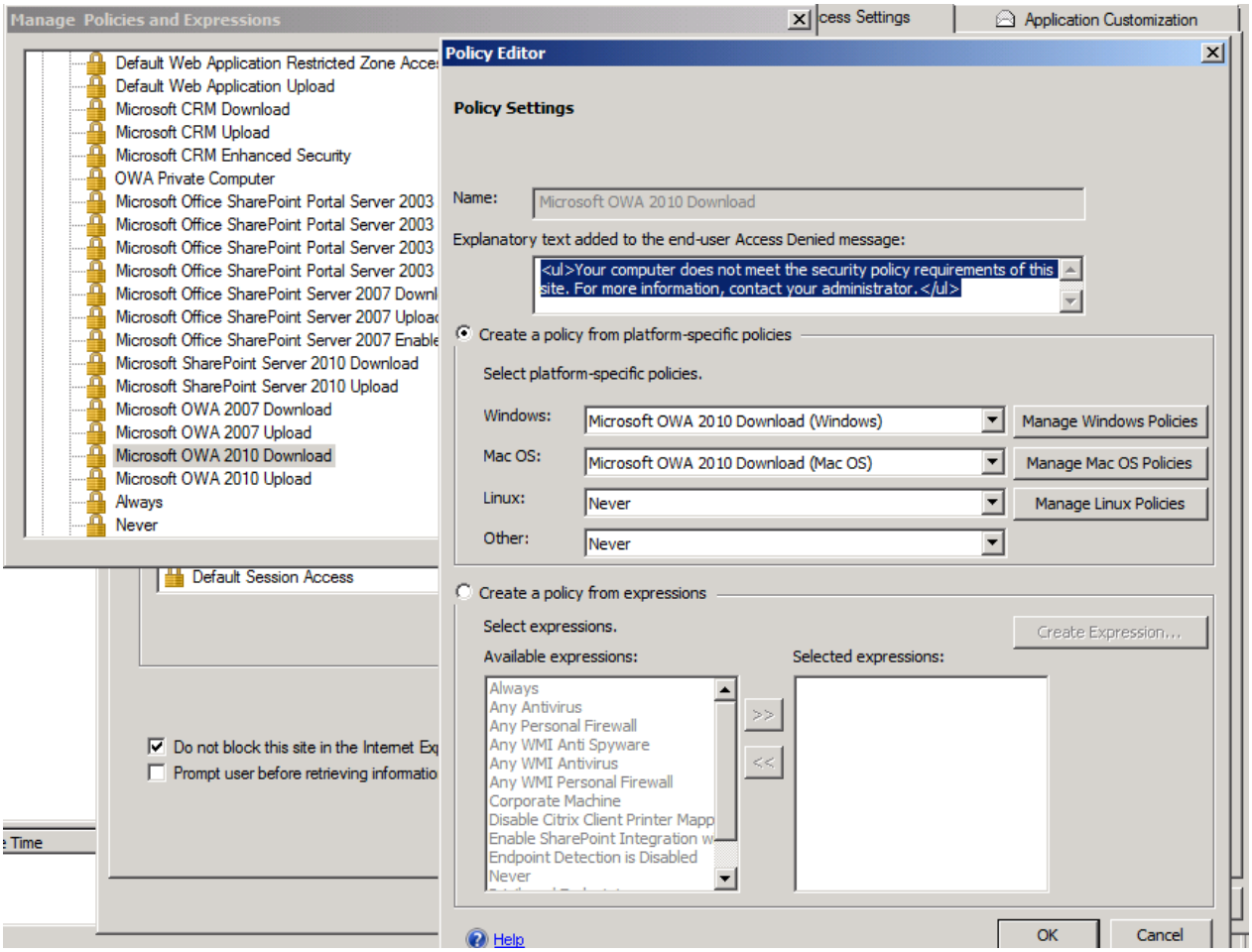

Figure 2: Default endpoint access policies

The predefined endpoint policies come with a lot of possible settings as shown in the following screenshot and it is possible to combine different requirements with AND filters. You can also combine settings with OR and NOT filters.

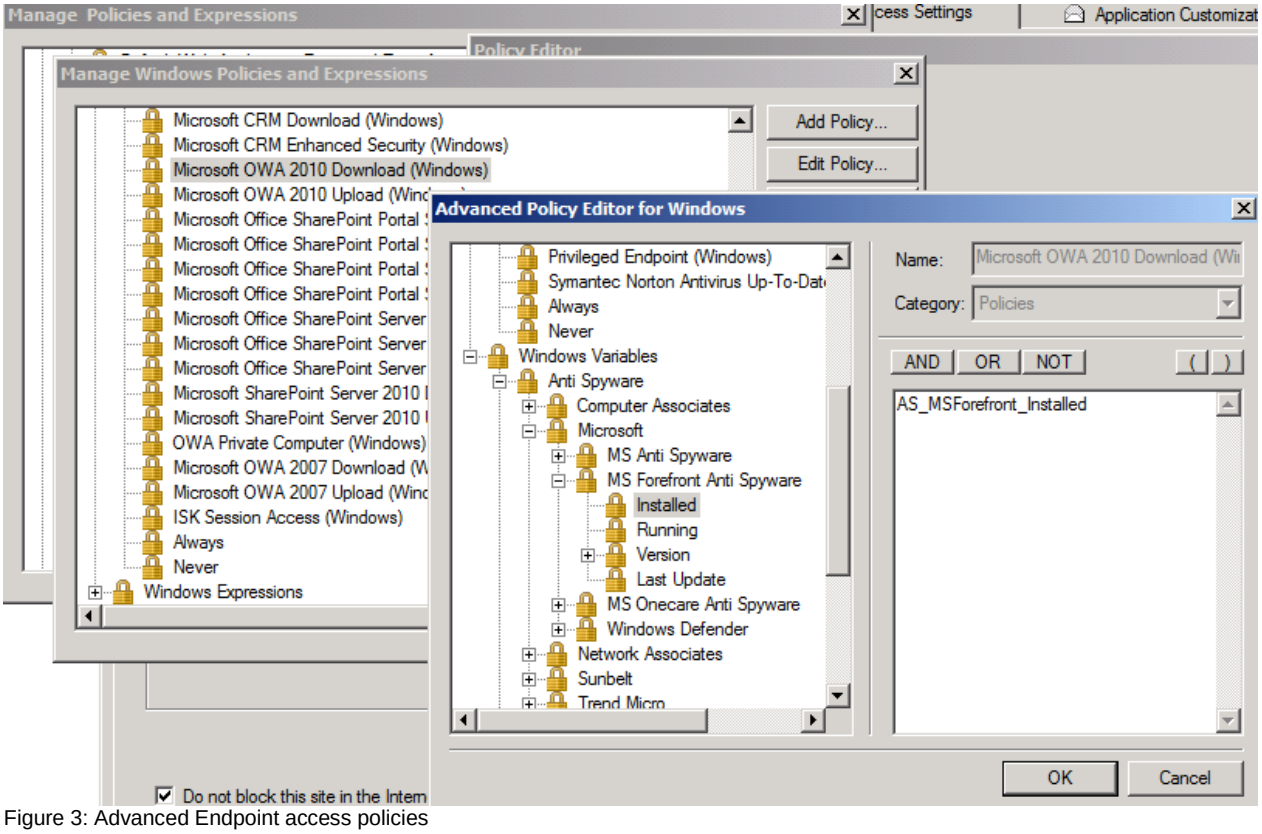

Figure 3: Advanced Endpoint access policies

I will show you later in this article how to create your own endpoint policies.

Forefront UAG endpoint components

Before you can use endpoint policies with Forefront UAG the client who wants to access the portal must install some software components on the local machine. This software is called Forefront UAG endpoint components. There are two versions of this component: ActiveX and Java Applet.
This software is used for interaction between the client and the Forefront UAG Server and will be used to check if the client fulfils all requirements which administrators has been defined in the endpoint policies on the Forefront UAG server. The following components are available:
(Copied from the following source: http://technet.microsoft.com/en-us/library/dd857328.aspx)

The Forefront UAG endpoint components that are installed on client endpoints to enable Forefront UAG features and functionality include:

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. For more information, see About the Endpoint Session Cleanup component.

Forefront UAG Endpoint Detection
There are two versions of this component: ActiveX and Java Applet.

Non-Web tunnelling

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

Forefront UAG Endpoint component installation

The endpoint components will be installed during the user first opens the portal, but it is also possible to manually install the endpoint components via software distribution like Microsoft System Center Configuration Manager, Active Directory group policies or third party software.

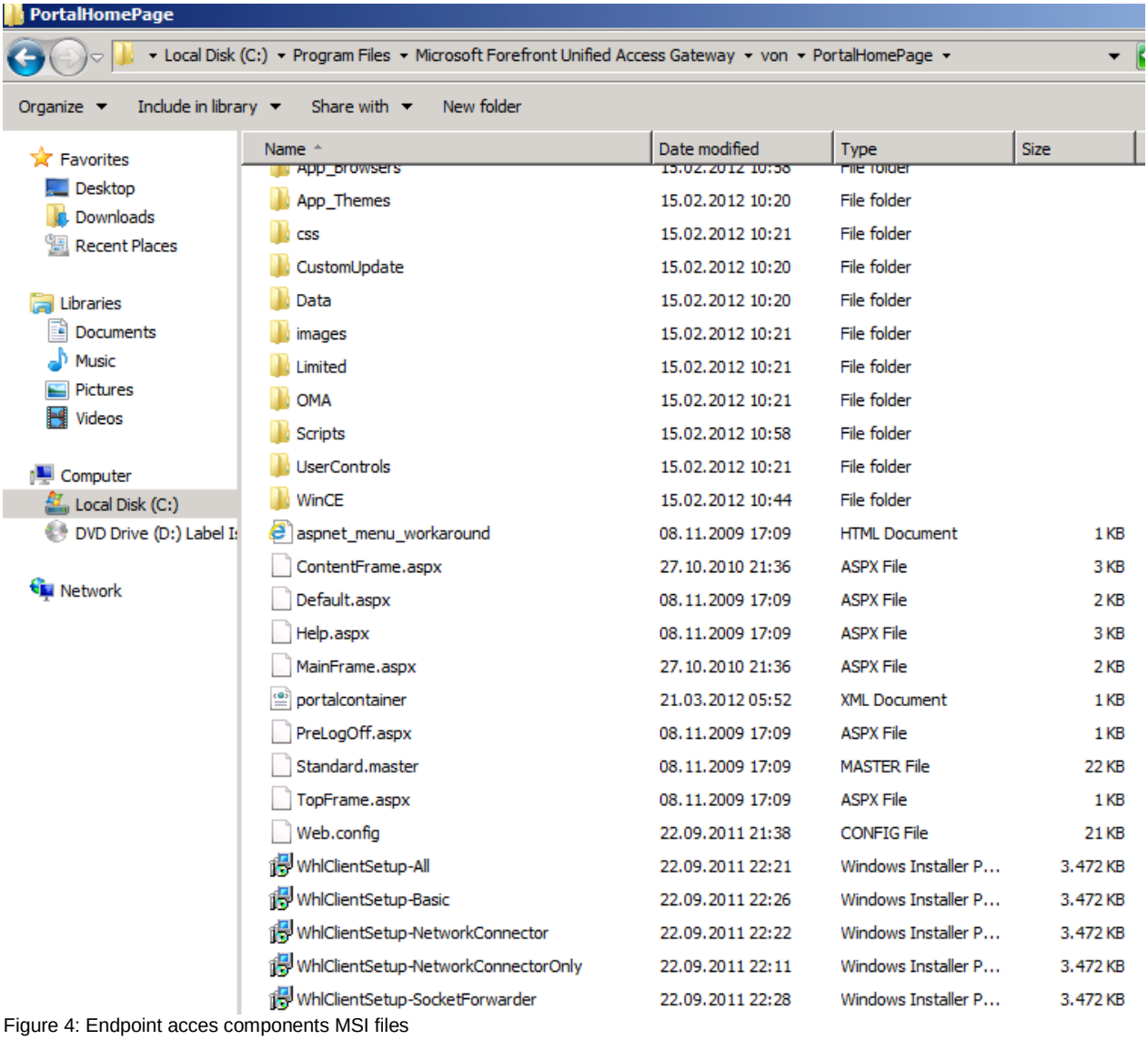

Figure 4: Endpoint acces components MSI files

It is also possible to configure the Forefront UAG Server portal to give clients the ability to install the endpoint components as a offline installer.

Component installation at client side

Due to the nature of modern web browsers there are some pitfalls when the endpoint components will be installed on the client. For example the Forefront UAG endpoint components requires that the portal website will be excluded from the pop-up blocker of Internet Explorer as shown in the following screenshot.

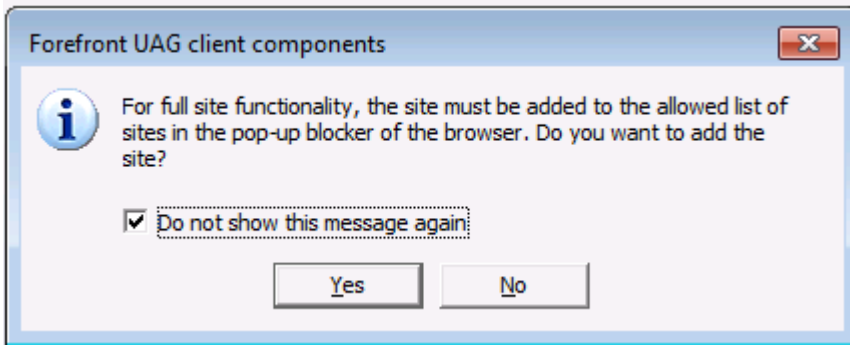

Figure 5: Installation warning message in Internet Explorer

After the endpoint components has been installed on the client, the client will be checked for compliance against the Forefront UAG portal endpoint policies.

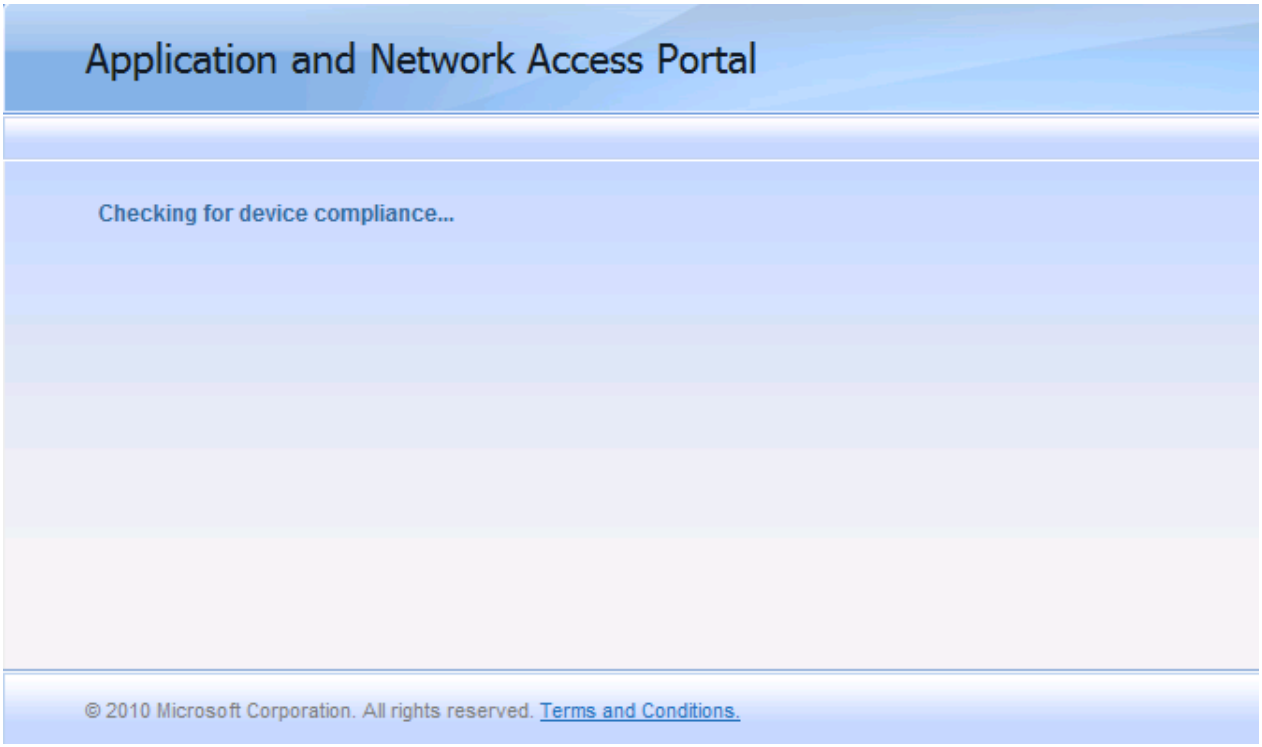

Figure 6: Portal access – Check for compliance

The first time users will also get the following Security Alert. Users should always trust this site to avoid displaying the Security alert again.

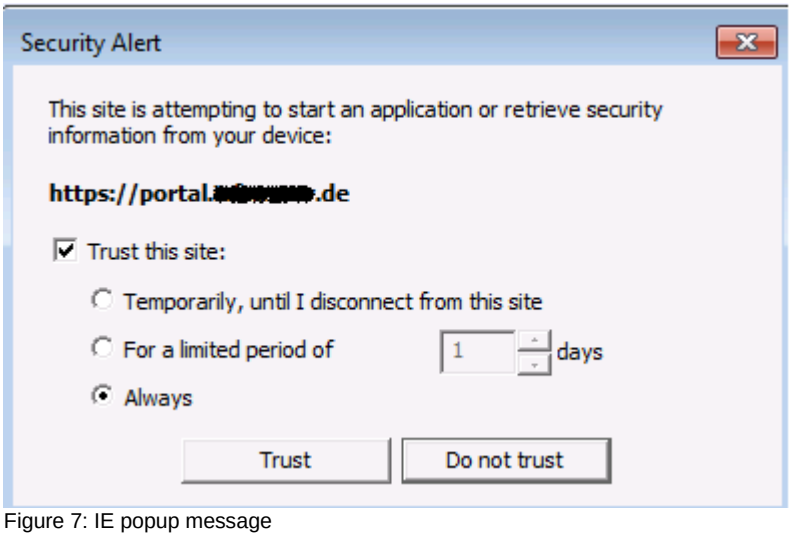

Figure 7: IE popup message

It is possible to automatically add the UAG portal website to the trusted sites and to automatically disable the pop-up blocker for the UAG website with the help of some Registry modifications. I will give you more information later in this article how to do this.

Forefront UAG Secure Endpoint Deployment

For more security Forefront UAG administrators can deploy certified endpoints. Certified endpoints are more trusted for the Forefront UAG Server and you will have more control about clients which try to access the UAG portal. A certified endpoint is a client which has a certificate issued from an internal Certificate Authority.
To activate the Forefront UAG Server for certified endpoints you have to enable the checkbox in the Forefront UAG portal settings as shown in the following screenshot.

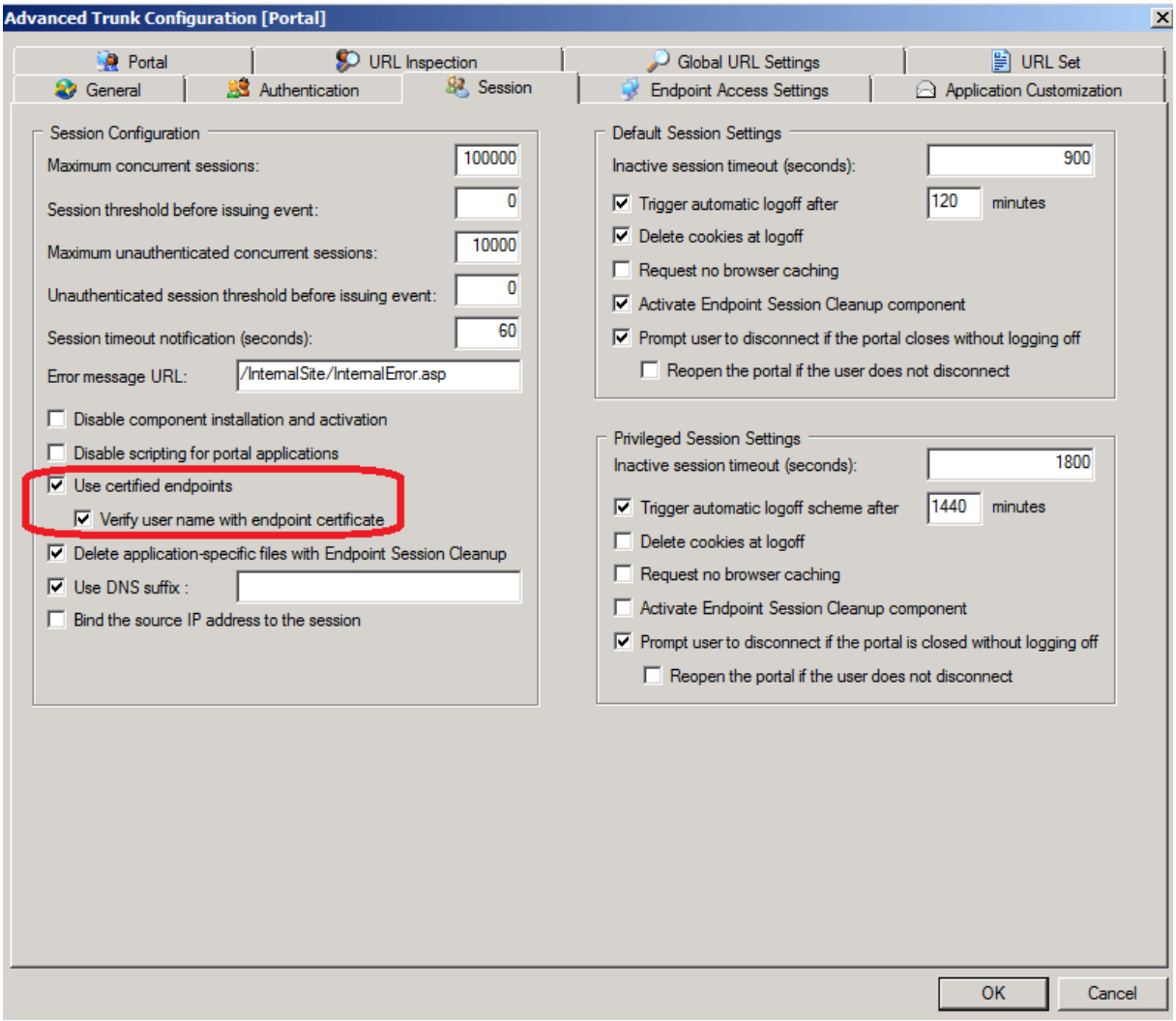

Figure 8: UAG certified endpoint

Before you can use Forefront UAG for certified endpoint access, a local certificate authority must be installed on the Forefront UAG Server. If an Active Directory integrated CA still exists you must install a subordinate CA on the Forefront UAG Server.

Certificate Authority installation

For this article I already deployed an Active Directory integrated Root CA so we will install a subordinate CA on the Forefront UAG Server.

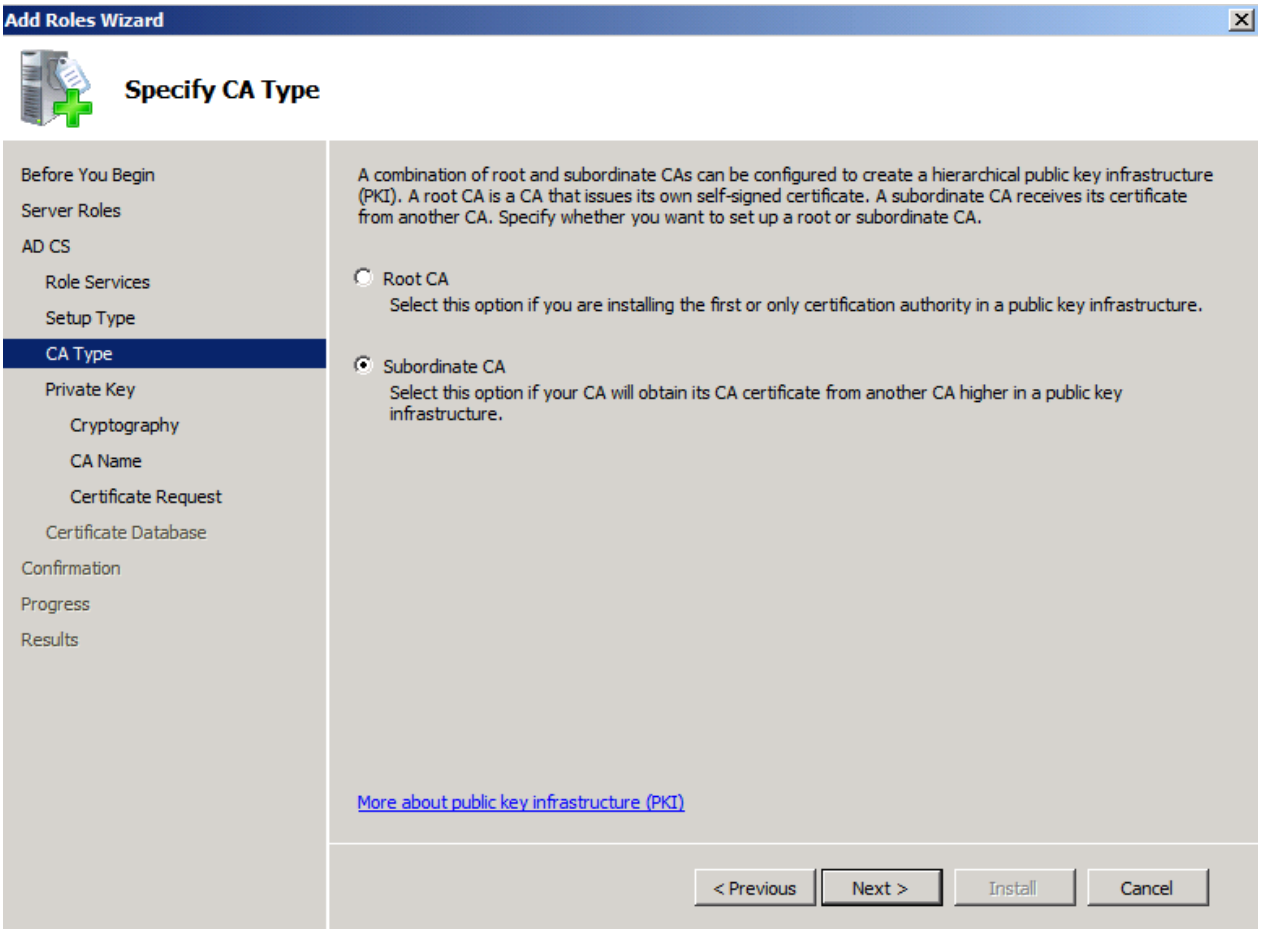

Figure 9: Subordinate CA installation

Enable certified endpoint enrollment

After the CA has been installed on the Forefront UAG Server you must start the UAG Management console again and Forefront UAG asks you if you want to implement the certified endpoint enrollment on the Forefront UAG Server.

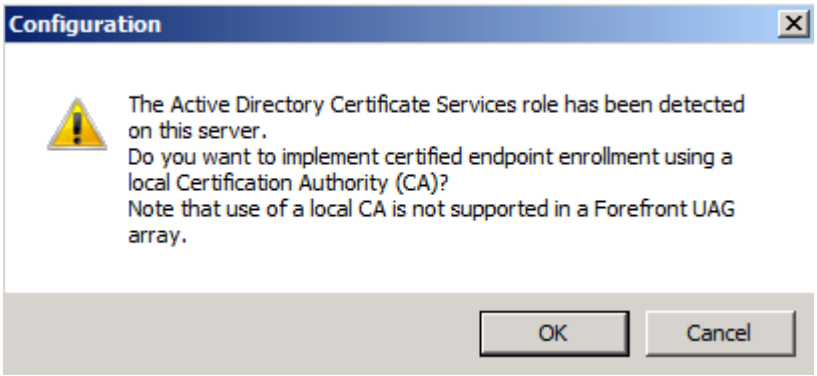

Figure 10: Enable certified endpoint

It takes some times until the certified endpoint enrollment has been activated. You will get the following message: “Forefront UAG support for certified client endpoint enrollment has been enabled successfully”.
After the activation has been succeeded you can use the Forefront UAG management console to add the Certified Endpoint Enrollment application to the portal. If the client doesn’t have a certificate installed you must change the endpoint

access settings in the portal trunk for the Certified Endpoint to Always, else the client cannot connect to the portal to enroll for the Certified Endpoint.

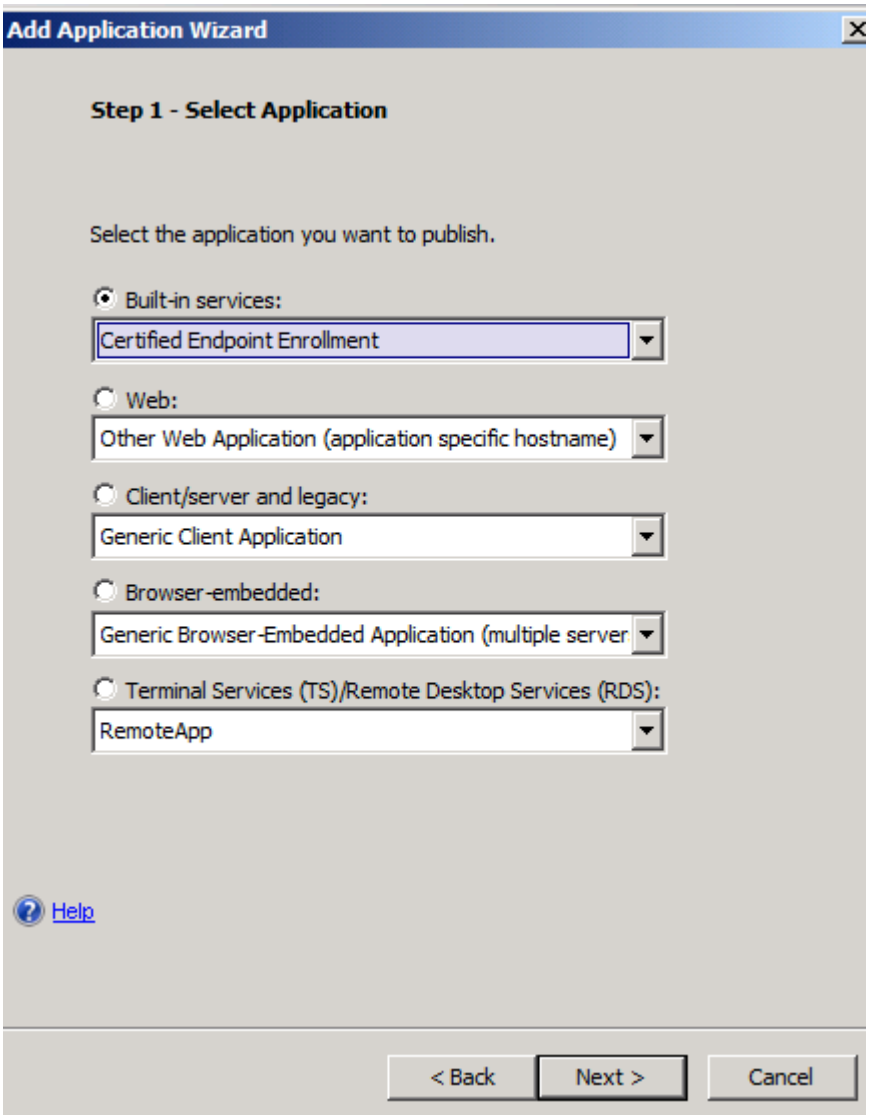

Figure 11: Publish certified endpoint

If the client has already a certificate installed in the local certificate store the user will get the following message and must select the appropriate certificate.

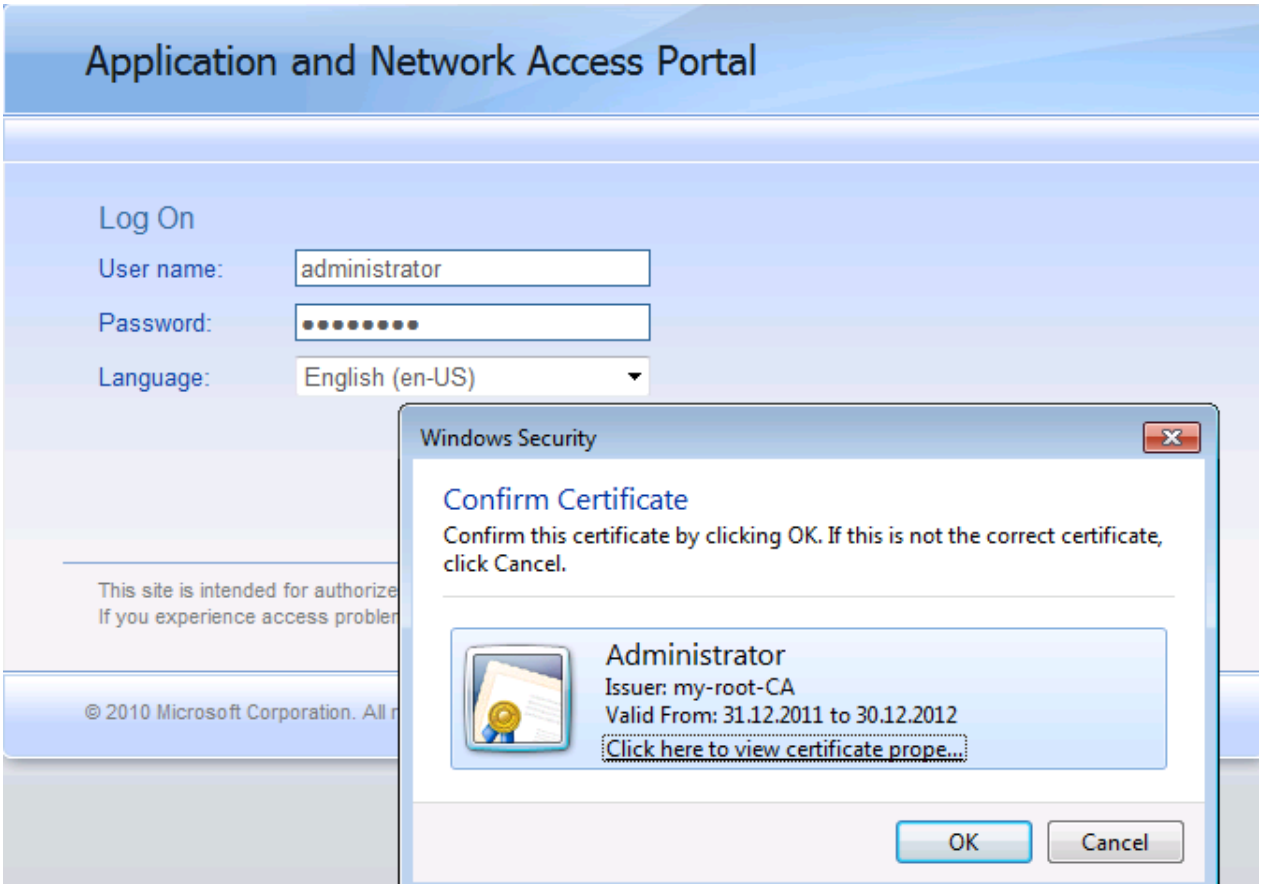

Figure 12: Client certificate question

After the user has been logged on successfully to the portal you can check if the client is now a certified and privileged device as shown in the following screenshot.

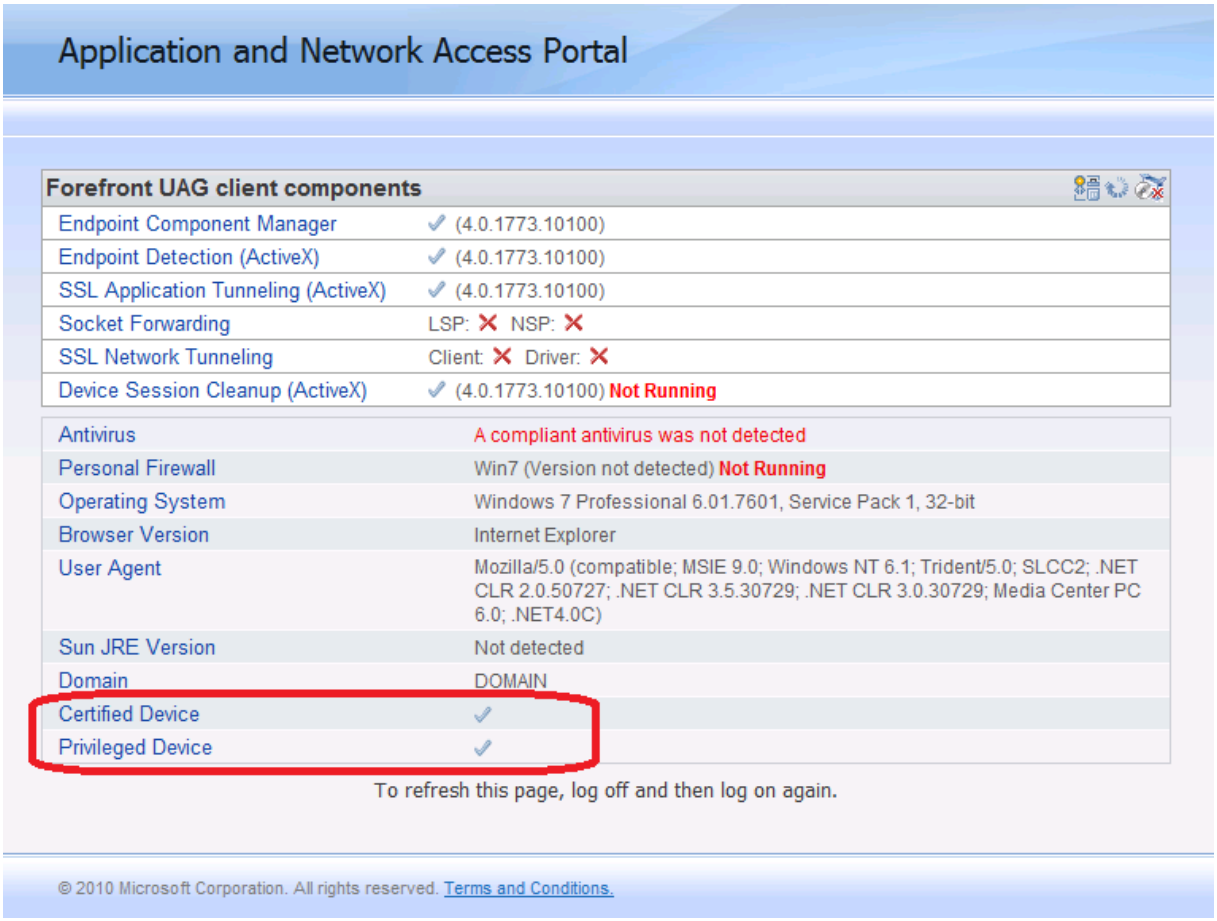

Figure 13: Certified endpoint

Forefront UAG endpoint component Registry patching

As I wrote earlier in this article it is possible to automate the pop-up message for the pop-up blocker and the trusted site settings in Internet Explorer when the client tries to access the portal the first time and the endpoint components will be first installed on the client.

Please note: This Registry patch will only work if you have full control over the client so typically you can use this Registry patching only if the client is a corporate client.

Check Site

```
 [HKEY_CURRENT_USER\Software\WhaleCom\Client\CheckSite]
"Managed"=dword:00000001
"CanAddSites"=dword:00000001
"CanAddHttpSites"=dword:00000000
"PromptInvalidCertTrusted"=dword:00000000
"PromptInvalidCertUntrusted"=dword:00000001
"TrustedSite0"=https://portal.isaserver.org
```

Avoid popup in Internet Explorer

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\Allow]
"portal.isaserver.org"=hex:
```

Forefront UAG Endpoint access policy customization

As I wrote earlier in this article where we talked about the Forefront UAG endpoint access policies it is possible to create your own endpoint access policies. For the example in this article we will create a policy which checks if the client is a corporate PC joined to the Active Directory domain isaserver.org. Navigate to the UAG portal properties and click Edit Endpoint Policies and create a new policy. Click Manage Windows Policies.

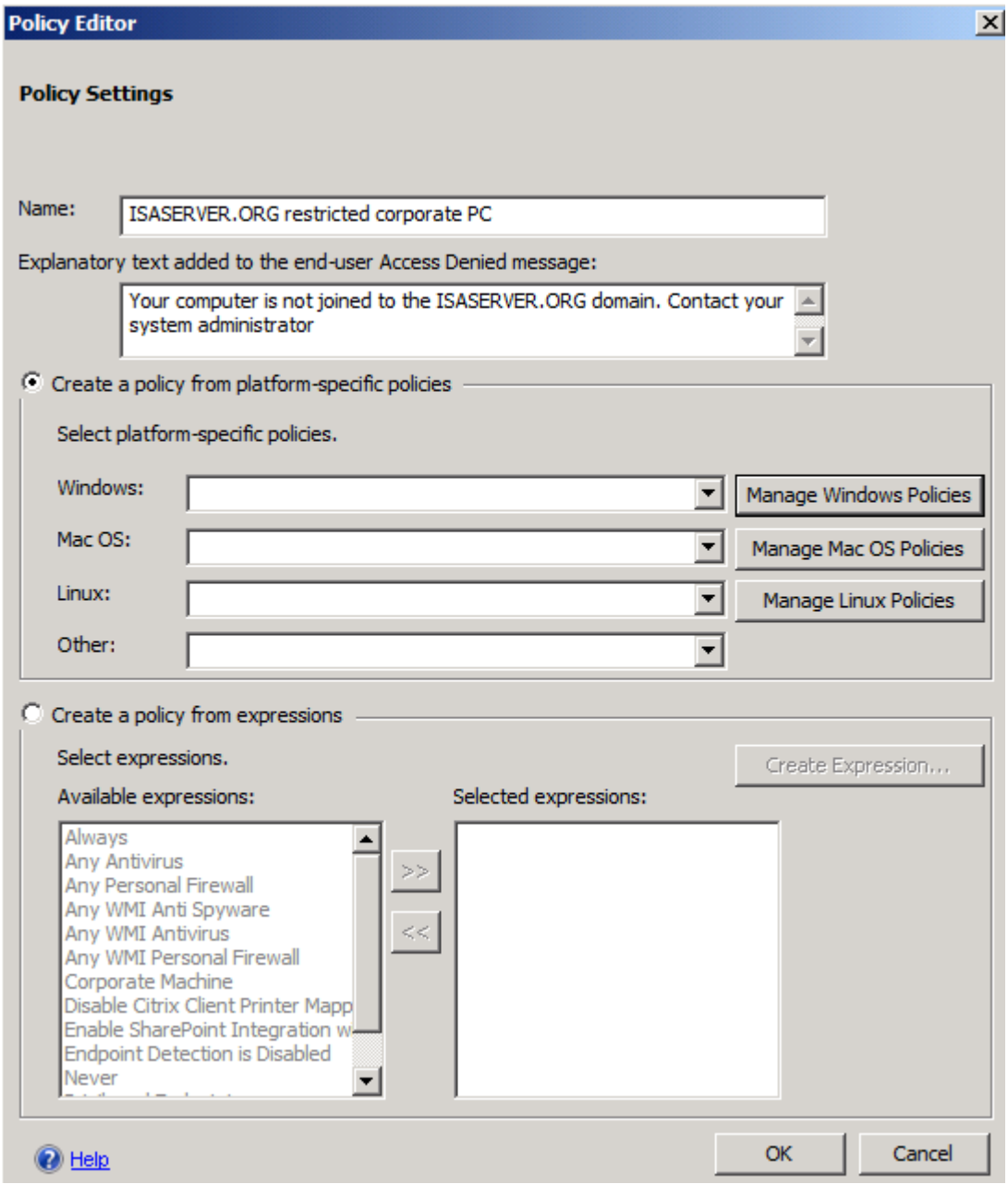

Figure 14: Customize Endpoint access policies

We must use the Windows variables from the Advanced Policy Editor. Select Networks – Domains – DNS domain and enter the text as shown in the following screenshot to check if the clients NetBIOS and DNS domain name is ISASERVER OR ISASERVER.ORG.

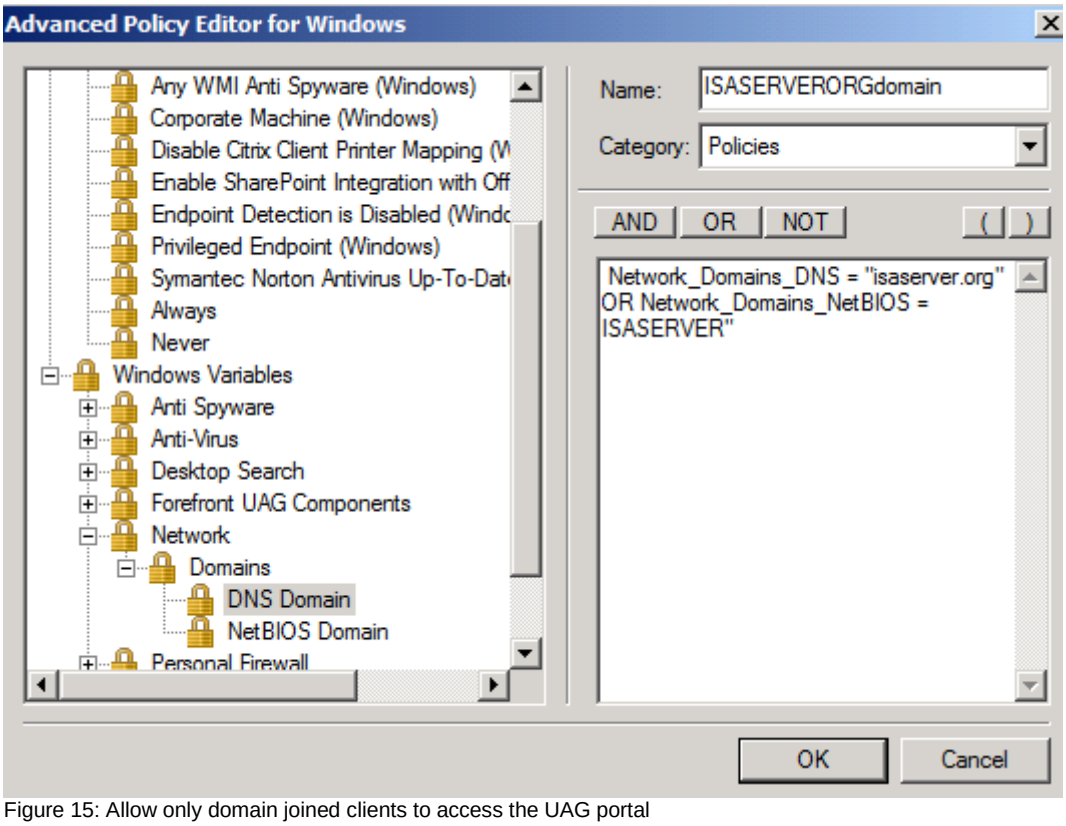

Figure 15: Allow only domain joined clients to access the UAG portal

After the policy has been created use the new policy in the platform specific policy for Windows. You can now use this new endpoint policy at Forefront UAG trunk level or for a specific application in the portal. In my opinion it makes more sense to use this policy at application level because every authenticated user can access the Forefront UAG portal after successful authentication and some basic endpoint policy settings has been checked but the important application with confidential content for example can only be accessed from corporate clients.

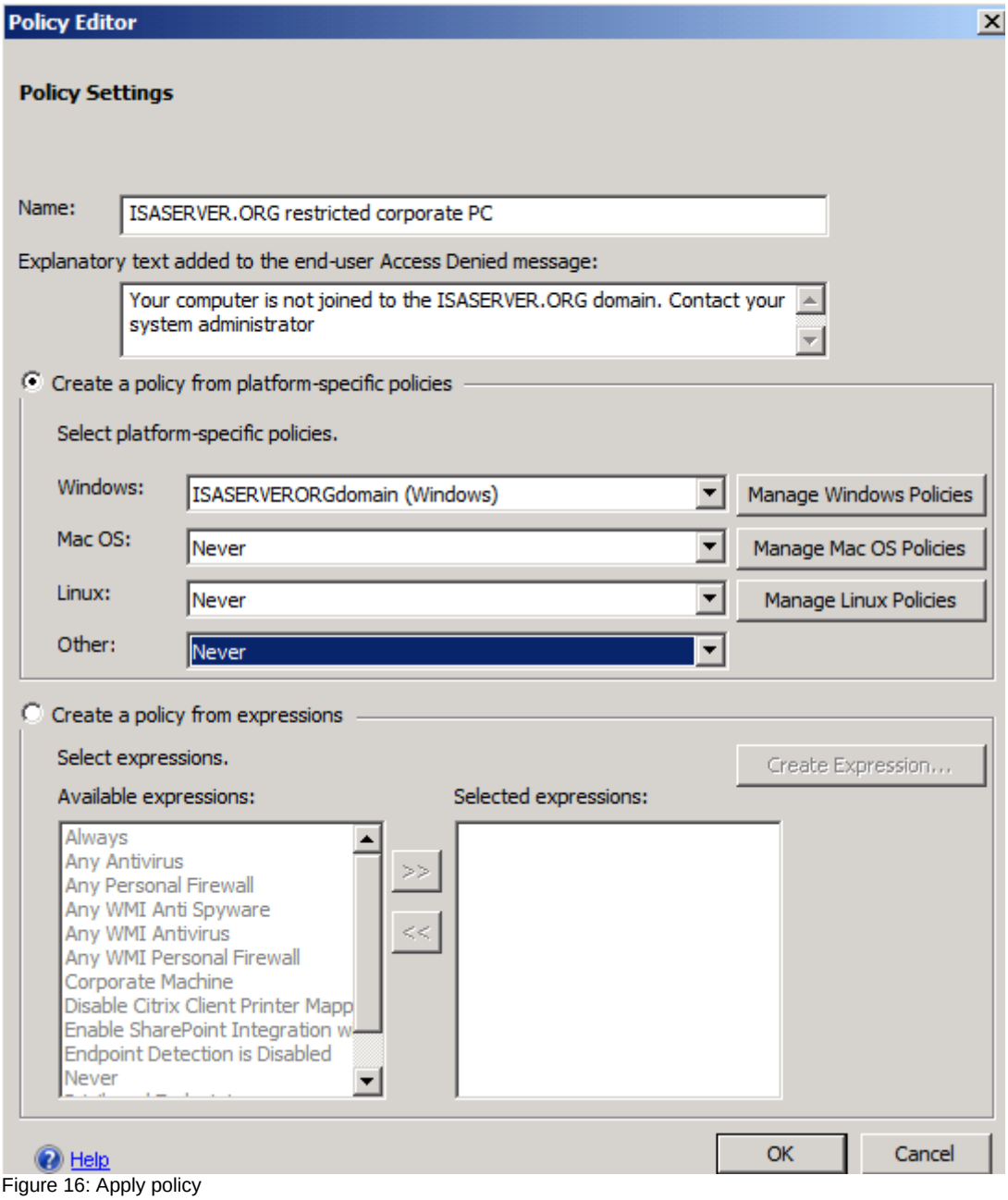

Figure 16: Apply policy

Forefront UAG Endpoint monitoring

Forefront UAG provides some monitoring capabilities regarding endpoint settings. A client is able to see detailed endpoint information in the portal as shown in the following screenshot.

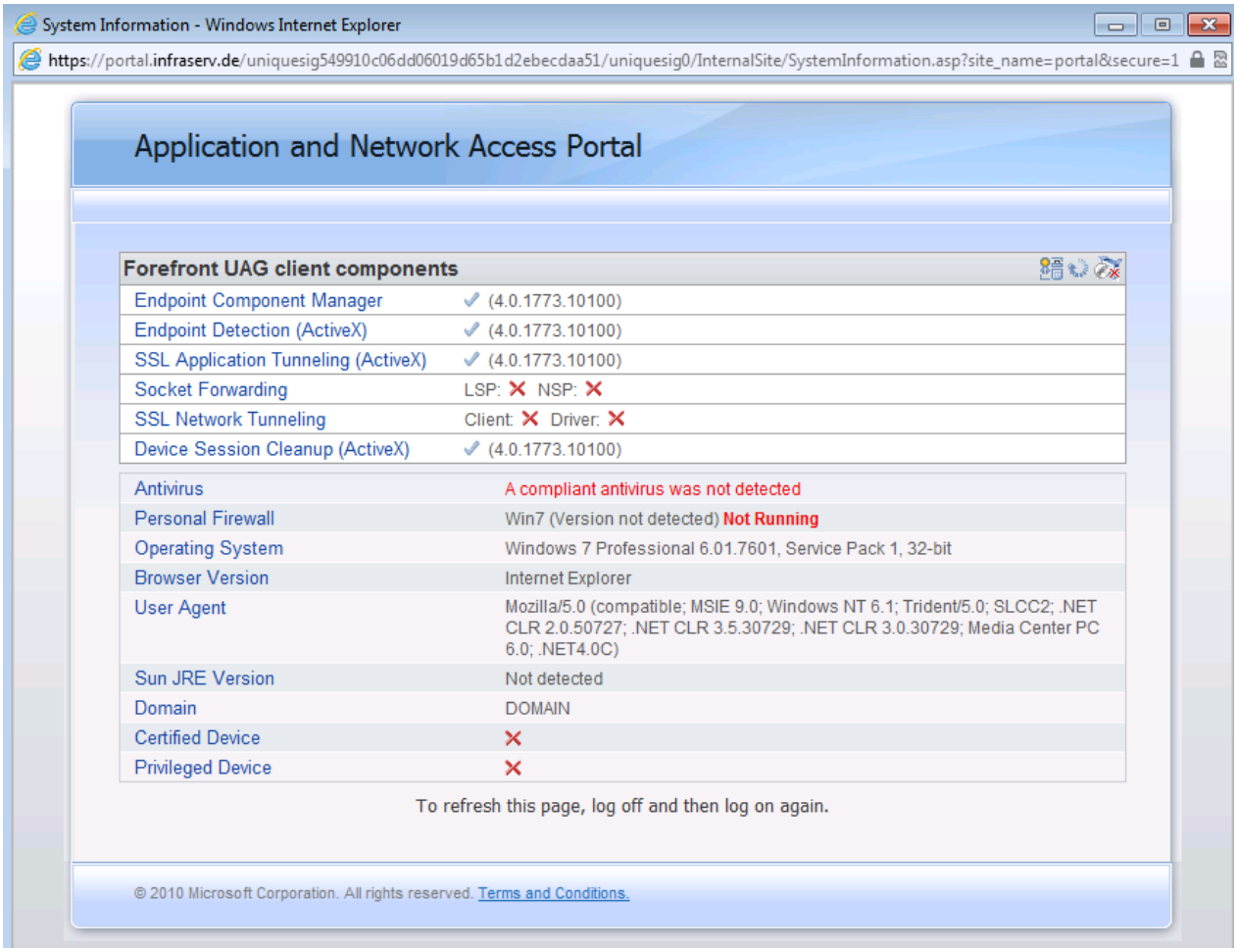

Figure 17: client compliance information in the portal

The Forefront UAG Administrator can use the Forefront UAG Web Monitor which is part of the Forefront UAG installation to see details about the connection state of the client and the detected endpoint settings. Start the Forefront UAG Webmonitor, navigate to the Session Monitor – Active Sessions and hit the Session ID of the logged on user. The Endpoint Information tab provides the same information about Forefront UAG components and detected components like Windows Firewall, Windows version, Browser version and more.

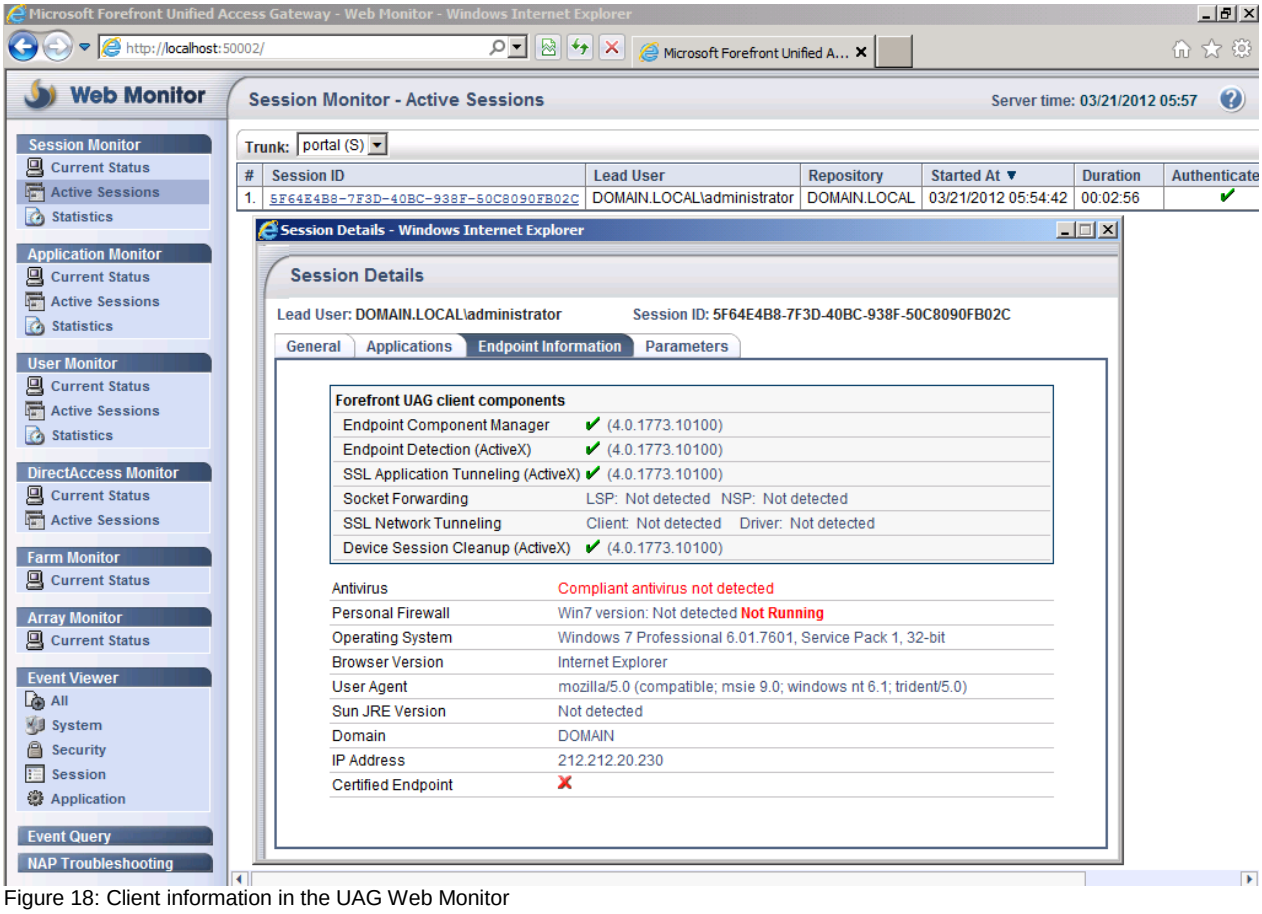

Figure 18: Client information in the UAG Web Monitor

Conclusion

In this article I tried to give you an overview about Forefront UAG endpoint access policies. Forefront UAG Endpoint access policies are a really good solutions for the administrator to check clients for compliance before they are allowed to access a Forefront UAG portal.

Related links

Introduction to endpoint component deployment design
http://technet.microsoft.com/en-us/library/dd857328.aspx
Configuring Forefront UAG access policies
http://technet.microsoft.com/en-us/library/dd857309.aspx
Planning to implement endpoint access policies
http://technet.microsoft.com/en-us/library/dd897093.aspx
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG
http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Forefront UAG technical overview
http://technet.microsoft.com/en-us/library/ee690443.aspx