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 <u>www.isaserver.org</u> 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.

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).

			J Federate A	Cattings	
🥸 General	Muthentication	Session	Finapoint Access	Settings	Application Customizatio
figure Forefront UA	G access policies, and Ne	twork Access Protection (N	AP) policies. NAP policies are	e downloaded from a	a Network Policy Server (NPS)
Use NAP policies	3				
C Deny acces	is to the logon page from (	endpoints that do not have N	IAP installed and running		
C Use Forefro	nt UAG endpoint policies	when endpoints do not have	NAP installed and running		
Select NPS serve	rs:				
			.dd		
		Re	move		
C · A	•	D:1 15 1	- +-		
Session Access Pol	licy	Privileged Endpoint	Policy	Socket Forward	ing Component Installation Pol
Access method:		Access method:		Access method	:
📟 Endpoint policy	y only	Endpoint policy	only 💌	📟 Endpoint p	olicy only
Endpoint policy:		Endpoint policy:		Endpoint policy	
🔒 Default Sessio	n Access	🖌 🔒 Default Privilege	ed Endpoint 💌	Always	•
			_	-	Socket Forwarding company
					Socket Forwarding component
		] _			
					Edit Endpoint Policies
Do not block this	site in the Internet Explore	er pop-up blocker			
Prompt user befo	re retrieving information fro	om endpoint			

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.



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: <u>http://technet.microsoft.com/en-us/library/dd857328.aspx</u>)

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.

<u>Forefront UAG Endpoint Detection</u> 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.

📗 PortalHomePage				
🌀 🕞 🗸 🕨 🗸 Local Disk	(C:)	d Access Gateway 👻 von 👻 l	PortalHomePage 🔻	- [
Organize 🔻 Include in libra	ry ▼ Share with ▼ New folder			
🔶 Eavorites	Name ^	Date modified	Туре	Size
Desktop Downloads 🗐 Recent Places	App_transers	15.02.2012 10:38 15.02.2012 10:20 15.02.2012 10:21 15.02.2012 10:20	File folder File folder File folder	
Documents	鷆 Data 鷆 images	15.02.2012 10:20 15.02.2012 10:21	File folder File folder	
<ul> <li>J) Music</li> <li>E Pictures</li> <li>E Videos</li> </ul>	Limited OMA Scripts	15.02.2012 10:21 15.02.2012 10:21 15.02.2012 10:58	File folder File folder File folder	
Computer	UserControls	15.02.2012 10:21 15.02.2012 10:44	File folder File folder	
😻 DVD Drive (D:) Label I:	aspnet_menu_workaround ContentFrame.aspx	08.11.2009 17:09 27.10.2010 21:36	HTML Document ASPX File	1 KB 3 KB
Theorem	Default.aspx Help.aspx MainFrame.aspx	08.11.2009 17:09 08.11.2009 17:09 27.10.2010 21:36	ASPX File ASPX File ASPX File	2 KB 3 KB 2 KB
	portalcontainer PreLogOff.aspx	21.03.2012 05:52 08.11.2009 17:09	XML Document ASPX File	1 KB 1 KB
	Standard.master	08.11.2009 17:09 08.11.2009 17:09	MASTER File ASPX File	22 KB 1 KB
	」)Web.config 授 WhlClientSetup-All	22.09.2011 21:38 22.09.2011 22:21	CONFIG File Windows Installer P	21 KB 3.472 KB
	WhiClientSetup-Basic     WhiClientSetup-NetworkConnector	22.09.2011 22:26 22.09.2011 22:22	Windows Installer P Windows Installer P	3.472 KB 3.472 KB
	WhiClientSetup-NetWorkConnectorOnly	22.09.2011 22:11	Windows Installer P	3.472 KB 3.472 KB

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.

Forefro	nt UAG client components	×
i	For full site functionality, the site must be added to the allowed list of sites in the pop-up blocker of the browser. Do you want to add the site?	
	☑ Do not show this message again	
	<u>Y</u> es <u>N</u> o	

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.

Application and Network Access Portal	
Checking for device compliance	
© 2010 Microsoft Corporation. All rights reserved. <u>Terms and Conditions.</u>	

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.

🙀 Portal 🛛 👂 URL Inspection	n 📔 URL Settings 🛛 🗎 URL Set
🍣 General 🛛 🎎 Authentication 🛛 🍇	Session 🔗 Endpoint Access Settings 📄 Application Customization
Session Configuration Maximum concurrent sessions: Session threshold before issuing event: Maximum unauthenticated concurrent sessions: Unauthenticated session threshold before issuing event: Session timeout notification (seconds): Error message URL: InternalSite/InternalError.asp Disable component installation and activation Disable scripting for portal applications Verify user name with endpoint certificate Verify user name with endpoint certificate Verify user name with endpoint Session Cleat Verify user IP address to the session	Default Session Settings       900         Inactive session timeout (seconds):       900         Inactive session timeout (seconds):       120         Index       Delete cookies at logoff         Index       Delete cookies at logoff         Index       Pelete cookies at logoff         Index       Pelete cookies at logoff         Index       Prompt user to disconnect if the portal closes without logging off         Index       Prompt user to disconnect if the user does not disconnect         Privileged Session Settings       1800         Inactive session timeout (seconds):       1800         Image:       Trigger automatic logoff scheme after       1440         Inactive session timeout (seconds):       1800         Image:       Delete cookies at logoff       1800         Image:       Delete cookies at logoff       1440         Image:       Delete cookies at logoff       Request no browser caching         Activate Endpoint Session Cleanup component       Prompt user to disconnect if the portal is closed without logging off         Image:       Prompt user to disconnect if the user does not disconnect       Reopen the portal if the user does not disconnect

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.

Add Roles Wizard		×
Specify CA Type		
Before You Begin Server Roles AD CS Role Services Setup Type	A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA. C Root CA Select this option if you are installing the first or only certification authority in a public key infrastructure.	
CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress	Subordinate CA Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.	
Results	More about public key infrastructure (PKI)         < Previous	
Figure 9: Subordinate CA installation	on	

### 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.

Add Application Wizard	×
Step 1 - Select Application	
Select the application you want to publish.	
Built-in services:	
Certified Endpoint Enrollment	
C Web:	
Other Web Application (application specific hostname)	
C Client/server and legacy:	
Generic Client Application	
C Browser-embedded:	
Generic Browser-Embedded Application (multiple server 💌	
Terminal Services (TS)/Remote Desktop Services (RDS):	
RemoteApp	
,	
Help	
<back next=""></back>	Cancel

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.

Application	and Ne	twork Access	Portal
Log On			
User name:	administrat	tor	
Password:	•••••	•	
Language:	English (er	n-US) 👻	
		Windows Security	
This site is intended If you experience ac © 2010 Microsoft Corp	for authorize cess probler poration. All r	Confirm Certific Confirm this certifica click Cancel. Adr Issue Valic Click	ate te by clicking OK. If this is not the correct certificate, ninistrator er: my-root-CA I From: 31.12.2011 to 30.12.2012 chere to view certificate prope
			OK Cancel

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.

# Application and Network Access Portal

Endpoint Component Manager <ul> <li>(4.0.1773.10100)</li> </ul> <li>Endpoint Detection (ActiveX)</li> <li>(4.0.1773.10100)</li> <li>SSL Application Tunneling (ActiveX)</li> <li>(4.0.1773.10100)</li> <li>Socket Forwarding</li> <li>LSP: × NSP: ×</li> SSL Network Tunneling     Client: × Driver: ×           Device Session Cleanup (ActiveX) <ul> <li>(4.0.1773.10100) Not Running</li> </ul> Antivirus         A compliant antivirus was not detected           Personal Firewall         Win7 (Version not detected) Not Running           Operating System         Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit           Browser Version         Internet Explorer           User Agent         Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)           Sun JRE Version         Not detected           Domain         DOMAIN           Certified Device             Privileged Device             Privileged Device	Forefront UAG client component	s 🔠 🖓 🖓
Endpoint Detection (ActiveX)       ✓ (4.0.1773.10100)         SSL Application Tunneling (ActiveX)       ✓ (4.0.1773.10100)         Socket Forwarding       LSP: × NSP: ×         SSL Network Tunneling       Client: × Driver: ×         Device Session Cleanup (ActiveX)       ✓ (4.0.1773.10100) Not Running         Antivirus       A compliant antivirus was not detected         Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓	Endpoint Component Manager	
SSL Application Tunneling (ActiveX) <ul> <li>(4.0.1773.10100)</li> </ul> Socket Forwarding       LSP: X NSP: X         SSL Network Tunneling       Client X Driver: X         Device Session Cleanup (ActiveX) <ul> <li>(4.0.1773.10100) Not Running</li> </ul> Antivirus       A compliant antivirus was not detected <li>Personal Firewall</li> <li>Win7 (Version not detected) Not Running</li> Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓         To refresh this page, log off and then log on again.	Endpoint Detection (ActiveX)	
Socket Forwarding       LSP: X NSP: X         SSL Network Tunneling       Client X Driver: X         Device Session Cleanup (ActiveX)       I (4.0.1773.10100) Not Running         Antivirus       A compliant antivirus was not detected         Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET 6LR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓         To refresh this page, log off and then log on again.	SSL Application Tunneling (ActiveX)	
SSL Network Tunneling       Client. × Driver: ×         Device Session Cleanup (ActiveX)       ✓ (4.0.1773.10100) Not Running         Antivirus       A compliant antivirus was not detected         Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓         To refrest this page, log off and then log on again.	Socket Forwarding	LSP: × NSP: ×
Device Session Cleanup (ActiveX)       《 4.0.1773.10100) Not Running         Antivirus       A compliant antivirus was not detected         Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET 4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       Image: Agent firewall         Privileged Device       Image: Agent firewall	SSL Network Tunneling	Client: 🗙 Driver: 🗙
Antivirus       A compliant antivirus was not detected         Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓         To refresh this page, log off and then log on again.	Device Session Cleanup (ActiveX)	✓ (4.0.1773.10100) Not Running
Personal Firewall       Win7 (Version not detected) Not Running         Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       ✓         Privileged Device       ✓         To refresh this page, log off and then log on again.	Antivirus	A compliant antivirus was not detected
Operating System       Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit         Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       Image: Certified Device         Privileged Device       Image: Certified Device         To refrest this page, log off and then log on again.	Personal Firewall	Win7 (Version not detected) Not Running
Browser Version       Internet Explorer         User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       Image: Certified Device         Privileged Device       Image: Certified Device         To refrest this page, log off and then log on again.	Operating System	Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit
User Agent       Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)         Sun JRE Version       Not detected         Domain       DOMAIN         Certified Device       Image: Certified Device         Privileged Device       Image: Certified Device         To refresh this page, log off and then log on again.	Browser Version	Internet Explorer
Sun JRE Version     Not detected       Domain     DOMAIN       Certified Device     Image: Certified Device       Privileged Device     Image: Certified Device	User Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Domain     DOMAIN       Certified Device     ✓       Privileged Device     ✓       To refresh this page, log off and then log on again.	Sun JRE Version	Not detected
Certified Device     Image: Certified Device       Privileged Device     Image: Certified Device       To refresh this page, log off and then log on again.	Domain	DOMAIN
Privileged Device  To refresh this page, log off and then log on again.	Certified Device	1
To refresh this page, log off and then log on again.	Privileged Device	✓
· · · · · · · · · · · · · · · · · · ·	Тот	refresh this page, log off and then log on again.
	© 2010 Microsoft Corporation. All rights reserve	ved. Terms and Conditions.

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:0000001 "CanAddSites"=dword:00000000 "CanAddHttpSites"=dword:00000000 "PromptInvalidCertTrusted"=dword:00000000 "PromptInvalidCertUntrusted"=dword:00000001 "TrustedSite0"=<u>https://portal.isaserver.org</u>

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.

Policy Edito			X
Policy Sett	ings		
Name:	ISASERVER.ORG restricted corporate PC		
Explanatory	text added to the end-user Access Denied message:		
	four computer is not joined to the ISASERVER.ORG domain. Contact system administrator	t your 🔺	
Create a	policy from platform-specific policies		
Select p	atform-specific policies.		
Windows		Manage Wir	dows Policies
Mac OS:	<b>_</b>	Manage Ma	c OS Policies
Linux:	•	Manage Li	nux Policies
Other:			
C Create a	policy from expressions		
Select e	pressions.	Create Ex	pression
Available	expressions: Selected expressions:		
Always Any An Any Pei Any WI Any WI Corpora Disable Enable Endpoir Never	ivirus sonal Firewall (I Anti Spyware (I Antivirus (I Personal Firewall te Machine Citrix Client Printer Mapp SharePoint Integration w t Detection is Disabled		
P Help		ОК	Cancel

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.

Policy Editor		×
Policy Settings		
Name: ISASE	ERVER.ORG restricted corporate PC	
Explanatory text	added to the end-user Access Denied message:	
Your	computer is not joined to the ISASERVER.ORG d m administrator	omain. Contact your 🔺
Create a polic	y from platform-specific policies	
Select platfor	m-specific policies.	
Windows:	ISASERVERORGdomain (Windows)	▼ Manage Windows Policies
Mac OS:	Never	Manage Mac OS Policies
Linux:	Never	Manage Linux Policies
Other:	Never	
C Create a polic	y from expressions	
Select expres	sions.	Create Expression
Available exp	ressions: Selected express	ions:
Always Any Antivirus Any Persona Any WMI An Any WMI An Any WMI Per Corporate M Disable Citrix Enable Share Endpoint Det Never	s I Firewall ti Spyware tivirus rsonal Firewall achine c Client Printer Mapp Point Integration w tection is Disabled	
Help		OK Cancel

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.

0.1773.10100) 0.1773.10100) 0.1773.10100)
0.1773.10100) 0.1773.10100) 0.1773.10100) 0.1773.10100)
0.1773.10100) 0.1773.10100) 0.1773.10100) 0.1773.10100)
0.1773.10100) 0.1773.10100) 0.1773.10100)
0.1773.10100) 0.1773.10100)
0.1773.10100)
× NSP: ×
t: 🗙 Driver: 🗙
0.1773.10100)
A compliant antivirus was not detected
Win7 (Version not detected) Not Running
Windows 7 Professional 6.01.7601, Service Pack 1, 32-bit
Internet Explorer
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Not detected
DOMAIN
×
×

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