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

Microsoft Forefront UAG – Forefront UAG monitoring and debugging – part I

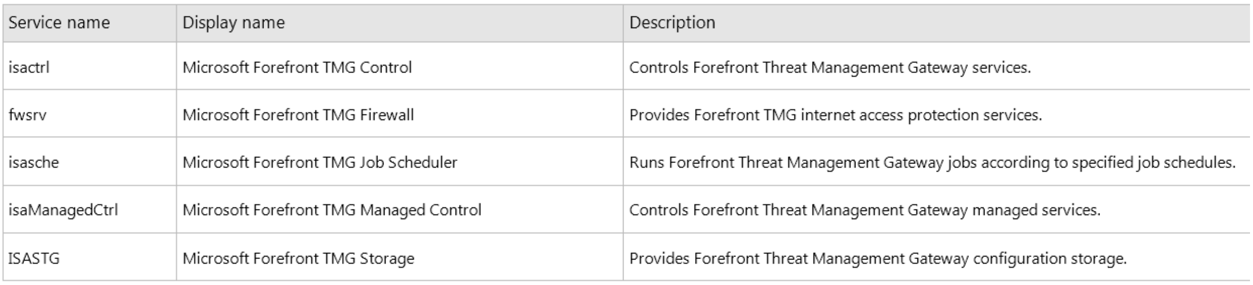
Abstract

This is a two part article series. In the first article we will talk about monitoring techniques in Forefront UAG to monitor user sessions, network traffic and many more. In part II of this article series will go deeper into Forefront UAG debugging and tracing capabilities.

Let's begin

Forefront UAG has some built in capabilities for monitoring the functionality of Forefront UAG and to monitor users accessing the Forefront UAG trunks.

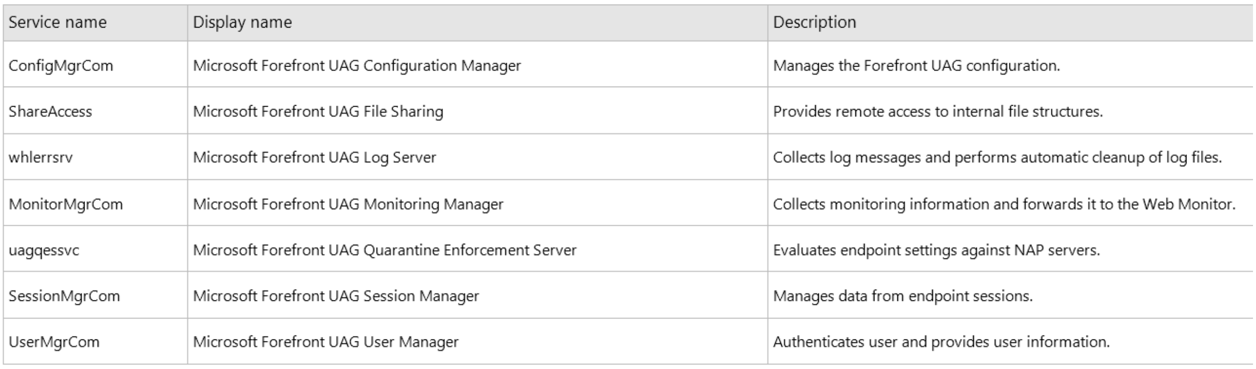
The first step in monitoring Forefront UAG is to keep an eye on the Forefront TMG and Forefront UAG services.
The following table lists all required Forefront TMG services which should be monitored carefully.



Service name	Display name	Description
isactrl	Microsoft Forefront TMG Control	Controls Forefront Threat Management Gateway services.
fwsrv	Microsoft Forefront TMG Firewall	Provides Forefront TMG internet access protection services.
isasche	Microsoft Forefront TMG Job Scheduler	Runs Forefront Threat Management Gateway jobs according to specified job schedules.
isaManagedCtrl	Microsoft Forefront TMG Managed Control	Controls Forefront Threat Management Gateway managed services.
ISASTG	Microsoft Forefront TMG Storage	Provides Forefront Threat Management Gateway configuration storage.

Table 1: Forefront TMG services (source: http://technet.microsoft.com/en-us/library/ff607335.aspx)

Table 2 lists all required Forefront UAG services.



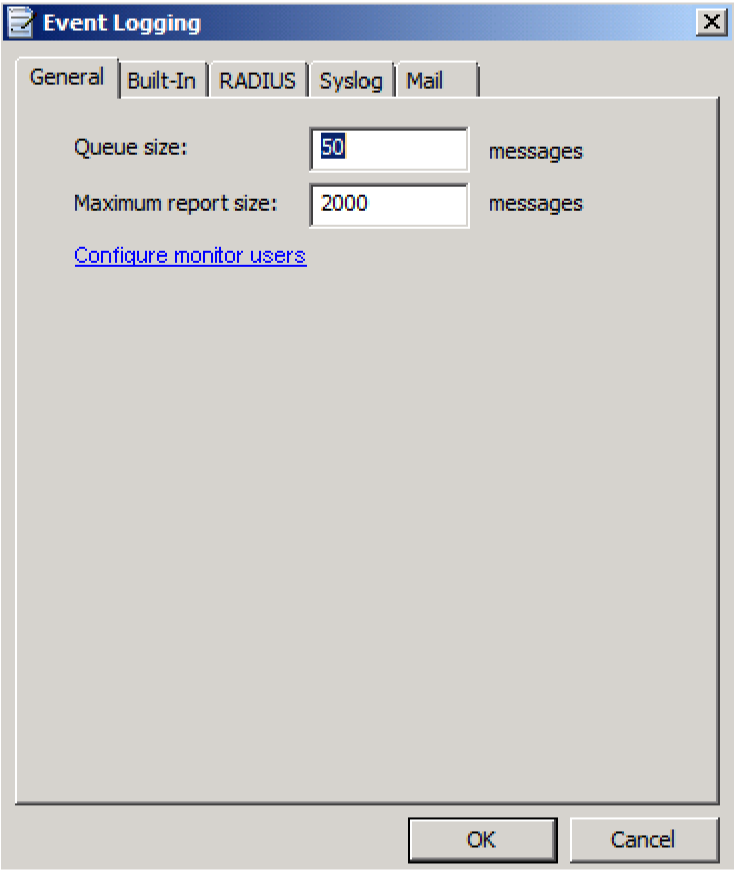
Service name	Display name	Description
ConfigMgrCom	Microsoft Forefront UAG Configuration Manager	Manages the Forefront UAG configuration.
ShareAccess	Microsoft Forefront UAG File Sharing	Provides remote access to internal file structures.
whlerrsrv	Microsoft Forefront UAG Log Server	Collects log messages and performs automatic cleanup of log files.
MonitorMgrCom	Microsoft Forefront UAG Monitoring Manager	Collects monitoring information and forwards it to the Web Monitor.
uagqessvc	Microsoft Forefront UAG Quarantine Enforcement Server	Evaluates endpoint settings against NAP servers.
SessionMgrCom	Microsoft Forefront UAG Session Manager	Manages data from endpoint sessions.
UserMgrCom	Microsoft Forefront UAG User Manager	Authenticates user and provides user information.

Table 2: Forefront UAG services (source: http://technet.microsoft.com/en-us/library/ff607335.aspx)

If you use the Microsoft System Center Operations Manager it is possible to monitor the Forefront TMG and UAG services and many more with SCOM and the help of TMG and UAG SCOM management packs.

Event logging

Forefront UAG and TMG stores many events in the Windows Server 2008 R2 event log and in addition it is possible to configure the Forefront UAG own monitoring. To configure general event logging in Forefront UAG start the UAG management console and navigate to *Admin – Event Log Settings*.

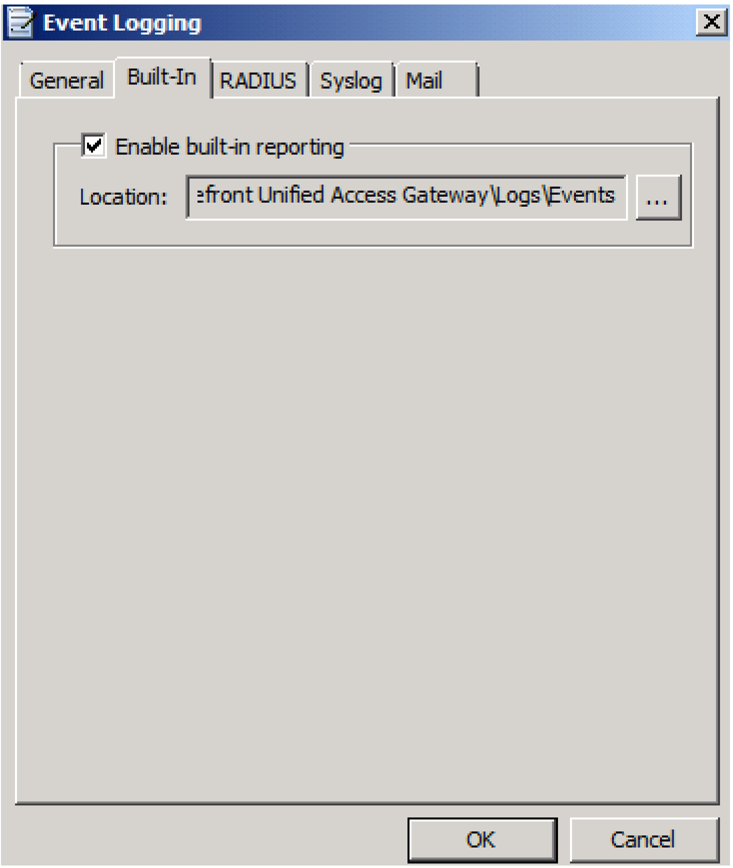


Queue size: 50 messages

Maximum report size: 2000 messages

Figure 1: Configure Forefront UAG logging

Forefront UAG has some built in log files which can be configured in the Forefront UAG management console as shown in the following screenshot.

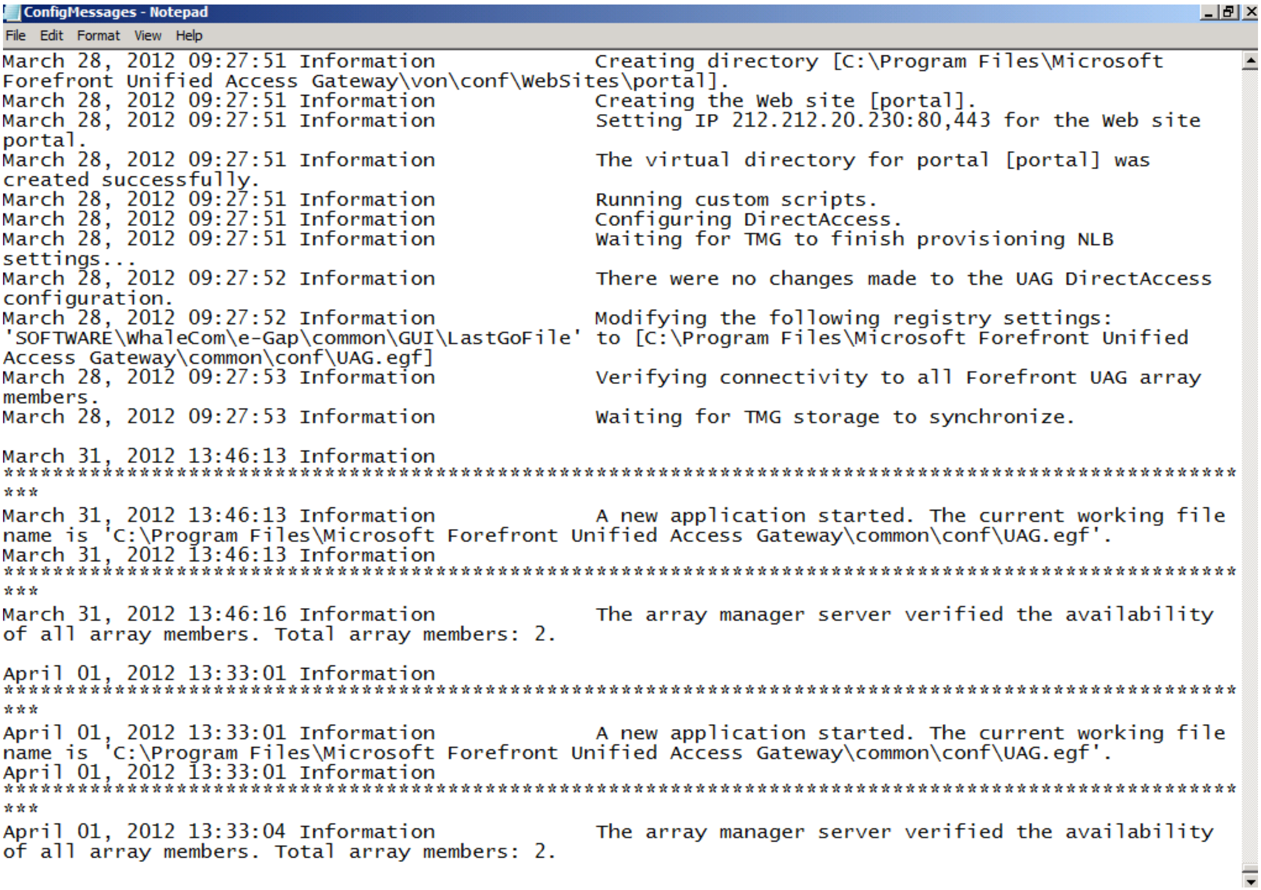


☑ Enable built-in reporting

Location: :front Unified Access Gateway\Logs\Events ...

Figure 2: UAG built in logging

The ConfigMessages log file shows the same content as the Forefront UAG Activation monitor. We will talk about the Forefront UAG Activation Monitor later in this article.



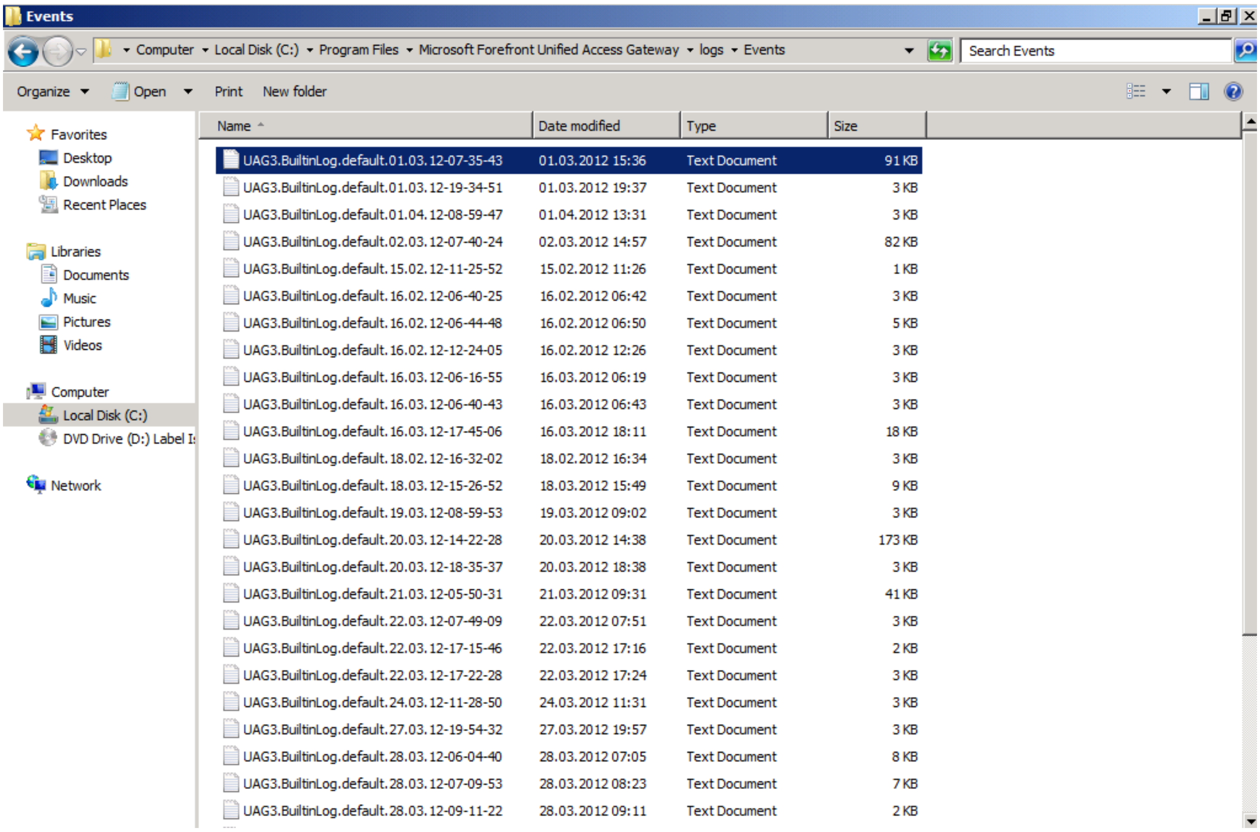
```
March 28, 2012 09:27:51 Information             Creating directory [C:\Program Files\Microsoft
Forefront Unified Access Gateway\von\conf\WebSites\portal].
March 28, 2012 09:27:51 Information             Creating the Web site [portal].
March 28, 2012 09:27:51 Information             Setting IP 212.212.20.230:80,443 for the Web site
portal.
March 28, 2012 09:27:51 Information             The virtual directory for portal [portal] was
created successfully.
March 28, 2012 09:27:51 Information             Running custom scripts.
March 28, 2012 09:27:51 Information             Configuring DirectAccess.
March 28, 2012 09:27:51 Information             Waiting for TMG to finish provisioning NLB
settings...
March 28, 2012 09:27:52 Information             There were no changes made to the UAG DirectAccess
configuration.
March 28, 2012 09:27:52 Information             Modifying the following registry settings:
'SOFTWARE\WhaleCom\e-Gap\common\GUI\LastGoFile' to [C:\Program Files\Microsoft Forefront Unified
Access Gateway\common\conf\UAG.egf]
March 28, 2012 09:27:53 Information             Verifying connectivity to all Forefront UAG array
members.
March 28, 2012 09:27:53 Information             Waiting for TMG storage to synchronize.

March 31, 2012 13:46:13 Information
****************************************************************************************************
***
March 31, 2012 13:46:13 Information             A new application started. The current working file
name is 'C:\Program Files\Microsoft Forefront Unified Access Gateway\common\conf\UAG.egf'.
March 31, 2012 13:46:13 Information
****************************************************************************************************
***
March 31, 2012 13:46:16 Information             The array manager server verified the availability
of all array members. Total array members: 2.

April 01, 2012 13:33:01 Information
****************************************************************************************************
***
April 01, 2012 13:33:01 Information             A new application started. The current working file
name is 'C:\Program Files\Microsoft Forefront Unified Access Gateway\common\conf\UAG.egf'.
April 01, 2012 13:33:01 Information
****************************************************************************************************
***
April 01, 2012 13:33:04 Information             The array manager server verified the availability
of all array members. Total array members: 2.
```

Figure 3: UAG ConfigMessages

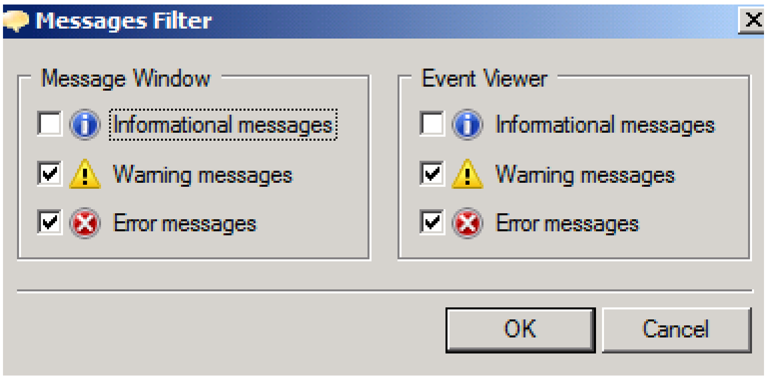
The BuiltIn logs of Forefront UAG can be very helpful for troubleshooting Forefront UAG and they are also very helpful for a better understanding how Forefront UAG works under the hood. You can find the builtIn log file in Logs – Events directory under the Forefront UAG installation directory.



Name	Date modified	Type	Size
UAG3.BuiltinLog.default.01.03.12-07-35-43	01.03.2012 15:36	Text Document	91 KB
UAG3.BuiltinLog.default.01.03.12-19-34-51	01.03.2012 19:37	Text Document	3 KB
UAG3.BuiltinLog.default.01.04.12-08-59-47	01.04.2012 13:31	Text Document	3 KB
UAG3.BuiltinLog.default.02.03.12-07-40-24	02.03.2012 14:57	Text Document	82 KB
UAG3.BuiltinLog.default.15.02.12-11-25-52	15.02.2012 11:26	Text Document	1 KB
UAG3.BuiltinLog.default.16.02.12-06-40-25	16.02.2012 06:42	Text Document	3 KB
UAG3.BuiltinLog.default.16.02.12-06-44-48	16.02.2012 06:50	Text Document	5 KB
UAG3.BuiltinLog.default.16.02.12-12-24-05	16.02.2012 12:26	Text Document	3 KB
UAG3.BuiltinLog.default.16.03.12-06-16-55	16.03.2012 06:19	Text Document	3 KB
UAG3.BuiltinLog.default.16.03.12-06-40-43	16.03.2012 06:43	Text Document	3 KB
UAG3.BuiltinLog.default.16.03.12-17-45-06	16.03.2012 18:11	Text Document	18 KB
UAG3.BuiltinLog.default.18.02.12-16-32-02	18.02.2012 16:34	Text Document	3 KB
UAG3.BuiltinLog.default.18.03.12-15-26-52	18.03.2012 15:49	Text Document	9 KB
UAG3.BuiltinLog.default.19.03.12-08-59-53	19.03.2012 09:02	Text Document	3 KB
UAG3.BuiltinLog.default.20.03.12-14-22-28	20.03.2012 14:38	Text Document	173 KB
UAG3.BuiltinLog.default.20.03.12-18-35-37	20.03.2012 18:38	Text Document	3 KB
UAG3.BuiltinLog.default.21.03.12-05-50-31	21.03.2012 09:31	Text Document	41 KB
UAG3.BuiltinLog.default.22.03.12-07-49-09	22.03.2012 07:51	Text Document	3 KB
UAG3.BuiltinLog.default.22.03.12-17-15-46	22.03.2012 17:16	Text Document	2 KB
UAG3.BuiltinLog.default.22.03.12-17-22-28	22.03.2012 17:24	Text Document	3 KB
UAG3.BuiltinLog.default.24.03.12-11-28-50	24.03.2012 11:31	Text Document	3 KB
UAG3.BuiltinLog.default.27.03.12-19-54-32	27.03.2012 19:57	Text Document	3 KB
UAG3.BuiltinLog.default.28.03.12-06-04-40	28.03.2012 07:05	Text Document	8 KB
UAG3.BuiltinLog.default.28.03.12-07-09-53	28.03.2012 08:23	Text Document	7 KB
UAG3.BuiltinLog.default.28.03.12-09-11-22	28.03.2012 09:11	Text Document	2 KB

Figure 4: UAG builtin logfiles

Administrators are able to filter Forefront UAG messages to reduce the amount of displayed events in the event viewer or the message window in the Forefront UAG management console.



Message Window

- ☐ Informational messages
- ☑ Warning messages
- ☑ Error messages

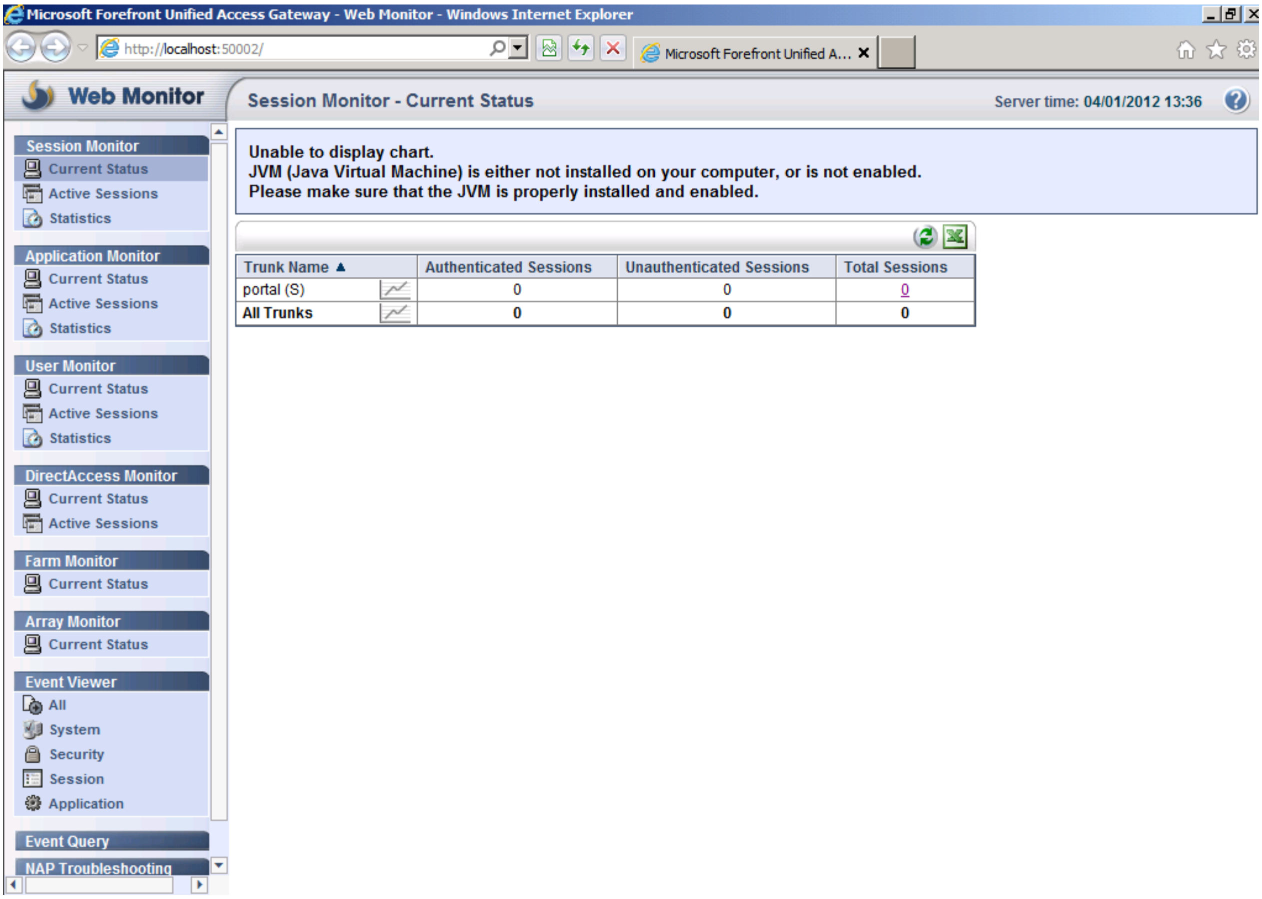
Event Viewer

- ☐ Informational messages
- ☑ Warning messages
- ☑ Error messages

Figure 5: UAG message filter

Forefront UAG Web Monitor

The Forefront UAG Web Monitor should be the first place for Forefront UAG Administrators to monitor the Forefront UAG Server. The Web Monitor is divided into different monitors. You are able to monitor the Active Sessions of users which are connected to the Forefront UAG portal trunks. You are also able to monitor the sessions for published applications in a Forefront UAG portal trunk and if you configured Forefront UAG for DirectAccess it is also possible to monitor the active DirectAccess sessions and to get an overwiev about the Forefront UAG DirectAccess state on the Forefront UAG Server. If you configured Forefront UAG as an array you are able to monitor the state of the Forefront UAG array.



Session Monitor - Current Status

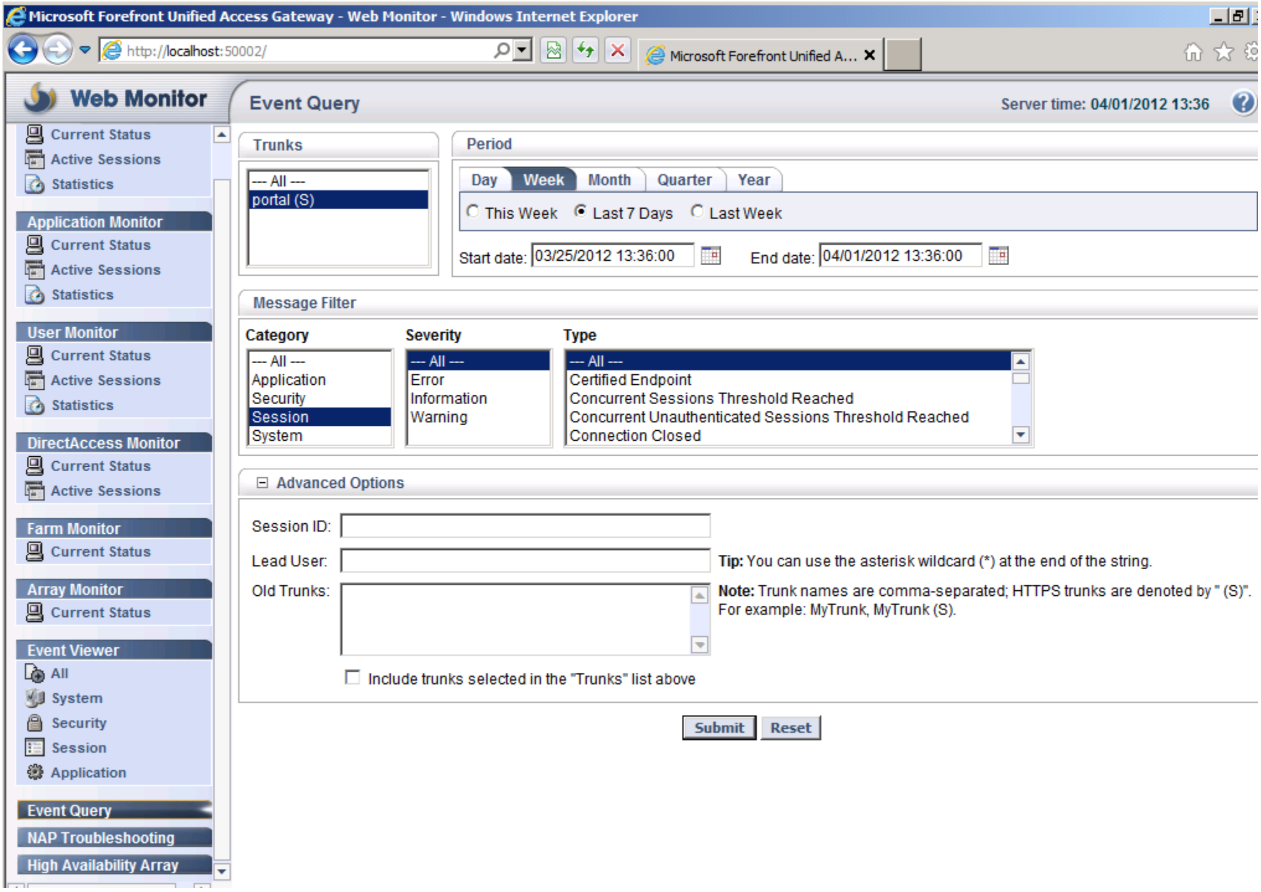
Server time: 04/01/2012 13:36

Unable to display chart.
JVM (Java Virtual Machine) is either not installed on your computer, or is not enabled.
Please make sure that the JVM is properly installed and enabled.

Trunk Name ▲	Authenticated Sessions	Unauthenticated Sessions	Total Sessions
portal (S)	0	0	0
All Trunks	**0**	**0**	**0**

Figure 6: Forefront UAG Web Monitor

With the Web Monitor you are able to filter all Forefront UAG messages for different trunks and Forefront UAG categories.



Event Query

Server time: 04/01/2012 13:36

Trunks: --- All --- | portal (S)

Period: Day | Week | Month | Quarter | Year

○ This Week ● Last 7 Days ○ Last Week

Start date: 03/25/2012 13:36:00 End date: 04/01/2012 13:36:00

Message Filter

Category: --- All --- | Application | Security | Session | System

Severity: --- All --- | Error | Information | Warning

Type: --- All --- | Certified Endpoint | Concurrent Sessions Threshold Reached | Concurrent Unauthenticated Sessions Threshold Reached | Connection Closed

Advanced Options

Session ID:

Lead User: **Tip:** You can use the asterisk wildcard (*) at the end of the string.

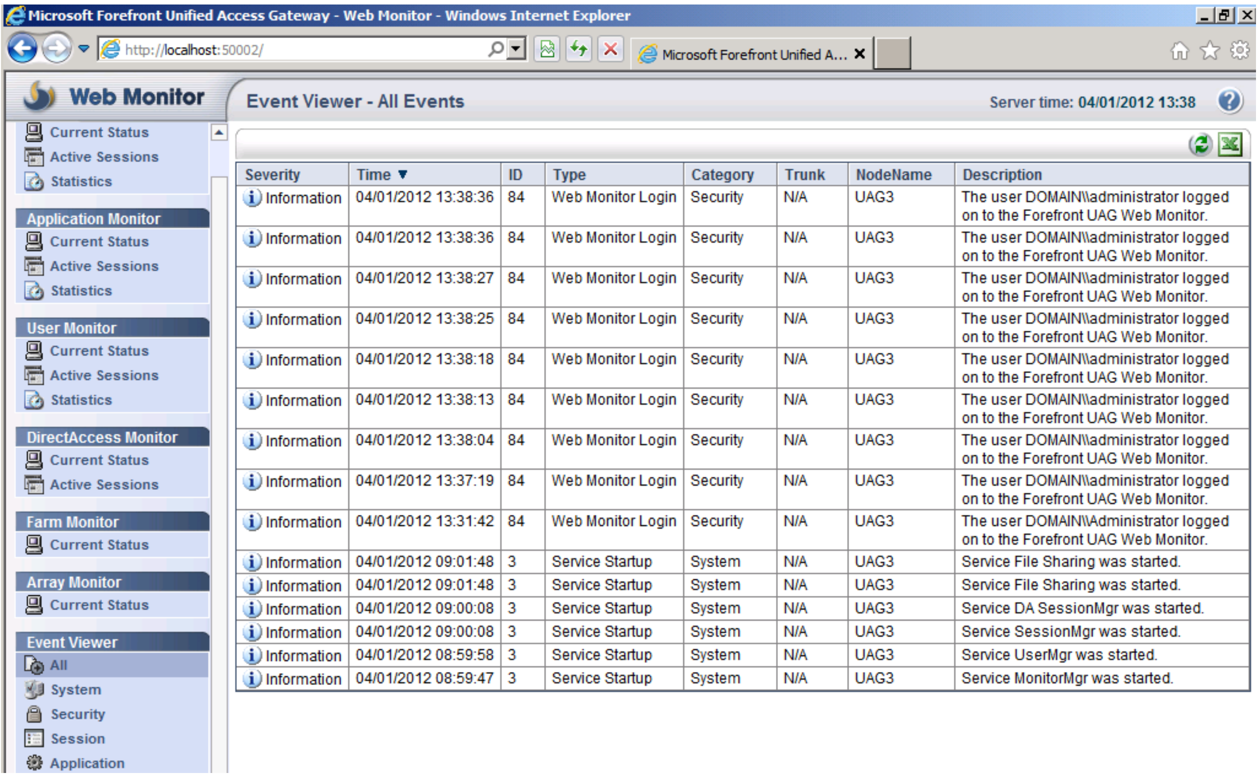
Old Trunks: **Note:** Trunk names are comma-separated; HTTPS trunks are denoted by " (S)". For example: MyTrunk, MyTrunk (S).

□ Include trunks selected in the "Trunks" list above

Submit Reset

Figure 7: Forefront UAG Web Monitor and custom event query

The Forefront UAG Web Monitor also allows you to filter / display Forefront UAG events. It is possible to filter events in Forefront UAG for the System, Security, Application and Session as shown in the following screenshot.



Event Viewer - All Events

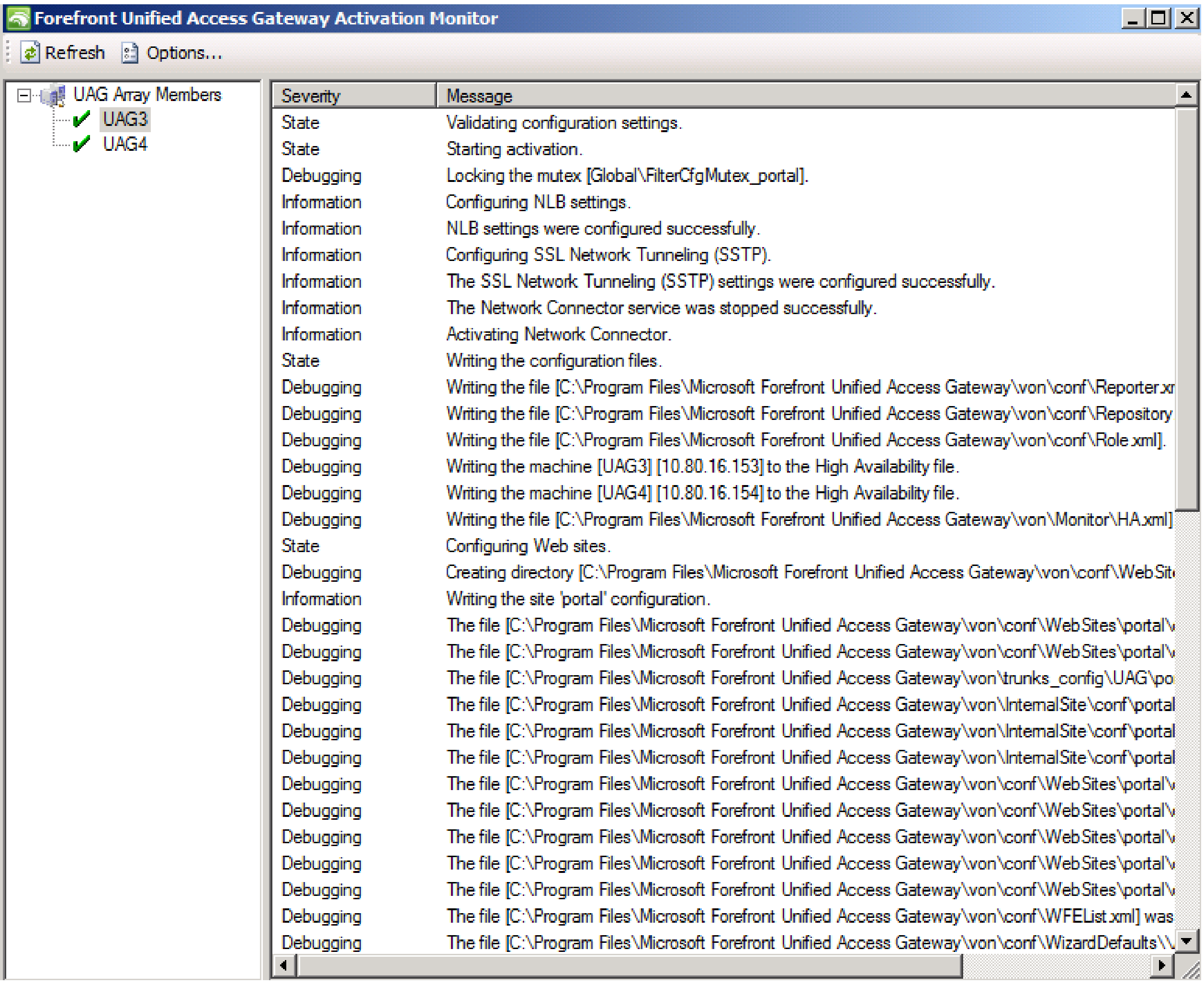
Server time: 04/01/2012 13:38

Severity	Time ▼	ID	Type	Category	Trunk	NodeName	Description
Information	04/01/2012 13:38:36	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:36	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:27	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:25	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:18	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:13	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:38:04	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:37:19	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 13:31:42	84	Web Monitor Login	Security	N/A	UAG3	The user DOMAIN\\Administrator logged on to the Forefront UAG Web Monitor.
Information	04/01/2012 09:01:48	3	Service Startup	System	N/A	UAG3	Service File Sharing was started.
Information	04/01/2012 09:01:48	3	Service Startup	System	N/A	UAG3	Service File Sharing was started.
Information	04/01/2012 09:00:08	3	Service Startup	System	N/A	UAG3	Service DA SessionMgr was started.
Information	04/01/2012 09:00:08	3	Service Startup	System	N/A	UAG3	Service SessionMgr was started.
Information	04/01/2012 08:59:58	3	Service Startup	System	N/A	UAG3	Service UserMgr was started.
Information	04/01/2012 08:59:47	3	Service Startup	System	N/A	UAG3	Service MonitorMgr was started.

Figure 8: Forefront UAG Event Viewer

Forefront UAG Activation Monitor

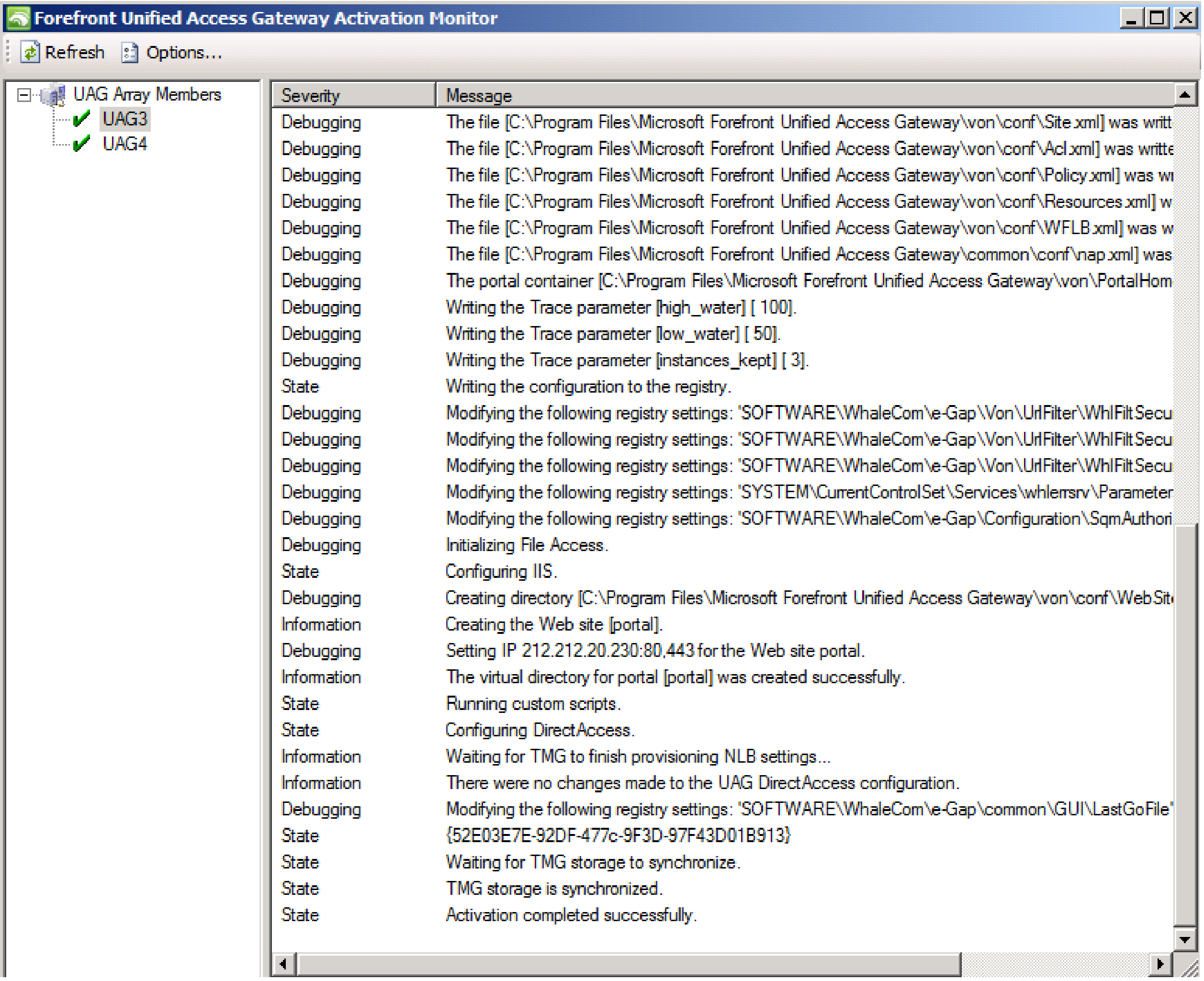
The Forefront UAG Activation monitor monitors all synchronization activities between the different Forefront UAG components and the underlying Forefront TMG Server. Forefront UAG synchronizes the configuration change made in Forefront UAG with Forefront TMG. The UAG Activation Monitor should always be used to see if configuration changes in Forefront UAG are sucessfully applied to the different Forefront UAG components and the Forefront TMG configuration.



Severity	Message
State	Validating configuration settings.
State	Starting activation.
Debugging	Locking the mutex [Global\FilterCfgMutex_portal].
Information	Configuring NLB settings.
Information	NLB settings were configured successfully.
Information	Configuring SSL Network Tunneling (SSTP).
Information	The SSL Network Tunneling (SSTP) settings were configured successfully.
Information	The Network Connector service was stopped successfully.
Information	Activating Network Connector.
State	Writing the configuration files.
Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Reporter.x
Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Repository
Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Role.xml].
Debugging	Writing the machine [UAG3] [10.80.16.153] to the High Availability file.
Debugging	Writing the machine [UAG4] [10.80.16.154] to the High Availability file.
Debugging	Writing the file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\Monitor\HA.xml]
State	Configuring Web sites.
Debugging	Creating directory [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSit
Information	Writing the site 'portal' configuration.
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\trunks_config\UAG\po
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\InternalSite\conf\portal
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\InternalSite\conf\portal
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\InternalSite\conf\portal
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSites\portal\
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WFEList.xml] was
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WizardDefaults\

Figure 9: Forefront UAG Activation Monitor

At the end of the following screesnhot you can see the integration between Forefront UAG and Forefront TMG. Forefront UAG synchronizes the configuration with the Forefront TMG storage (AD-LDS) and after that you see the message that the Forefront UAG activation was successfully.

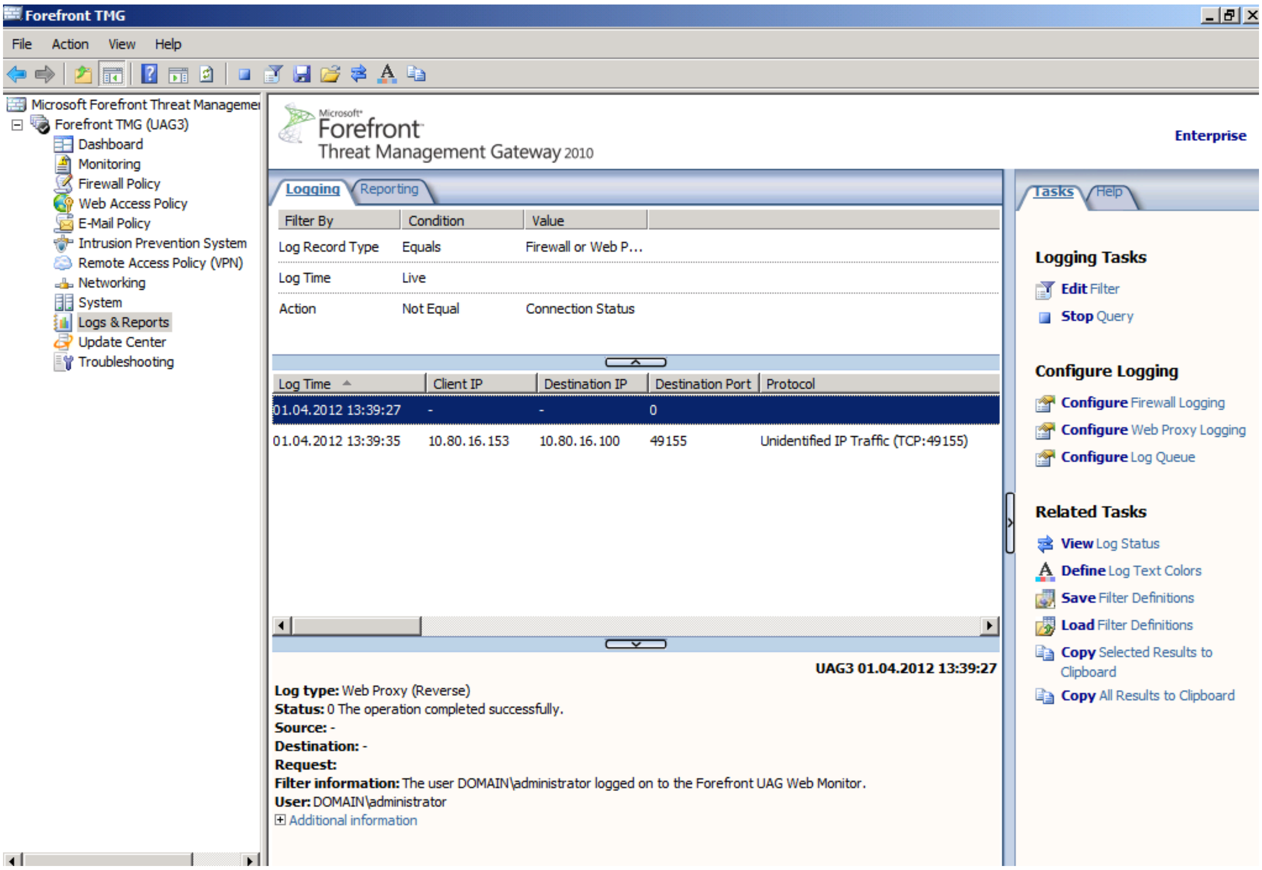


Severity	Message
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Site.xml] was writt
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Acl.xml] was writte
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Policy.xml] was wı
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\Resources.xml] w
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WFLB.xml] was w
Debugging	The file [C:\Program Files\Microsoft Forefront Unified Access Gateway\common\conf\nap.xml] was
Debugging	The portal container [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\PortalHom
Debugging	Writing the Trace parameter [high_water] [100].
Debugging	Writing the Trace parameter [low_water] [50].
Debugging	Writing the Trace parameter [instances_kept] [3].
State	Writing the configuration to the registry.
Debugging	Modifying the following registry settings: 'SOFTWARE\WhaleCom\e-Gap\Von\UrlFilter\WhlFiltSecu
Debugging	Modifying the following registry settings: 'SOFTWARE\WhaleCom\e-Gap\Von\UrlFilter\WhlFiltSecu
Debugging	Modifying the following registry settings: 'SOFTWARE\WhaleCom\e-Gap\Von\UrlFilter\WhlFiltSecu
Debugging	Modifying the following registry settings: 'SYSTEM\CurrentControlSet\Services\whlerrsrv\Parameter
Debugging	Modifying the following registry settings: 'SOFTWARE\WhaleCom\e-Gap\Configuration\SqmAuthori
Debugging	Initializing File Access.
State	Configuring IIS.
Debugging	Creating directory [C:\Program Files\Microsoft Forefront Unified Access Gateway\von\conf\WebSit
Information	Creating the Web site [portal].
Debugging	Setting IP 212.212.20.230:80,443 for the Web site portal.
Information	The virtual directory for portal [portal] was created successfully.
State	Running custom scripts.
State	Configuring DirectAccess.
Information	Waiting for TMG to finish provisioning NLB settings...
Information	There were no changes made to the UAG DirectAccess configuration.
Debugging	Modifying the following registry settings: 'SOFTWARE\WhaleCom\e-Gap\common\GUI\LastGoFile'
State	{52E03E7E-92DF-477c-9F3D-97F43D01B913}
State	Waiting for TMG storage to synchronize.
State	TMG storage is synchronized.
State	Activation completed successfully.

Figure 10: Forefront UAG Activation Monitor

Forefront TMG monitoring

Most of the Forefront UAG configuration changes must be made through the Forefront UAG management console and the Forefront UAG Web Monitor is a great resource for monitoring Forefront UAG activities but if you must have access to live logging activities for troubleshooting access from external clients to the Forefront UAG Server you must use the Forefront TMG live logging capabilities to see the allowed/denied network traffic from external clients as shown in the following screenshot.



Filter By	Condition	Value
Log Record Type	Equals	Firewall or Web P...
Log Time	Live	
Action	Not Equal	Connection Status

Log Time	Client IP	Destination IP	Destination Port	Protocol
01.04.2012 13:39:27	-	-	0	
01.04.2012 13:39:35	10.80.16.153	10.80.16.100	49155	Unidentified IP Traffic (TCP:49155)

UAG3 01.04.2012 13:39:27

Log type: Web Proxy (Reverse)
Status: 0 The operation completed successfully.
Source: -
Destination: -
Request:
Filter information: The user DOMAIN\administrator logged on to the Forefront UAG Web Monitor.
User: DOMAIN\administrator
⊞ Additional information

Figure 11: Forefront TMG live logging

Conclusion

In this article I tried to give you some helpful information how to monitor your Forefront UAG Server environment, how to monitor user sessions and how to use Forefront TMG for live logging Forefront UAG traffic. In part II of this article series will go deeper into Forefront UAG debugging and tracing capabilities.

Related links

Monitoring the status of Forefront UAG services
http://technet.microsoft.com/en-us/library/ff607335.aspx
Monitoring Forefront UAG DirectAccess SP1
http://technet.microsoft.com/en-us/library/gg313780.aspx
Planning for monitoring and logging
http://technet.microsoft.com/en-us/library/dd897042.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