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

Microsoft Forefront TMG – TMG Storage 101

Abstract

In this article I will show you in which places Forefront TMG Standard and Enterprise stores the Forefront TMG configuration. I will show you the differences between the data storage location in Forefront TMG Standard and Forefront TMG Enterprise managed by a central EMS. We will also cover how Forefront TMG stores a copy of the TMG configuration in the local registry.

Let’s begin

Before we start explaining how Forefront TMG stores it’s configuration data, I would like to explain the new terminology used in Forefront TMG. There are two different terms which are now commonly used:

- EMS (Enterprise Management Server)
- CSS (Configuration Storage Server)

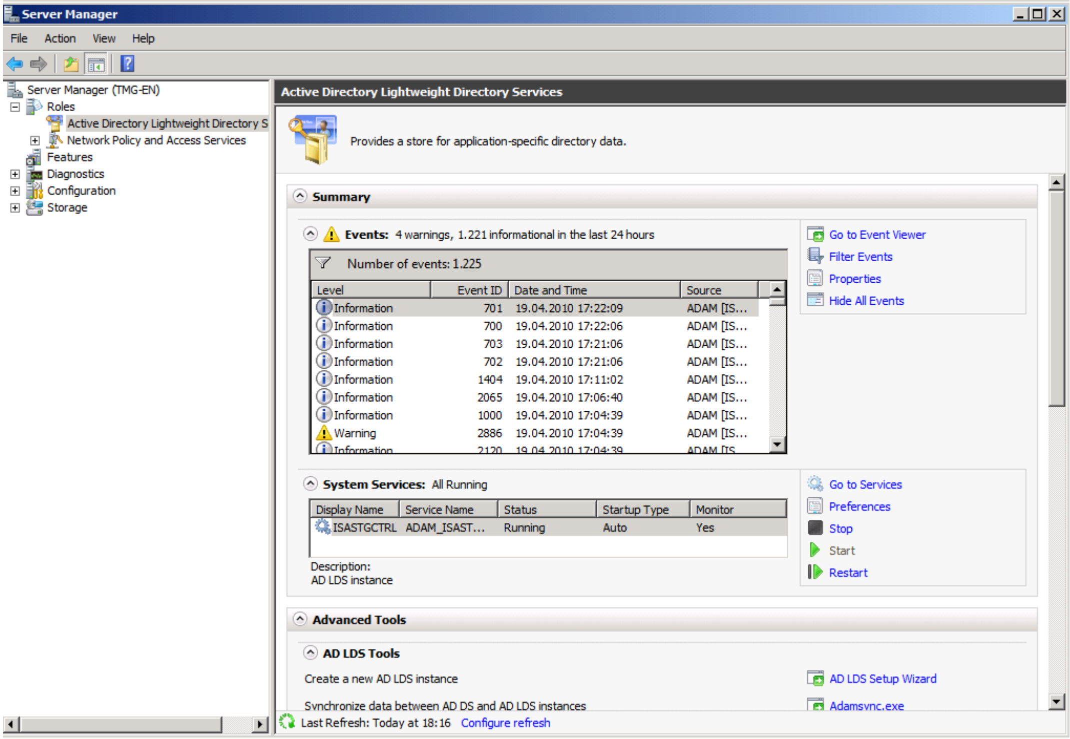
EMS

The Enterprise Management Server is a server which is used to manage a TMG Enterprise Array or even possibly, a standalone server. The EMS must be installed on a member Server with no other Forefront TMG services. Installation on a Windows Domain Controller is also not supported. You don’t have to buy a TMG license for the installed EMS. If you are experienced with ISA Server 2006 Enterprise, the Forefront TMG EMS is nearly the same as the Configuration Storage Server (CSS) used in ISA Server 2006 Enterprise with a few differences. With Forefront TMG it is now possible to join or disjoin an array after TMG installation. This makes enterprise configuration much more flexible because you doesn’t have to uninstall and reinstall the Forefront TMG Server to join other TMG arrays. It is also possible to update a Forefront TMG Standard version to Forefront TMG Enterprise without reinstallation.

CSS

The Configuration Storage Server (CSS) is used for all local TMG installations and provides storage for the TMG Server configuration. Every Forefront TMG server has a local CSS. When the TMG administrator joins the Server to a TMG Array, the local TMG Server will use the Enterprise Management Server (EMS). When the Enterprise CSS is applied, the local CSS (AD-LDS instance) will be disabled.

Let us first have a look at the installed Active Directory Lightweight Directory service installation. The Forefront TMG Setup preparation tool installs the Windows Server AD-LDS. AD-LDS will be used by Forefront TMG to save the TMG configuration data.



Active Directory Lightweight Directory Services

Provides a store for application-specific directory data.

Summary

Events: 4 warnings, 1.221 informational in the last 24 hours

Number of events: 1.225

Level	Event ID	Date and Time	Source
Information	701	19.04.2010 17:22:09	ADAM [IS...
Information	700	19.04.2010 17:22:06	ADAM [IS...
Information	703	19.04.2010 17:21:06	ADAM [IS...
Information	702	19.04.2010 17:21:06	ADAM [IS...
Information	1404	19.04.2010 17:11:02	ADAM [IS...
Information	2065	19.04.2010 17:06:40	ADAM [IS...
Information	1000	19.04.2010 17:04:39	ADAM [IS...
Warning	2886	19.04.2010 17:04:39	ADAM [IS...
Information	2120	19.04.2010 17:04:39	ADAM [IS

System Services: All Running

Display Name	Service Name	Status	Startup Type	Monitor
ISASTGCTRL	ADAM_ISAST...	Running	Auto	Yes

Description:
AD LDS instance

Advanced Tools

AD LDS Tools

Create a new AD LDS instance

Synchronize data between AD DS and AD LDS instances

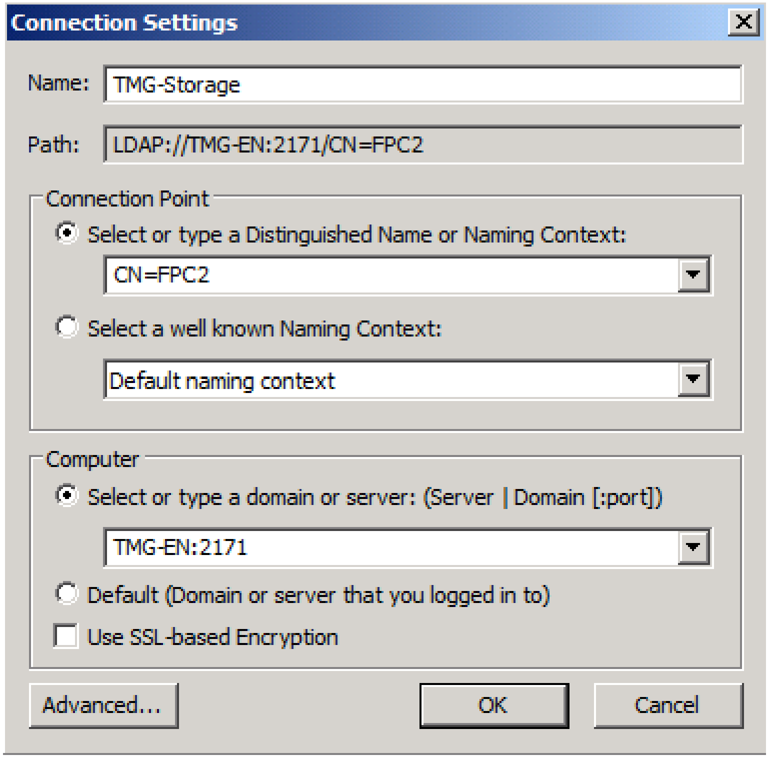
Last Refresh: Today at 18:16

Figure 1: Installed AD-LDS services

The ISASTGCTRL service is the AD-LDS service for the Windows AD-LDS instance. The Forefront TMG storage service (ISASTG) is responsible for storing the TMG configuration in AD-LDS and the local Windows registry.

Connecting to the Forefront TMG configuration via ADSIEDIT

Because the AD-LDS instance uses a directory structure like its big brother Active Directory, it is possible to connect to the AD-LDS instance via tools like LDP ADSIEDIT and other LDAP tools. For the example in this article we will use ADSIEDIT to connect to the AD-LDS instance. Start ADSIEDIT, and select CN=FPC2 as the CN, specify the server name with port 2171 and after that you will be able to connect to the data store of the AD-LDS instance.


Connection Settings

Name: TMG-Storage

Path: LDAP://TMG-EN:2171/CN=FPC2

Connection Point

● Select or type a Distinguished Name or Naming Context:

CN=FPC2

○ Select a well known Naming Context:

Default naming context

Computer

● Select or type a domain or server: (Server | Domain [:port])

TMG-EN:2171

○ Default (Domain or server that you logged in to)

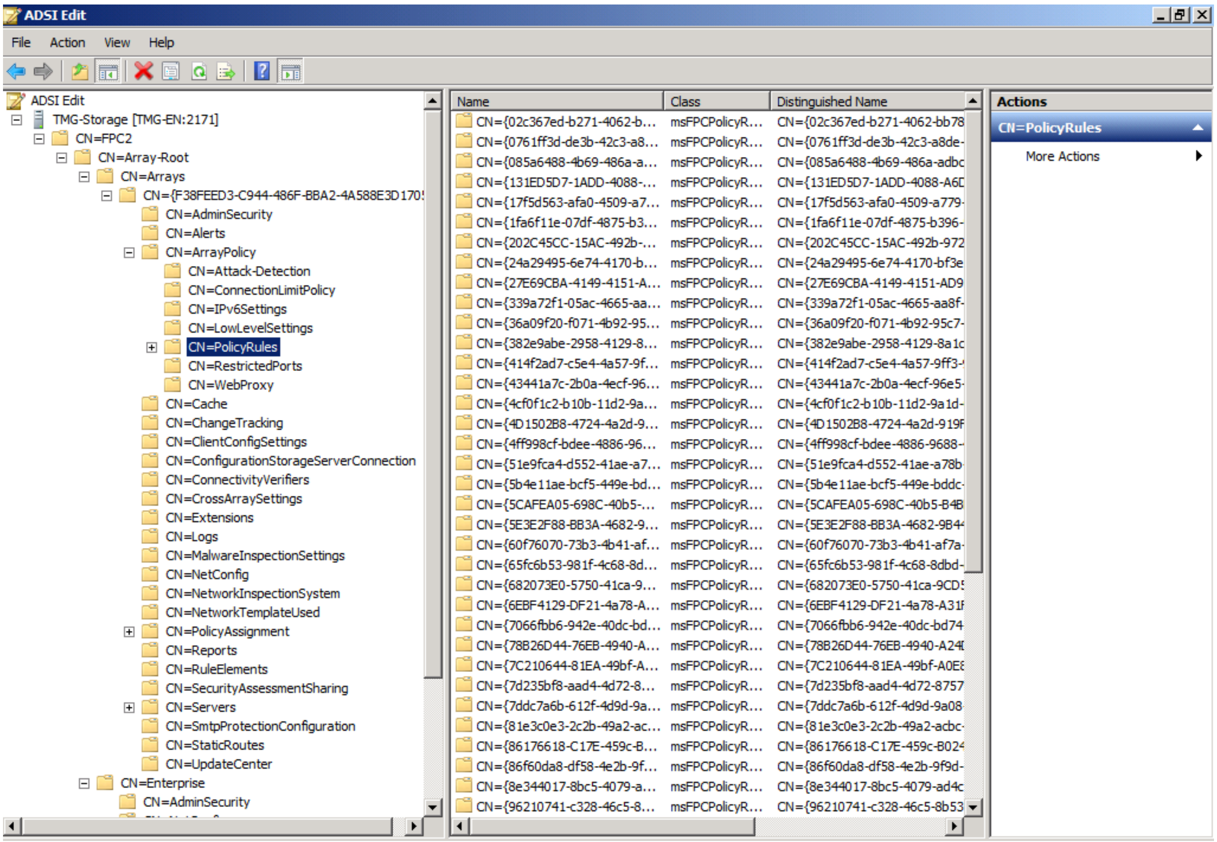
□ Use SSL-based Encryption

Figure 2: Connect to AD-LDS via ADSIEDIT

As shown in the following screenshot you will see entire Forefront TMG configuration.

Caution:

It is possible to change and add entries in the TMG configuration via ADSIEDIT but I strongly recommend not using ADSIEDIT to modify settings, if you are not absolutely familiar about the effects of such changes.



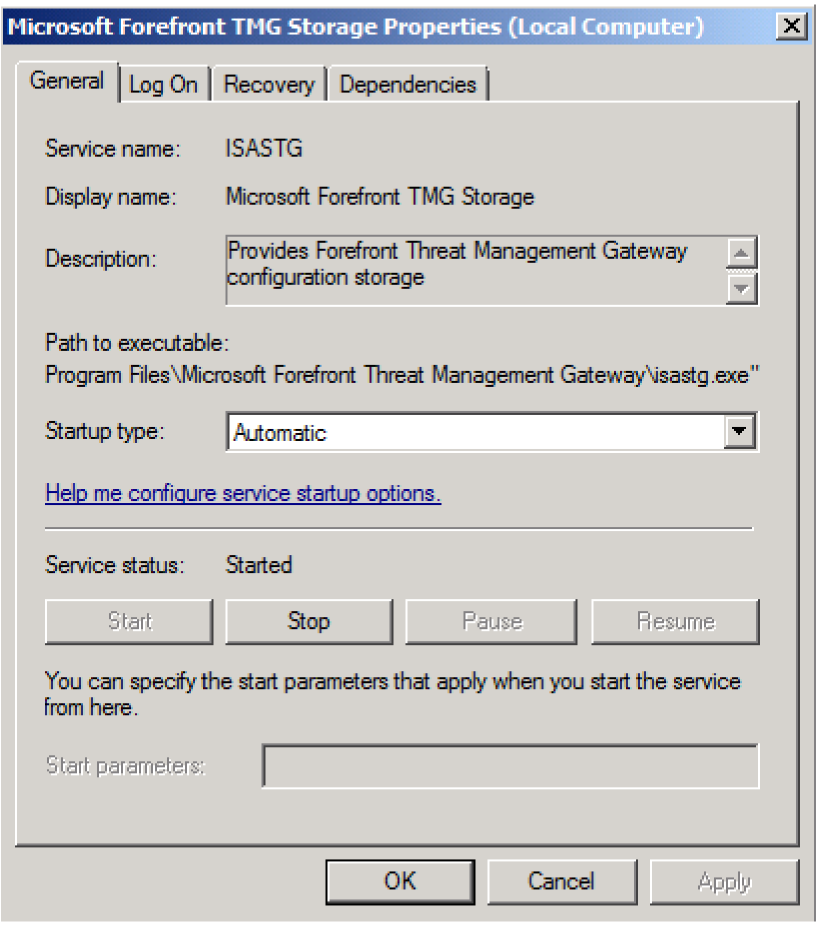
```
ADSI Edit
  TMG-Storage [TMG-EN:2171]
    CN=FPC2
      CN=Array-Root
        CN=Arrays
          CN={F38FEED3-C944-486F-BBA2-4A588E3D170
            CN=AdminSecurity
            CN=Alerts
            CN=ArrayPolicy
              CN=Attack-Detection
              CN=ConnectionLimitPolicy
              CN=IPv6Settings
              CN=LowLevelSettings
              CN=PolicyRules
              CN=RestrictedPorts
              CN=WebProxy
            CN=Cache
            CN=ChangeTracking
            CN=ClientConfigSettings
            CN=ConfigurationStorageServerConnection
            CN=ConnectivityVerifiers
            CN=CrossArraySettings
            CN=Extensions
            CN=Logs
            CN=MalwareInspectionSettings
            CN=NetConfig
            CN=NetworkInspectionSystem
            CN=NetworkTemplateUsed
            CN=PolicyAssignment
            CN=Reports
            CN=RuleElements
            CN=SecurityAssessmentSharing
            CN=Servers
            CN=SmtpProtectionConfiguration
            CN=StaticRoutes
            CN=UpdateCenter
        CN=Enterprise
          CN=AdminSecurity
```

Name	Class	Distinguished Name
CN={02c367ed-b271-4062-b...	msFPCPolicyR...	CN={02c367ed-b271-4062-bb78
CN={0761ff3d-de3b-42c3-a8...	msFPCPolicyR...	CN={0761ff3d-de3b-42c3-a8de-
CN={085a6488-4b69-486a-a...	msFPCPolicyR...	CN={085a6488-4b69-486a-adbc
CN={131ED5D7-1ADD-4088-...	msFPCPolicyR...	CN={131ED5D7-1ADD-4088-A6D
CN={17f5d563-afa0-4509-a7...	msFPCPolicyR...	CN={17f5d563-afa0-4509-a779-
CN={1fa6f11e-07df-4875-b3...	msFPCPolicyR...	CN={1fa6f11e-07df-4875-b396-
CN={202C45CC-15AC-492b-...	msFPCPolicyR...	CN={202C45CC-15AC-492b-972
CN={24a29495-6e74-4170-b...	msFPCPolicyR...	CN={24a29495-6e74-4170-bf3e
CN={27E69CBA-4149-4151-A...	msFPCPolicyR...	CN={27E69CBA-4149-4151-AD9
CN={339a72f1-05ac-4665-aa...	msFPCPolicyR...	CN={339a72f1-05ac-4665-aa8f-
CN={36a09f20-f071-4b92-95...	msFPCPolicyR...	CN={36a09f20-f071-4b92-95c7-
CN={382e9abe-2958-4129-8...	msFPCPolicyR...	CN={382e9abe-2958-4129-8a1c
CN={414f2ad7-c5e4-4a57-9f...	msFPCPolicyR...	CN={414f2ad7-c5e4-4a57-9ff3-
CN={43441a7c-2b0a-4ecf-96...	msFPCPolicyR...	CN={43441a7c-2b0a-4ecf-96e5-
CN={4cf0f1c2-b10b-11d2-9a...	msFPCPolicyR...	CN={4cf0f1c2-b10b-11d2-9a1d-
CN={4D1502B8-4724-4a2d-9...	msFPCPolicyR...	CN={4D1502B8-4724-4a2d-919F
CN={4ff998cf-bdee-4886-96...	msFPCPolicyR...	CN={4ff998cf-bdee-4886-9688-
CN={51e9fca4-d552-41ae-a7...	msFPCPolicyR...	CN={51e9fca4-d552-41ae-a78b
CN={5b4e11ae-bcf5-449e-bd...	msFPCPolicyR...	CN={5b4e11ae-bcf5-449e-bddc-
CN={5CAFEA05-698C-40b5-...	msFPCPolicyR...	CN={5CAFEA05-698C-40b5-B4B
CN={5E3E2F88-BB3A-4682-9...	msFPCPolicyR...	CN={5E3E2F88-BB3A-4682-9B4
CN={60f76070-73b3-4b41-af...	msFPCPolicyR...	CN={60f76070-73b3-4b41-af7a-
CN={65fc6b53-981f-4c68-8d...	msFPCPolicyR...	CN={65fc6b53-981f-4c68-8dbd-
CN={682073E0-5750-41ca-9...	msFPCPolicyR...	CN={682073E0-5750-41ca-9CD
CN={6EBF4129-DF21-4a78-A...	msFPCPolicyR...	CN={6EBF4129-DF21-4a78-A31
CN={7066fbb6-942e-40dc-bd...	msFPCPolicyR...	CN={7066fbb6-942e-40dc-bd74
CN={78B26D44-76EB-4940-A...	msFPCPolicyR...	CN={78B26D44-76EB-4940-A24
CN={7C210644-81EA-49bf-A...	msFPCPolicyR...	CN={7C210644-81EA-49bf-A0E
CN={7d235bf8-aad4-4d72-8...	msFPCPolicyR...	CN={7d235bf8-aad4-4d72-8757
CN={7ddc7a6b-612f-4d9d-9a...	msFPCPolicyR...	CN={7ddc7a6b-612f-4d9d-9a08
CN={81e3c0e3-2c2b-49a2-ac...	msFPCPolicyR...	CN={81e3c0e3-2c2b-49a2-acbc-
CN={86176618-C17E-459c-B...	msFPCPolicyR...	CN={86176618-C17E-459c-B02
CN={86f60da8-df58-4e2b-9f...	msFPCPolicyR...	CN={86f60da8-df58-4e2b-9f9d-
CN={8e344017-8bc5-4079-a...	msFPCPolicyR...	CN={8e344017-8bc5-4079-ad4c
CN={96210741-c328-46c5-8...	msFPCPolicyR...	CN={96210741-c328-46c5-8b53

Figure 3: Forefront TMG configuration in ADSIEDIT

Microsoft Forefront TMG Storage

During the Forefront TMG installation a service called Microsoft Forefront TMG Storage (ISASTG) will be created which provides Forefront TMG configuration storage and for interaction with the local registry which is used to save the TMG configuration locally.



Microsoft Forefront TMG Storage Properties (Local Computer)

Service name: ISASTG

Display name: Microsoft Forefront TMG Storage

Description: Provides Forefront Threat Management Gateway configuration storage

Path to executable:
Program Files\Microsoft Forefront Threat Management Gateway\isastg.exe"

Startup type: Automatic

Help me configure service startup options.

Service status: Started

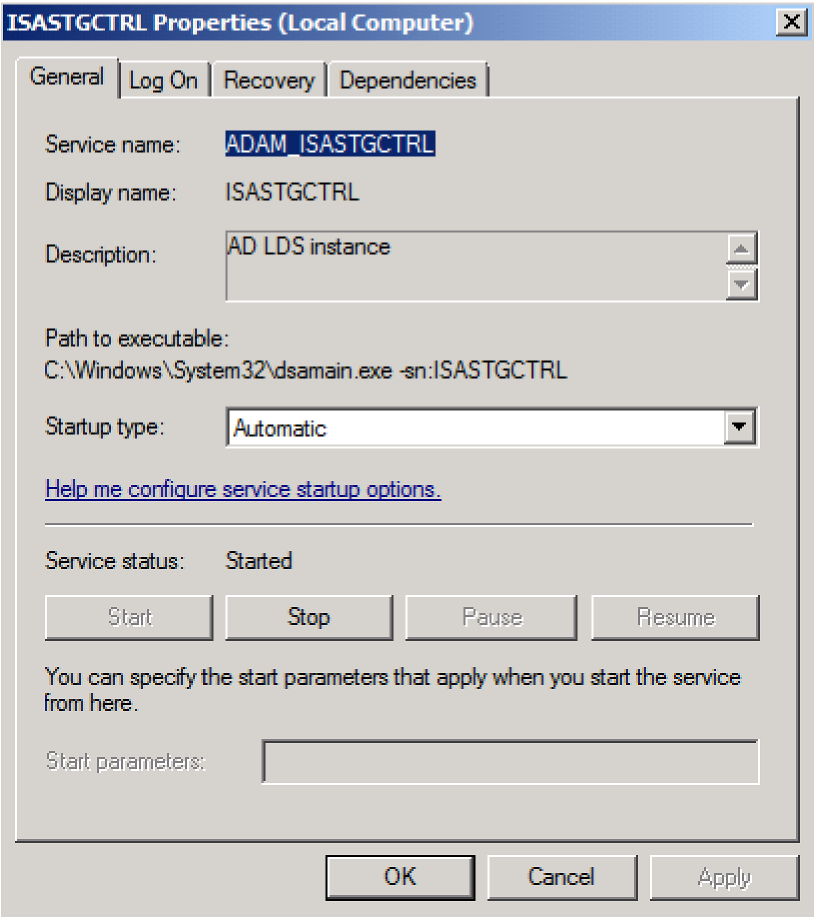
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 4: Forefront TMG storage (ISASTG)

ADAM_ISASTGCTRL

The AD-LDS instance installs a service called ADAM_ISASTGCTRL which is used to control the local installed AD-LDS instance. This service will be stopped and set to startup type DISABLED when the Forefront TMG Enterprise Server joins an array managed by a Forefront EMS.



ISASTGCTRL Properties (Local Computer)

Service name: ADAM_ISASTGCTRL

Display name: ISASTGCTRL

Description: AD LDS instance

Path to executable:
C:\Windows\System32\dsamain.exe -sn:ISASTGCTRL

Startup type: Automatic

Help me configure service startup options.

Service status: Started

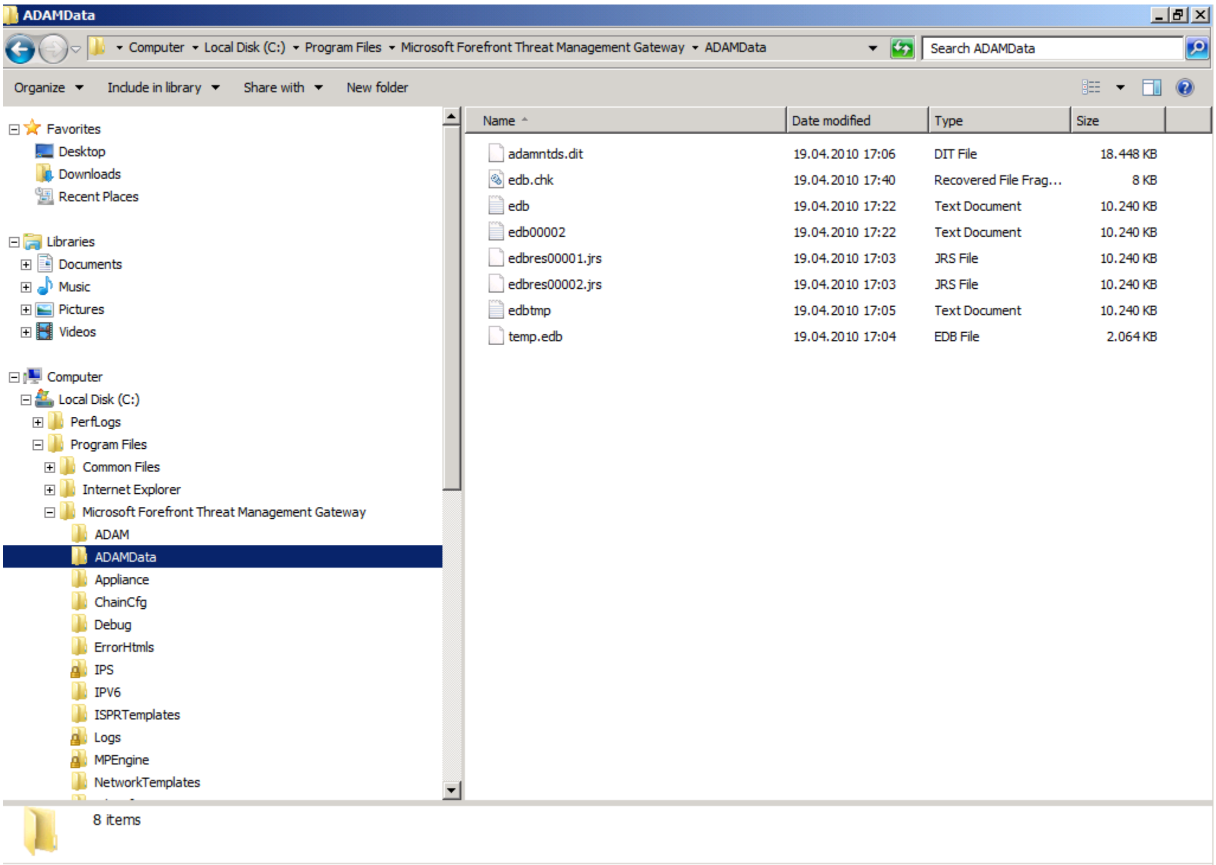
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 5: AD-LDS instance

AD-LDS database location

The Microsoft Forefront TMG AD-LDS instance is stored in the installation directory of Forefront TMG in a subdirectory called ADAMData.



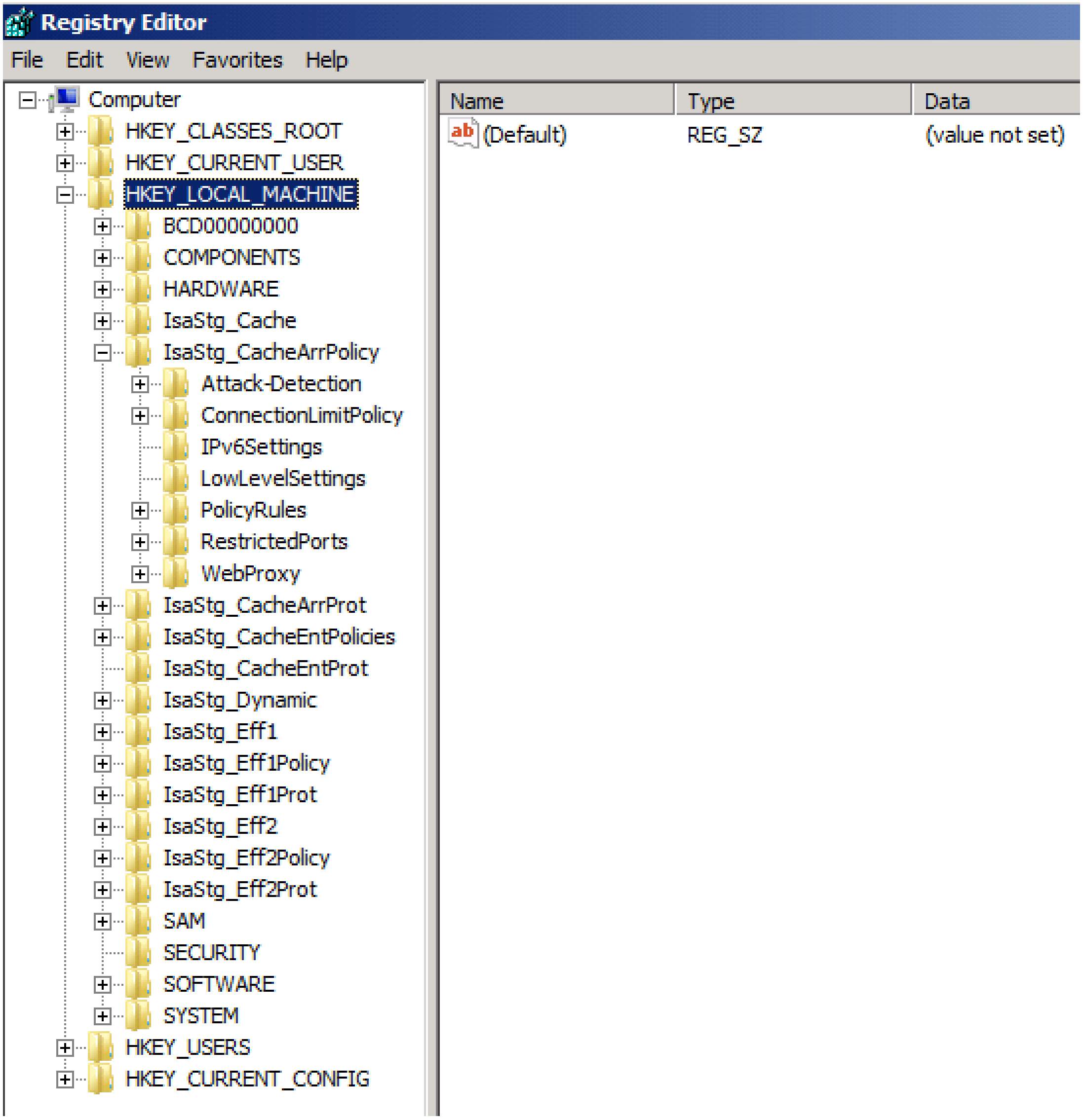
Computer ▸ Local Disk (C:) ▸ Program Files ▸ Microsoft Forefront Threat Management Gateway ▸ ADAMData

Name	Date modified	Type	Size
adamntds.dit	19.04.2010 17:06	DIT File	18.448 KB
edb.chk	19.04.2010 17:40	Recovered File Frag...	8 KB
edb	19.04.2010 17:22	Text Document	10.240 KB
edb00002	19.04.2010 17:22	Text Document	10.240 KB
edbres00001.jrs	19.04.2010 17:03	JRS File	10.240 KB
edbres00002.jrs	19.04.2010 17:03	JRS File	10.240 KB
edbtmp	19.04.2010 17:05	Text Document	10.240 KB
temp.edb	19.04.2010 17:04	EDB File	2.064 KB

Figure 6: AD-LDS database location

Forefront TMG configuration in the Registry

The Forefront TMG configuration will be stored in the local AD-LDS instance if the Forefront TMG Server is a standalone server or managed by a local array. A copy of the Forefront TMG configuration is also stored in the local registry under HKEY_LOCAL_MACHINE. Every time a new TMG configuration change has been applied by the Forefront TMG management console, the local registry gets updated. The Forefront TMG storage service is responsible for this task.



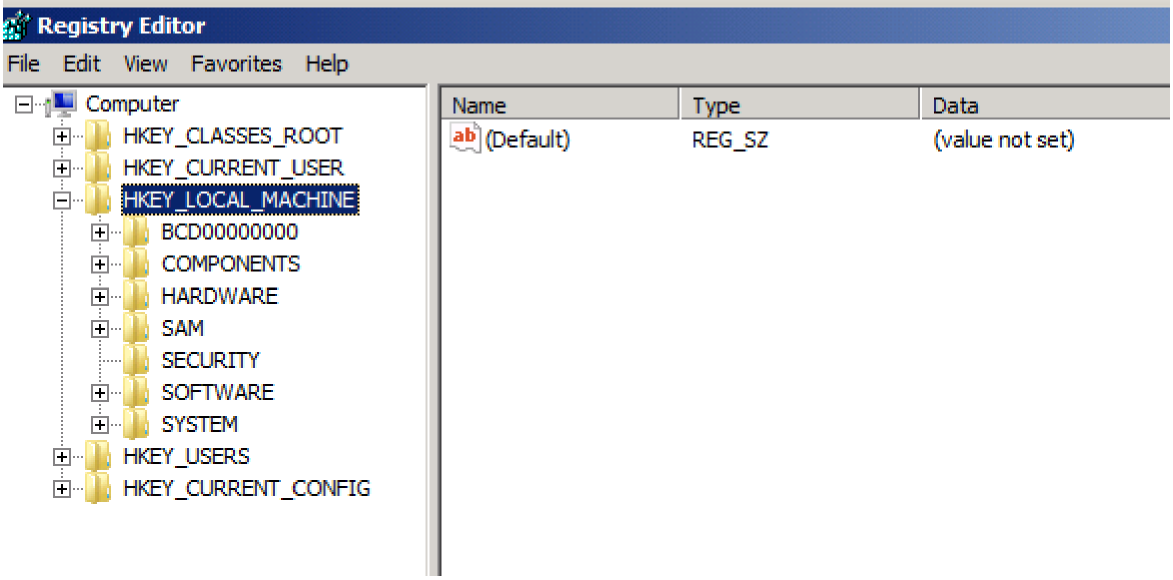
```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    COMPONENTS
    HARDWARE
    IsaStg_Cache
    IsaStg_CacheArrPolicy
      Attack-Detection
      ConnectionLimitPolicy
      IPv6Settings
      LowLevelSettings
      PolicyRules
      RestrictedPorts
      WebProxy
    IsaStg_CacheArrProt
    IsaStg_CacheEntPolicies
    IsaStg_CacheEntProt
    IsaStg_Dynamic
    IsaStg_Eff1
    IsaStg_Eff1Policy
    IsaStg_Eff1Prot
    IsaStg_Eff2
    IsaStg_Eff2Policy
    IsaStg_Eff2Prot
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

Name	Type	Data
ab (Default)	REG_SZ	(value not set)

Figure 7: Forefront TMG configuration in the registry

Stopped TMG services (TMG Storage)

If you stop the Forefront TMG Storage service, the registry keys will be deleted and automatically recreated after the service has successfully started again.

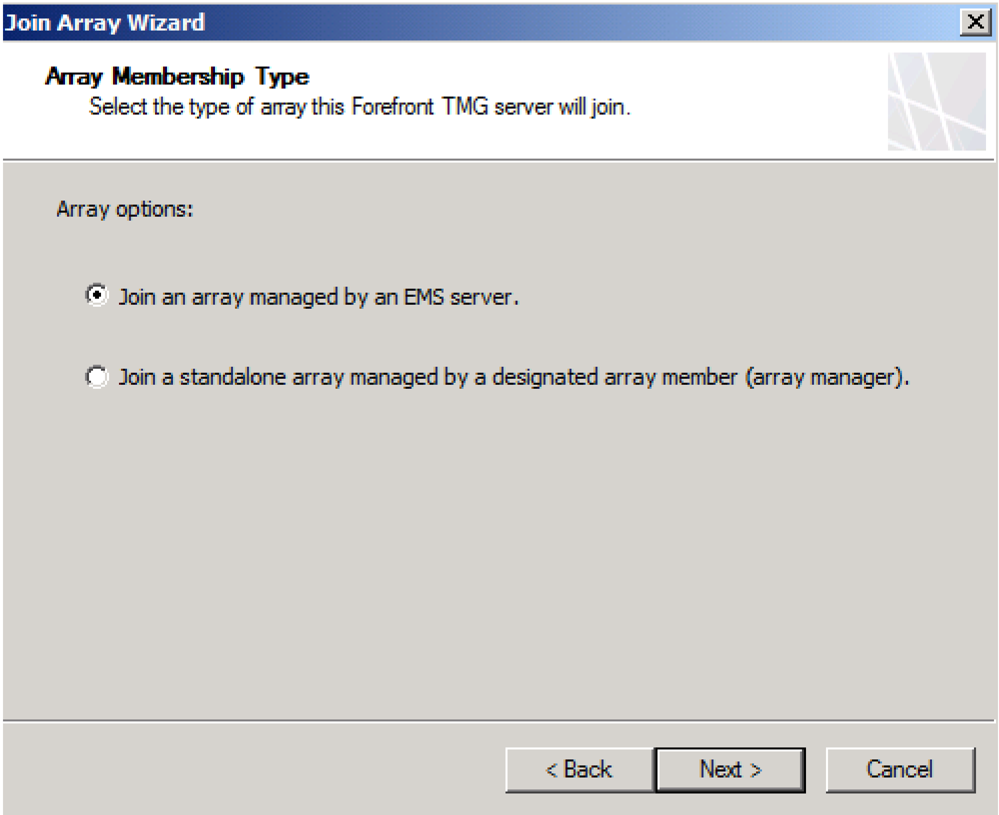


Name	Type	Data
(Default)	REG_SZ	(value not set)

Figure 8: No Forefront TMG registry entries after the TMG storage service has been stopped

Join Array

If you decide to join the Forefront TMG server to an array managed by an EMS (Enterprise Management Server), this is possible without uninstalling and reinstalling Forefront TMG. Start the TMG Management console and start the Join Array Wizard.



Array Membership Type

Select the type of array this Forefront TMG server will join.

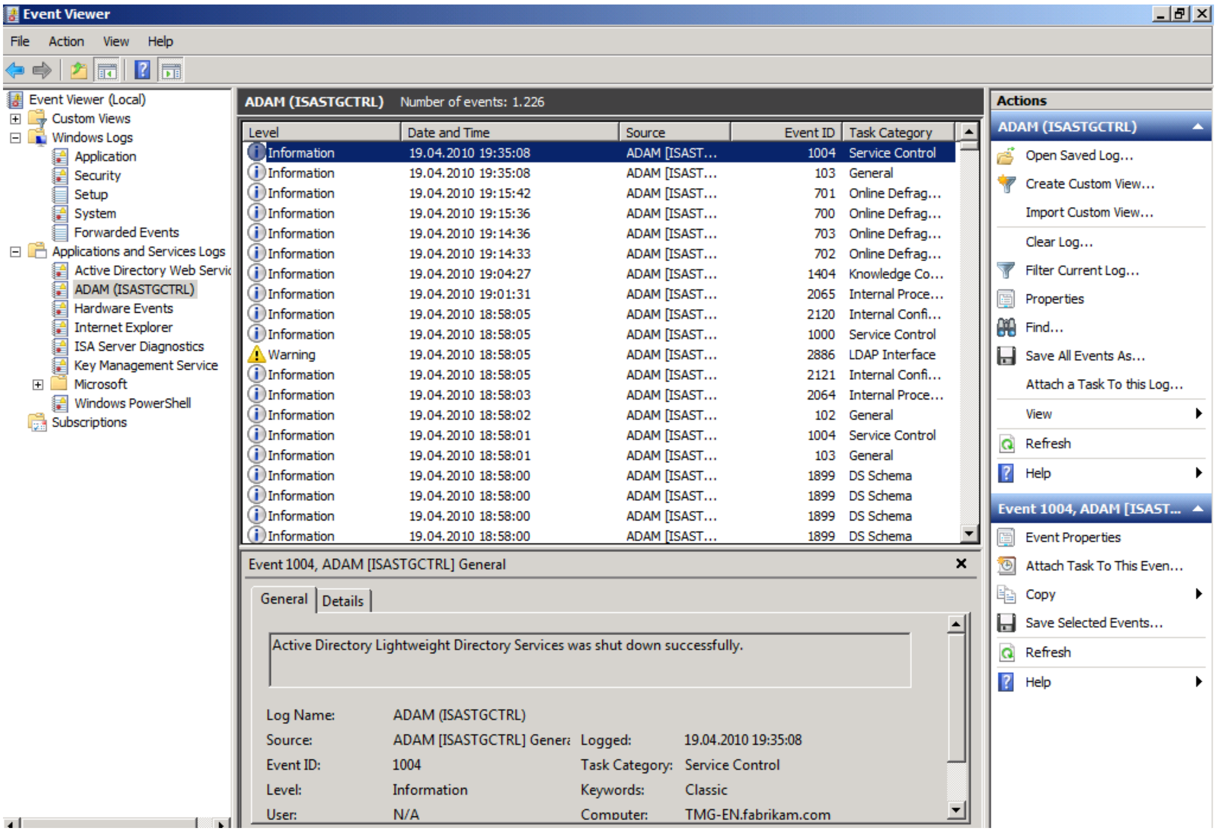
Array options:

● Join an array managed by an EMS server.

○ Join a standalone array managed by a designated array member (array manager).

Figure 9: Join an array managed by an EMS Server

During joining the TMG EMS, the local ISASTGCTRL service will be stopped and disabled.



ADAM (ISASTGCTRL) Number of events: 1.226

Level	Date and Time	Source	Event ID	Task Category
Information	19.04.2010 19:35:08	ADAM [ISAST...	1004	Service Control
Information	19.04.2010 19:35:08	ADAM [ISAST...	103	General
Information	19.04.2010 19:15:42	ADAM [ISAST...	701	Online Defrag...
Information	19.04.2010 19:15:36	ADAM [ISAST...	700	Online Defrag...
Information	19.04.2010 19:14:36	ADAM [ISAST...	703	Online Defrag...
Information	19.04.2010 19:14:33	ADAM [ISAST...	702	Online Defrag...
Information	19.04.2010 19:04:27	ADAM [ISAST...	1404	Knowledge Co...
Information	19.04.2010 19:01:31	ADAM [ISAST...	2065	Internal Proce...
Information	19.04.2010 18:58:05	ADAM [ISAST...	2120	Internal Confi...
Information	19.04.2010 18:58:05	ADAM [ISAST...	1000	Service Control
Warning	19.04.2010 18:58:05	ADAM [ISAST...	2886	LDAP Interface
Information	19.04.2010 18:58:05	ADAM [ISAST...	2121	Internal Confi...
Information	19.04.2010 18:58:03	ADAM [ISAST...	2064	Internal Proce...
Information	19.04.2010 18:58:02	ADAM [ISAST...	102	General
Information	19.04.2010 18:58:01	ADAM [ISAST...	1004	Service Control
Information	19.04.2010 18:58:01	ADAM [ISAST...	103	General
Information	19.04.2010 18:58:00	ADAM [ISAST...	1899	DS Schema
Information	19.04.2010 18:58:00	ADAM [ISAST...	1899	DS Schema
Information	19.04.2010 18:58:00	ADAM [ISAST...	1899	DS Schema
Information	19.04.2010 18:58:00	ADAM [ISAST...	1899	DS Schema

Event 1004, ADAM [ISASTGCTRL] General

Active Directory Lightweight Directory Services was shut down successfully.

```
Log Name:   ADAM (ISASTGCTRL)
Source:     ADAM [ISASTGCTRL] Genera  Logged:         19.04.2010 19:35:08
Event ID:   1004                      Task Category:  Service Control
Level:      Information               Keywords:       Classic
User:       N/A                       Computer:       TMG-EN.fabrikam.com
```

Figure 10: The ADAM ISASTGCTRL service gets disabled

Conclusion

In this article, I tried to show you where Forefront TMG saves the Forefront TMG configuration settings. Forefront TMG Standard and Enterprise uses AD-LDS to store the configuration but a copy of the TMG configuration is also stored in the local registry. If a Forefront TMG Enterprise Server joins an array managed by an EMS, the local AD-LDS instance (controlled by the ISASTRGCTRL service) will be disabled.

Related links

TMG Enterprise Arrays Explained
http://www.isaserver.org/tutorials/TMG-Enterprise-Arrays-Explained.html
Configure Forefront TMG to integrate with a TMG Array
http://www.isaserver.org/tutorials/Configure-Forefront-TMG-integrate-TMG-Array.html
Installing Threat Management Gateway 2010 RTM Enterprise Edition
http://www.isaserver.org/tutorials/Installing_Threat_Management_Gateway_2010_RTM_Enterprise_Edition.html
Upgrading from Forefront TMG Standard Edition to Enterprise Edition
http://technet.microsoft.com/en-us/library/dd896980.aspx