

## **What's going on during a Forefront TMG Installation?**

### **Abstract**

In this article I will explain in detail what's going on during a Forefront TMG installation. I will give a deep look into the Forefront TMG setup files, the registry and file system changes during a Forefront TMG installation with the help of tools like Process Monitor and we will also track Windows service changes during a Forefront TMG installation and I will also give you some tips for troubleshooting a failed Forefront TMG installation.

### **Let's begin**

A typical Forefront TMG installation requires many settings and configurations in the underlying Windows operating system. During a Forefront TMG installation, many Windows Server features and roles will be installed, Forefront TMG installs by default a local SQL Server 2008 SP1 express database for SQL Reporting services and databases for Forefront TMG Web proxy and Firewall logging. For this article I tried to cover every step during a Forefront TMG installation. To see what's happen during a Forefront TMG installation I used the Microsoft tool Process Monitor to see the changes and modifications of the Server during the installation process. For this article we will cover the following installation steps:

- AD-LDS installation
- TMG Log files
- Windows and TMG processes during the installation
- Created services
- Registry changes
- Windows Firewall settings
- Event Log entries

### **Servermanager**

The Forefront TMG preparation tool installs some Windows Server roles and features. Before the TMG installation there are no roles and features installed as you can see in the following screenshots:

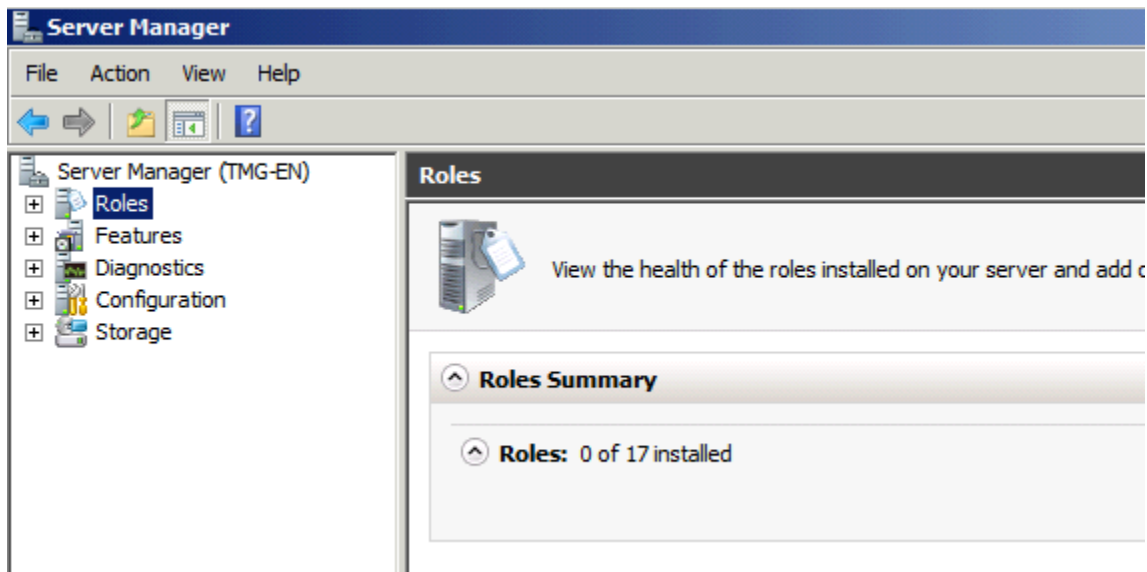


Figure 1: No installed Windows roles

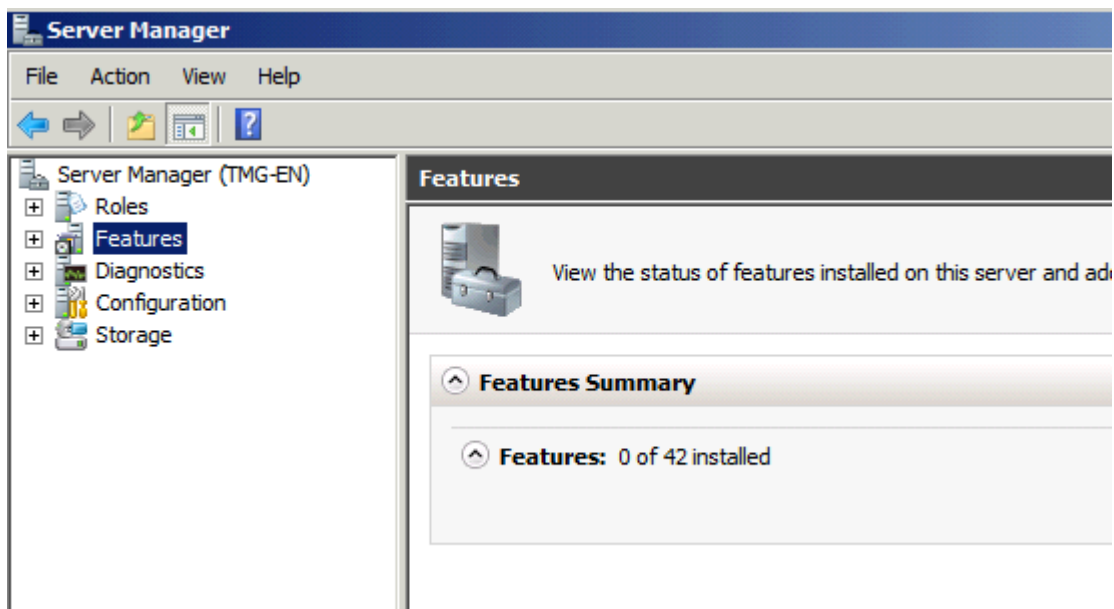


Figure 2: No installed Windows features

As a first step we have to run the Forefront TMG preparation tool which installs the required Windows roles and features:

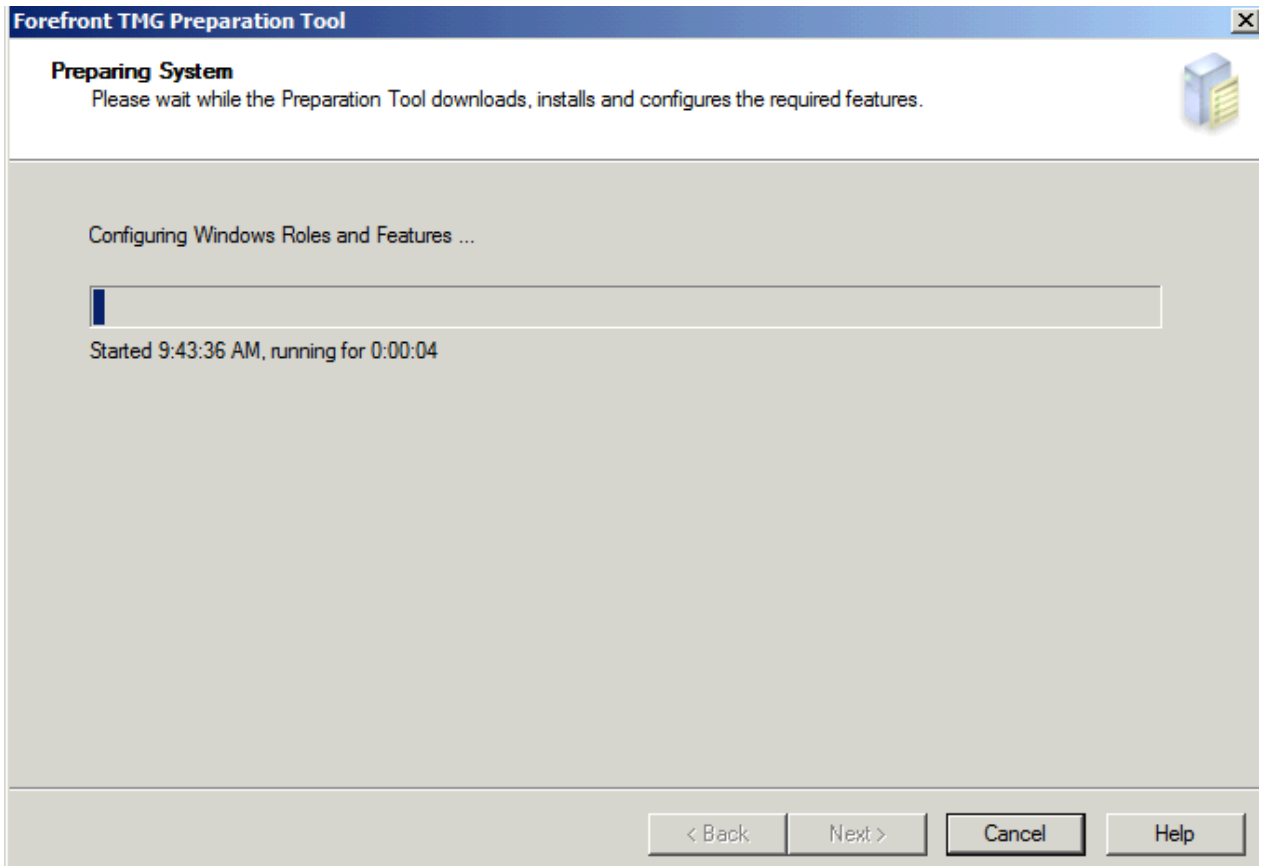


Figure 3: Forefront TMG preparation tool

The installation process is the Prerequisitesinstaller.exe.

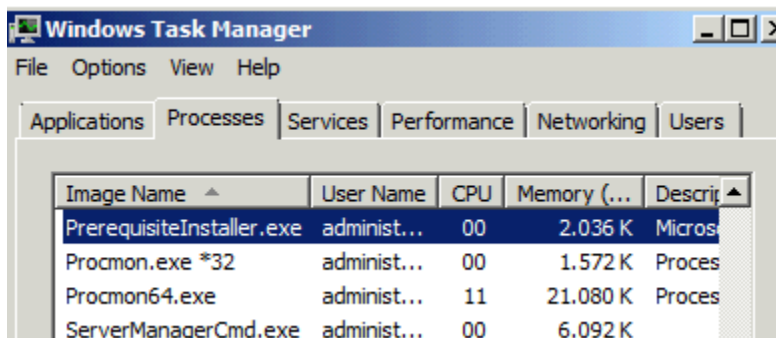


Figure 4: Forefront TMG preparation tool

To see what happens during the Prerequisites installation process I used the Microsoft Process monitor to filter all activities for this process.

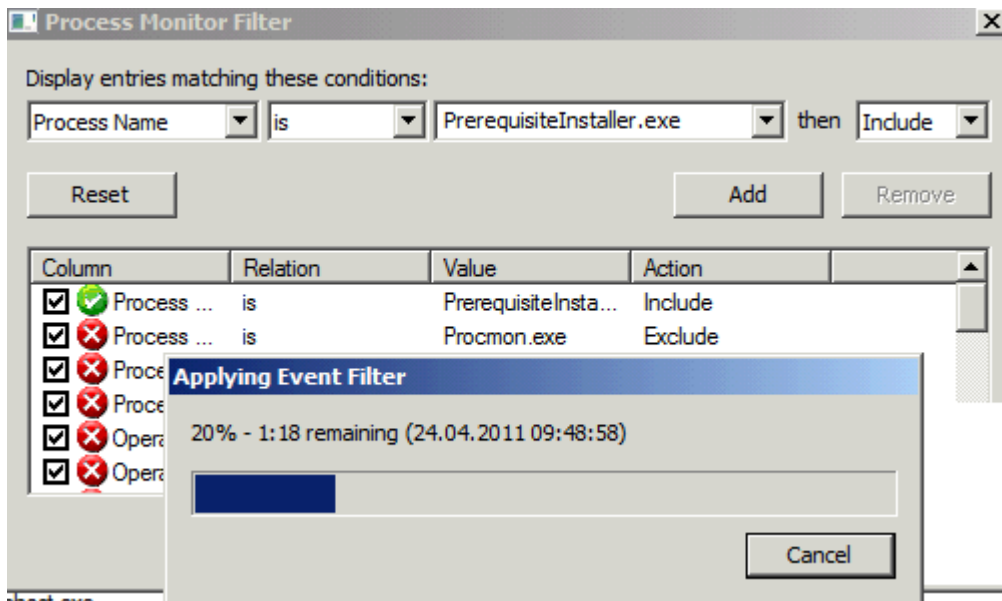


Figure 5: Process Monitor filter

As you can see there are many many activities during the installation process.

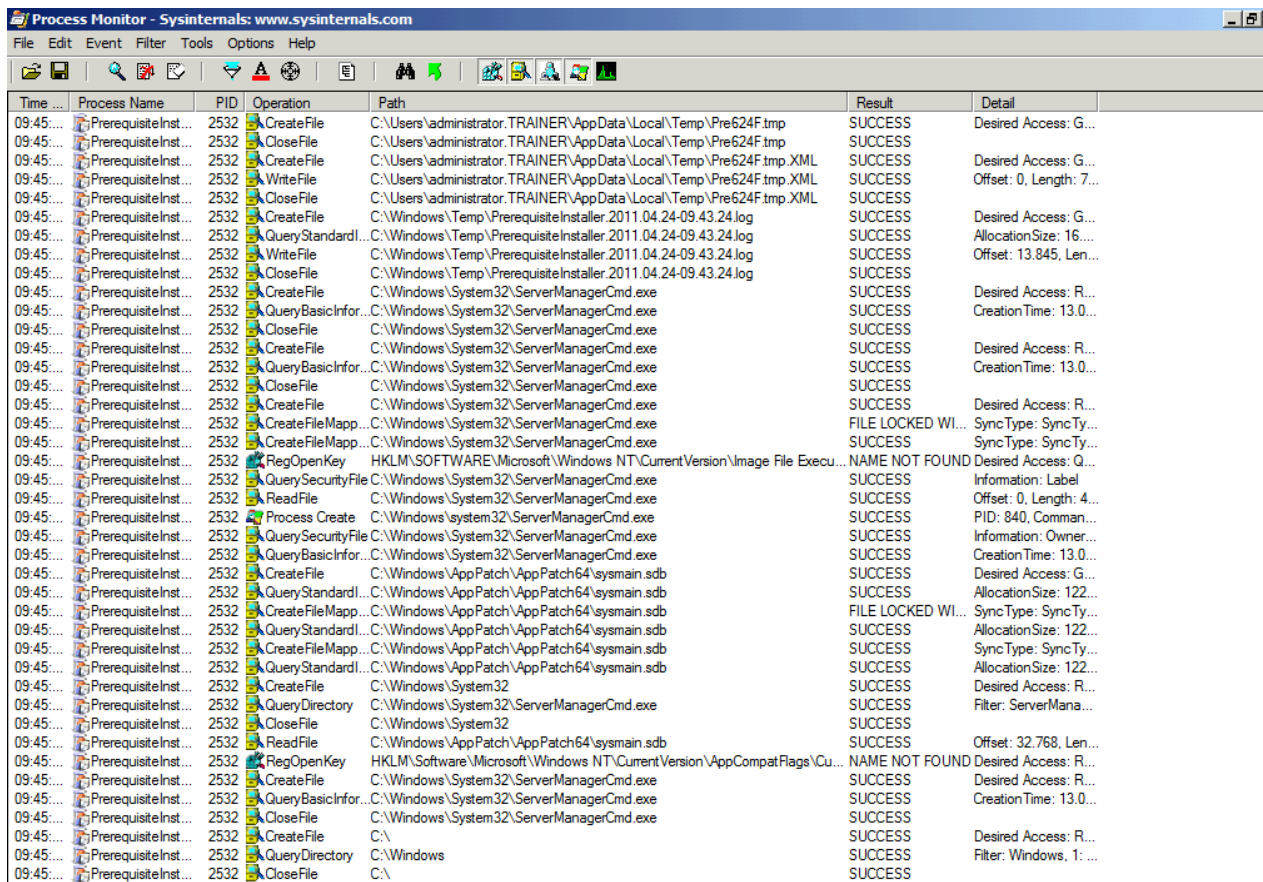


Figure 6: Installation process

The Forefront TMG installation process writes many log files into the Windows\temp directory.

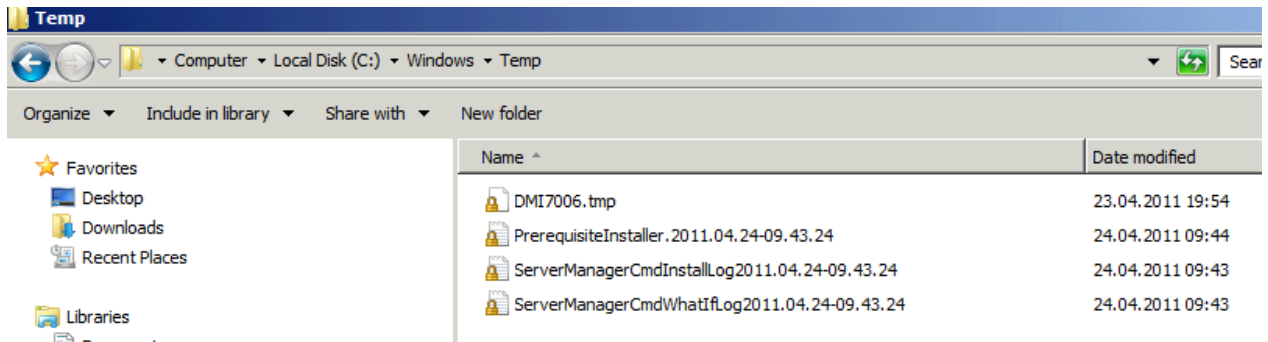


Figure 7: Forefront TMG log files

There are some logfiles for the Server Manager installation of the required Forefront TMG prerequisites.

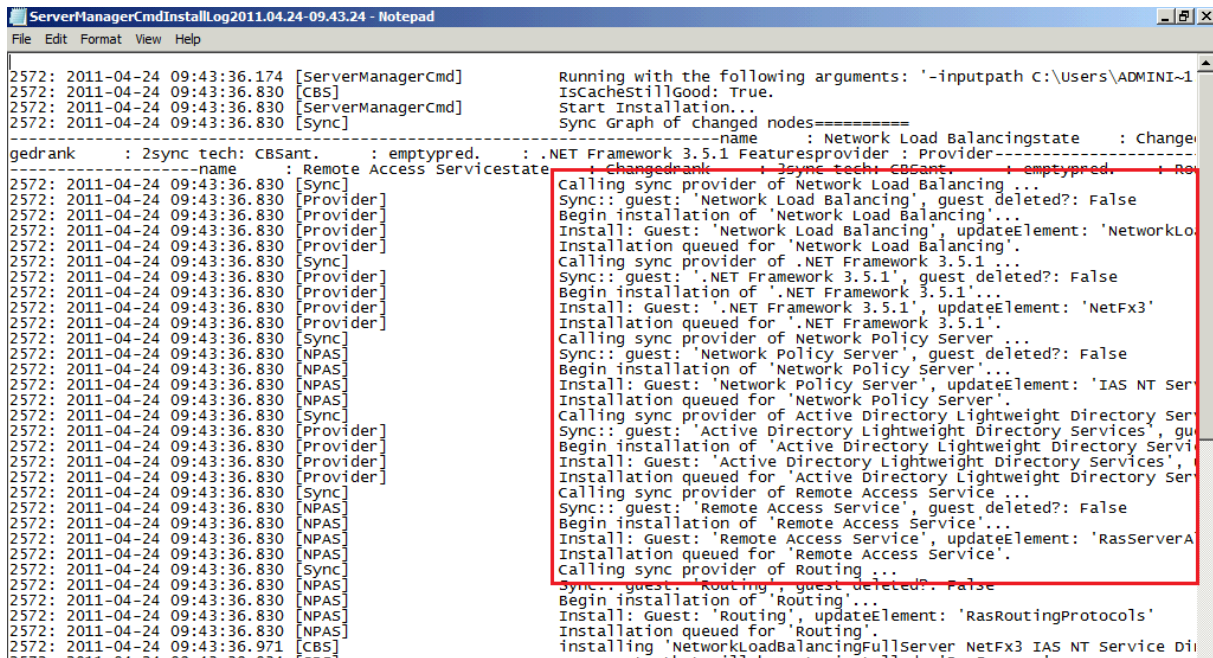


Figure 8: Server Manager log files

After the prerequisites have been installed successfully you can check the installed roles and features with Servermanager or ServerManagercmd.

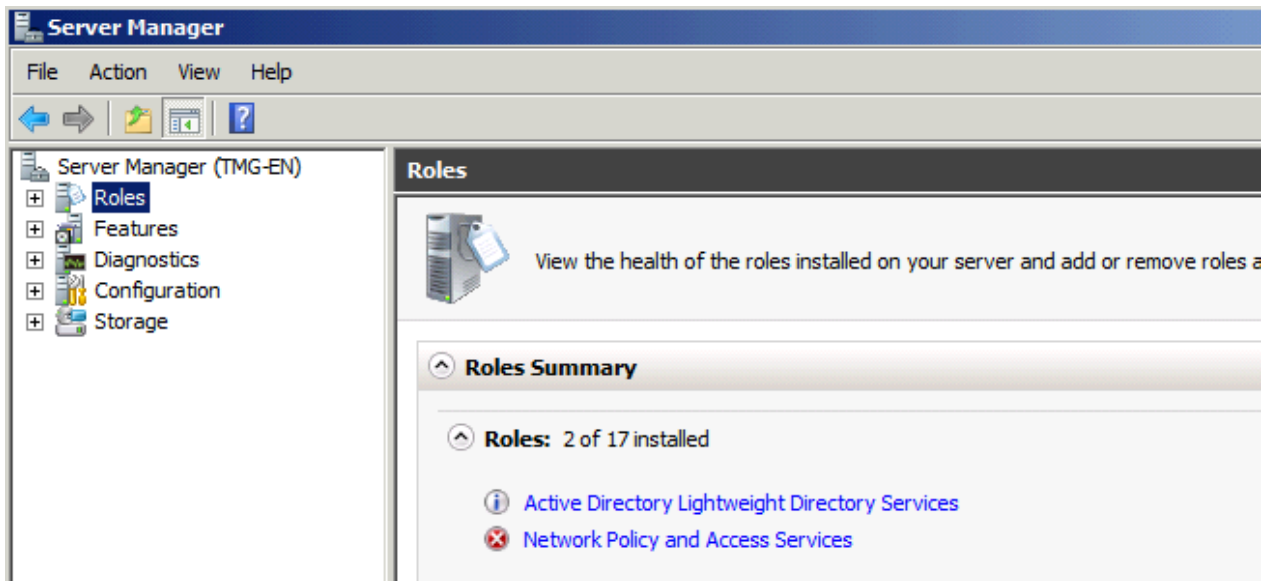


Figure 9: Installed roles

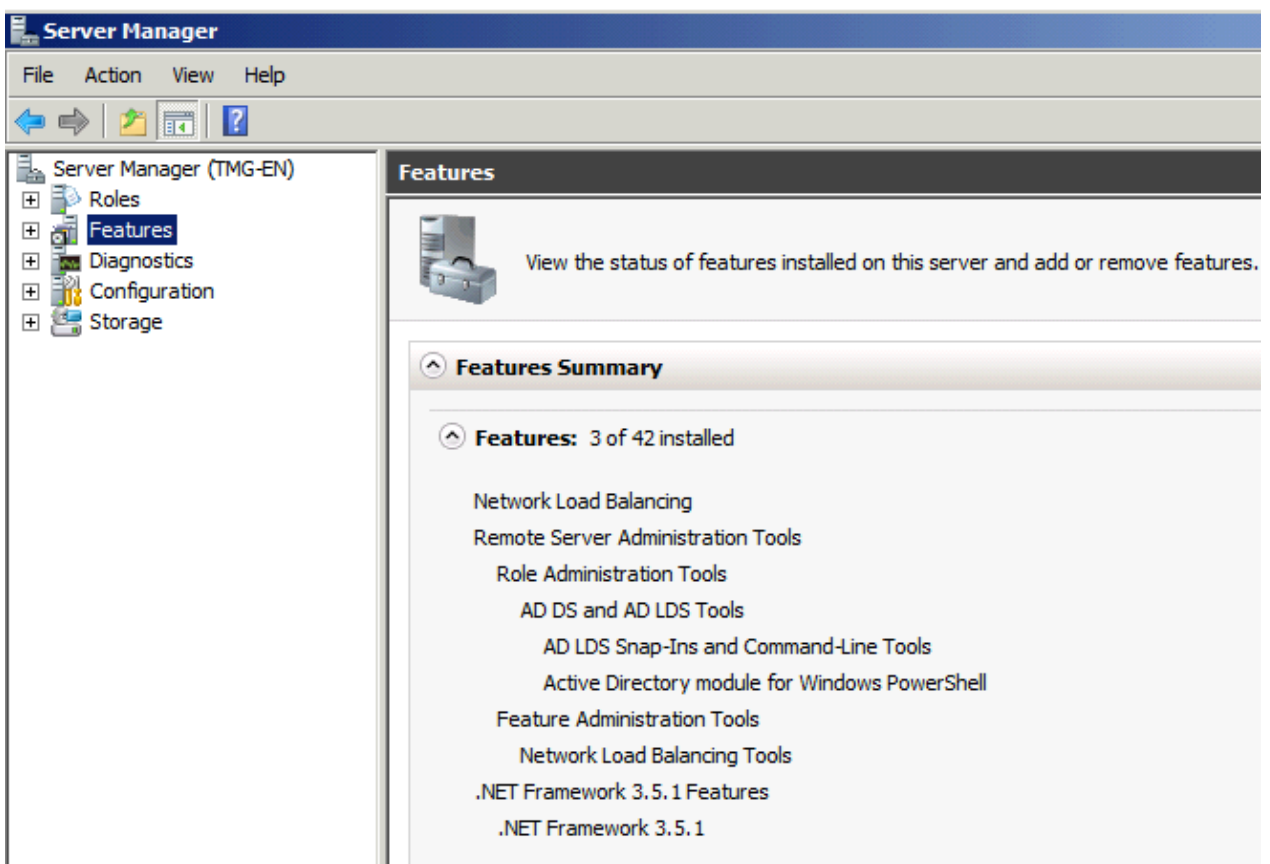


Figure 10: Installed features

## Step 1

### TMG Installation

Now we can start the Forefront TMG installation process. As a first step the local TMG configuration storage for the TMG configuration will be created. Forefront TMG uses a local AD-LDS instance.

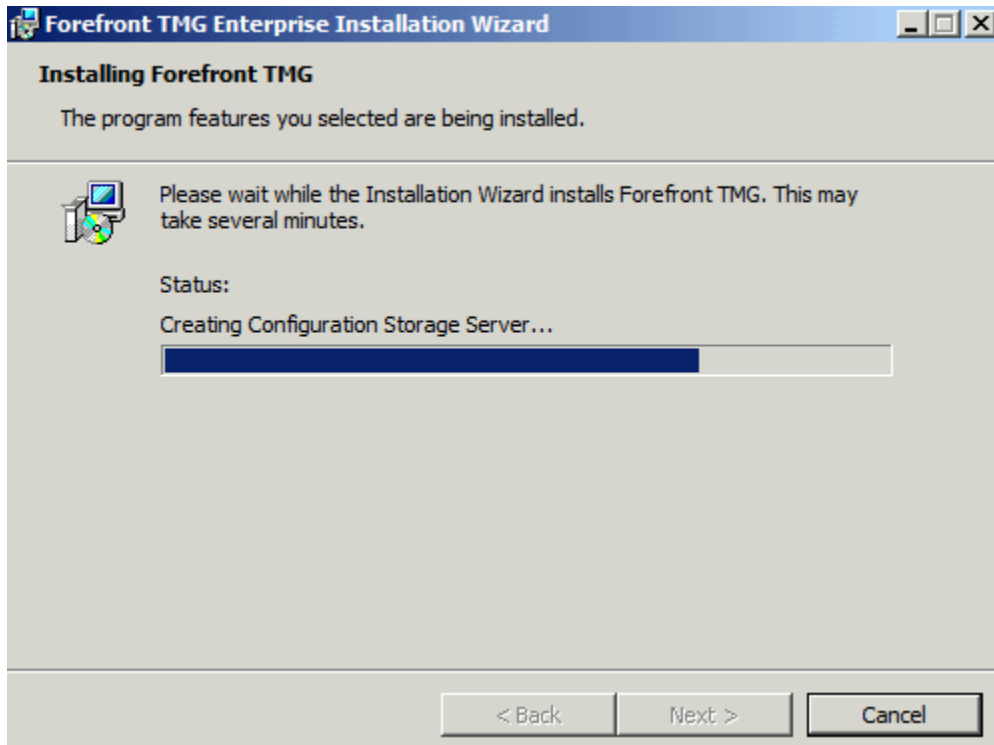


Figure 11: TMG configuration Storage Server

The required files for the AD-LDS instance will be installed during the prerequisites installer.

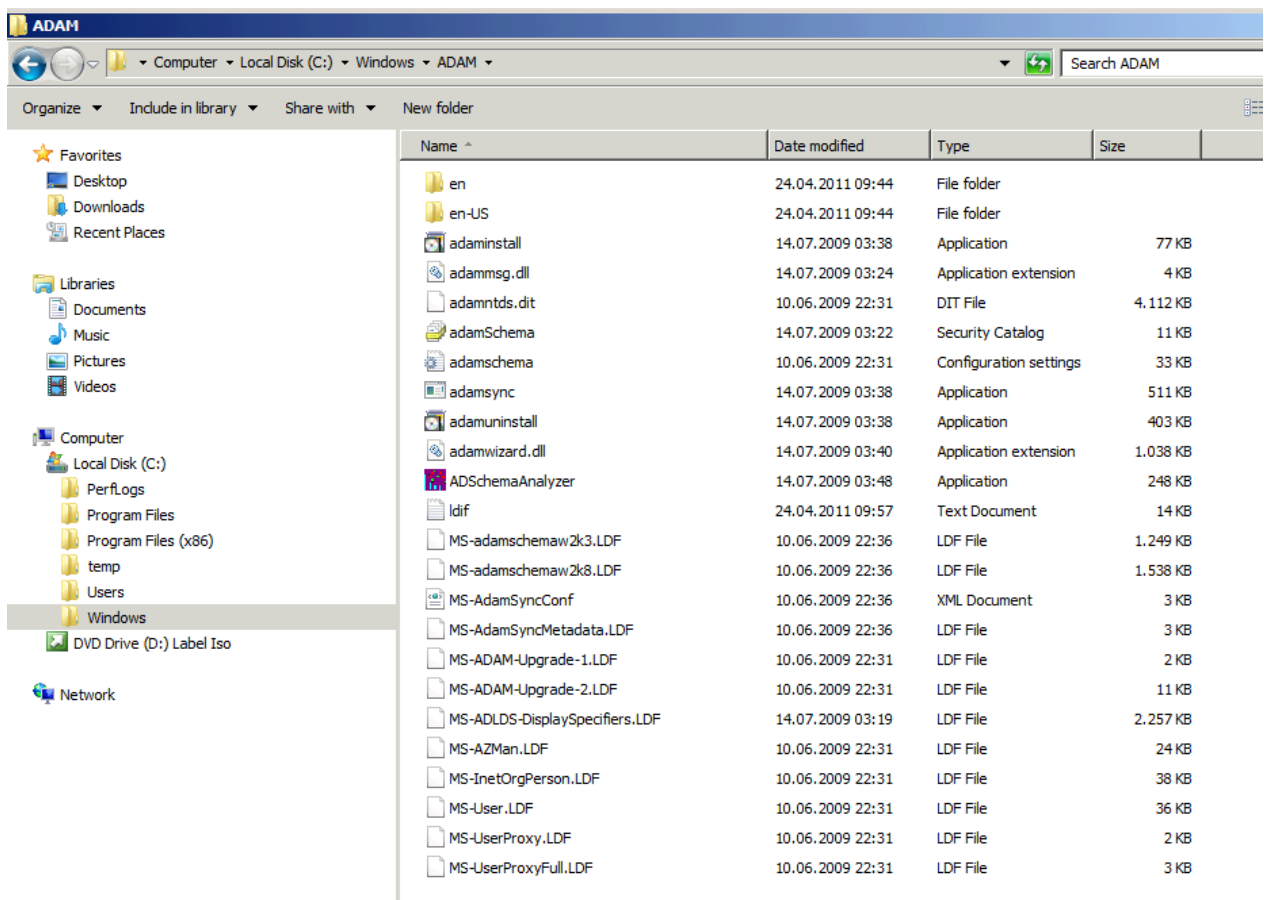
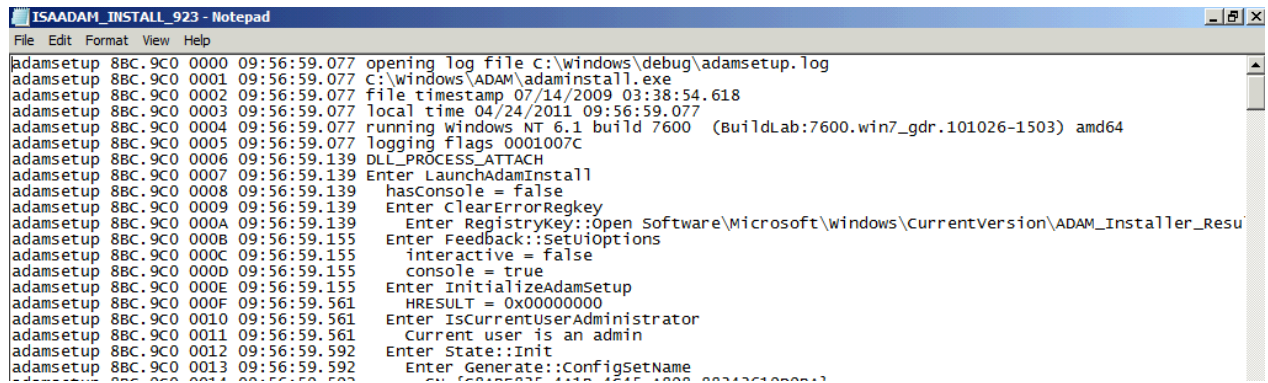


Figure 12: AD-LDS files



## ISAADAM\_INSTALL

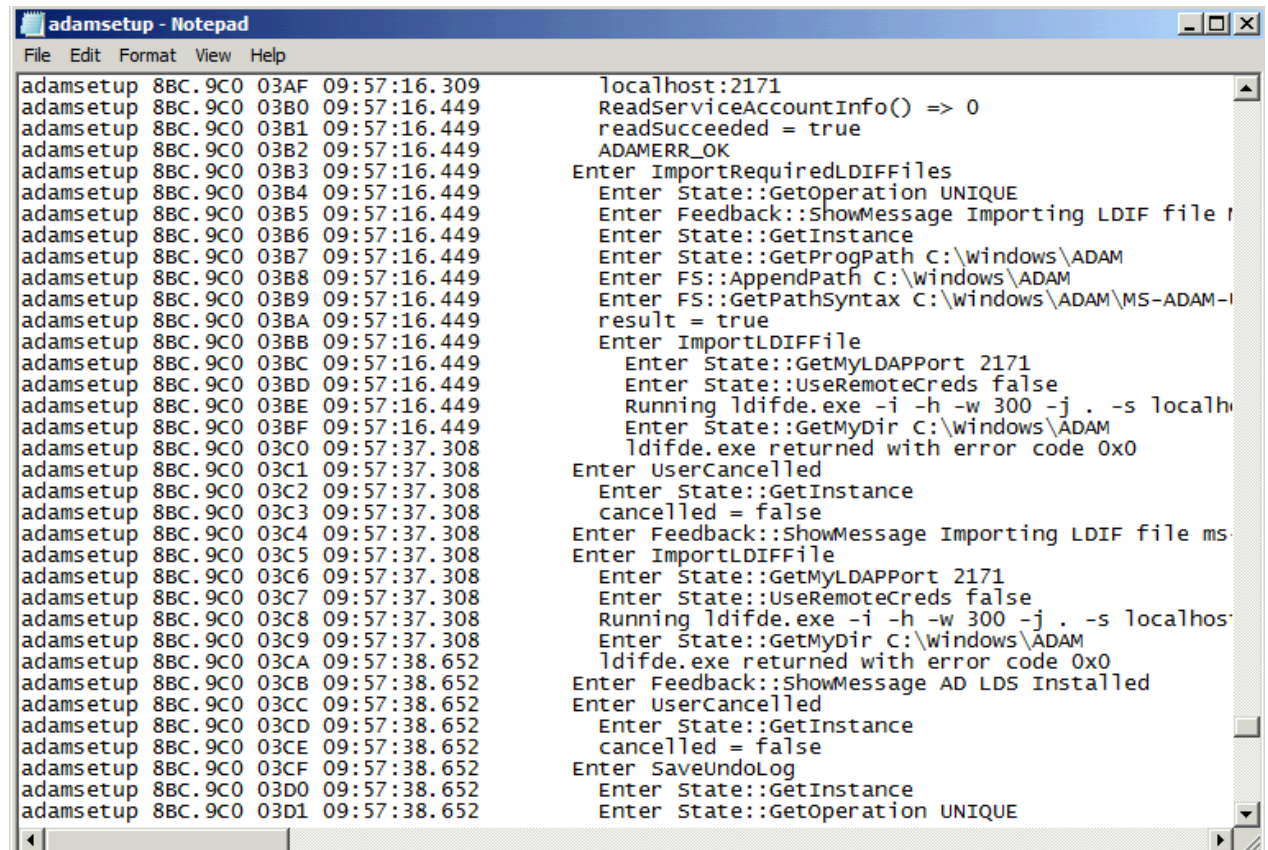
A log file will be created which protocols all installation steps.



```
ISAADAM_INSTALL_923 - Notepad
File Edit Format View Help
adamsetup 88C.9C0 0000 09:56:59.077 opening log file C:\windows\debug\adamsetup.log
adamsetup 88C.9C0 0001 09:56:59.077 c:\windows\ADAM\adaminstall.exe
adamsetup 88C.9C0 0002 09:56:59.077 file timestamp 07/14/2009 03:38:54.618
adamsetup 88C.9C0 0003 09:56:59.077 local time 04/24/2011 09:56:59.077
adamsetup 88C.9C0 0004 09:56:59.077 running windows NT 6.1 build 7600 (BuildLab:7600.win7_gdr.101026-1503) amd64
adamsetup 88C.9C0 0005 09:56:59.077 logging flags 0001007C
adamsetup 88C.9C0 0006 09:56:59.139 DLL_PROCESS_ATTACH
adamsetup 88C.9C0 0007 09:56:59.139 Enter LaunchAdamInstall
adamsetup 88C.9C0 0008 09:56:59.139 hasConsole = false
adamsetup 88C.9C0 0009 09:56:59.139 Enter ClearErrorRegkey
adamsetup 88C.9C0 000A 09:56:59.139 Enter RegistryKey::Open Software\Microsoft\windows\currentversion\ADAM_Installer_Resu
adamsetup 88C.9C0 000B 09:56:59.155 Enter Feedback::SetUIOptions
adamsetup 88C.9C0 000C 09:56:59.155 interactive = false
adamsetup 88C.9C0 000D 09:56:59.155 console = true
adamsetup 88C.9C0 000E 09:56:59.155 Enter InitializeAdamSetup
adamsetup 88C.9C0 000F 09:56:59.561 HRESULT = 0x00000000
adamsetup 88C.9C0 0010 09:56:59.561 Enter IsCurrentUserAdministrator
adamsetup 88C.9C0 0011 09:56:59.561 Current user is an admin
adamsetup 88C.9C0 0012 09:56:59.592 Enter State::Init
adamsetup 88C.9C0 0013 09:56:59.592 Enter Generate::ConfigSetName
```

Figure 13: AD-LDS log file

A more detailed AD-LDS log file can be found in C:\windows\debug\adamsetup.log



```
adamsetup - Notepad
File Edit Format View Help
adamsetup 88C.9C0 03AF 09:57:16.309 localhost:2171
adamsetup 88C.9C0 03B0 09:57:16.449 ReadServiceAccountInfo() => 0
adamsetup 88C.9C0 03B1 09:57:16.449 readSucceeded = true
adamsetup 88C.9C0 03B2 09:57:16.449 ADAMERR_OK
adamsetup 88C.9C0 03B3 09:57:16.449 Enter ImportRequiredLDIFFiles
adamsetup 88C.9C0 03B4 09:57:16.449 Enter State::GetOperation UNIQUE
adamsetup 88C.9C0 03B5 09:57:16.449 Enter Feedback::ShowMessage Importing LDIF file
adamsetup 88C.9C0 03B6 09:57:16.449 Enter State::GetInstance
adamsetup 88C.9C0 03B7 09:57:16.449 Enter State::GetProgPath C:\windows\ADAM
adamsetup 88C.9C0 03B8 09:57:16.449 Enter FS::AppendPath C:\windows\ADAM
adamsetup 88C.9C0 03B9 09:57:16.449 Enter FS::GetPathSyntax C:\windows\ADAM\MS-ADAM-
adamsetup 88C.9C0 03BA 09:57:16.449 result = true
adamsetup 88C.9C0 03BB 09:57:16.449 Enter ImportLDIFFile
adamsetup 88C.9C0 03BC 09:57:16.449 Enter State::GetMyLDAPPort 2171
adamsetup 88C.9C0 03BD 09:57:16.449 Enter State::UseRemoteCreds false
adamsetup 88C.9C0 03BE 09:57:16.449 Running ldifde.exe -i -h -w 300 -j . -s localh
adamsetup 88C.9C0 03BF 09:57:16.449 Enter State::GetMyDir C:\windows\ADAM
adamsetup 88C.9C0 03C0 09:57:37.308 ldifde.exe returned with error code 0x0
adamsetup 88C.9C0 03C1 09:57:37.308 Enter UserCancelled
adamsetup 88C.9C0 03C2 09:57:37.308 Enter State::GetInstance
adamsetup 88C.9C0 03C3 09:57:37.308 cancelled = false
adamsetup 88C.9C0 03C4 09:57:37.308 Enter Feedback::ShowMessage Importing LDIF file ms
adamsetup 88C.9C0 03C5 09:57:37.308 Enter ImportLDIFFile
adamsetup 88C.9C0 03C6 09:57:37.308 Enter State::GetMyLDAPPort 2171
adamsetup 88C.9C0 03C7 09:57:37.308 Enter State::UseRemoteCreds false
adamsetup 88C.9C0 03C8 09:57:37.308 Running ldifde.exe -i -h -w 300 -j . -s localhos
adamsetup 88C.9C0 03C9 09:57:37.308 Enter State::GetMyDir C:\windows\ADAM
adamsetup 88C.9C0 03CA 09:57:38.652 ldifde.exe returned with error code 0x0
adamsetup 88C.9C0 03CB 09:57:38.652 Enter Feedback::ShowMessage AD LDS Installed
adamsetup 88C.9C0 03CC 09:57:38.652 Enter UserCancelled
adamsetup 88C.9C0 03CD 09:57:38.652 Enter State::GetInstance
adamsetup 88C.9C0 03CE 09:57:38.652 cancelled = false
adamsetup 88C.9C0 03CF 09:57:38.652 Enter SaveUndoLog
adamsetup 88C.9C0 03D0 09:57:38.652 Enter State::GetInstance
adamsetup 88C.9C0 03D1 09:57:38.652 Enter State::GetOperation UNIQUE
```

Figure 14: AD-LDS log file

## AD-LDS database

The AD-LDS database will be installed in the Forefront TMG installation directory.



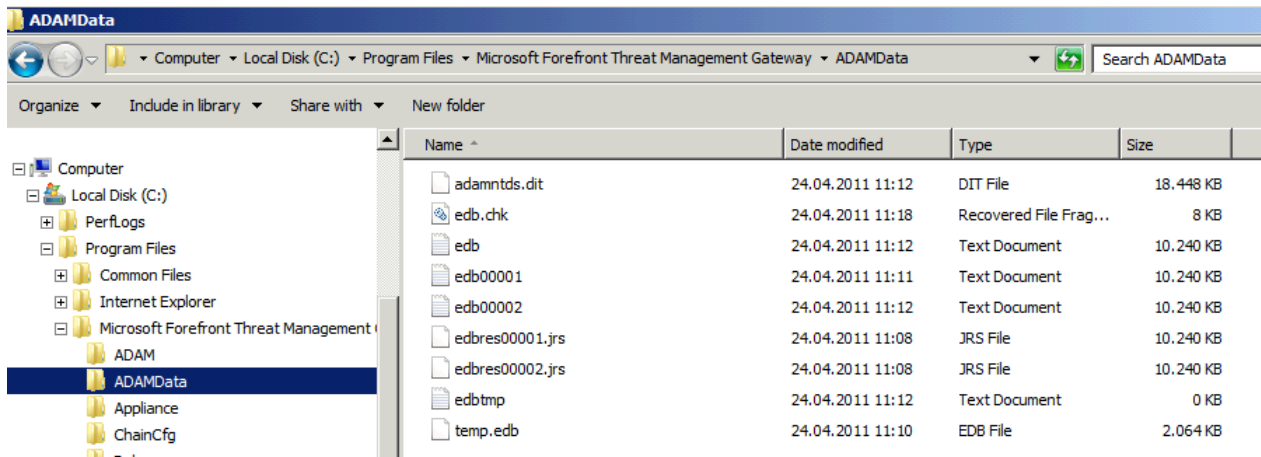


Figure 15: AD-LDS database

## AD-LDS Service (ISASTGCTRL)

A local AD-LDS (AD/AM) service will be created. The other Forefront TMG Services will be started after the Forefront TMG installation.

ISASTGCTRL	AD LDS ins...	Started	Automatic	Network S...
KtmRm for Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
Link-Layer Topology Discovery Mapper	Creates a ...		Manual	Local Service
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft ...	Started	Automatic (D...	Local System
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft ...	Started	Automatic (D...	Local System
Microsoft Fibre Channel Platform Registration Service	Registers t...		Manual	Local Service
Microsoft Forefront TMG Control	Controls F...		Automatic	Local System
Microsoft Forefront TMG Firewall	Provides F...		Automatic	Network S...
Microsoft Forefront TMG Job Scheduler	Runs Foref...		Automatic	Local System
Microsoft Forefront TMG Managed Control	Controls F...		Automatic	Local System
Microsoft Forefront TMG Storage	Provides F...	Started	Automatic	Local System

Figure 16: AD-LDS service

## Registry changes

During the Forefront TMG installation, a local AD-LDS instance will be created which holds the TMG configuration. The TMG configuration will also be stored in the local Registry and the TMG service will ensure that the AD-LDS database stores the configuration in the local Registry. The following screenshot shows the local Registry after the ISASTGCTRL service has been installed but not completely filled until the Forefront TMG setup has finished.

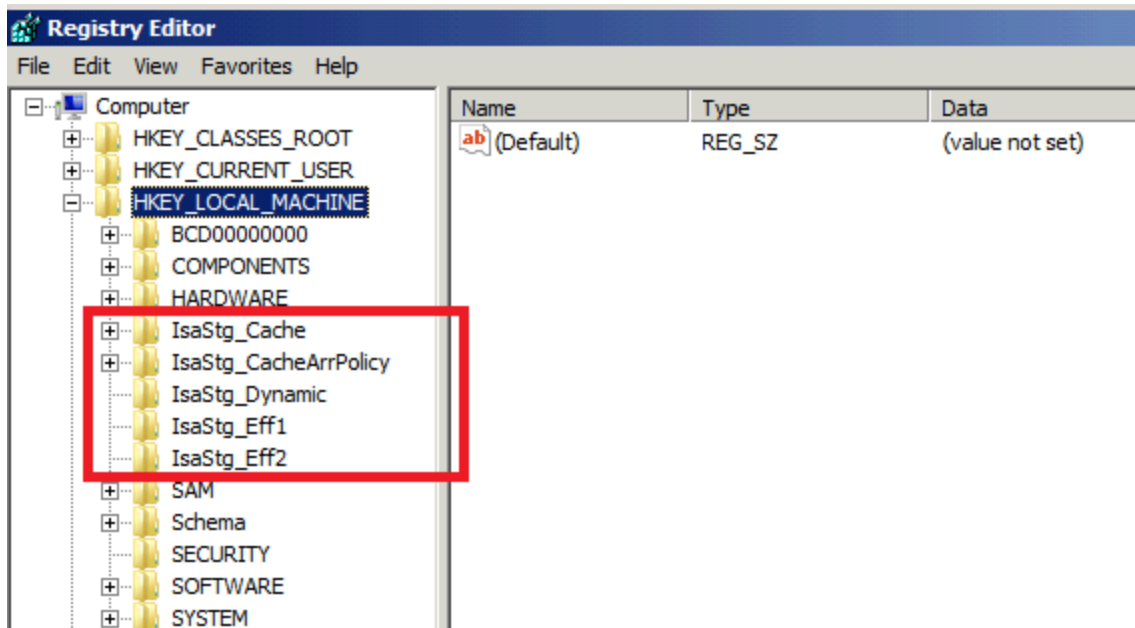


Figure 17: Local registry settings for TMG

After the local AD-LDS database has been created you can see that the TMG installation process writes into this database.

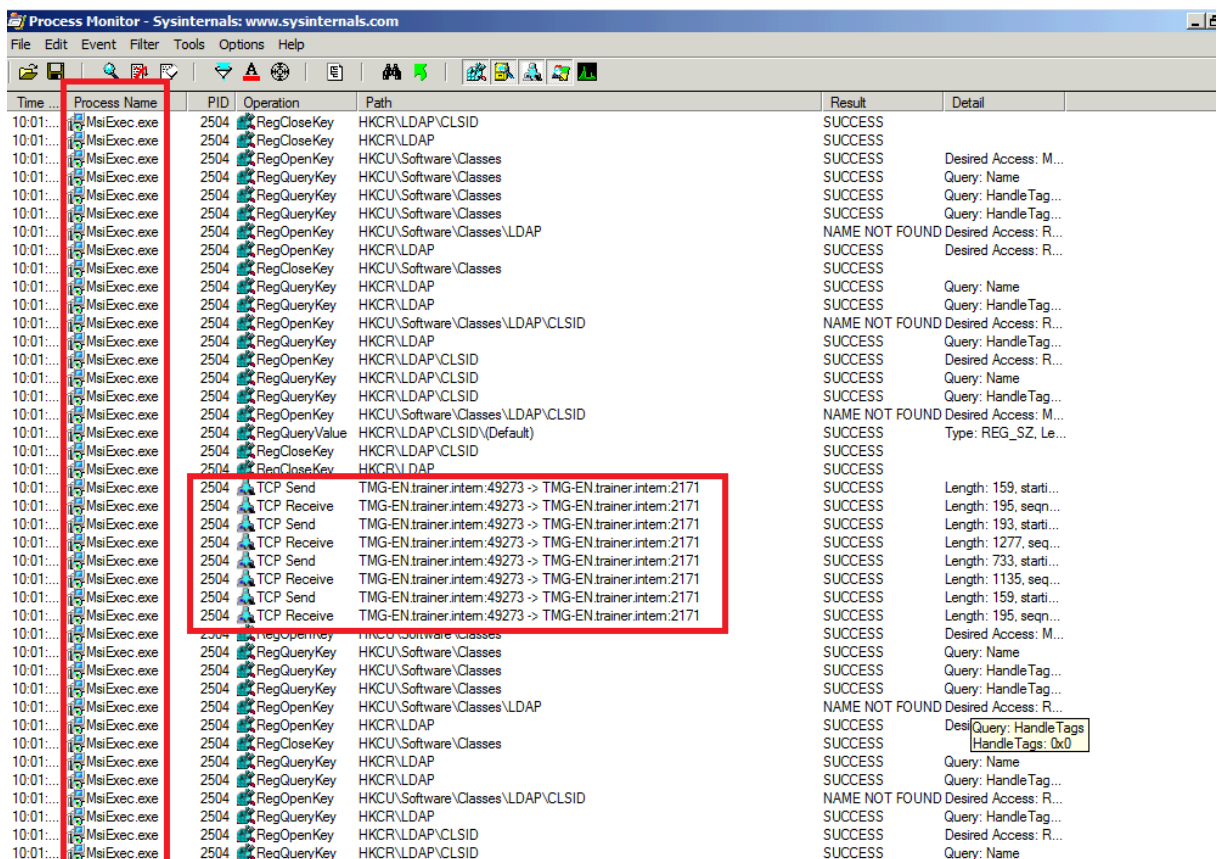


Figure 18: AD-LDS database will be filled during TMG installation

## Step 2

After the core components have been installed, additional components will be installed. These additional components are primarily the installation of the local SQL

Server 2008 SP1 Express databases for SQL Reporting services and the databases for the Forefront TMG Web proxy and Firewall logging.

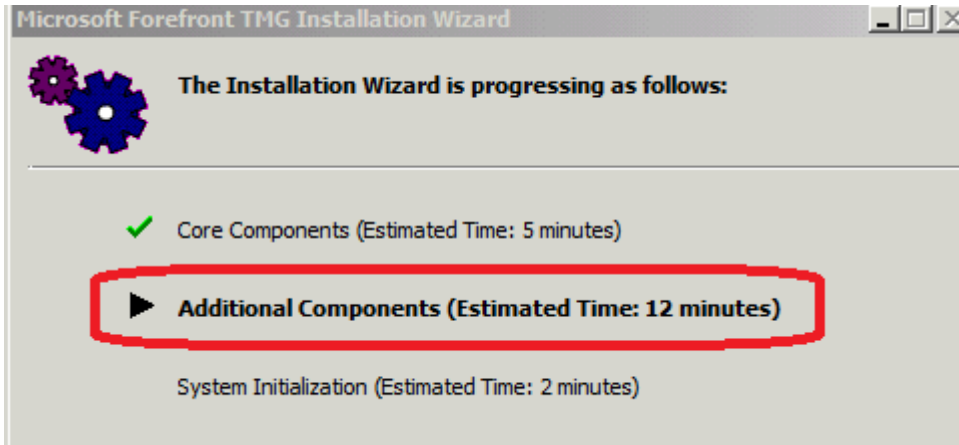


Figure 19: Step 2

## SQL Server 2008 Express installation

The screenshot shows the 'Process Monitor - Sysinternals: www.sysinternals.com' window. The main area displays a log of system events. The columns are: Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The log shows the installation of SQL Server 2008 Express, with many entries for 'setup100.exe' and various file operations. A red box highlights a specific entry in the log:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:14:19.2368642	setup100.exe	2812	CreateFile	C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Update Cache\...	NAME NOT FOUND	Desired Access: R...

Figure 20: SQL installation

During the SQL Express installation a hidden folder called config.msi in the root directory of the server will be created which contains a detailed log file.





The SQL Server reporting database will be installed in the local SQL Server installation directory.

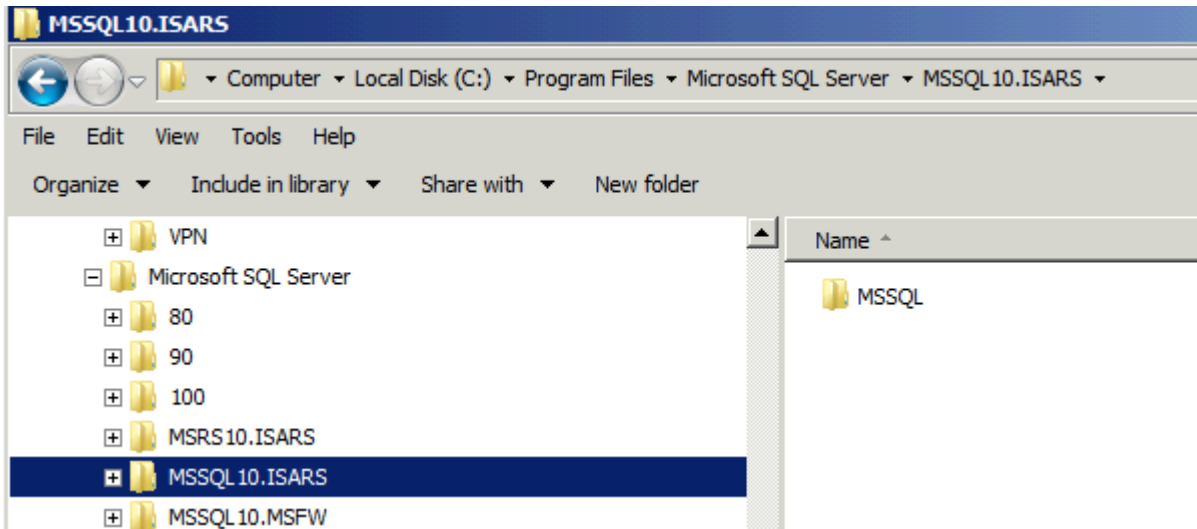


Figure 23: SQL reporting service database directory

It takes a while but after a few minutes you can see the new SQL Server databases for the TMG Web proxy and Firewall logging. These databases are stored in the local Forefront TMG installation directory.

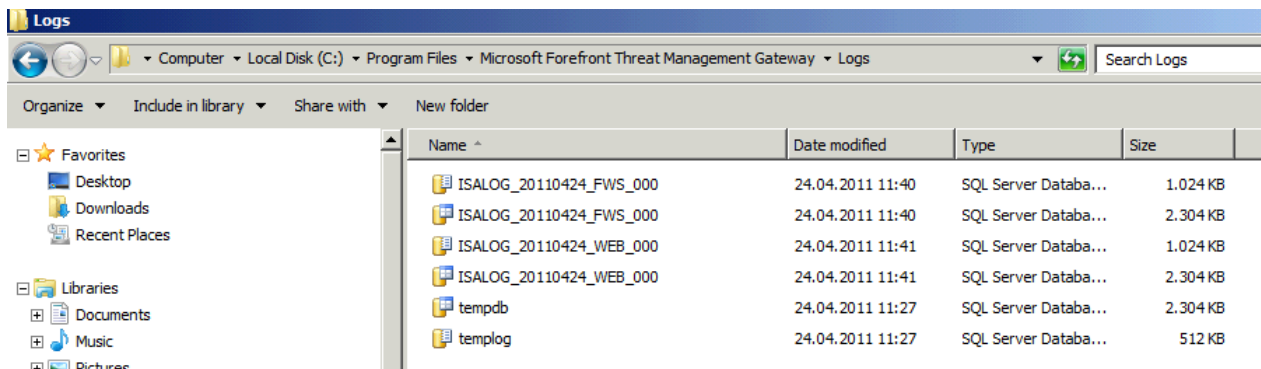


Figure 24: SQL databases for TMG

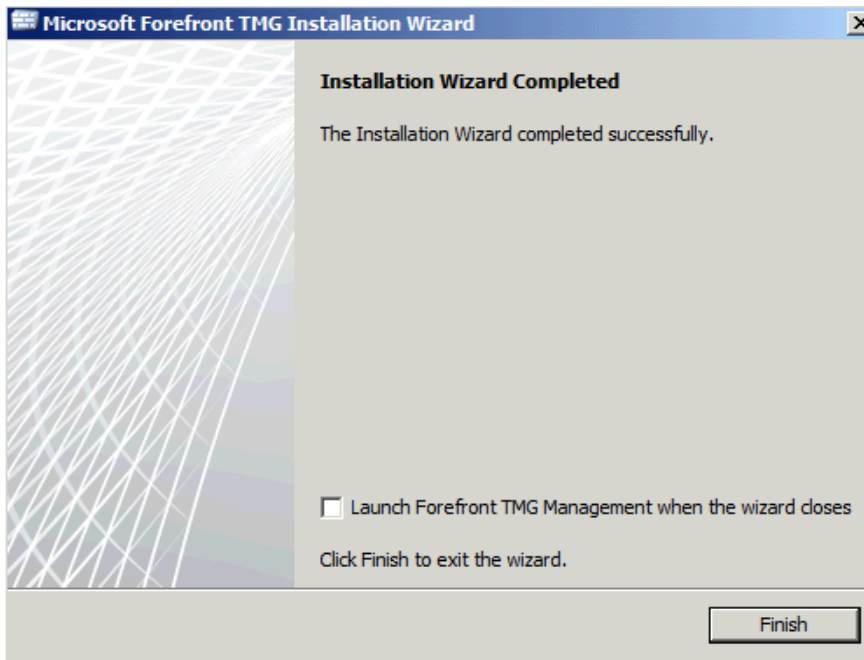


Figure 25: The Forefront TMG installation finished successfully.

After Forefront TMG has been installed, you can see the all TMG entries in the Registry.

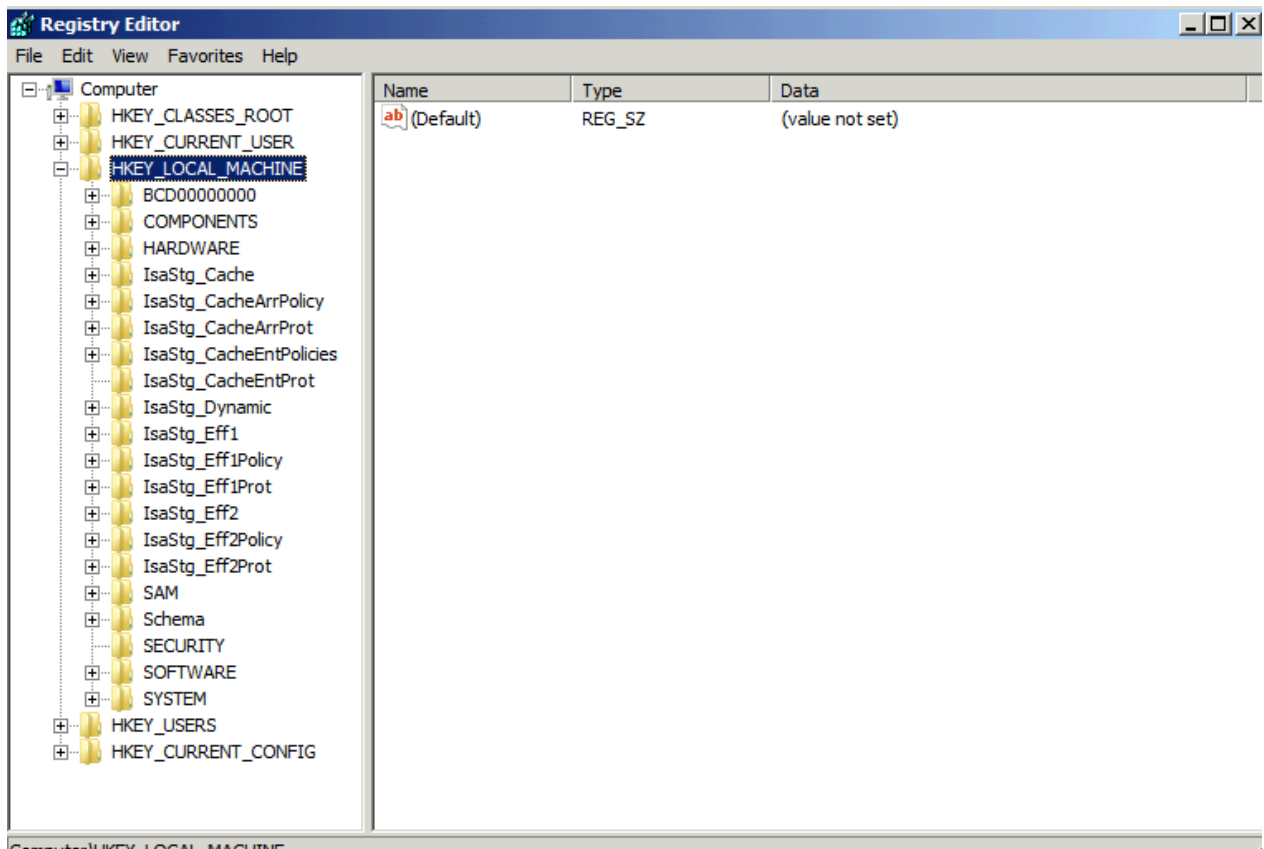


Figure 26: Forefront TMG settings in the local Registry

The local AD-LDS database has also been filled with the local TMG configuration. You can check this with ADSIEDIT as you can see in the following screenshot. We first have to connect to the AD-LDS instance.



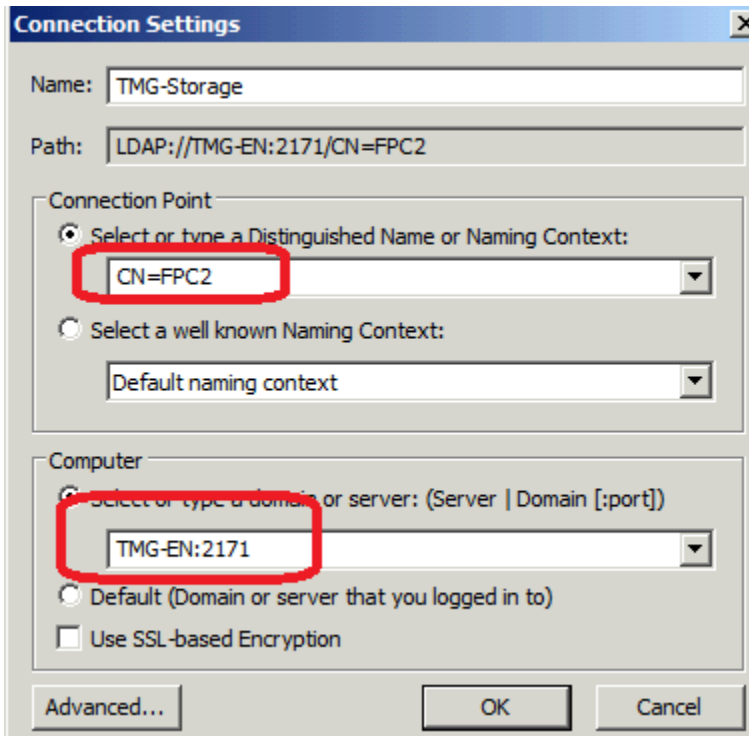


Figure 27: Connect to the Forefront TMG AD-LDS instance

After a successful connection you will see the entire Forefront TMG configuration in the AD-LDS database.

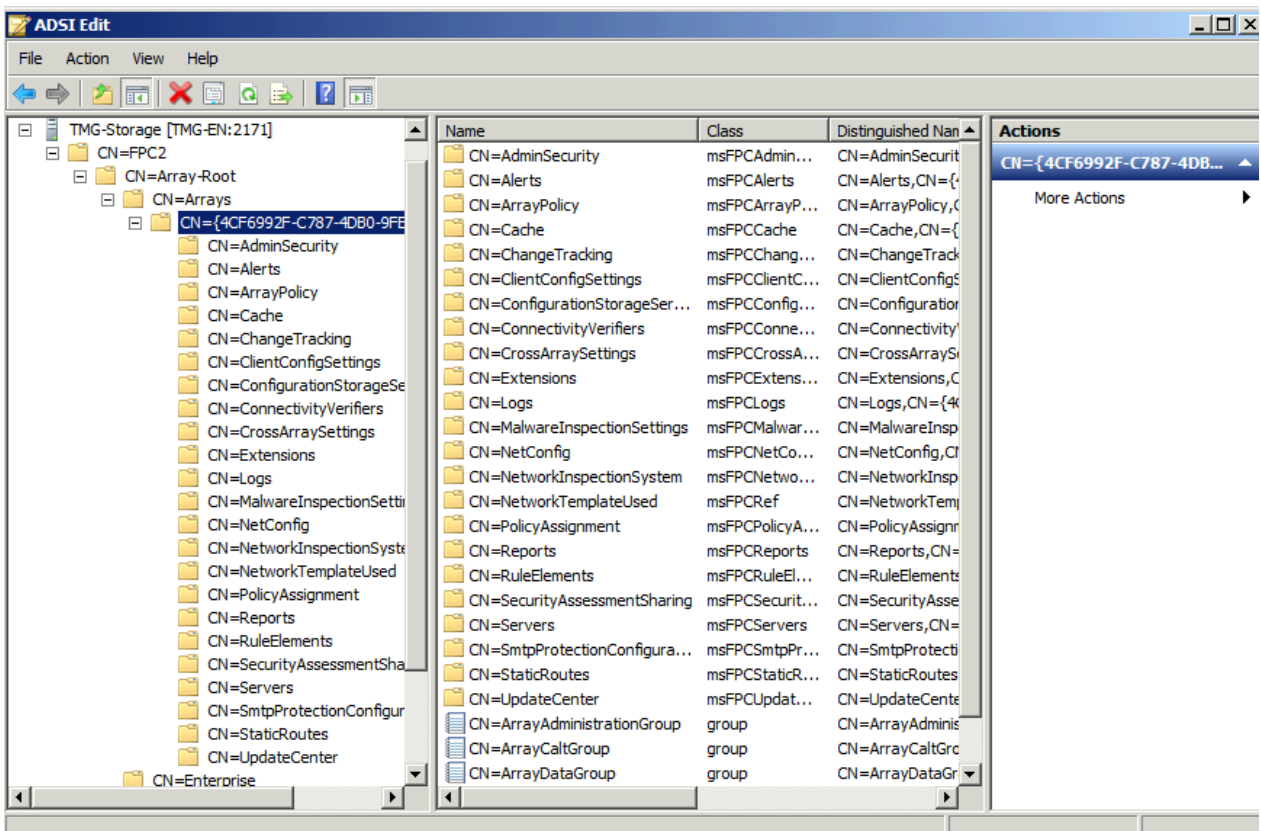


Figure 28: AD-LDS database content

## Forefront TMG Setup log files

After the installation of TMG you will also find all Forefront TMG log files during the installation in the Windows\Temp directory.

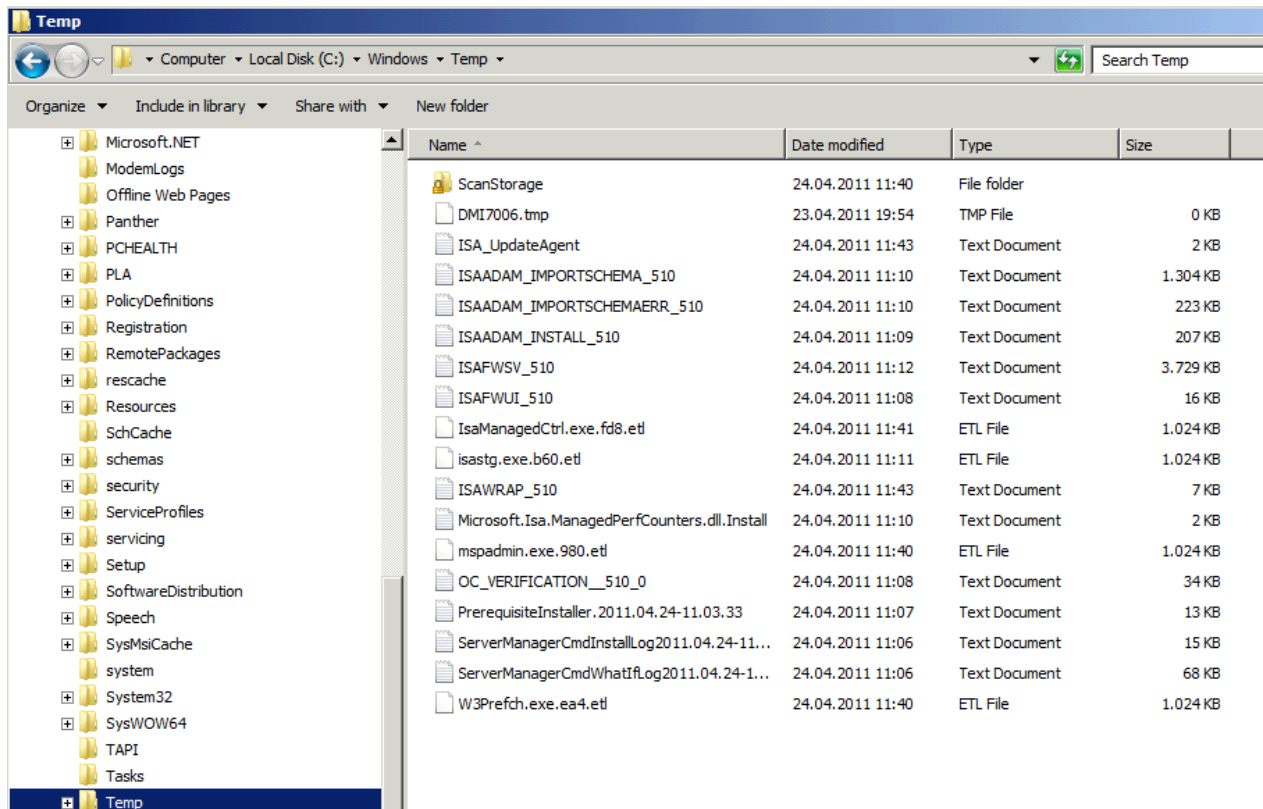


Figure 29: Forefront TMG settings in the local Registry

You can use these log files if the Forefront TMG installation fails. If the Forefront TMG installation failed you must also have a look into the entries in the Windows event log.

The following screenshot will give you a description of the Forefront TMG log files.

Log file	Description
ISAWRAP_www.log	The setup wrapper log file records general information about the success or failure of the firewall installation and about the success or failure of the Microsoft SQL Server Desktop Engine (MSDE) installation and Active Directory Lightweight Directory Services (AD LDS).
ISAFWSV_www.log	The Firewall service setup log file records events and errors that are related to the configuration of the Forefront TMG installation.
ISAMSDE_www.log	This log file records events and errors that are related to MSDE.
ISAFWUI_www.log	This log file records events and errors that are related to the configuration of the Forefront TMG installation.
ISAADAM_INSTALL_www.log	This log file records events and errors that are related to the installation of AD LDS storage when the Configuration Storage server is installed.
ISAADAM_UNINSTALL_www.log	This log file records the events and errors that are related to the removal of AD LDS storage from the computer. AD LDS storage is removed when the Configuration Storage server is uninstalled from the computer.
ISAADAM_IMPORTSCHEMA_www.log	This log file records the successful schema changes that are automatically applied to the AD LDS storage during installation.
ISAADAM_IMPORTSCHEMAERR_www.log	This log file will only be created if there are errors when the automatic schema changes are applied to the AD LDS storage during setup.

Figure 30: TMG Setup log files Source: <http://technet.microsoft.com/de-de/library/ee781947.aspx>

For example, I opened the Forefront TMG Firewall installation log file.

```

ISAFWSV_510 - Notepad
File Edit Format View Help
Property(C): TextInternalLeading = 3
Property(C): ColorBits = 16
Property(C): TTCSupport = 1
Property(C): Time = 11:12:55
Property(C): Date = 24.04.2011
Property(C): MsiNetAssemblySupport = 2.0.50727.4927
Property(C): Msiwin32AssemblySupport = 6.1.7600.16385
Property(C): RedirectedDllSupport = 2
Property(C): MsiRunningElevated = 1
Property(C): DATABASE = C:\Users\ADMINI~1.TRA\AppData\Local\Temp\5457c.msi
Property(C): OriginalDatabase = D:\FPC\MS_FPC_Server.msi
Property(C): SOURCEDIR = D:\FPC\
Property(C): MediaSourceDir = 1
Property(C): VersionHandler = 5.00
Property(C): UILevel = 5
Property(C): Preselected = 1
Property(C): ACTION = INSTALL
Property(C): EXECUTEACTION = INSTALL
Property(C): SERVER_SERVICE_RUNNING = 1
Property(C): AUTHENTICATEDUSERSGROUPNAME = Authenticated Users
Property(C): NETWORKSERVICEACCOUNTNAME = NETWORK SERVICE
Property(C): USERSACCOUNTNAME = Users
Property(C): PREREQ_DOT_NET_3_5_SPL_INSTALLED = 1
Property(C): ROOTDRIVE = C:\
Property(C): CostingComplete = 1
Property(C): OutOfDiskSpace = 0
Property(C): OutOfNoRBDiskSpace = 0
Property(C): PrimaryVolumeSpaceAvailable = 0
Property(C): PrimaryVolumeSpaceRequired = 0
Property(C): PrimaryVolumeSpaceRemaining = 0
Property(C): DCIP = 10.80.16.80
Property(C): FirstDialog = InstallWelcome
Property(C): FileSystemType = NTFS
Property(C): NextDialog = ReadyToInstall
Property(C): GoToClientSettingsDialog = 1
Property(C): ARRAY_INTERNALNET = 1 10.80.16.0-10.80.19.255
Property(C): PID = 02186-169-2504901-70715
Property(C): STANDALONE_Install = 1
Property(C): MSFIREWALLMNGACTION_Install = 1
=== Logging stopped: 24.04.2011 11:12:55 ===
MSI (c) (70:80) [11:12:55:658]: Note: 1: 1707
MSI (c) (70:80) [11:12:56:236]: Product: Microsoft Forefront Threat Management Gateway EE -- Installation operation complete
MSI (c) (70:80) [11:12:56:705]: windows installer installed the product. Product Name: Microsoft Forefront Threat Management
MSI (c) (70:80) [11:12:56:705]: Grabbed execution mutex.
MSI (c) (70:80) [11:12:56:705]: Cleaning up uninstalled install packages, if any exist
MSI (c) (70:80) [11:12:56:705]: MainEngineThread is returning 0
=== verbose logging stopped: 24.04.2011 11:12:56 ===

```

Figure 31: Forefront TMG Firewall service log file

During the Forefront TMG installation, TMG takes control over the local Windows Firewall through the Windows Filtering Platform (WFP).

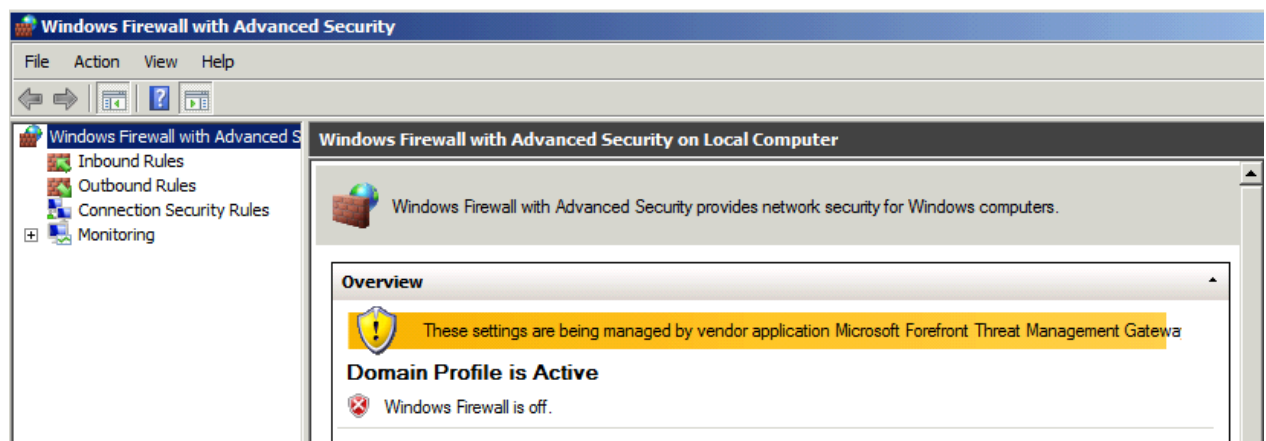


Figure 32: Forefront TMG controls the local Windows Firewall

## Troubleshooting Forefront TMG Setup

If something goes wrong during a Forefront TMG installation you can use the Superflow application for Forefront TMG to troubleshoot the installation process. The Superflow application will give you some more information about how to troubleshoot installation problem. You can download the Superflow application for free [here](#).

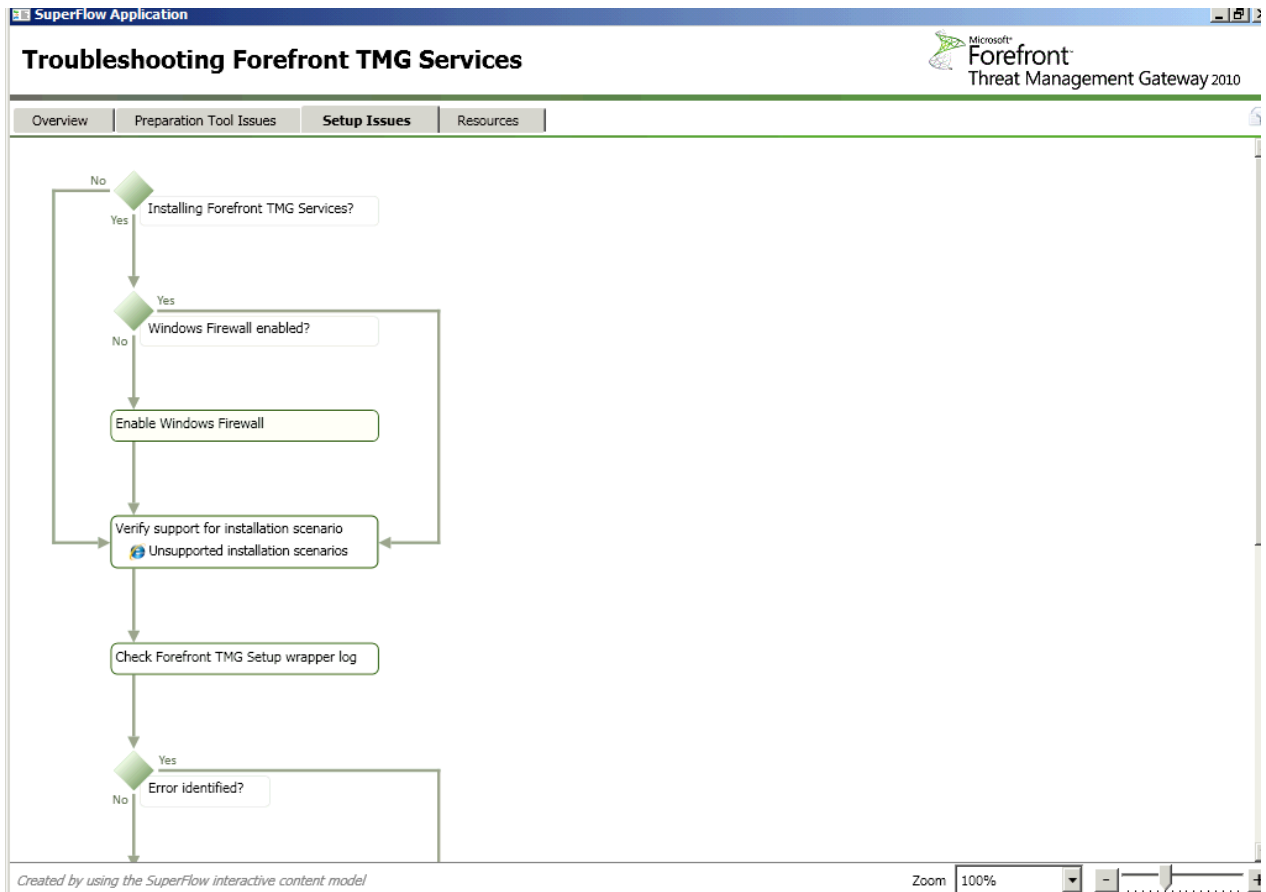


Figure 33: TMG SuperFlow

## Conclusion

I hope that my article will give you more insight into the installation process of Forefront TMG and what's going on under the hood of the GUI. I found it very useful to use the Process Monitor tool to see what will be created and changed in the underlying Windows Operating System and after the Forefront TMG installation has been finished, my Process Monitor recorded over eight! Million process activities (File system access, Registry access, process executions and more) ☺

## Related links

Microsoft (Sysinternals) Process Monitor

<http://technet.microsoft.com/en-us/sysinternals/bb896645>

Forefront TMG Setup log files

<http://technet.microsoft.com/de-de/library/ee781947.aspx>

Forefront TMG Troubleshooting

<http://technet.microsoft.com/en-us/library/dd897100.aspx>

SuperFlow for Troubleshooting Forefront TMG Installation

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=f1ebfda1-da51-44cc-99cb-96ad0fd40bdf>

Troubleshooting ERROR: Setup failed to install ADAM.\r\n (0x80074e46) and 0x80070643 while trying to install TMG 2010

<http://blogs.technet.com/b/isablog/archive/2010/07/07/troubleshooting-error-setup-failed-to-install-adam-r-n-0x80074e46-and-0x80070643-while-trying-to-install-tmg-2010.aspx>

Microsoft Forefront TMG – TMG Storage 101

<http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Storage-101.html>