

Configure Forefront TMG to integrate with an TMG Array

Abstract

In this article, I will show you how to integrate Microsoft Forefront TMG into an TMG array for centrally administration purposes.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

A few month ago, Microsoft released Beta 2 from Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

Before we start installing Microsoft Forefront TMG into an array, I would like to explain to you the new terminology used in Forefront TMG. There are two different terms:

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

EMS

The Enterprise Management Server is a server which is used to manage an TMG Enterprise Array or possible a standalone server.

CSS

The Configuration Storage Server (CSS) is used for all local TMG installations and provides the storage for the TMG Server configuration. Every TMG has a local CSS. After the TMG administrator joins the Server to an TMG Array, the local TMG Server will use the Enterprise CSS (EMS). After the local TMG server has joined the Enterprise CSS, the local CSS will be disabled.

First we have to create a new Microsoft Forefront Threat Management Gateway Enterprise. To do so, start the setup from the TMG setup installation file and select the appropriate option.

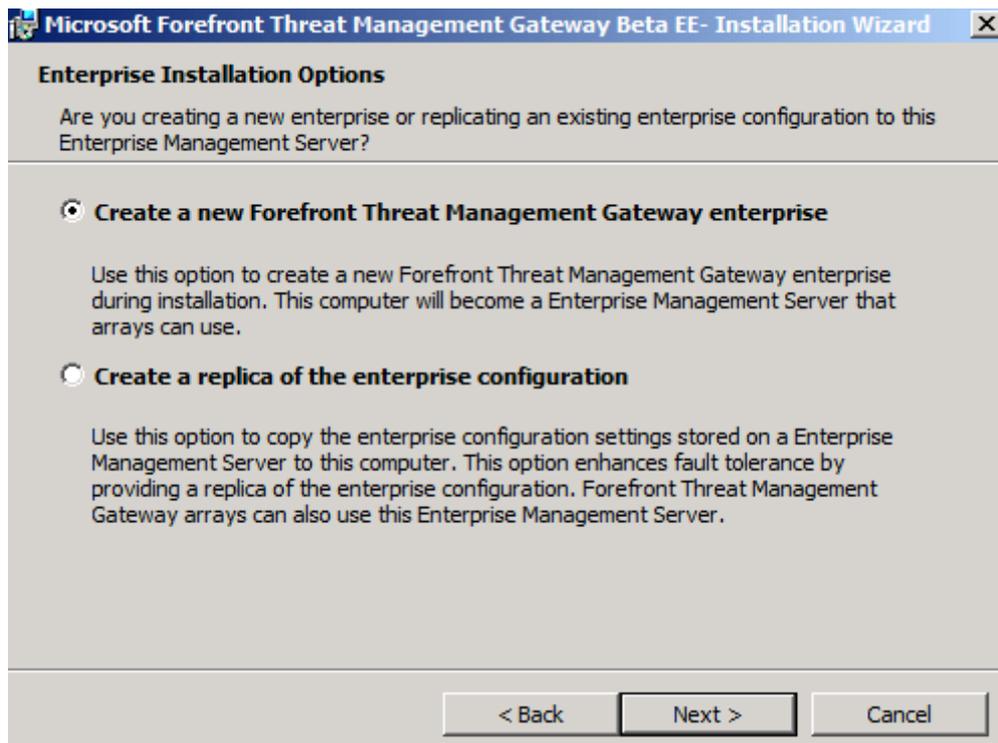


Figure 1: Create a new Microsoft Forefront Threat Management Gateway Enterprise

It is also possible to create a replica from the Enterprise configuration. This will create a new EMS server which works hand in hand with the other EMS server. An productive TMG Enterprise should always have two or more EMS Server.

You must specify an account which is used for the EMS service. In this lab, I used the Administrator account from the domain. In an production environment you should use another not so security critical account.

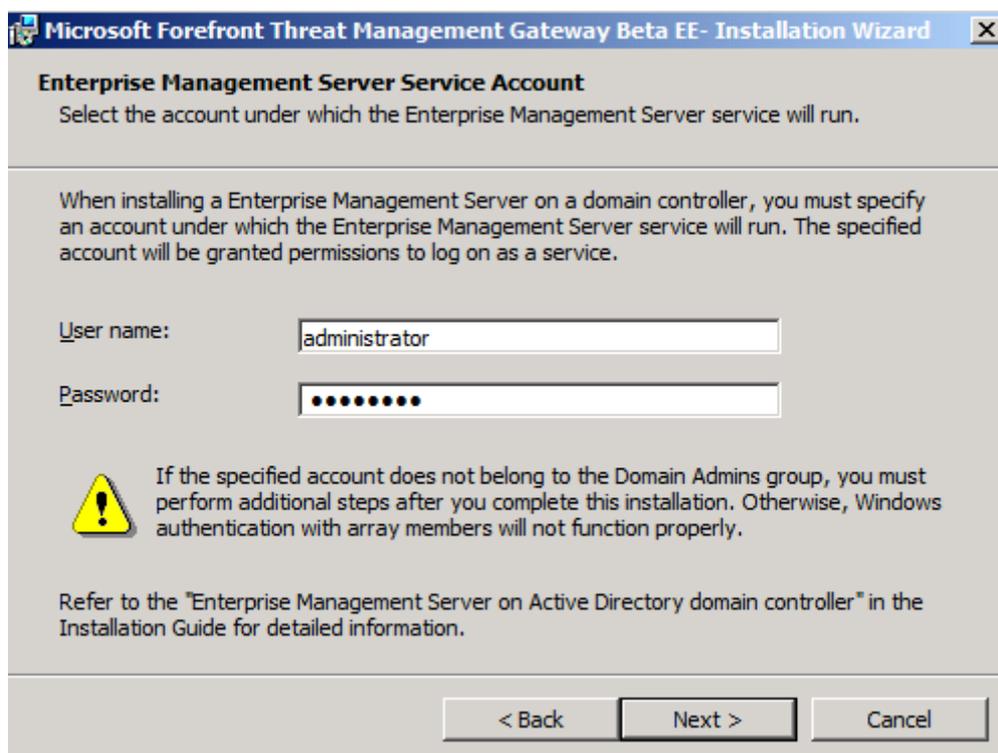


Figure 2: Enterprise Management Server Service Account

The following figure give you a overview about the new Microsoft Forefront Threat Management Console with the EMS Server installed. The configuration is similar to the ISA Server 2006 Management Console, as you can see in the following screenshot.

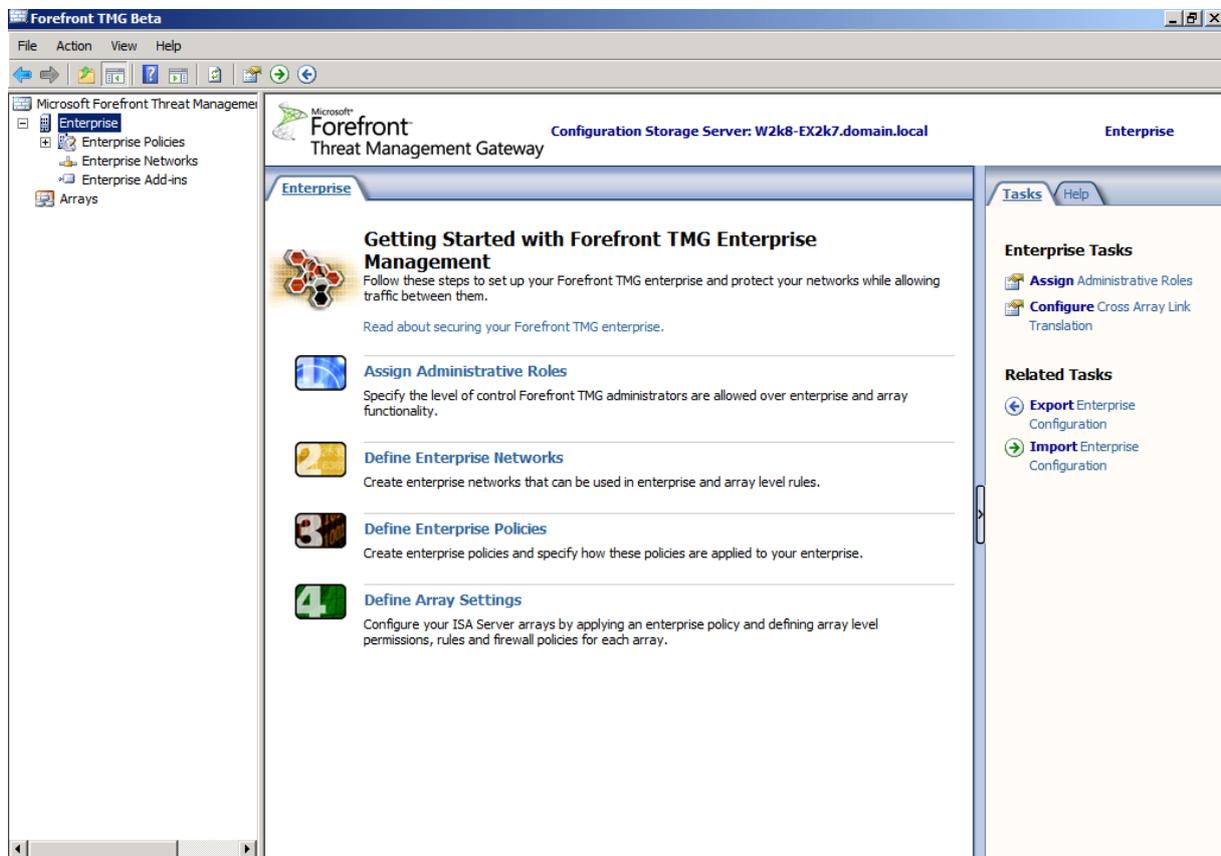


Figure 3: New Microsoft Forefront Threat Management Gateway Enterprise and console

Next, we have to create a new TMG Array, and after that it will be possible to join standalone TMG Servers to the new TMG Array. Start creating a TMG Array by executing the wizard to create new Arrays.



Figure 4: Wizard to create a new TMG Array

It is possible to create multiple Arrays in the TMG Enterprise, and there is a minimum of one Server per TMG Array. You must assign a name for the new Array.

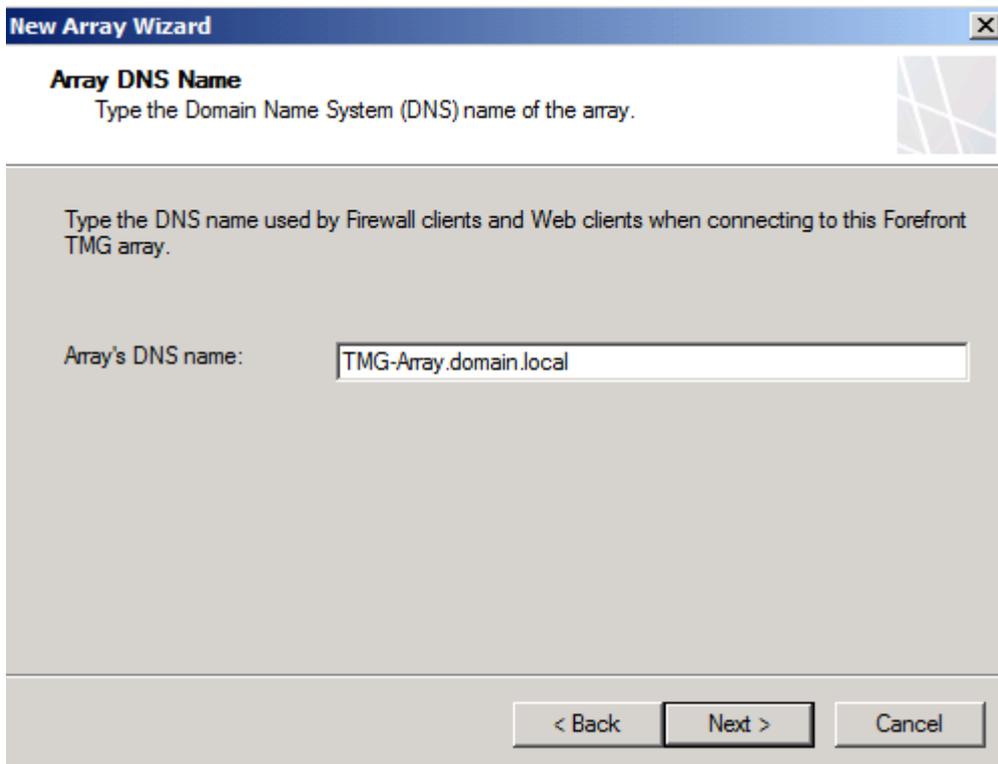


Figure 5: Specify the Array DNS Name

As a next step, every Array must have a resolvable DNS name. The DNS name is used by the TMG Server Firewall Client and the Webproxy client. You must create a corresponding DNS record in your internal DNS Server for the TMG Array servers.

Every Array must have an Enterprise Policy. Select the default Policy or better a newly created Enterprise Policy which should be used in the Array.

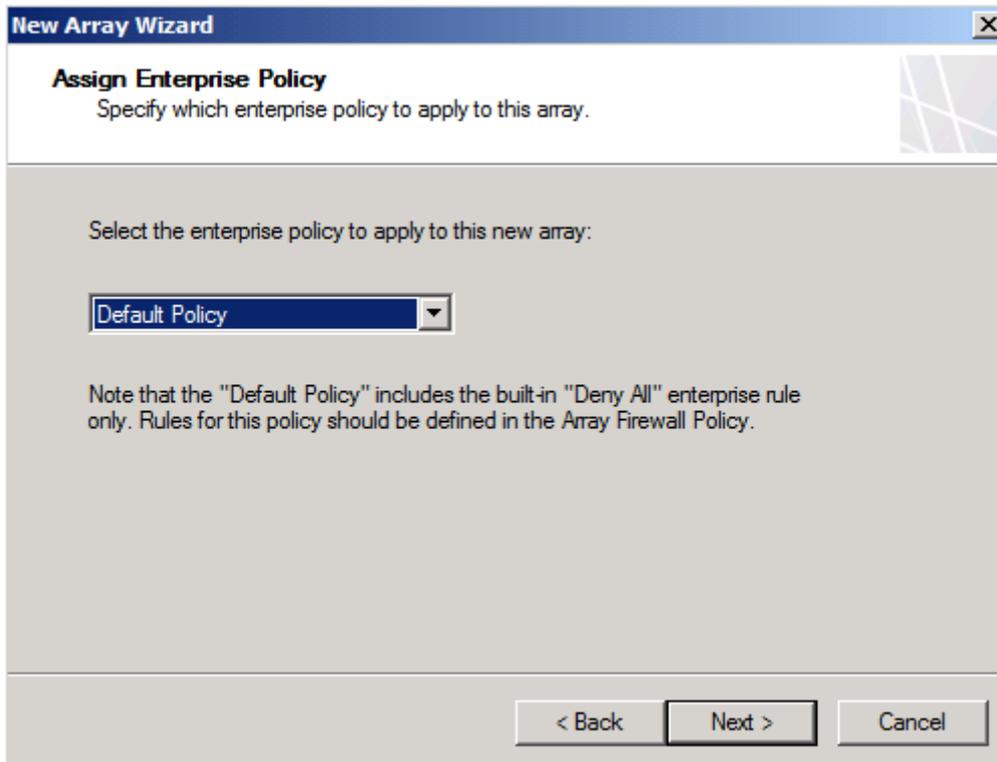


Figure 6: Assign an Enterprise Policy

Now it is time to select which type of Array Firewall policy rules can be created for the Array.

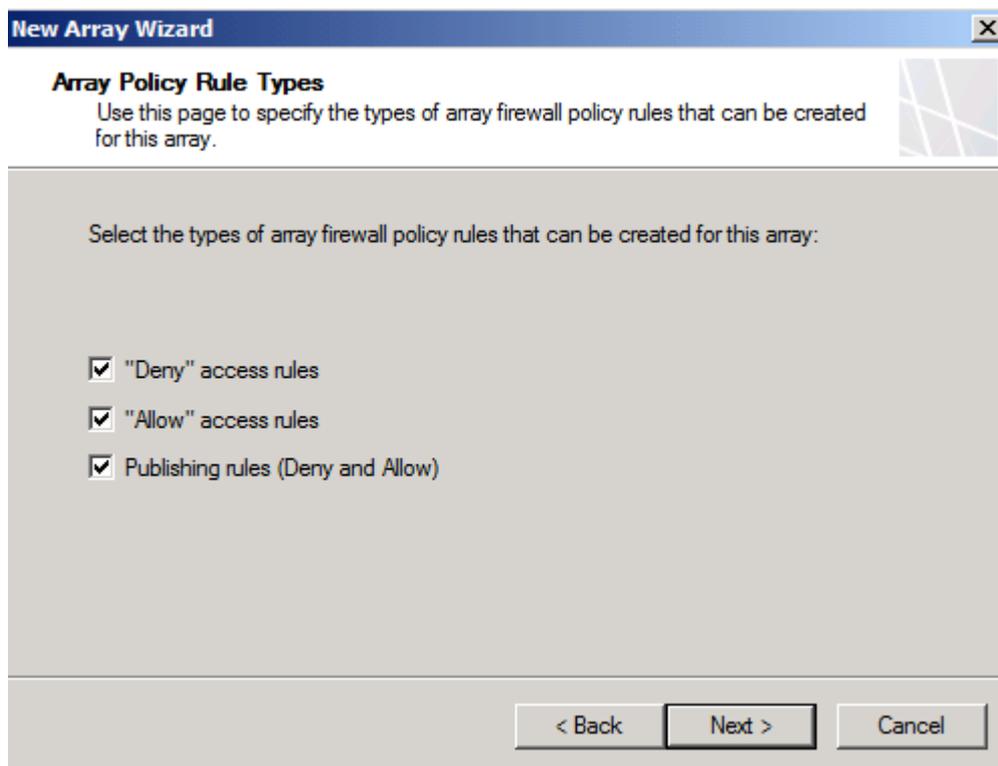


Figure 7: Specify Array Policy Rule Types

It takes some time to create the new TMG Array, depending on the performance of your system.

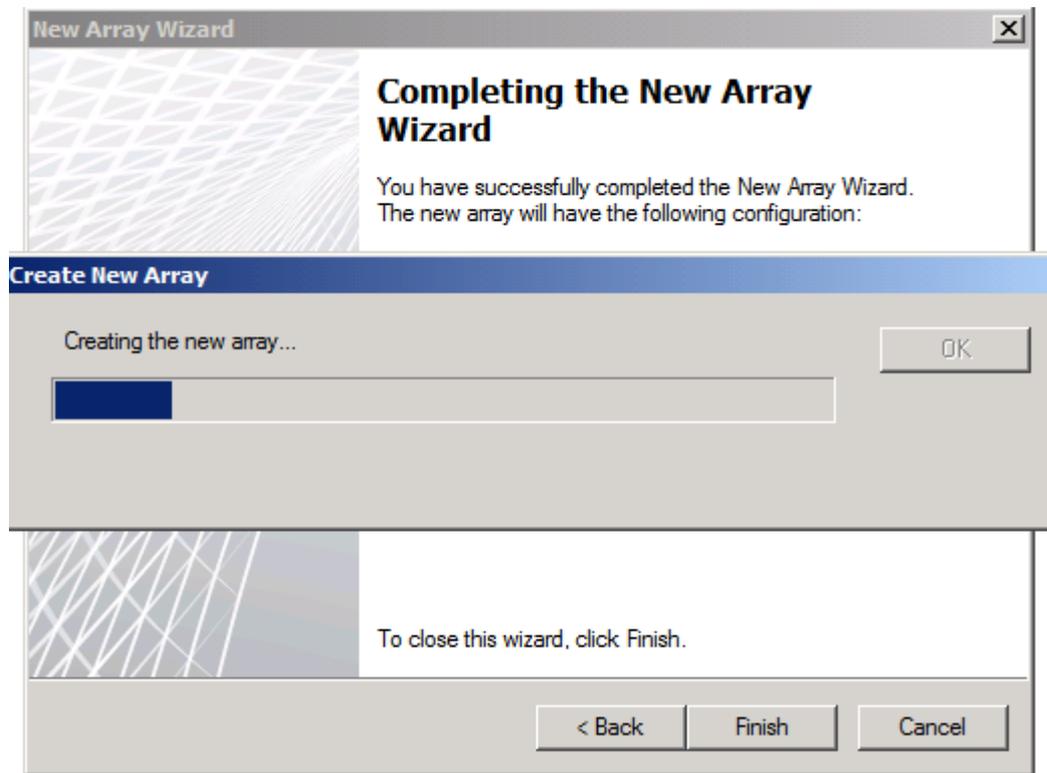


Figure 8: Create a new Array process

After some minutes, the TMG Array should be created successfully as you can see in the following screenshot. It is now possible to join the standalone TMG servers to the TMG Enterprise.

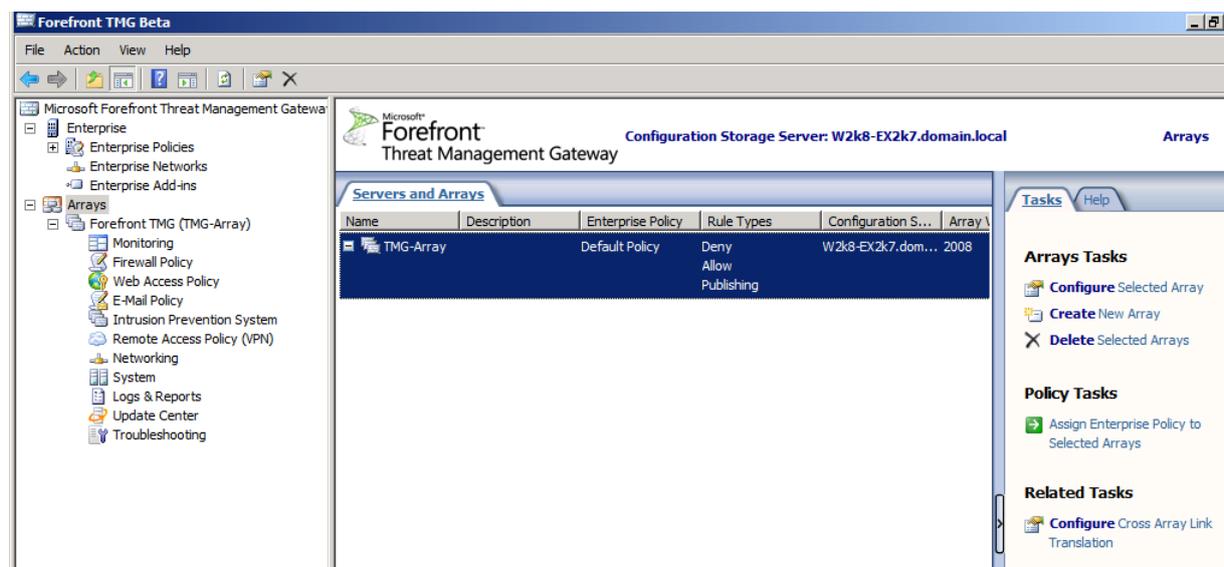


Figure 9: New created TMG Array

The installation of Microsoft Forefront TMG is part of other articles on www.isaserver.org so I only created one screenshot about the installation process to see which setup option you must choose in the TMG installation wizard.



Figure 10: Installing TMG

After the TMG setup has successfully finished, start the Microsoft Forefront Threat Management console and click the Join Array option in the task pane as shown in the following screenshot.

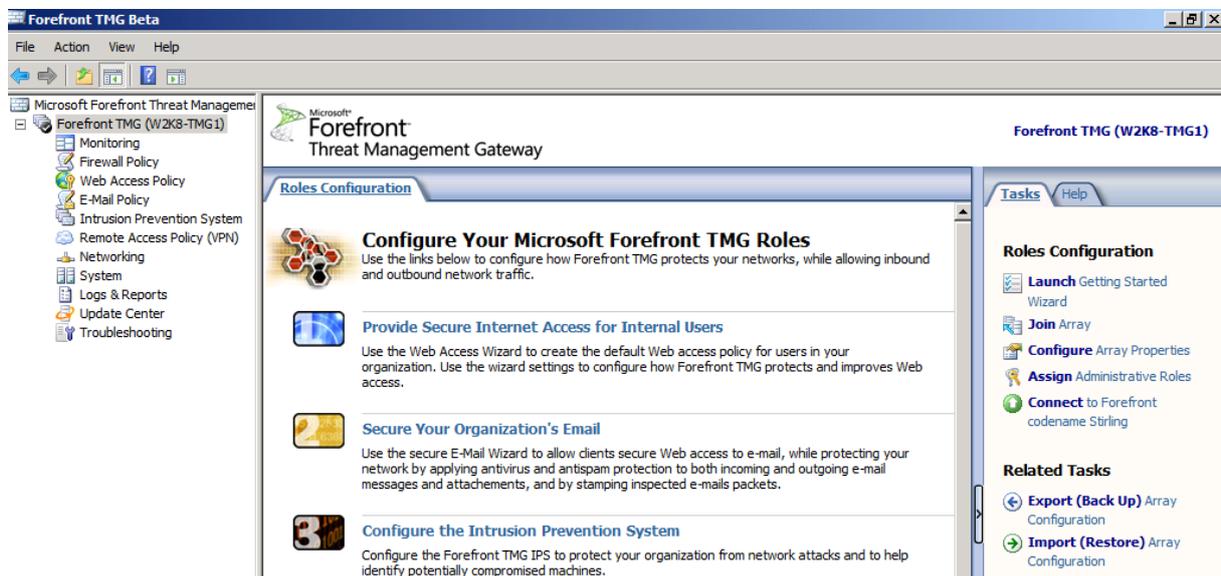


Figure 11: Start the Join Array Wizard

The Join Array Wizard starts



Figure 12: Join Array Wizard

Select the Array Membership type. Because we previously created an Enterprise Management Server and a TMG Array, we will join the standalone TMG server to the EMS.

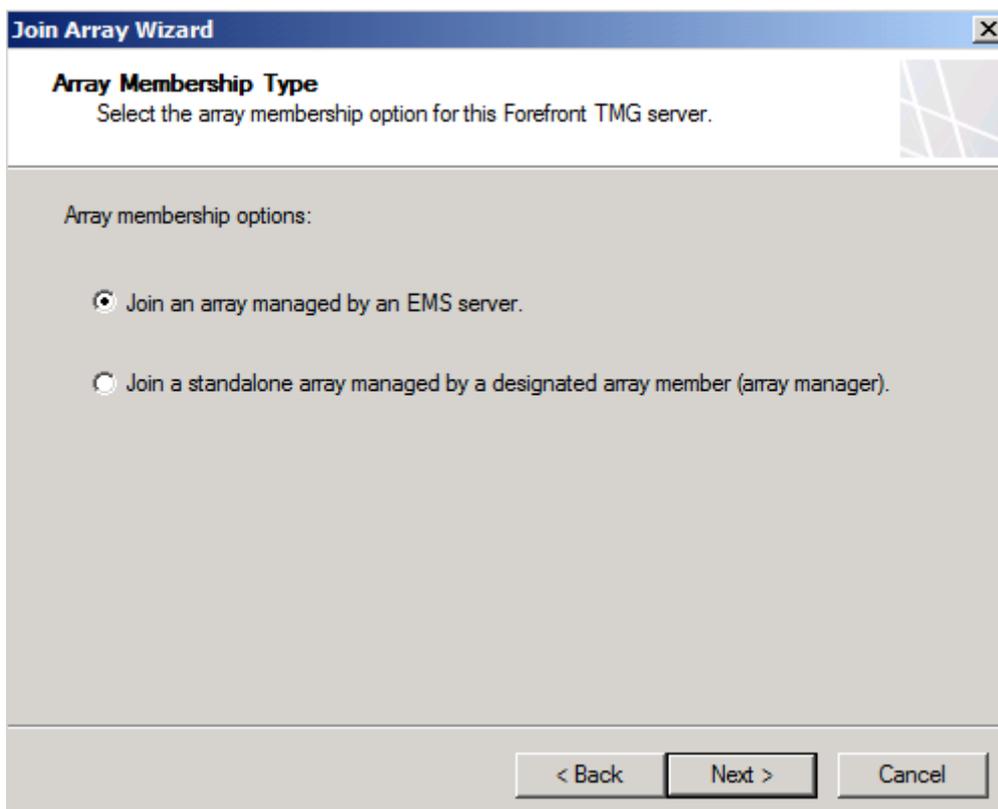


Figure 13: Join an array managed by an EMS Server

Specify the fully qualified domain name (FQDN) for the the EMS. It is also possible to change the account which has the rights to connect to the EMS server.

The screenshot shows a window titled "Join Array Wizard" with a close button (X) in the top right corner. Below the title bar, the text "Enterprise Management Server Details" is displayed in bold. Underneath, a subtitle reads "Select the EMS server and specify the user account used to connect to the selected server." The main area of the dialog contains a text input field labeled "EMS fully qualified domain name (FQDN):" with the text "W2k8-EX2k7.domain.local" entered. To the right of this field is a "Browse..." button. Below this is a section titled "User account with rights to connect to the EMS server" containing two radio button options: "Connect using the credentials of the logged on user" (which is selected) and "Connect using this account:". Under the second option are two text input fields labeled "User name:" and "Password:". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Figure 14: Specify the EMS FQDN

Because we already created an TMG Array in the EMS, we will select the previously created TMG Array. It is also possible to create a new Array, but this could take a longer time as creating the Array on the EMS Server because of network latency.

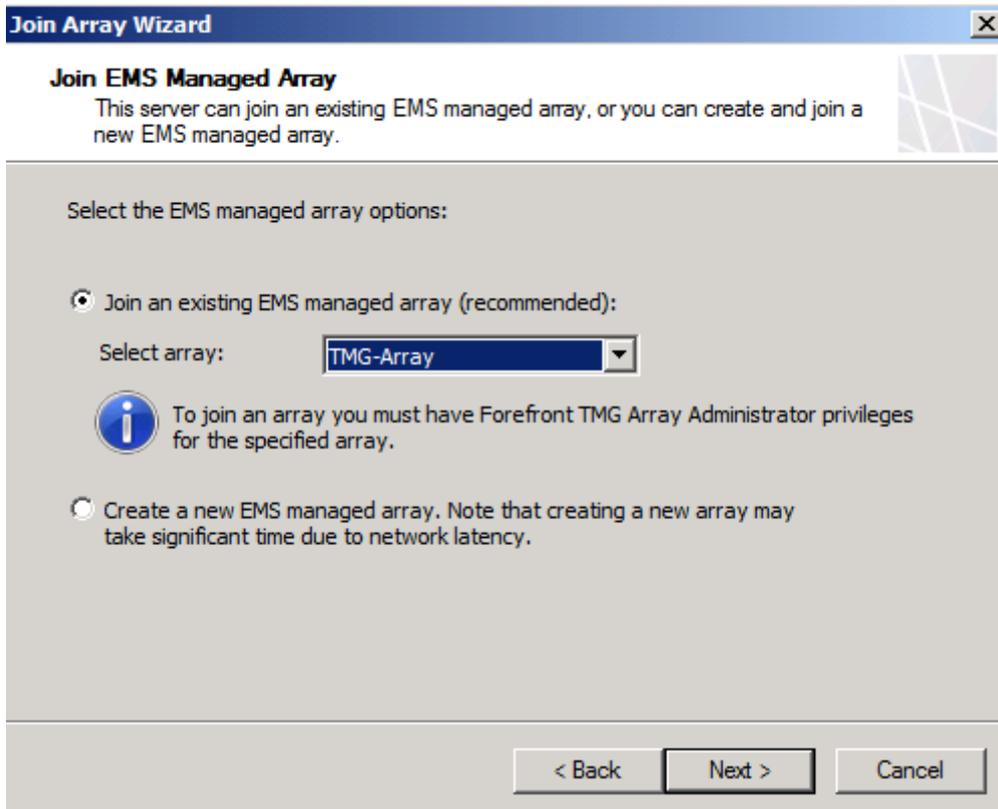


Figure 15: Join an existing EMS array

The TMG standalone server is now joining the TMG Array.

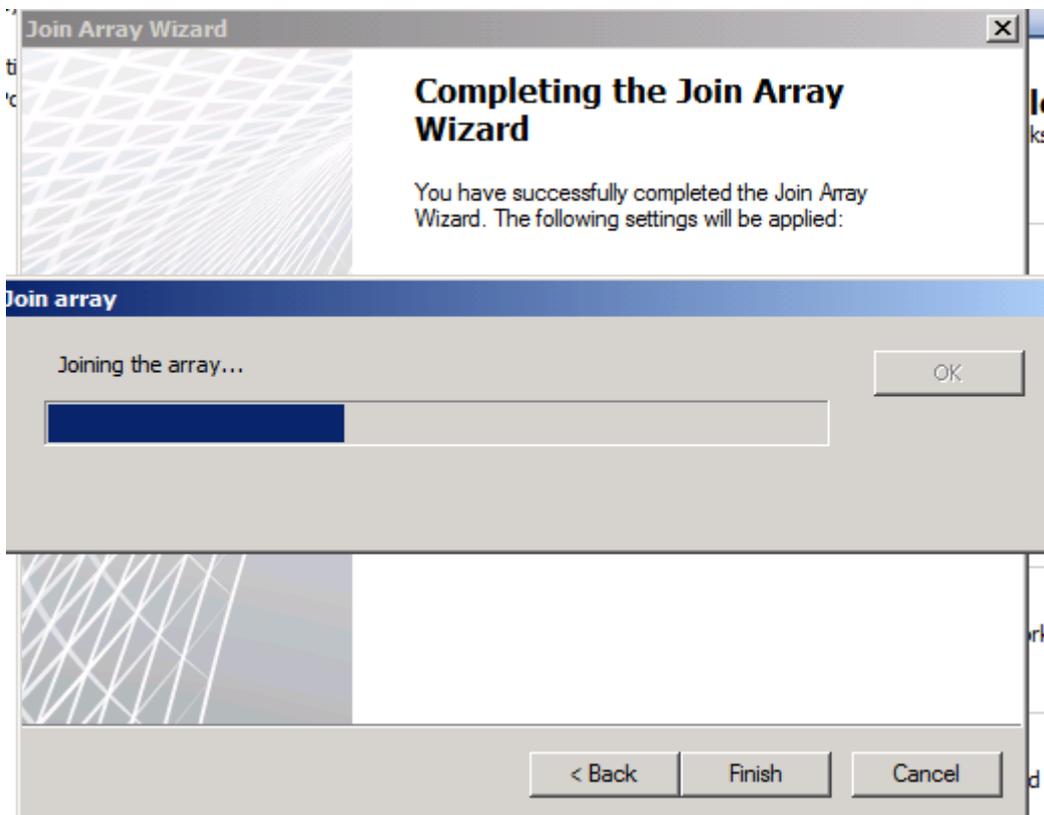


Figure 16: Join the array phase

After some time, the TMG standalone Server is now a member of the EMS Array.

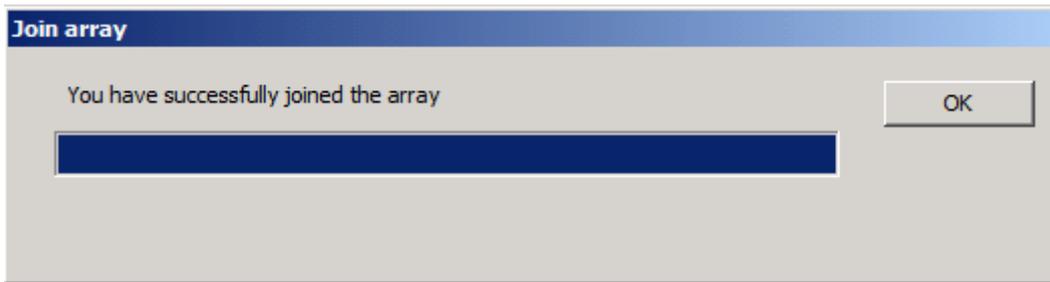


Figure 17: Array successfully joined

Start the TMG Management console and navigate to the properties of the newly Array joined TMG server and you will see that the TMG server is now managed by the EMS array.

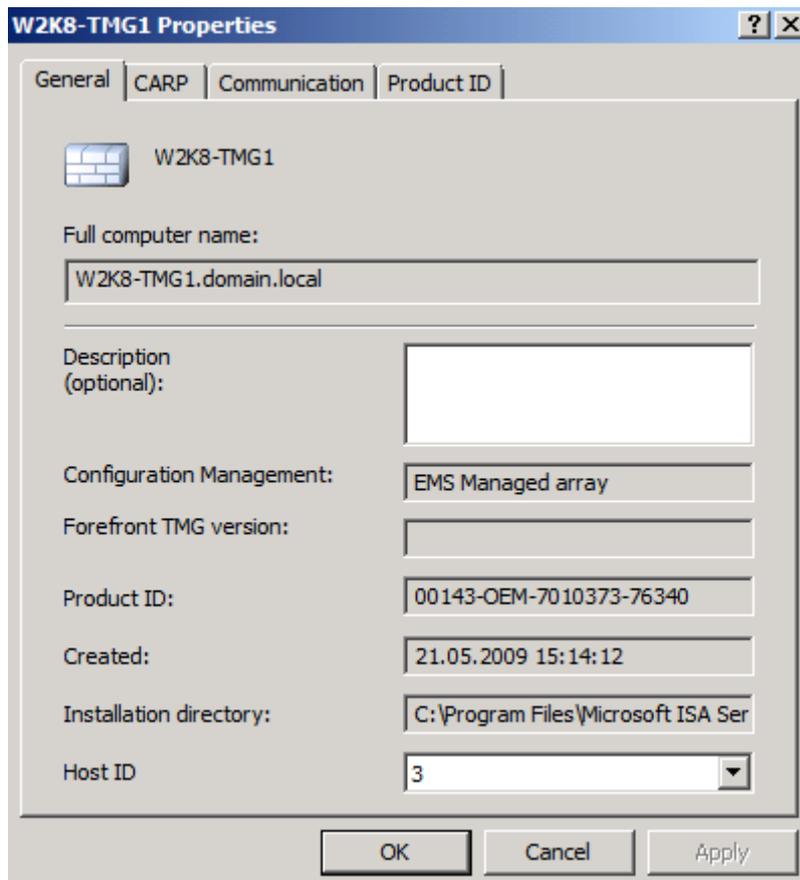


Figure 18: EMS Array information

To see which CSS (Configuration Storage Server) is used by the TMG Server, navigate to the TMG Array properties, click the Configuration Storage tab. If you have a second CSS Server, which is recommended, enter the additional CSS Server as an alternate Configuration Storage Server.

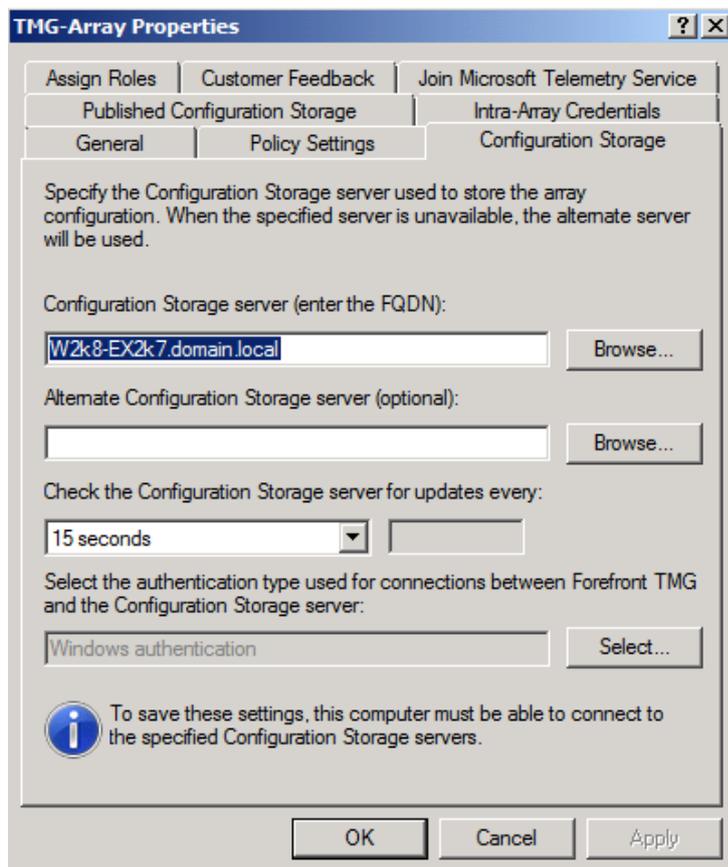


Figure 19: TMG Array properties

After joining the Server to the TMG Array, you can now configure TMG for your business needs.

Conclusion

In this article, I gave you an overview about how to integrate the Microsoft Forefront Threat Management Gateway into an TMG array to centrally manage all TMG servers within the TMG Enterprise or Array. There are not a lot changes from ISA Server 2006 Enterprise CSS concepts, so you should be quickly familiar with the EMS console in Microsoft Forefront TMG.

Related links

Forefront Threat Management Gateway Beta 2

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&DisplayLang=en>

Forefront TMG Beta 2 is Released

<http://blogs.technet.com/isablog/archive/2009/02/06/forefront-tmg-beta-2-is-released.aspx>

What's new in Forefront TMG Beta 2 (Part 1)

<http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html>

Installing and configuring Microsoft Forefront TMG Beta 2

<http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html>