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

Microsoft Forefront UAG – Creating a portal with Forefront UAG

Abstract

In this article I will show you the basic concepts behind a Forefront UAG trunk to create a portal for web access to access different internal applications like Microsoft Sharepoint, Exchange Server and more.

Let's begin

One of the biggest enhancements in Microsoft Forefront UAG comparing with Forefront TMG is the UAG capability to provide a web portal for users on the Internet which needs access to internal applications.

Forefront UAG uses a terminology called a portal trunk. A Trunk is a combination of a IP address, HTTP/HTTP port and a certificate when a HTTPS trunk should be created. The portal trunk is the entry point for all published applications into this portal. It is possible to authenticate against this portal again different directory services like Active Directory, Novell, Netscape and more. A portal trunk also allows the Administrator to apply Forefront UAG Endpoint access policies. An Endpoint access policy is able to check the client for compliance state. For example the client must have the Windows Firewall enabled, all Windows updates must be installed on the machine and the machine must be joined to the internal Active Directory domain. I will give you more insight into UAG endpoint access policies in another article published here at www.isaserver.org.
The client can access the UAG portal after some Forefront UAG Endpoint components have been installed on the client.

To create a new trunk we must open the Forefront UAG Management console (MMC). There are two types of trunks which can be created: A HTTP and a HTTPS trunk.

For the example in this article we will create a HTTPS portal trunk. This portal trunk can be used to publish different applications. I will give you more information about how to publish internal applications through a Forefront UAG portal in some additional articles published in the near future at www.isaserver.org.

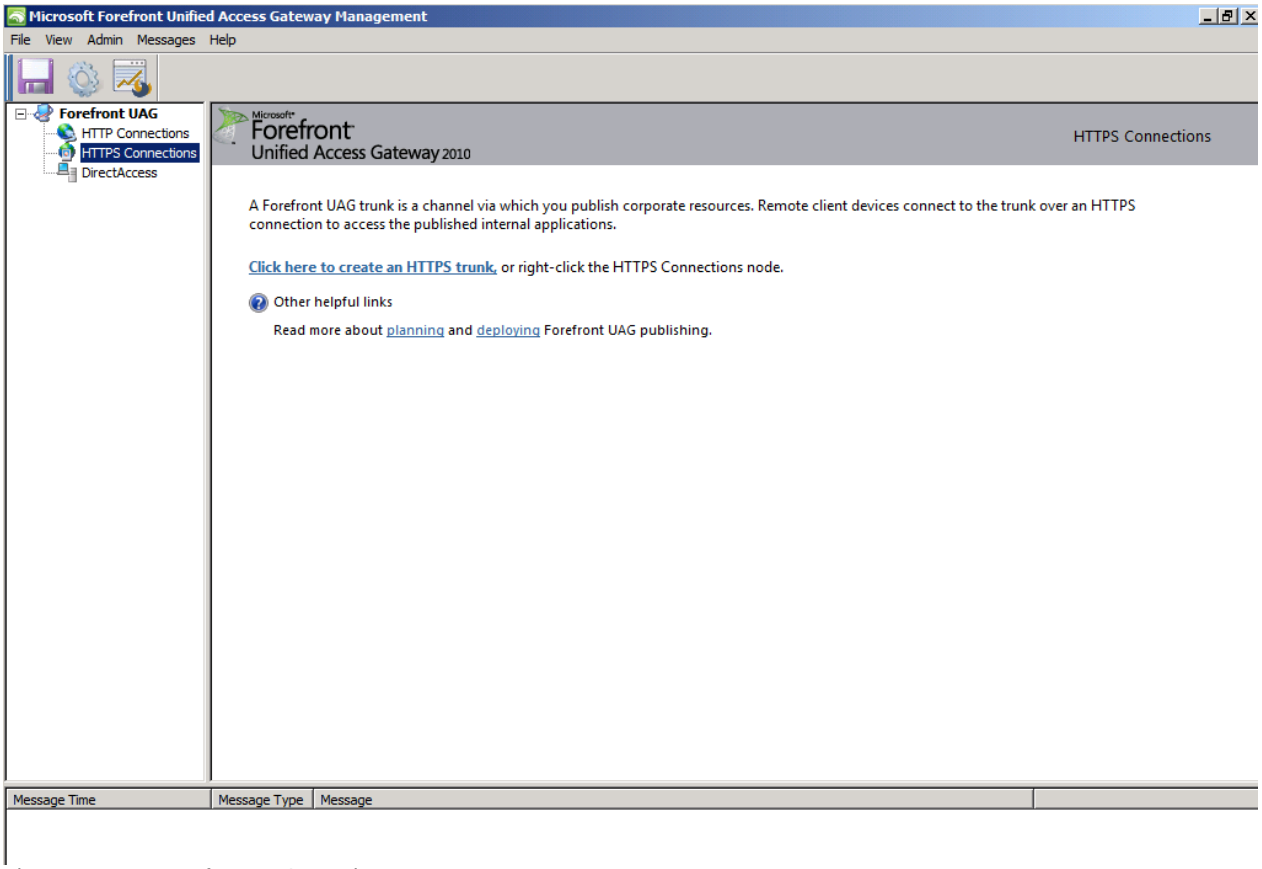

Figure 1: Empty Forefront UAG portal

Before we create a new portal we should first create a Authentication and Authorization repository. For the example in this article we will use Active Directory as a the authentication provider. Start the Forefront UAG MMC and navigate to Admin – Authentication and Authorization Servers.

Specify the Domain controllers used for authentication, the entry point (Distinguished Name (DN)) and a service account which must have read access to the Active Directory configuration. For SSO (Single Sign On) it is possible to enter the internal Active Directory Domain name.

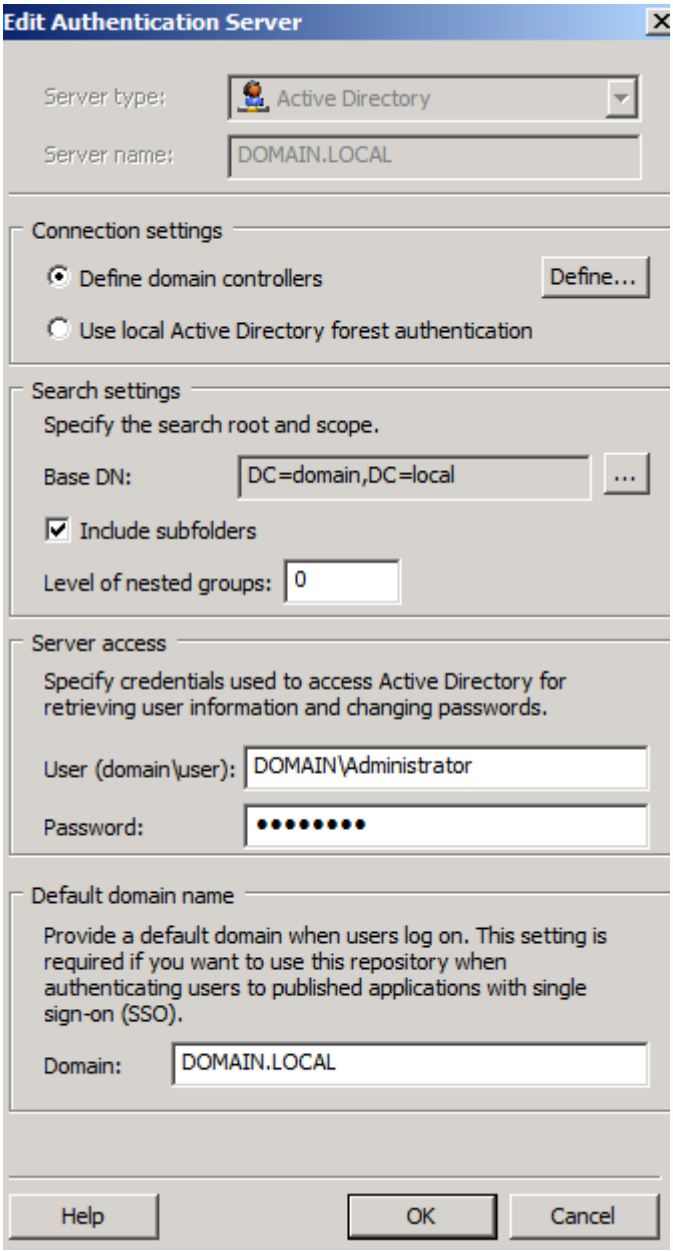

Figure 2: Configure authorization servers

After the Authorization/Authentication repository has been configured, we are able to create a new trunk. Right click the HTTPS connection and start the Welcome to the Create trunk Wizard. We would like to create a Portal Trunk as shown in the following screenshot.

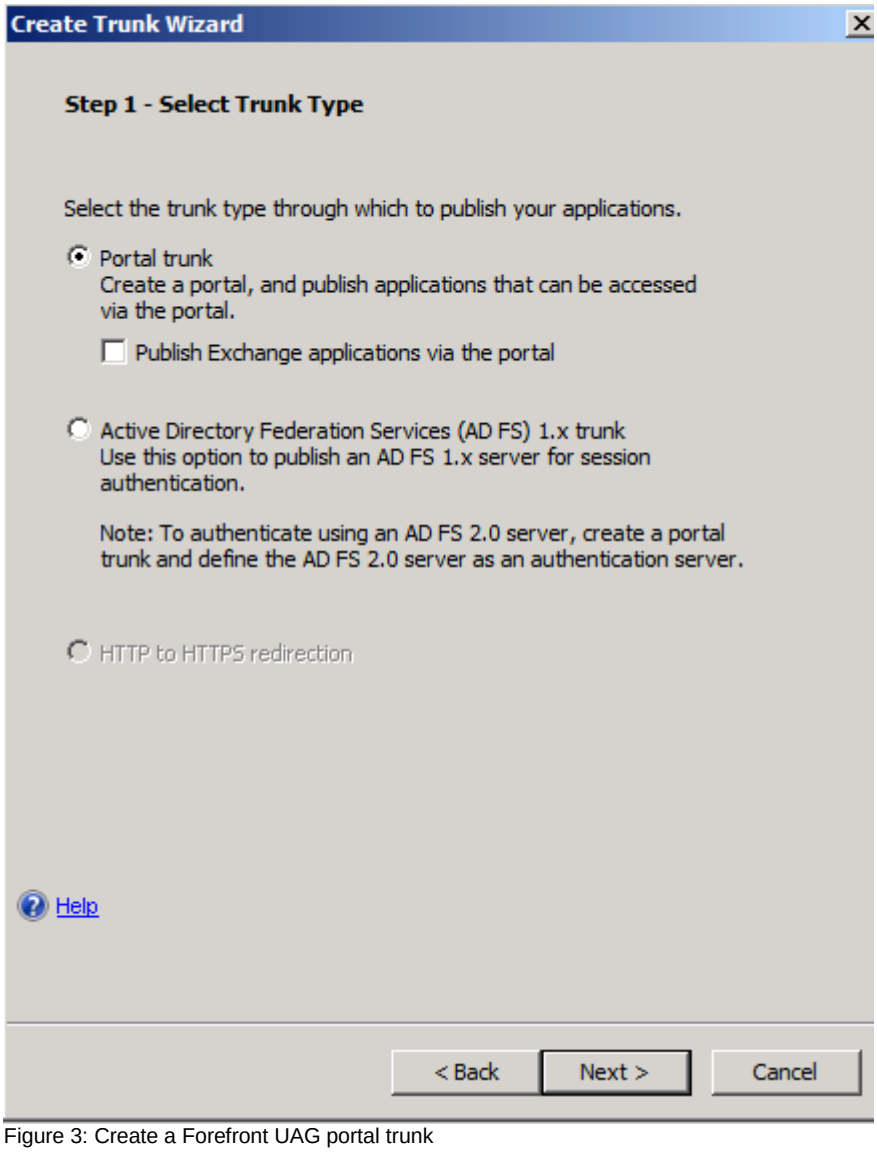

Figure 3: Create a Forefront UAG portal trunk

We must specify a portal trunk name and a public hostname which clients use to access the portal. The public Host name must match the certificate name you use for the HTTPS connection. Enter the public IP address and the port number used for the trunk and click Next.

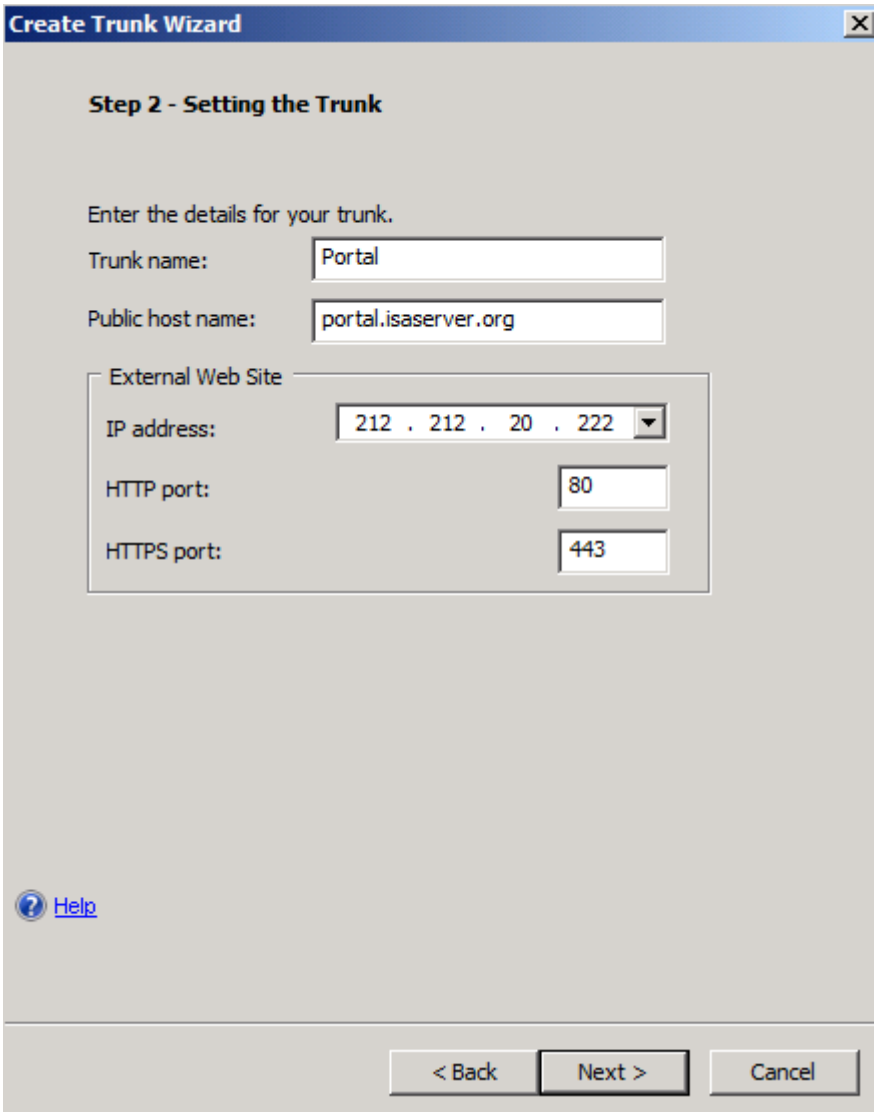

Figure 4: UAG trunk settings

In Step 3 we use the Authorization repository created earlier.

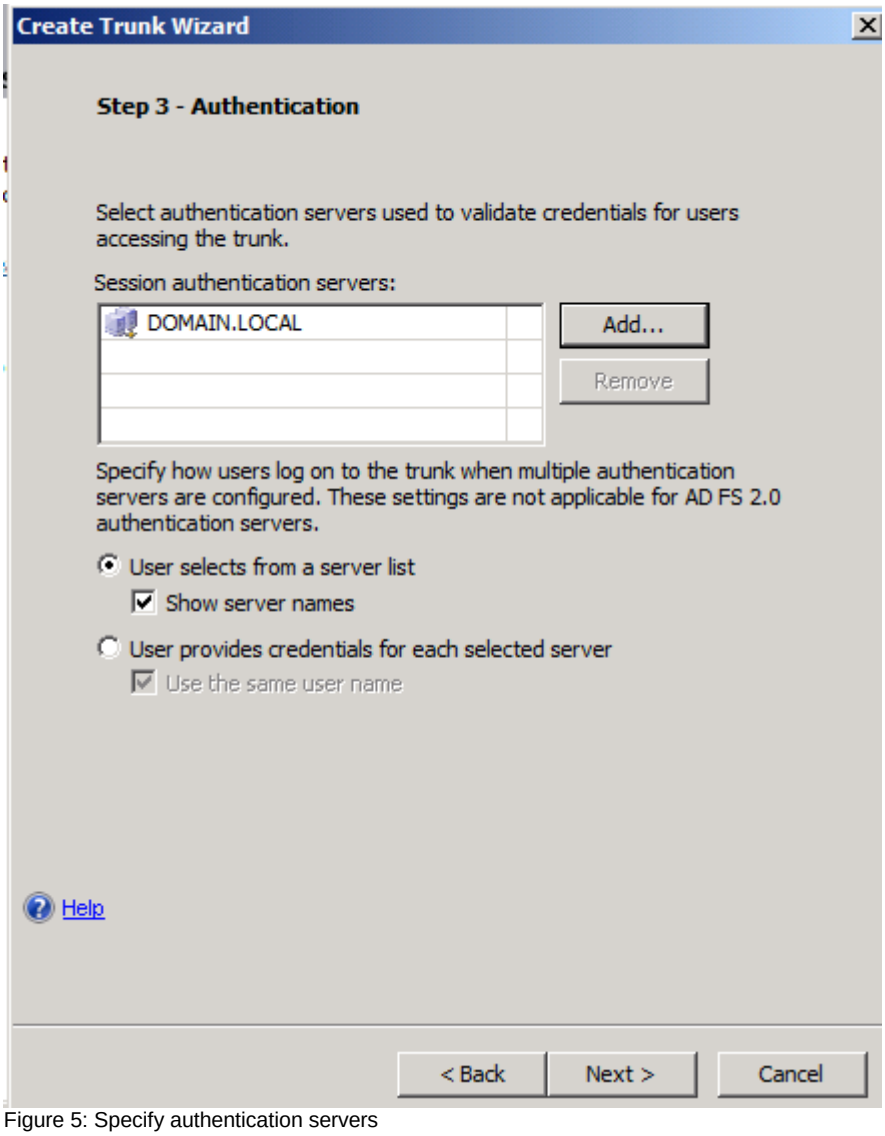

Figure 5: Specify authentication servers

The next step is to select the certificate which should be used to establish the SSL connection between the external clients and the Forefront UAG Server. The certificate can be issued from an internal Certification Authority (CA) or a commercial CA. In most cases it makes sense to use a certificate issued by a commercial CA because this certificate is trusted by the most used Web browsers today. The certificate must be stored with the private key (.PFX) into the local computer certificate store on the Forefront UAG Server.

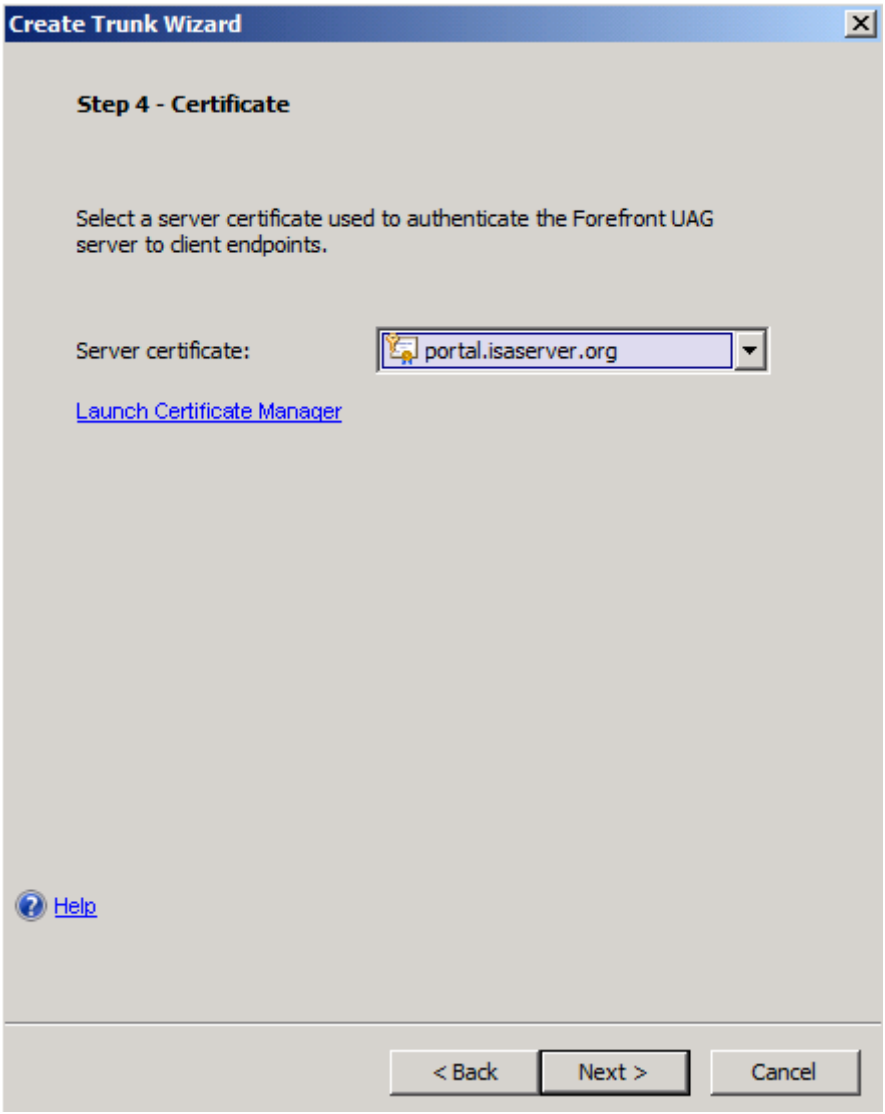

Figure 6: Specify authentication servers

You can use Forefront UAG Endpoint access policies or you can use NAP (Network Access Protection) to check clients before they can use the portal. You are able to use local NAP policies from the local installed NPS (Network Policy Server) or Forefront UAG own endpoint access policies. In most cases I recommend using Forefront UAG policies because they are more powerful.

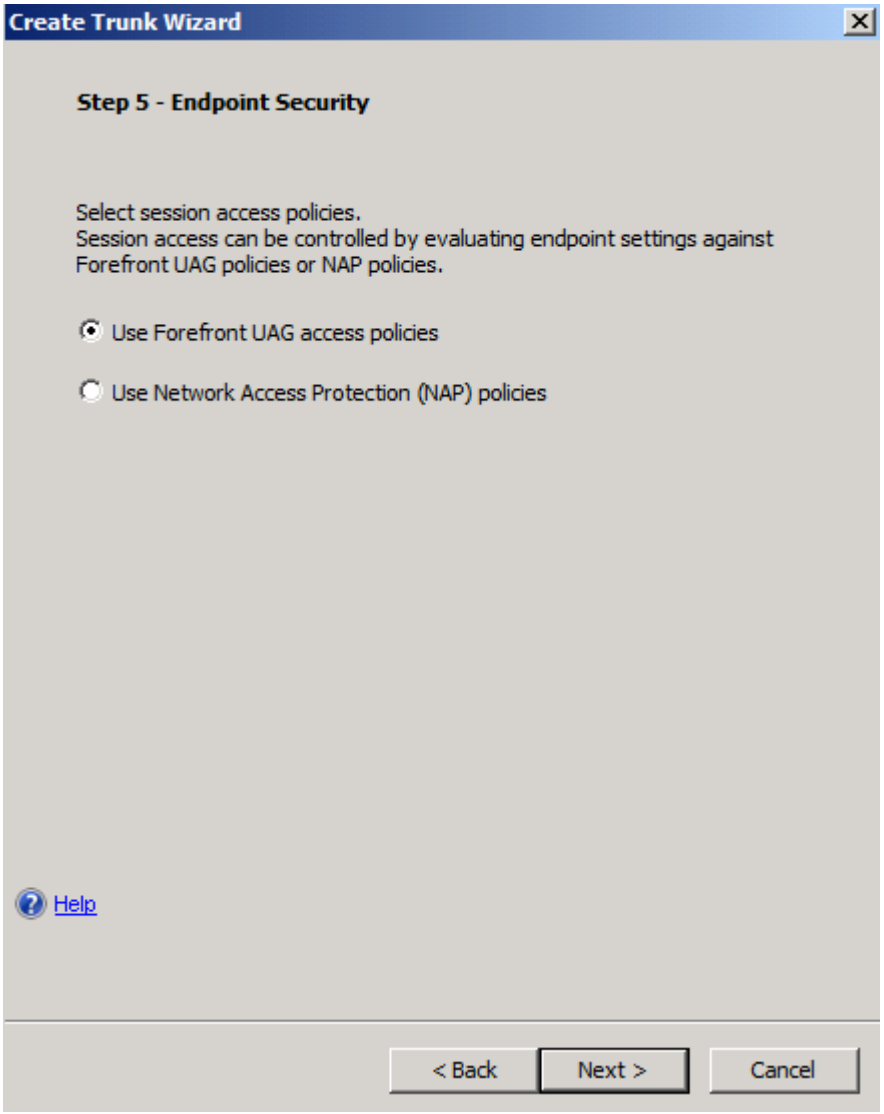

Figure 7: Endpoint Security

If you decided to use Forefront UAG policies you can now select which Endpoint policies you want to use. Forefront UAG comes with a lot of builtin Endpoint policies and Administrators are able to create its own Endpoint policies.

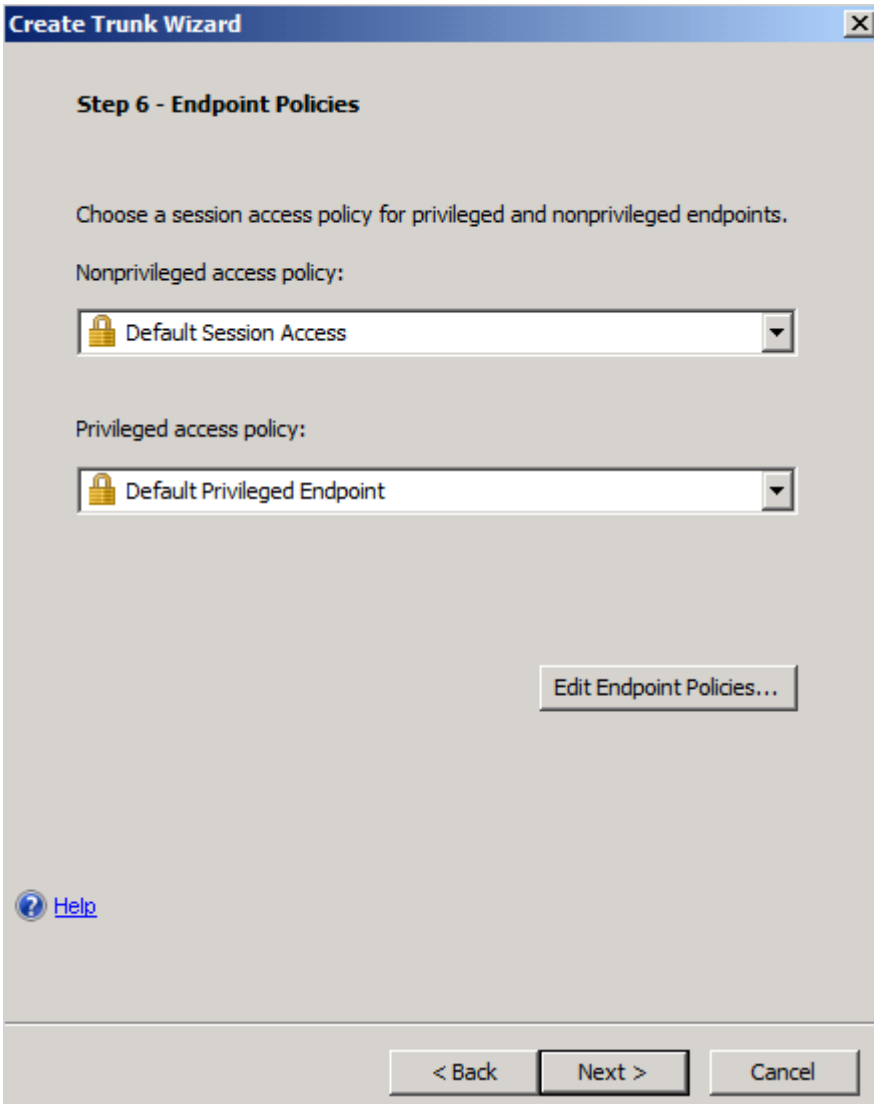

Figure 8: Endpoint access policies

After the wizard has been finished you will now see the created Forefront UAG portal trunk as shown in the following screenshot.

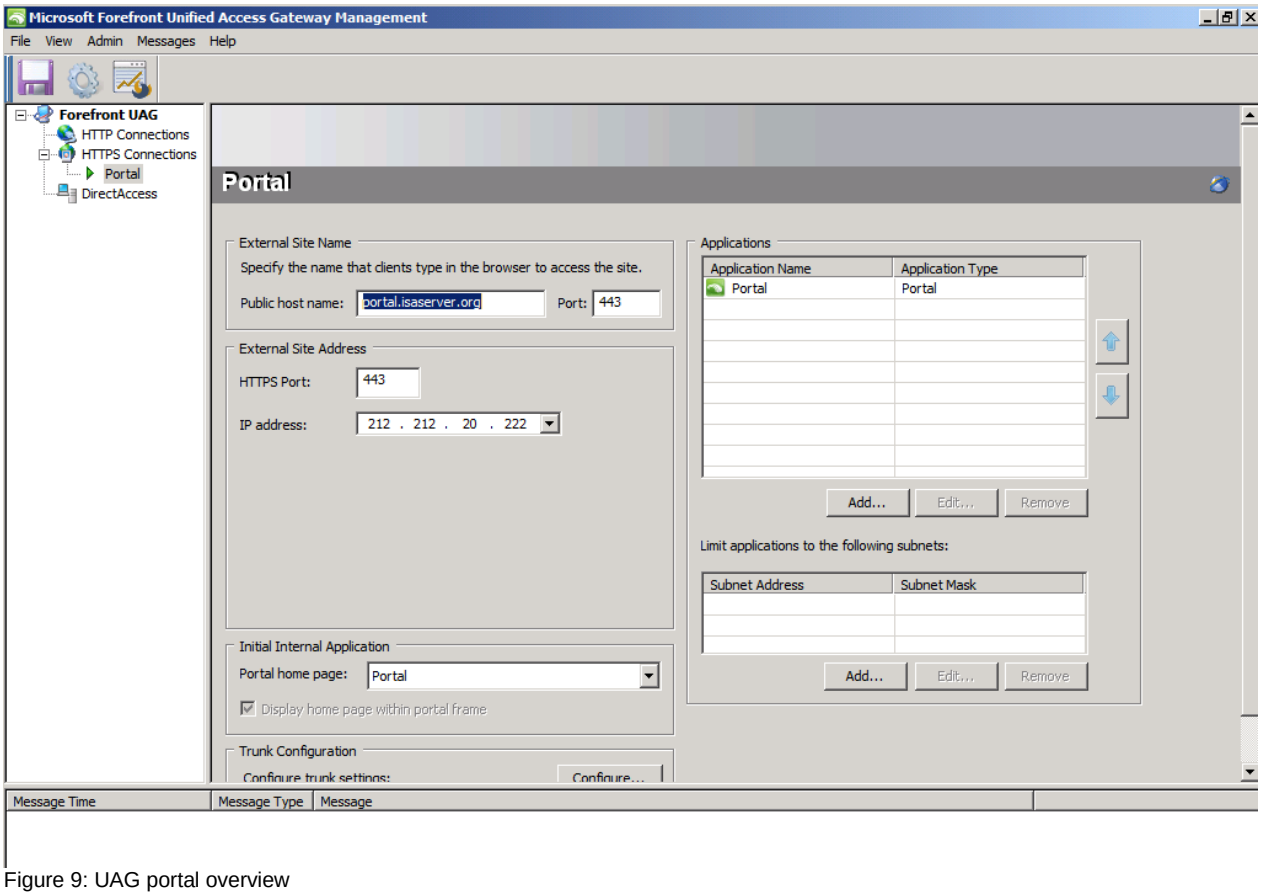

Figure 9: UAG portal overview

We must now save the configuration to store the changes to the UAG configuration. Click the floppy symbol to save the configuration. After that we can activate the configuration so that all changes will be effective after a short amount of time. To activate the configuration click the button right from the floppy symbol.

Configure trunk settings

After the trunk has been created we are now able to customize the trunk settings. I will give you a high level overview about the different configuration options. On the General tab we are able to specify the maximum number of users which should be able to currently access the portal trunk and we can also check the certificate used in the HTTPS portal trunk.

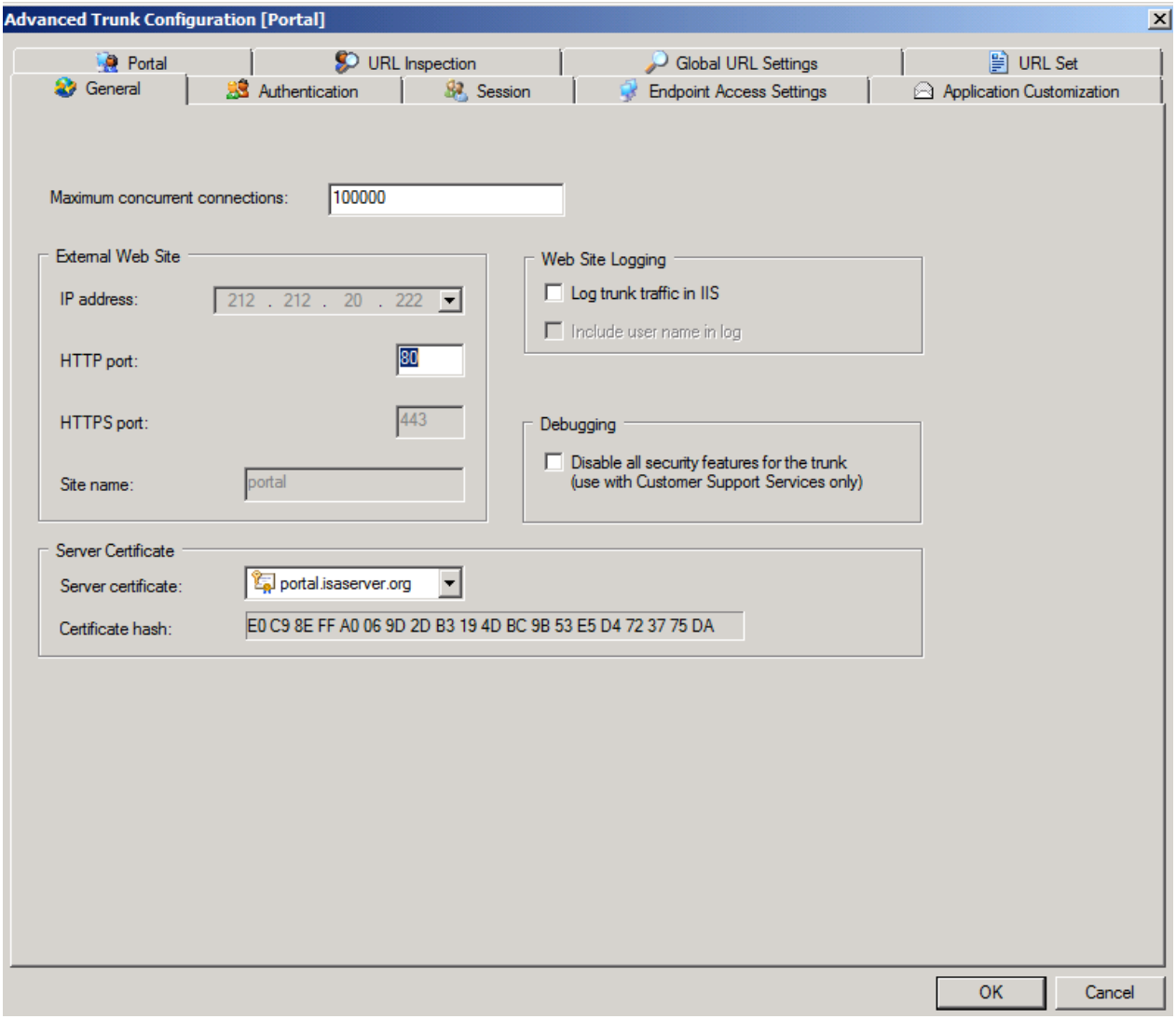

Figure 10: General portal settings

On the Authentication tab it is possible to specify the Authentication Server, if users should be able to change their passwords through the trunk and if you are familiar with Forefront UAG you are able to customize the Logon and Logoff scheme used by Forefront UAG.

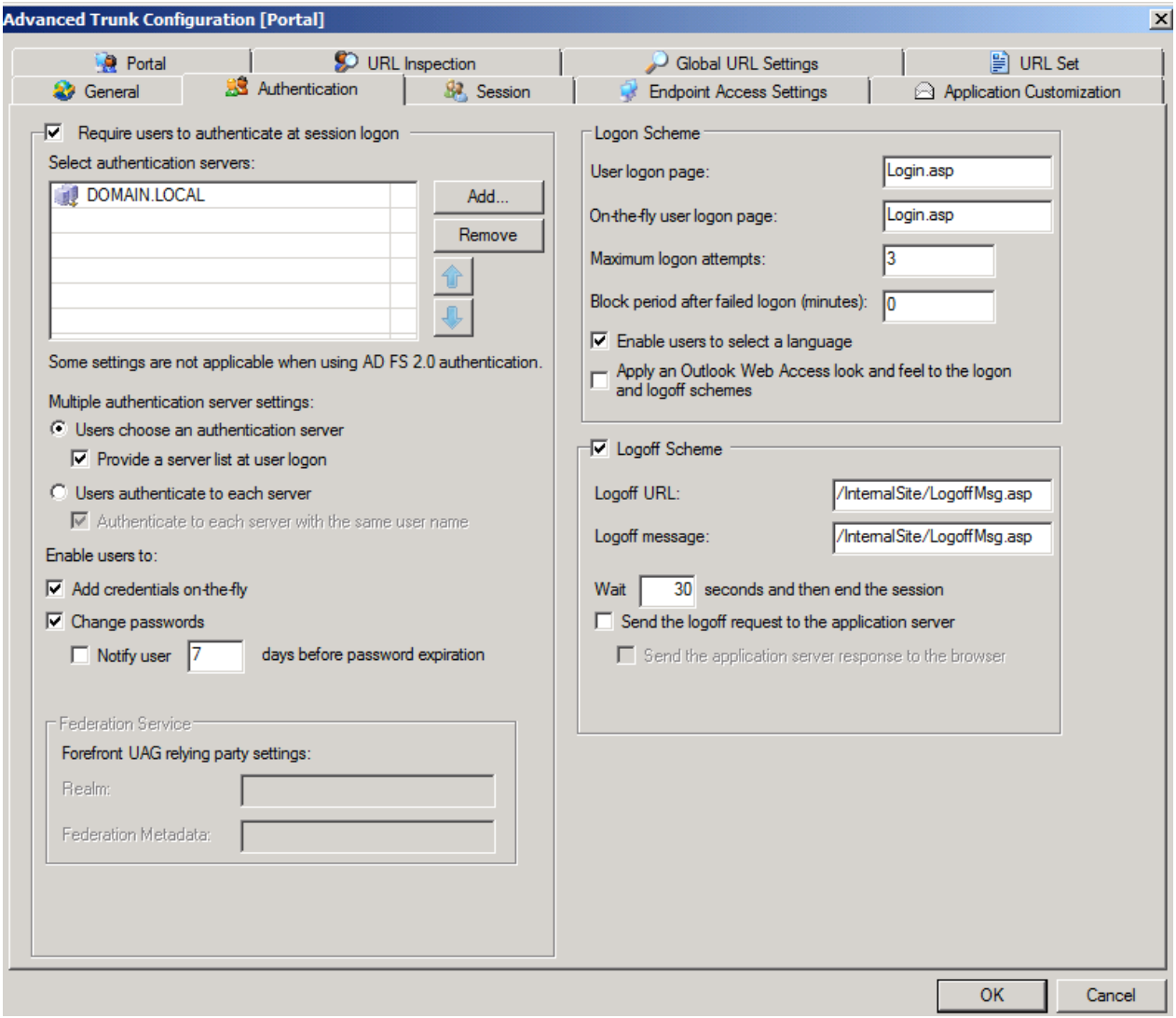

Figure 11: Authentication servers

The Session tab let you customize all relevant session access settings like connection timeouts, maxium session times for the Default and Privileged session access. Forefront UAG is able to distinguish between default (unmanaged) clients and more trusted (managed) clients. This configuration tab also allows Administrators to handle with some Endpoint access settings for clients connecting to the UAG portal.

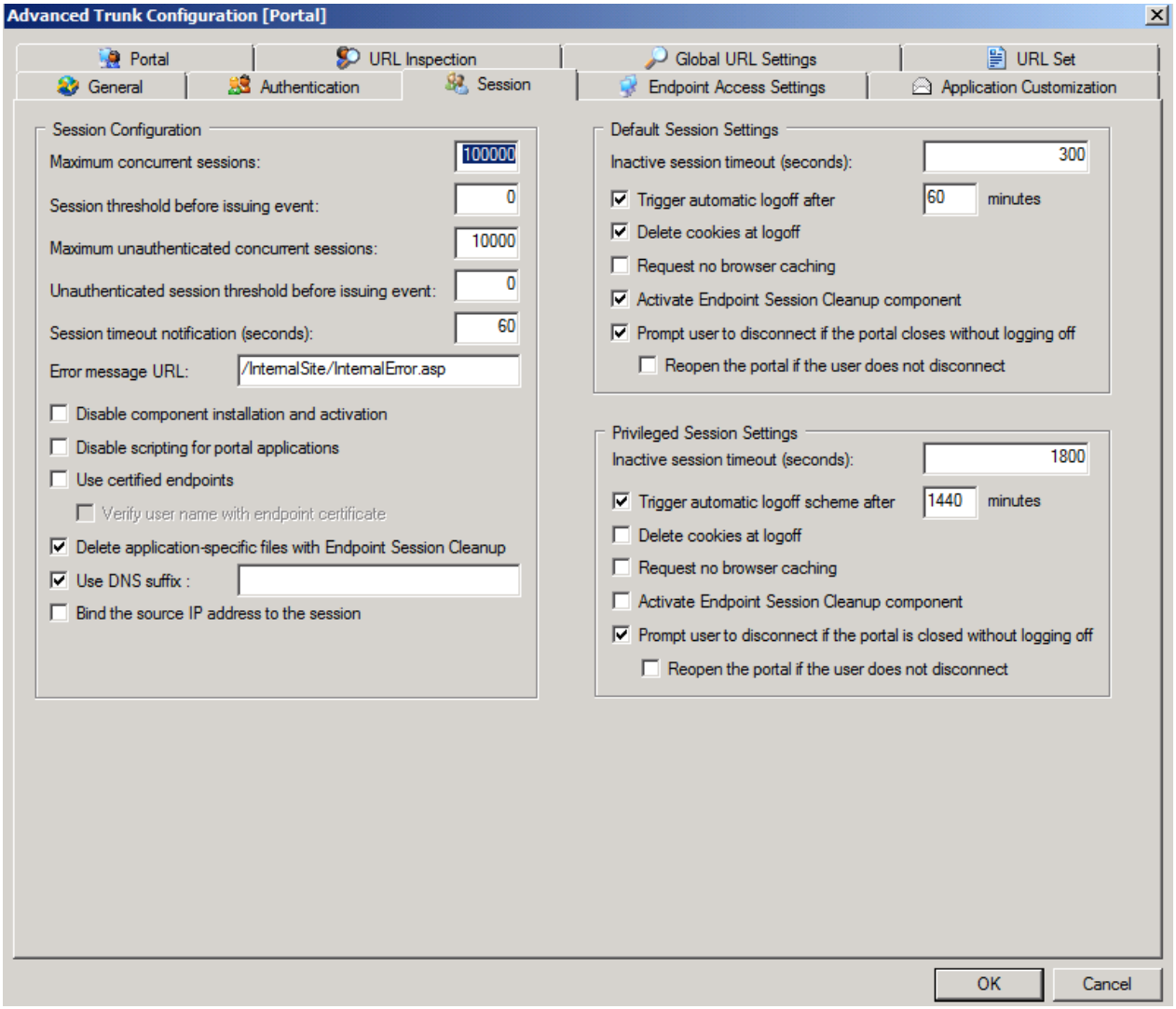

Figure 12: Portal session settings

The Endpoint Access Settings tab allows Administrator to decide to use NAP (Network Access Protection) or Forefront UAG Endpoint access policies to control which clients should be able to access the portal trunk.

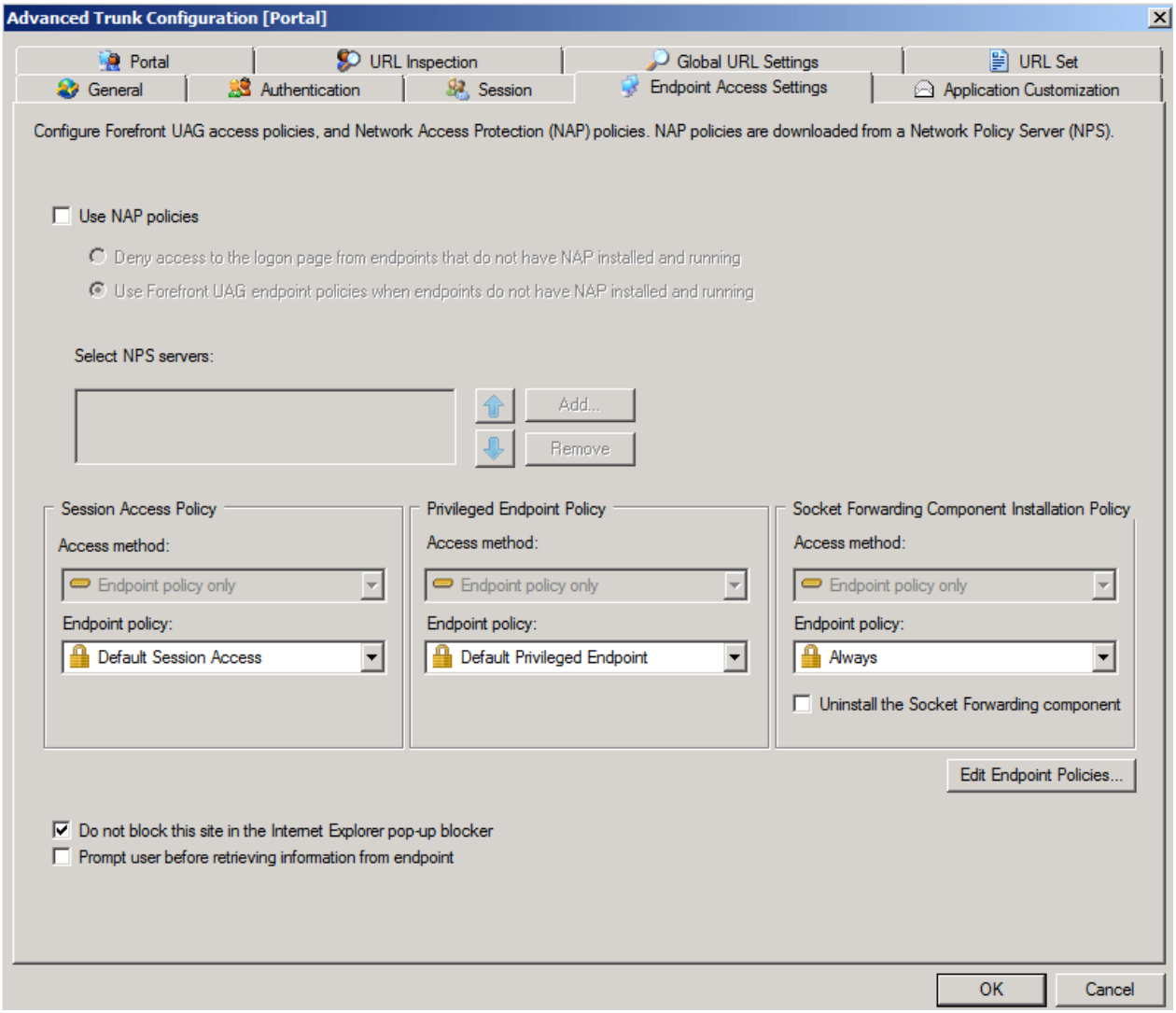

Figure 13: UAG Endpoint access settings

The Application Customization tab allows you to specify the file extensions for which Forefront UAG should be able to compress the content. It is also possible to enable GZip compression support

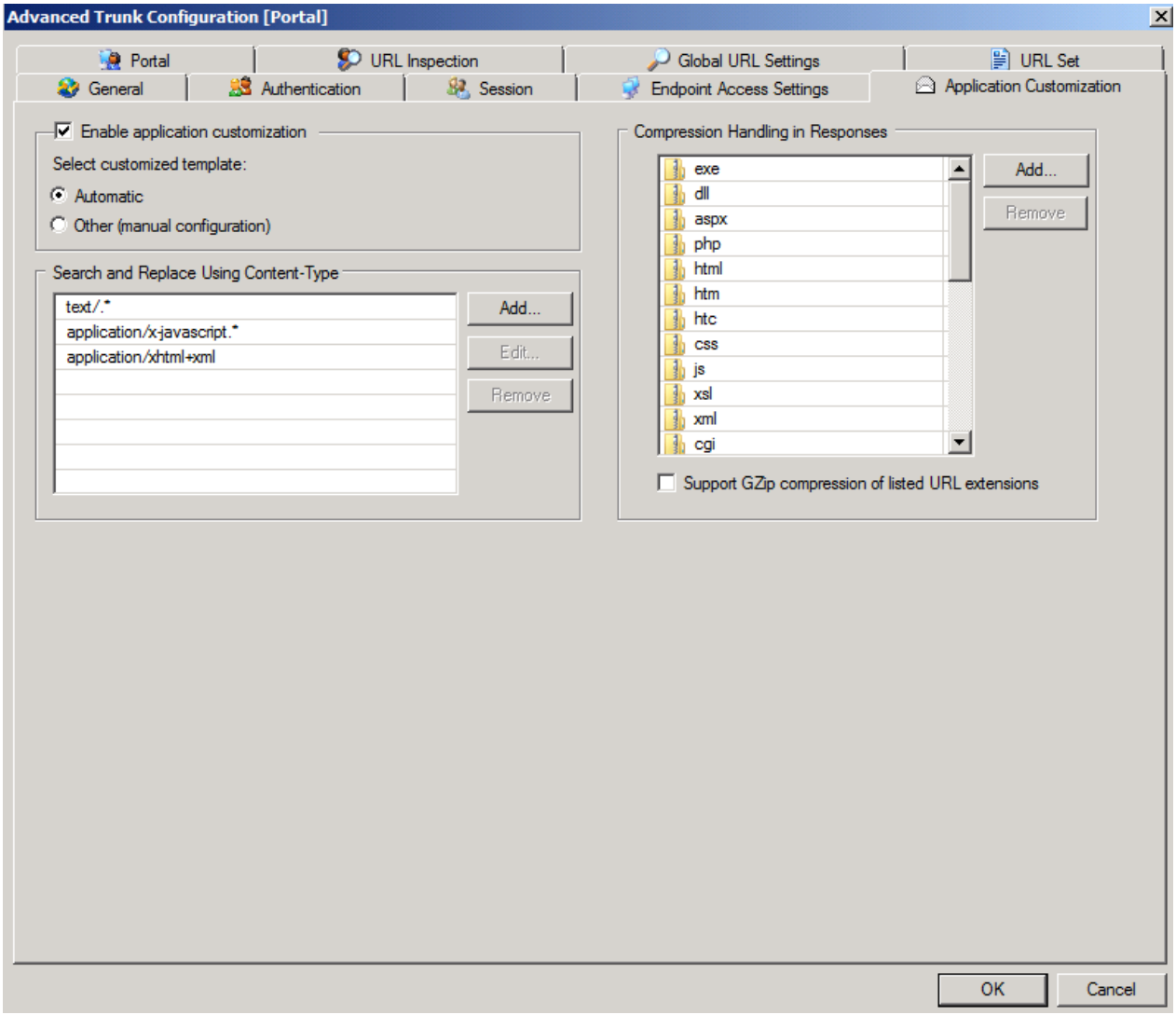

Figure 14: Application customization

The URL Inspection tab let Administrators specify the allowed HTTP access methods which should be allowed when users access the portal. Forefront UAG also uses deep HTTP inspection to filter the HTTP/HTTPS traffic for allowed and illegal characters as shown in the following screenshot.

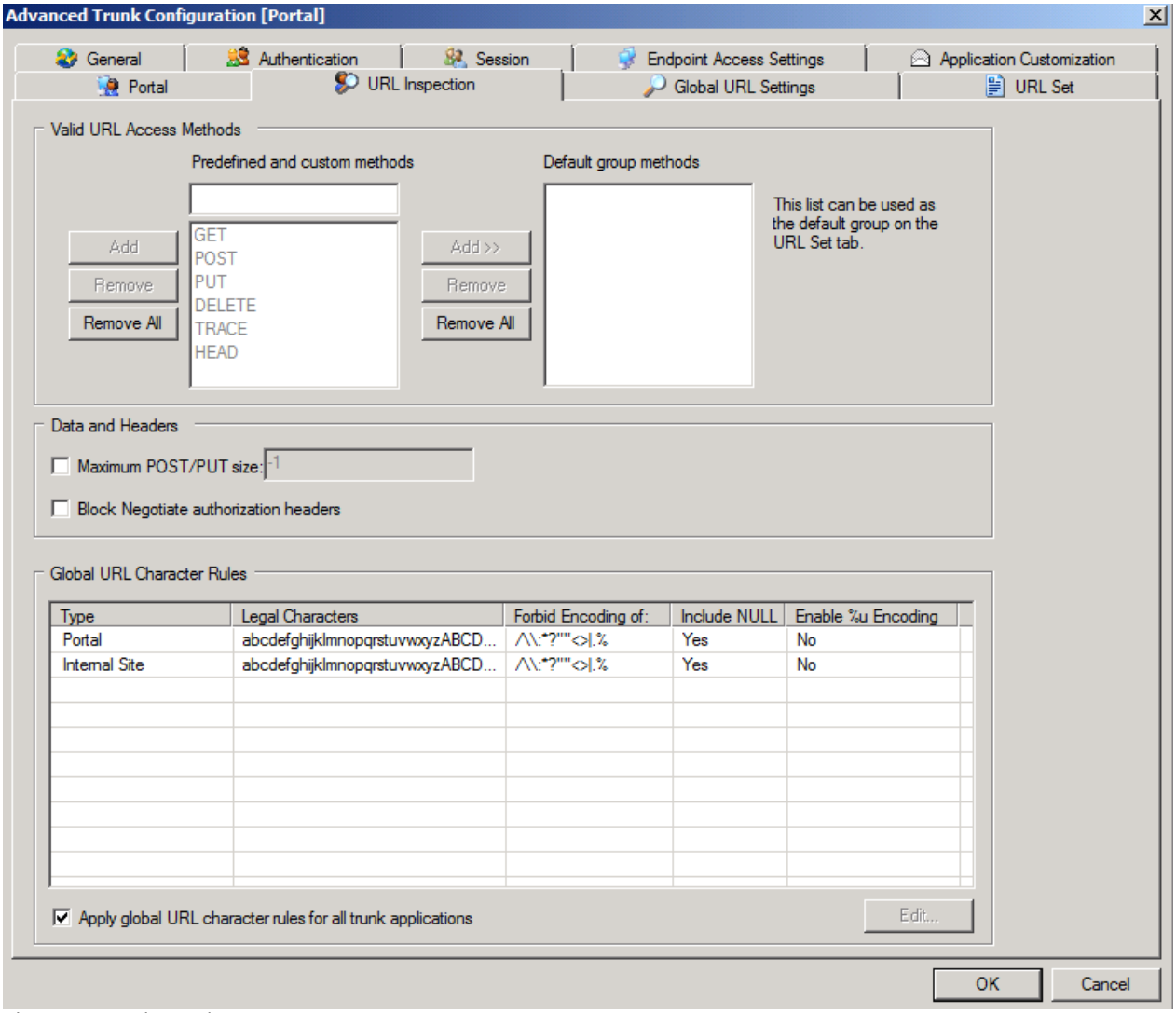

Figure 15: URL inspection

On the URL set tab Forefront UAG automatically creates global URL sets depending on the portal configuration and the applications published through the portal to control the allowed / illegal characters and the allowed / forbidden HTTP access methods. These created URL sets will be used by the underlying installed Forefront TMG Server as Firewall policy rules to controll access to the Forefront UAG Server.

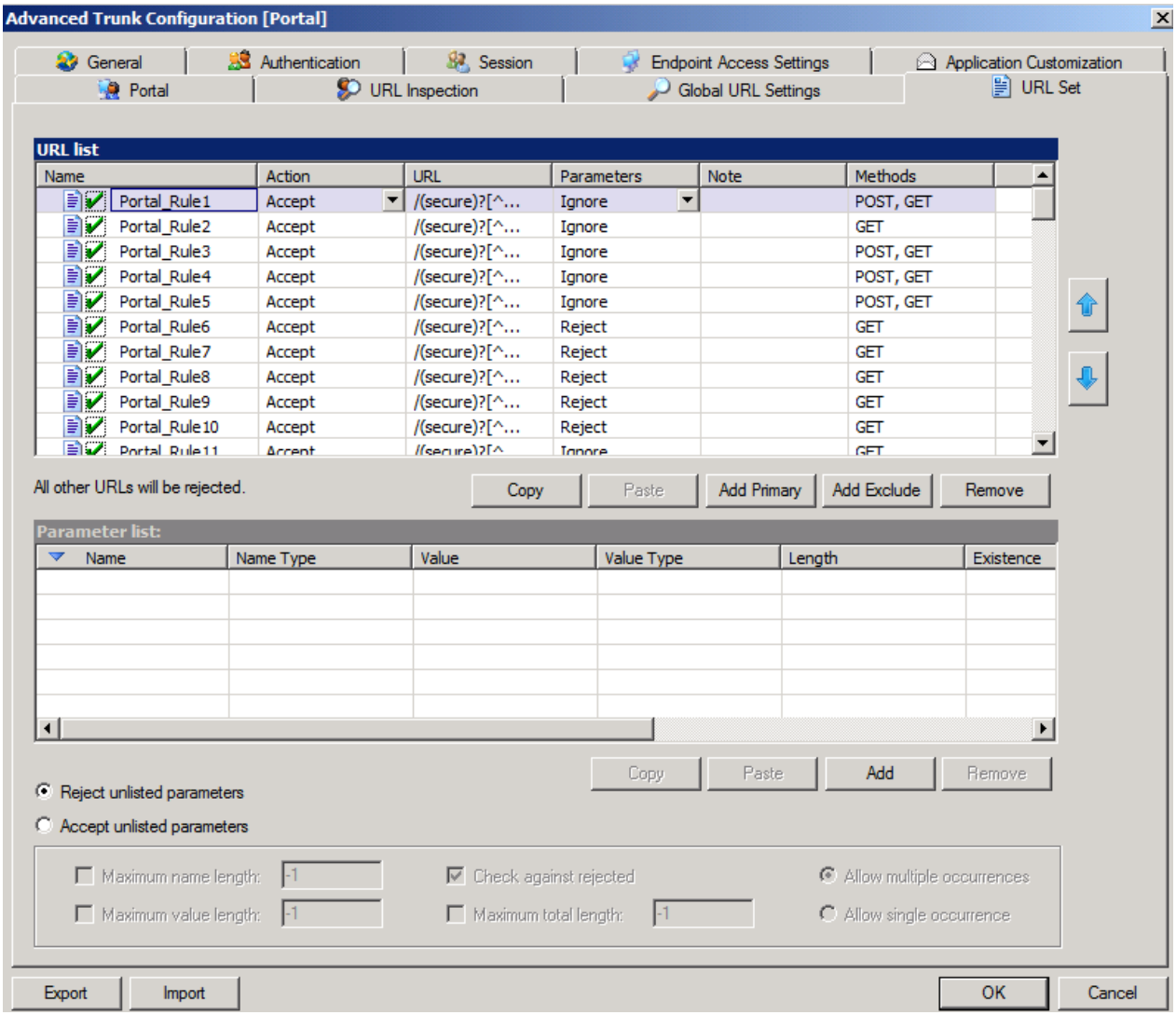

Figure 16: URL sets

This was a high level overview about the basic Forefront UAG portal trunk configuration. You should invest some time to get familiar with the powerful configuration options in Forefront UAG.

Conclusion

In this article I tried to explain the basic concepts behind Forefront UAG trunks to create a web portal for user which must access internal applications through the portal, created by Forefront UAG.

Related links

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