

Microsoft Forefront UAG – Publishing Microsoft Sharepoint Server 2010

Abstract

In this article I will show you how to publish Microsoft Office Sharepoint Server 2010 with Forefront UAG.

Let's begin

In a previous article published at www.isaserver.org I showed you how to create a portal trunk in Forefront UAG to publish internal applications like Microsoft Exchange, Microsoft CRM and many more. In this article we will use a newly created Forefront UAG portal trunk to publish an internal Microsoft Office Sharepoint Server 2010.

What are the differences publishing a Microsoft Sharepoint Server with Forefront TMG and Microsoft Forefront UAG

Forefront TMG also allows you to publish a Sharepoint Server but Forefront UAG has some capabilities for publishing a Sharepoint Server. In addition to the Forefront TMG capabilities Forefront UAG comes with the following major enhancements:

- Accessing a Sharepoint Server through a portal with different authentication providers
- Forefront UAG application optimizers to control access from the client to the Sharepoint Server through Forefront UAG
- Deeper HTTP and application aware filtering
- Forefront UAG Endpoint access policies
- More granular and deeper session monitoring

To publish a Microsoft Sharepoint Server start the Microsoft Forefront UAG Management Console go to the HTTPS portal trunk created earlier and click Add under in the Applications window to start a wizard which will help you to publish different applications in the Forefront UAG portal.

Select Web – Microsoft Office Sharepoint Portal Server 2010 to publish the internal Sharepoint Server 2010 or a farm of Sharepoint servers.

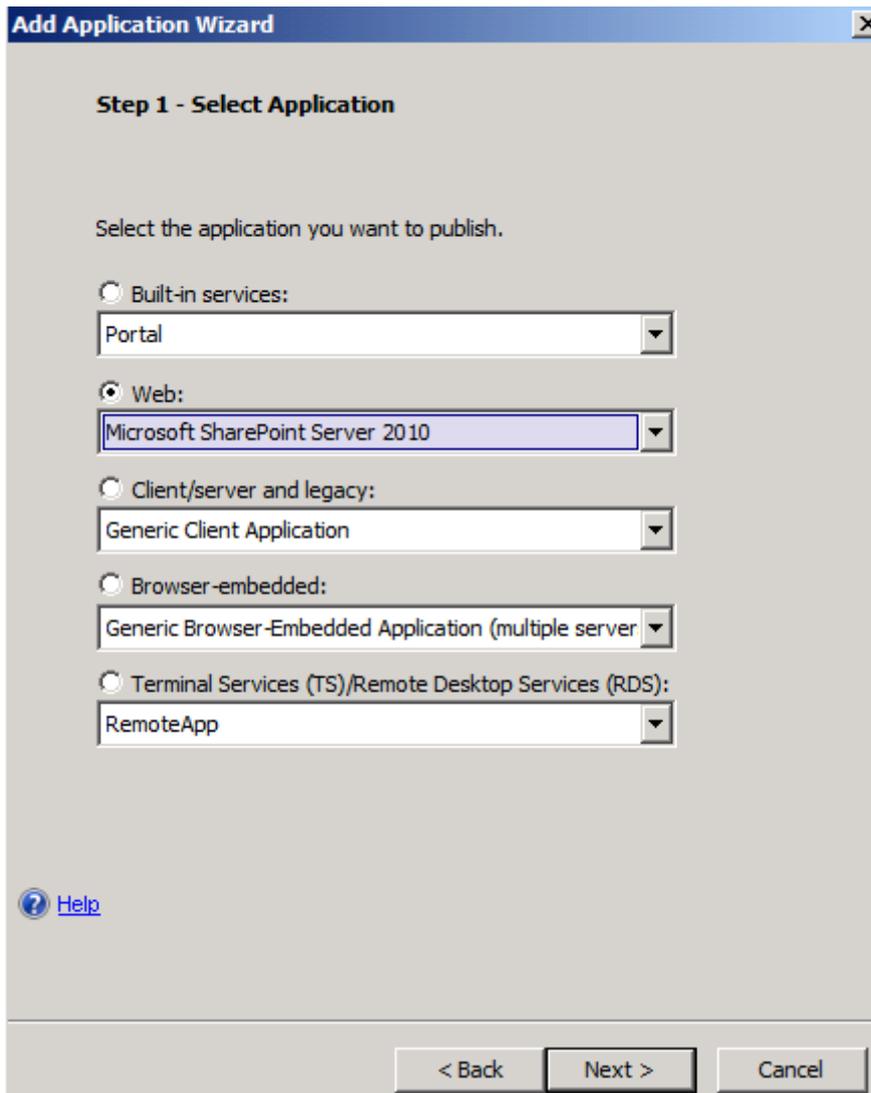


Figure 1: Sharepoint publishing wizard

Next, we must specify a name for the new application. In Step 3 it is possible to configure Endpoint policies for the application. Forefront UAG allows you to create Endpoint policies at the port trunk level and at the application level to control access to the portal and the application from external clients. If you are unfamiliar with UAG Endpoint policies leave the settings unchanged.

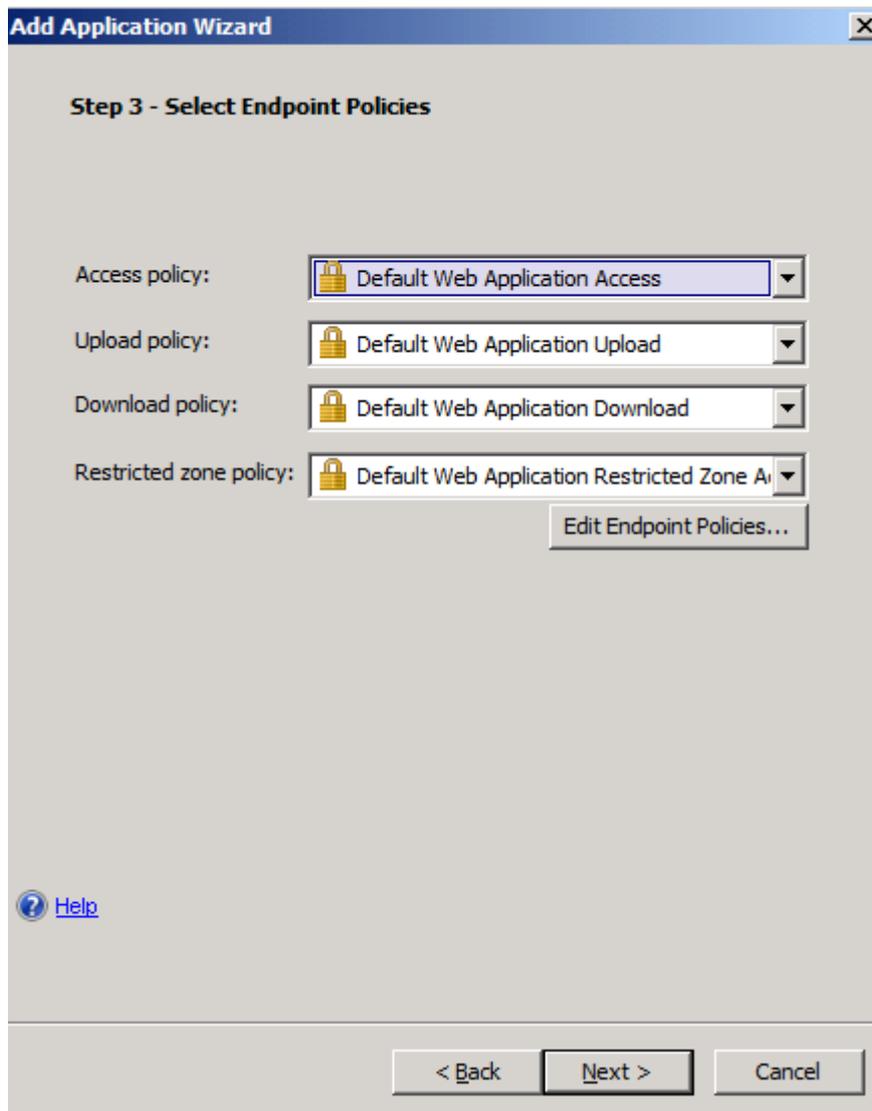


Figure 2: UAG endpoint policies

Next click configure an application server. In Step 5 enter the FQDN of the internal Microsoft Sharepoint Server 2010 and the port you would like to use when Forefront UAG should access the internal Sharepoint Server. If you want to restrict access to a specific path you are able to do this in the UAG configuration wizard.

Add Application Wizard [Close]

Step 5 - Web Servers

Address type: IP/Host Subnet Regular expression

Addresses:

Paths:

HTTP port: HTTPS port:

Public host name: .de

Replace the host header with the following

i To allow access to information protected by Information Rights Management, publish the Rights Management Services server via Forefront UAG.

? [Help](#)

< Back Next > Cancel

Figure 3: Specify internal Sharepoint server

In Step 6 we can use different authentication mechanisms. Because we want to enable SSO (Single Sign On) for users which access the Forefront UAG portal to use the internal Sharepoint Server.

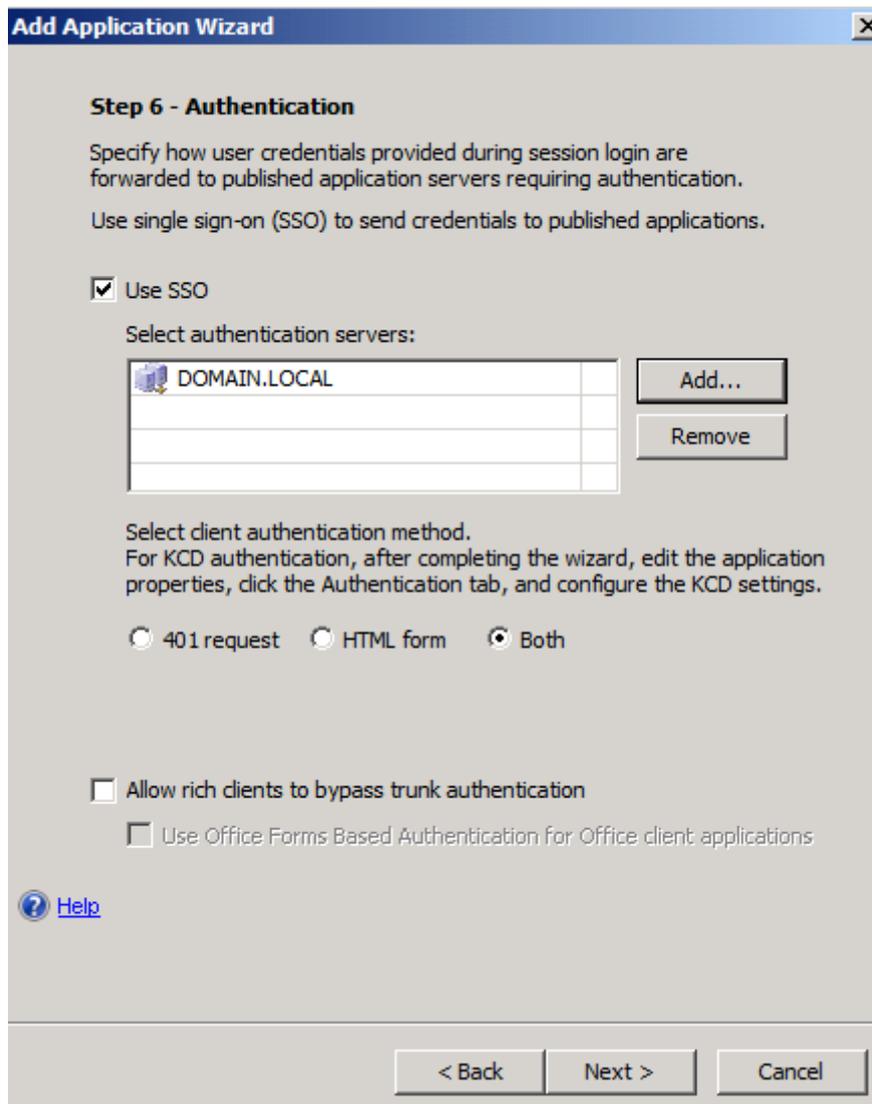


Figure 4: SSO for Sharepoint

We would like to add a portal and toolbar link, and if you want to open the Sharepoint Server application in a new window it is possible to enable this checkbox.

Add Application Wizard

Step 7 - Portal Link

Add a portal and toolbar link

Portal name:

Folder:

Application URL:

Icon URL:

Short description:

Description:

Open in a new window

[Help](#)

< Back Next > Cancel

Figure 5: Portal name

In Step 8 it is possible to configure the authorization settings to access the application in the portal. If you would like to grant all authenticated users access to the Sharepoint application leave the default setting unchanged. If you want to only grant specific users and user groups access to the Sharepoint application uncheck the checkbox and select the users and usergroups from the previous created repository to grant or deny them access to the Sharepoint application.

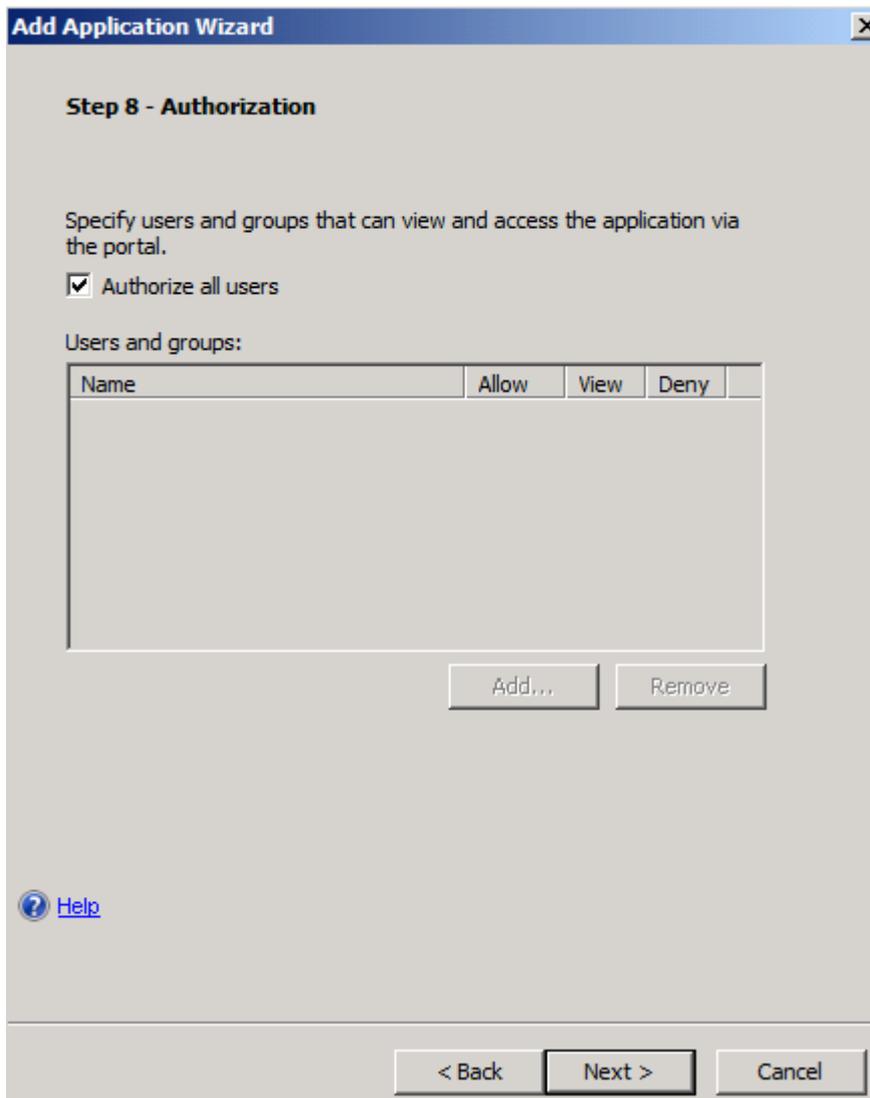


Figure 6: UAG authorization

Click Finish.

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.

After the application has been created in the portal we are now able to customize the settings of the Sharepoint application. I will only give you some high level steps for application customization.

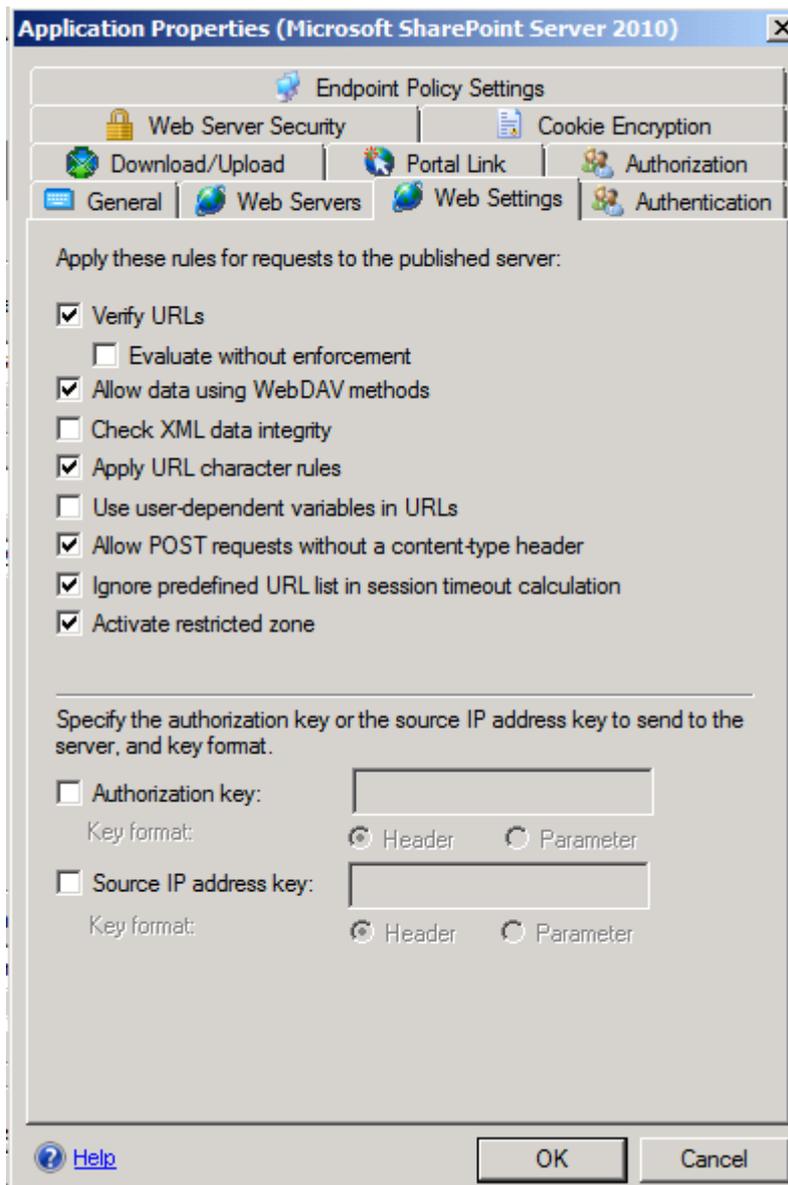


Figure 8: Web settings

The Download / upload tab allows you to control the download of content to the published Sharepoint Server.

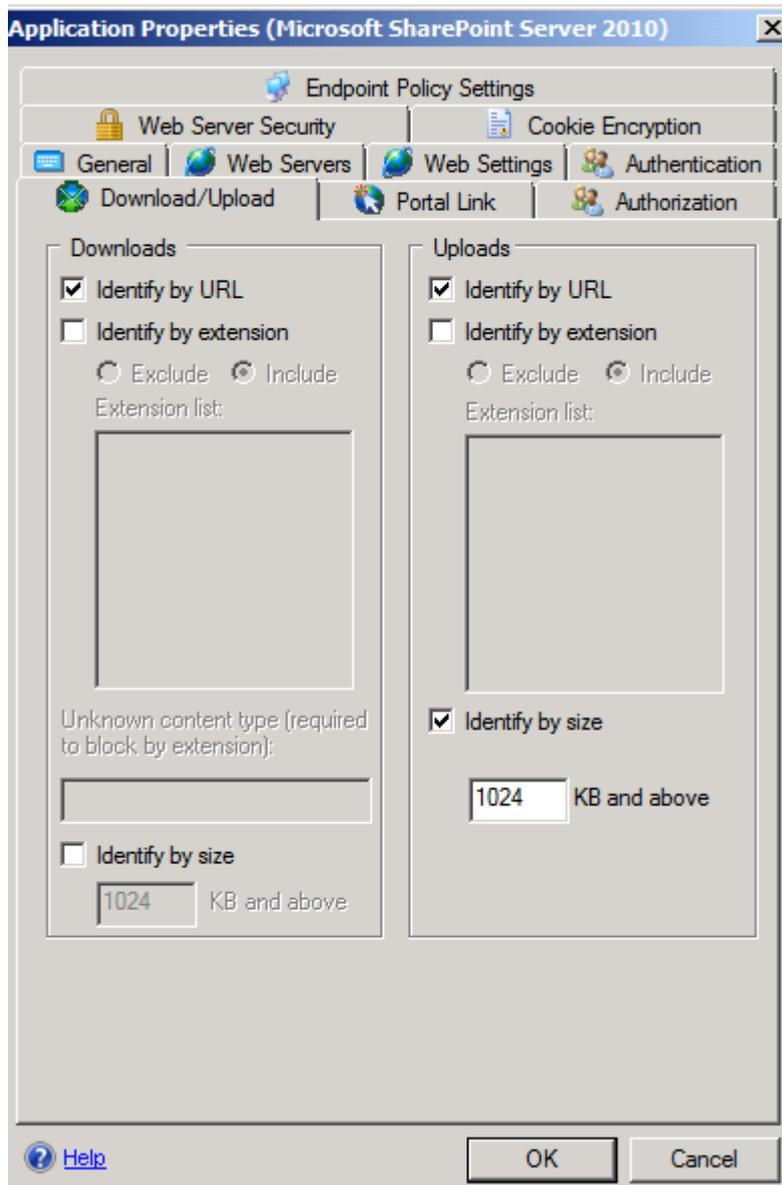


Figure 9: Download/upload settings

The Web Server Security tab allows you to activate the smuggling protection feature and the maximum size of the POST request. HRS can be used to block requests if the following conditions apply:

- The method is POST
- The content-type is not listed in the content-type list
- The length is greater than the specified maximum length

This option should be enabled only for servers that are vulnerable to HRS attacks. If this option is enabled when it is not required, applications may not behave as expected.

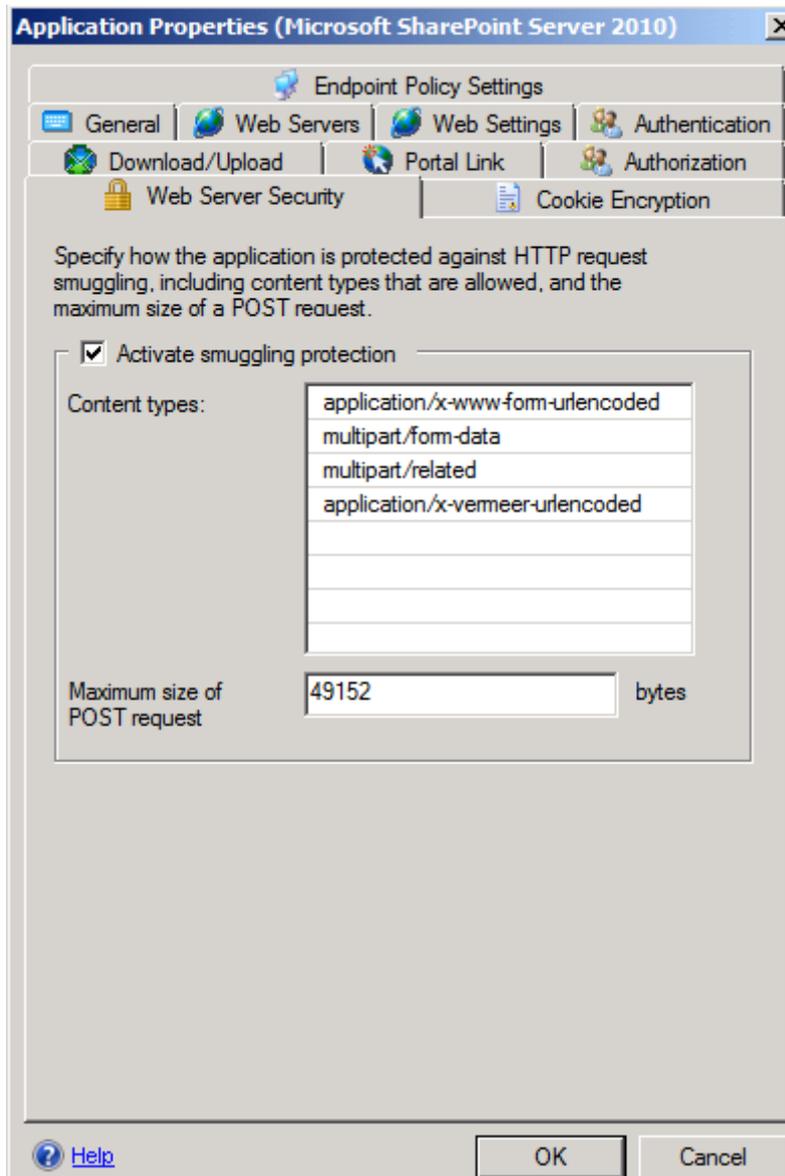


Figure 10: Web server security

The Cookie Encryption tab allows you to enable Cookie encryption to hide cookie names and values.

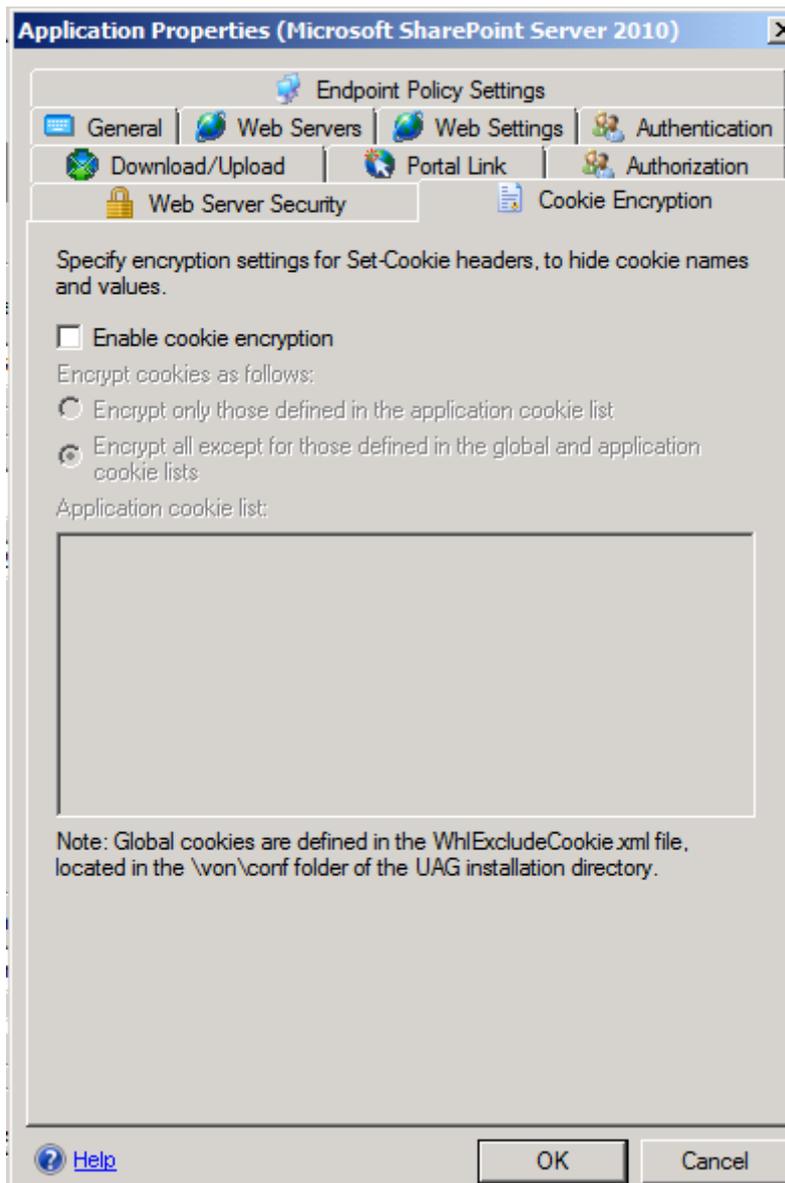


Figure 11: Cookie encryption

At client side

After all settings has been configured you can now test the connection from an external client. Open the portal website. If you visit the website the first time a set of ActiveX controls or Java applets depending on the browser version you use will be installed. These components are called the endpoint detection components which interacts with the Forefront UAG Server for applying Endpoint policies and for local interacting between the Forefront UAG Server and the client.

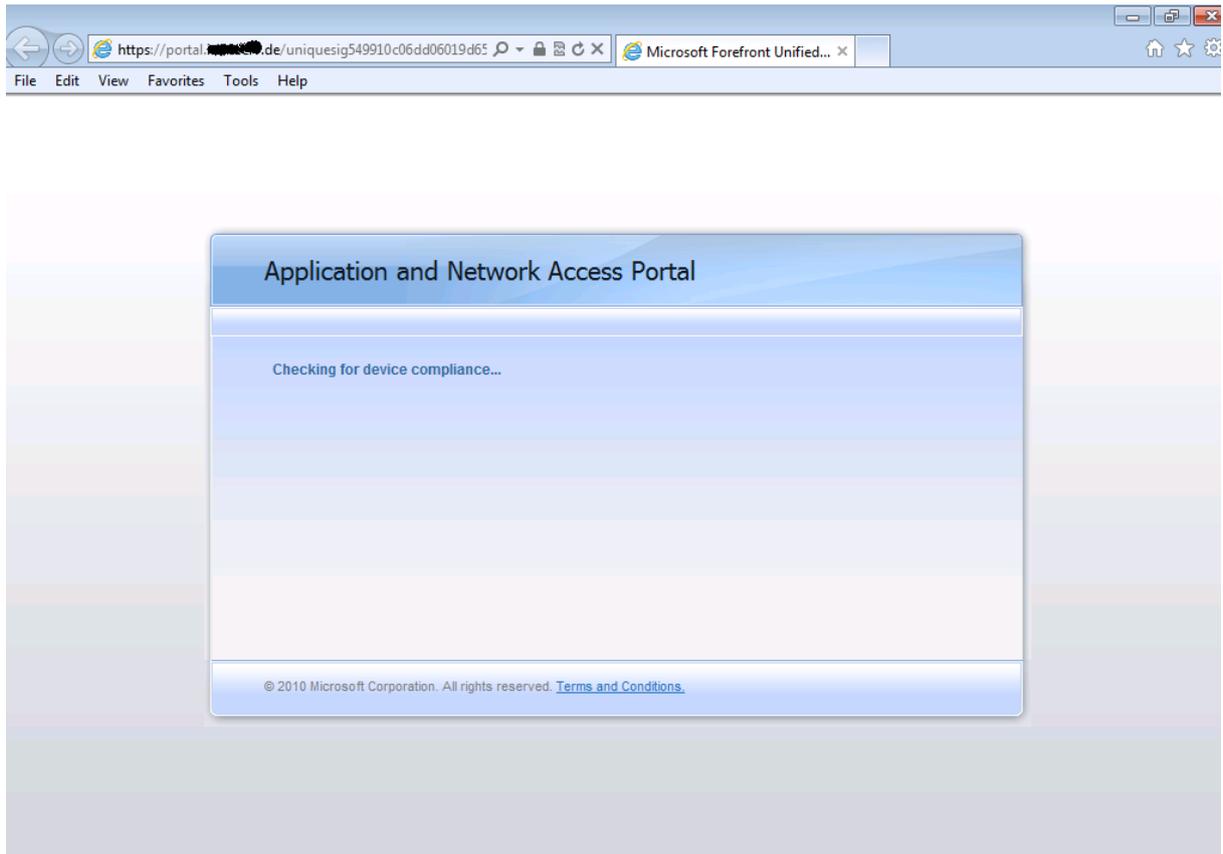


Figure 12: Portal endpoint detection

The user must enter the user name and the password.

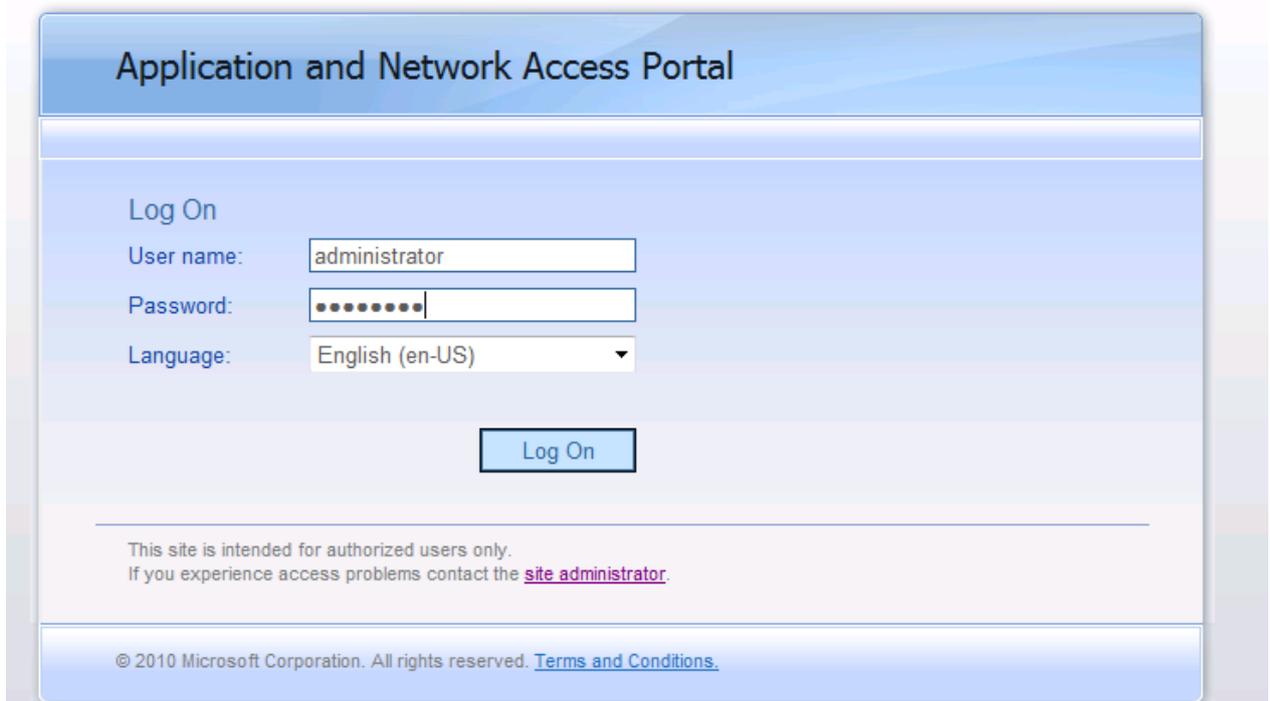


Figure 13: Logon to the portal

After the user has been authenticated he will get access to the Forefront UAG portal and can now use the published Sharepoint application.

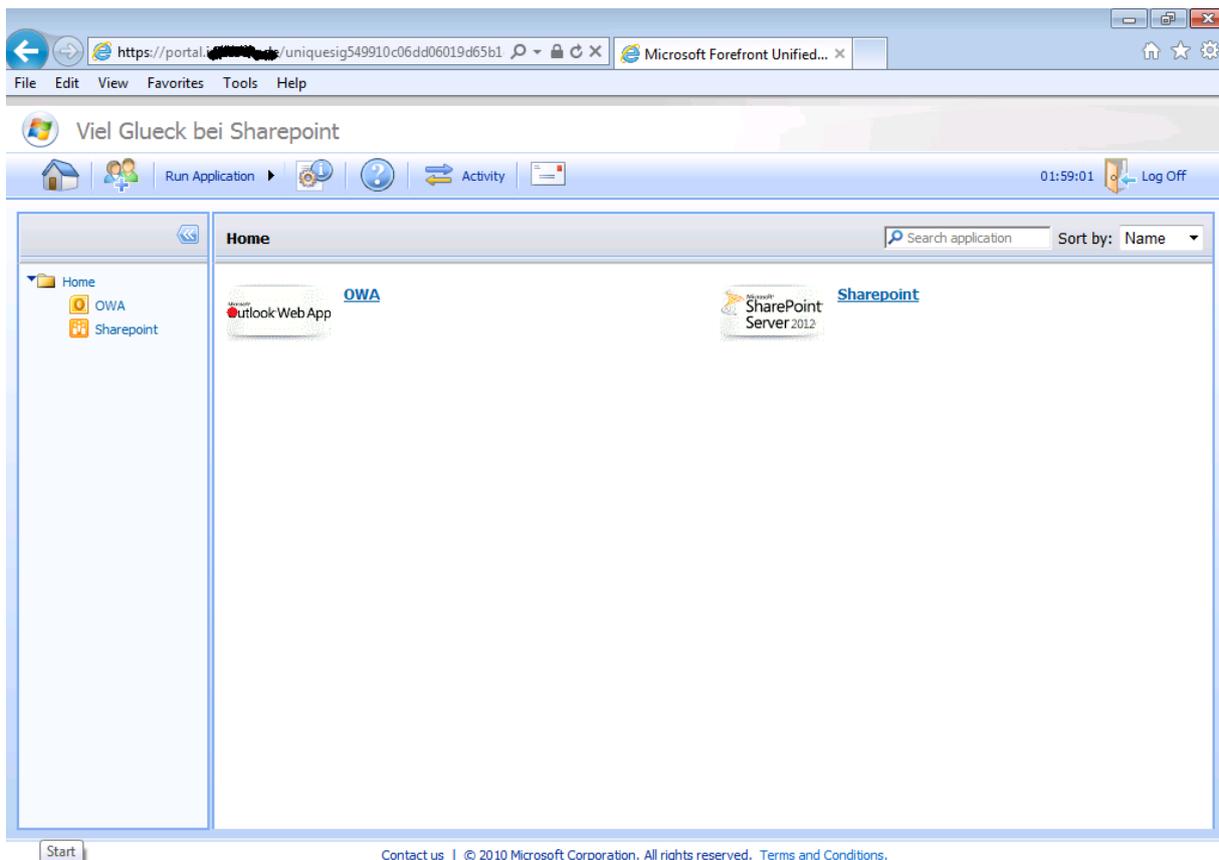


Figure 14: UAG portal accessing Sharepoint

Depending on the Forefront UAG configuration, the Sharepoint website will be opened in the same portal window or in another window.

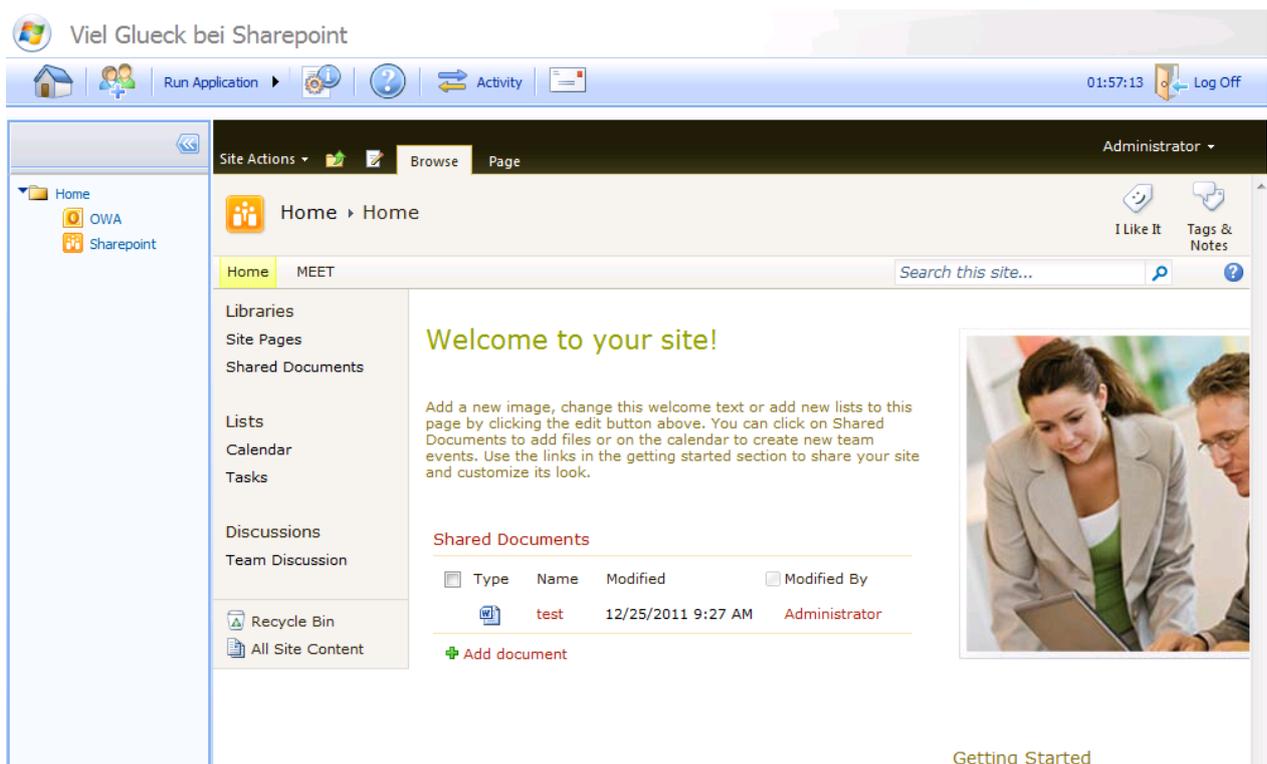


Figure 15: Sharepoint access through Forefront UAG

Conclusion

In this article we published a Microsoft Office Sharepoint Server 2010 with Microsoft Forefront UAG. As you have seen, publishing a Microsoft Office Sharepoint Server with Forefront UAG provides much more capabilities and customization as to publish a Microsoft Office Sharepoint Server with Microsoft Forefront TMG.

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>

Sharepoint publishing solution guide

<http://technet.microsoft.com/en-us/library/dd857299.aspx>