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

Forefront UAG authentication options

Abstract

In this article I will show you the different authentication options in Forefront UAG and specially the authentication configuration against Microsoft Active Directory for the Forefront UAG portal trunk and portal applications.

Let's begin

Forefront UAG provides various ways to authenticate users against different authentication providers. Forefront UAG provides support for:

- Active Directory
- AD FS 2.0
- Netscape LDAP Server
- Notes Directory
- Novell Directory
- NT Domain
- RADIUS
- RSA SecurID
- TACACS
- WINHTTP

Please note: The RADIUS authentication provider can be used to authenticate against third party software vendors and RADIUS is often used to provide two factor authentication and OTP (One Time Password) authentication.

To configure the authentication providers, start the Forefront UAG Management console and navigate to *Admin – Authentication and Authorization Servers*

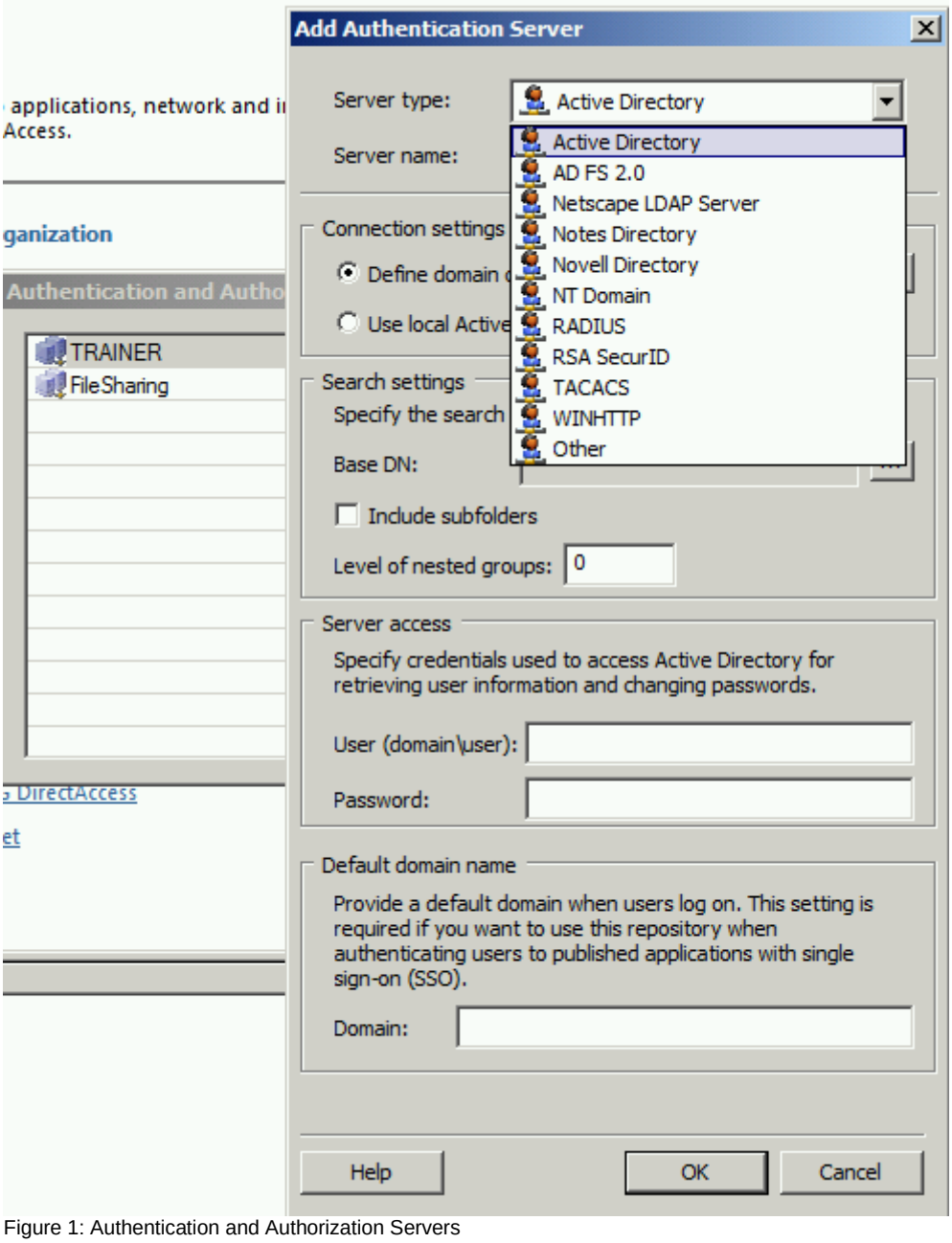

Figure 1: Authentication and Authorization Servers

The next screenshot shows a configured authentication Server with Active Directory. It is possible to specify the Domain Controllers and ports used for authentication. You must also specify a user account which will be used to read Active Directory information. Best practice is to use a dedicated service account with a complex non expiring password. You must also specify the search root and scope and provide a Base DN. In large Active Directory environments it might be helpful to specify the base DN where all user accounts are located, but this heavily depends on the structure of the Active Directory configuration. For Single Sign on (SSO), you can also specify the Active Directory domain.

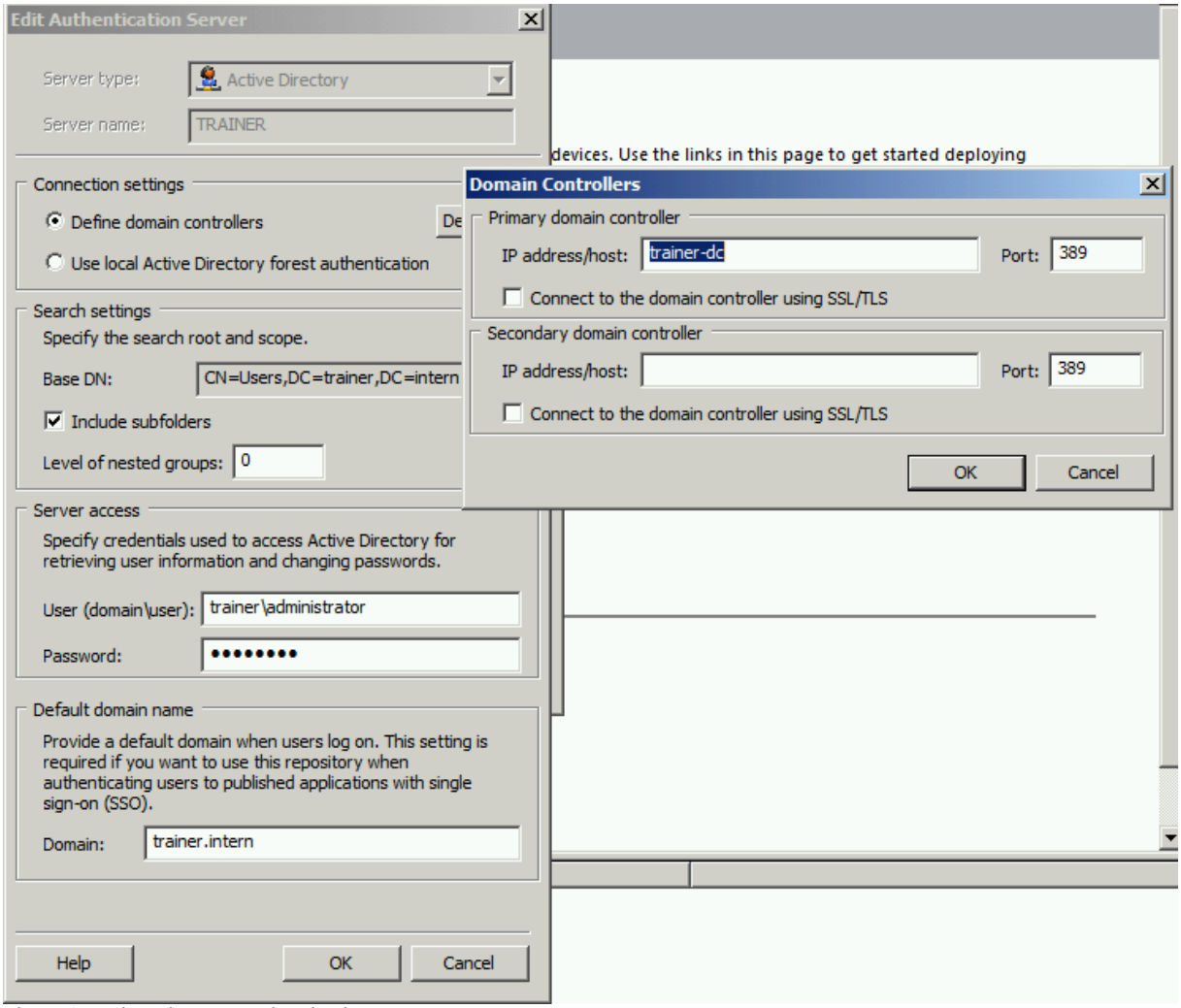

Figure 2: Active Directory authentication

Kerberos Constrained Delegation (KCD)

Some applications requires KCD, where the Forefront UAG Server authenticates in the name of the user. It is possible to configure KCD in the portal applications as seen in the following screenshot.

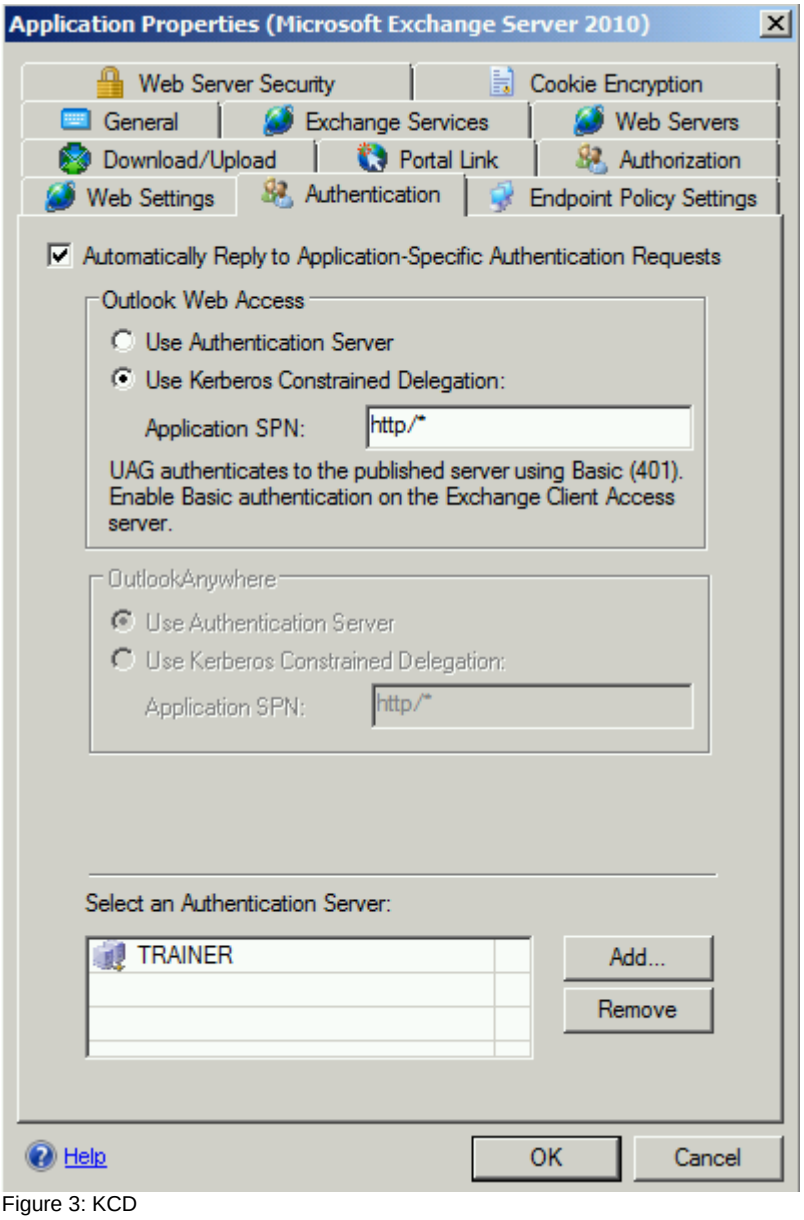

Figure 3: KCD

Because it is necessary to configure Active Directory for KCD, Forefront UAG provides the functionality to export the configured KCD settings. To export the KCD settings click *Admin – Export KCD Settings to Active Directory* in the Forefront UAG Management console.

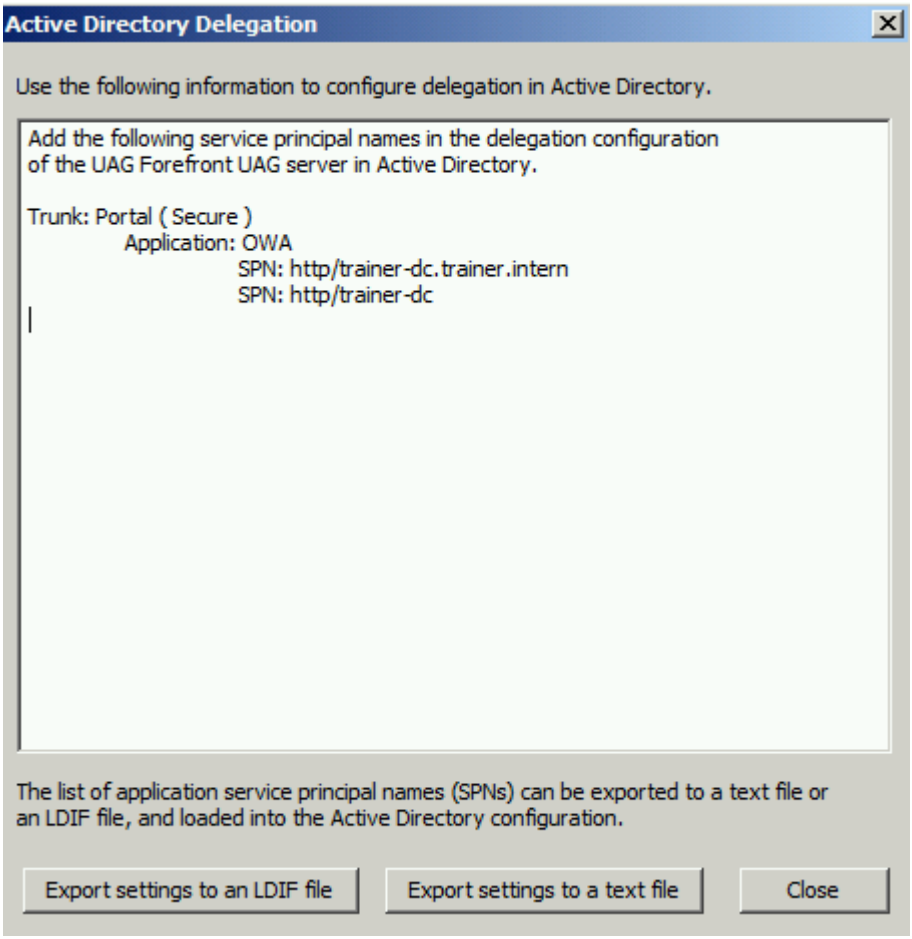

Figure 4: Export KCD

If you export the settings to an LDIF file, you can use LDIFDE on a Active Directory Domain Controller to automatically configure the KCD settings.

KCD use UPN

In some special constellations it is necessary to configure KCD to use the UPN (User Principal Name). To configure KCD to use UPN you must change the Registry on the Forefront UAG Server as described in the next screenshot.

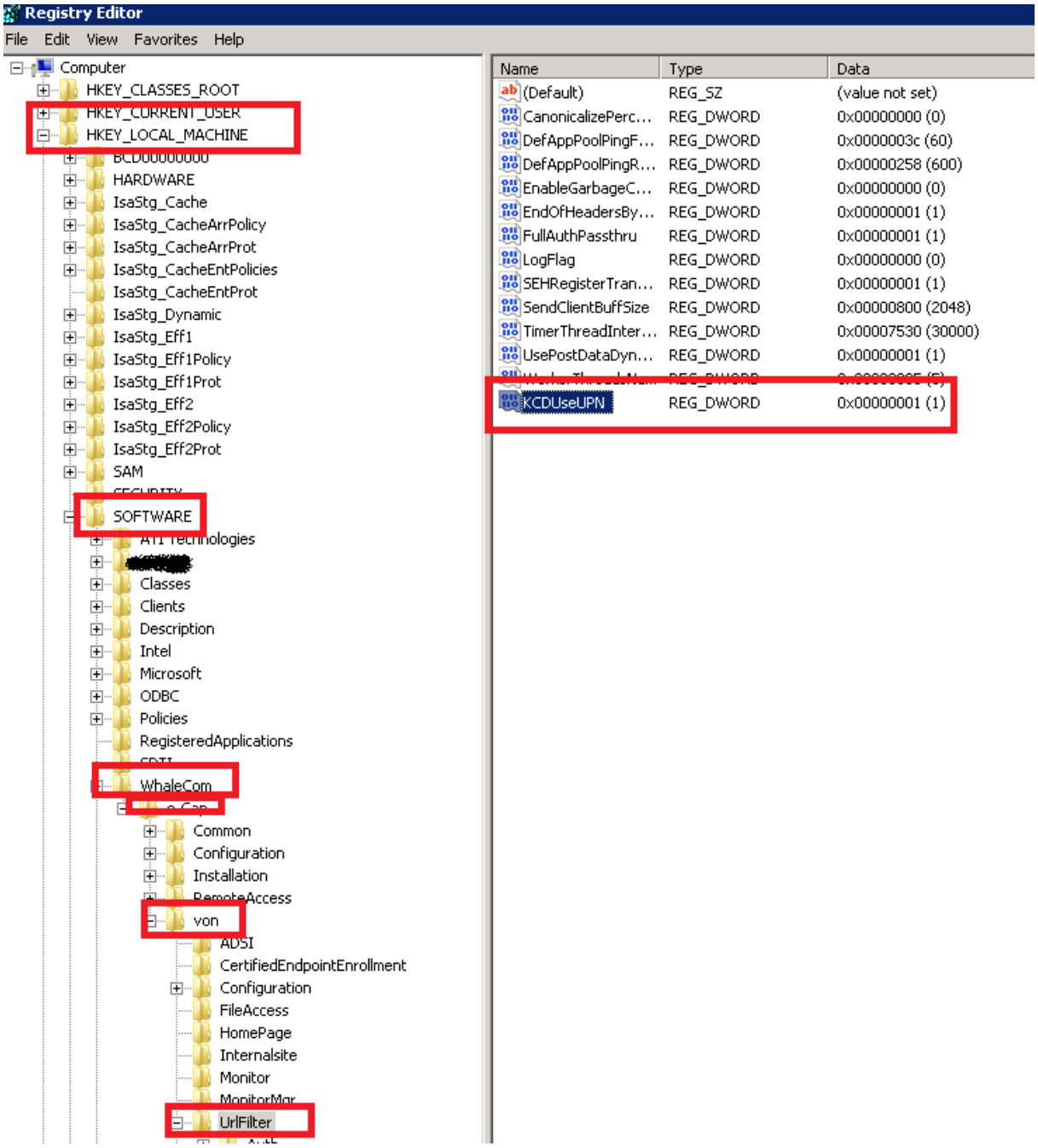

Figure 5: KCDuseUPN

The Registry key TranslateUPN must be set to 1 to enable client authentication using a user principal name (UPN) in a Forefront UAG portal.

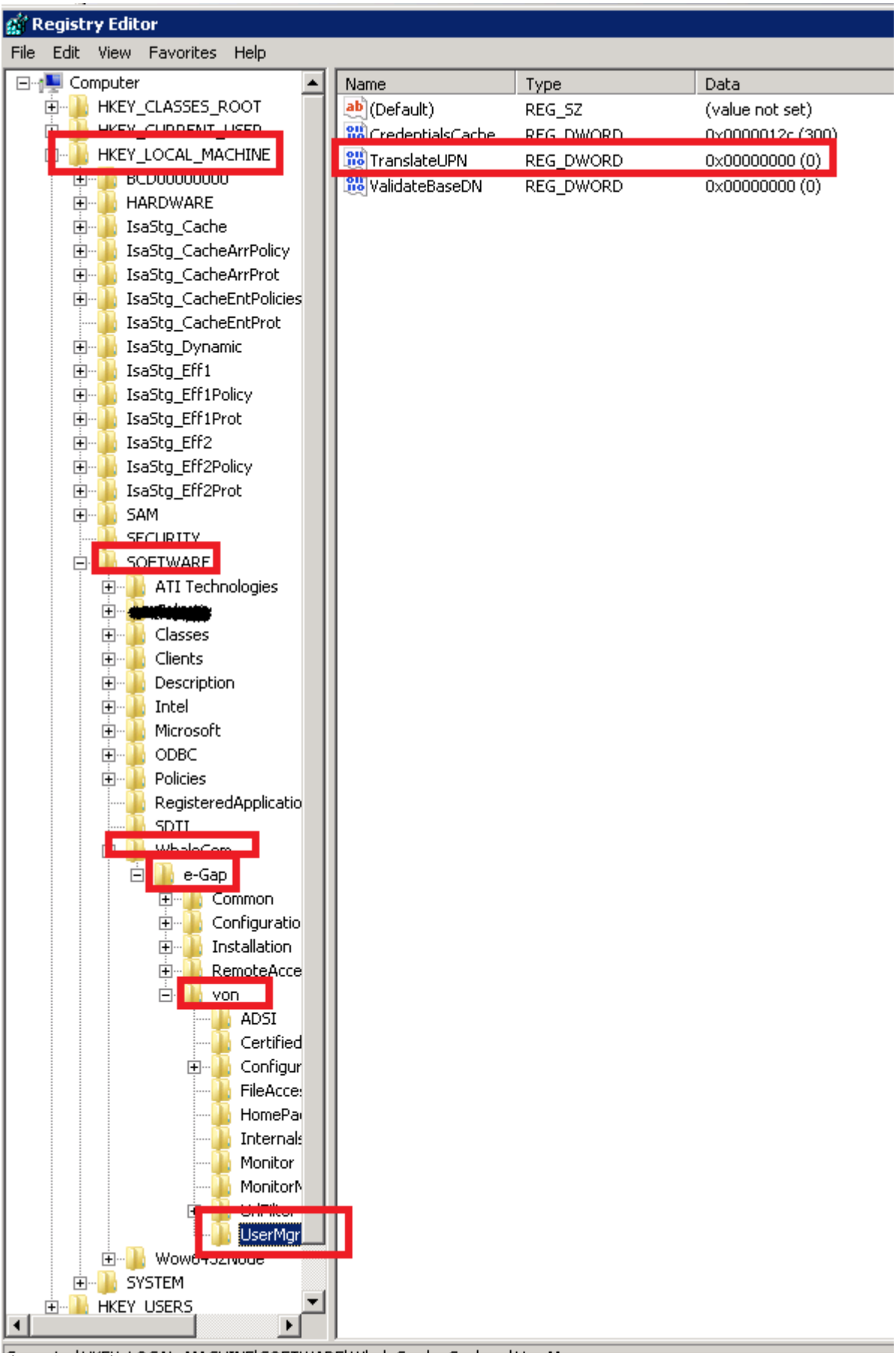

Figure 6: Translate UPN

If you want to allow users to use their UPN for Forefront UAG portal logon, you must reconfigure the Forefront UAG authentication repository.
Copy the file *repository_for_upn.inc* from the directory *...\Microsoft Forefront Unified Access Gateway\von\InternalSite\samples* to the *...\Microsoft Forefront Unified Access Gateway\von\InternalSite\inc\CustomUpdate* directory and rename the file exactly to the name as the authentication Repository.

Authorization in the Forefront UAG portal applications

The default setting in a Forefront UAG portal application is to authorize all users. This option allows all authenticated users to access the portal application. If you want to have more control about users and groups which should have access to portal applications uncheck the checkbox and specify users and groups from the authentication repository as seen in the following screenshot.

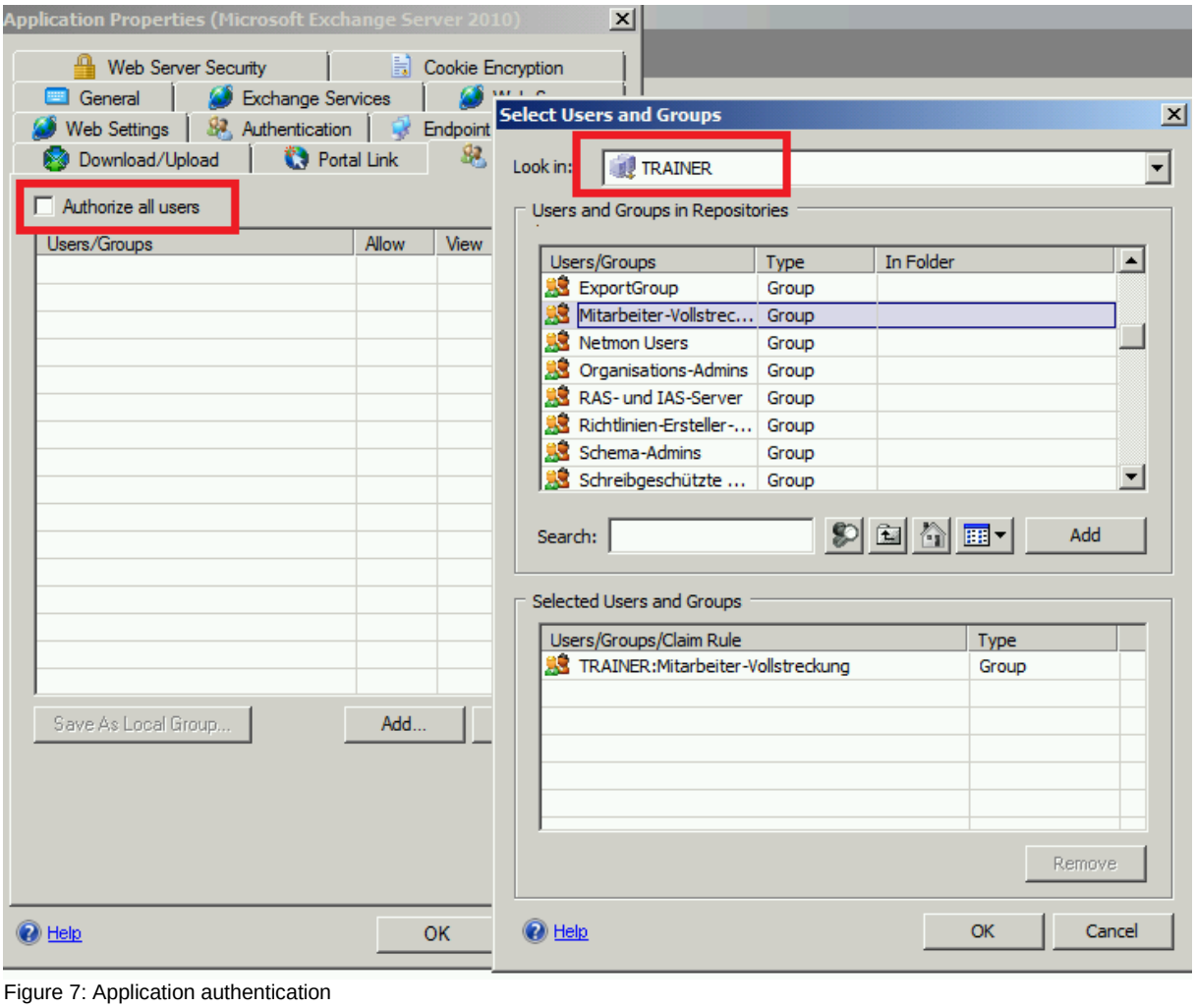

Figure 7: Application authentication

After you select a user or user group you have the option to allow / deny access to the application and it is also possible to hide applications in the portal for users which don't have access to a portal application.

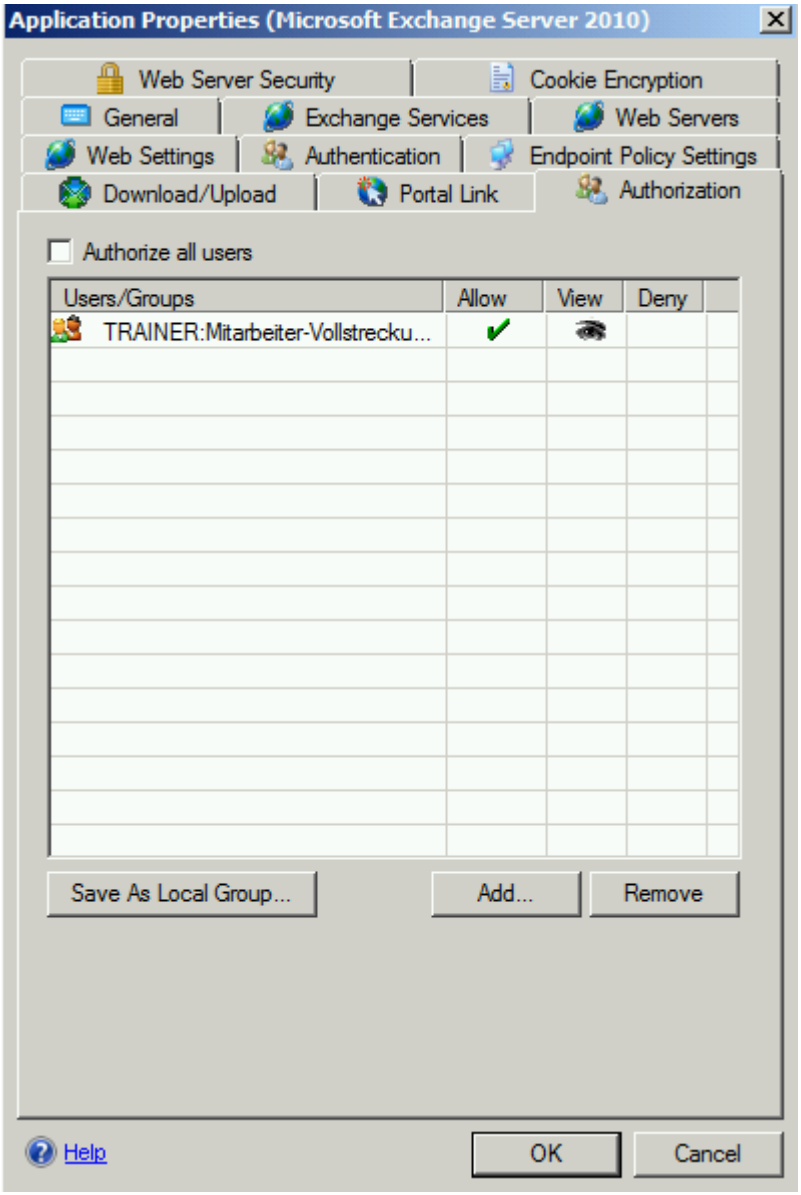

Figure 8: Access options

You can also use Forefront UAG to provide authentication against a local authentication repository. It is possible to store Active Directory groups as local groups in the local Forefront UAG authentication repository. Select the Active Directory group and click the button *Save as Local Group* and specify a name for the new local group.

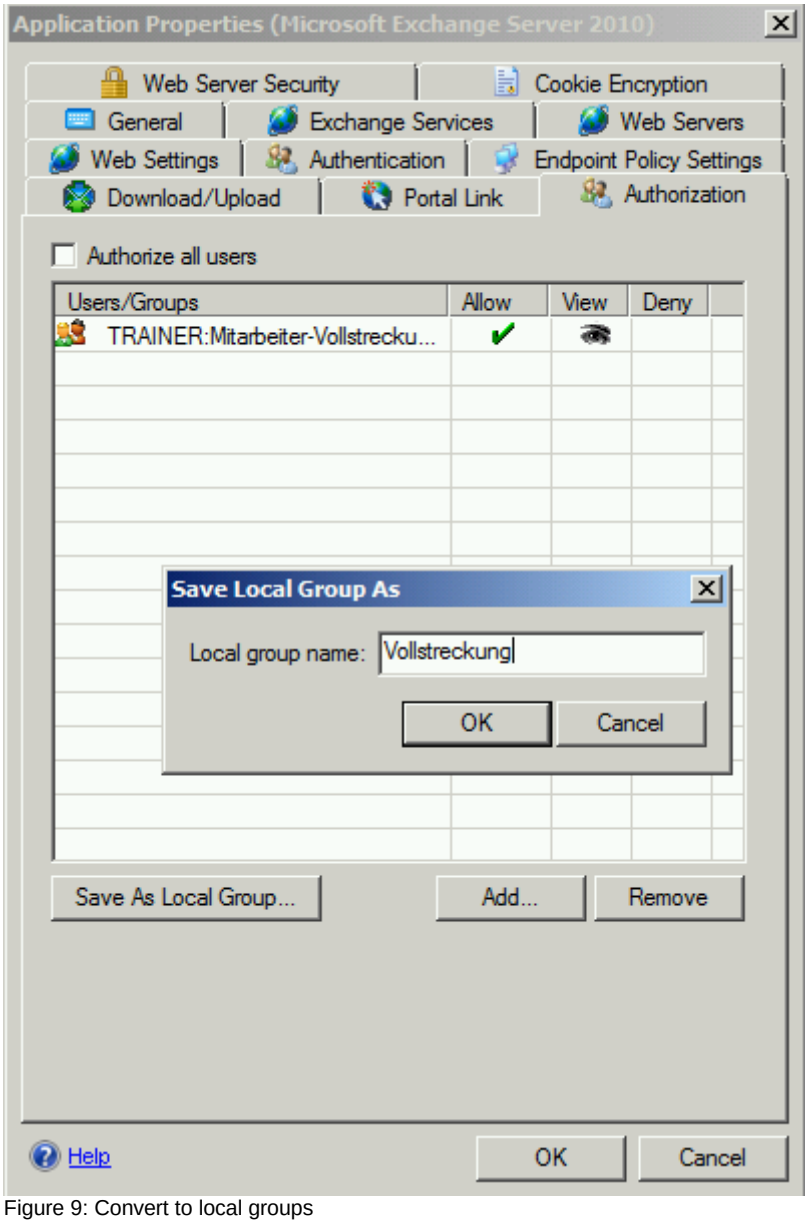

Figure 9: Convert to local groups

You are now able to provide authentication in portal applications against the local authentication repository. To configure the local authentication repository click *Admin – Portal Application Authorization* in the Forefront UAG Management console.

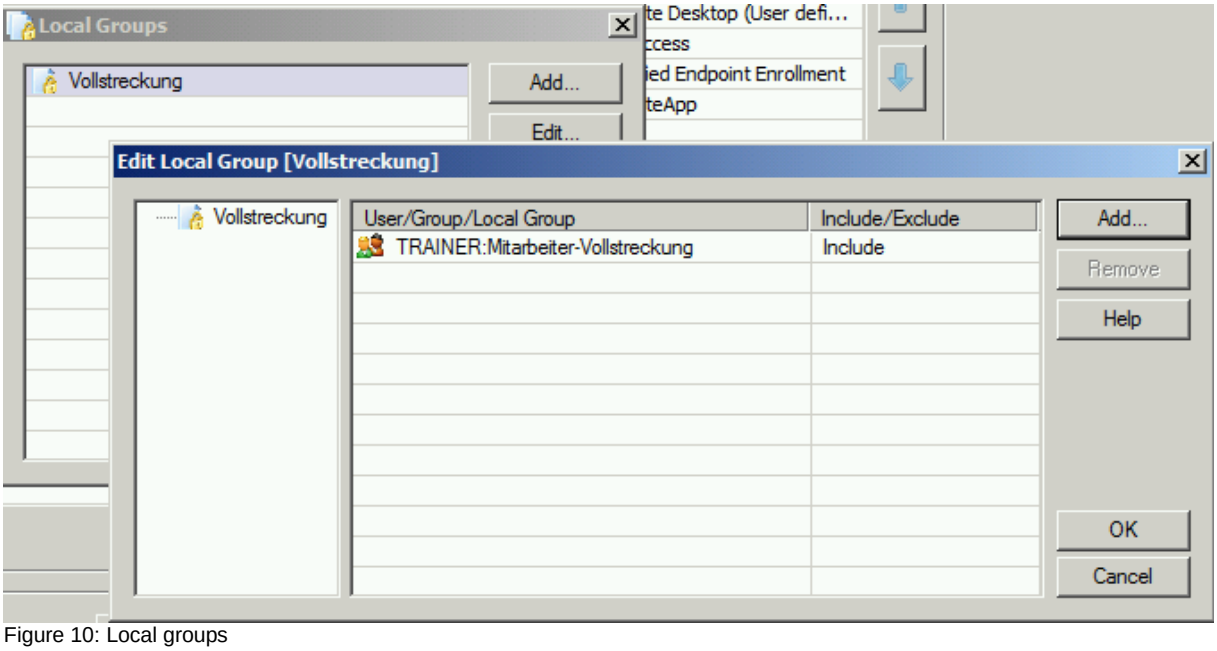

Figure 10: Local groups

Configure Trunk settings

In the Authentication tab of the Forefront UAG portal trunk you can select authentication Servers and additional configuration settings like the capability to allow users to change their password or to provide a list of authentication Servers at logon.

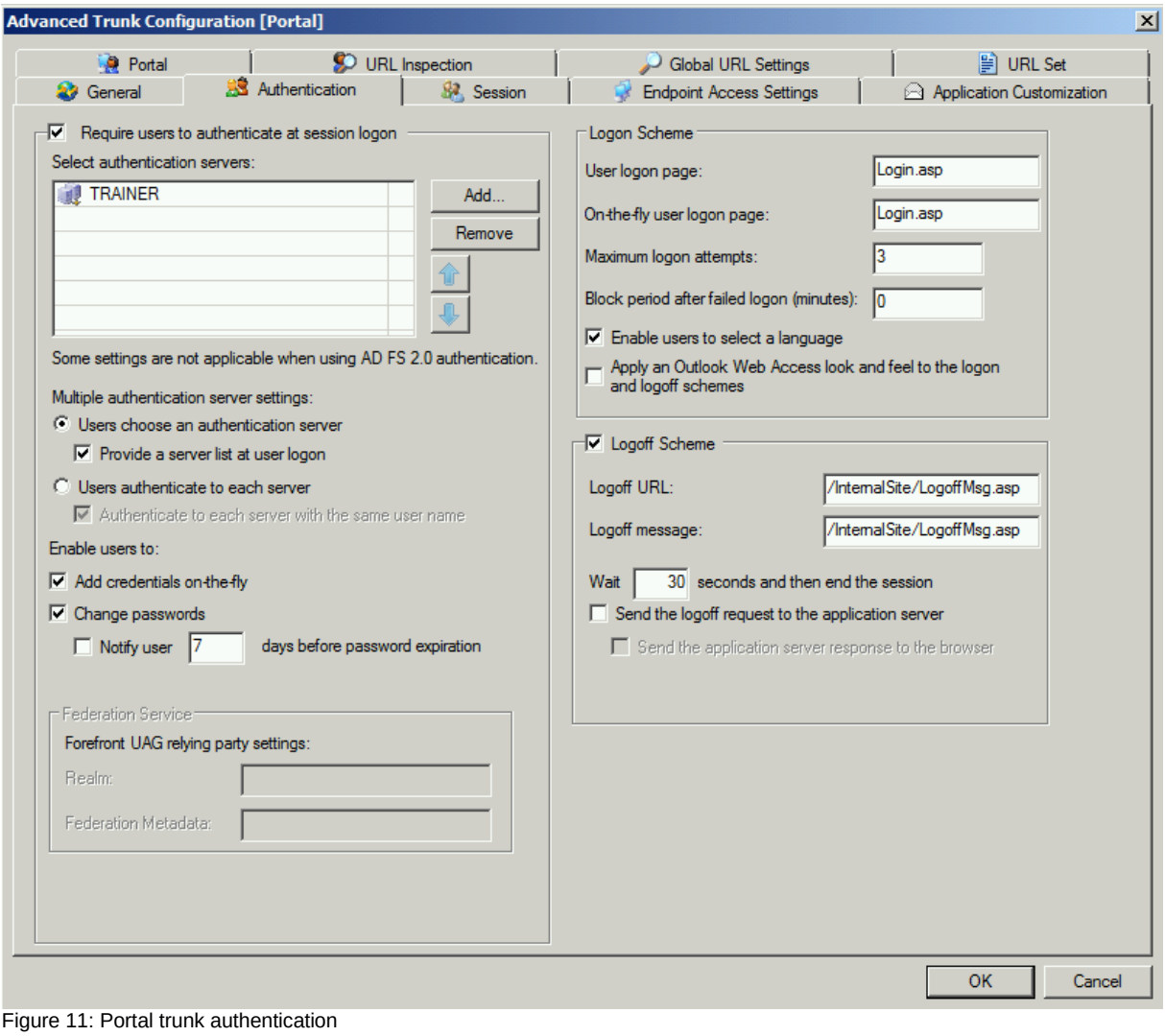

Figure 11: Portal trunk authentication

Client logon to the portal

After the Forefront UAG Server portal and portal applications has been configured for authentication, a user is now able to logon to the Forefront UAG portal.
The following screenshots shows the Log On dialog box for users which tries to access the Forefront UAG portal. Because there is only one authentication Server configured in the portal trunk, the users has no option to specify an authentication Server.

Figure 12: Portal logon

You can use the Forefront UAG Web Monitor to monitor all logged on users or failed logon attempts from users to the Forefront UAG portal. Start the Forefront UAG Web Monitor and click *Active Sessions* in the Session Monitor as shown in the following figure.

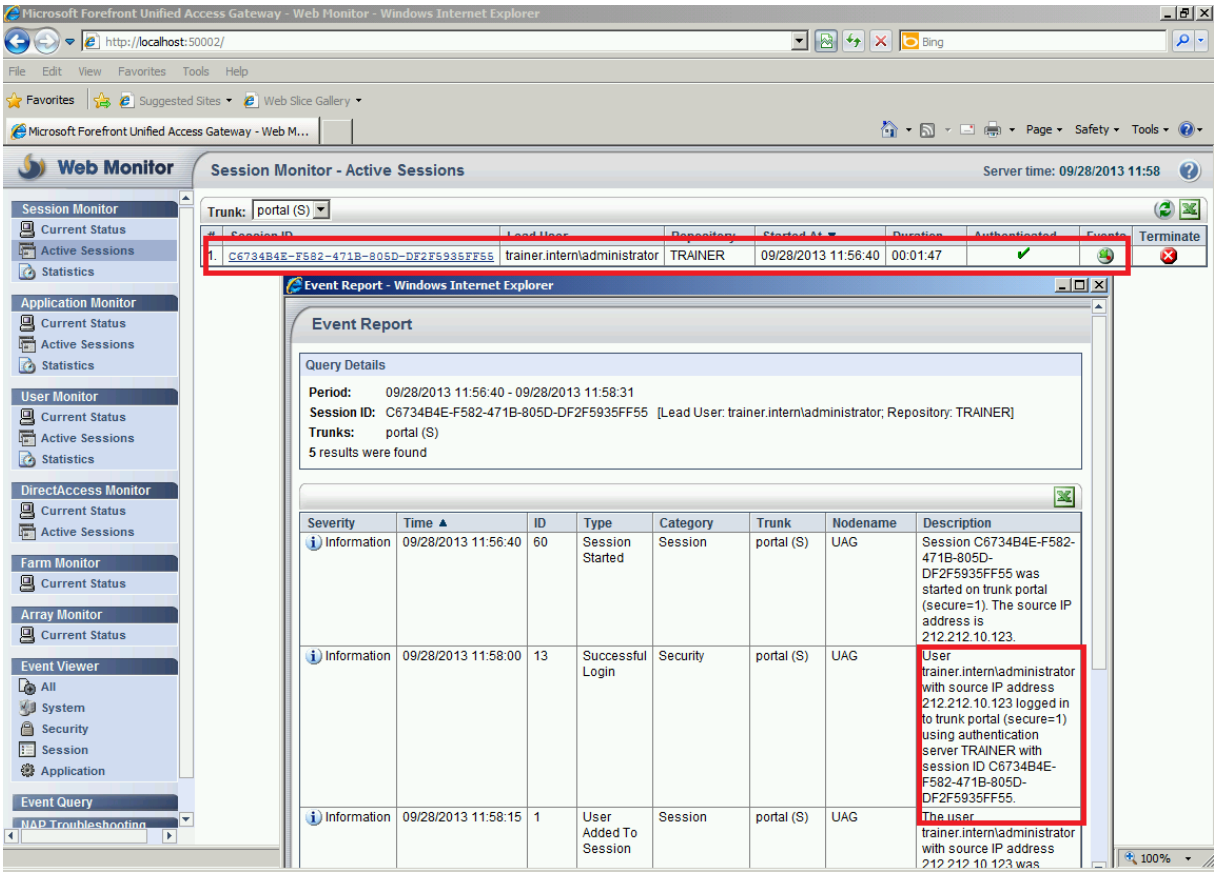

Figure 13: Monitor authenticated users

Conclusion

In this article I tried to explain the different authentication options in Forefront UAG. As you have seen, Forefront UAG provides a lot of different authentication options against different authentication providers and has support for certificate based authentication and two factor authentication with smartcards and One Time Passwords (OTP).

Related links

Configuring single sign-on with Kerberos constrained delegation
http://technet.microsoft.com/en-us/library/ee690462.aspx
How to get Client certificate authentication working on UAG 2010 Portal
http://social.technet.microsoft.com/wiki/contents/articles/17031.how-to-get-client-certificate-authentication-working-on-uag-2010-portal.aspx
SSO to SharePoint 2010 through UAG when using two authentication schemas
http://blogs.technet.com/b/edgeaccessblog/archive/2011/11/15/sso-to-sharepoint-2010-through-uag-when-using-two-authentication-schemas.aspx
Planning two-factor client authentication in Forefront UAG DirectAccess SP1
http://technet.microsoft.com/en-us/library/gg502571.aspx
Enabling UPN logon for forms-based authentication
http://technet.microsoft.com/en-us/library/ff607424.aspx
Forefront UAG registry keys
http://technet.microsoft.com/en-us/library/ee809087.aspx