

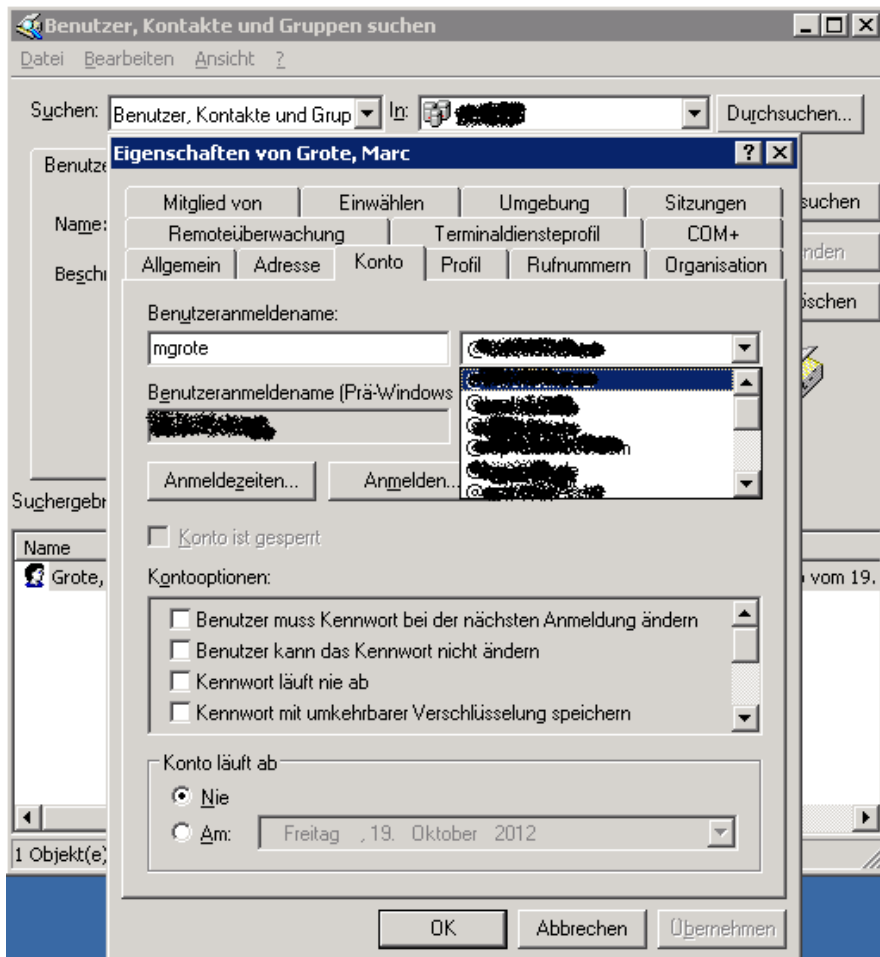
## Active Directory UPN Anmeldung

### UPN Informationen

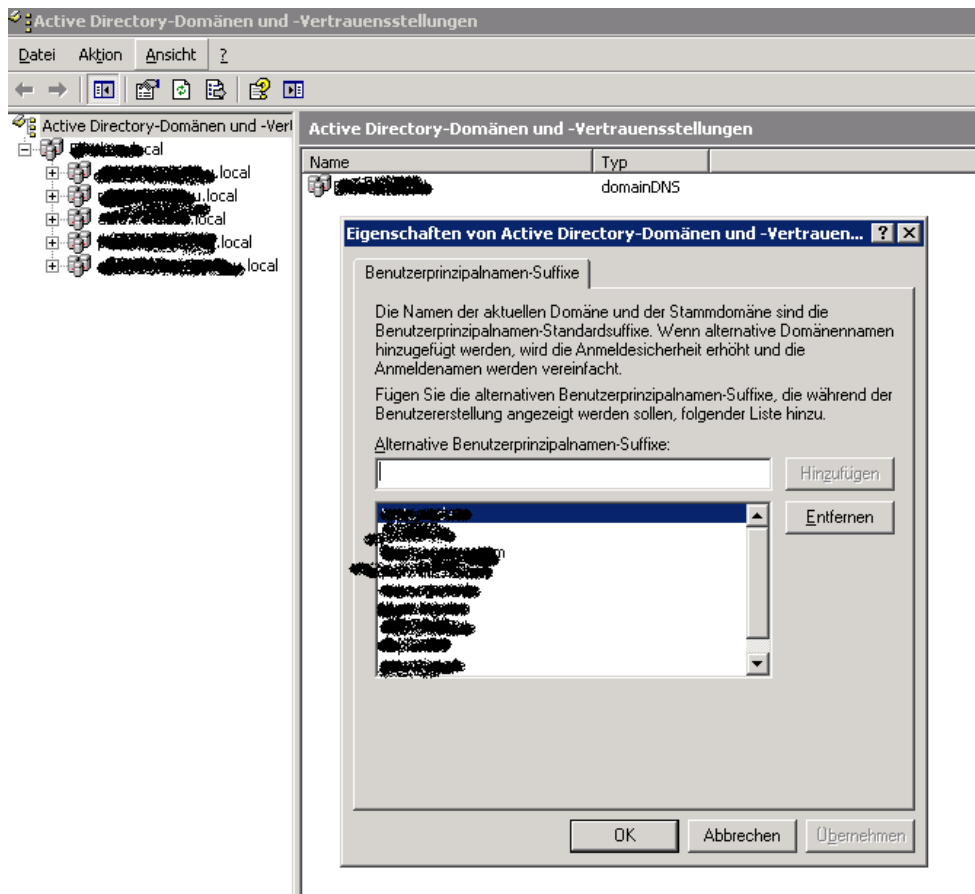
[http://technet.microsoft.com/en-us/library/cc739093\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc739093(v=ws.10).aspx)

[http://technet.microsoft.com/en-us/library/cc756018\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc756018(v=ws.10).aspx)

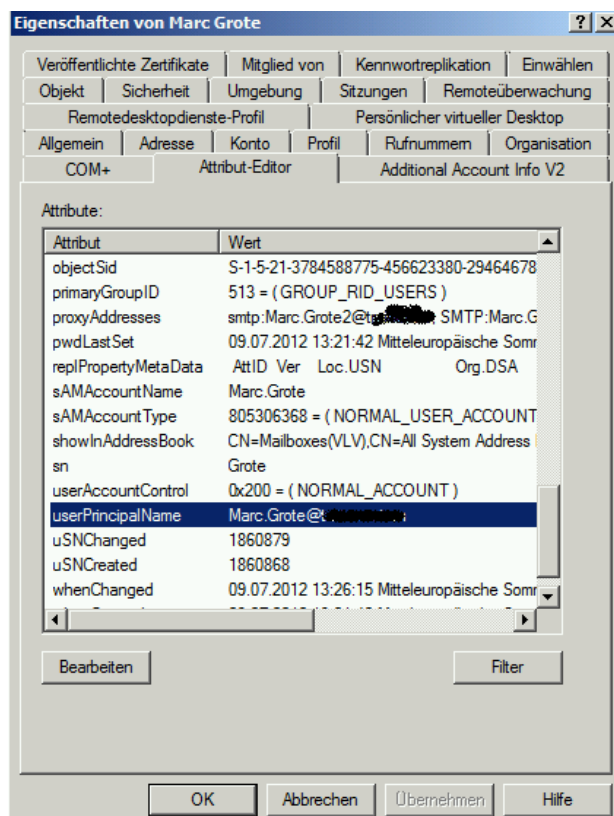
### UPN Suffix eines Benutzer Account



Konfigurierte UPN in dem XYZ.local Active Directory Forest

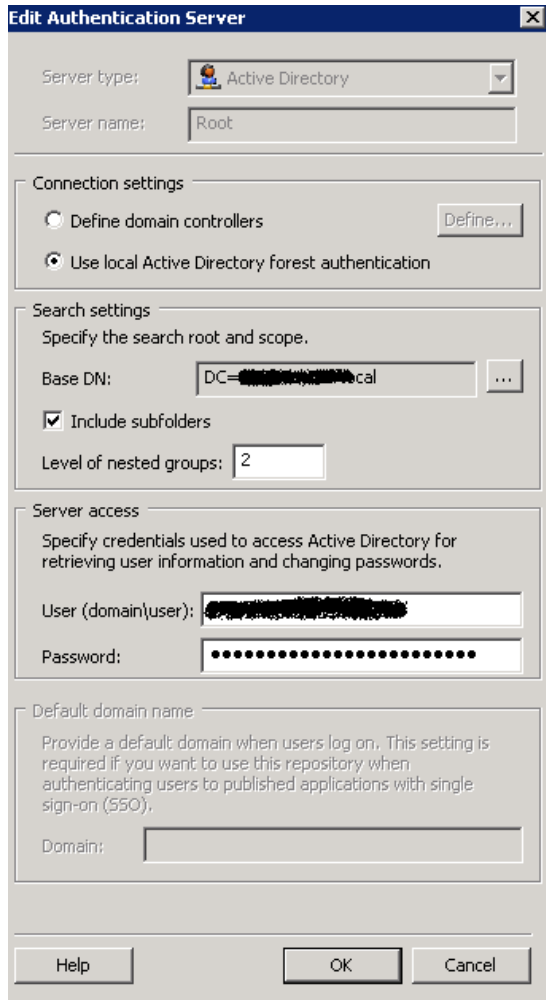


Einem Benutzer Account einen zusätzlichen UPN per Script Tools oder ähnlichem zu vergeben ist ebenfalls möglich. Es wird immer nur der aktive UPN fuer die Benutzeranmeldung zugelassen.



## Umstellung Forefront UAG auf UPN Logon

Forefront UAG wurde auf UPN Logon umgestellt. Benutzer welche sich am UAG Portal anmelden koennen einen Anmeldenamen verwenden, welcher als UPN Suffix hinterlegt und auf das Benutzerkonto gemappt ist.



Nach Umstellung auf UPN Login und Aenderung des Authentifizierungs Respositories ist derzeit eine laengere Anmeldephase am Portal zu verzeichnen, welche sich dadurch erklaren lasst, dass Forefront UAG eine Authentifizierungsanfrage zu den Domaenen Controllern der xyz.local Domaene sendet. Die DC in der xyz.local Domaene senden die Authentifizierungsanfrage zu den DC in den jeweiligen Active Directory Subdomaenen welche dann die Authentifizierung durchfuehren. Eine Optimierung der Anmeldezeiten wurde dann auf Forefront UAG Seite durch die Aenderung des Authentifizierungs Repository dahingehend durchgefuehrt, dass spezifische Domaenencontroller der xyz.local Forest Root Domaene angegeben wurden.

## Forefront UAG UPN aktivieren

### Neuen Authentication Server anlegen

**Edit Authentication Server** [X]

Server type: Active Directory

Server name: Root

**Connection settings**

Define domain controllers [Define...]

Use local Active Directory forest authentication

**Search settings**

Specify the search root and scope.

Base DN: DC=..., local [...]

Include subfolders

Level of nested groups: 2

**Server access**

Specify credentials used to access Active Directory for retrieving user information and changing passwords.

User (domain\user): [Redacted]

Password: [Redacted]

**Default domain name**

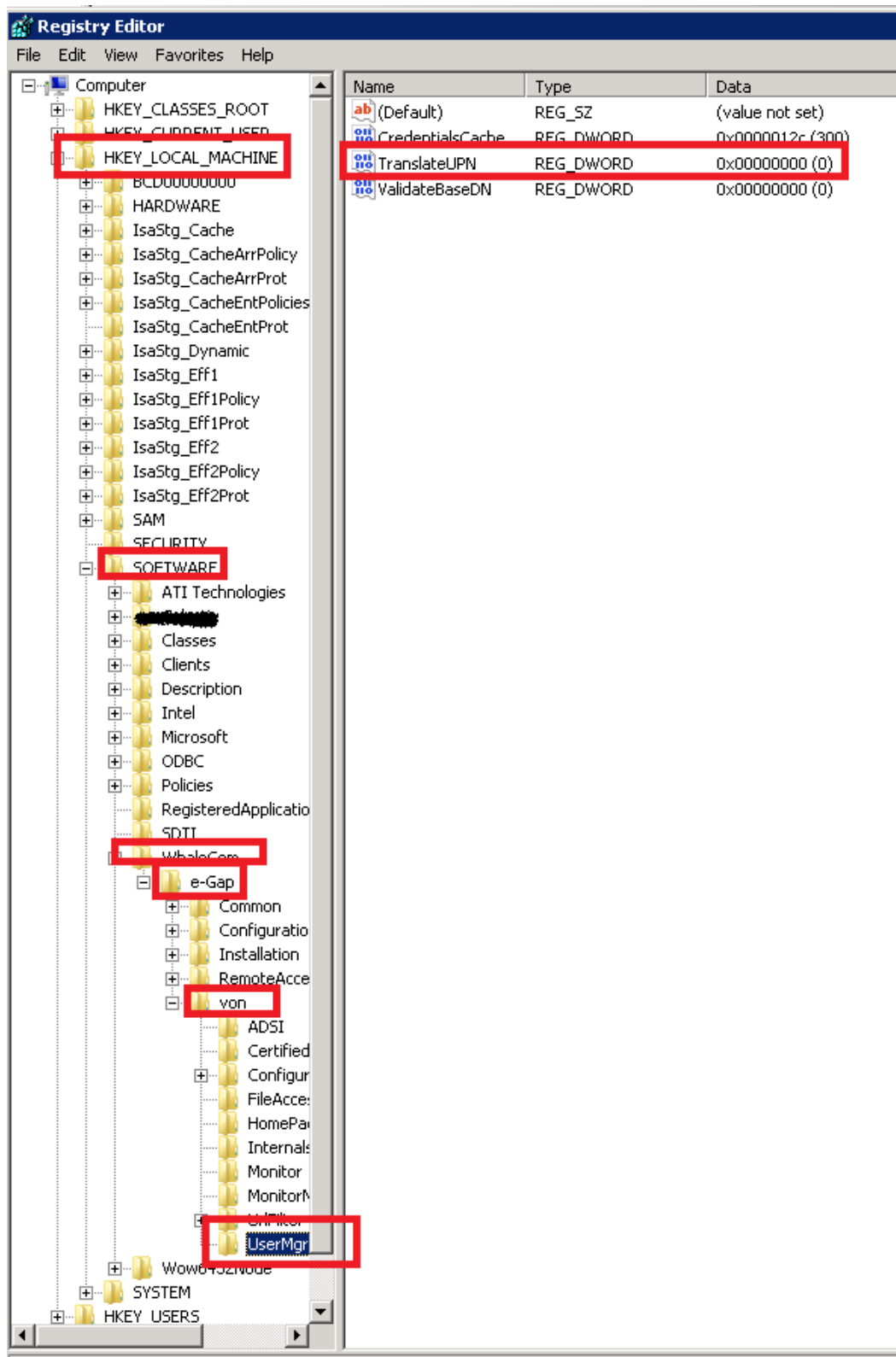
Provide a default domain when users log on. This setting is required if you want to use this repository when authenticating users to published applications with single sign-on (SSO).

Domain: [Redacted]

Help OK Cancel

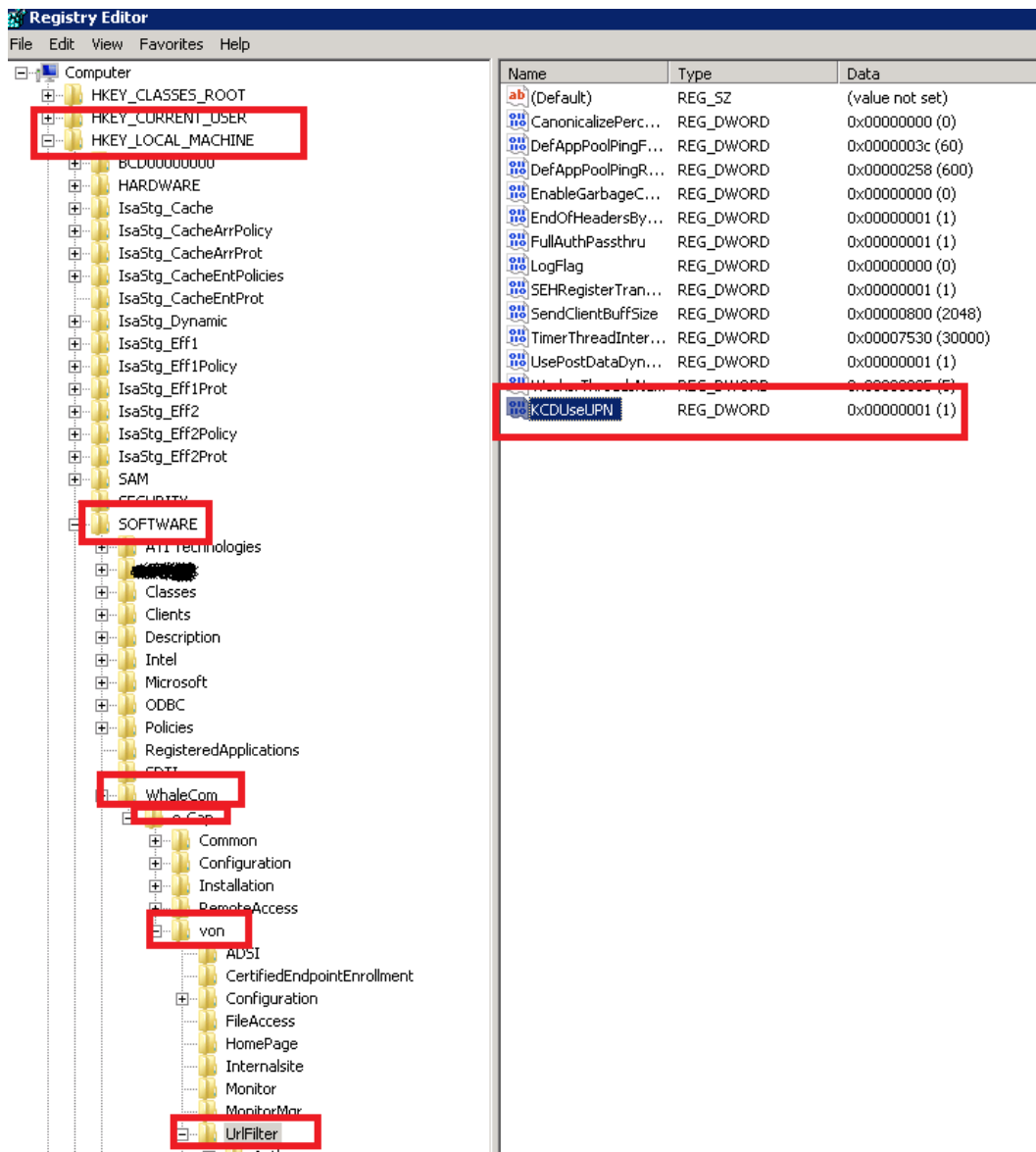
Registry Key Aenderung auf allen UAG Servern fuer die Aktivierung des UPN Logon.

Vorher:



TranslateUPN auf Wert = 1 setzen

## Kerberos Authentication fuer UPN aktivieren



Schlüssel anlegen mit Wert =1

Wert = 0 → DOMAIN\Benutzernamen Anmeldung.

Schlüssel nicht vorhanden = DOMAIN\Benutzernamen Anmeldung

## UAG Authentifizierungsrepository fuer UPN Login konfigurieren

Source:

<http://technet.microsoft.com/en-us/library/ff607424.aspx>

Die UPN Beispiel Datei repository\_for\_upn.inc aus dem Verzeichnis ...\\Microsoft Forefront Unified Access Gateway\\von\\InternalSite\\samples in das ...\\Microsoft Forefront Unified Access Gateway\\von\\InternalSite\\inc\\CustomUpdate Verzeichnis legen und umbenennen wie den Authentication Server im UAG

**CustomUpdate**

Computer > Local Disk (C:) > Program Files > Microsoft Forefront Unified Access Gateway > von > InternalSite > inc > CustomUpdate

File Edit View Tools Help

Organize Open New folder

★ Favorites  
Desktop  
Downloads

Name ^	Date modified	Type	Size
Root.inc	11/9/2009 1:09 AM	INC File	2 KB