

Smartsite
Putting your content to work

Active Directory/LDAP
Implementatiehandleiding
Voor Smartsite iXperion 1.3 en hoger



Copyright © 2011

Implementatiehandleiding Active Directory voor Smartsite iXperion

Auteur: ing. Silvio Bosch

Versiebeheer:

Versie	Status	Datum	Omschrijving en wijzigingen
1.0.2	concept	20-07-2010	Initiële versie
1.0.3	concept	11-08-2010	Reviewed door Mike en Twan
1.0.4	First release	16-08-2010	-
1.0.5	concept	22-11-2010	Toegevoegd LDAP koppeling Novell eDirectory
1.0.6	concept	23-11-2010	Toegevoegd mixed-mode configuratie
1.0.7	Release	29-03-2011	Toegevoegd toevoegen via ConfigEditor
1.0.8	Concept	14-06-2011	AD Scenario's toegevoegd Aanpassingen authentication
1.0.9	Concept	20-06-2011	Proxy server en domein policies
1.1.0	Concept	24-06-2011	Novell review
1.1.1	Second Release	26-06-2011	-
1.1.2	Concept	12-09-2011	Multi domaining 1.4 build 3
1.1.3	Third Release	23-09-2011	-

Implementatiehandleiding Active Directory voor Smartsite iXperion

Inhoudsopgave

1	Inleiding	6
2	Waarom een MS AD/LDAP koppeling?	6
2.1	Single Sign-On.....	6
2.2	Verschil Authentication en Security.....	6
2.2.1	Wat is Authentication.....	6
2.2.2	Wat is Security	8
3	Smartsite iXperion AD koppelingsprincipe	9
3.1	Mixed Mode Security	9
3.2	Smartsite iXperion Front-end en Back-end volledig gescheiden.....	9
3.3	Ondersteuning koppeling naar meerdere domeinen	9
	3.4 Ondersteuning Windows NT integrated Security database connectionstring	9
4	Mogelijke scenario's	10
4.1	Algemeen	10
4.2	Ondersteuning van 3 type koppelingen	11
5	Volledige Microsoft Active Directory Service koppeling	12
6	Configuratie Active Directory	12
6.1	Security Global Groups	13
6.2	Groepen, Rollen en Rol codes.....	20
6.3	Security Domain Local Groups	22
6.4	LDAP/AD logon user en het IIS website Application Pool account.....	28
6.4.1	Optioneel: Wijzigen Application pool account	29
6.5	Set Site Security Wizard	32
6.6	Web.config koppeling met 1 domein	33
6.6.1	ConfigSections	42
6.6.2	ConnectionStrings	42
6.6.3	Smartsite.ActiveDirectoryConfiguration	42
6.6.3.1	SmartsiteAccessGroup en ManagerAccessGroup	43
6.6.3.2	StoreFullyQualifiedLoginName	43
6.6.3.3	Databaseld.....	44
6.6.3.4	SearchBase	44
6.6.3.5	ObtainPrimaryGroup	44
6.6.3.6	ObtainParentGroupsForPrimaryGroup.....	45
6.6.3.7	MaxParentGroupRecursionDepth (default=0).....	45
6.6.3.8	UpdatePrimaryGroup	45
6.6.3.9	Membershipmappings.....	47
6.6.4	Authentication front-end.....	47
6.6.5	Membership Provider	47
6.6.6	Role provider	48

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.6.7	Authentication Back-end (CMS)	48
6.7	ADSI Edit	49
6.8	IIS integrated authentication.....	50
6.9	Site Registry Security Key	52
7	Domein- en Smartsite iXperion Primary Group	53
8	Disabling Single Sign-on	56
8.1	Voorkomen IE inlogbox in Smartsite Manager	56
9	Hoe een Domain Group Policy aan te maken.....	57
10	Smartsite ConfigEditor en Active Directory Configuratie	63
11	Proxy/ISA Server en Firewall.....	64
11.1	Outscaling.....	64
11.2	Smartsite Manager	64
12	Custom Errorhandling in Web.config	65
13	Integrated database connectionstring	67
14	Smartsite iXperion Mixed Mode Security.....	70
14.1	Mixed mode web.config	70
14.1.1	UpdatePrimaryGroup	70
14.2	Mixed mode domein configuratie	71
14.3	Smartsite iXperion mixed mode groepen structuur	72
14.4	IIS instellingen voor mixed mode security	74
14.4.1	IIS Anonymous authentication en Windows Integrated Authentication enabled	75
15	Active directory koppeling met meerdere domeinen	79
15.1	Outgoing en incoming trust (tweeweg-trust)	79
15.2	Groepen en users	80
15.2.1	StoreFullyQualifiedLoginName	80
	Doordat een gebruiker op meerdere domeinen onder dezelfde accountname kan voorkomen, dient de web.config parameter StoreFullyQualifiedLoginName altijd gelijk aan true te zijn.....	80
15.3	Web.config multi-domaining	81
15.4	Active directory tester	90
15.5	Multi-domain via Smartsite iXperion ConfigEditor	94
16	Smartsite iXperion LDAP koppeling met Novell eDirectory	95
16.1	Specifieke Membership Provider	95
16.2	Forms authentication	95
16.3	Configuration Web.config	95
16.3.1	Connection string	95
16.3.2	Membership provider.....	95
16.3.3	Settings	97
16.4	Forms authentication	98
16.4.1	Front-end.....	98

Implementatiehandleiding Active Directory voor Smartsite iXperion

16.4.2	Back-end	98
16.4.3	Registry configuratie	99
17	Novell configuratie.....	108
17.1	TLS/SSL en poort configuratie	108
18	IIS Configuratie voor Novell	110
18.1	Front-End Authentication.....	110
18.2	Back-end Authentication	113
18.3	Groepen in Novell.....	116
18.4	Groepen in Smartsite	117
18.5	Fouten ten gevolgen van Novell LDAP security settings	118

Implementatiehandleiding Active Directory voor Smartsite iXperion

1 Inleiding

Dit document beschrijft de Microsoft Active Directory Service / LDAP (Lightweight Directory Access Protocol) scenario's die door Smartsite iXperion 1.3 build 6 en hoger standaard worden ondersteund.

2 Waarom een MS AD/LDAP koppeling?

Door Smartsite iXperion te koppelen met Microsoft Active Directory Service of een LDAP database service zoals Novell, kan het beheer van de toegangsrechten voor zowel de front-end als de back-end (manager) van Smartsite iXperion worden verplaatst naar het niveau van systeembeheer.

2.1 Single Sign-On

Alleen wanneer gebruik wordt gemaakt van Microsoft Active Directory Service en Internet Explorer als browser, is het mogelijk gebruik te maken van Single Sign-On. Single Sign-On zorgt er voor dat wanneer een gebruiker met zijn AD account is ingelogd op zijn PC, hij met dezelfde AD gegevens automatisch inlogt in Smartsite iXperion, zonder daarbij opnieuw zijn account gegevens en password te hoeven in te geven.

2.2 Verschil Authentication en Security

Authentication en security worden nog wel eens doorelkaar gebruikt.

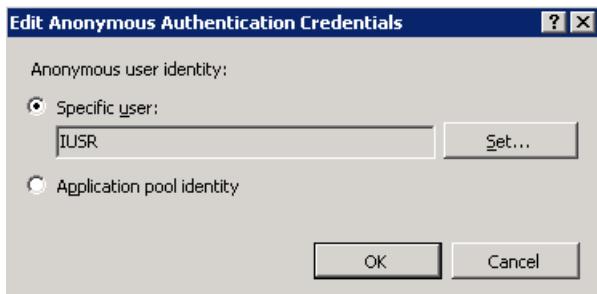
2.2.1 Wat is Authentication

Authentication is het mechanisme waarmee de gebruiker geautoriseerd wordt. Smartsite iXperion ondersteunt alleen IIS als http server. IIS ondersteunt de volgende Authentication mechanisme die compatible zijn met Smartsite iXperion:

- **Anonymous Authentication**

IIS gebruikt een voor gedefinieerd account (IUSR) om alle authentiseren gebruikers anoniem op de site te laten browsen.

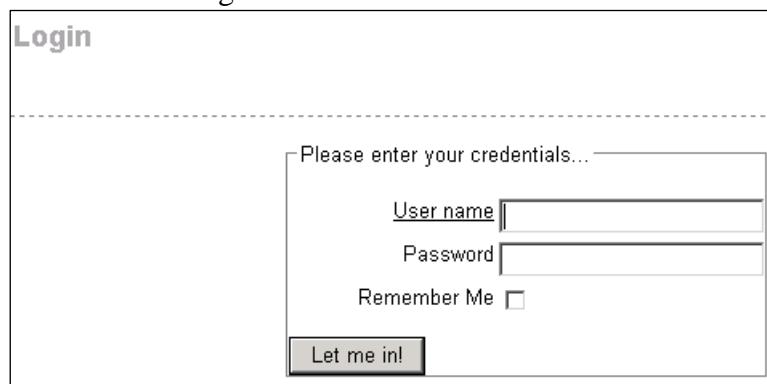
Implementatiehandleiding Active Directory voor Smartsite iXperion



Het IIS Anonymous account is in IIS instelbaar.

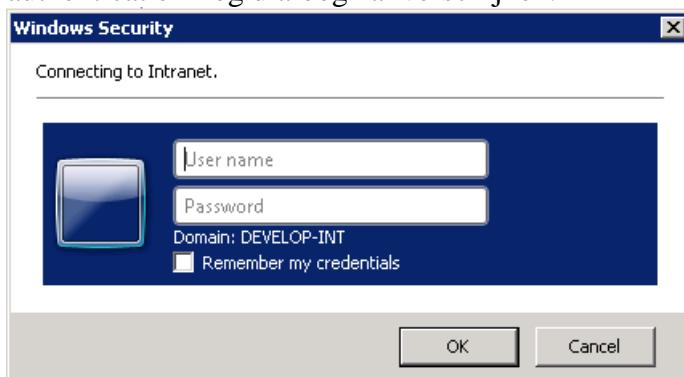
- **Forms Authentication**

Deze vorm wordt alleen in de front-end ondersteund, waarbij er een internet inlog formulier wordt getoond om te autoriseren.



- **Basic Authentication**

Gebruikersnaam en password worden Base64 encoded over het netwerk verzonden. Basic Authentication ondersteunt geen Single sign-on waardoor altijd een authenticatie inlog dialoog zal verschijnen.



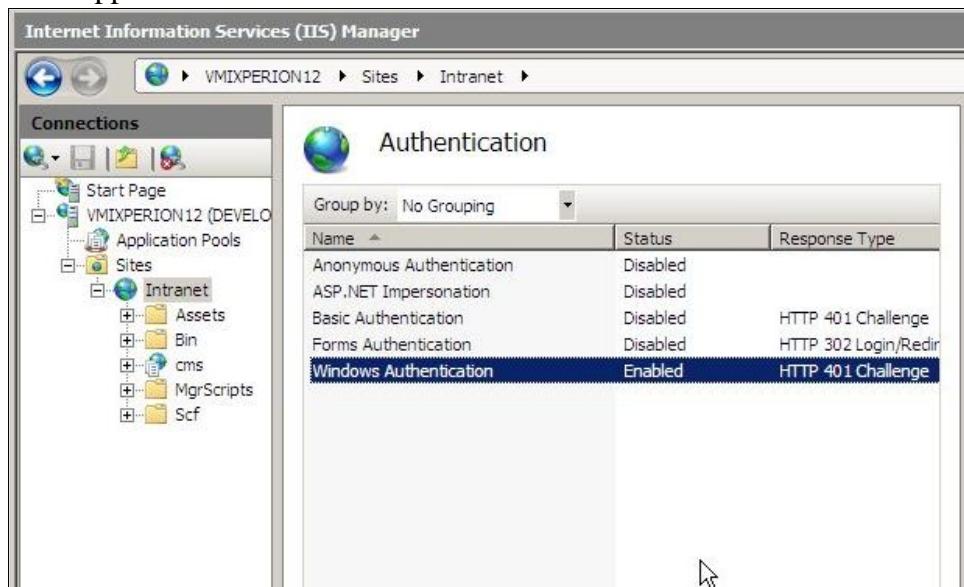
Implementatiehandleiding Active Directory voor Smartsite iXperion

- **Integrated Authentication**

Gebruikersnaam en password worden niet verzonden. Er wordt gebruik gemaakt van NT Challenge Respons via NTLM of Kerberos Authentication protocol.

Integrated Authentication ondersteunt als enige Single sign-on, dus men hoeft na inloggen op de client PC niet opnieuw zijn gebruikersnaam en password op te geven wanneer met de front-end of back-end van de site bezoekt.

In IIS zijn alle geïnstalleerde Authentication mechanisme zichtbaar voor zowel de site als de CMS application:



2.2.2 Wat is Security

Security is het mechanisme om gegevens te beschermen voor niet geautoriseerde gebruikers. Een gebruiker dient eerst geautoriseerd te zijn voordat hij via de ingestelde security zijn rechten kan ontlenen.

In Smartsite iXperion is de security geregeld op groeps (role) niveau. De groepen waarvan men lid is bepalen welke rollen men krijgt en op welke folders/items in de Smartsite folderhiërarchie men rechten heeft. De verschillende rollen geven toegang tot de toegekende acties.

Implementatiehandleiding Active Directory voor Smartsite iXperion

3 Smartsite iXperion AD koppelingsprincipe

Het Smartsite iXperion AD koppelingsprincipe is gebaseerd op het overnemen van de AD groepsnamen in de Smartsite iXperion groepsnamen definitie. Via een apart vinkje “externallymanaged” kan worden aangegeven of een groepsnaam te vinden is op het AD.

3.1 Mixed Mode Security

Naast de volledige AD koppelingsvariant is het mogelijk om niet alle groepen te definiëren op het AD. Deze vorm van koppeling heet in Smartsite iXperion termen: “Mixed Mode Security”. Bij deze vorm is het wel mogelijk gebruik te maken van IIS integrated Authentication en single sign-on, maar vindt het groepenbeheer plaats in Smartsite iXperion en niet door systeembeheer.

3.2 Smartsite iXperion Front-end en Back-end volledig gescheiden

Belangrijk is te weten dat de autorisatie en de security van de Smartsite iXperion Front-end en Back-end volledig gescheiden zijn en apart configurerbaar zijn.

Zo is het bijvoorbeeld mogelijk de front-end van een site volledig via IIS anonymous authentication te laten draaien en de back-end te voorzien van IIS integrated authentication met een volledige AD koppeling.

3.3 Ondersteuning koppeling naar meerdere domeinen

Een connectie naar meerdere Active Directory domeinen wordt vanaf Smartsite iXperion 1.4 build 3 en hoger ondersteund.

3.4 Ondersteuning Windows NT integrated Security database connectionstring

Een integrated OLEDB connectiestring naar een SQL database wordt vanaf Smartsite iXperion 1.4 build 3 en hoger ondersteund.

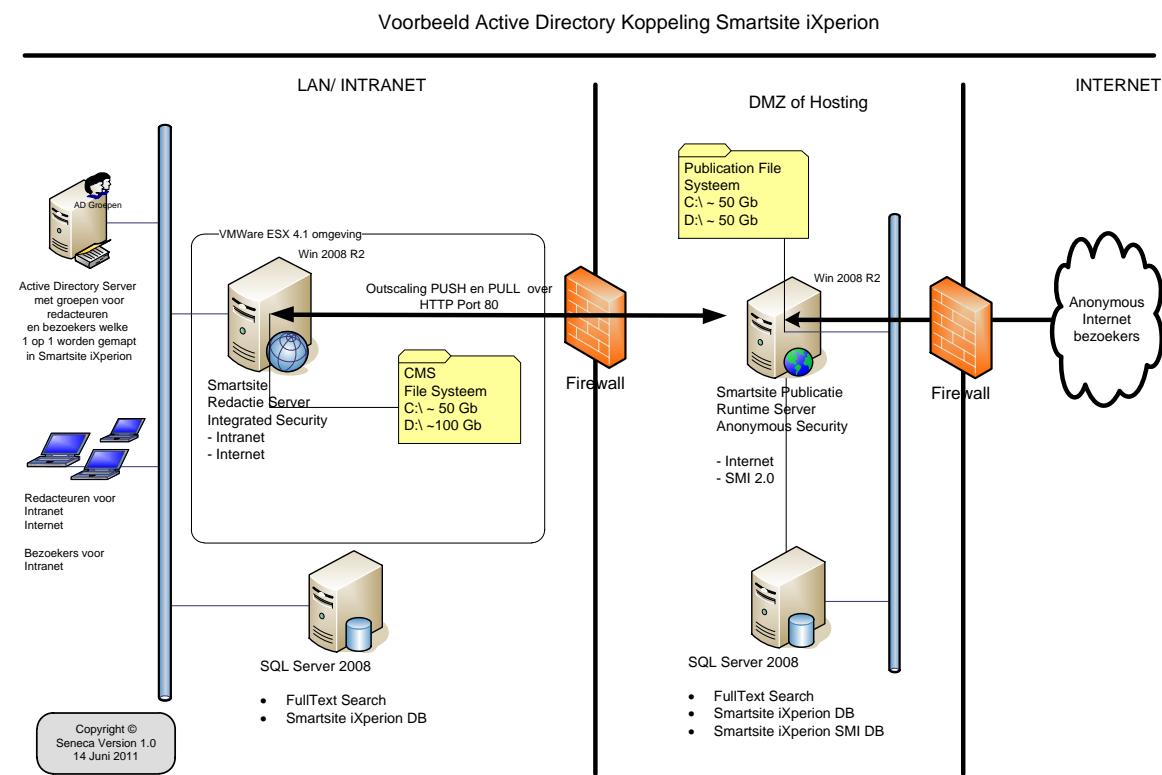
Implementatiehandleiding Active Directory voor Smartsite iXperion

4 Mogelijke scenario's

4.1 Algemeen

Microsoft Active Directory Service of een LDAP koppeling met Novell wordt door Smartsite iXperion standaard ondersteund in een gesloten LAN configuratie.

Hieronder een voorbeeld van veel voorkomend Intranet/Internet iXperion site scenario met een AD koppeling voor redacteuren en intranet bezoekers in een gesloten LAN.



In bovenstaand scenario loggen de intranet/internet redacteuren in via single sign-on in de Smartsite manager. De content en bestanden die ze toevoegen aan de internet tak in Smartsite, worden automatisch geoutscaled naar de server die geplaatst is bij de hosting partij. Het intranet kan via het LAN worden gebrowsed.

Implementatiehandleiding Active Directory voor Smartsite iXperion

4.2 Ondersteuning van 3 type koppelingen

Smartsite ondersteunt standaard de volgende 3 type koppelingen

1. Smartsite iXperion volledige Microsoft Active Directory Service koppeling
2. Smartsite iXperion Mixed Mode Security koppeling
3. Smartsite iXperion LDAP koppeling naar Novell eDirectory

Type Koppeling	Single Sign-on (IE)	Multi-domaining*	integrated Security database connectionstring*
Volledige Microsoft Active Directory Service	Ja	Ja	Ja
Mixed Mode Security	Ja	Ja	Ja
LDAP koppeling naar Novell eDirectory	Nee	Nee	Nee

*Voor Multi-domaining en een integrated database connectionstring is iXperion versie 1.4 build 3 of hoger vereist.

Implementatiehandleiding Active Directory voor Smartsite iXperion

5 Volledige Microsoft Active Directory Service koppeling

Bij een volledige MS AD koppeling wordt het volledige beheer van de gebruiker-accounts bij systeembeheer neergelegd. Systeembeheer beheert via het AD de toegang tot Smartsite iXperion voor zowel de front-end als de back-end door de AD accounts in de juiste AD groepen te plaatsen. Deze AD groepsnamen zijn 1 op 1 overgenomen in Smartsite iXperion. De groepen hebben op de gebruikelijke manier binnen Smartsite iXperion rechten gekregen op de folderstructuur binnen Smartsite. Het uitdelen van de (browse/edit) rechten op de folderstructuur binnen Smartsite iXperion is meestal geen taak van de systeembeheerder, maar een taak van de site webmaster.

6 Configuratie Active Directory

Voordat men de koppeling met het AD gaat maken dient er eerst goed te worden nagedacht over de groepsindeling op zowel het AD als die in Smartsite.

In deze handleiding gaan we uit van een eenvoudige groepsindeling.

- **Administrators**

Dit zijn personen die de website server onderhouden en het AD inrichten. Op deze manier kunnen zij nieuw aangemaakte AD groepen overnemen in Smartsite.

- **Webmasters**

Dit zijn personen die de Smartsite website beheren en alle acties waaronder de security tools tot hun beschikking hebben. Zij delen de groepsrechten uit op de Smartsite folderstructuur.

- **ChiefEditors**

Dit zijn personen die zelf artikelen publiceren of de door Editors gemaakte artikelen reviewen en daarna publiceren.

- **Editors**

Dit zijn personen die artikelen schrijven maar normaliter niet zelf publiceren.

- **Visitors1; Visitors2**

Dit zijn personen die op bepaalde gedeelte van de site structuur browse/view rechten toegekend krijgen. (Restricted Area's).

Naast deze groepen, gebruikt Smartsite intern nog de volgende 2 groepen.

- **StartGroup**

Dit is een groep die gereserveerd is voor Smartsite. Hierin bevinden zich soms

Implementatiehandleiding Active Directory voor Smartsite iXperion

gebruikers die zich bezig houden met site ontwikkeling. Tevens bevat deze groep verborgen gebruikers die voor specifieke Smartsite doeleinden worden gebruikt.

- **Guests**

- De Guests groep hoeft **niet** te worden aangemaakt op het domein.
- In principe dient iedereen lid te zijn van de Guests groep, zodat iedereen view access heeft op de Front-end van de site. De Guests groep is het anonymous account voor het bezoeken/browse van de site.

De Guests groep dient in Smartsite vanaf de Root van de gehele site View item rechten te hebben!

 Let op:

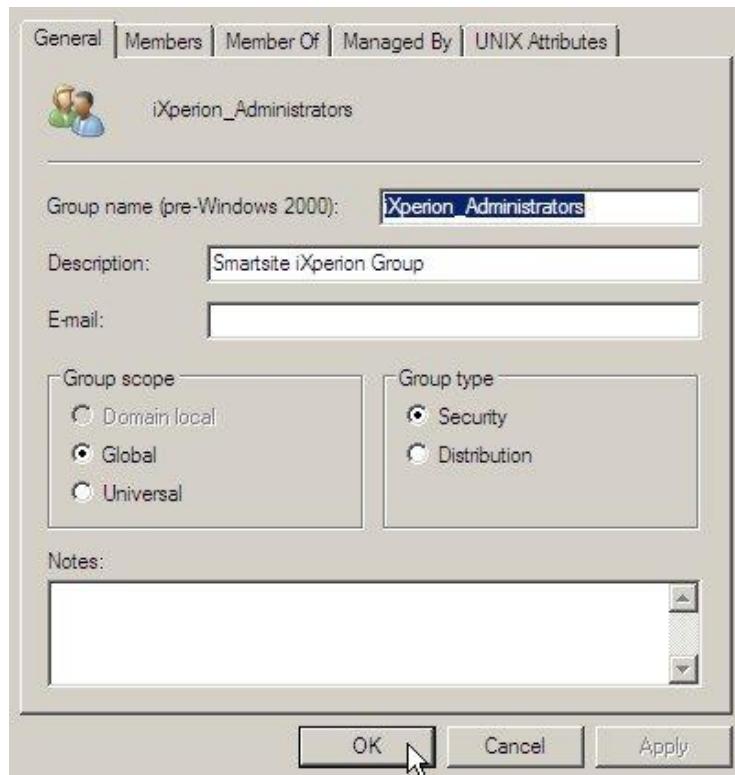
- De Guests groep dient te worden verwijderd voor restricted sites (Extranet) of wanneer gedeelte van site een inlog vereisen.
- De Guests groep dient altijd rechten te hebben op de login pagina's.
- De Guests groep mag **nooit** uit Smartsite worden verwijderd.
- De Guests groep beschikt over de Guests role welke net als de Visitors role over **geen** acties beschikt.
- Wanneer een AD gebruiker inlogt, wordt hij in het geval van de AD koppeling automatisch toegevoegd aan de Guests groep.

Op het AD dienen minimaal 2 type Global Security groepen te worden gedefinieerd en 2 Domain Local groepen te worden aangemaakt.

6.1 Security Global Groups

Om de groepen structuur van het AD in Smartsite iXperion te mappen dienen er Security Global Groups te worden aangemaakt op het domein. Het is tevens mogelijk al bestaande AD Global Groups te gebruiken en deze in Smartsite te mappen.

Implementatiehandleiding Active Directory voor Smartsite iXperion



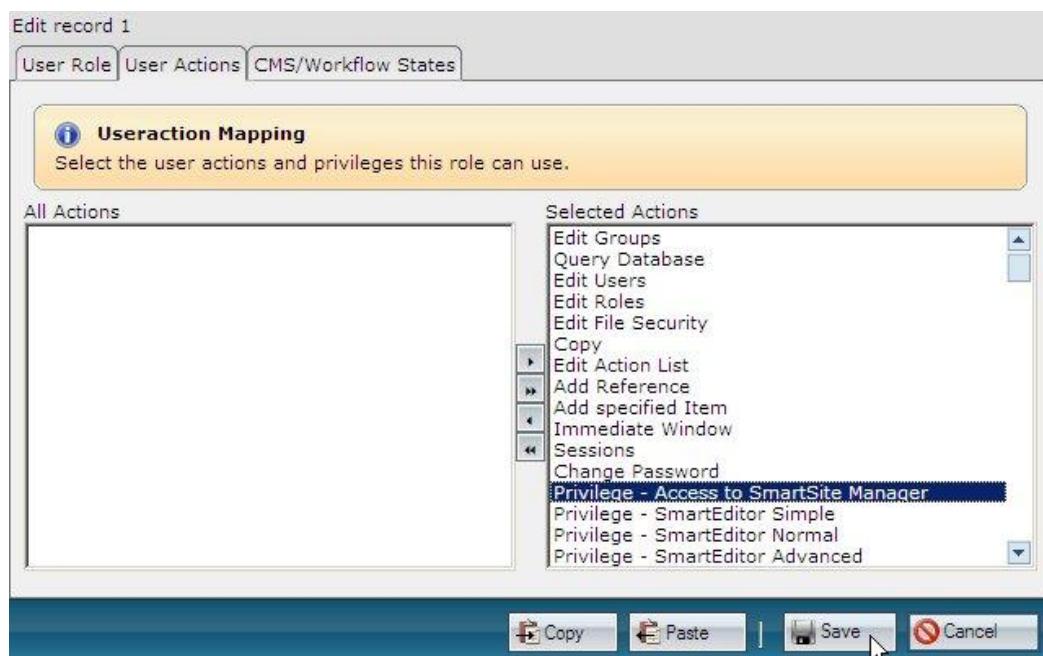
De groepsnamen die op het AD zijn aangemaakt dienen daarna in Smartsite te worden overgenomen via de actie Edit Groups. Met het vinkje “Externally Managed” dat bij Edit Group actie beschikbaar is, kun je aangeven dat de groep een domein groep is (Zie ook mixed-mode).

Er zijn twee 2 type groepen:

Manager Access Groepen

De Manager Access Groepen, zijn alle Domein Security Global Groups en beschikken over 1 of meerdere rollen. Die rollen beschikken over minimaal het “*Privilege - Access to Smartsite Manager*”. Deze groepen dienen op het domein aan beiden Security Domain Local Groups (SmartsiteAccess en SmartsiteManagerAccess) te worden toegevoegd.

Implementatiehandleiding Active Directory voor Smartsite iXperion



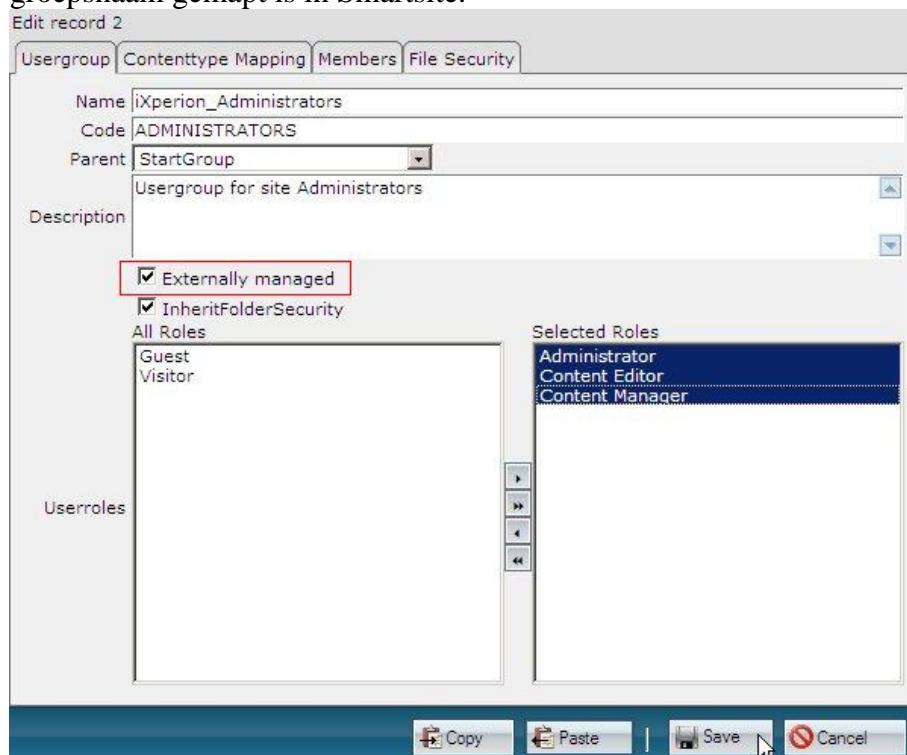
Privilege - Access to Smartsite Manager in Edit User Role.

Wanneer geen enkele rol beschikt over dit Privilege krijg je bij inloggen de melding:
User xxxx has no Manager privileges!



Implementatiehandleiding Active Directory voor Smartsite iXperion

Hieronder de iXperion_Administrators groep wel aanwezig is op het domein en via de groepsnaam gemapt is in Smartsite.



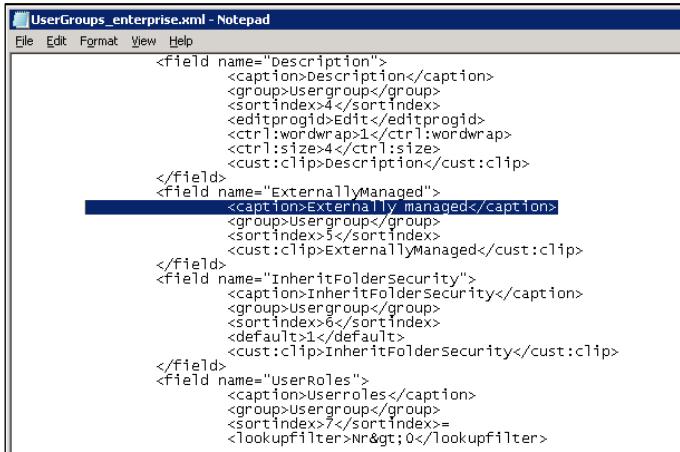
Het Externally managed vinkje dient geselecteerd te zijn voor alle AD groepen die worden gemapt in Smartsite.



Tip: De caption “externally managed” kan optioneel worden aangepast in het bestand `\Sites\Intranet\System\DataEditor\Meta\UserGroups_{versie}.XML`.

Versie is hierbij Enterprise, Standard of Professional.

Implementatiehandleiding Active Directory voor Smartsite iXperion

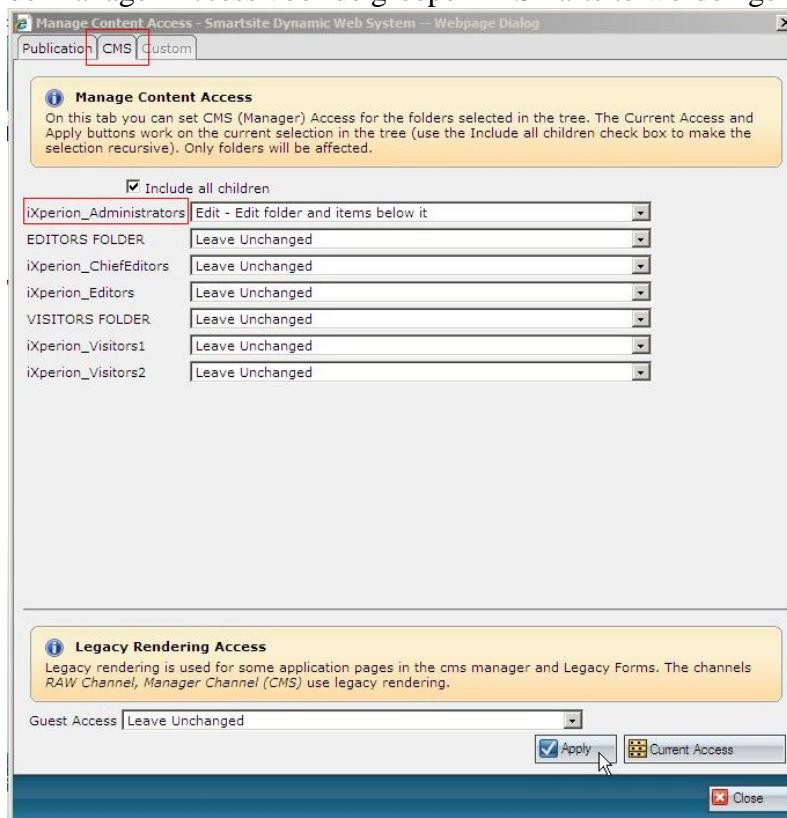


```

<field name="description">
    <caption>Description</caption>
    <group>Usergroup</group>
    <sortIndex>4</sortIndex>
    <editProgId>Edit</editProgId>
    <ctrl>WordWrap<ctrl>WordWrap</ctrl>
    <ctrl>Size<ctrl>Size</ctrl>
    <cust:clip>Description</cust:clip>
</fields>
<field name="ExternallyManaged">
    <caption>Externally managed</caption>
    <group>Usergroup</group>
    <sortIndex>5</sortIndex>
    <cust:clip>ExternallyManaged</cust:clip>
</fields>
<field name="InheritFolderSecurity">
    <caption>InheritFolderSecurity</caption>
    <group>Usergroup</group>
    <sortIndex>6</sortIndex>
    <default>1</default>
    <cust:clip>InheritFolderSecurity</cust:clip>
</fields>
<field name="UserRoles">
    <caption>Userroles</caption>
    <group>Usergroup</group>
    <sortIndex>7</sortIndex>
    <lookupFilter>Nr>&gt;0</lookupFilter>

```

Via het menu Configuration kan via de actie **Manage Content Access** en het tabblad CMS de Manager Access voor de groepen in Smartsite worden gezet.



Visitors Groepen (groepen voor restricted toegang front-end)

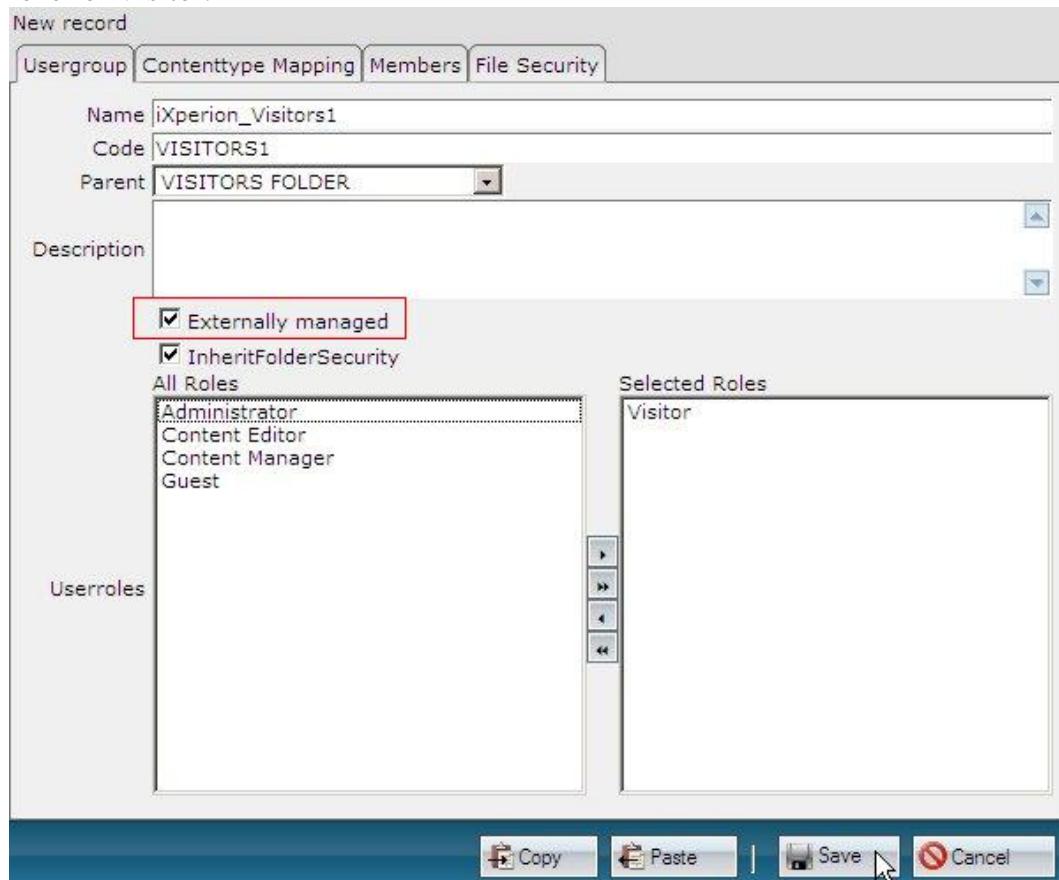
Naast dat je lid kunt zijn van Manager Access groepen die je toegang tot de Smartsite manager verschaffen en bepalen of en waar je items kunt toevoegen, kun je tevens of indien

Implementatiehandleiding Active Directory voor Smartsite iXperion

gewenst lid zijn van 1 of meer Visitors groepen. Visitors groepen worden gebruikt om restricted toegang te krijgen tot een site of een gedeelte van de site in de front-end (login vereist). Een Visitors groep wordt net als een Manager Access groep aangemaakt op het domein en gemapt in Smartsite.

⚠ Let op: Een Visitors groep bevat in Smartsite 1 rol zonder acties en privileges!

In onderstaand voorbeeld is de Visitors groep iXperion_Visitors1 toegevoegd met de actie loze rol Visitor.



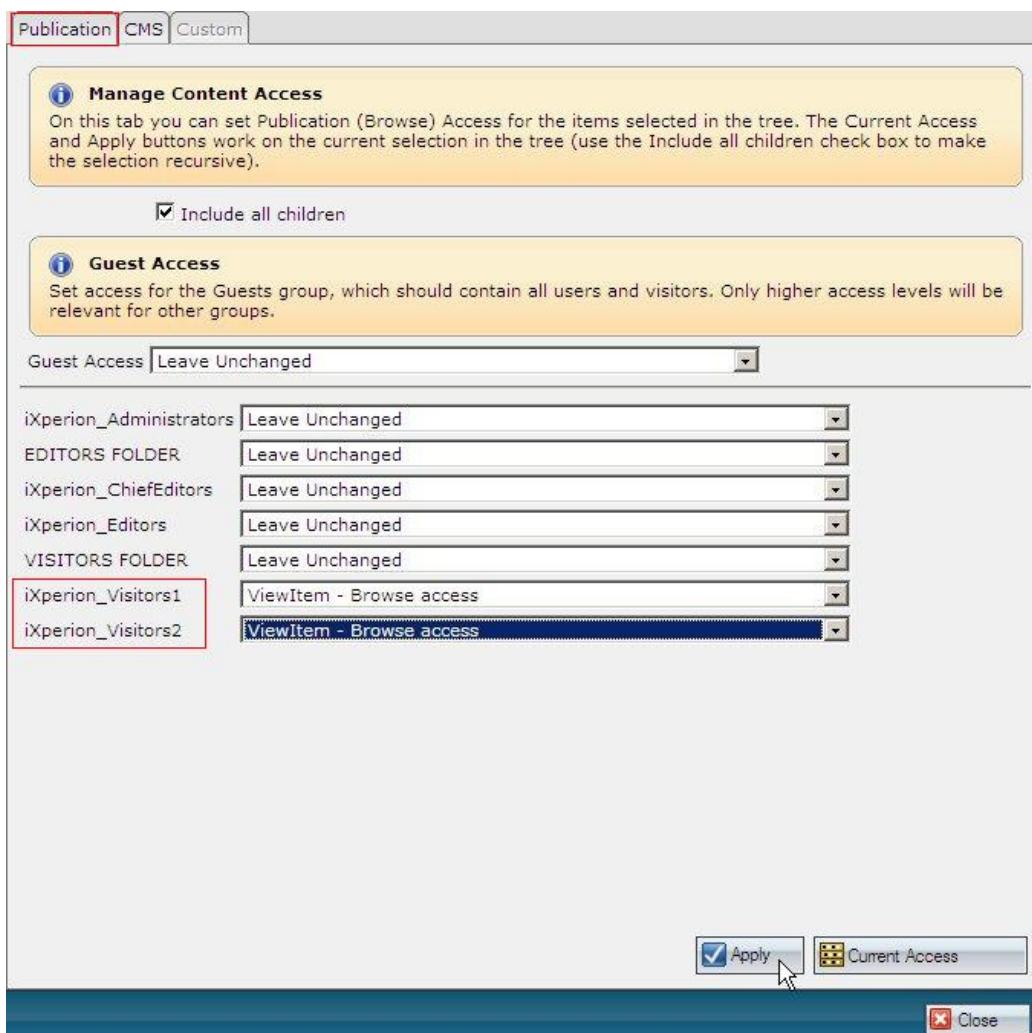
Ook de visitor groepen zijn AD groepen, dus dient externally managed aan te staan.

Voor Visitor groepen dienen tevens rechten te worden gezet.

Via het menu Configuration kan via de actie **Manage Content Access** en het tabblad Publication de Browse Access voor deze groepen worden gezet. Na het zetten van de Browse Access zijn de items restricted en zal je dus bij het oproepen van een item in een dergelijke folder in de front-end een loginbox krijgen waar je je accountgegevens moet

Implementatiehandleiding Active Directory voor Smartsite iXperion

invullen. Echter wanneer we IIS integrated authentication gebruiken zal je direct toegang krijgen als je lid bent van de visitors groep(en) via Single sign-on.

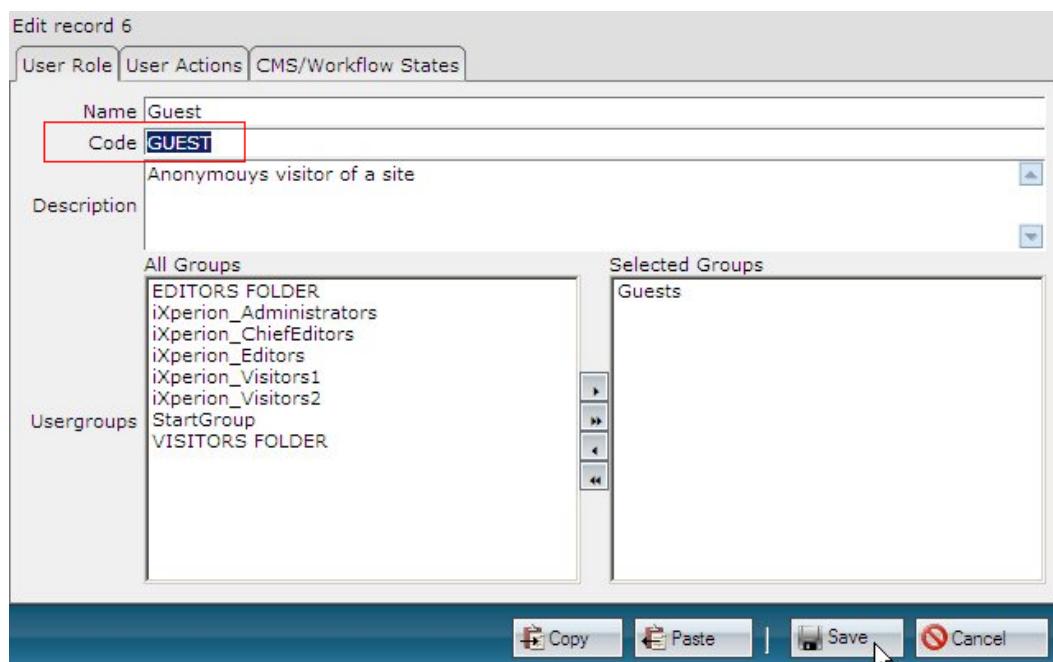


Zetten van browse access voor de Visitor groepen.

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.2 Groepen, Rollen en Rol codes

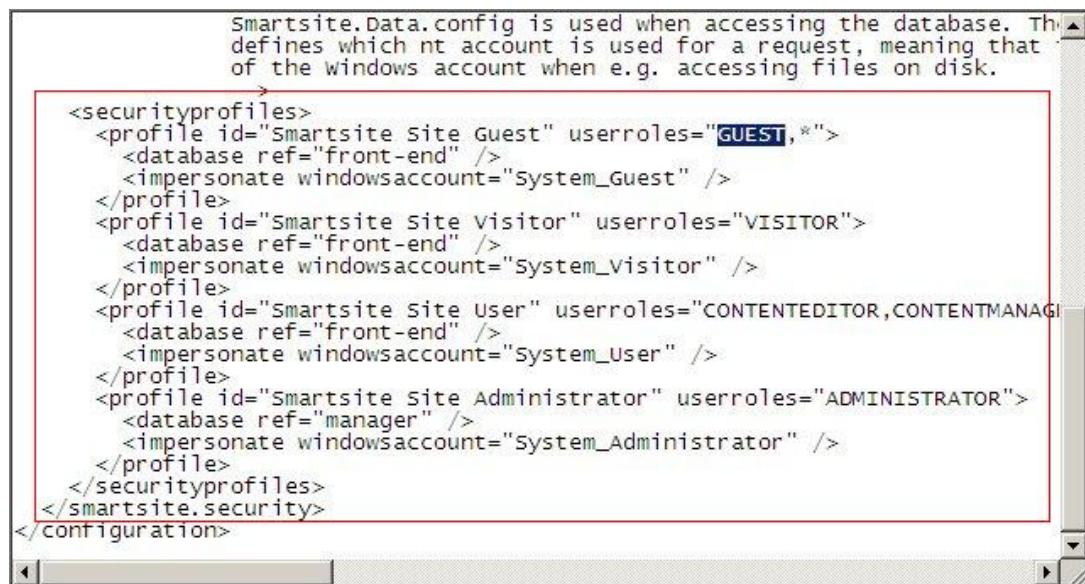
Iedere groep, Manager Access Groep of Visitor Groep (Guests) heeft 1 of meerdere rollen. De code van deze rollen is van belang voor de “impersonation” van de gebruikers die op Windows NT niveau worden gebruikt. D.w.z. dat wanneer een gebruiker inlogt in Smartsite iXperion, onderwater een andere NT gebruiker wordt gebruikt om de daadwerkelijk actie uit te voeren. Het impersonate windows account krijgt zijn rechten toegekend via NT groepen die door de site security wizard worden aangemaakt.



Voor de build-in Guests groep wordt standaard de code GUEST gebruikt.

Implementatiehandleiding Active Directory voor Smartsite iXperion

De code van de Rollen is in de Smartsite.Security.Config gekoppeld aan de Windows NT accounts.



```
smartsite.Data.config is used when accessing the database. This defines which nt account is used for a request, meaning that of the windows account when e.g. accessing files on disk.

<securityprofiles>
  <profile id="smartsite Site Guest" userroles="GUEST,*">
    <database ref="front-end" />
    <impersonate windowsaccount="System_Guest" />
  </profile>
  <profile id="smartsite Site Visitor" userroles="VISITOR">
    <database ref="front-end" />
    <impersonate windowsaccount="System_Visitor" />
  </profile>
  <profile id="Smartsite Site User" userroles="CONTENTEDITOR,CONTENTMANAGER">
    <database ref="front-end" />
    <impersonate windowsaccount="System_User" />
  </profile>
  <profile id="smartsite Site Administrator" userroles="ADMINISTRATOR">
    <database ref="manager" />
    <impersonate windowsaccount="System_Administrator" />
  </profile>
</securityprofiles>
</smartsite.security>
</configuration>
```

Het wijzigen van de Userrole codes is dus niet zomaar toegestaan. Wanneer de codes worden gewijzigd in Smartsite dienen deze ook in de Smartsite.Security.Config handmatig te worden aangepast, waarna de site herstart dient te worden.

- ⚠ Let op:** Bij het aanmaken van een nieuwe rol dient deze te worden voorzien van een geldige code die in de Smartsite.Security.Config gedefinieerd staat. Bij het aanmaken van rollen is het kopiëren van een rol daarom aan te bevelen.

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.3 Security Domain Local Groups

Voor de toegang tot Smartsite dienen 2 Security Domain **Local** groepen te worden aangemaakt op het domein.

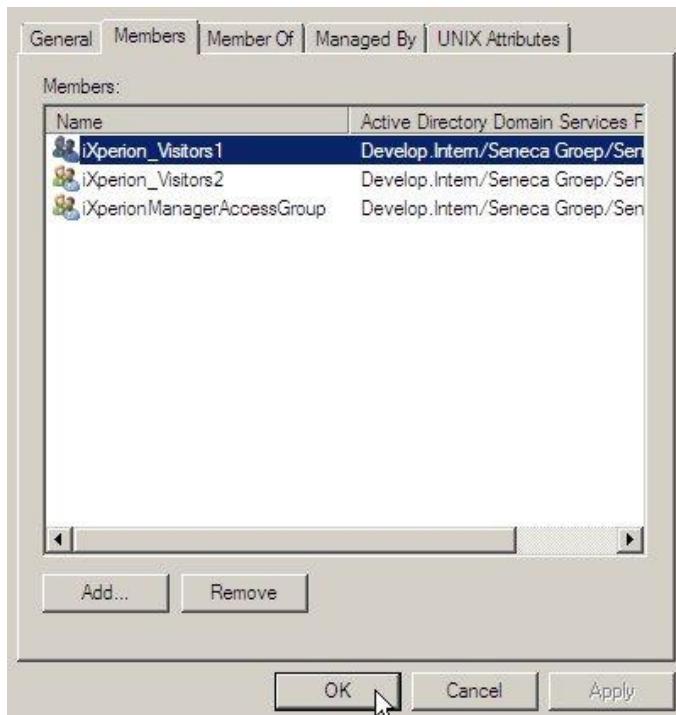


Aanmaken van een Domain Local Security Group op het domein.

1. Smartsite iXperion Access Group

In principe dienen **alle** te gebruiken AD Global Security Groups die in Smartsite worden aangemaakt te worden toegevoegd aan de Smartsite Access Group. Zoals de naam al zelf aangeeft, moet je lid zijn van Global Domain groepen in deze Local Domain groep om toegang te krijgen tot de Smartsite site voor zowel de front-end als de back-end. De naam groepsnaam van de Smartsite iXperion Access Group op het AD, kun je opgeven in de Web.config van de site in de *Smartsite.ActiveDirectoryConfiguration/settings* of *Smartsite.LDAPConfiguration/settings* sectie. (Zie voorbeeld web.config in de volgende paragraaf).

Implementatiehandleiding Active Directory voor Smartsite iXperion



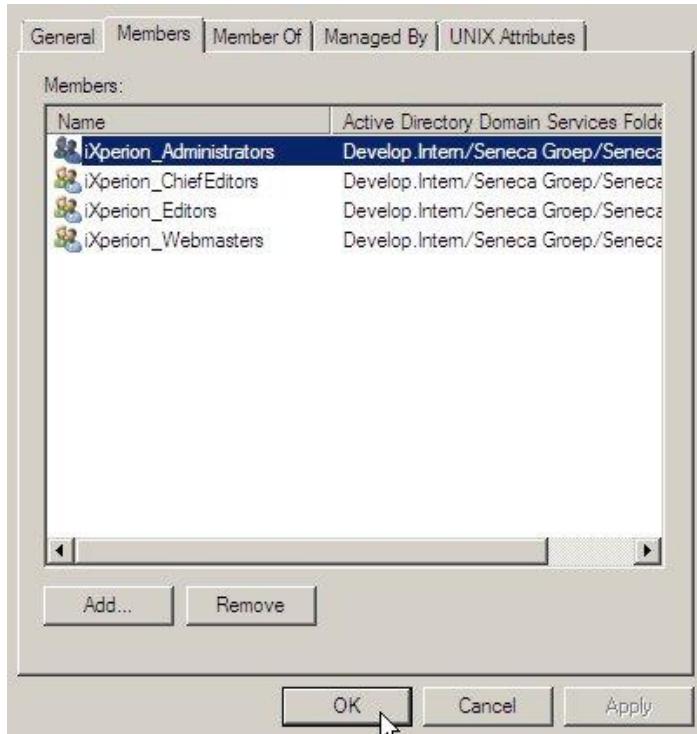
Smartsite iXperion Access Group met Vistor en Smartsite iXperion Manager Access Group.

Alle groepen die in Smartsite gemapt worden dienen te worden toegevoegd aan de Smartsite iXperion Access Group. Dit is eenvoudig te verwezenlijken door alle visitorgroepen en de local domein Smartsite iXperion Manager Access Group toe te voegen (zie figuur hierboven).

2. Smartsite iXperion Manager Access Group

De Smartsite iXperion Manager Access Group op het AD is in principe een filter op de Smartsite iXperion Access Group. Wanneer je via een Global Group lid bent van de Manager Access Group kun je in de Smartsite Manager inloggen. Afhankelijk van de rol(len) die zijn toegekend aan de groepen waarvan je lid bent, kun je verschillende acties uitvoeren en rechten toegedeeld krijgen. In de Manager Access Group dienen alle Global Domain Groups te worden geplaatst die gemapt zijn in Smartsite met uitzondering van de gemapte visitorgroepen.

Implementatiehandleiding Active Directory voor Smartsite iXperion



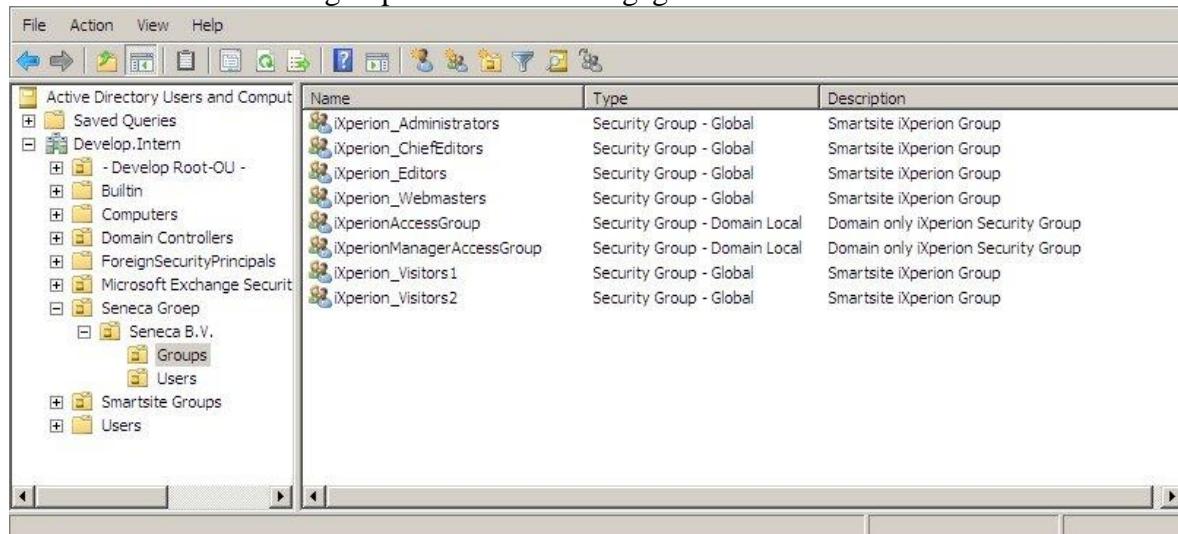
Net als bij de SmartsiteAccessGroup kun je de naam opgegeven voor de ManagerAccessGroup in de Web.config van de site in de *Smartsite.ActiveDirectoryConfiguration/settings* of *Smartsite.LDAPConfiguration/settings* sectie. De groepsnaam opgegeven op het domein neem je over in de value in de web.config (zie voorbeeld hieronder).

Web.config

```
<Smartsite.ActiveDirectoryConfiguration>
  <settings>
    <add name="SmartsiteAccessGroup" value="Smartsite access group" />
    <add name="ManagerAccessGroup" value="Manager access group" />
    <add name="StoreFullyQualifiedLoginName" value="false" />
    <add name="DatabaseId" value="e.g. DB_EmptySix" />
    <add name="SearchBase" value="e.g. cn=Users,dc=...,dc=..." />
  </settings>
  <membershipMappings>
    <add name="mm1" domain="your domain" providerName="ads" />
  </membershipMappings>
</Smartsite.ActiveDirectoryConfiguration>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

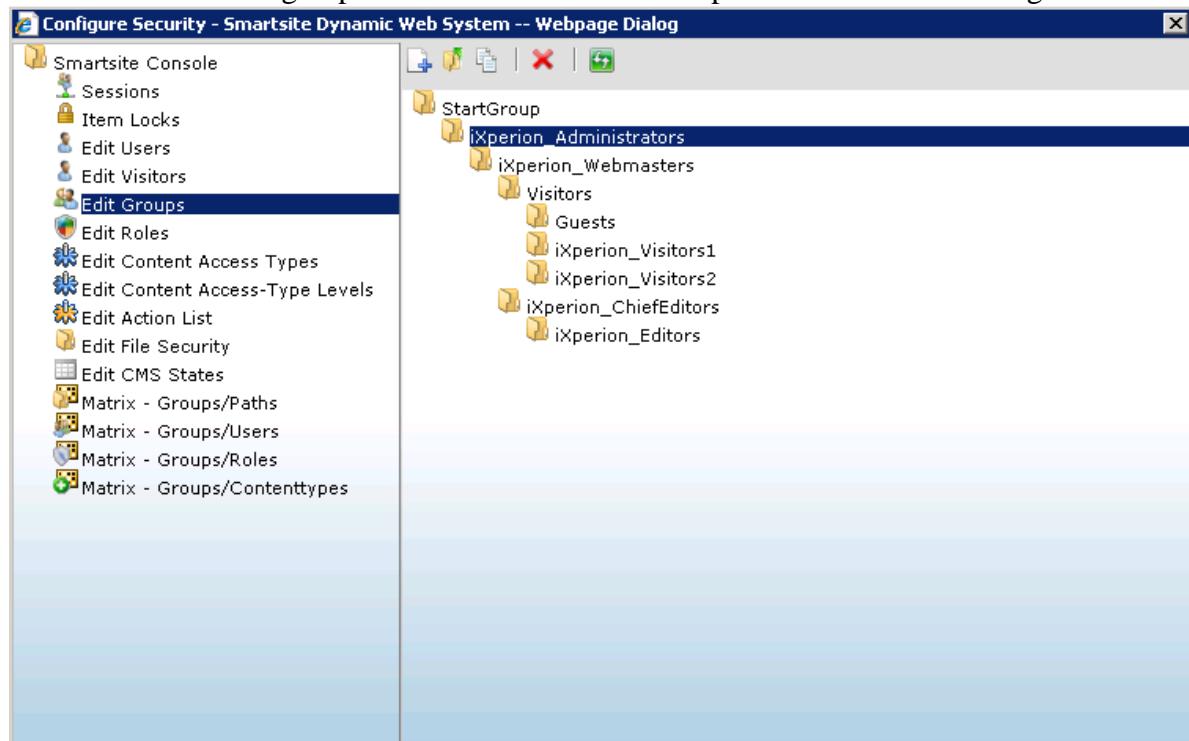
Hieronder een voorbeeld van de Active Directory Organizational Unit (OU) “Groups” op het AD. Hieronder is de groepen-structuur weergegeven.



Name	Type	Description
iXperion_Administrators	Security Group - Global	Smartsite iXperion Group
iXperion_ChiefEditors	Security Group - Global	Smartsite iXperion Group
iXperion_Editors	Security Group - Global	Smartsite iXperion Group
iXperion_Webmasters	Security Group - Global	Smartsite iXperion Group
iXperionAccessGroup	Security Group - Domain Local	Domain only iXperion Security Group
iXperionManagerAccessGroup	Security Group - Domain Local	Domain only iXperion Security Group
iXperion_Visitors1	Security Group - Global	Smartsite iXperion Group
iXperion_Visitors2	Security Group - Global	Smartsite iXperion Group

De iXperionAccessGroup en de iXperionManagerAccessGroup zijn Local domain groepen.

De overeenkomende groepen-structuur in Smartsite iXperion ziet er dan als volgt uit.



The screenshot shows the 'Edit Groups' section of the Smartsite console. On the left is a navigation tree with items like Sessions, Item Locks, Edit Users, Edit Visitors, Edit Groups (which is selected), Edit Roles, etc. On the right is a tree view of groups:

- StartGroup
 - iXperion_Administrators
 - iXperion_Webmasters
 - Visitors
 - Guests
 - iXperion_Visitors1
 - iXperion_Visitors2
 - iXperion_ChiefEditors
 - iXperion_Editors

Overzicht groepen structuur in Smartsite Edit Groups.

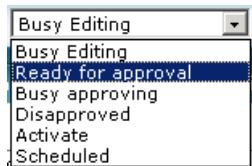
Implementatiehandleiding Active Directory voor Smartsite iXperion

⚠ Let op: De Guests groep hoeft niet te worden gedefinieerd op het domein.

Implementatiehandleiding Active Directory voor Smartsite iXperion

Parent groep

⚠ Let op: Doordat in de Smartsite iXperion de parent-groep van de ingelogde gebruiker wordt gebruikt in het workflow management (ready for approval), dient de groepsstructuur altijd hiërarchisch **aaneengesloten** te zijn voor de redactie groepen.



Smartsite iXperion workflow.

In bovenstaand voorbeeld ziet de aaneengesloten groepsstructuur er als volgt uit:

- iXperion_Administors
 - iXperion_Webmasters
 - iXperion_ChiefEditors
 - iXperion_Editors

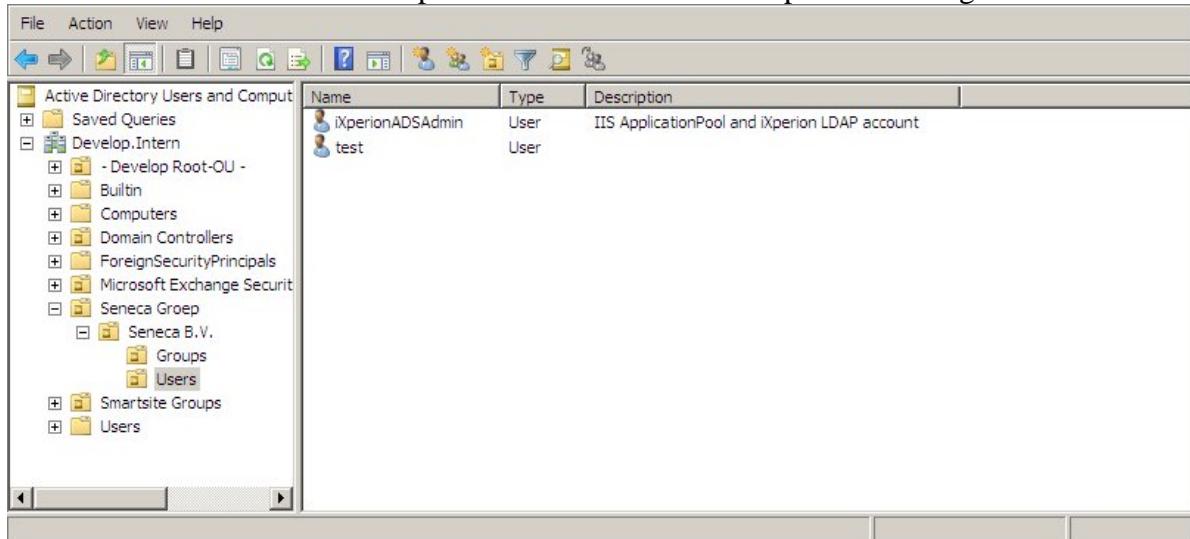
⚠ Let op: Alle groepen dienen “externally managed” te hebben aanstaan!

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.4 LDAP/AD logon user en het IIS website Application Pool account

Om Smartsite iXperion toegang te verschaffen tot de Active Directory informatie, zoals de users en groepen, dient er een account te zijn die deze informatie mag uitlezen.

Standaard wordt hiervoor het iXperionADSAdmin account op het domein gedefinieerd.



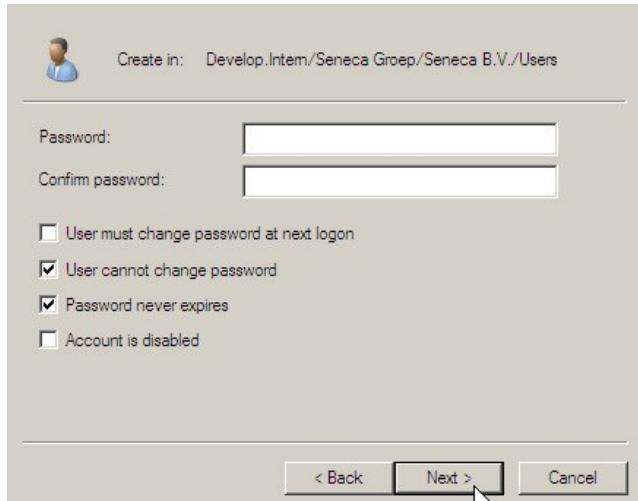
The screenshot shows the Windows Active Directory Users and Computers snap-in. The left pane displays the organizational structure of the domain, including 'Active Directory Users and Compute', 'Saved Queries', and several OUs like 'Develop.Intern', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Microsoft Exchange Securit', and 'Seneca Groep'. The 'Seneca Groep' OU contains 'Seneca B.V.', which further contains 'Groups' and 'Users'. The right pane is a table showing two users:

Name	Type	Description
iXperionADSAdmin	User	IIS ApplicationPool and iXperion LDAP account
test	User	

Het iXperionADSAdmin account wordt opgegeven in de web.config van de site zodat Smartsite over de benodigde logingegevens beschikt.

Het iXperionADSAdmin account dat op het AD wordt aangemaakt dient niet te verlopen (locked-out) omdat de application pools altijd aanwezig dienen te zijn (Service-account). Daarnaast is het niet raadzaam het password te vervangen. Kies daarom een lang password van minimaal 14 tekens (MD5-strong).

Implementatiehandleiding Active Directory voor Smartsite iXperion



Check "User cannot change password" en "Password never expires"

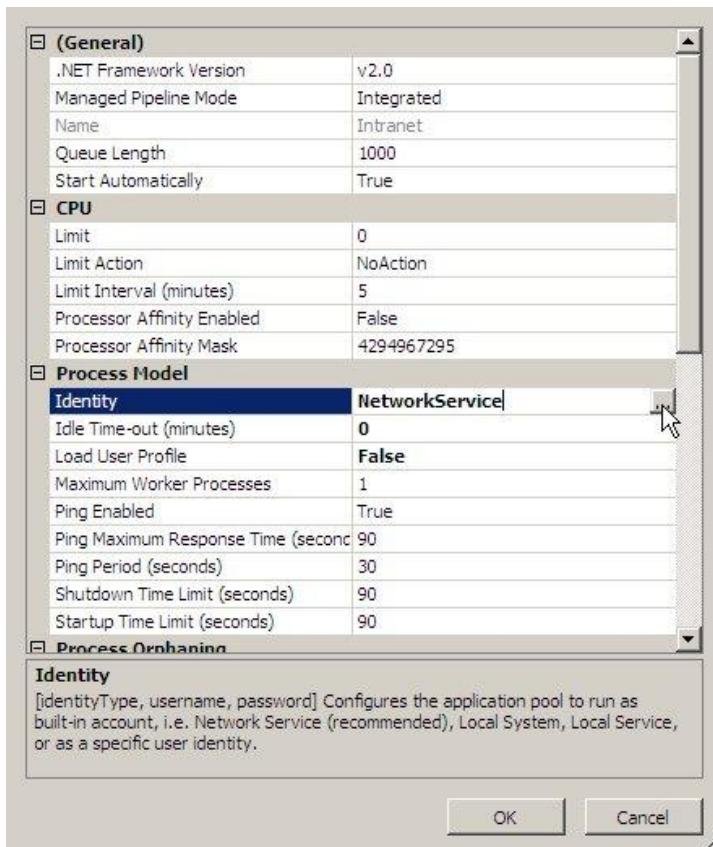
6.4.1 Optioneel: Wijzigen Application pool account



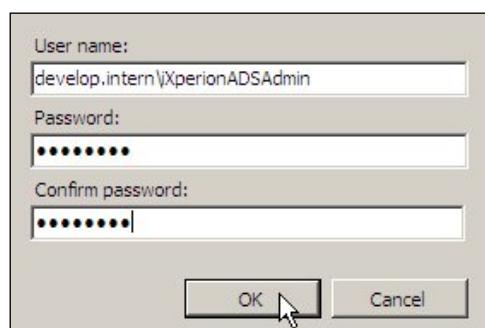
Tip: In principe is het mogelijk de application pools onder het Domain account iXperionADSAmin te laten draaien. Om de configuratie eenvoudig te houden wordt sterk geadviseerd voor de Applications pools het **Network Service account** te gebruiken!

Mocht men toch besluiten een domein account te gebruiken voor de IIS application pool, dan gaat het wijzigen van het application pool account in IIS als volgt:

Implementatiehandleiding Active Directory voor Smartsite iXperion

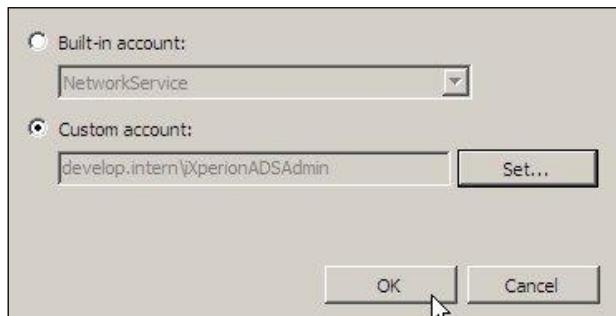


Selecteer de site (of de CMS virtuele directory) en klik de Advanced settings
 Onder het kopje “Process Model” en selecteer Identity.



Vul het domein account en password in.

Implementatiehandleiding Active Directory voor Smartsite iXperion

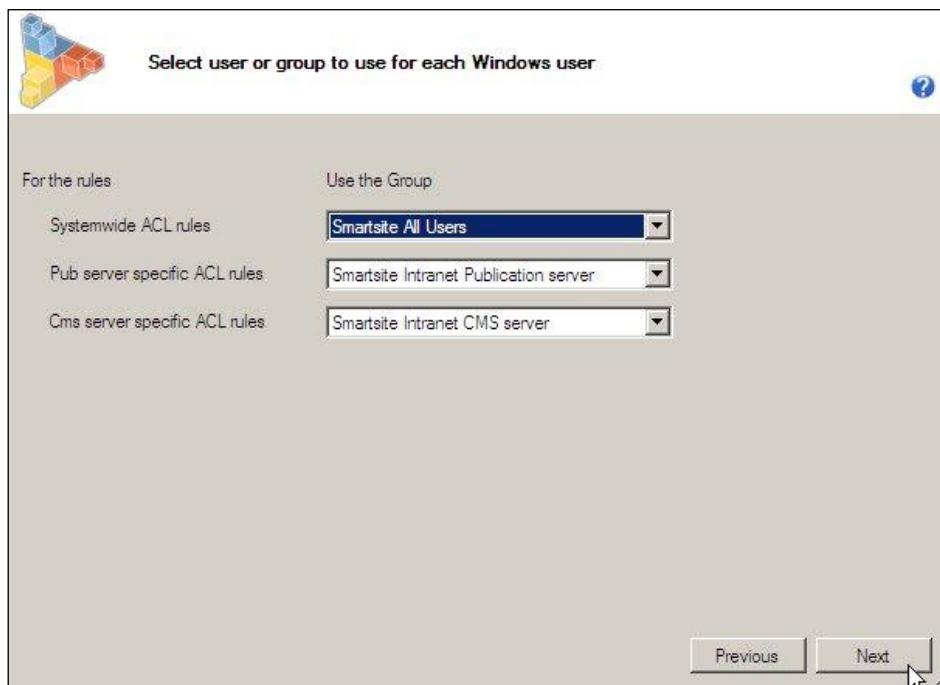


Wijzig het account naar het AD account iXperionADSAdmin.

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.5 Set Site Security Wizard

Via het Smartsite iXperion Windows menu of via de Smartsite ConfigEditor dient na het wijzigen van het account opnieuw de security te worden gezet. Stop IIS voordat de wizard wordt uitgevoerd via IISReset /stop.



Na het zetten van de security is het Application Pool account(s) automatisch toegevoegd aan de lokale NT groepen:

- Performance Monitor Users
- IIS_IUSRS
- Smartsite All Users
- Smartsite {sitename} CMS Server
- Smartsite {sitename} Publication server

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.6 Web.config koppeling met 1 domein

⚠ Let op: Gebruik altijd het web.config bestand dat wordt meegeleverde in de Emptysix site!

De Web.config wordt gebruikt voor zowel de front-end als de back-end (CMS) configuratie. Hieronder staat een standaard web.config voor de AD koppeling met de Active Directory (DEVELOP-INT/DEVELOP.INTERN). De onderdelen die moeten worden gewijzigd of worden toegevoegd t.o.v. de standaard Web.config zijn gemarkerd.

Voorbeeld:

```
<?xml version="1.0" encoding="utf-8"?>
<!--
Note: As an alternative to hand editing this file you can use the
web admin tool to configure settings for your application. Use
the Website->Asp.Net Configuration option in Visual Studio.
A full list of settings and comments can be found in
machine.config.comments usually located in
\Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
  <configSections>
    <!-- ADS SETTING DEFINE ActiveDirectoryConfiguration ENTRY -->
    <section name="Smartsite.ConfigurationSource"
type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.ConfigurationSourceSection,
Smartsite.Diagnostics.Logging, Version=1.0.0.0, Culture=neutral, PublicKeyToken=5fdb12a67e027fb6"
/>
    <section name="Smartsite.ActiveDirectoryConfiguration"
type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security" />
  </configSections>
  <connectionStrings>
    <!-- ADS SETTING Connection string must be UPPERCASE -->
    <add name="ActiveDirectoryConnection" connectionString="LDAP://DEVELOP.INTERN" />
  </connectionStrings>
  <!-- ADS SETTING Smartsite ActiveDirectory Configuration Groups -->
  <Smartsite.ActiveDirectoryConfiguration>
    <settings>
      <add name="SmartsiteAccessGroup" value="iXperionAccessGroup" />
      <add name="ManagerAccessGroup" value="iXperionManagerAccessGroup" />
      <add name="StoreFullyQualifiedLoginName" value="False" />
      <add name="SearchBase" value="dc=develop,dc=intern" />
      <add name="DatabaseId" value="manager" />
      <!-- settings below as of iXperion 1.4+ ; built-in default values shown as example -->
      <add name="ObtainPrimaryGroup" value="true" />
      <add name="ObtainParentGroupsForPrimaryGroup" value="true" />
      <add name="MaxParentGroupRecursionDepth" value="0" />
    </settings>
  </Smartsite.ActiveDirectoryConfiguration>
</configuration>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<add name="UpdatePrimaryGroup" value="true" />
</settings>
<membershipMappings>
    <!-- ADS SETTING DEFAULT DOMAIN SHOULD BE MENTIONED FIRST -->
    <add name="mm1" domain="DEVELOP-INT" providerName="ADMembershipProvider" />
    <add name="mm2" domain="DEVELOP.INTERN" providerName="ADMembershipProvider" />
</membershipMappings>
</Smartsite.ActiveDirectoryConfiguration>
<appSettings />
<system.web>
    <pages>
        <controls>
            <add tagPrefix="cms" assembly="Smartsite.AspNet.Bridge"
namespace="Smartsite.AspNet.Bridge" />
        </controls>
    </pages>
    <!--
        Set compilation debug="true" to insert debugging
        symbols into the compiled page. Because this
        affects performance, set this value to true only
        during development.
    -->
    <globalization fileEncoding="utf-8" />
    <compilation debug="False">
        <assemblies>
            <clear />
        </assemblies>
    </compilation>
    <machineKey
validationKey="BAE0B6B7179DDB95D3B407E90A8D6F9CFA4EE21FDC1CF8B3635D6B28D83A3D448BE
2427FC6C9B458E58DA3C0DC4515C13E938D9AB704139CD91A1E109C800D00"
decryptionKey="C4725BC47252B4ABFA80A832DD891E9C74D0FF482A6A362C" validation="SHA1" />
    <!--authentication mode="Windows"-->
    <!--identity impersonate="true"-->
    <!--
        The <authentication> section enables configuration
        of the security authentication mode used by
        ASP.NET to identify an incoming user.
    -->
    <!-- ADS SETTING Front-end authentication mode integrated security and Explicit REMOVE Forms
Login -->
    <authentication mode="Windows">
        <!-- <forms loginUrl="/Login" name="Smartsite" / -->
    </authentication>
    <authorization>
        <allow users="*" />
    </authorization>
    <!-- ADS SETTING defaultProvider="ADMembershipProvider" -->
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<membership defaultProvider="ADMembershipProvider" userIsOnlineTimeWindow="15">
    <providers>
        <clear />
        <!-- ADS SETTING CHANGE connectionUsername and connectionPassword. Use user principal
name (username@domainname) syntax -->
        <add applicationName="Smartsite" name="ADMembershipProvider"
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider, Smartsite.Security"
connectionStringName="ActiveDirectoryConnection"
connectionUsername="iXperionADSadmin@Develop.intern" connectionPassword="*****" />
        <add applicationName="Smartsite" name="SqlMembershipProvider"
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"
enablePasswordRetrieval="true" enablePasswordReset="true" passwordFormat="Clear"
requiresQuestionAndAnswer="false" writeExceptionsToEventLog="true" />
    </providers>
</membership>
<!-- ADS SETTING SET defaultProvider="ADRoleProvider" -->
<roleManager defaultProvider="ADRoleProvider" enabled="true" cacheRolesInCookie="true"
cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/" cookieRequireSSL="false"
cookieSlidingExpiration="true" cookieProtection="All">
    <providers>
        <clear />
        <add name="ADRoleProvider" applicationName="Smartsite"
type="Smartsite.Security.Authorization.ActiveDirectoryRoleProvider, Smartsite.Security"
connectionStringName="ActiveDirectoryConnection" writeExceptionsToEventLog="true" />
        <add applicationName="Smartsite" name="SqlRoleProvider"
type="Smartsite.Security.Authorization.SqlRoleProvider, Smartsite.Security"
connectionStringName="SmartsiteDbConnection" writeExceptionsToEventLog="false" />
    </providers>
</roleManager>
<!--
    The <customErrors> section enables configuration
    of what to do if/when an unhandled error occurs
    during the execution of a request. Specifically,
    it enables developers to configure html error pages
    to be displayed in place of a error stack trace.
-->
<customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">
    <error statusCode="403" redirect="NoAccess.htm" />
    <error statusCode="404" redirect="NotFound.htm" />
</customErrors>
-->
<identity impersonate="false" />
<httpModules>
    <!-- replace default FormsAuthentication with Smartsite one -->
    <remove name="FormsAuthentication" />
    <!--add name="FormsAuthentication"
type="Smartsite.AspNet.Bridge.CmsFormsAuthenticationModule,Smartsite.AspNet.Bridge" /-->
    <!--add name="ScriptModule" type="System.Web.Handlers.ScriptModule, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" /-->
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<add type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge" name="ixbridge" />
<add type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor"
name="ImageServer" />
<add type="Smartsite.Pdf.PdfModule,Smartsite.Pdf" name="PdfModule" />
<add name="ManagementInformation" type="Smartsite.ManagementInformation.SmiClient,
Smartsite.ManagementInformation" />
</httpModules>
<httpHandlers>
<add verb="*" path="*.asmx" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
<add verb="*" path="*_AppService.axd" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
<add verb="GET,HEAD" path="ScriptResource.axd"
type="System.Web.Handlers.ScriptResourceHandler, System.Web.Extensions, Version=1.0.61025.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35" validate="false" />
<add verb="*" path="*/*.{net}" type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge"
/>
<add path="/res/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" />
<add path="/res/*/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" />
</httpHandlers>
<anonymousIdentification enabled="true" />
<profile enabled="true" automaticSaveEnabled="true" defaultProvider="SmartsiteProfileProvider"
inherits="Smartsite.Core.PersonalProfile, Smartsite.Runtime">
<providers>
<clear />
<add name="SmartsiteProfileProvider" type="Smartsite.Core.ProfileProvider, Smartsite.Runtime"
ApplicationName="Smartsite" ApplicationGUID="7D95D073-2F92-4822-8C59-FC2DA67FB9A1" />
</providers>
</profile>
</system.web>
<!-- cms virtual directory configuration (manager configuration) --&gt;
&lt;!--
    to test if the manager uses the configured HttpHandler as described below,
    run the following script from the Immediate Window in the manager:
    ?Context.var(13,"hosttype")
    Result should be: Smartsite.Interop
--&gt;
&lt;location path="Members"&gt;
&lt;system.web&gt;
&lt;authorization&gt;
&lt;deny users="?" /&gt;
&lt;/authorization&gt;
&lt;/system.web&gt;
&lt;/location&gt;
&lt;Smartsite.ConfigurationSource selectedSource="File Configuration Source"&gt;</pre>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<sources>
    <add name="File Configuration Source"
type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.FileConfigurationSource,
Smartsite.Diagnostics.Logging, Version=1.0.0.0, Culture=neutral, PublicKeyToken=5fdb12a67e027fb6"
filePath="..../Smartsite.Logging.Config" />
</sources>
</Smartsite.ConfigurationSource>
<!-- WCF services configuration -->
<!-- this is a minimal set of endpoints, for example the mex endpoints have been removed -->
<system.serviceModel>
    <services>
        <!--Service for state synchronization between CMS and iXperion publication engine-->
        <service name="Smartsite.Core.Services.StateSyncService"
behaviorConfiguration="StateSyncServiceBehavior">
            <endpoint address="net.pipe://localhost/intranet/StateSyncService"
binding="netNamedPipeBinding" contract="Smartsite.Core.Services.IStateSyncService" />
        </service>
        <!--Service providing interoperability between the manager and iXperion functionality. Used for
rendering items (view & preview within the manager), AIM rendering, content validation, etc.-->
        <service name="Smartsite.Core.Services.InteropService"
behaviorConfiguration="InteropServiceBehavior">
            <endpoint address="net.pipe://localhost/intranet/InteropService"
binding="netNamedPipeBinding" bindingConfiguration="InteropServiceBinding"
contract="Smartsite.Core.Services.IInteropService" />
        </service>
        <!--Service providing schema information to the SXML editor-->
        <service name="Smartsite.Core.Services.SchemaService"
behaviorConfiguration="SchemaServiceBehavior">
            <endpoint address="http://Intranet/intranet/SchemaService" binding="basicHttpBinding"
bindingConfiguration="SchemaServiceBinding" contract="Smartsite.Core.Services.ISchemaService" />
        </service>
        <!--Service for state synchronization between iXperion publication engine and subscribers to this
service.-->
        <service name="Smartsite.Core.Services.EventSynchronizationService"
behaviorConfiguration="EventSynchronizationServiceBehavior">
            <endpoint address="http://intranet/intranet/EventSynchronizationService"
binding="wsDualHttpBinding" contract="Smartsite.Core.Services.IEventSubscriptionContract" />
        </service>
        <!--Common service for managing CMS-->
        <service name="Smartsite.Core.Services.ManagerService"
behaviorConfiguration="ManagerServiceBehavior">
            <endpoint address="http://intranet/intranet/ManagerService" binding="basicHttpBinding"
contract="Smartsite.Core.Services.IManagerService" />
        </service>
    </services>
    <bindings>
        <netNamedPipeBinding>
<binding name="InteropServiceBinding" maxReceivedMessageSize="1048576"><readerQuotas
maxStringContentLength="1048576" /></binding>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</netNamedPipeBinding>
<wsHttpBinding>
<binding name="wsHttpBindingConfig"><readerQuotas maxStringContentLength="32768"
/></binding>
<binding name="HitServiceBinding" maxReceivedMessageSize="100000000"><readerQuotas
maxStringContentLength="524288" /></binding>
</wsHttpBinding>
<basicHttpBinding>
<binding name="cmsWebserviceSoapBinding"><readerQuotas maxStringContentLength="16384"
/><security mode="TransportCredentialOnly"><transport clientCredentialType="Basic"
proxyCredentialType="None" realm="" /><message clientCredentialType="UserName"
algorithmSuite="Default" /></security></binding>
<binding name="SchemaServiceBinding"><readerQuotas maxStringContentLength="32768"
/></binding>
</basicHttpBinding>
<wsDualHttpBinding>
<binding name="WSDualHttpBinding_EventSubscriptionService"><readerQuotas
maxStringContentLength="16384" /><reliableSession ordered="true" inactivityTimeout="08:00:00"
/><security mode="Message"><message clientCredentialType="Windows"
negotiateServiceCredential="true" algorithmSuite="Default" /></security></binding>
</wsDualHttpBinding>
</bindings>
<!-- client section, only used when running the TestSuite -->
<client>
<!-- (client) endpoint definition used for connecting to the cmsWebservice -->
<endpoint address="http://intranet/cms/manager.dws" binding="basicHttpBinding"
bindingConfiguration="cmsWebserviceSoapBinding" contract="cmsWebserviceSoapPort"
name="cmsWebserviceSoapPort" />
<!-- (client) endpoint definition used for connecting to the EventSubscription/EventSynchronization
service -->
<endpoint address="http://intranet/intranet/EventSynchronizationService"
binding="wsDualHttpBinding" bindingConfiguration="WSDualHttpBinding_EventSubscriptionService"
contract="Smartsite.Core.EventSynchronizationClient.EventSubscriptionService"
name="WSDualHttpBinding_EventSubscriptionService">
</endpoint>
<endpoint address="http://192.168.252.7:2020/Intranet/HitService"
behaviorConfiguration="HitServiceBehavior" binding="wsHttpBinding"
bindingConfiguration="HitServiceBinding"
contract="Smartsite.ManagementInformation.Server.HitService" />
</client>
<!-- Uncomment diagnostics section to log the entire messages to the trace-log -->
<!--
<diagnostics wmiProviderEnabled="true">
    <messageLogging
        logEntireMessage="true"
        logMalformedMessages="true"
        logMessagesAtServiceLevel="true"
        logMessagesAtTransportLevel="true"
        maxMessagesToLog="3000"
    </diagnostics>
-->
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
>
  />
</diagnostics>
-->

<behaviors>
  <serviceBehaviors>
    <behavior name="StateSyncServiceBehavior" />
    <behavior name="InteropServiceBehavior" />
    <behavior name="SchemaServiceBehavior" />
    <behavior name="EventSynchronizationServiceBehavior" />
    <behavior name="ManagerServiceBehavior" />
  </serviceBehaviors>
  <endpointBehaviors>
    <behavior name="HitServiceBehavior">
      <dataContractSerializer maxItemsInObjectGraph="10000000" />
    </behavior>
  </endpointBehaviors>
</behaviors>
</system.serviceModel>
<!-- Uncomment system.diagnostics section to enable trace-logging -->
<system.diagnostics>
  <trace autoflush="true" />
  <sources>
    <source name="System.ServiceModel" switchValue="Error">
      <listeners>
        <add name="traceListener" />
      </listeners>
    </source>
    <source name="System.ServiceModel.MessageLogging">
      <listeners>
        <add name="traceListener" />
      </listeners>
    </source>
  </sources>
  <sharedListeners>
    <add name="traceListener" type="System.Diagnostics.XmlWriterTraceListener, System,
Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
initializeData="E:\Sites\Intranet\LogFiles\WCF\Intranet.svclog" />
  </sharedListeners>
</system.diagnostics>
<system.webServer>
  <modules>
    <add name="ixbridge" type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge"
preCondition="" />
    <add name="ImageServer"
type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor" preCondition="" />
    <add name="PdfModule" type="Smartsite.Pdf.PdfModule,Smartsite.Pdf" preCondition="" />
    <!-- update session module with modified preCondition -->
    <remove name="Session" />
    <add name="Session" type="System.Web.SessionState.SessionStateModule" preCondition="" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<!-- replace ASP.NET Forms Authentication with custom Smartsite one -->
<remove name="FormsAuthentication" />
<!--add name="FormsAuthentication"
type="Smartsite.AspNet.Bridge.CmsFormsAuthenticationModule,Smartsite.AspNet.Bridge"
preCondition="" /-->
    <remove name="Profile" />
    <add name="Profile" type="System.Web.Profile.ProfileModule" preCondition="" />
    <remove name="AnonymousIdentification" />
    <add name="AnonymousIdentification"
type="System.Web.Security.AnonymousIdentificationModule" preCondition="" />
        <remove name="ManagementInformation" />
        <add name="ManagementInformation" type="Smartsite.ManagementInformation.SmiClient,
Smartsite.ManagementInformation" preCondition="" />
    </modules>
    <handlers>
        <add name="net" path="*.net" verb="*"
type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge" resourceType="Unspecified"
requireAccess="Script" preCondition="integratedMode,runtimeVersionv2.0" />
        <add path="/*/*.net" verb="*" type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge"
name="Bridge" preCondition="" />
        <add name="PubResourceHandler" path="/res/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" preCondition="" />
    </handlers>
    <defaultDocument>
        <files>
            <clear />
            <add value="manager.dws" />
            <add value="smartsite.net" />
        </files>
    </defaultDocument>
    <!-- Disable detection of IIS6 / Classic mode ASP.NET configuration -->
    <validation validateIntegratedModeConfiguration="false" />
</system.webServer>
<location path="cms">
    <system.web>
        <globalization requestEncoding="iso-8859-1" />
        <!-- To upload large files -->
        <httpRuntime maxRequestLength="2097151" executionTimeout="999999"
shutdownTimeout="999" requestLengthDiskThreshold="256" />
        <!-- authentication mode="None" /-->
        <!-- ADS SETTING CMS authentication mode integrated security -->
        <authentication mode="Windows" />
        <authorization>
            <allow users="*" />
            <!-- allow access for all users, the manager uses it's own implementation for authenticating users
-->
        </authorization>
        <httpModules>
            <remove name="FormsAuthentication" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</httpModules>
<httpHandlers>
    <!--clear the inherited httpHandlers-->
    <clear />
    <!-- uncomment the WebserviceHandler entry when the site participates within an Outscaling
scenario -->
    <!-- <add verb="*" path="/cms/webservice.dws"
type="Smartsite.Interop.IIS.WebserviceHandler,Smartsite.Interop" /> -->
    <add verb="*" path="/cms/*.dws" type="Smartsite.Interop.Handler,Smartsite.Interop" />
</httpHandlers>
<compilation>
    <assemblies>
        <clear />
    </assemblies>
</compilation>
</system.web>
<!-- IIS 7.0+ configuration -->
<system.webServer>
    <modules>
        <remove name="FormsAuthentication" />
        <remove name="ixbridge" />
        <remove name="ImageServer" />
        <remove name="PdfModule" />
    </modules>
    <handlers>
        <remove name="Bridge" />
        <remove name="res1" />
        <remove name="res2" />
        <remove name="net" />
        <remove name="PubResourceHandler" />
        <add name="CMSInteropHandler" path="/cms/*.dws" verb="*"
type="Smartsite.Interop.IIS.Handler,Smartsite.Interop" preCondition="" />
    </handlers>
    <security>
        <requestFiltering>
            <requestLimits maxAllowedContentLength="204800000" />
        </requestFiltering>
    </security>
    <defaultDocument>
        <files>
            <clear />
            <add value="manager.dws" />
        </files>
    </defaultDocument>
    <!-- Disable detection of IIS6 / Classic mode ASP.NET configuration -->
    <validation validateIntegratedModeConfiguration="false" />
</system.webServer>
</location>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</configuration>
```

Forms Authentication dient explicet te worden verwijderd om de Smartsite manager juist te laten werken.

6.6.1 ConfigSections

Declareer de nieuwe Smartsite.ActiveDirectoryConfiguration sectie in de configSections.

```
<configSections>
    <!-- ADS SETTING DEFINE ActiveDirectoryConfiguration ENTRY -->
    <section name="Smartsite.ActiveDirectoryConfiguration"
        type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security" />
```

6.6.2 ConnectionStrings

In de Configuration.ConnectionStrings sectie in de web.config dient het Active Directory pad te worden opgegeven. Dit dient conform de LDAP standaard in hoofdletters tekst te worden opgegeven.

```
<connectionStrings>
    <!-- ADS SETTING Connection string must be UPPERCASE -->
    <add name="ActiveDirectoryConnection" connectionString="LDAP://DEVELOP-INT" />
</connectionStrings>
```

6.6.3 Smartsite.ActiveDirectoryConfiguration

```
<Smartsite.ActiveDirectoryConfiguration>
    <settings>
        <add name="SmartsiteAccessGroup" value="iXperionAccessGroup" />
        <add name="ManagerAccessGroup" value="iXperionManagerAccessGroup" />
        <add name="StoreFullyQualifiedLoginName" value="false" />
        <add name="DatabaseId" value="manager" />
        <add name="SearchBase" value="dc=develop,dc=intern" />
        <!-- settings below as of iXperion 1.4+ ; built-in default values shown as
example -->
        <add name="ObtainPrimaryGroup" value="true" />
        <add name="ObtainParentGroupsForPrimaryGroup" value="true" />
        <add name="MaxParentGroupRecursionDepth" value="0" />
        <add name="UpdatePrimaryGroup" value="true" />
    </settings>
    <membershipMappings>
        <add name="mm1" domain="DEVELOP-INT" providerName="ads" />
        <add name="mm2" domain="DEVELOP.INTERN" providerName="ads" />
    </membershipMappings>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</Smartsite.ActiveDirectoryConfiguration>
```

6.6.3.1 SmartsiteAccessGroup en ManagerAccessGroup

In de Smartsite.ActiveDirectoryConfiguration sectie dienen beiden Local Domain Groups, SmartsiteAccessGroup en de ManagerAccessGroup te worden opgegeven. De opgegeven waarden (values) dienen gelijk te zijn aan die groepsnamen gedefinieerd op het domein.

6.6.3.2 StoreFullyQualifiedLoginName

Wanneer deze waarde true is, dan wordt de “fully qualified user name (user@domain) in de AllUsers table geplaatst wanneer de gebruiker met succes inlogt in Smartsite.

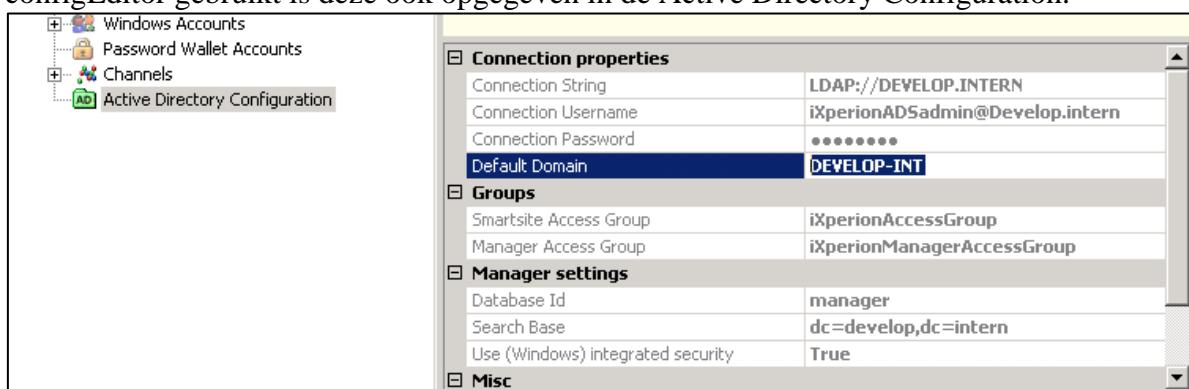
In de meeste gevallen zal bij het gebruik van 1 domein voor

StoreFullyQualifiedLoginName" value="false" worden gekozen. Zo werken bijvoorbeeld smoelenboek applicaties met de naam van de gebruiker zonder de domeinnaam.

De volgorde waarin de domeinen worden opgegeven in de web.config is belangrijk:

```
<add name="mm1" domain="DEVELOP-INT" providerName="ads" />
<add name="mm2" domain="DEVELOP.INTERN" providerName="ads" />
```

Het eerst genoemde domein is het zogeheten “Default Domain”. Wanneer je de Smartsite configEditor gebruikt is deze ook opgegeven in de Active Directory Configuration.

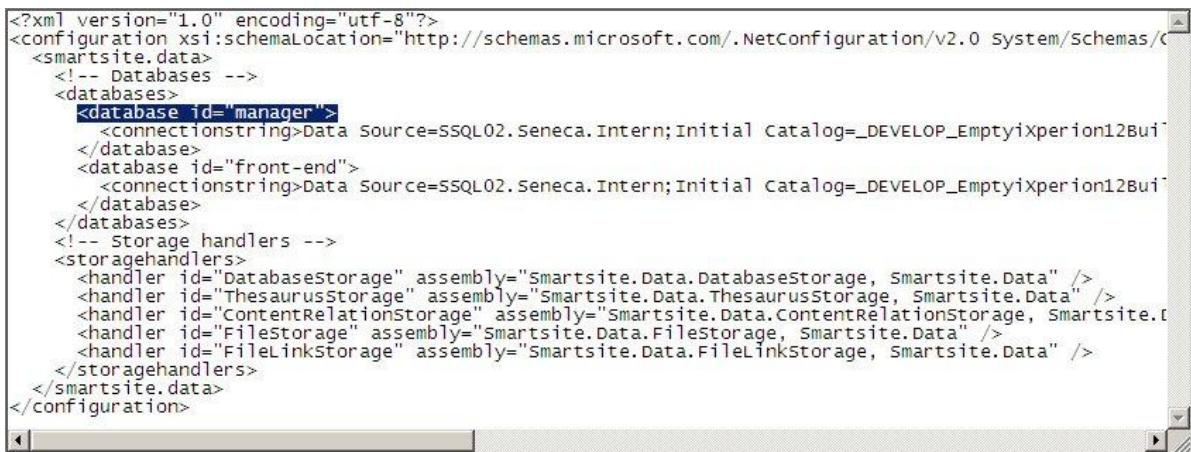


Wanneer een gebruiker inlogt met naam@DEVELOP-INT zal het Default Domain er worden afgesneden en alleen de naam worden toegevoegd aan de Alluser tabel.

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.6.3.3 Databased

Het DatabaseId dient gelijk te zijn en te verwijzen naar de database connectionstring in de Smartsite.Data.config voor de Back-end.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration xsi:schemaLocation="http://schemas.microsoft.com/.NetConfiguration/v2.0 System/Schemas/c
<smartsite.data>
  <!-- Databases -->
  <databases>
    <database id="manager">
      <connectionstring>Data Source=SSQL02.Seneca.Intern;Initial catalog=_DEVELOP_Emptyixperion12Bu1</connectionstring>
    </database>
    <database id="front-end">
      <connectionstring>Data Source=SSQL02.Seneca.Intern;Initial catalog=_DEVELOP_Emptyixperion12Bu1</connectionstring>
    </database>
  </databases>
  <!-- Storage handlers -->
  <storagehandlers>
    <handler id="DatabaseStorage" assembly="Smartsite.Data.DatabaseStorage, Smartsite.Data" />
    <handler id="ThesaurusStorage" assembly="Smartsite.Data.ThesaurusStorage, Smartsite.Data" />
    <handler id="ContentRelationStorage" assembly="Smartsite.Data.ContentRelationStorage, Smartsite.Data" />
    <handler id="FileStorage" assembly="Smartsite.Data.FileStorage, Smartsite.Data" />
    <handler id="FileLinkStorage" assembly="Smartsite.Data.FileLinkStorage, Smartsite.Data" />
  </storagehandlers>
</smartsite.data>
</configuration>
```

6.6.3.4 SearchBase

In de SearchBase parameter kun je de distinguishedName opgeven van het domein, organizational unit of groep waarvan de gebruikers die in Smartsite inloggen lid zijn. In veel gevallen zullen de gebruikers over het gehele domein verspreid staan en is de parameter vaak gelijk aan de domein distinguishedName (dc=develop, dc=intern).

Syntax:

O={Organisation};ou={naam OU};dc={Prefix-domein};dc={Suffix-domein}

6.6.3.5 ObtainPrimaryGroup

(iXperion 1.4 en hoger, default=true)

Wanneer de parameter ObtainPrimaryGroup de waarde true heeft haalt Smartsite apart de primary group van de in te loggen gebruiker op. Dit is standaard de Domain Users groep, maar kan afhankelijk van het domein beleid ook een andere groep zijn.

Wanneer Smartsite iXperion gebruik maakt van “Mixed Mode Security” wordt de Domain Users groep standaard toegevoegd aan de boven genoemde ManagerAccessGroup. In dat geval dient ObtainPrimaryGroup de waarde true te hebben.

Implementatiehandleiding Active Directory voor Smartsite iXperion

Wordt er geen gebruik gemaakt van de primary groep dan kan de waarde op false worden gezet wat het aan te op te halen groepen verminderd, en daarmee de performance ten goede komt.

6.6.3.6 ObtainParentGroupsForPrimaryGroup

(iXperion 1.4 en hoger, default=true)

Wanneer de waarde voor ObtainPrimaryGroup gelijk aan true is, kun je met de ObtainParentsGroupsForPrimaryGroup setting bepalen of recursief de Parent groeps dienen te worden opgehaald voor de ObtainPrimaryGroup.

Wordt er geen gebruik gemaakt van de Parent groepen van de primary groep dan kan de waarde op false worden gezet wat het aan te op te halen groepen vermindert, en daarmee de performance ten goede komt.

6.6.3.7 MaxParentGroupRecursionDepth (default=0)

(iXperion 1.4 en hoger, default=0)

M.b.v. de MaxParentGroupRecursionDepth setting kan bepaald worden hoeveel groeps niveau diep/omhoog Smartsite iXperion gaat zoeken.

Wanneer alle groepen gedefinieerd in Smartsite iXperion met het “Externally Managed” vinkje aan opgehaald kunnen worden door de MaxParentGroupRecursionDepth te beperken tot enkele niveaus, dan komt dit de performance ten goede.

Default is de waarde gelijk aan 0, wat aangeeft dat er geen beperking is en alle groepen recursief worden opgehaald.

6.6.3.8 UpdatePrimaryGroup

(iXperion 1.4 en hoger, default=true)

De UpdatePrimaryGroup setting is standard true, en is geïntroduceerd voor de ondersteuning van Smartsite iXperion “Mixed Mode Security”.

Wanneer Smartsite iXperion Mixed-Mode Security wordt gebruikt is de UpdatePrimaryGroup = false setting benodigd, om te voorkomen dat de AccessGroup als primary groep wordt gekozen voor alle gebruikers.



Tip: Doordat de primary groep niet meer door Smartsite wordt gezet, kan deze na inloggen handmatig worden gewijzigd.

Implementatiehandleiding Active Directory voor Smartsite iXperion

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.6.3.9 Membershipmappings

```
<membershipMappings>
    <add name="mm1" domain="DEVELOP-INT" providerName="ads" />
    <add name="mm2" domain="DEVELOP.INTERN" providerName="ads" />
</membershipMappings>
```

In de membershipMappings sectie dient zowel de NetBios naam als de FQDN voor het domein te worden opgegeven.

⚠ Let op: Gebruik de Netbios naam als default domein (mm1).

Door de providerName hetzelfde te houden worden beiden domeinnamen gemapt aan dezelfde provider.

Voor het opvragen van de NetBios naam van de AD server die in de web.config dient te worden opgegeven kun je het volgende commando gebruiken vanaf de CMS server command-prompt

```
nbtstat -A {IPADRES DNS/AD SERVER}
```

Waarbij { IPADRES DNS/AD SERVER } het IP Adres van de DNS/AD server

6.6.4 Authentication front-end

In de sectie <system.web> dient de authentication mode Op Windows te worden gezet (Let op XML: Hoofdletter gevoelig).

```
<system.web>
    <authentication mode="Windows">
```

6.6.5 Membership Provider

In de Membership Provider sectie dienen de account gegevens te worden opgegeven van het account dat connectie maakt met het AD. In de connectionUsername dient het AD account in Principal name syntax te worden opgegeven: username@domainname
Hier geven we het op het domein aangemaakte iXperionADSadmin account op.

```
<!-- ADS SETTING defaultProvider="ads" -->
<membership defaultProvider="ads">
    <providers>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<clear />
<!-- ADS SETTING CHANGE connectionUsername and connectionPassword. Use user
principal name (username@domainname) syntax -->
<add name="ads" applicationName="Smartsite"
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider,
Smartsite.Security" attributeMapUsername="SAMAccountName"
connectionStringName="ActiveDirectoryConnection"
connectionUsername="ixperionADAdmin@Develop.intern" connectionPassword="*****" />
<add applicationName="Smartsite" name="SqlMembershipProvider"
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"
enablePasswordRetrieval="true" enablePasswordReset="true" passwordFormat="Clear"
requiresQuestionAndAnswer="false" writeExceptionsToEventLog="true" />
</providers>
</membership>
```

6.6.6 Role provider

```
<!-- ADS SETTING SET defaultProvider="adsrp" -->
<roleManager defaultProvider="adsrp" enabled="true" cacheRolesInCookie="true"
cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/" cookieRequireSSL="false"
cookieSlidingExpiration="true" cookieProtection="All">
<providers>
<clear />
<add applicationName="Smartsite" name="SqlRoleProvider"
type="Smartsite.Security.Authorization.SqlRoleProvider, Smartsite.Security"
connectionStringName="SmartsiteDbConnection" writeExceptionsToEventLog="false" />
<add applicationName="Smartsite" name="adsrp"
type="Smartsite.Security.Authorization.ActiveDirectoryRoleProvider, Smartsite.Security"
connectionStringName="ActiveDirectoryConnection" writeExceptionsToEventLog="true" />
</providers>
</roleManager>
```

6.6.7 Authentication Back-end (CMS)

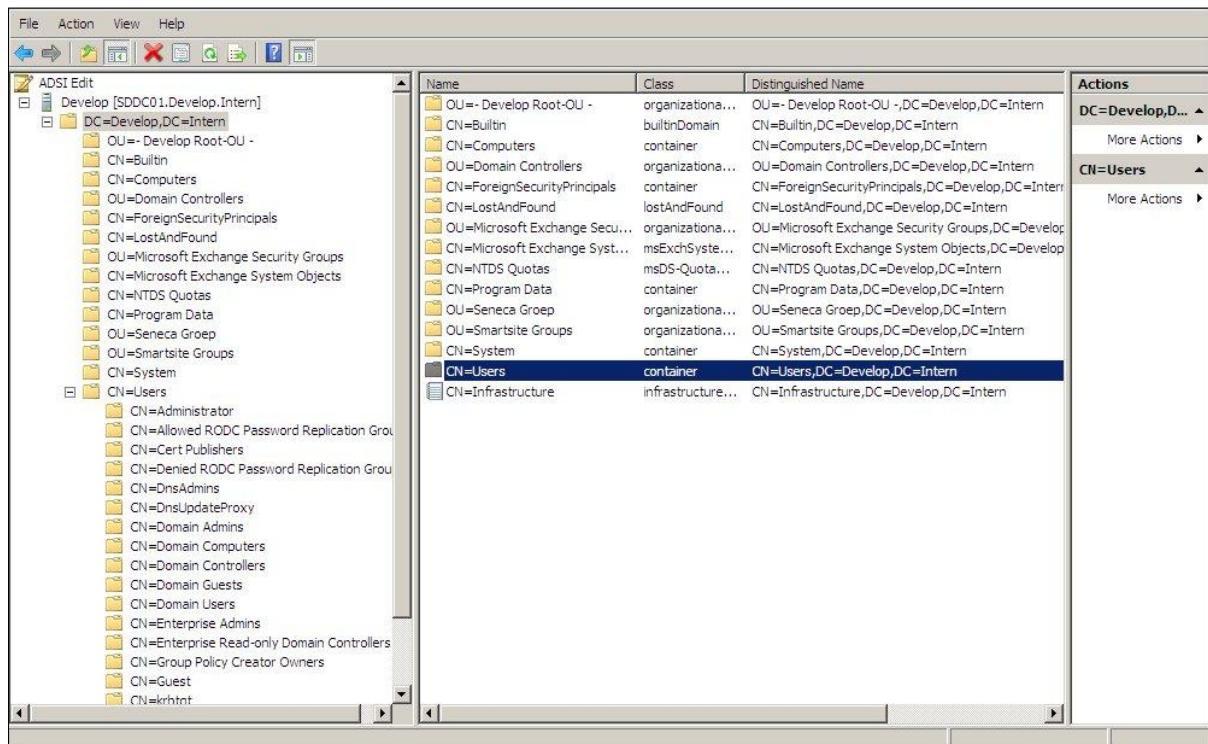
In de sectie <location path="cms"><system.web> dient de authentication mode Op Windows te worden gezet (Let op XML: Hoofdletter gevoelig)

```
<!-- ADS SETTING CMS authentication mode integrated security -->
<authentication mode="Windows" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

6.7 ADSI Edit

Door gebruik te maken van de Microsoft ADSI Edit tool, kun je eenvoudig de Distinguished Name (AD Path) achterhalen in de juiste syntax. Op deze manier kun je eenvoudig de SearchBase opgeven, hier: CN=Users,DC=Develop,DC=Intern

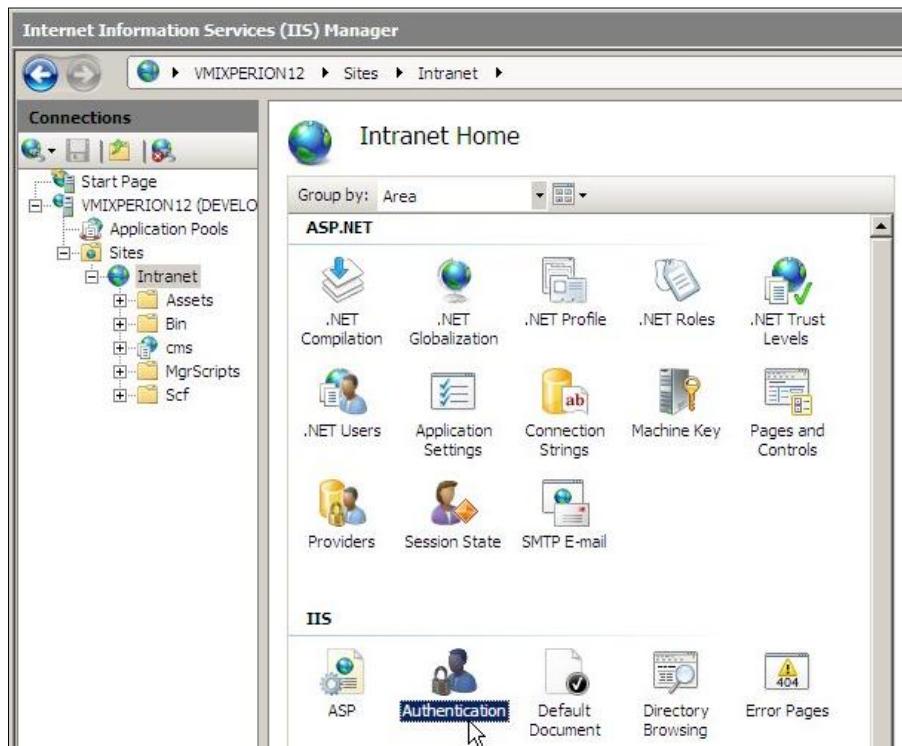


Implementatiehandleiding Active Directory voor Smartsite iXperion

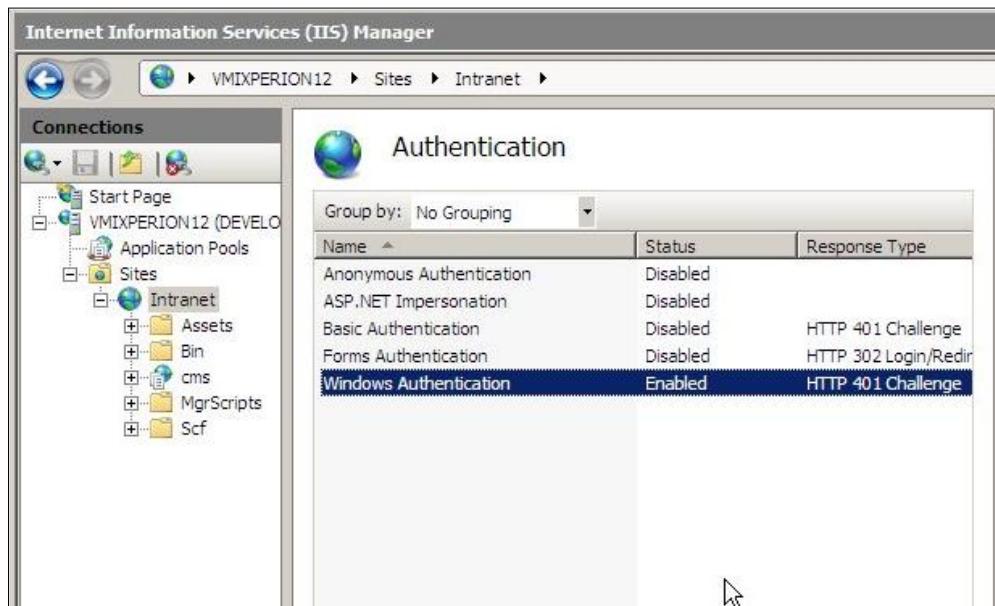
6.8 IIS integrated authentication

In IIS dient de authenticatie te worden ingesteld op alleen integrated Authentication.

Dit doe je door de IIS site aan te klikken en het icoon Authentication aan te klikken.



Implementatiehandleiding Active Directory voor Smartsite iXperion



- ⚠ Let op: Indien er in de site gebruik wordt gemaakt van **Smartsite 5 Formulieren** in de front-end, dan dient tevens **anonymous authentication** te worden enabled op de Site/CMS application.
- ⚠ Let op: Als er zowel openbare als restricted content is dient voor de voorkant ook 'Anonymous authentication' aan te staan.
- ⚠ Let op: Zet altijd eerst de Authentication voor de site (hier Intranet), en daarna pas voor de site/CMS application. Doe je dit niet dan worden de waarden van de site/CMS application overschreven door de site instellingen.

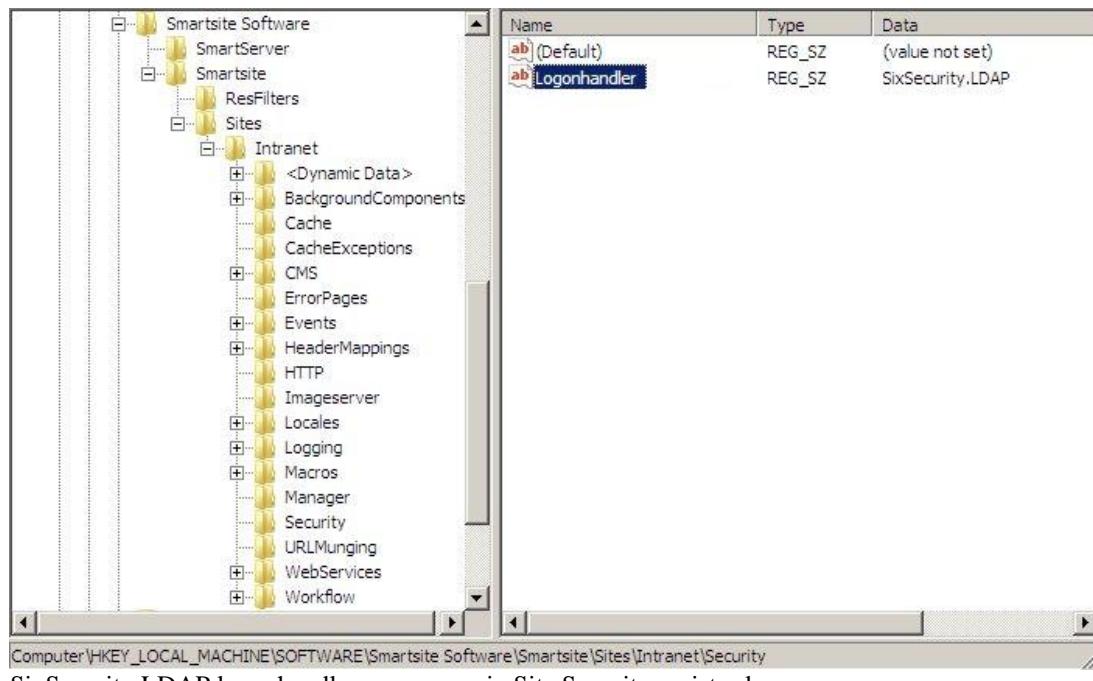
Implementatiehandleiding Active Directory voor Smartsite iXperion

6.9 Site Registry Security Key

Voordat het Smartsite iXperion CMS kan praten met het AD dient er een logonhandler **SixSecurity.LDAP** te worden gedefinieerd in de site registry Security key.

⚠ Let op: SixSecurity.windows Logonhandler is niet compatible met Smartsite iXperion en dient daarom niet meer te worden gebruikt.

HKEY_LOCAL_MACHINE\SOFTWARE\Smartsite Software\Smartsite\Sites\Intranet\Security

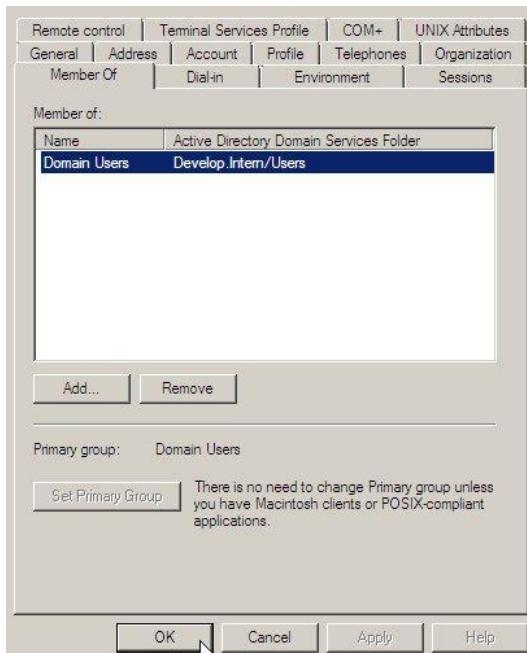


SixSecurity.LDAP logonhandler opgegeven in Site Security registry key.

Implementatiehandleiding Active Directory voor Smartsite iXperion

7 Domein- en Smartsite iXperion Primary Group

Iedere gebruiker op de Active Directory krijgt standaard een Primary Group toegewezen. Standaard is dit de Domain Users groep. Smartsite iXperion haalt apart de AD primary group op voor de ingelogde gebruiker.

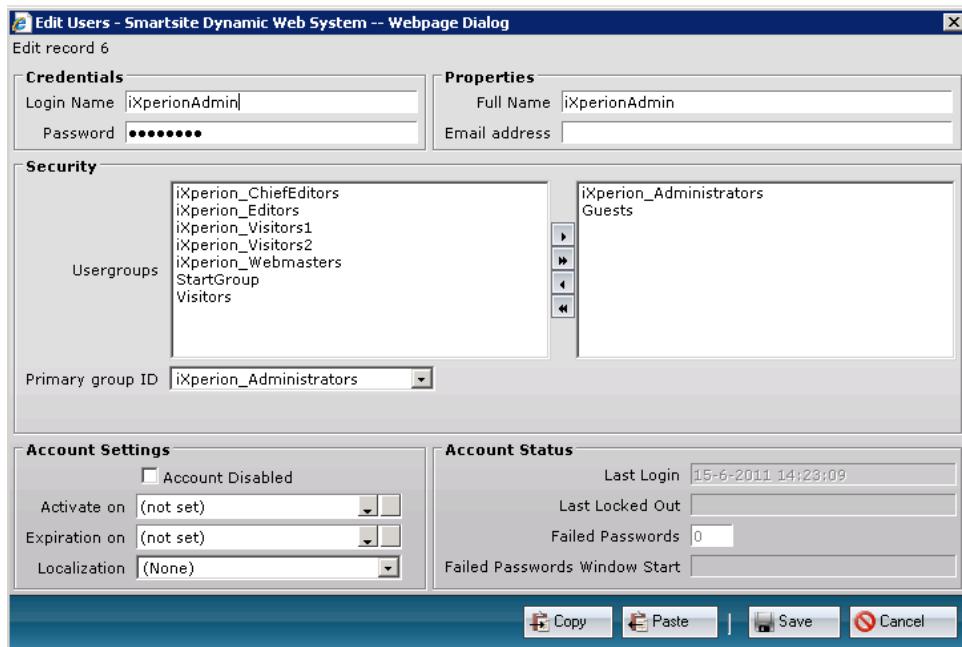


Primary group voor een gebruiker op het domein.

Echter er is een verschil tussen de Primary Group die gedefinieerd is op het domein en de Primary Group die gedefinieerd is binnen Smartsite iXperion.

Smartsite iXperion maakt gebruik van de Primary Group opgegeven in Smartsite om initiële beslissingen te nemen zoals wat is mijn default role, default view etc.

Implementatiehandleiding Active Directory voor Smartsite iXperion



“Primary group ID” bij Edit User actie, in Smartsite iXperion.

Omdat de groepen van het AD overgenomen worden (gemapt) in Smartsite iXperion zijn er 2 scenario's denkbaar.

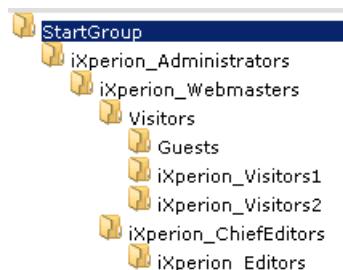
1. De AD Primary Group van de gebruiker is **niet** gemapt in Smartsite

Wanneer de AD Primary Group van de gebruiker **niet** in Smartsite gedefinieerd is zal Smartsite de opgegeven groepen hiërarchie in Smartsite gebruiken en de groep die het hoogste in de groepsstructuur aanwezig is als Smartsite primary groep toekennen.

Voorbeeld:

Wanneer iemand op het AD lid is van de groepen iXperion_Editors en iXperion_ChiefEditors en zijn AD Primary Groep is de groep Domain Users, dan zal in Smartsite de iXperion_ChiefEditors groep worden toegekend als de Primary groep.

Implementatiehandleiding Active Directory voor Smartsite iXperion



2. De AD Primary Group van de gebruiker is **wel** gemapt in Smartsite

Men zou verwachten dat wanneer de AD Primary Group van de gebruiker **wel** in Smartsite is gemapt, dat dan altijd deze groep als primary groep wordt gekozen.

Echter zal Smartsite **nog steeds** de opgegeven groepen hiërarchie in Smartsite toepassen en de groep die het hoogste in de groepen-structuur aanwezig is als primary groep toekennen.

Wil je bijvoorbeeld dat de AD Domain Users groep altijd als primary group in Smartsite iXperion wordt toegekend, zorg er dan voor dat de Domain Users groep boven in de groepen hiërarchie in Smartsite staat.

De Smartsite primary groep kan in Smartsite handmatig worden verandert, maar zal bij het verwijderen en opnieuw inloggen van de gebruiker opnieuw terugvallen op de primary group zoals hierboven beschreven.

Vanaf versie 1.4 build 2 is het tevens mogelijk dit gedrag te beïnvloeden en kan de met de hand ingestelde Smartsite primary groep worden behouden. In de web.config kan hiervoor de UpdatePrimaryGroup op false worden gezet:

```
<add name="ObtainPrimaryGroup" value="true" />
<add name="ObtainParentGroupsForPrimaryGroup" value="true" />
<add name="MaxParentGroupRecursionDepth" value="0" />
<add name="UpdatePrimaryGroup" value="false" />
```

⚠ Wanneer Smartsite iXperion Mixed-Mode Security wordt gebruikt is de UpdatePrimaryGroup = false setting benodigd, om te voorkomen dat de AccessGroup als primary groep wordt gekozen voor alle gebruikers.

Implementatiehandleiding Active Directory voor Smartsite iXperion

8 Disabling Single Sign-on

8.1 Voorkomen IE inlogbox in Smartsite Manager

Wanneer in de front-end geen integrated authentication wordt gebruikt maar voor de back-end wel, dan kan er geen gebruik worden gemaakt van de single sign-on functionaliteit van Smartsite. Smartsite zal dan namelijk bij het inloggen in de manager op de front-end willen inloggen via single sign-on maar geen password verstrekken. Hierdoor zal er iedere keer een loginbox verschijnen na het inloggen in de manager.

De Smartsite iXperion single sign-on functionaliteit kan worden uitgeschakeld via de EnableSSO (string value) setting in de Manager registry key van de site. Geef deze de waarde 0 (=False).

- ⚠ Let op: De Smartsite iXperion single sign-on functionaliteit is niet hetzelfde als de Windows IIS single sign-on functionaliteit met Windows Integrated Security.
- ⚠ Let op: De inlogbox zal ook verschijnen als het adres waarop je de site benaderd (serveraddress) niet opgenomen is als **A Name record** in de DNS maar als **Canonical Name record** (CName). Via ping kun je nagaan het adres als A Name record is opgenomen. De ping zal niet direct het IP nummer teruggeven maar eerst de alias en dan het IP adres. Neem het adres op als A Name record in de DNS en doe een ipconfig /flusdns op de server.

Implementatiehandleiding Active Directory voor Smartsite iXperion

9 Hoe een Domain Group Policy aan te maken

Om ervoor te zorgen dat de URL voor de site direct wordt toegevoegd aan de Trusted Site Zone in Internet Explorer is het verstandig een Domain Policy aan te maken.

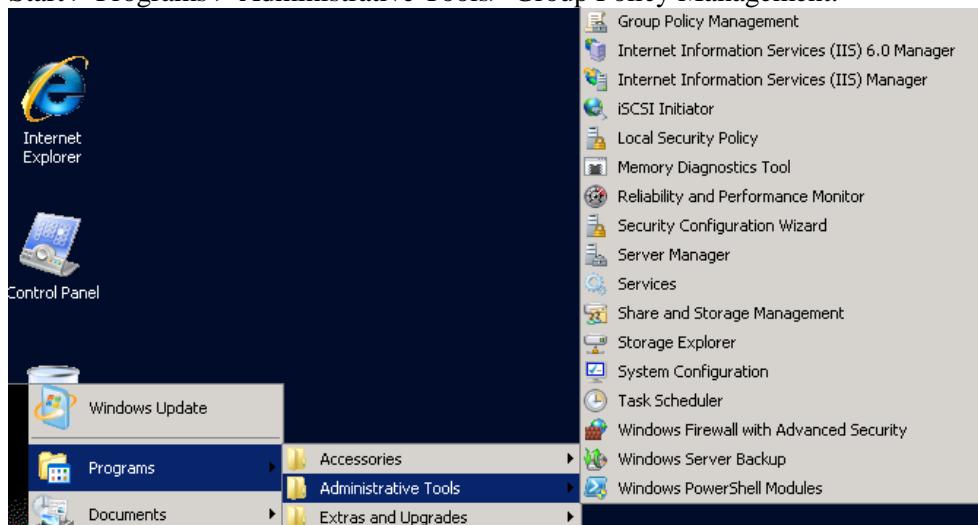


http://Intranet wordt automatisch toegevoegd aan alle client IE browsers door de domain Policy.

Voer de volgende stappen uit op de Domein (AD/DSN) server:

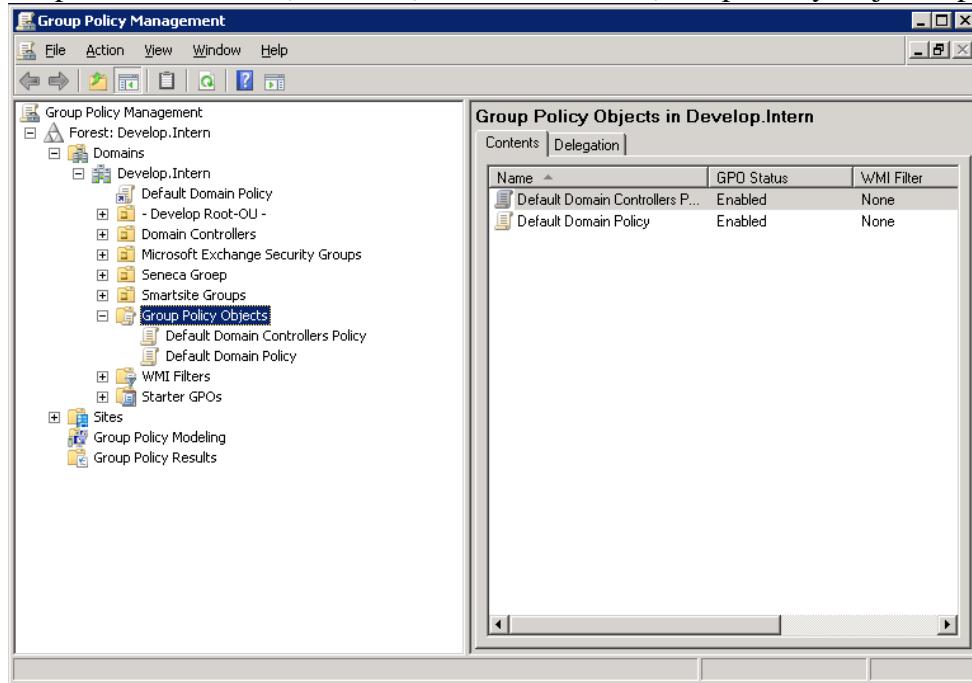
1. Op de domein server ga naar:

Start > Programs > Administrative Tools> Group Policy Management.

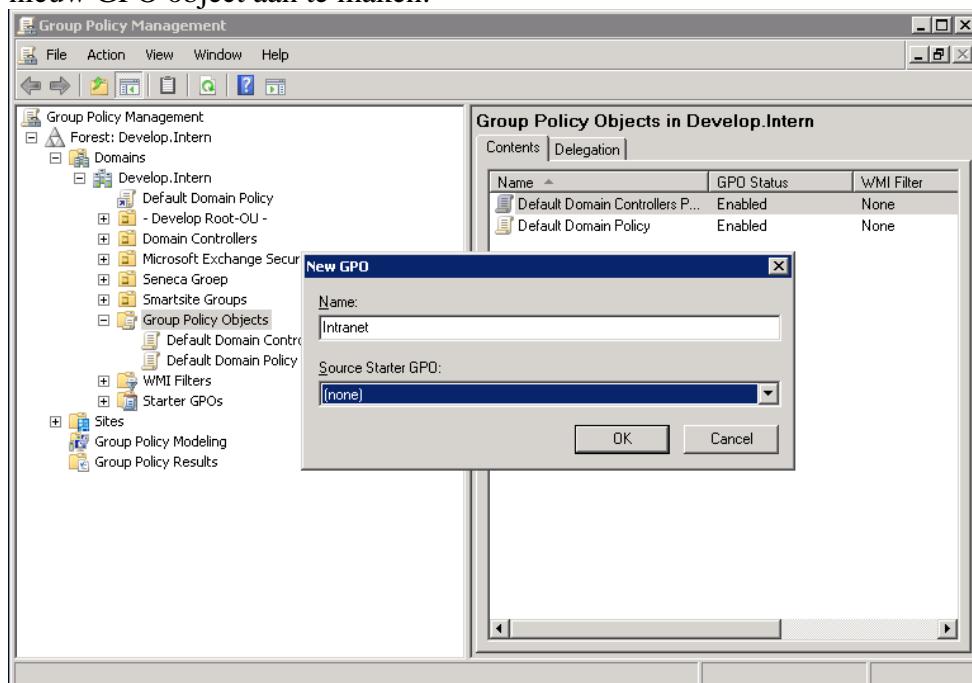


Implementatiehandleiding Active Directory voor Smartsite iXperion

2. Klap de folder Forest\Domains\Yourdomain.local\Group Policy Objects open.

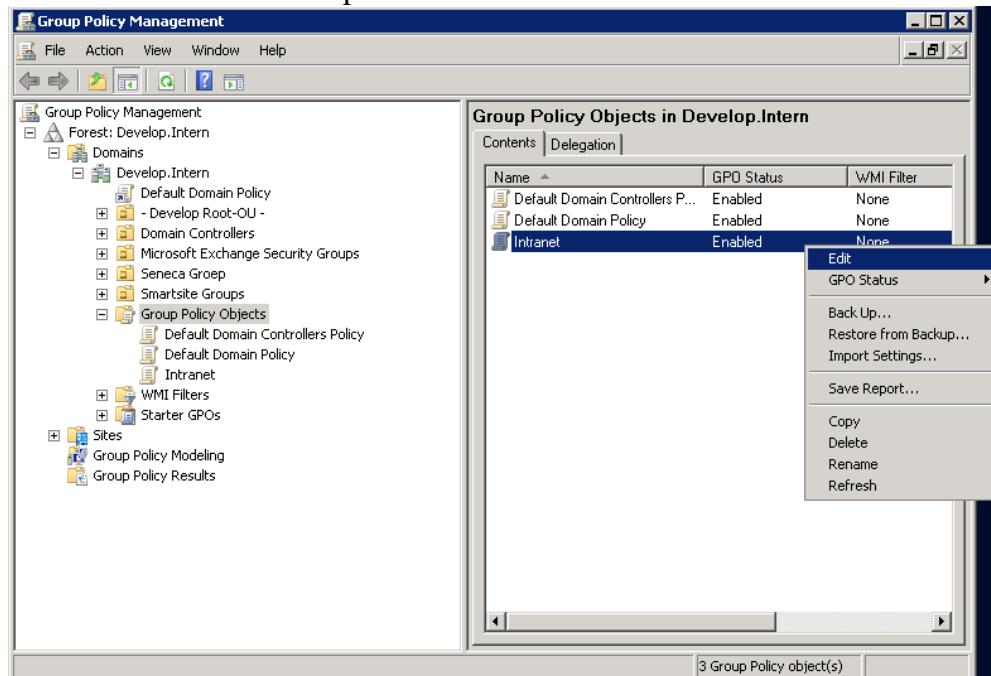


3. Klik met de rechtermuis op het Group Policy Objects, en selecteer New om een nieuw GPO object aan te maken.

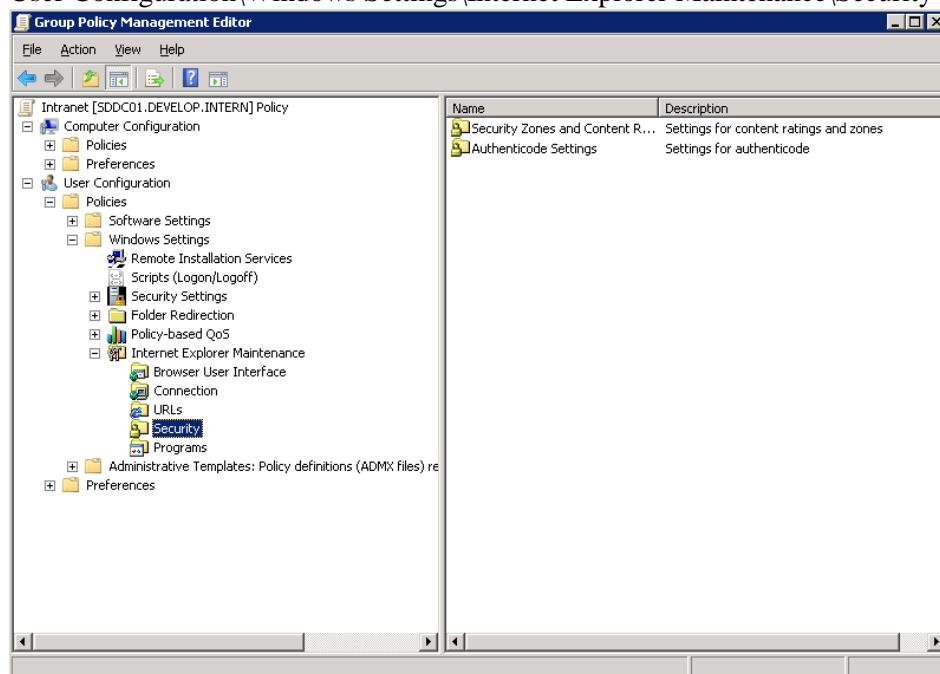


Implementatiehandleiding Active Directory voor Smartsite iXperion

Klik met de rechtermuis op de nieuwe GPO en selecteer Edit.



In de Group Policy Management Editor, open de folder
 User Configuration\Windows Settings\Internet Explorer Maintenance\Security

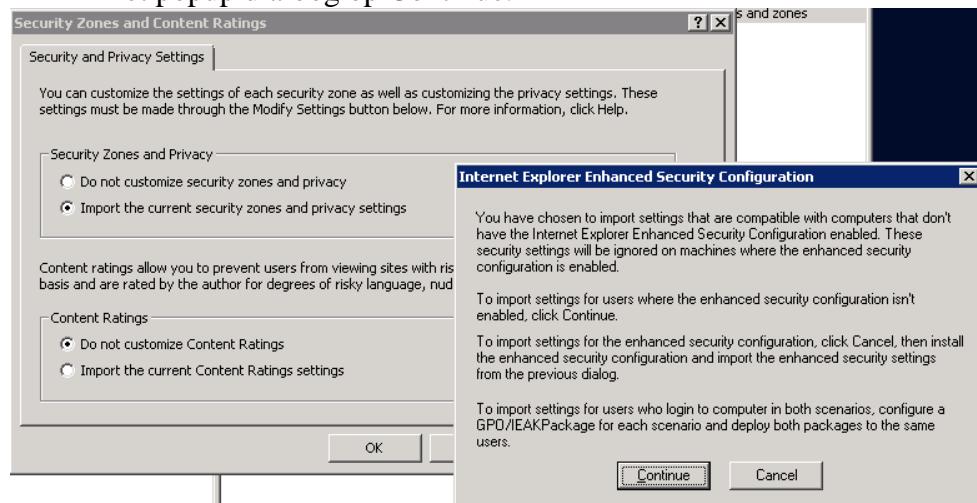


Implementatiehandleiding Active Directory voor Smartsite iXperion

Dubbelklik “Security Zones and Content Ratings” in het rechter scherm om het properties scherm te openen.

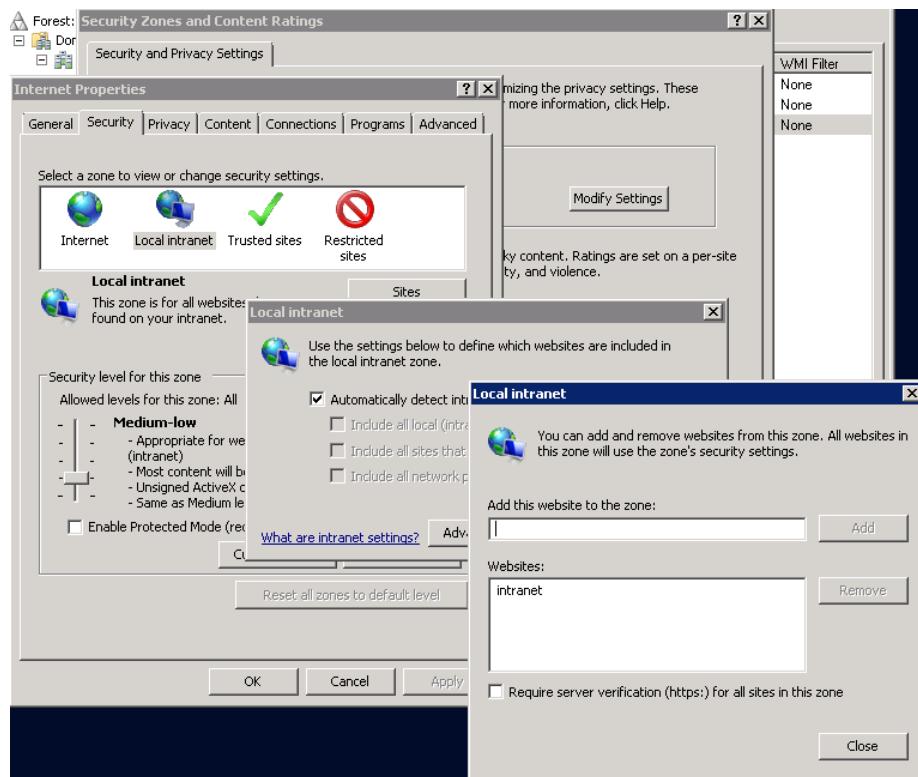
In de Security Zones and Privacy dialoog, selecteer “Import the current security zones and privacy settings.”

Klik in het popup dialoog op Continue.

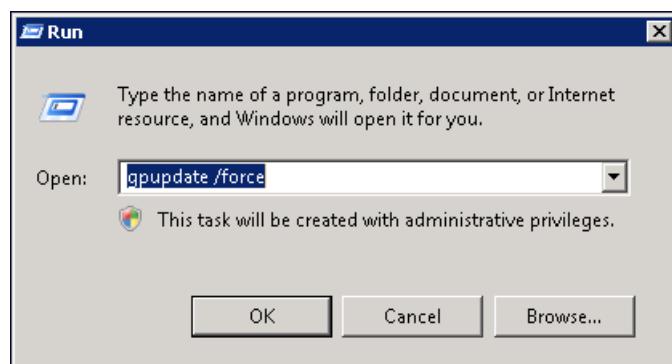


Klik “Modify Settings” en voeg de Smartsite iXperion site URL toe aan de Local Intranet Zone sites.

Implementatiehandleiding Active Directory voor Smartsite iXperion



4. Sluit alle schermen weer af.
5. Sluit de het Group Policy Editor scherm af.
6. Optioneel kun je via het Group Policy Management scherm de nieuwe GPO linken aan een OU.
7. Voordat de nieuwe domein policy actief wordt dient deze te worden geupdate.
8. Via het windows start menu voor het **gpupdate /force** commando uit.



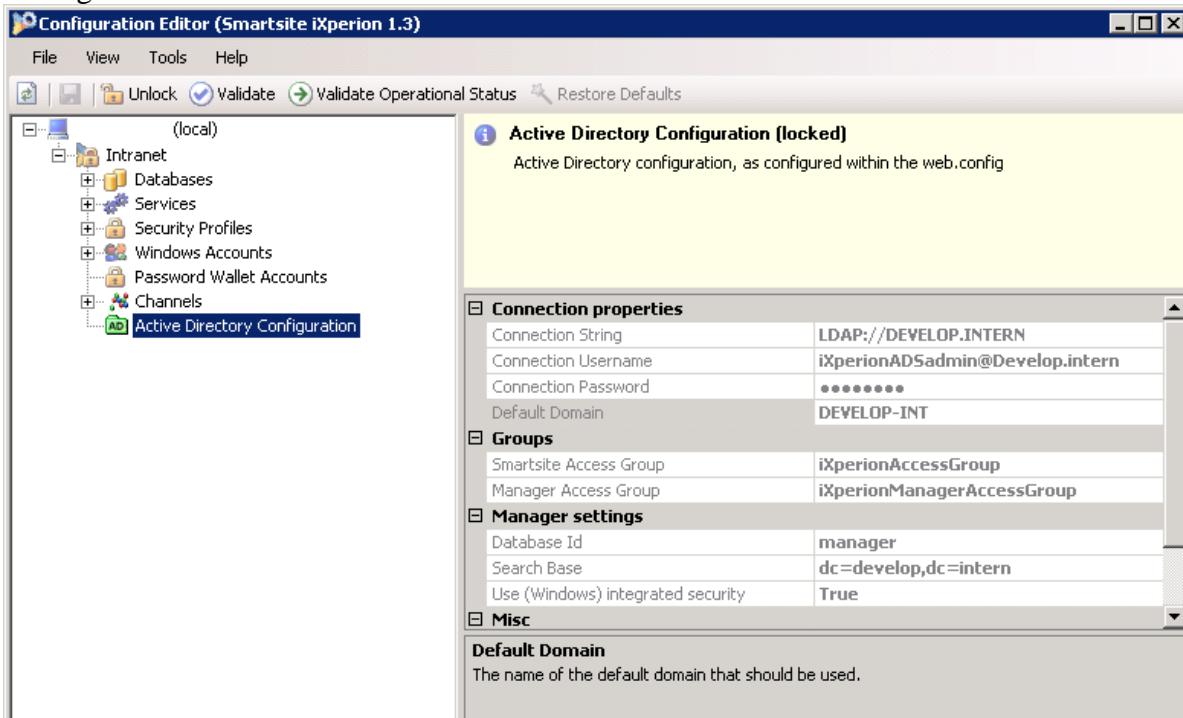
Implementatiehandleiding Active Directory voor Smartsite iXperion

9. Wanneer de redacteuren gebruik willen maken van de nieuwe policy, dan dienen zij opnieuw uit- en in te loggen in MS Windows.

Implementatiehandleiding Active Directory voor Smartsite iXperion

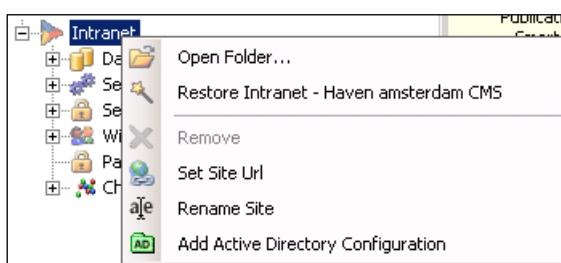
10 Smartsite ConfigEditor en Active Directory Configuratie

Bovenstaande handmatige AD configuratie is tevens in te stellen via de Smartsite ConfigEditor.



 **Let op:** De configeditor ondersteunt alleen de Active Directory Configuration!

Wanneer de site nog geen Active Directory configuratie bevat, kan de site worden *unlocked*. Via een rechter muisklik op de site, kan de *Add Active Directory Configuration* optie worden geselecteerd.



Implementatiehandleiding Active Directory voor Smartsite iXperion



Tip: Nadat je de configuratie via de configEditor hebt toegevoegd, controleer dan handmatig al de instellingen in de Web.config zoals hierboven beschreven.

11 Proxy/ISA Server en Firewall

11.1 Outscaling

Wanneer gebruik wordt gemaakt van outscaling wordt er XML data over HTTP poort 80 naar een buiten server gezonden (Webservice).

Voor een juiste werking van Smartsite iXperion dient de redactie server **geen** gebruik te maken van een proxy server. **De redactie server dient in de firewall te worden uitgesloten voor het gebruik van de proxyserver.**

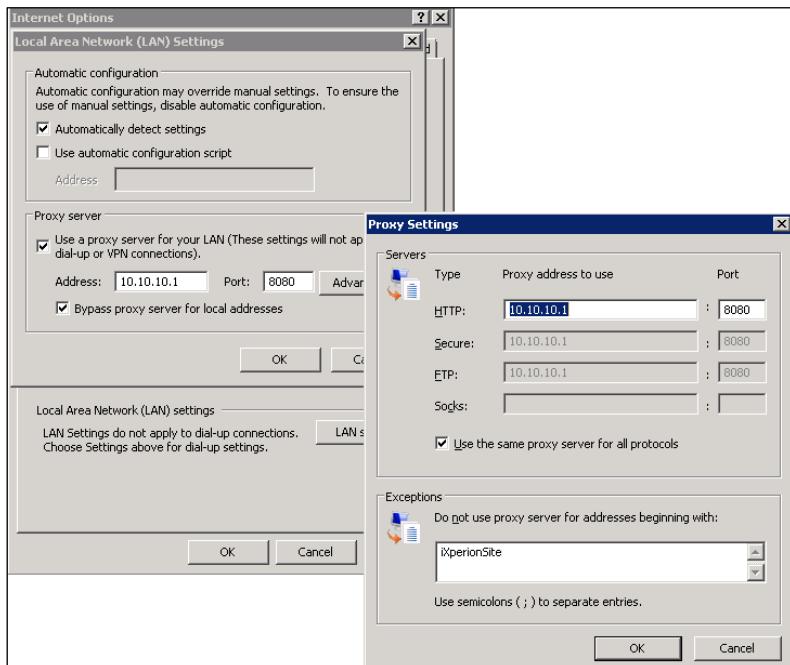
Daarnaast dient het externe IP adres te worden toegevoegd in de firewall van de ontvangende kant.

11.2 Smartsite Manager

Wanneer veel redacteuren de manager bevrager worden er vele requests gedaan. Wanneer intern via het LAN via een proxyserver wordt gebrowsed, dan kan dit performance problemen opleveren.

Seneca adviseert dan ook dat intern de URL/IP van de Smartsite iXperion site wordt uitgesloten voor het gebruik van de proxyserver. Dit kan worden gerealiseerd door het toevoegen van een domein-rule (zie ook hoofdstuk 9) of via de lokale connection-settings in de IE browser.

Implementatiehandleiding Active Directory voor Smartsite iXperion



Bypass proxy server connection-setting in Internet Explorer

12 Custom Errorhandling in Web.config

Wanneer in de web.config Custom errorhandling is opgenomen en de handleError property staat op de waarde false, dan verschijnt er in de front-end na inloggen de melding:

```
Server Error in '/' Application.

This type of page is not served.
Description: The type of page you have requested is not served because it has been
explicitly forbidden. The extension '.net' may be incorrect. Please review the URL
below and make sure that it is spelled correctly.
```

Deze waarde voor handleErrors dient altijd daarom altijd "true" te zijn anders worden er geen http errors waaronder http 401 (authenticatie) geraised en wordt er in de front-end geen juiste foutmelding weergegeven.

```
<customErrors handleErrors="true" mode="RemoteOnly">
    defaultRedirect="GenericErrorPage.htm">
        <error statusCode="403" redirect="NoAccess.htm" />
        <error statusCode="404" redirect="FileNotFoundException.htm" />
</customErrors>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

Om de foutmeldingen niet zichtbaar voor de bezoeker te maken dient de mode="RemoteOnly" te worden gebruiken.

Hieronder de definities volgens Microsoft:

- On -Specifies that custom errors are enabled. If no defaultRedirect attribute is specified, users see a generic error. The custom errors are shown to the remote clients and to the local host.
- Off - Specifies that custom errors are disabled. The detailed ASP.NET errors are shown to the remote clients and to the local host.
- RemoteOnly -Specifies that custom errors are shown only to the remote clients, and that ASP.NET errors are shown to the local host. This is the default value.

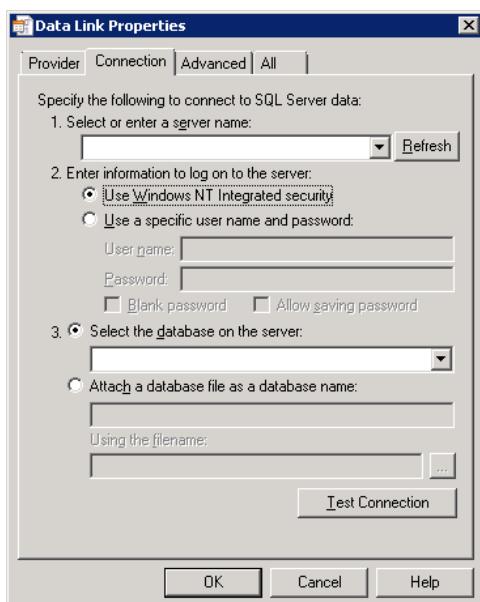
De default is RemoteOnly.

Zie: <http://msdn.microsoft.com/en-us/library/h0hfz6fc.aspx>

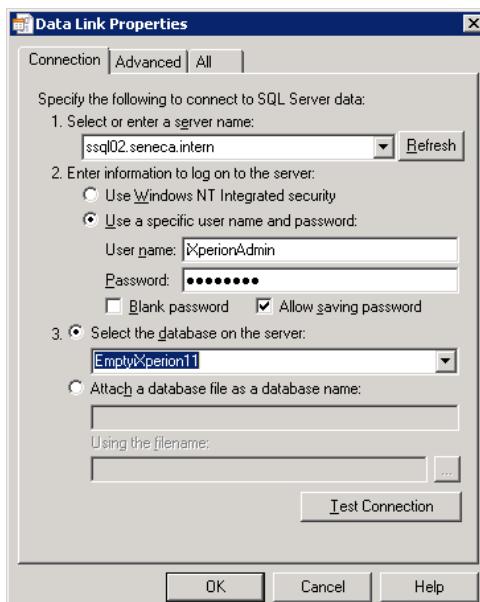
Implementatiehandleiding Active Directory voor Smartsite iXperion

13 Integrated database connectionstring

Een Windows NT integrated Security database connectionstring wordt door Smartsite iXperion 1.4 build 3 en hoger ondersteund.



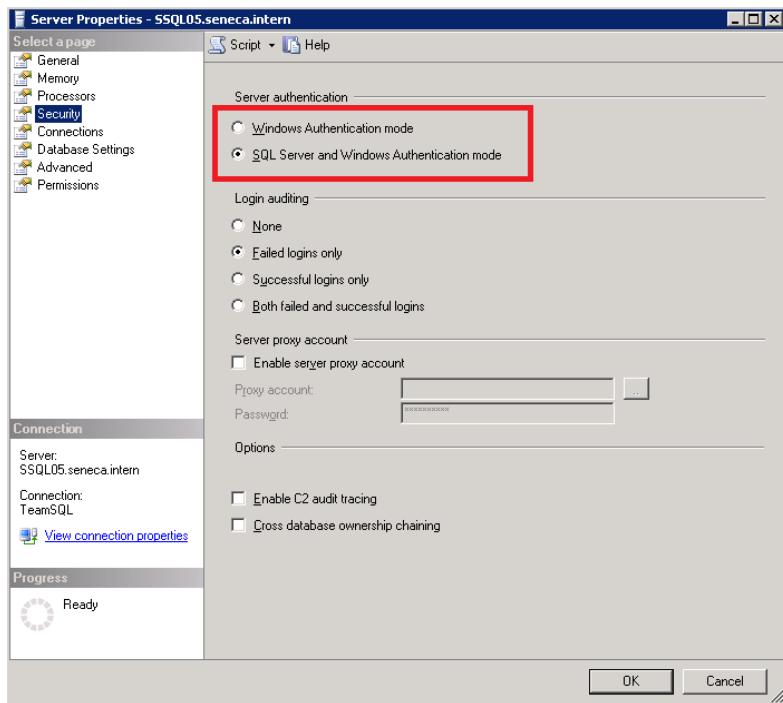
Windows NT integrated Security database connectiestring.



Username en Password in de database connectiestring.

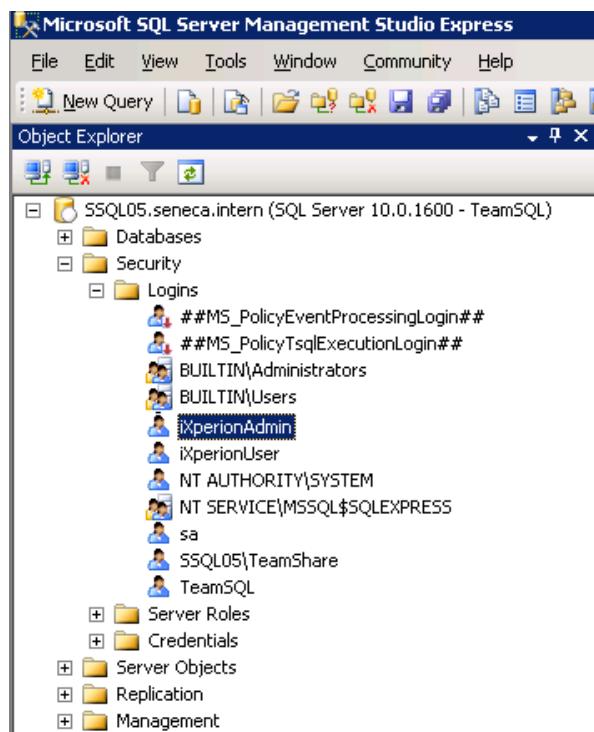
Implementatiehandleiding Active Directory voor Smartsite iXperion

De SQL Server waarmee wordt geconnect dient de gekozen connectie mode te ondersteunen. Op de SQL Server dient dan ook in de security Server authentication voor de optie “SQL Server and Windows Authentication mode” te worden gekozen.



Implementatiehandleiding Active Directory voor Smartsite iXperion

In SQL server kan bij het gebruik van een Smartsite iXperion 1.4 build 2 en lager alleen gebruik worden gemaakt van SQL logins, en niet van Windows NT accounts.



Implementatiehandleiding Active Directory voor Smartsite iXperion

14 Smartsite iXperion Mixed Mode Security

Het is mogelijk het groepenbeheer in Smartsite iXperion te laten plaats vinden en toch gebruik te maken van de single sign-on en een Active Directory koppeling.

Door gebruik te maken van Smartsite iXperion Mixed Mode Security wordt het groepen beheer niet meer neergelegd bij de systeembeheerder en de Active Directory, maar vindt dit in Smartsite zelf plaats door een aangewezen webmaster of hoofdredacteur.

De mixed mode implementatie is eigenlijk vrij eenvoudig.

14.1 Mixed mode web.config

De web.config ziet er hetzelfde uit al bij een volledige AD koppeling implementatie

Voorbeeld web.config mixed-mode security:

```
Smartsite.ActiveDirectoryConfiguration>
<settings>
<add name="SmartsiteAccessGroup" value=" ixperionAccessGroup" />
<add name="ManagerAccessGroup" value=" ixperionManagerAccessGroup" />
<add name="StoreFullyQualifiedLoginName" value="false" />
<add name="DatabaseId" value="manager" />
<add name="SearchBase" value="dc=develop,dc=intern" />
</settings>
<membershipMappings>
<add name="mm1" domain="DEVELOP-INT" providerName="ads" />
<add name="mm2" domain="DEVELOP.INTERN" providerName="ads" />
</membershipMappings>
</Smartsite.ActiveDirectoryConfiguration>
```

14.1.1 UpdatePrimaryGroup

Vanaf versie 1.4 build 2 is mogelijk de primaryGroup met de hand in te stellen zodat na inloggen van de gebruiker de Smartsite primary groep wordt behouden. In de web.config kan hiervoor de UpdatePrimaryGroup op false worden gezet:

```
<add name="ObtainPrimaryGroup" value="true" />
<add name="ObtainParentGroupsForPrimaryGroup" value="true" />
<add name="MaxParentGroupRecursionDepth" value="0" />
<add name="UpdatePrimaryGroup" value="false" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

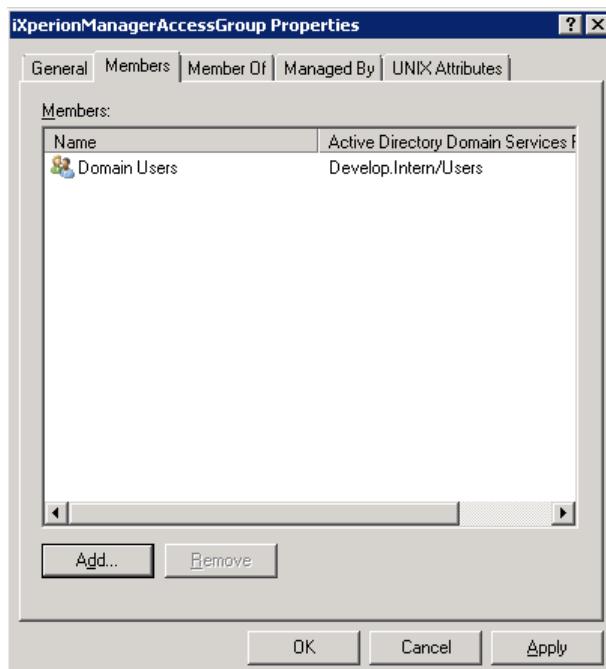
- ⚠ Wanneer Smartsite iXperion Mixed Mode Security wordt gebruikt is de UpdatePrimaryGroup = false setting benodigd, om te voorkomen dat de AccessGroup als primary groep wordt gekozen voor alle gebruikers.**

Zie: Hoofdstuk 6 voor overige settings.

14.2 Mixed mode domein configuratie

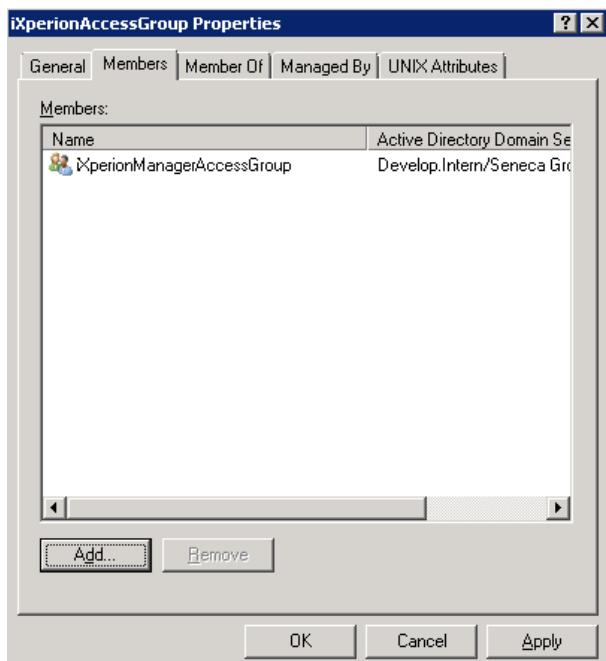
Op het domein wijkt de configuratie af van de standaard implementatie. Op het domein maken we nog steeds de Local Domain Security groepen SmartsiteAccessGroup en ManagerAccessGroup aan.

Aan de ManagerAccessGroup groep voegen we alle redactie groepen toe die toegang dienen te hebben tot Smartsite.



Om alle gebruikers van het domein toegang te geven voegen we de Domain Users groep toe aan de ManagerAccessGroup groep.

Implementatiehandleiding Active Directory voor Smartsite iXperion



De ManagerAccessGroup voegen we net als bij de standaard implementatie toe aan de AccessGroup zodat alle redacteuren toegang hebben tot de Smartsite Manager.
(Optioneel voegen we de visitor groepen toe.)

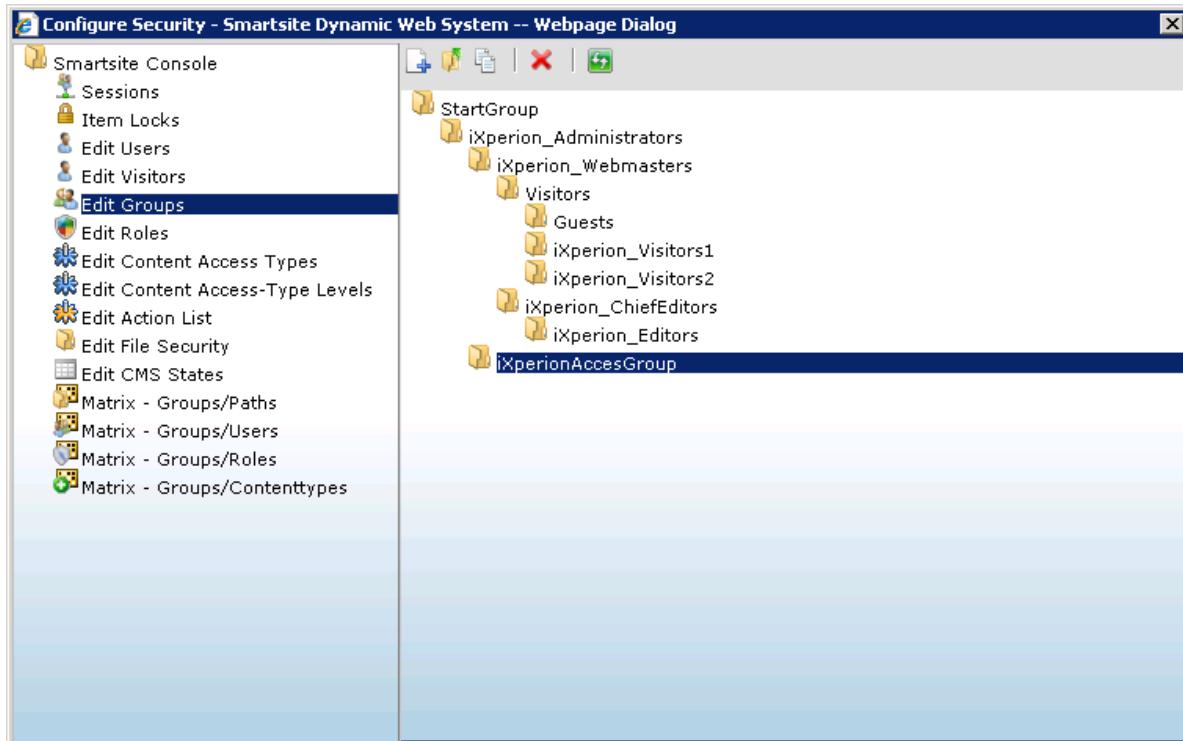
Hoewel iedereen nu automatisch toegang heeft tot zowel de front-end als de back-end van Smartsite wordt de daadwerkelijke toegang in Smartsite geregeld door de ingelogde gebruikers na inloggen over te hevelen naar de interne Smartsite groepen.

14.3 Smartsite iXperion mixed mode groepen structuur

Vervolgens passen we in Smartsite iXperion de groepen structuur aan.

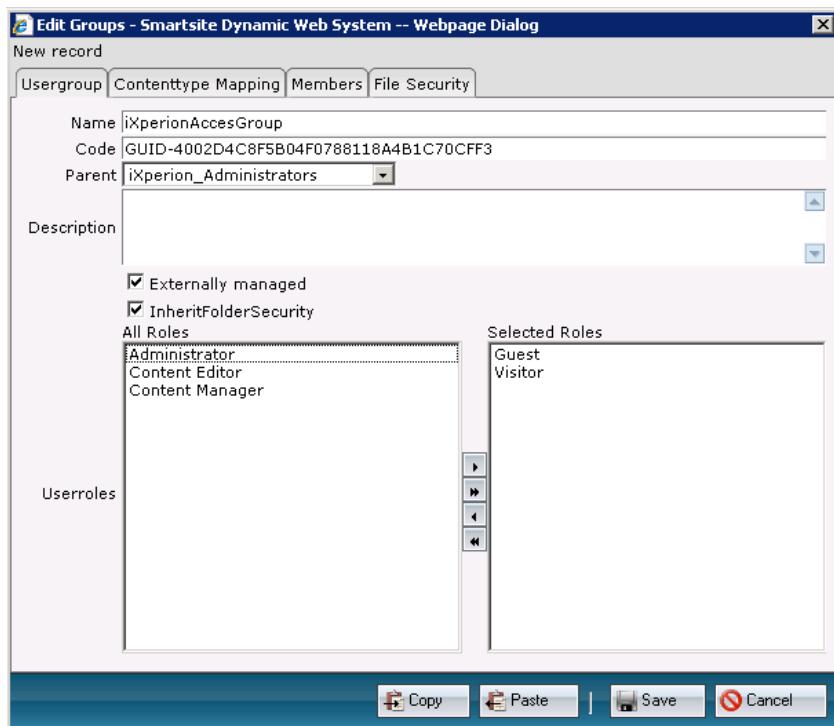
Door de SmartsiteAccessGroup opgeven in de Web.config in de Smartsite groepen structuur te mappen en **alleen voor deze groep** het Externally Managed vinkje aan te zetten, hebben alle personen die lid zijn van deze groep (Domain Users) direct toegang tot Smartsite.

Implementatiehandleiding Active Directory voor Smartsite iXperion



Echter de SmartsiteAccessGroup krijgt alleen de role Visitor en Guest welke niet over het privilege “**Access to the Smartsite Manager**” beschikken.

Implementatiehandleiding Active Directory voor Smartsite iXperion



- Het Externally managed vinkje staat aan
- Er zijn geen Contenttype Mappings
- File Security is none

De groep is uitsluitend bedoeld gebruikers toegang te verschaffen tot Smartsite.

14.4 IIS instellingen voor mixed mode security

Wanneer een persoon inlogt wordt hij automatisch toegevoegd aan de AllUser tabel en kan dan via normale Smartsite buildin security worden toegevoegd aan Smartsite Groepen. Wanneer de in te loggen gebruiker lid is van de ManagerAccessGroup wordt hij als user geregistreerd. Wanneer de in te loggen gebruiker alleen lid is van de SmartsiteAccessGroup wordt hij als visitor geregistreerd.

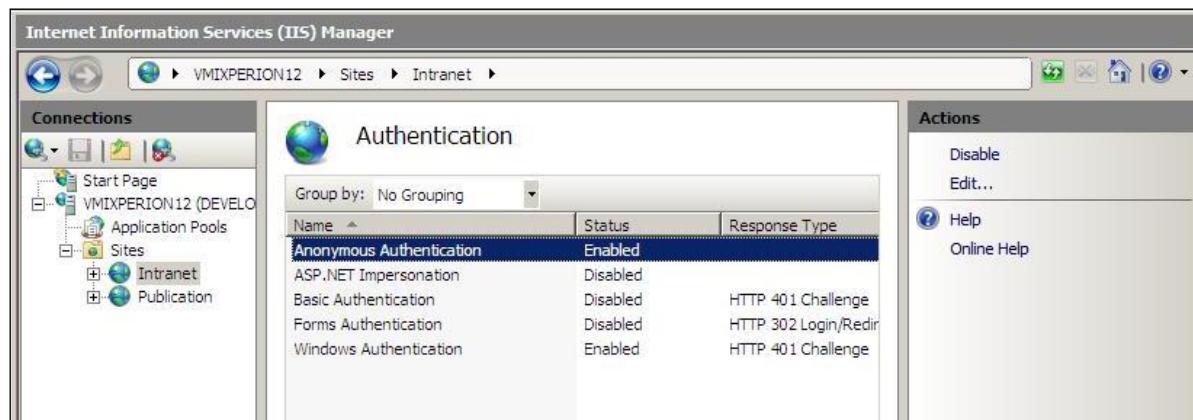
Dit kunnen Visitor groepen zijn of groepen die toegang tot de Smartsite Manager hebben. De manager access groepen beschikken over minimaal 1 role met de Privilege “Access to the Smartsite Manager”.

Implementatiehandleiding Active Directory voor Smartsite iXperion

Of de gebruiker bij inloggen wordt toegevoegd aan de AllUser tabel is afhankelijk van de IIS Authenticatie settings.

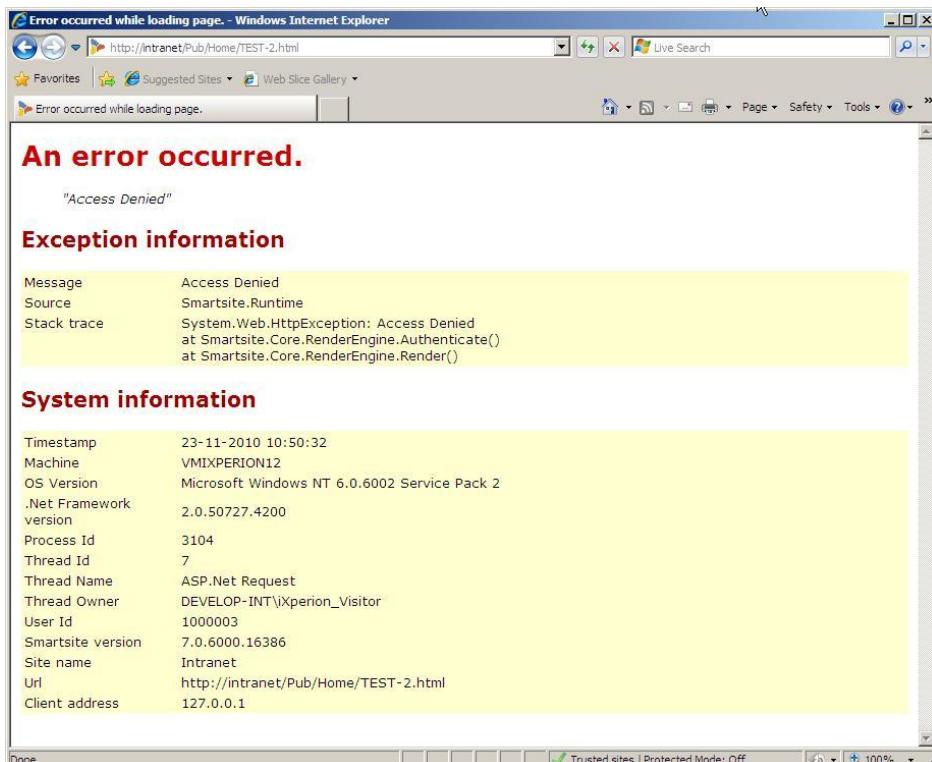
14.4.1 IIS Anonymous authentication en Windows Integrated Authentication enabled

Wanneer zowel Anonymous als Windows Authentication enabled zijn, kunnen gebruikers Anonymous de Front-end van de site benaderen. Hiervoor zal Smartsite het Guest account gebruiken. In dit geval zal Smartsite de useraccount gegevens **niet** opslaan in de AllUser tabel.



Om een account dat lid is of dient te worden van een visitor groep in Smartsite, dient deze eerst in te loggen in Smartsite. Dit kan de gebruiker doen door eerst een **restricted pagina** te bezoeken. Hij zal dan een *Access Denied* foutmelding krijgen, maar zijn accountgegevens zijn wel al toegevoegd in de Smartsite iXperion AllUsers tabel.

Implementatiehandleiding Active Directory voor Smartsite iXperion

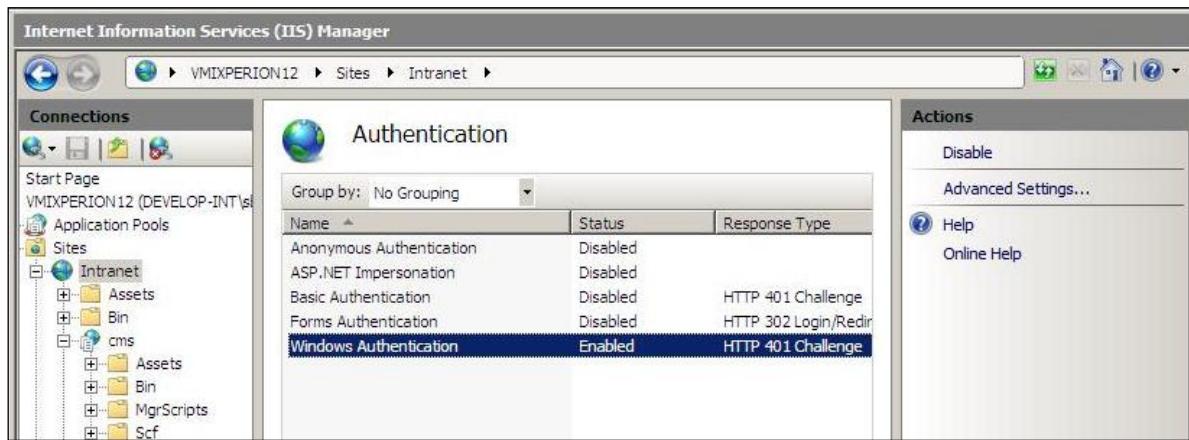


Access Denied error voor visitor1 account op een restricted item.

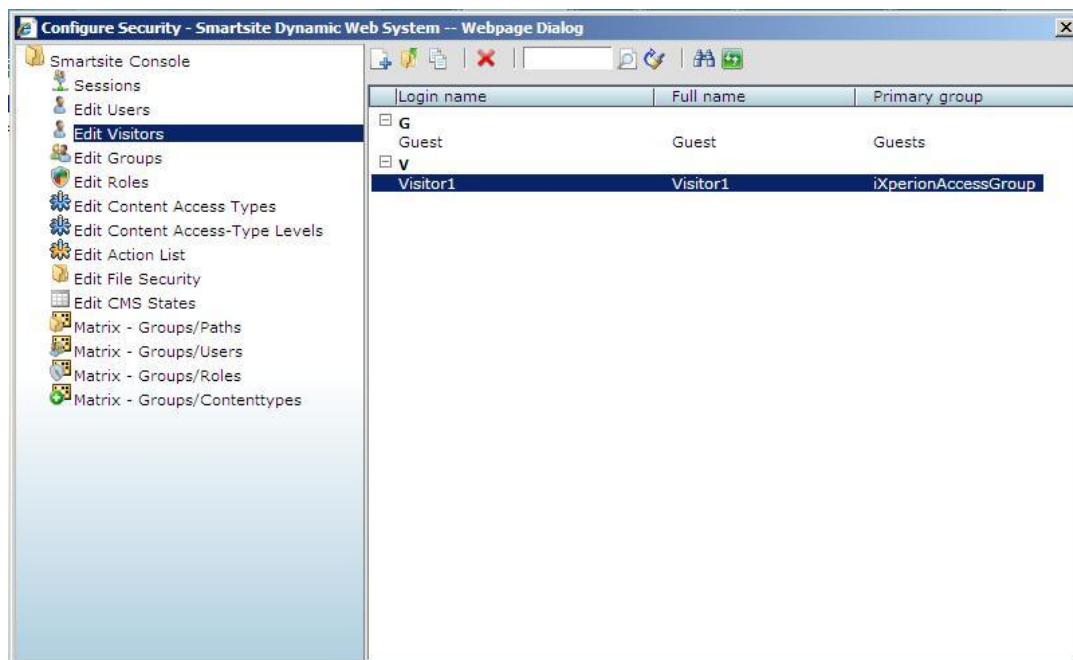


Tip: Het is tevens mogelijk de AD accounts al handmatig aan te maken in Smartsite met dezelfde accountnaam als op het domein en de gebruikers al toe te kennen aan de juiste Smartsite groepen. Na inloggen worden dan als nog de juiste groepen (AccessGroup en Guest) toegevoegd.

Implementatiehandleiding Active Directory voor Smartsite iXperion



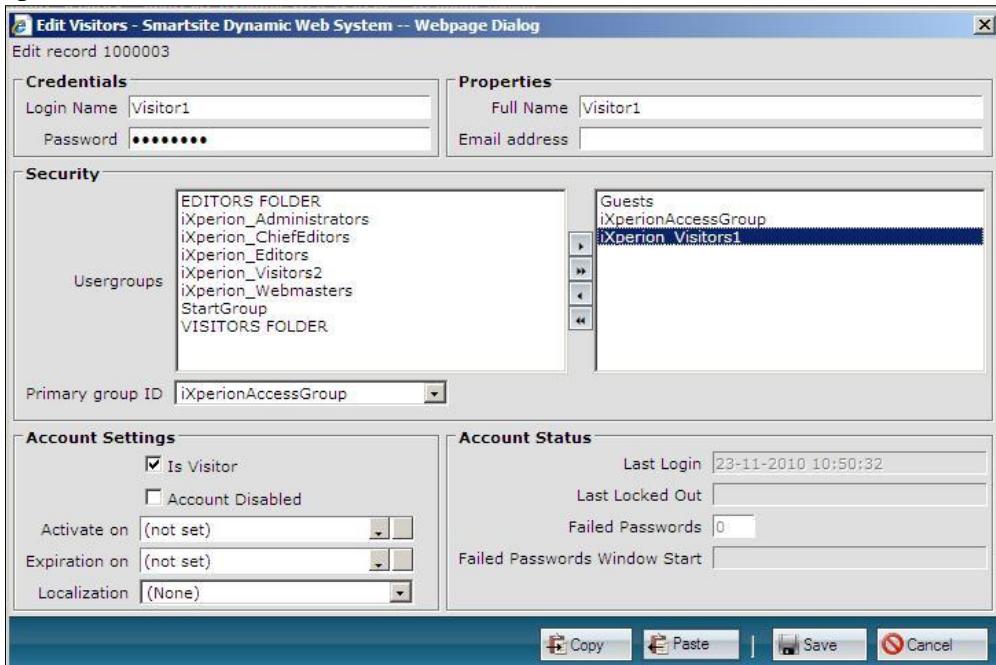
Wanneer alleen Windows Authentication enabled is, zal de account informatie altijd gelogd worden.



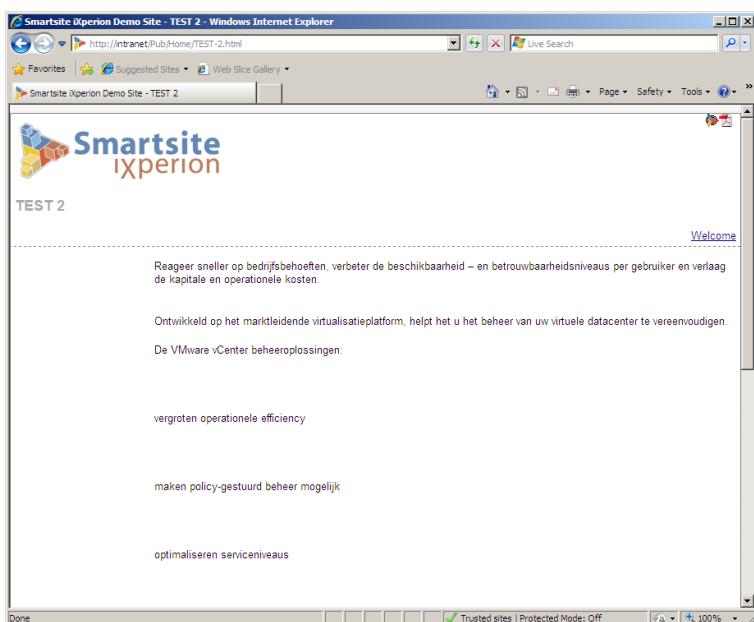
Visitor account is wel gelogd in Smartsite iXperion en lid van de AccessGroup (hier iXperionAccessGroup).

Implementatiehandleiding Active Directory voor Smartsite iXperion

Via Configure Security kan een webmaster via de Edit Visitors actie de gelogde gebruiker openen.



De webmaster kan de user nu toevoegen aan 1 of meerdere buildin Smartsite groepen.



Implementatiehandleiding Active Directory voor Smartsite iXperion

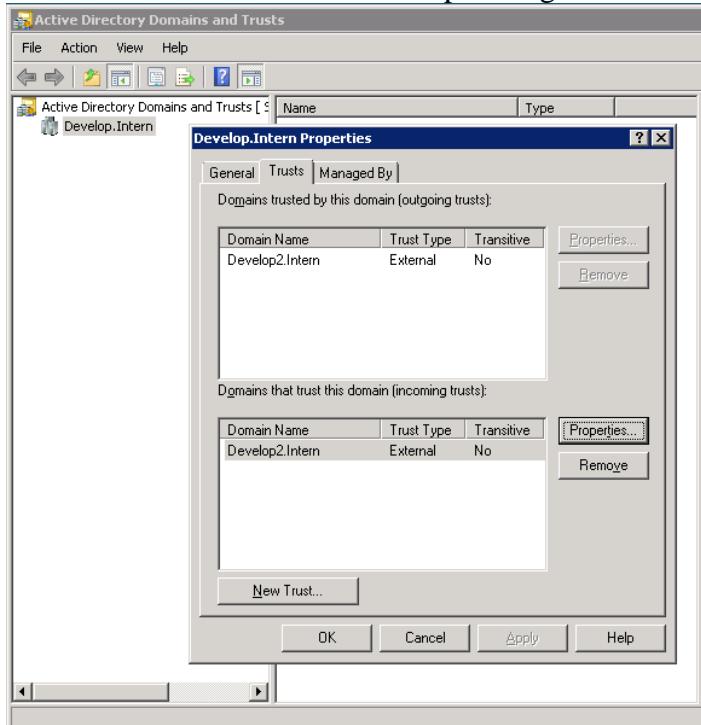
Voegt hij de gebruiker tevens toe aan de iXperion_Visitors1 groep die browse access heeft op het restricted item, dan zal de gebruiker daarna wel het items kunnen opvragen in de front-end.

15 Active directory koppeling met meerdere domeinen

Vanaf Smartsite iXperion 1.4 build 3 is het mogelijk te praten met meerdere domeinen (Multi-domaining).

15.1 Outgoing en incoming trust (tweeweg-trust)

Om het mogelijk te maken Smartsite iXperion met meerdere domeinen te laten praten dient er tussen het domein waarbij de Smartsite iXperion server is aangemeld en de andere domeinen een tweeweg trust relatie te zijn aangemaakt. Hierdoor is Smartsite instaat over de domeinen de account informatie op te vragen.

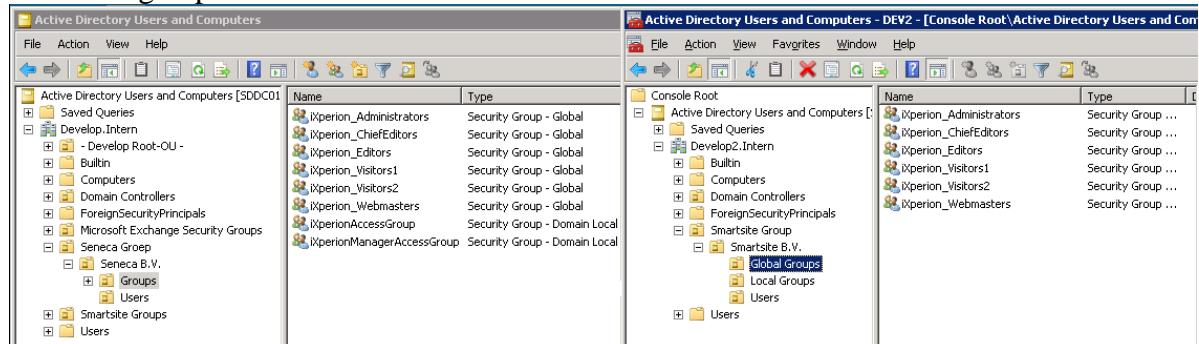


Active directory tweeweg-trust.

Implementatiehandleiding Active Directory voor Smartsite iXperion

15.2 Groepen en users

Wanneer Smartsite met meerdere domeinen connectie maakt is het mogelijk gebruik te maken van verschillende groepsnamen over de verschillende domein. De global groepen dienen te worden toegevoegd aan de Smartsite Access groepen en te worden gemapt in de Smartsite groepen structuur.



The screenshot shows two separate Active Directory management consoles. The left console, titled 'Active Directory Users and Computers [SDDC01]', displays a list of security groups under the 'Develop.Intern' organizational unit. The right console, titled 'Active Directory Users and Computers - DEV2 - [Console Root\Active Directory Users and Computers]', shows the same groups mapped into the 'Smartsite Group' under the 'SmartSite B.V.' organizational unit. This illustrates how global groups from one domain are represented as local groups within the Smartsite access structure.



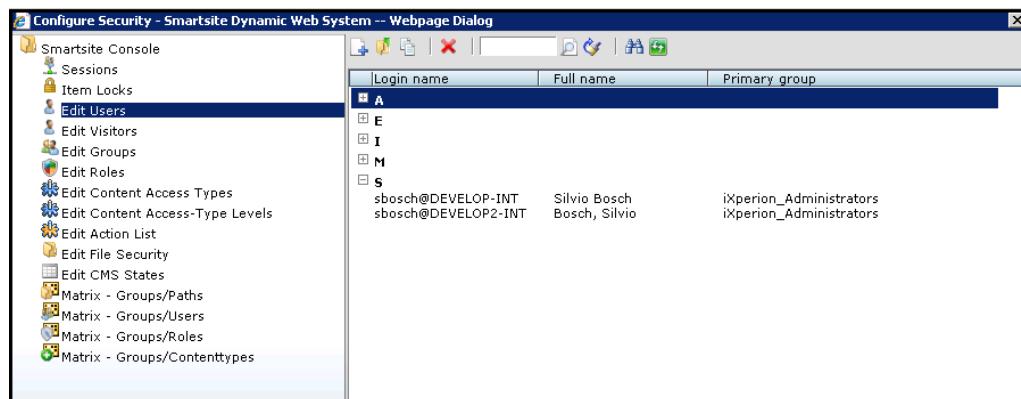
Seneca adviseert echter de groepsnamen op alle domeinen zoveel mogelijk hetzelfde te houden om het aantal groepen te beperken.

15.2.1 StoreFullyQualifiedLoginName

Doordat een gebruiker op meerdere domeinen onder dezelfde accountname kan voorkomen, dient de web.config parameter `StoreFullyQualifiedLoginName` altijd gelijk aan true te zijn.

```
<add name="StoreFullyQualifiedLoginName" value="true"/>
```

Hierdoor blijft bij het inloggen het gebruikers account uniek.



The screenshot shows the 'Edit Users' dialog in the Smartsite Dynamic Web System. On the left is a navigation tree with items like Sessions, Item Locks, Edit Users, Edit Visitors, etc. The main pane displays a table of users. One user, 'sbosch@DEVELOP-INT', is selected. The table columns are 'Login name', 'Full name', and 'Primary group'. The user's details are shown: 'sbosch@DEVELOP-INT', 'Silvio Bosch', and 'iXperion_Administrators'. This demonstrates how a single user account is represented across multiple domains.

Implementatiehandleiding Active Directory voor Smartsite iXperion

- ⚠ Let op:** Wanneer er een smoelenboek applicatie wordt gebruikt, dan dient deze rekening te houden met de domeinnaam in de accountnaam.

15.3 Web.config multi-domaining

Ten opzichte van de enkele AD koppeling dient bij multi-domaing alleen de web.config te worden uitgebreid met informatie over de andere domeinen.

```
<?xml version="1.0" encoding="utf-8"?>
<!--
Note: As an alternative to hand editing this file you can use the
web admin tool to configure settings for your application. Use
the Website->Asp.Net Configuration option in Visual Studio.
A full list of settings and comments can be found in
machine.config.comments usually located in
\Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <configSections>
        <!-- ADS SETTING DEFINE ActiveDirectoryConfiguration ENTRY -->
        <section name="Smartsite.ConfigurationSource"
type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.ConfigurationSourceSection
, Smartsite.Diagnostics.Logging, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=5fdb12a67e027fb6"/>
<section name="ADDevelop.Configuration"
type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security"/>
<section name="ADDevelop2.Configuration"
type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security"/>
    </configSections>
    <connectionStrings>
        <!-- ADS SETTING Connection string must be UPPERCASE -->
<add name="ADDevelopConnection" connectionString="LDAP://DEVELOP.INTERN"/>
<add name="ADDevelop2Connection" connectionString="LDAP://DEVELOP2.INTERN"/>
    </connectionStrings>

    <ADDevelop.Configuration>
        <settings>
            <add name="SmartsiteAccessGroup" value="iXperionAccessGroup"/>
            <add name="ManagerAccessGroup" value="iXperionManagerAccessGroup"/>
            <add name="StoreFullyQualifiedLoginName" value="true"/>
            <add name="SearchBase" value="dc=develop,dc=intern"/>
            <add name="DatabaseId" value="manager"/>
        </settings>
        <membershipMappings>
            <add name="mm1" domain="Develop-int" providerName="ADDevelop"/>
            <add name="mm2" domain="Develop.intern" providerName="ADDevelop"/>
        </membershipMappings>
    </ADDevelop.Configuration>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<ADDevelop2.Configuration>
    <settings>
        <add name="SmartsiteAccessGroup" value="iXperionAccessGroup"/>
        <add name="ManagerAccessGroup" value="iXperionManagerAccessGroup"/>
        <add name="StoreFullyQualifiedLoginName" value="true"/>
        <add name="SearchBase" value="dc=develop2,dc=intern"/>
        <add name="DatabaseId" value="manager"/>
    </settings>
    <membershipMappings>
        <add name="mm1" domain="Develop2-int" providerName="ADDevelop2"/>
        <add name="mm2" domain="Develop2.intern" providerName="ADDevelop2"/>
    </membershipMappings>
</ADDevelop2.Configuration>
<!-- ADS SETTING Smartsite ActiveDirectory Configuration Groups --&gt;
&lt;appSettings/&gt;
&lt;system.web&gt;
    &lt;pages&gt;
        &lt;controls&gt;
            &lt;add tagPrefix="cms" assembly="Smartsite.AspNet.Bridge"
namespace="Smartsite.AspNet.Bridge"/&gt;
        &lt;/controls&gt;
    &lt;/pages&gt;
    &lt;!--
        Set compilation debug="true" to insert debugging
        symbols into the compiled page. Because this
        affects performance, set this value to true only
        during development.
    --&gt;
    &lt;globalization fileEncoding="utf-8"/&gt;
    &lt;compilation debug="False"&gt;
        &lt;assemblies&gt;
            &lt;clear/&gt;
            &lt;add assembly="Smartsite.Base"/&gt;
            &lt;add assembly="Smartsite.Runtime"/&gt;
            &lt;add assembly="Smartsite.AspNet.Bridge"/&gt;
            &lt;add assembly="Smartsite.Security"/&gt;
            &lt;add assembly="Smartsite.Web"/&gt;
            &lt;add assembly="Smartsite.Tools"/&gt;
            &lt;add assembly="Smartsite.Data"/&gt;
            &lt;add assembly="Smartsite.Scf"/&gt;
        &lt;/assemblies&gt;
    &lt;/compilation&gt;
    &lt;machineKey
validationKey="BAE0B6B7179DDB95D3B407E90A8D6F9CFA4EE21FDC1CF8B3635D6B28D83A3D448BE2427F
C6C9B458E58DA3C0DC4515C13E938D9AB704139CD91A1E109C800D00"
decryptionKey="C4725BC47252B4ABFA80A832DD891E9C74D0FF482A6A362C" validation="SHA1"/&gt;
        &lt;!--authentication mode="Windows"--&gt;
        &lt;!--identity impersonate="true"--&gt;
    &lt;!--
        The &lt;authentication&gt; section enables configuration
    --&gt;</pre>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
of the security authentication mode used by
ASP.NET to identify an incoming user.
-->
<!-- ADS SETTING Front-end authentication mode integrated security and
Explicit REMOVE Forms Login -->
    <authentication mode="Windows">
        <!-- <forms loginUrl="/Login" name="Smartsite" / -->
    </authentication>
    <authorization>
        <allow users="*"/>
    </authorization>
<!-- ADS SETTING defaultProvider="ADMembershipProvider" -->
<membership defaultProvider="ADDevelop" userIsOnlineTimeWindow="15">
<providers>
    <clear/>
<!-- ADS SETTING CHANGE connectionUsername and connectionPassword. Use user principal
name (username@domainname) syntax -->
```

```
<add applicationName="Smartsite" name="SqlMembershipProvider"
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"
enablePasswordRetrieval="true"
enablePasswordReset="true"
passwordFormat="Clear"
requiresQuestionAndAnswer="false"
writeExceptionsToEventLog="true"/>

<add applicationName="Smartsite" name="ADDevelop"
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider,
Smartsite.Security"
connectionStringName="ADDevelopConnection"
connectionUsername=iXperionADSadmin@Develop.intern
connectionPassword="*****"
settingsSectionName="ADDevelop.Configuration/>

<add applicationName="Smartsite" name="ADDevelop2"
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider,
Smartsite.Security"
connectionStringName="ADDevelop2Connection"
connectionUsername=iXperionADSadmin@Develop.intern
connectionPassword="*****"
settingsSectionName="ADDevelop2.Configuration/>
</providers>

</membership>
<!-- ADS SETTING SET defaultProvider="ADRoleProvider" -->
<roleManager defaultProvider="ADRoleProvider" enabled="true" cacheRolesInCookie="true"
cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/" cookieRequireSSL="false"
cookieSlidingExpiration="true" cookieProtection="All"/>
<providers>
<clear/>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```

<add name="ADRoleProvider" applicationName="Smartsite"
type="Smartsite.Security.Authorization.ActiveDirectoryRoleProvider, Smartsite.Security"
connectionStringName="DevelopConnection" writeExceptionsToEventLog="true"/>
<add applicationName="Smartsite" name="SqlRoleProvider"
type="Smartsite.Security.Authorization.SqlRoleProvider, Smartsite.Security"
connectionStringName="SmartsiteDbConnection" writeExceptionsToEventLog="false"/>
</providers>
</roleManager>
<!--
The <customErrors> section enables configuration
of what to do if/when an unhandled error occurs
during the execution of a request. Specifically,
it enables developers to configure html error pages
to be displayed in place of a error stack trace.

<customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">
<error statusCode="403" redirect="NoAccess.htm" />
<error statusCode="404" redirect="NotFound.htm" />
</customErrors>
-->
<customErrors mode="RemoteOnly" defaultRedirect="/Ned/error_page_nl.html">
<error statusCode="404" redirect="/Ned/error_page_nl.html"/>
</customErrors>
<identity impersonate="false"/>
<httpModules>
<!-- replace default FormsAuthentication with Smartsite one -->
<remove name="FormsAuthentication"/>
<!--add name="FormsAuthentication"
type="Smartsite.AspNet.Bridge.CmsFormsAuthenticationModule,Smartsite.AspNet.Bridge" /-->
<!--add name="ScriptModule" type="System.Web.Handlers.ScriptModule, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" /-->
<add type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge" name="ixbridge"/>
<add type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor"
name="ImageServer"/>
<add type="Smartsite.Pdf.PdfModule,Smartsite.Pdf" name="PdfModule"/>
<add name="ManagementInformation" type="Smartsite.ManagementInformation.SmiClient,
Smartsite.ManagementInformation"/>
</httpModules>
<httpHandlers>
<add verb="*" path="*.asmx" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory, System.Web.Extensions, Version=1.0.61025.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35"/>
<add verb="*" path="*_AppService.axd" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory, System.Web.Extensions, Version=1.0.61025.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35"/>
<add verb="GET,HEAD" path="ScriptResource.axd"
type="System.Web.Handlers.ScriptResourceHandler, System.Web.Extensions, Version=1.0.61025.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" validate="false"/>
<add verb="*" path="/*.*.net"
type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge"/>
<add path="/*.res/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge"/>
<add path="/*.res/*/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge"/>
</httpHandlers>
<anonymousIdentification enabled="true"/>
<profile enabled="true" automaticSaveEnabled="true" defaultProvider="SmartsiteProfileProvider"
inherits="Smartsite.Core.PersonalProfile, Smartsite.Runtime">
<providers>
<clear/>
<add name="SmartsiteProfileProvider" type="Smartsite.Core.ProfileProvider,
Smartsite.Runtime" ApplicationName="Smartsite" ApplicationGUID="7D95D073-2F92-4822-8C59-FC2DA67FB9A1"/>
</providers>
</profile>
</system.web>
<!-- cms virtual directory configuration (manager configuration) -->
<!--

```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
to test if the manager uses the configured HttpHandler as described below,  
run the following script from the Immediate Window in the manager:  
?Context.var(13,"hosttype")  
Result should be: Smartsite.Interop  
-->  
<location path="Members">  
    <system.web>  
        <authorization>  
            <deny users="?" />  
        </authorization>  
    </system.web>  
</location>  
<Smartsite.ConfigurationSource selectedSource="File Configuration Source">  
    <sources>  
        <add name="File Configuration Source"  
            type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.FileConfigurationSource, Smartsite.Diagnostics.Logging,  
            Version=1.0.0.0, Culture=neutral, PublicKeyToken=5fdb12a67e027fb6" filePath="..\Smartsite.Logging.Config"/>  
    </sources>  
</Smartsite.ConfigurationSource>  
<!-- WCF services configuration -->  
<!-- this is a minimal set of endpoints, for example the mex endpoints have been removed -->  
<system.serviceModel>  
    <services>  
        <!--Service for state synchronization between CMS and iXperion publication engine-->  
        <service name="Smartsite.Core.Services.StateSyncService"  
            behaviorConfiguration="StateSyncServiceBehavior">  
            <endpoint address="net.pipe://localhost/intranet/StateSyncService"  
                binding="netNamedPipeBinding" contract="Smartsite.Core.Services.IStateSyncService"/>  
        </service>  
        <!--Service providing interoperability between the manager and iXperion functionality.  
Used for rendering items (view & preview within the manager), AIM rendering, content validation, etc.-->  
        <service name="Smartsite.Core.Services.InteropService"  
            behaviorConfiguration="InteropServiceBehavior">  
            <endpoint address="net.pipe://localhost/intranet/InteropService"  
                binding="netNamedPipeBinding" bindingConfiguration="InteropServiceBinding"  
                contract="Smartsite.Core.Services.IInteropService"/>  
        </service>  
        <!--Service providing schema information to the SXML editor-->  
        <service name="Smartsite.Core.Services.SchemaService"  
            behaviorConfiguration="SchemaServiceBehavior">  
            <endpoint address="http://Intranet/intranet/SchemaService"  
                binding="basicHttpBinding" bindingConfiguration="SchemaServiceBinding"  
                contract="Smartsite.Core.Services.ISchemaService"/>  
        </service>  
        <!--Service for state synchronization between iXperion publication engine and subscribers  
to this service.-->  
        <service name="Smartsite.Core.Services.EventSynchronizationService"  
            behaviorConfiguration="EventSynchronizationServiceBehavior">  
            <endpoint address="http://intranet/intranet/EventSynchronizationService"  
                binding="wsDualHttpBinding" contract="Smartsite.Core.Services.IEventSubscriptionContract"/>  
        </service>  
        <!--Common service for managing CMS-->  
        <service name="Smartsite.Core.Services.ManagerService"  
            behaviorConfiguration="ManagerServiceBehavior">  
            <endpoint address="http://intranet/intranet/ManagerService"  
                binding="basicHttpBinding" contract="Smartsite.Core.Services.IManagerService"/>  
        </service>  
    </services>  
    <bindings>  
        <netNamedPipeBinding>  
            <binding name="InteropServiceBinding" maxReceivedMessageSize="1048576">  
                <readerQuotas maxStringContentLength="1048576" />  
            </binding>  
        </netNamedPipeBinding>  
        <wsHttpBinding>  
            <binding name="wsHttpBindingConfig">  
                <readerQuotas maxStringContentLength="32768" />  
            </binding>  
            <binding name="HitServiceBinding" maxReceivedMessageSize="100000000">  
                <readerQuotas maxStringContentLength="524288" />  
            </binding>  
        </wsHttpBinding>  
    </bindings>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```

      </binding>
    </wsHttpBinding>
    <basicHttpBinding>
      <binding name="cmsWebserviceSoapBinding">
        <readerQuotas maxStringContentLength="16384"/>
        <security mode="TransportCredentialOnly">
          <transport clientCredentialType="Basic" proxyCredentialType="None" realm="" />
        <message clientCredentialType="UserName" algorithmSuite="Default" />
      </security>
    </binding>
    <binding name="SchemaServiceBinding">
      <readerQuotas maxStringContentLength="32768"/>
    </binding>
  </basicHttpBinding>
  <wsDualHttpBinding>
    <binding name="WSDualHttpBinding_EventSubscriptionService">
      <readerQuotas maxStringContentLength="16384"/>
      <reliableSession ordered="true" inactivityTimeout="08:00:00"/>
      <security mode="Message">
        <message clientCredentialType="Windows" negotiateServiceCredential="true" algorithmSuite="Default" />
      </security>
    </binding>
  </wsDualHttpBinding>
</bindings>
<!-- client section, only used when running the TestSuite --&gt;
&lt;client&gt;
  &lt;!-- (client) endpoint definition used for connecting to the cmsWebservice --&gt;
  &lt;endpoint address="http://intranet/cms/manager.dws" binding="basicHttpBinding" bindingConfiguration="cmsWebserviceSoapBinding" contract="cmsWebserviceSoapPort" name="cmsWebserviceSoapPort" /&gt;
  &lt;!-- (client) endpoint definition used for connecting to the EventSubscription/EventSynchronization service --&gt;
  &lt;endpoint address="http://intranet/intranet/EventSynchronizationService" binding="wsDualHttpBinding" bindingConfiguration="WSDualHttpBinding_EventSubscriptionService" contract="Smartsite.Core.EventSynchronizationClient.EventSubscriptionService" name="WSDualHttpBinding_EventSubscriptionService" /&gt;
  &lt;!-- DEPRECATED Post-RC1 --&gt;
  &lt;!-- identity --&gt;
  &lt;userPrincipalName value="iXperion_Admin" /&gt;
&lt;/identity --&gt;
&lt;/endpoint&gt;
&lt;endpoint address="http://192.168.252.7:2020/Intranet/HitService" behaviorConfiguration="HitServiceBehavior" binding="wsHttpBinding" bindingConfiguration="HitServiceBinding" contract="Smartsite.ManagementInformation.Server.HitService" /&gt;
&lt;/client&gt;
&lt;!-- Uncomment diagnostics section to log the entire messages to the trace-log --&gt;
&lt;!--
&lt;diagnostics wmiProviderEnabled="true"&gt;
  &lt;messageLogging logEntireMessage="true" logMalformedMessages="true" logMessagesAtServiceLevel="true" logMessagesAtTransportLevel="true" maxMessagesToLog="3000" /&gt;
&lt;/diagnostics&gt;
--&gt;
&lt;behaviors&gt;
  &lt;serviceBehaviors&gt;
    &lt;behavior name="StateSyncServiceBehavior"/&gt;
    &lt;behavior name="InteropServiceBehavior"/&gt;
    &lt;behavior name="SchemaServiceBehavior"/&gt;
    &lt;behavior name="EventSynchronizationServiceBehavior"/&gt;
    &lt;behavior name="ManagerServiceBehavior"/&gt;
  &lt;/serviceBehaviors&gt;
  &lt;endpointBehaviors&gt;
    &lt;behavior name="HitServiceBehavior"&gt;
      &lt;dataContractSerializer maxItemsInObjectGraph="10000000" /&gt;
    &lt;/behavior&gt;
  &lt;/endpointBehaviors&gt;
&lt;/behaviors&gt;
</pre>

```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```

      </behavior>
    </endpointBehaviors>
  </behaviors>
</system.serviceModel>
<!-- Uncomment system.diagnostics section to enable trace-logging --&gt;
&lt;system.diagnostics&gt;
  &lt;trace autoflush="true"/&gt;
  &lt;sources&gt;
    &lt;source name="System.ServiceModel" switchValue="Error"&gt;
      &lt;listeners&gt;
        &lt;add name="traceListener"/&gt;
      &lt;/listeners&gt;
    &lt;/source&gt;
    &lt;source name="System.ServiceModel.MessageLogging"&gt;
      &lt;listeners&gt;
        &lt;add name="traceListener"/&gt;
      &lt;/listeners&gt;
    &lt;/source&gt;
  &lt;/sources&gt;
  &lt;sharedListeners&gt;
    &lt;add name="traceListener" type="System.Diagnostics.XmlWriterTraceListener, System,
Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
initializeData="E:\Sites\Intranet\LogFiles\WCF\Intranet.svclog"/&gt;
  &lt;/sharedListeners&gt;
&lt;/system.diagnostics&gt;
&lt;system.webServer&gt;
  &lt;modules&gt;
    &lt;add name="ixbridge" type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge"
preCondition="" /&gt;
    &lt;add name="ImageServer"
      type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor" preCondition="" /&gt;
      &lt;add name="PdfModule" type="Smartsite.Pdf.PdfModule,Smartsite.Pdf" preCondition="" /&gt;
      &lt;!-- update session module with modified preCondition --&gt;
      &lt;remove name="Session"/&gt;
      &lt;add name="Session" type="System.Web.SessionState.SessionStateModule" preCondition="" /&gt;
      &lt;!-- replace ASP.NET Forms Authentication with custom Smartsite one --&gt;
      &lt;remove name="FormsAuthentication"/&gt;
      &lt;!--add name="FormsAuthentication"
      type="Smartsite.AspNet.Bridge.CmsFormsAuthenticationModule,Smartsite.AspNet.Bridge" preCondition="" /--&gt;
      &lt;remove name="Profile"/&gt;
      &lt;add name="Profile" type="System.Web.Profile.ProfileModule" preCondition="" /&gt;
      &lt;remove name="AnonymousIdentification"/&gt;
      &lt;add name="AnonymousIdentification"
      type="System.Web.Security.AnonymousIdentificationModule" preCondition="" /&gt;
      &lt;remove name="ManagementInformation"/&gt;
      &lt;add name="ManagementInformation" type="Smartsite.ManagementInformation.SmiClient,
Smartsite.ManagementInformation" preCondition="" /&gt;
    &lt;/modules&gt;
    &lt;handlers&gt;
      &lt;add name="net" path="*.net" verb="*"
      type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge" resourceType="Unspecified" requireAccess="Script"
      preCondition="integratedMode,runtimeVersionv2.0" /&gt;
      &lt;add path="*/*.*" verb="*"
      type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge" name="Bridge" preCondition="" /&gt;
      &lt;add name="PubResourceHandler" path="/res/*" verb="*"
      type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" preCondition="" /&gt;
    &lt;/handlers&gt;
    &lt;defaultDocument&gt;
      &lt;files&gt;
        &lt;clear/&gt;
        &lt;add value="manager.dws"/&gt;
        &lt;add value="nederlands.net"/&gt;
      &lt;/files&gt;
    &lt;/defaultDocument&gt;
    &lt;!-- Disable detection of IIS6 / Classic mode ASP.NET configuration --&gt;
    &lt;validation validateIntegratedModeConfiguration="false"/&gt;
  &lt;/system.webServer&gt;
  &lt;location path="cms"&gt;
    &lt;system.web&gt;
</pre>

```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<globalization requestEncoding="iso-8859-1"/>
<!-- To upload large files -->
<httpRuntime maxRequestLength="2097151" executionTimeout="999999"
shutdownTimeout="999" requestLengthDiskThreshold="256"/>
<!-- authentication mode="None" -->
<!-- ADS SETTING CMS authentication mode integrated security -->
<authentication mode="Windows"/>
<authorization>
    <allow users="*"/>
    <!-- allow access for all users, the manager uses it's own
implementation for authenticating users -->
</authorization>
<httpModules>
    <remove name="FormsAuthentication"/>
</httpModules>
<httpHandlers>
    <!--clear the inherited httpHandlers-->
    <clear/>
    <!-- uncomment the WebserviceHandler entry when the site
participates within an Outscaling scenario -->
    <!-- <add verb="*" path="/cms/webservice.dws"
type="Smartsite.Interop.IIS.WebserviceHandler,Smartsite.Interop" /> -->
    <add verb="*" path="/cms/*.dws"
type="Smartsite.Interop.IIS.Handler,Smartsite.Interop"/>
</httpHandlers>
<compilation>
    <assemblies>
        <clear/>
    </assemblies>
</compilation>
</system.web>
<!-- IIS 7.0+ configuration -->
<system.webServer>
    <modules>
        <remove name="FormsAuthentication"/>
        <remove name="ixbridge"/>
        <remove name="ImageServer"/>
        <remove name="PdfModule"/>
    </modules>
    <handlers>
        <remove name="Bridge"/>
        <remove name="res1"/>
        <remove name="res2"/>
        <remove name="net"/>
        <remove name="PubResourceHandler"/>
        <add name="CMSInteropHandler" path="/cms/*.dws" verb="*"
type="Smartsite.Interop.IIS.Handler,Smartsite.Interop" preCondition="" />
    </handlers>
    <security>
        <requestFiltering>
            <requestLimits maxAllowedContentLength="204800000"/>
        </requestFiltering>
    </security>
</system.webServer>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

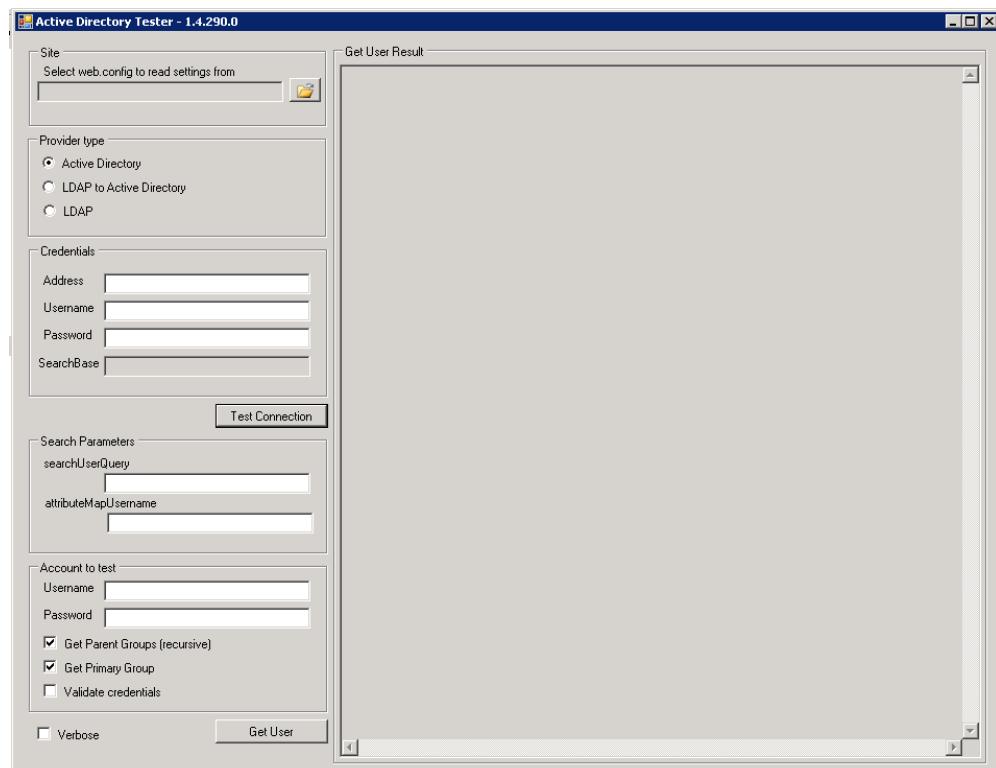
```
</security>
<defaultDocument>
    <files>
        <clear/>
        <add value="manager.dws"/>
    </files>
</defaultDocument>
<!-- Disable detection of IIS6 / Classic mode ASP.NET configuration
-->
<validation validateIntegratedModeConfiguration="false"/>
</system.webServer>
</location>
</configuration>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

15.4 Active Directory Tester

Met behulp van de Active Directory Tester kan de security configuratie die in de web.config is opgegeven worden getest.

De Active Directory Tester is te vinden in de Utilities\Active Directory Tester directory van de setup. Wanneer de web.config is geconfigureerd voor Active directory kun je deze na het starten van de Active Directory Tester direct inlezen.

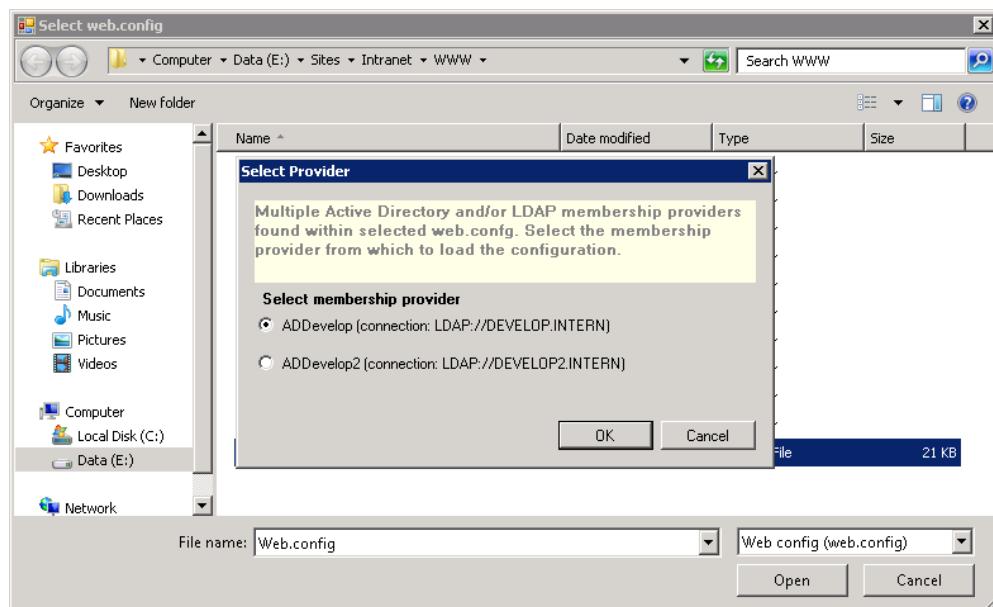


De Active Directory Tester

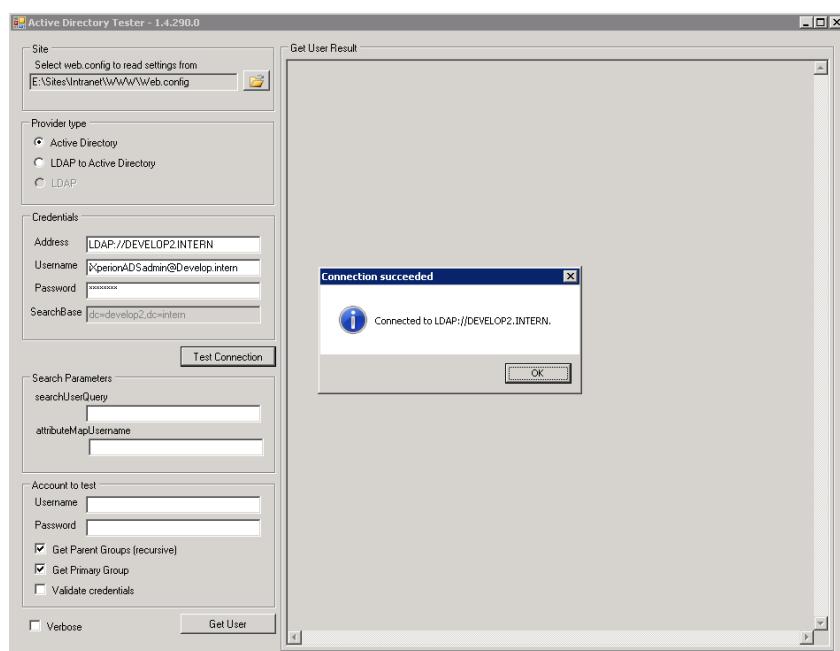


Selecteer de web.config in de www van de site.

Implementatiehandleiding Active Directory voor Smartsite iXperion

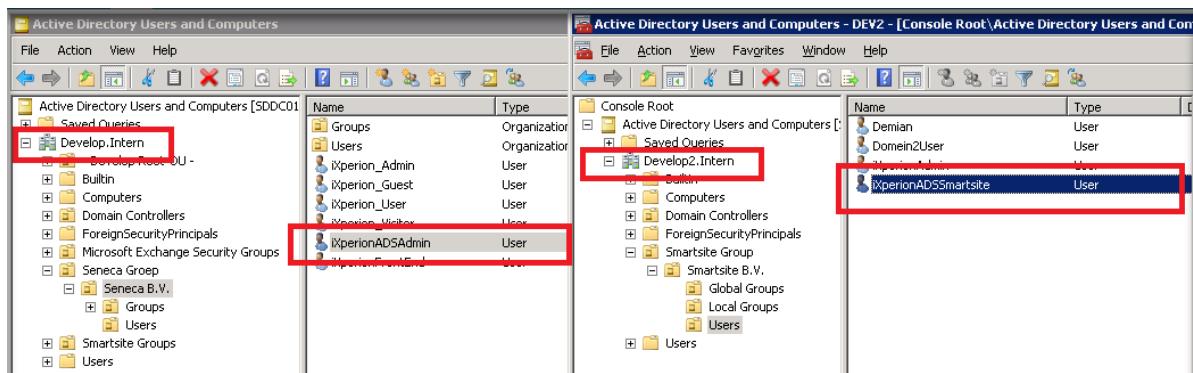
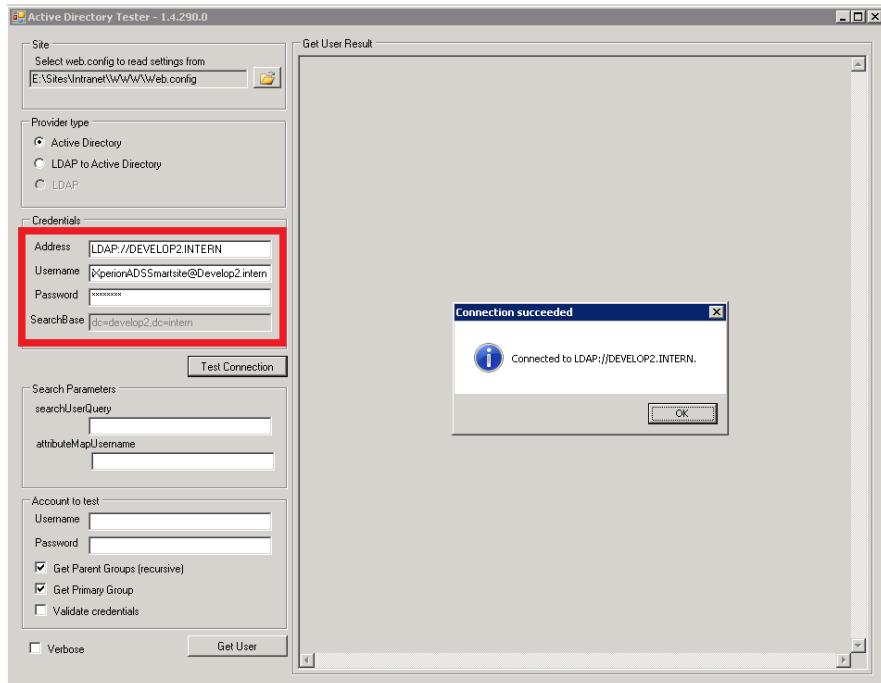


Wanneer er spraken is van meerdere domeinen zal er eerst de “Selecteer Provider” dialog verschijnen.



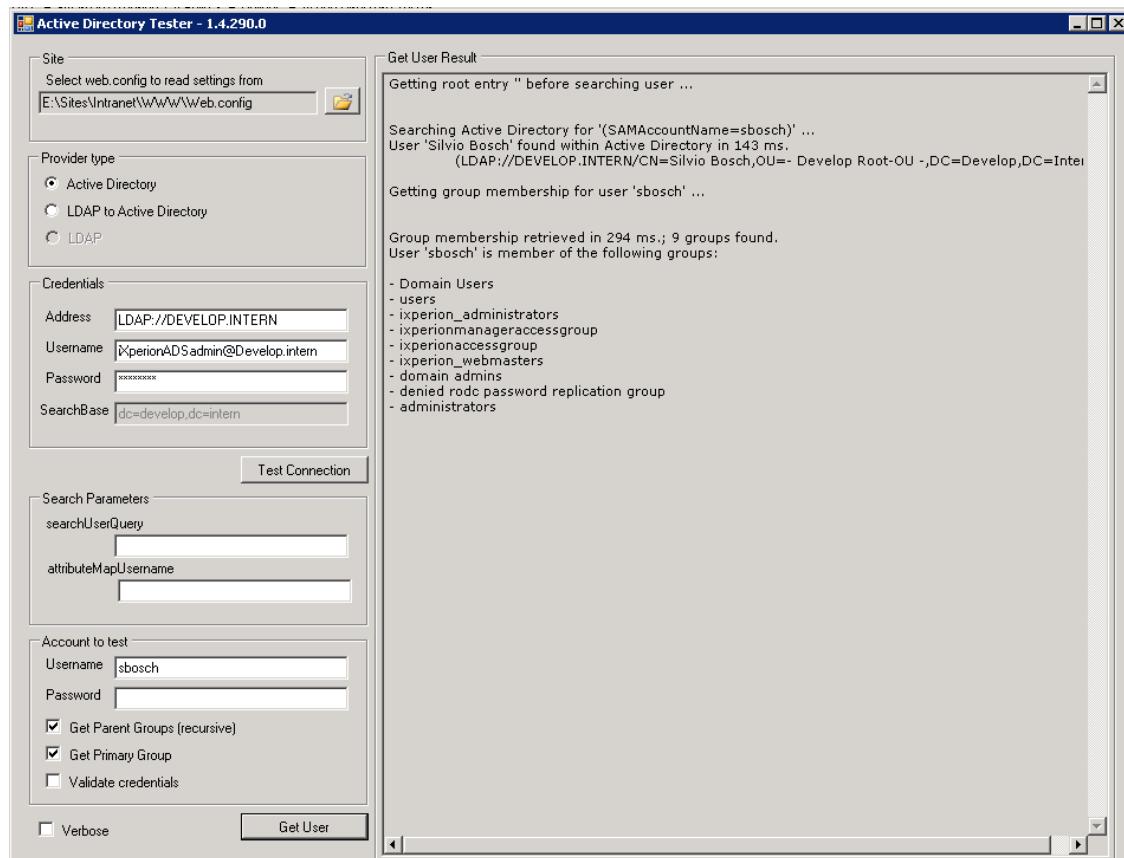
De gegevens worden automatisch ingevuld en je kunt de connectie naar het geselecteerde domein testen via de “Test connection” knop. Als de gegevens kloppen zal er een “Connection succeeded” dialoog worden getoond.

Implementatiehandleiding Active Directory voor Smartsite iXperion



Wanneer er spraken is van een tweede domein, dan kan hiervoor eventueel een ander account worden opgegeven in de web.config.

Implementatiehandleiding Active Directory voor Smartsite iXperion

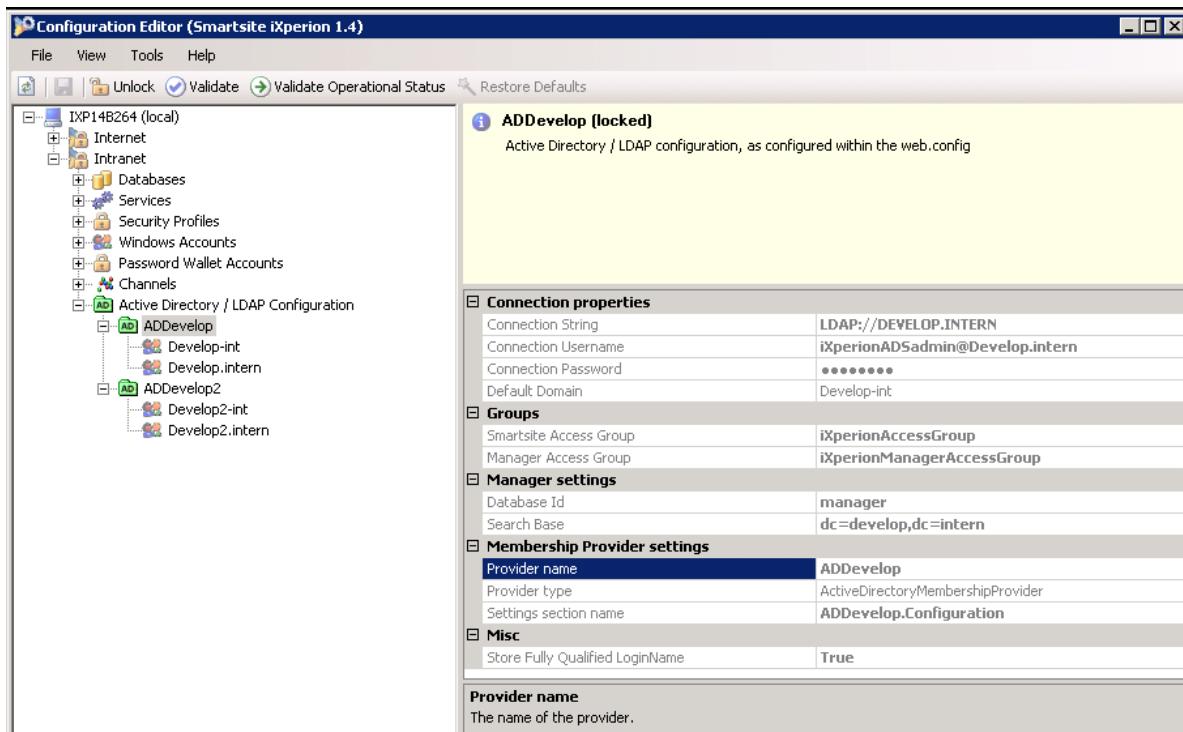


Na het invullen van een account username kunnen diens groepen worden gevraagd. Een gebruiker van de redactie zijde van Smartsite iXperion dient dan altijd lid te zijn van minimaal de iXperionManagerAccess groep en de iXperionAccess groep.

Implementatiehandleiding Active Directory voor Smartsite iXperion

15.5 Multi-domain via Smartsite iXperion ConfigEditor

De Smartsite iXperion ConfigEditor kan gebruikt worden om de configuratie te vereenvoudigen.



⚠ Let op: de Smartsite iXperion configeditor stel niet het IIS en web.config authenticatie mechanisme in, dit dient nog steeds handmatig te gebeuren.



Tip: Nadat je de configuratie via de configEditor hebt toegevoegd, controleer dan handmatig al de instellingen in de Web.config zoals hierboven beschreven.

Implementatiehandleiding Active Directory voor Smartsite iXperion

16 Smartsite iXperion LDAP koppeling met Novell eDirectory

16.1 Specifieke Membership Provider

Smartsite iXperion biedt standaard ondersteuning voor LDAP servers, zoals Novell eDirectory. Het enige verschil t.o.v. een Active directory configuratie is dat er een specifieke Membership Provider in de Web.config van de site dient te worden opgegeven om te kunnen koppelen met Novell eDirectory.

16.2 Forms authentication

Omdat Novell eDirectory geen integrated security ondersteunt is het in de front-end alleen mogelijk de gebruikers via forms authentication te laten inloggen. Hierbij worden de accountgegevens gevalideerd tegen de geconfigureerde Novell LDAP server.

Ook voor de backend geldt dat geen integrated security wordt ondersteunt en zal bij inloggen altijd de anonymous/basic authentication dialog worden getoond.

16.3 Configuration Web.config

16.3.1 Connection string

De configuration.ConnectionStrings sectie in de web.config bevat net als bij de Active directory configuratie het LDAP server adres. Echter dient alleen het IP adres te worden gespecificeerd zonder de LDAP:// syntax.

```
<connectionStrings>
    <add name="LDAPConnection" connectionString="ip-address" />
</connectionStrings>
```

16.3.2 Membership provider

Registreer de membership provider in configuration/system.web/membership en zet de defaultProvider.

```
<membership defaultProvider="ldap">
    (...)

    <providers>
        <clear />
        <add name="ldap" applicationName="Smartsite"
            type="Smartsite.Security.Authentication.LDAPMembershipProvider,
            Smartsite.Security"
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
    connectionStringName="LDAPConnection"
    connectionUsername="cn=adminusername,o=organization"
    connectionPassword="yourpassword"
    port="636" useSSL="true"
    bypassCertificateValidation="true"
  />
  (... do not remove the SqlMembershipProvider ...)
</providers>
</membership>
```

- **connectionStringName**

De connectionStringname dient te verwijzen naar een connection string opgegeven in de connectionStrings sectie van dezelfde web.config.

- **connectionUsername, connectionPassword**

In de Membership Provider sectie dienen de account gegevens te worden opgegeven van het account dat connectie maakt met de Novell eDirectory (iXperionNovelladmin).

In de connectionUsername dient het Novell account in distinguishedName syntax te worden opgegeven: cn=connectionUsername,SearchBase

- **searchUserQuery (optioneel)**

Optioneel kan de standaard LDAP query worden overschreven die gebruikt wordt om de gebruiker gegevens op te halen.

Default is dit: (&(ObjectClass=Person)(cn={0}))

- **port (optioneel)**

Optioneel kan het LDAP port nummer worden opgegeven. Wanneer *useSSL* gelijk aan true is dan is de **port** standaard 636.

Voorbeeld Anonymous 389 connectie

```
<add name="novell" applicationName="Smartsite"
  type="Smartsite.Security.Authentication.LDAPMembershipProvider,
  Smartsite.Security" connectionStringName="LDAPConnection"
  connectionUsername="cn=admin,o=SENECA" connectionPassword="admin" port="389"
  useSSL="false"/>
```

Voorbeeld SSL 636 connectie

```
<add name="novell" applicationName="Smartsite"
  type="Smartsite.Security.Authentication.LDAPMembershipProvider,
  Smartsite.Security" connectionStringName="LDAPConnection"
  connectionUsername="cn=admin,o=seneca" connectionPassword="admin" port="636"
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
useSSL="true" certificateLocation="E:\Sites\cert.der"  
bypassCertificateValidation="true" />
```

De poorten die kunnen worden opgegeven dienen overeen te komen met de poorten opgegeven in Novell eDirectory.

- **useSSL (optioneel)**
Defaults is *false*. Wanneer *useSSL* gelijk aan *true* is dan is de **port** standaard 636.
- **bypassCertificateValidation (optioneel)**
Wanneer een SSL connectie wordt gebruikt dan kan de certificate validatie resulteren in een slechte performance. Wanneer **bypassCertificateValidation** gelijk is aan *true* dan zal de LDAP membership provider deze validatie overslaan.
Defaults is *false*.
- **certificateLocation (optioneel)**
In deze parameter kan de locatie van het SSL client certificaat worden opgegeven.
- **groupMembershipAttribute (optioneel)**
Hiermee kan het standaard group membership attribute worden overschreven.
Defaults is *groupMembership*.

16.3.3 Settings

De Smartsite LDAP membership provider beschik over zijn eigen config sectie in configuration/configSections.

```
<configSections>  
  (...)  
  <section name="Smartsite.LDAPConfiguration"  
    type="Smartsite.Security.ActiveDirectoryConfigurationSection,  
    Smartsite.Security" />  
</configSections>
```

Net als bij de Active directory configuratie bevat de LDAP configuratie een sectie om de SmartsiteAccess en SmartsiteManagerAccess groep te definieren:
configuration/Smartsite.LDAPConfiguration

```
<Smartsite.LDAPConfiguration>  
  <settings>  
    <add name="SmartsiteAccessGroup" value="groupname"/>  
    <add name="ManagerAccessGroup" value="manager access groupname" />  
    <add name="StoreFullyQualifiedLoginName" value="false"/>  
    <add name="SearchBase" value="ou=...,o=..." />  
    <add name="DatabaseId" value="database id" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</settings>
<membershipMappings>
    <add name="mm1" domain="yourdomain" providerName="ldap" />
</membershipMappings>
</Smartsite.LDAPConfiguration>
```

- ⚠** Voor de Smartsite.LDAPConfiguration gelden dezelfde voorwaarden zoals beschreven in hoofdstuk: 6.6.3 Smartsite.ActiveDirectoryConfiguration

16.4 Forms authentication

16.4.1 Front-end

Zoals eerder aangegeven werkt de LDAP membership provider in de front-end alleen in combinatie met de Forms authentication.

```
<authentication mode="Forms">
    <forms loginUrl="/Login" name="Smartsite" />
</authentication>
```

16.4.2 Back-end

Voor de Back-end geldt dat we alleen gebruik kunnen maken van basic authentication. In de <location path="cms"> sectie dient de authentication mode daarom op None te staan.

```
<location path="cms">
    (...)

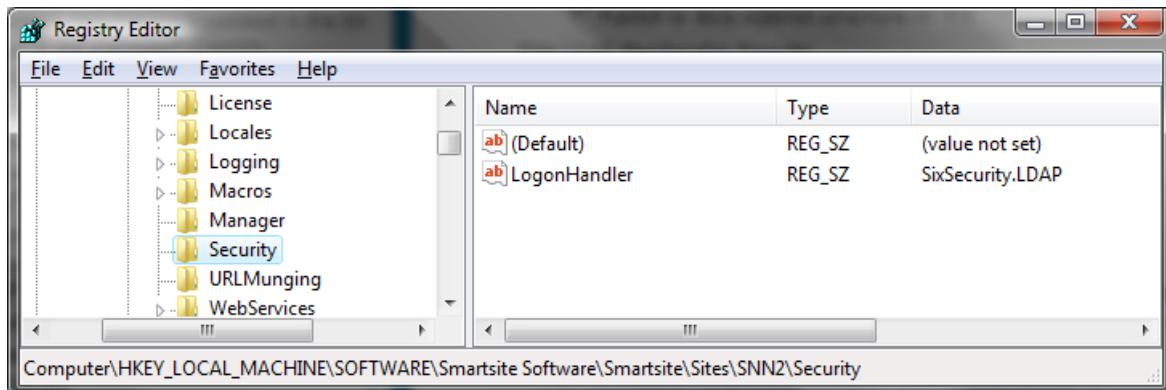
    <authentication mode="None" />
    <authorization>
        <allow users="*" />
    </authorization>
    (...)

</location>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

16.4.3 Registry configuratie

Net als bij de Active Directory configuratie wordt voor de backend gebruik gemaakt van de SixSecurity.LDAP logonHandler.



Web.config voorbeeld Novell eDirectory:

```
<?xml version="1.0" encoding="utf-8"?>
<!--
Note: As an alternative to hand editing this file you can use the
web admin tool to configure settings for your application. Use
the Website->Asp.Net Configuration option in Visual Studio.
A full list of settings and comments can be found in
machine.config.comments usually located in
\Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <configSections>
        <section name="Smartsite.LDAPConfiguration"
type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security" />
        <section name="Smartsite.ConfigurationSource"
type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.ConfigurationSourceSection
, Smartsite.Diagnostics.Logging, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=5fdb12a67e027fb6" />
    </configSections>
    <appSettings />
    <connectionStrings>
        <add name="LDAPConnection" connectionString="192.31.142.123" />
    </connectionStrings>
    <Smartsite.LDAPConfiguration>
        <settings>
            <add name="SmartsiteAccessGroup" value="Smartsite Software" />
            <add name="ManagerAccessGroup" value="ManagerAccessLocal" />
            <add name="StoreFullyQualifiedLoginName" value="false" />
            <add name="SearchBase" value="ou=SMARTSITE_GROUPS,o=SENECA" />
        </settings>
    </Smartsite.LDAPConfiguration>

```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<add name="DatabaseId" value="manager" />
</settings>
<membershipMappings>
    <add name="mml" domain="smartsite" providerName="novell" />
</membershipMappings>
</Smartsite.LDAPConfiguration>
<system.web>
    <pages>
        <controls>
            <add tagPrefix="cms" assembly="Smartsite.AspNet.Bridge"
namespace="Smartsite.AspNet.Bridge" />
        </controls>
    </pages>
    <!--
        Set compilation debug="true" to insert debugging
        symbols into the compiled page. Because this
        affects performance, set this value to true only
        during development.
    -->
    <globalization fileEncoding="utf-8" />
    <compilation debug="False">
        <assemblies>
            <clear />
        </assemblies>
    </compilation>
    <machineKey
validationKey="BAE0B6B7179DDB95D3B407E90A8D6F9CFA4EE21FDC1CF8B3635D6B28D83A3D448BE2427F
C6C9B458E58DA3C0DC4515C13E938D9AB704139CD91A1E109C800D00"
decryptionKey="C4725BC47252B4ABFA80A832DD891E9C74D0FF482A6A362C" validation="SHA1" />
        <!--authentication mode="Windows"-->
        <!--identity impersonate="true"-->
    <!--
        The <authentication> section enables configuration
        of the security authentication mode used by
        ASP.NET to identify an incoming user.
    -->
    <authentication mode="Forms">
        <forms loginUrl="/Login" name="Smartsite" />
    </authentication>
    <authorization>
        <allow users="*" />
    </authorization>
    <anonymousIdentification enabled="true" />
    <profile enabled="true" automaticSaveEnabled="true"
defaultProvider="SmartsiteProfileProvider" inherits="Smartsite.Core.PersonalProfile,
Smartsite.Runtime">
        <providers>
            <clear />
            <add name="SmartsiteProfileProvider" type="Smartsite.Core.ProfileProvider,
Smartsite.Runtime" ApplicationName="Smartsite" ApplicationGUID="DB487110-2809-42F0-
BDA0-742C088C75F3" />
        </providers>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
</profile>
<membership defaultProvider="novell" userIsOnlineTimeWindow="15">
    <providers>
        <clear />
        <add name="novell" applicationName="Smartsite"
type="Smartsite.Security.Authentication.LDAPMembershipProvider, Smartsite.Security"
connectionStringName="LDAPConnection" connectionUsername="cn=admin,o=seneca"
connectionPassword="admin" port="636" useSSL="true"
certificateLocation="E:\Sites\cert.der" bypassCertificateValidation="true" />
        <add applicationName="Smartsite" name="SqlMembershipProvider"
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"
enablePasswordRetrieval="true" enablePasswordReset="true" passwordFormat="Clear"
requiresQuestionAndAnswer="false" writeExceptionsToEventLog="true" />
    </providers>
</membership>
<roleManager defaultProvider="SqlRoleProvider" enabled="true"
cacheRolesInCookie="true" cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/"
cookieRequireSSL="false" cookieSlidingExpiration="true" cookieProtection="All">
    <providers>
        <clear />
        <add applicationName="Smartsite" name="SqlRoleProvider"
type="Smartsite.Security.Authorization.SqlRoleProvider, Smartsite.Security"
connectionStringName="SmartsiteDbConnection" writeExceptionsToEventLog="false" />
    </providers>
</roleManager>
<!--
    The <customErrors> section enables configuration
    of what to do if/when an unhandled error occurs
    during the execution of a request. Specifically,
    it enables developers to configure html error pages
    to be displayed in place of a error stack trace.

    <customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">
        <error statusCode="403" redirect="NoAccess.htm" />
        <error statusCode="404" redirect="NotFound.htm" />
    </customErrors>
-->
<customErrors mode="Off" />
<httpModules>
    <add type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge" name="ixbridge"
/>
    <add type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor"
name="ImageServer" />
        <add type="Smartsite.Pdf.PdfModule,Smartsite.Pdf" name="PdfModule" />
        <add name="ManagementInformation"
type="Smartsite.ManagementInformation.SmiClient, Smartsite.ManagementInformation" />
    </httpModules>
    <httpHandlers>
        <add verb="*" path="*/*.net"
type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge" />
        <add verb="*" path="/res/*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" />
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<add verb="*" path="/res/*/*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" />
</httpHandlers>
</system.web>
<!-- cms virtual directory configuration (manager configuration) -->
<!--
    to test if the manager uses the configured HttpHandler as described below,
    run the following script from the Immediate Window in the manager:
    ?Context.var(13,"hosttype")
    Result should be: Smartsite.Interop
-->
<location path="cms">
<system.web>
    <httpRuntime maxRequestLength="204800" executionTimeout="360" />
    <globalization requestEncoding="iso-8859-1" />
    <authentication mode="None" />
    <authorization>
        <allow users="*" />
        <!-- allow access for all users, the manager uses it's own implementation for
authenticating users -->
    </authorization>
    <httpModules>
        <!-- clear the inherited httpModules -->
        <clear />
        <!-- uncomment WindowsAuthentication when you want to use Windows Integrated
Security (<authentication mode="Windows" />) -->
        <!-- <add name="WindowsAuthentication"
type="System.Web.Security.WindowsAuthenticationModule"/> -->
        <add name="Session" type="System.Web.SessionState.SessionStateModule" />
    </httpModules>
    <httpHandlers>
        <clear />
        <!--clear the inherited httpHandlers-->
        <add verb="*" path="/cms/webservice.dws"
type="Smartsite.Interop.IIS.WebServiceHandler,Smartsite.Interop" />
        <add verb="*" path="/cms/*.dws"
type="Smartsite.Interop.IIS.Handler,Smartsite.Interop" />
    </httpHandlers>
    <compilation>
        <assemblies>
            <clear />
        </assemblies>
    </compilation>
</system.web>
<!-- IIS 7.0+ configuration -->
<system.webServer>
    <modules>
        <remove name="ixbridge" />
        <remove name="ImageServer" />
        <remove name="PdfModule" />
    </modules>
    <handlers>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<remove name="PubResourceHandler" />
<remove name="Bridge" />
<remove name="net" />
<add name="CMSInteropHandler" path="/cms/*.dws" verb="*"
type="Smartsite.Interop.IIS.Handler,Smartsite.Interop" preCondition="" />
</handlers>
<security>
<requestFiltering>
<requestLimits maxAllowedContentLength="204800000" />
</requestFiltering>
</security>
<defaultDocument>
<files>
<clear />
<add value="manager.dws" />
</files>
</defaultDocument>
<!-- Disable detection of IIS6 / Classic mode ASP.NET configuration -->
<validation validateIntegratedModeConfiguration="false" />
</system.webServer>
</location>
<location path="Members">
<system.web>
<authorization>
<deny users="?" />
</authorization>
</system.web>
</location>
<Smartsite.ConfigurationSource selectedSource="File Configuration Source">
<sources>
<add name="File Configuration Source"
type="Smartsite.Diagnostics.LoggingBase.Common.Configuration.FileConfigurationSource,
Smartsite.Diagnostics.Logging, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=5fdb12a67e027fb6" filePath="..../Smartsite.Logging.Config" />
</sources>
</Smartsite.ConfigurationSource>
<!-- WCF services configuration -->
<!-- this is a minimal set of endpoints, for example the mex endpoints have been
removed -->
<system.serviceModel>
<services>
<!--Service for state synchronization between CMS and iXperion publication
engine-->
<service name="Smartsite.Core.Services.StateSyncService"
behaviorConfiguration="StateSyncServiceBehavior">
<endpoint address="net.pipe://localhost/Intranet/StateSyncService"
binding="netNamedPipeBinding" contract="Smartsite.Core.Services.IStateSyncService" />
</service>
<!--Service providing interoperability between the manager and iXperion
functionality. Used for rendering items (view & preview within the manager), AIM
rendering, content validation, etc.-->
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<service name="Smartsite.Core.Services.InteropService"
behaviorConfiguration="InteropServiceBehavior">
    <endpoint address="net.pipe://localhost/Intranet/InteropService"
binding="netNamedPipeBinding" bindingConfiguration="InteropServiceBinding"
contract="Smartsite.Core.Services.IInteropService" />
</service>
<!--Service providing schema information to the SXML editor-->
<service name="Smartsite.Core.Services.SchemaService"
behaviorConfiguration="SchemaServiceBehavior">
    <endpoint address="http://Intranet/Intranet/SchemaService"
binding="basicHttpBinding" bindingConfiguration="SchemaServiceBinding"
contract="Smartsite.Core.Services.ISchemaService" />
</service>
<!--Service for state synchronization between iXperion publication engine and
subscribers to this service.-->
<service name="Smartsite.Core.Services.EventSynchronizationService"
behaviorConfiguration="EventSynchronizationServiceBehavior">
    <endpoint address="http://Intranet/Intranet/EventSynchronizationService"
binding="wsDualHttpBinding"
contract="Smartsite.Core.Services.IEventSubscriptionContract" />
</service>
<!--Common service for managing CMS-->
<service name="Smartsite.Core.Services.ManagerService"
behaviorConfiguration="ManagerServiceBehavior">
    <endpoint address="http://Intranet/Intranet/ManagerService"
binding="basicHttpBinding" contract="Smartsite.Core.Services.IManagerService" />
</service>
</services>
<bindings>
    <netNamedPipeBinding>
<binding name="InteropServiceBinding" maxReceivedMessageSize="1048576"><readerQuotas
maxStringContentLength="1048576" /></binding>
</netNamedPipeBinding>
<wsHttpBinding>
<binding name="wsHttpBindingConfig"><readerQuotas maxStringContentLength="32768"
/></binding>
<binding name="HitServiceBinding" maxReceivedMessageSize="100000000"><readerQuotas
maxStringContentLength="524288" /></binding>
</wsHttpBinding>
<basicHttpBinding>
<binding name="cmsWebserviceSoapBinding"><readerQuotas maxStringContentLength="16384"
/><security mode="TransportCredentialOnly"><transport clientCredentialType="Basic"
proxyCredentialType="None" realm="" /><message clientCredentialType="UserName"
algorithmSuite="Default" /></security></binding>
<binding name="SchemaServiceBinding"><readerQuotas maxStringContentLength="32768"
/></binding>
</basicHttpBinding>
<wsDualHttpBinding>
<binding name="WSDualHttpBinding_EventSubscriptionService"><readerQuotas
maxStringContentLength="16384" /><reliableSession ordered="true"
inactivityTimeout="08:00:00" /><security mode="Message"><message
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
clientCredentialType="Windows" negotiateServiceCredential="true"
algorithmSuite="Default" /></security></binding>
</wsDualHttpBinding>
</bindings>
<!-- client section, only used when running the TestSuite -->
<client>
    <!-- (client) endpoint definition used for connecting to the cmsWebservice -->
    <endpoint address="http://Intranet/cms/manager.dws" binding="basicHttpBinding"
bindingConfiguration="cmsWebserviceSoapBinding" contract="cmsWebserviceSoapPort"
name="cmsWebserviceSoapPort" />
    <!-- (client) endpoint definition used for connecting to the
EventSubscription/EventSynchronization service -->
    <endpoint address="http://Intranet/Intranet/EventSynchronizationService"
binding="wsDualHttpBinding"
bindingConfiguration="WSDualHttpBinding_EventSubscriptionService"
contract="Smartsite.Core.EventSynchronizationClient.EventSubscriptionService"
name="WSDualHttpBinding_EventSubscriptionService" />
    <endpoint address="http://localhost:2020/mysite/HitService"
behaviorConfiguration="HitServiceBehavior" binding="wsHttpBinding"
bindingConfiguration="HitServiceBinding"
contract="Smartsite.ManagementInformation.Server.HitService" />
</client>
<!-- Uncomment diagnostics section to log the entire messages to the trace-log -->
<!--
    <diagnostics wmiProviderEnabled="true">
        <messageLogging
            logEntireMessage="true"
            logMalformedMessages="true"
            logMessagesAtServiceLevel="true"
            logMessagesAtTransportLevel="true"
            maxMessagesToLog="3000"
        />
    </diagnostics>
-->
<behaviors>
    <serviceBehaviors>
        <behavior name="StateSyncServiceBehavior" />
        <behavior name="InteropServiceBehavior" />
        <behavior name="SchemaServiceBehavior" />
        <behavior name="EventSynchronizationServiceBehavior" />
        <behavior name="ManagerServiceBehavior" />
    </serviceBehaviors>
    <endpointBehaviors>
        <behavior name="HitServiceBehavior">
            <dataContractSerializer maxItemsInObjectGraph="10000000" />
        </behavior>
    </endpointBehaviors>
</behaviors>
</system.serviceModel>
<!-- The system.diagnostics section enables WCF trace-logging -->
<system.diagnostics>
    <sources>
        <source name="System.ServiceModel" switchValue="Error">
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

```
<listeners>
    <add name="traceListener" />
</listeners>
</source>
</sources>
<sharedListeners>
    <add name="traceListener" type="System.Diagnostics.XmlWriterTraceListener,
System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
initializeData="E:\Sites\Intranet\LogFiles\WCF\Intranet.svclog" />
</sharedListeners>
</system.diagnostics>
<!-- IIS 7.0+ configuration -->
<system.webServer>
    <modules>
        <add name="ixbridge" type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge"
preCondition="" />
        <add name="ImageServer"
type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor"
preCondition="" />
        <add name="PdfModule" type="Smartsite.Pdf.PdfModule,Smartsite.Pdf"
preCondition="" />
        <!-- update session module with modified preCondition -->
        <remove name="Session" />
        <add name="Session" type="System.Web.SessionState.SessionStateModule"
preCondition="" />
        <!-- replace ASP.NET Forms Authentication with custom Smartsite one (when using
Forms authentication; otherwise remove the two lines below) -->
        <remove name="FormsAuthentication" />
        <add name="FormsAuthentication"
type="Smartsite.AspNet.Bridge.CmsFormsAuthenticationModule,Smartsite.AspNet.Bridge"
preCondition="" />
        <remove name="Profile" />
        <add name="Profile" type="System.Web.Profile.ProfileModule" preCondition="" />
        <remove name="AnonymousIdentification" />
        <add name="AnonymousIdentification"
type="System.Web.Security.AnonymousIdentificationModule" preCondition="" />
        <remove name="ManagementInformation" />
        <add name="ManagementInformation"
type="Smartsite.ManagementInformation.SmiClient, Smartsite.ManagementInformation"
preCondition="" />
    </modules>
    <handlers>
        <add name="PubResourceHandler" path="/res/*" verb="*"
type="Smartsite.AspNet.Bridge.ResourceHandler,Smartsite.AspNet.Bridge" preCondition="" />
        <add name="net" path="*.net" verb="*"
type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge"
resourceType="Unspecified" requireAccess="Script"
preCondition="integratedMode,runtimeVersionv2.0" />
        <add name="Bridge" path="*/*.net" verb="*"
type="Smartsite.AspNet.Bridge.Handler,Smartsite.AspNet.Bridge" preCondition="" />
    </handlers>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

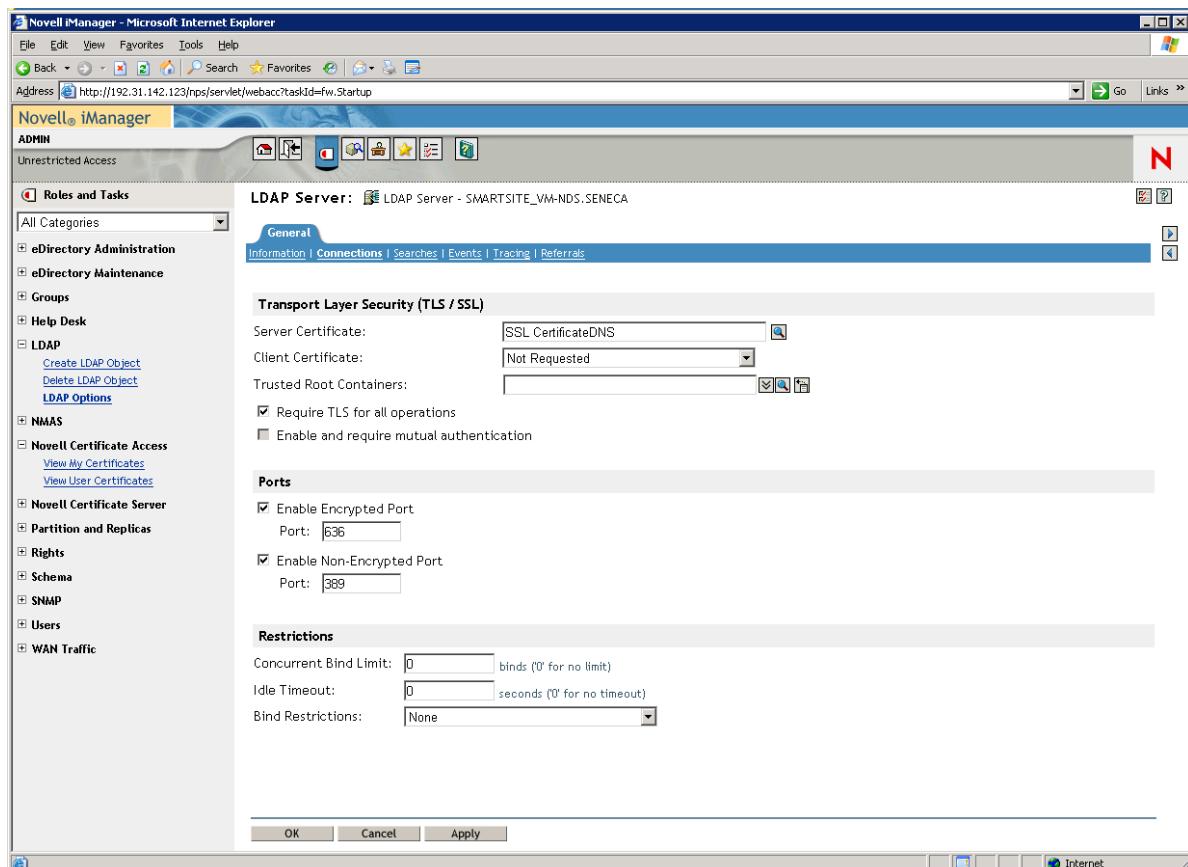
```
<defaultDocument>
  <files>
    <clear />
    <add value="manager.dws" />
    <add value="smartsite.net" />
  </files>
</defaultDocument>
<!-- Disable detection of IIS6 / Classic mode ASP.NET configuration -->
<validation validateIntegratedModeConfiguration="false" />
</system.webServer>
</configuration>
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

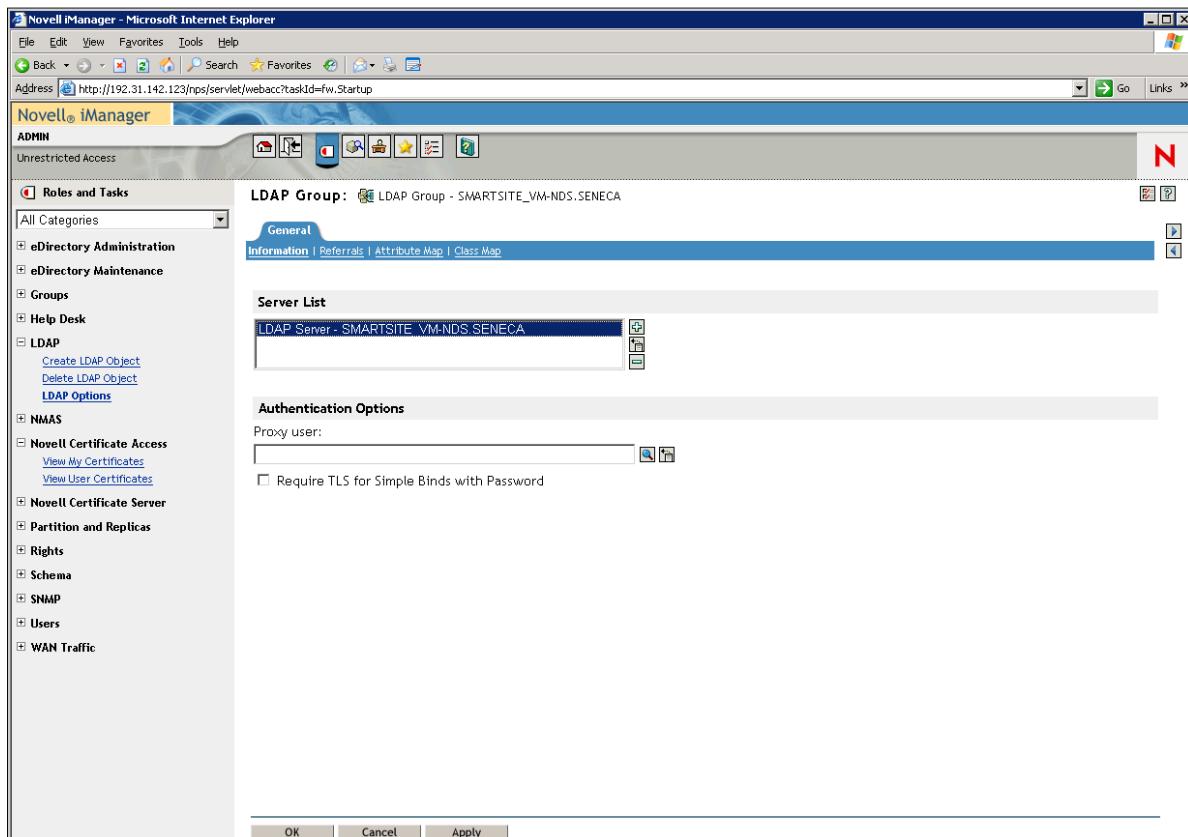
17 Novell configuratie

17.1 TLS/SSL en poort configuratie

```
<add name="novell" applicationName="Smartsite"
type="Smartsite.Security.Authentication.LDAPMembershipProvider, Smartsite.Security"
connectionStringName="LDAPConnection" connectionUsername="cn=admin,o=seneca"
connectionPassword="admin" port="636" useSSL="true"
certificateLocation="E:\Sites\cert.der" bypassCertificateValidation="true" />
```



Implementatiehandleiding Active Directory voor Smartsite iXperion

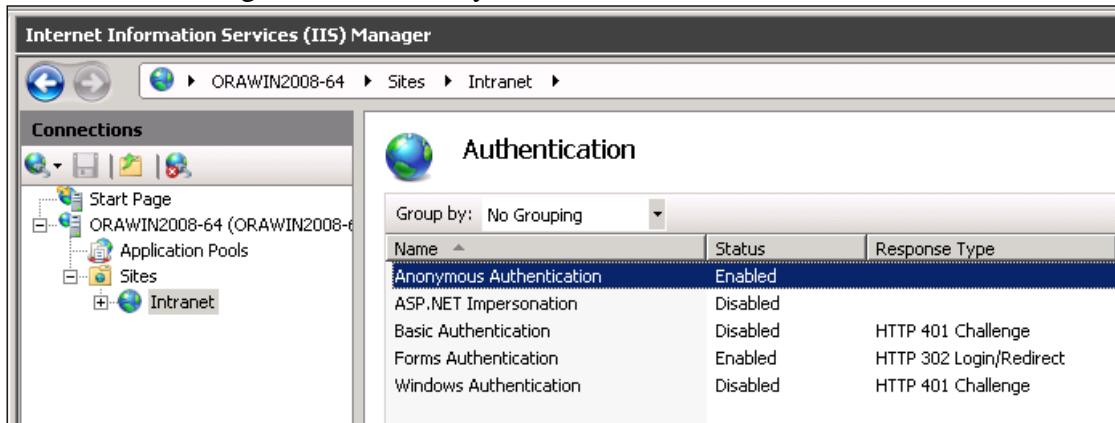


Implementatiehandleiding Active Directory voor Smartsite iXperion

18 IIS Configuratie voor Novell

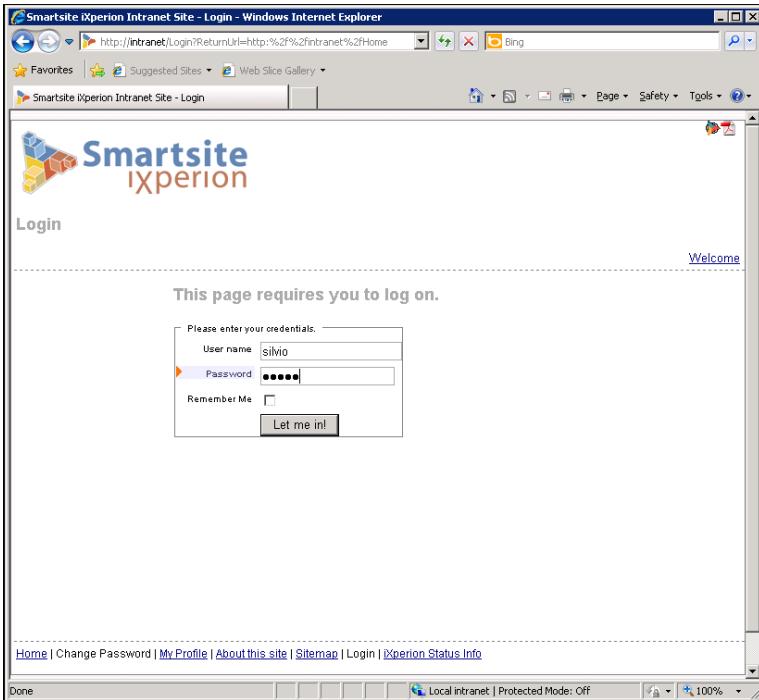
18.1 Front-End Authentication

De website maakt gebruik van Anonymous Authentication en Form-Based Authentication.



The screenshot shows the IIS Manager interface. On the left, the Connections pane lists 'Start Page', 'ORAWIN2008-64 (ORAWIN2008-64)', 'Application Pools', and 'Sites' with 'Intranet' selected. The main pane is titled 'Authentication' and displays a table of authentication methods:

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

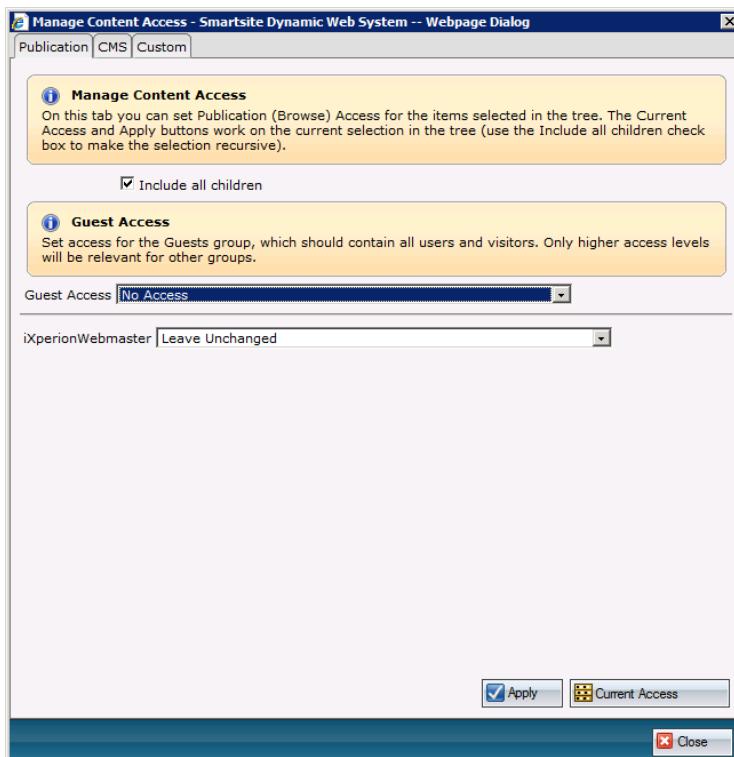


The screenshot shows a Windows Internet Explorer window with the title 'Smartsite iXperion Intranet Site - Login'. The address bar shows the URL 'http://intranet/Login?ReturnUrl=http%3A%2F%2Fintranet%2FHome'. The page itself is a 'Login' screen for the 'Smartsite iXperion' site. It features a logo at the top left, a 'Welcome' link at the top right, and a message 'This page requires you to log on.' Below this is a form with fields for 'User name' (set to 'Silvio'), 'Password' (redacted), and 'Remember Me' (unchecked). A 'Let me in!' button is at the bottom of the form. At the very bottom of the page, there is a footer with links: 'Home | Change Password | My Profile | About this site | Sitemap | Login | iXperion Status Info'.

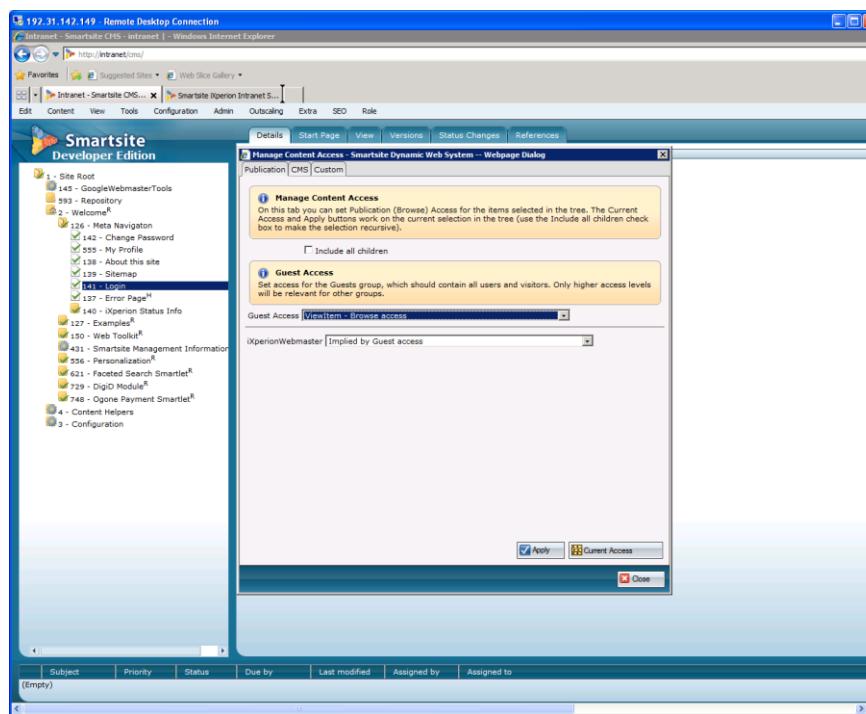
Form-Based logon is benodigd voor de front-end.

Wanneer de site altijd om een login dient te vragen, dient de site restricted te worden gemaakt, door Browse Access te ontnemen voor het Guest account.

Implementatiehandleiding Active Directory voor Smartsite iXperion

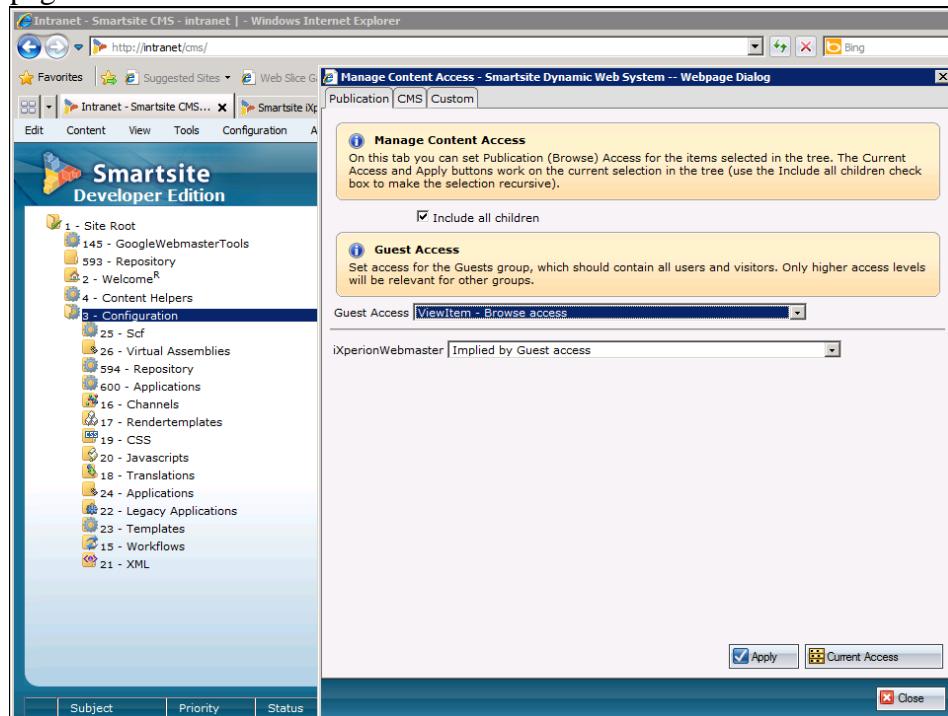


Op het Publication tabblad dient de Guest Access voor de gehele site op **No Access** te worden gezet.



Implementatiehandleiding Active Directory voor Smartsite iXperion

Echter de login pagina dient voor het Guest account beschikbaar te blijven om de login pagina te tonen.

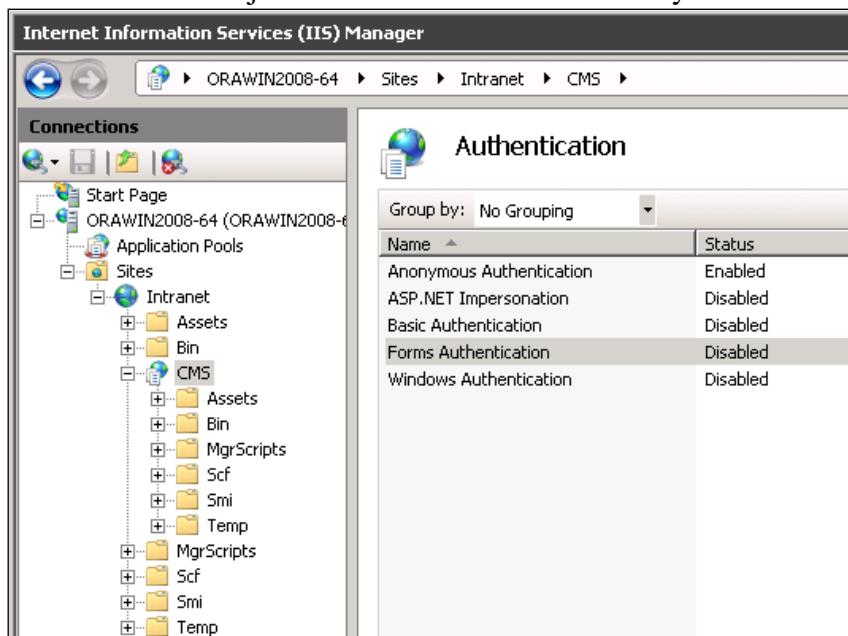


Zo ook dient het Guest account op de site configuratie items als CCS en Javascripts toegang te hebben.

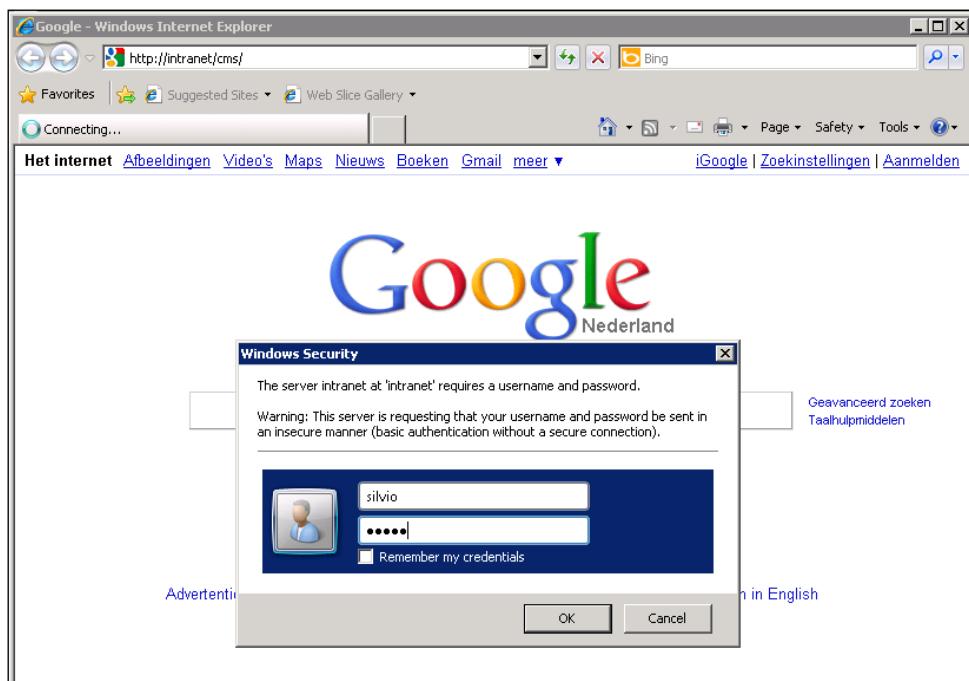
Implementatiehandleiding Active Directory voor Smartsite iXperion

18.2 Back-end Authentication

Voor de redactie zijden /CMS dient alleen IIS Anonymous Authentication aan te staan.

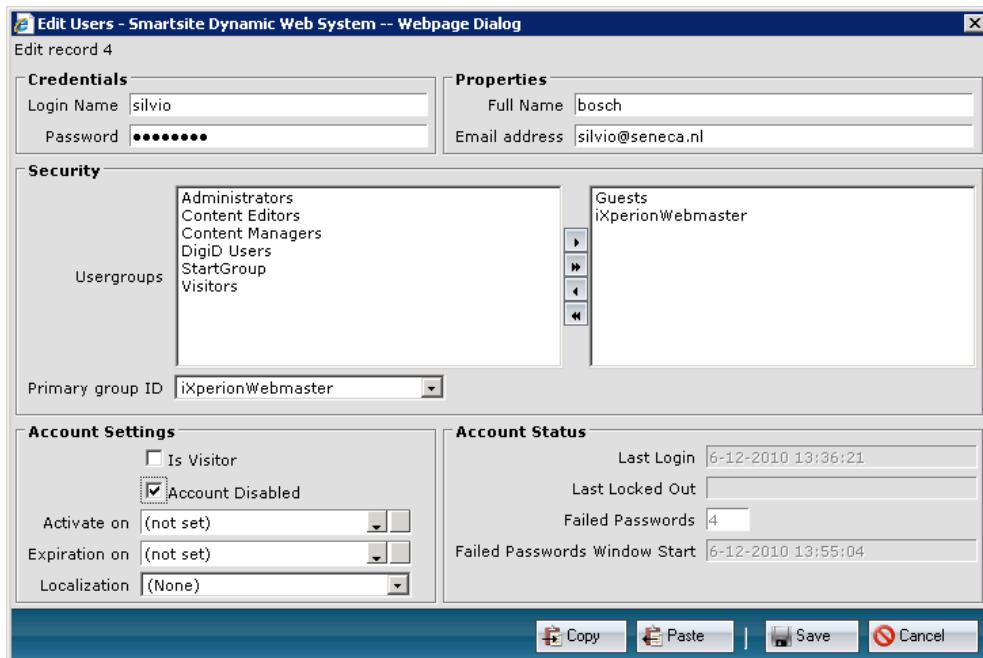


Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Basic Authentication	Disabled
Forms Authentication	Disabled
Windows Authentication	Disabled



Implementatiehandleiding Active Directory voor Smartsite iXperion

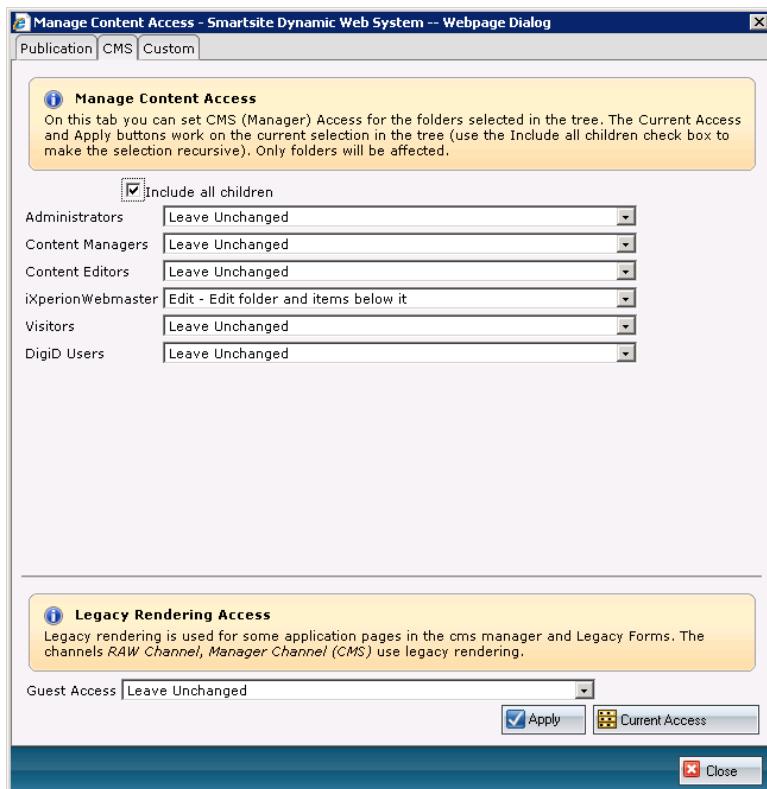
Men dient daarom altijd in te loggen met username en password (single-sign on zoals met Active directory is niet mogelijk).



The screenshot shows the 'Edit Users' dialog box. In the 'Properties' section, the 'Login Name' is set to 'silvio', 'Full Name' to 'bosch', and 'Email address' to 'silvio@seneca.nl'. Under 'Security', the 'Usergroups' list includes 'Administrators', 'Content Editors', 'Content Managers', 'DigiD Users', 'StartGroup', and 'Visitors'. The 'Primary group ID' is set to 'iXperionWebmaster'. In the 'Account Settings' section, the 'Account Disabled' checkbox is checked. The 'Account Status' section displays the last login as '6-12-2010 13:36:21', failed logins as '4', and the failed password window start as '6-12-2010 13:55:04'. At the bottom, there are buttons for 'Copy', 'Paste', 'Save', and 'Cancel'.

⚠ Let er op dat Smartsite na 3x verkeert inloggen het account Disabled. Dit dient handmatig te worden hersteld.

Implementatiehandleiding Active Directory voor Smartsite iXperion

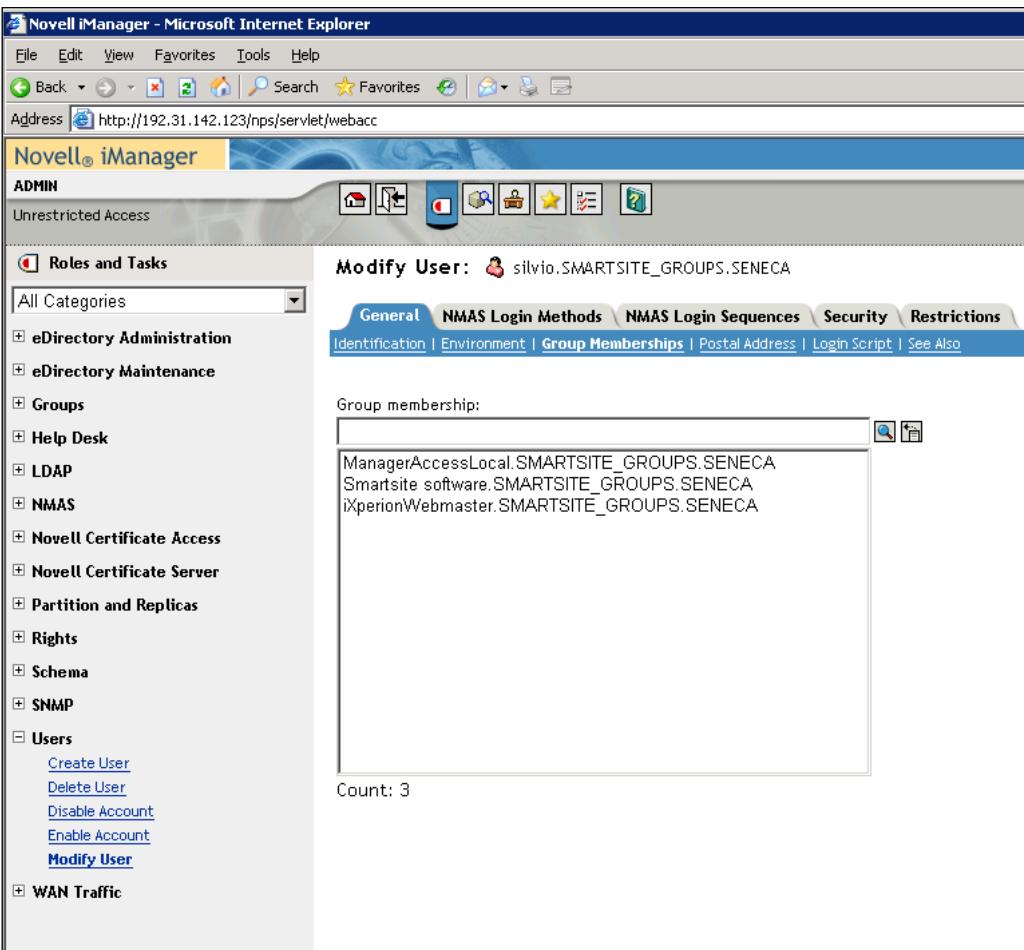


Zorg er voor dat de nieuwe groepen recht hebben op de redactie (cms) folderstructuur.

Implementatiehandleiding Active Directory voor Smartsite iXperion

18.3 Groepen in Novell

In Novell is de ondersteuning van geneste groepen pas beschikbaar vanaf versie 8.8.3 en later. Voor Smartsite iXperion houdt dit in dat de gebruikers aan alle groepen dienen te worden toegevoegd om toegang te krijgen tot Smartsite.



The screenshot shows the Novell iManager interface in Microsoft Internet Explorer. The left sidebar lists various administrative tasks under 'Roles and Tasks'. In the main panel, a user named 'silvio' is being modified. The 'Group membership' section displays three groups:

- ManagerAccessLocal.SMARTSITE_GROUPS.SENECA
- Smartsite software.SMARTSITE_GROUPS.SENECA
- iXperionWebmaster.SMARTSITE_GROUPS.SENECA

Count: 3

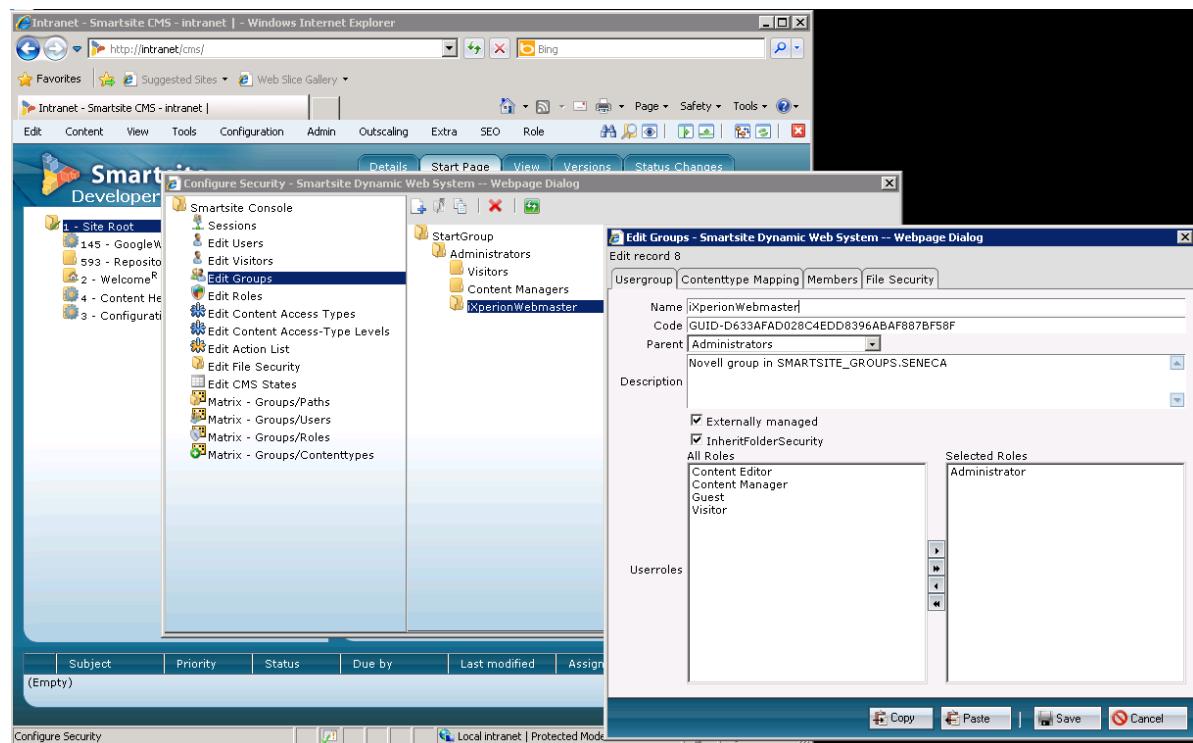
In bovenstaand voorbeeld is alleen de groep iXperionWebmaster opgenomen in de Smartsite interne groepen structuur.

Implementatiehandleiding Active Directory voor Smartsite iXperion

18.4 Groepen in Smartsite

Wanneer een gebruiker toegang dient te hebben tot de front-end en back-end, dient hij lid te zijn van minimaal 3 groepen:

De eerste 2 groepen “SmartsiteAccess” en “SmartsiteManagerAccess” staan opgegeven in de Web.config. Daarnaast dient de gebruiker lid te zijn van minimaal 1 groep die gemapt is in Smartsite en het vinkje “Externally Managed” heeft aanstaan. (Hier iXperionWebmaster).



Implementatiehandleiding Active Directory voor Smartsite iXperion

18.5 Fouten ten gevolgen van Novell LDAP security settings

De volgende error treedt op wanneer er geen gebruik wordt gemaakt van SSL maar er een anonymous authentication connectionstring (Non-Encrypted LDAP Port 389) wordt gebruikt.

```
<add name="novell" applicationName="Smartsite"
type="Smartsite.Security.Authentication.LDAPMembershipProvider, Smartsite.Security"
connectionStringName="LDAPConnection" connectionUsername="cn=admin,o=SENECA"
connectionPassword="admin" port="389" useSSL="false" />
```

Back-End

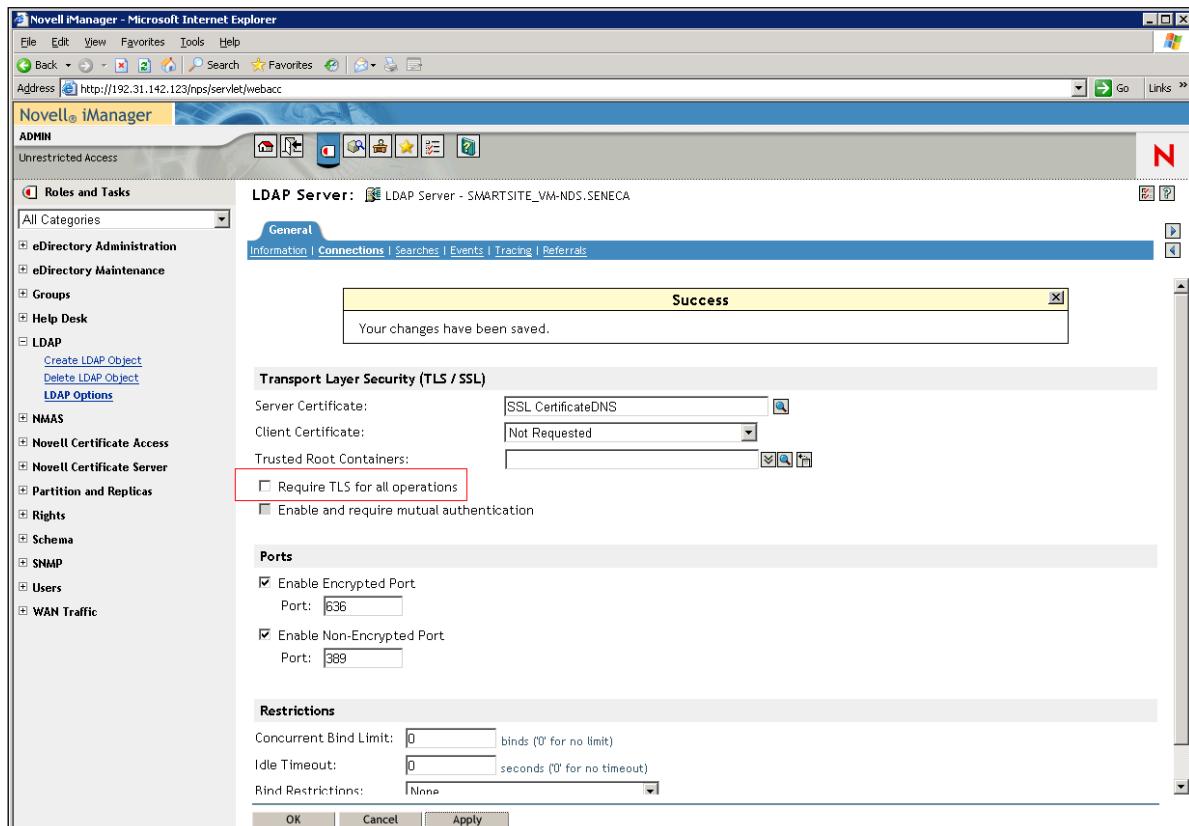
```
Server Error in '/CMS' Application.  
-----  
InitSecurity: Confidentiality is required for this operation.  
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.  
  
Exception Details: System.Exception: InitSecurity: Confidentiality is required for this operation.  
  
Source Error:  
  
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.  
  
Stack Trace:  
  
[Exception: InitSecurity: Confidentiality is required for this operation.]  
SixSmartsite.ControllerClass.StartSite(String siteName) +0  
Smartsite.Interop.IIS.Handler.InitSite(HttpContext context, Boolean& reload) +637  
Smartsite.Interop.IIS.Handler.ProcessRequest(HttpContext context) +532  
  
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute()
+181  
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean&
completedSynchronously) +75  
  
-----  
Version Information: Microsoft .NET Framework Version:2.0.50727.4952; ASP.NET
Version:2.0.50727.4955
```

Implementatiehandleiding Active Directory voor Smartsite iXperion

Front-End

```
Server Error in '/' Application.  
-----  
  
Configuration Error  
Description: An error occurred during the processing of a configuration file required  
to service this request. Please review the specific error details below and modify your  
configuration file appropriately.  
  
Parser Error Message: Confidentiality is required for this operation.  
  
Source Error:  
  
Line 71:      <providers>  
Line 72:          <clear />  
Line 73:          <add name="novell" applicationName="Smartsite"  
type="Smartsite.Security.Authentication.LDAPMembershipProvider, Smartsite.Security"  
connectionStringName="LDAPConnection" connectionUsername="cn=admin,o=SENECA"  
connectionPassword="admin" port="389" useSSL="false" />  
Line 74:          <add applicationName="Smartsite" name="SqlMembershipProvider"  
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"  
enablePasswordRetrieval="true" enablePasswordReset="true" passwordFormat="Clear"  
requiresQuestionAndAnswer="false" writeExceptionsToEventLog="true" />  
Line 75:      </providers>  
  
Source File: E:\Sites\Intranet\WWW\web.config    Line: 73  
  
-----  
Version Information: Microsoft .NET Framework Version:2.0.50727.4952; ASP.NET  
Version:2.0.50727.4955
```

Implementatiehandleiding Active Directory voor Smartsite iXperion



In Novell eDirectory staat dan in de LDAP server configuratie het “Require TLS for all operations” aangevinkt.