

Implementatiehandleiding Active Directory voor Smartsite iXperion



Active Directory/LDAP Implementatiehandleiding Voor Smartsite iXperion 1.3 en hoger



Copyright © 2011



Implementatiehandleiding Active Directory voor Smartsite iXperion

Auteur: ing. Silvio Bosch

Versiebe	heer:		
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	Inlei	ding	6
2	Waa	rom 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	Sma	rtsite 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	
conr	nection	string	9
4	Mog	elijke scenario's	10
	4.1	Algemeen	10
	4.2	Ondersteuning van 3 type koppelingen	11
5	Volle	edige Microsoft Active Directory Service koppeling	12
6	Con	figuratie 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	nt 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



	6.	6.7 Authentication Back-end (CMS)	48
	6.7 A	ADSI Edit	49
	6.8 I	IS integrated authentication	50
	6.9 5	Site Registry Security Key	52
7	Domei	n- en Smartsite iXperion Primary Group	53
8	Disabli	ing Single Sign-on	56
	8.1 \	/oorkomen IE inlogbox in Smartsite Manager	56
9	Hoe ee	n Domain Group Policy aan te maken	57
10	Sma	rtsite ConfigEditor en Active Directory Configuratie	63
11	Prox	y/ISA Server en Firewall	64
	11.1	Outscaling	64
	11.2	Smartsite Manager	64
12	Cust	om Errorhandling in Web.config	65
13	Integ	rated database connectionstring	67
14	Sma	rtsite iXperion Mixed Mode Security	70
	14.1	Mixed mode web.config	70
	14	4.1.1 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	4.4.1 IIS Anonymous authentication en Windows Integrated	
Αι	ithentica	ation enabled	75
15	Activ	e directory koppeling met meerdere domeinen	79
	15.1	Outgoing en incoming trust (tweeweg-trust)	79
	15.2	Groepen en users	80
	1	5.2.1 StoreFullyQualifiedLoginName	80
	D	oordat een gebruiker op meerdere domeinen onder dezelfde	
ac	countna	ime kan voorkomen, dient de web.config parameter	0.0
St	oreFully	QualifiedLoginName altijd gelijk aan true te zijn	80
	15.3	Web.config multi-domaining	81
	15.4	Active directory tester	90
40	15.5	Multi-domain via Smartsite iXperion ConfigEditor	
16	Sma	rtsite IXperion LDAP koppeling met Novell eDirectory	
	16.1	Specifieke Membership Provider	95
	16.2	Forms authentication	95
	10.3	Conliguration web.conlig	95
	10	5.3.1 CONNECTION STIING	
	10	5.3.2 iviendersnip provider	95
	16 /	5.5.5 settings	
	10.4	FUTTIS authentication	
	19	ס.4.ד רוטות-פוט	98



	1	6.4.2 Back-end	
	1	6.4.3 Registry configuratie	
17	Nove	ell configuratie	
	17.1	TLS/SSL en poort configuratie	
18	IIS C	onfiguratie voor Novell	
	18.1	Front-End Authentication	
	18.2	Back-end Authentication	
	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 frontend 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

Edit Anonymous Authentication Credentials	? ×
Anonymous user identity:	
• Specific <u>u</u> ser:	
IUSR	<u>S</u> et
O Application pool identity	
ОК	Cancel

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.

Login	
	Please enter your credentials
	User name
	Password
	Remember Me 🗖
	Let me in!

• 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.

Windows Securit	У		×
Connecting to Ir	tranet.		
	User name Password Domain: DEVELOP-INT Remember my credentia	ls	
		ОК	Cancel



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:

Internet Information Services (IIS) Manager				
	N12 🕨 Sites 🕨 Intranet 🕨			
Connections	Authentication			
Start Page	Group by: No Grouping			
Application Pools	Name 🔺	Status	Response Type	
È in Sites È Intranet È in Massets È in Massets	Anonymous Authentication ASP.NET Impersonation Basic Authentication Forms Authentication	Disabled Disabled Disabled Disabled	HTTP 401 Challenge HTTP 302 Login/Redir	
in - ∰ cms in - ∭ MgrScripts in - ∭ Scf	Windows Authentication	Enabled	HTTP 401 Challenge	
		4		

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 configureerbaar 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.



Voorbeeld Active Directory Koppeling Smartsite iXperion

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

Group name (pre-Windows 2	000): Xperion_Administrators
Description: Smartsite	iXperion Group
E-mail:	
Group scope C Domain local Global Universal	Group type G Security Distribution
Notes:	

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

Useraction Mapping Select the user actions and	privileges this role can use.
I Actions	Selected Actions Edit Groups Query Database Edit Users Edit Roles Edit File Security Copy Edit Action List Add Reference Add specified Item Immediate Window Sessions Change Password Privilege - Access to SmartSite Manager Privilege - SmartEditor Simple Privilege - SmartEditor Normal Privilege - SmartEditor Advanced

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

sergroup	Contenttype Mapping Members File S	Security
Name	iXperion_Administrators	
Code	ADMINISTRATORS	
Parent	StartGroup	
Description	Usergroup for site Administrators	
E	Externally managed	
	All Roles	Selected Roles
	Guest Visitor	Administrator Content Editor Content Manager
Userroles		b 333 4

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

📕 UserGroups_ei	nterprise.xml - Notepad
<u>File E</u> dit F <u>o</u> rmat	<u>V</u> iew <u>H</u> elp
	<pre><field name="Description"></field></pre>
	<pre><sortindex>5</sortindex> <cust:clip>ExternallyManaged</cust:clip> <field name="InheritFolderSecurity"> <caption>InheritFolderSecurity</caption> <group>Usergroup>/group> <sortindex>6</sortindex> <defaults1< default=""> <cust:clip>InheritFolderSecurity</cust:clip> </defaults1<></group></field> <caption>UserRoles"> <caption>UserRoles</caption> <group>Usergroup>/group> <sortindex>=</sortindex></group></caption></pre>

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.

Manage Content Acces	ss - Smartsite Dynamic Web System Webpage Dialog	×
Publication CMS Custo	n	
Manage Conte On this tab you can a Apply buttons work o selection recursive).	nt Access set CMS (Manager) Access for the folders selected in the tree. The Current Access and on the current selection in the tree (use the Include all children check box to make the Only folders will be affected.	
🔽 Includ	le all children	
iXperion_Administrators	Edit - Edit folder and items below it	
EDITORS FOLDER	Leave Unchanged	
iXperion_ChiefEditors	Leave Unchanged	
iXperion_Editors	Leave Unchanged	
VISITORS FOLDER	Leave Unchanged	
iXperion_Visitors1	Leave Unchanged	
iXperion_Visitors2	Leave Unchanged	
Legacy Rende Legacy rendering is RAW Channel, Manage	ring Access used for some application pages in the cms manager and Legacy Forms. The channels <i>per Channel (CMS)</i> use legacy rendering.	
Guest Access Leave U	nchanged	
	Close	

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.

New record		
Usergroup (Contenttype Mapping Members File Security	
Name	e [iXperion_Visitors1	
Code	e VISITORS1	
Parent		
Description	n	
-		
	Externally managed	
	InheritFolderSecurity All Roles Selected Roles	
	Administrator Visitor Content Editor Content Manager	
	Guest	
Userroles	s »	
	4	
	Copy Paste Save Save	S Cancel

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.

and Apply buttons wo the selection recursiv	ork on the current selection in the tree (use the Include all children check box to make re).
🔽 Include	ie all children
Guest Access	
Set access for the Gu relevant for other gro	lests group, which should contain all users and visitors. Only higher access levels will pups.
est Access Leave Un	nchanged
erion_Administrators	Leave Unchanged
ITORS FOLDER	Leave Unchanged
erion_ChiefEditors	Leave Unchanged
erion_Editors	Leave Unchanged
SITORS FOLDER	Leave Unchanged
erion_Visitors1	ViewItem - Browse access
erion_Visitors2	ViewItem - Browse access

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.

Edit record 6			
User Role Us	ser Actions CMS/Workflow States		
Name	Guest		
Code	GUEST		
Description	Anonymouys visitor of a site		
	I All Groups	Selected Groups	
Usergroups	EDITORS FOLDER iXperion_Administrators iXperion_ChiefEditors iXperion_Usitors1 iXperion_Visitors1 iXperion_Visitors2 StartGroup VISITORS FOLDER	Guests	
		🛱 Copy 🖨 Paste 🛛 🕁 Sav	e 🚫 Cancel

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.



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.

on Security Group
- Group type
 Security
C Distribution
<u>.</u>

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

& iXperion_Visitors1 iXperion_Visitors2 iXperionManagerAccessGroup	Develop.Intem/Seneca Groep/Se Develop.Intem/Seneca Groep/Se Develop.Intem/Seneca Groep/Se
& iXperion_Visitors2 & iXperionManagerAccessGroup	Develop.Intem/Seneca Groep/Se Develop.Intem/Seneca Groep/Se
😹 iXperionManagerAccessGroup	Develop.Intem/Seneca Groep/Se
4	

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

Inditie	Active Directory Domain Services Fold
Kperion_Administrators	Develop.Intern/Seneca Groep/Senec
KiXperion_ChiefEditors	Develop.Intem/Seneca Groep/Senec
KiXperion_Editors	Develop.Intem/Seneca Groep/Senec
🔏 iXperion_Webmasters	Develop.Intem/Seneca Groep/Senec
4	

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="DatabaseId" 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.

Active Directory Users and Comput	Name	Туре	Description
Saved Queries Develop.Intern Develop.Intern Develop.Root-OU Develop Root-OU De	Kperion_Administrators Kperion_ChiefEditors Kperion_Editors Kperion_Webmasters KperionAccessGroup KperionManagerAccessGroup Kperion_Visitors1 Kperion_Visitors2	Security Group - Global Security Group - Global Security Group - Global Security Group - Global Security Group - Domain Local Security Group - Global Security Group - Global	Smartsite iXperion Group Smartsite iXperion Group Smartsite iXperion Group Smartsite iXperion Group Domain only iXperion Security Group Domain only iXperion Security Group Smartsite iXperion Group Smartsite iXperion Group
l al			

De iXperionAccessGroup en de iXperionManagerAccessGroup zijn Local domain groepen.

Smartsite Console
 Item Locks Edit Users Edit Visitors Edit Roles Edit Content Access Types Edit Content Access Type Levels Edit Action List Edit CMS States Matrix - Groups/Users Matrix - Groups/Contenttypes

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

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.

File Action View Help				
🗢 🔿 🙍 📅 🖬 🖬 🙆 .	s 🛛 🖬 🐮 🐮 🕇	172	1 B	
Active Directory Users and Comput	Name	Туре	Description	
🕀 🧱 Saved Queries	& iXperionADSAdmin	User	IIS ApplicationPool and iXperion LDAP account	
🖃 🏥 Develop.Intern	🔏 test	User		
표 🛅 - Develop Root-OU -				
🕀 🚞 Builtin				
🕀 🚞 Computers				
🕀 📔 Domain Controllers				
E ForeignSecurityPrincipals				
🕀 🗾 Microsoft Exchange Securit				
🖃 🗾 Seneca Groep				
🖃 🖬 Seneca B.V.				
Groups				
a Users				
🕀 🔟 Smartsite Groups				
🕀 🛄 Users				

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

Password:		
Confirm password:		
User must change passv	word at next logon	
User cannot change pas	ssword	
Password never expires		
Account is disabled		

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

6.4.1 Optioneel: Wijzigen Application pool account

Fip: In principe is het mogelijk de application pools onder het Domain account iXperionADSAdmin 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

	(General)			
	.NET Framework Version	v2.0		
	Managed Pipeline Mode	Integrated		
	Name	Intranet		
	Queue Length	1000		
	Start Automatically	True		
Ξ	CPU			
	Limit	0		
	Limit Action	NoAction		
	Limit Interval (minutes)	5		
	Processor Affinity Enabled	False		
	Processor Affinity Mask	4294967295		
Ξ	Process Model			
	Identity	NetworkService		
1	Idle Time-out (minutes)	0 72		
	Load User Profile	False		
	Maximum Worker Processes	1		
	Ping Enabled	True		
	Ping Maximum Response Time (second	90		
	Ping Period (seconds)	30		
	Shutdown Time Limit (seconds)	90		
	Startup Time Limit (seconds)	90		
F	Process Ornhaning			

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

levelop.intern	VXperionADSAdmin
assword:	
•••••	
Confirm passw	ord:

Vul het domein account en password in.



Implementatiehandleiding Active Directory voor Smartsite iXperion

InetworkService	*		
Custom account:			
develop.intern\jXperionADSAdmin	Set		

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.

Select user or gr		Ø	
For the rules	Use the Group		
Systemwide ACL rules	Smartsite All Users	•	
Pub server specific ACL rules	Smartsite Intranet Publication server	•	
Cms server specific ACL rules	Smartsite Intranet CMS server	•	
		Previous	Next

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 gemarkeerd.

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"> <confiaSections> <!-- 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"</pre> 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" />



```
<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</p>
Login -->
  <authentication mode="Windows">
<!-- <forms loginUrl="/Login" name="Smartsite" / -->
  </authentication>
  <authorization>
   <allow users="*" />
  </authorization>
  <!-- ADS SETTING defaultProvider="ADMembershipProvider" -->
```



```
<membership defaultProvider="ADMembershipProvider" userIsOnlineTimeWindow="15">
  <providers>
 <clear />
 <!-- ADS SETTING CHANGE connectionUsername and connectionPassword. Use user principal</p>
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="FileNotFound.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" /-->
```



```
<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"</pre>
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) -->
 <!--
     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"</pre>
contract="Smartsite.Core.Services.IManagerService" />
    </service>
   </services>
   <bindings>
    <netNamedPipeBinding>
<br/><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</pre> 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"</pre> /></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"



/>
>
 behaviors>
<servicebehaviors></servicebehaviors>
<behavior name="StateSyncServiceBehavior"></behavior>
<behavior name="InteropServiceBehavior"></behavior>
<behavior name="SchemaServiceBehavior"></behavior>
<pre><behavior name="EventSynchronizationServiceBehavior"></behavior></pre>
<behavior name="ManagerServiceBehavior"></behavior>
<endpointbehaviors></endpointbehaviors>
<behavior name="HitServiceBehavior"></behavior>
<datacontractserializer maxitemsinobjectgraph="10000000"></datacontractserializer>
Uncomment system.diagnostics section to enable trace-logging
<system.diagnostics></system.diagnostics>
<trace autoflush="true"></trace>
<sources></sources>
<source name="System.ServiceModel" switchvalue="Error"/>
listeners>
<add name="traceListener"></add>
<source name="System.ServiceModel.MessageLogging"/>
listeners>
<add name="traceListener"></add>
<sharedlisteners></sharedlisteners>
<add <="" name="traceListener" td="" type="System.Diagnostics.XmlWriterTraceListener, System,</td></tr><tr><td>Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"></add>
initializeData="E:\Sites\Intranet\LogFiles\WCF\Intranet.svclog" />
<system.webserver></system.webserver>
<modules></modules>
<add <="" name="ixbridge" td="" type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge"></add>
preCondition=""/>
<add <="" name="ImageServer" td=""></add>
type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor" preCondition="" />
<add name="PdfModule" precondition="" type="Smartsite.Pdf.PdfModule,Smartsite.Pdf"></add>
update session module with modified preCondition
<remove name="Session"></remove>
<add name="Session" precondition="" type="System.Web.SessionState.SessionStateModule"></add>



```
<!-- 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 maxReguestLength="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>
    <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 expliciet 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 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 opgeven. 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 opgeven 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.

HIM WINDOWS ACCOUNTS		
Password Wallet Accounts	nection properties	<u> </u>
🛨 🖓 Channels	nection String LD	AP://DEVELOP.INTERN
Active Directory Configuration	nection Username iXp	erionADSadmin@Develop.intern
	nection Password 🔹	•••••
	ault Domain DE	VELOP-INT
	ups	
	rtsite Access Group iXp	erionAccessGroup
	ager Access Group iXp	erionManagerAccessGroup
	nager settings	
	abase Id 🛛 🗖 🗖 🗖	anager
	rch Base dc	=develop,dc=intern
	(Windows) integrated security	Je
	c	<u> </u>

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



Implementatiehandleiding Active Directory voor Smartsite iXperion

6.6.3.3 Databaseld

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



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

6.6.3.9 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-pompt

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

6.6.6 Role provider

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 --> <code><authentication mode="Windows" /></code>
```



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

File Action View Help				
			[
ADSI Edit Develop [SDDC01.Develop.Intern] DC=Develop.DC=Intern OU=- Develop.Roct-OU - CN=Builtin CN=Computers OU=Domain Controllers CN=ForeignSecurityPrincipals CN=KortAndFound OU=Microsoft Exchange Security Groups CN=Microsoft Exchange System Objects CN=Program Data OU=Program Data	Name OU =- Develop Root-OU - OU =- Develop Root-OU - ON = Bultin ON = Computers OU = Domain Controllers OU = Domain Controllers OU = NetostAndFound OU = Nicrosoft Exchange Syst ON = Sence Groep OI = Sence Groep	Class organizationa builtinDomain organizationa container lostAndFound organizationa msExchSyste msDS-Quota container organizationa organizationa	Distinguished Name OU=- Develop Root-OU -,DC=Develop,DC=Intern CN=Builtin,DC=Develop,DC=Intern OU=Domain Controllers,DC=Develop,DC=Intern OU=Domain Controllers,DC=Develop,DC=Intern CN=ForeignSecurityPrincipals,DC=Develop,DC=Intern OU=Microsoft Exchange Security Groups,DC=Develop CN=Microsoft Exchange System Objects,DC=Develop CN=NITDS Quotas,DC=Develop,DC=Intern CN=Program Data,DC=Develop,DC=Intern OU=Seneca Groep,DC=Develop,DC=Intern OU=Seneca Groep,DC=Develop,DC=Intern	Actions DC=Develop,D A More Actions A CN=Users More Actions
CIN=System Groups CIN=System CIN=System CIN=Administrator CIN=Administrator CIN=Administrator CIN=Denied RODC Password Replication Grou CIN=Denied RODC Password Replication Grou CIN=DensUpdateProxy CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Domain Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Computers CIN=Compile Compile Computers CIN=Compile Compile Comp	CN=System CN=Users CN=Infrastructure	container container infrastructure	CN=System,DC=Develop,DC=Intern CN=Users,DC=Develop,DC=Intern CN=Infrastructure,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.

Internet Information Services	(IIS) Manage	r			
	N12 🕨 Sites	▶ Intranet ▶			
Connections	S Int	ranet Hom	9		
Start Page	Group by: A	rea	-		
Application Pools	ASP.NET				_
E Sites		0	P.		٠
tin	.NET Compilation	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels
⊞ <mark>™</mark> MgrScripts ⊞ <mark>™</mark> Scf		*	ab	8	
	.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls
	62	8			
	Providers	Session State	SMTP E-mail		
	IIS				
		2	0		404
	ASP	Authentication	Default Document	Directory Browsing	Error Pages



Internet Information Service	s (IIS) Manager		
	ON12 🕨 Sites 🕨 Intranet 🕨		
Connections	Q Authentication		
Start Page	Group by: No Grouping	•	
Application Pools	Name 🔺	Status	Response Type
	Anonymous Authentication ASP.NET Impersonation Basic Authentication Forms Authentication Windows Authentication	Disabled Disabled Disabled Enabled	HTTP 401 Challenge HTTP 302 Login/Redir HTTP 401 Challenge

- ▲ 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.





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.

Member of:	
Name	Active Directory Domain Services Folder
Domain Users	Develop.Intern/Users
Add	Remove
Add	Remove Domain Users There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant
Add	Remove Domain Users JP There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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

👩 Edit Users - Smartsite Dynamic Web System Webj	page Dialog 🛛 🔀
Edit record 6	
Credentials	Properties
Login Name XperionAdmin	Full Name iXperionAdmin
Password ••••••	Email address
Security	
iXperion_ChiefEditors iXperion_Editors iXperion_Visitors1 iXperion_Visitors2 iXperion_Webmasters StartGroup Visitors1 iXperion_Webmasters StartGroup Visitors Itage Visitors Visitors Visitors Yistors	iXperion_Administrators Guests
Account Settings	☐ Account Status
C Account Disabled	Last Login 15-6-2011 14:23:09
Activate on (not set)	Last Locked Out
Expiration on (not set)	Failed Passwords 0
Localization (None)	Failed Passwords Window Start
	🔁 Copy 🗲 Paste 🔰 🔚 Save 🚫 Cancel

"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 backend 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/				
Trusted sites Protected Mode: Off	🔄 🖓 🛨 🔍	100%		
http://Intranet wordt automatisch too	egevoegd aan	alle client	E browsers a	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.

U			
			Group Policy Management
			Internet Information Services (IIS) 6.0 Manager
		1	Internet Information Services (IIS) Manager
			iSCSI Initiator
Internet		-	Local Security Policy
Explorer			Memory Diagnostics Tool
		6	Reliability and Performance Monitor
			Security Configuration Wizard
			Server Manager
Control Panel		0,	Services
		3	Share and Storage Management
		<u> </u>	Storage Explorer
<u></u>	_	<u>_</u>	System Configuration
Windows Update		()	Task Scheduler
		<u></u>	Windows Firewall with Advanced Security
🛗 Programs	🖡 🎉 Accessories	الله 🖌 🐌	Windows Server Backup
	🔒 Administrative Tools		Windows PowerShell Modules
Documents	Extras and Upgrades	•	



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.

Security Zones and Content Ratings	<u>? X</u>
Security and Privacy Settings	
You can customize the settings of each security zone as well as custor settings must be made through the Modify Settings button below. For Security Zones and Privacy	nizing the privacy settings. These more information, click Help.
O Do not customize security zones and privacy	Internet Explorer Enhanced Security Configuration
© Import the current security zones and privacy settings	You have chosen to import settings that are compatible with computers that don't have the Internet Explorer Enhanced Security Configuration enabled. These
Content ratings allow you to prevent users from viewing sites with ris basis and are rated by the author for degrees of risky language, nud Content Ratings	security settings will be ignored on machines where the enhanced security configuration is enabled. To import settings for users where the enhanced security configuration isn't enabled, click Continue.
Do not customize Content Ratings Import the current Content Ratings settings	To import settings for the enhanced security configuration, click Cancel, then install the enhanced security configuration and import the enhanced security settings from the previous dialog.
	To import settings for users who login to computer in both scenarios, configure a GPD/IEAKPackage for each scenario and deploy both packages to the same users.

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



A Forest: Security Zones and Content Ratings	
Gecurity and Privacy Settings	WMI Filter
Internet Properties ? 🗙 mizing the privacy settings. These	None
more information, click Help.	None
General Security Privacy Content Connections Programs Advanced	None
Select a zone to view or change security settings.	
Internet Local intranet Trusted sites Restricted sites ky content. Ratings are set on a per-site	
Local intranet	
This zone is for all website: found on your intranet.	
Use the settings below to define which websites are included in	
Security level for this zone	
Allowed levels for this zone: All	×
- I - Medium-low	
Appropriate for we	n this zone. All websites in Htings
- L. (Intranet) - Indiade di sites di el cono siste di sites di el cono siste di sites di el cono siste di e	congo.
- Unsigned ActiveX c	
- Same as Medium le Add this website to the zone:	
Enable Protected Mode (rec <u>What are intranet settings?</u> Adv.	Add
C Websites:	
Recet all paper to default level intranet	Remove
OK Cancel Apply Dequire convertigication (https://fex.all.cit	in this zone
	.com chio 2016
	-
	Close

- 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.

🖅 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	gpupdate /force
	🕐 This task will be created with administrative privileges.
	OK Cancel Browse



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.

🗭 Configuration Editor (Smartsite iXperion 1.3)					
File View Tools Help					
👔 🔚 🛅 Unlock 🥑 Validate 📀 Validate Operational Status 🦄 Restore Defaults					
(local) Intranet Databases Services Security Profiles Windows Accounts Password Wallet Accounts	Active Directory Configuration (locked) Active Directory configuration, as configured within the web.config				
🕀 Mannels					
Active Directory Configuration	Connection String	LDAP://DEVELOP.INTERN			
	Connection Username	iXperionADSadmin@Develop.intern			
	Connection Password	••••••			
	Default Domain	DEVELOP-INT			
	🗆 Groups				
	Smartsite Access Group	iXperionAccessGroup			
	Manager Access Group	iXperionManagerAccessGroup			
	Manager settings				
	Database Id	manager			
	Search Base	dc=develop,dc=intern			
	Use (Windows) integrated security	True			
🗆 Misc					
	Default Domain The name of the default domain that show	uld be used.			

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

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

🚊 🍉 Intranet		Publicad	
📃 🕀 👔 Da 📂	Open Folder		
🕀 🛷 Se 🛝	Restore Intranet - Haven amsterdam CMS		
🗄 📲 🕺 💘	Remove		
📄 🔂 Pa	Set Site Url		
aje	Rename Site		
ĀD	Add Active Directory Configuration	1	



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 bevragen 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

nternet Options	? ×
.ocal Area Network (LAN) Settings	
Automatic configuration Automatic configuration may override manual settings. To ensure use of manual settings, disable automatic configuration	e the
Automatically detect settings	
Use automatic configuration script	
Address	
Proxy server	Drown Eatlings
Use a proxy server for your LAN (These settings will not ap	roxy sectings
Address: 10.10.10.1 Port: 8080 Advar	Type Proxy address to use Port
Bypass proxy server for local addresses	нттр: 10.10.10.1 : 8080
	Secure: 10.10.10.1 : 8080
	ETP: 10.10.10.1 : 8080
Local Area Network (LAN) settings	Sogks: :
LAN Settings do not apply to dial-up connections. LAN s Choose Settings above for dial-up settings.	☑ Use the same proxy server for all protocols
	Exceptions
	Do not use proxy server for addresses beginning with:
OK Cancel	XperionSite
	Use semicolons (;) to separate entries.
	OK Cancel
- ypass proxy server connection-se	etting in Internet Explorer

12Custom 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.



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.

🚮 Data Link Properties 🛛 🗙				
Provider Connection Advanced All				
Specify the following to connect to SQL Server data:				
1. Select or enter a server name:				
2. Enter information to log on to the server:				
Use Windows NT Integrated security.				
C Use a specific user name and password:				
User name:				
Password:				
Blank password Allow saving password				
3. 💿 Select the database on the server:				
· · · · · · · · · · · · · · · · · · ·				
C Attac <u>h</u> a database file as a database name:				
Using the filename:				
Test Connection				
OK Cancel Help				

Windows NT integrated Security database connectiestring.

📑 Data Link Properties 🛛 🗙				
Connection Advanced All				
Specify the following to connect to SQL Server data: 1. Select or enter a server name: Ssql02.seneca.intern 2. Enter information to log on to the server: C Use Windows NT Integrated security © Use a specific user name and password:				
User <u>n</u> ame: KperionAdmin				
Password:				
Blank password Allow saving password				
3. • Select the <u>d</u> atabase on the server:				
EmptyXperion11				
Attach a database file as a database name:				
Liging Rep filmenter				
OK Cancel Help				

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.

Server Properties - SSQL05.seneca.intern				
Select a page	🛒 Script 👻 📑 Help			
General Memory Processors Connections Database Settings Advanced Permissions	Server authentication			
Connection	Passw <u>o</u> rd:			
Server: SSQL05.seneca.intern	Options			
Connection:	Enable C2 audit tracing			
View connection properties	Cross database ownership chaining			
Ready				
	OK Cancel			



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:

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.

iXperion	XperionManagerAccessGroup Properties				? X		
Genera	al Members	Member Of	Manag	ged By	UNIX Attrib	utes	
<u>M</u> eml	Members:						
Nar	ne			Active [Directory Don	nain Service	es F
8	Domain Users		I	Develo	p.Intern/User	s	
	A <u>d</u> d	<u>R</u> emove					
			OK		Canaal	1 0]
			UK		Caricel		W .

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

iXperionAccessGroup Properties ? 🗙				
General Members Member Of Managed By UNIX Attributes				
Members:				
Name	Active Directory Domain Se			
& KperionManagerAccessGroup	Develop.Intern/Seneca Gro			
Add				
	Cancel Applu			

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

🥭 Edit Groups	s - Smartsite Dynamic Web System Webpage Dialog 🛛 🛛 🔀
New record	
Usergroup	Contenttype Mapping Members File Security
Name	iXperionAccesGroup
Code	GUID-4002D4C8F5B04F0788118A4B1C70CFF3
Parent	iXperion_Administrators
Description	
Description	
Userroles	✓ Externally managed ✓ InheritFolderSecurity All Roles Administrator Content Editor Content Manager
	🔁 Copy 🕹 Paste 📔 🔚 Save 🚫 Cancel

- 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

Error occurred while lo	ading page Windows Internet Explorer	N.	_1013
🔁 💽 🗢 浡 http://intr	anet/Pub/Home/TEST-2.html	💽 🔄 🗙 🌠 Live Search	<u>م</u>
Favorites	poested Sites 🔹 🖉 Web Slice Gallery 🔹		
Error occurred while loadi		🗛 • 🔊 • 🖃 🚔 • Page • S	afety - Tools - 🙆 -
P En or occurred while lobal	ng page.		
An error	occurred		
All ciror	occurred		
"Access Denied	d"		
2			
Exception in	nformation		
Messane	Access Denied		
Source	Smartsite Buntime		
Stack trace	System, Web, HttpException: Access Denied		
	at Smartsite.Core.RenderEngine.Authenticate()		
	at Smartsite.Core.RenderEngine.Render()		
System info	ormation		
Timestamp	23-11-2010 10:50:32		
Machine	VMIXPERION12		
OS Version	Microsoft Windows NT 6.0.6002 Service Pack 2		
Net Framework	2 0 50727 4200		
version	2000/2711200		
Process Id	3104		
Inread 1d			
Thread Name	ASP.Net Request		
Inread Owner	1000002		
Smartaita varsian	7.0.6000 16386		
Sita nome	7.0.0000.10360		
Url	http://intranet/Pub/Home/TEST-2.html		
Client address	127.0.0.1		
and the dealers of	227.01012		
ne		Trusted sites Protected Mode: Off	🖗 🕶 🔍 100% 🔹

Access Denied error voor visitor1 account op een restricted item.

Fip: 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.

CONTRACTOR OF THE OWNER.		Properties
Login Name 🛛	/isitor1	Full Name Visitor1
Password	•••••	Email address
Security		
Usergro	iXperion_Administrators iXperion_ChiefEditors iXperion_Editors iXperion_Visitors2 iXperion_Webmasters StartGroup	iXperionAccessGroup
Primary group	VISITORS FOLDER ID iXperionAccessGroup	×
Primary group Account Sett	VISITORS FOLDER ID iXperionAccessGroup	Account Status
Primary group Account Sett	VISITORS FOLDER ID iXperionAccessGroup ings IV Is Visitor	Account Status Last Login 23-11-2010 10:50:32
Primary group Account Sett	VISITORS FOLDER ID [XperionAccessGroup ings IS Visitor Account Disabled	Account Status Last Login 23-11-2010 10:50:32 Last Locked Out
Primary group Account Sett Activate on	VISITORS FOLDER ID iXperionAccessGroup ings V Is Visitor Account Disabled (not set)	Account Status Last Login 23-11-2010 10:50:32 Last Locked Out Failed Passwords 0
Primary group Account Sett Activate on Expiration on	VISITORS FOLDER ID iXperionAccessGroup ings Is Visitor Account Disabled (not set)	Account Status Last Login 23-11-2010 10:50:32 Last Locked Out Failed Passwords 0 Failed Passwords Vindow Start

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

Interview Province Interview Demostie - TEST 2 <	Smartsite iXperion Demo Site	- TEST 2 - Windows Intern	et Explorer						_	
	C C P http://intranet/Pub	/Home/TEST-2.html					💌 🐓 🗙 🦉 Live Search			<u>- م</u>
	🔶 Favorites 🛛 🍰 🏀 Suggested S	iites 🔹 🙋 Web Slice Gallery	•							
Since the provided for the service of the serv	>> Smartsite iXperion Demo Site - TES	T 2					🏠 • 🗟 - 🖃 🖶 • Page	• Safety •	Tools + 🔞	- "
Welcome Reageer aneller op bedrijfsbehoeften, verbeter de beschikbaarheid – en betrouwbaarheidsniveaus per gebruiker en verlaag de kapitale en operationele kosten. Ontwikkeld op het marktleidende virtualisatieplatform, helpt het u het beheer van uw virtuele datacenter te vereenvoudigen. De VM/ware vCenter beheeroplossingen: vergroten operationele efficiency maken policy-gestuurd beheer mogelijk optimaliseren serviceniveaus	Smart IXpe	site erion							₽ 2	
Reageer aneller op bedrijfsbehoeften, verbeter de beschikbaarheid – en betrouwbaarheidaniveaus per gebruiker en verlaag de kapitale en operationele kosten. Ontwikkeld op het marktleidende virtualisatieplatform, helpt het u het beheer van uw virtuele datacenter te vereenvoudigen. De VM/ware vCenter beheeroplossingen: vergroten operationele efficiency maken policy-gestuurd beheer mogelijk optimaliseren serviceniveaus	TEST 2								Welcon	ne
Ontwikkeld op het marktleidende virtualisatieplatform, helpt het u het beheer van uw virtuele datacenter te vereenvoudigen. De VI/Iware vCenter beheeroplossingen: vergroten operationele efficiency maken policy-gestuurd beheer mogelijk optimaliseren serviceniveaus	Re de	eageer sneller op bedrijfs I kapitale en operationele	behoeften, ve kosten.	erbet	er de bi	eschikb	aarheid – en betrouwbaarheidsniveaus p	er gebruiker	en verlaag	
vergroten operationele efficiency maken policy-gestuurd beheer mogelijk optimaliseren serviceniveaus	Or	ntwikkeld op het marktlei e VMware vCenter beheel	dende virtual roplossingen	lisatie ::	eplatfor	m, helpt	t het u het beheer van uw virtuele datace	enter te verei	envoudigen.	
maken policy-gestuurd beheer mogelijk optimaliseren serviceniveaus	ver	rgroten operationele effici	iency							
optimaliseren serviceniveaus	ma	aken policy-gestuurd beh	eer mogelijk							
Dona // Try start sites Brokentart Minder of C () () () ()	op	timaliseren serviceniveau	IS							
I Initial cities protected protect				_			A more detailed in the second study off		A 1000	-



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 Domains	and Trusts				
File Action View Help					
🗢 🔿 🙍 🖬 📑 🗟 🛛	?				
Active Directory Domains and	Trusts [S Name		Тур	e	
Develop.Intern	velop.Intern Properties				? ×
	aeneral Trusts Managed	By			
	Domains trusted by this dom	ain (outgoing tru	usts):		
	Domain Name	Trust Type	Transitive	Propertie	s
	Develop2.Intern	External	No	Pomou	
				Demov	
	Domains that trust this doma	iin (incoming tru:	sts):		
				[
	Domain Name	Trust Type	Transitive	Propertie	s
	Develop2.Intern	External	NO	Remov	e
					_ []
	New Trust				
-					
	ОК	Cancel	Apply	He	lp
	رك				

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.

Active Directory Users and Computers		🚟 Active Directory Users and Computers -	DEV2 - [Console Root\Active Dire	ctory Users and Com
File Action View Help		 Ele Action View Favorites Window Image: Action View Favorites Window Image: Action View Favorites Window Image: Action View Favorites Window 	Help 🗟 📘 📊 😤 🕸 🖆 🍸 💆	132. 132.
Active Directory Users and Computers [SDC01] Name Type Image: Saved Queries Image: Social Science Image: Social Science Image: Saved Queries Image: Social Science Image: Social Science Image: Saved Queries Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Image: Social Science Ima	ty Group - Global ty Group - Domain Local ty Group - Domain Local	Console Root Console Root Console Root Saved Queries Develop2.Intern Develop2.Intern Dulkin Computers Dulkin Computers Oreign5ecuntyPrincipals Smartsite Group Smartsite Group Smartsite B.V. Global Groups Local Groups Users Users	Name X Kperion_Administrators X Kperion_ChiefEditors X Kperion_Editors X Kperion_Visitors1 X Kperion_Visitors2 X Kperion_Webmasters	Type I Security Group Security Group Security Group Security Group Security Group Security Group

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.





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"</pre>
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"
        artsite.Se
                  curity.ActiveDirectoryConfigurationSection,
     </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>
     <add name="mm1" domain="Develop-int" providerName="ADDevelop"/>
<add name="mm2" domain="Develop.intern" providerName="ADDevelop"/>
                                  domain="Develop.intern" providerName="ADDevelop"/>
         </membershipMappings>
     </ADDevelop.Configuration>
```







of the security authentication mode used by
ASP.NET to identify an incoming user.
>
<pre><!-- ADS SETTING Front-end authentication mode integrated security and</pre--></pre>
Explicit REMOVE Forms Login>
<authentication mode="Windows"></authentication>
<pre><!-- <forms loginUrl="/Login" name="Smartsite" /--></pre>
<pre></pre>
<authorization></authorization>
<allow users="*"></allow>
ADS SETTING defaultProvider="ADMembershipProvider"
<pre><membership defaultprovider="ADDevelop" userisunlinetimewindow="15"></membership></pre>
<pre><pre>cproviders> </pre></pre>
<pre><clear></clear></pre>
<pre><!-- ADS SETTING CHANGE connectionosername and connectionPassword. Use user principal </pre--></pre>
name (username@domainname) syntax>
<add <="" applicationname="Smartsite" name="SqlMembershipProvider" td=""></add>
type="Smartsite.Security.Authentication.SqlMembershipProvider, Smartsite.Security"
enablePasswordRetrieval="true"
enablePasswordReset="true"
passwordFormat="Clear"
requiresQuestionAndAnswer="false"
writeExceptionsToEventLog="true"/>
<pre><add <="" applicationname="Smartsite" name="ADDevelop" pre=""></add></pre>
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider,
Smartsite.Security"
connectionStringName="ADDevelopConnection"
connectionUsername=1XperionADSadmin@Develop.intern
connectionPassword="******"
settingsSectionName="ADDevelop.Configuration"/>
<pre>Kadd applicationName="Smartsite" name="ADDevelop2"</pre>
type="Smartsite.Security.Authentication.ActiveDirectoryMembershipProvider,
Smartsite.Security"
connectionstringName="AuDevelop2Connection"
connectionUsername= <u>1XperionADSadmin@Develop.intern</u>
connectionPassWord="******"
settingsSectionName="ADDevelop2.Configuration"/>
<pre><!-- ADS SETTING SET defaultProvider="ADKoleProvider"--> </pre>
<pre><rolemanager <="" cacherolesincookie="true" defaultprovider="ADRoleProvider" enabled="true" pre=""></rolemanager></pre>
cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/" cookieRequireSSL="false"
<pre>cookieSlidingExpiration="true" cookieProtection="All"></pre>
<pre><pre>cproviders></pre></pre>
<clear></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="FileNotFound.htm" /> </customErrors> --> <customErrors mode="RemoteOnly" defaultRedirect="/Ned/error page nl.html"> <pror statusCode="404" redirect="/Ned/error_page_nl.html"/> </customErrors> <identity impersonate="false"/> <httpModules> <!-- replace default FormsAuthentication with Smartsite one --> <!--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"/> </httpHandlers> <anonymousIdentification enabled="true"/> <profile enabled="true" automaticSaveEnabled="true" defaultProvider="SmartsiteProfileProvider"</pre> 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=5fdbl2a67e027fb6" 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"</pre> behaviorConfiguration="StateSyncServiceBehavior"> <endpoint address="net.pipe://localhost/intranet/StateSyncService"</pre> 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"</pre> behaviorConfiguration="InteropServiceBehavior"> <endpoint address="net.pipe://localhost/intranet/InteropService"</pre> binding="netNamedPipeBinding" bindingConfiguration="InteropServiceBinding" contract="Smartsite.Core.Services.IInteropService"/> </service> <!--Service providing schema information to the SXML editor--> <service name="Smartsite.Core.Services.SchemaService"</pre> behaviorConfiguration="SchemaServiceBehavior"> <endpoint address="http://Intranet/intranet/SchemaService"</pre> 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"</pre> behaviorConfiguration="EventSynchronizationServiceBehavior"> <endpoint address="http://intranet/intranet/EventSynchronizationService"</pre> binding="wsDualHttpBinding" contract="Smartsite.Core.Services.IEventSubscriptionContract"/> </service> <!--Common service for managing CMS--> <service name="Smartsite.Core.Services.ManagerService"</pre> $behavior {\it Configuration} = "{\it Manager Service Behavior"} >$ <endpoint address="http://intranet/intranet/ManagerService"</pre> 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"/>



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 --> <client> <!-- (client) endpoint definition used for connecting to the cmsWebservice --> <endpoint address="http://intranet/cms/manager.dws" binding="basicHttpBinding"</pre> bindingConfiguration="cmsWebserviceSoapBinding" contract="cmsWebserviceSoapPort" name="cmsWebserviceSoapPort"/> <!-- (client) endpoint definition used for connecting to the EventSubscription/EventSynchronization service --> <endpoint address="http://intranet/intranet/EventSynchronizationService"</pre> binding="wsDualHttpBinding" bindingConfiguration="WSDualHttpBinding_EventSubscriptionService' contract="Smartsite.Core.EventSynchronizationClient.EventSubscriptionService" name="WSDualHttpBinding_EventSubscriptionService"> <!-- DEPRECATED Post-RC1 --> <!-- identity> <userPrincipalName value="iXperion_Admin" /> </identity --> </endpoint> <endpoint address="http://192.168.252.7:2020/Intranet/HitService"</pre> 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"/>



Implementatiehandleiding Active Directory voor Smartsite iXperion

</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=""/> <!-- 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,</pre> 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="nederlands.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="9999999"
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>
```



<defaultdocument></defaultdocument>
<files></files>
<clear></clear>
<add value="manager.dws"></add>
Disable detection of IIS6 / Classic mode ASP.NET configuration</td
>
<validation validateintegratedmodeconfiguration="false"></validation>



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.

🛃 Active Directory Tester - 1.4.290.0	
Site	- Get User Result
Select web.config to read settings from	
Provider type	
Active Directory	
C LDAP to Active Directory	
C LDAP	
Credentials	
Address	
Username	
Password	
SearchBase	
Test Connection	
Search Parameters	
searchUserQuery	
attributeMapUsername	
Account to test	
Username	
Password	
Get Parent Groups (recursive)	
🔽 Get Primary Group	
☐ Validate credentials	
Verbose Get User	

De Active Directory Tester

Site	
Select web.config to read settings from	
E:\Sites\Intranet\WWW\Web.config	2

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



Implementatiehandleiding Active Directory voor Smartsite iXperion

📴 Select web.config					×
Computer	▼ Data (E:) ▼ Sites ▼ Intranet ▼ WWW ▼	▼ 2	Search WWW		2
Organize 🔻 New folder					0
🔶 Favorites	Name *	Date modified	Туре	Size	
E Desktop Downloads	Select Provider Multiple Active Directory and/or LDAI found within selected web.confg. Sel provider from which to load the confi	^o membership provid ect the membership guration.	ers		
Documents Music Pictures Videos	Select membership provider ADDevelop (connection: LDAP://DEVELOP ADDevelop2 (connection: LDAP://DEVELO	.INTERN) P2.INTERN)			
P Computer Local Disk (C:)	<u> </u>	OK Cano	el jie	21 1	(B
👊 Network 📃					
File na	me: Web.config	•	Web config (we Open	b.config) Cancel	

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

🔜 Active Directory Tester - 1.4.290.0	-	
Site	Cet User Result	
Select web.config to read settings from E:\Sites\Intranet\W/WW\Web.config		-
Provider type C Active Directory LDAP to Active Directory C LDAP to Active Directory C LDAP Credentials Addess LDAP.//DEVELOP2INTERN Username VyperiorADSadmin@Develop intern Password Saterkiese		
SearchParameters SearchParameters searchUseQuery attributeMapUsemame	Connected to LDAP-//DEVELOP2.INTERN.	
Account to test Username Password Get Parent Groups (recursive) Get Primary Group Validate credentials		
Cet User	<u>x</u>	ľ

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

Active Directory Tester - 1.4.290.0	
Site Select web.config to read settings from E:\Sites\Intranet\WWW\Web.config	Get User Result
Provider type C Active Directory C LDAP to Active Directory C LDAP Credentials Address LDAP://DEVELOP2.INTERN	
Usemane (VoerionADSSmartate@Develop2.intem) Password Search8ase do-develop2.do-initiem Test Connection	Connection succeeded Connected to LDAP://DEVELOP2.INTERN.
Search Parameters searchUserQuery atributeMapUsername	
Account to test Usemane Password G Get Parent Groups (recursive) G Get Primary Group	
Verbose Get User	



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

🔛 Active Directory Tester - 1.4.290.0	
Site	Get User Result
Select web.config to read settings from	Getting root entry " before searching user
E:\Sites\Intranet\WWWWeb.config	
	Searching Active Directory for '(SAMAccountName=sbosch)'
Provider type	(LDAP://DEVELOP.INTERN/CN=Silvio Bosch,OU=- Develop Root-OU -,DC=Develop,DC=Inter
 Active Directory 	Getting group membership for user 'sbosch'
C LDAP to Active Directory	
C LDAP	Group membership retrieved in 294 ms.; 9 groups found. User 'sbosch' is member of the following groups:
Credentials	- Domain Users
	- users - ixperion_administrators
	- ixperionmanageraccessgroup
Reperional Sadmin@Develop.intern	- ixperion_webmasters
Password ******	- denied rodc password replication group
SearchBase dc=develop,dc=intern	- administrators
Test Connection	
Search Parameters	
searchUserQuery	
attributeMapUsername	
Account to test	
Username sbosch	
Password	
Get Parent Groups (recursive)	
🔽 Get Primary Group	
□ Validate credentials	
Get User	

Na het invullen van een account username kunnen diens groepen worden bevraagd. 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

Registeer 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



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.

📸 Registry Editor		The Party of Street, or other					
<u>File Edit View Favorites H</u> elp							
License	*	Name	Туре	Data			
D Locales		(Default)	REG_SZ	(value not set)			
D - Logging		ab LogonHandler	REG_SZ	SixSecurity.LDAP			
D Macros				-			
Manager							
▶ · · · · · · · · · · · · · · · · · · ·	-						
٠ III	•	< III.		۰. ۲			
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Smartsite Software\Smartsite\Sites\SNN2\Security							

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"</pre>
type="Smartsite.Security.ActiveDirectoryConfigurationSection, Smartsite.Security" />
   <section name="Smartsite.ConfigurationSource"</pre>
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"</pre>
      <add name="StoreFullyQualifiedLoginName" value="false" />
      <add name="SearchBase" value="ou=SMARTSITE GROUPS,o=SENECA" />
```



```
<add name="DatabaseId" value="manager" />
    </settings>
  <membershipMappings>
 <add name="mm1" domain="smartsite" providerName="novell" />
    </membershipMappings>
  </Smartsite.LDAPConfiguration>
  <svstem.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"</pre>
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>
```



```
</profile>
    <membership defaultProvider="novell" userIsOnlineTimeWindow="15">
   <providers>
<clear />
       <add name="novell" applicationName="Smartsite"
     "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="FileNotFound.htm" />
            </customErrors>
            -->
    <customErrors mode="Off" />
    <httpModules>
      <add type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge" name="ixbridge"
/>
      <add type="Smartsite.ImageProcessor.ImageServerModule,Smartsite.ImageProcessor"</pre>
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" />
```



```
<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>
```



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



```
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"</pre>
bindingConfiguration="cmsWebserviceSoapBinding" contract="cmsWebserviceSoapPort"
name="cmsWebserviceSoapPort" />
      <!-- (client) endpoint definition used for connecting to the
EventSubscription/EventSynchronization service -->
      <endpoint address="http://Intranet/Intranet/EventSynchronizationService"</pre>
binding="wsDualHttpBinding"
bindingConfiguration="WSDualHttpBinding EventSubscriptionService"
contract="Smartsite.Core.EventSynchronizationClient.EventSubscriptionService"
name="WSDualHttpBinding EventSubscriptionService" />
      <endpoint address="http://localhost:2020/mysite/HitService"</pre>
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">
```



```
<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 -->
  <svstem.webServer>
    <modules>
      <add name="ixbridge" type="Smartsite.AspNet.Bridge.Hook,Smartsite.AspNet.Bridge"</pre>
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

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" />
```

🔄 Novell iManager - Microsoft Internet Explorer						
Eile Edit View Favorites Tools Help						
🕒 Back + 🕤 - 💌 😰 🐔 🔑 Search 🔅 Favorites 🥑 🗇 - 😓 🚍						
Address 🕘 http://192.31.142.123/nps/servlet/webact?taskId=fw.Startup						
Novell _® iManager	1023					
ADMIN						
Unrestricted Access			N			
Roles and Tasks	LDAP Server: 🕅 LDAP Server - SA	8				
All Categories	General					
eDirectory Administration	Information Connections Searches Events	4				
eDirectory Maintenance						
🗄 Groups	Transport Laver Security (TLS / SSI					
🗉 Help Desk	Somer Contificates					
🗆 LDAP	server cercificate:					
Create LDAP Object	Client Certificate:	Not Requested				
LDAP Options	Trusted Root Containers:					
E NMAS	✓ Require TLS for all operations					
Novell Certificate Access	Enable and require mutual authentication					
View My Certificates						
View User Certificates	Ports					
E Novell Certificate Server	Enable Encrypted Port					
Partition and Replicas	Port: 636					
E Rights	✓ Enable Non-Encrypted Port					
± Schema	Port: 389					
E SNMP						
E Users	Restrictions					
WAN Traffic	Concurrent Bind Limit: 0	binds (10 for po limit)				
	Idle Timeout:					
	Rind Dostrictions:	seconds (u for no timeout)				
	bind Rescrictions. [None	•				
	OK Cancel Apply					
	Cancer Apply					
e			S Internet			


Implementatiehandleiding Active Directory voor Smartsite iXperion

🚈 Novell iManager - Microsoft Internet E	xplorer		
Eile Edit View Favorites Iools Help	D		- R
🔾 Back 🔻 🕥 👻 😰 🐔 🔎 Search	n 📌 Favorites 🛷 🛛 😥 💀		
Address 🕘 http://192.31.142.123/nps/servle	t/webacc?taskId=fw.Startup	💌 🔁 Go	Links »
Novell _® iManager			
ADMIN			N.L
Unrestricted Access			N
Roles and Tasks	LDAP Group: 🏽 LDAP Group - SMARTSITE_VM-NDS-SENECA		8
All Categories	General		
eDirectory Administration	Information Referrals Attribute Map Class Map		
E Groups	Server List		
🗄 Help Desk			
🗆 LDAP			
Create LDAP Object Delete LDAP Object			
LDAP Options	Authentication Ontions		
I NMAS			
Novell Certificate Access			
View User Certificates	Require TLS for Simple Binds with Password		
Novell Certificate Server			
Partition and Replicas			
🗉 Schema			
I SNMP			
🗉 Users			
🗉 WAN Traffic			
	OK Cancet Apply		



Implementatiehandleiding Active Directory voor Smartsite iXperion

18IIS Configuratie voor Novell

18.1 Front-End Authentication

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

Internet Information Services (IIS) Manager				
	🕨 Sites 🕨 Intranet 🕨			
Connections	Authentication			
GRAWIN2008-64 (ORAWIN2008-6	Group by: No Grouping	•		
Application Pools	Name 🔺	Status	Response Type	
🖻 🔂 Sites	Anonymous Authentication	Enabled		
🕀 😜 Intranet	ASP.NET Impersonation	Disabled		
	Basic Authentication	Disabled	HTTP 401 Challenge	
	Forms Authentication	Enabled	HTTP 302 Login/Redirect	
	Windows Authentication	Disabled	HTTP 401 Challenge	
Smartsite iXperion Intranet Site - Login - Windows Internet Explo				
✓ Favorites				
> Smartsite iXperion Intranet Site - Login	🛐 🔹 🔜 🖌 🖃 🖶 🔹 Bage 🕶 Saf	ety + Tools + 🕡 +		
Smartsite Ixperion		₩ 2 [▲]		
		Welcome		
This page requires you	to log on			
User name silvio				
Password				
Remember Me				
Let me in!				
Home Change Password My Profile About this site Sitemap Log	in <u>iXperion Status Info</u>			
Done	🚯 Local intrapet Protected Moder Off	▼ ▼ 100% ▼		
	Second intranet Letotected House, OIL	100 %		

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

Manage Content Access - Smartsite Dynamic Web System Webpage Dialog	
ublication CMS Custom	
Manage Content Access On this tab you can set Publication (Browse) Access for the items selected in the tree. The Curre Access and Apply buttons work on the current selection in the tree (use the Include all children or box to make the selection recursive).	nt heck
☑ Include all children	
Guest Access Set access for the Guests group, which should contain all users and visitors. Only higher access I will be relevant for other groups.	levels
iuest Access No Access	
(perionWebmaster Leave Unchanged	
Apply E Current Access	s
	Close

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.



🔏 Google - Windows Internet Explorer		_ 🗆 🗙
S S Thtp://intranet/cms/	💌 🕁 🔀 Bing	₽ •
😭 Favorites 🛛 🚔 🙋 Suggested Sites 🔹 🙋 Web Slice Gallery 🔹		
Connecting	🟠 + 🗟 + 🖃 (🚋 🔹 Page 🔹 Safety 👻 Tools 👻 🔞 👻
Het internet <u>Afbeeldingen</u> <u>Video's</u> <u>Maps</u> <u>Nieuws</u> <u>Boeke</u>	<u>n Gmail meer</u> v iGo	oogle Zoekinstellingen Aanmelden
Windows Security The server intranet at 'intranet' Warning: This server is requesting an insecure manner (basic authors) Silvio silvio silvio Remember	requires a username and password. Ing that your username and password be sent in ntication without a secure connection). my credentials OK Cancel	Geavanceerd zoeken Taalhulpmiddelen



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).

🥖 Edit Users - Sn	nartsite Dynamic Web System We	bpage Dialog 🛛 🛛 🗙	
Edit record 4			
Credentials		Properties	
Login Name silvio		Full Name bosch	
Password ••••••		Email address silvio@seneca.nl	
Security			
Usergrou Primary group)	Administrators Content Editors Content Managers DigiD Users StartGroup Visitors	Guests iXperionWebmaster	
Account Settin	ngs	□ □ Account Status	
	🗆 Is Visitor	Last Login 6-12-2010 13:36:21	
ļ	Account Disabled	Last Locked Out	
Activate on ((not set)	Failed Passwords 4	
Expiration on (not set)		Failed Passwords Window Start 6-12-2010 13:55:04	
Localization	(None)		
		🛱 Copy 🛛 🚑 Paste 🔰 🔚 Save 🛛 🚫 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

🗿 Manage Content Ad	cess - Smartsite Dynamic Web System Webpage Dialog	1
Publication CMS Cu	stom	
(i) Manage Con On this tab you c and Apply button make the selection	tent Access In set CMS (Manager) Access for the folders selected in the tree. T work on the current selection in the tree (use the Include all child n recursive). Only folders will be affected.	he Current Access ren check box to
[V] In	lude all children	
Administrators	Leave Unchanged	•
Content Managers	Leave Unchanged	•
Content Editors	Leave Unchanged	•
iXperionWebmaster	Edit - Edit folder and items below it	•
Visitors	Leave Unchanged	•
DigiD Users	Leave Unchanged	-
Legacy Ren Legacy rendering	dering Access is used for some application pages in the cms manager and Legacy	r Forms. The
Guest Access Leave	: Unchanged	
1		Current Access
		🗵 Close

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.

🕗 Novell iManager - Microsoft Internet Ex	بهاorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
🔇 Back 🔹 🕥 👻 👔 🐔 🔎 Search	👷 Favorites 🛛 🖉 + 😓 🕞
Address 🐻 http://192.31.142.123/nps/servlet	/webacc
Novell _® iManager	
ADMIN	
Unrestricted Access	
Roles and Tasks	Modify User: 🗳 silvio.SMARTSITE_GROUPS.SENECA
All Categories	Conners] MILLEL Maked, MILLEL Committee Deskinister
eDirectory Administration	Identification Environment Group Memberships Postal Address Login Script See Also
• eDirectory Maintenance	
± Groups	Group membership:
	ManagerAccessLocal.SMARTSITE_GROUPS.SENECA
	Smartsite software.SMARTSITE_GROUPS.SENECA
1 NMAS	IXperionWebmaster.SMARTSITE_GROUPS.SENECA
Novell Certificate Access	
🗄 Novell Certificate Server	
Partition and Replicas	
🛨 Rights	
🗄 Schema	
⊕ SNMP	
Create User	
Delete User	Count: 3
Disable Account Enable Account	
Modify User	
WAN Traffic	

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).

Intranet - Smartsite CMS - intranet - Windows Internet Explorer		
S S + http://intranet/cms/	💌 🐓 🗙 🔁 Bing	- Q
🖕 Favorites 🛛 🏡 🙋 Suggested Sites 👻 🙋 Web Slice Gallery 💌		
> Intranet - Smartsite CMS - intranet	👌 • 🔊 - 🖃 🖷	a + Page + Safety + Tools + 🕢 +
Edit Content View Tools Configuration Admin Outscaling	g Extra SEO Role 👍	
Smart : Configure Security - Smartsite Dynamic Developer Smartsite Console 145 - Googlew Sessions 593 - Reposito Edit Users 2 - Welcome ^R Edit Groups 4 - Content He Edit Content Access Types 3 - Configureit Edit Content Access Types Edit Content Access Types Edit Content Access Types	Start Page View Version Web System Webpage Dialog StartGroup Administrators Visitors Content Managers StarperionWebmaster	
Subject Priority Subject Subj	Last modified Assign	Novell group in SMARTSITE_GROUPS.SENECA Description Image: Content Editor Content Editor Content Editor Guest Vistor
(Empty)		
Configure Security	Cocal intranet Protected Mode	n Copy 🖨 Paste 🔰 🖶 Save 🚫 Cancel



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> <clear /> Line 72: 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" /> <add applicationName="Smartsite" name="SqlMembershipProvider" Line 74: 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

🚈 Novell iManager - Microsoft Internet E	xplorer		
Eile Edit View Favorites Iools Help)		- -
🔾 Back 🔹 🕥 👻 😰 🐔 🔎 Search	n 📩 Favorites 🛛 🖉 - 🚴 🕞		
Address 💩 http://192.31.142.123/nps/servle	t/webacc	💌 🔁 Go	Links »
Novell _® iManager			
ADMIN			
Unrestricted Access			Ν
Roles and Tasks	LDAP Server: 😥 LDAP Server - SMARTSITE VM-NDS.SENECA		1
All Categories	_		_
eDirectory Administration	General		
eDirectory Maintenance			
E Groups	Success	el l	<u> </u>
E Help Desk	Success	-	
	Your changes have been saved.		
Create LDAP Object			_
Delete LDAP Object	Transport Layer Security (TLS / SSL)		
	Server Certificate: SSL CertificateDNS		
T Novell Certificate Access	Client Certificate: Not Requested 🔽		
Novell Certificate Server	Trusted Root Containers:		
Partition and Replicas	Require TLS for all operations		
	Enable and require mutual authentication		
E Schema			
E SNMP	Ports		
∃ Users	Enable Encrypted Port		
🗄 WAN Traffic	Port: 636		
	Enable Non-Encrypted Port		
	Port: 389		
	Restrictions		
	Concurrent Bind Limit:		
	Rind Deskelations		•
	OK Cancel Apply		

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