

Objecten in Adlib uitsluiten van webweergave

Inleiding

Iedereen die gegevens in Adlib wil laten zien op internet, krijgt ermee te maken: bepaalde dingen wil je juist niet laten zien. Hoe geef je dat aan?

Het is mogelijk om Adlib te voorzien van vinkvakjes "niet tonen op internet", of "mag getoond worden op internet". Een webbouwer moet daar dan rekening mee houden.

Het is ook mogelijk om te werken met record-uitsluiting. Een webbouwer merkt daar niets van, zij of hij krijgt gewoon de 'verboden' records niet te zien. In dit document ziet u hoe dit kan worden ingericht.

Inhoud

Inleiding	1
Record-uitsluiting in het Zuiderzeemuseum	2
Uitsluiting van beelden.....	8
Standaardwaarden voor de velden UR en RQ instellen in Designer	9
Reden voor uitsluiting van records opgeven.....	10
Bijlage 1: Excluding anonymous internet users from specific records	11
Setup in IIS 7 (Windows 2008).....	2
Setup in IIS 6 (Windows 2003).....	4
Further setup in MS SQL Server Management Studio.....	6
Excluding records in the Adlib application	7
Bijlage 2 – database-instellingen voor record-uitsluiting.....	9
Colofon	13

Record-uitsluiting in het Zuiderzeemuseum

door Shannon van Muijden
databeheerder Collectie
Zuiderzeemuseum Enkhuizen
shannon.van.muijden@zuiderzeemuseum.nl

Het Zuiderzeemuseum gebruikt twee velden in Adlib om objecten uit te sluiten van online weergave, dit zijn de velden **recordbeveiliging.gebruiker** met tag UR en **recordtoegang.rechten** met tag RQ. In Adlib-modelapplicatie 4.5 zijn deze velden al gedefinieerd, zie bijlage 2 voor de instellingen. Voor de gebruiker zijn deze velden zijn te vinden in het tabblad Beheergegevens in de Museum- en Bibliotheekcatalogus, en in de Multimedia-documentatie. We regelen het uitsluiten van objecten in de database **collect (museumcatalogus)**, en het uitsluiten van losse foto's in de database **media**.

Als een object in collect wordt uitgesloten van online weergave worden er automatisch ook geen beelden online getoond die aan dat object zijn gekoppeld. Er wordt bij het online tonen dus altijd uitgegaan van de database collect.

De betreffende velden worden niet opgenomen in de api, maar de informatie daarin wordt onder water in de **Internet Information Services (IIS) Manager** verwerkt. Hieronder een uitleg hoe dat in z'n werk gaat:

1. Op de server zijn gebruikers ingesteld. Dit zijn de mensen die werkzaam zijn op de server en elke dag inloggen via een gebruikersnaam en wachtwoord. Er moet een nieuwe gebruiker (local user) toe worden gevoegd aan de server waar Adlib op draait, dit is de gebruiker die wordt gedefinieerd als de 'internet-gebruiker' oftewel iemand die van buitenaf toegang wil krijgen tot informatie op de locale server. Standaard gebruikt Windows hier de term IUSR voor. In IIS staat dat als volgt vermeld:

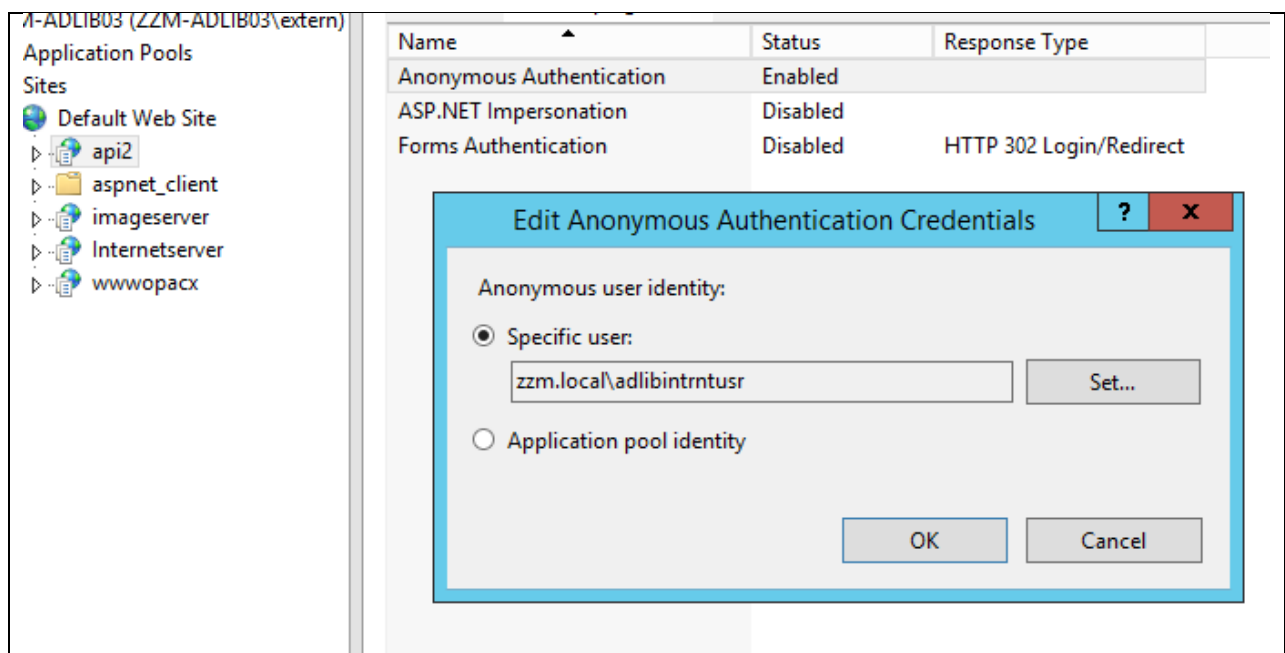
This built-in account does not need a password and will be the default identity that is used when anonymous authentication is enabled. If you look in the applicationHost.config file you will see the following definition: ¹

```
<anonymousAuthentication enabled="true" userName="IUSR"  
defaultLogonDomain="" />
```

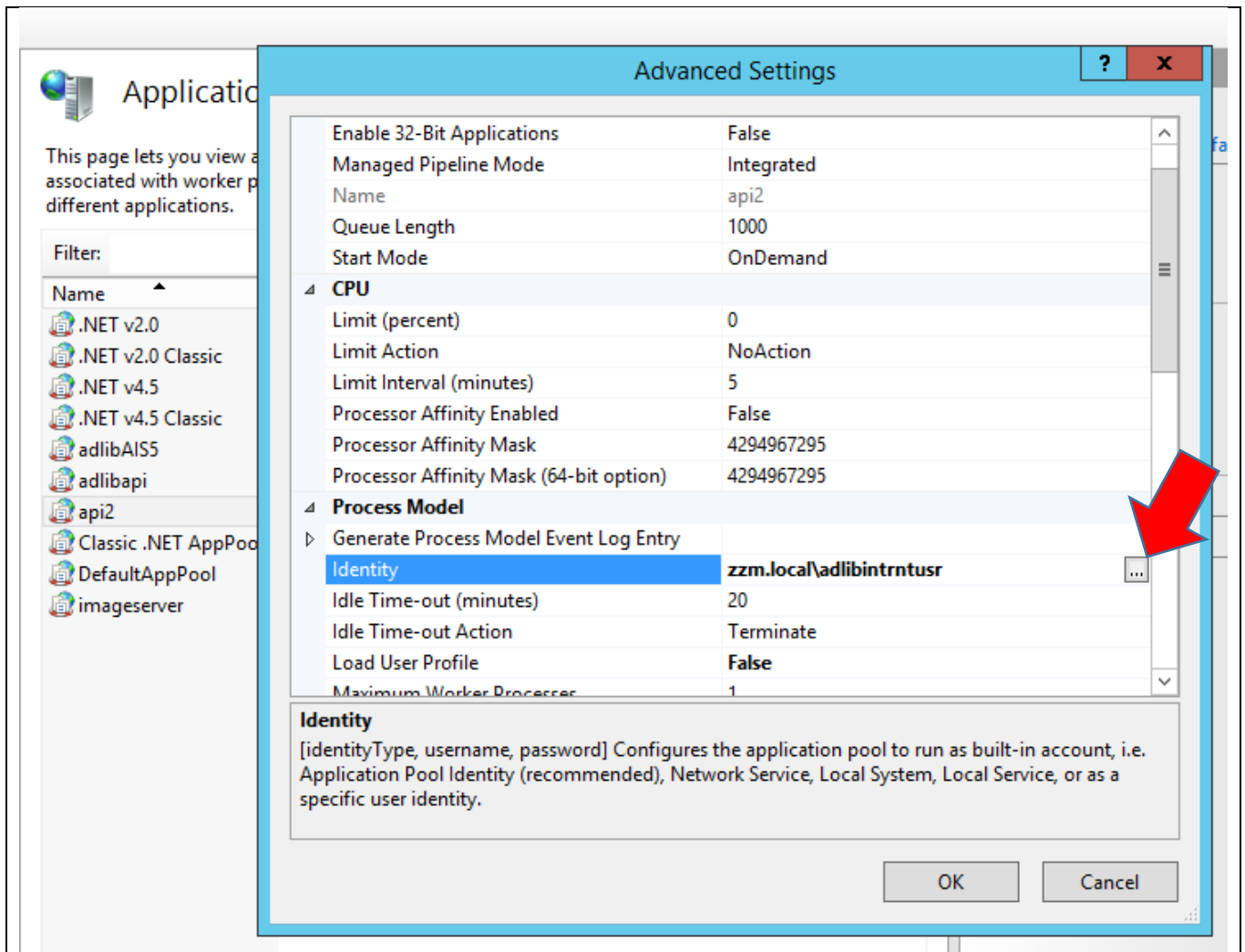
Het is makkelijker om in plaats van IUSR te gebruiken, zelf een nieuwe 'internet'-gebruiker aan te maken. Wij hebben hiervoor de gebruiker met naam **adlibintrntusr** aangemaakt. Deze gebruiker moet op de local server worden aangemaakt door de systeembeheerder.

2. Als deze user is aangemaakt moet hij in IIS worden gedefinieerd als zijnde de eigenaar van de application pool waar de betreffende internet-api onder valt. Zie bijlage 1 onder aan dit document voor uitleg over het instellen van gebruikers op de application server.
3. Anonymous Authentication moet op Enabled staan, met de specific user ingesteld op de betreffende internet-gebruiker, bij ons als volgt:

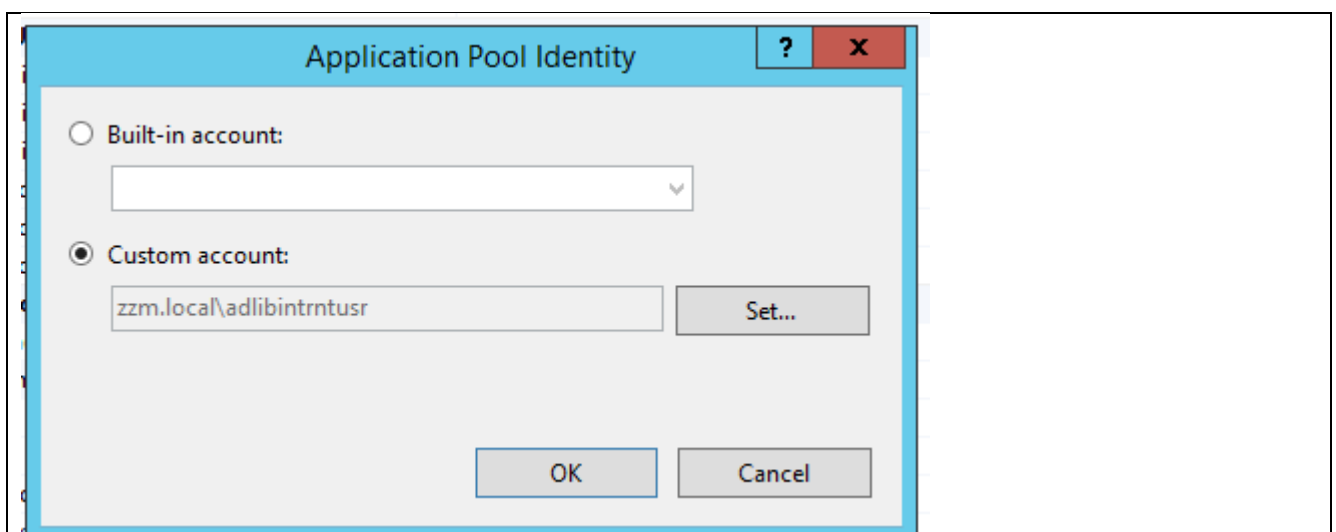
¹ Bron: <http://www.iis.net/learn/get-started/planning-for-security/understanding-built-in-user-and-group-accounts-in-iis>



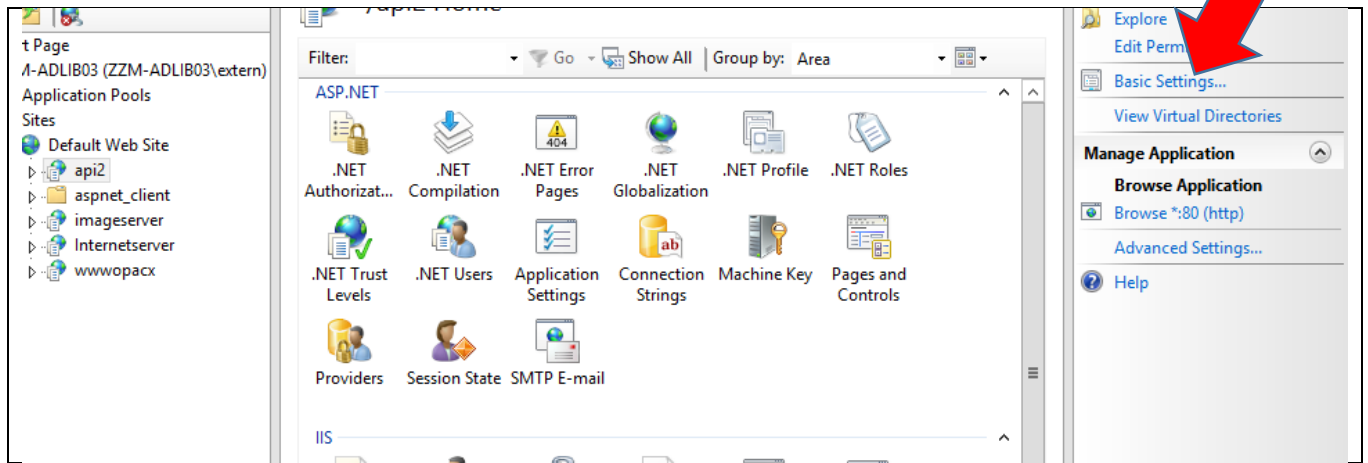
En in de advanced settings van de api als volgt bij Identity:



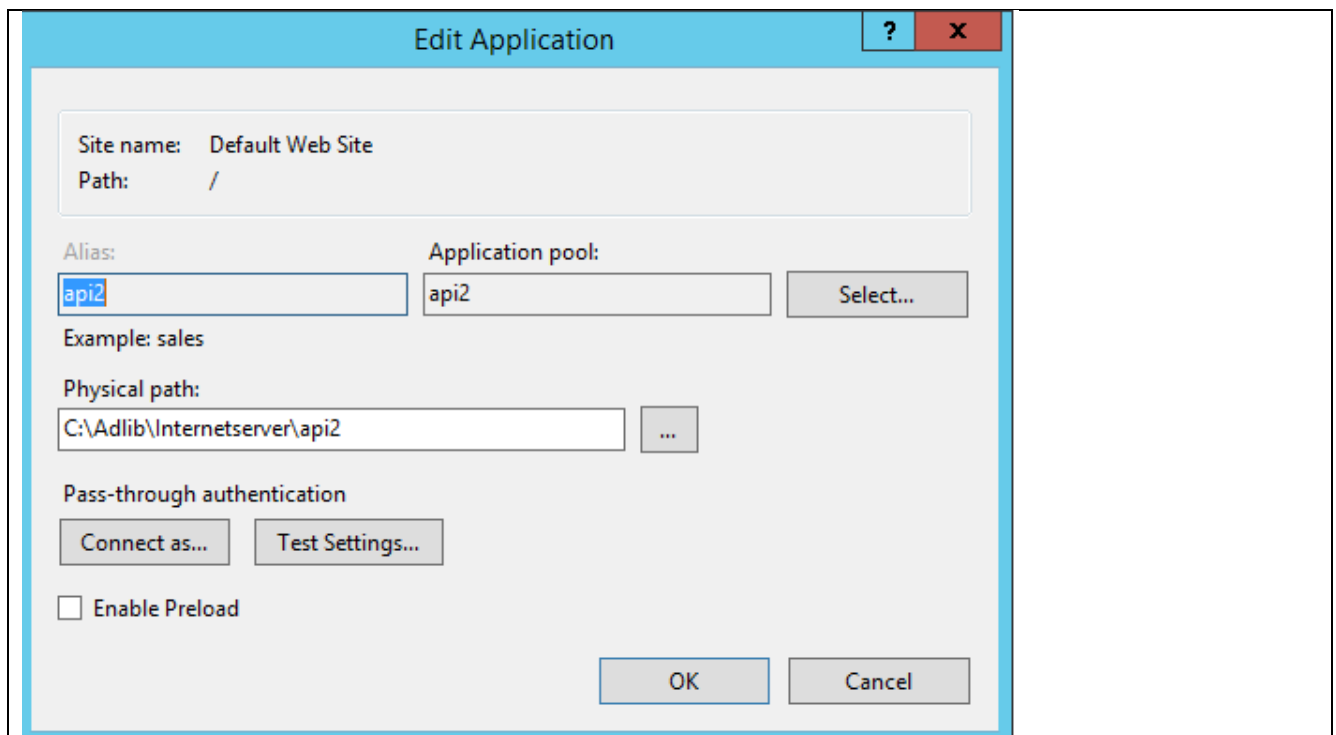
Druk op het vierkantje met drie puntjes achter de user (rode pijl). De user moet daar als volgt in staan onder Custom account:



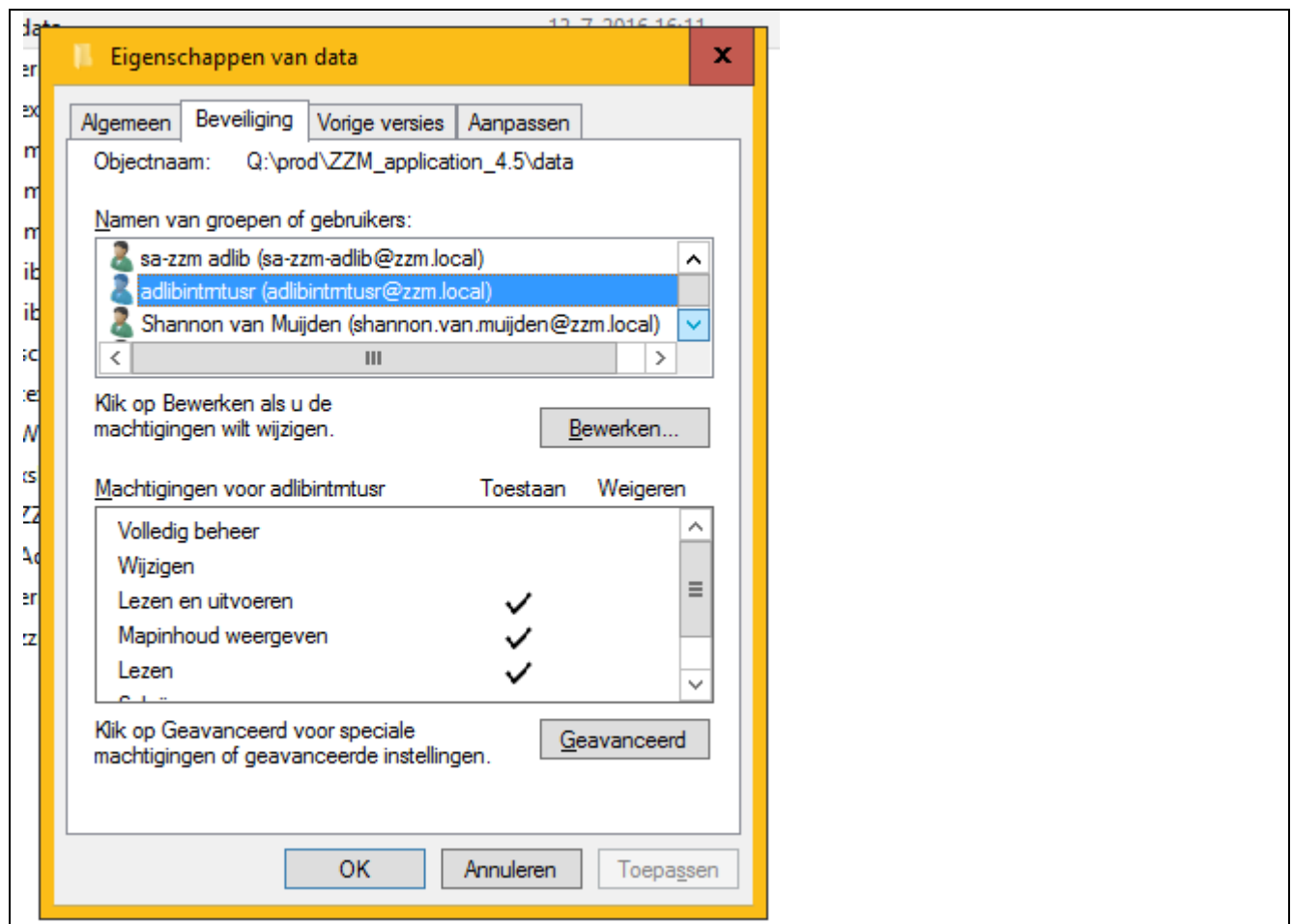
4. In IIS, in het Home-menu van de betreffende api, moet in Basic settings (zie hieronder)



de Application pool ingesteld staan op de betreffende internet-api. Dat is bij ons api2:



- Ga naar de map op de server waar de Adlib applicatie zich bevind. Klik op de map data (..\ZZM_application_4.5\data) en kies eigenschappen.



In het tabblad Beveiliging moet de betreffende user worden ingesteld, dwz; de user moet toegang hebben tot de map data. Via de knop Bewerken... kan een user worden toegevoegd.

- De internetgebruiker is nu aangemaakt als gebruiker op de lokale server en eigenaar van de api die de koppeling Adlib-metadata naar internet regelt. Er rest nu nog een ding en dat is in Adlib aangeven dat de gebruiker de naam (in dit geval) adlibintmtusr heeft in het veld UR.

Recordtoegang	
Gebruiker / groep	Rechten
adlibintmtusr	Alleen lezen
Eigenaar	administrator
Webuitsluiting	
Reden van uitsluiting	

Dit kan gemakkelijk met een zoek-en- vervang actie in Adlib worden uitgevoerd. Denk er hierbij aan dat het veld UR moet worden ingevuld in de database collect (objecten in eigen beheer) **en ook in de database media (multimedia-documentatie)**. Ook het veld rechten (RQ) moet worden ingevuld. **Geen (of 0) bij geen internetweergave en Alleen lezen (of 1) bij internetweergave**. Het invullen van deze velden kan lang duren als er veel objecten in de database zitten. Het is wel mogelijk om meerdere zoek-en- vervang acties tegelijk te laten lopen, maar denk er hierbij aan dat niemand op dat moment in Adlib mag muteren anders wordt er een foutmelding weergegeven. Het gemakkelijkst is dus om deze zoek-en- vervang invulacties 's nachts of in het weekend te laten lopen.

7. Als het veld UR in Adlib (zowel in collect als media) gevuld is met de naam van de gebruiker en de rechten in veld RQ zijn gevuld met of Geen of Alleen lezen dan kan er getest worden door de metadata via de api op te vragen. Vul in de browser het lokale pad naar de api in gevolgd door /wwwopac.ashx?database=collect&SEARCH=priref=8 (priref is het recordnummer uit Adlib, database collect. In dit geval dus recordnummer 8, wat een record is dat op 'Alleen lezen', dus online tonen staat)

Als het record **online getoond mag worden** dan is hij als volgt zichtbaar:

This XML file does not appear to have any style information associated with it. The document tree is shown below:

```
<adlibXML>
  <recordList>
    <record priref="8" created="2015-11-25T22:11:02" modification="2016-07-13T15:36:17" selected="Fa
      <ACCESS_RIGHTS>
        <record_access.rights>
          <value lang="neutral">1</value>
          <value lang="0">Read</value>
          <value lang="1">Lezen</value>
          <value lang="2">Lire</value>
          <value lang="10">קורא</value>
        </record_access.rights>
        <record_access.user>adlibintrntusr</record_access.user>
      </ACCESS_RIGHTS>
      <Associated_subject>
        <association.subject.type>
          <value lang="neutral">GEOKEYW</value>
          <value lang="0">geography</value>
          <value lang="1">geografie</value>
          <value lang="2">géographie</value>
          <value lang="3">Geografie</value>
          <value lang="4">جغرافي</value>
          <value lang="5">geografia</value>
          <value lang="6">γεωγραφία</value>
          <value lang="9">geografi</value>
          <value lang="10">גאוגרפיה</value>
          <value lang="11">geografi</value>
        </association.subject.type>
        <association.subject>
          <value lang="">Hindeloopen</value>
        </association.subject>
        <associated.subject.erfgeo_uri>http://sws.geonames.org/2754059/</associated.subject.erfgeo_u
        <associated.subject.latitude>52.94212</associated.subject.latitude>
        <associated.subject.longitude>5.40081</associated.subject.longitude>
      </Associated_subject>
      <Content_subject>
        <content.subject>
          <value lang="">Bijbel</value>
        </content.subject>
        <content.subject.erfgeo_uri/>
        <content.subject.latitude/>
        <content.subject.longitude/>
        <content.subject.tax/>
        <content.subject.tax.rank/>
        <content.subject.type/>
      </Content_subject>
      <current_location.name>d3_rB_pA</current_location.name>
      <current_owner>
        <value lang="">Stichting Zuiderzeemuseum</value>
      </current_owner>
      <Description>
        <description>
          In het oude testament komt een aantal romantische ontmoetingen voor. Op dit haardscherm zi;
          huwelijksgeschenk.
        </description>
      </Description>
      <Dimension>
        <dimension.value>92.0</dimension.value>
        <dimension.type>
          <value lang="">hoogte</value>
        </dimension.type>
      </Dimension>
    </record>
  </recordList>
</adlibXML>
```

Als het record **online niet getoond mag worden** dan is het volgende zichtbaar:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<adlibXML>
  <recordList/>
  <diagnostic>
    <hits>0</hits>
    <xmltype>Grouped</xmltype>
    <link_resolve_time unit="mS" culture="nl-NL">0</link_resolve_time>
    <first_item>1</first_item>
    <search>priref Equals '9958'</search>
    <sort/>
    <limit>1</limit>
    <hits_on_display>0</hits_on_display>
    <response_time unit="mS" culture="nl-NL">15,6087</response_time>
    <xml_creation_time unit="mS" culture="nl-NL">0</xml_creation_time>
    <dbname>collect</dbname>
    <dsname>intern</dsname>
  </diagnostic>
  <cgistring>
    <param name="database">collect</param>
  </cgistring>
</adlibXML>
```

Uitsluiting van afbeeldingen

Door in de database media per foto de recordtoegang-rechten in te stellen is het mogelijk te selecteren welke foto's je bij een record wilt tonen. Heb je bijvoorbeeld 3 foto's bij 1 record, en je wilt daarvan maar 2 online tonen, zet de rechten van die laatste twee foto's op 'Alleen lezen' (of 1) en zet de rechten van de foto die je niet online wilt tonen op 'Geen' (of 0).

Voorbeeld bij ons:

Aan object 006643 hangen drie beelden

Lijstscherf Beelddocumentatie - [Objectnummer = 006643] Miniaturweergave

☐		ea47ddc7-dff1-4a3b-5539-bcaf3c474b59 / / /
☐		b8096a47-1ead-8e48-98cf-c1a1fc6befc9 / / /
☐		ff0de9ac-18cb-c962-8301-464bf2b480b5 / / /

Alleen de onderste twee willen wij online tonen, de zwart-wit foto niet. De rechten staan als volgt ingesteld (in volgorde):

Recordtoegang		
Gebruiker / groep	Rechten	
adlibintrntusr	Geen	
Eigenaar	administrator	
Online status in collect	Lezen	Webuitsluiting reden in collect

Recordtoegang		
Gebruiker / groep	Rechten	
adlibintrntusr	Alleen lezen	
Eigenaar	administrator	
Online status in collect	Lezen	Webuitsluiting reden in collect

Recordtoegang		
Gebruiker / groep	Rechten	
adlibintrntusr	Alleen lezen	
Eigenaar	administrator	
Online status in collect	Lezen	Webuitsluiting reden in collect

Te zien is hier ook dat het betreffende scherm met Adlib Designer is aangepast om ook de online status van het record in de collect database te tonen. De schermen (.fmt bestanden) kunnen op verzoek opgestuurd worden, alleen je zult zelf in Designer de bijbehorende velden moeten aanmaken. Bij uitsluiting kan in collect ook een reden worden gegeven, meer daarover volgt hieronder.

Standaardwaarden voor de velden UR en RQ instellen in Designer

Het is handig om in Designer bij de velden UR en RQ in de databases collect en media in te stellen dat deze standaard worden gevuld met de waarden 'internet-gebruikersnaam' en rechten 'Geen'. Hierdoor staat elk nieuw record dat aangemaakt wordt automatisch offline.

Ga naar het veld UR in Designer en klik op het tabblad Standaardwaarden. Zet het type op Waarde en vul in tekst achter English en Dutch de internet gebruikersnaam in.

Veldeigenschappen			Standaardwaarden	Meertalige velden	Teksten voor d
Standaardwaarden					
Type	Waarde				
Tekst					
	Taal	Tekst			
▶	English	adlibintrntusr			
	Dutch	adlibintrntusr			
	French				
	German				
	Arabic				
	Italian				
	Greek				
	Portuguese				

Hetzelfde geldt voor het veld RQ, met als standaardwaarde 'None' en 'Geen'.

Veldeigenschappen		Opsomwaarden		Standaardwaarden		Meertalige velden	
Standaardwaarden							
Type	Waarde						
Tekst							
	Taal	Tekst					
►	English	None					
	Dutch	Geen					
	French						
	German						
	Arabic						
	Italian						
	Greek						
	Portuguese						

Doe dit voor de velden UR en RQ in database collect en de velden UR en RQ is database media.

Reden voor uitsluiting van records opgeven

Joop Vanderheiden, specialist informatie- en bedrijfssystemen bij de Rijksdienst voor het Cultureel Erfgoed heeft een mooi scherm gemaakt om heel gemakkelijk aan te geven wat de reden van webuitsluiting van een record is. Het betreft het scherm Beheergegevens, waar dus ook de internet-gebruiker en online rechten worden aangegeven (scherm objman.fmt). Dit scherm hebben wij van hem overgenomen en naar onze wensen aangepast.

In dit scherm bevindt zich een kader Webuitsluiting met een veld voor **Reden van uitsluiting**. Dit is een uitklapmenu.

Webuitsluiting	
Reden van uitsluiting	
Andere reden	auteursrechten
	portretrechten / privacy
Invoer	
Naam	registratiefoto
Conv. Lotus Domino	anders (hieronder invullen)

Het veld **Andere reden** is een vrij veld.

Het veld Reden van uitsluiting is in Designer een opsomveld waar elke gewenste waarde kan worden ingevuld:

Veldeigenschappen		Opsomwaarden		Standaardwaarden		Meertalige velden		Teksten voor de gebruikersinterface		Z39.50 Instellingen		Toegangsrechten	
Soort opsomveld													
Bron van opsomveld		Vaste lijst											
Sorteer de opsomwaarden		Ongesorteerd											
dynamicEnumerationListLab													
Opsomwaarden													
	Waarde	Taalwaarde (Dutch)											
►	0	auteursrechten											
	1	portretrechten / privacy											
	2	registratiefoto											
	3	anders (hieronder invullen)											
*													

Dit is een manier om bijvoorbeeld auteursrechten en portretrechten aan te geven.

Bijlage 1: Excluding anonymous internet users from specific records

Deze bijlage is ontleend aan de [documentatie van de Adlib API](#).



Adlib Information Systems

Copyright © 2011 Adlib Information Systems B.V. ® All rights reserved. Adlib® is a product of Adlib Information Systems B.V. ®

The information in this document is subject to change without notice and should not be construed as a commitment by Adlib Information Systems. Adlib assumes no responsibility for any errors that may appear in this document. The software described in this document is furnished under a licence and may be used or copied only in accordance with the terms of such a licence. While making every effort to ensure the accuracy of this document, products are continually being improved.

As a result of continuous improvements, later versions of the products may vary from those described here. Under no circumstances may this document be regarded as a part of any contractual obligation to supply software, or as a definitive product description.

Inhoud

1.1 Setup in IIS 7 (Windows 2008)	2
1.2 Setup in IIS 6 (Windows 2003)	4
1.3 Further setup in MS SQL Server Management Studio	6
1.4 Excluding records in the Adlib application	7

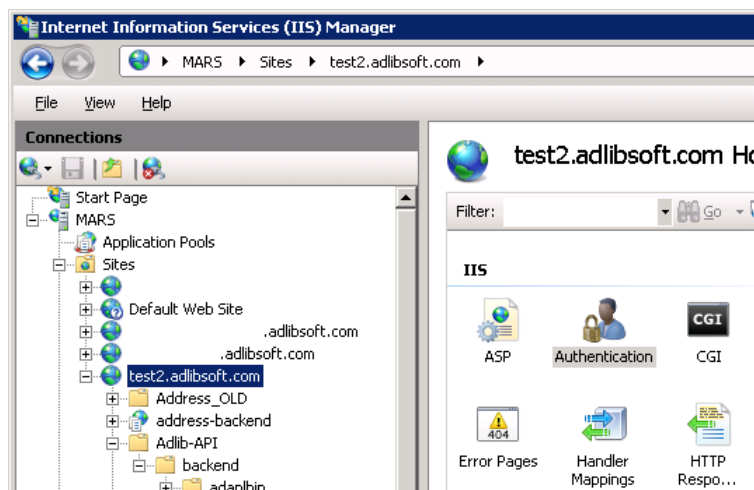
Excluding anonymous internet users from specific records

When you have an Adlib Internet Server web application, you may not just want to limit general database access for anonymous internet users to read-only access, but you may also want to exclude certain records completely from showing up in a search result on the website.

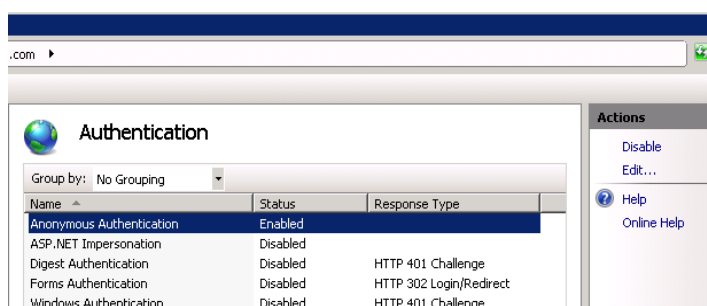
Setup in IIS 7 (Windows 2008)

(See the next chapter for setup in IIS 6.) In general, the best way to achieve this in IIS 7 is as follows:

1. Create a new Active Directory account which you will be using as the account under which any anonymous internet user will access your website after this setup, if that doesn't exist already. This account must have read access to the share(s) and files on the server(s) on which the web application, the .inf's and SQL Server database are located. Choose a handy name for the new account, like "anonymous" or "internetuser".
(See: <http://support.microsoft.com/kb/322684> for some information about how to create an Active Directory user account.)
2. From the *Administrative tools*, open the IIS Manager and in it select your website. Double-click the *Authentication* icon on the right.



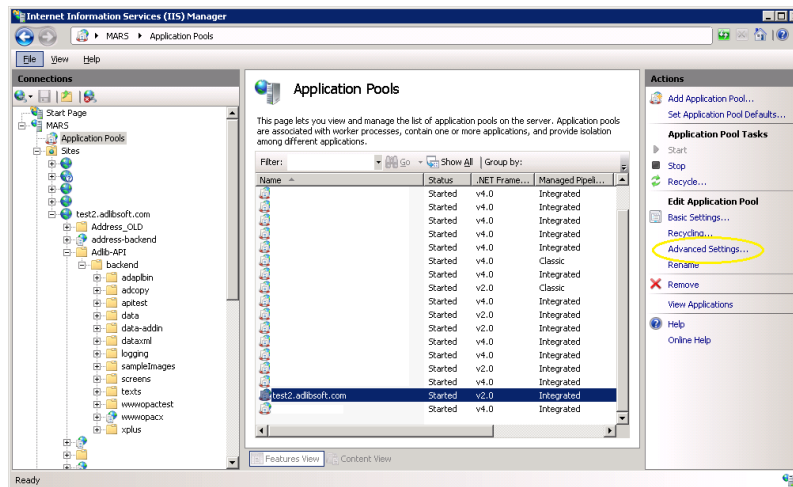
3. Select *Anonymous Authentication* and click *Edit...* under *Actions*.



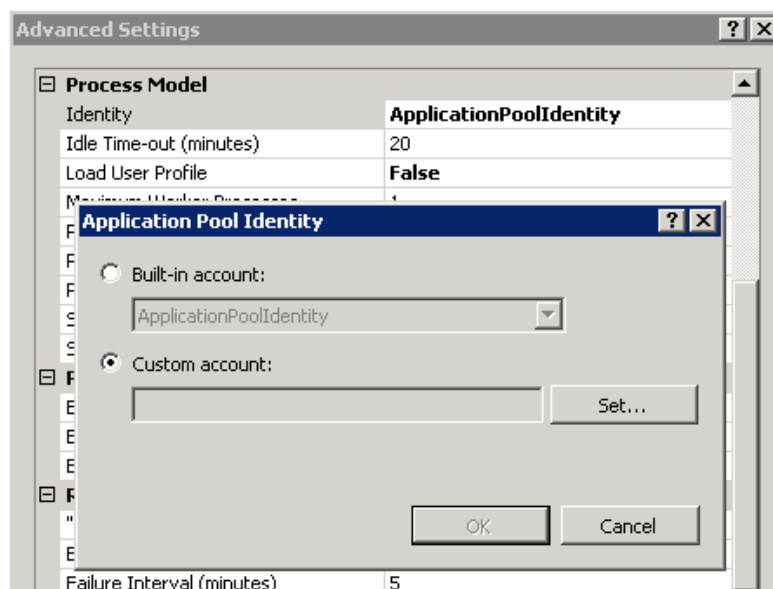
4. Mark the *Application pool identity* option, and click *OK*.



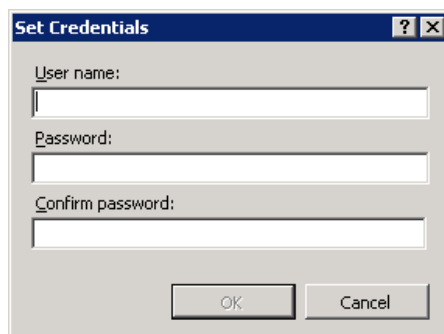
- In the left window pane, select *Application pools*, then select the application pool for your website and click the *Advanced settings...* option in the right window pane.



- In the *Advanced Settings* window, select *Identity* and click the ... button which appears behind the identity name on the right. The *Application Pool Identity* window opens. Mark the *Custom account* option. Click the *Set...* button



- In *User name*, enter the account name you created earlier, preceded by your domain and a backslash (e.g. ADLIB\anonymous), and in *Password* and *Confirm password* enter the password you assigned to it. Click *OK*.

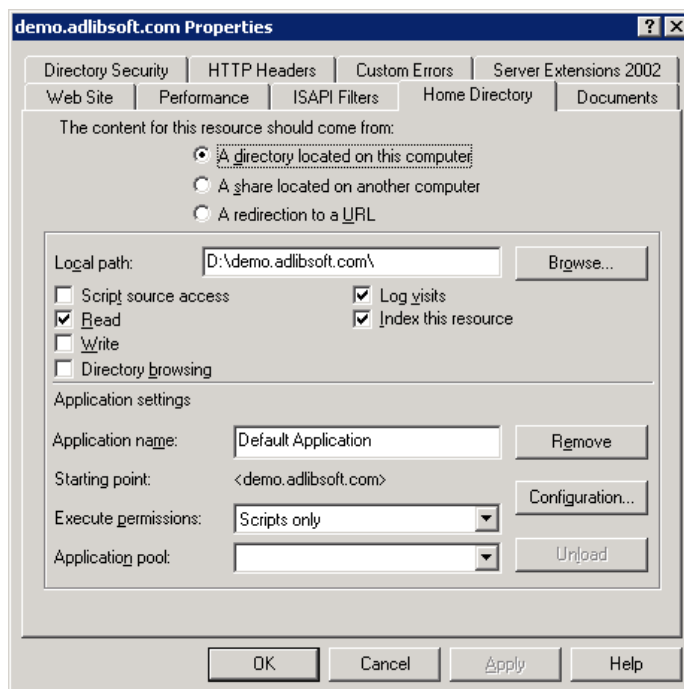


- Click *OK* in the three open windows and close IIS.

Setup in IIS 6 (Windows 2003)

In general, the best way to achieve this in IIS 6 is as follows:

1. Create a new Active Directory account which you will be using as the account under which any anonymous internet user will access your website after this setup, if that doesn't exist already. This account must have read access to the share(s) and files on the server(s) on which the web application, the .inf's and SQL Server database are located. Choose a handy name for the new account, like "anonymous" or "internetuser".
(See: <http://support.microsoft.com/kb/322684> for some information about how to create an Active Directory user account.)
2. From the *Administrative tools*, start the IIS Manager and open the *Websites* node. Right-click your website and select *Properties* in the pop-up menu. Click the *Home Directory* tab in the window that opens, and check that the proper *Application pool* has been set under which *wwwopac.ashx* must be running. Later we'll adjust this application pool for anonymous access.



3. Click the *Directory Security* tab. In the *User name* field, enter the name of the new Active Directory account you just created, preceded by your domain and a backslash. Also enter the associated password in the *Password* field. This account will be used to access your website. Click *OK* in both opened windows to close them.

Authentication Methods [X]

☒ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: MYDOMAIN\anonymous Browse...

Password:

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☒ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

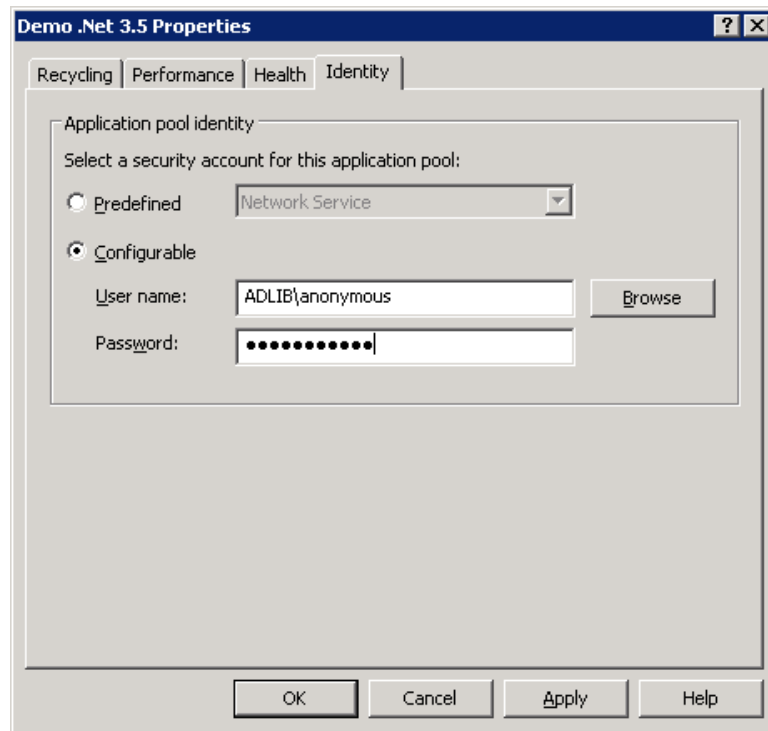
☐ .NET Passport authentication

Default domain: Select...

Realm: Select...

OK Cancel Help

4. In the IIS Manager, open the *Application pools* node, right-click the application pool in which your website runs and choose *Properties*. Select the *Identity* tab in the window that opens and mark the *Configurable* option. Then set the *User name* and *Password* to your new Active Directory account name (preceded by your domain and a backslash) and password. Click *OK* to close this window.

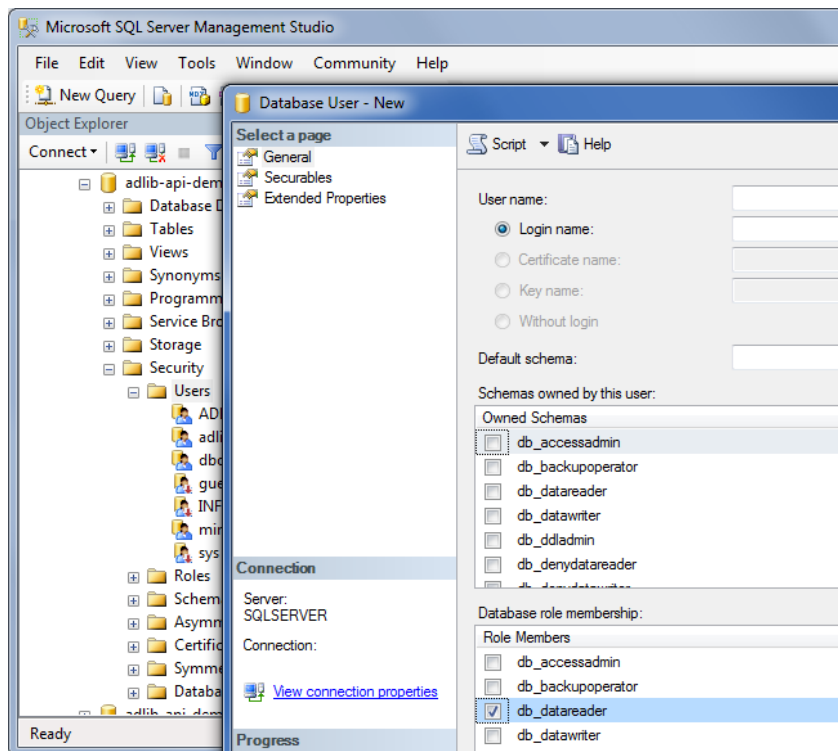


5. Close IIS.

Further setup in MS SQL Server Management Studio

If you use Windows authentication to handle access to the SQL Server database, you'll have to set the new account name as a user in that database, with read-only rights.

So, open Microsoft SQL Server Management Studio, select the relevant database and under *Security*, right-click the *Users* node and choose *New user*. In the *Database user – New* window, enter the account name you created earlier in both the *User name* and the *Login name* entry field, preceded by the proper domain and a backslash. In the *Database role membership* list at the bottom of the window then mark the *db_datareader* role, before clicking *OK*.



If you are using SQL Server authentication instead of Windows authentication, then the new Active Directory user account already has read-only access to the SQL Server database. So you don't need to add it as a user in the database.

Excluding records in the Adlib application

Assuming you have already set up the record access rights functionality in your Adlib (adlwin.exe) application, you can now use the anonymous internet user account name you created (without domain this time) to exclude records. The user must enter this name in Adlib records and possibly (depending on the setup) select the access rights *None*. If a record has *None* access rights it will now be excluded from wwwopac search results entirely. Note that only the record owner (who created the record) can enter or edit these access rights.

Entry Despatch					Loss/damage	Accompanying texts	Notes	Management details
Record access								
User / group		Rights						
anonymous		None						
Owner								
Input								
Name	Date	Time	Dataset	Notes				
Edit								
Name	Date	Time	Dataset	Notes				

In the Designer Help, see the topic *General Topics > User authentication and access rights > Use the authorisation functionality* for information about how to set up record authorisation in your application. In the example above the user name "anonymous" has been entered in the *User* field and in the *Rights* field *None* has been selected to specify that this user account has no access to this record. It is very well possible though that you or the application manager decided to implement record access rights slightly differently, in which case the user only needs to enter the anonymous internet user

account name in the *User* field to automatically exclude the anonymous users from access to this record: in that case there is no *Rights* drop-down list to select other access rights from.

Bijlage 2 – database-instellingen voor record-uitsluiting

In collect, document en media zijn twee velden nodig: recordbeveiliging.gebruiker en recordtoegang.rechten. De velddefinities ziet u hieronder. Beide velden moeten lid zijn van de veld groep ACCESS_RIGHTS. Omwille van herkenbaarheid is het aan te bevelen om de namen van de velden hetzelfde te houden als in dit voorbeeld (uit Adlib Modelapplicatie 4.5).

Dit is de velddefinitie van recordbeveiliging.gebruiker:

The screenshot shows the 'Field properties' dialog box for a field named 'recordbeveiliging.gebruiker'. The 'Identification' tab is active, showing the field tag 'UR'. The 'Field type' section has 'Normal field' selected. The 'Field names' section shows a table of translations for the field name across different languages. The 'General' section shows various settings for the field, including a maximum length of 50, a data type of 'Text', and a group membership of 'ACCESS_RIGHTS'.

Language	Text
English	record_access.user
Dutch	recordbeveiliging.gebruiker
French	accès_enregistrement.usager
German	Datensatz_Zugang.Benutzer
Arabic	
Italian	accesso_record.utente
Greek	
Portuguese	

General

Maximum length: 50

Repeatable: ☒

Data type: Text

Presentation format:

Member of group: ACCESS_RIGHTS

Exchangeable: ☒

Occurrence sort order: Ascending

Multi lingual: ☐

Do not show in lists: ☐

Dit is de velddefinitie van recordtoegang.rechten:

Field properties Enumeration values Default values Multi language fields User

Identification

Field tag

Field type

☐ Normal field ☐ Automatic numbering field

☐ Linked field

☒ Enumerative field

Field names

Text

	Language	Text
▶	English	record_access.rights
	Dutch	recordtoegang.rechten
	French	accès_enregistrement.droits
	German	Datensatz_Zugang.Rechte
	Arabic	
	Italian	accesso_record.diritti
	Greek	
	Portuguese	

General

Maximum length

Repeatable ☒

Data type

Presentation format

Member of group

Exchangeable ☒

Occurrence sort order

Multi lingual ☐

Do not show in lists ☐

Recordtoegang.rechten is een enumeratief veld. Dit zijn de enumeratiewaardes (in het Nederlands):

Field properties Enumeration values Default values Multi lang

Enumeration type

Enumeration source Fixed list

Sort enumeration values Unsorted

dynamicEnumerationListLab

Enumeration values

	Value	Language value (Dutch)
▶	0	Geen
	1	Lezen
	2	Lezen en schrijven
	3	Volledig
*		

En dit is de default-waarde:

Field properties Enumeration values Default values

Default values

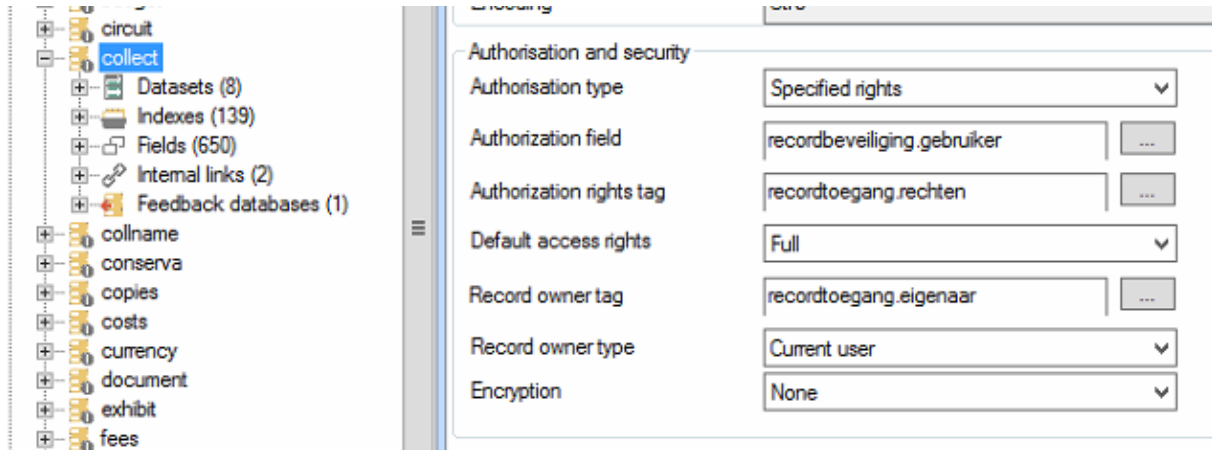
Type Value

Text

	Language	Text
▶	English	None
	Dutch	Geen
	French	
	German	
	Arabic	
	Italian	
	Greek	
	Portuguese	

In de Database Properties zijn de volgende instellingen nodig:

- Authorisation type moet zijn Specified Rights
- Authorisation field moet zijn recordbeveiliging.gebruiker
- Authorisation rights tag moet zijn recordtoegang.rechten



Record owner tag en record owner type spelen geen rol bij record-uitsluiting.

Colofon

Het hoofdstuk *Record-uitsluiting in het Zuiderzeemuseum* is geschreven door Shannon van Muijden,
Contact: Shannon.van.Muijden@Zuiderzeemuseum.nl.

Bijlage 2 is ontleend aan de documentatie van de Adlib API, gepubliceerd door Axiell ALM.

Overige tekst en redactie door Rolf Blijleven voor de Adlib Gebruikersgroep.

Contact: techsupport@AdlibUG.nl