Active Directory Integration in Sitecore Intranet Portal

Author: Sitecore A/S
Date: Thursday, 27 March 2008
Release: Revision 1.0
Language: English

Sitecore is a trademark of Sitecore A/S. All other brand and product names are the property of their respective holders.

The contents of this document are the property of Sitecore A/S. Copyright © 2001-2007 Sitecore A/S. All rights reserved.
## Contents:

1. **Introduction**  
   Replication (Mixed Mode) vs. Live Validation  
   Overview of the Sample Code  
   3  
2. **Using the Sample Code**  
   Setting the Canteen When Importing Users  
   Change the Extranet Domain Assembly  
   Web.config Settings  
   4  
3. **Running the Replication Task**  
   Prepare security domain for importing AD users  
   Running the Replication Task Manually  
   Scheduling the Replication Task  
   6  
4. **Setup single sign-on for AD users**  
   7  
5. **Troubleshooting**  
   8  
6. **Hardcoded Settings**  
   8  
7. **Download Sample Code**  
   9
1. Introduction

This article focuses on integrating Active Directory user information into Sitecore Intranet Portal. Such integration requires a bit of work and maybe also some customization.

In the present article we provide you with the two different options for AD integration:

1. Use the standard LDAP module of Sitecore CMS (http://sdn5.sitecore.net/Products/LDAP.aspx)
2. Use the sample AD integration code that is provided with the Sitecore Intranet Portal (which is described in this document).

For most customers, we recommend using the sample AD integration code that is provided with the Sitecore Intranet Portal.

Usage of the sample code has several advantages:

- Built-in phonebook integration.
  The standard phonebook in the Intranet Portal uses the information stored under “/sitecore/content/intranet/home/userinfo”. Replicating the AD information to this location is implemented as part of the sample code.

- Easy support for value assignment to various UserInfo fields as a part of the replication.
  As an example, the sample code assigns a canteen to a user based on the user’s Active Directory groups.

- Increased flexibility.
  The code could for example be extended to query multiple Active Directory servers.

- Full control.
  You can make any changes or additions to the code to make it work as desired for a specific customer. For example, you can specify the user’s “Refers to” UserInfo field based on AD groups, if applicable.

Replication (Mixed Mode) vs. Live Validation

No matter if you use the LDAP module or use the provided code, we suggest that you use “Mixed Mode” validation, where the AD users are replicated to Sitecore’s extranet database while still validating the user’s password against AD.

The primary reason to use replication (and to use the sample code instead of the LDAP module) is that the Intranet Portal Phonebook expects the phonebook information to be stored as UserInfo items below “/sitecore/content/intranet/home/userinfo”.

Overview of the Sample Code

The sample code consists of two parts:

1. The code which imports users from AD into Sitecore’s extranet database (and sets properties on the UserInfo object)

2. The code which validates a user against AD (this is necessary since we cannot extract the password from AD as a part of the replicated data).

The sample code consists of the following classes to import users:

- LDAPImportTask
- UserAdministration
- LDAPUtil
- ADUser

The following class validates a user against AD:

- CustomDomain

The following web form is used to manually run an AD replication task:

- Ldap.aspx with codebehind

2. Using the Sample Code

The sample code is an example of a complete “Mixed Mode” AD integration which implements the replication of users to Sitecore Intranet Portal and live validation of the user credentials against the AD. This section describes the settings that are used by the sample code.

Typically you will want to modify the code to set one or more UserInfo fields when doing the import. For an example of this, please see “Setting the Canteen When Importing Users” later in this document.

Most of the settings for the sample code are stored in the web.config file (see the following section). There are, however, also a few hard-coded settings (described later in this document).

Setting the Canteen When Importing Users

The sample code shows how to set the user’s preferred canteen based on AD groups.

You would typically want to customize this part of code since the path to the canteen items in Sitecore is currently hard-coded in the sample code.

This functionality is implemented by the SetCanteenOnUser method in the ADUser class.
Change the Extranet Domain Assembly

In order to validate the users’ credentials against the Active Directory server, the following line in web.config file must be changed to use the custom LDAP domain:

```xml
<domain id="extranet" singleInstance="true" type="Intranet.Samples.LDAP.CustomDomain, Intranet.Samples.LDAP"/>
```

**Web.config Settings**

The following settings should be entered in web.config file to use the Active Directory integration using the sample code:

```xml
<setting name="ActiveDirectoryServers" value="alfa|bravo" />
<setting name="ActiveDirectoryQuery" value="/OU=SampleOrgUnit,DC=example,DC=com" />
<setting name="ActiveDirectoryUser" value="ldapread" />
<setting name="ActiveDirectoryPassword" value="123456" />
<setting name="ActiveDirectoryFilter" value="(objectClass=person)(objectCategory=user)" />
```

The pipe-delimited list of AD-servers to lookup users in.
System starts querying the first server; if that one fails, next server in list will queried. If no server in list is reachable, an error is logged.

The query for lookup in Active Directory to import intranet users

Readonly account to use with Active Directory

Readonly account password to use with Active Directory

Filter for Active Directory query

Pipe delimited list of properties to load from the Active Directory
cn, samaccountname, distinguishedname, displayname is hardcoded
<setting name="ActiveDirectoryPropertiesToLoad" value="mail|mobile|telephone|number|streetaddress|postalcode|l|co" />

<!-- AD Fieldmapping
Pipe delimited list of fields maps to use when importing users
<AD field>,<sc field>|...
 -->
<setting name="ActiveDirectoryFieldMap" value="displayname,name|mail,email|mobile,cell|telephone|number,phone" />

<!-- AD Logfile folder
Indicates the relative path to the logfile folder
 -->
<setting name="ActiveDirectoryLogFolder" value="\dataFolder\AD logfiles" />

3. Running the Replication Task

Prepare security domain for importing AD users

Add items to the extranet domain:

- Create the following folders in the "extranet" domain (using the User Manager)
  - /Roles/AD roles
  - /Users/AD users
- Also create a role called "AD user" in the "AD roles" folder

Running the Replication Task Manually

You can run the AD replication task manually. This is very useful when configuring and testing the module.

Start the AD replication by navigating to the following URL:
/forms/ldap.aspx

For instance, if you are using “intranet” as you server host name, you would start the replication task by entering the following URL:
http://intranet/forms/ldap.aspx

Source code for the ldap.aspx is provided.

Scheduling the Replication Task

When the replication works as desired, set up a scheduled task to replicate AD users one or more times a day, depending on your requirements. This is done by creating a scheduled task in Sitecore that runs LDAPImportTaks.ImportFromActiveDirectory.
The simplest way to set this up is to add a line in the `<scheduling>` section of the web.config file. Alternatively, you can add the scheduled task by creating a Task Command item and a Task Schedule item under the `/system/Tasks` node in the “master” database.

Please refer to the following article for detailed information on running scheduled tasks in Sitecore:

http://sdn5.sitecore.net/SDN5/FAQ/Administration/Scheduled%20tasks.aspx

4. Setup single sign-on for AD users

1. In the web.config file, change the “loginPage” attribute for the site “intranet” to “/forms/DirectLogin.aspx”
2. Remove "Anonymous access" and enable "Integrated Windows Authentication" for /forms/DirectLogin.aspx
3. Make sure that the "extranet" domain is using the Intranet.Samples.LDAP.CustomDomain class (specified in the web.config file)

4. Check that necessary items exist in the “extranet” domain
   4.1. Folders:
       ▪ /Roles/AD roles
       ▪ /Users/AD users
   4.2. Role "AD user" in the "AD roles" folder

5. Troubleshooting

In critical situations, the sample code will throw an exception with a description of the error. This should help you if you run into problems when installing and configuring the module.

You can also debug using the manual replication page (ldap.aspx), modifying it to introduce logging to the logwriter near expected points of failure.

You should also look for error information in the Sitecore CMS log file.

Finally, the LDAPImportTask will create separate log files related to AD replication. The log files are placed in the folder specified by the “ActiveDirectoryLogfolder” setting.

6. Hardcoded Settings

The sample code contains a couple of hard-coded settings that you might need to change – depending on the requirements for the AD integration.

Below is the list of the methods (and code lines) that contain hard-coded settings.

- public ADUser(string sName, string[] groups)
  - Domain domain = Factory.GetDomain("extranet");

- private void CreateUser(string name, Domain domain, string[] groups)
  - Item users = db.Items["/sitecore/Users/AD users"];  
  - Item roles = db.Items["/sitecore/roles/AD roles"];  
  - RoleItem aduserRole = domain.GetRole("AD user");
    - If this role exists in the extranet domain, it is automatically added to the replicated users
7. Download Sample Code

Follow the link below to download the sample code for this article: