

## 1.0 Denali Administration and Security



Immediately upon entering the site address into their browser, Denali users will be both welcomed and presented with **one** of the three Log-in entry screens shown below:



Username:   
Password:

Denali Authentication



Username:

Windows Authentication



**Log In**  
Active Directory Login  
Username:   
Password:

Active Directory Authentication

The particular screen displayed will depend upon whether Denali is configured to use Denali's internal Authentication (default), Windows Authentication or Active Directory Authentication. Authentication is basically the method used to determine "who" is attempting to access the Denali site. A valid Login Authentication is required by one of these methods in order to gain access to any page within the Denali site\*. We'll cover the details of Denali's Authentication methods in Section 1.7.

\* Denali also provides a "No-login" option which allows users to enter the site using a shared Guest account. This will be discussed in the Authentication section below.


**Very Important:** As initially configured, there is only one username and password for Denali. The initial username is "**admin**", and the password is also "**admin**". This initial username and password combination has been "seeded" into the Member's Directory module as identity **Jim H. Smith**. This name has been placed in the Directory with the username "**admin**" and password "**admin**". The Member's Directory module is used to store the names of Denali members along with their usernames, passwords, security levels and profiles.

You will now be able to add as many additional Denali members as you need. A **Super Administrator** security rating is required to add new users and to set individual security levels in the Member's Directory. The **Jim H. Smith** identity has been given this highest security level of **Super Administrator**. The Jim Smith identity should eventually be replaced in the Member's Directory with the name of at least one **Super Administrator** from your organization. This will be described below. For now, however, **do not delete the Jim H. Smith identity** until at least one new **Super Administrator** has been added to the Directory. This should become a bit clearer after reading the sections which follow.

### 1.1 How Denali Security Works

The Denali application is made up of approximately 600 Active Sever Pages (.aspx) which represent the majority of the Denali code. When a user logs into Denali, their username and password are compared to values already in the Member's Directory (database). If the Denali administrator has included the username and password in the Directory, the user is authenticated and assigned a session variable value consistent with their security authorization levels. This session variable value remains associated

with the user as they move about Denali. When a user selects an (.aspx) page in Denali, that page will check their security level and only permit entry if appropriate. This prevents a user from simply typing in an Active Server Page URL other than the login page and gaining access “thru-the-side-door”.

 **Document Security:** The normal Denali security system (username and password) covers only Active Server Pages (.aspx), and the functions they control – like database access. Document folders and files (Word, PowerPoint, Excel, Acrobat, etc.) within the Denali site are not covered by this Denali login security – but instead are covered by a combination of Denali’s “forced-downloading” option, and the security features of the IIS webserver and the Windows Operating System itself. Without the proper security settings in IIS and Windows, document files can be vulnerable to unauthorized access by someone typing in the exact URL of a specific document into their browser’s address field. See Section 4.26 for details on document security within Denali.

DCASoft offers no assurances that data placed in the Denali database or documents in storage folders are secure.

## **1.2 Role Based Security Profiles**

Denali’s ***Security Model*** allows the system administrator to assign usernames and passwords for 6 levels of pre-defined Security.

- Super Administrator
- Administrator
- Advanced User
- Basic User
- Associate
- Guest

## An Overview of the Pre-defined Security Profiles:

#	FoxSuite Module	Guest	Associate	Basic User	Advanced User	Administrator	Super
1	Members	No Access	Browse	Browse	Browse	Browse	Super Admin
2	Contacts	No Access	Browse	Author	Author	Author	Author
3	Businesses	No Access	Browse	Author	Author	Author	Author
4	Wiki-Board	No Access	Browse	Browse	Author	Author	Author
5	To-Do List	No Access	Author	Author	Author	Author	Author
6	Link Manager	No Access	Browse	Browse	Author	Author	Author
7	Resource Management	No Access	Browse	Author	Author	Author	Author
8	News	Browse	Browse	Browse	Browse	Author	Author
9	Forums,Chat,Cork	No Access	Browse	Browse	Author	Author	Author
10	Main Calendar	Browse	Browse	Browse	Browse	Author	Author
11	Org Calendars	No Access	Browse	Browse	Browse	Author	Author
12	Projects	No Access	Browse	Browse	Author	Author	Author
13	Content Management	No Access	Browse	Browse	Author	Author	Author
14	Photo Galleries	Browse	Browse	Author	Author	Author	Author
15	Timesheets	No Access	Submit/Edit	Submit/Edit	Submit/Edit	Full Access	Full Access
16	Email	No Access	No Access	Full Access	Full Access	Full Access	Full Access
17	Messaging	No Access	Full Access	Full Access	Full Access	Full Access	Full Access
18	Reminders	No Access	Full Access	Full Access	Full Access	Full Access	Full Access
19	Future						
20	Future						
21	Individual Calendar	No Access	Full Access	Full Access	Full Access	Full Access	Full Access
22	Business Charts	No Access	No Access	Full Access	Full Access	Full Access	Full Access
23	Personal Folders	No Access	Full Access	Full Access	Full Access	Full Access	Full Access
24	eMeeting Rooms	No Access	Full Access	Full Access	Full Access	Full Access	Full Access
25	Data Mmgt. and Forms	No Access	No Access	No Access	No Access	Full Access	Full Access
26	Docs Directory	No Access	Browse	View/Edit Files	Full Access	Full Access	Full Access
27	Expense Reports	No Access	Submit	Submit	Submit	Full Access	Full Access
28	Task Management	Browse	Edit Tasks	Edit Tasks	Full Access	Full Access	Full Access
29	Training Scheduler	Browse	Browse	Reg & Add	Reg & Add	Full Access	Full Access
30	Help Desk	No Access	Submit Ticket	Submit Ticket	Help Response	Full Access	Full Access
31	General Access	Browse	Browse	Browse	Advanced	Admin	Full Access
32	Organizations	Browse	Browse	Advanced	Advanced	Admin	Full Access
33	Forums	No Access	Browse	Advanced	Advanced	Admin	Full Access
34	Dashboards	No Access	Browse	Browse	Browse	Full Access	Full Access
35	Blogs	No Access	Browse	Advanced	Advanced	Full Access	Full Access
36	Future						

**Super Administrators** are able to create new members, and also to create, name, and save additional security profiles as needed and appropriate for their organizations. A school, for instance, might need to create security profiles for Teachers, Students, Parents, etc. To create a new profile - the **Super Administrator** would use the tools provided on the Denali Admin Panel. Using these tools, the **Super Administrator** would be allowed to create a **Security Profile Name** for use as a “template” for other members needing identical security assignments. The administrator might, for instance, create a security profile for the first student in a school, and then name that profile “Student”. Each subsequent student would require only a selection of the “Student” security profile from a pull-down box – saving the work of individual module assignments.

By default, all usernames and passwords are assigned by the Denali Super Administrator - and cannot be changed by members. Administrators can, however, configure Denali to allow members to change their own passwords, their own usernames, or both. This configuration is done in the Denali web.config file using any text editor as shown below:

```
<add key="pwoption" value="0"/>
```



The default value of “0” does not allow members to change their username or password. A value of “1” allows members to change their password, and a value of “2” allows members to change both their username and password. Username and Password changes, if allowed, are made by members on their “My Profile” page.

Usernames and passwords must be unique, and contain between 4 and 20 characters. Usernames and passwords can be any combination of letters and numbers - but are case sensitive. No special characters (other than letters or numbers) are allowed in either a username or password.

You will see later that usernames, in particular, play a key role in providing individual instances of certain applications like “to-do” lists, calendars, email, etc. Usernames identify the user for the Denali database so that their e-mail, calendars, action items, etc. can be displayed and updated as unique applications.

### **1.3 Adding a new Denali Member**

A new Denali member is created in the Member’s Directory by clicking the **Members** menu-item, and then selecting the **Add New Member** button. We’ll be discussing the Member’s Directory in more detail in Section 4.0 of this manual – but for now want to show the minimum security fields that would be completed in the Member Directory when a new user is created.

<b>Security Profile:</b>			
User Name *	<input type="text"/>	Password *	<input type="text"/>
		Security	- Make Selection -  

### **1.4 Editing Member Profiles**

Existing member profiles can be edited by **Super Administrators** in the Member Directory.


**Important Reminder:** It was mentioned earlier that the single identity in the starting Member Directory (Jim H. Smith) has **admin** as a Username, and **admin** as a Password. While this identity should eventually be replaced, **do not** delete Jim Smith without first creating a **new Super Administrator** with a new username and new password. Contact DCASoft at [www.dcasoft.com](http://www.dcasoft.com) if you have any questions about the Denali Security model.

### **1.5 Creating New Custom Security Profiles**


As was mentioned above, Denali comes with 6 pre-defined Security Profiles:

- Super Administrator
- Administrator
- Advanced User
- Basic User
- Associate
- Guest

**Super Administrators** can create, name, and save additional Security Profiles by going to the **Admin Panel** and selecting **Add/Edit Profile**. The screen shown below will be displayed showing the existing security profiles which can be edited. There is also an **Add New Profile** button. The 6 default (original) security profiles cannot be deleted.

 Return

## Named Security Profiles



These are named Security Profiles. Think of them as Templates that can be used when creating new members. Using an existing Security Profile saves the administrator from having to make security selections for each module - by using a profile that has already been saved and is appropriate for the new member.  
Click on the Security Profile Name to View or Edit the Security Settings or Click the New Entry button to Create a new Profile.

Delete Checked

	Profile Name	Security Code
<input type="checkbox"/>	<a href="#">Administrator</a>	12222224244243232222223223333334
<input type="checkbox"/>	<a href="#">Advanced User</a>	122222212112431322222322313223
<input type="checkbox"/>	<a href="#">Associate</a>	11112111111111110220020320112111
<input type="checkbox"/>	<a href="#">Basic User</a>	122121212111131322222322212211
<input type="checkbox"/>	<a href="#">Guest</a>	0000000101000100000000000001101
<input type="checkbox"/>	<a href="#">Super Administrator</a>	5222222424424323222223223333335

< >

Clicking the **Add New Profile** button will bring up the screen shown below. **Super Administrators** can use this screen to Create/Name a new profile and select module-by-module permissions for this new profile. Once saved, the new named security profile will be available for application to new members in the security drop-down box on the **Add New Member** screen in the Member's Directory.

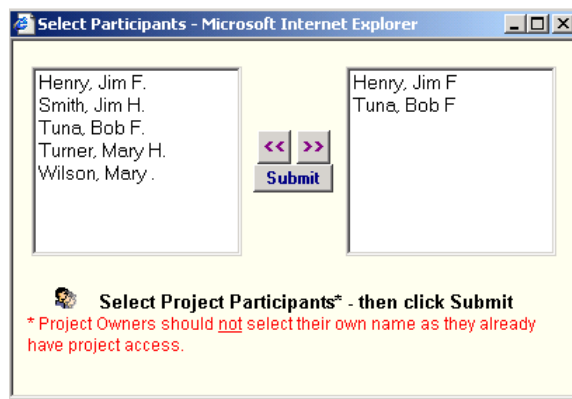
Return
Create a New Security Profile

<b>Security Profile Name: *</b>			
Module	Access Permissions		
Members Directory ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Contacts Directory ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Business Directory ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Wiki-Board ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
To-do List ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Link Manager ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Resource Management ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
News Posting ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Discussion Board ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Main Calendar ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Group Calendar ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Projects ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Content Management ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Presentation Galleries ?	<input checked="" type="radio"/> No Access	<input type="radio"/> Browse	<input type="radio"/> Author
Module	Access Permissions		
Timesheets	<input checked="" type="radio"/> No Access	<input type="radio"/> Submit / Edit	<input type="radio"/> Edit Codes / Global Rpts

Creating a new custom Security Profile results in a 36 digit code where each digit is keyed to a module number and defines the security level within that module. Administrators can be oblivious to this complexity as Denali will take care of all the details. For those so inclined, **Appendix 1** gives all the details on this subject.

### **1.6 Access Control Lists**

Certain modules within Denali utilize an additional security layer called **Access Control Lists** to fine-tune user access, and allow “shared-ownership” of resources and data. An example of this would be the Projects module. When a user with security access to the Projects module creates a new project – that person is then considered the “Project Owner”. Other users with overall security access to the Projects module are not allowed to view this new project unless granted specific access by the Project Owner. The Project Owner can create an Access Control List of individuals with permission to view this project. Access Control Lists are used throughout Denali to control access to specific resources like meeting rooms, discussion forums, team files, projects, etc. Generally the owner, or creator, of the resource controls the Access List using a popup window similar to the one shown below.



In summary – sometimes having basic security access to a module is not always enough to view all resources. Resource “owners” can limit access to specific individuals using Access Control Lists.


### **Super Administrators – Deleting Non-owned Resources**

A problem could develop when resource owners move on and leave resources behind that need to be deleted. The normal Denali **Administrator** profile does not allow the Administrator to delete resources they don’t “own” themselves. To solve this problem, Denali has a special security level named the “Super” or **Super Administrator**. A **Super Administrator** can delete the following resources even if they do not own the resources themselves:

- Teams
- Organizations
- Projects
- Discussion Boards / Corkboards
- Photo Albums
- eMeeting Rooms
- Private docs Folders

**Important Note:** Although the Super Administrator profile has wide-ranging authorization – Super Administrators cannot do everything, and do not “own” everything. Super Administrators do not for instance “co-own” resources with the resource creator. A project “creator/owner” still owns and controls their projects – the Super Administrator’s only role in these instances is to be able to delete resources if the project owner should leave the company.

### **1.7 User Authentication Methods**

As noted earlier, Denali supports three methods of user login (Authentication). The default authentication method is the internal **Denali** username/password method, but the System Administrator can alternately select either **Windows** authentication or **Active Directory** authentication by clicking the  icon at the top of the Denali homepage to access the Denali Configuration Panel.

**User Authentication** Denali  Windows  Active Directory  No Login

Each authentication method has its advantages and disadvantages, so it is important that you take the time to decide which method is appropriate for your organization and infrastructure.

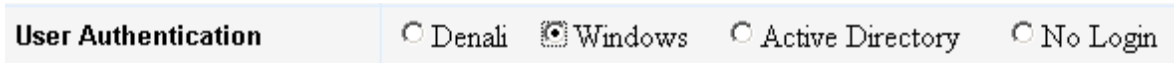
**Denali Authentication:** Denali Authentication (default) requires users to enter their Denali username and password when logging into the Denali application. It is a very straightforward method of authentication. The advantage of this method is that it is stand-alone and is completely under the control of the Denali administrator. Denali Authentication is the preferred authentication method, and perhaps the only choice when using Denali over the Internet to control otherwise “anonymous” access. The disadvantage of this method in a Windows 2000/2003 Intranet environment is that it would be a somewhat redundant system to setup and maintain, and would require users already logged-in to their Windows workstations to log-in a 2<sup>nd</sup> time.

**Windows Authentication:** Denali has the ability to authenticate users based on their current Windows workstation authentication. When using the Windows Authentication option, a user who has already logged in and been authenticated on their Windows domain, would not be required to re-enter login credentials to enter Denali. They can simply click **Login** at the login screen to enter the Denali application. There are, however, a couple important prerequisites for using Windows Authentication:

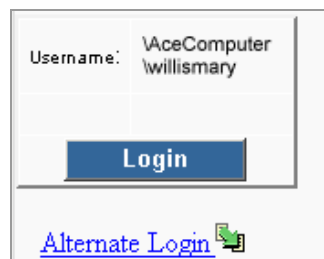
- 1) A Member Directory record **must** exist in Denali for the user with a **username** entry matching their Windows **username** (password not required).
- 2) For Windows authentication to function properly, you must de-activate **Anonymous** access, and activate **Integrated Windows Authentication** in Internet Information Services (IIS) for the Denali site.
- 3) Windows Authentication will only work with the Internet Explorer browser.

Windows Authentication would not be appropriate for an Internet environment, but offers the Single Signon (SSO) advantage for organizations with existing Windows networks (Intranets).

Let's take a look at exactly how to setup Denali for Windows Authentication. First, as mentioned above – the Administrator will want to select the Windows Authentication option in the Denali Configuration Panel.



The Admin will also need to de-activate Anonymous Access in IIS for the Denali site. Finally – the Admin will want to create or edit Member Directory profiles to be sure the Username field contains the exact Windows username the user is using to Login to their Windows workstation. Let's look at an example. User Mary Willis logs into her Windows workstation (domain name **acecomputer**) in the morning using the username **willismary**. If Denali has been set for Windows Authentication – Mary will see the screen below when she attempts to enter Denali.



Mary can simply click the Login button to enter Denali .... if her Administrator has entered a Denali Members directory record with the **username** field containing **willismary**.



The password is not relevant in this particular Member record – it is the username that is the important factor for finalizing Windows Authentication.

**Note:** In the Windows Authentication scenario above – the user was actually authenticated based on her Windows login credentials when she first logged into her Windows workstation. You may therefore wonder why users must also have a record in the Denali member's directory (?). The reason this is important is so that the Windows login be associated with a Denali security profile. This is the “authorization” part of the user management process, and the security profile defines what each user can and cannot do once inside Denali.

The **Alternate Login** link shown above defaults back the Denali Authentication screen for users without the proper Windows credentials, or when Denali may be in a mixed – mode Intranet /Internet configuration.

What we basically have is a system of both Authentication – “Who the user is”, and a system of Authorization – “What the user can do”. Authorization is controlled by the Denali security profile.

### **Active Directory Authentication:**

Denali has the ability to authenticate users based on their Active Directory usernames and passwords. When a Denali user enters their Active Directory username and password – Denali checks these credentials against the domain’s Active Directory database to verify the user exists. If a match is found, Denali allows the user to enter the application. Also, if an AD match is confirmed, but no Denali member record matching the username exists, a **Basic User** Denali member record will be created “on-the-fly” for this new user. There are, however, 2 important prerequisites for using Active Directory Authentication with Denali:

1) Active Directory Authentication must be selected in the Denali Configuration Panel.



User Authentication       Denali     Windows     Active Directory     No Login

2) For Active Directory authentication to function, the Denali web.config file must be edited using the 4 steps shown below.

**Note** – you should make a backup copy before editing the web.config file. This will allow you to return to Denali or Windows authentication later if you choose.

### **Editing the Denali web.config file for Active Directory Authentication**

1. You will first want to “un-comment” the **connectionStrings** and **authentication mode** sections by removing just the comment markers shown in red below. Removing the comment markers will allow these two sections to become an active part of the new web.config file.

```

<!-- .....
<connectionStrings>
  <add name="ADConnectionString"
connectionString="LDAP://dcasoft.AD.com/CN=Users,DC=dcasoft,DC=AD,DC=com"
  />
</connectionStrings>
.....-->

```

Remove these comment lines.

```

<!-- .....
<authentication mode="Forms">
  <forms
    name=".ADAuthCookie"
    timeout="30"
  />
</authentication>

<authorization>
  <deny users="?" />
  <allow users="*" />
</authorization>

<membership defaultProvider="MyADMembershipProvider">
  <providers>
    <add
      name="MyADMembershipProvider"
      type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web,
Version=2.0.0.0, &#xD;&#xA; Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a"

      connectionStringName="ADConnectionString"
      connectionUsername="dcasoft\Administrator"
      connectionPassword="project3B" attributeMapUsername="sAMAccountName"
      attributeMapPasswordQuestion="displayName" />
    </providers>
  </membership>
.....-->

```

Remove these comment lines

2. You must also delete the existing Authentication mode tag.

```
<authentication mode="None" />
```

3. You must edit the web.config files' Active Directory Connection String.

\* **Editing the web.config file's Connection String** – the Active Directory connection string in the web.config file must be edited so that it points to your Active Directory's user container.

```
connectionString="LDAP://dcasoft.AD.com/CN=Users,DC=dcasoft,DC=AD,DC=com"
```

The connection string shown above connects to the **Users** container within the domain named **dcasoft.AD.com**. Update the red/bold portion of the string to point to the relevant user's container within your domain.

### **LDAP Connection String syntax**

The connection string to the Active Directory user store is in the following format:

***LDAP[s]:// hostname:port/base\_dn ...***

When LDAP:// is specified, standard LDAP is used to connect to the LDAP server - normally port 389. When LDAPS:// is specified, LDAP over SSL is used to connect the LDAP server – normally port 636.

- **hostname** is the name (or IP address) of the LDAP server . For Example:  
ldap.example.com or 192.202.185.90
- **port** is the port number of the LDAP server (for example 389). If no port is specified, the standard LDAP port (389) or LDAPS port (636) is used.
- **Basedn** is the distinguished name (DN) of the entry in the directory. This DN identifies the entry that is the starting point of the search. If no base DN is specified, the search starts at the root of the directory tree.

### **Examples of LDAP Connection Strings**

**LDAP://dcasoft.AD.com/ DC=dcasoft,DC=AD,DC=com**

No port or user store is specified – so port 389 is used and the search is started at the root of the directory tree.

**LDAP://dcasoft.AD.com:389/CN=Users,DC=dcasoft,DC=AD,DC=com**

Port # 389 is specified, and the search is specified as the **Users** Directory.

**LDAP://dcasoft.AD.com/ou=sales,DC=dcasoft,DC=AD,DC=com**

No port is specified, and the search is specified as the organization unit **sales**.

4. You must edit the web.config files' Active Directory Connection Username and Password.

\* **Editing the web.config files's Connection Username and Password** – the Active Directory Administrator username and password must be edited – portions in red/bold. If not an Administrator account – then the service account that you use to connect to Active Directory must have sufficient permissions.

```
connectionUsername="dcasoft\Administrator"  
connectionPassword="project3B"
```

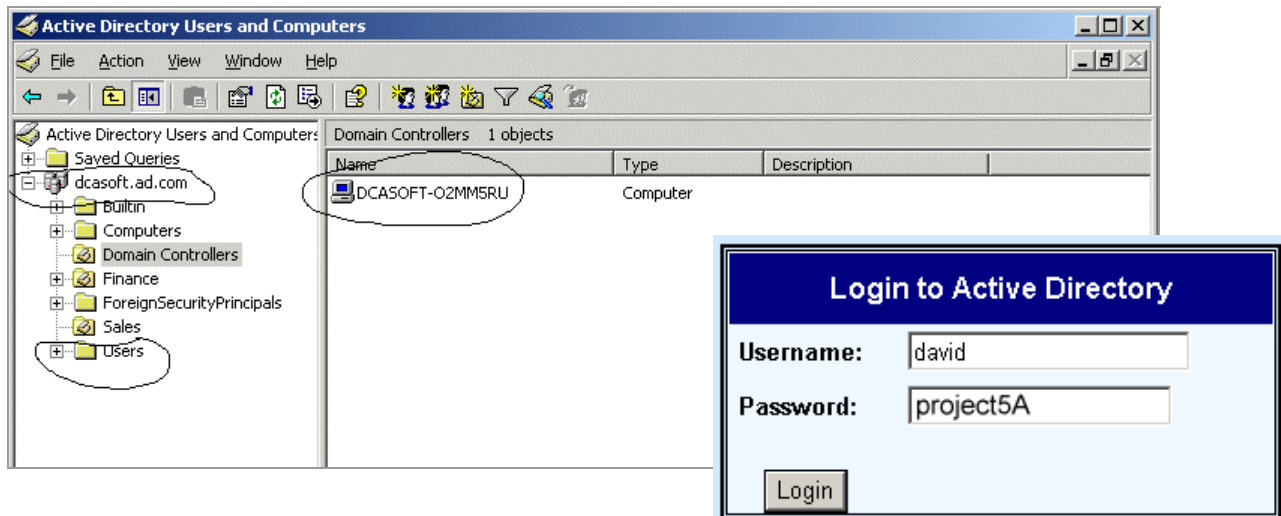
### A Specific Active Directory Example:

Domain: **dcasoft.ad.com**

Domain Controller / Server Name: **DCASOFT-O2MM5RU**

Admin Account Username: **Administrator** or **david**

Admin Account Password: **Project5A**



### Possible Connection Strings:

***LDAP://dcasoft.AD.com/CN=Users,DC=dcasoft,DC=AD,DC=com"***

***LDAP://dcasoft-o2mm5ru/CN=Users,DC=dcasoft,DC=AD,DC=com"***

You can also use an IP address.

### Possible Connection Usernames:

***connectionUsername="dcasoft\Administrator"***

**connectionUsername="david@dcasoft.ad.com"**

**Possible Connection Password:**

**connectionPassword="project5A"**

**Logging in using Active Directory**

Let's look at an example of how Active Directory Authentication would work. User Frank Reynolds wants to login to the Denali application that has been set-up to utilize Active Directory Authentication. Frank will be presented with the following Login Screen.



Frank would enter his Active Directory username **frank** and his password **project6H** and click the Login button.

**Note** – Denali has been configured to use the simple user name format (sAMAccountName) so usernames would have the format **frank** and not **frank@DomainName**.

Denali would validate these login credentials against the Active Directory database, and, if successful, Frank would be taken to a 2nd Login Confirmation screen (shown below).



On the Confirmation screen, Frank can simply click the Login button to enter Denali.

**Important Note:** In the Active Directory scenario above – the user *frank* is actually authenticated based on his Active Directory credentials. If, however, no corresponding member record with the username *frank* is found in Denali – a member record is created for Frank with the **Basic User** security profile and a randomly generated password. The Denali Administrator would need to Edit Frank’s Denali Member Directory security profile and password for future logins.

## **Active Directory Authentication - Security Issues**

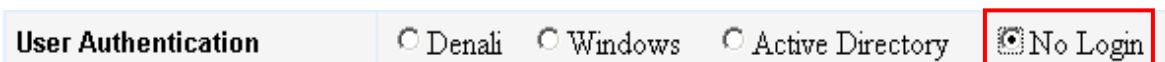
In implementing Active Directory authentication – Denali utilizes ASP.NET 2.0’s Forms Authentication methodology and the ActiveDirectoryMembershipProvider. There are, however, a couple of security considerations that deserve noting:

- 1) As shown above, the Active Directory Administrator or Service Account name and password must be supplied in plain text in the web.config file. ASP.NET never serves requests for configuration files (because they often contain sensitive information) – but the issue may still be a concern.
- 2) Because ASP.NET forms authentication uses standard HTML forms for entering credentials, the username and password are sent over the network in plain text. For this reason it is strongly recommended that you encrypt the traffic between the browser and the server using SSL.

### **1.8 Enabling a No-Login “Guest” Account**

Denali Administrators can establish a no-login “Guest” account which allows site visitors without a Member Directory profile to access certain features within Denali without logging-in. To establish the Guest account the administrator must do 2 things:

- 1) Go to the Denali Configuration Panel and click the “No Login” radio button for **User Authentication** method.



- 2) Check to be sure there is a generic Member record in the Denali Member’s Directory with both the Username and Password being “**guest**” – such a record was created by default when Denali was originally installed. You can select or edit any security profile you want for this Guest Account – just keep in mind that all guests will be sharing the same account and Security Profile.