Directory Manager
Segmented Installation

Background

Directory Manager is a Web-based utility that allows an authorized user to update other user's information in the Active Directory. The Directory Manager administrator or installer specifies which attributes can be updated and the search criteria that is available to the authorized user.

Group authorization, drop-down lists, attribute configuration, configuration data, and interface configuration data is stored in the XML files that are installed with Directory Manager and later customized by the installer. A user is authorized to use Directory Manager by creating a group in Active Directory called **Directory Update Managers** and then putting that user that needs to use Directory Manager in the **Directory Update Managers** group.

Permissions to update a user or contact object in the Active Directory is given, not to the user, but to the service or proxy account that is specified during the Directory Manager installation. The service or proxy user is usually made a member of the domain's Account Operators group but permissions can be further restricted.

By default, Directory Manager will allow the authorized user to view and update any user account anywhere in the Active Directory domain. The limit of this, of course, is that the proxy account must have the necessary permissions to update the user or contact. For example, if the service or proxy account is a member of Account Operators, then Domain Admin and "operator" users cannot be updated. This is a built-in feature of Windows.

Restricting to a Single Organizational Unit

The AppSettings.XML file in Directory Manager allows an administrator to restrict the view of users listed in Directory Manager to a single organizational unit (OU) and all the child OUs under that OU.

Let's take as an example the Active Directory organizational unit structure shown in Figure 1. Most of the users are under a single parent OU (CorporateUsers). There may be some system or service accounts under the Users container, but all of the valid users are found under CorporateUsers.

Figure 1: Example organizational unit structure

You can restrict the display listing in Directory Manager so that only users found in the OUs under CorporateUsers are displayed. (Sorry, LDAP will not let you filter out some of the OUs under that OU; all are included.)

You restrict the display listing to a single OU (or parent OU) using the AppSettings.XML file. Locate the <ouFilter…> tag in that file. This portion of the AppSettings.XML file is shown in Figure 2.

```
<!-- OUs allows user to search an entire OU. OU name should be listed like this: name="All Users" or name="A
<!-- The domain name must be the DNS domain name of the Active Directory, such as domain="acme.local" -->
<!-- If baseSearchOU is used, all searches will start from that base OU. If you want specify OU filters do nc
<!-- searchBaseOU specifies the starting point for the search listing.  Leave blank for no search base, all OUs
<!-- Specify OU name without OU=, i.e. searchBaseOU="All Users" - You cannot specify Users container. -->
<ouFilter text="Organizational Unit" enabled="yes">
  <OUs domain="colonialmovers.int" searchBaseOU="CorporateUsers">
    <OU name="" displayText="" />
    <OU name="" displayText="" />
  </OUs>
```

Figure 2: Filtering out users based on a parent OU

To activate the OU filter (also called a searchBaseOU), you must set the enabled=”yes” option in the <ouFilter…> tag. Then, in the <OUs….> tag, specify the DNS domain of your Active Directory (in the domain option) and the OU name (in the searchBaseOU option.)

Allowing Different Managers to Update Different Users

There are times when an organization has multiple OUs and needs to designate a different administrator for each OU. Let’s say that the organization show in Figure 1 requires a different administrator for the Battlestar OU and a different administrator for the Firefly OU. The design and security model for Directory Manager makes this a bit more

difficult, but it is possible. The catch is that you must run two different instances of Directory Manager however there is no additional software licensing to do this. Here is an example of the high level steps to do this for the Battlestar OU; these steps assume that you have already installed the Directory Manager:

1. Create an Active Directory security group called **Battlestar Directory Managers**.
2. Add the authorized managers for the Battlestar OU to the **Battlestar Directory Managers** group.
3. Copy the c:\inetpub\wwwroot\DirectoryManager folder to c:\inetpub\wwwroot\DM-Battlestar
4. Using IIS Manager, create a new virtual directory on the default Web site called DM-Battlestar
5. Edit the AppSettings.XML file found in c:\inetpub\wwwroot\DM-Battlestar so that this instance of Directory Manager only shows users under the \CorporateUsers\Battlestar OU and so that only members of the **Battlestar Directory Managers** group can use this instance.
6. Customize the DirectorySettings.XML file found in the c:\inetpub\wwwroot\DM-Battlestar for the users in that OU.
7. Give the URL http://servername/DM-Battlestar to the authorized users of Directory Manager

This process works for a couple of different reasons. First Directory Manager is a Web application can uses the configuration files found in the local directories under the virtual directory. Second, the AppSettings.XML file allows you to configure a filter so that only users under a specific OU will be shown.

This additional instance of Directory Manager will use the configuration files found under c:\inetpub\wwwroot\DM-Battlestar but it will use the **same** service/proxy account that was configured during the initial installation.

A couple of the above steps require some additional explanation in order to get right. The first, and simplest of these, is to add the **Battlestar Directory Managers** group to the AppSettings.XML file. Locate the <authorizedUserGroups> section of the AppSettings.XML file and add this group to that section. Note that you can only use security groups here, you cannot code individual user accounts in to this section.

```
31      <!-- In order for a user to be authorized to use Directory Manager, they must be a member of one of these groups. Or you can add your own. -->
32      <authorizedUserGroups>
33        <group>Domain Admins</group>
34        <group>Account Operators</group>
35        <group>Administrators</group>
36        <group>Battlestar Directory Managers</group>
37      </authorizedUserGroups>
```

Figure 3: Adding an additional authorized users group to the AppSettings.XML file

You must apply a filter to the AppSettings.XML file so that only the http://servername/DM-Battlestar instance of Directory Manager will only show the users from the /CorporateUsers/Battlestar OU. This step is also performed in the

AppSettings.XML file in the <ouFilter…> section. Locate this section and ensure that the DNS domain name is in the domain property and that the explicit OU name is entered in the searchBaseOU.

```
<!-- OUs allows user to search an entire OU. OU name should be listed like this: name="All Users" or name="All Users/New York" -->
<!-- The domain name must be the DNS domain name of the Active Directory, such as domain="acme.local" -->
<!-- If baseSearchOU is used, all searches will start from that base OU. If you want specify OU filters do not include the baseSearch
<!-- searchBaseOU specifies the starting point for the search listing.  Leave blank for no search base, all OUs queried. -->
<!-- Specify OU name without OU=, i.e. searchBaseOU="All Users" - You cannot specify Users container. -->
<ouFilter text="Organizational Unit" enabled="yes">
  <OUs domain="colonialmovers.int" searchBaseOU="CorporateUsers/Battlestar">
    <OU name="" displayText="" />
    <OU name="" displayText="" />
  </OUs>
```

Figure 4: Configuring an OU filter for a single OU

After configuring the AppSettings.XML file to show only a single OU of users and to restrict the use of this instance Directory Manager to just a specific set of users, the next step is to create an additional virtual directory in IIS Manager so that users can access the new URL.

In IIS Manager, open up Web Sites and Default Web Site (or which ever web site you want this instance to run on) and right click. Then choose New -> Virtual Directory. The click Next. In the Alias box (shown in Figure 5), type in the name of the virtual directory (in this case DM-Battlestar).

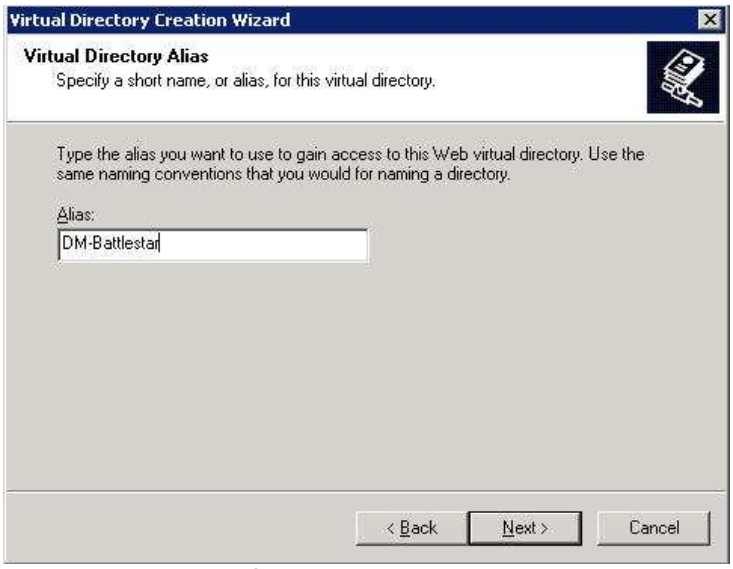

Figure 5: Configuring the virtual directory name

The virtual directory alias is used as part of the path in the URL (eg http://servername/DM-Battlestar)

Click Next to enter the path to the folder that contains the application's files. Figure 6 shows the path for this particular virtual directory; in this case c:\inetpub\wwwroot\DM-Battlestar.

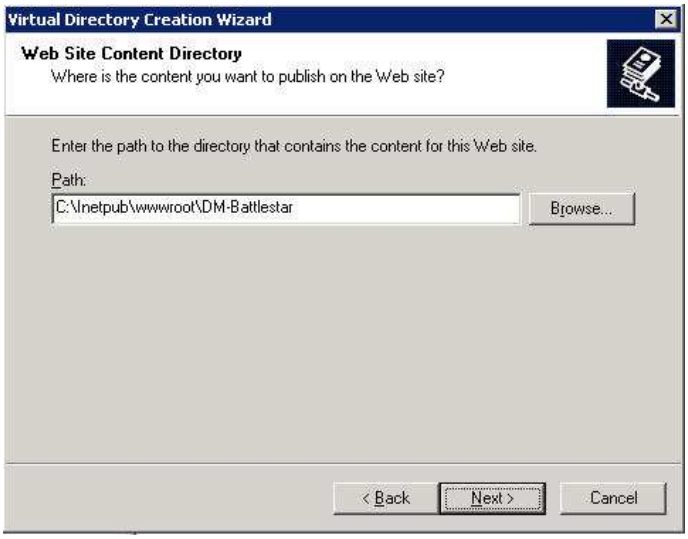

Figure 6: Specifying the path for the virtual directory's files

Click Next to move on to the Virtual Directory Access Permissions page of the wizard (shown in). Here you must make sure that the Read and the Run Scripts (such as ASP) checkboxes are checked).

Figure 7: Defining virtual directory permissions

When you have selected Run and Run Scripts, click the Next button and then click the Finish button to create the virtual directory. Now you will see a new virtual directory called DM-Battlestar under the Default Web Site. Right click on the DM-Battlestar virtual directory do the following:

1. On the Documents page, make sure that the Default.ASPX is available
2. On the ASP.NET page, select ASP.NET version 2.0.50727

The new instance of Directory Manager should now be ready to be used. You can repeat this process for additional virtual directories that you may require.