

Modifying the schema

Modifying Active Directory's schema

Active Directory is at the heart of your Windows 2000 or Windows 2003-based network. It contains all of the objects that represent network resources, all the people that can access those resources, and how they all relate to one another. Within each object is a set of properties that contains information about the object. For example, the user object includes properties that describe the user's name, address, and telephone number, as well as what rights the user has on the network. But, what do you do if you want include additional information, such as hire dates, that doesn't have a predefined property inside of an object?

Don't worry. Microsoft has given you the ability to extend Active Directory's schema to include these new properties. In this article, I'll show you how it's done.

What's Active Directory schema?

Think of Active Directory's schema as the recipe book for Active Directory. It describes all of the objects, object classes, and properties within Active Directory. It controls what types of objects can exist in Active Directory, as well as what properties can exist within those objects.

Active Directory's schema covers your network's entire forest structure. All Active Directory trees, domains, and domain controllers within an Active Directory forest share the same schema.

Active Directory comes with many preexisting object classes and properties. For example, within the user object, you'll find fields that describe the user's name, location, group membership, and security rights.

All new user objects that you create are built off of a base user-object class template that the schema defines. This gives the same basic attributes to each occurrence of the user object throughout the schema.

If you look through a basic object's properties, such as the user object, you'll see dozens of different attributes that you can set. Chances are, you don't even use most of them. Occasionally, however, there may be an attribute you want to store but can't, since you don't have a location to put it in. That's when you'll need to change the schema to add the additional attributes.

Danger!

Changes made when modifying the schema cannot be undone. Be very careful when making schema modifications. It is all too easy to severely damage your Active Directory tree.

The schema can only be edited by the domain controller (DC) that has the flexible single master operation (FSMO) role of Schema Master.

The tools you'll need for schema editing

Microsoft provides two tools for making modifications to the Active Directory schema: Active Directory Service Interfaces (ADSI) Edit and the Active Directory Schema Editor.

ADSI Edit is a tool that allows direct editing of the schema. Using it requires an extensive knowledge of Active Directory, Lightweight Directory Access Protocol (LDAP), and ADSI. It's very difficult to use and understand and isn't a good choice for beginners, or even those with midlevel skills, especially if you only want to make a minor schema adjustment. This tool could cause major nightmares within your Active Directory structure if not used with great care.

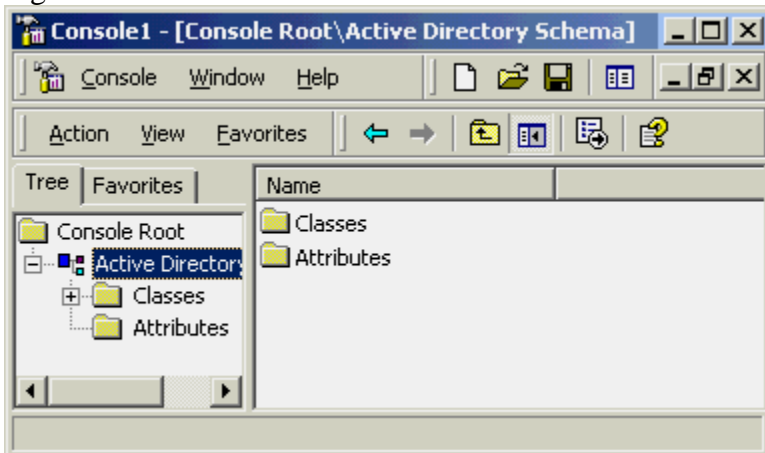
The Active Directory Schema Editor is supplied along with Windows 2000 as a Microsoft Management Console (MMC) snap-in. Windows 2000's Setup program doesn't install the Active Directory Schema Editor in its default routine. You must both register the snap-in and create an MMC before you can use it. Since the schema is such a sensitive area within Active Directory, I recommend setting up a new MMC console for schema modification and allowing only highly trusted and knowledgeable network personnel to have access to this console.

To register the Active Directory Schema Editor, open a command prompt, type `regsvr32 schmmgmt.dll` and press [Enter]. When you do, you'll see a RegSrv32 dialog box appear displaying the message "DllRegisterServer in schmmgmt.dll succeeded". Once the `schmmgmt.dll` is registered for use on the server, you can then use it as an MMC snap-in.

To install the Active Directory Editor snap-in, click Start | Run and enter `MMC /a` in the Run dialog box. This opens a blank MMC console in author mode. Maximize the Console Root window to make the MMC easier to view and work with. Next, select Add/Remove Snap-In from the Console menu. When the Add/Remove Snap-In window appears, click Add. Doing so will display the Add Standalone Snap-In window, which contains a list of available snap-ins that you can use to create your MMC.

Scroll through the list of snap-ins until you see Active Directory Schema. Select it and then click Add. Click Close to close the Add Standalone Snap-In dialog box and then click OK to close the Add/Remove Snap-In dialog box. You'll then see the Active Directory Schema MMC appear, as shown in Figure A.

Figure A



You must create a custom MMC to use the Active Directory Schema Editor.

To save yourself the hassle of having to create a custom MMC every time you want to use the Active Directory Schema Editor, you should save the MMC before going any further. Click Save from the Console menu. When the Save As window appears, type Active Directory Schema Editor in the File Name field. Accept the default location, which will cause the Schema Editor to be saved in the Administrative Tools folder. Next time you want to start the Schema Editor, click Start | Programs | Administrative Tools | Active Directory Schema Editor.

Let the modification begin!

Now that you have got the tools to do the job properly, it's time to look at what it takes to modify Active Directory's schema. By way of an example, I will provide you with a scenario where you might choose to modify the Active Directory schema. Let's suppose that you are a junior administrator for your organization, and you have just come from a meeting with your supervisor. During the meeting, she informed you that the company has decided to start an internship program to help the local college with the placement of its graduates.

You're directed to create a method for keeping track of interns that are hired by your organization. Your supervisor asked you to give each employee a status: full-time for regular employees and intern for the company's new class of interns. She also asked you to place the interns together in a group so that they can all be found in one place when searching the network.

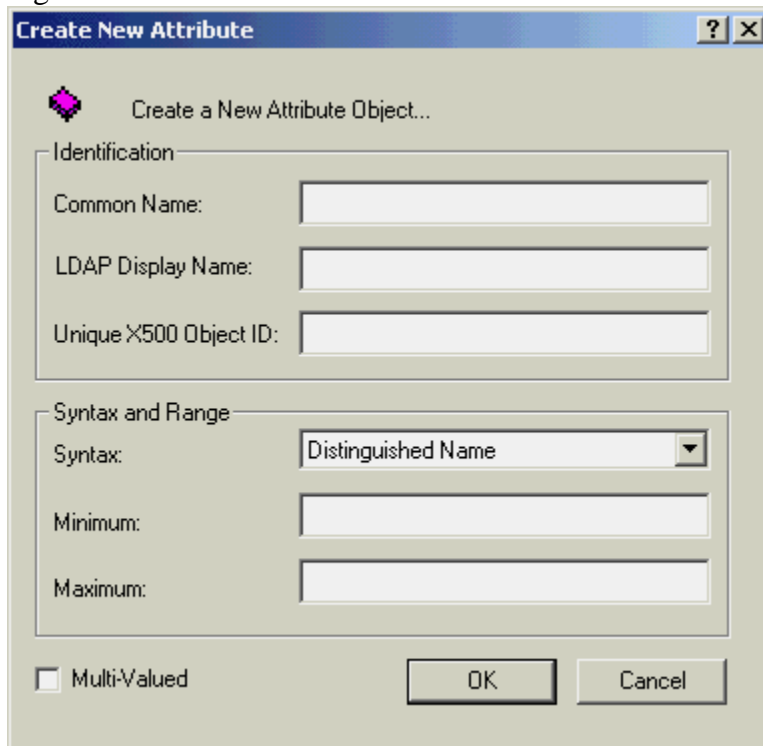
First, create an OU for the interns called Interns_OU in the Active Directory Users And Computers utility. After you create the group, you can modify the user object class to add an extra attribute for the employee status. This modification can be completed using the following steps.

Start the Active Directory Schema Editor. In the left pane of the console, select the Attribute folder. Click the Action Menu and choose Create New Attribute.

You'll then see a very nasty message appear on your screen that reminds you that the changes you make to your Active Directory become a permanent part of your Active Directory structure.

Read the warning, taking into consideration the change you're making to your server's schema before proceeding. Click Continue to clear the message and continue. The Create New Attribute window, as shown in Figure B, will appear. On this screen, you'll fill out the information for your new attribute.

Figure B



You can create new attributes for objects in your Active Directory tree.

Enter a name for your attribute in the Common Name field. Naming Active Directory attributes must follow a very precise syntax in order to meet international naming standards. Create a common name with the following syntax: `dnsname-year-product-attribute-name`. The parts of the name are:

- **Dnsname** - This is the registered DNSname of your organization.
 - **Year** - This is the four-digit year that the attribute was created.
 - **Product** - This is the product that's using the attribute. This must be a unique descriptor that starts with an uppercase letter.
- Attribute-name** - This is a descriptive name of the attribute. If you use more than one word to describe the attribute, you must separate the word with a hyphen (hire-date, for example).

The LDAP Display Name field contains the LDAP information for the attribute. The name is the same as the common name, but you must remove all hyphens from the common name's attribute-name section.

At the X500 OID prompt, enter a unique value for your organization, appending divisional and other identifiers as needed. Don't just make this number up. If you do, you can cause a conflict with other X.500 implementation on the Internet. If you don't have an X.500 object ID, you should apply for one from the [American National Standards Institute](#), which handles registrations in the United States.

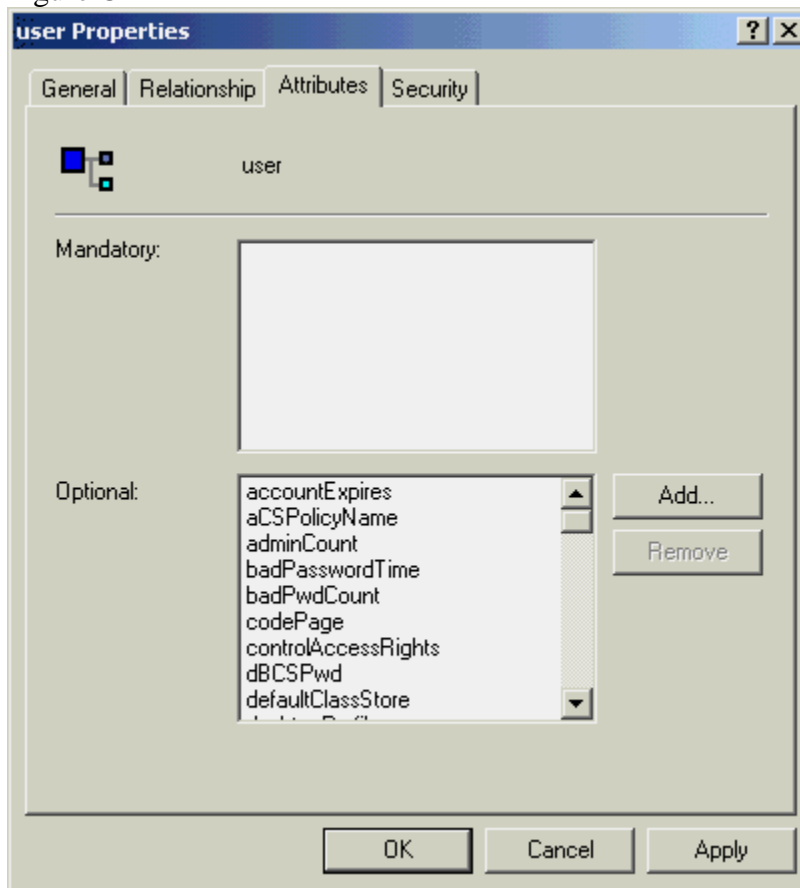
Select a syntax for the attribute you are creating from the Syntax drop-down list box. You have several choices, including Boolean, Integer, Case Sensitive String, and Case Insensitive String. In this case, we are using a text value, so the best choice for this option will be Case Insensitive String. If appropriate, enter a minimum and maximum value for your attribute in the Minimum Value and Maximum Value fields, respectively. Because the attribute can have more than one value, select the Multi-Valued check box. Click the OK button to create your attribute.

You have just created your first Schema attribute in Active Directory. Now you will need to open the Classes portion of the console and assign this attribute to the user class so that you can use it when creating new users.

Begin by expanding the Classes folder in the left pane of the Active Directory Schema console window. Next, scroll to the bottom of the list and locate the User class. You can also click the first class listed and press [U] to quickly go to the user class.

Next, select Properties from the Action menu. This will show the properties pages for the entire User class in Active Directory. Select the Attributes tab, as shown in Figure C.

Figure C



To add a new attribute, click the Attributes tab in the User Properties window.

Click Add to display the Select Schema object screen. Scroll through the Select A Schema Object list box and locate and select your new attribute. Click OK after you've selected the new object to close the Select A Schema Object window. Then click OK again to close the User Properties window and activate your new attribute. You can now go into Active Directory Users And Computers and select a User object to view your new attribute.

Conclusion

You have just successfully extended the schema. This was a rather simple example, but in reality, it reflects exactly the reason why and how you'd go about modifying Active Directory's schema.

The schema is the lifeblood of your Active Directory implementation. Please think very carefully and plan well before you begin modifying the schema in a production Active Directory environment. Don't forget that mistakes you make are irreversible and can lead to the collapse of your Active Directory tree.