Windows Server Platforms - User and Group Management

Windows Server Platforms - User and Group Management

On this page:

Add Users to a Group
Create a Security Group of Users
Create a Policy to Add a Security Group to the Local Adminstrators Group
Add a Domain Account to the Administrators Group with Addadmin.exe
User Profiles
Related Links

Add Users to a Group

The group is one area where win.mit.edu, or WIN, diverges from a typical Windows Domain. WIN users and groups are defined and maintained in the MIT system of record, Moira.

There are a variety of tools available to add an existing user to an existing group. These include the Moira list management web interface, `moira` commands like `blanche` , and the WIN machine `Moira MMC` snap-in.

On a WIN machine you may run `moira` or `blanche` from the command line or the run menu. You may also start the `Moira MMC` snap-in from the menu item **Start-> Programs-> Administrative Tools-> Moira Account Management.**

To add a user to a group using the Moira MMC:

1. Select **List Management** from the left panel and right click on the selection.
2. Select **Find Lists**.
3. Click on **Name**, enter the list name and hit **Search**.
4. Select the list name and hit **Display**.
5. Right click on the list name and select **Properties**.
6. Click on the **Members** tab.
7. If you have the permission, the **Add** button will be sensitized, so click on it.
8. Choose the type of object you wish to add and enter its name.
9. Click **OK**.

Create a Security Group of Users

In WIN each group of users and each group of machines is also defined in Moira. To create a security group of users, in this case to assign its members rights to a particular group of machines:

1. Ask to create a group (Web Moira, certificates required) that contains the userids of users to be allowed access to the machines.
2. Request a container, an organizational unit which contains the machines to be controlled. (This can be a sub-OU of an OU which already has other policies applied, e.g. an existing OU of machines installing Office XP.)
3. Create or request a new group policy on the newly-created OU. Edit the policy as follows:
    - Expand Computer configuration... **Windows Settings > Security Settings > Local Policies > User Rights Assignment**
    - Double-click **Access This Computer From the Network** and click on **Add** - add the newly created user group
    - Double-click **Logon Locally** and click on **Add** - add the user group created at Step 1.

By defining these two options, you automatically deny access to other users. You do not need to define deny options - doing so may have unintended results!

Create a Policy to Add a Security Group to the Local Adminstrators Group

Requirements: Container Administrator rights, i.e., rights over an organizational unit

Create a security group which contains the user ids of the users who will be allowed local administrator access to the computers in the organizational unit.

Note: The name of the group cannot contain any spaces.

Create a `.bat` file containing the following simple script:

```
net localgroup administrators LocalAdministratorGroupName /add
```

Where *LocalAdministratorGroupName* is the name of the group of local administrators previously created in the Active Directory.

Add the script to a group policy:

1. Select the OU to which you want the policy to be applied.
2. Right-click **Properties...** , click on the **Group Policy** tab, select **New...**
3. Give the group policy a name (prefixed with the name of your departmental OU).
4. Click **Edit**.
5. Expand **Computer Configuration > Windows Settings > Scripts...**
6. Double-click **Startup...** , select **Add**.
7. Type the script name and location in the Script Parameters box,
   e.g., `\\campus\software\dept\myDept\localAdmin.bat`.

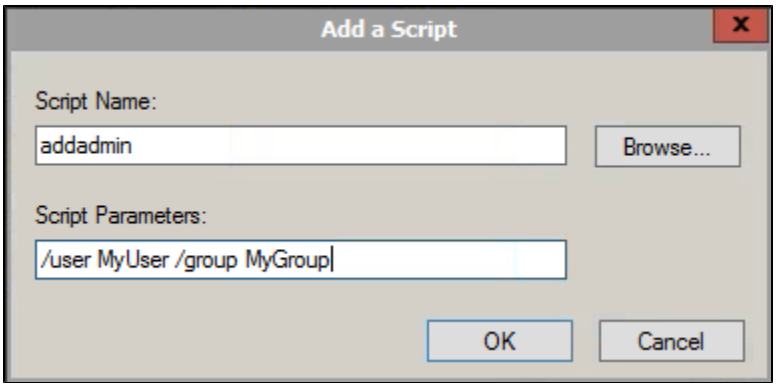
For an existing group policy you will need to edit that policy using steps 4-7 above.

Note: You can edit only policies that you have created yourself, or for which you have been expressly granted editing permissions by the original policy creator.

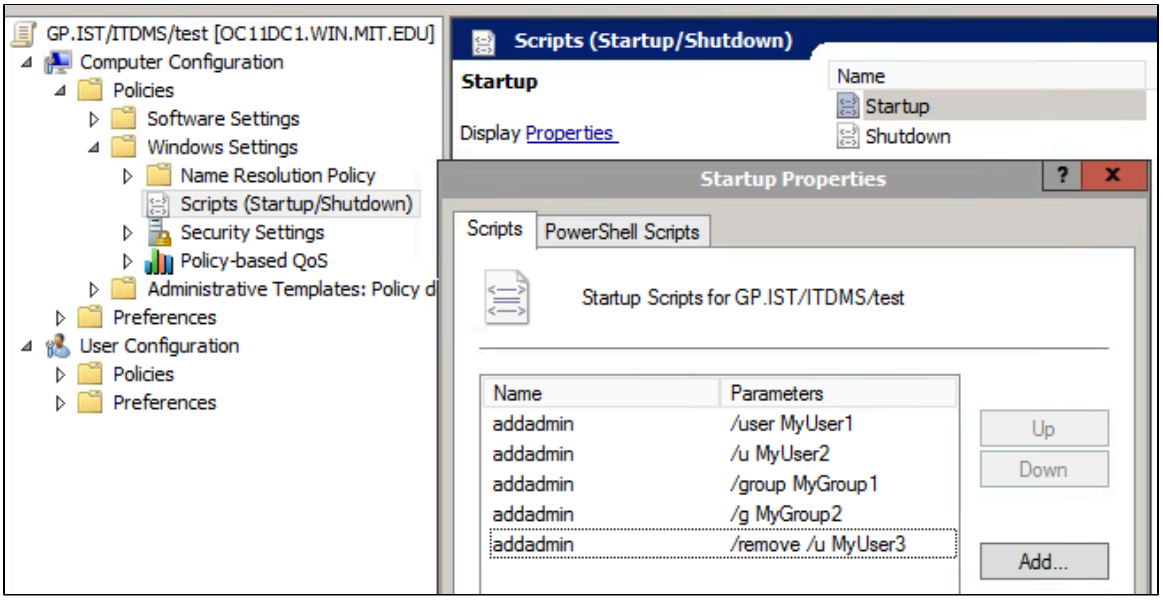
Add a Domain Account to the Administrators Group with Addadmin.exe

Addadmin.exe is located on the path of each WIN machine. Type `addadmin` at a command-line prompt for usage information. This program can add (or remove) a domain account to (or from) the local Administrators group on the machine. The container admin may want to use this as a machine startup script to ensure that a container admin group always has local admin rights on each machine in the container.

A domain user or group can be added to local administrators group by invoking Addadmin.exe as a Startup Script (**Computer Configuration > Windows Settings > Scripts > Startup**, choose **Add...**) For example, to add the **MyUser** and **MyGroup** to the local administators group, use the follow settings (as shown in the image):



Both **/u** and **/g** be used as shorthand for **/user** and **/group**. The example below has separated out the addition of users and groups into separate entries in the Startup script list for clarity. Note that the **/remove** switch will remove a domain user or group from the local administrators group if it is present.



User Profiles

Please see the document Managing Your User Profile for more information.

Related Links

- The win.mit.edu Domain
- Windows Server Platforms
- WIN.MIT.EDU Landing Page
- Windows Server Software Landing Page