

Installing and Starting a PC Spawner on Windows Operating Systems

A Windows *spawner program* enables a local host to connect to a remote host. The spawner resides on the remote host where it listens for requests from a client host for connection (via SAS/CONNECT[®] software) to the remote host. When the spawner receives a request, it launches a SAS[®] session on behalf of the connecting client.

This article explains how to

- set user rights (which are required in order to start/install the program)
- install the spawner as a Windows service or by running it manually
- delete a spawner, as needed.

Step 1: Define Windows User Rights for Administrator

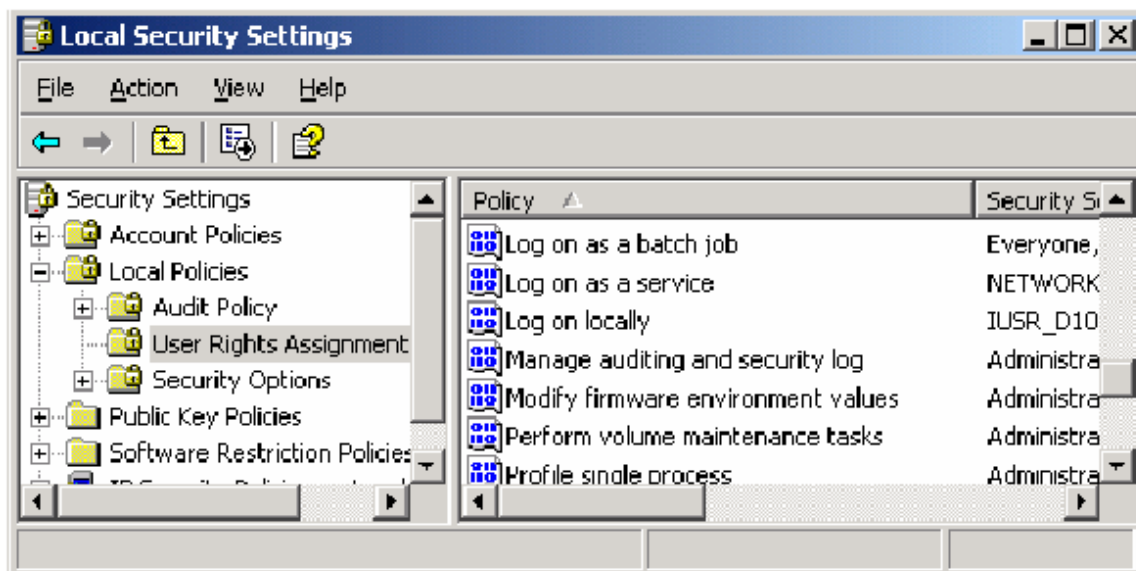
To install a PC spawner program as a Windows service, you must sign on to the operating system as the local administrator. If you do this, you do not need to do anything additional to define user rights.

However, you will need to define user rights if you have either

- run the PC spawner manually (instead of starting it as a Windows service)
- defined the PC spawner program as a Windows service, but configured it to run as a user other than LocalSystem (the default).

If you have performed either of these tasks, you will need to define the user rights by following these steps:

1. Click the Start button and select Settings ➔ Control Panel. Then select Administrative Tools ➔ Local Security Policy to display the Local Security Settings window.
2. In the Local Security Settings window, select Security Settings, then expand the Local Policies tree and select User Rights Assignment as shown in Display 1.



Display 1. User Rights Assignment Policy in the Local Security Settings Window

The user who invokes the PC spawner program must be a part of the Administrators group. The PC spawner program creates Windows processes as other users. To do this, the spawner program must load the profile of the user under which that process will run. Only administrators can load user profiles; therefore, you need to add the Administrators group to the following user rights:

- Act as part of the operating system (You only have to add the Administrators group for the Windows NT or Windows 2000 systems, but not for Windows XP and later versions.)
- Adjust memory quotas for a process (On Windows NT and Windows 2000 systems, this right will be listed as `Increase quotas`.)
- Replace the process level token
- Bypass traverse checking (the default is Everyone)
- Log on locally (the default is Everyone)

To set the administrator's user rights on Windows NT,

1. click the Start button and select Programs ➤ Administrative Tools ➤ User Manager
2. select User Rights from the Policies drop-down list
3. select the Show Advanced User Rights check box
4. add rights using the Right drop-down list.

To set the administrator's user rights on Windows 2000,

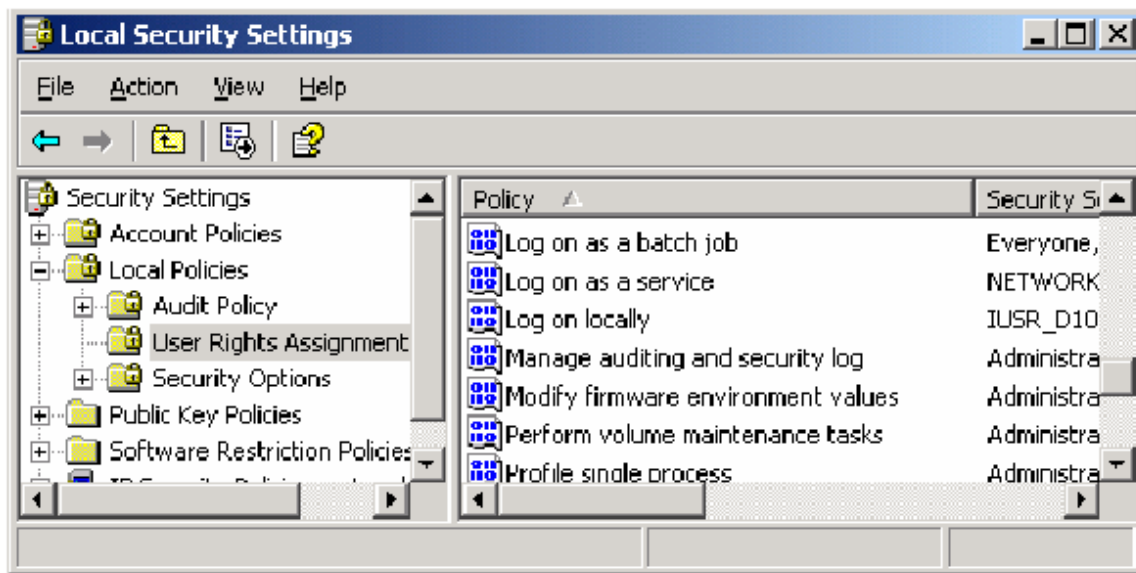
1. click the Start button and select Settings ➤ Control Panel. In the Control Panel, select Administrative Tools ➤ Local Security Policy.
2. click Security Settings, expand the Local Policies tree, and click User Rights Assignment.
3. add rights by double-clicking each right and assigning the appropriate users.

To set the administrator's user rights on Windows XP,

1. click the Start button and select Settings ➔ Control Panel. In the Control Panel, select Administrative Tools ➔ Local Security Policy.
2. expand the Local Policies tree and click User Rights Assignment.
3. add rights by double-clicking each right and assigning the appropriate users.

Step 2: Define Windows User Rights for All Users Who Sign on to the PC Spawner Program

All users who sign on to the PC spawner program must have the permission for the user right Log on as a batch job as shown in Display 2.



Display 2. User Right Assignment: Log on as a batch job

You can grant permission to log on as a batch job to individual users or to a group of SAS users. However, a general testing rule is to grant everyone permission (using the Everyone group) while testing the connection, and then tighten security after initial testing is complete.

Step 3: Installing the PC Spawner Program

You can start a PC spawner program by installing it as a Windows service or by running the program manually. The next sections explain how to start and stop the spawner using each of these methods.

Starting the PC Spawner as a Windows Service

To start the PC spawner as a Windows service, follow these steps:

1. Open a DOS command window by selecting **Start** ➤ **Run**. Then type **CMD.EXE** in the **Open** field and click **OK**.
2. In the DOS window, change to the **!SASROOT** directory by submitting the following command from the DOS prompt:

```
cd !sasroot-path
```

Depending on which version of SAS you use, the value for **!SASROOT-PATH** will be one of the following:

- **C:\SAS> (for SAS 6)**
 - **C:\Program Files\SAS Institute\SAS\V8> (for SAS 8)**
 - **C:\Program Files\SAS\SAS 9.1> (for SAS 9.1)**
3. Install the spawner using the **-i** command. You must install the spawner before you can start it as a service.

```
!sasroot-path:> spawner.exe -i -c tcp
```

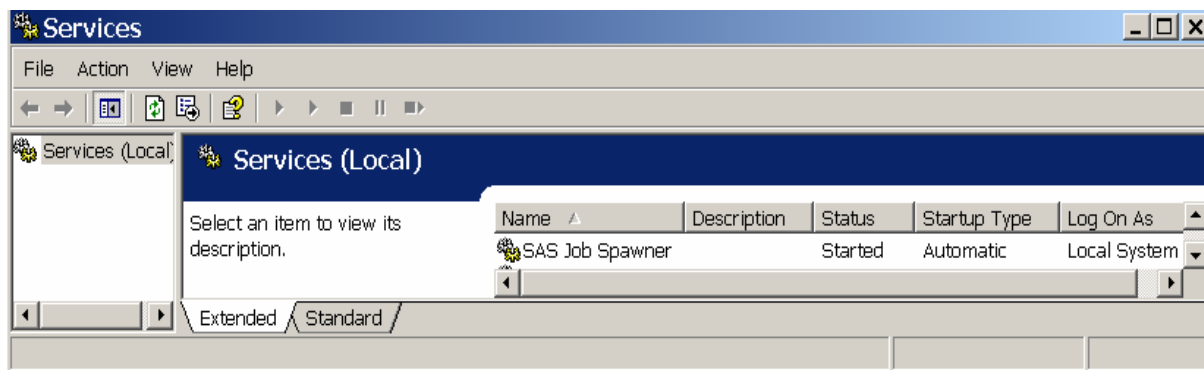
4. Submit the following command from the DOS prompt:

```
net start "SAS job spawner"
```

You can also start the spawner from the Windows Control Panel by following these steps:

1. Click the **Start** button and select **Start** ➤ **Settings** ➤ **Control Panel**. In the **Control Panel**, select **Administrative Tools** ➤ **Services**.
2. Click **SAS Job Spawner** in the right pane.
3. On the **Services** window toolbar, select **Action** ➤ **Start**.

The **Status** field in the right pane should now display **Started**, as shown in Display 3.



Display 3. Verification That the Spawner Started

Notes

- For SAS 8.2 and earlier, you can have only one PC spawner program running on a Windows server unless you have applied the SAS 8.2 hot fix 82BB79.
- If you want to invoke a SAS 8 process (TS065 and higher) or a SAS 6 process by using the same spawner program, you should use the SAS 8 spawner program. To do that, you need to modify the script so that it points to either the SAS 8 executable file or the SAS 6 executable file.

Stopping the PC Spawner as a Windows Service

To stop the PC spawner program, submit the following command from a DOS prompt:

```
net stop "SAS job spawner"
```

You can also stop the spawner from the Windows Control Panel by following these steps:

1. Click the Start button and select Start ➤ Settings ➤ Control Panel. In the Control Panel, select Administrative Tools ➤ Services.
2. Click SAS Job Spawner in the right pane.
3. On the Services window toolbar, select Action ➤ Stop.

Deleting the PC Spawner as a Windows Service

If you need to delete the PC spawner program, use the following command at the DOS prompt:

```
!sasroot-path:> spawner.exe -d
```

As mentioned previously in “Step 3: Installing the PC Spawner Program”, the value for *!SASROOT-PATH* depends on which version of SAS you use.

Starting and Stopping the PC Spawner Program Manually

To start a PC spawner program manually, you must be signed on as the Local Administrator with the rights described previously in the section “Step 1: Define Windows User Rights for Administrator”.

To start the spawner, follow these steps:

1. Open a DOS command window by selecting Start ➤ Run. Then, type CMD.EXE in the Open field and click OK.
2. In the DOS window, change to the *!SASROOT* directory by submitting the following command at the DOS prompt:

```
!sasroot-path:> spawner.exe -c tcp -security
```

Depending on which version of SAS you use, the value for *!SASROOT-PATH* will be one of the following:

- C:\SAS> (for SAS 6)
- C:\Program Files\SAS Institute\SAS\V8> (for SAS 8)
- C:\Program Files\SAS\SAS 9.1> (for SAS 9.1)

To stop the spawner manually, use either of the following methods:

- Use the keyboard combination CTRL-C.
- Double-click in the upper-left corner of the window that runs the spawner.

Spawner Installation Command Options

For a complete list of spawner command options, see the online documentation for your version of SAS. You will find the spawner information in the “Communications Access Methods” sections for SAS/CONNECT and SAS/SHARE® software.