# Task Scheduler and security: Management Services

By Archiveddocs

Archived: 2026-04-05 14:52:44 UTC

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

## Task Scheduler and security

When creating a scheduled task, you must enter a user name and password, either in the **Add Scheduled Task Wizard** or in the **Run as** box in the **Task** tab of the scheduled task's property dialog box. When the scheduled task runs, the program you've scheduled runs as if it were started by the user you specified, with that user's security context. For example, if the user specified for a scheduled task is a member of the Backup Operators group on the local computer, the program specified in the scheduled task file runs as if a member of the Backup Operators group is logged onto the local computer. If another user is logged on to the computer at the time a scheduled task specified for a different user runs, the task runs but is not visible to the current user.

By default, to schedule a task, you must be a member of the Administrators, Backup Operators, or Server Operators group on the local computer. By default, when creating a scheduled task, you cannot enter a user who belongs to a group that has more rights than the group you belong to. For example, if you are a member of the Backup Operators group on the local computer, you cannot specify a member of the Administrators group when creating a scheduled task. However, a member of the Administrators group can enable a member of any group to create or modify scheduled tasks, by using the **cacls** command to modify the discretionary access control list (DACL) of the **Tasks** folder. By default, the **Tasks** folder is located in the **\Windows** folder on the hard drive of the local computer, for example **C:\Windows\Tasks**. For more information about using **cacls**, see Cacls. For more information about groups, see Default local groups and Default groups.

**Note**

- A user for whom you assign permissions to the **Tasks** folder using **cacls** will be able to access scheduled tasks for all users. Choose which users to give access to the **Tasks** folder judiciously.

In Windows Server 2003 family operating systems, passwords have an expiration date. If you are scheduling recurring tasks that run indefinitely, you need to be aware of the expiration date on your passwords. If the password changes for an account on a domain, then you must update the tasks scheduled to run under that account.

When a job is created through Task Scheduler, account information for all tasks that use the same **run as** account is stored only once. Task Scheduler validates the **run as** account when a job is created, which prevents incorrect

**run as** account information from being saved and, as a result, prevents other existing jobs that use the same account from being affected. If the password validation fails, a job file is created, but it will not run.

If the **run as** account password has expired or the account has been deleted and recreated, the password must be updated for jobs to run. Updating the password for one job automatically updates it for all jobs that use the same **run as** account.

When you create a scheduled task, the user credentials you specify for that specific task are securely stored on the local computer.

For security-related tips on using Task Scheduler, see Task Scheduler Best practices.

**Notes**

- To view the user and group permissions for a scheduled task, right-click the task, click **Properties**, and then click the **Security** tab.
- To view or change advanced user and group permissions, on the **Security** tab, click **Advanced**, click the user for whom you want to view or change permissions, and then click **View/Edit**.
- For information about viewing past scheduled tasks, see View a log of past scheduled tasks.
- For general information about Task Scheduler, see Task Scheduler overview.

---