# Domain controller: Allow server operators to schedule tasks

By Archiveddocs

Archived: 2026-04-06 01:50:51 UTC

Applies To: Windows Server 2003, Windows Vista, Windows XP, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8

This security policy reference topic for the IT professional describes the best practices, location, values, and security considerations for this policy setting.

This policy setting determines whether server operators are allowed to submit jobs by means of the **at** command. If you enable this policy setting, jobs that are created by server operators by means of the **at** command run in the context of the account that runs the Task Scheduler service. By default, that is the Local System account.

Note

This security option setting affects only the scheduler tool for the **at** command. It does not affect the Task Scheduler tool.

Enabling this policy setting means jobs that are created by server operators through the **at** command will be executed in the context of the account that is running that service—by default, that is the Local System account. This means that server operators can perform tasks that the Local System account is able to do, but server operators would normally not be able to do, such as add their account to the local Administrators group.

The impact of enabling this policy setting should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by using the Task Scheduler Wizard, but those jobs will run in the context of the account that the user authenticates with when setting up the job.

- Enabled
- Disabled
- Not defined
- Best practices for this policy are dependent on your security and operational requirements for task scheduling.

*GPO_name*\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

The following table lists the actual and effective default values for this policy. Default values are also listed on the policy’s property page.

| Server type or GPO | Default value |
|---|---|
| Default Domain Policy | Not defined |
| Default Domain Controller Policy | Not defined |
| Stand-Alone Server Default Settings | Not defined |
| DC Effective Default Settings | Not defined |
| Member Server Effective Default Settings | Not defined |
| Client Computer Effective Default Settings | Not defined |

There are no differences in this policy between operating systems beginning with Windows Server 2003.

This section describes features and tools that are available to help you manage this policy.

None. Changes to this policy become effective without a computer restart when they are saved locally or distributed through Group Policy.

The **at** command schedules commands and programs to run on a computer at a specified time and date. The Schedule service must be running to use the **at** command. For more information about the **at** command, see At [Vista].

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Tasks that run under the context of the Local System account can affect resources that are at a higher privilege level than the user account that scheduled the task.

Disable the **Domain controller: Allow server operators to schedule tasks** setting.

The impact should be small for most organizations. Users (including those in the Server Operators group) can still create jobs by means of the Task Scheduler snap-in. However, those jobs run in the context of the account that the user authenticates with when setting up the job.

---