March 15, 2024

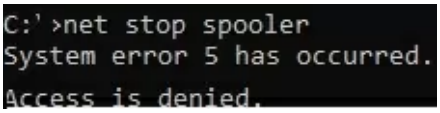
How to Allow Non-Admin User to Start/Stop Service in Windows

By default, regular (non-admin) users cannot manage Windows services. This means that users cannot stop, start, restar change the settings and permissions of Windows services. In some cases, a user must have permission to restart or man certain services. In this article, we'll look at several ways to manage the permissions for Windows services. As an exampl we'll show how to allow a non-admin user to restart a specific Windows service.

Suppose you need to give the domain account *contoso\tuser* the right to restart the *Print Spooler* service. If the non-adm user tries to restart the service, an error will be displayed:

```
net stop spooler
```

```
System error 5 has occurred. Access is denied.
```



In Windows, there are several ways to grant service permissions:

Contents:

Manage Service Permission with Windows CMD

You can use the built-in sc.exe (Service Controller) console command to manage the permissions of a Windows service

Edge computing is geëvolueerd.
Jouw IPC ook?

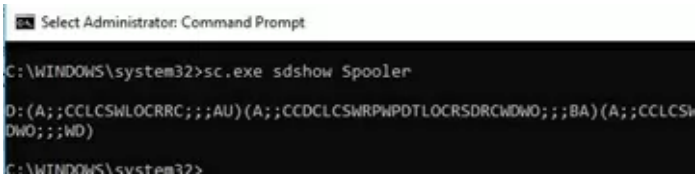
AliExpress

- `sc sdset` – change service permissions

The main disadvantage of this method is that the format for the granting of rights to the service is very complicated. Sec Description Definition Language (SDDL) format is used.

You can get the current service permissions as an SDDL string:

```
sc.exe sdshow Spooler
```




```
D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Kies zelf de apparat
Mastercom
Op

What are all these symbols?

```
S: – System Access Control List (SACL)
D: – Discretionary ACL (DACL)
```

```
CC – SERVICE_QUERY_CONFIG (query service settings)
LC – SERVICE_QUERY_STATUS (get service status)
SW – SERVICE_ENUMERATE_DEPENDENTS
LO – SERVICE_INTERROGATE
CR – SERVICE_USER_DEFINED_CONTROL
RC – READ_CONTROL
RP – SERVICE_START
WP – SERVICE_STOP
DT – SERVICE_PAUSE_CONTINUE
```

Kies zelf de apparatuur.

Voor het onderwijs, gemeenten, zorginstellingen en kantooromgevingen.

The last 2 characters are the objects (user, group, or SID) to which permissions are granted. Here is a list of predefined groups.

```
AU Authenticated Users
AO Account operators
RU Alias to allow previous Windows 2000
AN Anonymous logon
AU Authenticated users
BA Built-in administrators
BG Built-in guests
BO Backup operators
BU Built-in users
CA Certificate server administrators
CG Creator group
CO Creator owner
DA Domain administrators
DC Domain computers
DD Domain controllers
DG Domain guests
DU Domain users
EA Enterprise administrators
ED Enterprise domain controllers
WD Everyone
PA Group Policy administrators
```

```
LS Local service account
SY Local system
NU Network logon user
NO Network configuration operators
NS Network service account
PO Printer operators
PS Personal self
PU Power users
RS RAS servers group
RD Terminal server users
RE Replicator
RC Restricted code
SA Schema administrators
SO Server operators
SU Service logon user
```

Kies zelf de apparatuur.

Voor het onderwijs, gemeenten, zorginstellingen en kantooromgevingen.

You can use pre-defined groups in the DACL, or you can specify any user or group by SID. Use the command to get the S for the current user:

```
whoami /user
```

Or, you can use the Get-ADUser cmdlet to find the SID for any domain user:

```
Get-ADUser -Identity 'sadams' | select SID
```

Use the Get-ADGroup cmdlet to get the domain group SID:

```
Get-ADGroup -Filter {Name -eq "ny-ithelpdesk"} | Select SID
```

To assign an SDDL string with permissions to a specific service, use the **sc sdset** command. In this example, add the following line to the service ACL.

Kies zelf de apparatuur.

Voor het onderwijs, gemeenten, zorginstellingen en kantooromgevingen.

```
(A;;RPWPCR;;;S-1-5-21-2133228432-2794320136-1823075350-1000)
```

- **A** – Allow
- **RPWPCR** – **RP** (SERVICE_START) + **WP** (SERVICE_STOP) + **CR** (SERVICE_USER_DEFINED_CONTROL)
- **SID** – user or group SID

Add your ACL to the end of the string returned by sdshow. Use the **sc sdset** command to apply the new permissions to a service:

```
sc sdset Spooler "D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;RPWPCR;;;S-1-5-21-2133228432-2794320136-1823075350-1000)"
```

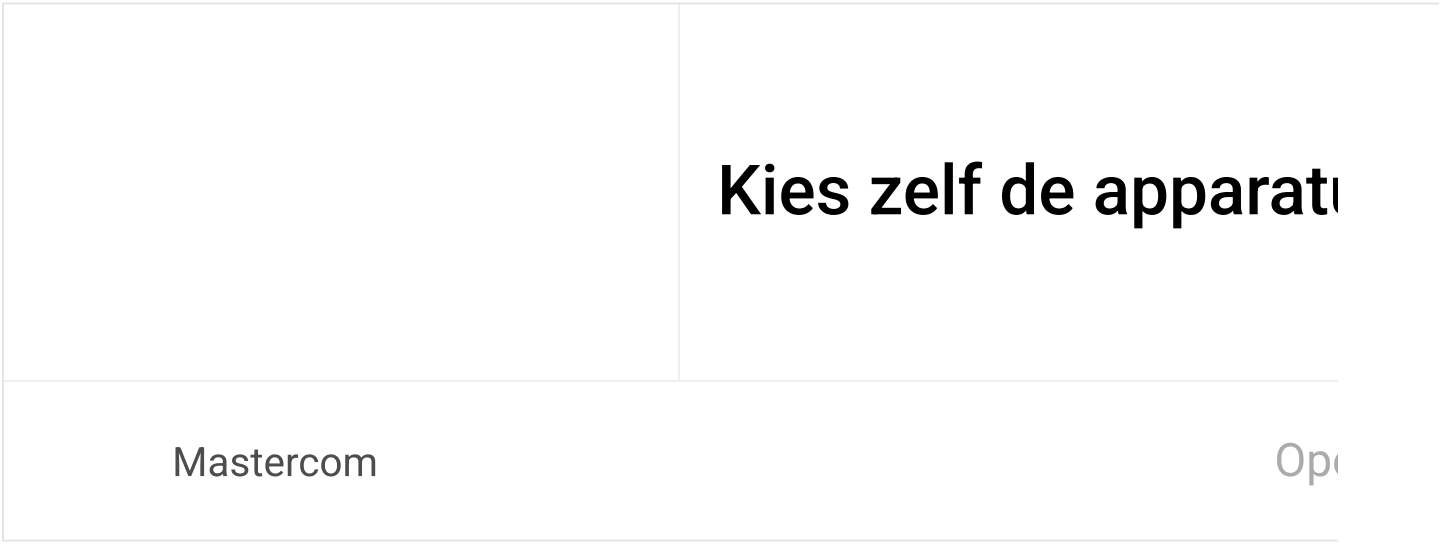
Kies zelf de apparatu

Mastercom Op

If you have a valid DACL, the command will return:

```
[SC] SetServiceObjectSecurity SUCCESS
```

Check that the non-admin user can now stop and start the service:




```
net stop spooler && net start spooler
```

A more convenient way to view the current list of service permissions is to use the **psservice.exe** tool (https://learn.microsoft.com/en-us/sysinternals/downloads/psservice):

```
psservice.exe security spooler
```

```
SERVICE_NAME: Spooler
DISPLAY_NAME: Print Spooler
        ACCOUNT: LocalSystem
        SECURITY:
        [ALLOW] NT AUTHORITY\Authenticated Users
                Query status
                Query Config
                Interrogate
                Enumerate Dependents
                User-Defined Control
                Read Permissions
        [ALLOW] NT AUTHORITY\SYSTEM
                Query status
                Query Config
                Interrogate
                Enumerate Dependents
                Pause/Resume
                Start
                Stop
                User-Defined Control
                Read Permissions
```

```
                Stop
                User-Defined Control
                Read Permissions
        [ALLOW] BUILTIN\Administrators
                All
```

Kies zelf de apparat

Mastercom

Op

In previous versions of Windows, you could use the **SubInACL** console tool (part of the Windows Resource Kit) to manage service permissions.

To allow the contoso\tuser user account to restart the service:

```
subinacl.exe /service Spooler /grant=contoso\tuser=PTO
```

In this case, the user has been granted the permissions to Pause/Continue, Start, and Stop the service. Complete lis of available privileges:

```
F : Full Control
R : Generic Read
W : Generic Write
X : Generic eXecute
L : Read controL
Q : Query Service Configuration
S : Query Service Status
E : Enumerate Dependent Services
C : Service Change Configuration
T : Start Service
O : Stop Service
P : Pause/Continue Service
```

> To revoke a user's assigned rights to a service, use the **/revoke** option:
>
> ```
> subinacl.exe /service Spooler /revoke=contoso\tuser
> ```
>
> However, SubInACL is not currently available for download from the Microsoft website and is not recommended for use.

How to Change Service Permission Using Process Explorer

You can manage service permissions from the GUI using the **Process Explorer** tool (https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer).

1. Run the Process Explorer as an administrator and look for the process of the service that you need in the list of processes. In this example it is `spoolsv.exe` (the spooler executable C:\Windows\System32\spoolsv.exe). Open t process properties and go to the **Services** tab;

3. Add the user or group you want to grant service permissions. By default only the following service permissions ar available: Full Control, Write, and Read;
4. You can assign **Write** permission to a service so that users can start and stop it. However, this also allows the us change or even remove the service;
5. To allow only the start/stop of the service, click on the **Advanced** button -> select your user, click on **Edit** -> cli **Show Advanced Permissions**. Leave only **Start**, **Stop**, **Read**, **Query Status,** and **Custom Control** options the permissions list;
6. Save changes;
7. The assigned user can now restart the service.

Set Service Permissions Using PowerShell

The built-in **Set-Service** service management cmdlet allows you to set the permissions on a service using the SDDL forr similar to sc sdset:

```
Set-Service -Name Spooler -SecurityDescriptorSddl $SDDL
```

> This version of the cmdlet is available only after you install/ upgrade PowerShell Core.
>
> In Windows PowerShell 5.1, this command fails:
>
> ```
> Set-Service : A parameter cannot be found that matches parameter name 'SecurityDescriptorS
> ddl'.
> ```

You can also manage permissions on various Windows objects using the **Carbon** module from the PowerShell Gallery. In the module:

```
Install-Module -Name 'Carbon'
Import-Module 'Carbon'
```

To grant permissions to the service, use the command:

```
Grant-CServicePermission -Identity woshub\maxadm -Name spooler -QueryStatus -EnumerateDependents -Start -Stop
```

List the service's current ACL:

```
Get-ServicePermission -Name spooler|fl
```

How to Use Group Policy to Grant the Permissions for a Service

If you need to grant users permission to start and stop the service on all domain servers or computers, the easiest way t this is to use the Group Policy (GPO) features.

1. Create a new GPO or edit the existing one and link it to the necessary Active Directory container (OU) with the computer objects. Go to **Computer Configuration -> Windows Settings -> Security Settings -> System**

2. Locate the **Print Spooler** service and open its properties;
3. Enable the **Define this policy settings** option, enable auto-start for the service, and click **Edit Security**;
4. In the service security settings, add the user or domain group that you want to assign permissions to the service Grant Start, stop and pause and Read permission;

5. All you need to do is wait for the Group Policy settings to be updated on the client computers and check that you user can now restart the service.

Where are the Windows service security permissions stored?

The security settings for all services for which you changed the default permissions are stored in their own registry key `HKLM\System\CurrentControlSet\Services\<servicename>\Security` in the **Security** parameter (REG_BINARY type).

This means that one of the ways to set the same permissions on other computers is to export/import this registry parameter. You can use the GPO to deploy changes to the registry on domain computers.

If you want the user to be able to stop/start/restart the service remotely (without granting them local sign-in permissions RDP access), you need to allow them to remotely enumerate the Service Control Manager service (`scmanager`).

The following command allows the remote group (user) with the specified SID to enumerate the list of services on the re computer:

```
sc sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC
(A;;CCLCRPRC;;;{PASTE_YOUR_SID_HERE})S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

Otherwise, you will get an error when you try to query services on the remote Windows host:

```
sc \\lonts-01 query
```

```
[SC] OpenSCManager FAILED 5:
Access is denied.
```

So we have looked at several different ways of managing permissions to Windows services that allow granting non-admir users any permissions for system services.

RELATED READING

How to Restore Deleted EFI System Partition in...
March 11, 2024

How to Run Program without Admin Privileges and...
June 8, 2023

How to Install Remote Server Administra Tools (RSAT)...
March 17, 2024

17 COMMENTS

ARAN

April 28, 2016 - 2:35 am

How to Grant non-Administrators Rights like remote desktop users to Install softwares only and allow runnin softwares which demands admin permission to run the software ?

JAY ADAMS

November 4, 2016 - 1:32 pm

You can easily grant non-administrators the ability to manage services with **System Frontier**. The RBAC m is very flexible, but easy to manage through a single web interface.

CHRIS CARPENTER

April 27, 2018 - 10:41 pm

The SubInACL Tool worked perfectly for my needs. I have one non-admin user who needs to restart a single service occasionally. Problem solved. Thanks!

ALEX

Update Medic Service) in Windows 10 Pro! Finally!

RICH

August 1, 2019 - 9:07 pm

when granting a non-administrator the rights to start/stop/query a service as described above, if they do, dc change the 'LogOnAs' attribute for the service? The services I am exposing must also access network resour to which the non-admin users will NOT have access. Would the above break this use case?

ALLOW ACCESS TO SOUND SETTINGS TROUBLE SHOOTER IN GROUP POLICY

November 30, 2020 - 11:16 am

[…] Possibly this How to Allow Non-Admin Users to Start/Stop Windows Service? | Windows OS Hub […]

PAUL

March 26, 2021 - 1:07 pm

Just used the first method at the top adding (A;;RPWPCR;;;RD) for remote access users to restart a service. Thanks for the help!

WINDOWS: EINEM BENUTZER DAS RECHT ZUM STARTEN UND STOPPEN FÜR EINEN BESTIMMTEN DIENST GEBEN – ANDY'S BLOG

May 6, 2021 - 12:54 pm

[…] WindowsOSHub – How to Allow Non-Admin Users to Start/Stop Windows Service? […]

UMESH

May 14, 2021 - 6:34 pm

The only method that worked in our environment was using process explorer.
In my opinion, it's also the easiest.
Thank you!

SERG

April 18, 2022 - 6:56 am

How to grant users rights to manage services:
_https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/grant-users-rights-manag services

May 4, 2022 - 7:42 am

Thank you!

BINBBONG

July 5, 2022 - 12:40 pm

subinacl doesn't officially exist anymore. I wonder when will Microsoft deprecate commands like "dir"...

SAM

March 16, 2023 - 6:27 pm

So we can allow non-admins to restart the service, but services won't restart in CMD or PowerShell without running those as administrator, so we can't have a shortcut to restart the service?

STEVE

June 16, 2023 - 7:28 am

just discovered that adding permissions to services seems to only be not working on Windows Server 2019 Servers. It works just fine on Windows Server 2012 R2 Servers. I am not sure whether or not Windows 201 Servers are affected.
If anyone has any information on how to add permissions for non-admins to remotely start/stop services on Windows 2019 Server, please let me know.
UPD:
Solution for Server 2019 specific problem with assigning access to SCManager
reg add HKLM\SYSTEM\CurrentControlSet\Control /v RemoteAccessExemption /t REG_DWORD /d 1 /f
Credit to tadmaz-quad for posting the question and the answer – Thanks !!
https://social.technet.microsoft.com/Forums/en-US/a9b38117-1e98-4a9e-a4d8-7bbbc3ace2f2/remotely-stopstart-services-not-working-for-nonadmins?forum=ws2019
https://support.microsoft.com/en-us/help/4457739/blocking-remote-callers-from-starting-or-stopping-servic when-they-a

SERG

January 9, 2024 - 12:10 pm

Read security descriptor of a service
Read binary data from registry
$BinarySD = Get-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Spooler\Security -Name Sec
| Select -ExpandProperty Security
$Converter = [system.management.ManagementClass]::new("Win32_SecurityDescriptorHelper")

FERNANDO

November 23, 2024 - 3:55 pm

Hi! Great Post! 🙂
I want the user to be able to stop/start/restart the service remotely (without granting them local sign-in permissions or RDP access). So, I need to allow them to remotely enumerate the Service Control Manager service (scmanager). I read the post and I need to run the following command in the remote computer:
sc sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;
(A;;CC;;;AC)(A;;CCLCRPRC;;;{PASTE_YOUR_SID_HERE})S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
However, I received de following error:
[SC] ConvertStringSecurityDescriptorToSecurityDescriptor FAILED 1337: The security ID structure is invalid.
Do you you I the command is correct? Thanks!

ADMIN

November 26, 2024 - 6:02 am

Replace the "PASTE_YOUR_SID_HERE" block in the command with your user SID .

LEAVE A COMMENT

Your Comment

Name*

Email*

Website

NOTIFY ME OF FOLLOWUP COMMENTS VIA E-MAIL. YOU CAN ALSO SUBSCRIBE WITHOUT COMMENTING.

POST COMMENT

Updatir
Fix: Re
How to
Configu
Allow N
Configu
How to

@2014 - 2024 - Windows OS Hub. All about operating systems for sysadmins

BACK TO TOP