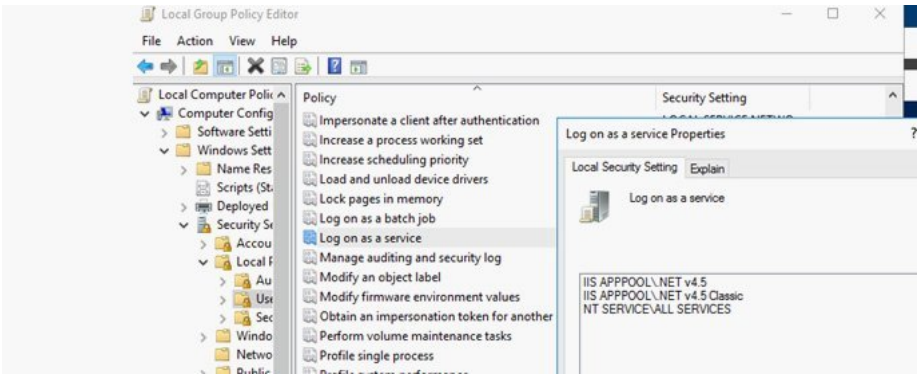
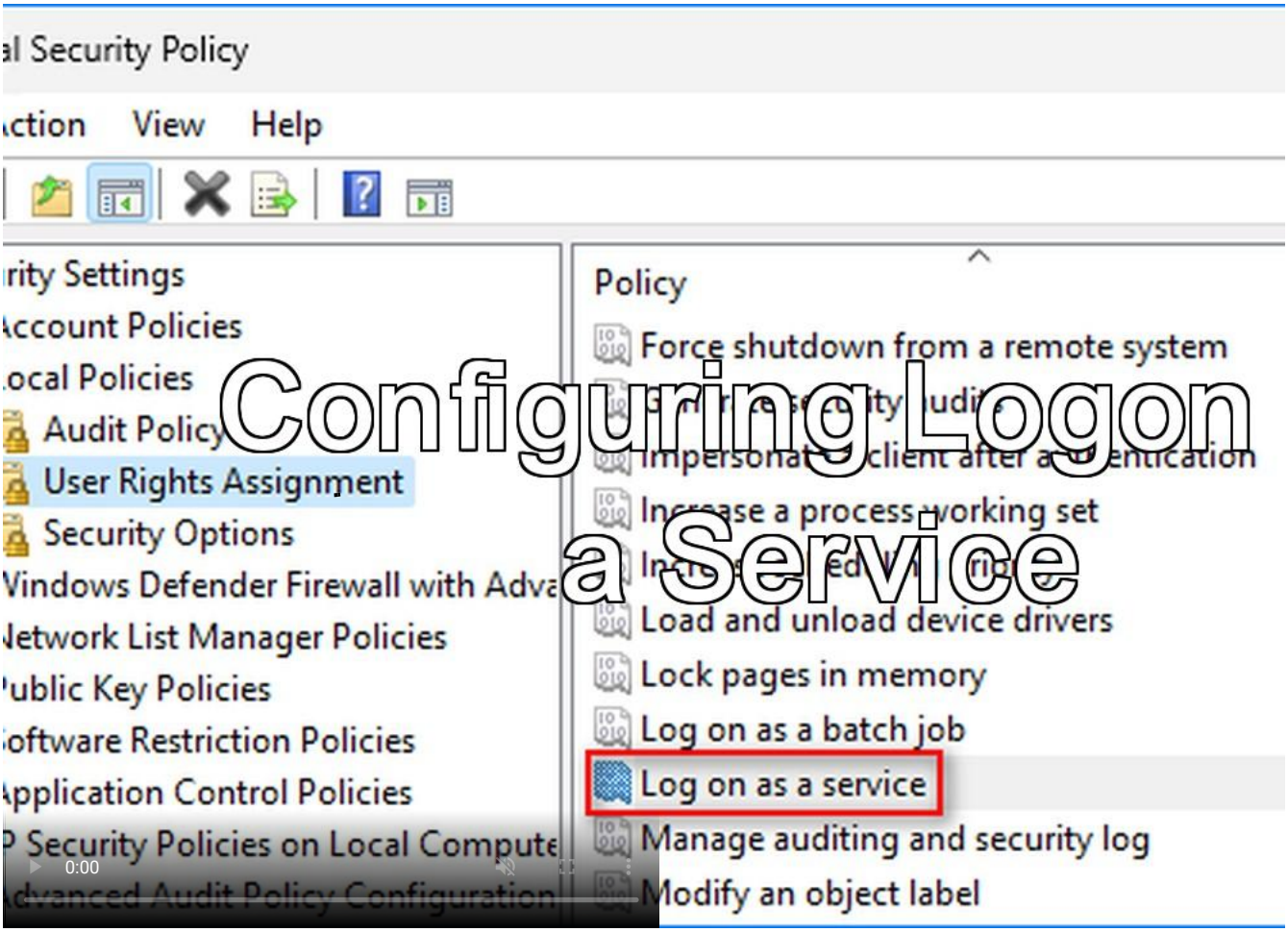
Configuring “Logon as a service” permission via GPO and PowerShell

theitbros.com/logon-as-a-service

Cyril Kardashevsky



“**Log on as a service**” is a security policy that allows certain users to run Windows network services whether they are logged on locally or not. This policy is used when you need to run a specific application or service on a computer in the background, without user interaction and without granting local administrator privileges.



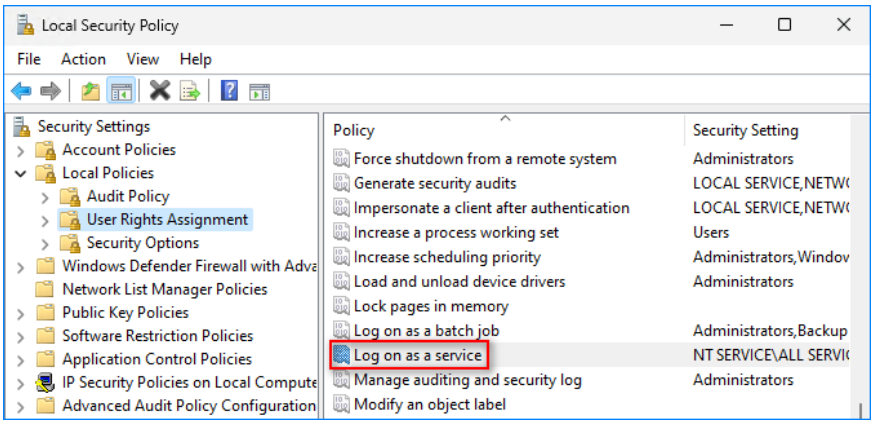
00:03 / 03:54 10 Sec

In this post, we’ll cover how to configure the ‘Log on as service’ policy using a GPO or from the PowerShell command line, and how to configure the service to run under a specific user account.

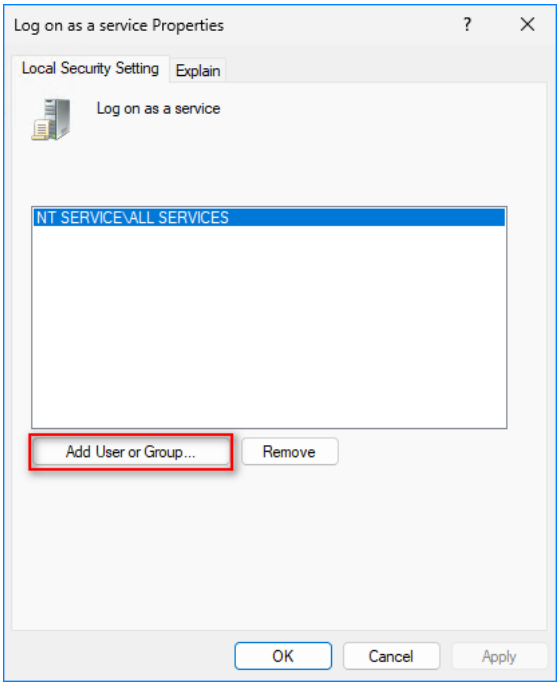
How to Configure “Log on as a service” Rights Assignments via Group Policy

You can configure the “Log on as a service” rights assignment via the local or domain group policy. Use the Local Security Policy (**secpol.msc**) to configure the policy on a specific computer. Or, run the Group Policy Management console (**gpmc.msc**), create and configure new GPO to configure Logon as service policy for multiple domain computers.

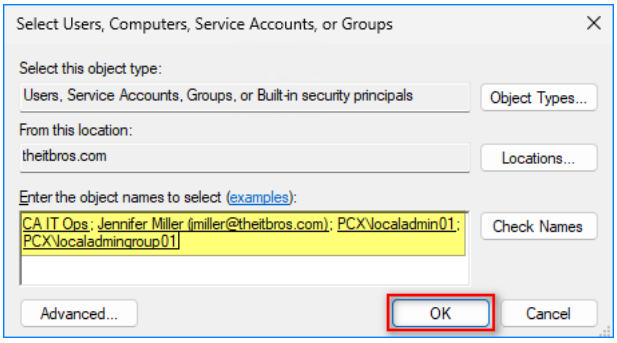
1. Navigate to **Security Settings** → **Local Policies** → **User Rights Assignments** and double-click the "**Log on as a service**" policy.



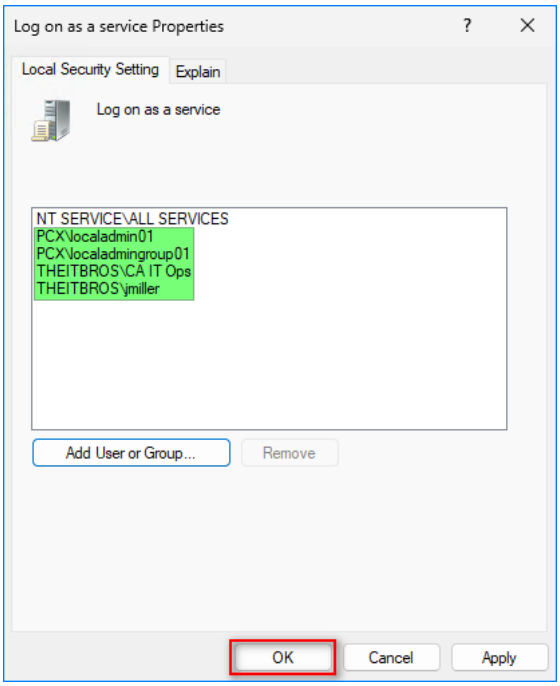
2. By default, only the NT SERVICE\ALL SERVICES group is specified here. Click **Add User or Group**.



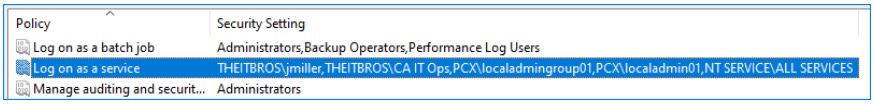
3. Specify the groups or users (domain or local) to grant "Log on as a service" rights and click **OK**. You can add local or domain users and groups.



4. Click **OK** to save the list.



5. Wait for the Group Policy update or run **gpupdate /force** to force the update immediately.

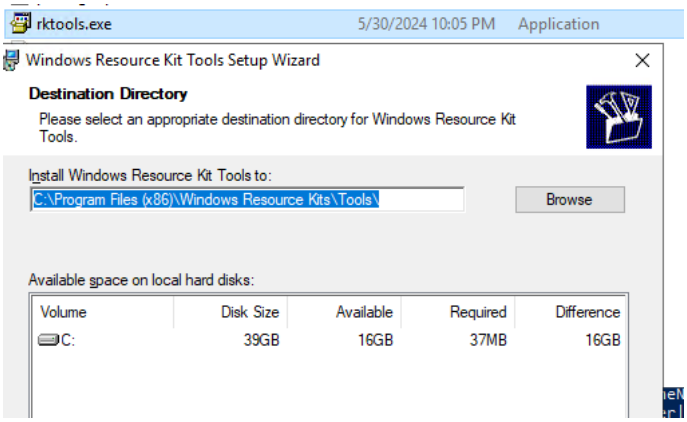


Managing "Log on as a service" Permission with PowerShell

You can change the settings for the 'Log on as a service' policy from the PowerShell command line.

The easiest way to grant 'Log on as a service' permissions is to use the **NTRights.exe** command line tool, which is part of the *Windows Server 2003 Resource Toolkit*. Unfortunately, the direct download link for this package has been removed from the Microsoft site, but you can download it from WebArchive.

Install the Resource Toolkit on the computer and run a command prompt as an Administrator.

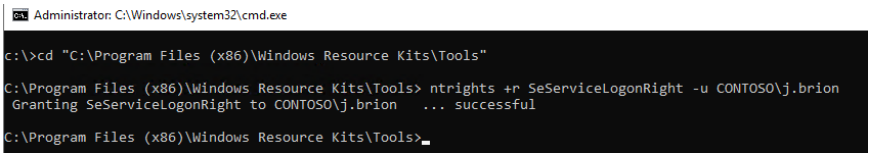


Navigate to the directory:

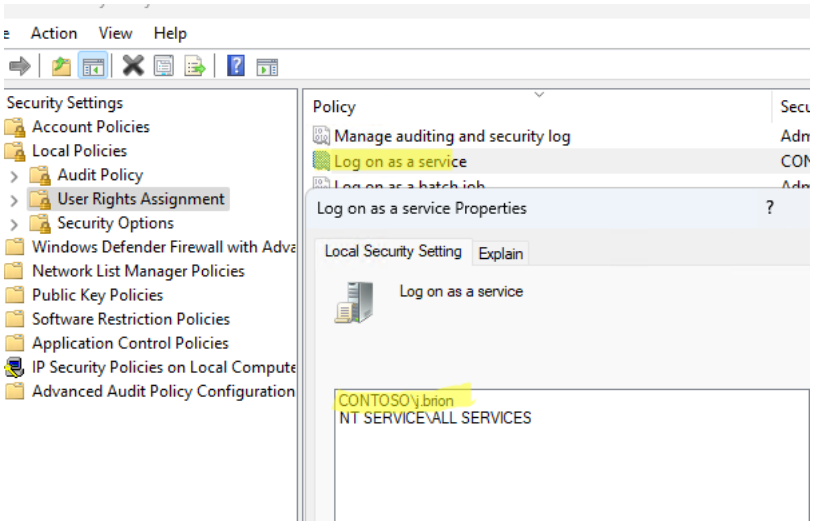
```
cd "C:\Program Files (x86)\Windows Resource Kits\Tools"
```

To grant the user CONTOSO\j.brion Log on service privileges, run the command:

```
ntrights +r SeServiceLogonRight -u CONTOSO\j.brion
```



Check that the user has been assigned rights in the Local Security Policy snap-in.



To remove a user from a policy, run:

```
ntrights -r SeServiceLogonRight -u CONTOSO\j.brion
```

To manage permissions, you can also use the built-in **secedit.exe** tool**.** We have created three PowerShell script wrappers for the secedit.exe tool that you can download from the following links

- **[PS-Manage-Log-On-As-A-Service]** — The public GitHub repository.
- **[Get-ServiceLogonRight.ps1]** — A script to retrieve the local machine's current "Log on as a service" rights.
- **[Add-ServiceLogonRight.ps1]** — A script to add a user and group to the "Log on as a service" policy.
- **[Remove-ServiceLogonRight.ps1]** — A script to remove a user or group from the current "Log on as a service" policy.

List the current accounts in the "Log on as a service" policy:

```
.\Get-ServiceLogonRight.ps1
```

Add a user or group to the "Log on as a service" policy:

```
.\Add-ServiceLogonRight.ps1 -UserOrGroup <DOMAIN\group>
```

```
[PS] .\Get-ServiceLogonRight.ps1
localadmin01
localadmingroup01
THEITBROS\CA IT Ops
THEITBROS\jmiller
NT SERVICE\ALL SERVICES
[PS] _
```

```
[PS] .\Add-ServiceLogonRight.ps1 -UserOrGroup localadmin02

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
[PS] .\Add-ServiceLogonRight.ps1 -UserOrGroup localadmingroup02

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
[PS] .\Add-ServiceLogonRight.ps1 -UserOrGroup 'THEITBROS\ebrown'

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
[PS] .\Add-ServiceLogonRight.ps1 -UserOrGroup 'THEITBROS\CA Server Admins'

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
[PS] _
```

Remove a user from a policy:

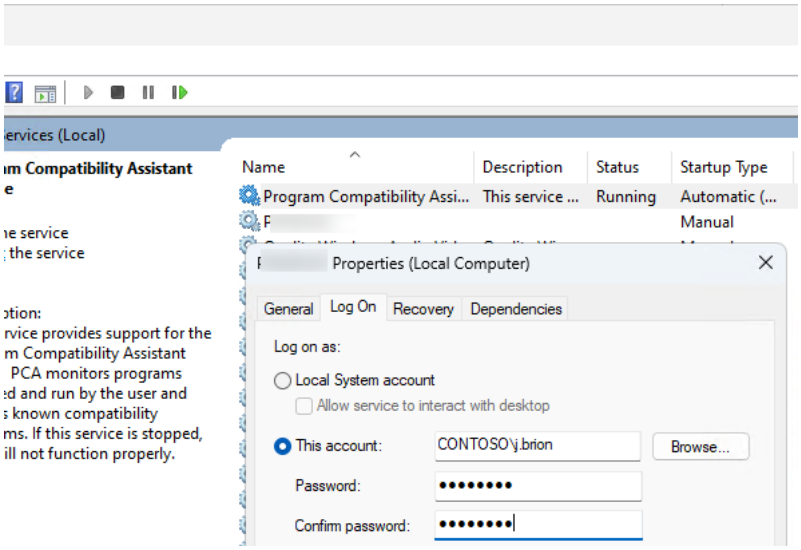
```
# Remove a local user

.\Remove-ServiceLogonRight.ps1 -UserOrGroup localadmin02
```

How to configure a Windows service to run as a specific user

Now you can reconfigure your Windows service to run in a user context.

1. Open the service management console (services.msc).
2. Find the service and open its properties.
3. Got to the **Log on** tab > select **This account**.

4. Select account name and type it password.



5. Try starting the service to check if it works correctly in the user's context.

An error may occur when starting the service:

> Could not start the <service name> service on Local Computer.
>
> Error 1069: The service did not start due to a logon failure.

This indicates that you have entered a wrong username or password.

Note that for the user account used to start the service, we recommend you to enable the Password never expires checkbox in the account properties.