Configure and deploy group policies - Microsoft dev tunnels

By plequere-ms

Archived: 2026-04-06 02:05:59 UTC

Configure and deploy Group Policy Administrative Templates for Dev Tunnels

In this article

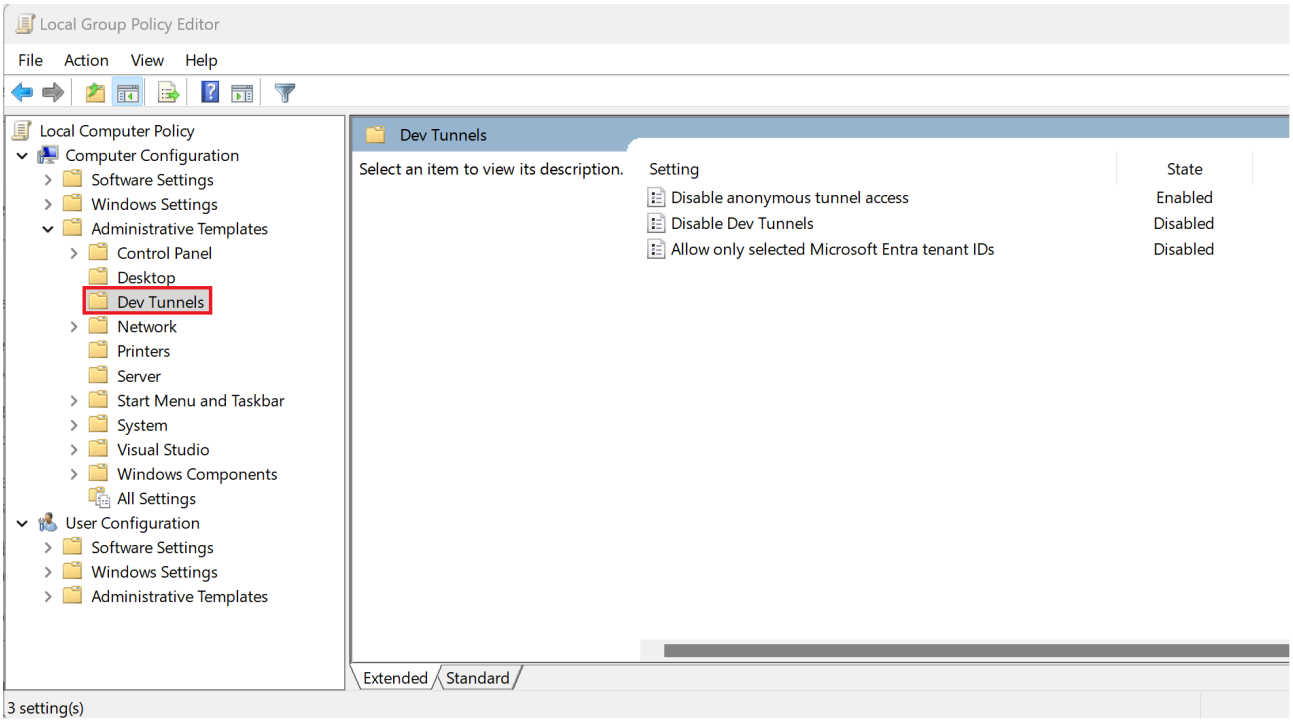
IT Administrators in organizations may want to control certain aspects of Dev Tunnels to achieve consistency or compliance across their organization. An easy way to accomplish this level of control is to configure and then deploy group policy settings to the client machines. The Dev Tunnels in Visual Studio, port forwarding built into Visual Studio Code, the Visual Studio Code Remote - Tunnels extension, and `devtunnel` CLI policies are consolidated in the Administrator Template files (ADMX/ADML) for Dev Tunnels.

In this quickstart, you'll learn how to configure and deploy Dev Tunnels group policy settings across your organization.

- Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 8.1, Windows 10, Windows 11
- Active Directory
- Access to Local Group Policy Editor

Note

The policies are only applicable on Windows machines.



- **Disable anonymous tunnel access**: Disallow anonymous tunnel access. Enabling this policy enforces users to select either private or organization for tunnel access. This means users cannot connect to an existing tunnel with anonymous access control, host an existing tunnel with anonymous access control, or add anonymous access to existing or new tunnels.
- **Disable Dev Tunnels**: Disallow users from using the Dev Tunnels service. All commands, with few exceptions, should be denied access when this policy is enabled. Exceptions: unset, echo, ping, and user.
- **Allow only selected Microsoft Entra tenant IDs**: Users must authenticate within the given tenant list to access Dev Tunnels. When enabling this policy, multiple tenant IDs can be added by using a semicolon or comma to separate each. All commands, with few exceptions, should be denied access when this policy is enabled and the user's tenant ID isn't in the list of allowed tenant IDs. Exceptions: unset, echo, ping, and user. Follow the steps in this article to find your Microsoft Entra tenant ID.

1. Head over to the Microsoft Download Center and download the Administrator Template files (ADMX/ADML) for Dev Tunnels.
2. Navigate to the `C:\Windows\PolicyDefinitions` folder and add the `TunnelsPolicies.admx` file.
3. Navigate to the `C:\Windows\PolicyDefinitions\en-US` folder and add the `TunnelsPolicies.adml` file.

1. Open Command Prompt and run `gpupdate /force` to ensure the policy files are configured.
2. Open the Windows Local Group Policy Editor.
3. Navigate to Computer Configuration > Administrative Templates > Dev Tunnels.
4. Apply the desired policy changes.

Additional resources

Training

- Last updated on 02/12/2026
