

Deploying Coro Agent with Windows Server GPO

This guide describes how to deploy the Coro Agent to your Windows endpoints through Windows Server Group Policy Object (GPO) manager.

To configure a new GPO, perform one of the following processes.

Choose from:

- **Using the PowerShell script provided by Coro Support**
- **Using the Agent installer file downloaded from the Coro console**

Important

GPOs check for the existence of application IDs in the endpoint device registry to determine installation status. If the ID does not exist, an app is pushed to the device. When installed apps like Coro update themselves to a newer version, the ID can change. Consequently, a GPO can attempt to reinstall the original app, which can lead to corruption or uninstallation of the later version. Coro recommends disabling the GPO after deployment to avoid this scenario.

Alternatively, create a new organizational unit (OU) in Active Directory and add endpoint devices that do not already have the Coro Agent installed. Then, link the GPO to that OU so that it installs Coro Agent only on those devices.

Using the PowerShell script provided by Coro Support

1. On your Windows server device, access the *Group Policy Management* app. Then, either create a new GPO or edit your preferred existing policy.

Make a note of the ID of the policy. For example: