Manage Trusted Publishers

By Archiveddocs

Archived: 2026-04-05 20:08:36 UTC

Applies To: Windows 7, Windows Server 2008 R2

Software signing is being used by a growing number of software publishers and application developers to verify that their applications come from a trusted source. However, many users do not understand or pay little attention to the signing certificates associated with applications that they install.

The policy settings in the **Trusted Publishers** tab of the certificate path validation policy allows administrators to control which certificates can be accepted as coming from a trusted publisher.

This topic includes procedures for the following tasks:

- Configuring the trusted publishers policy settings for a local computer
- Configuring the trusted publishers policy settings for a domain
- Allowing only administrators to manage certificates used for code signing for a local computer
- Allowing only administrators to manage certificates used for code signing for a domain

Configuring the trusted publishers policy settings for a local computer

Administrators is the minimum group membership required to complete this procedure.

To configure the trusted publishers policy settings for a local computer

1. Click **Start**, type **gpedit.msc** in the **Search programs and files** box, and then press ENTER.
2. In the console tree under **Local Computer Policy\Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.
3. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.
4. Select the **Define these policy settings** check box, select the policy settings that you want to apply, and then click **OK** to apply the new settings.

Configuring the trusted publishers policy settings for a domain

Domain Admins is the minimum group membership required to complete this procedure.

To configure the trusted publishers policy settings for a domain

1. Click **Start**, point to **Administrative Tools**, and click **Server Manager**.
2. Under **Features Summary**, click **Add Features**. Select the **Group Policy Management** check box, click **Next**, and then click **Install**.
3. After the **Installation Results** page shows that the installation of the Group Policy Management Console (GPMC) was successful, click **Close**.
4. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
5. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** Group Policy object (GPO) that you want to edit.
6. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
7. In the console tree under **Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.
8. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.
9. Select the **Define these policy settings** check box, select the policy settings that you want to apply, and then click **OK** to apply the new settings.

Allowing only administrators to manage certificates used for code signing for a local computer

Administrators is the minimum group membership required to complete this procedure.

To allow only administrators to manage certificates used for code signing for a local computer

1. Click **Start**, type **gpedit.msc** in the **Search programs and files**, and then press ENTER.
2. In the console tree under **Default Domain Policy** or **Local Computer Policy**, double-click **Computer Configuration**, **Windows Settings**, and **Security Settings**, and then click **Public Key Policies**.
3. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.
4. Select the **Define these policy settings** check box.
5. Under **Trusted publisher management**, click **Allow only all administrators to manage Trusted Publishers**, and then click **OK** to apply the new settings.

Allowing only administrators to manage certificates used for code signing for a domain

Domain Admins is the minimum group membership required to complete this procedure.

To allow only administrators to manage certificates used for code signing for a domain

1. Click **Start**, point to **Administrative Tools**, and click **Server Manager**.
2. Under **Features Summary**, click **Add Features**. Select the **Group Policy Management** check box, click **Next**, and then click **Install**.
3. After the **Installation Results** page shows that the installation of the GPMC was successful, click **Close**.
4. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
5. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** GPO that you want to edit.
6. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
7. In the console tree under **Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.
8. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.
9. Select the **Define these policy settings** check box, implement the changes you want, and then click **OK** to apply the new settings.

Additional references

- Certificate Path Validation

Source: https://technet.microsoft.com/en-us/library/cc733026.aspx