Microsoft TechNet

Control Printer Driver Installation Security

Applies To: Windows 7, Windows Server 2008 R2

The default security settings for Windows 7 and Windows Server 2008 R2 allow users who are not members of the local **Administrators** group to install only trustworthy printer drivers, such as those provided with Windows or in digitally signed printer-driver packages. This helps to ensure that users do not install untested or unreliable printer drivers or drivers that have been modified to contain malicious code (malware). However, it means that sometimes users cannot install the appropriate driver for a shared printer, even if the driver has been tested and approved in your environment.

The following sections provide information about how to allow users who are not members of the local **Administrators** group to connect to a print server and install printer drivers that are hosted by the server:

- Installing printer-driver packages on the print server
- Using Group Policy to deploy printer connections to users or computers
- Using Group Policy to modify printer driver security settings

Installing printer-driver packages on the print server

Printer-driver packages are digitally signed printer drivers that install all the components of the driver to the driver store on client computers (if the server and the client computers are running Windows 7 Windows Server 2008 R2). Additionally, using printer-driver packages on a print server that is running Windows 7 or Windows Server 2008 R2 enables users who are not members of the local **Administrators** group to connect to the print server and install or receive updated printer drivers.

To use printer-driver packages, on a print server that is running Windows Server 2008 R2 or Windows 7, download and install the appropriate printer-driver packages from the printer vendor.

Note

You can also download and install printer-driver packages from a print server to client computers that are running Windows Server 2003, Windows XP, and Windows 2000. However, the client computers do not check the driver's digital signature or install all components of the driver into the driver store because the client operating system does not support these features.

Using Group Policy to deploy printer connections to users or computers

Print Management can be used with Group Policy to automatically add printer connections to the Printers folder, without requiring the user to have local Administrator privileges. For more information, see Deploying Printers by Using Group Policy [http://technet.microsoft.com/en-us/library/cc754699.aspx] .

Using Group Policy to modify printer driver security settings

You can use the Point and Print Restrictions Group Policy setting to control how users can install printer drivers from print servers. You can use this setting to permit users to connect to only specific print servers that you trust. Because this setting prevents users from connecting to other print servers that could potentially host malicious or untested printer drivers, you can disable printer driver installation warning messages without adversely compromising security.

Carefully evaluate your users' printing needs before limiting which print servers they can connect to. If users occasionally need to connect to shared printers in a branch office or another department, make sure to include those printer servers on the list (if you trust the printer drivers that are installed on the servers).

You can also use the Point and Print Restrictions setting to disable warning prompts entirely, although this setting disables the enhanced printer driver installation security of Windows 7 and Windows Server 2008 R2 for these users.

Note

> The following procedure assumes that you are using the version of the Group Policy Management Console (GPMC) that is included with Windows Server 2008 R2. To install GPMC on Windows Server 2008 R2, use the Add Features Wizard of Server Manager. If you are using a different version of GPMC, the steps might vary slightly.

To modify the Point and Print Restrictions setting

1. Open the Group Policy Management Console (GPMC).
2. In the GPMC console tree, navigate to the domain or organizational unit (OU) that stores the user accounts for which you want to modify printer driver security settings.
3. Right-click the appropriate domain or OU, click **Create a GPO in this domain, and Link it here**, type a name for the new GPO, and then click **OK**.
4. Right-click the GPO that you created and then click **Edit**.
5. In the Group Policy Management Editor window, click **Computer Configuration**, click **Policies**, click **Administrative Templates**, and then click **Printers**.
6. Right-click **Point and Print Restrictions**, and then click **Edit**.

> **Note**
>
> The **Point and Print Restrictions** setting can also be found under **User Configuration\Policies\Administrative Templates\Control Panel\Printers**. This policy is ignored by Windows 7 and Windows Server 2008 R2, but is enforced by earlier editions of the operation system including versions Windows XP with SP1, Windows Server 2003 with SP1, and Windows Server 2008. We recommend that you change this policy setting in both locations so that all down-level clients have a consistent experience.

To permit users to connect only to specific print servers that you trust

1. In the **Point and Print Restrictions** dialog box, click **Enabled**.
2. Select the **Users can only point and print to these servers** check box if it is not already selected.
3. In the text box, type the fully qualified server names to which you want to allow users to connect. Separate each name with a semi-colon.
4. In the **When installing drivers for a new connection** box, choose **Do not show warning or elevation prompt**.
5. In the **When updating drivers for an existing connection** box, choose **Show warning only**.
6. Click **OK**.

> **Note**
>
> To disable driver installation warning messages and elevation prompts on computers that are running Windows 7 and Windows Server 2008 R2, in the **Point and Print Restrictions** dialog box, click **Disabled**, and then click **OK**. This setting disables the enhanced printer driver installation security of Windows 7 and Windows Server 2008 R2.

Additional considerations

- You must have administrative credentials to perform this task.

Additional references

- Managing Printers and Print Servers [http://technet.microsoft.com/en-us/library/cc754769.aspx]
- Printing Architecture and Driver Support (http://go.microsoft.com/fwlink/?LinkID=92657 [http://go.microsoft.com/fwlink/?LinkID=92657])

Tags: bflat code system.xml

Community Content