Microsoft Windows

Point and Print Security on Windows Vista

Updated June 12, 2008

Abstract

This paper provides system administrators with the best practices for configuring Point and Print security on Windows Vista client computers in environments where print servers and client computers might have different versions of Windows.

This information applies for the following operating systems:

Windows Vista

References and resources discussed in this paper are listed at the end of this paper.

Contents

Introduction 3
Point and Print Security Best Practices....3
- Use Deployed Printers 4
- Use the Default Security Settings....4
- Point and Print to Specific Print Servers Only 6
- Use Printers with In-Box Drivers Only 7
- Use Windows XP-Level Security....8
- Use Printers with Printer Driver Packages 8

Point and Print Restrictions Group Policy Setting 8
Additional Information 11

Disclaimer

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

Document History

Date	Change
June 12, 2008	Updated website information
August 6, 2006	First publication

Introduction

Microsoft Windows Vista™ is the most secure version of Microsoft® Windows® to date. As a part of this improved security, Windows notifies users and asks for their permission before it allows a change to the operating system such as installing software or a printer driver.

Point and Print is the Windows feature that automatically downloads and installs a printer driver when a user connects to a shared printer. Point and Print also updates the printer driver on the client computer when the driver configuration is updated on the print server.

The Point and Print Restrictions group policy setting has been updated to help you manage the improved security of the Point and Print feature in Windows Vista. This paper describes the best practices for configuring Point and Print security on Windows Vista client computers in environments where the print servers are running earlier versions of Windows. It also describes the user experience for the options that have been added to the Point and Print Restrictions group policy setting in Windows Vista.

Point and Print Security Best Practices

Point and Print security is controlled by group policy settings. You can configure the group policy settings that manage Point and Print security by using the group policy object editor (gpedit.msc). Figure 1 shows the location of the Point and Print Restrictions group policy setting in the group policy object editor.

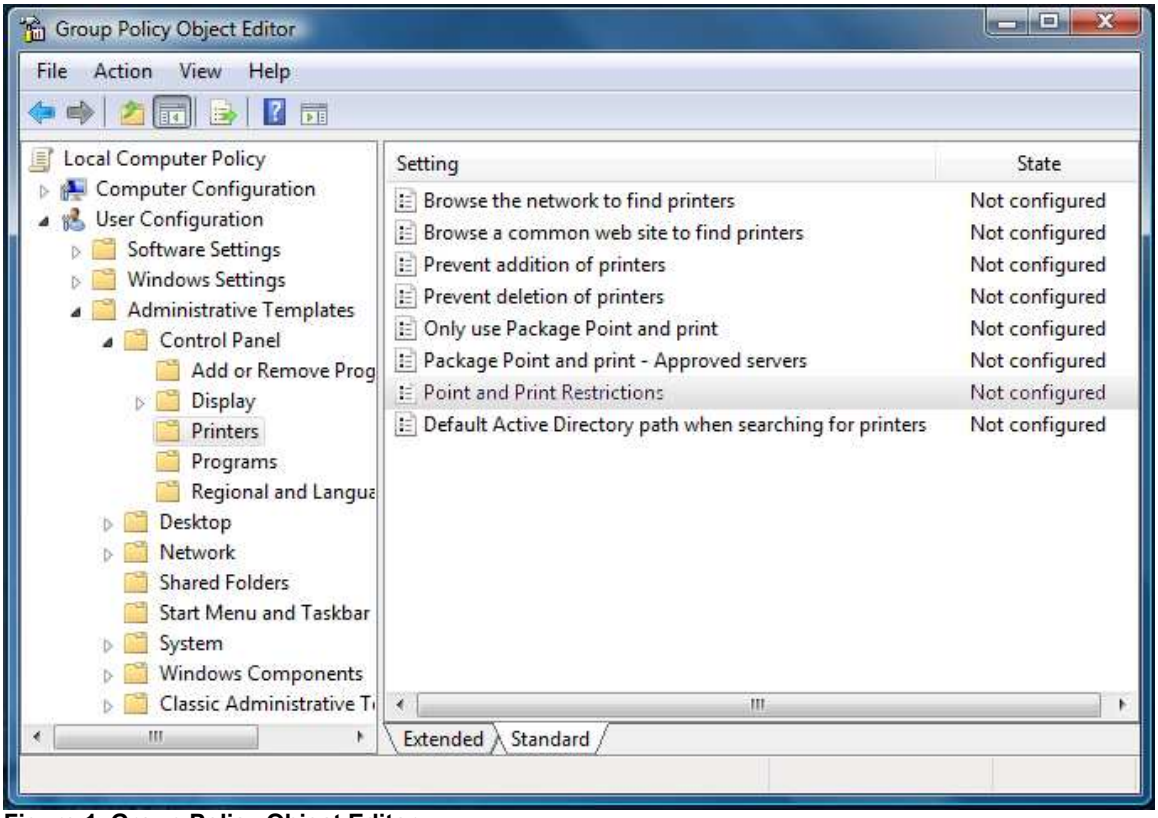

Figure 1. Group Policy Object Editor

The following sections describe different ways to configure Point and Print security. These options allow you to optimize the user experience and security for your specific environment. Be sure to consider how other group policy settings might interact with the Point and Print Restrictions group policy setting when you configure Point and Print security. Incorrect configuration of printing Group Policy settings can prevent clients from printing.

Use Deployed Printers

You can deploy printers to groups of users by using a group policy object. This is the most secure practice and is useful in small and large organizations or anywhere computers and printers are organized by function, workgroup, or location.

With deployed printers, you define the printers for the user or group and group policy installs the printers on the client computers that are managed by group policy. If you also restrict the users from installing printers on their computer, the client computers can use only those printers that you deploy in the group policy.

Configuration

Open the Print Management console from the **Administrative Tools** menu to create the group policy object and define the printers to deploy. The procedure to deploy printers is described in the Print Management console help under the *Deploy printers by using Group Policy* topic.

After you configure the deployed printers, configure the Point and Print Restrictions group policy setting as follows:

- Point and Print Restrictions: **Enabled**
- When updating drivers for an existing connection: **Show Warning Only**

Use the default value for all other settings.

User Experience

The deployed printers are automatically installed on the client computer when the group policy settings are refreshed or when the user logs on. The user will not see any warning messages when the printers are installed for the first time. If you update the printer configuration on the print server after the deployed printers have been installed on the client computer, the user will see the warning message shown in figure 2. This message informs the user that Point and Print must update the driver or configuration for the printer. The user can click **Install printer** in the warning dialog box and the driver will be updated, even if they do not have administrator-level privileges.

Use the Default Security Settings

The default printer security settings of Window Vista provide a high degree of security and warn the user before software is installed on the client computer. The default security settings also restrict software installation to only users with administrator-level privileges.

With the default security, trustworthy printer drivers, such as those provided in-box or in printer driver packages, can be installed by a user without administrator-level privileges. In-box printer drivers are the printer drivers that are delivered with the Windows operating system. See the section titled “Use Printers with In-Box Drivers Only” later in this paper for more information on using in-box printer drivers. See the section titled “Use Printers with Printer Driver Packages” later in this paper for more information on printer driver packages.

Configuration

No additional configuration is necessary.

User Experience

If a user connects to a shared printer and the required printer driver is not on their computer, or if the driver for an installed printer has been updated on the print server, Point and Print begins the installation process.

First, the user sees a warning message similar to figure 2.

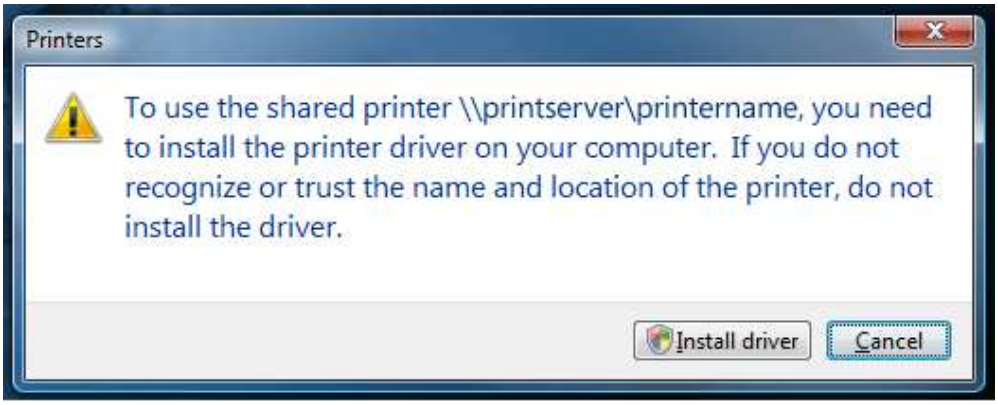

Figure 2. Printer Connection Warning Dialog Box

After a user with administrator-level privileges clicks Install driver, a dialog box similar to figure 3 is displayed to prompt the user for permission to continue.

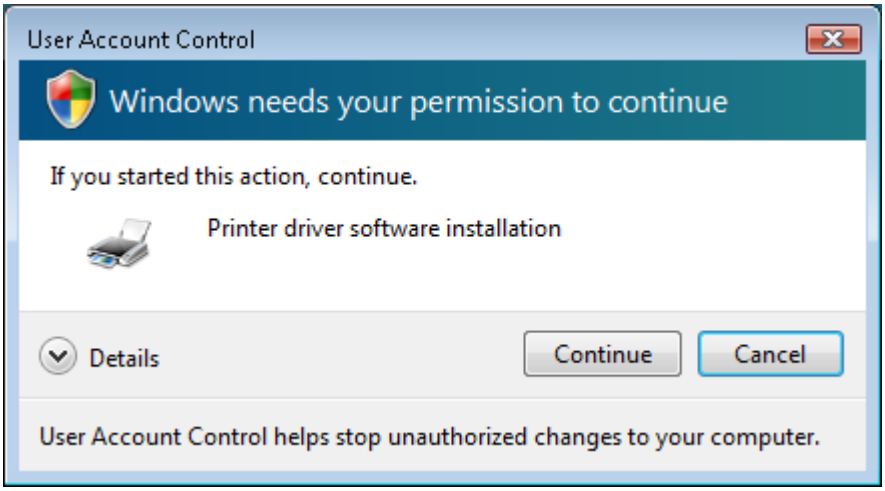

Figure 3. User Account Control Dialog Box

After a user *without* administrator-level privileges clicks **Install driver**, a dialog box similar to figure 4 is displayed. The user must be able to enter a password for an account that has administrator-level privileges in this dialog box or the printer installation will fail.

Figure 4. User Account Control Dialog Box for Administrator Password

Point and Print to Specific Print Servers Only

The Point and Print Restrictions group policy setting enables you to limit users to connect only to specific print servers. With this setting, you could, for example, allow users to connect only to printers on print servers that you manage. Because this group policy setting prevents users from connecting to any other print servers, you can disable the warning messages that would otherwise be displayed.

Configuration

Configure the Point and Print Restrictions group policy setting in the group policy object editor and set:

- Point and Print Restrictions: **Enabled**.
- Users can only point and print to these servers: **Checked.**
- Enter the fully qualified server names in the text box and separate each name with a semi-colon.
- When installing drivers for a new connection: **Do not show warning or elevation prompt**.
- When updating drivers for an existing connection: **Show warning only**.

Figure 5 shows the Point and Print Restrictions group policy setting that allows users to Point and Print to print servers: PrintServer1 and PrintServer2 in contoso.com.

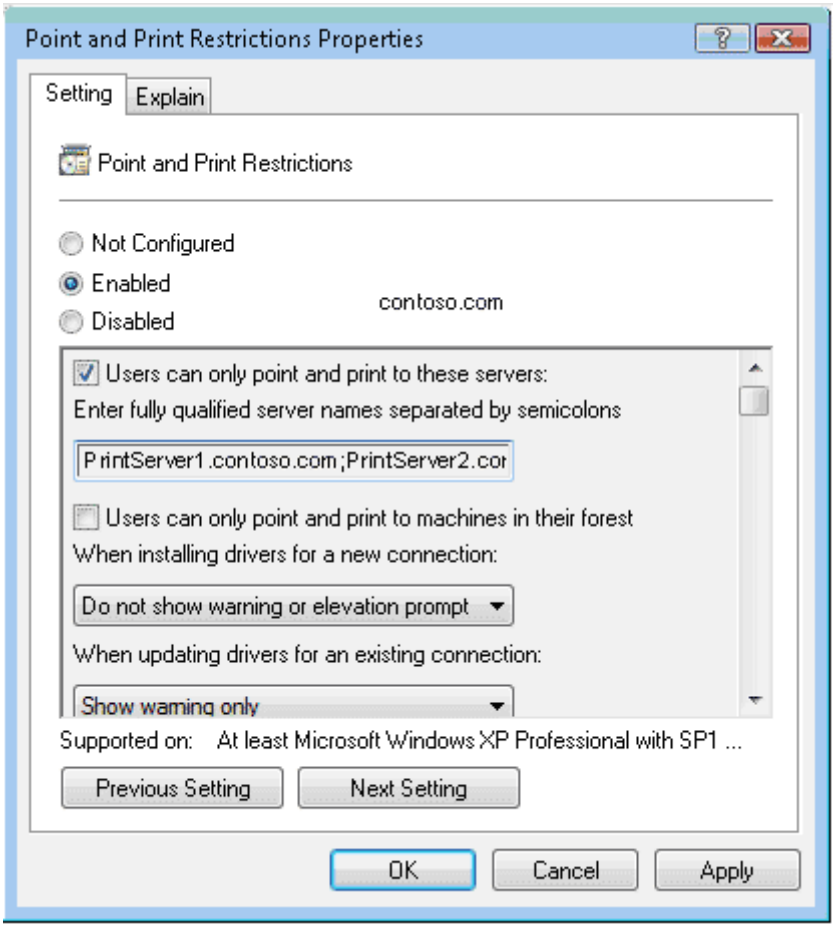

Figure 5. Point and Print Restrictions Properties for Specific Print Servers

User Experience

When a user connects to a printer that is shared on a print server listed in the Point and Print Restrictions group policy setting, Point and Print installs the necessary printer drivers and does not require any additional user interaction. The user will, however, see a warning message similar to figure 3 before Point and Print updates the driver or printer configuration on the client computer. The user will not be able to connect to print server that is not listed in the group policy setting.

Use Printers with In-Box Drivers Only

Printers with in-box printer drivers can be installed without downloading any software from the print server. If all printers hosted on your print servers have in-box printer drivers, users will not see any warning messages when they connect to a shared printer.

Configuration

Verify that all shared printers have in-box drivers for the versions of Windows that are installed on the client computers in your enterprise.

User Experience

When the user connects to a shared printer that has an in-box printer driver, the printer driver will be installed by using software that is available on the client

computer. Point and Print will not download any software and the user will not see any warning dialog boxes.

Use Windows XP-Level Security

You can use the Point and Print Restrictions group policy setting to provide a Windows Vista client computer with the same level of Point and Print security that it had with Windows XP.

Configuration

Configure the Point and Print Restrictions Properties group policy setting and set:

- Point and Print Restrictions: **Disabled**.

Use the default value for all other settings.

User Experience

Users will not see any additional warning messages when they connect to a shared printer and Point and Print installs a new printer driver or when Point and Print updates the printer driver for an existing connection.

Use Printers with Printer Driver Packages

Windows Vista introduces Package Point and Print which works like Point and Print found on earlier versions of Windows but uses a secure group of files called a printer driver package. Printer driver packages are signed, secure, and they can be installed by users who do not have administrator-level privileges.

Package Point and Print is not supported on versions of Windows prior to Windows Vista. This option can only be used in environments with shared printers that are hosted on print servers running Windows Vista or Microsoft Windows Server® code name "Longhorn."

Configuration

Confirm that the shared printers are hosted on Windows Vista or Windows Server “Longhorn” computers. Confirm that the shared printers use a printer driver package by contacting the printer vendor. This option does not require a group policy setting.

User Experience

Because printer driver packages are secure, they are downloaded and installed without presenting any warning messages to the user.

Point and Print Restrictions Group Policy Setting

Figure 6 highlights the new options that were added to the Point and Print Restrictions group policy setting in Windows Vista.

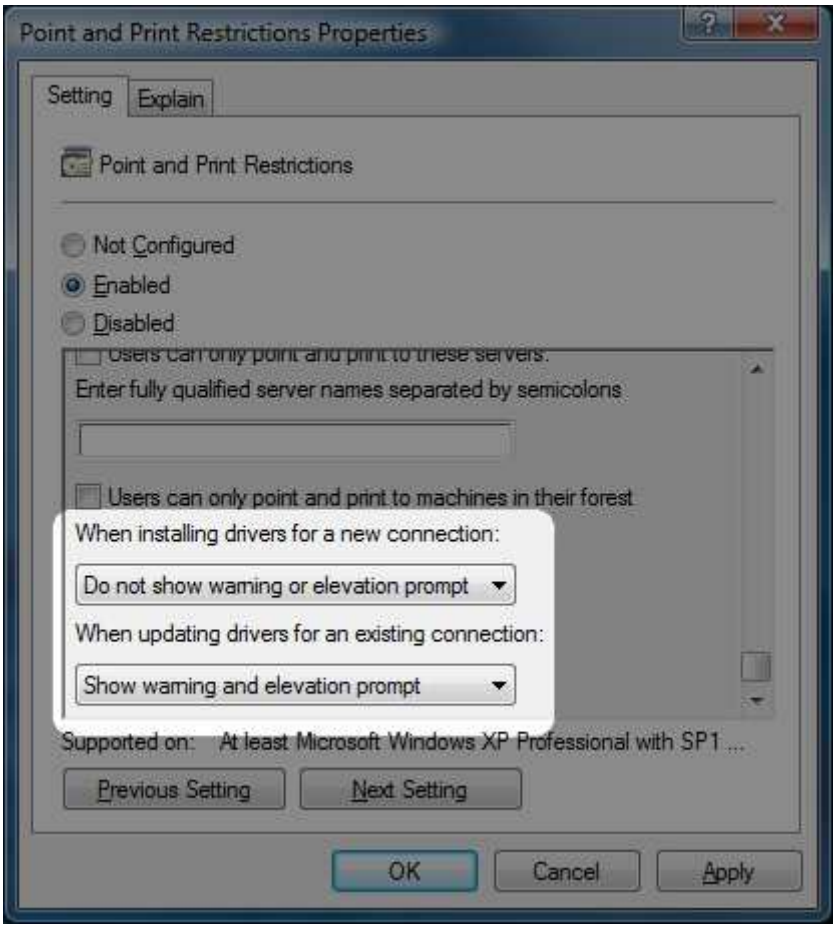

Figure 6. New Options of the Point and Print Restrictions Group Policy Setting

By default, Windows Vista security shows two dialog boxes when you install a printer that requires a printer driver to be downloaded and installed:

- a warning message (figure 7)
- an elevation prompt (figure 8 or 9)

If the user installs a printer with a printer driver that has already been installed successfully on their Windows Vista client computer then these dialog boxes will not appear.

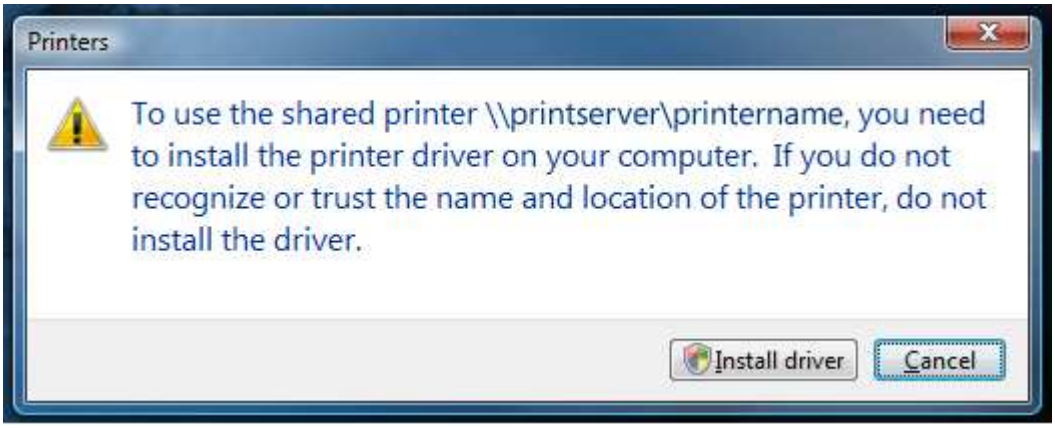

Figure 7. Point and Print Warning Dialog Box

After the dialog box in figure 7, if the user does not have administrator-level privileges, they will see a dialog box that is similar to figure 8. If the user has administrator-level privileges, they will see a dialog box that is similar to figure 9.

Figure 8. Printer Driver Software Account Elevation Dialog Box

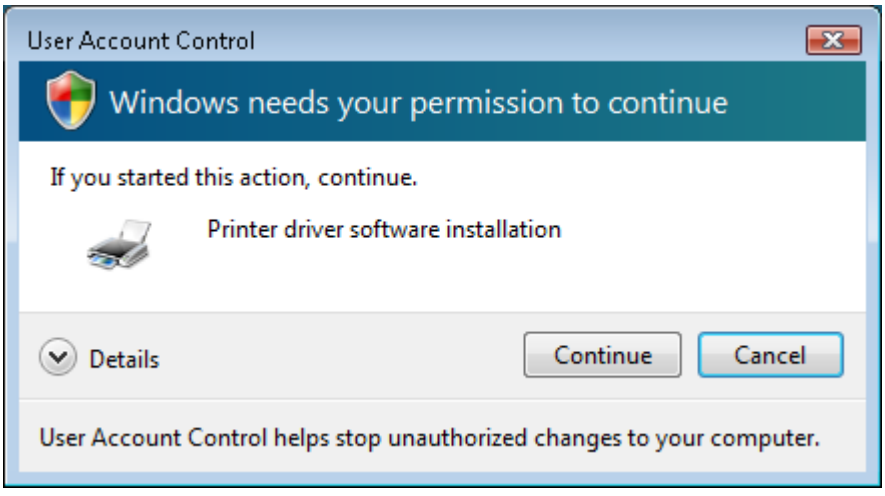

Figure 9. Printer Driver Software Installation Warning Dialog Box

Using the Point and Print Restrictions group policy setting, you can enable or disable these dialog boxes for the initial driver installation and its subsequent update by selecting one of the following configuration options:

- Show warning and elevation prompt
- Show warning only
- Do not show warning or elevation prompt

Note that the *Show warning only* option is only available when updating drivers for an existing connection.

Show warning and elevation prompt

This is the default setting. When selected, the dialog box shown in figure 7 and depending on the privilege level of the user, either figure 8 or 9 will be displayed. This option is available when installing drivers for a new connection and when updating drivers for an existing connection.

Show warning only

When this option is selected, only the warning dialog box shown in figure 7 will be displayed when Point and Print must update a driver for an existing connection. This option is available only when updating drivers for an existing connection.

Do not show warning or elevation prompt

When this option is selected, no warning dialog boxes are displayed. This option provides the Windows XP user experience for Point and Print and is available when installing drivers for a new connection and when updating drivers for an existing connection.

Additional Information

Additional information on the Point and Print Restrictions group policy setting is at http://go.microsoft.com/fwlink/?LinkId=73628

Additional information on print servers and printing in Windows Server 2003 is at http://go.microsoft.com/fwlink/?LinkId=73629 and at http://go.microsoft.com/fwlink/?LinkId=73630

Additional information on other print topics is at http://go.microsoft.com/fwlink/?LinkId=73631

Updated June 12, 2008