

User Rights on a Print Console Workstation

2002-09-20

Creo Inc.
3700 Gilmore Way
Burnaby, BC
Canada V5G 4M1
(604) 451-2700

Copyright 2002 Creo Inc. All rights reserved.

Revision History

Revision	Date	Author	Comments
1st	Sept, 2002	A.Blignaut/J.Delgado	Draft release for testing

CONTENTS

Revision History i

1. Background Information 1
   - 1.1 Workstation User Rights 1
   - 1.2 Shared DLLs 1
   - 1.3 Prinergy entries to the system path 1

2. The Solution 1
   - 2.1 Customer Account Specifications 2
   - 2.2 Disable Windows Installer 3
   - 2.3 Disable Add/Remove Programs 5

1. BACKGROUND INFORMATION

Print Console was designed to: be installed using the Administrator user account and launched using the PCOperator user account. As Prinergy UADM and Service Shell applications were added to the workstation this scheme was broken.

Up to and including Print Console version 3.0, Prinergy 2.0 and earlier, and Service Shell 2.3 and earlier, the following problems were encountered.

1.1 Workstation User Rights

Although Print Console can operate with the rights set to **Administrator** or **PCOperator**, Prinergy UADM and Service Shell ServiceMonitor executables require that the rights be set to **Administrator**. This setting is a security concern for many customers.

1.2 Shared DLLs

These earlier versions of software programs share common DLL files, for example – levt.dll. But the version of levt.dll that Prinergy requires is different from the version of levt.dll that Print Console and Service Shell require. This creates confusion and failures where the wrong version of the same file has been called up by either program.

1.3 Prinergy entries to the system path

Depending on the order of installation of the applications, the Prinergy entries to the system path may be located after Service Shell's and/or Print Console's. This causes the wrong executables and dll's to be launched by Prinergy.

2. THE SOLUTION

Run the applications under the **PCOperator** user account – this account has Power User rights. To take advantage of this solution, the application versions shown below must be used.

- Microsoft Windows 2000 Server or Professional
- Print Console version 3.1 or higher
- Prinergy version 2.1 or higher
- Service Shell version 2.4 or higher

The following changes have been made to these applications:

- Print Console no longer requires the levt.dll
- Both, Service Shell Client and Service Shell Host can now run with Power User rights. The ServiceMonitor executable, which adds the LaunchServiceHost service, has also been changed to run with Power User rights.
    - Service Shell installer adds and removes LaunchServiceHost.exe service when the Service Shell is installed and removed, respectively.
    - ServiceMonitor.exe only starts and stops LaunchServiceHost.exe service at startup and shutdown respectively.
- Prinergy has made changes to the system path and to the way they launch their executables

Note: When logged on as **PCOperator**, the network icon in bottom-right task bar does not show.

2.1 Customer Account Specifications

Customer required account specifications include:

1. user cannot change password
2. user password never expires
3. user cannot Add/Remove programs
4. user cannot modify system registry

The first two requirements are satisfied by the way in which Print Console creates the PCOperator account during installation. PCOperator, being a Power User account, also satisfies the fourth requirement.

As PCOperator, you can add and remove programs that do not:

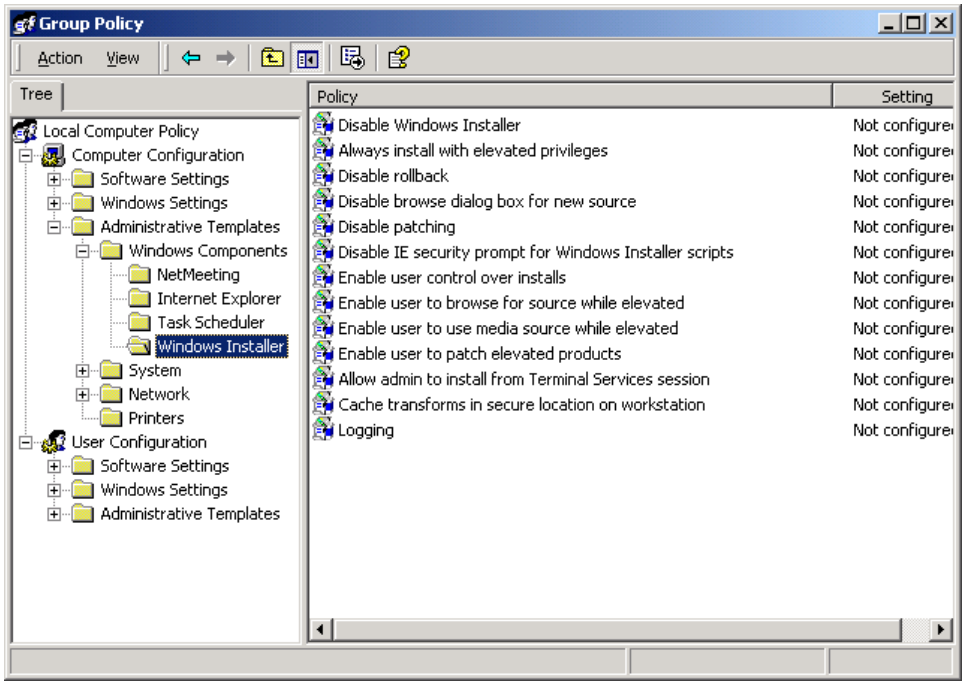
- modify system registry
- modify any application registry key under the hive HKEY_LOCAL_MACHINE
- create user accounts with similar or lower user rights

Unfortunately, the Print Console installer cannot implement a solution to the third requirement. Therefore, the **Windows Installer** and **Add/Remove Programs** utility must be disabled manually.

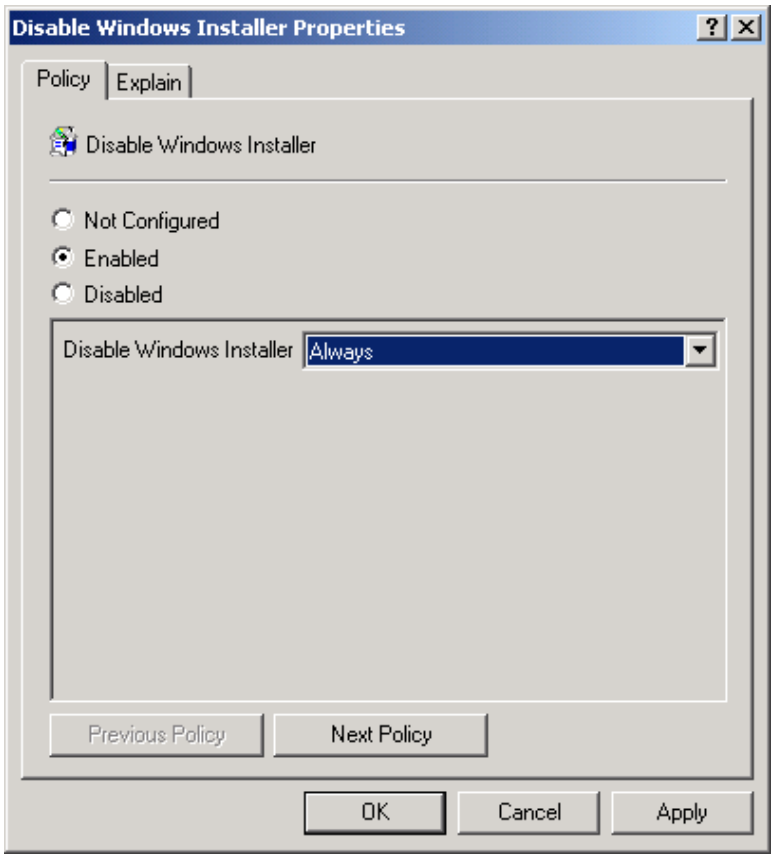
2.2 Disable Windows Installer

1. Login to the workstation as Administrator
2. Disable Windows installer for all users except for the Administrator. This will not stop a user from copying executables to the hard drive, but it will prevent him/her from installing programs, which require registering components or modifying system folders. The steps to disable the Windows installer are:

    - Run gpedit.msc from Start--->Run menu, the Group Policy MMC will be displayed.
    - Expand Computer Configurations tree
    - Expand Administrative Templates
    - Expand Windows Components
    - Highlight Windows Installer

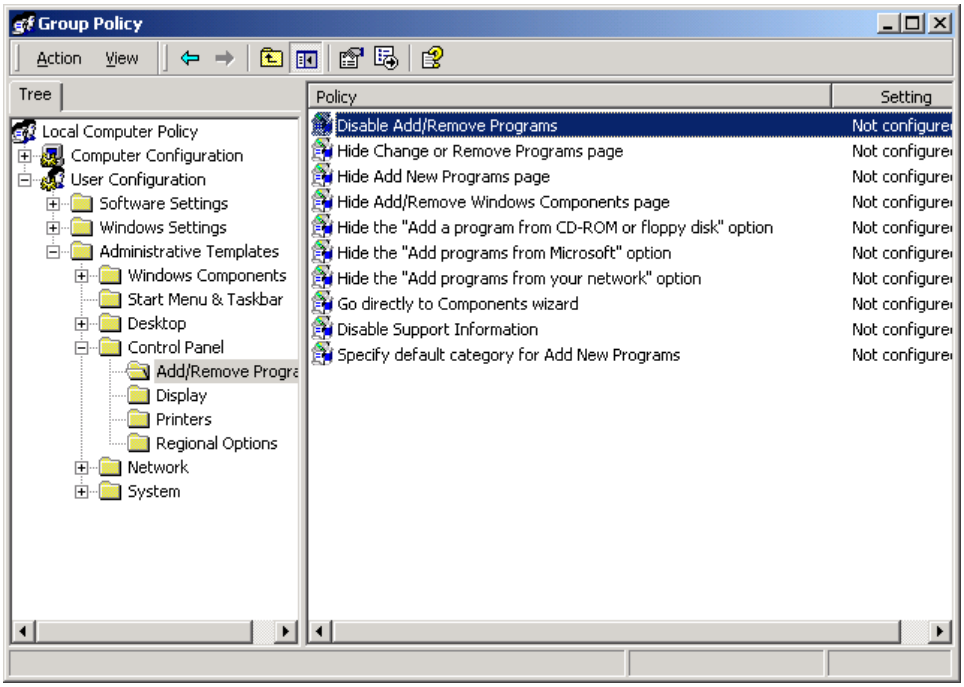


- In the right-hand pane, double-click on **Disable Windows Installer**.
- Select the **Enable** radio button and set the **Disable Windows Installer** to **Always**.


Disable Windows Installer Properties
Policy
Explain
Disable Windows Installer
Not Configured
Enabled
Disabled
Disable Windows Installer
Always
Previous Policy
Next Policy
OK
Cancel
Apply

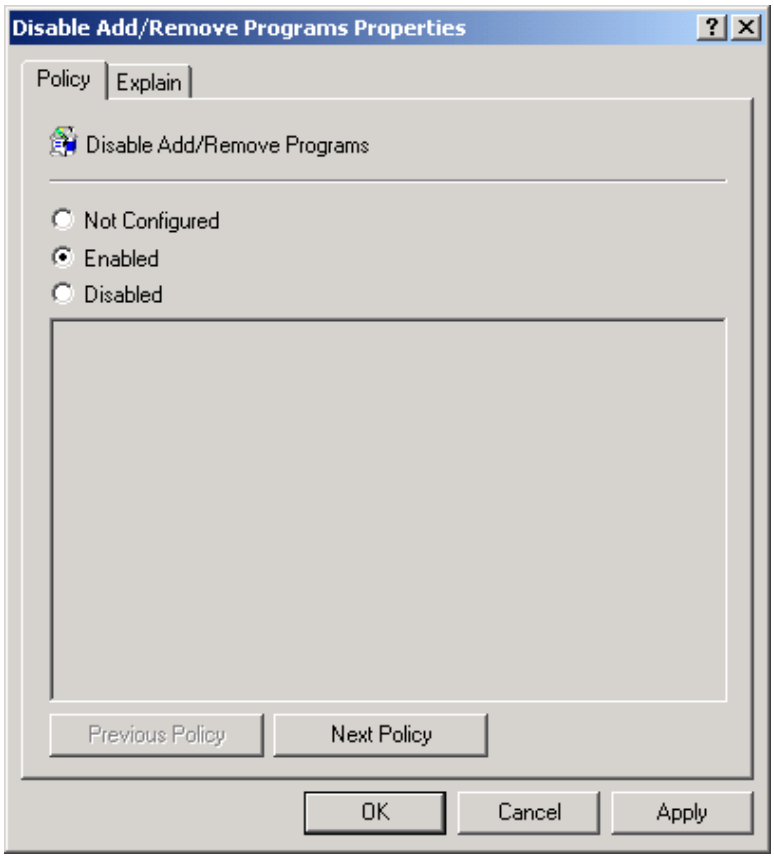
2.3 Disable Add/Remove Programs

- Run gpedit.msc from Start--->Run menu, the Group Policy MMC will be displayed.
- Expand User Configuration tree
- Expand Administrative Templates
- Expand Control Panel
- Highlight Add/Remove Programs



- In the right-hand pane, click **Disable Add/Remove Programs.** The **Disable Add/Remove Programs Properties** window opens.

- Enable the **Enabled** radio button.



This prevents users from using Add/Remove Programs. Add/Remove Programs is removed from the Control Panel and menus.

Note: These changes have no impact on the Administrator account. A user with a Power User account will only be able to add programs that do not require system registry access, components registration, and use of the Windows installer.