Toolkit to Disable Automatic Delivery of Internet Explorer 7

Overview

To help our customers become more secure and up-to-date, Microsoft will distribute Internet Explorer 7 as a high-priority update via Automatic Updates for Windows XP and Windows Server 2003 soon after the final version of the browser is released (planned for fourth quarter 2006). This Blocker Toolkit is intended for those organizations that would like to block automatic delivery of Internet Explorer 7 to machines in environments where Automatic Updates is enabled.

- The Blocker Toolkit will prevent machines from receiving Internet Explorer 7 as a high-priority update via Automatic Updates and the "Express" install option on the Windows Update and Microsoft Update sites. The Blocker Toolkit will not expire.

- The Blocker Toolkit will <u>not</u> prevent users from manually installing Internet Explorer 7 as a Recommended update from the Windows Update or Microsoft Update sites, from the Microsoft Download Center, or from external media.

- Organizations do not need to deploy the Blocker Toolkit in environments managed with an update management solution such as Windows Server Update Services or Systems Management Server 2003. Organizations can use those products to fully manage deployment of updates released through Windows Update and Microsoft Update, including Internet Explorer 7, within their environment.

For more details on how Internet Explorer 7 will be distributed via Automatic Updates and information on other options for blocking deployment within organizations, please review the TechNet announcement here.

Toolkit Components

This toolkit contains two components:

- An executable blocker script
- A Group Policy Administrative Template (.ADM file)

Supported Operating Systems

Windows XP Home [SP2], Windows XP Professional [SP2], Windows XP Tablet PC [SP2], Windows XP Media Center [SP2], Windows XP x64 Professional [RTM], Windows Server 2003 Standard [SP1], Windows Server 2003 Enterprise [SP1], Windows Server 2003 Datacenter [SP1], Windows Server 2003 Web Server [SP1], Windows Server 2003 (x64) Standard [SP1], Windows Server 2003 (x64) Enterprise [SP1], Windows Server 2003 (x64) Datacenter [SP1], Windows Server 2003 (IA64) Enterprise [SP1], Windows Server 2003 (IA64) Datacenter [SP1]

Blocker Script

The script creates a registry key and sets the associated value to block or unblock (depending on the command-line option used) automatic delivery of Internet Explorer 7 on either the local machine or a remote target machine.

Registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Setup\7.0`

Key value name: `DoNotAllowIE70`

Value	Result
Key is not defined	Distribution is *not* blocked.
0	Distribution is *not* blocked.
1	Distribution is blocked.

The script has the following command-line syntax:

`IE70Blocker.cmd [<machine name>] [/B] [/U] [/H]`

Machine Name

The `<machine name>` parameter is optional. If not specified, the action is performed on the local machine. Otherwise,

the remote machine is accessed via the remote registry capabilities of the REG command. If the remote registry can't be accessed due to security permissions or the remote machine can't be found, an error message is returned from the REG command.

Switches

Switches used by the script are mutually exclusive and only the first valid switch from a given command is acted on. The Script can be run multiple times on the same machine without problem.

Switch	Description
/B	Blocks distribution
/U	Unblocks distribution
/H (or /?)	Displays the following summary help:

```
This tool can be used to remotely block or unblock the delivery of
Internet Explorer 7 via Automatic Updates.

------------------------------------------------------------
Usage:
IE70Blocker.cmd [<machine name>] [/B][/U][/H]
B = Block Internet Explorer 7 deployment
U = Allow Internet Explorer 7 deployment
H = Help

Examples:
IE70Blocker.cmd mymachine /B (blocks delivery on machine "mymachine")

IE70Blocker.cmd /U (unblocks delivery on the local machine)
------------------------------------------------------------
```

Group Policy Administrative Template (.ADM file)

The Group Policy Administrative Template (.ADM file) allows administrators to import the new Group Policy settings to block or unblock automatic delivery of Internet Explorer 7 into their Group Policy environment, and use Group Policy to centrally execute the action across systems in their environment.

After adding this administrative template to the Group Policy Editor you must uncheck the **"Only show policy settings that can be fully managed"** in the Filtering dialog before the new policy becomes visible in the Group Policy Editor. This option is found by highlighting "Administrative Templates", then selecting "View" then "Filtering". You will then see the policy under **"Computer Configuration / Administrative Templates / Windows Components** / **Windows Update** / **Automatic Updates Blockers".** This setting is available only as a Computer setting; there is no per User setting.
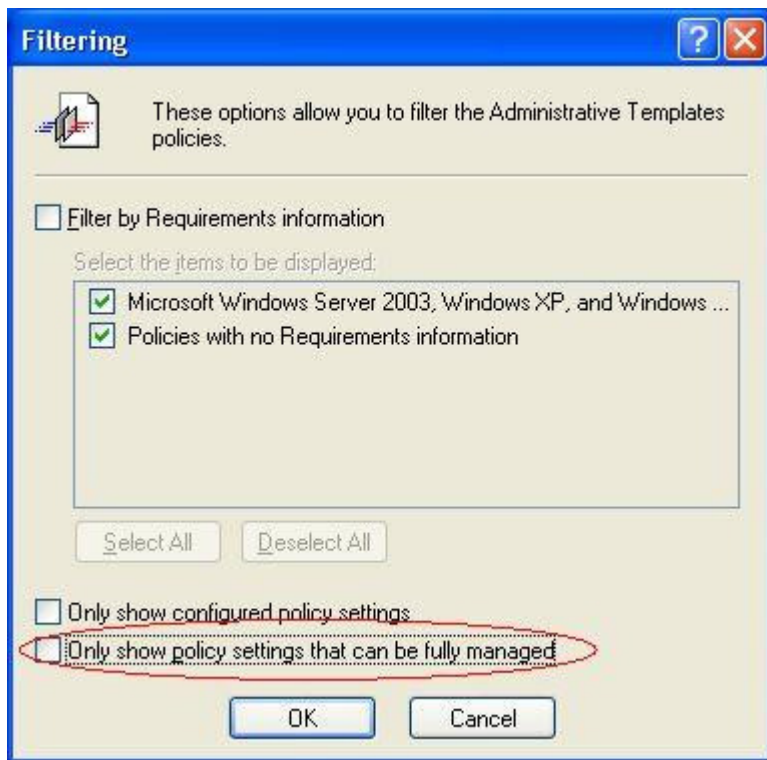
Note: This registry setting is not stored in a policies key and is thus considered a preference. Therefore if the Group Policy Object that implements the setting is ever removed or the policy is set to "Not Configured", the setting will remain. To unblock distribution of Internet Explorer 7 using Group Policy set the policy to "Disabled".

Related Resources

1. [Internet Explorer 7 Blocker Toolkit Q&A](#)

2. [Internet Explorer 7 via Automatic Updates](#)

3. [Internet Explorer 7 Product Site](#)

4. [Readiness Toolkit for Developers, Testers & ITPros](#)

5. [Microsoft Update Management Solutions](#)