



Windows Vista™

Winlogon Notification Packages Removed: Impact on Windows Vista Planning and Deployment

Microsoft Corporation

Published: September 2006

Author: Michiko Short

Abstract

In Windows Vista and later, Winlogon notification packages are no longer supported. Winlogon notification packages are discussed in detail in the next section. After upgrading systems to Windows Vista, Winlogon will not load Winlogon notification packages. Organizations that are using Winlogon notification packages must either remove the functionality or create a new solution when deploying Windows Vista and later.

Microsoft

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.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

Winlogon Notification Packages Removed: Impact on Windows Vista Planning and Deployment.....	5
What Were Winlogon Notification Packages?	5
Identifying Winlogon Notification Packages	6
Windows Server 2003 SP 1:.....	6
Windows XP SP 2:.....	7
Windows 2000 SP 4:.....	7
Using Service Control Manager (SCM) Notifications	7
Using the System Event Notification Service (SENS)	9
Using Group Policy Scripts	9
Policy Settings Related to Script Processing	10
Security Context for Script Processing.....	11

Winlogon Notification Packages Removed: Impact on Windows Vista Planning and Deployment

In Windows Vista and later, Winlogon notification packages are no longer supported. Winlogon notification packages are discussed in detail in the next section. After upgrading systems to Windows Vista, Winlogon will not load Winlogon notification packages. Organizations that are using Winlogon notification packages must either remove the functionality or create a new solution when deploying Windows Vista and later.

What Were Winlogon Notification Packages?

In pre-Windows Vista versions of Windows, Winlogon notification packages are registered DLLs that the Winlogon process loads. These DLLs receive Winlogon notifications and handle different Winlogon events. Winlogon previously supported the following events.

Previously supported Winlogon notification packages

Event	Description
Lock	Occurs when the user locks the workstation.
Logoff	Occurs when a user logs off from the system. The Logoff event is always performed synchronously.
Logon	Occurs when a user logs on the system.
Shutdown	Occurs just before the system shuts down.
StartScreenSaver	Occurs when the screen saver has started. StartScreenSaver event notification is for informational purposes only.

Event	Description
StartShell	Occurs after the user has logged onto the system, network connections have been established, and the user specified shell program, (usually Explorer.exe), has been started.
Startup	Occurs when the system is started up or rebooted.
StopScreenSaver	Occurs when the screen saver has stopped. StopScreenSaver event notification is for informational purposes only.
Unlock	Occurs when the user unlocks the workstation or when a system administrator overrides the lock and logs the user off.

The DLL could also impersonate the logged on user or be called asynchronously as well.

Winlogon notification packages are only supported in Windows 2000, Windows XP and Windows Server 2003. For more information about Winlogon notification packages, see "Winlogon Notification Packages" in Security (<http://go.microsoft.com/fwlink/?LinkId=70570>).

Identifying Winlogon Notification Packages

If a system is using a Winlogon notification package, it is registered in the registry under the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
```

The following Windows components use Winlogon notifications and their registration will exist in a default installation.

Windows Server 2003 SP 1:

- Crypt32chain: crypt32.dll
- Cryptnet: cryptnet.dll
- Cscdll: cscdll.dll
- Dimsntfy: dimsntfy.dll

- ScCertProp: wlnotify.dll
- Schedule: wlnotify.dll
- ScLgntfy: sclgntfy.dll
- Senslogn: wlnotify.dll
- Termsrv: wlnotify.dll
- Wlballoon: wlnotify.dll

Windows XP SP 2:

- Crypt32chain: crypt32.dll
- Cryptnet: cryptnet.dll
- Cscdll: cscdll.dll
- ScCertProp: wlnotify.dll
- Schedule: wlnotify.dll
- ScLgntfy: sclgntfy.dll
- Senslogn: wlnotify.dll
- Termsrv: wlnotify.dll
- Wlballoon: wlnotify.dll

Windows 2000 SP 4:

- Crypt32chain: crypt32.dll
- Cryptnet: cryptnet.dll
- Cscdll: cscdll.dll
- ScLgntfy: sclgntfy.dll
- Senslogn: wlnotify.dll
- Termsrv: wlnotify.dll
- Wzcnotif: wzcldg.dll

Using Service Control Manager (SCM) Notifications

Service Control Manager (SCM) has notifications corresponding to most of the Winlogon notifications. Creating a service and using SCM notifications will not only work in Windows Vista, but also the same solution will work in Windows XP and Windows Server 2003 environments. SCM notifications are delivered asynchronously, but services can impersonate users if they have permission to find the user token based on the SessionId.

The service will need to register for its service control handler function to receive SCM notifications during the SetServiceStatus call. The SERVICE_STATUS structure (<http://go.microsoft.com/fwlink/?LinkID=70746>) will need to include SERVICE_ACCEPT_SESSIONCHANGE 0x00000080 as an accepted control. The following table has the corresponding HandlerEx control code and WM_WTSSESSION_CHANGE status code combination equivalent to each Winlogon event.

HandlerEx control codes

Winlogon Event	HandlerEx Control Code	WM_WTSSESSION_CHANGE Status Code
Lock	SERVICE_CONTROL_SESSIONCHANGE	WTS_SESSION_LOCK
Logoff	SERVICE_CONTROL_SESSIONCHANGE	WTS_SESSION_LOGOFF
Logon	SERVICE_CONTROL_SESSIONCHANGE	WTS_SESSION_LOGON
Shutdown	SERVICE_CONTROL_SHUTDOWN	none
Unlock	SERVICE_CONTROL_SESSIONCHANGE	WTS_SESSION_UNLOCK

Note

SCM does not have notifications corresponding to the following Winlogon events:

StartScreenSaver - Is supported in SENS, see [Using the System Event Notification Service \(SENS\)](#).

StartShell - In Windows Vista and later, due to asynchronous starting of services, there is nothing in the system equivalent to the StartShell event. If your service needs the network connections established it should use logon and wait for the network.

Startup - Creating a service that starts at startup would be an option.

StopScreenSaver - Is supported in SENS, see [Using the System Event Notification Service \(SENS\)](#).

For additional information about HandlerEx, see HandlerEx in the System Services (<http://go.microsoft.com/fwlink/?LinkId=70743>).

For additional information about creating a service, see MSDN Services reference (<http://go.microsoft.com/fwlink/?LinkId=70744>).

Using the System Event Notification Service (SENS)

The System Event Notification Service (SENS) has notifications corresponding to most of the Winlogon notifications. Creating a new application using SENS will not only work in Windows Vista, but also the same solution will also work in Windows 2000, Windows XP, and Windows Server 2003 environments. Applications typically are not synchronous, but if the application process has SE_ASSIGNPRIMARYTOKEN_NAME and SE_INCREASE_QUOTA_NAME privileges, then it can impersonate users. SENS notifications do not have notifications corresponding to the following Winlogon events:

- Shutdown: Supported in SCM notifications. See [Using Service Control Manager \(SCM\) Notifications](#).
- Startup: Creating a service that starts at startup would be an option.

The application will need to subscribe to one or more of the SENS logon events. The following table has the corresponding ISensLogon method equivalent to each Winlogon event.

ISensLogon methods

Winlogon Event	ISensLogon Method
Lock	DisplayLock
Logoff	Logoff
Logon	Logon
StartScreenSaver	StartScreenSaver
StartShell	StartShell
StopScreenSaver	StopScreenSaver
Unlock	DisplayUnlock

For additional information about ISensLogon, see ISensLogon in Network Management (<http://go.microsoft.com/fwlink/?LinkId=70745>).

Using Group Policy Scripts

Group policy provides administrators the ability to execute four types of scripts:

- Computer startup script
- Logon script

- Computer shutdown script
- Logoff script

For more information about how to create and target a script based Group Policy, see article 322241 in the Microsoft Knowledge Base (<http://go.microsoft.com/fwlink/?LinkId=73697>)

Policy Settings Related to Script Processing

By default, all scripts are executed asynchronously to improve system boot and login performance. However, there is a Group Policy option to have scripts executed synchronously.

Note

Computer boot and logons will be blocked until the script execution completes in case Computer startup scripts and Logon scripts can be executed synchronously.

Please note that this is not a recommended configuration and should only be used if no other methods are available. You must also extensively test the script to ensure that it does not cause any system performance problems. The following are some of the relevant Group Policy settings associated with the script processing policy.

Computer configuration script options

Option	Description
Run startup scripts synchronously	Enable this option to force the system to run the scripts synchronously, one after another. This option exists for computer and user configuration, and each can have a different value. In case of conflict, the computer configuration setting prevails.
Run startup scripts visible	Enable this option to run startup scripts in a visible window.
Maximum wait time for Group Policy scripts	Use this option to set the script timeout interval. The default interval is 600 seconds (10 minutes), and valid intervals range from 0 to 32000 seconds

Similar Group Policy settings are also available for user based logon or logoff scripts.

Security Context for Script Processing

Group Policy scripts are processed under the system context. In Windows Vista, both computer and user Group Policy scripts are executed in elevated mode (Scripts are run with a full administrator access token).