

## Re: Force users documentation to automatically save

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/26444.html>

---

**From:** Al Dunbar [MS-MVP] (*alan-no-drub-spam\_at\_hotmail.com*)

**Date:** 02/26/05

Date: Sat, 26 Feb 2005 09:36:16 -0700

"Brandon McCombs" <bmccombs@ma.rr.com> wrote in message  
news:421E80AA.BCAAC35E@ma.rr.com...

>  
>  
> *Joe wrote:*  
>  
> > *I am installing the "Winexit.scr" screen saver onto the corporate  
> > workstations. I will use the Force application termination option to  
quit  
> > programs and exit windows xp professional. Is there a way to create a  
policy  
> > to force user's documentation to save their data before this screen  
saver  
> > starts? Thank you for your time  
> >  
> > *Joe*  
>  
> *That is too specific of a requirement for anything to exist to provide  
that  
> level of functionality. You would have to define what "user  
documentation"  
> entails and what applications that would include to even have a shot of  
being  
> able to implement that.**

Forcing open files to be saved when the screensaver starts up is not a good idea (even if it were possible). I often click save as a kind of fail-safe checkpoint, then make tentative changes, knowing I can exit without saving in the event that I screw something up.

Forcing the users to manually save their documents when the screensaver starts up (even if it were possible) would be counterproductive. This would prevent the screensaver from logging them off if the user was not there to actually save his work.

microsoft.public.windowsxp.general: Re: Force users documentation to automatically save

Our policy is that the screensaver simply locks the workstation. If the user is still around they have the opportunity to unlock and save before logging off. If not, an administrator does the unlocking or a user power-cycles the workstation, both of which will cause open files not to be saved.

This may seem harsh, but it is less of a problem than leaving a session active, and thereby failing to secure sensitive data. Sure, mistakes will be made, but you cannot make it impossible for mistakes to be made – if you could, then perhaps you wouldn't need any users ;-). But it is the user that is accountable for their work – just let them be.

/Al