



# Dell Data Protection | Protected Workspace

## User's Guide



Dell Data Protection | Protected Workspace v2.3



© 2013 Dell Inc.

Trademarks used in this text: Dell™, the DELL logo, Dell Precision™, OptiPlex™, Latitude™, and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

June 2013

Rev. A00

## Table of Contents

<b>Purpose and Intended Audience</b> .....	<b>5</b>
<b>What is Dell Data Protection   Protected Workspace?</b> .....	<b>5</b>
<b>Dell Data Protection   Protected Workspace Icons</b> .....	<b>5</b>
Dell Data Protection   Protected Workspace Desktop Icon .....	5
Dell Data Protection   Protected Workspace System Tray Icon.....	5
Dell Data Protection   Protected Workspace Start Menu Folder .....	5
<b>Common End User Tasks</b> .....	<b>6</b>
Starting the Dell Data Protection   Protected Workspace Environment or Launching new Browser Window .....	6
Additional ways to launch a new browser window.....	7
Dell Data Protection   Protected Workspace Setup .....	9
Changing your home page in Dell Data Protection   Protected Workspace protected browsers .....	10
<b>Internet Explorer</b> .....	<b>10</b>
<b>Mozilla Firefox</b> .....	<b>11</b>
Downloading a File in Dell Data Protection   Protected Workspace.....	12
<b>File Download Additional Dialogs</b> .....	<b>14</b>
Opening a document with Dell Data Protection   Protected Workspace .....	15
Dell Data Protection   Protected Workspace Auto Restore .....	18
Dell Data Protection   Protected Workspace Threat Detection .....	18
<b>Dell Data Protection   Protected Workspace System Tray Options</b> .....	<b>21</b>
Open Internet Explorer.....	21
Open Firefox.....	21
Restore.....	21
Suspect Activity Details.....	22
Import Bookmarks.....	22

Preferences.....	22
About.....	23
Exit .....	23
<b>Preference Menu Options.....</b>	<b>24</b>
General Tab.....	24
<b>Basics .....</b>	<b>24</b>
<b>Border .....</b>	<b>25</b>
Apps Tab.....	26
Privacy Tab (v2.2.1-14451 only) .....	27
<b>Privacy Settings.....</b>	<b>27</b>
Auto-Restore Tab.....	28
<b>Automatic Restore.....</b>	<b>28</b>
Security Tab .....	29
<b>Activity Blocking .....</b>	<b>29</b>
<b>Downloads.....</b>	<b>30</b>
Trusted Sites Tab.....	30
<b>Subscription Renewal.....</b>	<b>31</b>

## Purpose and Intended Audience

---

This document is intended to provide information and instruction for tasks that are considered day-to-day for end users of the DDP | Protected Workspace product.

## What is Dell Data Protection | Protected Workspace?

---

DDP | Protected Workspace (DDP|PW) is an isolated environment that is created on the PC and can run web browsers and document viewers which are isolated from the native PC. This protected environment helps protect an end user PC from being infected with malware and helps stop other malicious attacks. By browsing in a protected browser in the DDP | PW isolated environment and by viewing documents within the protected environment, DDP | PW is able to stop malware from being installed on the local PC and exposing that PC to other types of attacks and security vulnerabilities.

## Dell Data Protection | Protected Workspace Icons

---

After the Installation of DDP | Protected Workspace, one new icon will be located on the desktop, one new icon will be located in the system tray (while the application is running) and a new folder will be created within the Start Menu. The following section helps to identify each of these new icons and what their functions are.

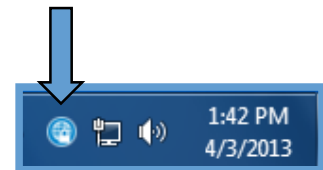
### Dell Data Protection | Protected Workspace Desktop Icon

The DDP | Protected Workspace icon found on the desktop is a point of execution for the application. Double clicking on this icon will start the DDP|PW application if it is not currently running or will launch a new browser window if it is running in the background. This icon can be pinned to the quick launch toolbar to allow for easier access.



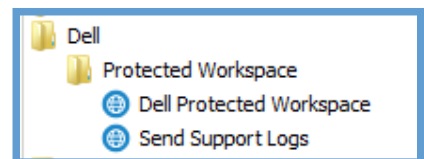
### Dell Data Protection | Protected Workspace System Tray Icon

The DDP | Protected Workspace system tray icon can be found in the PC system tray when DDP|PW protected environment is running. End User actions, such as opening a new browser window, restoring DDP|PW to a clean state or modifying user preferences are available from this tray icon. More details on what options are available and how to use them can be found later in this document.



### Dell Data Protection | Protected Workspace Start Menu Folder

DDP | Protected Workspace can also be launched (either starting the program or opening a new browser window) by going to the start menu, choosing All Programs, then Dell, then Protected Workspace. Within this folder is the DDP|PW link. Additionally, this folder contains a support tool that can be used to send support logs to the support team in case of an issue with the product.



## Common End User Tasks

---

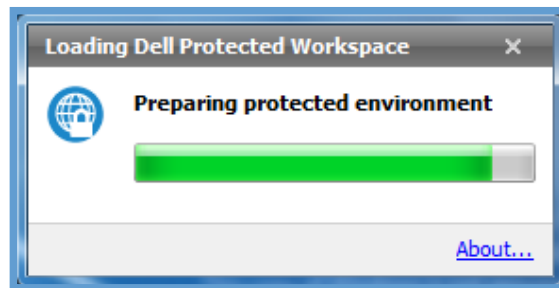
The following section offers step by step instructions for most day to day end user tasks.

### Starting the Dell Data Protection | Protected Workspace Environment or Launching new Browser Window

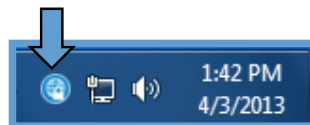
To start the DDP | Protected Workspace isolated environment or to launch a new protected browser window within the protected environment, double-click on the DDP | PW icon on the desktop.

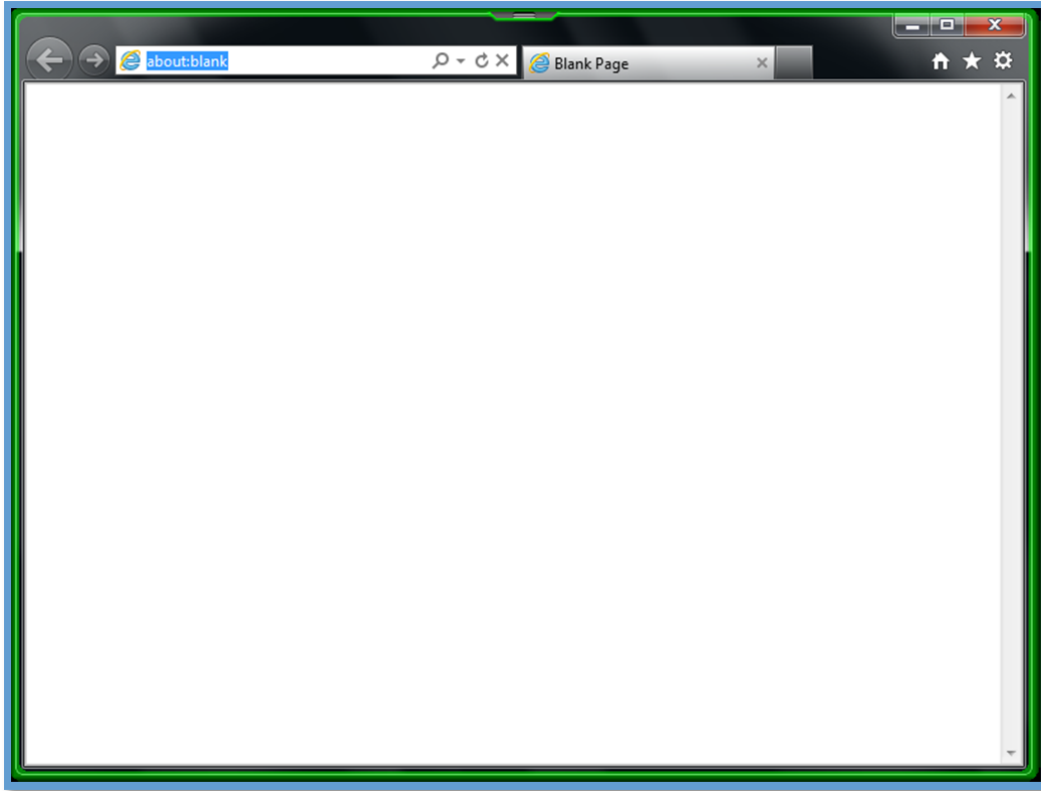


After clicking on the icon, a dialog box with progress bar will appear if the product is not running already. It will be displayed over the system tray and will show the progress of the protected environment startup.



Once this dialog box closes or if the environment is already running, the DDP | Protected Workspace system tray icon will be visible and a new browser will open in the protected environment. A new protected browser window will be displayed immediately or once the protected environment finishes loading.





Applications running in the DDP | Protected Workspace isolated environment contain a customizable border color (shown as neon green above) that highlights any windows opened within the protected environment. This is to help the end user distinguish between the native applications and those running in the isolated environment.

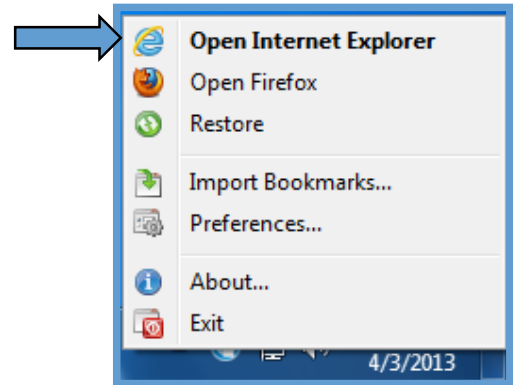
### [Additional ways to launch a new browser window](#)

When DDP | Protected Workspace is already running and a user wants to open a new or additional browser window in the isolated environment, they can accomplish this by doing one of three simple tasks.

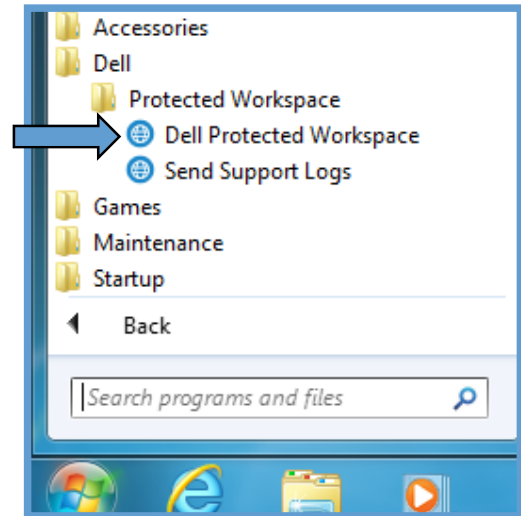
The first is to double-click on the DDP | Protected Workspace icon on the desktop.



The second is to right click on the DDP | Protected Workspace system tray icon, and select either “Open Firefox” or “Open Internet Explorer” from the menu. Note that the preferred browser (the one opened by double clicking the DDP | Protected Workspace desktop icon) is **bold**. In this screen shot, Internet Explorer is the preferred browser.



Finally, the user can go to the Start Menu, choose All Programs, open the Dell folder, then the Protected Workspace folder, and finally choose “Dell Protected Workspace”.





## Dell Data Protection | Protected Workspace Setup

When DDP | Protected Workspace is run for the first time, a first run wizard will be displayed.

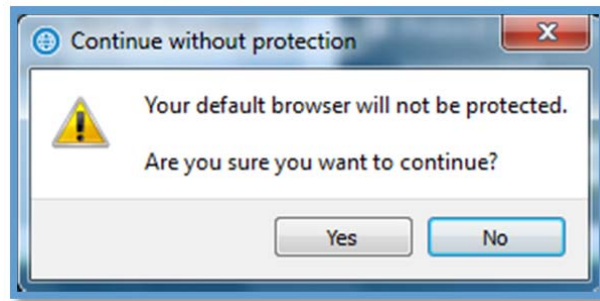


When the end user selects Next, they will be guided through a quick tour of the DDP | Protected Workspace product. End users can click "Next" to progress through the first run tour, "Previous" to return to the prior screen, or "Skip Tour" to exit the process.



In the "Select Your Protection" setup users can customize some of the behaviors of the protected environment. The first option allows the user to choose if the DDP | Protected Workspace protected

environment will be used to protect the default web browser. If the Browser option is left unselected, users will get a notification informing them that the default browser will not be protected.



The next option is for document protection. DDP | Protected Workspace will protect Microsoft Word, Microsoft PowerPoint, and Microsoft Excel documents as well as Adobe Acrobat or Adobe Reader documents.

The final option on this screen is about the border that will be shown on the application windows in the protected environment. A user may choose to disable the border completely, by unselecting this option (not recommended) or may choose to define an alternative color by pressing the "Pick color..." button.

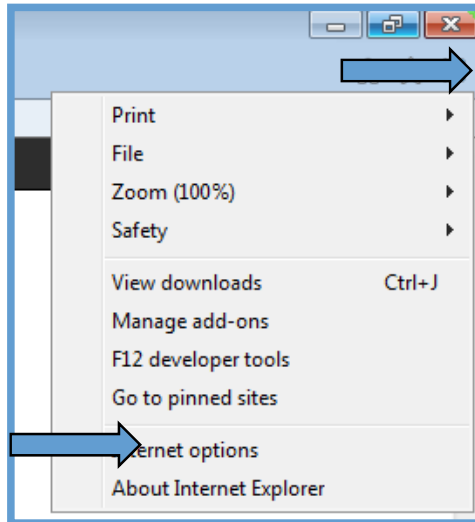
Once finished, pressing the "Start Tour" button will allow the end user to walk through the first run tour before starting the product for the first time. Alternatively, users can click "Skip Tour" to start the product.

## [Changing your home page in Dell Data Protection | Protected Workspace protected browsers](#)

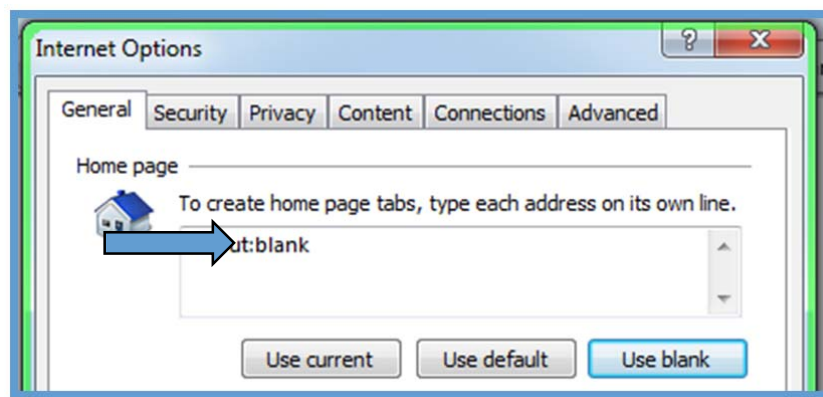
### **Internet Explorer**

The homepage of a browser running in the DDP | Protected Workspace environment is customizable like any other web browser. To change the homepage from Internet Explorer running in the protected environment, select "Tools" or the tools icon, from the menu at the top of protected Internet Explorer window. After the drop down menu appears, select "Internet Options" from the list of options.

Note: Screenshots below are from IE9, but the outlined steps should also work for IE7 through IE10.



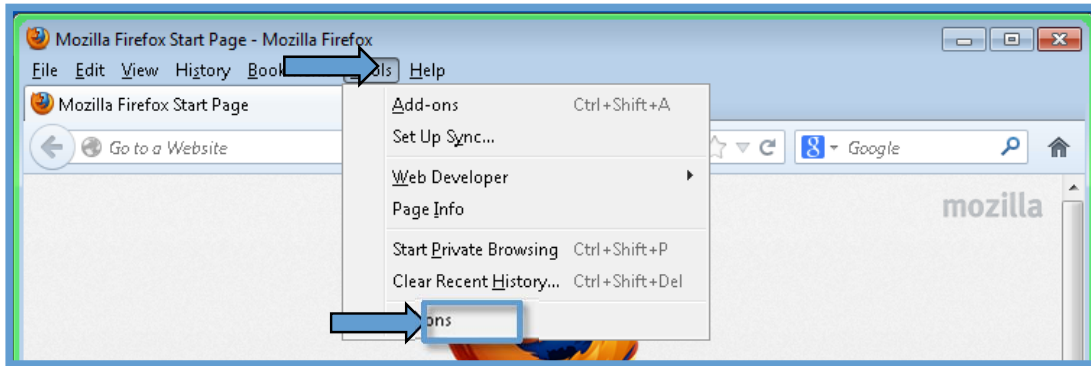
When the Internet Options box appears, delete any text that exists in the box below “To create homepage tabs, type each address on its own line.” Once this box is cleared, enter the address for the new homepage, such as <http://www.google.com>.



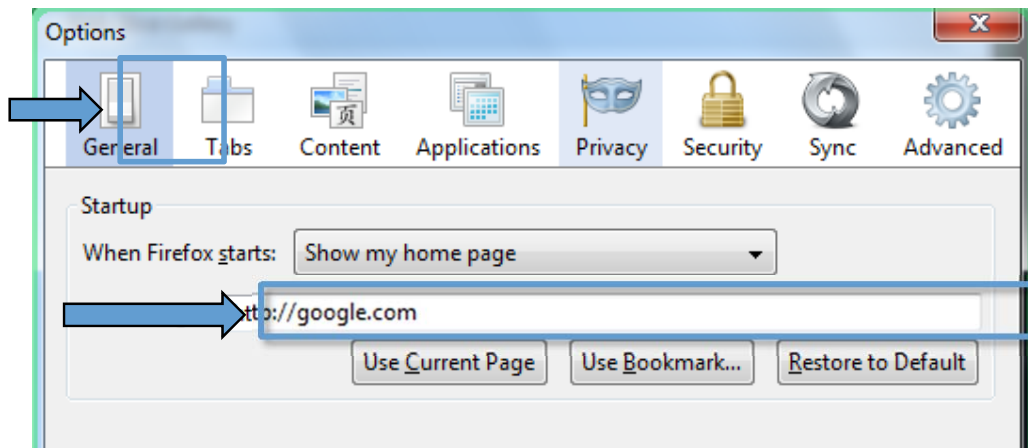
Click OK when finished. Open a new DDP | Protected Workspace browser window to verify the homepage is now set to the new page entered.

### Mozilla Firefox

To change the homepage for Mozilla Firefox in the protected environment, select “Tools” from the menu at the top of a protected Firefox window. After the drop down menu appears, select “Options” from the list of options.



When the Options box appears, verify that the “General” tab is selected. Next to “When Firefox starts:” select “Show my homepage” from the dropdown (if not selected already). Now delete any text that exists in the box labeled “Home Page”. Once this box is cleared, enter the address for the new homepage, such as <http://www.google.com>. Then click “OK”.



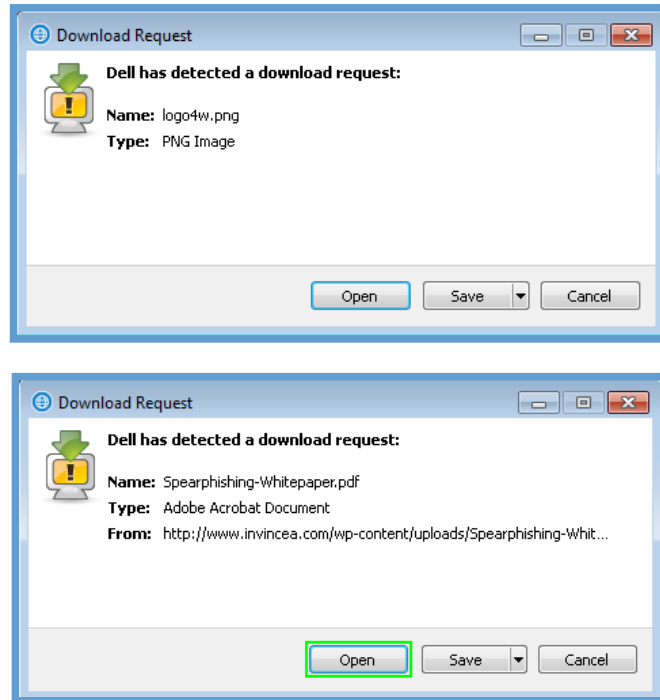
### Downloading a File in Dell Data Protection | Protected Workspace

Within the DDP | Protected Workspace protected environment, downloading files is slightly different than in a typical web browser. Since the DDP|PW environment is isolated from the PC, there is a special download interface that is needed to download files. This also allows for some files to be checked for malicious content before being saved.

To download a file within the DDP | Protected Workspace environment, click on a file download link on a website displayed in the protected environment. Once the download starts, a DDP|PW Download Request dialog will appear. This is used to confirm that the user intended to download a file, and the file wasn't downloaded by accident or via a malicious website.

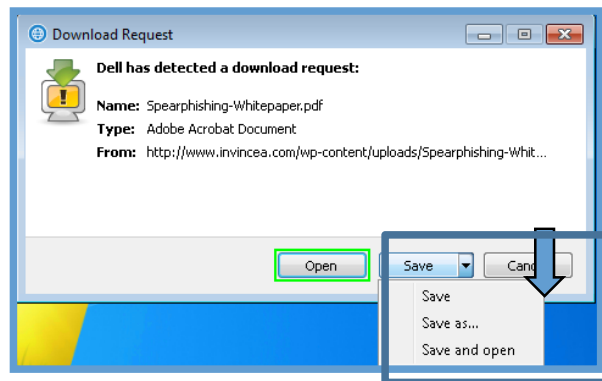
If the download was intended, then choose “Save” to continue, otherwise choose “Cancel. As the download progresses, a download progress dialog will be displayed. Users also have the ability to “Open” the downloaded item directly from the protected environment. Pressing the “Open” button will

download the file to a temporary directory and then will open it in the default application for that file type. This option is not available for executable files or files that do not have a default application on the PC.

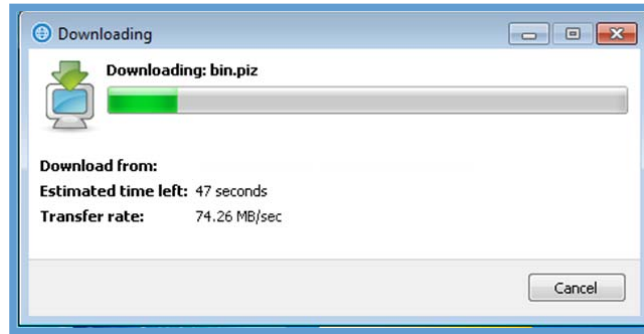


When users are presented with a file that can be opened in a protected application, such as a PDF file, the “Open” button will be highlighted with a border around it to indicate that.

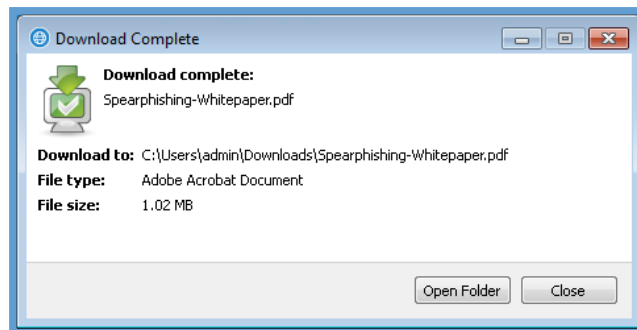
Alternatively, users have the option to use the “Save” drop down menu (by clicking on the downward facing arrow) to do a “Save As...” or “Save and open.”



While the file is being downloaded to the PC, a download dialog box will be displayed with a progress bar. The download process may take slightly longer from the DDP | Protected Workspace environment than a normal web browser due to the extra security layers that are in place.



When the file has finished downloading, DDP | Protected Workspace will scan it and finish the transfer from the isolated environment to the host PC. A finalizing dialog will display during this process. When the process has completed, a Download Complete dialog will display. From this dialog, the dialog box can either be closed or the folder that the file was downloaded to can be opened.



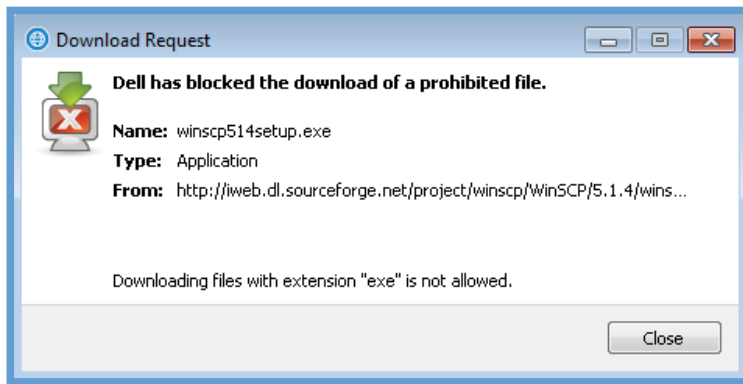
The “Save” button on a DDP | Protected Workspace download request file will save the file to the default download folder. The default download folder is the User Downloads folder, which is typically found at C:\Users\\Downloads.

### File Download Additional Dialogs

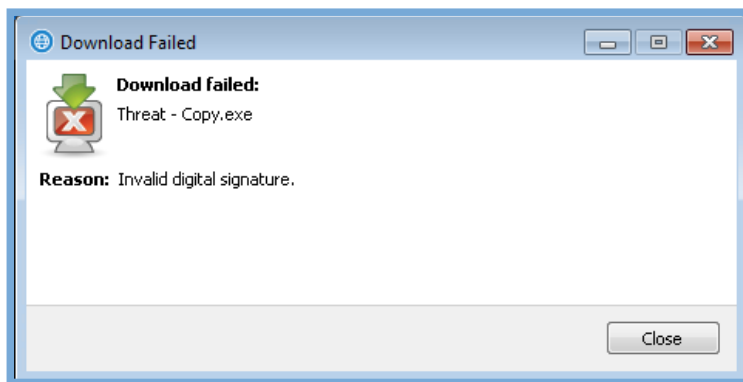
DDP | Protected Workspace also has advanced download features that help to protect the end user PC. Some of these options may prevent certain files from being downloaded in the DDP | PW environment.

One of these options is the ability to block downloads for certain types of files. If a file download is blocked by type, the following message will be displayed when a request to download the file type happens. This option can be enable in the preferences menu. When enabled, the following extensions will be blocked:

bas, bat, chm, cmd, com, cpl, crt, dll, exe, hlp, hta, inf, ins, isp, msc, msi, msp,  
mst, pif, reg, scr, sct, shb, shs, sys, vb, vbe, vbs, wsc, wsf, wsh



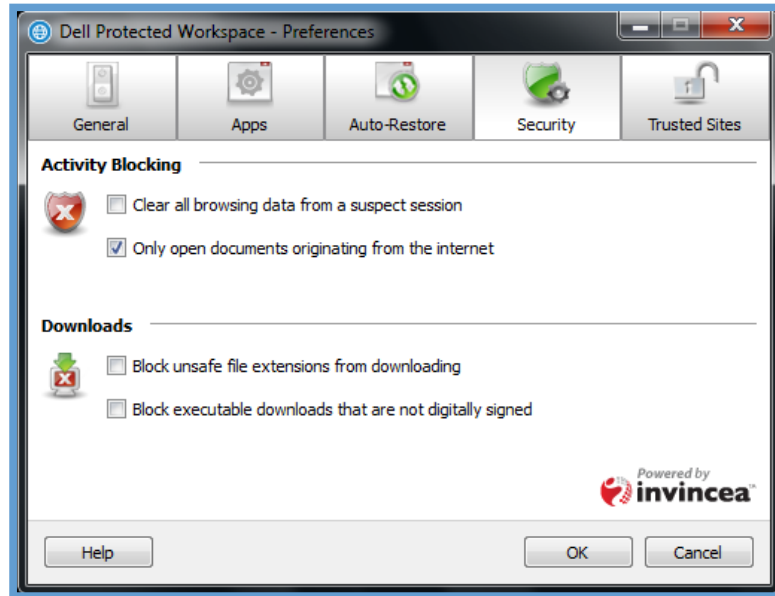
Additionally, downloads can be blocked if the digital signature of a file is not valid. This can be enabled via the user preference menu as well. The following dialog will be displayed if these conditions are met.



### Opening a document with Dell Data Protection | Protected Workspace

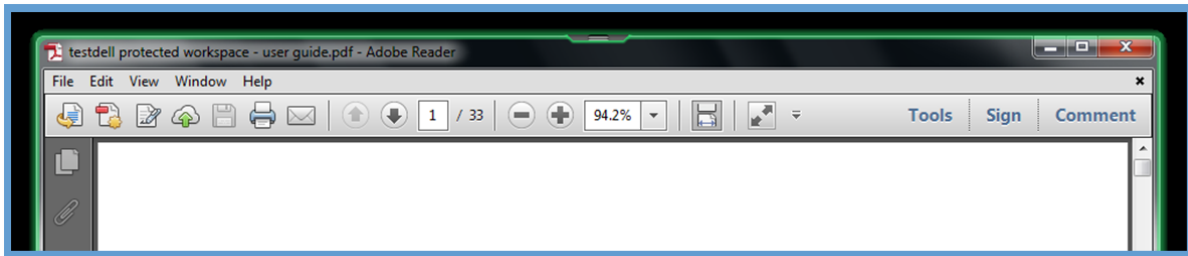
In addition to preventing malware from infecting the end user PC via a website or file download, DDP | Protected Workspace also offers the ability to isolate documents inside the protected environment. This helps to prevent malicious documents from affecting the end user PC.

By default, DDP | PW will only open documents originating from the internet in a protected environment. To change this setting, right click on the DDP | PW icon in the system tray and select Preferences. Once the Preferences window opens, select the Security tab. Under the Activity Blocking section uncheck "Only open documents originating from the internet" option. This will now open all documents in DDP | PW regardless of where they originate from.



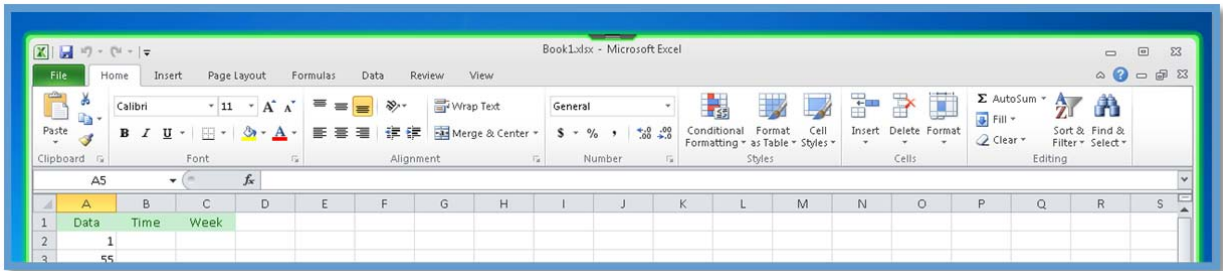
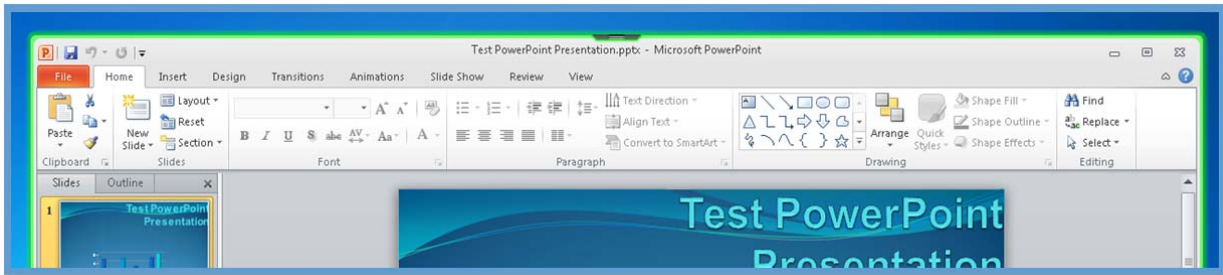
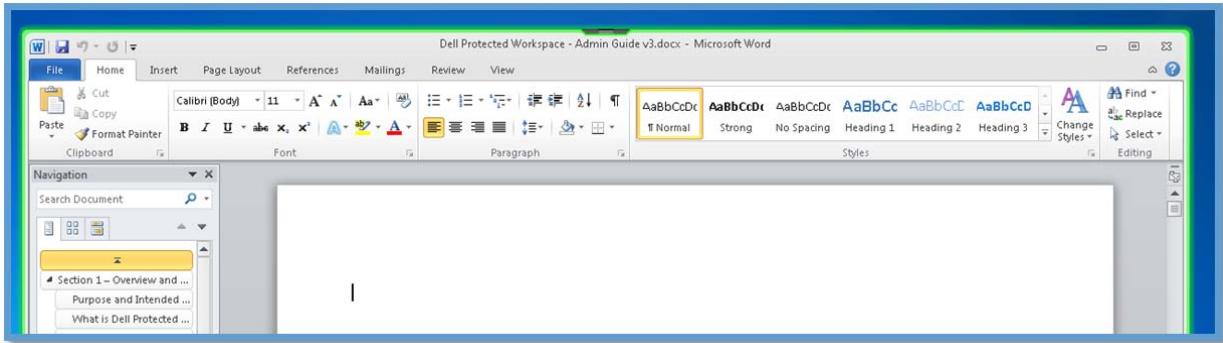
An example of the document protection feature is using the DDP | Protected Workspace environment to view PDF documents. When document protection is enabled for PDF files double-clicking on any PDF file on the computer will open the document in a protected instance of the document application.

The protected documents can be identified by the customized border color that surrounds the application when it is active, just as the protected browser shows. The window below displays a green border, identifying it to be inside the protected environment.

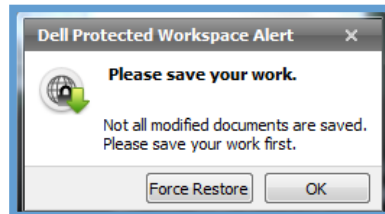


Microsoft Word, Microsoft Excel, and Microsoft PowerPoint files also can be accessed in the DDP | Protected Workspace environment. After double-clicking a supported file type, the document will open in the protected application in the DDP|PW environment. Below are screenshots of protected instances of Microsoft Word, Microsoft Excel, and Microsoft PowerPoint in the DDP|PW environment. These applications display the same colored border as the protected browsers and PDF readers to help identify that the application is being protected by DDP|PW.





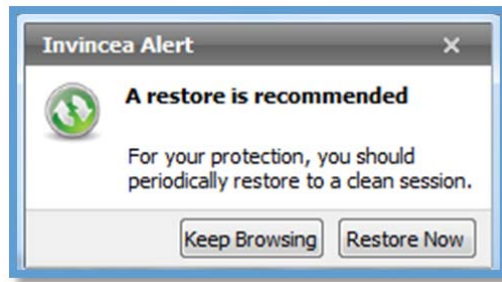
In the event of a restore while you are working in a document, a notification will inform users to save the work so a restore may happen.



## Dell Data Protection | Protected Workspace Auto Restore

The DDP | Protected Workspace product has an auto restore feature built-in that will restore the protected environment back to a clean state on a set schedule. This schedule can be customized by the end user.

When an auto restore happens, the following dialog appears. This allows the user to restore immediately or to delay the restore until a better time. It is recommended that the “Restore Now” option be used to ensure the protected environment is reset to a clean state.

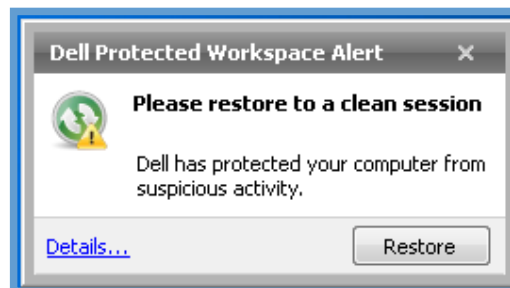


It is recommended that Auto-Restore be enabled to ensure that a fresh browser is used each day. The recommended (and default) setting is that the DDP | Protected Workspace environment be restored every 72 hours if not more frequently. Restoring the protected environment will help to ensure that the environment is always clean and free of malicious activity.

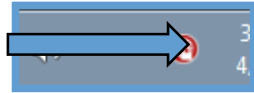
It is also important to note that the DDP | Protected Workspace environment is restarted each time the computer is restarted or a new user logs onto the PC. The Auto-Restore timer will restart each time the product is restarted when the auto-restore timer is in “After Elapsed” mode.

## Dell Data Protection | Protected Workspace Threat Detection

DDP | Protected Workspace has a built in threat detection agent that will detect unsafe behavior within the protected environment. When a threat is detected, the DDP|PW product will notify the end user that a restore of the environment is needed. A notification alert will be displayed above the system tray indicating suspicious activity.



Users can click the “Restore” button, which will restart the protected environment to a clean state. Users also have the option to close the notification and continue working. When doing so, the DDP | Protected Workspace Icon will be displayed in red.

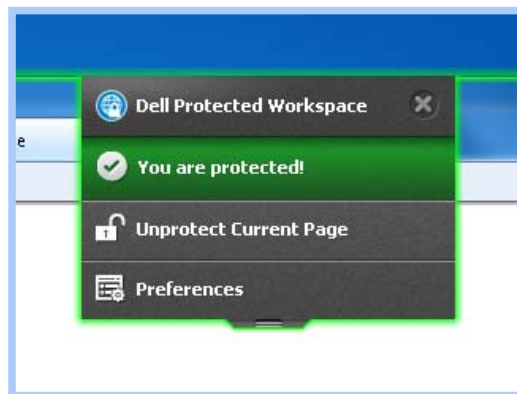


## Using the Dell Data Protection | Protected Workspace Browser Drop Down Menu

The Browser Drop Down menu is a convenient menu that can be used for two different purposes. The menu is found on the in the middle of the top edge of the any protected browser window.



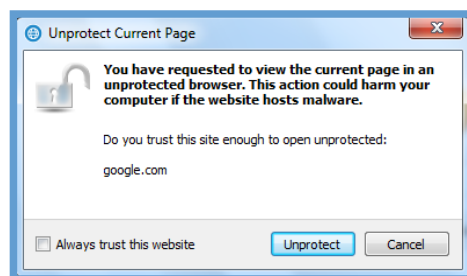
By pressing the gray button, a drop down menu will appear.



The menu provides for two accessible options. The first is the ability to open the preferences menu. This action is the same as opening the preferences menu from the system tray icon.

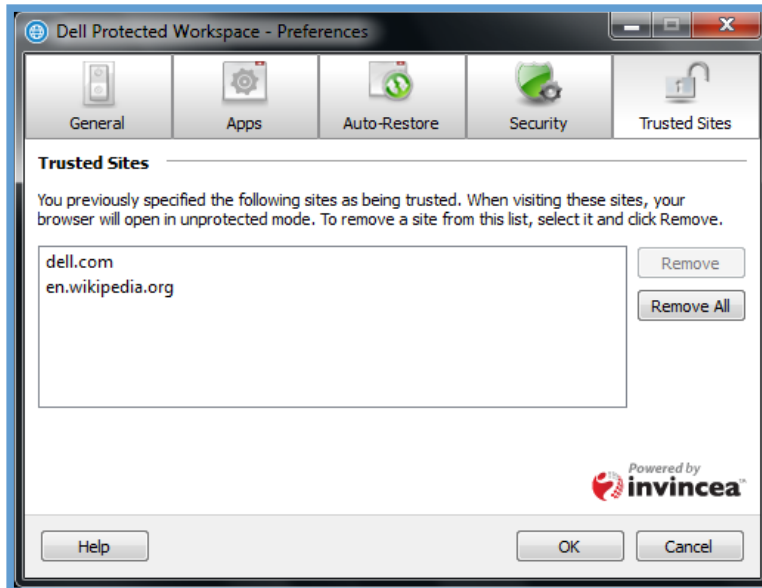
The second option is to open the current page that is being viewed in the browser in an unprotected browser window. This is useful if a page is not rendering correctly inside of the DDP | Protected Workspace browser. Selecting this option will take the current URL and open within an unprotected browser (using the same browser as in the protected environment).

The user will be prompted before the site is move to the unprotected browser to ensure they are aware of the potential danger of browsing outside of the protected environment. The user can choose to continue by pressing the "Unprotect" button or can cancel the action by pressing the "Cancel" button.



There is also an option to “Always trust this website” which will always open the site in an unprotected browser if it is browsed to in a protected session. These sites can be managed in the preferences menu.

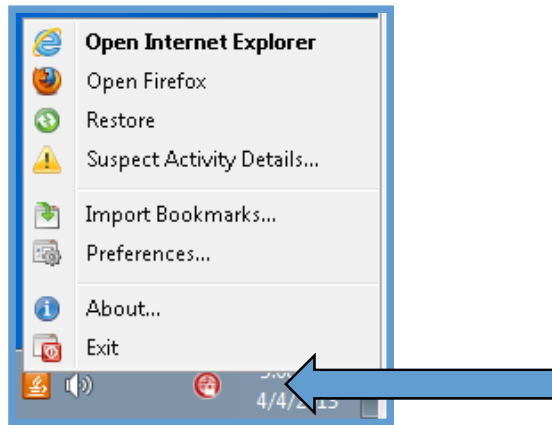
The preferences menu allows for the user to view the sites that have been permanently listed as trusted sites and to also remove a site if it no longer needs to be trusted. This can be done by selecting the site in the list and pressing the “Remove” button. If the user wishes to remove all sites, they can press the “Remove all” button.



## Dell Data Protection | Protected Workspace System Tray Options

---

The following section outlines the menu options available from the DDP | Protected Workspace System Tray Icon. The System Tray Menu can be accessed by right-clicking on the DDP|PW Icon in the system tray.



### Open Internet Explorer

“Open Internet Explorer” is used to open a new Internet Explorer window within the DDP | Protected Workspace environment. If Internet Explorer is the only browser available or is set as the preferred browser, it will appear **bold** and at the top of the menu.

### Open Firefox

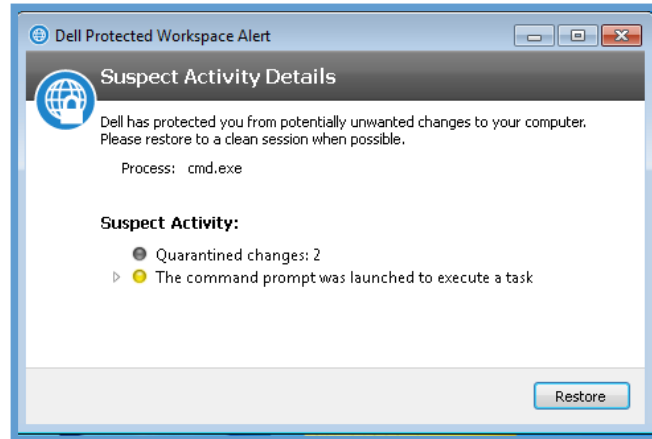
“Open Firefox” is used to open a Mozilla Firefox browser window within the DDP | Protected Workspace environment. If Mozilla Firefox is not available in the secured environment, it will not be displayed in this menu. The preferred browser defined in the preferences menu is **bold** and listed first (i.e. if **Mozilla Firefox** is the preferred browser, it will be listed first in this menu and will be **bold**.)

### Restore

The Restore option is used to restore the DDP | Protected Workspace environment to a clean state if suspicious activity has been detected or if the environment needs to be reset for any other reason. It is recommended that the DDP|PW environment is restored at least once every 72 hours if the end user PC is not shutoff or rebooted each night.

### Suspect Activity Details...

When suspicious activity has been detected by DDP | Protected Workspace threat detection engine, users may select the “Suspect Activity Details...” option to view further information regarding the activity. Users can click the “Restore” button from this window to restore the DDP|PW environment back to a clean state.



### Import Bookmarks...

The Import Bookmarks... option is used to import bookmarks from the native web browser(s) into the protected browsers. Currently, bookmarks can be imported from Internet Explorer and/or Mozilla Firefox. Bookmarks should be imported when the DDP | Protected Workspace Browser is first installed and any time that the bookmarks in the native browsers are updated. The bookmarks are not automatically synced so any future additions of bookmarks in the native browser that need to be opened in the protected browser sessions will need to be re-synced to DDP|PW via this link. Also, bookmarks cannot be exported or synced from the DDP|PW environment browsers back to the native browser(s).

### Preferences...

The Preferences... option is used to configure customizable settings for the DDP | Protected Workspace environment applications, such as auto-restore or setting DDP|PW as the default browser. The Preference options are explained in greater detail in the next section.

## About...

The About... option is used to view the current version of the DDP | Protected Workspace software that is running and to access available help information by clicking on the “Help” button located in the lower left corner of the About window. Users may also run the Tour again by selecting the “Tour” button.

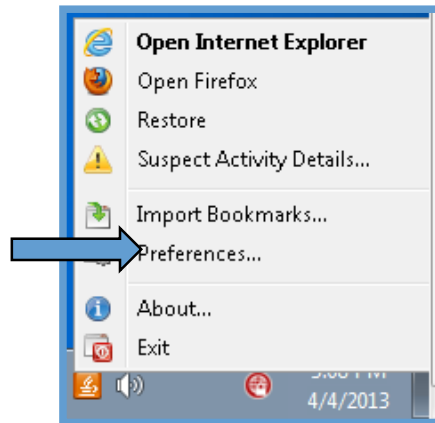


## Exit

The Exit option is used to cleanly close down the DDP | Protected Workspace environment when it is no longer needed or when it needs to be restarted completely.

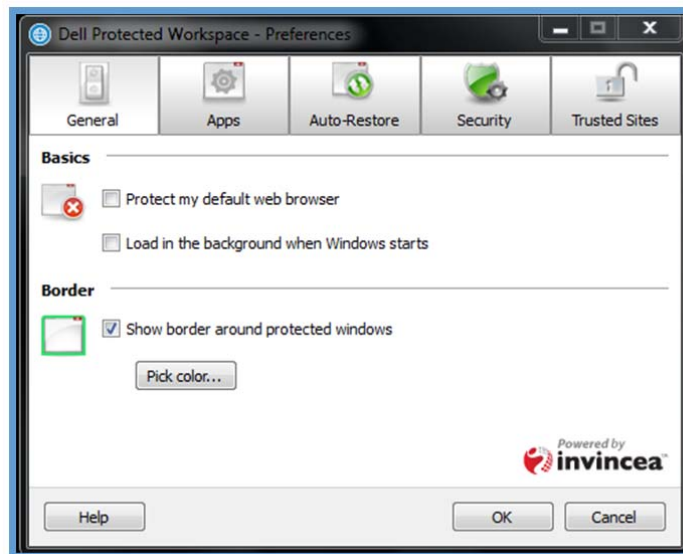
## Preference Menu Options

The following section identifies the options that are available in the user preferences interface. The Preferences interface can be accessed by right clicking on the DDP | Protected Workspace System tray icon and selecting Preferences...



### General Tab

The General Tab provides options for browser handling and application startup, along with the ability to control the protected environment application borders.



### Basics

The Basics section of the General tab allows modification of the two different options listed below.

#### *Protect my default web browser*

When this check box is selected, DDP | Protected Workspace will function as the default browser and will handle all default browser requests from other application. By unchecking this option, DDP|PW will



need to be manually opened in order to start a new protected browsing session. It is recommended that this option be selected to provide the most protection for your PC.

### *Load in the background when Windows starts*

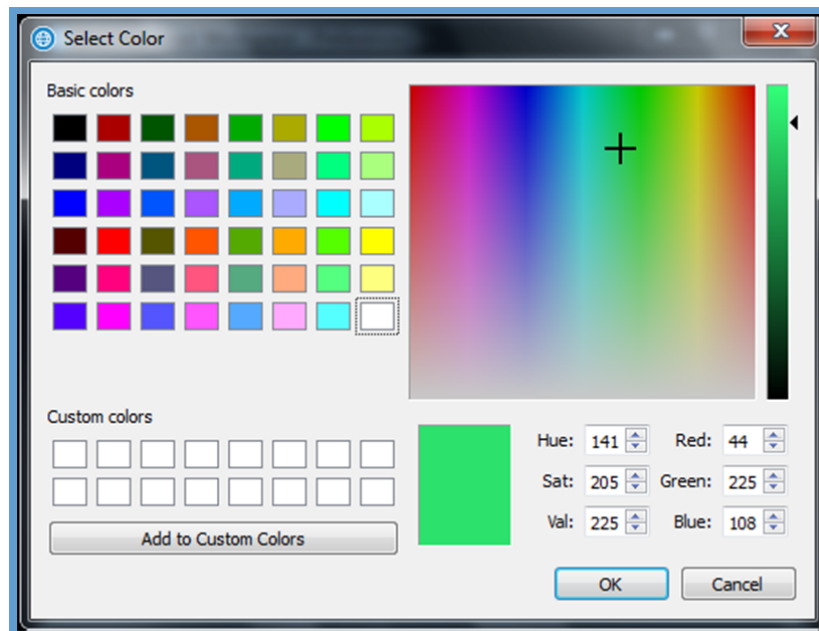
This check box will define if the DDP | Protected Workspace product will start automatically in the background each time the computer is restarted and as the user logs in. It is recommended that this option be checked so that the first time the product is used, there is no delay in bringing up the browser window.

### **Border**

The Border section of the General tab allows the user to enable or disable a colored border that is shown around protected application windows. To enable the border, simply check the option box. When this box is not checked, no border will be displayed. By default, the browser displays with a green border, but this can be customized by pressing the “Pick Color...” button and choosing a new color from the color picker. The new color will take affect when the OK button is pressed on the Preferences dialog.

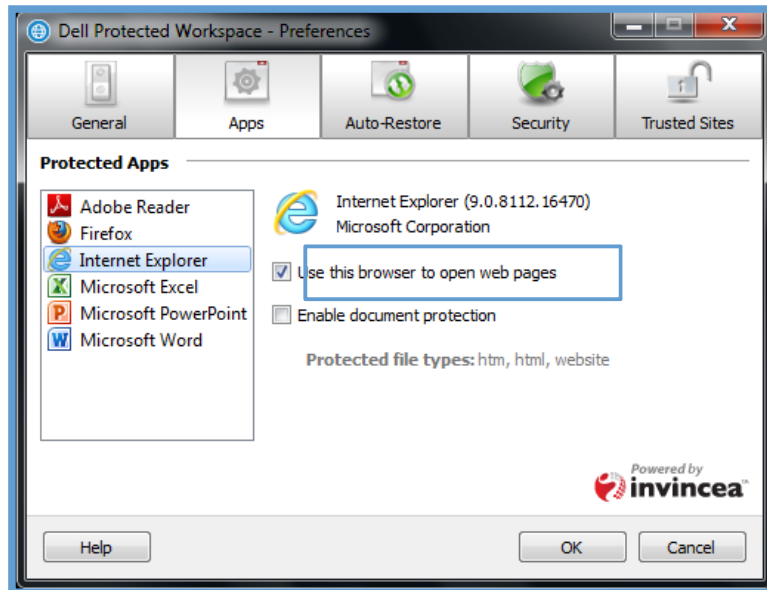
### *Color Selector Dialog*

To select a new border color, select one of the pre-populated colors, or enter your own color combination. Press OK to select the new color.

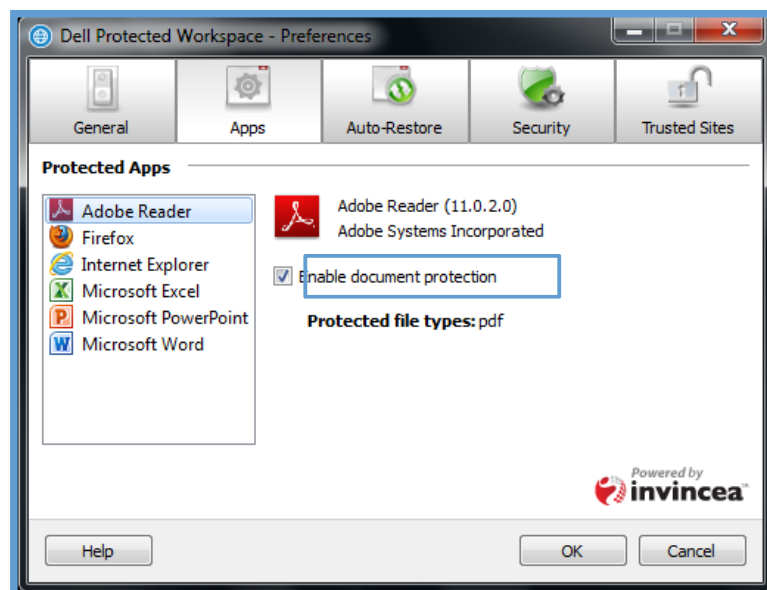


## Apps Tab

The Apps Tab provides the ability to specify which programs within the protected environment will be used to handle browsing and document protection. For web browsing, all available web browsers will be listed, and the user can choose which one will be preferred for browsing in the protected environment. This can be done by selecting “Use this browser to open web pages” for the browser that is preferred.

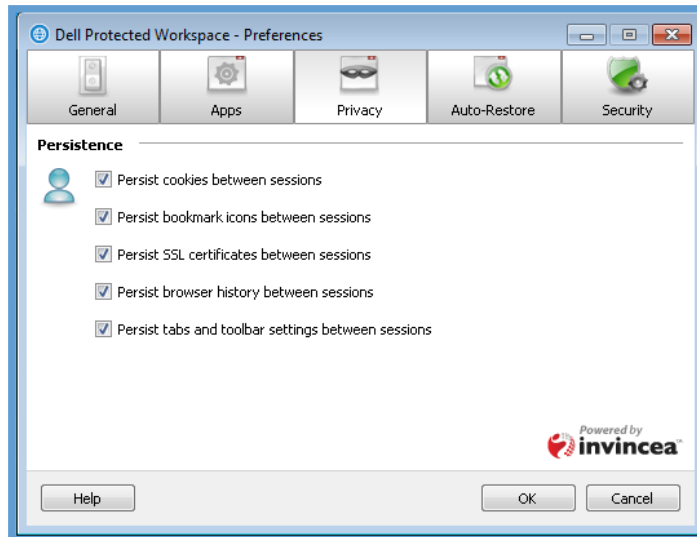


Additionally, for document handling, certain application can be specified to handle different documents types. By default, Adobe Reader is enabled to protect PDF documents within the protected environment, but alternative applications may be available, such as Adobe Acrobat. Document handling can also be enabled on Internet Explorer or Firefox for static pages htm/html pages stored on the local PC.



## Privacy Tab (v2.2.1-14451 only)

The Privacy Tab provides options for configuring the persistence of web browser content between restores of the DDP | Protected Workspace environment.



## Privacy Settings

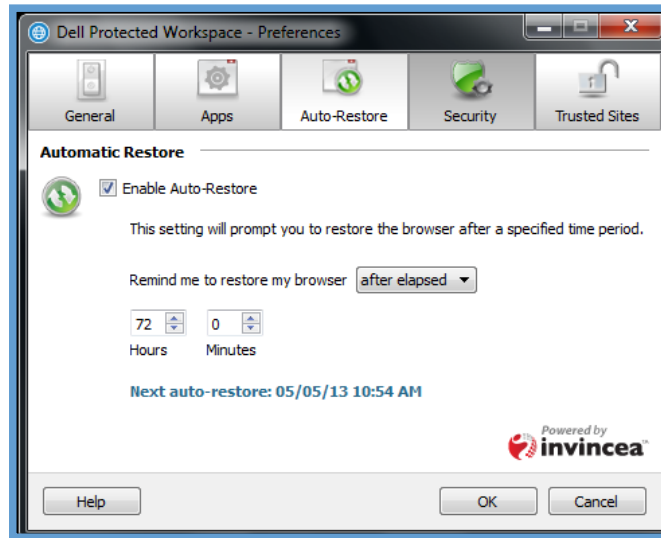
Within the Privacy Tab, the option to choose persistence of protected browser settings is available. By selected the check box next to any option, the protected browser will retain settings such as browsing history, bookmarks, passwords, auto-complete values and other configuration when the protected environment is restarted or restored. De-selecting any or all of these options will cause information and settings to be discarded each time DDP | Protected Workspace environment is restarted or restored. The recommended setting is to leave all boxes checked for persistence.

The following is a list of the settings available:

- Persist cookies between sessions
- Persist bookmark icons between sessions
- Persist SSL certificates between sessions
- Persist browser history between sessions
- Persist tabs and toolbar setting between sessions

## Auto-Restore Tab

The Auto-Restore Tab provides options for configuring the Auto-Restore settings.



### Automatic Restore

The Automatic Restore section of the Auto-Restore tab provides the ability to enable and disable a scheduled restore of the DDP | Protected Workspace environment. The Auto-Restore can be customized to occur on a defined schedule.

Selecting the Enable Auto-Restore checkbox will enable the auto restore feature with the settings selected. The restore will close all open DDP | Protected Workspace Browser windows and restore the DDP | PW browser to a clean state. If the checkbox is unselected, Auto-Restore will be disabled.

#### *Remind me to restore my browser option*

The “Remind me to restore my browser” option provides a drop down menu with three options: daily, weekly and after elapsed. The end user will be able to customize the schedule on which the DDP | Protected Workspace environment is auto restored based on these available options.

#### Daily Option

The “Daily” option changes the dialog box to allow the end user to select what specific time each day the protected environment will auto restore.

#### Weekly Option

The “Weekly” option changes the dialog box to allow the end user to select what day of the week the protected environment will be auto restored and at what exact time that day the auto restore will occur.

#### After Elapsed Option

The “After Elapsed” option allows the end user to select the time period in hours and minutes between protected environment restores. This time period will begin from the last time the DDP | Protected Workspace Browser was restored or started. For example, if this option is set to 12 hours, the

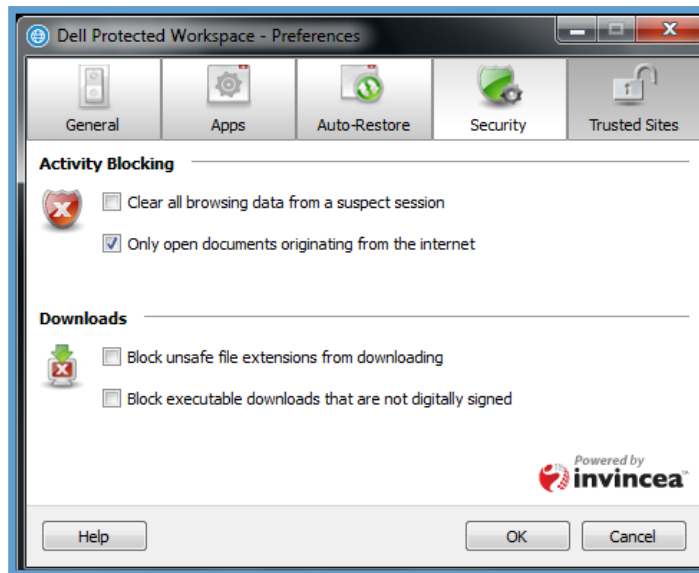
protected environment will be restored after the environment has been continually running for that period of time. The timer resets each time a restore or restart of the product is done. By default, Auto-Restore is enabled and set to restore every 72 hours.

### *Next auto-restore Display*

The Next auto-restore display indicates when the next auto-restore will take place based on the settings that are configured.

## Security Tab

The Security Tab provides options for configuring the Security settings.



### **Activity Blocking**

The Activity Blocking section of the Security tab gives the end user the ability to configure additional options on how certain activities are handled. Selecting the check mark in front of an option will enable that feature.

#### *Clear all browsing data from a suspect session*

This option allows for the DDP | Protected Workspace environment to clear all browsing data during a suspect session (when a suspicious activity alert is displayed). If the option is not checked, then the browsing history and data will remain intact when the restore happens. It is recommended that this option be enabled to ensure malicious changes to homepages or bookmarks are not persisted.

#### *Only open documents originating from the internet*

This option will allow only documents from the internet to be opened in the DDP | Protected Workspace environment. Documents which are created locally can be opened outside of the protected environment. When not selected, all documents will be opened in the protected environment (for document types that are handled by DDP|PW).

## Downloads

The Downloads section of the Security Tab gives the end user the ability to configure additional options on how files are handled when downloaded.

### *Block unsafe file extensions from downloading*

This option allows for DDP | Protected Workspace to immediately stop any blacklisted file types from being downloaded by a browser in the protected environment. If this option is not checked, the files will be downloaded to the DDP|PW downloads folder unless an infection is detected.

The following is a list of file types that will be blocked by enabling this option:

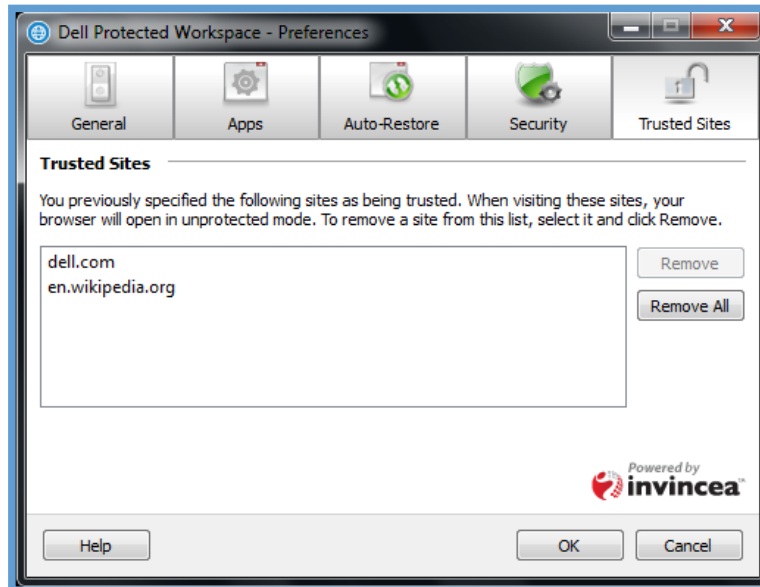
bas, bat, chm, cmd, com, cpl, crt, dll, exe, hlp, hta, inf, ins, isp, msc, msi, msp, mst, pif, reg, scr, sct, shb, shs, sys, vb, vbe, vbs, wsc, wsf, wsh

### *Block executable downloads that are not digitally signed*

This option allows for DDP | Protected Workspace to immediately stop downloading executable files without a digital signature. Executable downloads that are digitally signed (verified within the PE header) will be downloaded. If this option is not checked, the files will be downloaded to the “downloads” folder unless an infection is detected.

## Trusted Sites Tab

The Trusted Sites Tab provides the ability to remove previously specified Trusted Sites.



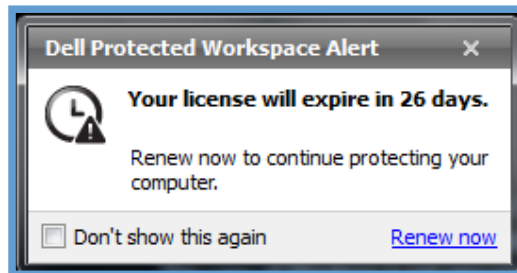
This tab displays the sites that were trusted via the “Unprotected this page” option in the drop down menu. Domains / URLs that were specified as “Always trust this site” will be listed. If a user wishes to remove a single domain / URL from this list, they can select the domain / URL to be removed and then can press the “Remove” button. If a user wishes to clear all of the domains / URLs listed, they can press the “Remove All” button.

## Subscription Renewal

---

DDP | Protected Workspace is a subscription based product that includes a one year subscription (when preinstalled on a DELL system). When the end of the subscription is approaching, DDP|PW will display a dialog above the system tray to indicate that the subscription needs to be renewed.

At 30 days prior to the end of the one year subscription to DDP | Protected Workspace, users will see a notification above the system tray with a link to renew the license. The notification will be displayed each time the product is restarted unless the “Don’t show this again” check box is selected. The dialog will then reappear seven days prior to the end of the subscription.



To renew a DDP|PW subscription, follow the “Renew now” link to the subscription renewal page. This action must be completed from each PC that needs to be renewed, as the “Renew now” URL includes the unique identifier needed to renew each PC's subscription.