Dell Data Protection | Protected Workspace

Administrator's Guide

June 2013 **Rev. A00**

Table of Contents

Section 1 – Overview and Basic Installation

Purpose and Intended Audience

This guide is intended for IT administrators who will be installing, deploying, and administering DDP | Protected Workspace. This guide is designed to help identify system requirements, identify pre-deployment tasks and to suggest deployment methodologies.

What is Dell Data Protection | Protected Workspace?

DDP | Protected Workspace provides a secure way to browse the internet by leveraging the existing web browser installed on an end user PC and allowing it to run inside the Protected Workspace isolated browsing environment (or bubble). DDP|PW also protects common documents safely such as Adobe PDFs, Microsoft Word, PowerPoint, and Excel. The isolated environment keeps unexpected malware from executing or installing on the host machine and is detected by the DDP|PW behavior based threat detection. Upon detection, the isolated environment is destroyed and a clean environment is recreated to ensure the end user machine is not compromised.

System Requirements

Supported Operating Systems

- Windows 7, 32 and 64-bit

Supported Hardware Platforms

- Dell OptiPlex
- Dell Precision
- Dell Latitude

Minimum System Specs:

- 1 GB RAM
- 500 MB free disk space
- Intel Pentium or better

Recommended System Specs:

- 2 GB RAM
- 500 MB free disk space
- Intel Core 2 Duo or better

Connectivity Requirements:

- A connection to http://delllicense.invincea.com (port 80) is required in order to activate the product license.
- A connection to https://dellupdate.invincea.com (port 443) is required for product updates

Supported Software

DDP | Protected Workspace leverages software installed on an end user machine and runs that software inside an isolated environment. To ensure proper functionality within the isolated environment, only certain software and versions are supported. Any unsupported software or version will not be moved into the isolated environment and will continue to only run in the native interface.

Supported Browsers

- Internet Explorer 7-10
- Mozilla Firefox 10-21

Supported PDF Readers

- Adobe Reader 9, X, and XI
- Adobe Acrobat 9, X and XI

Supported Document Programs

- Microsoft Word, 2010 and 2013
- Microsoft Excel, 2010 and 2013
- Microsoft PowerPoint, 2010 and 2013

Supported Browser Plugins

- Java Runtime Environment 1.6+
- Adobe Flash 11 +
- Apple QuickTime 7 +
- Microsoft Silverlight

Basic Installation

DDP | Protected Workspace is packaged with a pre-defined set of preferences and configuration and can be installed without any custom configuration. It can be installed by following these steps.

1. Download the DDP | Protected Workspace Installer.
2. Run the DellSetup_<version>.exe.
3. Select the installer defaults.
4. Finish the DDP | Protected Workspace installer.
5. Start DDP | Protected Workspace by double clicking on the desktop icon.

Section 2 – Enterprise End-User Deployments

Deploying Dell Data Protection | Protected Workspace with Software Deployment Tools

DDP | Protected Workspace installation is supported with many different software deployment tools. Currently, Protected Workspace is tested with GPO, IBM Tivoli Endpoint Manager (previously BigFix), Microsoft SCCM and Symantec Altiris, however deployments should work with all deployment tools.

Protected Workspace EXE Installer Options

This section details options to be used for installing Protected Workspace on end-user PCs directly or with a system management tool.

- Silent install using default options
  `DellSetup_<version>.exe /S /v/qn`
- Silent install with changing the install folder. Example changes install path to C:\TEST:
  `DellSetup_<version>.exe /S /v"/qn INSTALLDIR="C:\TEST"`
- Silent uninstall (leave user files)
  `DellSetup_<version>.exe /S /x /v/qn`
- Silent uninstall (removes user files)
  `DellSetup_<version>.exe /S /x /v "/qn PRESERVE=\"0\""`
- Silent upgrade
  `DellSetup_<version>.exe /S /v/qn`

Connectivity requirements

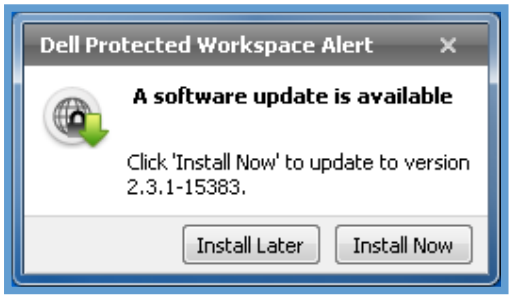
Product Activation

After installing DDP | Protected Workspace, the product requires internet access in order reach out to the activation servers. If internet access is not available, the product will ask the user to check the settings and try again.

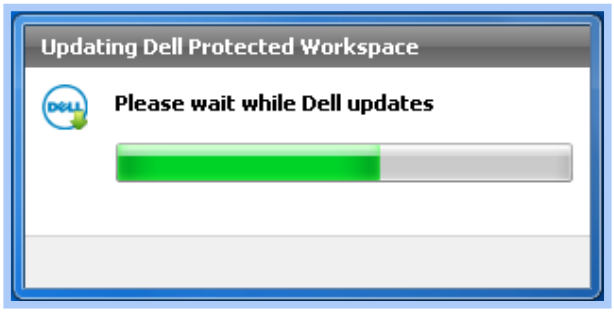
If the environment contains a web proxy or other device, it is important that access to http://delllicense.invincea.com be allowed on port 80.

Product Updates

DDP | Protected Workspace is designed to notify the user when an update is available. When an update is applied, the update will be downloaded in the background while the product is running, and will apply when the product is restored or exited and restarted.



During the update process, a dialog box will display over the system tray, indicating that the update is taking place.



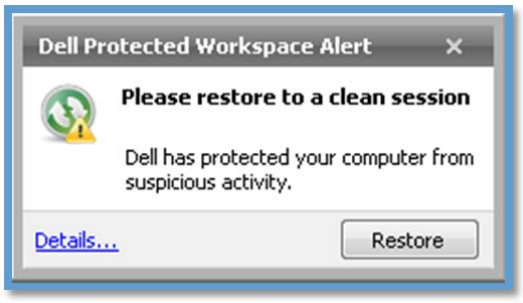
In order for the automatic updates to occur, it is important that the product have a connection to the internet and that if the environment contains a web proxy or other device, access to http://dellupdate.invincea.com be allowed on port 443.

Section 3 – Administration

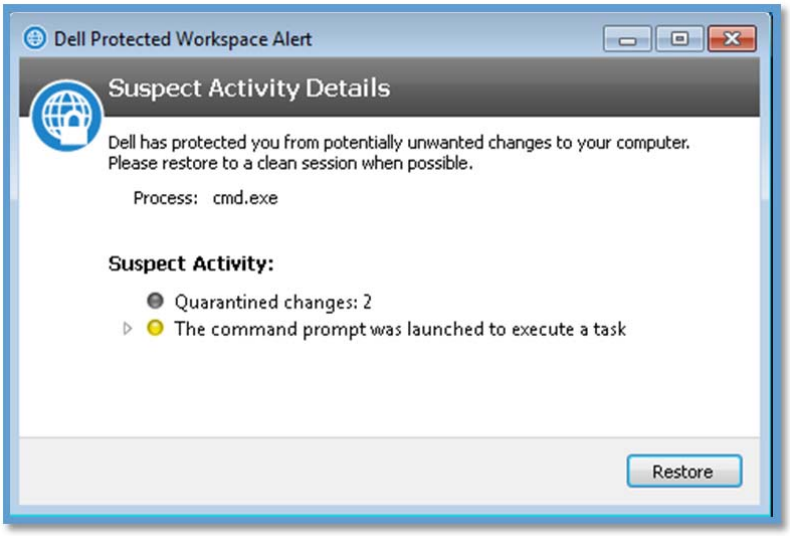
End-User Experience

Threat Detection

DDP | Protected Workspace offers built in threat detection to help identify if the DDP|PW environment has been compromised by an untrusted process. When suspicious activity has been detected, a dialog will display over the system try indicating that the user should restore to a clean session. It is recommended that the Restore button be pressed immediately to restore to a clean session, but the user does have the option to close the dialog box with the "x" in the corner and to continue using the product. A restore can be done at a later time.



The user can click the "Details..." link in the bottom left corner of the message to display additional details about the suspicious activity. The dialog will identify the process that was flagged as suspicious and will also give details about what that process did within the protected environment. From this dialog, the user can either close the window by clicking on the X in the upper right corner, or can restore the session using the restore button.



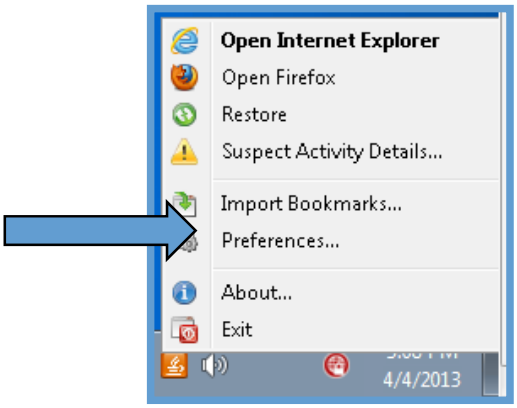
If the user chooses to restore later by dismissing the Suspicious Activity dialog the Protected Workspace icon on the system tray will turn red until the user restores DDP | Protected Workspace to a clean state.

DDP | Protected Workspace ensures that any threat is contained within the protected environment and that the end user system has been protected.

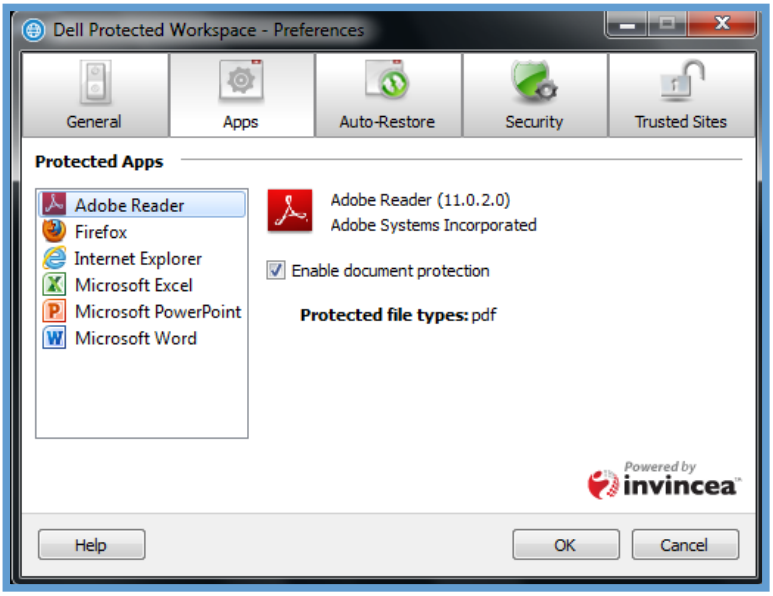
Apps Tab

A tab called the "Apps" tab in the preference GUI allows the users can use to specify which programs within the protected environment will be used if there are multiple options (such as with both Internet Explorer and Firefox) and which programs will act as default handlers for certain file (such as Adobe Reader for PDFs).

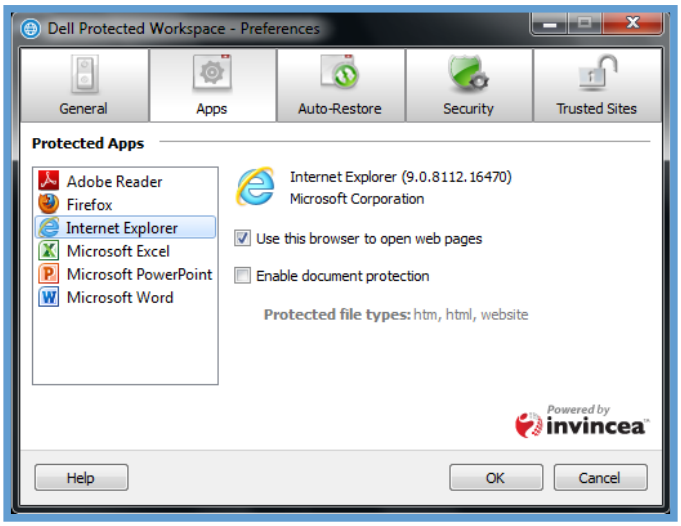
To access the Apps tab, right clicking on the DDP|PW Icon in the system tray, and selecting "Preferences…"



Below is a screenshot of the Apps tab. Applications that have defined file handlers within the protected environment will list "Protected File Types" and will have a checkbox to enable that application as the handler for that file type. For example, if both Adobe Reader and Adobe Acrobat are installed on a client machine, the user can choose which will be used to open PDF files with the protected environment. The user will not be able to select multiple applications for the same handler.



Additionally, from the Apps tab, users will be able to select which browser will be used to open webpages by default within the protected environment. The user can select "Use this browser to open web pages" for either Internet Explorer or Firefox.



Administrative Preferences Override

In some organizations, administrators may want to disable the ability for DDP | Protected Workspace from reaching out to the DDP|PW servers for software updates, error reporting and threat detection reporting. These options can be disabled by adding an override file on each PC. It is recommended that these options not be used unless absolutely necessary.

The override file is a simple XML file that can be created in Notepad or a similar text editor. Create a file with the name "preferences.xml" and copy the following text into it:

```
<?xml version="1.0" encoding="UTF-8" ?>
<preferences ver="3">
     <error_report enabled="false" />
     <software_update enabled="false" interval="daily" user_modifiable="false" />
     <send_threat_reports enabled="false" prompt="false" />
</preferences>
```

Once this file is created, it needs to be placed on to each PC that needs the override. The location for this file needs to be:

C:\ProgramData\Invincea\Enterprise\Admin

Once this file is in place, start (or restart) the DDP | Protected Workspace product and these overrides will take effect.

Override Settings Details

<error_report enabled="false" />

The error_report option disables the ability for DDP | Protected Workspace product to send error reports when a product error occurs. When an error window is displayed the "Submit" will be disabled.

<software_update enabled="false" interval="daily" user_modifiable="false" />

The software_update option disables the ability for DDP | Protected Workspace product to automatically apply critical updates to the product. These critical updates allow for errors to be correct as they are reported and should be allowed to ensure that latest critical updates are always applied.

<send_threat_reports enabled="false" prompt="false" />

The send_threat_reports option disables the ability for DDP | Protected Workspace product to report home when a suspicious activity is detected. These reports help to ensure that the product detection is working correctly and is not triggering alerts when no actual threat is present.

Administrative Trusted Sites Override

By design the DDP | Protected Workspace product runs the users native web browsers within an isolated environment. This isolated environment keeps the user's PC safe from malicious content but can also cause some interoperability issues with certain websites. If these websites are business critical and trusted, the users have the ability to manually trust them locally. By trusting them, these sites will be opened within the native browser if the URL is browsed to in the protected environment.

As an added convenience, administrators have the ability to apply an override file that adds a set of trusted sites without any user interaction.

The override file is a simple TXT file that can be created in Notepad or a similar text editor. Create a file with the name "trustedsites.txt"

Once this file is created, it needs to be placed on to each PC that needs the override. The location for this file needs to be:

C:\ProgramData\Invincea\Enterprise\Admin

Once this file is in place, start (or restart) the DDP | Protected Workspace product and these overrides will take effect.

The format of the trusted URLs needs to be in REGEX format. The following section outlines how to create URLs in the correct format.

Here are some examples of correctly formatted URLs. The pound sign (#) indicates a file comment:

```
#The following lines designate trusted sites/domains
^https?://([^/]*\.)*adobe\.com/.*
^https?://([^/]*\.)*acrobat\.com/.*
^https?://([^/]*\.)*webex\.com/.*
^https?://([^/]*\.)*dell\.com/.*
^https://internal\.dell\.com:8080/.*
^ftp://dell/.*
```

The product performs a line by line examination of the trustedsites.txt file and stops at the first match. The following section outlines some possible entries into the trustedsites.txt file and what the resulting outcome would be.

```
^ftp://dell/.*
```

The above entry would match anything that starts with *ftp://dell/* and would allow any additional text after the last /.

```
^https?://([^/]*\.)*dell\.com/.*
```

The above entry would match anything that starts with "http://" or "https://", ends with ".dell.com/" and allows any sub domains of dell.com. [^/]* is anything that doesn't contain a "/" so "dell.com" must show up in the base portion of the URL. In other words, this will match http://anything.dell.com/*, but will not match http://fakedell.com/* or http://anything.com/?imageurl=fake.dell.com/*.

```
^https://internal\.dell\.com:8080/.*
```

The above entry will match the exact site and port specified and anything that follows.

To add local IP subnets, use the following format:

```
^https://192\.168\.1\.*(:\d{1,5})?/.*
```

The above entry will match any URL that uses http or https, and is accessed with a 192.168.1.x subnet IP address. It also allows for any port to be used on this URL.

It is important to note that trustedsites is not able to do DNS lookups. Therefore, trusting a specific subnet of addresses does not trust their associated DNS names. If DNS names need to be used for the trustedsite list, each DNS name must be listed out.

```
^https://([^/]*\.)*sharepoint\.*
^https://([^/]*\.)*myinternalserver\.*
```

Regex Pattern Recommendations

Below are some regex patterns that can be used to create custom entries.

"^" Beginning of the line.

"?" Match zero or 1 of the previous character

"$" End of the line.

"\." Period character. (A "." matches any character.)

".*" Match any number (zero or more) of any characters.

untrusted= Un-match the regex instead of match.

"[^/]*" Match any number of any characters except "/".

Trusted Sites Caution:

Be aware that the whole URL string is passed to DDP | Protected Workspace and matched against this list. Slight variations in syntax can make a difference between matching and matching in the way you intend. As an example, the URL:

```
http://www.dell.com$
```

is not safe and would not match. It would not match because a trailing "/" is often added by Windows before the URL is passed to applications. It is not safe because this string could be part of the parameters of an URL and not the web site you intended.

.*www.dell.com.*

matches if "www.dell.com" appears anywhere in the URL, not just as the address - such as matching http://www.fakesite.com/spoofsite=http://www.dell.com/

User Trusted Sites List

From DDP | Protected Workspace, a user has the ability to trust sites locally. These sites will be added to the beginning of the list of sites provided within an administrative override file. For example, if an admin trusts the following:

```
^https://([^/]*\.)*sharepoint\.*
^https://([^/]*\.)*myinternalserver\.*
```

And a user trusts:

```
google.com
yahoo.com
```

Then the full list of trusted sites for this PC will include all of the sites outlined:

```
^https?://([^/]*\.)*google\.com/.*
^https?://([^/]*\.)*yahoo\.com/.*
^https://([^/]*\.)*sharepoint\.*
^https://([^/]*\.)*myinternalserver\.*
```

Troubleshooting

Manually Troubleshooting Installation Issues

There are two log files that are generated during the installation of DDP | Protected Workspace that can offer insight as to why an installation may have failed.

The first file is the MSI output file. If the installer is run manually via the standard executable, this file will be created in the C:\Windows\Temp directory. The log file name will be InvEnterpriseMSI.log. This file will provide details on failures that happened during pre-checks, such as disk space, memory or other system requirements.

The second file is the DDP | Protected Workspace installer file. It will be located in the same directory as the MSI file, and will be named InvEnterpriseInstall.log. This log will provide indication of failures during the installation and configuration process. Any errors will be tagged in capital letters with the word ERROR or FATAL after the date and time stamp. Any line that is tagged with DEBUG, TRACE or INFO can be ignored.

Manually Troubleshooting Post-Installation Issues

There are three log files that are primarily used to identify issues post-installation.

The first file is the log file for the DDP | Protected Workspace Service and is named InvProtectSvc.log. This is a global log file that logs information across all user accounts. The first location is:

C:\Windows\Temp\Invincea\

This log provides information about the applications that we detect during startup (such as the version if IE, Adobe Reader, Java, Flash, etc.) and what locations of the host system are accessible by the isolated environment or not.

As with the installer log files, errors will be noted at ERROR or FATAL after the date and time stamp.

> 2012-05-02 08:04:33,203 **ERROR** Inv.MC.TCPConnection - [5864] SSL Handshake error: An existing connection was forcibly closed by the remote host

The second file is the log file for the instance of DDP | Protected Workspace running under a user context. This file is named inv.log and is located in the users AppData folder. Each user on a single PC will have an inv.log file. This file will help identify if there are unsupported versions of an application installed, or communication issues with needed resources.

While logged in as the user having issues, the log file can be found at this address on all OSs:

> %APPDATA%\Invincea\Enterprise\inv.log

Again, any errors will be marked with ERROR or FATAL after the time and date stamp.

> 2012-05-22 12:48:59,157 **ERROR** Inv.TaskMgr - Error: Timeout when performing Restore, Wait for Guest Connect