



# Opatch Agent

## User Manual

(build 2017.10.10.10620)

revision 84

(c) Opatch by ACROS Security, 2018

<https://0patch.com>



## Contents

1. What is Opatch?.....	3
2. Understanding Opatch.....	5
3. Supported Operating Systems.....	7
4. Network Connectivity.....	8
5. Installing Opatch Agent.....	10
6. Agent Registration.....	11
7. Opatch Console .....	12
8. Console Layout .....	13
9. Dashboard .....	14
10. Applications.....	16
11. Patches .....	19
12. Settings .....	20
13. Log .....	20
14. Pop-up Messages .....	21
15. Tray Icon .....	24
16. Updating Opatch Agent .....	25
17. Troubleshooting .....	27



## 1. What is Opatch?

Opatch is a microscopic solution for a huge security problem. It delivers tiny patches of code to computers worldwide to fix software vulnerabilities through which criminals and spies can break in and take control.

These "3rd party" fixes (we call them "Opatches") are tiny patches of code (usually just a few bytes – so small that they could be delivered via Twitter), making them inexpensive to test and review, and extremely unlikely to cause functional problems to corrected software. Moreover, system administrators are able to apply or remove them without having to re-launch corrected applications (much less restart computers), avoiding any downtime for users that is typically associated with official security updates.

Opatch is resolving various painful IT security issues of today:

<b>The Pain</b>	<b>The Opatch Solution</b>
No vendor patches are available for 0day vulnerabilities, leaving users exposed to 0day attacks.	Opatch provides patches for various 0day vulnerabilities using our extensive global network of security researchers.
Patches exist, but are not applicable (e.g. many Java applications require particular version of Java, so it is not possible to update to the latest version).	Opatch provides patches for non-current (old) versions of applications (including Java), preventing attackers from exploiting known security bugs.
Official patch deployment is expensive, causing a huge financial burden for big corporations.	Opatch is extremely light-weight, allowing you to apply and remove patches in running processes instantly without a need to restart applications or reboot computers.
Vendor patches could be extremely complex and replace hundreds of megabytes of code, making it impossible to control code on critical systems.	Opatches are so tiny that an administrator can manually review each one of them before deploying it. An average Opatch consists of just a few machine code instructions.
Patch deployment testing is very difficult for high-availability systems (especially if patching requires system restart).	Opatch never requires you to restart a computer, or even relaunch an application or restart a service. Opatches are applied to running processes - and removed from them if you so choose.
Large vendor patches often break or modify functionalities.	Each Opatch addresses one single vulnerability and introduces no functional changes to the application. Users will never notice that a Opatch has been installed.



No patches are available for custom-built software.	We can create Opatches for any software product you may be using.
Legacy software is often unsupported and without security fixes.	We can create Opatches for software that is no longer supported, even if its vendor no longer exists. If you're using it, we can Opatch it.
No patches are available for many widely used, but no-longer-supported platforms (e.g. Windows XP or Microsoft Office 2003).	We create Opatches for unsupported Windows platforms and products, allowing you to continue using them with maximum possible protection.
No patches are available because software vendor does not exist any-more.	We can create Opatches for software that is no longer supported, even if its vendor no longer exists.
Absence of security patches means non-compliance with various standards.	Opatches can help you stay compliant with standards that require staying up-to-date with security fixes.
Patch production, testing and deployment are very expensive for software vendors.	Developing, testing and deploying of Opatches is as inexpensive as it could possibly be.



## 2. Understanding Opatch

This article provides a short description of the basic concepts you need to be familiar with in order to understand how Opatch works and how you can use it.

Software products often contain **vulnerabilities** - flaws that allow attackers to take control of one's computer.

A **patch** is a small package with a few code instructions that replace a vulnerable section of code in a running application. A patch therefore **fixes a vulnerability**.

A patch is considered **installed** as soon as it is downloaded from the server and stored in a local database. This does not automatically mean that it is applicable to your computer, only that it is there waiting to be used in case it is needed.

An installed patch can get **applied** to a **running process** in order to eliminate a vulnerability in that process. This means that the vulnerable code section in the process is replaced with corrected code from the patch. While normally, a patch always gets applied to the vulnerable process it was designed for, but this can be prevented by either disabling the patch, excluding an application from patching, or disabling the Opatch Agent.

When a patch is **removed** from a running process, the corrected code from the patch is removed, and the original (vulnerable) code is restored in the process. Consequently, the process again becomes vulnerable to the attack previously blocked by the patch.

Opatch does not change executable files on the file system. It only modifies running processes, which makes it really easy and quick to apply and remove patches without even relaunching applications, much less restarting your computer. Patching is done instantly and (if you want) silently, and so is un-patching.

Normally, all applications are being patched, which allows Opatch to provide maximal protection. However, for troubleshooting purposes, any application can be manually **excluded from patching**. Such application does not get any patches applied until it gets **un-excluded**.

Each patch, when downloaded from the server, is initially **enabled**, which means it is getting applied to processes it was designed for.

For troubleshooting purposes, any patch can be manually **disabled**, which causes its immediate removal from all processes in which it is applied, and prevents its application to newly launched processes. Naturally, a disabled patch can be manually re-enabled.

The **Opatch Server** can mark an installed patch as **revoked**, which permanently disables the patch without an option to manually enable it. This usually happens because a better patch was issued for the vulnerability fixed by the revoked patch.



Patches are being applied to processes by the **Opatch Agent** running on the computer. Opatch Agent must be **registered** on the Opatch server in order to receive patches. To register Opatch Agent, one needs a **Opatch account** on the Opatch Server.

Once registered, Opatch Agent periodically contacts Opatch Server to see if any new patches are available - and downloads them if they are. We call this process **syncing** (i.e., synchronizing with server).

Opatch Agent also periodically sends **telemetry data** to Opatch server, allowing us to monitor for problems and usage in order to be able to provide a better service. Telemetry data consists of computer name and platform, local IP addresses, data on executable modules being loaded on the computer, data on applied and disabled patches, data on excluded applications and whether Agent is enabled or not.



### 3. Supported Operating Systems

Opatch Agent currently works on the following platforms:

- Windows Workstations
  - Windows 10, 32 and 64 bit
  - Windows 8.1, 32 and 64 bit
  - Windows 8, 32 and 64 bit
  - Windows 7 SP1, 32 and 64 bit
  - Windows Vista, 32 and 64 bit
  - Windows XP SP3, 32 and 64 bit (fully updated)
- Windows Servers
  - Windows Server 2016 64 bit
  - Windows Server 2012 R2 64 bit
  - Windows Server 2008 R2 SP1, 32 and 64 bit
  - Windows Server 2008, 32 and 64 bit
  - Windows Server 2003 R2, 32 and 64 bit
  - Windows Server 2003 SP2, 32 and 64 bit (fully updated)



## 4. Network Connectivity

In order to get registered and download patches from the server, Opatch Agent needs to be able to connect to the Opatch Server. It initially connects to the Opatch Server immediately after installation when you register the Agent, and then every 60 minutes when it »syncs« with the server to see if any new patches have become available.

Note that the Opatch Agent is protecting you and applying all applicable patches it has previously downloaded from the Opatch Server even when your computer is offline or otherwise unable to connect to the Opatch Server. Being unable to connect to the server only means that the local patch database cannot be updated.

### Firewall

Your firewall, if you have one, must allow the Opatch Agent to connect to host **dist.Opatch.com** on port **443**. In case you can set networking permissions for individual processes, you need to allow processes **OpatchConsole.exe** and **OpatchService.exe** to initiate the above connections.

### Proxy Server

If you want Opatch Agent to establish connections via a proxy server, you need to configure that manually in the registry. As administrator, launch **regedit.exe** and open the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Opatch** key. There are three values under this key that allow you to configure proxy server communication:

- **ProxyHost** – if empty, no proxy server will be used (the default setting); if non-empty, the proxy host in this value will be used, along with the proxy server port in the ProxyPort value
- **ProxyPort** – if proxy server is used, this value will be used as the proxy server port
- **ProxyScheme** – this value defines the proxy authentication scheme as follows
  - 0 – no authentication will be performed on the proxy server
  - 1 – BASIC authentication

If **ProxyScheme** is set to 1 (BASIC authentication), there are two additional values you have to set under the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Opatch\ProtectedSettings** key. Note that unless you run **regedit.exe** as administrator, you won't be able to even open this key because non-admin users are not allowed to read proxy server credentials.

- **ProxyUsername** – this value will be used as username
- **ProxyPassword** – this value will be used as password





Note that even after you configure a proxy server, Opatch Agent will still attempt to make a direct connection to the server if it fails to do so via the proxy server. This allows portable computers to stay up to date with patches both inside the corporate network and outside.



## 5. Installing Opatch Agent

**Note 1: Do not try to install Opatch Agent remotely via Remote Desktop Connection.** You must install Opatch Agent by directly logging in to the machine.

**Note 2: If you want to install Opatch Agent in a Windows XP Mode, please consider:**

in order to install Opatch Agent inside "Windows XP Mode", you need to "Disable Integration Features" in the Windows Virtual PC "Tools", then install Opatch Agent, and finally (optionally) select "Enable Integration Features" in the "Tools" menu. Note that the Virtual PC "Windows XP Mode" is using Remote Desktop Connection for accessing the Windows XP desktop.

In order to install Opatch Agent, you need to have - preferably the latest - installer package. You can obtain the latest Opatch Agent installer package from <http://Opatch.com/download.htm>.

- Windows Vista, Windows 7, Windows 8 and Windows 2008 Server
  - If you are logged in as a member of Local Administrators, double-click the installer package and confirm the elevation prompt when requested.
  - If you are not logged in as a member of Local Administrators, double-click the installer package and provide username and password for an administrator account when requested.
- Windows XP and Windows 2003 Server
  - If you are logged in as a member of Local Administrators, double-click the installer package.
  - If you are not logged in as a member of Local Administrators, log out and log in as a member of Local Administrators, then double-click the installer package.

When asked, confirm your acceptance of end-user license agreement.

Select where on the file system you want to have Opatch Agent installed, or simply keep the suggested location.

Keep the "Launch Opatch Console" checkbox ticked to have the Opatch Console automatically launched when installation is completed. Note that you may have to confirm elevation or provide administrative credentials for Opatch Console to get launched.

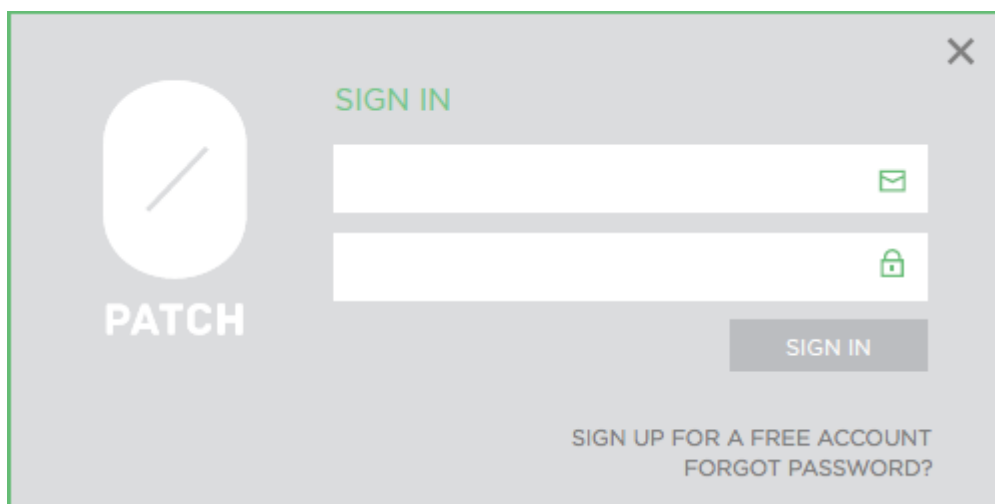
If you want to launch Opatch Console at any time, you can do so by right-clicking the Opatch icon in the system tray and selecting the "Console" menu item, or via the Start button.

## 6. Agent Registration

Before Opatch Agent can download any patches from the server and start protecting your computer, it needs to get registered on the server. This links the Agent to your Opatch account on the Opatch server.

Agent registration is done by signing in to your Opatch user account with your email address and password from the Opatch Console. If you leave the "Launch Opatch Console" checkbox ticked when installing Opatch Agent, the Console will automatically get launched and will immediately ask you to sign in.

**Note: Make sure that network connectivity is properly configured as described in section 4, otherwise you will be receiving »Unable to connect to the server« error message.**



The Console will not be accessible until the Agent has been successfully registered. As soon as the Agent is registered, it will start downloading patches from the Opatch server and applying them to running processes on your computer (as applicable).

**Note: If you don't have a Opatch account yet, you can get a free account by registering at <https://dist.Opatch.com/User/Register>.**

If Opatch Agent is already registered to a Opatch account and you wish to register it to another account instead, you can launch Opatch Console and click "Register to another email". This will open the Sign In form, allowing you to provide email and password for the other Opatch account. If you successfully sign in, the Agent will be registered to the new Opatch account; otherwise, it will remain being registered to the previous Opatch account.



## 7. Opatch Console

Opatch Console allows you to:

- view important information about patches and applications on your computer,
- enable or disable Opatch Agent,
- enable or disable individual patches,
- exclude selected applications from patching,
- configure the appearance of pop-up messages,
- update Opatch agent to the latest version, and
- view the activity log.

Opatch Console is automatically launched after successful installation of Opatch Agent if you leave the "Launch Opatch Console" checkbox ticked.

You can launch Opatch Console at any time by right-clicking the Opatch icon in the system tray and selecting the "Console" menu item, or via the Start button.

Note that Opatch Console needs to be running with administrative privileges. If you're not logged in to Windows as a member of Local Administrators, you will need to provide administrative credentials to launch the Console. On Windows Vista, Windows 7, Windows 8 and Windows Server 2008 you may need to confirm the elevation prompt.

## 8. Console Layout

Opatch Console consists of three main areas as shown in the following image.



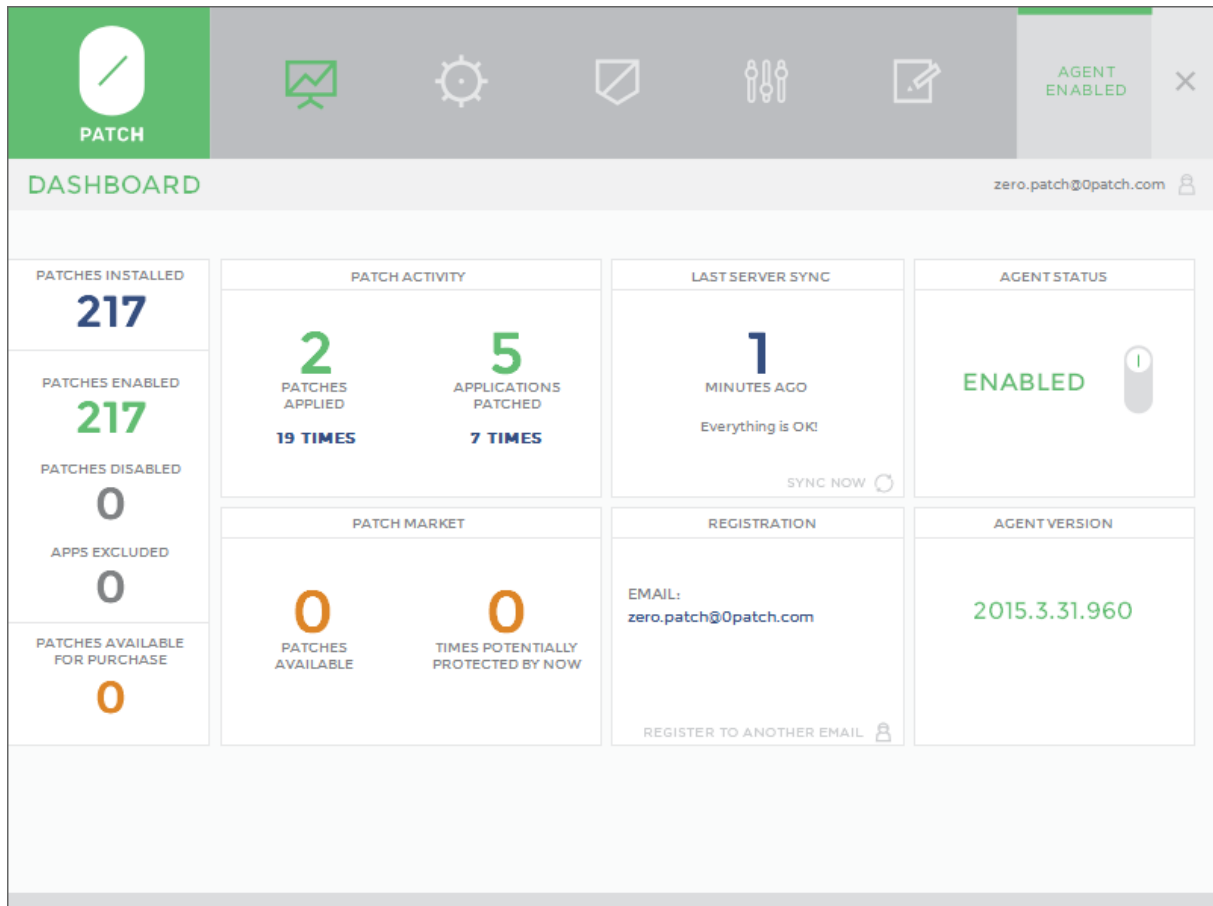
The **Menu bar** provides access to various pages of the Console: Dashboard, Applications, Patches, Settings and Log. It also shows the email address of the Opatch account to which the Agent is registered.

The **Counters** display the number of patches present on your computer, the number of enabled and disabled patches, the number of applications that have been excluded from patching, and the number of patches that are available for purchase.

The **Main area** displays the content of the page selected via the menu.

## 9. Dashboard

The dashboard provides top-level information about the status of your computer. It consists of various areas as shown on the following image.



The **Patch Activity** box displays real-time counters for:

- how many individual patches have been applied at least once to applications on your computer,
- how many times a patch has been applied on your computer,
- how many individual applications have been patched (with one or more patches) on your computer, and
- how many times applications on your computer have been patched.



The **Last Server Sync** box displays the amount of time passed since the last time Opatch Agent has successfully received updates from the Opatch server (i.e., the last time it has done a successful "sync"). It also provides short information about the status of the last sync attempt, or any problems that may be causing the Agent to fail syncing.

The **Agent Status** box allows you to enable or disable the Agent. Normally, the Agent is enabled, which means it is patching applications on your computer and periodically downloading new patches from Opatch server. If you disable the Agent, it removes all patches from currently patched applications and stops applying patches to them until you re-enable it.

The **Patch Market** box shows how many times patches that you haven't purchased would have protected your computer if you had purchased them. This allows you to assess the value of a license before you purchase it.

The **Registration** box shows the email address to which Opatch Agent is currently registered. You can change the registration to another email by clicking "Register to another email"

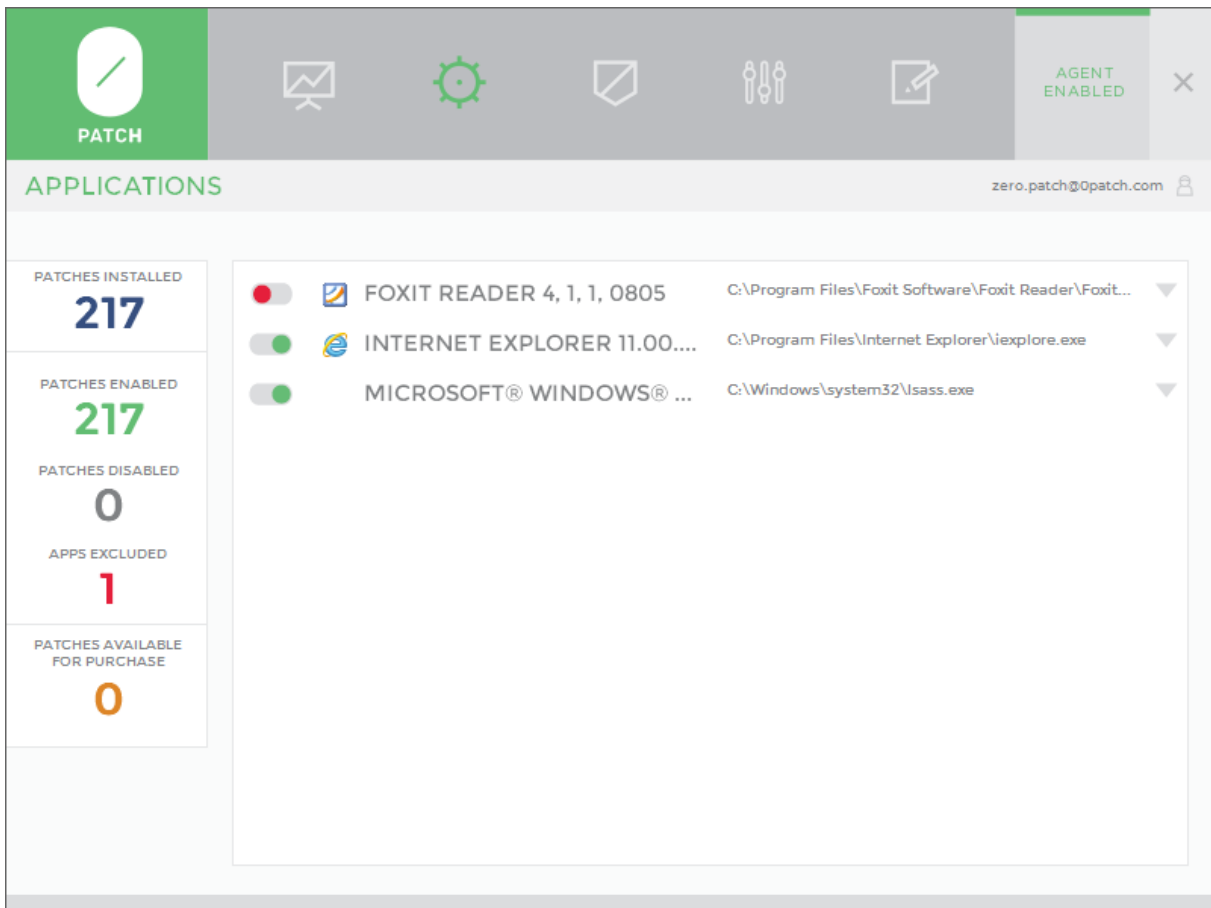
The **Agent Version** box shows the version number of Opatch Agent. When a new agent is available, this box also provides the "Get latest agent" button you can use to launch the update process and install the latest Agent.

## 10. Applications




The Applications page displays a list of all applications on your computer that have been patched at least once, and allows you to:

- exclude individual applications from patching, and
- see which patches have been applied to each application.

**Note: The Applications page does not show currently running applications, but those that have been patched at least once.**



The screenshot shows the PATCH Applications page. The top navigation bar includes the PATCH logo, several icons (mail, gear, shield, sliders, document), and an 'AGENT ENABLED' status with a close button. The main header is 'APPLICATIONS' with a user profile icon for 'zero.patch@opatch.com'. On the left, a summary panel displays: PATCHES INSTALLED: 217; PATCHES ENABLED: 217; PATCHES DISABLED: 0; APPS EXCLUDED: 1; PATCHES AVAILABLE FOR PURCHASE: 0. The main content area lists three applications with their patch status (toggle), icons, names, and file paths:

Toggle	Icon	Application Name	File Path	Action
<input type="checkbox"/>		FOXIT READER 4, 1, 1, 0805	C:\Program Files\Foxit Software\Foxit Reader\Foxit...	▼
<input checked="" type="checkbox"/>		INTERNET EXPLORER 11.00....	C:\Program Files\Internet Explorer\iexplore.exe	▼
<input checked="" type="checkbox"/>		MICROSOFT® WINDOWS® ...	C:\Windows\system32\lsass.exe	▼



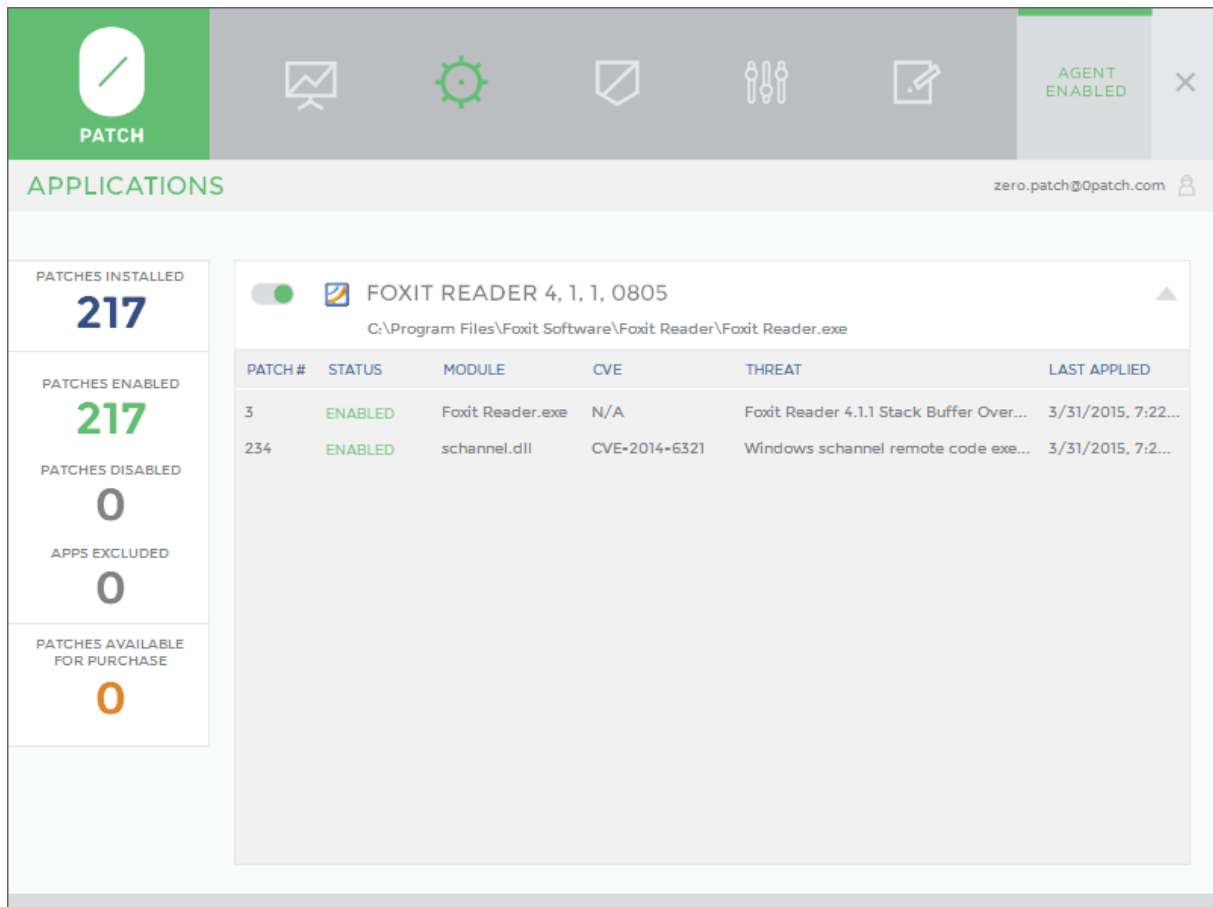
## Excluding an application from patching

If you want to prevent Opatch Agent from applying patches to an application, you can exclude that application from patching by simply switching the button next to the application name in the applications list from "included" (green dot) to "excluded" (red dot). As soon as you exclude an application from patching, all patches are removed from that application in case the application is currently running, and patches will no longer be applied to the application when it gets launched - until you "un-exclude" the application from patching by switching its button back to "included."

The above image shows an example of Foxit Reader being excluded from patching.

## Viewing application's patching statistics

If you click on the application in the applications list (anywhere except on the button), the patching statistics is displayed for that application. This includes a list of all patches that have been applied to that application at least once, and the time of last application for each of these patches.



The screenshot displays the Opatch Agent interface. On the left, a sidebar shows summary statistics: 217 patches installed, 217 patches enabled, 0 patches disabled, 0 apps excluded, and 0 patches available for purchase. The main area shows the 'APPLICATIONS' list with 'FOXIT READER 4, 1, 1, 0805' selected. A toggle switch is turned on (green dot). Below the application name, a table lists applied patches:

PATCH #	STATUS	MODULE	CVE	THREAT	LAST APPLIED
3	ENABLED	Foxit Reader.exe	N/A	Foxit Reader 4.1.1 Stack Buffer Over...	3/31/2015, 7:22...
234	ENABLED	schannel.dll	CVE-2014-6321	Windows schannel remote code exe...	3/31/2015, 7:2...



You can not enable or disable individual patches on this page (because individual patches can only be enabled or disabled globally for all applications, not just for one), but you can click on any patch to be taken directly to the Patches page with the selected patch marked so that you can find it and enable or disable it.

Once an application's patching statistics is shown, you can return to the applications list by clicking anywhere on the application's title.

## 11.Patches

The **Patches** page displays a list of all patches present on your computer, and allows you to enable or disable individual patches.

The screenshot shows the Opatch Patches management interface. On the left, a sidebar displays summary statistics:

- PATCHES INSTALLED: 217
- PATCHES ENABLED: 216
- PATCHES DISABLED: 1
- APPS EXCLUDED: 0
- PATCHES AVAILABLE FOR PURCHASE: 0

The main area displays a table of patches with the following columns: PATCH #, STATUS, MODULE, CVE, and THREAT. Patch 18 is highlighted in red, indicating it is disabled.

PATCH #	STATUS	MODULE	CVE	THREAT
2	ENABLED	Annots.api	CVE-2009-0927	Adobe Collab.getIcon() Buffer Overfl...
3	ENABLED	Foxit Reader.exe	N/A	Foxit Reader 4.1.1 Stack Buffer Overfl...
4	ENABLED	Esript.api	CVE-2008-2992	Adobe util.printf() Buffer Overflow
6	ENABLED	js3250.dll	CVE-2011-2371	Firefox 3.6.16 ReduceRight() Integer ...
16	ENABLED	tdwnmgr.dll	CVE-2013-6877	RealPlayer 16.0.2.32 Buffer Overflow...
18	DISABLED	ALLPlayer.exe	CVE-2013-7409	AllPlayer 5.8 Buffer Overflow In .M3...
21	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
22	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...
23	ENABLED	awt.dll	CVE-2013-2465	Oracle Java storeImageArray functio...
26	ENABLED	awt.dll	CVE-2013-2465	Oracle Java storeImageArray functio...
27	ENABLED	awt.dll	CVE-2013-2465	Oracle Java storeImageArray functio...
28	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...
29	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
30	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
31	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...
32	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
33	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...
34	ENABLED	awt.dll	CVE-2013-2465	Oracle Java storeImageArray functio...
35	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
36	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...
37	ENABLED	awt.dll	CVE-2013-2465	Oracle Java storeImageArray functio...
38	ENABLED	awt.dll	CVE-2013-2470	Oracle Java lookupByteBI function h...
39	ENABLED	awt.dll	CVE-2013-2473	Oracle Java Blit function heap buffer...

You can enable or disable individual patches by switching the button for that patch between "enabled" (green dot) and "disabled" (red dot). Once you disable a patch, it immediately gets removed from all running applications and stops being applied to newly launched applications. Similarly, when you enable a patch, it immediately gets applied to all running applications where applicable.

The above image shows an example of patch 18 for application AllPlayer being disabled.

## 12.Settings

The Settings page allows you to manage Opatch Agent's configuration.

The **Pop-up Settings** allow you to select which pop-up messages you wish to have displayed.

POP-UP SETTINGS	
<input checked="" type="checkbox"/>	Inform me about all patching events
<input type="checkbox"/>	Don't inform me about successfully applied patches
<input type="checkbox"/>	Inform me only about important system events

## 13.Log

The Log page allows you to see a log of important Opatch events. The Log page automatically shows the most recent events when you switch to it, but if it remains open, you have to manually refresh it using the "Refresh" button to see events that occurred after opening the Log page.

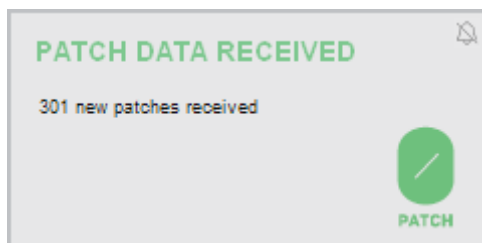
```
C:\Program Files (x86)\Opatch\Logs\Opatch.log REFRESH ↻
2015/11/12 15:14:44 Opatch Agent is no longer supported. Please update agent to keep receiving new patches.
2015/11/12 15:14:44 User invoked sync
2015/11/12 15:14:28 User invoked sync
2015/11/12 15:12:24 Patch 3 removed from application Foxit Reader.exe
2015/11/12 15:12:24 Patch 3 disabled
2015/11/12 15:12:04 Patch 3 applied in application Foxit Reader.exe
2015/11/12 15:12:04 Patch 3 enabled
2015/11/12 15:12:03 Patch 3 removed from application Foxit Reader.exe
2015/11/12 15:12:03 Patch 3 disabled
2015/11/12 15:11:56 Patch 3 applied in application Foxit Reader.exe
2015/11/12 15:11:56 Patch 3 enabled
2015/11/12 15:11:25 Patch 3 not applied to application Foxit Reader.exe because it is disabled
2015/11/12 15:11:22 Patch 3 disabled
2015/11/12 15:11:17 Application Foxit Reader 4, 1, 1, 0805 re-included for patching
2015/11/12 15:10:25 Application Foxit Reader.exe launched but excluded from patching
2015/11/12 15:10:08 Application Foxit Reader.exe launched but excluded from patching
2015/11/12 15:04:12 Patch 4 applied in application AcroRd32.exe
2015/11/12 15:04:12 Patch 4 applied in application AcroRd32.exe
2015/11/12 15:04:12 Patch 2 applied in application AcroRd32.exe
2015/11/12 15:04:12 Patch 2 applied in application AcroRd32.exe
2015/11/12 15:03:42 Application Foxit Reader.exe launched but excluded from patching
2015/11/12 15:03:23 Application Foxit Reader.exe launched but excluded from patching
2015/11/12 15:03:04 Application Foxit Reader.exe launched but excluded from patching
2015/11/12 12:22:42 Patch 4 applied in application AcroRd32.exe
2015/11/12 12:22:42 Patch 4 applied in application AcroRd32.exe
2015/11/12 12:22:42 Patch 2 applied in application AcroRd32.exe
2015/11/12 12:22:42 Patch 2 applied in application AcroRd32.exe
2015/11/12 12:22:40 Patch 6 applied in application firefox.exe
2015/11/12 12:22:26 Patch 6 applied in application firefox.exe
2015/11/12 12:22:10 Patch 4 applied in application AcroRd32.exe
2015/11/12 12:22:10 Patch 4 applied in application AcroRd32.exe
```

## 14. Pop-up Messages

Opatch Agent can inform you about various events using pop-up messages. You can control which pop-up messages you wish to have displayed via Opatch Console's Settings page. In addition, you can instantly silence most pop-up messages by clicking the »crossed bell« icon in the upper right corner of every pop-up.

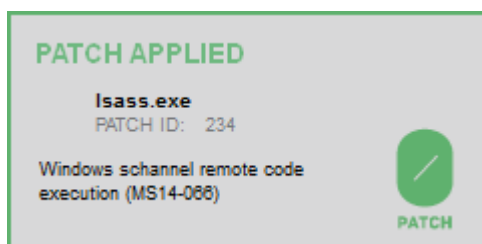
### Patch Data Received

The "Patch Data Received" message informs you that Opatch Agent has just received new patches from the Opatch server, and/or that some patches have been revoked.



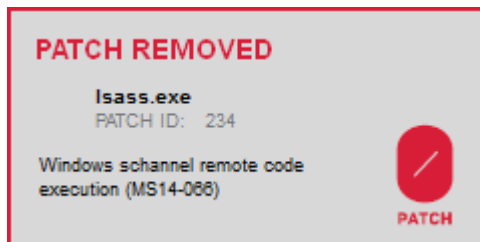
### Patch Applied

The "Patch Applied" message informs you that a patch has just been applied to a process on your computer. The message tells you which process was patched and which patch was applied to it.



## Patch Removed

The "Patch removed" message informs you that a patch has just been removed ("un-applied") from a process on your computer. The message tells you which patch was removed from which process.

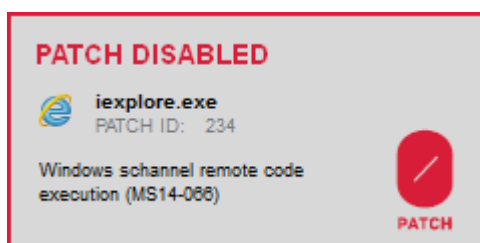


This usually occurs when:

- the patch was disabled via Opatch Console while the application it was applied to was running,
- the application was excluded from patching via Opatch Console while that application was running, or
- Opatch Agent was disabled via Opatch Console.

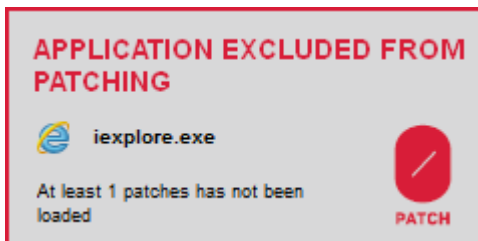
## Patch Disabled

The "Patch disabled" message informs you that a patch would have been applied to a process on your computer - but wasn't because the patch is disabled. (You can use the Patches page in Opatch Console to enable the patch, which will immediately get it applied to the process.)



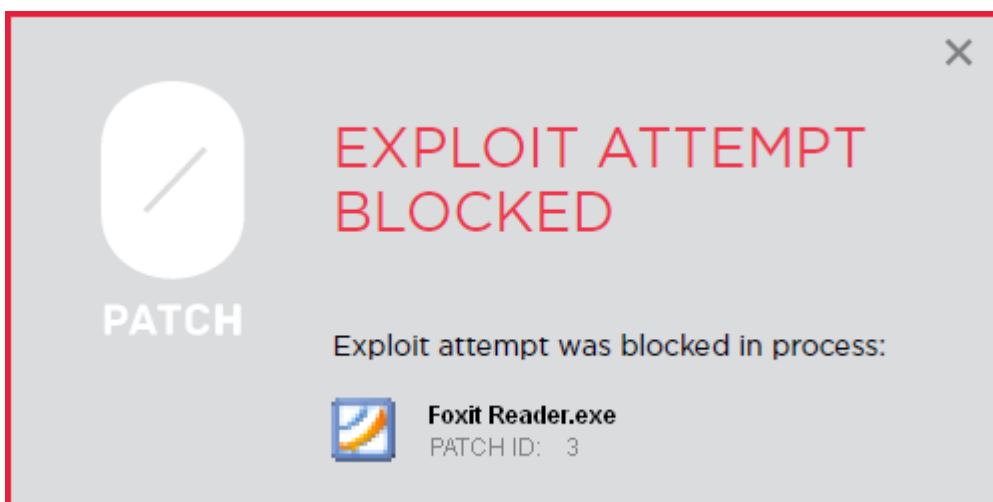
## Application Excluded From Patching

The "Application excluded from patching" message informs you that an application has just been launched that is excluded from patching. This means that any patches that would normally have been applied to this application, were not applied. (You can use the Applications page in Opatch Console to "un-exclude" the application, which will immediately get all applicable patches applied to it.)



## Exploit Attempt Blocked

The "Exploit attempt blocked" message alerts you that one of the patches applied to processes running on your computers has detected an attack (also called "exploit") against the vulnerability it is patching. You don't have to do anything when this happens, as the attack was blocked by the patch.



## 15. Tray Icon

You may have to manually set the Opatch tray icon to show in your system tray / notification area.

The Opatch icon in the system tray serves two functions:

- it provides quick visual information about the status of Opatch Agent, and
- it provides a way to quickly launch Opatch Console, contact the Opatch support team and view this user manual.



The "Everything is OK" icon tells you that everything is okay with the Agent. Patches are being applied and new patches are being downloaded from the Opatch server as they become available.



The "Disconnected" icon tells you that while Opatch Agent is applying available patches to your applications, it can't connect to the Opatch server to download new patches as they become available. This is not a critical condition, as your computer may simply be disconnected from the Internet. As soon as it reconnects to the Internet, Opatch Agent will connect to the server and the icon will turn back to the green "Everything is OK" icon.



The "Unregistered" icon tells you that the agent is not registered on the server and can therefore not download patches from it. When the agent is not registered, you need to register it by launching the Console and signing in with your email and password.



The "Disabled" icon tells you that Opatch Agent is disabled and is not applying patches to applications running on your computer. When the Agent is disabled, Opatch it not protecting your computer. In order to enable the Agent, launch Opatch Console and use the button in the "Enable/Disable Agent" box.



## 16. Updating Opatch Agent

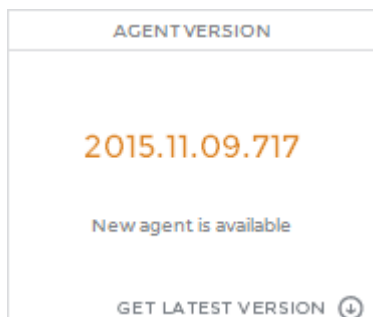
**Note 1: Do not try to update Opatch Agent remotely via Remote Desktop Connection.**

You must update Opatch Agent by directly logging in to the machine and clicking "Get latest version" in the Opatch Console.

**Note 2: If you want to update Opatch Agent in a Windows XP Mode, please consider:**

in order to update Opatch Agent inside "Windows XP Mode", you need to "Disable Integration Features" in the Windows Virtual PC "Tools", then update Opatch Agent by clicking "Get latest version" in the Opatch Console, and finally (optionally) select "Enable Integration Features" in the "Tools" menu. Note that the Virtual PC "Windows XP Mode" is using Remote Desktop Connection for accessing the Windows XP desktop.

As Opatch technology is being developed, new versions of Opatch Agent are being developed and made available to users. When a new Agent is released, Opatch Console will start notifying you about the new version in the Dashboard's "Agent Version" box. You will also find the "Get latest version" button there, which will launch the agent update process.



When you press the "Get latest version" button and confirm that you want to update the Agent, a new Agent version will be downloaded from the server and your Agent will get replaced by this new version. After a successful Agent update, the new Opatch Console will get launched, and you'll be able to verify its version in the "Agent Version" box in Console's Dashboard.

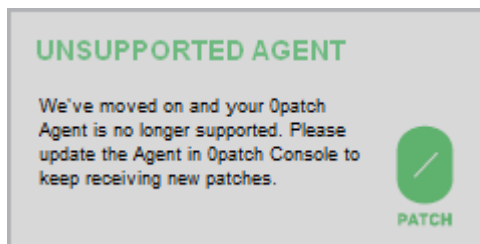
When a new Agent version is available, but your version is still supported (see the following section about unsupported agents), you can continue to use Opatch Agent without any limitations, and will also continue to receive new patches as they get released. Feel free to update the Agent when it is convenient for you.

**Note: Agent update currently resets all Agent settings, including excluded applications and disabled patches. However, proxy server settings and agent status (enabled or disabled) are preserved.**

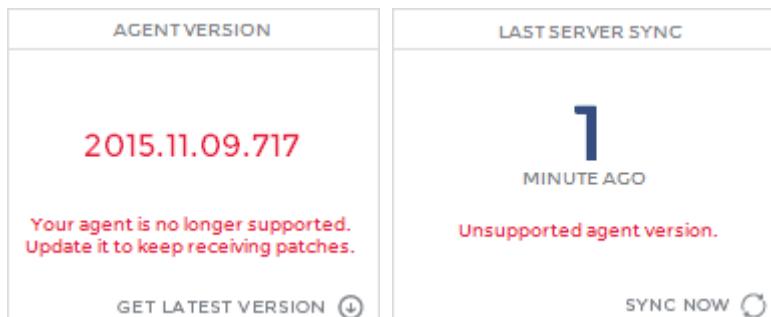
## Unsupported Agent

When a new Opatch Agent version is released, some previously supported versions may no longer be supported by the Opatch Server. This usually happens when a major change was introduced to format or content of data communicated between Opatch Agent and Opatch Server.

In case your Opatch Agent becomes unsupported, you will see the following popup message.



In addition, the Console's Dashboard will show you the following messages in the »Agent Version« and »Last Server Sync« boxes.



When your Agent is no longer supported, it cannot receive new patches any more, but it continues to apply the patches it has previously downloaded to processes on your computer. It is highly recommended to update the Agent when it becomes unsupported.

## 17. Troubleshooting

**Problem:** Agent can't connect to the server (I'm getting the »Unable to connect to the server« error)

**Solution:**

1. Try to open any web site with your web browser. If this doesn't work, your computer is probably not connected to the Internet. Solution: make sure your computer is connected to the Internet.
2. If the previous step was successful, try to open <https://dist.Opatch.com> with your web browser. If this doesn't work, the Opatch server might be temporarily unavailable. Solution: try again later.
3. If the previous step was successful, and you're on a Windows XP or Windows Server 2003 computer, try to open <https://dist.Opatch.com> with Internet Explorer. If this doesn't work, but you can open non-HTTPS pages like <http://www.aaa.com>, make sure your computer is fully updated. To install all updates, run `wuauc1t /detectnow` as administrator and wait for updates to download.
4. If the previous step was successful, your computer may be behind a firewall or your Internet connections may be proxied through a web proxy server. Solution: make sure to configure network connectivity as described in section 4.

**Problem:** Opatch Agent installation failed

**Solution:**

5. Make sure you're not trying to install Opatch Agent through Remote Desktop Connection – that currently doesn't work.
6. If you're installing Opatch Agent in a »Windows XP Mode« computer, make sure you've disabled integration features via the Windows Virtual PC "Tools", "Disable Integration Features."
7. Try to reinstall Opatch Agent. If it fails again, restart your computer and try to install Opatch Agent again.
8. It may be that a previous installation of Opatch Agent has left some residues on the system. Do the following on your computer as local administrator to clean up these residues:
  - Execute **sc delete Opatchservice** to delete the Opatch service.
  - Execute **sc delete Opatchdriver** to delete the Opatch kernel driver.
  - Delete the entire **Opatch** folder under the **Program Files** (on 32-bit Windows) or **Program Files (x86)** folder (on 64-bit Windows) – or wherever you tried to install Opatch Agent if you chose not to use the default location.
  - Launch **regedit.exe** and delete the entire **HKLM\Software\Opatch** registry key.
9. Now try to install Opatch Agent again.



**Problem:** When uninstalling or updating Opatch Agent, this error message pops up: »Removal of Opatch Agent failed. Error 1605 occurred while removing OpatchAgent.«

**Solution:** Please ignore this error message. In our tests, we occasionally get this error message and are currently investigating it. The error doesn't seem to cause any problems (beyond showing the error message) and Opatch Agent actually does get properly removed or updated.

**Problem:** Comodo Firewall doesn't work after system restart when Opatch Agent is installed

**Solution:** We're aware of an incompatibility issue with Comodo Firewall whereby enabling the »Enable adaptive mode under low system resources« option results in some Comodo processes failing to launch, and network connectivity being disabled after computer restart. The only workaround for this issue is to untick the »Enable adaptive mode under low system resources« option under HIPS Settings in the Comodo Firewall console.

**Problem:** One of my applications is crashing when Opatch Agent is installed

**Solution:** If Opatch Agent applied at least one patch to the application, you will find the application listed in the Applications page of the Opatch Console. The first thing to try is to exclude this application from patching by switching the button next to it in the list of applications. If this doesn't stop your application from crashing, please continue to the next troubleshooting tip.

**Problem:** One of my applications is *still* crashing when Opatch Agent is installed (even after trying the previous troubleshooting tip)

**Solution:** We're aware of some compatibility issues with (mostly low level debugging-related) applications, for instance with Visual Studio 2010 Express Edition. If you want Opatch Agent to leave some of your processes alone (i.e., not even inject our loader into them), you can edit the registry value named **HKLM\Software\Opatch\ExcludeModules** and enter in it names of all executable (.exe) files you want excluded, separated by pipe character ('|'). For example, to exclude Visual Studio 2010 Express Edition and notepad.exe from being injected by Opatch Agent, put "vcexpress.exe|notepad.exe" into the said value. Then to enforce this new setting, you have to change the value of **HKEY\_LOCAL\_MACHINE\SOFTWARE\Opatch\CallbackKeys\UnloadLoaderDll\Counter** to any other number than it already has (this removes the loader from all processes), and restart the Opatch Service service.

**Problem:** Opatch Tray crashes after installing or updating Opatch Agent, and I have AVG Internet Security installed.

**Solution:** AVG's Behavior Shield and Ransomware Protection seem to interfere with our launching of



Opatch Tray after installation. The only workaround we know of is to add an exception for the entire Opatch folder under Behavior Shield: In AVG, click on Customize -> Exceptions -> Browse, then browse to "C:\Program Files (x86)\Opatch" and click OK -> OK -> OK.

**Problem:** Comodo Firewall doesn't start, its user interface cannot be opened and there is no Internet connectivity after installing Opatch Agent. (Reported for Comodo Firewall 10.0.0.6092)

**Solution:** The only way we know of to resolve this issue is to disable the "Enable adaptive mode under low system resources" setting in Comodo Firewall's console under Settings -> HIPS - HIPS Settings. (This setting is disabled by default.)

**Problem:** When Opatch Agent is installed, EMET occasionally reports an »EAF mitigation«-related event in some process, then terminates that process.

**Solution:** Disable »EAF« and »EAF+« in EMET for affected applications. (We observed this problem in EMET 5.5 with Adobe Acrobat and Opatch Console.)

**Problem:** Opatch Agent installation or update fails while Avast Free Antivirus makes a »quick 15-second scan« of newly-installed executables.

**Solution:** Temporarily disable Avast while installing or updating Opatch Agent. If the problem occurred during Opatch Agent update, you may have ended up with no Opatch Agent installed; in this case, please download and install the latest Agent version again. (Download link: <https://dist.Opatch.com/download/latestagent.>)

**Problem:** I have problems that the above instructions do not solve.

**Solution:** Email our technical support at [support@Opatch.com](mailto:support@Opatch.com) or report your problem at <https://Opatch.com/support.htm>. We'll appreciate your taking your valuable time for this and will address your problem as quickly as possible.