

Nachtblitz 1.4.27 Release Notes – March 23, 2016

The Developer abides.

Stephan Röger

Contact

Constructive criticism and an outside view are critical for software improvement. You can provide input by email to nachtblitz@mail.i2p. This address works only from within the I2P network which is in the best interest of your own anonymity. You can also give feedback on Nachtblitz at the Freedom Forum (<http://freedomforum.i2p>).

Considerations

What is Nachtblitz?

It's a file sharing client for the I2P network running on .NET. It masters the I2P dialect of eD2k, so it's able to interact with iMule. Nachtblitz is suited for anonymous file sharing.

What does the name Nachtblitz mean?

Night + lightning: Something that travels swiftly through the dark. How to pronounce? It's up to you.

Where to get Nachtblitz?

Echelon has kindly agreed to host it, so the official way is to download Nachtblitz anonymously inside the I2P network from Echelon's site using a normal web browser:

<http://echelon.i2p/nachtblitz/>

How to install Nachtblitz?

No installation is needed. Just extract the files from the release archive into a folder on your hard drive and run *Nachtblitz.exe*. The application does not require write access to the folder with the binaries.

Nachtblitz has no auto-update functionality, but can generally detect if an update is available while operating. Updating must happen manually, by downloading the latest release archive with a browser and extracting it. Note that it's not recommended to mix release files from different archives, so better use a fresh folder or remove all old files when updating.

Is Nachtblitz free of spyware?

Let me make this clear: Yes! Nachtblitz is completely free of malware, spyware and ads. It does not phone home. Users of an anonymous file sharing client want and expect strong privacy protection. Consequently Nachtblitz is built to prevent that your true identity gets exposed. With some technical skills you can build Nachtblitz yourself, as the full source code is open and includes project files for Visual Studio (you can use them with VS2008 or later).

Are the binaries code-signed with a key from a CA?

The main reason I sign the binaries is to enable you to check if a binary comes from me or not. For this a certificate authority (CA) is not required, so the key I use is self-generated and not from a CA. Consequently, your operating system will not trust the corresponding certificate by default. The upside of this is that if a CA has security problems (for example if the root certificate is compromised), Nachtblitz is definitely not affected. All deployed binaries are "Authenticode"-signed using Microsoft's sign tool. In addition, all .NET-based assemblies are strong-name signed during compilation with the same key.

Are the Nachtblitz binaries 32-bit or 64-bit code?

The binaries I supply are in fact .NET *assemblies* which are (in this case) platform agnostic, meaning they do not target a specific platform. They contain code in the *Common Intermediate Language* (CIL), which gets translated into native code for the appropriate platform on launch. This translation is done by the .NET Runtime and is called *just-in-time compilation*. It happens incredibly fast, so you won't even notice it. What all this means is that Nachtblitz will run in 32-bit or 64-bit mode depending on the mode of the .NET Runtime, which usually depends on if you're using a 32-bit or 64-bit operating system.

An exception is the Nachtblitz native library, which is already fully compiled into native code (hence the name) targeting x86 and x86-64 (Nativex86.dll/Nativex86-64.dll).

What software does one need in order to make Nachtblitz run?

- .NET compatible operating system (like Windows or Unix with Wine)
- .NET Runtime and Framework (any from 2.0 to 4.5), included in modern Windows
- Working I2P router (requiring Java Runtime Environment) with SAM bridge enabled

What version of the .NET Framework should be used?

In short, **.NET Framework 4** (4.0 or 4.5) is currently recommended to run Nachtblitz on – though Nachtblitz also works on 2.0 or 3.5. It is recommended to have the full framework and not just the so called *Client Profile* (reduced) edition.

In more detail:

For Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 (also R2) and Windows 7, the Framework 4 is recommended. The following online installer can be used to install the appropriate Framework 4 for your machine architecture:

<https://www.microsoft.com/en-us/download/details.aspx?id=17113>

Note that Framework 4 can only be installed if Framework 4.5 is not installed yet. If you are running Windows 8 or Windows Server 2012, you should already have the Framework 4.5 preinstalled.

If you are running Windows 2000, then Framework 2.0 Service Pack 2 is recommended. An offline installer can be downloaded here:

<https://www.microsoft.com/en-us/download/details.aspx?id=1639>

It is strongly recommended to use Windows Update to receive vital security updates for your operating system as well as any installed .NET Frameworks.

How to run Nachtblitz on a platform other than Windows?

The recommended way is using Wine and the original .NET Framework 2.0. The Nachtblitz project's webpage contains a tutorial on how to run on Wine. If that's not an option, you could virtualize Windows.

What software is needed to build Nachtblitz binaries?

I build Nachtblitz using the following tools, usually with the latest updates installed:

- Microsoft Visual Studio 2008
- Microsoft Visual Studio 2010
- Microsoft Windows SDK v7.0a (included in Visual Studio 2010)

Do you provide free software consulting to developers of a Nachtblitz fork?

I voluntarily provide people with free and open-source file sharing software. I also do some free tech support for the users of this software. In this I'm supported by a number of voluntary users and translators, which contribute to the project for free. However, I do not aid in the development of a Nachtblitz fork, because any such activity would diminish the time and effort I can spend on developing the original Nachtblitz. As I figure the original Nachtblitz is the solution and not the problem, I believe that its development is my most valuable contribution to the community and preferable to dispersing development resources.

How does one enable the SAM bridge of the I2P router?

In the English web interface of the I2P router (as of version 0.9.1):

On the main page of the I2P router, click on *I2P INTERNALS*. Navigate to the *I2P Client Configuration* using the upper navigation bar on the right pane. Make sure *Run at Startup* is checked next to *SAM application bridge*. If not, check it and click on *Save Client Configuration* at the bottom (you may have to restart the router for this to take effect).

Does one have to change firewall rules in order to use Nachtblitz?

You usually do not, since personal firewalls normally do not regulate traffic that goes through the loopback network interface of the local machine (that normally has the IPv4 address 127.0.0.1). If your firewall works different, you would have to explicitly allow Nachtblitz to connect to the I2P routers SAM bridge at 127.0.0.1 port 7656 (default) using the TCP protocol. It is not recommended to connect to an I2P SAM bridge that is not on the machine the client runs on without extra protection, since the (last mile) traffic between the SAM bridge and Nachtblitz is not encrypted.

Can one safely tell his/her I2P addresses to others?

This is a very important question touching the heart of I2P anonymity. On the one hand it is clear that Nachtblitz has to reveal your I2P addresses to other clients in order to interact with them. But on the other hand there is a secret involved, in that others may not be able to link your I2P addresses to your true identity. So I would recommend that you never tell your I2P addresses to anyone (for example if you are asked in a forum or per mail). Same goes for your user hash, client ID, nickname, SecIdent keys, etc. Leave that stuff to the client.

Does Nachtblitz allow others to browse the shared directories?

No, as a design decision Nachtblitz does not reveal the catalogue of shared files to others if asked. It will also refuse to reveal the names of the directories the files are in. Other clients can only ask Nachtblitz if a certain file (meaning eD2k file id) is available. Still someone could try to guess all the files you provide by checking for what files your client was published as a source, but this procedure would be cumbersome and not necessarily reliable.

What's the difference between *incomplete* and *missing* files?

The concept of *incomplete* versus *missing* files is alien to users accustomed to iMule and needs some clarification. Nachtblitz discriminates three types of files:

- **Incomplete files:** Files that are not yet fully downloaded and exist only in the client's application data files. They are not directly visible on your hard drive yet. Of the three types, only incomplete files are supposed to ever get downloaded.
Colors: **orange** when inactive, **blue** when active.
- **Complete files:** Files that reside inside a shared directory and are accessible to Nachtblitz. You can see them on your hard drive as well as in Nachtblitz. Of the three types, this type is the only that directly represents an object on your hard drive.
Colors: **green** when inactive, **blue** when active.
- **Missing files:** Missing files are like shadows of former complete files. Those files once resided inside a shared directory in the form of complete files, but aren't there anymore. Possible reasons: They were deleted, moved out or got inaccessible or had their file content changed. Nachtblitz still has a concept of those files and stores some information about them (like transferred volume, speed limits, etc.). As soon a file with matching file content is detected inside any shared directory, the missing file becomes a complete file again. Nachtblitz won't download a missing file (you can however manually convert a missing file into an incomplete file using the context menu on the files tab: "Turn Selected Missing Files into Incomplete Files" – which will enable you to download this file).
Color: **red** (always inactive).

You can manually remove incomplete and missing files from Nachtblitz by using the context menu on the files tab ("Remove Selected Incomplete or Missing Files"). If there are a lot of missing files listed (hundreds or more), you might consider removing some of them in order to free up resources. But be careful not to select and remove files you do want to keep.

Expert info: When Nachtblitz launches, it only knows incomplete and missing files. Not until Nachtblitz scans the shared directories will some of the missing files become complete files (usually without the user noticing). Please note that Nachtblitz identifies files not primarily by their name and other metadata, but actually through their file content (the binary stream the file is really about).

How to create custom tabs?

While the main window of Nachtblitz is in the foreground, press the F3 key in order to view the *Files* tab. Right below the topmost tab control there's a subordinated tab control. Right click on any tab from this control and a context menu will appear that allows you to create/modify/hide/remove your own tabs.

What is the temp folder for?

The *temp folder* is used like a scratchpad and holds files that usually only exist for a couple of seconds, rarely longer. The main purpose of these temp files is keeping the application's memory footprint small. The temp folder is not used to hold partial downloads (the way iMule uses its temporary directory). Nachtblitz's partial downloads are stored in the *application data directory* (see below).

Where does Nachtblitz store partially downloaded files?

While a file is partially present on your local drive, its fragments are stored inside the *application data directory*. You can tell where the client stores this data: Options dialog -> Application Directories -> Application data.

What is the preview folder?

The *preview folder* becomes necessary since Nachtblitz's partial downloads are not interpretable by other applications and thus can't be directly used for previewing. So when a partially downloaded file needs to be previewed, Nachtblitz creates a preview file in the preview folder, copies the beginning of the partially downloaded file into the preview file and plays/runs it. From time to time you might wish to remove the preview files to reclaim wasted drive space (the options dialog has a button to do this conveniently).

What application data files contain sensitive data?

This paragraph is about the threat imposed by someone who has physical access to your hard drive against your will, say after stealing the drive. The client uses four files (Core.index, Core.body, Incompl.index, Incompl.body) on your hard drive to store basically everything it needs to know (preferences, search history, incomplete downloads, etc.). But this is not to say that there aren't other possible traces on your hard drive. Nachtblitz will for example make use of temporary files that are short lived, but might be recovered by someone who forensically examines your hard drive. Also keep in mind that any application you execute (the I2P router as well) will use memory, and memory can be written into the page file by your operating system. Through this and other OS-related mechanisms (like hibernation or anti virus logs), there are always possible traces of your online activity on your system drive. For this reason you might consider encrypting your entire system partition using free software like *TrueCrypt* (version 7.1a). If you're using Windows and don't want to encrypt your system partition, you might at least set the following registry value to 1 (it's zero by default):

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session  
Manager\Memory Management\ClearPageFileAtShutdown
```

This will make the operating system fill your page file(s) with zeros each time you shut down.

Nachtblitz has finished downloading at 100% completeness, but the downloaded file doesn't appear on the hard drive.

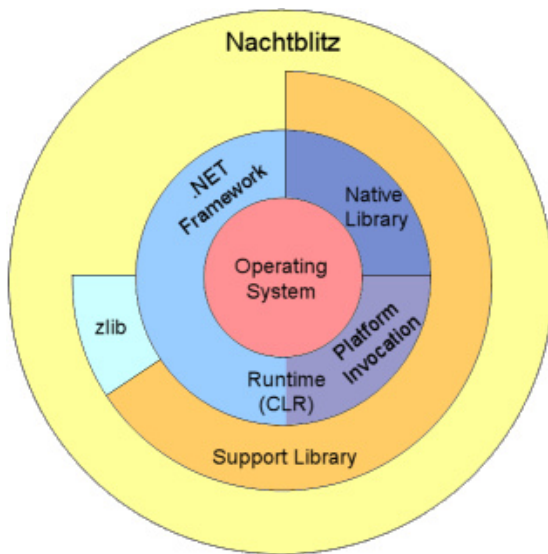
Please make sure you have set an output dir (Options dialog -> Shared Directories -> Set Output Dir). If you did and the file isn't created after a few minutes, one reason can be that your hard drive is running out of free space. Make sure you have at least the size of the file you downloaded (better a couple of hundred megabytes more) available after downloading has finished.

Is an ingoing connection used for uploading and an outgoing for downloading?

Not necessarily. An ingoing connection is one that was initiated by a peer and accepted by your client. An outgoing connection was initiated by your client and accepted by a peer. Regardless of who initiated the connection, both endpoints can send and receive data through the connection (full-duplex): Each of both connected clients can upload and download through any established connection.

Is Nachtblitz a 100% managed application?

Managed in this context is a .NET specific term. Yes, Nachtblitz is 100% managed if you really need that. There are three ways in which Nachtblitz can run. 1) Fully managed and “safe”. 2) Fully managed with minor (so called) “unsafe” portions for better speed. 3) Managed, safe and unsafe, plus native (MS Windows and Wine only) for even better speed. Option three is the default. If you desperately need (the painfully slow) option one, you will have to recompile the support library without the conditional compilation symbol *FAST*. The schematic to the left shows the major execution components of Nachtblitz and their relation to another, with the main executable layered around (in the default configuration).



What is TAICH?

At some point I will explain that in detail. TAICH stands for “Tigerized Advanced Intelligent Corruption Handling”. It has nothing to do with AICH, I was just too lazy to invent an entirely new name. It’s also not about the so called “tiger tree” that other P2P networks use (BitTorrent, Gnutella2). But it too uses a form of tiger tree, just a different one. I recommend including the TAICH hash whenever you distribute an eD2k link for the I2P network (Nachtblitz created collections always include it). A TAICH hash uses the same encoding as an I2P address (casing matters) and looks for example like the following line:
vemr-~92P3tskPXJBIBCvQjpuJaKhk6-

Nachtblitz crashed – what to do?

Please see if there is a file named “NachtblitzCrashLog.txt” in the folder...

“C:\Users\<USER NAME>\AppData\Roaming\Nachtblitz”

...or (on Windows XP) in the folder...

“C:\Documents and Settings\<USER NAME>\Application Data\Nachtblitz”

...and mail that to me (see contact information presented earlier in this document). If you aren’t using the latest version of the client (please check the website), try upgrading to the latest release and see if the problem persists. If you are already using the latest version and the error happens too often, you might try if an older version doesn’t have the problem and downgrade until the problem is fixed.

Are translations available?

So far four translations (French, German, Polish and Spanish) besides English are available. If a desired translation is missing, consider creating one yourself. There is a guide in the folder *Translations* of the Nachtblitz release archive.

TRADEMARK NOTICE

ANY TRADEMARKS THAT THIS DOCUMENT AND ANY ASSOCIATED MATERIAL MENTIONS OR DISPLAYS ARE THE SOLE PROPERTY OF THEIR RESPECTIVE OWNERS.

DISCLAIMER OF WARRANTY, DISCLAIMER OF LIABILITY

THE CONTENT OF THIS DOCUMENT AND OF ANY ASSOCIATED MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF NON-INFRINGEMENT. THE AUTHOR(S), OWNER(S), PUBLISHER(S), DISTRIBUTOR(S) AND APPLICABLE INTELLECTUAL-PROPERTY OWNER(S) OF THIS DOCUMENT AND OF ANY ASSOCIATED MATERIAL DISCLAIM ANY AND ALL WARRANTIES OF ANY KIND. IN NO EVENT WILL ANY OF THOSE PARTIES BE LIABLE TO YOU OR TO ANY OTHER PARTY FOR ANY DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR OF ANY ASSOCIATED MATERIAL.

TERMS AND CONDITIONS OF SOFTWARE

IN ORDER TO USE THE NACHTBLITZ SOFTWARE, YOU HAVE TO AGREE TO THE TERMS AND CONDITIONS STATED IN THE ACCOMPANIED LICENSE FIRST. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, DO NOT USE THE SOFTWARE.