G Data

TechPaper #0274

Offline Updates for standalone clients

G Data PreSales

Whitepaper_03-2012

G Data. Security Made in Germany.

Table of Contents

0. Introduction 2

0.1 Typographic conventions 2

1. Application & Restrictions 2

2. Preparation 3

3. Exporting virus signatures 4

4. Importing virus signatures 6

0. Introduction

This document will cover the procedures which are required to perform offline updates for G Data's Security Client if the latter is isolated from the network or does not have access to a ManagementServer.

0.1 Typographic conventions

To emphasize and clarify some details in this document, the critical passages will be made prominent using color or a different font:

`Command line input, folder paths and registry paths will use a monospaced font`

Any window titles, settings or menu sequences will be printed in italics

In case a passage has to be emphasized to avoid undesired consequences, it will be prefixed with the word **Caution**, printed in **red** color and a **bold typeface**.

1. Application & Restrictions

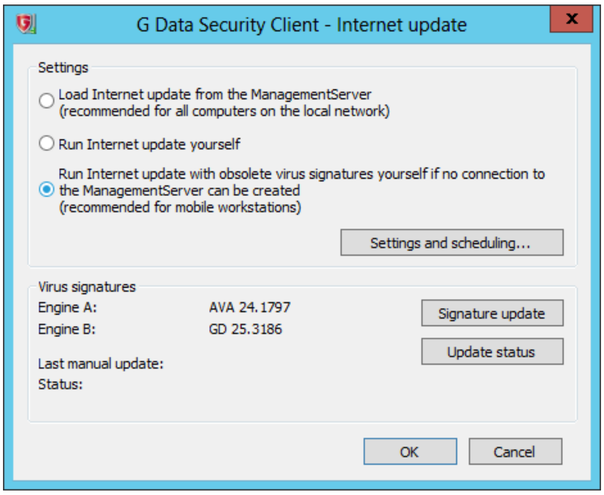
Offline updates for clients may be required for any reason a ManagementServer cannot be installed in a network. It must be noted, however, that the procedures outlined in this document deviate significantly from the recommended course of action for update distribution which is still the use of a ManagementServer and/or a number of SubnetServers. The dedicated Offline Update Tool which is provided by G Data must only be resorted to if no other means of update distribution are feasible. Centralized administration is always to be considered preferable and will continue to be the primary means of administration and update distribution.

At the time of writing (May 2nd, 2014), the Client Offline Update Tool is only available for users located in some geographical regions. Also, the Client Offline Update Tool is not part of a default G Data installation. It is provided only on request. A signed document from the partner/distributor/customer is required in which the partner/distributor/customer declares that the Offline Update Tool will not be (re-)distributed to any third party.

2. Preparation

The tool which is provided with this document is used to both export the virus signatures from a ManagementServer and also to import the updates on the client.
A ManagementServer of version 13 is required in order to procure the virus signature updates.

Likewise, the client must be configured so that it can be updated using the G Data Offline Update Tool. Make sure that permissions are assigned so the user is capable of updating the virus signatures himself:



G Data Security Client - Internet update

Settings

○ Load Internet update from the ManagementServer (recommended for all computers on the local network)

○ Run Internet update yourself

● Run Internet update with obsolete virus signatures yourself if no connection to the ManagementServer can be created (recommended for mobile workstations)

Virus signatures
Engine A: AVA 24.1797
Engine B: GD 25.3186
Last manual update:
Status:

Screenshot 1: *Client update settings*

Furthermore, the client must be assigned to the ManagementServer which will provide the signature updates. Both client and ManagementServer must have the same version and be set to the same type of license (i.e. AntiVirus, ClientSecurity or EndpointProtection). The access data which is entered in the *Internet update* options on the G Data Security Client must be identical to the access data which is entered on the ManagementServer for downloading updates. The update server region must also correspond to what is set on the ManagementServer.

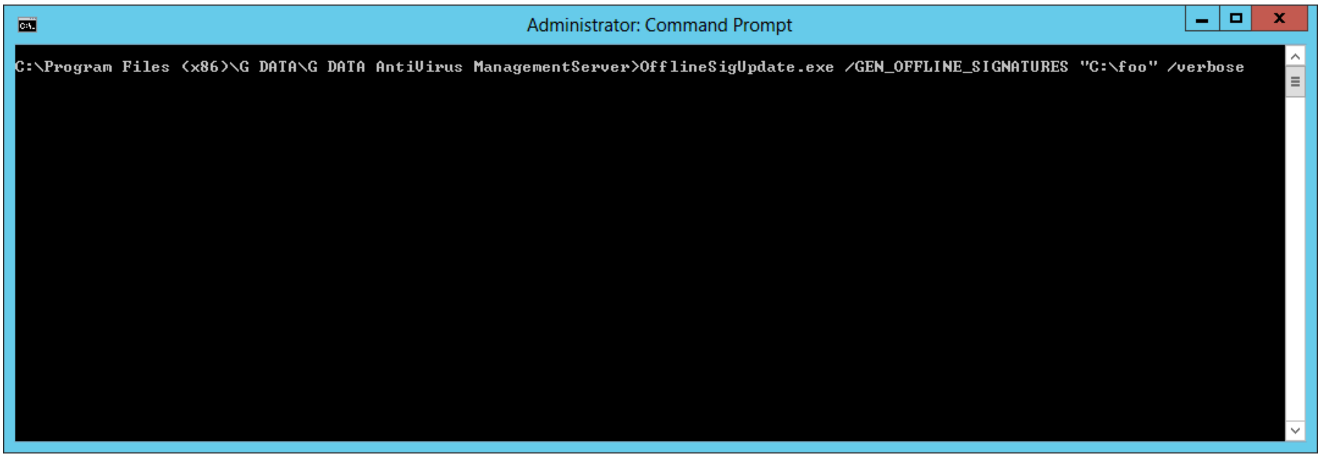
3. Exporting virus signatures

When you downloaded the archive containing the Offline Update Tool, unpack it to the ManagementServer's program folder. Per default this is `C:\Program Files (x86)\G DATA\G DATA AntiVirus ManagementServer\`.

To run the tool, a command line window with administrator permissions is required. Also, a target directory must be created to which the ManagementServer can export the offline update files.
Use the `cd` command to navigate to the ManagementServer's program directory. Then, invoke the tool using the following command:

```
OfflineSigUpdate.exe /GEN_OFFLINE_SIGNATURES “path_to_target_folder”
```

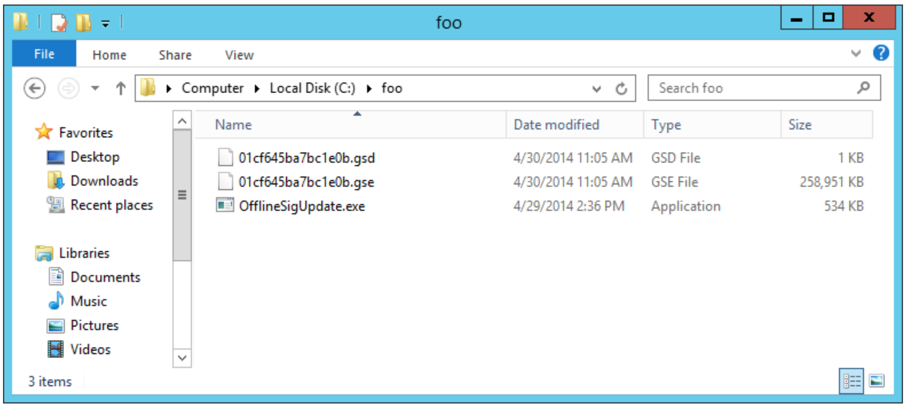
The quotation marks around the target folder designation must be included.
If needed, the command can be extended using the parameter `/verbose` to enable additional output.



```
C:\Program Files (x86)\G DATA\G DATA AntiVirus ManagementServer>OfflineSigUpdate.exe /GEN_OFFLINE_SIGNATURES "C:\foo" /verbose
```

Screenshot 2: *Invocation of the tool via command line; the target directory in this case is* `C:\foo`

When started, the Offline Update Tool will create three files in the target folder:
One *.gse file which contains the virus signatures
One *.gsd file with configuration data
One copy of the Offline Update Tool



Name	Date modified	Type	Size
01cf645ba7bc1e0b.gsd	4/30/2014 11:05 AM	GSD File	1 KB
01cf645ba7bc1e0b.gse	4/30/2014 11:05 AM	GSE File	258,951 KB
OfflineSigUpdate.exe	4/29/2014 2:36 PM	Application	534 KB

Screenshot 3: *Output files*

Once the signature export is completed, the target folder will contain all the required information to update the G Data Security Client.

4. Importing virus signatures

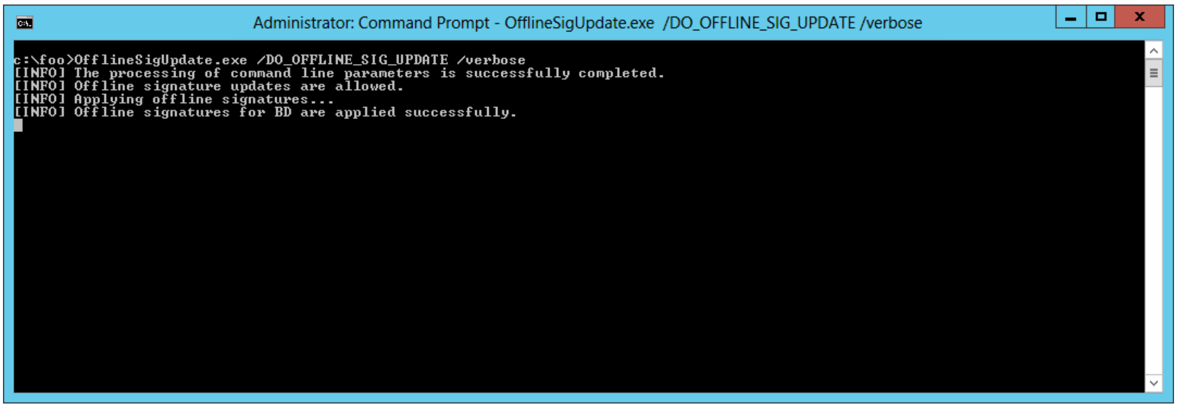
As outlined above, all the data required to update the virus signatures on the client are in the directory that the virus signatures were exported to. Take the entire contents of this directory and transfer it to a medium of your choice.

Caution:

All three files are required; if any of the files are missing, the virus signatures cannot be imported on the client.

To import the virus signatures, the Offline Update Tool must be run from a command line window with administrator permissions. Use the `cd` command to navigate to the location where the update files have been stored. As with the export command, you can extend the command with the `/verbose` parameter to get more output. The syntax is as follows:

```
OfflineSigUpdate.exe /DO_OFFLINE_SIG_UPDATE
```



Administrator: Command Prompt - OfflineSigUpdate.exe /DO_OFFLINE_SIG_UPDATE /verbose

```
c:\foo>OfflineSigUpdate.exe /DO_OFFLINE_SIG_UPDATE /verbose
[INFO] The processing of command line parameters is successfully completed.
[INFO] Offline signature updates are allowed.
[INFO] Applying offline signatures...
[INFO] Offline signatures for BD are applied successfully.
```

Screenshot 4: *Running the signature update on the client; the location of the update files here is `C:\foo`.*

All information in this document was carefully checked and properly validated.
Errors & omissions excepted.