



Information Engineering Technology

Configuring DeniComp RSHD



Release 8.7.3

Table Of Contents

Configuring DeniComp's RSHD for GuardIEn	3
Remote Shell Daemon	3
Install RSHD.....	3
Configure RSHD.....	3
Shared Network Drives	4
Appendix A – Multiple CSE Specifics	5
Shared Drive for GuardIEn HOME	5
GuardIEn Remote Scripts	5
PAD Listing Shared Drive.....	5
Task Dispatcher / Queues Shared Drive.....	5
Code Generation Shared Drive	5
Known Restrictions and Problems	5
Appendix B – Remote Installs	6
GuardIEn Remote Build Scripts	6
Remote Build Target Properties.....	6
Appendix C – GuardIEn Remote Data Client.....	7
Environment	7

Configuring DeniComp RSHD

This paper describes how to configure the DeniComp Remote Shell Daemon software for use with GuardIEn. Appendices are provided for additional detail where there are differences in the configuration depending upon how you wish to use the Daemon.

Remote Shell Daemon

The Remote Shell Daemon software handles rsh commands to execute processes on remote servers. GuardIEn utilises this mechanism in the following areas:

- Multiple CSE configuration – for executing CSE tasks on remote servers, such as downloads/uploads/generates etc.
- Remote Builds onto Windows or UNIX servers – invokes the Gen Build Tool/IT on another server to build load modules
- "GuardIEn Remote Data Client" installations – where GuardIEn processes are executed on the user's client workstation, connecting remotely to a central GuardIEn database

Install RSHD

Obtain a copy of the DeniComp RSHD software first and install it on the appropriate server where RSH commands need to be serviced. This software may be supplied as an evaluation copy from IET, or from DeniComp web site at <http://www.denicomp.com/> For Windows servers, you will need *Winsock RSHD/NT* software.

Configure RSHD

Most of the set-up is done via the Control Panel for WRSRDH:

- Attempt Redirection on every command – ON
- Default window type – MINIMIZED
- Environment Variable File - <wrshdnt install path>\%ruser%.var
- Execute all RSH commands as user - <user>/<password> - e.g. gdn – it is recommended that you define a special user just for GuardIEn e.g. gdn, and define this user to Windows. You will never actually log onto Windows with this user, but RSH will use this logon. If you wish to perform processing on the same server with different environments, then you can easily configure another user with their own USERID.var file.
- All other options in the Control Panel for WRSRDH should be blank or off
- Configure WRSRDH variable files... create a <userid>.var file containing the environment you need to process your rsh commands. The processes will actually run under gdn (or whatever you choose above). Note: no SET keywords should be used in the .var files. The value of <userid> should be the same as the value entered for the FTP userid in the GuardIEn encyclopaedia definition. An example .var file for a Remote Gen 7.6 CSE installation, might look something like this:

```
AEHOME=c:\CA\GEN\  
COOL-BASE=c:\CA\GEN\  
IEF=c:\CA\GEN\  
IEFCONST=c:\CA\CLIENT\  
IEFCSGEN=c:\CA\CSE\bin  
IEFGEN=c:\CA\GEN\  
IEFGXTP=c:\CA\translat\  
IEFH=c:\CA\GEN\  
IEFLAN=c:\CA\CLIENT\  
IEF_CCP=c:\CA\CLIENT\  
IEF_DIRGROUP=DIR  
IEF_ENCYGROUP=ENCY  
IEF_MDMODE=TCPIP  
IEF_RDSNODE=localhost  
INCLUDE=c:\CA\GEN;c:\CA\CSE\include;%INCLUDE%  
LIB=c:\CA\CSE\lib;c:\CA\GEN;%LIB%  
PATH=c:\CA\GEN;c:\CA\CLIENT;c:\CA\CSE\bin;c:\CA;%PATH%  
IEF_MDNAME=iefmd
```

Shared Network Drives

You will probably need Shared Network Drives to support your GuardIEn installation, so that all involved machines on your network can see the same network location with the same name. For example, you may need to share the GuardIEn *Home* directory as drive X: All involved machines will need to see X: the same.

For WRSHD configuration, create a file called automap.ini in the WRSHD home that has NET USE commands for the Network Drives you have e.g.:

```
net use x: \\server\c$\gdn
```

Start the WRSHD service and verify from a DOS Prompt with something like the following (replace csea with the userid from the userid.var file you created earlier). You should see the correct environment variables returned for user csea.

```
rsh SERVER2 -l gdn set
```

Appendix A – Multiple CSE Specifics

Please refer to your platform's specific installation guide for Multiple-CSEs, which contains the same information as described below.

Shared Drive for GuardIEn HOME

You will need a shared drive, which all of the CSE servers see as the same drive, such as X: This needs to point to the main GuardIEn HOME directory. You should configure this share BEFORE installing GuardIEn itself, as you will need to specify this Home directory when running the install program.

GuardIEn Remote Scripts

Copy supplied files `gdruncmd.exe`, `gdrmrtrun.bat`, `gdpingmd.bat`, `gdgetvar.bat` etc. (placed in the `\setup87\remote` Directory where you installed GuardIEn by the set-up program) into each of the remote servers to a directory that is in the PATH of the remote server e.g. `\windows\system32`, or simply ensure that the path where you place these files is also specified by the PATH variable in your user.var file (see the section above on Configuring RSHD).

PAD Listing Shared Drive

Use *System Administration Client* to point the System Parameter PADDSDN to the shared PAD List path e.g. PADDSDN = "x:\PADList". Use *Project Administration Client* to point the Project Property (General Category) PAD List Path to the same directory as above (do this for all your Projects). X: needs to be a shared drive that all CSE server machines see as the same.

You will also need to create subdirectories within this PADList directory for each CSE Code e.g. `x:\PADList\CSE1\` because each CSE's PADs will be stored in a separate sub-directory.

Task Dispatcher / Queues Shared Drive

The Task Dispatcher will physically run on the main GuardIEn server, submitting remote shell commands (rsh) to invoke CSE processes, such as downloads/uploads etc., on remote CSEs.

In the Queue Manager, point all of your Queues to a common Shared Network Path e.g. X: for the drive and `\GdnQueues\` for the path. The Task Dispatcher will take care of stopping/starting your queues automatically according to their start/stop times.

Code Generation Shared Drive

Code Generation must be performed into shared network drives too. Amend any Code Generation paths in your Target Properties to point to a common Shared Network Path e.g. `X:\MYPROJ\DEV\` etc. You *do not need* to do this for generations out of the CSE on the main GuardIEn server.

Known Restrictions and Problems

1. Do not use spaces in the path names for the shared directories, i.e. queue home, pad listing and code generation. If you do, you should specify them with DOS short names e.g. `progra~1` instead.
2. The system date/time on each of the servers should be synchronised, ideally kept in synch with a time synchronisation service.
3. Local install methods will execute on the GuardIEn server. If the installs have to execute on another server, then remote install method should be used.

Appendix B – Remote Installs

Please refer to the *Remote Installation* document for other information on configuring your servers for remote builds.

GuardIEn Remote Build Scripts

Copy supplied files `gdchdrv.exe`, `gdckfile.bat`, `GdRemRmt.bat` etc. into each of the remote servers to a directory that is in the PATH of the remote server. It is probably best to create a specific directory for this purpose e.g. `c:\Gdn\RemoteInstall\`, then add this directory to the PATH setting in your `USERID.var` file for the Remote Shell Daemon configuration.

Remote Build Target Properties

Configure your Target for Install Method *Remote (Gen)*, and set suitable values for:

- Remote Build Path (local directory on build server where RMTs will be transferred to, and build will take place)
- Remote Build Script (normally `GdRemRmt.bat`)
- Remote Machine Name (DNS name or IP Address of the build server)
- Remote Logon Id (USERID to logon to RSH with – with a corresponding `USERID.var` file for the correct environment)
- Remote External Libraries (optionally an override for the `EXTERNAL_LIB` setting)

Appendix C – GuardIEn Remote Data Client

The GuardIEn Remote Data Client is used only in situations where you have no Transaction Enabler software. A central GuardIEn database resides on the CSE server, but all software processing is performed on 'fat' clients on the user's workstation, connecting remotely to the GuardIEn/CSE database.

Certain processing for this configuration requires the use of RSH commands, such as PAD Listing. Below is the set-up you require in order to make this work.

Environment

You will need to define the USERID that will logon to RSH to perform PAD extracts, and this user will require the correct environment to perform CSE functions, in particular generation. Therefore, define a user such as *gdn* and create a *gdn.var* file containing all environment settings for your CSE e.g.

```
AEHOME=c:\CA\GEN\  
COOL-BASE=c:\CA\GEN\  
IEF=c:\CA\GEN\  
IEFCONST=c:\CA\CLIENT\  
IEFCSGEN=c:\CA\CSE\bin  
IEFGEN=c:\CA\GEN\  
IEFGXTP=c:\CA\translat\  
IEFH=c:\CA\GEN\  
IEFLAN=c:\CA\CLIENT\  
IEF_CCP=c:\CA\CLIENT\  
IEF_DIRGROUP=DIR  
IEF_ENCYGROUP=ENCY  
IEF_MDMODE=TCPIP  
IEF_RDSNODE=localhost  
INCLUDE=c:\CA\GEN;c:\CA\CSE\include;%INCLUDE%  
LIB=c:\CA\CSE\lib;c:\CA\GEN;%LIB%  
PATH=c:\CA\GEN;c:\CA\CLIENT;c:\CA\CSE\bin;c:\CA;%PATH%  
IEF_MDNAME=iefmd
```