

Information Engineering Technology

Install Guide - Clients



Release 8.7.3

Table Of Contents

Welcome	Error! Bookmark not defined.
Introduction	3
Architecture	3
Communications	3
About The Installation Guides	4
Software for Download	4
Client Install	5
Pre-Requisites	5
Download Files	5
Install Software	5
Network Installation	6
Local Files	6
Local Windows Firewall	6
VMWare <i>ThinApp</i> Support.....	6
Communications Middleware.....	7
GuardIEn Server Selection	7
Client Manager.....	7
Client Manager Directory Services.....	8
MQ Series.....	8

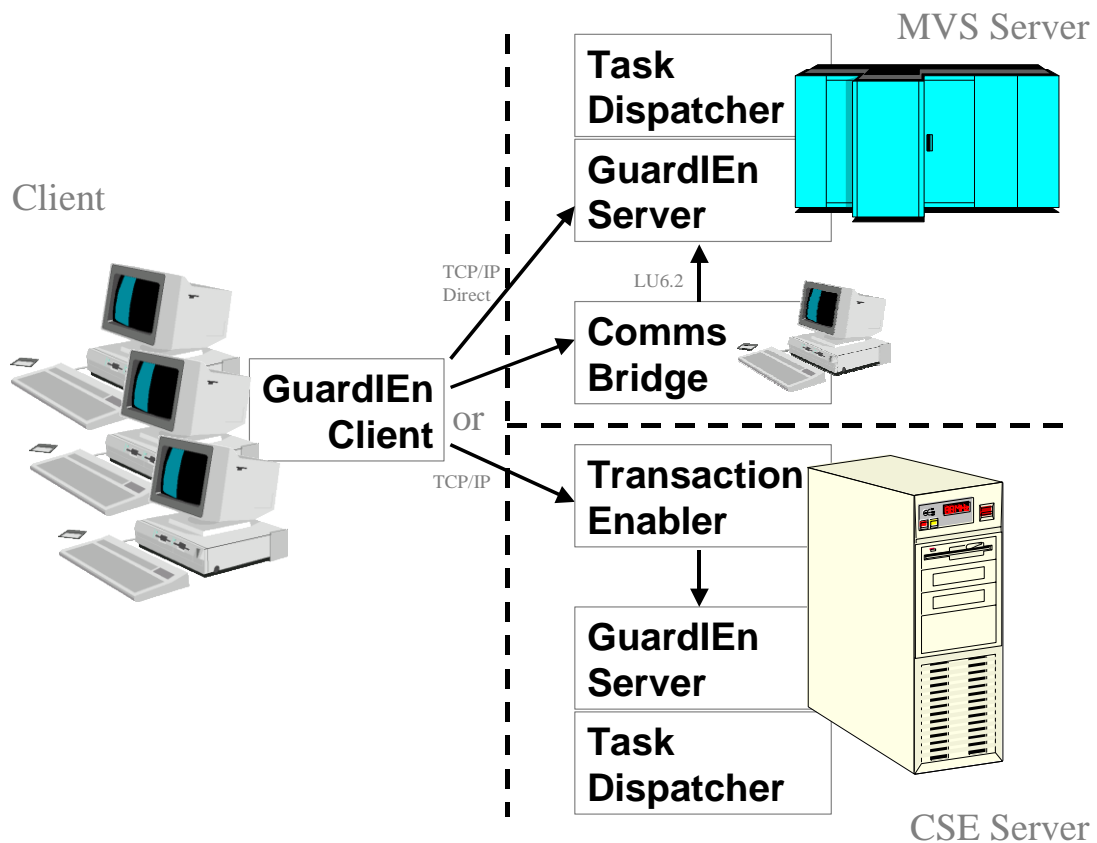
Introduction

Architecture

GuardIEn is a Gen-developed *client/server* application. This means that there are two parts to the install process: the GUI *clients* which are deployed on each workstation; and *servers* which reside alongside your Gen encyclopaedia.

Communications

As with any Gen-developed client/server application, you will require some communications software (*middleware*) so that the client programs can talk to the servers.



GuardIEn uses *TCP/IP* on the workstations, so there is no need for *Client Manager*, although you can still use this if you wish. Depending upon your server platform, you will also need other middleware to complete the link. You may choose any standard configuration e.g. *Transaction Enabler* on Windows/UNIX servers, or *Comms Bridge* and *LU6.2* on MVS servers, or direct *TCP/IP* Connect to MVS. For further details on appropriate middleware, consult your Gen documentation.

You can also use MQ Series to communicate to GuardIEn (host encyclopaedia only).

For further details on appropriate middleware, consult your Gen documentation.

The individual chapters of this guide give more information on pre-requisites for communications.

About The Installation Guides

There are a number of documents to help you with the install process. Below is a quick summary of what they are and which ones you will need to use:

- *THIS DOCUMENT*: You always need to perform Client Installs for each workstation where you wish to use GuardIEn, regardless of server platform.
- *Install Guide - <Platform/Ency>.doc*: You will also need to perform a Server Install. Choose the appropriate one depending on your encyclopaedia platform. GuardIEn servers are always installed on the same server as your encyclopaedia. If you eventually intend to use GuardIEn with multiple encyclopaedias then you should choose the server most capable of handling the workload for the first, or *main*, install. There are different versions of this install guide for each server platform
- *Verification*: The server install guides also include chapters on how to verify that the installation is ok and perform essential initial customisation. You *MUST* work through these sections after you have performed the client and server installs.

There are also further documents available that may be relevant to you. These increase the flexibility and automation possible using GuardIEn:

- *Multiple Encyclopaedias.doc*: If you have multiple encyclopaedias (Windows CSE only), this document shows you how to configure GuardIEn to access and manage them.
- *Remote Builds.doc*: If you intend to perform construction (generation/installation) using GuardIEn, and your application's target platform is *not* the same as your encyclopaedia platform, then you can use this guide to see how you can complete the configuration to allow fully automated remote builds. These instructions are included in the online help installed with the GuardIEn client.
- *Technical Papers*: There are also various papers on technical issues which you may wish to tackle with your GuardIEn install. These documents are included in the online help installed with the GuardIEn client.

Software for Download

All IET software is available for download from the IET support centre: <https://support.iet.co.uk>. Software is secured on the web site, so you will need register and then request access.

Download the relevant files for your platforms (client + one server) into a temporary directory on a workstation. The individual install chapters in this guide detail the files you will need and what you should do with them.

Client Install

Client Installs needs to be performed on each of the workstations where you intend you use GuardIEn. This install process is handled through a standard *Installshield* mechanism making the client set-up very quick and simple.

Pre-Requisites

- Windows 7 or higher
- Minimum screen resolution of 1024x768 (16 or 32-bit colour required)
- Communications Bridge or Direct TCP/IP connection to server, or MQS to IMS/CICS
- 200Mb Disk Space (for full GuardIEn and help/documentation install)
- Windows Appearance 'border padding' setting should be set to 0
- The %APPDATA% location cannot use a UNC path name
- Flash Player OCX – required if you intend to use the Tutorials supplied with GuardIEn. The Flash software normally resides in %WINDOVS%\Macromed\Flash or (%WINDOVS%\SysWOW64\Macromed\Flash for 64 bit Windows) and in particular the OCX called Flash11e.ocx. These are not supplied with GuardIEn due to security considerations – each site must decide whether they wish to distribute the Flash Player internally.

Download Files

Download GDCLNxxx.exe (where xxx is the version required) from the web site into a temporary directory e.g. c:\temp\gdinst:

Install Software

- Execute GDCLNxxx.EXE. This extracts the set-up files into a temporary directory and then automatically launches a set-up program that installs the client software.

Installation Path

The GuardIEn client software is normally installed on your C: drive in \Program Files under a sub-directory of \GuardIEn. You may choose a different path during the set-up if you wish

Choose Setup Type

If you are installing Release 8.7 for the first time, choose New Installation. If you are upgrading to the latest 8.7 release from a prior 8.7 release, choose upgrade i.e. applying an 8.7 Service Pack. If you want to run GuardIEn from a shared network drive, select Network Installation. If you need to omit certain components, choose Customised new installation, but this is not recommended.

Communications Middleware

There are three options for the communications middleware: Direct TCP/IP, Client Manager and MQ Series. These are detailed below. Note that MQ Series is only available for communicating with MVS servers.

Gen 8.6 Runtimes

The GuardIEn clients need various Gen 8.6 runtime files to be available. By default, the set-up program copies the required files into the \bin subdirectory of your installation path so there is nothing more you need to do.

Gen Toolset Plug-ins

Various GuardIEn and genIE functions can be accessed from within a Gen Toolset via the Toolset Plug-in interface. By default GuardIEn and genIE will be registered as available Plug-in applications. If the installation software detects that these Plug-ins are already registered, then it will ask you if you want to register this installation instead (overwriting the previous registration).

Network Installation

Instead of loading the GuardIEn software onto your workstation, you can execute the GuardIEn software from a network drive. Choose Network installation instead of Standard or Custom. The GuardIEn client software must have first been installed on the network machine.

Whilst the majority of the GuardIEn client software will be located on a shared network drive, there are a few local files that are setup on each user's workstation. These are local .ini files that are used to store workstation settings, for example, filter values.

Local Files

The GuardIEn client stores several user options (i.e. filter settings) in local .ini files. These are normally located in the user's home directory, i.e. C:\Documents and Settings\\Application Data\IET*.

Local Windows Firewall

If your site requires use of your local windows firewall it may be necessary to explicitly allow the main 'GuardIEn' executable, the GuardIEn launcher 'GDCLLA' and the 'Gen r8 No DB Stub for GuardIEn' runtime through your domain and/or private network firewall ports.

VMWare *ThinApp* Support

GuardIEn can be installed under VMWare's *ThinApp* platform, but may not operate correctly. In particular, windows launched from the main GuardIEn client may not be visible, although they are actually started. To work-around this problem, which is a runtime-behaviour difference of *ThinApp*, you should set some environment variables in the workstation's general environment:

```
SET GDN_DO_NOT_MINIMIZE_LAUNCHER=YES  
SET GDN_DO_NOT_BLOCK_RESTORES=YES  
SET GDN_GDEXWIN_NO_HIDE=YES
```

This should enable most of GuardIEn's functionality to be used under *ThinApp*, although it is not guaranteed as 100% compatible.

Communications Middleware

GuardEn Server Selection

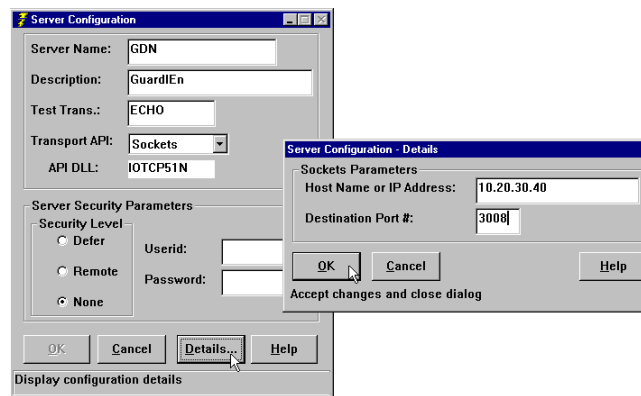
By default GuardEn uses a *Direct TCP/IP* connection from the client to the GuardEn servers, and so there is no need for the Client Manager. The Gen runtimes use the data in the commcfg.ini file to determine how to connect to the server. The GuardEn installation will have created a default entry for this file. If you want to connect to multiple GuardEn servers, see the GuardEn Server Select topic in the on-line help documentation for details on how to configure multiple GuardEn servers.

The GuardEn Server Select utility is not used if you are using MQ series as the middleware.

Client Manager

GuardEn uses *TCP/IP* on the workstations, so there is no need for *Client Manager*, although you can still use this if you wish.

If you do still wish to use the Client Manager, create a new server entry in Client Manager using the *Server->Config* option. Give it a name of GDN or similar, and provide the other properties as show below. If your site is using directory services (see below), you may need to specify a particular name.



Press *Details...* and provide the following properties. Replace the IP address shown below with the host name or IP address of the server that contains the TE. If this is the only server that you require, you should make it the *default server*.

If you will be connecting to the server via a Comms Bridge, you should enter the *Port* number for the Comms Bridge. Otherwise, enter the *Port* number you wish to use for the *Transaction Enabler* directly. A default server installation on a CSE will use *Port 80870*.

If you are using a CICS or IMS server, then you will normally need to set the security level to Remote and provide your MVS userid and password when prompted to logon to the client manager. Certain MVS installations do not use client manager security and your site may elect to use GuardEn security instead. Contact your system administrator for information if you are not sure what parameters to use.

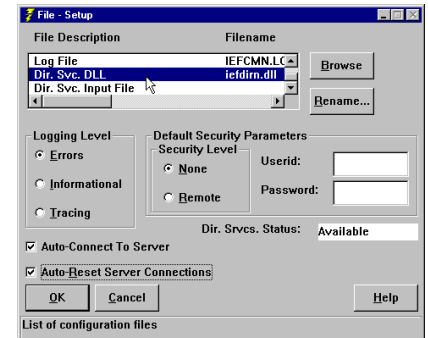
Client Manager Directory Services

If you are using the Client Manager and the client needs to connect to multiple servers, for example one for GuardIEn and one for the application being developed using Gen, then you will need to use the Client Manager *directory services* to instruct the Client Manager to use the GDN server for GuardIEn and the *default server* can then be used for your other applications.

Default DLL

The default directory services exit is installed in the sample directory below the directory where the Client Manager was installed. The default exit uses a file containing tranocode-to-server mapping. The <GuardIEn>\DIRSVCS directory contains a file called IETDIR.TRN that contains a mapping of the GuardIEn trancodes.

- To enable directory services for your Client Manager:
- Copy the IEFDIRN.DLL file from the Gen sample directory to the Client Manager directory
- Copy the IEFDIR.TRN file from the GuardIEn DIRSVCS directory to the Client Manager directory
- Open the Client Manager set-up dialog box (*File->Setup*)
- Enter the name of the *Dir Svc DLL* file (IEFDIRN.DLL)
- Enter the name of the *Dir Svc Input* file (IEFDIR.TRN)
- Stop and restart the Client Manager
- Check that directory services is enabled/available in the *File - Setup* dialog box.



Custom DLL

The default directory services exit uses the IEFDIR.TRN file to map transaction codes to the server. The DIRSVCS directory also contains a customised version of the DLL in the file IEFDIR.C. This is a modified version of the CA-supplied exit that does not require the IEFDIR.TRN file. If the first two characters of the tranocode are 'G7', the custom exit returns a server name of *GDN*. The advantage of this exit is that the IEFDIR.TRN files do not have to be updated when new server transaction codes are used in future releases of GuardIEn.

If you want to use the customised version, compile the revised source and create a custom version of the DLL. The MAKENT.BAT batch file will compile and link the DLL.

MQ Series

The GuardIEn client can communicate with GuardIEn servers (on MVS) using MQ Series. This is accomplished through the use of the MQ series client software. There is no need to install a local MQ series Queue Manager on the client workstation.

To enable MQ as the middleware, you should select MQ as the middleware option when installing the GuardIEn client. You will be asked to provide the MQ Queue Manager name. This is the name of the MQ Queue Manager on MVS.

The GuardIEn install will customise the commcfg.ini file in the GuardIEn client \bin directory and add an entry for each transaction. It assumes that there is one MQ Queue for each GuardIEn server. If you wish to use the Gen Transaction Dispatcher for CICS (TDC), then you will need to amend the commcfg.ini file to specify the correct queue name.

The CA MQ runtimes (MQ*.dll) should be copied into the GuardIEn client \bin directory from a custom Gen 8.6 installation of MQ Series Middleware – and you must be licensed by CA to obtain this product.

You must also ensure that you have installed the MQ series client software. As a minimum, this will probably require you to setup the MQSERVER environment variable. For example, the following setting connects the clients to the SYSTEM.DEF.SVRCONN channel on IP address 19.150.50.102 with port 1414.

```
SET MQSERVER=SYSTEM.DEF.SVRCONN/TCP/19.150.50.102(1414)
```