Gnome Display Manager Reference Manual

Martin K. Petersen

mkp@mkp.net

Gnome Display Manager Reference Manual
by Martin K. Petersen

Table of Contents

Terms and conventions used in this book 4
1. Overview 5
    1.1. Introduction 5
    1.2. The GDM Daemon 5
    1.3. XDMCP 6
    1.4. The Greeter 7
        1.4.1. Text entry 7
        1.4.2. The Menu 7
        1.4.3. The face browser 8
        1.4.4. The Logo 8
2. The Configuration Directory 10
    2.1. The Script Directories 10
    2.2. The Configuration File - gdm.conf 11
        2.2.1. Daemon Configuration 12
        2.2.2. Security Options 15
        2.2.3. XDCMP Support 17
        2.2.4. Common GUI Configuration Options 20
        2.2.5. Greeter Configuration 20
        2.2.6. XDCMP Chooser Options 23
        2.2.7. Local X Server Configuration 24

Terms and conventions used in this book

GDM - Gnome Display Manager. Used to describe the software package as a whole.

gdm - The Gnome Display Manager daemon (gdm).

Greeter - The graphical login window (gdmlogin).

Chooser - The host chooser which appears on remote displays sending INDIRECT queries (gdmchooser).

Paths without a leading '/' are relative to the installation prefix. I.e. share/pixmaps/ refers to /usr/share/pixmaps if GDM was configured with –prefix=/usr.

Chapter 1. Overview

1.1. Introduction

GDM is a replacement for XDM, the X Display Manager. Unlike its competitors (X3DM, KDM, WDM) GDM was written from scratch and does not contain any original XDM / X Consortium code.

1.2. The GDM Daemon

GDM was written with simplicity and security in mind. The overall design concept is this:

Upon startup the gdm daemon parses its config file gdm.conf. For each of the local displays gdm forks an Xserver and a slave process. The main gdm process will then listen to XDMCP requests from remote displays and monitor the local display sessions.

The gdm slave process opens the display and starts gdmlogin, the graphical login program. gdmlogin runs as a dedicated user and communicates asynchronously with the slave process through a pipe.

GDM relies heavily on the presence of PAM, Pluggable Authentication Modules, but supports regular crypt() and shadow passwords on legacy systems.

Remote displays can connect to the XDMCP port on the GDM host. gdm will grant access to hosts specified in the gdm service section in your TCP Wrappers configuration file. GDM does not support remote display access control on systems without TCP Wrappers. XDMCP support can be turned off completely, however.

GDM includes several measures making it more resistant to denial of service attacks on the XDMCP service. A lot of the protocol parameters, handshaking timeouts etc. can be fine tuned. The defaults should work for most systems, however. Don't change them unless you know what you're doing.

In general GDM is very reluctant regarding reading/writing of user files. For instance it refuses to touch anything but regular files. Links, sockets and devices are ignored. The value of the RelaxPermissions parameter determines whether GDM should accept files writable by the user's group or others. These are ignored by default.

All operations on user files are done with the effective userid of the user. If the sanity check fails on the user's .Xauthority file, a fallback cookie is created in /tmp.

Finally, the sysadmin can specify the maximum file size GDM should accept, and, if the face browser is enabled, a tunable maximum icon size is also enforced. On large systems it is still advised to turn off the face browser for performance reasons. Looking up icons in homedirs, scaling and rendering face icons can take quite a long time. YMMV.

1.3. XDMCP

GDM also supports the X Display Manager Protocol (XDMCP) for managing remote displays.

GDM listens to UDP port 177 and will repond to QUERY and BROADCAST_QUERY requests by sending a WILLING packet to the originator.

GDM can also be configured to honor INDIRECT queries and present a host chooser to the remote display. GDM will remember the user's choice and forward subsequent requests to the chosen manager.

GDM only supports the MIT-MAGIC-COOKIE-1 authentication system. Little is gained from the other schemes, and no effort has been made to implement them so far.

Since it is fairly easy to do denial of service attacks on the XDMCP service, GDM incorporates a few features to guard against attacks. Please read the XDMCP reference section below for more information.

Even though GDM tries to outsmart potential attackers, it is still adviced that you block UDP port 177 on your firewall unless you really need it. GDM guards against DoS attacks, but the X protocol is still inherently insecure and should only be used in controlled environments.

Even though your display is protected by cookies the XEvents and thus the keystrokes typed when entering passwords will still go over the wire in clear text. It is trivial to capture these. You should also be aware that cookies, if placed on an NFS mounted directory, are prone to eavesdropping too.

1.4. The Greeter

The greeter is the graphical user interface that is presented to the user. The greeter contains a menu at the top, an optional face browser, an optional logo and a text entry widget.

1.4.1. Text entry

The text entry field is used for entering logins, passwords, passphrases etc. gdmlogin is controlled by the underlying daemon and is basically stateless. The daemon controls the greeter through a simple protocol where it can ask the greeter for a text string with echo turned on or off. Similarly, the daemon can change the label above the text entry widget to correspond to the value the authentication system wants the user to enter.

1.4.2. The Menu

The menu bar in the top of the greeter enables the user to select the requested session type/desktop environment, select an appropriate locale/language and optionally shutdown/reboot the machine. The greeter window can also be iconified to make room for other applications on the login screen.

1.4.3. The face browser

The greeter provides a face browser containing icons for all the users on a system. The icons can be installed globally by the sysadmin or in the users' home directories.

The face browser makes a few assumptions about your environment. First of all, the greeter runs under a dedicated userid, and therefore any face icons located in user directories must be readable to the gdm user. I.e. all home- and ~/.gnome directories must be made readable and executable to the "other" group on the system.

Similarly, face icons placed in the global face directory must be readable to the gdm user.

Please note that loading and scaling face icons located in user home directories can be a very time consuming task. Especially on large systems or systems running NIS. The browser feature is only intended for systems with relatively few users.

To filter out unwanted user names in the browser, an exclude option is implemented. The greeter will automatically ignore usernames listed in the Exclude statement in the config file.

When the browser is turned on, valid usernames on the machine are inherently exposed to a potential intruder. If your system is connected directly to the Internet, this might be a bad idea.

1.4.4. The Logo

The greeter can optionally display a logo in the login window. The image must be in a format readable to the Imlib library (GIF, JPG, PNG, TIFF, XPM and possibly others), and it must be readable to the gdm user. See the Logo option in the reference section below for detauls.

Chapter 2. The Configuration Directory

The configuration files for GDM are located in the etc/gdm/ directory.

This is a listing of the config directory contents:

Init/
PostSession/
PreSession/
Sessions/
gdm.conf

gdm.conf is the main GDM configuration file. The options will be described later in this chapter.

gdm.conf is configuration file for both gdm, gdmlogin, and gdmchooser since a lot of parameters overlap.

The remaining configuration is done by dropping scripts in the subdirectories of the etc/gdm folder. This approach makes it easy for package management systems to install window managers and different session types without requiring the sysadmin to edit files.

2.1. The Script Directories

In this section we will explain the Init, PreRoot and PostRoot directories as they are very similar.

When the X server has been successfully started, GDM will try to run the script called Init/<displayname>. I.e. Init/:0 for the first local display. If this file is not found, GDM will attempt to to run Init/Default. The script will be run as root and GDM blocks until it terminates. Use the Init/* script for programs that are supposed to run alongside with the GDM login window. xconsole for instance. Commands to set the background etc. goes in this file too.

It is up to the sysadmin to decide whether clients started by the Init script should be killed before starting the user session. This is controlled with the KillInitClients option in gdm.conf.

When the user has been successfully authenticated, GDM tries to run the PreSession script. Similar to the Init-scripts, PreSession/<displayname> will be executed, if this file doesn't exist, GDM will attempt to run PreSession/Default. The script will be run as root and GDM blocks until it terminates. Use this script for local session management or accounting stuff. The $USER environment variable contains the login of the authenticated user. The script should return 0 on success. Any other value will cause GDM to terminate the current login process.

Then the session script is run. Session scripts are located in the etc/gdm/Session directory. Which one GDM runs, depends on the session the user chose in the Sessions-menu in the greeter. If no session is selected and the user has no last session stored in his ~/.gnome/gdm file, the system will choose or first script found or – if Sessions/Default exists – this will be run. For instance you can create a symlink from Gnome to Default to make Gnome the default desktop environment.

When the user terminates his session, the PostSession script will be run. Operation is similar to Init and PreSession. That is, GDM will attempt to execute the script PostSession/<displayname> and if that doesn't exist PostSession/Default will be run. Again the script will be run with root priviledges, the slave daemon will block and the $USER environment variable will contain the name of the user who just logged out.

Note that the PostSession script will be run even when the display fails to respond due to an I/O error or similar. Thus, there is no guarantee that X applications will work during script execution.

Neither of the Init, PreSession or PostSession scripts are necessary and can be left out. At least one session script is required for proper operation.

2.2. The Configuration File - gdm.conf

The daemon and the accompanying utilities share a common configuration file: etc/gdm/gdm.conf.

The configuration file is divided into sections each containing variables that define the behaviour for a specific part of the GDM suite.

gdm.conf follows the standard GNOME configuration file syntax. Keywords in brackets define sections, strings before an equal sign (=) are variables and the data after equal sign represents their value.

In general, 0 represents disable and 1 represents enable for boolean configuration options.

2.2.1. Daemon Configuration

[daemon]

Chooser

Chooser=bin/gdmchooser –disable-sound

Full path and name of the chooser executable followed by optional arguments.

DefaultPath

DefaultPath=/bin:/usr/bin:/usr/bin/X11:/usr/local/bin

Specifies the path which will be set in the user's session.

DisplayInitDir

DisplayInitDir=etc/gdm/Init

Directory containing the display init scripts. See the "Script Directories" section for more info.

Greeter

Greeter=bin/gdmlogin –disable-sound

Full path and name of the greeter executable followed by optional arguments.

Group

Group=gdm

The group id under which gdmlogin/gdmchooser are run.

HaltCommand

HaltCommand=/sbin/shutdown -h now

Full path and arguments to command to be executed when user selects Halt from the System menu.

KillInitClients

KillInitClients=1

Determines whether GDM should kill X clients started by the init scripts when the user logs in.

LogDir

LogDir=var/gdm

Directory containing the log files for the individual displays. By default this is the same as the ServAuthDir.

PidFile

PidFile=var/run/gdm.pid

Name of the file containing the gdm process id.

PostSessionScriptDir

PostSessionScriptDir=etc/gdm/PostSession

Directory containing the scripts run after the user logs out. See the "Script Directories" section for more info.

PreSessionScriptDir

PreSessionScriptDir=etc/gdm/PreSession

Directory containing the scripts run before the user logs in. See the "Script Directories" section for more info.

RebootCommand

RebootCommand=/sbin/shutdown -r now

Full path and optional arguments to the program to be executed when user selects Reboot from the System menu.

RootPath

RootPath=/sbin:/usr/sbin:/bin:/usr/bin:/usr/bin/X11:/usr/local/bin

Specifies the path which will be set in the root's session and the {Init,PreSession,PostSession} scripts executed by GDM.

ServAuthDir

ServAuthDir=/var/gdm

Directory containing the X authentication files for the individual displays. Should be owned by gdm.gdm with permissions 750.

SessionDir

SessionDir=etc/gdm/Sessions

Directory containing the scripts for all session types available on the system.

User

User=gdm

The username under which gdmlogin / gdmchooser are run.

UserAuthDir

UserAuthDir=

The directory where user's .Xauthority file should be saved. When nothing is specfied the user's home directory is used.

UserAuthFBDir

UserAuthFBDir=/tmp

If GDM fails to update the user's .Xauthority file a fallback cookie is created in this directory.

UserAuthFile

UserAuthFile=.Xauthority

Name of the file used for storing user cookies.

2.2.2. Security Options

[security]

AllowRoot

AllowRoot=0

Graphical root logins are disallowed by default. Set this value to 1 to enable priviledged user logins.

On systems that support PAM, this parameter is ignored. It's up to the PAM libraries to determine whether the user is on a local display or not.

RelaxPermissions

RelaxPermissions=0

By default GDM ignores files and directories writable to other users than the owner.

Changing the value of RelaxPermissions makes it possible to alter this behaviour:

0 - Paranoia option. Only accepts user owned files and directories.

1 - Allow group writable files and directories.

2 - Allow world writable files and directories.

RetryDelay

RetryDelay=3

The number of seconds GDM should wait before reactivating the entry field after a failed login.

UserMaxFile

UserMaxFile=65536

GDM will refuse to read/write files bigger than this number (specified in bytes).

In addition to the size check both gdm and gdmlogin are extremely picky about accessing files in user directories. Neither will follow symlinks and they can optionally refuse to read files and directories writable by other than the owner. See the RelaxPermissions option for more info.

VerboseAuth

VerboseAuth=0

Specifies whether GDM should print authentication errors in the message field in the greeter.

Depending on your system setup, usernames might be exposed when this option is on.

2.2.3. XDCMP Support

[xdmcp]

DisplaysPerHost

DisplaysPerHost=1

To prevent attackers from filling up the pending queue, GDM will only allow one connection for each remote machine. If you want to provide display services to machines with more than one screen, you should increase the DisplaysPerHost value accordingly.

Enable

Enable=0

Setting this to 1 enables XDMCP support allowing remote displays/X terminals to be managed by GDM.

gdm listens for requests on UDP port 177. See the Port option for more information.

If GDM is compiled to support it, access from remote displays can be controlled using the TCP Wrappers library. The service name is gdm

You should add

```
gdm: .my.domain
```

to your /etc/hosts.allow. See the hosts_access(5) man page for details.

Please note that XDMCP is not a particularly secure protocol and that it is a good idea to block UDP port 177 on your firewall unless you really need it.

HonorIndirect

HonorIndirect=1

Enables XDMCP INDIRECT choosing (i.e. remote execution of gdmchooser) for X-terminals which don't supply their own display browser.

MaxPending

MaxPending=4

To avoid denial of service attacks, GDM has fixed size queue of pending connections. Only MaxPending displays can start at the same time.

Please note that this parameter does *not* limit the number of remote displays which can be managed. It only limits the number of displays initiating a connection simultaneously.

MaxPendingIndirect

MaxPendingIndirect=4

GDM will only provide MaxPendingIndirect displays with host choosers simultaneously.

MaxSessions

MaxSessions=16

Determines the maximum number of remote display connections which will be managed simultaneously. I.e. the total number of remote displays that can use your host.

MaxWait

MaxWait=30

When GDM is ready to manage a display an ACCEPT packet is sent to it containing a unique session id which will be used in future XDMCP conversations.

GDM will then place the session id in the pending queue waiting for the display to respond with a MANAGE request.

If no response is received within MaxWait seconds, GDM will declare the display dead and erase it from the pending queue freeing up the slot for other displays.

MaxWaitIndirect

MaxWaitIndirect=30

The MaxWaitIndirect parameter determines the maximum number of seconds between the time where a display requests a chooser and completion of protocol negotiation. If the timeout is exceeded, GDM will remove the display from the pending list freeing up the slot for other displays.

Port

Port=177

The UDP port number gdm should listen to for XDMCP requests. Don't change this unless you know what you're doing.

2.2.4. Common GUI Configuration Options

[gui]

Gtkrc

Gtkrc=

Path to a gtkrc containing the theme for use in gdmlogin / gdmchooser.

MaxIconWidth

MaxIconWidth=128

Specifies the maximum icon width (in pixels) that the face browser will display. Icons larger than this will be scaled.

MaxIconHeight

MaxIconHeight=128

Specifies the maximum icon height (in pixels) that the face browser will display. Icons larger than this will be scaled.

2.2.5. Greeter Configuration

[greeter]

Browser

Browser=0

Set to 1 to enable the face browser. See the "Greeter" section for more information on the face browser.

DefaultFace

DefaultFace=share/pixmaps/nophoto.png

Default icon file for users without a personal picture in ~/gnome/photo. The image must be in an Imlib supported format and the file must be readable for the gdm user.

DefaultLocale

DefaultLocale=english

This language is used for the session unless nothing is specified in ~user/.gnome/gdm and the user didn't select a language in the Locale menu in the greeter.

Exclude

Exclude=bin,daemon,adm,lp,sync,shutdown,halt,mail,...

Comma-separated list of usernames to exclude from the face browser. The excluded users will still be able to log in.

Font

Font=-adobe-helvetica-bold-r-normal-*-*-180-*-*-*-*-*-*

Font to use for the welcome message in the greeter.

GlobalFaceDir

GlobalFaceDir=share/faces/

Systemwide directory for face files. The sysadmin can place icons for users here without touching their homedirs. Faces are named after their users' logins.

I.e. <GlobalFaceDir>/johndoe would contain the face icon for the user "johndoe". No image format extension should be specified.

The face images must be stored in Imlib supported formats and they must be readable for the GDM user.

A user's own icon file will always take precedence over the sysadmin provided one.

Icon

Icon=share/pixmaps/gdm.xpm

Icon to use for gdmlogin when it's in the iconified state. The image must be in an Imlib supported format and it must be readable for the GDM user. If no file is specified the iconify feature is disabled.

LocaleFile

LocaleFile=etc/gdm/locale.alias

File in GNU locale format with entries for all supported languages on the system.

Logo

Logo=share/pixmaps/gnome-logo-large.png

Image file to display in the logo box. The file must be in an Imlib supported format and it must be readable by the GDM user. If no file is specified the logo feature is disabled.

Quiver

Quiver=1

Controls whether gdmlogin should shake the display when an incorrect username/password is entered.

SystemMenu

SystemMenu=0

Turns the Shutdown/Halt menu on/off.

Welcome

Welcome=Welcome to %n

Controls which text to display next to the logo image in the greeter. The following control chars are supported:

%% the '%' character

%d display's hostname

%h Fully qualified hostname

%m machine (processor type)

%n Nodename (i.e. hostname without .domain)

%r release (OS version)

%s sysname (i.e. OS)

2.2.6. XDCMP Chooser Options

[chooser]

DefaultHostImage

DefaultHostImage=share/pixmaps/nohost.png

File name for the default host icon. This image will be displayed if no icon is specified for a given host. The file must be in an Imlib supported format and it must be readable for the GDM user.

HostImageDir

HostImageDir=share/hosts

Repository for host icon files. The sysadmin can place icons for remote hosts here and they will appear in gdmchooser.

The file name must match the fully qualified name (FQDN) for the host. The icons must be stored in Imlib supported formats and they must be readable to the gdm user.

ScanTime

ScanTime=3

Specifies how many seconds the chooser should wait for replies to its BROADCAST_QUERY.

2.2.7. Local X Server Configuration

[servers]

0

0=/usr/bin/X11/X

Control section for local X servers. Each line indicates the local display number and the command that needs to be run to start the X server(s).

GDM will append "-auth <ServAuthDir>/:n.Xauth :n", where n is the display number.