PAM Plugin and Server Manual

Provided by XPA Systems, http://www.xpasystems.com
for pGina, http://pgina.xpasystems.com

What is the PAM Plugin?

The PAM plugin for pGina 1.6.2 and higher, is a plugin intended to provide seamless integration with an existing Unix user base through the use of an existing PAM infrastructure.

The PAM plugin has two parts, a server and the pGina plugin. The server portion is PAM aware and runs on a Unix machine that utilizes PAM for user authentication. The pGina plugin authenticates against that server. By utilizing the existing PAM configuration, this server and plugin allow for authenticating windows clients by any means currently also possible with PAM.

Requirements

Server

The pgina_pam server requires the following libraries:

- OpenSSL 0.9.7a or higher (older revisions may work, but are not recommended) – http://www.openssl.org

The server has been compiled and tested with the following:

- GCC 2.95.2 and higher
- Linux 2.4.19, Solaris 8, Solaris 9

Plugin

The pGina plugin portion requires only 1 MB of disk space and pGina 1.6.2 or higher.

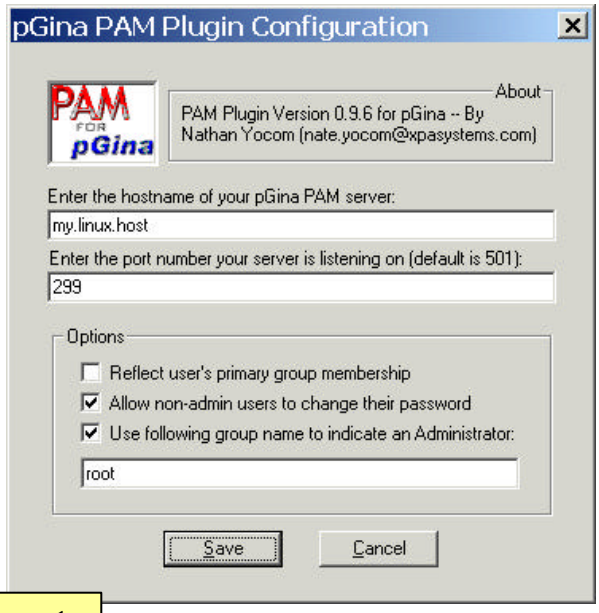

Figure 1

Installing the Plugin

After downloading the zip file provided on the pGina website (http://pgina.xpasystems.com) unzip it and run the executable under the extracted "Windows Installer" directory. This will install, but NOT configure the plugin.

Configuring the Plugin

Configuration of the plugin is performed just as any other plugin – run the configuration utility that was provided with pGina 1.6.2 or higher, select "Load Plugin" and choose the PAMPlugin.dll from the location to which you installed in the previous step. This will invoke the configuration dialog shown in Figure 1.

The first entry space provided is for the hostname or IP address of the server running the pgina_pam server. The next is the port that the server is listening on (299 is the default).

The last few options affect the behavior of the plugin.

Reflect user's primary group membership – When this is turned on, pGina will try to add successfully authenticated users to a local windows group by the same name as their primary unix group. The local windows group must exist for this to work. For example, if the unix user nyocom is in the primary group faculty then pGina will add the user to the faculty group on the windows machine being accessed so long as the faculty group exists.

Allow non-admin users to change their password – When this is turned on, users who are not administrators (local admin accounts, or accounts falling into the next setting) are allowed to attempt a password change. Note that password changing does not work when the server is run in the Solaris environment (this is being worked on), so any attempts against a Solaris server will result in failure.

Use following group name to indicate an administrator – When this is turned on, pGina will check the users primary group membership against the comma separated list of groups you provide. If any match, then the user is created as a local administrator on the windows machine.

A Note on Expired Passwords

Unix PAM can return several values upon authentication, including values indicating that the users password has, or is about to expire. In either of these cases, the pGinaPAM plugin will display a dialog box for the user, asking them to change their password by giving a new password.