pGina Manual

http://pgina.xpasystems.com

http://www.xpasystems.com

Introduction

pGina is, in short, a replacement for domain authentication in a Windows environment. pGina, through the use of plug-in technology, allows an administrator to choose from any number of existing authentication sources and methods. Should an administrator wish to implement a custom authentication method, or extend an existing method, she may also create her own plug-in from the readily available example source and pGina plug-in API.

pGina works by inserting itself into the Windows operating system as a GINA (Graphical Identification and Authentication) module, hence the name. Without pGina installed, when a Windows system begins to boot, a process called Winlogon loads a Microsoft GINA that is responsible for handling system events like CTRL+ALT+DEL, screen saver activation, logon attempts, etc. When pGina is installed, it inserts itself between the Winlogon process and Microsoft's GINA and handles those things directly related to its own operation (logon, locking etc) and passes everything else transparently to the Microsoft module.

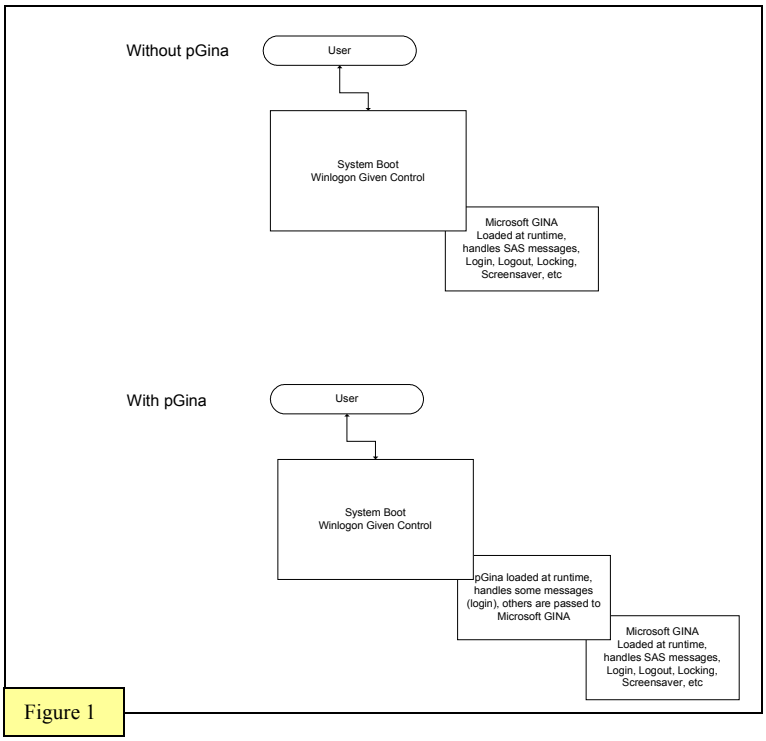


Figure 1

When Winlogon loads pGina, pGina in turn loads a plug-in chosen by the administrator. When a user attempts to login, pGina will use the selected plug-in to determine whether they should be authenticated or not. Should the plug-in allow the user to proceed, pGina will create an account for them on the local machine, add them to groups as specified by the plug-in, map drives both globally and specific to that user, and many other things depending on configuration and customization.

To accurately understand how pGina can help someone lets examine the situation for a generic administrator named Joe. Joe is responsible for a set of windows 2000 machines, as well as a large set of Linux machines. Currently Joe is forced to maintain duplicate usernames and passwords on both his Windows and UNIX servers. In addition to this, the UNIX server is also the central file server, so all the windows server is really doing is user authentication. Currently his Linux clients authenticate using the LDAP protocol. Joe can use pGina to authenticate all of his windows users from the same UNIX server by simply installing pGina, then installing the LDAP plug-in. Now Joe only has to administer a single username and password resource, no longer needing his windows server. This frees up a large portion of his time for other tasks, and reduces overhead in the cost of the Windows server and applicable client licenses.

Installation

The installation of pGina is fairly straightforward and follows many of the same conventions that other Windows programs use. ***Please note: Should pGina ever crash, or otherwise become unusable, it will prevent any access to the system. For this reason it is important to know how to boot into Safe Mode, have a rescue diskette, or otherwise be familiar with remote registry editing.***

First things first: you will need to download the latest installer from the website at http://pgina.xpasystems.com. After downloading, be sure you are logged in as a local administrator (or have local administrator privileges), that your machine is NOT part of a domain (unless using a plugin that does domain interaction) and run the installer. Confirm that you would like to install pGina and you should then be presented with a screen similar to Figure 2.

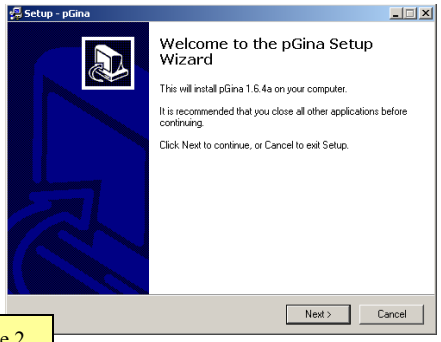


Figure 2

Here you may select the location to which you would like pGina installed. Using the default is recommended (and will be assumed throughout the remainder of this manual).

After selecting the desired location, click the Next button to continue on to Figure 3.

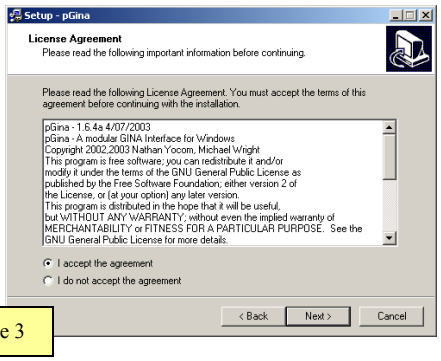


Figure 3

This dialog displays a copy of the Gnu Public License. Be sure you agree and understand and choose the "I accept the agreement" option, then click "Next" to continue to Figure 4.

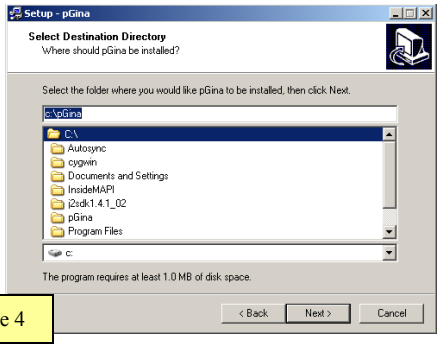


Figure 4

You will now be presented with the option of where to install pGina and necessary files. Select a different path or folder and select "Next" to continue on to Figure 5.

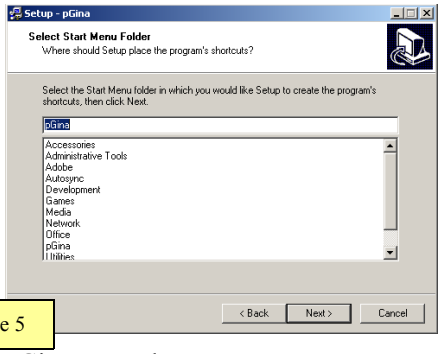


Figure 5

You may now select where in the current users start menu the pGina menu will be created. After choosing, select "Next" to continue on to Figure 6.

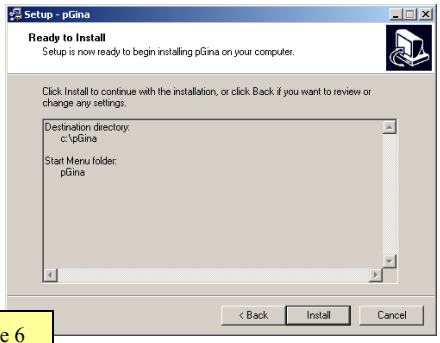


Figure 6

This screen allows you to confirm your earlier choices. Use the Back button to go back and change anything. After selecting "Install", all the necessary files will be unpacked and installed to your system in the selected location.

As a rule the default installation will work without configuration on the majority of systems, however, it is not recommended that you skip configuration before rebooting. Figure 7 shows the final dialog in the installation procedure.

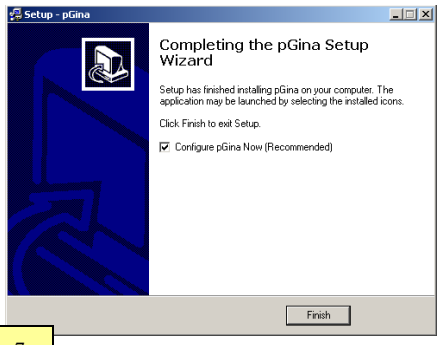


Figure 7

To skip configuration, uncheck the "Configure pGina Now" box and select "Finish". Otherwise select "Finish" to exit the installer and run the configuration utility.

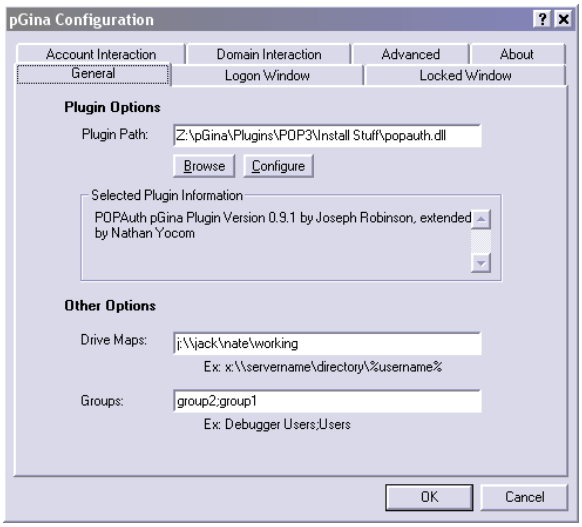
Configuring pGina

Figure 4

To configure pGina, again be sure you are logged in as an administrator or with full administrative privileges, then run the Configure pGina program by going to Start->Programs->pGina->Configure pGina. After a short splash screen has been displayed, a configuration dialog will be provided. It is through this dialog that you can change settings and options for pGina and its behavior. Let's examine the individual options and their effects on pGina.

Figure 4

General Configuration



The most commonly used options are provided on the General tab. This includes the plugin which pGina should use for authentication, drives which should be mapped for each user, as well as group membership for all users.

Plugin Options

To select or change a plugin click the Browse button and locate the plugin of choice. Information about the selected plugin is displayed in the "Selected Plugin Information" box. If a plugin allows for custom configuration clicking on the Configure button will bring up the plugin's configuration dialog(s).

Other Options

Also available on the General tab is the Drive Maps option. If set, any and all indicated drives will be mapped for all users who successfully log in. Drives are specified as DRIVE:UNC-PATH, for instance: to map drive J to \\jack\nate\working this is set to J:\\jack\nate\working. Multiple drives can be specified by separating entries with a semicolon.

Additionally, you may specify a set of groups that all users should belong to. This list takes the form of GROUP;GROUP2. For instance, if all users should be in both the Users group, as well as the Power Users group, you would enter: "Users;Power Users" without the quotes.

Added in 1.7.8:

- The options under "Other Options" in previous versions have been moved to the new "Profile" tab.
- "Show authentication method selection box" – this experimental option adds a drop down to the login dialog which allows users to select from the local machine, domain (if in a domain) and the active plugin for authentication. If the selected method fails, authentication fails (as opposed to the default behaviour of pGina to try all methods in order plugin, domain, local sam)
- "Name to display for plugin selection" – if the "Show authentication method selection box" is selected, the option in the dropdown for the plugin will have this name. This allows the admin to put things like "U. of Somewhere LDAP Server" or otherwise inform the user as to what the plugin does.

Logon Window Customization

By clicking on the Logon Window tab you can access all the options that affect the look and behavior of the logon window.

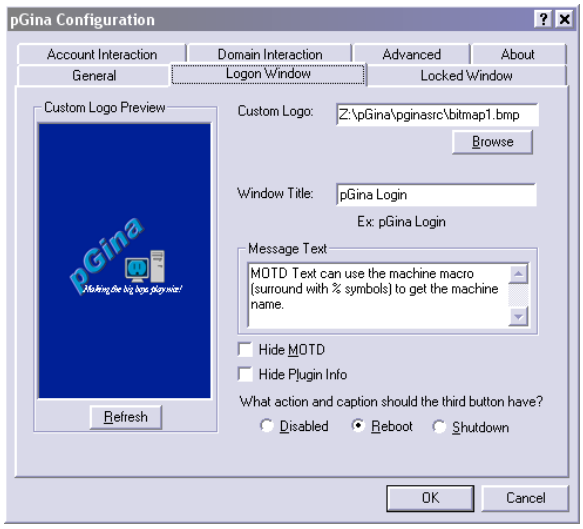
You may use the browse button to browse for a custom bitmap image to use for the logon window logo. Once selected, if valid, the image will be displayed in the preview box on the left (if not, you may press the Refresh button to refresh the view). This box displays the logo exactly as it will appear on the Logon

window. As a reference, the default logo included with pGina is 100 pixels wide, 146 pixels tall and has a resolution of 300x300 at 24bpp. Only bitmap images are valid.

The Window Title option allows you to enter a custom title for the logon window.

Message of the day text is displayed above the username and password boxes when the logon window is shown. As a matter of convenience, the text %machine% is replaced at runtime with the name of the local machine (no dns suffix), you may also use the %ip% macro to have the machines ip address displayed. If you choose to hide the message of the day, you will not be able to edit the text above (as it wouldn't be shown anyway).

Plugin information (like that shown in the General tab) is displayed below the username and password boxes. If you would rather this information not be displayed, simply check the Hide Plugin Info box.



The third button available on the logon window at runtime is configurable. This button can be disabled, cause a restart, or shutdown the machine.

Added in 1.7.8: You can now use the %ip% macro in the Message Text. At initial boot, this may show 0.0.0.0 as the network has not yet been initialized.

Locked Window Customization

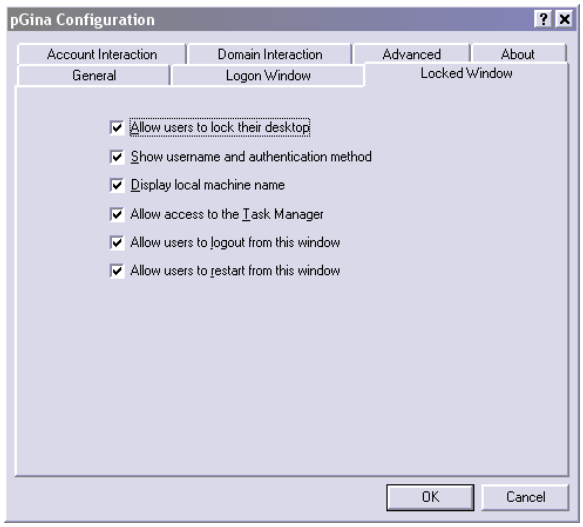
The window displayed when a user attempts to lock the machine by pressing CTRL+ALT+DEL while logged in is also customizable.

If **not** checked the "Allow users to lock their desktop" option disables the Lock button.

If checked, the second option results in the username and method of authentication (Plugin, Local, Domain) to be shown.

If checked, the third option will result in the name of the local machine being displayed.

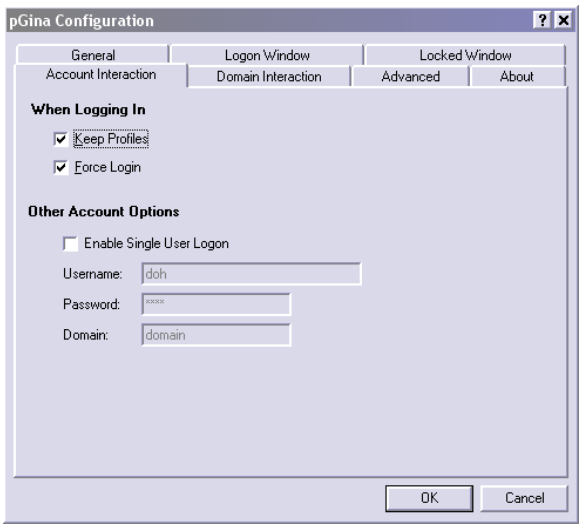
If **not** checked the fourth option disables the Task Manager button (This does not disable other shortcuts like CTRL+SHIFT+ESC).



If checked, the last two options affect the users ability to restart and logout.

Added in 1.7.6: "Do Not Allow Password Changing" disables the users ability to change their password using Ctrl+Alt+Del, "Allow Administrators To Unlock" enables "True Unlock" which means that an administrator can unlock a users desktop *without forcing the user to logoff*, and a Custom Logo option has been added to allow for customization of the Locked window's logo display.

ACCOUNT INTERACTION



Under normal circumstances, pGina handles logins by creating local accounts to match those authenticated by the plugin. This results in the creation of a profile on disk (according to the machine policy and default profile settings in Windows itself). Management of this behavior is possible using the Account Interaction tab.

When the Keep Profiles option is checked, the on disk account and profile are **not** removed on logout. This means that changes to the profile are kept between logins. When **not** checked, profiles and the local accounts are removed from the machine in their entirety, resulting in a new (based on the default, which is customizable in Windows) profile at each login.

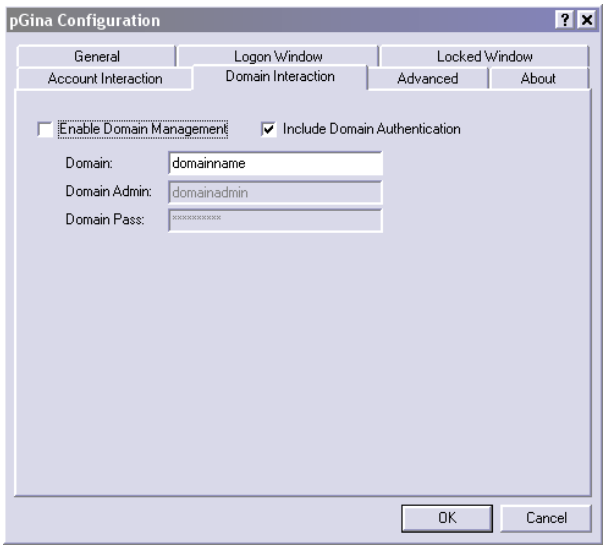
Whenever Keep Profiles is turned on, it is possible that a users password may change elsewhere, resulting in a user that is authenticated by the plugin of choice, but inconsistent with the local account. When checked, the Force Login option eliminates this issue by forcing the local password to match that authenticated by the plugin on login.

Also available is the Single User Logon option. When this is used, the given username and password (and domain if entered, otherwise local machine is assumed) are used to log onto the machine, instead of the username and password authenticated by the plugin. This allows for filtering access to a single account based on the ability to authenticate another, i.e. authenticate by plugin then login with a single account (without needing to compromise that accounts password). When this option is used, the Keep Profiles and Force Login options have no effect.

Added in 1.7.6: An "Honor Locked Accounts" option has been added, when this and Force Login are both enabled pGina will NOT reset the password on locked/disabled accounts allowing them in.

Added in 1.7.8: The "Enable account caching" option will create a local account with a preset expiration time and is to be used in conjunction with domain logins. The expiration time is in seconds. This is an EXPERIMENTAL feature and should only be used if you are **sure** you need it.

DOMAIN INTERACTION



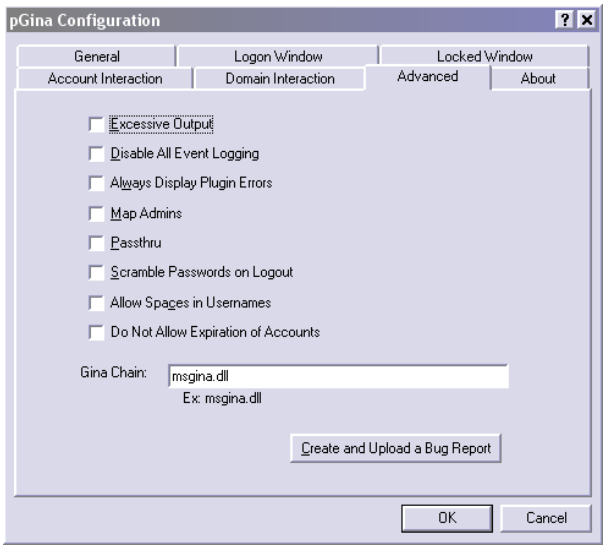
pGina also has some options for interacting in advanced ways with an existing Domain infrastructure. While this was not the original intention of pGina, it has become a very useful and needed tool in some instances. When the "Include Domain Authentication" option is checked, the given domain will also be included in the authentication chain. When this is the case, pGina will first try to authenticate with the chosen plugin, then with the given domain, then with the local machine.

When the Enable Domain Management option is checked pGina will redirect its account management (see the Account Interaction section) to the domain provided. This means that accounts will be created, deleted and

managed just as pGina would do locally. As of 1.7.4 this requires either an NT4 server or an Active Directory Server running in Mixed Mode (pure AD support is planned for future releases). An administrative username and password on the domain is required so that pGina can effect the necessary changes.

ADVANCED OPTIONS

The last configuration tab available is the Advanced tab.



When selected, the Excessive Output option turns on debugging output which is logged to the Event Log and is viewable with the windows administrator tool Event Viewer.

If selected, the Disable All Event Logging option turns off all normal as well as debug output. This prevents things like audit events from being logged.

If selected, the Always Display Plugin Errors results in a message describing any errors the plugin encountered even if authentication then succeeds with a local or domain account. If turned off, an error is only displayed if authentication totally fails.

By default, pGina only applies the Map Drives settings from the General Configuration tab to users who are authenticated by the chosen plugin. When selected, the Map Admins option results in local administrator accounts also mapping the given drive(s).

When selected, the passthru option results in pGina hiding itself and passing all control to the standard Microsoft Gina, resulting in standard windows GINA behavior.

At times, the desired management of profiles is to use the Keep Profile option in the Account Interaction section. However, the profile that remains on disk does so with the password used at that time. If the network connection is then lost, or the plugin fails authentication and the local username and pass are used then access is granted. The Scramble Passwords on Logout allows for the retention of local accounts without also inherently providing local access by resetting the password of the local account to a random value. It is **very** important that this option be enabled **only** when the Force Password option is also used. Failure to do so will result, by design, it the inability to access local accounts.

Some protocols, such as LDAP automatically ignore leading spaces, when the "Allow Spaces in Usernames" option is **not** selected, pGina will not attempt authentication for usernames which are entered with spaces in them.

Added in 1.7.6: An "Enable Experimental TS/RDP Support" turns on special code within pGina that enables TS/RDP logins to work (without the double login). This is labeled as experimental as there are many TS/RDP features (autologin, cancel==disconnect etc) options that are not yet implemented.

Added in 1.7.8: The "Respect Autologin registry information" option tells pGina whether it should automatically log on the user specified in the well know windows autologin registry. If turned on, and the registry information is valid, the user will be logged on, otherwise the information is ignored.

Added in 1.8.1: The "Autologin using plugin" option tells pGina to automatically log the user in using the normal pGina authentication process instead of just automatically logging the user into through the local SAM. You should enter the information in the User and Password fields shown. The information is NOT stored in the normal windows autologin registry key. If "Show autologin errors" is enabled, then pGina will

report a login failure as normal when the autologin is executed, otherwise it will ignore it and show the normal login dialog box. We recommend you use this method of autologin instead of the "respect autologin information" setting.

Other References

Microsoft Support Article on "Setting up a custom default user profile":
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q305709

Other pGina Documentation
http://pgina.xpasystems.com

Online Discussion Forums
http://forums.xpasystems.com/

Professional Consultation, Implementation and Support
http://www.xpasystems.com

Mailing Lists:
General: http://lists.sourceforge.net/mailman/listinfo/pgina-general
Updates: http://lists.sourceforge.net/mailman/listinfo/pgina-updates
Developers: http://lists.sourceforge.net/mailman/listinfo/pgina-devel

Other GINA Documentation
http://msdn.microsoft.com/library/en-us/security/security/winlogon_and_gina_start_page.asp