pGina Administration and Users Documentation

By: Nathan Yocom

What is pGina?

pGina, through the use of plug-in technology, allows an administrator to choose from any number of authentication sources and methods when users login to a Windows 2000/XP machine. 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. This allows for centralization of authentication and authorization management against a theoretically limitless number of user/group/security management solutions.

How does it work?

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.

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 and/or authorized. Should the plug-in allow the user to proceed, pGina will create an account for them on the local machine or domain (depending on configuration), add them to groups as specified by the plug-in and configuration, map drives both globally and specific to that user, and many other things depending on its numerous configuration options.

Installation

The installation of pGina is fairly straightforward and follows many of the same conventions that other Windows programs use. ***Please note: As pGina is a modification of Operating System level components, 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.***

Prerequisites: Windows 2000/XP, Latest SP level (5 and 2 respectively as of this writing)

After obtaining the installer, 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 you intend to make use if pGina's Domain Interaction/Management features) and run the installer.

Configuring pGina

pGina's default configuration is intended to be the safest for us in initial testing, however, there are a large number of options, each of which can be used to tailor pGina's behavior for a specific task or environment. Those options stored as registry entries in the HKEY_LOCAL_MACHINE\Software\pGina key. While hand-editing these entries is an option, pGina includes a GUI tool for configuration that makes this a much easier task. To access this tool, look under your Start menu, Programs, pGina, and choose "Configuration Tool". Alternatively, run the Configure.exe application installed in the same folder as pGina. This will present you with a tabbed dialog of settings, grouped according to function.

Plugin Tab

The plugin tab includes options which direct pGina as to which plugin it should load, where that plugin can be found, and allows for configuration of that particular plugins custom options (if available in the plugin).

Plugin Path - 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).

Show authentication method selection box – When selected, pGina will display a dropdown box on the login dialog which includes options for authenticating against a single specific target (local machine, plugin, or domain if configured). When not selected (default) pGina uses an intelligent process to perform authentication. Specifically:

1. Attempt authentication first using the plugin of choice, if that fails, and the plugin is not set as required
2. Attempt authentication against the domain of choice (if configured), if that fails
3. Attempt authentication against the local machine

For more information on the exactly process pGina uses in this state, see the "Authentication Stack" section of this document.

Name to display for plugin selection – Only effective when "Show authentication method selection box" is enabled, this specifies how the plugins is referred to in the dropdown box.

Logon Window Tab

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

Custom Logo - 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 need to 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.

Save last successful username – when enabled, the last user who successfully authenticated will automatically be filled in for the username field on the login dialog box. This is a useful feature when a machine is often used repetitively by the same user, allowing them to simply enter a password and hit enter to login.

Window Title – This is the title displayed for the login dialog box

Message of the day text - 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, or %mac% to display the machine's mac address. 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). Also note that in some circumstances Windows will start the GINA before it has fully loaded and started network services, so after initial boot the %ip% and %mac% macros may result in 'empty' addresses (0.0.0.0 or 00:00:00:00).

Hide plugin info – Plugin information (copyright, name, author, version, whatever the plugin may decide) is displayed near the bottom of the login dialog box. Enable this option to prevent this information from being displayed.

What action and caption should the third button have? - Under the password text box are three buttons, including Login and Cancel. The last of these is configurable in caption and action. Choose "Restart" if you'd like the button to effect an un-authenticated reboot of the machine, "Shutdown" to power off the machine, or "Disabled" to prevent the button from being selected at all.

Locked Window Tab

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

Allow users to lock their desktop – When disabled, users will not be able to lock their session.

Show username and authentication method – When enabled, the dialog will indicate both who is logged in, and how they were authenticated (i.e. via plugin, domain, or local SAM).

Display local machine name – When enabled, the dialog will indicate what the name of the local machine is.

Allow access to the task manager – When disabled, the user will not be able to execute the task manager application through this dialog.

Allow users to logout from this window – When disabled, users cannot effect a logout from this dialog.

Do not allow password changing – When enabled, users will be unable to change their password from this dialog.

Allow administrators to unlock a users desktop - enables "True Unlock" which means that an administrator can unlock a users desktop **without forcing the user to logoff.** This is different from the standard windows behavior of allow an administrator to force a users session to logoff from this dialog. This applies to administrators both on the local machine, and as defined by the chosen plugin.

Allow any users to force locked desktop to logoff – When enabled, a button will be shown on the locked dialog which when pressed will force the current session to logoff. This is useful in environments where desktops are often left locked by accident.

Account Interaction Tab

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 accounts, unless "Keep Accounts" is selected) 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 whose password is inconsistent with that of 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.

The Enable account caching and expiration option, when enabled, accounts are created with a preset expiration time and is to be used in conjunction with domain logins. The expiration time is in seconds. ***Note: This is an EXPERIMENTAL feature and should only be used if you are sure you need it.***

Domain Interaction Tab

pGina also has some options for interacting in advanced ways with an existing Domain infrastructure. When the "Include Domain Authentication" option is checked, the given domain will also be included in the authentication stack. 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 "Require Domain" is selected, accounts not authenticated by the domain (other than local administrators) will fail to authenticate at all.

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 Tab

The advanced tab provides a method for changing settings which effect some of the more subtle/advanced behaviors of pGina.

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 Profiles 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. Note that pGina is still loaded, but does not take an active role in the GINA interface.

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 on logout. 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 some 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.

"Enable Experimental TS/RDP Support" turns on special code within pGina that enables TS/RDP logins to work. This is labeled as experimental as there are many TS/RDP features (autologin, cancel==disconnect etc) options that are not yet implemented.

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.

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 in 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.

Profiles Tab

The profiles tab allows for configuration of profile related behavior on a global basis (as opposed to plugins, which can affect these options on a per-user basis).

Drive Maps - 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.

Groups – here 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. If a group specified does not exist, it will be created.

Default Profile Path/Profile Path – These options are intended for use with a plugin which supports roaming profiles – at the time of this writing this is limited to the FTP/SFTP plugin, please refer to the documentation for that plugin for more details regarding the use of these fields. Also note that in this case the "I am using a plugin that supports roaming profiles" should be selected.

Default Session Timeout – A time in seconds (0 for infinite) after which users will be forced to logoff.

Logoff on Screensaver Activation – When selected, during a users session whenever the screensaver activates they will be logged of. This is modified by the following options:

> *Grace Time:* Number of seconds during which the user is warned (and can optionally cancel) the logoff
>
> *Allow user to cancel:* When enabled, the user can cancel the automatic logoff
>
> *Idle timeout when workstation is locked:* Apply the auto-logoff behavior when the screensaver activates and the machine is locked as well

Troubleshooting Options

While we always hope pGina works as you'd expect, there may be times that a set of conflicting options results in behavior beyond expectaction. There are several ways you can troubleshoot the pGina process. What follows is a set of steps you can use to isolate the problem to one of several specific areas:

1. Test the plugin with the plugin tester (included with pGina) - if this does not work correctly, your problem could be related to that specific plugin and its configuration
2. If the plugin works as expected, look at the Event Viewer and view the pGina logs to see if there are any obvious errors. Note that it can be helpful to clear this log then perform the steps that cause the issue, as the log can otherwise be quite overwhelming.
3. If not immediatley apparent in the logs, try turning on Excessive Output, and re-reviewing the logs. There will be quite a bit more information.
4. Verify policies – ensure you don't have a windows group or user policy that prevents pGina from performing its job, such as password strength policies, account creation policies etc
5. Simplify – if you are using a complex set of options like Domain Management, TS/RDP, etc, try simplifying – does the problem persist if you remove the machine from the domain and use simple Single User Login?

If these steps don't make it apparent where/what the issue is, please see the “Where to go for support” section of this document.

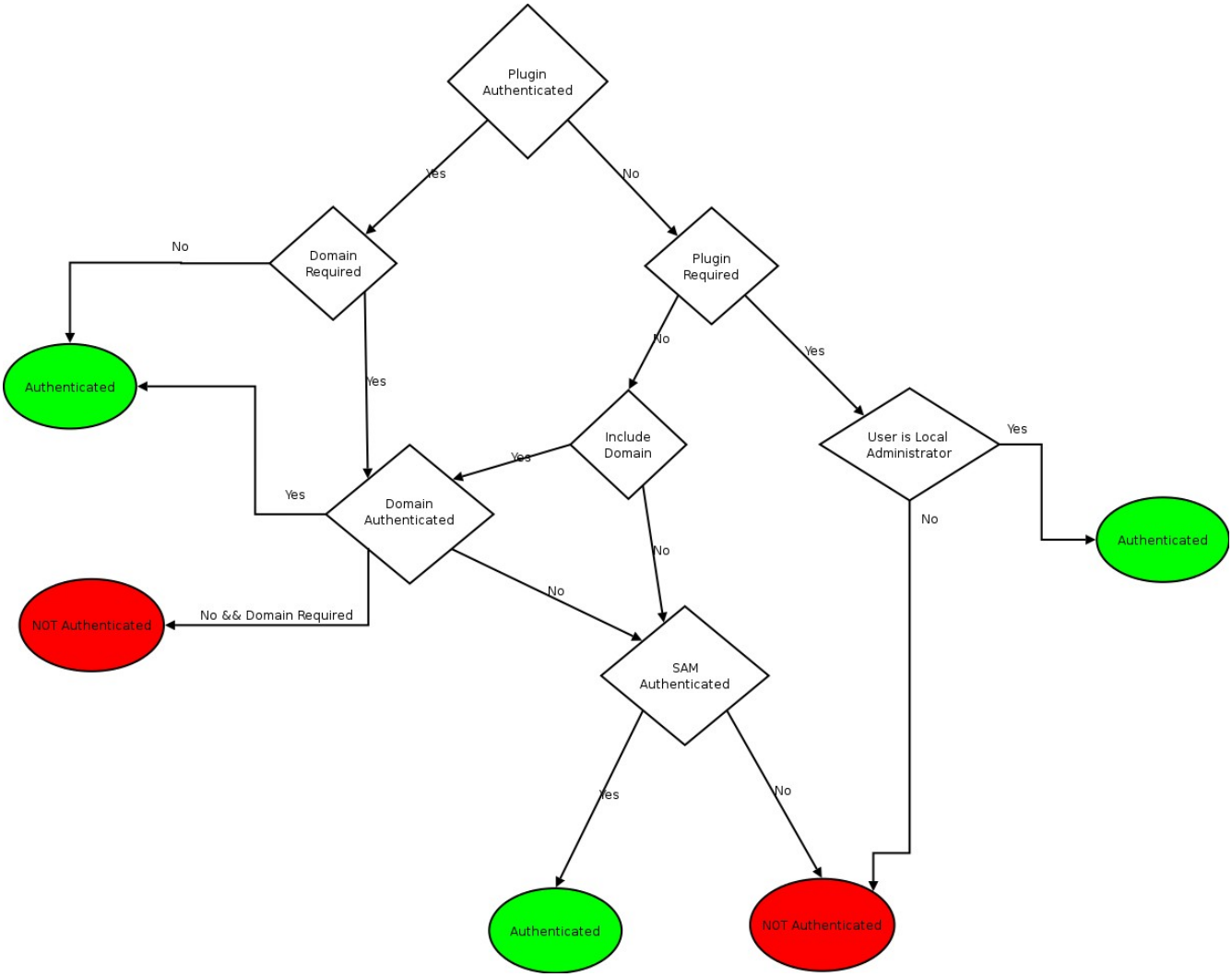
Security Concerns and Notes

It is important for the administrator to fully understand pGina's functionality and method of configuration storage. Some basic security tips which should be followed post-installation are as follows:

- All pGina settings are stored in HKLM\Software\pGina – Only the SYSTEM and Administrator (or group of administrators who should be able to configure pGina) need access to this, it is advisable you set an ACL accordingly
- All pGina files are stored in their installation location - Only the SYSTEM and Administrator (or group of administrators who should be able to configure pGina) need access to this, it is advisable you set an ACL accordingly

The Authentication Stack

The approach pGina takes to authentication and authorization can become complex when many options (Domains, plugins, etc) come into play. What follows is a diagram of the process pGina goes through after a user enters their username and password and clicks the Login button:



Other Useful Information

As an open source project, you should consult the pGina homepage at http://www.pgina.org for forums, mailing lists, irc info etc.