RADIUS Plugin for pGina | Admin Manual

Provided by Holger Weiß <holger@ZEDAT.FU-Berlin.DE>
ZEDAT | Freie Universität Berlin | http://www.ZEDAT.FU-Berlin.DE/

Please read this manual before using the RADIUS Plugin for pGina!

Overview

The RADIUS Plugin for pGina provides RADIUS authentication and (optionally) RADIUS accounting for Microsoft® Windows™ clients. It can be configured to either allow any of your users to do RADIUS authentication requests in order to log in to the Windows PC, or to permit only those users who already have an account on the local Windows PC to authenticate against your RADIUS server. As an example, this distinction enables us to use RADIUS authentication not only for pool PCs to which all students of our university have access, but also for personal Windows PCs of the staff to which students should *not* have access. The RADIUS Plugin for pGina is Free Software (that is, its GPL'd).

Requirements

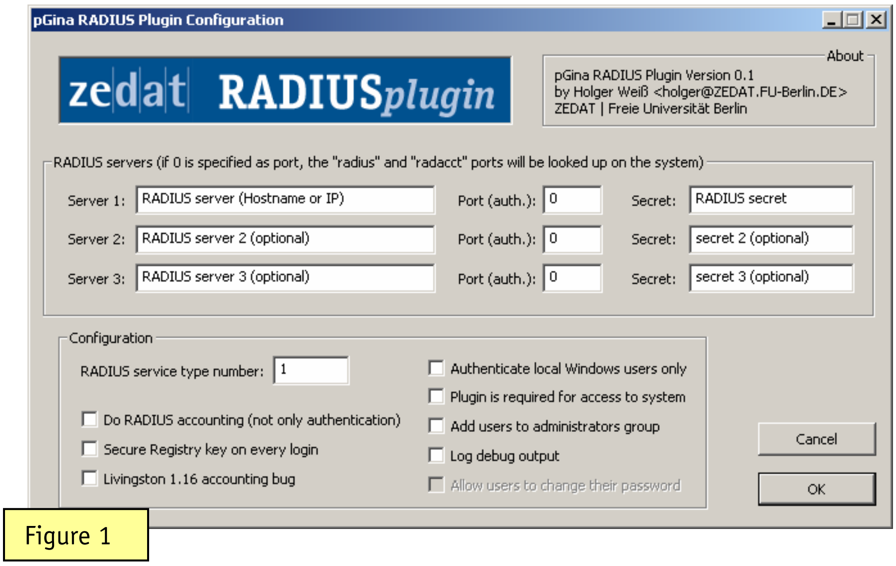
A working installation of pGina is of course required in order to use the RADIUS Plugin. pGina can be found on http://pgina.xpasystems.com/. The RADIUS Plugin requires much less than 1 MB of disk space. So far, it is tested with pGina 1.7.0 and 1.7.2 on Windows 2000 and Windows XP clients only; I don't know (and I'm sceptical) about Windows NT. In any case, please let me know if you have tested the RADIUS Plugin with newer and/or older versions of pGina and/or Windows.

Downloading and Installing the Plugin

After downloading the Windows installer file provided on the RADIUS Plugin website (http://Userpage.FU-Berlin.DE/~holger/radiusplugin/), run the executable. This will install, but *not* configure the plugin.

Configuring the Plugin

Configuration of the RADIUS Plugin is performed just as any other plugin – run the configuration utility that was provided with pGina 1.6.2 or higher, click on the "…" button next to the "Plugin Path" field and then choose the RADIUSplugin.dll from the location to which you installed it in the previous step. Once selected, you can configure the plugin by clicking on the "Configure Plugin" button at the bottom of the dialog. This will invoke the configuration dialog shown in Figure 1.



pGina RADIUS Plugin Version 0.1
by Holger Weiß <holger@ZEDAT.FU-Berlin.DE>
ZEDAT | Freie Universität Berlin

RADIUS servers (if 0 is specified as port, the "radius" and "radacct" ports will be looked up on the system)

Server 1: RADIUS server (Hostname or IP) Port (auth.): 0 Secret: RADIUS secret
Server 2: RADIUS server 2 (optional) Port (auth.): 0 Secret: secret 2 (optional)
Server 3: RADIUS server 3 (optional) Port (auth.): 0 Secret: secret 3 (optional)

Configuration

RADIUS service type number: 1

☐ Do RADIUS accounting (not only authentication)
☐ Secure Registry key on every login
☐ Livingston 1.16 accounting bug
☐ Authenticate local Windows users only
☐ Plugin is required for access to system
☐ Add users to administrators group
☐ Log debug output
☐ Allow users to change their password

Figure 1

RADIUS servers section

Within this section, the RADIUS server(s) to use for authentication (and accounting) are specified. If you specify multiple RADIUS servers, they are tried in order. The first server to return success or failure causes the RADIUS Plugin to return success or failure. Only if a server fails to respond it is skipped, and the next server in turn is used. Specifying more than one server is of course fully optional. For each server to use, there are three fields:

SERVER

This is the hostname or IP address of the RADIUS server to use for authentication and (optionally) accounting.

PORT (AUTH.)

This is the UDP port number used for RADIUS authentication. RADIUS accounting will be done one port higher. The default port name for authentication is “`radius`”; the default port name for accounting is “`radacct`”. Those will be used if `0` is specified as port number; they will be looked up from `%SystemRoot%\system32\drivers\etc\services`.

SECRET

This is your RADIUS password. Please note that the *secret will be saved plaintext to the Windows Registry*, which means that *anybody who is in the “administrators” group* on the Windows PC will be able to read it! See also the option “Secure Registry key on every login”.

Configuration section

Within this section, various options that influence the operation of the RADIUS Plugin may be specified.

RADIUS SERVICE TYPE NUMBER

This field allows you to specify the numerical value of the service type attribute sent to the RADIUS server. The RADIUS Plugin uses this attribute for accounting requests only, not for authentication requests. For possible values see RFC 2865, 5.6 (although you can of course use a custom value instead). The default value used by the plugin is `1` (“Login”).

DO RADIUS ACCOUNTING (NOT ONLY AUTHENTICATION)

If this option is set, the RADIUS Plugin will not only provide RADIUS authentication, but also send an accounting start request when the user logs in and an appropriate stop request when the user logs out.

SECURE REGISTRY KEY ON EVERY LOGIN

No matter whether or not this option is set: The RADIUS Plugin will *always* set an access control list (ACL) on its Registry key `HKLM\Software\pGina\RADIUSplugin` (which includes the password of your RADIUS server). This ACL gives only the “administrators” group read and write access to the key. Any users not in this group won’t have any access to that key, but *all users in the “administrators” group will have full access* to it. This ACL will be *(re)set every time you close the RADIUS Plugin configuration dialog* by clicking “Ok”! Moreover, if you set this option, the ACL will also be set *every* time a user logs in.

LIVINGSTON 1.16 ACCOUNTING BUG

When used, the accounting response vector is *not* validated. This option will probably only be necessary on *really* old (i.e. Livingston 1.16) servers.

AUTHENTICATE LOCAL WINDOWS USERS ONLY

If this option is set, only those users who already have an account on the local Windows PC will be allowed to do RADIUS authentication requests. For users that don’t exist locally, the RADIUS server won’t be asked, but the plugin will report an appropriate error instead. If this option is not set, any user (except for “administrator”) may do RADIUS authentication requests.

PLUGIN IS REQUIRED FOR ACCESS TO SYSTEM

This option dictates the actions of pGina upon a failed authentication attempt. If the plugin is required, then only a local administrator account can login via the local SAM. If the plugin is not required, then pGina will check to see if a local account and password exist which match the attempted login.

ADD USERS TO ADMINISTRATORS GROUP

Setting this option would add *all* users that authenticate via RADIUS to the “administrators” group. You may find this useful for some debugging purposes, but it should of course *never be set for production use*. Future versions of the RADIUS Plugin will probably allow configuring *which* users to put in the “administrators” group.

LOG DEBUG OUTPUT

If set, the RADIUS Plugin will write some output to the Windows event log, this should be useful for debugging. However, if this option is not set, no logging output will be produced at all, since the pGina logs should normally suffice.

ALLOW USERS TO CHANGE THEIR PASSWORD

The option to allow users to change their RADIUS password is *not* implemented yet. If you would be interested in testing such an option, please let me know!

Uninstalling the Plugin

If the RADIUS Plugin is still in use, pGina must first be configured to use another plugin. After logging in with the new plugin, use the uninstaller provided with the RADIUS Plugin in order to remove it. This will delete all RADIUS Plugin files and the Registry key.

Contact

The RADIUS Plugin for pGina is written by Holger Weiß <holger@ZEDAT.FU-Berlin.DE>. Feel free to drop me an e-mail if you have any questions, bug reports or comments on the RADIUS Plugin.