By Nick Owen
Published: 2007-03-07 17:17

How to configure Apache to use Radius for Two-factor Authentication

This document describes how to add **WiKID two-factor authentication** to Apache 2.x using mod_auth_xradius or mod_ldap. Our configuration was as follows:

- Fedora Core 5
- Apache 2.2.2-10
- mod_auth_xradius. We recommend using **mod_auth_xradius** rather than mod_auth_radius. Documentation for mod_auth_xradius can be found in the README file and **here**.
- For two-factor authentication, we were using WiKID, in this case, the commercial version.

Here's how it will work, when the user clicks on a two-factor protected link, they will be prompted for a username and password. The user generates the one-time passcode on their WiKID token and enters it into the password prompt. Apache will route the username and one-time password to the WiKID server via mod_auth_xradius. If the username and one-time password match what WiKID expects, the server will tell Apache to grant access. First, we add Apache to the WiKID Strong Authentication Server as a network client, then add radius to Apache. I assume you already have a WiKID domain and users setup.

So, start by adding a new Radius network client to the WiKID server for your web server:

- Log into WiKID server web interface (*`http://yourwikidserver/WiKIDAdim`*).
- Select **Network Clients** tab.
- Click on **Create New Network Client.**
- Fill in the requested information.

- For the IP Address, use the web server IP address
- For Protocol, select Radius
- Hit the Add button, and on the next page, enter a shared secret
- Do not enter anything into the Return Attribute box

- From the terminal or via ssh, run 'stop' and then 'start' to load the network client into the built-in WiKID radius server

That is it for the WiKID server.

Now to get Apache ready for two-factor authentication. We need to get and install mod_auth_xradius for Apache 2.x. First, we need to install httpd-devel so we can compile mod_auth_xradius:

```
# yum install httpd-devel

# wget http://www.outoforder.cc/downloads/mod_auth_xradius/mod_auth_xradius-0.4.6.tar.bz2

# bunzip2 mod_auth_xradius-0.4.6.tar.bz2

# tar -xvf mod_auth_xradius-0.4.6.tar

# cd mod_auth_xradius-0.4.6

# ./configure --with-apxs=/sbin/apxs

# make

# make install
```

Be sure to check the location of *apxs*.

Now you need to add two more things to your *httpd.conf*. First add

```
LoadModule auth_xradius_module modules/mod_auth_xradius.so
AuthXRadiusCache dbm conf/authxcache
```

Check out the **xradius docs for other options**. It is important to cache the authentication results. If you don't, every http request will generate an authentication request every attempt to validate the one-time passcode except the first attempt will fail.

```
<directory "/var/www/html/radius">
  AuthType Basic
  AuthName "Please enter your username and WiKID one-time passcode for entry to this site."
  AuthXRadiusAddServer "wikid_server_address:1812" "wikidserver_shared_secret"
  AuthXRadiusTimeout 7
  AuthXRadiusRetries 2
  require valid-user
</directory>
```

You will want to change *wikid_server_address* to the IP address of the WiKID server and *wikidserver_shared_secret* to the shared secret you configured above in the WiKID server.

You can enter the same information into a .htaccess file, or a directory directive if you like, depending on where the information you want protected by two-factor authentication is. We used the location directive to put a virtual directory behind two-factor authentication. For more information about

Links

- WiKID Strong Authentication - **Two-Factor Authentication**
- OutOfOrder.cc - **Mod_auth_xradius**
- Apache - **The Apache Webserver**