Using Zarafa with SecurePass

A key problem for many enterprises is how to collaborate effectively and securely on mobility. Zarafa's open source collaboration software provides a cost-effective and reliable replacement to proprietary software such as Microsoft Exchange. The web app goes beyond the traditional web client, working from any browser and featuring drag & drop of attachments to send emails and files quicker. An integrate calendar provides multi-user weekly calendaring and advanced delegation. Zarafa can integrate SecurePass to manage users, permissions and email alias. An identity management system is a valuable tool for the entire organisation, especially to avoid intrusions from malicious users and prevent identity theft. Considering that Zarafa could be integrated to CRM, social networks, void and management softwares, it's even more important and convenient to improve protection of online data by granting access only to authorized users.

Integration options

Zarafa offers integration through the LDAP protocol. Be it Active Directory or OpenLDAP, Zarafa needs that the LDAP schema is extended to hold Zarafa specific information. Although SecurePass exposes its services also through LDAP, it currently does not support extending its schema, therefore other options must be used.

This guide will help you configuring Zarafa with SecurePass using two different approaches:

1) Using SecurePass' Single Sign On (SSO)
2) By modifying the login code

1) Single Sign On

The advantage of using SecurePass' Single Sign On system is that users accessing Zarafa will be transparently signed in. It requires less efforts than modifying a source code and also will allow easier future upgrades.

This approach uses Zarafa's capabilities of detecting the *REMOTE_USER* attribute after a successful login with Apache. We will therefore proceed as if it was a standard CAS web server, as described here: http://support.secure-pass.net/wiki/index.php/Apache

Add the needed CAS lines to the Zarafa webacces config in */etc/httpd/conf.d/zarafa-webaccess.conf* as follows:

```
<Directory /usr/share/zarafa-webaccess/>
    DirectoryIndex index.php
    Options -Indexes +FollowSymLinks
    AllowOverride Options
    Order allow,deny
    Allow from all

   AuthType CAS
   require valid-user
</Directory>
```

Modify the zarafa *server.cfg* and add the apache user to the *local_admin_users*.
Example:

```
local_admin_users = root vmail apache
```

If Zarafa has been installed to host a single domain/company, alter the file *config.php* in */usr/share/zarafa-webaccess* and change *LOGINNAME_STRIP_DOMAIN* to 'true'.

2) Login integration

The main advantage of modifying the Login page of Zarafa is that the customer can combine both existing Active Directory integration and the additional security of SecurePass. As a matter of fact, the login page will display both Password and SecurePass (refer to the screenshot). This is a useful situation if you want to have Web Access through Internet, while allowing MAPI or IMAP on the internal network.

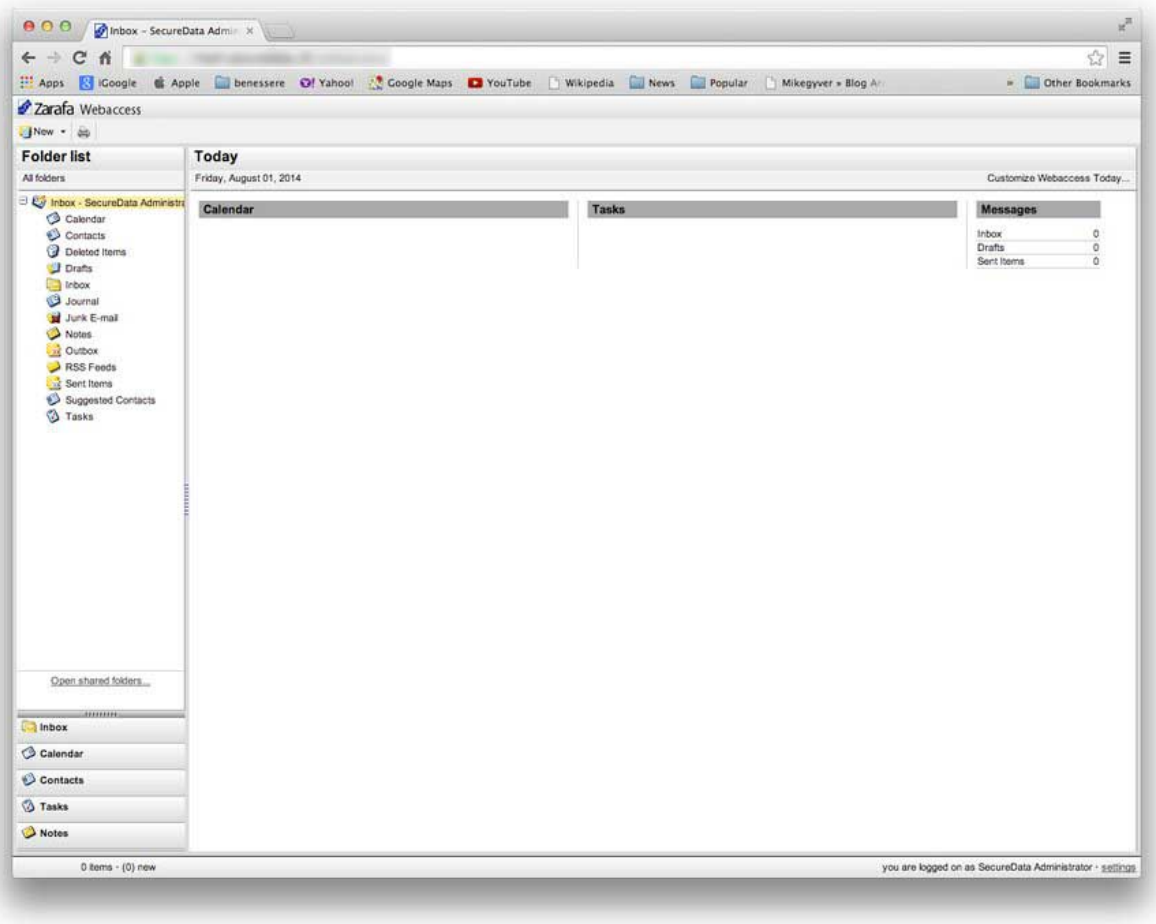
This step requires modifications in the PHP code

that handles the login requests.

Files are usually located into */usr/share/zarafa-webaccess*. Create a *securepass* subdirectory that will hold the radius class and download the class itself as follows:

```
# mkdir securepass
# wget
https://raw.githubusercontent.com/gpaterno/wp-securepass/master/
radius.class.php
```

Then patches index.php and client/login.php with the code provided in the appendix of this guide. Use the *patch* command to apply the modifications.



See also

- Register to SecurePass
- Configure pdSense with SecurePass
- Secure and real time collaboration with Etherpad and SecurePass

Appendix: index.php

```
--- index.php.orig    2014-06-03 21:42:37.000000000 +0200
+++ index.php    2014-06-03 22:27:36.000000000 +0200
@@ -114,6 +114,8 @@

        require("server/core/class.pluginmanager.php");
        require("server/core/class.plugin.php");
+
+    require("securepass/radius.class.php");

        // Destroy session if an user loggs out
        if($_GET && array_key_exists("logout", $_GET)) {
@@ -144,6 +146,24 @@
                }
        }

+      // SecurePass
+      if($_POST && array_key_exists("otp", $_POST)) {
+
+             $otp = $_POST["otp"];
+
+             $radius_host = 'radius1.secure-pass.net';
+             $radius_secret = 'CHANGEME';
+
+             $radius = new Radius($radius_host, $radius_secret);
+
+             // Check the password via RADIUS
+             if (! $radius->AccessRequest($_SESSION["username"], $otp)) {
+                          $hresult = "FAILED_SECUREPASS_AUTH";
+                          $_SESSION = array();
+                          $_SESSION["hresult"] = $hresult;
+             }
+      }
+

        // Create global mapi object. This object is used in many other files
        $GLOBALS["mapisession"] = new MAPISession();
```

Appendix: login.php

```
--- client/login.php.orig    2014-06-03 21:44:33.000000000 +0200
+++ client/login.php    2014-06-03 22:28:33.000000000 +0200
@@ -91,6 +91,9 @@
                      case MAPI_E_NETWORK_ERROR:
                             echo _("Cannot connect to the Zarafa Server.");
                             break;
+              case FAILED_SECUREPASS_AUTH;
+                     echo _("SecurePass authentication failed.");
+                     break;
                      default:
                             echo "Unknown MAPI Error:
".get_mapi_error_name($_SESSION["hresult"]);
               }
@@ -118,6 +121,10 @@
                                                                   <td><input
type="password" name="password" id="password" class="inputelement"></td>
                                                            </tr>
                                                            <tr>
+                                                           <th><label
for="otp"><?=_("SecurePass")?>:</label></th>
+                                                           <td><input type="password"
name="otp" id="otp" class="inputelement"></td>
+                                                    </tr>
+                                                    <tr>
                                                                   <th><label
for="language"><?=_("Language")?>:</label></th>
                                                                   <td>
                                                                          <select
name="language" id="language" class="inputelement">
```