

Example - How to Install and Configure YubiX

<https://campus.barracuda.com/doc/46898293/>

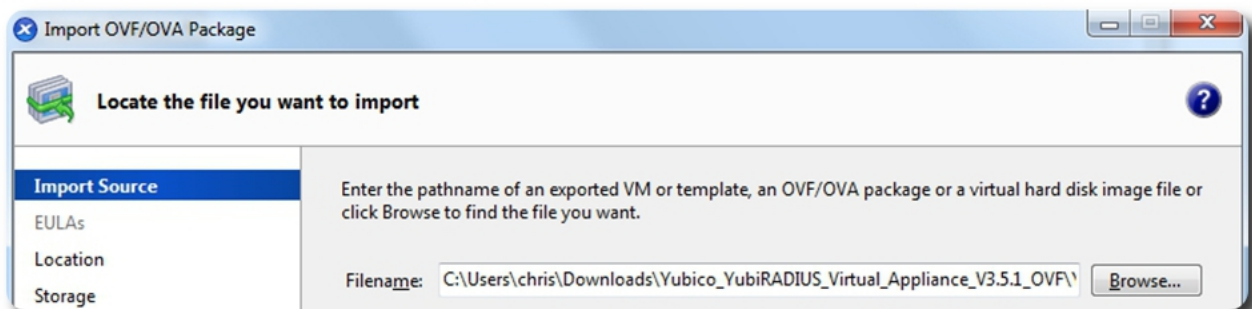
Deploy the YubiX virtual appliance to authenticate users on the Barracuda SSL VPN. After YubiX is installed, Barracuda SSL VPN can be configured to act as a RADIUS client.

Prerequisites

- A YubiKey
- A VM host server to load the Virtual Appliance
- An external user database that both the SSL VPN and YubiX servers can connect to, such as Active Directory or LDAP.

Installing the YubiX virtual appliance

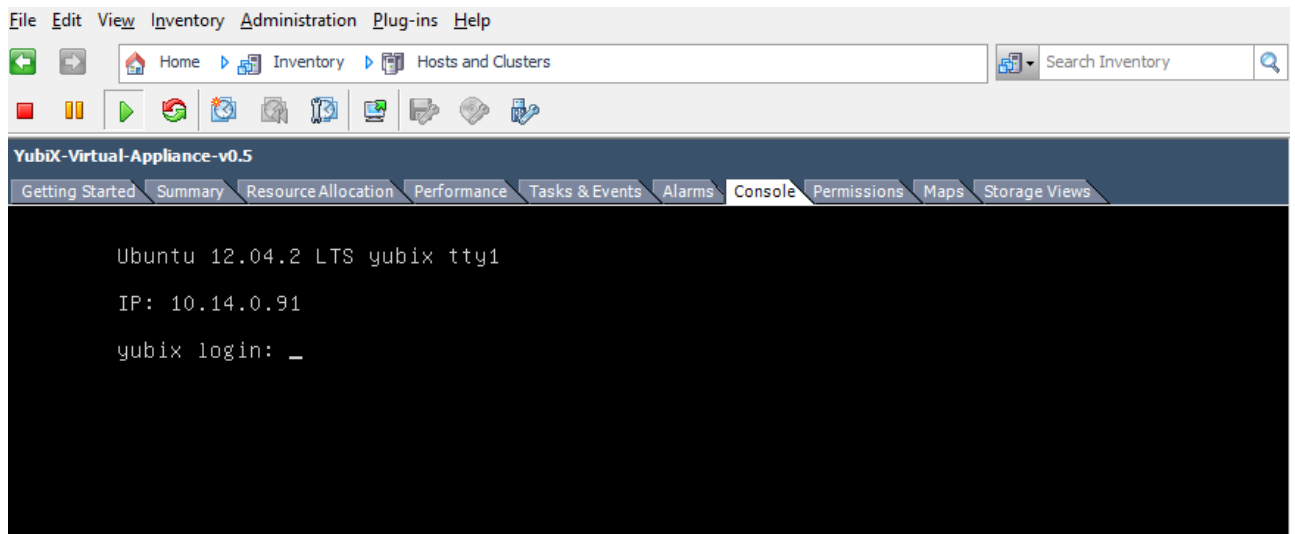
1. Go to <http://www.yubico.com>.
2. Download a virtual appliance of the YubiX. You will need to register on the Yubico website to download the virtual appliance image. Enter your registration details and click **Submit**. Yubico will send an email containing a link to the image. Click the link to download the image.
3. Extract the VM from the zip.
4. Edit the .vmx file, change the config.version from 7 to 8, and save the file.
5. Import the virtual machine into your VM host server (e.g., XenServer).



6. Edit the machine settings, remove the Ethernet adapter, and add a new one. This allows the VM to connect to the network.

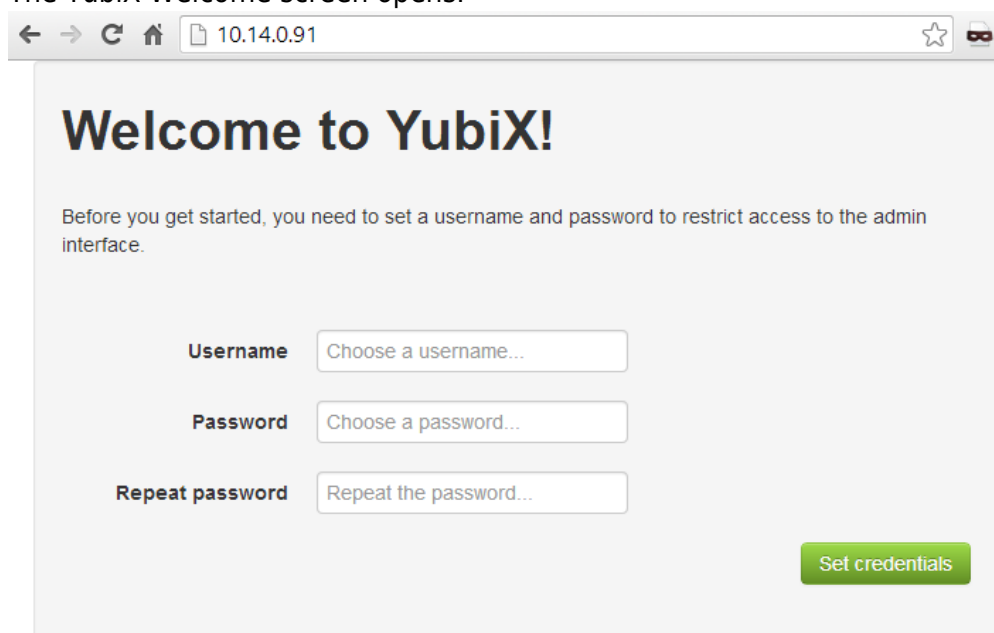
Configuring the YubiRADIUS virtual appliance

1. After the virtual appliance has imported, start it and connect to the console. Log in with user **yubikey** and password **yubico**.

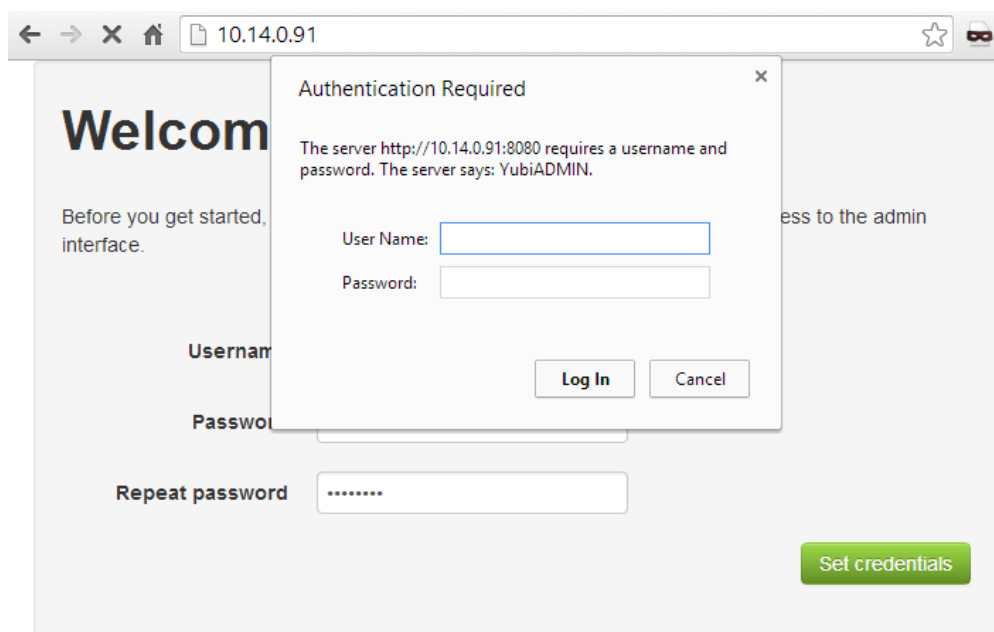


This example configuration uses DHCP by default.

2. With a web browser, navigate to the IP address of the appliance. You can find it on the console. The YubiX Welcome screen opens.



3. Create a username and set and confirm the password.
4. Click **Set credentials**. You get prompted for YubiADMIN.



5. Log in with the username and password you just created.
6. In the left menu, select **FreeRADIUS**, then click the **RADIUS Clients** tab.
7. Add a new RADIUS client to the bottom of the file, which should match the IP address of your SSL VPN. Choose a unique shared secret.

Changes require the FreeRADIUS server to be restarted.

File: /etc/freeradius/clients.conf

```

204 #}
205
206
207 #client 10.10.10.10 {
208 #   # secret and password are mapped through the "secrets" file.
209 #   secret      = testing123
210 #   shortname   = liv1
211 #   # the following three fields are optional, but may be used by
212 #   # checkrad.pl for simultaneous usage checks
213 #   nastype     = livingston
214 #   login      = !root
215 #   password    = someadminpas
216 #}
217
218 #####
219 #
220 # Per-socket client lists. The configuration entries are exactly
221 # the same as above, but they are nested inside of a section.
222 #
223 # You can have as many per-socket client lists as you have "listen"
224 # sections, or you can re-use a list among multiple "listen" sections.
225 #
226 # Un-comment this section, and edit a "listen" section to add:
227 # "clients = per_socket_clients". That IP address/port combination
228 # will then accept ONLY the clients listed in this section.
229 #
230 #clients per_socket_clients {
231 #   client 192.168.3.4 {
232 #       secret = testing123
233 #   }
234 #}
235
236 client 10.14.0.190 {
237     secret      = testing123
238     shortname    = sslvpn
239 }
```

Save **Reset form**

8. Click **Save**.
9. In the left menu, select **YubiAuth**, then click on **Password Validation**.
10. Select the **Authenticate users against LDAP** check box.
11. Enter a valid LDAP server URL and Bind DN for your AD/LDAP service.

YubiADMIN

Dashboard

MODULES

YubiAdmin

YubiX System

YubiAuth

YubiKey Key Storage Module

YubiKey Validation Server

FreeRADIUS

General
Database
Password Validation
OTP Validation

Manage Users
Advanced

LDAP authentication

Settings for authenticating users against an LDAP server. When LDAP authentication is used only users that exist on the LDAP server will be permitted to log in, and password validation will be delegated to the LDAP server.

☒ **Authenticate users against LDAP**

Check this to authenticate users passwords externally against an LDAP server.

LDAP server URL

ldap://10.14.0.2


Bind DN for user authentication

cn=,ou=Employees,dc=co,dc=co,dc=uk


☒ **Automatically create users from LDAP**

Auto-create missing users in YubiAuth upon log in if the user is valid in the LDAP database.

12. This configuration will use the YubiCloud validation servers. Verify and/or create access rules on your network's firewall to allow outbound access on TCP ports 80 and 443 to api.yubico.com, api2.yubico.com, api3.yubico.com, api4.yubico.com, and api5.yubico.com.
13. Get a client ID and API key:
 1. Go to <https://upgrade.yubico.com/getapikey/>
 2. Enter your email address that you used to register with Yubico.
 3. Select the password field, insert your YubiKey and select **Get API Key** to have Yubico enter the password for you.

 <https://upgrade.yubico.com/getapikey/>

yubico
the key to the cloud

 **Yubico Get API Key**

Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

Your **e-mail** address:

YubiKey **one-time** password:

14. On the **YubiAuth > OTP validation** page, insert the resulting Client ID and Secret Key into the **Client ID** and **API Key** fields respectively and click **Save**.

Client ID

☐ Show API Key

API Key

Confirm API Key

You should now be able to do a test authentication locally on the YubiX box in the shell, using:

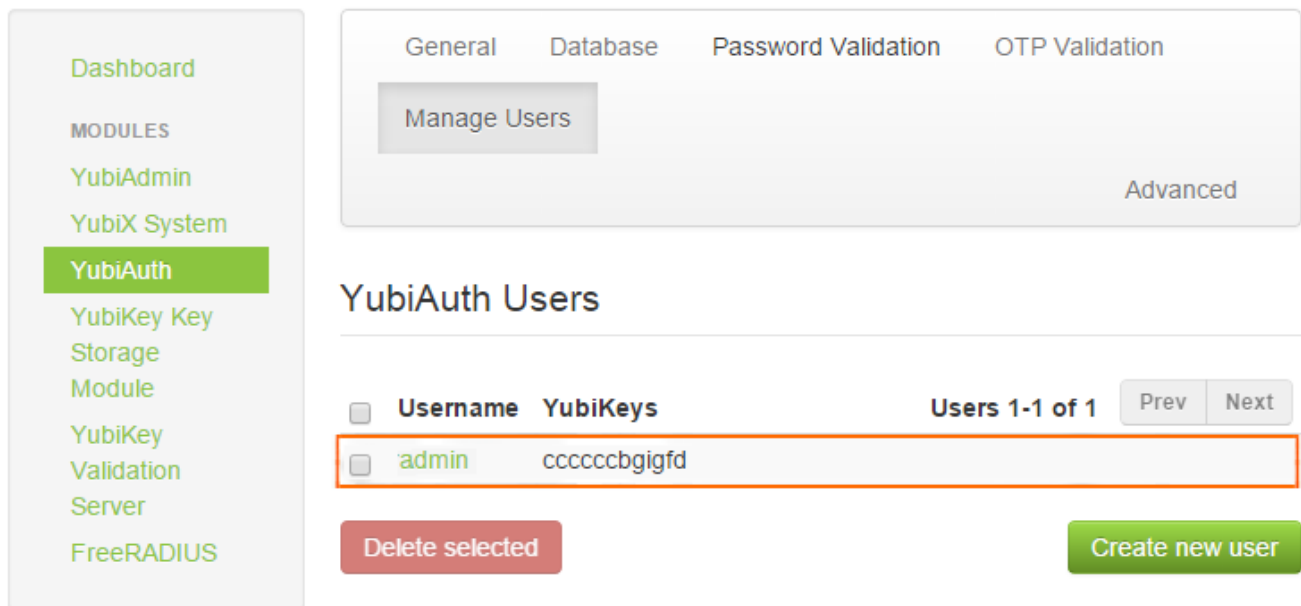
```
radtest user1 passwordccccccccccbbtrtikevthrvhceudvvuveidihckgrgl 127.0.0.1
0 testing123
Sending Access-Request of id 51 to 127.0.0.1 port 1812
```

```
User-Name = "user1"
User-Password = "testingccccccccccbbtrtikevthrvhceudvvuveidihckgrgl"
NAS-IP-Address = 127.0.1.1
NAS-Port = 0
```

```
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=51,
length=20
```

This will add that AD user into the **Manage Users** section and assign the Yubikey you used to that account.

YubiADMIN



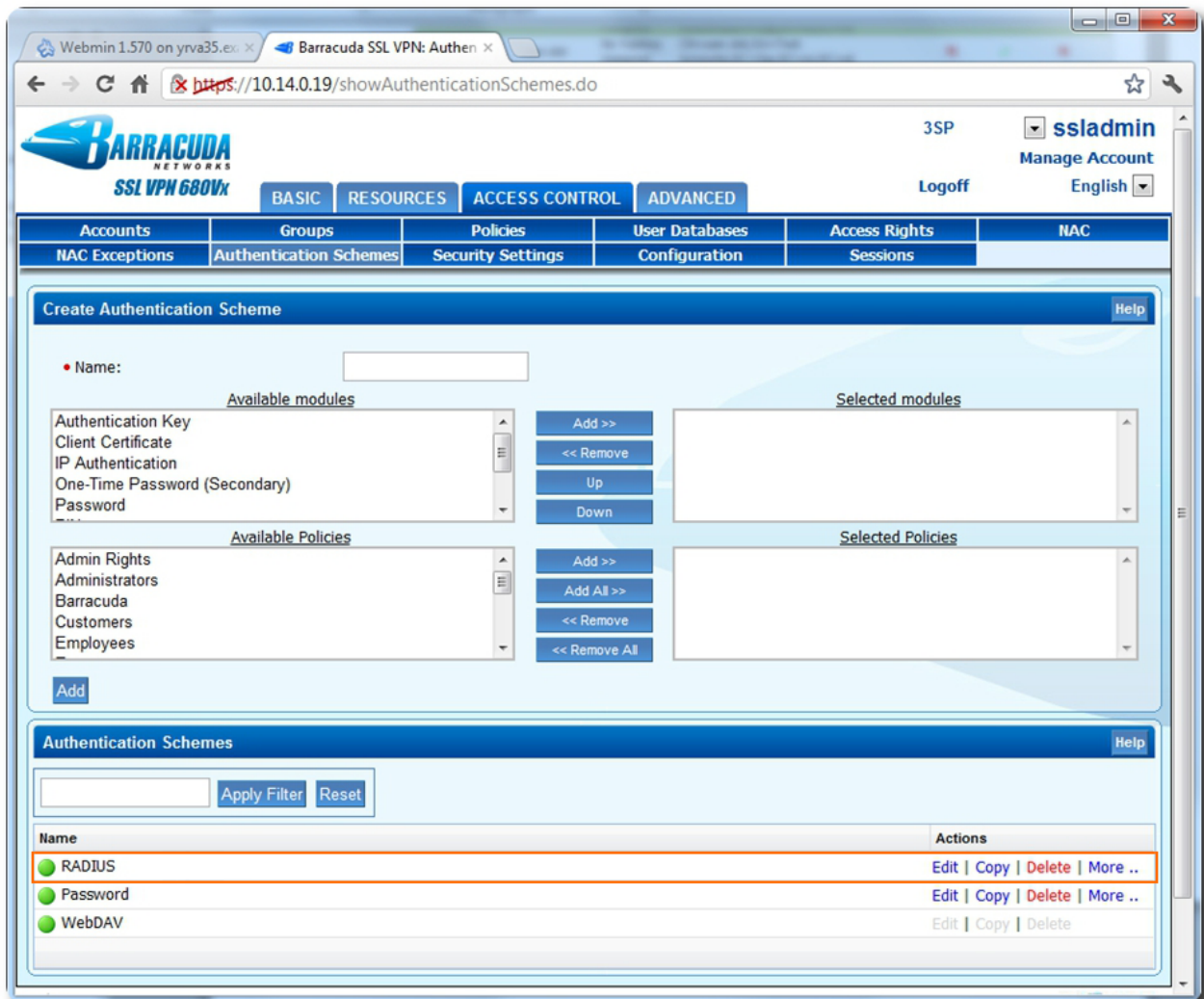
The screenshot shows the YubiADMIN web interface. On the left is a sidebar menu with the following items: Dashboard, MODULES, YubiAdmin, YubiX System, YubiAuth (highlighted in green), YubiKey Key Storage Module, YubiKey Validation Server, and FreeRADIUS. The main content area has tabs for General, Database, Password Validation, and OTP Validation. Below these tabs is a 'Manage Users' button. To the right of the tabs is an 'Advanced' link. Below the tabs, the section is titled 'YubiAuth Users'. It contains a table with two columns: 'Username' and 'YubiKeys'. There is one user listed: 'admin' with the YubiKey 'ccccccbgigfd'. The table has a 'Users 1-1 of 1' indicator and 'Prev' and 'Next' buttons. Below the table are two buttons: 'Delete selected' and 'Create new user'.

Username	YubiKeys
admin	ccccccbgigfd

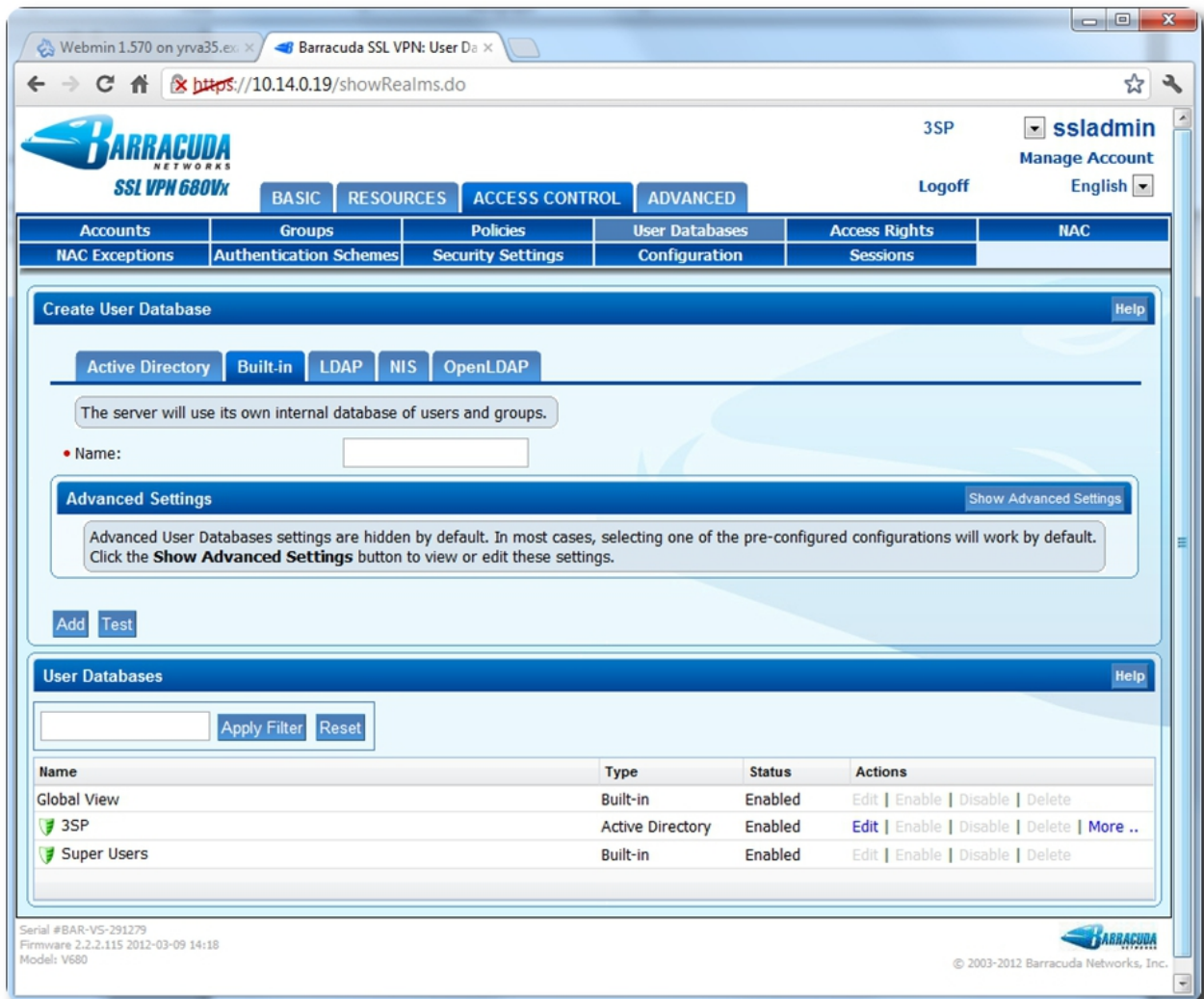
You can now test with an external RADIUS client, such as NTRadPing, to see if external requests are being answered. Note that you must have a RADIUS client configured for the machine you test from.

Configuring Barracuda SSL VPN

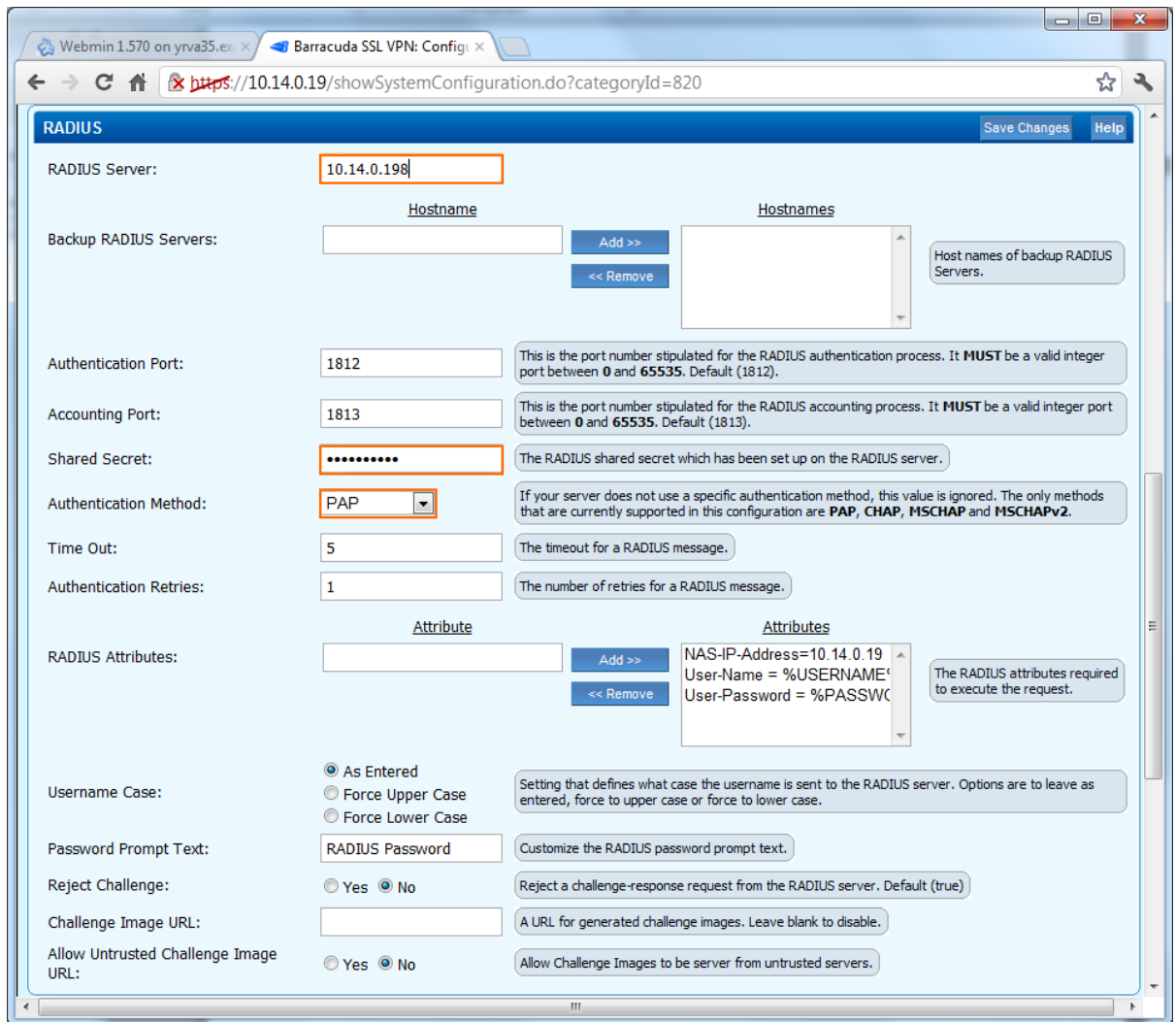
1. Log on to the Barracuda SSL VPN web interface as *ssladmin*.
2. Navigate to **ACCESS CONTROL > Authentication Schemes**.
3. Create a new authentication scheme that contains the RADIUS module (Select **RADIUS**, click **Add**). Select a policy that will be able to use this authentication (such as *Everyone* for example) and click **Add**. The new module will appear. This may be set as the default module by clicking **More** next to the item and choosing **Increase Priority** until it appears at the top of the list.



4. Navigate to **ACCESS CONTROL > User Databases** and ensure you are connected to the same user database that YubiRADIUS is connected to. If not, edit the user database and alter the settings so that this is correct.



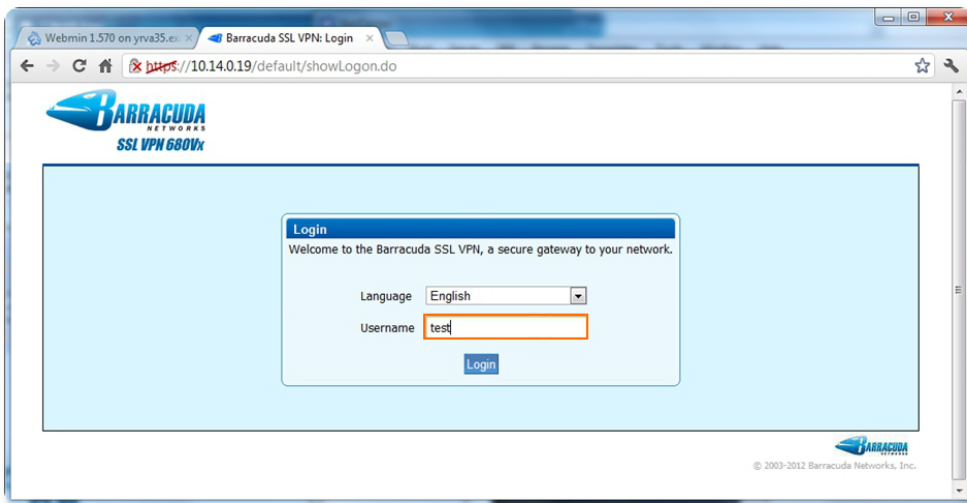
5. Navigate to **ACCESS CONTROL > Configuration** and scroll to the **RADIUS** section.
 1. Enter the hostname or IP address for the YubiRADIUS appliance in the **RADIUS Server** field.
 2. Keep the ports the same.
 3. Enter the same shared secret as used in the YubiRADIUS RADIUS client configuration earlier.
 4. Set the **Authentication Method** to **PAP**.
You can keep all other default settings.
 5. Click **Save Changes**.



The screenshot shows the 'RADIUS' configuration page in the Barracuda SSL VPN web interface. The page is titled 'RADIUS' and has a 'Save Changes' button in the top right. The configuration fields are as follows:

- RADIUS Server:** 10.14.0.198
- Backup RADIUS Servers:** (Empty list with 'Add >>' and '<< Remove' buttons)
- Authentication Port:** 1812 (Help text: This is the port number stipulated for the RADIUS authentication process. It **MUST** be a valid integer port between 0 and 65535. Default (1812).)
- Accounting Port:** 1813 (Help text: This is the port number stipulated for the RADIUS accounting process. It **MUST** be a valid integer port between 0 and 65535. Default (1813).)
- Shared Secret:** (Masked with dots)
- Authentication Method:** PAP (Help text: If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are PAP, CHAP, MSCHAP and MSCHAPv2.)
- Time Out:** 5 (Help text: The timeout for a RADIUS message.)
- Authentication Retries:** 1 (Help text: The number of retries for a RADIUS message.)
- RADIUS Attributes:** (List of attributes: NAS-IP-Address=10.14.0.19, User-Name = %USERNAME%, User-Password = %PASSWORD%)
- Username Case:** As Entered (Help text: Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.)
- Password Prompt Text:** RADIUS Password (Help text: Customize the RADIUS password prompt text.)
- Reject Challenge:** No (Help text: Reject a challenge-response request from the RADIUS server. Default (true).)
- Challenge Image URL:** (Empty field, Help text: A URL for generated challenge images. Leave blank to disable.)
- Allow Untrusted Challenge Image URL:** No (Help text: Allow Challenge Images to be server from untrusted servers.)

6. You can now connect to the Barracuda SSL VPN via this user account. Enter the username and click **Login**.

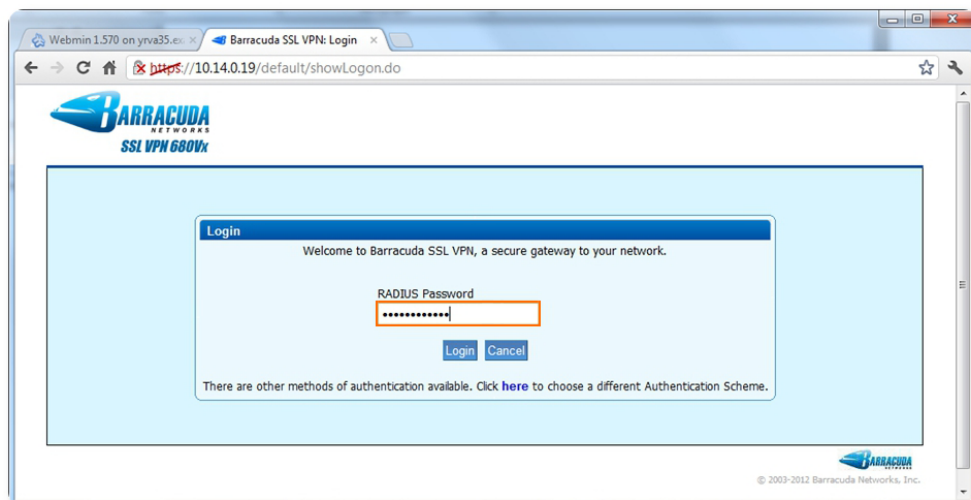


The screenshot shows the 'Barracuda SSL VPN Login' page. The page has a blue header with the Barracuda logo and 'SSL VPN 6800v'. The main content area is light blue. A 'Login' box contains the following fields:

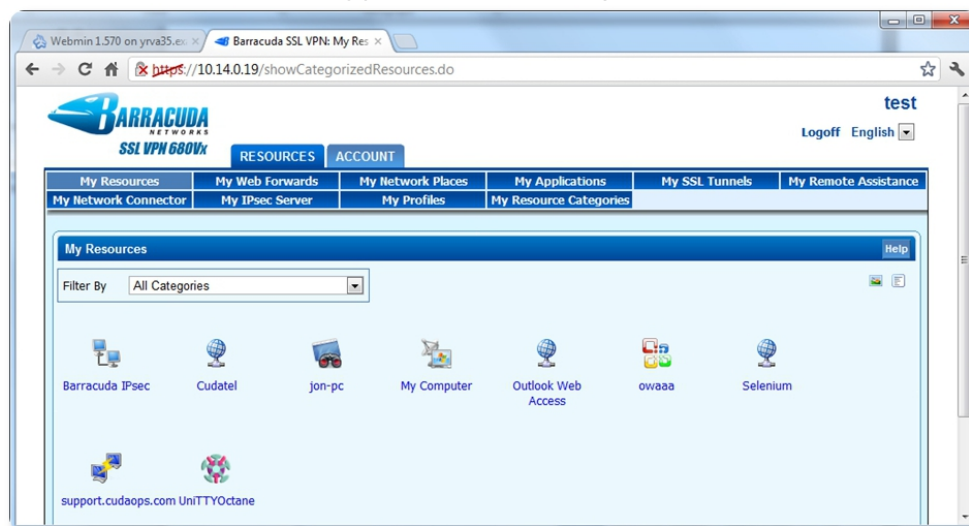
- Language:** English (dropdown menu)
- Username:** test
- Login:** (button)

Below the login box, there is a copyright notice: © 2003-2012 Barracuda Networks, Inc.

7. Enter the user's user database password **WITHOUT** pressing **Enter**, and immediately press the **YubiKey** button (so that the password is a combination of the user's password + the YubiKey password).



The user should now be logged on successfully:



Figures

1. yrd_v_app1.png
2. yrd_v_app_01.png
3. yrd_v_app_02.png
4. yrd_v_app_03.png
5. yrd_v_app_04.png
6. yrd_v_app_05.png
7. yrd_v_app_06.png
8. yrd_v_app_07.png
9. yrd_v_app_users.png
10. yrd_v_app21.png
11. yrd_v_app22.png
12. yrd_v_app23.png
13. yrd_v_app24.png
14. yrd_v_app25.png
15. yrd_v_app26.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.