Apache HTTP Server

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Ryan Sheridan	mailto:rsheridan@securenvoy.com	

Two-Factor for Apache HTTP Server

This document describes how to integrate Apache HTTP Server with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Apache is the most commonly used Web Server on Linux systems. Web Servers are used to serve Web Pages requested by client computers. Clients typically request and view Web Pages using Web Browser applications such as Firefox, Opera, Chrome, or Mozilla.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as SSH), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone or SecurEnvoy Soft Token app to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilizing the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Linux

Ubuntu Server 14.04.3, Apache HTTP Server 2.4.7

Microsoft

Microsoft Windows Server 2012, Windows Server 2012 R2

SecurEnvoy

SecurEnvoy Server

SecurAccess software release v7.3.501

© 2014 SecurEnvoy Ltd. All rights reserved

Index

Apache HTTP Server 1
Authenticating Users Using SecurAccess Server by SecurEnvoy 1
Index 3
1.0 Prerequisites 3
1.1 Configure Ubuntu Apache for Radius 4
2.0 Configuration of SecurEnvoy 6
3.0 Test Two-Factor Authentication 7
4.0 Notes 7

1.0 Prerequisites

It is assumed that the Ubuntu Server with Apache Server is installed is authenticating users with a username and password to a LDAP User Data Store such as Active Directory.

SecurEnvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the ADFS server(s), additional open ports will be required.

The following table shows what token types are supported.

Token Types Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓

Token Types Not Supported	
OneSwipe QRCode	X

© 2014 SecurEnvoy Ltd. All rights reserved

1.1 Configure Ubuntu Apache for Radius

First, we need to install the Apache HTTP Server (development headers), in order to compile the radius package

```
$ # sudo apt-get install apache2-dev
```

Next, download and extract the mod_auth_xradius package

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

Apache has made changes to the API from V2.2 to V2.4, but this has not been reflected in the mod_auth_xradius packages to date, so manual change must be made in the /src/xradius_cache.c file. As noted below open the file in the the nano editor, Find the two instance of 'unixd_config' and replace with 'ap_unixd_config', and then save the file.

```
# sudo nano /src/xradius_cache.c
```

Now, its time to compile the mod_auth_xradius package

```
# ./configure --with-apxs=/sbin/apxs
# sudo make
# sudo make install
```

Confirm the source file location of the module and move it to the 'mods-available' directory in Apache.

```
# sudo cp /usr/lib/apache2/modules/mod_auth_xradius.so /etc/apache2/mods-available
```

Now, we need to enable module for use by Apache by editing in the nano text editor

```
#cd /etc/apache2
#sudo nano mods-enabled/mod_auth_xradius.load
```

© 2014 SecurEnvoy Ltd. All rights reserved

Add the following lines and save the file

```
LoadModule auth_xradius_module /etc/apache2/mods-
available/mod_auth_xradius.so
AuthXRadiusCache dbm /var/authxcache
```

In order to bypass failure of initial authentication requests it is important to cache HTTP authentication requests. We have cached these results in the file authxcache in the /var/ directory. Create directory / cache file, and apply permissions

```
#sudo nano /var/authxcache
#sudo chown :www-data /var/authxcache
#sudo chmod 755 /var/authxcache
```

Now, we need to update the apache2.conf with the lines below order to reflect the configuration changes. This change will apply two-factor protection at the root and sub sites. **Note: You may modify the <Directory "/var/www/html/YOURDIR"> to protect specific sub sites

```
<Directory "/var/www/html/">
 AuthType Basic
 AuthBasicProvider xradius
 AuthName "Please enter your username and Password + SecurEnvoy OTP."
 AuthXRadiusAddServer "SecurEnvoy_server_address:1812"
"SecurEnvoyServer_shared_secret"
 AuthXRadiusTimeout 7
 AuthXRadiusRetries 2
 require valid-user
</Directory>
```

Finally, restart your Apache server for changes to take affect.

```
#sudo service apache2 restart
```

Now, you are ready to test. For Troubleshooting, see /var/log/auth.log' while you test.

Note: that we have not made any changes to the account setup, so the user is expected to have an account in Active Directory or similar. You can configure Apache for LDAP authentication using Windbind to Active Directory (https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto).

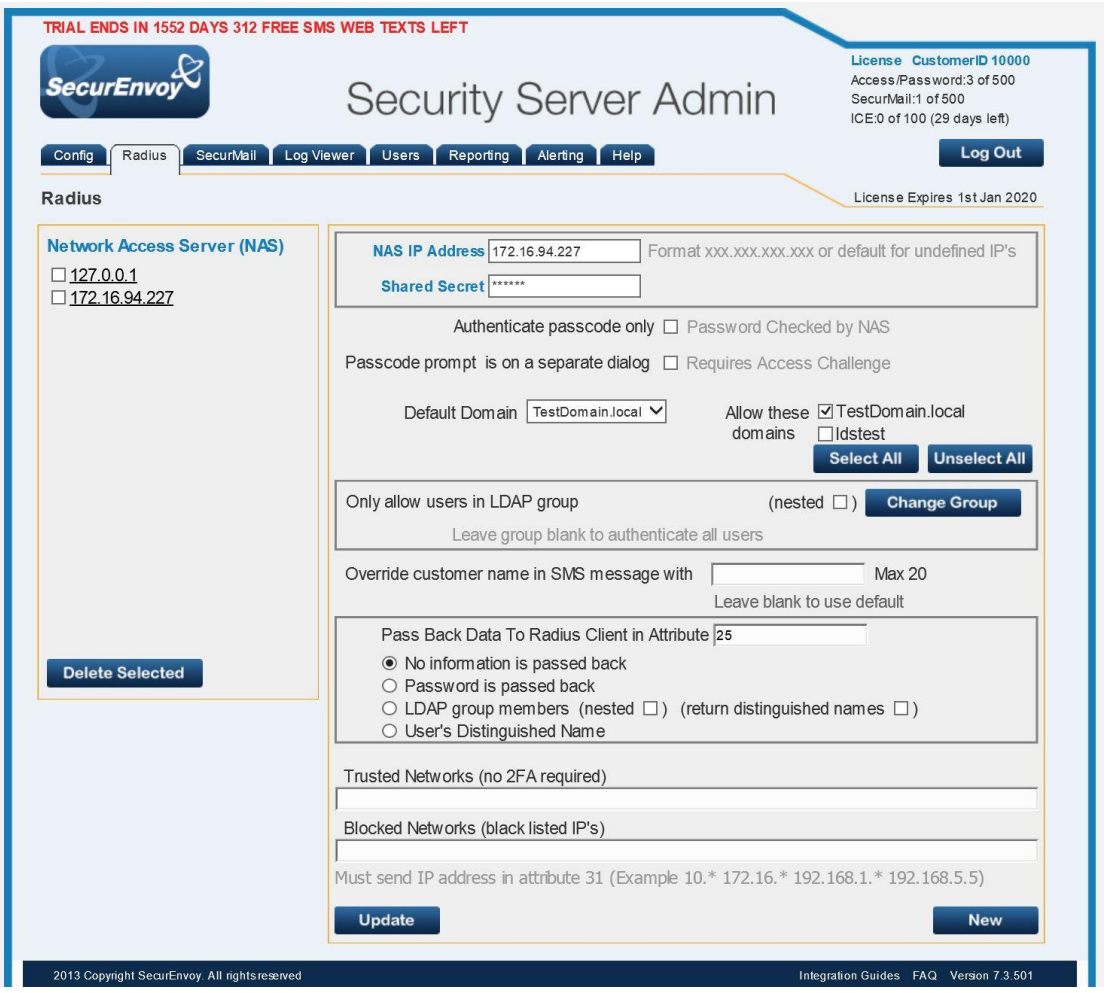
© 2014 SecurEnvoy Ltd. All rights reserved

2.0 *Configuration of SecurEnvoy*

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** tab



Enter IP address and Shared secret for each Apache Server that wishes to use SecurEnvoy Two-Factor authentication.

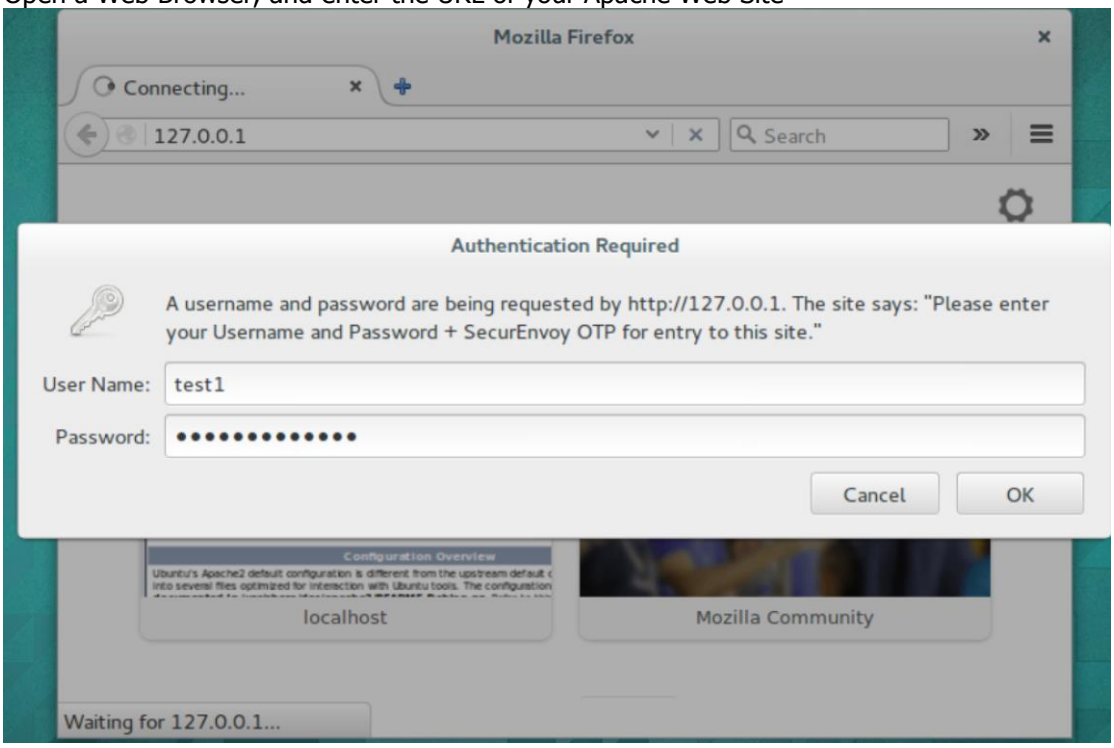
Click to **Uncheck** the box "Passcode prompt is on a separate dialog".

Click **"Update"** to confirm settings.

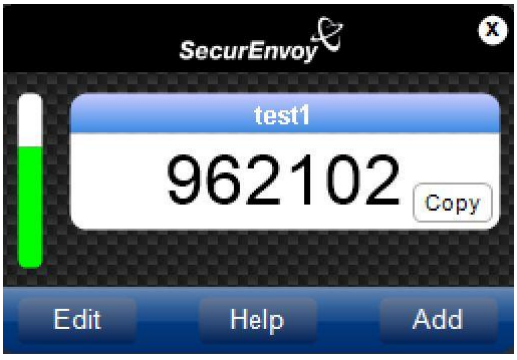
Click **"Logout"** when finished. This will log out of the Administrative session.

3.0 Test Two-Factor Authentication

Open a Web Browser, and enter the URL of your Apache Web Site



Enter your LDAP "Username" and "Password" + "6 Digit Passcode" (Passcode delivered via Soft Token in this example)



4.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved