SSH to Ubuntu 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	

SSH to Ubuntu Server

This document describes how to integrate Ubuntu Server (Linux) SSH with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Secure Shell (**SSH**), sometimes known as Secure Socket Shell, is a Linux/UNIX-based command interface and protocol for securely getting access to a remote computer.

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, Putty SSH client

Microsoft

Microsoft Windows Server 2012, Windows Server 2012 R2

SecurEnvoy

SecurEnvoy Server

SecurAccess software release v7.3.501

Index

1.0 Prerequisites

It is assumed that the Ubuntu Server with SSH 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

1.1 Configure Ubuntu Linux for PAM Radius

Install the PAM Radius package:

```
$ sudo apt-get install libpam-radius-auth
```

Configure the PAM Radius:

```
$ sudo vim /etc/pam_radius_auth.conf
```

Edit the line "other-server other-secret 3" replacing 'other-server' with IP address or hostname of your SecurEnvoy Security Server and change 'other-secret' the shared secret for this network client. (The Shared secret should match the SecurEnvoy Radius profile configuration)

Now that the package is setup and pointing to your SecurEnvoy Security server, let's configure a service to use it.

Edit your /etc/pam.d/sshd file and add the line:

```
auth       sufficient  pam_radius_auth.so
```

Just above:

```
# Standard Un*x authentication.
@include common-auth
```

Now, you are ready to test. For Troubleshooting, run 'tail -f /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 that via LDAP authentication using Windbind to Active Directory (https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto).

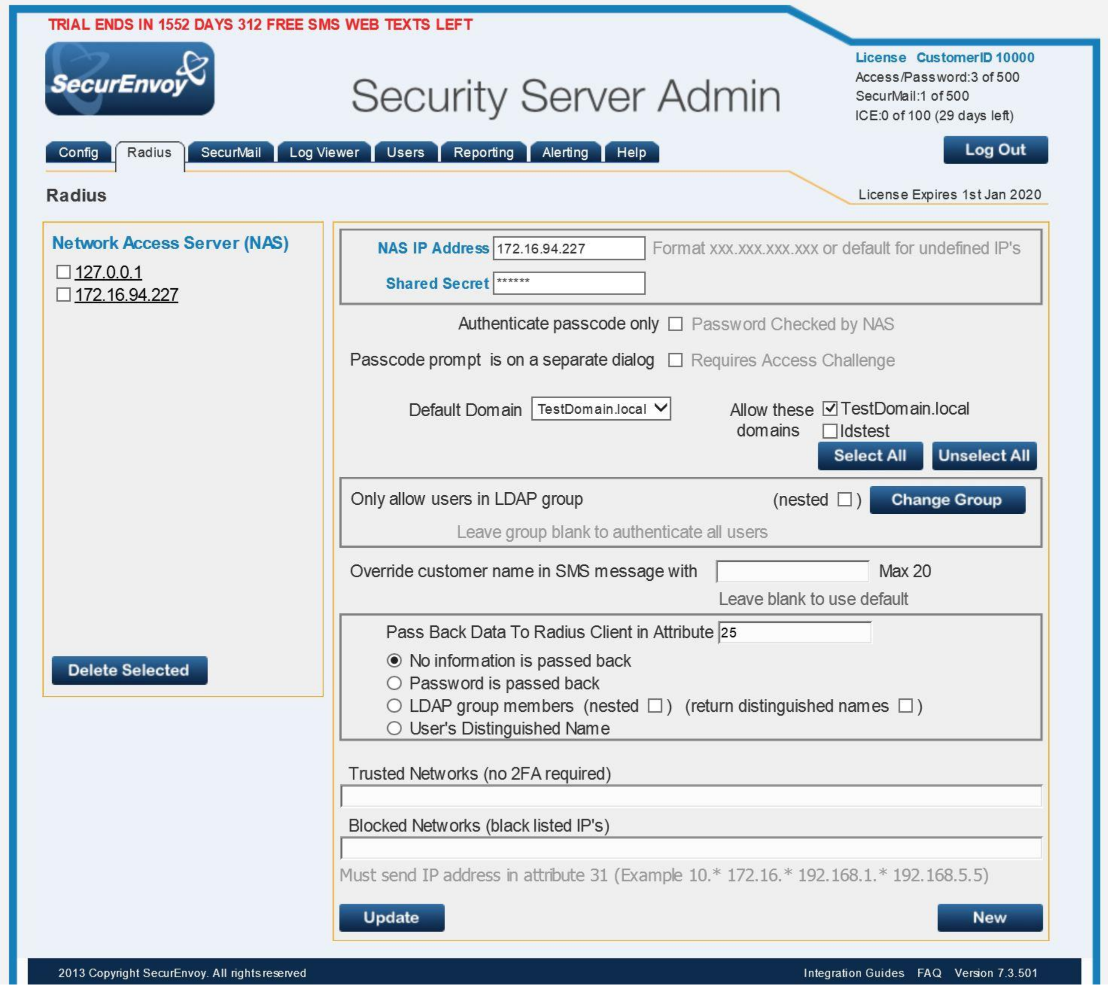
9

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



TRIAL ENDS IN 1552 DAYS 312 FREE SMS WEB TEXTS LEFT

Security Server Admin

License CustomerID 10000
Access/Password:3 of 500
SecurMail:1 of 500
ICE:0 of 100 (29 days left)

License Expires 1st Jan 2020

Radius

Network Access Server (NAS)

□ 127.0.0.1
□ 172.16.94.227

NAS IP Address 172.16.94.227 Format xxx.xxx.xxx.xxx or default for undefined IP's

Shared Secret ******

Authenticate passcode only □ Password Checked by NAS

Passcode prompt is on a separate dialog □ Requires Access Challenge

Default Domain TestDomain.local

Allow these domains ☑ TestDomain.local
□ ldstest

Only allow users in LDAP group (nested □)

Leave group blank to authenticate all users

Override customer name in SMS message with Max 20

Leave blank to use default

Pass Back Data To Radius Client in Attribute 25

● No information is passed back
○ Password is passed back
○ LDAP group members (nested □) (return distinguished names □)
○ User's Distinguished Name

Trusted Networks (no 2FA required)

Blocked Networks (black listed IP's)

Must send IP address in attribute 31 (Example 10.* 172.16.* 192.168.1.* 192.168.5.5)

2013 Copyright SecurEnvoy. All rights reserved

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

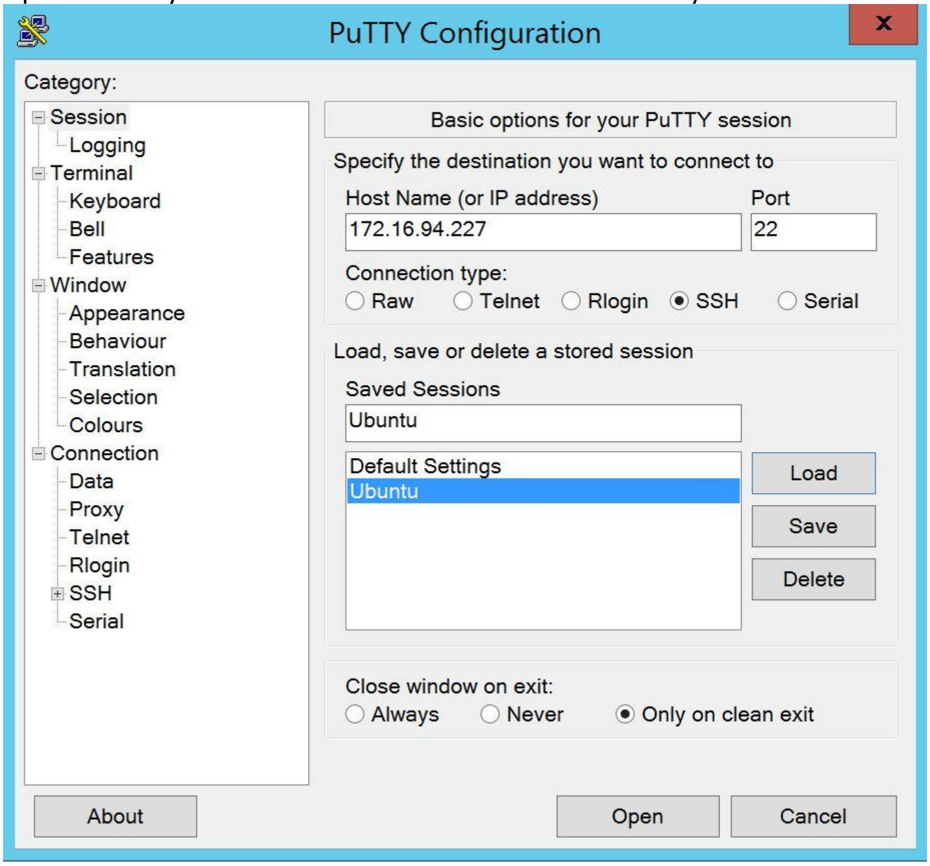
Click to **Uncheck** the box "Passcode prompt is on a separate dialog".

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

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

3.0 Test Two-Factor Authentication

Open the Putty SSH Client – Connect to the IP Address of your Ubuntu SSH Server



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 172.16.94.227

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

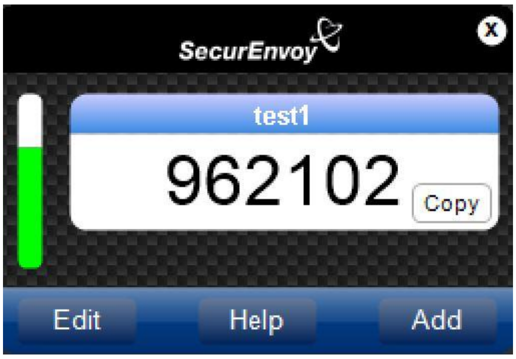
Load, save or delete a stored session

Saved Sessions: Ubuntu

Default Settings
Ubuntu

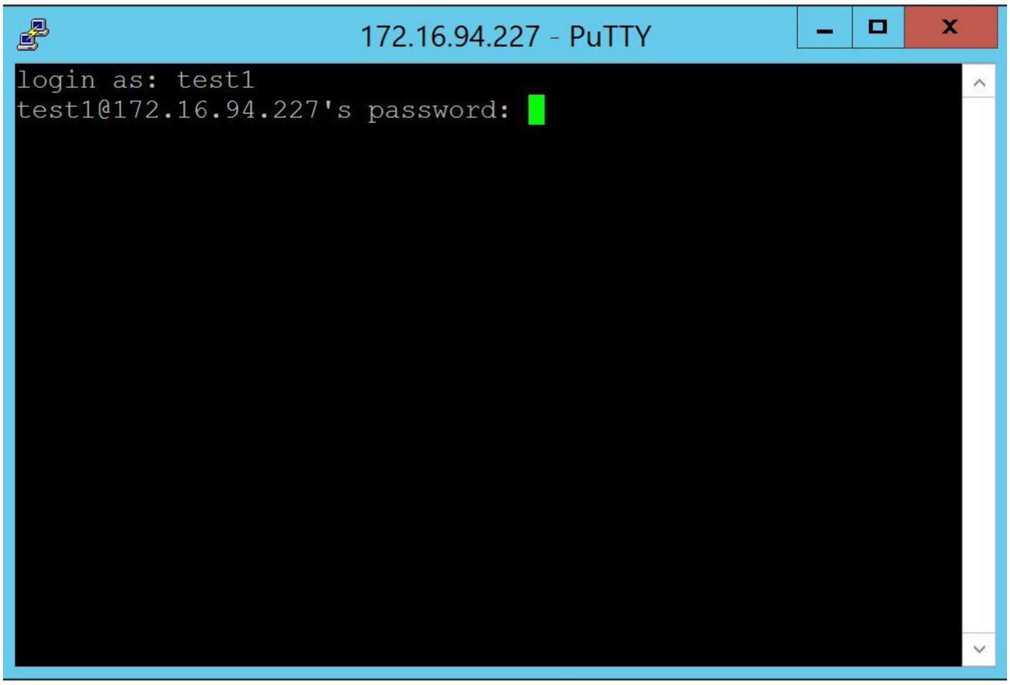
Close window on exit: ○ Always ○ Never ● Only on clean exit

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



test1

962102



```
login as: test1
test1@172.16.94.227's password:
```

4.0 Notes