

UNIOTP PAM AUTHENTICATION GUIDE

VERSION 1.1

SecuTech

www.eSecuTech.com

The data and information contained in this document cannot be altered without the express written permission of SecuTech Solution Inc. No part of this document can be reproduced or transmitted for any purpose whatsoever, either by electronic or mechanical means.

The general terms of trade of SecuTech Solution Inc. apply. Diverging agreements must be made in writing.

Copyright © SecuTech Solution Inc. All rights reserved.

WINDOWS is a registered trademark of Microsoft Corporation.

The WINDOWS-logo is a registered trademark ^(TM) of Microsoft Corporation.

Software License

The software and the enclosed documentation are copyright-protected. By installing the software, you agree to the conditions of the licensing agreement.

Licensing Agreement

SecuTech Solution Inc. (SecuTech for short) gives the buyer the simple, exclusive and non-transferable licensing right to use the software on one individual computer or networked computer system (LAN). Copying and any other form of reproduction of the software in full or in part as well as mixing and linking it with others is prohibited. The buyer is authorized to make one single copy of the software as backup. SecuTech reserves the right to change or improve the software without notice or to replace it with a new development. SecuTech is not obliged to inform the buyer of changes, improvements or new developments or to make these available to him. A legally binding promise of certain qualities is not given. SecuTech is not responsible for damage unless it is the result of deliberate action or negligence on the part of SecuTech or its aids and assistants. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

Contact Information

HTTP: www.eSecuTech.com

E-Mail: Sales@eSecuTech.com

Please Email any comments, suggestions or questions regarding this document or our products to us at: Sales@eSecuTech.com

Version	Date
1.0	2011.7.25
1.1	2012.4.4

CE Attestation of Conformity



UniOTP is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. UniOTP satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment.

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Conformity to ISO 9001:2000



The Quality System of SecuTech Solution Inc., including its implementation, meets the requirements of the standard ISO 9001:2000

ROHS



All UniOTP products are environmental friendly with ROHS certificates.

Table of Contents

ABOUT THIS GUIDE	1
CHAPTER 1: PAM AUTHENTICATION AGENT INSTALLATION AND CONFIGURATION	2
1.1 Extracting files for Installation.....	2
1.2 Install PAM Authentication Agent	3
1.3 Check the PAM Agent Installation	4
CHAPTER 2: CONTROL FLAG KEYWORDS.....	5
CHAPTER 3: PAM AGENT CONFIGURATION.....	6
3.1 Configure the secu_pam_agent.conf file	6
3.2 Configure the PAM Authentication Agent	7
3.3 Configure Desktop login authentication	8
3.4 Configure remote terminal login authentication.....	9
CHAPTER 4: TESTING PAM AUTHENTICATION AGENT	10
4.1 Testing Command line authentication	10
4.2 Testing Desktop login authentication	11
4.3 Testing remote login authentication.....	12

About this guide

This User guide includes introduction of UniOTP PAM Authentication Agent installation and configuration in the Red Hat Enterprise Linux 5 operating system, and using the UniOTP authentication system to protect login authentication.

Chapter 1: PAM Authentication Agent installation and configuration

1.1 Extracting files for Installation

Please navigate to the directory where you saved your setup package (pam_secu.tar.gz). For example, in our system, the setup package is stored in /tmp/Desktop. Use the cd command to switch to that folder, and the tar command to extract the setup package, as the following picture shows:

```
[root@localhost tmp]# cd Desktop
[root@localhost Desktop]# ls
pam_secu.tar.gz
[root@localhost Desktop]# tar zxvf pam_secu.tar.gz
```

You will see the following information, after the package has been extracted. All extracted files will be stored in the same directory as the pam_secure.tar.gz.

```
[root@localhost Desktop]# tar zxvf pam_secu.tar.gz
./libc.so.6
./libstdc++.so.5
./libuniotp_agent_c.so
./pam_secu.so
./secu_pam_agent.conf
./install
[root@localhost Desktop]# _
```

1.2 Install PAM Authentication Agent

To install the PAM Agent, you must login as root and then input “./install” to start installing the PAM Agent.

```
[root@localhost Desktop]# ./install
```

The following information will be displayed.

```
Welcome to use UniOTP PAM Agent
Checking dependent libraries...
Checking libstdc++.so.5...
Library libstdc++.so.5 [Ok]
Checking libc.so.6...
Library libc.so.6 [Ok]
Install libuniotp_agent_c.so ...
Install sample configuration file ...
pam_secu.so has been installed in /lib/security/
Change configuration file now?[y/n]
```

After installation, the system will ask you “Change configuration file now? [y/n]”. If you want to change the configuration file now, input y and press enter, otherwise, input n and press enter. For this example, please input n and press enter, configuration shall be described later in this document. The following information will be displayed:

```
n
UniOTP PAM Agent installation has been finished.
Configuration file(secu_pam_agent.conf) for UniOTP PAM Agent
is installed /etc/
Before you restart your computer after you configure an
application to use UniOTP One-Time-Password to do authentication,
you should confirm you have configure the
configuration file(/etc/secu_pam_agent.conf) correctly!
```

Please make sure the configuration file has been configured correctly, before restarting your computer, otherwise it may cause login failure next time.

1.3 Check the PAM Agent Installation

You can check if the PAM agent has been installed successfully, by the following the method below.

Please navigate to `/lib/security` to check the `pam_secu.so` file.

```
[root@localhost security]# ls /lib/security
pam_access.so      pam_keyinit.so    pam_permit.so      pam_tally2.so
pam_ccreds.so      pam_krb5           pam_pkcs11.so      pam_tally.so
pam_chroot.so      pam_krb5afs.so    pam_postgresok.so  pam_time.so
pam_console.so     pam_krb5.so       pam_pwhistory.so   pam_timestamp.so
pam_cracklib.so    pam_lastlog.so    pam_rhosts_auth.so pam_tty_audit.so
pam_debug.so       pam_ldap.so       pam_rhosts.so      pam_umask.so
pam_deny.so        pam_limits.so     pam_rootok.so      pam_unix_acct.so
pam_echo.so        pam_listfile.so   pam_rps.so         pam_unix_auth.so
pam_env.so         pam_localuser.so  pam_securetty.so   pam_unix_passwd.so
pam_exec.so        pam_loginuid.so   pam_secu.so        pam_unix_session.so
pam_faildelay.so   pam_mail.so       pam_selinux.so     pam_unix.so
pam_filter         pam_mkhomeDir.so  pam_shells.so      pam_userdb.so
pam_filter.so      pam_motd.so       pam_smb_auth.so    pam_warn.so
pam_ftp.so         pam_namespace.so  pam_stack.so       pam_wheel.so
pam_group.so       pam_nologin.so    pam_stress.so      pam_xauth.so
pam_issue.so       pam_passwdqc.so   pam_succeed_if.so
[root@localhost security]#
```

Go to `/usr/lib` to check the `libuniotp_agent_c.so` file.

```
libtiff.so.3
libtiff.so.3.8.2
libtiffxx.so.3
libtiffxx.so.3.8.2
libtk8.4.so
libuniotp_agent_c.so
```

Go to `/etc` to check the `secu_pam_agent.conf` file

```
[root@localhost etc]# ls /etc/secu_pam_agent.conf
/etc/secu_pam_agent.conf
```

If all these files can be found in the corresponding directory, the PAM Agent has been installed successfully, and the next step is to configure the PAM Agent.

Chapter 2: Control flag keywords

There are four control-flag keywords: required, requisite, sufficient, optional and include.

Required: This indicates that the success of the module is required for the module-type facility to succeed. Failure of this module will not be apparent to the user until all of the remaining modules (of the same module-type) have been executed.

Requisite: Similar to required, however, in the case that such a module returns a failure, control is directly returned to the application. The return value is associated with the first required or requisite module to fail.

Note: this flag can be used to protect against the possibility of a user getting the opportunity to enter a password over an unsafe medium. It is conceivable that such behaviour might inform an attacker of valid accounts on a system. This possibility should be weighed against the concerns of exposing a sensitive password in a hostile environment.

Sufficient: The success of this module is deemed 'sufficient' to satisfy the Linux-PAM library that this module-type has succeeded in its purpose. In the event that no previous required module has failed, no more 'stacked' modules of this type are invoked. (Note, in this case subsequent required modules are not invoked.). A failure of this module is not deemed as fatal to satisfying the application that this module-type has succeeded.

Optional: This control-flag marks the module as not being critical to the success or failure of the user's application for service. In general, Linux-PAM ignores such a module when determining if the module stack will succeed or fail. However, in the absence of any definite successes or failures of previous or subsequent stacked modules this module will determine the nature of the response to the application. One example of this case is when the other modules return something like PAM_IGNORE.

Include: This tells PAM to include all lines of given type from the configuration file specified as an argument to this control. The idea is to create few "systemwide" pam configs and include parts of them in application pam configs.

pam_secu.so supports debug functions. If you input debug following pam_secu.so the debug information will be added to the system log file (eg. auth sufficient pam_secu.so debug). You can specify the configuration file by using conf -directory (eg. auth sufficient pam_secu.so conf -/etc/secu_pam_agent.conf. The agent will find the configuration file from the specified directory, instead of the default).

Chapter 3: PAM Agent Configuration

3.1 Configure the secu_pam_agent.conf file

This file contains settings about system account, mapping of dynamic password names for system accounts, authentication server IP address shared keys and authentication server port. For more details, please read the introduction in the secu_pam_agent.conf file.

```
[root@localhost etc]# vi secu_pam_agent.conf
```

The following file will be opened. Add a system user and other corresponding parameters as following picture:

```
[root]
uniotp_account=newtest
authserver=192.168.1.225
share=hello
port=1812
maxwait=3
```

[User name]: a valid system account name (example: [root])

- **uniotp_account:** Map an account name of dynamic password to user name
- **authserver:** Authentication server IP address
- **share:** Shared secret key from the authentication service administrator
- **port:** Authentication servers connecting port
- **maxwait:** The maximum time waiting for authentication server response

3.2 Configure the PAM Authentication Agent

The PAM authentication agent configuration is adding the OTP Server PAM authentication agent program to the authentication module service, which is in /etc/pam.d.

```
[root@localhost pam.d]# cd /etc/pam.d
```

3.2.1 Configure command line login authentication

Open the login file in directory “/etc/pam.d”, and add “auth required pam_secu.so” to the row:

```
[root@localhost pam.d]# vi /etc/pam.d/login
```

```
#%PAM-1.0
auth      required      /lib/security/pam_secu.so
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth      include       system-auth
account   required      pam_nologin.so
account   include       system-auth
password  include       system-auth
```

Save and quit, you have now finished all PAM agent configurations for command line login authentication.

3.3 Configure Desktop login authentication

Open the PAM configuration file for gdm in directory “/etc/pam.d”, and add “auth required pam_secu.so” in the first row.

```
[root@localhost ~]# vi /etc/pam.d/gdm_  
  
#%PAM-1.0  
auth      sufficient      pam_secu.so  
auth      required        pam_env.so  
auth      include          system-auth
```

Please save and quit. You have now finished all PAM agent configurations for desktop login authentication.

Please make sure the configuration file has been configured correctly, before restarting your computer, otherwise it may cause login failure next time.

3.4 Configure remote terminal login authentication

Open the sshd file in directory /etc/pam.d and add “auth sufficient pam_secu.so sshd” in the row:

```
[root@localhost pam.d]# vi sshd
```

```
#%PAM-1.0
auth      sufficient    pam_secu.so    _sshd
auth      include       system-auth
account   required      pam_nologin.so
account   include       system-auth
password  include       system-auth
session   optional      pam_keyinit.so force revoke
session   include       system-auth
session   required      pam_loginuid.so
```

For remote login authentication configuration, you can only use sufficient.

Please save and quit, you have now finished all PAM agent configurations for remote terminal login authentication.

Chapter 4: Testing PAM Authentication Agent

4.1 Testing Command line authentication

Input user name [root] and press enter. The system will ask for OTP[PIN]. Input the dynamic password generated by your OTP device and your PIN following OTP in this line and press enter. In the next Password line, input your static password and press enter. You will login as root, if you see "[root@localhost ~]#".

```
Red Hat Enterprise Linux Server release 5.6 (Tikanga)
Kernel 2.6.18-238.el5 on an i686

localhost login: root
OTP[PIN]:
Password:
Last login: Thu Jul 14 00:38:50 on tty2
[root@localhost ~]# _
```

4.2 Testing Desktop login authentication

After configuring the gdm file, you can login to the system by using the GUI, please input the user name when the following login interface appear.



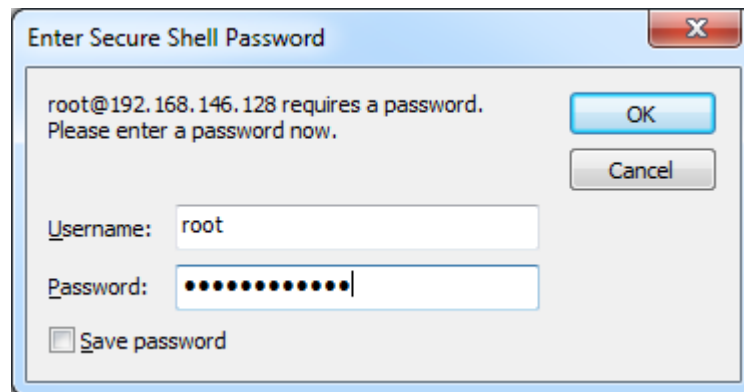
Input user name [root], and then the OTP password interface will appear.



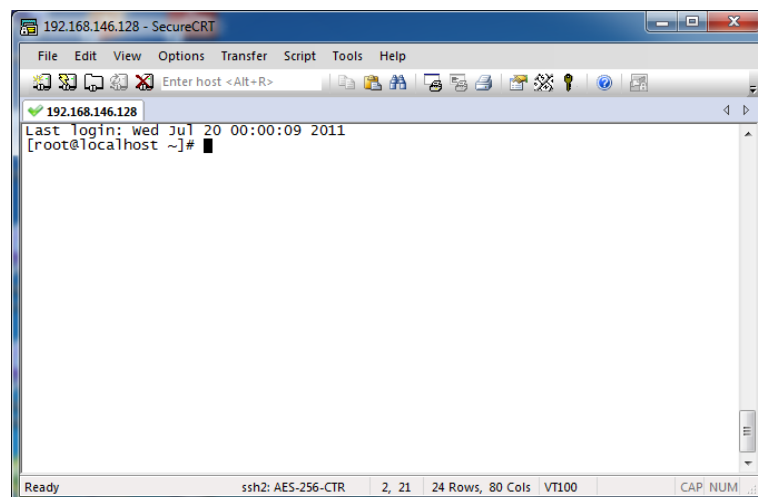
Please Input OTP and PIN, and then press enter. If you can login the system, you have successfully configured the PAM agent for desktop login authentication.

4.3 Testing remote login authentication

We use SecureCRT as the remote login tool. After UniOTP protection is enabled for remote login authentication. You must input OTP+PIN in password to login to the host computer, and click on OK.



Once login has been successful, the following picture is displayed:



Follow us!



[Twitter](#)



[Facebook](#)



[Youtube](#)



[Linked in](#)



About SecuTech

SecuTech Solution Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.



www.eSecuTech.com SecuTech Solution Inc.

North America

1250 Boulevard René-
Lévesque Ouest, #2200,
Montreal, QC, H3B 4W8,
Canada
T: +1 -888-259-5825
F: +1 -888-259-5825 ext.0
E: INFO@eSecuTech.com

China

Level 12, #67 Bei Si Huan
Xi Lu,
Beijing, China, 100080
T: +8610-8288 8834
F: + 8610-8288 8834
E: CN@eSecuTech.com

APAC

Suite 5.14, 32 Delhi Rd,
North Ryde,
NSW, 2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002
Lyon, France
T: +33-042-600-2810
F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com

©Copyright 2012 SecuTech Solution Inc. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech UniOTP and the SecuTech logo are trademarks of SecuTech Inc. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.