How obsolete is the trusted mode? - This thread has been closed

» IT Resource Center

» Login
» Register
» My profile

» Search knowledge base
» **Forums**
» Patch database
» Download drivers, software and firmware
» Warranty check
» Support Case Manager
» Software Update Manager
» Training and Education
» More maintenance and support options

» Online help
» Site map

Create a new message | Receive e-mail notification if a new reply is posted | Reply to this message

Author	Subject: How obsolete is the trusted mode? Add to my favorites This thread has been closed
Petr Wünsch	Oct 7, 2010 07:05:55 GMT

When HP-UX 11.31 had been released it was stated that trusted mode would be obsolete and that it would eventualy disapear from HP-UX. Trusted mode should be replaced with userdb, /etc/security.dsc, /etc/default/security and /etc/shadow. However, today I have installed a new HP-UX 11.31 September 2010 system and I realised I am not able to enforce password policies (eg. min password length) to root user without converting the system to trusted mode.

Does anybody know, what is the current status of trusted system? Or what are the best practices for configuring a "secure" system?

And in respect to that question, how can I enforce min. password length for root without converting to trusted mode?

A quote from 'man security':
MIN_PASSWORD_LENGTH

This attribute controls the minimum length of new passwords. On trusted systems it applies to all users. On standard systems it applies to non-root local users and to NIS users.

Member icons

HP moderator
Expert in this area

Member status

ITRC Pro *ITRC Pro* 250 points
ITRC Graduate *ITRC Graduate* 500 points
ITRC Wizard *ITRC Wizard* 1000 points
ITRC Royalty *ITRC Royalty* 2500 points
ITRC Pharaoh *ITRC Pharaoh* 7500 points
Olympian *Olympian* 20000 points
1-Star Olympian *1-Star Olympian* 40000 points

Note: If you are the author of this question and wish to assign points to any of the answers, please login first.For more information on assigning points ,click here

Sort Answers By: Date or Points

	Oct 7, 2010 07:59:54 GMT Unassigned
turgay cavdar This member has accumulated 1000 or more points	

Trusted mode had been disappeared on hp-ux 11.31. Not all the functionalities transferred to userdb. In /etc/security.dsc file you can see what you can do as per-user, system-wide, etc... For example we have a problem with disabling password aging for specific users, it was possible in 11.23 but not possible for 11.31.

@@more /etc/security.dsc
#Revision=@(#)B.11.31_LR 1
##
#
Do not edit this file.
#
##

2-Star Olympian *2-Star Olympian* 80000 points

» How to earn points

» Support forums FAQs

Question status

Magical answer Message with a response that solved the author's question

Favorites status

Add to my favorites

Delete from my favorites

This thread has been closed Thread closed

```
# Programs use this file to obtain information about the attributes
# defined in /etc/default/security and /var/adm/userdb.
# Each attribute is described by a line below; information includes:
# 1) name
# 2) min value
# 3) max value
# 4) value of the hardwired default used if no system-wide value is set
# 5) flags indicating how the attribute can be used:
# S : can configure a system-wide default in /etc/default/security
# u : can configure a per-user value in /var/adm/userdb
# s : can configure a per-user value in /etc/shadow if shadow mode
# p : can configure a per-user value in /etc/passwd if standard mode
# L : the attribute applies only to local users in /etc/passwd
# i : indicates an internal attribute in /var/adm/userdb that is
# normally modified only by programs that enforce system security
# 6) description message number in /usr/lib/nls/*/libsec.cat
# 7) description message; description of the attribute

ABORT_LOGIN_ON_MISSING_HOMEDIR;0;1;0;S;1;Abort login if no home directory? (0=No 1=Yes)
ALLOW_NULL_PASSWORD;0;1;1;LuS;2;Allow login with null password? (0=No 1=Yes)
AUDIT_FLAG;0;1;1;uS;3;Should a user account be audited? (0=No 1=Yes)
AUTH_MAXTRIES;0;999;0;uS;4;Number of consecutive authentication failures allowed (0=No limit)
BOOT_AUTH;0;1;0;LS;5;Is authentication required to boot the system into single user mode? (0=No 1=Yes)
BOOT_USERS;;;root;LS;6;Names of users who can boot the system into single user mode
DISPLAY_LAST_LOGIN;0;1;1;uS;7;Should the last login be displayed? (0=No 1=Yes)
INACTIVITY_MAXDAYS;0;999;0;LsS;8;Number of days of account inactivity allowed (0=No limit)
LOGIN_TIMES;;;Any;uS;9;List of days/times that a user can login to the system (see security(4)).
MIN_PASSWORD_LENGTH;3;8;6;LuS;10;Minimum length for new passwords
NOLOGIN;0;1;0;S;11;Can /etc/nologin be used to disable non-root logins? (0=No 1=Yes)
NUMBER_OF_LOGINS_ALLOWED;0;999;0;uS;12;Maximum number of simultaneous logins allowed (0=No limit)
PASSWORD_HISTORY_DEPTH;1;24;1;LuS;13;Number of passwords in password history
PASSWORD_MIN_LOWER_CASE_CHARS;0;7;0;LuS;14;Minimum number of lower case chars for new passwords
PASSWORD_MIN_UPPER_CASE_CHARS;0;7;0;LuS;15;Minimum number of upper case chars for new passwords
PASSWORD_MIN_DIGIT_CHARS;0;6;0;LuS;16;Minumum number of digits for new passwords
PASSWORD_MIN_SPECIAL_CHARS;0;6;0;LuS;17;Minimum number of special chars for new passwords
PASSWORD_MAXDAYS;-1;441;-1;LpsS;18;Maximum number of days that a password is valid (-1=Disable aging)
PASSWORD_MINDAYS;0;441;0;LpsS;19;Minimum number days to elapse before a password can be changed (0=No restriction)
PASSWORD_WARNDAYS;0;441;0;LsS;20;Number of days to warn before a password expires (0=No warning)
SU_DEFAULT_PATH;;;;S;21;Set the specified PATH when su to a non superuser account (null=Retain path)
SU_KEEP_ENV_VARS;;;;S;22;Force su to propagate specified unsafe environment variables (null=No propagation)
SU_ROOT_GROUP;;;;S;23;Name of the group allowed to su to root (null=No restrictions)
UMASK;0;0777;0;uS;24;Default umask (leading zero denotes octal value)
auth_failures;;;;i;100;Number of consecutive authentication failures
auth_forigin;;;;i;101;Origin (host or tty) of last authentication failure
auth_ftime;;;;i;102;Time of last authentication failure
login_origin;;;;i;103;Origin (host or tty) of last successful login
login_time;;;;i;104;Time of last successful login
pwhist;;;;i;105;Password history
```

Petr Wünsch — Oct 7, 2010 09:27:01 GMT — N/A: Question Author

---

Actually, you still can convert system to trusted. Either using tsconvert or smh. The option still exists. Trusted system did not disapear.

Anyway, did you try to disable password aging on a per user level by userdbset command?
userdbset -u <user> PASSWORD_MAXDAYS=-1

turgay cavdar This member has accumulated 1000 or more points

Oct 7, 2010 13:51:10 GMT Unassigned

userdbset -u user PASSWORD_MAXDAYS=-1 command doesn't work for me...

#userdbset -u user PASSWORD_MAXDAYS=-1
Unknown attribute : PASSWORD_MAXDAYS

Emil Velez Expert in this area This member has accumulated 2500 or more points

Oct 7, 2010 23:27:00 GMT Unassigned

I would open up a ticket.. It may be a patch issue but password aging is certainly supported in SMSE security.

The only real functionality that is not in SMSE security that trusted system has is the ability to edit files to set the per user policy and system generated passwords. Other than that I think all of the functionality is there.

turgay cavdar This member has accumulated 1000 or more points

Oct 8, 2010 07:10:07 GMT Unassigned

Yes i opened a case for this error (in may 2010), and HP support said they are aware of the problem and they are trying to fix this with a patch. But they didnt give any specific release date for this fix.

Doug Lamoureux Expert in this area

Oct 12, 2010 00:50:03 GMT 5 pts

There will be a patch to 11.31 available in early 2011 that allows you to apply password policies to the root user.

For now you'll need to use Trusted Mode to get that functionality.

Regarding
userdbset -u user -a PASSWORD_MAXDAYS=-1

not working, the PASSWORD_MAXDAYS setting for a specific user is not stored in the userdb. If you would like to set (disable) this setting for a user use:

/usr/bin/password -x -1 user

Not all security settings are settable in the userdb - To find out more about each setting take a look at the /etc/security.dsc file. Each entry has a set of flags (5th parameter of the line), these flags are described at the top of the file:

S : can configure a system-wide default in /etc/default/security
u : can configure a per-user value in /var/adm/userdb
s : can configure a per-user value in /etc/shadow if shadow mode
p : can configure a per-user value in /etc/passwd if standard mode
L : the attribute applies only to local users in /etc/passwd
i : indicates an internal attribute in /var/adm/userdb that is
normally modified only by programs that enforce system security

For example the MIN_PASSWORD_LENGTH setting has the flags LpsS

PASSWORD_MAXDAYS;-1;441;-1;LpsS;18;Maximum number of days that a password is valid (-1=Disable aging)

L - Local users
p - Set on a per-user basis with passwd
s - Settable in shadow mode
S - System wide default settable in /etc/default/security

Also from the security man page:

"PASSWORD_MAXDAYS
...
This attribute applies only to local users and does not apply to trusted systems. The passwd -x option can be used to override this
value for a specific user."

Cheers,
Doug

turgay cavdar This member has accumulated 1000 or more points

Oct 12, 2010 04:44:35 GMT 2 pts

Hi Doug,

>If you would like to set (disable) this >setting for a user use:
>/usr/bin/password -x -1 user

Actually "passwd -x -1 user" command is working but this doesn't disable the password aging. When the user uses "passwd" command to set it's password then the users aging parameter is set to "PASSWORD_MAXDAYS" (in /etc/default/security file) again.

TL/SVROPS

May 11, 2011 02:52:15 GMT 3 pts

Regarding the statement:
There will be a patch to 11.31 available in early 2011 that allows you to apply password policies to the root user.

Patches **PHCO_40838** and PHCO_40839 are now available and make it possible to apply all the Shadow mode login and password restrictions imposed on normal users to the root user account.

Petr Wünsch

May 11, 2011 06:34:23 GMT **Thread closed by author**

Let us hope those patches realy fix the issue. I am planning to test it some time later.

Thanks for all your replies.

Create a new message Receive e-mail notification if a new reply is posted
Reply to this message

Printable version