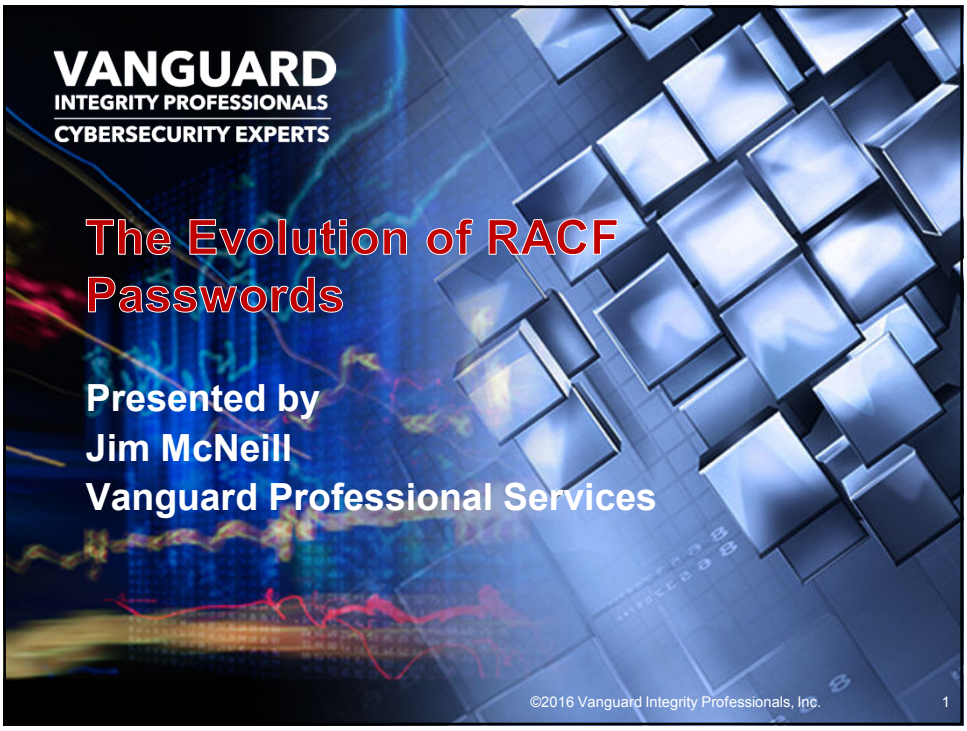


Legal Notice

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Copyright

Trademarks

The following are trademarks of Vanguard Integrity Professionals – Nevada:

- Vanguard Administrator
- Vanguard Advisor
- Vanguard Analyzer
- Vanguard SecurityCenter
- Vanguard SecurityCenter for DB2
- Vanguard Offline
- Vanguard Cleanup
- Vanguard PasswordReset
- Vanguard Authenticator
- Vanguard inCompliance
- Vanguard IAM
- Vanguard GRC
- Vanguard QuickGen
- Vanguard Active Alerts
- Vanguard Configuration Manager
- Vanguard Configuration Manager Enterprise Edition
- Vanguard Policy Manager
- Vanguard Enforcer
- Vanguard ez/Token
- Vanguard Tokenless Authenticator
- Vanguard ez/PIV Card Authenticator
- Vanguard ez/Integrator
- Vanguard ez/SignOn
- Vanguard ez/Password Synchronization
- Vanguard Security Solutions
- Vanguard Security & Compliance
- Vanguard zSecurity University

Made in the USA

2

Trademarks

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- The following are trademarks or registered trademarks of the International Business Machines Corporation:

CICS	IMS	S/390	z9
CICSPlex	MQSeries	System z	z10
DB2	MVS	System z9	z13
eServer	NetView	System z10	z/Architecture
IBM	OS/390	System/390	z/OS
IBM z	Parallel Sysplex	VTAM	z/VM
IBM z Systems	RACF	WebSphere	zEnterprise
IBM z13	RMF	z Systems	

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
- Other company, product, and service names may be trademarks or service marks of others.

Made in the USA

Topics

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Legacy Password Support
- APARs: OA43998 / OA43999
  - Default Password/Protected
  - Standalone Expired
  - Special Characters
  - Password Phrase ONLY
  - KDFAES Encryption
  - PWCLEAN
  - PWCONVERT

Made in the USA

Legacy Password Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Password Expiration Interval
- Password Expiration Warning
- Password Change History
- Password Minimum Change Interval
- Password Syntax Rules
- Unsuccessful Logon Attempts
- Mixed Case
- ADDUSER Sets LAST RACINIT Date
- Password Phrase Support

Made in the USA

Password Expiration Interval

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
SETR LIST
     :
PASSWORD PROCESSING OPTIONS:
 PASSWORD CHANGE INTERVAL IS  30 DAYS
     :
```

Made in the USA

Password Expiration Warning

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS   30 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS 1
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT
   10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER  5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS      5 DAYS.
```

Made in the USA

Password Change History

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS


```
      :
PASSWORD PROCESSING OPTIONS:

  PASSWORD CHANGE INTERVAL IS   30 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS 1
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT
   10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
      :
      :
      :
```

Made in the USA

Password Minimum Change Interval

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
SETR LIST
    :
PASSWORD PROCESSING OPTIONS:
 PASSWORD MINIMUM CHANGE INTERVAL IS 1
    :
```


Password Syntax Rules

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(6:8)   LLLLLLLL
    RULE 2  LENGTH(6:8)   mmmmmmmm
    RULE 3  LENGTH(6:8)   xxxxxxxx
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-SPECIAL
    x-MIXED ALL
```

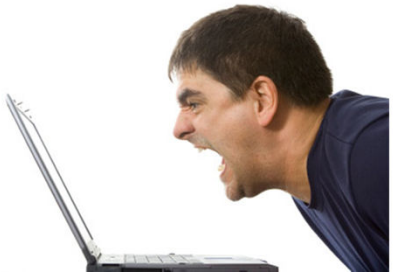
New keywords in z/OS 2.2: MIXEDALL(x), SPECIAL(s)

Unsuccessful Logon Attempts

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
SETR LIST
    :
    :
PASSWORD PROCESSING OPTIONS:

  AFTER  3  CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
```



Made in the USA

Mixed Case

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

New in z/OS 1.7

0123456789 #$@

ABCDEFGHIJKLMN
OPQRSTUVWXYZ
abcdefghijklmnop
qrstuvwxyz

```
SETR LIST
    :
    :
PASSWORD PROCESSING OPTIONS:
 MIXED CASE PASSWORD SUPPORT IS IN EFFECT
    :
    :
```

Made in the USA

ADDUSER Sets LAST RACINIT Date

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

New in z/OS 1.7

- Old way
  - Last RACINIT date set to zeros
  - ID would not be revoked due to inactivity for first logon
- New way
  - Last RACINIT date set to current date
  - ID revoked on first logon if not used within Inactive interval

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

New in z/OS 1.8

Enhanced in z/OS 1.9

Exploited in z/OS 1.10

ADDUSER | AU (userid ...)
PHRASE ('passphrase')

ALTUSER | ALU (userid ...)
PHRASE ('passphrase')

PASSWORD | PW | **PHRASE**
PHRASE('current-passphrase' 'new-passphrase')

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- z/OS 1.8
  - Maximum length: 100 characters
  - Minimum length: 14
  - The password rules specified by the SETROPTS command **do not** apply to password phrases.
  - Use exit ICHPWX11 for additional phrase syntax checking. IBM provides a sample ICHPWX11 exit written in REXX.
  - Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
  - Must contain at least 2 alphabetic characters (A - Z, a - z)
  - Must contain at least 2 non-alphabetic characters (numeric, punctuation, or special character)
  - Must not contain more than 2 consecutive characters that are identical
  - If a single quotation mark is intended to be part of the password phrase, you must use two single quotation marks together for each single quotation mark.

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- z/OS 1.9
  - Maximum length: 100 characters
  - Minimum length: 9 characters when ICHPWX11 is present and allows it
  - The password rules specified by the SETROPTS command **do not** apply to password phrases.
  - Use exit ICHPWX11 for additional phrase syntax checking. IBM provides a sample ICHPWX11 exit written in REXX.
  - Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
  - Must contain at least 2 alphabetic characters (A - Z, a - z)
  - Must contain at least 2 non-alphabetic characters (numeric, punctuation, or special character)
  - Must not contain more than 2 consecutive characters that are identical
  - If a single quotation mark is intended to be part of the password phrase, you must use two single quotation marks together for each single quotation mark.

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- z/OS 1.10
  - Password Phrases are exploited by z/OS 1.10. For example, TSO/E and UNIX System Services will support password phrases.
  - CICS, IMS, NETVIEW, CA7, Session Managers and other IBM and OEM products must be at a level that supports Password Phrases
  - TSO
    - LOGON PASSPHRASE(ON) must be added to IKJTSO00
  - CICS SIT parameter
    - GMTRAN=CESL, (Password Phrase transaction) or
    - GMTRAN=CESN, (Password only transaction)

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
------------------------------ TSO/E LOGON ------------------------------------

   Enter LOGON parameters below:                RACF LOGON parameters:

   Userid    ===> JIMM

   Password  ===>

   Procedure ===> VSS22                         Group Ident  ===>

   Acct Nmbr ===> 2345

   Size      ===> 128000

   Perform   ===>

   Command   ===> ISPF NOLOGO

   Enter an 'S' before each option desired below:
    -New Password    -Nomail    -Nonotice  S -Reconnect    -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

Enter "S" here to request new password or phrase

Password Phrase Support (CESN)

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
                        Signon to CICS                  APPLID CICSTS51

SERVICE1 System CICS Region



Type your userid and password, then press ENTER:

         Userid . . . . ________    Groupid . . . ________
         Password . . .
         Language . . . ___

     New Password . . .

DFHCE3540 Ensure that passwords are entered in the correct case.




DFHCE3520 Please type your userid.
F3=Exit
```


Password Phrase Support (CESL)

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

```
                        Signon to CICS                  APPLID CICSTS51

SERVICE1 System CICS Region



Type your userid and password, then press ENTER:

         Userid . . . . ________    Groupid . . . ________
         Password . . .

         Language . . . ___

     New Password . . .

DFHCE3540 Ensure that passwords are entered in the correct case.




DFHCE3520 Please type your userid.
F3=Exit
```

Password Phrase Support

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

ADDUSER (AU) *user-id*
PASSWORD(*password*) | NOPASSWORD
PHRASE('passphrase') | NOPHRASE

ALU RJSMITH PHRASE('This is #1 Phrase')

Using IRR. FACILITY Class Profiles

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Authorize LISTUSER functions through FACILITY class profiles:

- **IRR.LU.OWNER.*owner***
  Allows listing of user profiles based on the owner of the user profiles
- **IRR.LU.TREE.*owner***
  Allows listing of user profiles that are within the scope of a selected group tree
- **IRR.LU.EXCLUDE.*user-ID***
  Exclude selected user profiles from the scope

Using IRR. FACILITY Class Profiles

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Authorize password reset functions through FACILITY class profiles:

- **IRR.PWRESET.OWNER.*owner***
  Allows resetting of user password and password phrases based on the owner of the user profiles
- **IRR.PWRESET.TREE.*owner***
  Allows resetting of password and password phrases for users that are within the scope of a selected group tree
- **IRR.PWRESET.EXCLUDE.*user-ID***
  Exclude selected user profiles from the scope

  Cannot be used to give a Password or Password Phrase to a PROTECTED user

Non-Expiring or Not Expired

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Non-Expiring Password
  - The password will NEVER have to be changed
  - Use the RACF PASSWORD command
    PASSWORD USER(FTPSEC) NOINTERVAL

- Not Expired Password
  - The password does not have to be changed at the NEXT system entry
  - Use the RACF ALTUSER command
    ALU FTPSEC PASSWORD(SNOOK) NOEXPIRED

APARs: OA43998 / OA43999

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Then the BIG change
- For z/OS 1.12, 1.13 and 2.1.
- Included in z/OS 2.2

Default Password/Protected

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Prior to z/OS 2.2 (without the APARS)
  - ADDUSER FRED DFLTGRP(PAYROLL)
  - Fred's password defaulted to PAYROLL
- z/OS 2.2 and above
  - ADDUSER FRED DFLTGRP(PAYROLL)
  - FRED is PROTECTED
  - ADDUSER FRED DFLTGRP(PAYROLL) PASSWORD
    - You will be prompted for a new password
    - If in NOPROMPT mode, the command will fail

Made in the USA

Standalone EXPIRED

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- ALU BOB EXPIRED
  - Does not affect current Password
  - Bob must change his password at next logon

Additional Special Characters

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

. < + | & ! * - % _ > ? : =

```
SETR LIST
    :
PASSWORD PROCESSING OPTIONS:
 SPECIAL CHARACTERS ARE ALLOWED.
```

Made in the USA

Additional Special Characters

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- IBM APAR II14765 is MUST reading
  - IMS (e.g., commands, VTAM logon, etc) provides full special characters support with APAR PI48111.
  - Tivoli NetView for z/OS does not accept the period '.' character or the equal sign '=' character in passwords
  - TSO/E will not accept a password that begins with a question mark '?' character.
  - z/OS CommServer users should avoid using the colon ':' character in passwords passed to the z/OS FTP server.
  - BDT at release HBD6602 shipped support in PTF UA77241
  - CICS 5.1 initial support came in APAR PI21866. They have two fixes on top of that: PI33454, PI39336 .
- This is NOT an exhaustive list.

Password Phrase Only

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Prior to z/OS 2.2
  - If you gave a user a Password Phrase they could still logon with their password
- z/OS 2.2 and above
  - ALU BOB Phrase('my new long password') NOPASS will disallow Bob from using his old password
  - ALU BOB NOPASS
    - Assumes Bob already had a Password Phrase else makes BOB a PROTECTED user

Made in the USA

KDFAES Encryption

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- A few BIG CAVEATS:
- All of the following assumes your passwords are DES encrypted (not Masking or Installation Defined)
- You should already have an ICHDEX01 RACF exit that specifies DES only.
  - "Masking is weak and should never be used. The use of masking, even as a secondary check to DES when the password does not match, introduces a serious vulnerability in your system." IBM recommendation.
- With KDFAES active ICHDEX01 is not required and Password Phrases can be 9-100 characters long.
- Extra space in RACF database
- Extra cycles encrypting new passwords and comparing new password to history

KDFAES Encryption

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- To enable:
  - SETROPTS PASSWORD(ALGORITHM(KDFAES))
    - The RACF panels do NOT support enabling KDFAES
  - Existing DES Passwords will continue to evaluate
  - Existing DES Password Phrases will continue to evaluate
  - When a Password or Password Phrase is changed, it will be stored as the current Password or Password Phrase in the new KDFAES format.
  - Users' existing history entries will remain in legacy format but new entries will be in KDFAES format

KDFAES Encryption

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- To disable:
  - SETROPTS PASSWORD(NOALGORITHM)
    - The RACF panels do NOT support disabling KDFAES
  - Existing KDFAES Passwords will continue to evaluate
  - Existing KDFAES Password Phrases will continue to evaluate
  - When a Password or Password Phrase is changed, it will be stored as the current Password or Password Phrase in the DES format.
  - Users' existing history entries will remain in KDFAES format but new entries will be in DES format

PWCLEAN

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Performs the following functions:
  - Removes residual password and password phrase history entries resulting from lowering the SETROPTS PASSWORD(HISTORY(*n*)) value.
  - Removes any password history and password phrase history from a PROTECTED user.
- ALU FRED PWCLEAN

PWCONVERT

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Performs the PWCLEAN function and
  - If KDFAES is active:
    - If the current password is in legacy format, converts it to KDFAES format.
    - Converts any legacy-format password history entries to KDFAES.
  - If KDFAES is not active:
    - Deletes any password and password phrase history entries that are in KDFAES format.
- PWCONVERT does nothing with the current password phrase. After KDFAES is enabled, the phrase must be changed before it is encrypted with the new algorithm.
- PWCONVERT does nothing with phrase history entries. They remain in their legacy form until they are replaced in the history.
- ALU FRED PWCONVERT

Recommendations

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Implement KDFAES encryption as soon as possible
- Consider upper/lower case
- Consider Password Phrases
- Questions, comments?