Only YOU can know and respond with certainty…

ICE/PSWD is based on this simple premise:

The only person who ACTUALLY knows what you're doing at any point in time is YOU!

Therefore, it should be considered true that system integrity is enriched by the inclusion of the end user within the overall system security paradigm.

Getting Started with ICE/PSWD Notification & Enforcement Applications

Available in ICE 18.0

Contact us for additional information:

NewEra Software Technical Support

800-421-5035 or 408-520-7100
Or text support requests to 669-888-5061

support@newera.com

www.newera.com

Rev: 2023-9-18

1 Table of Contents:

2 Overview of ICE/PSWD System Operations:

The objective of ICE/PSWD is to enrich the functions of the IBM Security Server RACF (RACF), the dominant security subsystem serving the z/OS community. This effort is intended to expand/extend z/OS security in five specific ways with the goal of including the actual end user in the overall security paradigm. The result will be an opportunity for end users to step up, front and center, and accept responsibility and accountability for the monitoring of usage and change to their System Logon Credential(s).

2.1 Passwords and Pass Phrases

ICE/PSWD supports the use of both passwords and pass phrases. In this document the use of password is intended to mean both.

2.2 RACF Specific Enrichment Functions

The RACF Exits, ICHPWX01 and ICHRIX02, and the proprietary EXIT extensions will be employed to implement the features and functions described herein. While this functional enrichment can be applied broadly to all system users, the primary use model is best directed toward users or processes whose credentials are considered HIGHLY authorized.

2.2.1 Logon Notification

Only the end user knows for certain if they are actually logging on to the system. Therefore, it makes sense to validate this action with the user. ICE/PSWD intercepts the logon event, at the point of RACF credential validation, and reports successful or failed attempts to the user via email or SMS. This notification process extends the security paradigm out to the users, affording them the opportunity to report (immediately) suspicious (it's not me) activity against their logon credentials to the Security Staff for action.

Without such notification, users with proper credentials are at the mercy of the "hacker" whose actions might not be discovered until some future time, in a post-action review, but are, nonetheless, attributed to the credential owner. An example is an FTP session logon that results in the uploading of a program that will be used later to ransom mainframe data.

2.2.2 Password Change Notification

To prevent co-option/corruption of a logon credential, it is best to think like a hacker (the person who stole the credential). Using a valid logon credential, the hacker can logon to TSO, CICS, FTP, a VTAM application, etc. ICE/PSWD can report such a logon to the end user. But people are busy; and in this case, time is of the essence as the first thing the hacker is likely to do is change the password. Generally, this is easy to do as part of the logon sequence. In such a case, notification could be sent to both the user and the Security staff, directly.

Without such notification of the password change, the rightful owner would likely be locked out of the system and unable to logon. There would be no knowledge of the value used to reset the password. Whatever mischief the hacker was up to will be attributed to the person whose UserId was hacked. In this case, the program that found its way onto the system via FTP, as discussed earlier, may be in an APF library and may already be sending ransom notes, and the placement of that module attributed to the person assigned the compromised UserId.

2.2.3 Pending Password Expiration Notification

There are many ways to strengthen a logon credential. One such way is through frequent password Resets/Updates. Resetting a user's password frequently will tend to make it more difficult for a hacker in possession of a co-opted credential to make use of it. While RACF does provide logon notification of pending expiration when accessing the system via TSO, it does not do so under FTP, VTAM, CICS, or other VTAM applications, and the notice provided under TSO is often overlooked and dismissed with the press of the enter key.

ICE/PSWD provides a method of offering asynchronous password expiry notification to end users that is not dependent on the RACF SETROPTS setting, PASSWORD_EXPIRATION_WARNING, or the user logging on to TSO. This method can apply to individual users, to a group of RACF users, or to the user community as a whole. Such a well-planned set of notifications would provide the user community time to plan for and formulate meaningful passwords and apply them prior to expiration.

2.2.4 Password Syntax Format Rule to UserId Binding

The IBM RACF Security Server provides for eight syntax format rules. While these rules will typically vary considerably in complexity, it is nonetheless up to the individual end user, during a password reset, to determine which rule they might use and match it during the reset process.

Some users might select the most complex rule available, but some would say that it's human nature to select the simplest rule, perhaps for productivity sake (complex formats take thought and therefore time to develop) or more likely, because a less complex password value is just easier to remember. Many users will not even know that there is more than one rule, and no matter how many rules are defined, they are likely to repeat the pattern of the rule that they know best.

These concerns notwithstanding, binding a user to two or more complex password formats options can lead to a stronger logon credential.

To accomplish this binding, ICE/PSWD can pair individual users, RACF and TCE groups of users, or the community as a whole, to one or more SETROPTS defined syntax format rules (These pairings can be uniquely defined). The result is that, if they exist at all, the simplest SETROPTS rules are no longer available for selection or usable to the defined users, groups, or general user community.

2.2.5 Password Reset Using a One-Time Password (OTP)

Multi-Factor Authentication (MFA) is generally used to ensure that those individuals who are logging onto a system are in possession of additional materials - a secret code or a physical object that can, in addition to an otherwise valid logon credential, be used to authentic a user's rights to logon.

While ICE/PSWD has many of the attributes of MFA, it differs as follows: ICE/PSWD exploits the use of One-Time Passwords (OTP) and becomes operational only at the intercept of an attempted password reset. MFA on the other hand is active for all logons, BUT not at all active at the password reset intercept point. In addition, the MFA secret or object is known to the user and, thus, may be stolen or misappropriated. The OTP Token used by ICE/PSWD is unknown to the user, is generated by the system, and transmitted to the user, via email of SMS, at the time of password reset. During this initial password reset attempt, the user's old password is *not* reset.

Although similar to MFA, OTP is different in that it requires the user to return to the "token issuing system" with all three credential elements: the userID, the OTP value, and the old password as specified in the initial password reset attempt. The user would then attempt a logon as needed for a password reset, all within a time limit (Time Window), by entering their userID, the old password, and the OTP value as the new password.

During the re-logon attempt, if the user enters the correct supplied OTP value in the new password field and confirms it, the new password value, as chosen for the initial reset request, will become the user's new password. These actions must occur within the specified time window.

If the user does not return within the time window, they start over again. If the user forgets the OTP Token, or enters it incorrectly, they start over again. If the user returns to a system (an ICE resident system) other than the "Token Issuing System", they start over again.

If the ICE primary address space IFOM is down when they return, they may encounter an unexpected outcome (education would overcome this). The user would have to begin the reset process anew, re-entering the new password in both the new and the confirm password fields. This is necessary as the token and password information stored in the IFOM Address Space is no longer available.

2.3 No RACF Changes Required, No RACF Controls Bypassed

None of the enrichment functions described herein require, in any way, changes to current RACF User Profiles or RACF SETROPTS Setting; nor do any of the described enrichment functions in any way bypass any RACF controls.

2.4 In the Event of an Unlikely System Failure

In the unlikely event of an ICE malfunction, the operational "Fall Back" is always to native RACF processes. Should such a failure occur, report it to NewEra Technical Support, support@newera.com, for immediate problem resolution.

3 The ICE/PSWD Administrators Primary Menu

Like any External Security Manager (ESM), ICE/PSWD could become difficult to administer for a large user population without the aid of a Configuration Manager. The Administrator's Primary Menu serves this function.

To reach the Primary Menu, an ICE/Administrator, as defined during system initialization, would first logon to the ICE Primary Menu which is supported as a VTAM Application (VTAM APPL). On the Primary Menu Command Line, they would enter the following and press enter.

```
TSO #PSWD ADMIN
```

Depending on the options selected during initialization, this may or may not display an Application Access control panel similar with the one shown below.

```
◊──────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - ICE/PSWD Admin Interface                 ◊
◊                                  ---AppToken--- -                  ◊
◊                   Enter Password >               +                 ◊
◊                  Next Select > .. Yes > Then Press Enter            ◊
◊──────────────────────────────────────────────────────────────────────◊
```

If the control panel does appear, it indicates that during initialization the ICE Administrator created and assigned an Application Token to ICE/PSWD functions. To move beyond this point, you will need to correctly enter that Token Value.

If the value is entered correctly, the ICE/PSWD Primary Menu – Enriching RACF Controls will appear. A sample is shown below.

```
       NSIMDSM 0110    ICE 18.0 - Enriching RACF Controls - ADCDPL

.. UserLogons  .. UserPswCng  .. PswdExpire  .. FormatRule  .. OTPControl
.. __________  .. __________  .. __________  .. __________  .. ___UserId

.. List All Accounts .. Search for Accounts ________ .. Events and Report

---------------z/OS Security Server RACF Password Controls-----------------
                .. Encryption Algorithm  Legacy KDFAES

------Control Settings------ SET SOP | ------Control Settings------ SET SOP
.. Password Change Interval  _45 _45 | .. Revoke Inactive UserId    _15 _15
.. Minimum Change Interval   __3 __3 | .. Mixed Case Supported      Yes Yes
.. Generations of Passwords  __5 __5 | .. Special Characters OK     Yes Yes
.. Failures Before Revoked   __4 __3 | .. Expiration Day Warning    _10 _10

----------------- Password Format Rules - Min:Max(Syntax) -----------------
RUL1 6:8(LLLLLLLL) RUL2 5:8(CcvV$NWA) RUL3 7:7(A*Vv$cs ) RUL4 -:-(--------)
SOP1 6:8(LLLLLLLL) SOP2 5:8(CcvV$NWA) SOP3 7:7(A*Vv$cs ) SOP4 -:-(--------)
RUL5 -:-(--------) RUL6 -:-(--------) RUL7 -:-(--------) RUL8 -:-(--------)
SOP5 -:-(--------) SOP6 -:-(--------) SOP7 -:-(--------) SOP8 -:-(--------)

.. SOP Update by PROBI1  Date 2021/01/08 Authority Just_the_way_it_works
```

The notation in the panel heading line, in this case NSIMDSM 0110, is a bit of information you will need when requesting Technical Support. It indicates the date of the build of the Version of ICE/PSWD that is currently executing and displaying the Primary Menu.

The upper part of the panel provides access to Service Accounts by ICE/PSWD Service Element - UserLogons, UserPswCng, PswdExpire, FormatRule, OTPControl - Selecting each with an 'S' will display a Worksheet that provides a summary of the Element Configuration of each individual user, group, or pseudo (sudo) user. Entering a UserId in the field below an Element Name and selecting it with an 'S', or just 'Clicking' it, will display the Element Configuration of the Id entered, if any.

The area immediately below supports listing of all Service Accounts, searching for a single user, displaying the related Full-Service Account, and a pathway to Event and Reports.

The middle part of the panel shows RACF Database Encryption Settings. Below that, under 'SET' Heading, it shows the current SETROPTS Setting of the eight primary RACF Password Controls, as compared to Standard Operation Practice values, shown under the 'SOP' Heading. SOP values may be updated any time by using the 'SOP Update' feature, shown at the bottom of the panel. To view an explanation of each of the nine settings, cursor into the name field and press enter. This will display a setting description similar to the one shown below, for Encryption.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Password Control Element                     ◊
◊        Element Name: PASSWORD_ENCRYPTION_ALGORITHM                      ◊
◊                                                                        ◊
◊  ----------------Configuration Element Description----------------     ◊
◊   The KDFAES (Key Derivation Function with AES) is only available       ◊
◊   when RACF password enhancements have been applied. The patches        ◊
◊   must be deployed and KDFAES activated otherwise LEGACY encryp-        ◊
◊   tion (DES) will be used. KDFAES is recommended unless RACF data       ◊
◊   base is shared with z/VM, which does not support KDFAES               ◊
◊   Use SETR Command Operands: PASSWORD(ALGORITHM(KDFAES))|NO....         ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Before each of the nine elements is a selection point. Entering an 'S' there and pressing enter will display the SETROPTS Dialog for the selected Element. A Sample for Minimum Change Interval is shown below:

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - RACF Configuration Element                   ◊
◊        Element Name: PASSWORD_MINIMUM_CHANGE_INTERVAL         +         ◊
◊                                                                        ◊
◊       --------------Update Element Configuration----------------       ◊
◊          > Current Setting is 0   > Change Setting to 3   <             ◊
◊             To Update Select > .. Yes > Then Press Enter               ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

'SET' and 'SOP' values are carried into the panel making it easy to update SETROPTS to a new Standard Operating Practice value. The sample below shows Password Minimum Change being updated to three days.

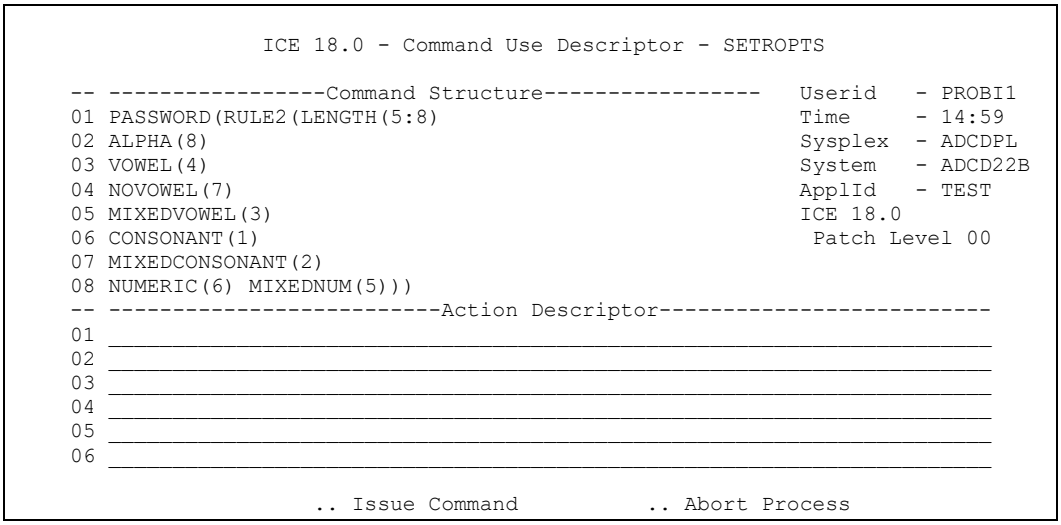
```
                ICE 18.0 - Command Use Descriptor - SETROPTS

-- ------------------Command Structure-----------------   Userid   - PROBI1
01 PASSWORD(MINCHANGE(3))                                Time     - 14:31
02                                                       Sysplex  - ADCDPL
03                                                       System   - ADCD22B
04                                                       ApplId   - TEST
05                                                       ICE 18.0
06                                                        Patch Level 00
-- --------------------------Action Descriptor--------------------------
01 ____________________________________________________________________
02 ____________________________________________________________________
03 ____________________________________________________________________
04 ____________________________________________________________________
05 ____________________________________________________________________
06 ____________________________________________________________________

                  .. Issue Command          .. Abort Process
```

All such updates require ESM and ICE/OPER authorization. They also require that an explanation be provided in the Action Descriptor section. This Descriptor, along with the actual command and system reply, are written as an historical event record to the TCE Control Journal, to be used for reporting and analysis.

The lower section of the panel shows the current SETROPTS settings of Password Format Rules and the Related SOP for each Rule Position 1 – 8. To decode a Rule, cursor under it and press enter. This Action will display an explanation of the rule as shown below for Rule Position Two - 5:8(CcvV$NWA).

```
◊──────────────────────────────────────────────────────────────────────◊
◊               ICE 18.0 - Password Format Rule Decoded                ◊
◊                                Rule: RULE2                           ◊
◊         ------------Password Format Configuration----------          ◊
◊          > Min and Max /  ..  ..  ..  ..  /.  ..  ..  /. <          ◊
◊          - --Content-- -  01  02  03  04  05  06  07  08 -          ◊
◊          > Alphabetic  A  ..  ..  ..  ..  ..  ..  ..  /. <          ◊
◊          > Alphnumeric L  ..  ..  ..  ..  ..  ..  ..  .. <          ◊
◊          > Vowel       V  ..  ..  ..  /.  ..  ..  ..  .. <          ◊
◊          > NoVowel     W  ..  ..  ..  ..  ..  ..  /.  .. <          ◊
◊          > MixedVowel  v  ..  ..  /.  ..  ..  ..  ..  .. <          ◊
◊          > Consonant   C  /.  ..  ..  ..  ..  ..  ..  .. <          ◊
◊          > MixConstant c  ..  /.  ..  ..  ..  ..  ..  .. <          ◊
◊          > Numeric     N  ..  ..  ..  ..  ..  /.  ..  .. <          ◊
◊          > MixNumeric  m  ..  ..  ..  ..  ..  ..  ..  .. <          ◊
◊          > National    $  ..  ..  ..  ..  /.  ..  ..  .. <          ◊
◊          > Special     s  ..  ..  ..  ..  ..  ..  ..  .. <          ◊
◊          > MixedAll    x  ..  ..  ..  ..  ..  ..  ..  .. <          ◊
◊          > Anything    *  ..  ..  ..  ..  ..  ..  ..  .. <          ◊
◊                                                                      ◊
◊             To Update Select > .. Yes > Then Press Enter             ◊
◊──────────────────────────────────────────────────────────────────────◊
```

The Rule can be updated by first changing (Checking '/.' or Unchecking '..') its composition, entering 'S' on the Select entry point, and pressing enter. This action will display the required command syntax in the Descriptor Window, as shown below:



All such updates require ESM and ICE/OPER authorization. They also require that an explanation be provided in the Action Descriptor section. That Descriptor along with the actual command and system reply are written as an historical event record to the TCE Control Journal, to be used for reporting and analysis.

3.1 ICE/PSWD Events & Reports – The Admin Setup & View

When you select "Events and Report" from the primary menu, the Events and Periodic Background Reporting Menu is presented.

```
          NSIMDSM 0110    ICE 18.0 - Enriching RACF Controls - ADCDPL

  .. UserLogons  .. UserPswCng  .. PswdExpire  .. FormatRule  .. OTPControl
  .. ___0 __518  .. ___0 ____0  .. ___0 ____0  .. ___0 ____0  .. ___0 ____0
  .. ManageCngs  .. CmmdUpdate  .. SubmitJobs  .. OtherEvent  .. EveryEvent
  .. ___0 ____7  .. ___0 ____3  .. ___0 ____0  .. ___0 ____0  .. ___0 __528

 ------------------ICE/PSWD Periodic Background Reporting-------------------

  ---------Admin Report Cycle-------- | ----------User Report Cycle--------
  /. Activate /. Summary /. CngOnly   |  /. Activate /. Summary /. CngOnly
                                      |
  /. Day - 00 00 - 12 Hour Interval   |  /. Day - 00 00 - 24 Hour Interval
        24hh mm   1|2|4|6|8|12|24     |        24hh mm   1|2|4|6|8|12|24
  /. Wks - 00 00 - MON_____________   |  /. Wks - 00 00 - SUN_____________
        24hh mm   SUN,MON,TUE,Etc.    |        24hh mm   SUN,MON,TUE,Etc.
  /. Mth - 00 00 - 1,2_____________   |  /. Mth - 00 00 - 1,2_____________
        24hh mm   Day:1,2,9,25,EOM    |        24hh mm   Day:1,2,9,25,EOM
  /. Pre PAT_____________________     |  /. Pre PRR_____________________
     Dom @COMPANY_____________________   |     Dom @COMPANY_____________________
     Email Admin Reports TO Address   |     Copy Users' Reports TO Address

                        .. Update Reporting Cycle
```

The upper portion of the panel is devoted to displaying events. By the numbers, it shows those that are new, since the last time the panel was updated, and the total number currently contained in the ICE Event Log. Cursor into the insertion point, preceding one of the ten Event Categories, enter an 'S', and press enter to View all Events within that Category. Cursor to the insertion point, immediately below, enter 'S', and press enter to View New Events. The number immediately to the right of this insertion point is the number of New Events. The number to its right is the number of Total Events.

A sample of the PSWD Event Activity Worksheet is shown below:

```
         ICE 18.0 - PSWD Event Activity Worksheet    Row 1 to 14 of 159
NSIMDSM:0110                                              --Event Records--
----------- Controls Environment - IFO.TEST - ADCDPL has 159 Events -----------
Row Selections: Browse_Event_Detail
To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help
- Rows --------Event Identity------- -------------------Summary----------------

_ ____ ________ _____ ________ _____ ________ _______PSWD Event Descriptions---
S Numb yy/mm/dd hh:mm -UserId- Event -Origin-
_ 0001 21/01/13 07.48     IFOS CMMDS ROUTE    ADCD22B,D PARMLIB
_ 0002 21/01/13 07.12     IFOS CMMDS ROUTE    ADCD22B,D PARMLIB
_ 0003 21/01/13 07.00   AROBI1 EDITS NSEENSSA IFO.TEST.PARMLIB/B2WRKD
_ 0004 21/01/13 06.37   AROBI1 LOGON STC07109 00 Password or phrase is authoriz
_ 0005 21/01/13 06.35   PHARL1 LOGON STC07109 00 Password or phrase is authoriz
_ 0006 21/01/13 06.33   AROBI1 LFAIL STC07109 04 Password or phrase is not_auth
_ 0007 21/01/13 06.30   ADMIN1 EDITS NSEENSSA IFO.TEST.PARMLIB/B2WRKD
_ 0008 21/01/13 06.28   ADMIN1 LOGON STC07109 00 Password or phrase is authoriz
```

The Events listed in this Worksheet are extracted from the ICE Event Log. The Log contains several different event types displaying them in this common format. In many cases, but not all, a Log Entry will have a corresponding Control Journal Entry. The Control Journal contains far more information than the Log and retains it for longer periods of time. Event retention in the Log is determined by the allocated size of the Log File during ICE initialization. The bigger the allocation, the bigger the file; and therefore, the greater the number of records. When the Log fills up, it 'Wraps Around'; writing over oldest events.

3.1.1 Worksheet Column Heading

- yy/mm/dd Date when the Event was recognized and recorded.
- hh:mm Time the Event was recognized and recorded.
- UserId UserId of the user associated with the Event.
- Event Event Name - A Short description.
- Origin The origin of Event - STC, Command, Member, TSOLOGON.
- Describe A Longer description of the Event and/or Origin.

3.1.2 Worksheet Row Selection Command

- B If the Event has a corresponding Journal Entry, it may be browsed entering 'B' next to a target & pressing enter.

The lower portion of the panel is split into two sections. To the left are the Interval Reporting Settings, exclusively used for ADMIN Reports. To the right are the default Interval settings that will be first inherited as defaults by each new user Service Account.

Both Reporting Cycles – ADMIN, USER – share comparable control constructs. Both can be active/inactive, receive summary/detail reports, and receive them at each interval, or only on changes.

Both Reporting Cycles – ADMIN, USER – may receive reports Daily, and/or Weekly, and/or Monthly, at any interval, within a Day, a Week or a Month.

It is important to note that the recipient email address, associated with both – ADMIN, USER – is split between to fields, ‘Pre’ and ‘Dom’. ‘Pre’, the Email Prefix, is that portion of an email address up to, but not including, the ‘@’. ‘Dom’ is the Email Domain. This split allows for longer addresses to be entered, in limited panel space and importantly it allows the ICE/PSWD Administrator to Bind USER Emails to a specific Email Domain Server.

At each interval – Day, Wks, Mth – Activity Reports are prepared and delivered to the recipient Email Addresses. To run the Interval Background Reports in the Foreground, do the following:

For Day Reporting, enter 'RUN DAY' on the Panel Command Line and press enter. This action will call the Daily Report Module 'NSIMPCD', show some SysPrint Log messages on the screen, display the Daily Report in ISPF View, and send an Email containing the report to the recipient.

For Wks Reporting, enter 'RUN WKS' on the Panel Command Line and press enter. This action will call the Weekly Report Module 'NSIMPCW', show some SysPrint Log messages on the screen, display the Weekly Report in ISPF View, and send an Email containing the report to the recipient.

For Mth Reporting, enter 'RUN MTH' on the Panel Command Line and press enter. This action will call the Monthly Report Module 'NSIMPCM', show some SysPrint Log messages on the screen, display the Monthly Report in ISPF View, and send an Email containing the report to the recipient.

Note that all three of these actions – RUN DAY, RUN WKS, RUN MTH – will bring each reporting cycle 'Up-to-Date', replacing the 'Log Index Pointer' with a new pointer based on the current foreground execution. In the background, reports will still run 'On Cycle' at the defined intervals using the updated Pointer. Additional foreground options – EMAIL, PRINT, STORE – are available.

If you elect to change either of the Reporting Cycles – ADMIN, USER – remember that you must also 'UPDATE' before the new settings will take effect. To do this, place 'S' on the insertion point preceding 'Update Reporting Cycle', as shown at the bottom of the panel, and press enter. This action will immediately update NSEDETxx, an ICE Parmlib Member, and dynamically activate the change within the ICE Environment such that it will take effect immediately.

3.2 ICE/PSWD NSEDETxx Background – ADMIN

The NSEDETxx Control Cards, shown below, are used to configure the ADMIN Reporting Intervals. Whenever you make a change to the Reporting Cycle(s), you must perform an 'UPDATE' before the new settings take effect. To do this, place 'S' on the insertion point preceding 'Update Reporting Cycle' option, shown at the bottom of the Interval Reporting Panel, and press enter. This action will immediately update NSEDETxx and dynamically activate the change within the ICE Environment such it will take effect immediately.

3.2.1 To Control ADMIN Reporting Intervals

```
PCMONREPDAY ON
PCMONREPDAY CYCLE(DAILY) TIME(01:10)

PCMONREPWKS ON
PCMONREPWKS CYCLE(WEEKLY(SUN)) TIME(02:20)

PCMONREPMTH ON
PCMONREPMTH CYCLE(MONTHLY(1,2)) TIME(03:30)
```

NSEDETxx control over the report cycles may be overridden and ADMIN Reports run directly from the Panel Command Line by entering one of the following and pressing enter.

- RUN DAY
- RUN WKS
- RUN MTH

These will display the Daily, Weekly, or Monthly ADMIN Report. It is important to note that running reports in the foreground will interrupt the scheduled interval but will not diminish the integrity of the report itself. Events will be reported up to the point of foreground execution and then continue until the end of the interval at which time new events will be reported and, if required, and emails sent.

Foreground execution also supports PRINT and STORE options by entering the following on the Panel Command Line.

- RUN DAY PRINT or STORE
- RUN WKS PRINT or STORE
- RUN MTH PRINT or STORE

3.3 ICE/PSWD Notices & Services Settings Worksheet

When you select "List All Accounts" from the primary menu, the PSWD Notices & Services Settings Worksheet is presented.

```
           ICE 18.0 - PSWD Notice & Service Settings      Row 1 to 8 of 8
NSIMDSM 0103                                              ---PSWD Services--
-------------------- 8 - UserIds with Active PSWD Services --------------------
Row Selections: Show_Full_Service_Account
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Numb ---------------PSWD Password Notice & Service Settings-----------------

_ ____ ________ ________ _________ _________ _________ _________ _________
S ROWS NoticeId BkgLCERO UserLogons UserPswCng PswdExpire FormatRule OTPControl
_ 0001 ?        ---L---- --UpDate-- ----/--/-- ----/--/-- ----/--/-- ----/--/--
_ 0002 .DEFAULT -------- -NSEENSxx- -NSEENSxx- -NSEENSxx- ----/--/-- -NSEOTPxx-
_ 0003 PHARL1   -------O -NSEENSxx- -NSEENSxx- -NSEENSxx- -NSEPWRxx- 2021/01/01
_ 0004 PHARL2   Upd-C--- -NSEENSxx- -NoChange- -NSEENSxx- -NSEPWRxx- -NSEOTPxx-
_ 0005 PROBI2   ---L---- --UpDate-- ----/--/-- ----/--/-- ----/--/-- ----/--/--
_ 0006 ADMIN1   UpdLCERO 2021/01/03 -NoChange- --Config-- 2021/01/03 2021/01/03
_ 0007 AROBI3   -------- ----/--/-- ----/--/-- ----/--/-- -NSEPWRxx- ----/--/--
_ 0008 AROBI1   Upd---R- ----/--/-- ----/--/-- ----/--/-- 2021/01/02 ----/--/--
****************************** Bottom of data ********************************




 Option ===>                                                Scroll ===> CSR
```

This worksheet shows a summary of each Service Account. The Service Name Columns may show the name of the related configuration Parmlib Member, date of the last service account update or the words '—Update--' or '-NoChange-' or '--Config--. The 'BkgLCERO' Column shows the state of a user's authority to update their Interval Report Setting & each of the individual Service Account elements. '---' & '-' means user has no authority to update the related functions.

3.3.1 Worksheet Column Heading

- Rows - The worksheet row number.
- ServAcct - The UserId, ? or .Default is who owns the Service Account.
- BkgLCERO - A summary of Service Account Update Authority.
- Userlogons - Logon Notification Controls and Settings.
- UserPswCng - Password Change Notification Controls and Settings.
- PswdExpire - Password Expiration Notification Controls & Settings.
- FormatRule - Format Rule Binding Controls and Settings.
- OTPControl - One Time Password Controls and Settings.

3.3.2 Worksheet Row Selection Command

- S - Cursor to entry point immediately preceding a target ServAcct, enter 'S', press enter to show FULL UserId, ? or .Default Service Account.

3.4 ICE/PSWD ADMIN/USER Primary Service Account

The Service Account Panel presents an overview of a specific user ICE/PSWD configuration. Those with ADMIN authority access this menu from the 'PSWD Notice & Service Settings' Worksheet while individual users access via the ICE Primary Menu by entering the following Line Command.

TSO #PSWD ALERT

```
          NSIMDSM 0103    ICE 18.0 - Enriching RACF Controls - PHARL2

.. UserLogons  .. UserPswCng  .. PswdExpire  .. FormatRule  .. OTPControl
.. 2021/01/03  .. --Config--  .. -NSEENSxx-  .. ----/--/--  .. 2021/01/03
     ADMIN2         ADMIN2          ______         ______          ADMIN2

-----------------ICE/PSWD Periodic Background Reporting------------------

 --------Event Worksheets-------- | ------User Report Cycle /. Allow----
   ---ICE/PSWD--- ---ICE/TCE---   |  /. Activate /. Summary /. CngOnly
   .. UserLogons  .. ManageEdit   |
   ..    32   518  ..     0     7 |  .. Day - 00 00 - 24 Hour Interval
   .. UserPswCng  .. CmmdUpdate   |          24hh mm   1|2|4|6|8|12|24
   ..     0     0  ..     0     3 |  .. Wks - 00 00 - SUN
   .. PswdExpire  .. SubmitJobs   |          24hh mm   SUN,MON,TUE,Etc.
   ..     0     0  ..     0     0 |  /. Mth - 00 00 - 1,2
   .. FormatRule  .. OtherEvent   |          24hh mm   Day:1,2,9,25,EOM
   ..     0     0  ..     0     0 |  /. Pre PAT_____________________
   .. OTPControl  .. EveryEvent   |      Dom @COMPANY_____________________
   ..     0     0  ..    32   528 |      Copy UserId Reports TO Address

      .. Your PSWD Access Token          .. Update Service Account

                    .. Your PSWD Access Token
```

The ADMIN and USER view and function of the panel are similar with one exception. ADMIN view shows an Allow option, the USER view does not. If the ADMIN sets the Allow option 'ON' with a '/', the USER will be able to update certain of the Report Cycle settings – Day, Wks, Mth, Summary, CngOnly, Pre and Dom. IF the ADMIN sets the Allow option 'OFF' by Unchecking, the USER will not be granted update authority and the panel will dynamically change to reflect this disallow setting by removing the 'Update Service Account' option.

In either view, the upper portion of the panel shows the summary status of the five ICE/PSWD Service Elements. If the Element name is shown in RED, it is meant to indicate the USER has not been granted update authority to the Element. The USER can view the Element configuration but may not update. If shown in WHITE, the USER has been granted update authority. Selecting an Element will show its current configuration.

The area below the Element name shows its configuration status. If a date appears, it is meant to indicate the last time the configuration was updated. If a Member name appears – NSEENSxx, NSEPWRxx, NSEOTPxx – it is meant to indicate that the Element was configured directly in the named Member and has yet to be updated via this configuration interface. If '--Config--' appears, it is meant to indicate that the Element has a configuration file but has no active Control Card within its associated Member. If '----/--/--' appears, it is meant to indicate that the Element has neither a configuration file nor active Control Cards.

The left portion of the panel is devoted to displaying USER events. By the numbers, it shows those that are new since the last time the panel was updated and the total number currently contained in the ICE Transaction Log. Cursor into the insertion point preceding one of the ten Event Categories, enter an 'S' and press enter to View all Events within that Category. Cursor into the insertion point immediately below, enter 'S' and press enter to View New Events. The number immediately to the right of this insertion point is the number of New Events. The number to its right is the number of Total Events.

The right portion of the panel is devoted to controlling the USER Reporting Cycle. As described above, a USER may or may not have been granted update authority to the Report Cycle options.

At each interval – Day, Wks, Mth – Activity Reports that reflect only events related to the USER activity are prepared and delivered to the recipient Email Addresses. To run this Interval Background Report in the Foreground, do the following:

- For Day Reporting, enter 'RUN DAY' on the Panel Command Line and press enter. This action will call the Daily Report Module 'NSIMPWD', show some SysPrint Log messages on the screen, display the Daily Report in ISPF View, and send an Email containing the report to the recipient.

- For Wks Reporting, enter 'RUN WKS' on the Panel Command Line and press enter. This action will call the Weekly Report Module 'NSIMPWW', show some SysPrint Log messages on the screen, display the Weekly Report in ISPF View, and send an Email containing the report to the recipient.

- For Mth Reporting, enter 'RUN MTH' on the Panel Command Line and press enter. This action will call the Monthly Report Module 'NSIMPWM', show some SysPrint Log messages on the screen, display the Monthly Report in ISPF View, and send an Email containing the report to the recipient.

Note that all three of these actions – RUN DAY, RUN WKS, RUN MTH – will bring each reporting cycle 'Up-to-Date' replacing the 'Log Index Pointer' with a new pointer based on the current foreground execution. In the background, reports will still run 'On Cycle' and the defined intervals, using the updated Pointer. Additional foreground options – EMAIL, PRINT, STORE – are available.

3.5 ICE/PSWD NSEDETxx Background – USER

Upon first entry into a USER Service Account, the USER Report Cycle settings will be the DEFAULT settings, defined by the Administrator. From the ADMIN View, certain of these settings – Day, Wks, Mth, Summary, CngOnly, Pre, Dom – may be updated. They may also be updated in the USER View only if the USER has been granted update authority.

The ADMIN View has one other option not available to the USER: the Activate option. Using this option, the Administrator may '/' to activate or UnCheck to deactivate the Report Cycle, on a USER by USER basis.

The NSEDETxx Control Cards shown below are used to configure the USER Reporting Intervals. Whenever you make a change to the Reporting Cycle(s), you must perform an 'UPDATE' before the new settings take effect. You can do this by placing 'S' on the insertion point preceding 'Update Reporting Cycle' option, shown at the bottom of the Interval Reporting Panel, and press enter. This action will immediately update NSEDETxx and dynamically activate the change within the ICE Environment such that it will take effect immediately.

3.5.1 To Control USER Reporting Intervals

```
PSWDRPTSDAY ON
PSWDRPTSDAY CYCLE(DAILY) TIME(01:10)

PSWDRPTSWKS ON
PSWDRPTSWKS CYCLE(WEEKLY(SUN)) TIME(02:20)

PSWDRPTSMTH ON
PSWDRPTSMTH CYCLE(MONTHLY(1,2)) TIME(03:30)
```

NSEDETxx control over the report cycles may be overridden and USER Reports run directly from the Panel Command Line by entering one of the following and pressing enter.

- EVENT or CHNGS DAY
- EVENT or CHNGS WKS
- EVENT or CHNGS MTH

These will display the Daily, Weekly or Monthly USER Report. If EVENT is specified, the report will contain only the Users New Events. If CHNGS is specified, the report will contain only changes to the Users Configuration Settings. It is important to note that running reports in the foreground will interrupt the scheduled interval but will not diminish the integrity of the report itself. Events will be reported up to the point of foreground execution and then continue until the end of the interval at which time new events will be reported and, if requested, an email sent.

Foreground execution also supports PRINT and STORE options by entering the following on the Panel Command Line.

- EVENT or CHNGS DAY PRINT or STORE
- EVENT or CHNGS WKS PRINT or STORE
- EVENT or CHNGS MTH PRINT or STORE

3.6 ICE/PSWD NSEENSxx Background – ACTION Block

The NSEDETxx and NSEENSxx ICE Parmlib members work together. NSEDETxx controls the Report Cycle kicking off as configured, calling the Report Module which returns the requested Interval Report to be used as an Email Attachment. The 'WHO' in who get the report is determined by ACTION BLOCKS and their Control Cards as contained in the NSEENSxx member.

In the specific case of USER Interval Report distribution, all users are grouped into a single – DAY, WKS, MTH – ACTION BLOCK as shown below. This ensures that all users receive their corresponding reports – DAY, WKS, MTH – on the same day or date and time.

```
ACTION PSWDMON(PSWDRPTSDAY) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
TO AROBI1@COMPANY
TARGETUSER PROBI2
TO PROBI2@COMPANY
ACTION .END

ACTION PSWDMON(PSWDRPTSWKS) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
TO AROBI1@COMPANY
TARGETUSER PROBI2
TO PROBI2@COMPANY
TARGETUSER ADMIN1
TO ABC@COMPANY
ACTION .END

ACTION PSWDMON(PSWDRPTSMTH) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
```

```
TO AROBI1@COMPANY
TARGETUSER PHARL2
TO CAT@COMPANY
ACTION .END
```

3.7 ICE/PSWD Logon Notification – Control Settings Panel

This panel shows the current Logon Notification configuration for the noted UserId. Notices may be sent with each logon or during certain times, on certain days and upon receipt of specific Return Codes. Named Systems and Named UserIds (when .Default) may be excluded from the notification process.

```
◊-------------------------------------------------------------------------◊
◊               ICE 18.0 - Logon Change Rule Details                      ◊
◊            Selected NoticeId PHARL2__ /. Allow Updates                  ◊
◊                                                                         ◊
◊        TO:           /. PAT                                             ◊
◊        Copy:         /. ESM                                             ◊
◊        Alias:        /. CHUCK BARRY                                     ◊
◊        Subject:      /. YOU JUST LOGGED ON                              ◊
◊        Inactive On:  /. (SYS1,SYS2,SYS3)                                ◊
◊        Active Time:  /. STM(0700) ETM(1900)                             ◊
◊        Active Day:   .. DAYS(SAT,SUN)                                   ◊
◊        Active RC:    .. NOTEQUAL(00)                                    ◊
◊        From:         /. SUPPORT                                         ◊
◊        Domain:       /. @COMPANY.COM                                    ◊
◊        EMailDebug:   /. ON          JrlPost: /.. OFF                    ◊
◊                                                                         ◊
◊      Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return         ◊
◊-------------------------------------------------------------------------◊
◊-------------------------------------------------------------------------◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return              ◊
◊-------------------------------------------------------------------------◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may only view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- TO: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Inactive On: - Named Systems that will NOT report Logons.
- Active Time: - Start and End time when notification is active.
- Active Day: - Days when notification is active.
- Active RC: - Return Codes to report or not report logons.
- MsgBody: - Supplemental message provides notice clarification.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.

- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

3.8 ICE/PSWD Logon Notification – ACTION Block

In the ACTION BLOCK shown below, it is important to note that the DOMAIN Control Card *MUST* precede all TO, CC and FROM prefix addresses. And that the use of DOMAIN is exclusive to the ACTION BLOCK containing it as it will NOT carry over to other ACTION BLOCKS.

```
ACTION SYSLOGON(PHARL2) METHOD(EMAIL) SCOPE(REPORT)
DOMAIN @COMPANY.COM
TO PAT
CC ESM
ALIAS 'CHUCK BARRY'
SUBJECT 'YOU JUST LOGGED ON'
NOTIFICATION INACTIVE(SYS1,SYS2,SYS3)
WHEN ACTIVE STM(0700) ETM(1900)
WHEN ACTIVE SAT,SUN
WHEN ACTIVE NOTEQUAL(00)
FROM SUPPORT
DEBUG ON
JRLPOST OFF
ACTION .END
```

3.9 ICE/PSWD Change Notification – Control Settings Panel

This panel shows the current Password Change Notification configuration for the noted UserId. Notices may be sent with each RESET attempt all the time or at certain times or only on certain days of the week or both taken together. Named Systems may be excluded as can named UserIds when the .DEFAULT Global setting is in use.

```
◊-------------------------------------------------------------------------◊
◊               ICE 18.0 - Password Change Notice Rules                   ◊
◊             Selected NoticeId PROBI1   /. Allow Updates                  ◊
◊                                                                         ◊
◊        To:           /. JIM@COMPANY.COM                                 ◊
◊        Alias:        /. JOHN BROWN                                      ◊
◊        Subject:      /. PASSWORD RESET ALERT                            ◊
◊        Inactive On:  /. (SYS2,SYS3)                                     ◊
◊        Active Time:  /. STM(0800) ETM(2000)                             ◊
◊        Active Day:   /. DAYS(FRI,SAT,SUN)                               ◊
◊        From:         /. SUPPORT@TECHLAND.COM                            ◊
◊        Domain:       ..                                                 ◊
◊        EMailDebug:   /. ON           JrlPost: /. ON                     ◊
◊                                                                         ◊
◊      Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return         ◊
◊-------------------------------------------------------------------------◊
◊-------------------------------------------------------------------------◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return              ◊
◊-------------------------------------------------------------------------◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- To: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Inactive On: - Named Systems that will NOT report Logons.
- Active Time: -Start and End time when notification is active.
- Active Day: - Days when notification is active.
- MsgBody: - Supplemental message provides notice clarification.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

3.10 ICE/PSWD Change Notification – ACTION Block

```
ACTION PSWDCHNG(PROBI1) METHOD(EMAIL) SCOPE(REPORT)
TO ABC@COMPANY.COM
CC ESM@COMPANY.COM
ALIAS 'JOHN BROWN'
SUBJECT 'PASSWORD RESET ALERT'
NOTIFICATION INACTIVE(SYS2,SYS3)
WHEN ACTIVE STM(0800) ETM(2000)
WHEN ACTIVE DAYS(FRI,SAT,SUN)
FROM SUPPORT@TECHLAND.COM
DEBUG ON
JRLPOST ON
ACTION .END
```

3.11 ICE/PSWD Expire Notification – Control Settings Panel

This panel shows the current Password Expire Notification configuration for the noted UserId. Notice of pending password expiration will be sent on the day(s) prior to expiration defined in 'Interval'. The Interval may be 1 day or several days depending on specific circumstances. For example, one Interval might be Interval 9, meaning nine days prior to expiration. A second example could be Interval 0, 1, 3, 5, 10, 15, meaning that notification of pending password expiration would occur 15 days prior and then 10, five, three and one day prior to password expiration with a final notification occurring on the day the password expires.

```
◊-------------------------------------------------------------------------◊
◊                ICE 18.0 - Expire Notice Rule Details                    ◊
◊             Selected NoticeId GBAGS1   /. Allow Updates                  ◊
◊                                                                         ◊
◊        To:           /. GHB@COMPANY.COM                                 ◊
◊        Alias:        /. JANE SMITH                                      ◊
◊        Subject:      /. EXPIRATION_NOTICE                               ◊
◊        Intervals:    /. 0,1,2,3,5,10,15                                 ◊
◊        From:         /. CAT@COMPANY.COM                                 ◊
◊        Domain:       ..                                                 ◊
◊        EMailDebug:   /. ON           JrlPost: /. OFF                    ◊
◊                                                                         ◊
◊      Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return         ◊
◊-------------------------------------------------------------------------◊
◊-------------------------------------------------------------------------◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return              ◊
◊-------------------------------------------------------------------------◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- TO: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Intervals: - The notice interval(s) - Days before expiration.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

3.12 ICE/PSWD Expire Notification – ACTION Block

```
ACTION PSWDEXP(GBAGS1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
TO GHB@COMPANY.COM
ALIAS 'JANE SMITH'
SUBJECT 'EXPIRATION_NOTICE'
INTERVAL (0,1,2,3,5,10,15)
FROM CAT@COMPANY.COM
DEBUG ON
JRLPOST OFF
ACTION .END
```

3.13 ICE/PSWD Format Rule Binding – Control Settings Panel

Binding is a process that associates a specific UserId with one or more specific format rules. Binding ensures that privileged users and system administrators be required to guard their logon credentials with the more complex Rules. To bind the selected User/Group to a rule, enter the TYPE of binding; USR|RCF|TCE. Next, check '/' one or more of the valid Rules. UnCheck to remove or enter 'D' to delete UserId Binding.

One or more Password format rule(s) may be defined for enforcement by the External Security Manager. This enforcement notwithstanding, users attempting to reset a password only need comply with the least complex of the available rules. The panel shows under the names RULE1 - RULE8, those rules that are actually defined. Those that are active appear in their defined slot and reflect the minimum and maximum password length and format syntax. Rule slots that show --:--(--------) have no rule defined. To decode a valid rule, cursor under it and press return. This action will display an explanation of the rule.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Password Rule Binding - Update                 ◊
◊                                                                          ◊
◊            Selected NoticeId USR : MFITZ1__ /. Allow Updates              ◊
◊                                                                          ◊
◊  ---------------------Valid Password Format Rules---------------------   ◊
◊  /. 6:8(LLLLLLLL) /. 5:8(CcvV$NWA) /. 7:7(A*Vv$cs ) .. -:-(--------)    ◊
◊  .. -:-(--------) .. -:-(--------) .. -:-(--------) .. -:-(--------)    ◊
◊                                                                          ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. Then Press Return        ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊           Updates Not Allowed Enter 'R' > .. > Press Return              ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

3.14 ICE/PSWD Format Rule Binding – ACTION Block

```
USERID MFITZ1 RULES(RULE1,RULE2,RULE3)
```

3.14.1 NSEPWRxx ACTION BLOCK Types

- USR = USERID
- RCF = RACFGRP
- TCE = TCEGRP

3.15 ICE/PSWD One Time Password – Control Settings Panel

The panel shows the One-Time Password (OTP) configuration for the noted UserId. A user attempting a password reset would be failed pending receipt of the OTP Token and their return to the originating system to retry the reset using the Token as the new password within the Time & Retry Limit. If the user exceeds the value set as the Retry Limit they may be optionally revoked.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊               ICE 18.0 - OTP Password Change Controls                  ◊
◊             Selected NoticeId PROBI1   /. Allow Updates                 ◊
◊                                                                        ◊
◊        To:           /. PRR                                            ◊
◊        Alias:        /. SAM SMITH                                      ◊
◊        Subject:      /. UNDER OTP CONTROL                              ◊
◊        OTPActive:    /. FAIL                                           ◊
◊        TimeWindow:   /. 05:00                                          ◊
◊        TerminalMsg:  /. YES                                            ◊
◊        ResetLimit:   /. 3                                              ◊
◊        OnLimit:      /. REVOKE                                         ◊
◊        From:         /. SUPPORT                                        ◊
◊        Domain:       /. @CORPORATE.COM                                 ◊
◊        Excluded:     .. (only when NoticeId = . DEFAULT)               ◊
◊        EMailDebug:   /. ON           JrlPost: /. NO                    ◊
◊                                                                        ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return          ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return             ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- To: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- OTPActive: - If set to FAIL prevents bypass of active OTP Control.
- TimeWindow: - Time to respond before OTP Expires - mm:ss
- TerminalMsg: - If Default OTP Instruction is to be used - ON|OFF.
- ResetLimit: - Number failed reset attempts before restart needed.
- OnLimit: - Set REVOKE if UserId to be revoked if Limit reached.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.

- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal

For a definition of each field, cursor into the field and press enter.

3.16 ICE/PSWD One Time Password – ACTION Block

```
ACTION PSWDOTP(PROBI1) METHOD(EMAIL) SCOPE(REPORT)
DOMAIN @CORPORATE.COM
TO PRR
ALIAS 'SAM SMITH'
SUBJECT 'UNDER OTP CONTROL'
TIMEWINDOW 05:00
RETRYLIMIT 3 ONLIMIT(REVOKE)
TERMMSG ON
FROM SUPPORT
DEBUG ON
JRLPOST NO
ACTION .END
```

3.17 ICE/PSWD USERS Application Access Token

The ICE Administrator assigned a Default AppToken to guard access to ICE/PSWD and its functions. You may continue to use the default AppToken to access your Account. However, it would be much better if you Self-Assigned a private AppToken to better protect access to your account using the dialog shown below.

```
◊──────────────────────────────────────────────────────────────────────◊
◊               ICE 18.0 - Define An Application Token                 ◊
◊                                                                      ◊
◊                                  ---AppToken--- -                    ◊
◊                      Your Token > CXNJTTNBHHJF   +                   ◊
◊           ---------------------------------------------              ◊
◊                    Change Token >                                    ◊
◊                    Confirmation >                                    ◊
◊                                                                      ◊
◊                Next Select > .. Yes > Then Press Enter               ◊
◊──────────────────────────────────────────────────────────────────────◊
```

A Self-Assigned AppToken must be composed entirely of alphanumeric characters and be from 8-14 of such characters in length. Once you Self-Assign, the Default AppToken will be failed if you attempt to use it to access your account.

If you forget your AppToken, only the ICE Administrator can revoke it and in doing so, reinstate the Default.

You may reset your private AppToken as often as you like. Frequent reset provides high levels of protection and is recommended.

Once an AppToken is self-assigned, it will appear encoded as the value of 'Your Token' in the dialog. To decode the encoded value, cursor under '± ' and press enter. The popup will display the decoded value.

To reset your AppToken to the Default set by the ICE Administrator, enter as the Change Token value '*RESET*' and confirm '*RESET*' as the Confirmation Value then press return. The AppToken is immediately reset to the Default Value and the self-assigned AppToken is erased.

4 User Notification Upon Logon:

Logging on to IBM Z is serious business. Whether the logon UserId has credentials with limited resource access or is highly privileged, the result can be the same. When that credential has been comprised, system integrity has been lost.

4.1 An Introduction to Logon Notification

The primary objective of Logon Notification is to involve the owner of the logon credential in the overall IBM Z security paradigm. Such involvement would allow the owner to effectively "Self-Audit" logon events. This is critical as the logon credential owner is the only one who knows for certain if the Logon event is, in fact, valid and not the result of their compromised credential.

While notification of the last prior logon exists in TSO, it is in fact "after the fact" and may not attract the attention of the user. In addition, there are many more entry points used for logging on that do not present such last use information.

ICE/PSWD collects information during logon that is used to build the logon notification. This is then sent to the user as in the following example.

```
01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR----------- VerifySuccess -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:13:43:07 DT:11/21/17
03C|-VERIFY(X): This is an alias-----------------RC: 00--------------------
```

There are a number of SYSLOGON Session Types Monitored including:

Where SYSLOGON Session Types Monitored include:

```
01 TOKSAS   - System address space
02 TOKCMND  - Command
03 TOKCONS  - Console operator
04 TOKSTP   - Started procedure
05 TOKMNT   - Mount
06 TOKTSO   - TSO logon
07 TOKBCH   - Internal reader batch job
08 TOKXBM   - Internal reader execution batch monitor
09 TOKRJE   - RJE operator
10 TOKNJE   - NJE operator
11 TOKNJEUS - VERIFYX unknown userid token
12 TOKEBCH  - External reader batch job
13 TOKRBCH  - RJE batch job
14 TOKNBCH  - NJE batch job
15 TOKNSYS  - NJE sysout
16 TOKEXBM  - External XBM
17 TOKRXBM  - RJE XBM
18 TOKNXBM  - NJE XBM
19 TOKAPPC  - APPC session
```

```
20 TOKOSRV  - OMVSSRV session
21 TOKIP    - IP session
```

4.2 How Logon Notification selects/processes an Event

The implementation of this function is totally transparent to the end user, as their logging on to the system is unchanged. This notwithstanding, the user is defined in NSEENSxx, with an ACTION statement defining the parameters for the notification.

```
ACTION SYSLOGON(USER01) METHOD(EMAIL) SCOPE(REPORT)
SUBJECT 'SYSTEM LOGON ALERT'
TO USR@COMPANY.COM
WHEN ACTIVE  STM(0800)  ETM(2000)
WHEN RETCODE LESSTHAN(14)
ACTION .END
```

The RETURNCODE parameter specifies requirements for the return code from RACF where conditional RACF SYSLOGON Return Codes are:

```
00 - Success
04 - User profile not defined to RACF
08 - Password or phrase is not authorized
0C - Password or phrase has expired
10 - Invalid setting/usage for new pwd/phrase
14 - User not defined to group
18 - REQUEST=VERIFY failed by exit
1C - User is revoked
20 - N/A
24 - User access to specified group is revoked
28 - OID parm required but not supplied
2C - OID parm not valid for specified user
30 - User not authorized for POE in class
34 - User not authorized to use application
38 - SECLABEL checking failed
3C - N/A
40 - N/A
44 - A default TOKEN is used as input TOKEN
48 - Unprivileged user VERIFY tranquil state
4C - NODES checking failed
50 - Surrogate submit attempt failed
54 - JESJOBS check failed
58 - N/A
5C - Error retrieving RACF database data
60 - N/A
64 - Invalid REQUEST=VERIFY macro usage
```

4.3 SYSLOGON Notification Examples

Placing an equivalent set of Control Cards, as shown below, in the ICE NSEENSxx Parmlib Member:

```
ACTION SYSLOGON(BOBLNG2) METHOD(EMAIL)
TO BOB01@COMPANY.com
WHEN RETURNCODE(00,08,1C)
ACTION END.
```

This will generate, depending on Logon circumstances, both a successful and unsuccessful notifications.

Examples of Successful Logon Notifications:

```
01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR----------- VerifySuccess -
02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:BOB01       TM:09:48:53 DT:11/28/17
03C|-VERIFY(X): BOB01------RC: 00 Password or phrase is authorized
```

Examples of Failed Logon Notifications:

```
01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR-------------- VerifyFail -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:BOB01       TM:14:56:58 DT:02/17/17
03C|-VERIFY(X): BOB01-----RC: 08 Password or phrase is not authorized

01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR-------------- VerifyFail -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:BOB01       TM:15:14:00 DT:02/17/17
03C|-VERIFY(X): BOB01-----RC: 1C User is revoked
```

4.4 Replacing UserId specifics with an Alias in Notifications

The ALIAS control card can be used to alter the userid information contained in the notification data. In the example below, with ALIAS specified, the userid value in line 02C is masked with "********" and the userid value in line 03C is replaced with the ALIAS value up to a maximum of 32 characters.

```
ACTION SYSLOGON(ESSJDL2) METHOD(ESMEMAIL)
TO jiml@COMPANY.com
ALIAS 'TOP DOG ALIAS'
WHEN RETURNCODE(00,08,1C)
ACTION END.
```

The resulting notification would be formatted as follows:

```
01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR-------------- VerifyFail -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:15:14:00 DT:02/17/17
03C|-VERIFY(X): THIS IS AN ALIAS----------------------RC: 1C User is revoked
```

4.5 Specifying Watchful Periods

A "Watchful Period" is represented by a day(s) of the week and/or times of day in which system logon events are to be reported. In the following example,

events would only be reported if they occurred on Saturday and Sunday and also met the RETURNCODE condition defined.

```
ACTION SYSLOGON(ESSJDL2) METHOD(ESMEMAIL)
TO jiml@COMPANY.com
ALIAS THIS IS AN ALIAS'
WHEN RETURNCODE(00,08,1C)
WHEN DAY|DAYS(SAT,SUN)
ACTION END.
```

The “Watchful Period” may also be limited to start at a specific time of day and end at a specific time of day, as shown in the following example.

```
ACTION SYSLOGON(ESSJDL2) METHOD(ESMEMAIL)
TO jiml@COMPANY.com
ALIAS ’THIS IS AN ALIAS'
WHEN RETURNCODE(00,08,1C)
WHEN DAY|DAYS(SAT,SUN)
WHEN ACTIVE STM(0800) ETM(2200)
ACTION END.
```

In this example, notification would be sent based on the concatenation of all WHEN conditions such that notification would only occur between 8:00AM and 10:00PM (note that military time is used for time values) on a Saturday or a Sunday, but only when the return code for the logon attempt was 00, 08 or 1C.

The “Watchful Period” may begin at a time certain in the future and end at a time certain in the future. For example

```
ACTION SYSLOGON(ESSJDL2) METHOD(ESMEMAIL)
TO jiml@COMPANY.com
ALIAS ’TOP DOG ALIAS'
WHEN RETURNCODE(00,08,1C)
WHEN DAY|DAYS(SAT,SUN)
WHEN ACTIVE SDT(171222) STM(0800) EDT(180105) ETM(2200)
ACTION END.
```

In this example, the “Watchful Period” will begin on December 12, 2020 and end on January 05, 2021. It will be active on Saturdays and Sundays, if any fall between the dates specified, and only between the hours of 8:00AM to 10:00PM.

4.6 System Logon Log Record:

When a System Logon is detected, a Log Record is created and stored in the ICE Event Log using the Record Identifier of “SL”. If the event is associated with a (?) SYSLOGON Action Block, the Log Record Identifier is “XL”.

4.7 ICE/PSWD Logon Notification – Control Settings Panel

This panel shows the current Logon Notification configuration for the noted UserId. Notices may be sent with each logon or during certain times, on certain days, and upon receipt of specific Return Codes. Systems and '.Default' UserId be excluded by name.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊               ICE 18.0 - Logon Change Rule Details                       ◊
◊            Selected NoticeId PHARL2__ /. Allow Updates                   ◊
◊                                                                          ◊
◊       TO:           /. PAT                                               ◊
◊       Copy:         /. ESM                                               ◊
◊       Alias:        /. CHUCK BARRY                                       ◊
◊       Subject:      /. YOU JUST LOGGED ON                                ◊
◊       Inactive On:  /. (SYS1,SYS2,SYS3)                                  ◊
◊       Active Time:  /. STM(0700) ETM(1900)                               ◊
◊       Active Day:   .. DAYS(SAT,SUN)                                     ◊
◊       Active RC:    .. NOTEQUAL(00)                                      ◊
◊       From:         /. SUPPORT                                           ◊
◊       Domain:       /. @COMPANY.COM                                      ◊
◊       EMailDebug:   /. ON          JrlPost: /.. OFF                      ◊
◊                                                                          ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return           ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊         Updates Not Allowed Enter 'R' > .. > Press Return                ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view, if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- TO: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Inactive On: - Named Systems that will NOT report Logons.
- Active Time: - Start and End time when notification is active.
- Active Day: - Days when notification is active.
- Active RC: - Return Codes to report or not report logons.
- MsgBody: - Supplemental message provides notice clarification.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

4.8 ICE/PSWD Logon Notification – ACTION Block

In the ACTION BLOCK shown below, it is important to note that the DOMAIN Control Card MUST precede all TO, CC and FROM prefix addresses; and that the use of DOMAIN is exclusive to the ACTION BLOCK containing it, as it will NOT carry over to other ACTION BLOCKS.

```
ACTION SYSLOGON(PHARL2) METHOD(EMAIL) SCOPE(REPORT)
DOMAIN @COMPANY.COM
TO PAT
CC ESM
ALIAS 'CHUCK BARRY'
SUBJECT 'YOU JUST LOGGED ON'
NOTIFICATION INACTIVE(SYS1,SYS2,SYS3)
WHEN ACTIVE STM(0700) ETM(1900)
WHEN ACTIVE SAT,SUN
WHEN ACTIVE NOTEQUAL(00)
FROM SUPPORT
DEBUG ON
JRLPOST OFF
ACTION .END
```

5 User Notification Upon Password Change

Changing a password and/or passphrase, from time to time is an important and necessary part of an effort to protect the integrity of a full logon credential. It has often been said that the first thing that an intruder, using a stolen credential, is likely to do is reset the password and/or passphrase. The reason is simple: unless the owner is notified of the change, their only clue of this wrongdoing will be an inability to logon, at some future time. This could be long after the damage is done, the intruder is long gone, and the attribution for any actions now documented as that of the unsuspecting credential owner.

5.1 An Introduction to Password Change Notification

The purpose of Password Change Notification is to alert the rightful owner of a logon credential that their password has been changed. Their receipt of such notification allows them to react accordingly - if it is determined that the password change notification is valid, no action is required. If it is determined that the password was changed without the owner's knowledge, the event can be reported to system security immediately and appropriate action can be taken.

5.2 How PW Change Notification selects/processes an Event

Here are three examples of Password Change Notifications captured from three different reset execution points:

```
01C|-SRC: TSOCMD--------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:ESSJDL2     TM:09:46:17 DT:12/22/16
03C|-PSWDCHNG: MTECH3-------------------------------------------------------

01C|-SRC: OPERCMD--------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:ESSJDL2     TM:10:03:55 DT:12/22/16
03C|-PSWDCHNG: MTECH2-------------------------------------------------------

01C|-SRC: LOGON----------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:10:00:31 DT:12/22/16
03C|-PSWDCHNG: CHUCK BARRY----------------------------------------------------
```

SRC: can be TSOCMD, OPERCMD, or LOGON depending on how the password reset was initiated.

The USRID on line 2 will by default be the UserId that triggered the request. If the ALIAS Control is present, USRID will be "********". If this is an admin reset, as the OPERCMD example was, then USRID will be the UserId that issued the ALU command. Similarly, that's what will be displayed if the command was issued from the operator console.

If it is a LOGON triggered request, it will be the UserId of the user logging on.

The PSWDCHNG value on line 3 is the UserId for which the password is being reset or, if the ALIAS Control Card is being used, the thirty-two-character value assigned.

Note, two different UserIds were the target of password changes (MTECH2 and MTECH3). Two of these resets were admin resets (one from TSO, one from a console command), and one of the resets was a user-triggered reset at logon.

5.3 PSWDCHNG Notification Examples

Here are the NSEENSxx control cards in use:

```
ACTION PSWDCHNG(MTECH3) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
SUBJECT 'PSWDCHNG notification for MTECH3'
FROM from_email@company.com
TO email@company.com
ACTION .END

ACTION PSWDCHNG(MTECH2) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
SUBJECT 'PSWDCHNG notification for MTECH2'
FROM from_email@company.com
TO email@company.com
ACTION .END
```

So, regardless of who resets the password, the user or an admin, the user will still be notified of the change.

5.4 Common Usage Control Cards

```
ALIAS '------------------------------32'
WHEN DAY|DAYS(dayday) and
WHEN ACTIVE SDT(yymmdd) STM(hhmm) EDT(yymmdd) ETM(hhmm)
```

The ALIAS sub-parameter provides the same functionality with the PSWDCHNG ACTION BLOCK, as provided within the SYSLOGON ACTION BLOCK described in the previous section.

5.5 Password Change Log Record:

When a password change is detected, a Log Record is created and stored in the ICE Event Log, using the Record Identifier of “PC”.

5.6 ICE/PSWD Change Notification – Control Settings Panel

The panel shows the current Password Change Notification configuration for the noted UserId. Notices may be sent with each RESET attempt, all the time, or at certain times, or only on certain days of the week, or both taken together. Named Systems may be excluded as can named UserIds when the .DEFAULT Global setting is in use.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Password Change Notice Rules                 ◊
◊              Selected NoticeId PROBI1   /. Allow Updates                ◊
◊                                                                        ◊
◊        To:           /. JIM@COMPANY.COM                                ◊
◊        Alias:        /. JOHN BROWN                                     ◊
◊        Subject:      /. PASSWORD RESET ALERT                           ◊
◊        Inactive On:  /. (SYS2,SYS3)                                    ◊
◊        Active Time:  /. STM(0800) ETM(2000)                            ◊
◊        Active Day:   /. DAYS(FRI,SAT,SUN)                              ◊
◊        From:         /. SUPPORT@TECHLAND.COM                           ◊
◊        Domain:       ..                                                ◊
◊        EMailDebug:   /. ON           JrlPost: /. ON                    ◊
◊                                                                        ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return         ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return             ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- To: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Inactive On: - Named Systems that will NOT report Logons.
- Active Time: -Start and End time when notification is active.
- Active Day: - Days when notification is active.
- MsgBody: - Supplemental message provides notice clarification.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

5.7 ICE/PSWD Change Notification – ACTION Block

```
ACTION PSWDCHNG(PROBI1) METHOD(EMAIL) SCOPE(REPORT)
TO PRR@COMPANY.COM
CC ESM@COMPANY.COM
ALIAS 'JOHN BROWN'
SUBJECT 'PASSWORD RESET ALERT'
NOTIFICATION INACTIVE(SYS2,SYS3)
WHEN ACTIVE STM(0800) ETM(2000)
WHEN ACTIVE DAYS(FRI,SAT,SUN)
FROM SUPPORT@TECHLAND.COM
DEBUG ON
JRLPOST ON
ACTION .END
```

6 Notification of Upcoming Password Expiration:

It is considered likely that most users, both general and privileged, will wait until their password has expired before they reset. Since not all users logon every day, they may be unsure as to a pending expiration and the need to reset.

6.1 An Introduction to RACF Password Expire Notification

Based on an optional setting found in SETROPTS and appearing in the SETROPTS listing, RACF provides notification (ICH0002I) of upcoming password expiration on a user by user basis as they logon.

When no warning is given to the user of an upcoming expiration, the user may be surprised and frustrated at being unable to logon to commence work. This may cause them to rush through the reset process. The resulting new password may not have the desired strength. Providing advanced notice of expiration will help to resolve these issues.

Currently, when Notice is to be given, it can only be sent if the user logs on to TSO (or submits a batch job). Users who access a system via FTP, CICS, VTAM, etc. would not receive any notification, even though a similar access through TSO would generate notification. For some system users, notification is not possible because of the type of subsystem to which they logon. For TSO users, the fact that they receive notice gives them time to think about, and time to consider the merits of, an upcoming password reset.

A snippet, extracted from the standard SETROPTS report showing both cases, is shown below:

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS LEGACY
  PASSWORD CHANGE INTERVAL IS  45 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   3 DAYS.
  MIXED CASE PASSWORD SUPPORT ARE IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  PASSWORD HISTORY BEING MAINTAINED 5.
  USERIDS NOT BEING AUTOMATICALLY REVOKED.
  NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
```

or perhaps

```
PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.

ICH70002I YOUR PASSWORD WILL EXPIRE IN (10) DAYS.
```

6.2 Failure to Notify May Lead to System Vulnerability

It is considered an Integrity Best Practice to frequently reset one's password in order to void any current valid password that may have been compromised from being used by someone other than the rightful credential owner.

In the SETROPTS example described above, the password change interval is set to 45 days and the expiration warning to 10 days. This means that for the 35 days immediately preceding expiration, the user would not know of an upcoming warning and the need to reset their password. In addition, the user would receive notification, if they logged on to TSO, each time they logged on, beginning on day 10, and continuing until a password change became mandatory. As far as it goes, and as applied globally, this is all good.

As a supplemental to the RACF SETROPTS PASSWORD(WARNING()) option, ICE/PSWD allows for pending password expiration notification, based on individual or group needs. Such notifications can be defined for specific days preceding expiration, as opposed to each day once a warning threshold day has been reached.

These notifications are not tied to a system logon event. Such an approach enriches RACF protections, allows for customization that fits individual or group needs, and provides a user with the time often needed to develop a new replacement password. When combined with the ICE/PSWD Format Rule Enhancement, passwords will become more complex and users will most likely take additional time to formulate suitable replacements.

6.3 How Expiration Notification Selects/Processes an Event

The Expire Notification task is initiated with an ICE TASK=NEZUOPTS control card in NSEPRMxx. This module provides support for RACF UserId password expiry notification, supported by the PSWDEXP(UserId) ACTION BLOCKs in NSEENSxx. When initiated, NEZUOPTS triggers a RACF UserId extraction three minutes after the ICE Started Task startup. Based on UserId password expiry dates and NSEENSxx PSWDEXP ACTION BLOCK settings, email notification will be made to specified recipients. Collectively, these actions inform users of a pending password expiry situation.

The EXPINTERVAL control card in the action block will indicate which day(s) interval expiry notification should occur. Here is an example EXPINTERVAL control card:

EXPINTERVAL (0,1,2,3,5,7,14)

In this case, a user whose password has a defined RACF expiry window, and who has a corresponding NSEENSxx PSWDEXP ACTION BLOCK, will receive e-mail notification of their password pending expiry 14 days before it expires, 7 days before it expires, 5 days before it expires, and then 3, 2, and 1 day before it expires and finally on the day of expiration. This process requires no system access attempts by a user nor does it depend on the RACF password expire warn value being set in SETROPTS.

It should be noted that after the initial UserId password expiry check, the notification process will trigger each subsequent day at 00:15AM.

6.4 Notifying ALL Users not Previously Defined for Notification

Optionally, in V2R3 Systems, where the WORKATTR field WAEMAIL is populated, all users not specifically defined for Expire Notification may be included in the Notification Process, at intervals of 0,1,2,3,7,14 days prior to expiration, by using the ".DEFAULT" PSWDEXP ACTION BLOCK set, shown below:

```
ACTION PSWDEXP(.DEFAULT) METHOD(ESMEMAIL)
EXPINTERVAL (1,2,3,7,14)
EXCLUDE userid
EXCLUDE (userid1,userid2,userid3,...,useridn)
ACTION END.
```

Of course, it is possible that some user in such a far-reaching population as the RACF Environment would need to be excluded from such notification. Accomplish this by using the EXCLUDE Control Card either singularly or in sets by UserIds.

For non-V2R3 systems, or when desirable to define Expiration by UserId, use the following Control Card set.

```
ACTION PSWDEXP(user_id) METHOD(ESMEMAIL) OBJ(ALL) SCOPE(REPORT)
SUBJECT 'Expire Notification'
FROM CORPORATE
EXPINTERVAL (1,2,3,7,14)
TO PAT
ALIAS 'TIME TO ACT'
DOMAIN @COMPANY.COM
ACTION END.
```

6.5 Master ICE Address Space (IFOM) Setup in NSEPRMxx

The Expire Notification Task is initiated by the TASK=NEZUOPTS control card in NSEPRMxx:

```
TASK= NEZUOPTS
```

This control card should be specified in the BEGINPARALLEL section of the NSEPRMxx ICE Parmlib Member.

6.6 Password Expire Event Log Record:

When a password expire event is detected, a Log Record is created and stored in the ICE Event Log using the Record Identifier of "PE".

6.6.1 Expire Notification – Password will expired

```
01C|-SRC: EXPCHECK-------------THE CONTROL EDITOR------------ ExpiryNotify -
02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:********    TM:07:20:07 DT:01/14/18
03C|-PSWDEXP: SAM COOK--------------------------Password expires in 1 day---
```

6.6.2 Expire Notification – Password has expired

```
01C|-SRC: EXPCHECK-------------THE CONTROL EDITOR------------ ExpiryNotify -
02C|SYSPLX:ADCDPL SYSNM:ESSD6 USRID:START2 TM:12:39:30 DT:01/16/18
03C|-PSWDEXP: PST1300---Password expired today------------------------------
```

6.7 ICE/PSWD Expire Notification – Control Settings Panel

The panel shows the current Password Expire Notification configuration for the noted UserId. Notice of pending password expiration will be sent on the day(s) prior to expiration defined in 'Interval'. The Interval may be "ZERO" or one day or several days depending on specific circumstances. For example, for one Interval might = Interval 9; meaning nine days prior to expiration. Or Interval might = Interval 0,1,3,5,10,15; meaning start sending fifteen days prior to expiration and again 10, five, three, and one day prior, and then for the last time on the day of expiration.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊               ICE 18.0 - Expire Notice Rule Details                      ◊
◊             Selected NoticeId GBAGS1   /. Allow Updates                   ◊
◊                                                                          ◊
◊        To:           /. GHB@COMPANY.COM                                  ◊
◊        Alias:        /. JANE SMITH                                       ◊
◊        Subject:      /. EXPIRATION_NOTICE                                ◊
◊        Intervals:    /. 1,2,3,5,10,15                                    ◊
◊        From:         /. CAT@COMPANY.COM                                  ◊
◊        Domain:       ..                                                  ◊
◊        EMailDebug:   /. ON           JrlPost: /. OFF                     ◊
◊                                                                          ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return           ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return               ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- TO: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- Intervals: - The notice interval(s) - Days before expiration.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal.

For a definition of each field, cursor into the field and press enter.

6.8 ICE/PSWD Expire Notification – ACTION Block

```
ACTION PSWDEXP(GBAGS1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
TO GHB@COMPANY.COM
ALIAS 'JANE SMITH'
SUBJECT 'EXPIRATION_NOTICE'
INTERVAL (1,2,3,5,10,15)
FROM CAT@COMPANY.COM
DEBUG ON
JRLPOST OFF
ACTION .END
```

6.9 ICE/PSWD Expire Notification – Messages

The following are snippets of Expiration Messages. After the very last day in the notification series of days no additional messages will be sent.

```
Password expired today------

Password expires in 1 day---

Password expires in n days--
```

7 Enforcement of RACF Password Format Rules

Insisting on stronger passwords for all users and processes will help to improve overall credential integrity. However, enforcing syntax format standards can be tricky to implement, given that not all users have equal system privileges.

7.1 An Introduction to RACF Password Processing

RACF Password Syntax Rules are specified by RACF Commands and appear in the SETROPTS Listing. They can vary from the very simple to incredibly complex, specifying exactly which character type must appear in a particular position in the password. Your Security Administrator can specify up to eight password rules.

These are examples of a progression of complexity using actual RACF Command sequence/syntax to set Syntax Format requirements for Rules 1, 2 and 3:

For Rule1:

```
PASSWORD(RULE1(LENGTH(6:8)
ALPHANUM(1,2,3,4,5,6,7,8)))
```

For Rule2:

```
PASSWORD(RULE2(LENGTH(5:8)
CONSONANT(1)
MIXEDCONSONANT(2)
MIXEDVOWEL(3)
VOWEL(4)
ALPHANUM(5)
NUMERIC(6)
NOVOWEL(7) ALPHA(8)))
```

For Rule3:

```
PASSWORD(RULE3(LENGTH(7)
CONSONANT(1)
ALPHANUM(2)
VOWEL(3)
MIXEDVOWEL(4)
ALPHANUM(5)
MIXEDCONSONANT(6) NOVOWEL(7)))
```

In these cases, the result is a set of Password Syntax Rules that range from the very simple, Rule1, to the more complex, Rule2 and Rule3. When taken together, with other Password Processing Options, these rules form the basis for the creation and enforcement of the individual users' UserId/Password IBM Z access credential. Shown below is the password section, extracted from the standard SETROPTS Report:

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS LEGACY
  PASSWORD CHANGE INTERVAL IS  45 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   3 DAYS.
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT.
  SPECIAL CHARACTERS ARE ALLOWED.
  PASSWORD HISTORY BEING MAINTAINED 5.
  USERIDS BEING AUTOMATICALLY REVOKED.
  PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED 6 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
  RULE 1  LENGTH(6:8)   LLLLLLLL
  RULE 2  LENGTH(5:8)   CcvV$NWA
  RULE 3  LENGTH(7)     A*Vv$cs
```

It should be clear from this illustration that the individual RACF Syntax Rules can vary greatly from one RACF installation to any other. If you have the appropriate access credential and access to a TSO Session, you can access the SETROPTS by issuing one of the following commands:

SETR LIST or from ISPF enter on the command line *TSO SETR LIST*.

Once the RACF Syntax Rules are in place and understood, individual users select/create new passwords as their existing ones expire. Which Syntax Rule they select, in the creation of a new password, is totally up to them. They may select something simple, for example, Rule1 as outlined above, or something more complex, like Rule2 or Rule3. Most importantly, the user must only satisfy ONE of the defined password rules for the new password to be allowed.

7.2 Syntax Flexibility May Lead to System Vulnerability

While this flexibility to select from the available Syntax Rules might lead to stronger individual passwords, it is a common concern that users might either be instructed to use, or drift toward, the simplest Syntax Rule, often because it's just easier. Considering the average user, those with limited system resource access, this may not result in a loss of system integrity, when viewed within the context of the applied RACF Security Controls, taken as a whole.

However, when specifically considering highly privileged users, it is possible that system vulnerabilities may emerge, with each passing password update/reset, as nothing limits the described flexibility to individual users, nor does any process bind privileged users to a specific, more complex Syntax Rule.

While Highly Privileged Access users are more aware of their place in the general security paradigm, we are, as they say, only human.

7.3 Binding a UserId or GroupId to One or More Syntax Rule

Using ICE/PSWD, you can specify which password rules individual, Groups, or Users must meet. In order to bind a GroupId or UserId to one or more Password Syntax Rules, you can do the following:

In the ICE Parmlib Menber NSEPWRxx, enter one or more of the following Control Cards:

```
RACFGRP racfgrp RULES(rule1,rule2,...,rule8)
USERID  userid  RULES(rule1,rule2,...,rule8)
TCEGRP  tcegrp  RULES(rule1,rule2,...,rule8)
```

where “RACFGRP” specifies an established RACF GroupId, “USERID” is a defined RACF UserId, and “TCEGRP” is an established Integrity Controls Environment/TCE GroupId.

The RULES sub-parameter is used to bind the specified RACFGRP, USERID, or TCEGRP to a set of one or more (up to eight) Syntax Format Rules.

When more than one RULE is defined for a user, the RULEs are matched in numerical order with RULE01 processed first, RULE02 second and so on through RULE08 regardless of the order they appear in the Control Card rule set.

7.4 How Binding Processes a Password Update/Reset

If one of the Syntax Rules specified in NSEPWRxx for a RACFGRP, USERID or TCEGRP exists in the available RACF rule set, and if the user enters a password value that doesn't match one of those specified rules, the password is rejected, and the user is re-prompted to try a different new password.

If none of the Syntax Rules specified for a RACFGRP, USERID, or TCEGRP in NSEPWRxx are defined in RACF, then the password Syntax Rule enforcement process defaults to normal RACF syntax rule checking. This failsafe method of processing Password Updates/Resets ensures that a user is never “Locked Out” from the system.

If OTP Control and Rule Binding are both in place for a user, Rule Binding is validated before the OTP Controls are applied thus preventing OTP Email from

being sent before a valid password format has been applied to the new password, during the update/reset process.

7.5 Binding Users Not Specifically Defined in NSEPWRxx

Optionally, all users not specifically defined by RACFGRP, USERID, or TCEGRP may be bound to one or more Syntax Rules using the ".DEFAULT" Control Card shown below:

```
USERID .DEFAULT RULES(rule1,rule2,...,rule8)
```

7.5.1 How .DEFAULT Processes a Rule

The USERID keyword is used in conjunction with the USERID sub-parameter value ".DEFAULT" and defines the rules to be used for all users not previously defined. If no Groups or Users were previously defined, this single Control Card would enforce the named Syntax Rules for ALL users.

If the user falls into no specifically defined rule entry, and a "USERID .DEFAULT" rule entry is present, where at least one of the rules in that entry definition is defined to RACF, the password value must meet the defined RACF password rule, or a password change will be denied.

If none of the rules specified in the ".DEFAULT" entry is defined in RACF, then the password Syntax Rule enforcement process defaults to normal RACF password syntax checking. This failsafe method of processing Password Updates/Resets ensures that a user is never "Locked Out" from the system.

The placement of the "USERID .DEFAULT" control card within the Action Block is not critical. It will only be used if there is no other specific control card valid for a UserId.

7.5.2 Matching a User to a Rule

To determine if a valid RULE definition exists for a UserId, the process is as follows.

1. If a matching USERID control card is found for a UserId, that RULE is set and will be used.

2. If no USERID control card exists but the UserId is connected to a RACF group for which a RACFGRP control card has been defined, then the RACFGRP RULE is set and will be used.

3. If no USERID control card exists and the user is not connected to any defined RACFGRP, but the UserId has been assigned to a TCEGRP that has a defined RULE, then that RULE is set and will be used.

4. If the user has not fallen into any of the possible USERID, RACFGRP, or TCEGRP RULE sets, then the .DEFAULT RULE set, if it exists, will be applied.

7.6 User Failed to Match any NSEPWRxx Defined Rule

A Change/Reset Failure is triggered if NSEPWRxx has a defined RULES() set that contains at least one valid, defined RACF rule, but the password that was entered does not conform to at least one of those rules.

In such a case, a log record is written with 'RF' identifier to indicate that at least one of the specified RULES is active, in both NSEPWRxx and SETROPTS, and that the password used, in an attempted password reset, does not meet any of the rule(s).

7.7 Defined NSEPWRxx Rule Fail to Match SETROPTS Rules

It is possible that Format Rules defined in NSEPWRxx will not match those that are currently defined and active within SETROPTS.

In such a case, if none of the RULES specified fail to match a single SETROPTS defined rule, a Log Record is created and written using the Record Identifier of "RX" as detailed in the next section.

7.8 Syntax Rule Exception – No Match in NSEPWRxx

To ensure that a user is never "Locked Out" from the system, when Syntax Rule Sets defined in NSEPWRxx do not contain Rule(1-8) definitions that match actual SETROPTS Syntax Rules(1-8), such conditions pass control of the Password Update/Change process directly back to RACF. This condition, referred to as a "Syntax Rule Exception", results in an 'RX' (Rule eXception) log record being written, and if external notification is enabled for the associated UserId, a Rule Exception external notification e-mail is sent.

7.9 Master ICE Address Space (IFOM) Setup in NSEPRMxx

In order for any of this to be activated within IFOM, the following control card must be specified in NSEPRMxx:

```
TASK=NEZSISSI                          /*  SUBSYSTEM MANAGER   */
```

This control card should be specified in the BEGINPARALLEL section.

7.10 NEZPWX01 and NEZRIX02 are Required Modules

The NEZPWX01 and NEZRIX02 load modules that get created with the IFOM install process need to be moved into an active system LPA dataset and renamed to ICHPWX01 and ICHRIX02, respectively, and the system IPLed, to activate these modules as RACF exits.

NEZPWX01 is IFOM's ICHPWX01 new password exit module for capturing password change events. It is activated whenever a new password reset event is triggered. When it is invoked by RACF, it determines if the IFOM subsystem is active. If it is, it sends a function request to the IFOM new password subsystem function routine, waits until that request returns, and then triggers notification of a new password event through to IFOM. In addition, this exit controls RACF password rule enforcement.

7.11 Password Format Rule Event Log Records

When a password format failure event is detected, a Log Record is created and stored in the ICE Event Log using the Record Identifier of “RF”. If a Rule Exception is detected, the Record Identifier will be “RX”.

7.12 ICE/PSWD Format Rule Binding – Control Settings Panel

Binding is a process that associates a specific UserId with one or more specific format rules. Binding provides a method that allows privileged users and system administrators to better guard their logon credentials with the more complex Rules. To bind the select User/Group to a rule, enter the TYPE of binding; USR|RCF|TCE. Next, check '/' one or more of the valid Rules, enter 'S', and press enter. UnCheck to remove or enter 'D' to delete UserId Binding.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Password Rule Binding - Update                 ◊
◊                                                                          ◊
◊            Selected NoticeId USR : MFITZ1__ /. Allow Updates             ◊
◊                                                                          ◊
◊  --------------------Valid Password Format Rules--------------------     ◊
◊  /. 6:8(LLLLLLLL) /. 5:8(CcvV$NWA) /. 7:7(A*Vv$cs ) .. -:-(--------)     ◊
◊  .. -:-(--------) .. -:-(--------) .. -:-(--------) .. -:-(--------)     ◊
◊                                                                          ◊
◊     Update Enter 'S' > .. Delete Enter 'D' > .. Then Press Return        ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊           Updates Not Allowed Enter 'R' > .. > Press Return              ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

7.13 ICE/PSWD Format Rule Binding – ACTION Block

```
USERID MFITZ1 RULES(RULE1,RULE2,RULE3)
```

7.13.1 NSEPWRxx ACTION BLOCK Types

- USR - USERID
- RCF - RACFGRP
- TCE - TCEGRP

8 Implementing Enhanced (OTP) Password Change

Enhanced Password Change/Reset Control requires a user who changes a password to complete an additional authentication step. First, the user attempts a normal password reset. Next, ICE/PSWD generates a time-sensitive, One-Time Password (OTP) value that is sent to the user via email or SMS text. In an accompanying message, the user is instructed to return to the originating system, within the specific time window, to attempt a logon and retry. To accomplish this, the user will need to enter both the current password and the OTP value as a new password value (with confirmation). If this is completed successfully, the user's password reset will be completed.

The ICE System Administrator can specify how many times a user can attempt to enter the current password and supplied OTP value. If the user exceeds this retry value, the related OTP value is purged from active status. In such a case, the UserId may be automatically revoked. If the UserId is not automatically revoked, the user would be required to begin the process anew.

8.1 An Introduction to One Time Password (OTP) Changes

When used this Password Change/Reset Control will require user education as it will alter the way users Change/Reset their passwords. Users bound to this process will need to:

- Be active Email or SMS users.
- Return to the originating system to complete the Change/Reset.
- Select the Password Reset Option (again).
- Enter the OTP Value as the New Password and
- Confirm the OTP Value.

If these steps are followed, the "New Password" entered at the start of the Change/Reset process will be confirmed, become their new password and the user will be logged on successfully. Should they fail to enter the OTP value, or confirm it incorrectly, the password Change/Reset will fail. They may try again up to the RETRY Limit which, if exceeded, could result in their UserId being revoked.

8.1.1 TIMEWINDOW (mm:ss)

TIMEWINDOW control card is found within the OTPNOTFY ACTION block.

This specifies the length of time from the initial password reset attempt that the user must return to the system and enter their current password and the OTP value as the new password entry for the password change to be completed.

If nothing is specified, the default value is set to 15:00 minutes. The maximum value is 15:00 minutes, while the lowest allowable value is 00:30 seconds.

TIMEWINDOW(10:00)

8.1.2 TERMINALMSG (TRMMSG)

TERMINALMSG control card is found within the OTPNOTFY ACTION block.

TERMINALMSG ON|OFF

If TERMINALMSG is ON, the following will appear on the User Terminal.

A request to reset a password or phrase value has been intercepted. You will receive an e-mail that will supply a one-time use OTP value which you will be entered during your next logon and password or phrase reset attempt. The OTP value you receive will be used as a new password or phrase value and will be Required at your next logon/reset. Remember that value. Your next logon/reset attempt must be completed by 13:32:03. If that time expires, the one-time use OTP value will no longer be valid.

8.1.3 RETRYLIMIT(n)

RETRYLIMIT control card is found within the OTPNOTFY ACTION block.

This specifies how many attempts the user has to enter the OTP value and new password correctly within the specified time period.

If nothing is specified, the default value is set to 5 password reset attempts. The maximum value is 9 attempts, while the lowest allowable value is 0 attempts.

RETRYLIMIT 7

8.1.4 ONLIMIT(REVOKE)

An optional extension to the RETRYLIMIT allows for the User's Logon Id to be Revoked if the retry limit is reached.

RETRYLIMIT 7 ONLIMIT(REVOKE)

8.1.5 OTPACTIVE

OTPACTIVE is an optional extension of OTP control over the OTP Logon/Password Reset process. It operates only within the OTP TIMEWINDOW and when set to FAIL will prevent a user from bypassing the completion of an OTP Password Reset.

OTPACTIVE LOGON(FAIL|NOFAIL) – Default NOFAIL

8.1.6 OTP User Notification - One Time Password Token

```
01C|-SRC: LOGONRST-------------THE CONTROL EDITOR--------------- OTPNotify -
02C|SYSPLX:ADCDPL SYSNM:ESSD6 USRID:MTECH3 TM:15:29:37 DT:02/07/18
03C|-OTPNOTIFY: MTECH3-----------------------------------------------------
To complete the reset request, logon to the system of record prior
to 15:35:14 system time using OTP new value OTPWWWBSsdL9Qn

01C|-SRC: LOGONRST-------------THE CONTROL EDITOR--------------- OTPNotify -
02C|SYSPLX:ADCDPL SYSNM:ESSD6 USRID:MTECH3 TM:16:34:11 DT:01/27/18
03C|-OTPNOTIFY: MTECH3-----------------------------------------------------
To complete the reset request, logon to the system of record prior
to 16:39:48 system time using OTP new value NRrWqw7E
```

This condition results in an 'ON' (OTP Notice) log record being written.

EXCEPTION: OTPACTIVE LOGON(FAIL) should be used with caution in logon scenarios under the control of - CL/Supersession (and other similar Session Managers) or when the IKJTSO00 PARM PASSWORDPREPROMPT is set 'ON'- where password reset operations are preceded with old password pre-validation operations. If in doubt about your installation settings contact NewEra Technical Support, support@newera.com, for assistance.

8.1.7 OTP User Notification - Token Expiration

```
01C|-SRC: LOGONEXP-------------THE CONTROL EDITOR--------------- OTPExpire -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:MTECH3      TM:14:24:43 DT:01/01/18
03C|-OTPEXPIR: MTECH3-----------------------------------------------------
The time window to complete the OTP password reset operation expired.
```

This condition results in an 'OE' (OTP Expired) log record being written.

8.1.8 OTP User Notification - Token Logon Retry

```
01C|-SRC: LOGONRET-------------THE CONTROL EDITOR---------------- OTPRetry -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:MTECH3      TM:14:24:43 DT:01/01/18
03C|-OTPRETRY: MTECH3-----------------------------------------------------
An invalid OTP value was entered for a password reset operation.  Confirm
valid OTP value from prior e-mail.
```

This condition results in an 'OR' (OTP Retry) log record being written.

8.1.9 OTP User Notification - Token Logon Failed

```
01C|-SRC: LOGONTRM-------------THE CONTROL EDITOR----------------- OTPFail -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:MTECH3      TM:14:24:43 DT:01/01/18
03C|-OTPFAILD: MTECH3-------------------------------------------------------
The OTP password reset operation is terminated due to invalid OTP value.
```

This condition results in an 'OE' (OTP Failed) log record being written.

8.1.10 OTP User Notification – Bad OTP Token Used

```
01C|-SRC: RESETTRM-------------THE CONTROL EDITOR--------------- OTPBadnew -
02C|SYSPLX:ADCDPL SYSNM:ADCD22B USRID:PHARL2 TM:12:24:08 DT:02/09/18
03C|-OTPBADNEW: PHARL2 ------------------------------------------------
-----------------------------------EVENT DATA-----------------------------------
A new phrase value that will fail RACF phrase syntax checks was specified.
The current logon was terminated and the active OTP event was purged.
```

This condition results in an 'OB' (OTP Bad) log record being written.

8.2 Logging On When an OTP Event is Pending

OTP processing does not in any way prevent a user from logging on, even when an OTP password reset is in progress. To do this, a user would simply use their old password, if it remains valid, and, if necessary, bypass the password reset process altogether. Under such a circumstance, the following TSO or IFOS message will be displayed before the READY prompt.

```
OTP event in progress. Complete pwd reset with OTP value by hh:mm:ss.
```

Where hh:mm:ss represents the termination of the TIMEINDOW first reported to the user, at the origin of the OTP process.

8.3 ICE/PSWD One Time Password – Control Settings Panel

The panel shows the One-Time Password (OTP) configuration for the noted UserId. UserIds attempting a password Change/Reset will be failed, pending receipt of the OTP Token and their return to the originating system to retry the Change/Reset using the Token within the Time & Retry Limit.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - OTP Password Change Controls                 ◊
◊              Selected NoticeId TAPIA1   /. Allow Updates                ◊
◊                                                                        ◊
◊        To:           /. BOB                                            ◊
◊        Alias:        /. SAM SMITH                                      ◊
◊        Subject:      /. UNDER OTP CONTROL                              ◊
◊        TimeWindow:   /. 05:00                                          ◊
◊        TerminalMsg:  /. YES                                            ◊
◊        ResetLimit:   /. 3                                              ◊
◊        OnLimit:      /. REVOKE                                         ◊
◊        From:         /. SUPPORT                                        ◊
◊        Domain:       /. @CORPORATE.COM                                 ◊
◊        EMailDebug:   /. ON           JrlPost: /. NO                    ◊
◊                                                                        ◊
◊      Update Enter 'S' > .. Delete Enter 'D' > .. > Press Return        ◊
◊──────────────────────────────────────────────────────────────────────────◊
◊──────────────────────────────────────────────────────────────────────────◊
◊          Updates Not Allowed Enter 'R' > .. > Press Return             ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

Users that access their Service Accounts and this Service Element may see a different view if the ICE/PSWD Administrator has denied them update. When update is denied, the user may view the configuration and return to the Full-Service Account panel.

Configuration Options Include:

- To: - The full email or prefix - part before the '@'.
- Copy: - The full email or prefix - of copy recipient.
- Alias: - A character value to mask the actual UserId.
- Subject: - The subject of the Email - be specific.
- OTPActive - If set FAIL user cannot bypass OTP Logon/Reset Control

- TimeWindow: - Time to respond before OTP Expires - mm:ss
- TerminalMsg: - If Default OTP Instruction is to be used - ON|OFF.
- ResetLimit: - Number failed reset attempts before restart needed.
- OnLimit: - Set REVOKE if UserId to be revoked if Limit reached.
- From: - The full email or prefix - of sender.
- Domain: - Takes the form of @xxxxx.xxx - Required with prefix.
- ExcludeId: - Used with .DOMAIN to exclude certain UserId.
- EMailDebug: - Set ON|OFF|NULL when needed for Debugging Email.
- JrlPost: - Set ON|OFF|NULL for Posting to the Control Journal

For a definition of each field, cursor into the field and press enter.

8.4 ICE/PSWD One Time Password – ACTION Block

```
ACTION PSWDOTP(PROBI1) METHOD(EMAIL) SCOPE(REPORT)
DOMAIN @CORPORATE.COM
TO BOB
ALIAS 'SAM SMITH'
SUBJECT 'UNDER OTP CONTROL'
TIMEWINDOW 05:00
RETRYLIMIT 3 ONLIMIT(REVOKE)
TERMMSG ON
FROM SUPPORT
DEBUG ON
JRLPOST NO
ACTION .END
```

9 ICE/PSWD ADMIN & USER Interval Reporting:

ICE/PSWD supports the distribution of Targeted Interval Reports to ICE Administration - ADMIN – and individual users defined within the scope of ICE Control Boundaries – USERs.

9.1 Setting the ADMIN Event Activity Reporting - Intervals

The panel shown below is used exclusively by ICE Administration to activate and define – Report Type, Content and Interval(s) - for both ADMIN and USERs by setting the controls shown below the `"----ICE/PSWD Periodic Background Reporting----"` panel heading. The controls above are used to access stored Activity Events and will be explained separately.

```
          NSIMDSM 0103    ICE 18.0 - Enriching RACF Controls - ADCDPL

  .. UserLogons  .. UserPswCng  .. PswdExpire  .. FormatRule  .. OTPControl
  .. ___0 __518  .. ___0 ____0  .. ___0 ____0  .. ___0 ____0  .. ___0 ____0
  .. ManageCngs  .. CmmdUpdate  .. SubmitJobs  .. OtherEvent  .. EveryEvent
  .. ___0 ____7  .. ___0 ____3  .. ___0 ____0  .. ___0 ____0  .. ___0 __528

------------------ICE/PSWD Periodic Background Reporting-------------------

 ---------Admin Report Cycle-------- | ----------User Report Cycle--------
 /. Activate /. Summary /. CngOnly   |  /. Activate /. Summary /. CngOnly
                                     |
 /. Day - 00 00 - 12 Hour Interval   |  /. Day - 00 00 - 24 Hour Interval
       24hh mm   1|2|4|6|8|12|24     |        24hh mm   1|2|4|6|8|12|24
 /. Wks - 00 00 - MON_____________   |  /. Wks - 00 00 - SUN_____________
       24hh mm   SUN,MON,TUE,Etc.    |        24hh mm   SUN,MON,TUE,Etc.
 /. Mth - 00 00 - 1,2_____________   |  /. Mth - 00 00 - 1,2_____________
       24hh mm   Day:1,2,9,25,EOM    |        24hh mm   Day:1,2,9,25,EOM
 /. Pre PAT_____________________     |  /. Pre PRR_____________________
    Dom @COMPANY_________________    |     Dom @COMPANY_________________
    Email Admin Reports TO Address   |     Copy Users' Reports TO Address

                        .. Update Reporting Cycle
```

9.2 Setting the ADMIN Event Activity Reporting – Action Block

To create and send the ADMIN Interval Report, check "/." to Activate the process. To suspend all ADMIN Interval Reporting, UnCheck and Update. Reports may be created and sent Daily, Weekly, and Monthly by Checking the related controls. Each has its own unique 24 hour start time and interval specification. The ADMIN recipient Email Address is split between "Pre" and "Dom". "Pre" (Prefix) should contain only that portion of the Email Address up to, but not including, the "@". "Dom" (Domain) should contain that portion of the Email Address beginning with the "@" and continuing to the end.

Settings that control the Interval(s) are found in the ICE Parmlib Member, NSEDETxx. These are updated automatically to reflect panel settings whenever Update is selected. A sample of typical NSEDETxx setting follows.

9.2.1 To Control ADMIN Reporting Intervals – NSEDETxx

```
PCMONREPDAY ON
PCMONREPDAY CYCLE(DAILY) TIME(01:10) INTERVAL(24)

PCMONREPWKS ON
PCMONREPWKS CYCLE(WEEKLY(SUN)) TIME(02:20)

PCMONREPMTH ON
PCMONREPMTH CYCLE(MONTHLY(1,2)) TIME(03:30)
```

9.2.2 To Control USER Report Distribution – NSEENSxx

```
ACTION DETECTOR(PCMONREPDAY)
TO PAT@COMPANY.COM
ACTION .END

ACTION DETECTOR(PCMONREPWKS)
TO CAT@COMPANY.COM
ACTION .END

ACTION DETECTOR(PCMONREPMTH)
TO CAT@COMPANY.COM
ACTION .END
```

9.3 ICE/PSWD ADMIN Interval Reporting - Applications

Admin Interval Reporting is performed, as scheduled Daily and/or Weekly and/or Monthly by the three separate applications described below. Each application maintains an INDEX POINTER to the ICE Event Log, by interval, to the last event reported. At each subsequent interval, only those events that occurred after that last event, if any, are reported or not reported depending on the user's individual 'CngOnly' setting.

9.3.1 PCMONREPDAY - NSIMPCD Application

Classifies Events by Day, builds and distributes resulting reports to the ADMIN recipient Email Address defined in the Admin Report Cycle section of the Panel.

9.3.2 PCMONREPWKS - NSIMPCW Application

Classifies Events by Week, builds and distributes resulting reports to the ADMIN recipient Email Address defined in the Admin Report Cycle section of the Panel.

9.3.3 PCMONREPMTH - NSIMPCM Application

Classifies Events by Month, builds and distributes resulting reports to the ADMIN recipient Email Address defined in the Admin Report Cycle section of the Panel.

9.4 ICE/PSWD ADMIN Interval Reporting – Sample

The ADMIN Report may be in either Summary or Detail Format depending on the 'Summary' setting. The report shown below is a Daily Summary Report. @ADMIN@ is the default UserId associated with ADMIN Report Creation.

```
TCE0000I ICE/PWSD ACTIVITY EVENT DETECTOR - ICE 18.0 - NSIMPCD P1 - M01/D04/Y18
TCE0000I  EXECUTING ON SYSTEM - ADCD22B - AGAINST TARGET USERID - @ADMINS@
TCE0000I  REPORT IS DATED - 2021/01/06 - AT TIME - 07:29:40
|
TCE0000I ICE/PSWD EVENT ACTIVITY SUMMARY:
|
TCE0000I +-------------------------------------------------------------------------+
TCE0000I |               Recent Daily Trends in ICE/PSWD Activity                  |
TCE0000I +---------------------+---------------------------------------------------+
TCE0000I |     SMFID:ADCD      |    INTERVAL DATES, TIMES, ELEMENT ALERTS          |
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |        DATES        |01/06|01/06|01/05|01/05|01/05|01/05|01/05|01/05|
TCE0000I |        TIMES        |07:29|00:00|15:44|15:44|15:37|15:37|15:36|15:23|
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |        TOTAL        |   8 |   7 |   0 |   1 |   1 |   0 |   1 |   1 |
TCE0000I +--Integrity_element--+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |     UserLogons      |   7 |   1 |   0 |   1 |   1 |   0 |   1 |   1 |
TCE0000I |     UserPswCng      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     PswdExpire      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     FormatRule      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     OTPControl      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     ManageEdit      |   1 |   1 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     CmmdUpdate      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     SubmitJobs      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     OtherEvent      |   0 |   5 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
|
TCE0000I ICE/PWSE EVENT RECORDS:
|
| Row yy/mm/dd hh:mm -UserId- Event -Origin- ------PSWD Event Descriptions------
| --- -------- ----- -------- ----- -------- ----------------------------------
| 001 21/01/06 05:59 PATS01 LOGON STC05588 00_Password_or_phrase_is_authorized
| 002 21/01/06 06:00 PATS02 LOGON TSOLOGON 00_Password_or_phrase_is_authorized
| 003 21/01/06 06:41 BOBY01 LOGON STC05591 00_Password_or_phrase_is_authorized
| 004 21/01/06 06:41 USER02 LFAIL STC05592 04_Password_or_phrase_not_authorize
| 005 21/01/06 07:00 EDITS NSEENSSA IFO.TEST.PARMLIB/B2WRKD
| 006 21/01/06 07:07 USER01 LOGON STC05591 00_Password_or_phrase_is_authorized
| 007 21/01/06 07:16 USER02 LOGON STC05591 00_Password_or_phrase_is_authorized
| 008 21/01/06 07:26 TOMY02 LOGON STC05591 00_Password_or_phrase_is_authorized|
TCE0000I END EVENT RECORDS:
|
/*************************************************************************/
/*              RPTDSN:IFO.TEST.$PSW.@ADMINS@.DAYWKS($$DAYIN1)             */
/*************************************************************************/
|     NewEra Software, Inc.
|         Our Job? Help you avoid problems and improve z/OS integrity.
****************************** Bottom of Data ******************************
```

9.5 ICE/PSWD ADMIN Settings Change Report - Sample

9.6 Setting A USER Event Activity Report Model - Interval

To create and send USER Interval Reports, it is first necessary for the ICE Administrator to build a generic reporting model that will be used as the settings default for ALL users. The second step is to modify the model to fit the specific needs of the individual users and to target their individual email addresses.

To create an Interval Report Model, check "/." Activate in the User Report Cycle section of the ADMIN panel. To suspend all USER Interval Reporting, UnCheck and Update. Report MODEL/Defaults may be created to send Daily, Weekly, and Monthly by Checking the related control. Each has its own unique 24 hour start time and interval specification. The Default Recipient Email Address is split between "Pre" and "Dom". "Pre" (Prefix) should contain only that portion of the Email Address up to, but not including, the "@". "Dom" (Domain) should contain that portion of the Email Address beginning with the "@" and continuing to the end.

Settings that control the Interval(s) are found in the ICE Parmlib Member, NSEDETxx. These are updated automatically to reflect panel settings whenever Update is selected. A sample of typical NSEDETxx setting follow.

9.6.1 To Control USER Reporting Intervals - NSEDETxx

```
PSWDRPTSDAY ON
PSWDRPTSDAY CYCLE(DAILY) TIME(01:10) INTERVAL(24)

PSWDRPTSWKS ON
PSWDRPTSWKS CYCLE(WEEKLY(SUN)) TIME(02:20)

PSWDRPTSMTH ON
PSWDRPTSMTH CYCLE(MONTHLY(1,2)) TIME(03:30)
```

9.7 Modifying A USER Event Activity Report Model/Default

This panel can be accessed by both the ICE Administrator and a User with a defined ICE/PSWD UserId. Users will see a slightly different layout depending on whether, or not, the ICE Administrator will allow the user to update the Report Cycle Settings – Activate, Summary, CngOnly, Day, Wks, Mth, Pre and Dom. The Actual interval settings – Time and Interval – cannot be updated. If the user is not authorized to update the settings, the "Update Service Account" will be automatically removed.

Selections that appear above the "----ICE/PSWD Periodic Background Reporting----" panel heading provide access to the individual elements of a user's Service Account. Those that appear under the heading "---Event Worksheets---" show, by Service Element, recent and total Activity Events and provide a pathway to related Event Record Worksheets.

```
          NSIMDSM 0103    ICE 18.0 - Enriching RACF Controls - PHARL2

.. UserLogons  .. UserPswCng  .. PswdExpire  .. FormatRule  .. OTPControl
.. 2021/01/03  .. 2021/01/03  .. -NSEENSxx-  .. ----/--/--  .. 2021/01/03
     ADMIN2         ADMIN2         ______         ______         ADMIN2

-----------------ICE/PSWD Periodic Background Reporting------------------

 --------Event Worksheets-------- | ------User Report Cycle /. Allow----
   ---ICE/PSWD--- ---ICE/TCE---   |  /. Activate /. Summary /. CngOnly
   .. UserLogons  .. ManageEdit   |
   ..   32   518  ..    0     7   |  .. Day - 00 00 - 24 Hour Interval
   .. UserPswCng  .. CmmdUpdate   |         24hh mm   1|2|4|6|8|12|24
   ..    0     0  ..    0     3   |  .. Wks - 00 00 - SUN
   .. PswdExpire  .. SubmitJobs   |         24hh mm   SUN,MON,TUE,Etc.
   ..    0     0  ..    0     0   |  /. Mth - 00 00 - 1,2
   .. FormatRule  .. OtherEvent   |         24hh mm   Day:1,2,9,25,EOM
   ..    0     0  ..    0     0   |  /. Pre PAT_____________________
   .. OTPControl  .. EveryEvent   |     Dom @COMPANY_____________________
   ..    0     0  ..   32   528   |     Copy UserId Reports TO Address

      .. Your PSWD Access Token         .. Update Service Account
```

```
                    .. Your PSWD Access Token
```

9.7.1 ICE/PSWD NSEENSxx Background – ACTION Block

There is only one NSEENSxx Action Block controlling Report Distribution for all users. Each UserId is assigned to a TARGETUSER Control Card followed by the user's associated Email Address.

```
ACTION PSWDMON(PSWDRPTSDAY) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
TO AROBI1@COMPANY
TARGETUSER PROBI2
TO PROBI2@COMPANY
ACTION .END

ACTION PSWDMON(PSWDRPTSWKS) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
TO AROBI1@COMPANY
TARGETUSER PROBI2
TO PROBI2@COMPANY
TARGETUSER PROBI1
TO ABC@COMPANY
ACTION .END

ACTION PSWDMON(PSWDRPTSMTH) METHOD(EMAIL) SCOPE(REPORT)
TARGETUSER AROBI1
TO AROBI1@COMPANY
TARGETUSER PHARL2
TO CAT@COMPANY
TARGETUSER PROBI1
TO ABC@COMPANY
ACTION .END
```

9.8 ICE/PSWD USER Interval Reporting - Applications

User Interval Reporting is performed, as scheduled Daily and/or Weekly and/or Monthly by the three separate applications described below. Each application maintains an INDEX POINTER to the ICE Event Log, for each user, by interval to the last event reported. At each subsequent interval, only those events that occurred after that last event, if any, are reported or not reported depending on the user's individual 'CngOnly' setting.

9.8.1 PSWDRPTSDAY – NSIMPWD

Classifies Events by Day, builds and distributes resulting reports to the UserId defined on the 'DAY' TARGETUSER Control Card.

9.8.2 PSWDRPTSDAY – NSIMPWW

Classifies Events by Week, builds and distributes resulting reports to the UserId defined on the 'WKS' TARGETUSER Control Card.

9.8.3 PSWDRPTSDAY – NSIMPWM

Classifies Events by Month, builds and distributes resulting reports to the UserId defined on the 'MTH' TARGETUSER Control Card.

9.9 ICE/PSWD USER Interval Reporting – Sample

The USER Report may be in either Summary or Detail Format, depending on the 'Summary' setting. The report shown below is a Daily Summary Report. Events shown in the report are only for the noted UserId.

```
TCE0000I ICE/PWSD ACTIVITY EVENT DETECTOR - ICE 18.0 - NSIMPWD P1 - M01/D04/Y18
TCE0000I  EXECUTING ON SYSTEM - ADCD22B - AGAINST TARGET USERID - USER01
TCE0000I  REPORT IS DATED - 2021/01/06 - AT TIME - 07:29:19
|
TCE0000I ICE/PSWD EVENT ACTIVITY SUMMARY:
|
TCE0000I +-------------------------------------------------------------------------+
TCE0000I |               Recent Daily Trends in ICE/PSWD Activity                  |
TCE0000I +---------------------+---------------------------------------------------+
TCE0000I |     SMFID:ADCD      |    INTERVAL DATES, TIMES, ELEMENT ALERTS          |
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |        DATES        |01/06|01/05|01/05|01/05|01/05|01/05|01/05|01/05|
TCE0000I |        TIMES        |07:29|15:48|15:24|12:57|12:56|12:55|12:53|12:51|
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |        TOTAL        |   3 |  10 |  19 |   1 |   1 |   1 |   1 |   1 |
TCE0000I +--Integrity_element--+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I |     UserLogons      |   3 |   4 |   4 |   1 |   1 |   1 |   1 |   1 |
TCE0000I |     UserPswCng      |   0 |   0 |   1 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     PswdExpire      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     FormatRule      |   0 |   0 |   1 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     OTPControl      |   0 |   0 |   1 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     ManageEdit      |   0 |   2 |   6 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     CmmdUpdate      |   0 |   2 |   6 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     SubmitJobs      |   0 |   0 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I |     OtherEvent      |   0 |   2 |   0 |   0 |   0 |   0 |   0 |   0 |
TCE0000I +---------------------+-----+-----+-----+-----+-----+-----+-----+-----+
|
TCE0000I ICE/PWSE EVENT RECORDS:
|
| Row yy/mm/dd hh:mm -UserId- Event -Origin- ------PSWD Event Descriptions------
| --- -------- ----- -------- ----- -------- ----------------------------------
| 001 21/01/05 15:50   USER01 LOGON STC05542 00_Password_or_phrase_is_authorized
| 002 21/01/06 05:59   USER01 LOGON STC05588 00_Password_or_phrase_is_authorized
| 003 21/01/06 05:58   USER01 LFAIL STC05588 00_Password_or_phrase_not_authorize
|
TCE0000I END EVENT RECORDS:
|
/*************************************************************************/
/*               RPTDSN:IFO.TEST.$PSW.@PROBI1.DAYWKS($$DAYIN1)           */
/*************************************************************************/
|     NewEra Software, Inc.
|         Our Job? Help you avoid problems and improve z/OS integrity.
****************************** Bottom of Data ******************************
```

9.10 ICE/PSWD USER Settings Change Report – Sample

```
TCE0000I ICE/PWSD ACTIVITY EVENT DETECTOR - ICE 18.0 - NSIMPWM P1 - M01/D27/Y18
TCE0000I EXECUTING ON SYSTEM - ADCD22B - AGAINST TARGET USERID - PROBI1
TCE0000I REPORT IS DATED - 2021/01/28 - AT TIME - 15:08:56
|
TCE0000I ICE/PSWD SETTINGS CHANGE SUMMARY:
|
TCE0000I +-----------------------------------------------------------------+
TCE0000I | Recent Monthly Trends in ICE/PSWD Activity |
TCE0000I +--------------------+--------------------------------------------+
TCE0000I | SMFID:ADCD | INTERVAL DATES, TIMES, ELEMENT ALERTS |
TCE0000I +--------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I | DATES |01/28|01/28|01/28|--/--|--/--|--/--|--/--|--/--|--/--|
TCE0000I | TIMES |15:08|15:03|14:58|--:--|--:--|--:--|--:--|--:--|--:--|
TCE0000I +--------------------+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I | TOTAL | 7 | 1 | 2 | --- | --- | --- | --- | --- |
TCE0000I +--Integrity_element--+-----+-----+-----+-----+-----+-----+-----+-----+
TCE0000I | UserLogons | 1 | 0 | 0 | --- | --- | --- | --- | --- |
TCE0000I | UserPswCng | 1 | 5 | 0 | --- | --- | --- | --- | --- |
TCE0000I | PswdExpire | 1 | 0 | 0 | --- | --- | --- | --- | --- |
TCE0000I | FormatRule | 1 | 0 | 0 | --- | --- | --- | --- | --- |
TCE0000I | OTPControl | 1 | 0 | 1 | --- | --- | --- | --- | --- |
TCE0000I | AllSetting | 2 | 1 | 1 | --- | --- | --- | --- | --- |
TCE0000I +--------------------+-----+-----+-----+-----+-----+-----+-----+-----+
|
TCE0000I ICE/PWSE SETTING CHANGES:
|
ACTION REPTSETS(PROBI1) - Date:2021/01/28 Time:15:08:49 User:PROBI1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| REPORTING | NEWEVENT / | NEWEVENT |
| INTERVAL | DAYILY | DAYILY / |
+--------------+-------------------------------+-------------------------------+
ACTION PSWRULE(PROBI1) - Date:2021/01/28 Time:15:08:26 User:PROBI1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| RULE3 | 7:7(A*Vv$cs.) / | 7:7(A*Vv$cs.) |
ACTION PSWDEXP(PROBI1) - Date:2021/01/28 Time:15:08:15 User:PROBI1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVALS | 0,1,2,3,5,10,25 / | 0,1,2,3,5,10,30 / |
+--------------+-------------------------------+-------------------------------+
ACTION PSWDCHNG(PROBI1) - Date:2021/01/28 Time:15:08:00 User:PROBI1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| CC | PAT@NEWERA.COM | PAT@NEWERA.COM / |
| EMAILDEBUG | | ON / |
+--------------+-------------------------------+-------------------------------+
ACTION SYSLOGON(PROBI1) - Date:2021/01/28 Time:15:07:36 User:PROBI1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ALLOW | ALLOW - | ALLOW / |
| TO | PRR@NEWERA.COM - | PRR@NEWERA.COM / |
| CC | SYSSEC@NEWERA.COM - | SYSSEC@NEWERA.COM / |
| MSGBODY |REPORT SUSPICIOUS ACTIVITY TO SECURITY - |REPORT SUSPICIOUS ACTI
| ALIAS | HELPER BEE - | HELPER BEE / |
| SUBJECT | YOU JUST LOGGED ON - | YOU JUST LOGGED ON / |
| ACTIVE TIME | GREATERTHAN(00) - | GREATERTHAN(00) / |
| INACTIVE ON | - | |
| ACTIVE DAY | DAYS(SAT,SUN,MON,TUE) - | DAYS(SAT,SUN,MON,TUE) / |
| ACTIVE RC | - | |
| FROM | SUPPORT@NEWERA.COM - | SUPPORT@NEWERA.COM / |
| DOMAIN | - | |
| EMAILDEBUG | ON - | ON / |
| JRLPOST | - | |
+--------------+-------------------------------+-------------------------------+
|
TCE0000I END SETTINGS CHANGES:
|
/*******************************************************************************/
/* RPTDSN:IFO.TEST.$PSW.@PROBI1.MTHCHNGS($$MTHAN1) */
/*******************************************************************************/
| NewEra Software, Inc.
| Our Job? Help you avoid problems and improve z/OS integrity.
******************************** Bottom of Data ********************************
```

9.11 ICE/PSWD USER Settings File – Sample

The settings of each Service Account, configured by either the ICE Admin or the User, are recorded in the user's Settings File. The dataset holding these files is allocated automatically as a PDSE using the high-level qualifier assigned to ICE during installation and takes this form – HLQ.$PSW.USRSETS. Individual files, members, in this dataset are named using the user's assigned UserId. This dataset should be protected in a manner consistent with site security policy.

```
/*****************************************************************************/
/*                                                                           */
/* ICE/PSWD:Password Notice/Controls - Master Account Record - ADMIN1        */
/* Date:2021/01/27 - Time:13:59:19 - User:ADMIN1                             */
/*                                                                           */
/*****************************************************************************/
FMTRUL_UPUSR= ADMIN1
FMTRUL_UPDAT= 2021/01/26
FMTRUL_UPTIM= 16:37:55
FMTRUL_UPTYP= USR
FMTRUL_ALLOW= /
FMTRUL_RULE1= / 1:8(********)
FMTRUL_RULE2= - 5:8(CcvV$NWA)
FMTRUL_RULE3= / 7:7(A*Vv$cs.)
FMTRUL_RULE4= - -:-(--------)
FMTRUL_RULE5= - -:-(--------)
FMTRUL_RULE6= - -:-(--------)
FMTRUL_RULE7= - -:-(--------)
FMTRUL_RULE8= - -:-(--------)
SLOGON_UPUSR= ADMIN1
SLOGON_UPDAT= 2021/01/26
SLOGON_UPTIM= 16:45:41
SLOGON_ALLOW= /
SLOGON_CNGTO= / ABC@NEWERA.COM
SLOGON_CNGCC= / SYSSEC@NEWERA.COM
SLOGON_CNGMB= / REPORT_SUSPICIOUS_ACTIVITY_TO_SECURITY
SLOGON_CNGAL= / IS_THIS_YOU?
SLOGON_CNGSJ= / YOU_JUST_LOGGED_ON
SLOGON_CNGSE= -
SLOGON_CNGAT= / STM(0800)_ETM(2200)
SLOGON_CNGAD= / DAYS(SAT,SUN,MON,TUE)
SLOGON_CNGRC= / GREATERTHAN(00)
SLOGON_CNGFR= / SUPPORT@NEWERA.COM
SLOGON_CNGDM= -
SLOGON_CNGID= -
SLOGON_CNGDB= / ON
SLOGON_CNGJP= -
PSWOTP_UPUSR= ADMIN1
PSWOTP_UPDAT= 2021/01/26
PSWOTP_UPTIM= 17:26:39
PSWOTP_ALLOW= /
PSWOTP_OTPTO= / PRR
PSWOTP_OTPCC= / SUPPORT
PSWOTP_OTPAL= / TIME_TO_FINISH
PSWOTP_OTPSJ= / OPTSJ
PSWOTP_OTPTW= / 12:30
PSWOTP_OTPTM= / YES
PSWOTP_OTPRL= / 5
PSWOTP_OTPOL= / REVOKE
PSWOTP_OTPAC= / FAIL
PSWOTP_OTPFR= / PAT
PSWOTP_OTPDM= / @NEWERA.COM
PSWOTP_OTPID= -
PSWOTP_OTPDB= / ON
PSWOTP_OTPJP= / ON
PSWCNG_UPUSR= ADMIN1
PSWCNG_UPDAT= 2021/01/26
PSWCNG_UPTIM= 18:03:19
PSWCNG_ALLOW= /
```

```
PSWCNG_CNGTO= / ABC@NEWERA.COM
PSWCNG_CNGCC= -
PSWCNG_CNGMB= -
PSWCNG_CNGAL= -
PSWCNG_CNGSJ= / PASSWORD_CHANGE
PSWCNG_CNGSE= -
PSWCNG_CNGAT= -
PSWCNG_CNGAD= -
PSWCNG_CNGFR= / SUPPORT@NEWERA.COM
PSWCNG_CNGDM= -
PSWCNG_CNGID= -
PSWCNG_CNGDB= -
PSWCNG_CNGJP= -
EXPIRE_UPUSR= ADMIN1
EXPIRE_UPDAT= 2021/01/27
EXPIRE_UPTIM= 13:55:07
EXPIRE_ALLOW= /
EXPIRE_EXPTO= / ABC@NEWERA.COM
EXPIRE_EXPCC= / ABC@NEWERA.COM
EXPIRE_EXPAL= / MAYBE_TIME_TO_RESET
EXPIRE_EXPSJ= / EXPIRATION_NOTICE
EXPIRE_EXPIN= / 0,1,2,3,5,10,25
EXPIRE_EXPFR= / CAT@NEWERA.COM
EXPIRE_EXPDM= -
EXPIRE_EXPID= -
EXPIRE_EXPDB= -
EXPIRE_EXPJP= -
USRSET_UPUSR= ADMIN1
USRSET_UPDAT= 2021/01/27
USRSET_UPTIM= 13:59:19
USRSET_USRTK= -
USRSET_LSLOG= 2018027_10.50.56.44
USRSET_FGACT= USRSET_FGACT
USRSET_BGDAY= USRSET_BGDAY
USRSET_BGWKS= USRSET_BGWKS
USRSET_BGMTH= ACTION_REPTSETS(ADMIN1)_-_Date:2021/01/27_Time:13:59:22_User:PROBI
USRSET_LSDAY= 2018028_07.35.48.87
USRSET_LSWKS= -
USRSET_LSMTH= 2018028_07.35.48.87
USRSET_SETLL= /
USRSET_SETUA= /
USRSET_SETAU= /
USRSET_SETCU= /
USRSET_SETDU= /
USRSET_SETWU= /
USRSET_SETMU= /
USRSET_SETEU= /
USRSET_SETEM= PRR
USRSET_SETED= @NEWERA
USRSET_SETCA= /
/*****************************************************************************/
/* Account DSN(Mbr):IFO.TEST.$PSW.USRSETS(ADMIN1)                            */
/*****************************************************************************/
| NewEra Software, Inc.
| Our Job? Help you avoid problems and improve z/OS integrity.
******************************** Bottom of Data ********************************
```

9.12 ICE/PSWD USER Setting Change Log – Sample

Changes made to the User Settings File are captured in the Settings Change Log. The dataset holding these files is allocated automatically as a PDSE using the high-level qualifier assigned to ICE during installation and takes this form – HLQ.$PSW.CNGSETS. Individual files, members, in this dataset are named using the user's assigned UserId. This dataset should be protected in a manner consistent with site security policy. Extracts from this file form the basis of the ADMIN and USER Settings Change reports.

```
/*******************************************************************************/
/*                                                                             */
/* ICE/PSWD:Password Notice/Controls - Configuration Changes - ADMIN1          */
/* Date:2021/01/27 - Time:13:59:22 - User:ADMIN1                               */
/*                                                                             */
/*******************************************************************************/
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:13:59:22 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVAL | DAYILY | DAYILY / |
| INTERVAL | WEEKLY | WEEKLY / |
+--------------+-------------------------------+-------------------------------+
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:13:55:25 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVAL | DAYILY / | DAYILY |
| INTERVAL | WEEKLY / | WEEKLY |
+--------------+-------------------------------+-------------------------------+
ACTION PSWDEXP(ADMIN1) - Date:2021/01/27 Time:13:55:09 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVALS | 0,1,2,3,5,10,15 / | 0,1,2,3,5,10,25 / |
+--------------+-------------------------------+-------------------------------+
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:13:53:11 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| EMAIL | COPY | COPY / |
+--------------+-------------------------------+-------------------------------+
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:13:37:50 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| EMAIL | COPY / | COPY |
+--------------+-------------------------------+-------------------------------+
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:13:36:08 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVAL | DAYILY | DAYILY / |
| EMAIL | COPY | COPY / |
+--------------+-------------------------------+-------------------------------+
ACTION REPTSETS(ADMIN1) - Date:2021/01/27 Time:12:05:15 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVAL | MONTHLY | MONTHLY / |
+--------------+-------------------------------+-------------------------------+
ACTION PSWDEXP(ADMIN1) - Date:2021/01/27 Time:10:52:25 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| INTERVALS | 0,1,2,3,5,10,15,30 / | 0,1,2,3,5,10,15 / |
+--------------+-------------------------------+-------------------------------+
ACTION PSWDEXP(ADMIN1) - Date:2021/01/27 Time:10:43:39 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ALLOW | ALLOW - | ALLOW / |
| TO | ABC@NEWERA.COM - | ABC@NEWERA.COM / |
| CC | ABC@NEWERA.COM - | ABC@NEWERA.COM / |
| ALIAS | THE KING - | THE KING / |
| SUBJECT | EXPIRATION_NOTICE - | EXPIRATION_NOTICE / |
| INTERVALS | 0,1,2,3,5,10,15 | 0,1,2,3,5,10,15 / |
| FROM | CAT@NEWERA.COM - | CAT@NEWERA.COM / |
| DOMAIN | - | |
| EMAILDEBUG | - | |
| JRLPOST | - | |
+--------------+-------------------------------+-------------------------------+
ACTION PSWDCHNG(ADMIN1) - Date:2021/01/26 Time:18:03:22 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ALLOW | ALLOW | ALLOW / |
| TO | | ABC@NEWERA.COM / |
```

```
| SUBJECT | | PASSWORD CHANGE / |
| FROM | | SUPPORT@NEWERA.COM / |
+--------------+--------------------------------+--------------------------------+
ACTION PSWDEXP(ADMIN1) - Date:2021/01/26 Time:18:00:52 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| EMAILDEBUG | ON / | OFF |
+--------------+--------------------------------+--------------------------------+
ACTION PSWDOTP(ADMIN1) - Date:2021/01/26 Time:17:26:41 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ONLIMIT | ONLIMIT(REVOKE) / | REVOKE / |
| OTPACTIVE | LOGON(FAIL) / | FAIL / |
+--------------+--------------------------------+--------------------------------+
ACTION PSWDOTP(ADMIN1) - Date:2021/01/26 Time:17:22:42 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ONLIMIT | ONLIMIT(REVOKE) | ONLIMIT(REVOKE) / |
+--------------+--------------------------------+--------------------------------+
ACTION PSWDOTP(ADMIN1) - Date:2021/01/26 Time:17:22:23 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ONLIMIT | ONLIMIT(REVOKE) / | ONLIMIT(REVOKE) |
+--------------+--------------------------------+--------------------------------+
ACTION PSWDOTP(ADMIN1) - Date:2021/01/26 Time:17:20:29 User:ADMIN1
+---Controls---+---------Prior Settings--------+--------Updated Settings-------+
| ONLIMIT | ONLIMIT(REVOKE) | ONLIMIT(REVOKE) / |
+--------------+--------------------------------+--------------------------------+
```

10 Operational Components and Requirements:

10.1 NEZPINIT is a Required Primary Support Routine within IFOM

NEZPINIT is activated with a TASK statement in NSEPRMxx similar to the following:

```
TASK=NEZPINIT SUBSYS(ssnm)            /*  PASSWORD SUBSYSTEM  */
OR
TASK=NEZPINIT SUBSYS(ssnm) OTPCASE(UPPER)
OR
TASK=NEZPINIT SUBSYS(ssnm) OTPCASE(MIXED)
```

If OTPCASE is not specified, the default is OTPCASE(UPPER).

If OTPCASE(UPPER) is specified or becomes the default, all OTP values will only contain upper case characters and possibly numbers.

This TASK statement must be located in a BEGINPARALLEL block. The SUBSYS() parameter is required. It defines the name of the MVS subsystem under which the IFOM password subsystem will run. This subsystem name **MUST** be different than the subsystem name that is used for the IFOM start. It must also be different than any other subsystem that could be active.

10.2 NEZRIX01 to Extend the ICHRIX01 RACF Exit

NEZRIX01 is intended to extend the ICHRIX01 RACF exit. It should be linked as a stand-alone module as follows:

```
INCLUDE OBJECTX(NEZRIX01)
ENTRY NEZRIX01
SETCODE AC(1)
NAME ICHRIX01(R) * RACROUTE REQUEST=VERIFY(X) *
```

NEZRIX01 needs to be copied into an IPL active LPA dataset, and a system IPL needs to be performed to activate this extended exit in RACF.

10.3 Complete Isolation from Other ICE Components

The features of ICE/PWSE/OPT are completely isolated from all other ICE Components, and will come into effect only if:

The TASK=NEZPINIT SUBSYS(ssnm) is included in the NSEPRMxx member. The NEZRIX01 module gets activated as the ICHRIX01 RACF exit.

Without both in place, the OTPNOTFY ACTION block definition will have no effect.

11 Configuration Control Cards

11.1 DOMAIN

On occasion, to limit data entry, it can be beneficial to provide a standard email server domain. When this is desirable, the DOMAIN control card is used.

The DOMAIN Control Card, specified in NSEENSxx Parmlib member, can be used in both the METHOD BLOCK and any subsequent ACTION BLOCK, where only the email address prefix is specified in the TO/FROM/CC Control Card (that part just before the @ in the email address).

Note: If the DOMAIN Control Card is to be used, it must appear in the NSEENSxx Parmlib member before any paired TO/FROM/CC control card, which contain only an e-mail address prefix and the address is not domain qualified. The correct form of the DOMAIN paired value is "@domain_name.com", where domain name contains the email domain authorized to receive notices.

11.2 TO/FROM/CC

The TO/FROM/CC control card may be specified with a paired value that is fully qualified containing both an email prefix and domain name. When used in conjunction with the DOMAIN control card, DOMAIN resolution only occurs when a TO/FROM/CC control card does not contain a domain suffix, that is, the portion of an email address that includes the "@" and the trailing domain name. An example of both the DOMAIN and TO/FROM/CC control cards is shown below:

```
METHOD EMAIL
DOMAIN @primary.domain
TO control
METHOD .END

ACTION (PSWDCHNG | SYSLOGON | PSWDEXP) METHOD(EMAIL)
TO user1.last
FROM boss.last@home.domain
ACTION .END
```

In the sequence shown above, the TO email address will resolve to: user1.last@primary.domain

```
ACTION (PSWDCHNG | SYSLOGON | PSWDEXP) METHOD(EMAIL)
DOMAIN @secondary.domain
TO user1.last
FROM boss.last@home.domain
ACTION .End
```

In the sequence shown above, the TO email address will resolve to:

user1.last@secondary.domain

The process that resolves the full email address uses the most recently specified DOMAIN value required. The length of a fully resolved email address is limited to 64 characters. (Domain is strictly enforced at a max of 48 characters). The prefix may resolve the reminder to any length up to a practical limit of between 54 to 56 bytes.)

When the DOMAIN control card is specified, it must be specified prior to any TO/FROM/CC control cards that would require the DOMAIN control card's value to complete the full email address.

Any DOMAIN value that exceeds 48 characters will be deemed as a control card error. Any TO/FROM/CC specified value that requires a domain suffix for resolution that does not have an active DOMAIN setting (either ACTION or METHOD) would be deemed as a control card error.

This is one additional bit of clarification regarding the DOMAIN control card. DOMAIN control cards do not remain in effect across ACTION block changes. When a new ACTION block is detected, the only DOMAIN that is active is the METHOD block's DOMAIN (if one was specified). To have an ACTION block specific DOMAIN active for an ACTION block, there must be a valid DOMAIN control card contained in that ACTION block.

A fully qualified Email Address can coexist with a conjoined Prefix and Domain. But both cannot be configured and are mutually exclusive from within the Administrator Interface.

11.3 SYSLOGON(?) - Undefined User Logon Attempted

It may be considered desirable to report Logons attempted by any undefined UserIds. Such attempts may indicate that someone is “Knocking” on the system, looking for a way in. Such attempts can be reported to the appropriate area using the following Action Block sequence.

```
ACTION SYSLOGON(?) METHOD(EMAIL)
WHEN RETCODE EQUAL(04)    (04 = Logon attempt was failed)
TO sysadmin@company.com
ACTION END.
```

External notification senses a return code 04 condition, it will send a notice containing the unknown UserId to the email address specified on the TO Control Card, as shown below.

```
01C|-SRC: SYSLOGON(TOKTSO )---THE CONTROL EDITOR-------------- VerifyFail -
02C|SYSPLX:ADCDPL SYSNM:ADCD22B USRID:PUBITJ TM:17:10:30 DT:02/09/18
03C|-VERIFY(X): PUBITJ----RC: 04 User profile not defined to RACF ----------
```

The related Log Record will carry an Id of "LX".

11.4 ALIAS

You may want to mask the defined userid that would optionally appear in the individual notifications sent to users, where they have defined PSWDCHNG, SYSLOGON, and PSWDEXP NSEENSxx ACTION BLOCKS for security reasons. This is done using the ALIAS sub-option. The ALIAS sub-option is limited to a 32-character quoted string and the content of this string appears in any email notification and log record. An ALIAS Control Card Example is shown below:

```
ACTION PSWDCHNG(MTECH3) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
SUBJECT 'PSWDCHNG notification for MTECH3'
FROM  user10@company TO user8@company
ALIAS 'TOP DOG ALIAS'
DEBUG ON
TEMPDSALLOC UNIT(TRK) PRIMARY(1) SECONDARY(1)
DEBUGDSALLOC UNIT(TRK) PRIMARY(1) SECONDARY(1)
ACTION .END
```

In the example below, you can see the ICE log showing the USRID is masked and the ALIAS value inserted in a password change notice.

```
01C|-SRC: TSOCMD---------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:08:34:38 DT:11/15/17
03C|-PSWDCHNG: TOP DOG ALIAS ------------------------------------------------
```

Examples below detail differences between ALIAS Vs. Non-ALIAS encoding.

With ALIAS:

```
01C|-SRC: EXPCHECK-------------THE CONTROL EDITOR------------ ExpiryNotify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:13:41:22 DT:11/21/17
03C|-PSWDEXP: Length 8 userid-------------------Password expires in 83 days-

01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR------------ VerifySuccess -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:13:43:07 DT:11/21/17
03C|-VERIFY(X): John Q. Public -------------------RC: 00--------------------

01C|-SRC: TSOCMD---------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:********    TM:13:44:43 DT:11/21/17
03C|-PSWDCHNG: IFO test userid------------------------------------------------
Your pwd changed at 13:44 on 2017/11/21 from system ESSD3
```

Without ALIAS:

```
01C|-SRC: EXPCHECK-------------THE CONTROL EDITOR------------ ExpiryNotify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:IFOM        TM:13:01:03 DT:11/21/17
03C|-PSWDEXP: LEN8USR1--Password expires in 83 days-------------------------

01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR------------ VerifySuccess -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:ESSJDL2     TM:13:56:34 DT:11/21/17
03C|-VERIFY(X): ESSJDL2---RC: 00 Password or phrase is authorized ----------
```

```
01C|-SRC: TSOCMD---------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:ESSD3    USRID:ESSJDL3     TM:13:44:43 DT:11/21/17
03C|-PSWDCHNG: ESSJDL3-----------------------------------------------------
Your pwd changed at 13:44 on 2017/11/21 from system ESSD3
```

Note that in the case of SYSLOGON, not all information is logged in ICE when ALIAS is used. In the case of PSWDEXP and PSWDCHNG, all available data is displayed; it is just shifted further to the right.

11.5 WHEN ACTIVE DAYS | DAY(MON,...,SUN)

WHEN ACTIVE DAYS|DAY is used to limit PSWDCHNG or SYSLOGON NSEENSxx ACTION block notification to specific days of the week. By example, the following control card set limits logon notification to Saturday and Sunday.

```
ACTION SYSLOGON(PHARL1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
WHEN ACTIVE DAYS(SAT,SUN)
SUBJECT 'You Logged on to the System'
FROM  support@COMPANY.com
TO CAT@COMPANY.com
ACTION END.
```

11.6 WHEN ACTIVE SDT() STM() EDT() ETM()

WHEN ACTIVE SDT() STM() EDT() ETM() is used to limit PSWDCHNG or SYSLOGON NSEENSxx ACTION block notification to intervals and time of day. By example, the following control card set would limit logon notification to Saturday and Sunday between 8:00AM and 10:00PM.

```
ACTION SYSLOGON(PHARL1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
WHEN ACTIVE DAYS(SAT,SUN)
WHEN ACTIVE STM(8000) ETM(2200)
SUBJECT 'You Logged on to the System'
FROM  support@COMPANY.com
TO CAT@COMPANY.com
ACTION END.
```

Sub-Parms Include:

- SDT(yymmdd) – Start Date
- STM(hhmm) – Start Time
- EDT(yymmdd) – End Date
- ETM(hhmm) – End Time

11.7 WHEN RETCODE EQUAL(04,…,21)

WHEN RETCODE is used to limit SYSLOGON NSEENSxx ACTION block notification by return code. By example, the following control card set would limit logon notification to Saturday and Sunday between 8:00AM and 10:00PM, but only when the return code from a system logon attempt is equal to 04 or 20.

```
ACTION SYSLOGON(PHARL1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
WHEN ACTIVE DAYS(SAT,SUN)
WHEN ACTIVE STM(8000) ETM(2200)
WHEN RETCODE EQUAL(04,20)
SUBJECT 'You Logged on to the System'
FROM  support@COMPANY.com
TO CAT@COMPANY.com
ACTION END.
```

Other valid RETCODE Conditions:

- NOTEQUAL(04,...,24) – Multi-Value pairing
  - Excludes specified return codes from notifications
- GREATERTHAN(24) – Single Value pairing
  - Notifications only sent if return code is more than 24
- LESSTHAN(30) – Single Value pairing
  - And for return codes less than 30

11.8 EXPINTERVAL(1,…,nn)

The EXPINTERVAL control card is used exclusively for the PSWDEXP ACTION Block to indicate which day(s) prior to expiration an expiry notice will be sent. Here is an example EXPINTERVAL control card:

EXPINTERVAL (1,2,3,5,7,14)

Globally, this notification can be sent to all UserIds using the following control card set:

```
ACTION PSWDEXP(.DEFAULT)
EXPINTERVAL (1,2,3,7,14)
ACTION .END
```

UserIds may be excluded from such global notification by using the EXCLUDE sub-command for each required user within the Action Block set, as in the following example.

```
USERID ESMUSR1 EXCLUDE
```

Note, these global functions are planned for a future release, as supported by users requiring support for z/OS V2R3.

11.9 NOTIFICATION INACTIVE(SYS1,…,SYS8)

NOTIFICATION INACTIVE is used to limit PSWDCHNG or SYSLOGON NSEENSxx ACTION block notification actions, in order to exclude specific systems by System Name. By example, the following control card set would exclude logon notification from SYSTEMA and SYSTEMZ:

```
ACTION SYSLOGON(PHARL1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
NOTIFICATION INACTIVE(SYSTEMA, SYSTEMZ)
SUBJECT 'You Logged on to the Named System’
FROM support@COMPANY.com
TO CAT@COMPANY.com
ACTION END.
```

11.10 MSGBODY (&DATE, &TIME, &SYSTEM)

MSGBODY is used to enhance PSWDCHNG or SYSLOGON notification messages, as specified in the NSEENSxx ACTION block. Substitution keyword symbols &DATE, &TIME, and &SYSTEM are resolved and automatically inserted into the specified message body and appear as a fourth line in addition to the standard password change or system logon notification message. Following is an example control card set:

```
ACTION PSWDCHNG(PHARL1) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
NOTIFICATION EXCLUDE(SYSTEMA, SYSTEMZ)
SUBJECT 'You Logged on to the Named System’
FROM support@COMPANY.com
TO CAT@COMPANY.com
USERID ALIAS ’YOU ARE TOP DOG'
MSGBODY 'Your password changed - &TIME on &DATE from system &SYSNAME'
ACTION END.
```

And, upon password change would generate a message as follows:

```
01C|-SRC: TSOCMD---------------THE CONTROL EDITOR------------------ Notify -
02C|SYSPLX:ADCDPL   SYSNM:SYS10    USRID:********     TM:13:44:43 DT:11/21/17
03C|-PSWDCHNG: YOU ARE TOP DOG-----------------------------------------------
Your password changed - 10:51 on 2017/09/25 from system SYS10
```

11.11 TIMEWINDOW

TIMEWINDOW control card is found within the OTPNOTFY ACTION block.

This specifies the length of time, between when the initial password change attempt was made, and the time by which the user must return to the system

and enter their current password and the OTP value, for the password change to be completed.

If nothing is specified, the default value is set to 15:00 minutes. The maximum value is 15:00 minutes, while the lowest allowable value is 00:30 seconds.

TIMEWINDOW(10:00)

11.12TERMINALMSG (TRMMSG)

TERMINALMSG control card is found within the OTPNOTFY ACTION block.

TERMINALMSG ON|OFF

If TERMINALMSG is ON, the following will appear on the User Terminal.

```
The request to reset your password value has been intercepted. You
will receive an e-mail that will supply a one-time use OTP value
which will be entered during your next logon and password reset
attempt. The OTP value you receive will be used as a new password
value and will be required at your next logon/reset. Remember that
value. Your next logon/reset attempt must be completed by hh:mm:ss.
If that time expires, the one-time use OTP value will no longer be
valid.
```

11.13 RETRYLIMIT

RETRYLIMIT control card is found within the OTPNOTFY ACTION block.

This specifies how many attempts the user has to enter the OTP token and new password correctly within the specified time period.

If nothing is specified, the default value is set to 5 password reset attempts. The maximum value is 9 attempts, while the lowest allowable value is 0 attempts.

RETRYLIMIT 7

11.14 ONLIMIT

An optional extension to the RETRYLIMIT allows for the User's Logon Id to be Revoked if the retry limit is reached.

RETRYLIMIT 7 ONLIMIT(REVOKE)

11.15 OPTACTIVE

OTPACTIVE is an optional extension of OTP control over the OTP Logon/Password Reset process. It operates only within the OTP TIMEWINDOW and when set to FAIL will prevent a user from bypassing the completion of an OTP Password Reset.

OTPACTIVE LOGON(FAIL|NOFAIL) – Default NOFAIL

EXCEPTION: OTPACTIVE LOGON(FAIL) should be used with caution in logon scenarios under the control of - CL/Supersession (and other similar Session Managers) or when the IKJTSO00 PARM PASSWORDPREPROMPT is set 'ON'- where password reset operations are preceded with old password prevalidation operations. If in doubt about your installation settings contact NewEra Technical Support, support@newera.com, for assistance.

11.16 DEBUG

Is used in conjunction with the NSEENSxx METHOD BLOCK that should, by default contain the definitions of related Debug Dataset Allocation and Dataset Naming. This should only be use with advice from NewEra Technical Support.

DEBUG ON|OFF

11.17 JRLPOST

ICE/PSWD Events are, by default, written to the ICE Event Log. An ICE Log Record is a one line 256-byte summary of relevant event data. To enrich the history of an event, turn ON Journal Posting which will capture 'ALL' related event information and record it in the ICE Control Journal.

JRLPOST YES|NO

12 Installing the Integrity Controls Environment:

Prior to using an ICE Application, you must first download and install the Integrity Controls Environment (ICE). If you do not already have the ICE download, you may request it by sending an email to support@newera.com. The returned "Download Link" email will contain both product and documentation links. It is recommended that you first download and carefully read the ICE Installation Guide as it explains the steps necessary to complete a successful ICE installation.

12.1 Getting ICE Application License Keys

If you are licensed for either Image FOCUS or The Control Editor (the ICE Viewer does not require a license key), you may download the Integrity Controls Environment from the "Download Link" email in one of two ways: "Fully Authorized" or "Self Authorized". Downloading from the "Fully Authorized" link, the applications are licensed automatically. Downloading from the "Self-Authorization" link will require you to add the license keys, which are provided in the "Download Link" email, to the NSEPRMxx Member in ICE Parmlib, following installation.

If you are licensed for either ICE/PSWD or ICE/RACF, you will receive a separate, unique set of license keys for these applications via email. These license keys must be placed in the ICE USERLIB Dataset created during system installation. ICE/PSWD and ICE/RACF license keys may be added at any time to a running instance of ICE and do not require re-initialization of the ICE Master Address Space. To request an ICE/PSWD or ICE/RACF license key, send an email to support@newera.com with the requested product as the email subject.

12.2 Installing an Application License Key

This is an example of an ICE/OPER/MVS License Key. The ICE/OPER/RACF key looks similar but varies with application specific content.

```
COMPANY= NEWERA_SOFTWARE,_INC.
LICAREA= DAOFXFSB_TPG%XBS (UPDATE BY:12/31/16)
APPAUTH= DA12C8FCP$FSOFXF (APPLICATION:OPER)
TRMAUTH= DA1*12:$$XFSBDN! (TERM:PERPETUAL)
```

These keys must be placed into the ICE USERLIB dataset for the related applications to become operational.

The member name of the ICE/PSWD key must be $OPERKEY.
The member name of the ICE/RACF key must be $RACFKEY.

12.3 ICE/PSWD Application Requirements

ICE is enabled "out of the box" with program elements that allow users, of either Image FOCUS or The Control Editor, to define and monitor the occurrence of MVS and RACF operator commands, recording them as detected, in the command log that was defined during ICE installation. When either the ICE/PSWD or ICE/RACF applications are licensed, these ICE program elements expand, allowing for the creation and deployment of an Extended Master Console subsystem accessible only by authorized and permitted users of either application.

12.4 Logging on to the ICE Primary Menu

With the ICE Environment installed, it is time to logon to the Primary Menu. To do this, you will need to know the APPLID of the VTAM Application that controls access to all ICE Applications. The system programmer who installed ICE will know the correct name.

With the correct application_name in hand, launch a 3270 session just as you would when logging on to TSO/ISPF. The logon syntax will vary from site to site but might look something like this:

```
LOGON APPLID=application name
```

A shorthand variation might look like this:

```
L application_name
```

Consult your system programmer for the correct format of the command.

In the userid/password confirmation panel, enter your userid and password as you would if logging on to TSO/ISPF. If access is granted, the ICE Primary Menu is displayed.

12.5 The ICE Primary Menu

The ICE Primary Menu, shown below, lists access options for Image FOCUS, The Control Editor, and the ICE Viewer. Depending on your licensing status, certain options may be highlighted in white to indicate that they are available for use. Those options highlighted in yellow require additional licensing.

```
                ICE 18.0 - The Integrity Control Environment

      P   ProdView  .. - Image Focus Production Views          Userid   - PROBI1
                                                              Time     - 12:11
      W   WorkView  .. - Image Focus Workbench Views          Terminal - 3278
                                                              System - ADCD113
      R   DRecView  .. - Image Focus Recovery Views           Applid   - TEST
                                                              Image Focus 18.0
      C   Controls  .. - Controls Environment Settings        Patch Level 00

      V   ICEViews  .. - IPLCheck Results Focal Point

      D   Defining  .. - IFO Definitions and Settings

                          ****************************
                          * Background Task: RUNNING *
                          * No/TSO Recovery: DOWN    *
                          ****************************

      X   Exit         - Terminate

       NewEra Software, Inc.
          Our Job? Help you make repairs, avoid problems, and improve IPL
integrity.
      Option  ===>
```

12.6 Product Evaluation Keys

Evaluation keys for these additional options may be requested at any time by sending an email to support@newera.com. The option to be used in this exercise, “Defining”, is always available for use.

12.7 When Neither Image FOCUS/The Control Editor is Licensed

Note that when neither Image FOCUS nor The Control Editor is licensed, access to the “Defining” Option is provided for initially permitting users to access the ICE/PSWD Applications. If access is permitted, both ICE/PSWD Administrators and Users will access both MVS and RACF Applications via the Primary Command Line.

13 Empowering the ICE Administrator

It is considered a "Best Practice" to designate trusted ICE users as ICE System Administrators. In this role, they will be allowed access to critical ICE configuration settings; for example, the establishment of dataset and command boundaries, the permitting of user access to configuration members, and operator commands, Activity Monitors, and Audit Reports.

Even though it is a "Best Practice" to designate ICE System Administrators, the "Default State" of ICE, as it relates to Image FOCUS, The Control Editor, and the ICE Viewer, does not require an Administrator. ICE/PSWD and ICE/RACF Applications, however, do require oversight by someone (or more than one person) acting in the role of ICE System Administrator.

Defining ICE Administrators and permitting user access is a Five Step process. In Step One, you will define the Administrators. In Step Two, you will permit users to access the "Use Functions" of all, or selected, ICE applications. In Step Three, you will learn how to create an optional "Secondary Password". In Step Four, you will set the ICE Padlock Global Control Default Value: NONE, WARN, or DENY. Any updates made in the previous four steps will only become effective when activated, as described in Step Five.

The ICE Administrator/User Control Panel shown below supports all the options used in the various steps described.

```
                ICE 18.0 - ICE Administrator/User Controls

I   SetAdmin  .. - Authorize ICE Administrators          Userid   - PROBI1
                                                        Time     - 11:22
N   NSEParms  .. - Set NSEParms Category Boundary       Sysplex  - ADCDPL
                                                        System   - ADCD113
G   Padlocks  .. - Global Padlock Access Controls       ApplId   - TEST
                                                        Image Focus 18.0
U   UserMode  .. - ICE User/Application Controls        Patch Level 00

P   Password  .. - Set Password Prompting Controls

L   UserLogs  .. - ICE User/Application Audit Log

A   Activate  .. - Dynamically Activate Controls



X   Exit         - Return to the TCE Primary Menu
```

13.1 Step One: Defining ICE System Administrators

To select the Defining option from the ICE Primary Menu, do one of the following:

Place the cursor under the option and press enter, enter an "S" or "D" on the entry-point shown after the option name, and press enter, or enter "D" on the primary menu command line and press enter.

Note that for a more detailed description of each option that appears in a menu's selection list, press PFK1.

From the menu that is displayed, select the ICEAdmin option. This will display the ICE Administrator/User Controls Panel, pictured above. From this menu, select the SetAdmin option. This action will bring up the ICE Administrator Assignment Panel.

Use the ICE Administrator Assignment Panel to name one Primary and up to six Supplemental ICE Administrators, using their respective TSO UserIds. Only those named in this panel will be afforded access to ICE/PSWD and/or ICE/RACF Administration Functions. These functions include naming commands to be logged, permitting user access to ICE Extended Master Console functions, supported by either product, and setting command Audit Intervals.

Primary and Supplemental authorities differ in only one way. The Primary Administrator may, when needed, display Application Access Passwords in Clear Text. This is a privilege not enjoyed by other Supplemental Administrators.

When you are finished assigning Administrators, select PFK3 to save your updates and return to the prior menu. From here, you will now select the UserMode option and proceed to Step Two.

Note that these new or updated settings will not be in effect until they are activated. The Activation process is described in Step Five.

13.2 Step Two: Permitting Application Access

Users of ICE/OPER/MVS and/or ICE/OPER/RACF must be specifically permitted access by the ICE Administrator. To permit access to a user, select the UserMode option from the menu. This will display a listing of all authorized ICE Users, related applications, access rights, and access windows, if any. For a detailed description of the listing, its column headings, and selection options, use PFK1.

To add a new user, use the "Add_User_Rule" option. To do this, place an "A" on the entry point preceding any row and press enter. This action will display the Add ICE User Pop-Up as shown below:

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Adding ICE User Access Rules                 ◊
◊                                                                        ◊
◊ --User-- -----Application Access Rule----- ----FreeForm Comment----    ◊
◊ ---Id--- --Rules-- ---Start--- ---Stops--- ----------Text----------    ◊
◊ -------- Prod Mode yymmdd hhmm yymmdd hhmm ------------------------    ◊
◊ -USERID- PSWD ---- ------ ---- ------ ---- 15/03/24_10:33_PROBI1      ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

This panel consists of several entry points (fields), two of which are mandatory: User Id and Prod.

In the "User Id" field, enter the TSO UserId of the individual for whom you wish to permit access. In the "Rules Prod" field, enter the ICE Product Code, in this case either OPER or RACF.

Optionally, in the "Rules Mode" field, enter the action to be taken when a user attempts to issue a command outside of a defined "Access Window". The choices are: NONE, WARN, or DENY. When WARN or DENY is specified, the named "User Id" will be allowed full application access to the named Product Code but will be WARNED or DENIED access to the ICE Extended Master Console for issuing Commands.

The "Starts" and "Stops" date (yymmdd) and time (hhmm) values are used to create an "Access Window" that opens and closes as defined.

Use PFK1 for a detailed description of these functions. When you are done making changes, press PFK3 to exit and save your work.

13.3 Step Three: Creating a Secondary Password

ICE/OPER/MVS and ICE/OPER/RACF are powerful z/OS System Utilities. As such, it is considered a "Best Practice" to further control user access to them by making use of the "Secondary Password" option.

To define a password, select the Password option from the menu. This action will display the TCE OPER Prompt (Password) Control Options Listing.

The options of interest within this current context of Command Sets are: MVSCOMMDS, RACFCMDS, and SETCOMMDS. When set, the user will be prompted for the assigned password, and granted access only if the correct application password is entered. If not, they are DENIED or WARNED. There is

no limit to how many times a user may attempt a new password following a failed attempt.

To assign a password to a Command Set, place an "A" on the Entry Point preceding the targeted Command Set, and press enter. The following Prompt Pop-up will appear.

```
◊──────────────────────────────────────────────────────────────────────────◊
◊                ICE 18.0 - Adding a TCE/OPER Prompt                       ◊
◊                                                                          ◊
◊   ---Password--- Mode ---Start--- ---Stops--- ---This-Addition---        ◊
◊   -------------- ---- yymmdd hhmm yymmdd hhmm yymmdd-hhmm-UserIds        ◊
◊   ENTER_PASSWORD ---- ------ ---- ------ ---- 150324_1147_ADMIN1         ◊
◊──────────────────────────────────────────────────────────────────────────◊
```

This panel supports a number of entry points (fields), two of which are mandatory: Password and Mode. Passwords must be at least 6 and no more than 16 alphabetic characters. A password is encoded as a "One-Way Cipher" and stored in association with its related Command Set. Passwords are never shown in "Clear Text" except to the TCE Administrators, when they are using special "Admin-Helper" (±) Functions.

The Mode setting, NONE, WARN, or DENY, denotes the action to be taken by ICE if the user enters an incorrect password.

The password applies 24X7 unless the "Starts" and "Stops" date (yymmdd) and time (hhmm) values are used to create an "Access Window" that opens and closes as defined.

Use PFK1 for a detailed description of these functions. When you are done making changes, press PFK3 to save your work and exit.

13.4 Step Four: Setting the ICE Padlock Global Control Value

The Padlock Global Settings are the "Overlords" of access to ICE defined resources. By default, all Padlock Controls are set to "WARN". To update these Global Settings, select the "Padlocks" option from the menu. This action will display the Padlock Access Controls Features Panel.

Change the Global Settings focus on the upper part of the panel as shown below:

```
----------------------Padlock Access Controls-----------------------

TCE Padlock Mode of Controlling Access:   .. Deny   /. Warn   .. None

Mode - WARN - Users without Padlock Access Rights Warned of Denials.
```

Note, the Default Setting "Warn" is checked "/". To change this, place the check "/" beside the desired Global Setting and press enter to update the panel.

The lower part of the panel, seen below, shows the control settings for each of the Boundaries Classifications supported within the Integrity Controls Environment.

```
----Current Definition---- Cm ---Boundaries--- Cm ----Updated Definition----

                        ON .. Control Category .. ON                       .
                        ON .. Control Datasets .. ON                       .
                       OFF .. Control Commands .. ON                       .
                       OFF .. Control WrkGroup .. OFF                      .
                       OFF .. Control RoleBase .. OFF                      .
                       OFF .. Control IFOUsers .. ON                       .
```

As it relates to ICE/OPER/MVS and ICE/OPER/RACF, you will need to turn on the specific Padlock Controls, "Commands" and "IFOUsers", which are by default turned OFF. To do this, type the word "ON" to the right of both "Control Commands" and "Control IFOUsers", and press enter. The panel will update showing your selections.

When you are done making changes, press PFK3 to save your work and exit.

13.5 Step Five: Activating ICE Settings

Once you have completed Step One through Step Four, you will need to activate your settings. To do this, select "Activate" from the menu and press enter. The following message will appear on the screen to confirm that Activation has completed successfully:

```
◊——————— NSEJRNxx and NSESELxx have been Successfully Activated. ———————◊
```

14 Index

15 Technical Support

NewEra Software, Inc.

Mailing Address:

18625 Sutter Boulevard, Suite 950
Morgan Hill, CA 95037

Phone:

(408) 520-7100
(800) 421-5035

Text:

(669) 888-5061

FAX:

(888) 939-7099

Email Address:

support@newera.com

Web Site:

http://www.newera.com

Technical Support:

24 hours a day, 7 days a week
1-800-421-5035
support@newera.com