The argument is often 'too much' vs. 'too little' Security.
Today the only answer to this debate is a program that thoughtfully pursues
'z/OS Defenses In Depth' without impacting productivity.

Getting Started with Multi-Factor Edit (MFE)

An Optional Resource Access Control Structure within The Integrity Controls Environment (ICE)

ICE 16.0 Patch 5

NewEra Software Technical Support
800-421-5035 or 408-520-7100
support@newera.com

Rev: 2020-07-30

1. Table of Contents

2. What is Multi-Factor Edit (MFE)?

Multi-Factor Edit (MFE) is an extension of the available ICE control structures that surround The Control Editor (TCE) Category Definitions. In practice, MFE Access Control requires that a TCE Category must also be defined as an MFE Controlled Category (also called an MFE Controlled Profile). Once such a Profile is defined all access to its underlying resources - Datasets, Files and/or Load Libraries - will be Denied and/or Warned unless or until users are permitted access. The identity of permitted users is "Challenged" at the point of attempted resource access. This challenge requires a response that will specifically "Verify" the users identity. This response is a One-Time-Token "The Factor" known only to the user or a designee. In addition, surveillance over MFE Profiled Resources may be enhanced, such that changes made to them outside the Controls Environment will not only be noticed and documented but they will also be marked and "Isolated" in the TCE Control Journal. This isolation is designed to prevent these non-conforming resource copies from being used as "Certified" versions, eligible for use as a legitimate Restore Point.

2.1. User Access Verification

All users seeking access to resources defined by an MFE Category/Profile must have their identity and MFE Permission verified before they are allowed access. This verification is accomplished through the use of One-Time-Token. These Tokens, generated as Pass Tickets by the system's External Security Manager (ESM) are based on organization defined "keymasked" and made known to the MFE permitted user in one of three ways:

2.1.1. Email/SMS Directly to the User

The prerequisite for this option is a Valid Email Address. The address can be limited (enforced by MFE) to only those addresses that are known to the ESM and are resident in the WAEMAIL Field of their respective Security Databases. If WAEMAIL is not configured and WAEMAILONLY is not set to 'YES' any Email Address is accepted. When a valid Email Address is provided and proves reachable, the user will receive an "Alert", in real time, containing the necessary Token in real time when resource access is attempted.

This Token is valid for 2 minutes from the time of issuance. When resource access is attempted, the user's workflow is interrupted by a panel containing a Token Input Field. If the Token is entered correctly into the field within the time limit, access is allowed and the resource is displayed in ISPF Edit. If the Token is mis-entered or times out, access will be denied. Any attempt to gain access following a denial or successful attempt begins the process anew.

2.1.2. Email/SMS to a Third Party

This option has the same Valid Email Address prerequisite. What differs is that the user is no longer the target of the Token Delivery Email; instead one or two designees become the Email Targets and they receive the "Alert", again in real time, as the user waits to be "Told" the Token Value. This Token is valid for 5 minutes from the time of issuance. While the Token goes to the designee, its use is bound to the initiating user and only that user may use the Token. As an added “Outside-The-System” control, a challenge conversation/dialog between the user and the recipient designee could be added to create yet another Factor before the Token value is revealed. If the Token is mis-entered or times out the access will be denied. Any attempt to gain access following a denial or successful attempt would begin the process anew.

2.1.3. NoEMail PIN and Suffix Combination

When Email/SMS is not a practical option, a combination of a user’s private PIN and a system generated, on-screen displayed suffix may be used. The user’s private PIN should be thought of as an additional Factor somewhat like a password in that it is determined by the user, known only to the user, stored encrypted and never shown in clear text. The needed suffix is generated by the system using the same Pass-Ticket generation process used by the Email Option. The resulting Suffix is displayed on the users screen, again in real time. The user next concatenates a fully-qualified Token entry using the private PIN and the generated suffix. The suffix is bound to the user and therefore only the user may use it legitimately. The suffix will be valid for 2 minutes. If the combined PIN and Suffix are mis-entered or the Suffix times out, access will be denied. Any attempt to gain access following a denial or successful attempt would begin the process anew.

2.2. Resource Certification

Certification is a programmatic process of constant vigilance for Category Resource Change actions that are NOT AUTHORIZED within a TCE or MFE Defined Control Structures. As it applies to MFE this oversight is strictly enforced at two very distinct policy enforcement points:

2.2.1. On-Access Attempts

During an access attempt, the resource being requested is, from its current location and in its current state, read and compared with its most recent version as contained in the Control Journal. If they are a 100% match, the process will continue. If they are not, a message is displayed, the process interrupted pending acceptance of the current resource by the user. If acceptance is not wanted, the current copy of the resource will be written to the Control Journal and “Isolated’. If the user wishes to proceed the last Control Journal Copy will be presented and, updated or not, will become the “Certified” resource copy.

2.2.2. At Interval Change Detection

Interval change detection, is an hourly process in which ALL TCE Category Resources - Datasets, Libraries, Files - are compared to their known LAST Version as contained in the Control Journal. Note this, if a difference were found in a Category that is NOT an MFE Profiled Category, the differing resource would be written to the Control Journal as a Detected Change thus creating a new version of the resource. When the Category is an MFE Profiled Category this is not the case. An MFE Profiled Resource will still be written to the Control

Journal but in this case as an EXCEPTION, ISOLATED and NOT, as a New Version. These Exception Records are used only for analytic and reporting purposes. Such Exceptions will remain in their isolated state until they, as is the case with On-Access events, are RECERTIFIED as VALID working copies. When an action is taken to RECERTIFY, a copy of the known resource will be written anew to the Control Journal becoming the most recent version to be useable as a Restore and Compare Point.

2.3. User Verification and Resource Certification

User Verification and Resource Certification may be used independently as they are not dependent on each other or they may be used together to achieve a higher level of ICE Resource Access Control and Integrity.

2.4. Resource Recertification Tools and Options

The Recertification Option panel is offered to the user as a Policy Decision Point when a Non-Compliant Resource is encountered. This panel supports four Recertification tools and options.

2.4.1. Browse

Display the Target in ISPF Browse.

2.4.2. Restore

Extract last Journal copy of Target and Restore it over the Actual Target. If this option is taken, the restored copy is considered a Recertified version.

2.4.3. Accept

Use the Target "as is" Un-Certified.

2.4.4. Compare

Display a Target specific HISTLIST Compare Options.

2.4.5. Return

Exit/PFK3 back to the Member List

3. Frequently Asked Questions

If you have additional questions, please send them to NewEra Technical Support at this Email Address – support@newera.com – with a subject of – "MFE Q&A".

3.1. Can MFE support all three External Security Managers?

Yes! MFE is fully compatible with IBM RACF, ACF2 and Top Secret.

3.2. What ESM Support does MFE Require?

Like all z/OS System Utilities, MFE is dependent on the ESM for protection of its programmatic, source and extracted data structures. This would include its ICE Parmlib configuration members, Control Journals, LOAD Libraries and other Program Objects.

3.3. What ESM Support does MFE Exploit?

Each of the three ESMs support PASSTICKET Token Generation and WORKATTR/WAEMAIL. MFE exploits these ESM features as follows:

3.3.1. PASSTICKET Token Generation

An MFE PASSTICKET is an eight character string generated on demand at the point of a resource access attempt. It is useful only once with a maximum valid lifetime of from two to five minutes depending on mode of operations – Independent User Vs. Designee Dependent.

MFE use of the Token Generator and the resulting generated PASSTICKET is totally dependent on the ESM permission and the generator's underlying "KeyMask". The following command sequence shows the setup steps required to permit the ICE Primary Started Task, IFOM access to the Token Generator and define the keymask for IBM RACF:

```
Step 1) setropts classact(ptktdata)
Step 2) setropts raclist(ptktdata)
Step 3) rdefine ptktdata ifom uacc(none) ssignon(keymasked(0123456789abcdef))
Step 4) setropts refresh raclist(ptktdata)
```

Once these steps are completed MFE will automatically cause Tokens to be generated for exclusive use as One-Time Access Tokens. The "KeyMask" may be changed and refreshed at any time without impacting its use by IFOM or any other Task that may be permitted to its use.

3.3.2. WORKATTR/WAEMAIL

MFE supports WAEMAIL lookup, that is, when a UserId is provided by MFE, the ESM will return the user's stored Email Address, or not, if the address is unknown. Reverse lookup is also supported, such that when MFE provides an Email Address the ESM will return the UserId if the address is stored, or not if the address is unknown.

This optional Policy Decision Point is primarily used to validate Token Delivery Email Addresses and is activated by adding this single Control Card to the ICE NSEJRNxx ParmLib Member:

WAEMAILONLY YES

Once activated, ONLY ESM Controlled/Authorized Email Addresses will be considered as valid and usable by MFE for Email Token Delivery.

The lookup and reverse lookup capabilities of MFE may also be used in Interval Reporting of changes in the WAEMAIL profiles being maintained by the External Security Manager.

3.3.3. Password Expiration

Each ESM maintains a dated reference as to when a user password will expire. MFE uses this date to optionally notify users of the pending expiration of their passwords.

3.4. Is there Messaging/Alerting of MFE Events?

Yes, each MFE interaction has its own specific alert. Here is a sample of three common alerts. The first was issued and sent to a user with the accompanying, highlighted, PASSTICKET Token. The second was issued and sent to a designated third party. Third indicates an MFE entry failure and may be sent to a list of "Need to Know" administrators and/or auditors.

```
-SRC: MFEDIT---------------THE CONTROL EDITOR--------------- MFEPermit -
 SYSPLX:ADCDPL SYSNM:ESSD6 USRID:ESSJDL1 TM:06:40:44 DT:06/23/20
-MFEPERMIT: ESSJDL1-----------------------------------------------------
-----------------------------------EVENT DATA----------------------------
Edit request MFE token: V2MBRWDX Expires in approximately 2 minute(s).
Category: S913.TEST Dsn: ESSJDL1.ACF2.RULES

-SRC: MFEDIT---------------THE CONTROL EDITOR---------------- MFE3part -
 SYSPLX:ADCDPL SYSNM:ESSD6 USRID:******** TM:07:03:22 DT:06/23/20
-MFEPERMIT: ESSJDL1-----------------------------------------------------
-----------------------------------EVENT DATA----------------------------
Edit request MFE token: 8FS7RV50 MFE edit continues on valid token entry.
Category: S913.TEST Dsn: ESSJDL1.ACF2.RULES

-SRC: MFEDIT---------------THE CONTROL EDITOR----------------- MFEFail -
 SYSPLX:ADCDPL SYSNM:ESSD6 USRID:ESSJDL1 TM:07:02:23 DT:06/23/20
-MFEPERMIT: ESSJDL1-----------------------------------------------------
-----------------------------------EVENT DATA----------------------------
Edit request MFE token: ******** Invalid token entered.
Category: S913.TEST Dsn: ESSJDL1.ACF2.RULES
```

In addition, all such alerts are written to the TCE Control Journal using the following journal tags:

```
<ALLOW> - Resource access was allowed.
<WARNS> - User was warned of access failure but allowed because in Warn Mode.
<FAILS> - User notified of access failure and denied resource access.
<3PART> - Designee notified of in process access attempt.
<SETUP> - MFE Operation experienced setting problem.
```

These journal tags allow for real-time queries of MFE related events; on-line from TSO/ISPF or at defined intervals for ADMIN and AUDIT Reporting.

3.5. Does MFE offer a Reporting Package?

Yes, both TSO/ISPF and Interval Reporting are standard, built-in features of MFE.

While a number of default canned reports are generated on demand, AdHoc reports can be created by entering the following command string on the TSO/ISPF Command Line.

TSO $CLI,*MYQRY

This command sequence will display the TCE ADHOC Query & Display panel shown here:

```
◊─────────────── Function - TCE ADHOC Query & Display ───────────────◊
◊                ICE 16.0 MY - TCE Journalled Events                  ◊
◊                                                                     ◊
◊  ---------------- Set the Data Characterization Profile ----------  ◊
◊                    by Category .. or by EventClass ..               ◊
◊  --------------------- Set the Journal Query Range ---------------  ◊
◊  Begins with .. YY     MM     DD     & Ends with .. YY     MM     DD  ◊
◊  ---------------------- Check Presentation Format ----- .. NewOnly  ◊
◊    .. Active-Matrix  .. In-Summary  .. MetaDetail  .. FullDetail    ◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

Use PFK1 for Panel Help and directions.

On the other hand, Setting up MFE Interval Reports is done via the TCE Primary, MFE Support Interface. This MFE Specific Menu may be reached by logging onto the ICE Primary Menu, a VTAM application or by entering the command string on the TSO/ISPF Command Line.

TSO $CLI,*MYMFE

```
   -NSIMCLX 0707-  ICE 16.0 - MY Category Select - Multi-Factor Edit

--------TCE Parameter Settings------- ---CTLxx--- ------Last Update------
L  ADCD23C IFO.TEST.PARMLIB        SA 00 Yes   26          OBI1     2020/
P --LPAR-- ---ParmDsn Qualifier--- Sf Sf Act Ctls -UserId- yy/mm/dd hh:mm

----------------Controlled Dataset Category MFE Profiles---------------
Cm ----Category---- Mfe Cm ----Category---- Mfe Cm ----Category---- Mfe
.. SYSTEM.IPLPARM   --- .. PATS.OVERRIDE    (b) ..
.. SEQ.RPTS         --- .. JIMS.TEST        (c) ..
.. PAT.TEST1        --- ..                      ..
.. SYSTEM.TCPPARMS  --- ..                      ..
.. S047.DATASET     --- ..                      ..
.. PATS.STATS       --- ..                      ..
.. RFAUL1.PARMLIB   --- ..                      ..
.. GHB.PARMLIB      (v) ..                      ..
.. GHB.STAGED       (v) ..                      ..
.. PATS.ONETIME     (c) ..                      ..
.. NSEPARM.CONTROL  --- ..                      ..
.. SYSTEM.PARMLIB   (b) ..                      ..

   Dataset   Prompts   PadLock   MFEdits   EmlNote   On-Edit   DesCript
```

Once in the menu "Click" under MFEdits to reveal ADMIN and AUDIT reporting functions. If the user is a TCE ADMIN, the "Options Line" will shift to

```
Profile Log   Permit Log   MFAdmin   MFE Events   MFE Monitor
```

If the user is an MFE AUDIT, the "Options Line" will shift to

```
Profile Log   Permit Log   MFAudit   MFE Events   MFE Monitor
```

"Click" under MFAdmin or MFAudit to shift the "Options Line" back to its original state.

```
Dataset   Prompts   PadLock   MFEdits   EmlNote   On-Edit   DesCript
```

3.6. Does MFE Treat all users the same?

No, MFE treats General MFE Users, Administrators and Auditors differently, permitting each group to access only functions that are specifically designed to satisfy group needs.

A General MFE User is an individual that has been assigned an MFE User Profile and has been Permitted to one or more MFE Category Profiles. Such MFE users will likely experience only the "Challenge" to enter a Token that is presented by MFE Profiled Resources when they attempt to access. However, when the "NoEMail" is in use, the user will have to register and maintain a "Private MFEPrefix/PIN". To do this, they must enter the following command sequence on the TSO/ISPF Command Line:

TSO $CLI,*MYPIN

When the user presses enter, the following panel is displayed:

```
◊───────── Function - MFE UserId Permit Prefix Maintenance ─────────◊
◊              ICE 16.0 MY - MFE UserId Prefix Create                ◊
◊                                                                    ◊
◊  Old Prefix:_________  New Prefix:_________  Confirm New:_________ ◊
◊                                                                    ◊
◊           Enter 'S' .. and Press Enter to Create Prefix            ◊
◊                                                                    ◊
◊────────────────────────────────────────────────────────────────────◊
```

Use PFK1 for Panel Help and directions.

TCE Administrators and MFE Auditors are users with elevated TCE/MFE UserIds. The distinction between users is made in the NSEJRNxx ICE Parmlib Member using the following Control Cards:

For those that serve as TCE Administrators:

```
TCEPRIME userid
TCEADMIN (userid,userid,userid,userid,userid,userid)
```

The userid defined as TCEPRIME has the highest level of privilege within ICE/TCE/MFE.

For those that serve as MFE Auditors:

```
MFEAUDITOR userid
MFEROAUDITOR (userid,userid,userid,userid,userid,userid)
```

The userid defined as MFEAUDITOR has the highest level of privilege within the Auditor Group.

3.7. Does MFE Support All Dataset and File Types?

MFE Verification – Profile, Permit, Challenge – supports MVS Datasets, Load Libraries and Unix Files. MFE Certification provides direct vigilance over MVS Datasets and UNIX Files. A LOAD Library specific process provide vigilance over Libraries and Modules identifying changes by comparing META Data values from one hourly execution to the next.

3.8. Does ICE/TCE/MFE write SMF Records?

No! As is true with all ICE records, they are instead written to a secure Sequential Dataset Repository (Allocated as in RB4K Format) called the Control Journal(s). The architecture of this Event Driven Journaling and the many access controls that surround it allow it to be used by MFE as a “Block Chain” of all MFE events and actions. It represents the complete history (and isolation) of resource versions without the need for outboard instream message capture and/or post-processing.

3.9. Can MFE be Configured to Support Multiple Systems?

Yes! MFE, like all ICE controls, can share its configuration definitions and resources across a defined number of systems within a Managed ICE Group, eight by default.

3.10. Is MFE a Priced and/or Separately Licensed Product?

No! MFE is a fully integrated optional use component of The Control Editor (TCE) and can be used without additional Licensing or License Fee.

4. MFE Control Structures

The Control Structures that define and manage MFE and those that will be used to encode policy and then enforce them - MFE Profiles and Permits - are members housed in the ICE ParmLib Dataset – yourHLQ.PARMLIB.

4.1. Take Care, Use Caution

While each of these structures can be supported directly (with appropriate access rights) using TSO/ISPF, it is not a recommended ‘Best Practice’. While, as explained below, this appears simple, as Profiles and Permits increase in number, maintaining these manually may lead to confusion and diminished system integrity. To avoid such difficulty, a full interactive interface is available when using the MFE Boundary Definition Panels which may be accessed directly from the ICE Primary Menu or from the TSO/ISPF Command Line using the command sequence:

```
TSO $CLI,*MYMFE
```

The MFE Control Structures are explained in some detail here so that what they do and how they do it can be more clearly understood.

4.2. NSEJRNxx

NSEJRNxx is used to define the TCE Control Journals, Panel Descriptors and Settings of various TCE Options. MFE Settings and Options defined here include: ICE Resource Sharing, Administrators, Auditors, WAEMAIL Controls and MFE Descriptor.

4.2.1. MFE Control Sharing for Multi-System Support

MFE controls can be specific to a named System or support any number of systems in an ICE Managed Group. When control sharing is active, the definitions defined in the NSEJRNxx Member are those of the first system to enter the group. These configuration definitions determine the journal configuration. Should that Controlling System leave the Group for some reason, the next active system would assume control of the Group and the Journal attributes and its configuration. If the departing system returns it will automatically assume the configuration of the current controlling system.

To ensure the consistent application of MFE Control across all systems in a Group, it is a recommended ICE Best Practice to use a Shared ICE Parmlib Dataset containing a single NSEJRNxx member.

4.2.2. SHARE JOURNAL (number of LPARs in ICEPlex)

The ‘number’ specifies the maximum number of systems that can share the ICE Control Journal. The default is eight systems.

4.2.3. SHARE CONTROL (number of LPARs in ICEPlex)

The ‘number’ specifies the maximum number of systems that can share the NSECTLxx and NSEJRNxx configurations. The default is eight systems.

4.2.4. TCEPRIME userid

The TCE Prime Administrator has all/total ICE access privileges.

4.2.5. TCEADMIN (userid,userid,userid,userid,userid,userid)

TCE Administrators are somewhat less privileged than the TCE Prime Administrator. Up to six , comma separated, UserIds may be specified.

4.2.6. DETCHNGNOTIFY

Upon entry into Controlled Datasets, MFE Compares the current content of the selected member with the last copy stored. By default when a change is detected, a Pop-Up offering Certification Options is displayed. In NON-MFE Categories, the DETCHNGNOTIFY Control Card can be used to turn the Pop-Up off. If the Pop-Up is turned OFF, MFE will dynamically override the setting and turn it back ON.

4.2.7. MFEAUDITOR userid

The specified UserId is the Senior MFE Auditor and has all the privileges of a Read Only Auditor with a unique privileges that allow for the defining of Audit Report Sets, Reporting Intervals and Report Recipients.

4.2.8. MFEROAUDITOR (userid,userid,userid,userid,userid,userid)

MFE Read Only Auditors are somewhat less privileged, they may view and copy Profile Activity Logs and Permit Activity Logs, query the Journal for MFE Events and View Audit Report Sets defined by the Senior MFE Auditor. Up to six , comma separated, UserIds may be specified.

4.2.9. WAEMAILONLY YES|NO

WAEMAIL is a field in the WORKATTR User Profile Segment maintained by the External Security Manager. Typically used to distribute JES output, it can be also be used by MFE. If set YES, MFE will ensure that all Permitted User Profiles contain Email Addresses that are known to the ESM.

4.2.10. DESCPNL CAT(.MFE1DFT) PANEL(panel_name) BPC(parm)

Each CATEGORY has associated with it a Default or Defined Descriptor Panel. Use this Control Card to specifically define the Default panel to be used exclusively by MFE defined Categories.

4.3. NSECTLxx

NSECTLxx Control Cards are constructed as “Sets” of - MVS Datasets, UNIX Files or Load Libraries - bracketed by CATEGORY Statements to form a Category Control BLOCK.

4.3.1. CATEGORY category_name TYPE(parm) CNTL(parm) CHNG(parm)

The opening CATEGORY Statement defines the Category Name, Category Type – EDIT, LOAD and optionally the ROOT Directory for a set of UNIX Directories named that will be defined within the BLOCK and the Control and Change Parameters. The closing CATEGORY Statement, CATEGORY .END, is required to terminate the Control Block Structure.

4.3.1.1. TYPE

Specify ‘EDIT’ to signify that the CATEGORY will contain only MVS Partitioned or Sequential Datasets. Do not mix Partitioned and Sequential Datasets in the same CATEGORY. Specify ‘LOAD’ when defining a CATEGORY that contains only Load Libraries.

4.3.1.2. ROOT

When defining a UNIX File CATEGORY, specify the Root Directory that will precede the concatenation of Directory (DIRS) and/or File (FILE) specifications contained within the CATEGORY.

4.3.1.3. CNTL

Set the CNTL parm ‘ON’ to capture actions such as Un-Cataloging a Dataset, Deletion of a Module/Member, Renaming a Module/Member.

4.3.1.4. CHNG

Set the CHNG parm ‘ON’ to activate the Hourly Change Detection process for the CATEGORY.

4.3.1.5. AUTHVFY

The MFE specific Control Card activates Multi-Factor Edit User Verification and therefore presents a ‘Challenge’ to permitted users attempting access to resources defined within the CATEGORY. All other unpermitted users are automatically denied/warned during an access attempt. The following parms define these Verification actions.

- *FAILMSG/FMSG*

If set 'ON' a screen message is displayed when an access attempt is denied or token entry is rejected. The Default is 'ON'.

- *TOKENDISP/TKND*

If set 'OFF' the Token entry field is 'NULL' meaning the Token characters are not visible to the user when entering the Token. The Default is 'ON'.

- *WARN*

If the Keyword 'WARN' appears with the AUTHVFY Control Card, any user attempting access will be WARNED that the resource is under MFE Controls and that they would normally be denied access BUT that these controls have been currently relaxed to allow them access. Recommended for use only during initial testing and training of how MFE functions to enhance access control.

- *START/STOP DATE - SDT/EDT(yymmdd)*

If Start Date, YYMMDD is specified, MFE will be inactive until the start of that day. End Date is not necessary if MFE is to continue indefinitely.

- *START/STOP TIME - STM/ETM(hhmm)*

If Start Time (24 hour), HHMM is specified, MFE will be inactive until that time of day. If Start Date is also specified, it will be at the specified time on Start Day. If End Time is specified, MFE will cycle 'ON' then 'OFF' throughout the 24 hour period.

4.3.1.6. CERTVFY

Specifying this single Control Card, CERTVFY, will turn on Resource Certification Actions during Hourly Change Detection and during resource access attempts. On-Access Certification detection will result in the presentation of a panel showing multiple Certification Actions and/or Options.

4.3.2. CATEGORY .END

Required, ends the CATEGORY Control Block Set.

4.4. NSEENSxx

NSEENSxx – Defines MFE User Token Delivery Profiles – User’s Direct Email Address, 3rdParty Email Address(es), NoEMail Option - and their ‘WHEN” Permitted Categories/Profile Set. In addition, it defines the Email addresses of Administrators and/or Auditors that will receive Notifications/Alerts and/or Interval Reporting of MFE events.

4.4.1. ACTION MFEPERMT(userid) METHOD(parm)

MFEPERMT defines the delivery METHOD that will be used to send users (by UserId) an MFE Token or MFE Suffix.

When the use of Email is NOT an option, the METHOD parm should be set to ‘NOEMAIL’. This will result in the user, on Access Challenge, receiving a Suffix value that must be used with the user’s Private PIN. Only the correct concatenation of this “Token Material” entered into the challenging panel can permit access.

When the use of Email is acceptable, the METHOD parm should be set to ‘EMAIL’. This will result in the User or a Designee receiving an Email/SMS containing a Time Sensitive, One-Time Token. Only the correct entry of this Token into the challenging panel can permit the user access.

4.4.1.1. TO (permitted user’s email address)

Only one TO Email Address is honored. It must also be used as the FROM Address.

4.4.1.2. 3RDPARTY

Use this Control Card to direct Token delivery to a Third Party Designee. When used, the TO Email Address(es), one is acceptable, two advisable, must not be that of the user. This notwithstanding the FROM must always be that of the user.

4.4.1.3. FROM (permitted user’s email address)

The Email Address of the user.

4.4.1.4. START/STOP DATE - SDT/EDT(yymmdd)

If Start Date, YYMMDD is specified, MFE will DENY the user access until the start of that day. End Date is not necessary if MFE permission is to continue indefinitely. (Planned, not yet implemented)

4.4.1.5. START/STOP TIME - STM/ETM(hhmm)

If Start Time (24 hour), HHMM is specified MFE will DENY the user access until that time of day. If Start Date is also specified, it will be at the specified time on Start Day. If End Time is specified, MFE will cycle ‘ON’ then ‘OFF’ thoughtout a 24 hour period. (Planned, not yet implemented)

4.4.1.6. MFEPREFIX

The value of MFEPREFIX, which is maintained by the user, is always encoded using an MFE specific substitution cipher and may only be updated using the MFE Line Command Interface command sequence shown below.

TSO $CLI,*MYPIN.

4.4.1.7. WHEN MFECATEGORY(category_name)

The WHEN Control Card defines which MFE Category/Profiles a user will be permitted to validly access when presented by correctly completing an Access Challenge.

4.4.2. ACTION .END

Required, ends the MFEPERMT Control Block Set.

4.4.3. ACTION MFECAT(category_name)

This Action Block Set is used to define the TO and FROM Email Address(es) and Subject of Notification/Alert emails that will be sent in real time to TCE/MFE Administrators denoting MFE Actions and/or Events.

4.4.3.1. TO (as many as necessary)

4.4.3.2. FROM

4.4.3.3. SUBJECT

4.4.4. ACTION .END

4.4.5. ACTION MFEAUD(category_name)

This Action Block Set is used to define the TO and FROM Email Address(es) and Subject of Notification/Alert emails that will be sent in real time to MFE Auditors denoting MFE Actions and/or Events.

4.4.5.1. TO (as many as necessary)

4.4.5.2. FROM

4.4.5.3. SUBJECT

4.4.6. ACTION .END

4.4.7. ACTION MFEAMDAY/WKS/MTH(userid)

This Action Block Set is used to define the TO and FROM Email Address(es) and Subject of Interval Reporting emails, will be sent to TCE/MFE Administrators containing a specified set of MFE Activity Reports.

4.4.7.1. TO (as many as necessary)

4.4.7.2. FROM

4.4.7.3. SUBJECT

4.4.8. ACTION .END

4.4.9. ACTION MFEAUDAY/WKS/MTH(userid)

This Action Block Set is used to define the TO and FROM Email Address(es) and Subject of Interval Reporting emails, will be sent to TCE/MFE Auditors containing a specified set of MFE Activity Reports.

4.4.9.1. TO (as many as necessary)

4.4.9.2. FROM

4.4.9.3. SUBJECT

4.4.10. ACTION .END

4.4.11. ACTION PSWDEXP(USERID) METHOD(EMAIL) SCOPE(REPORT)

This Action Block Set is used to define the TO and FROM Email Address(es) and Subject of Expiration Notifications will be sent to Users with MFE Permit Profiles.

4.4.11.1. TO

Permitted MFE User’s Email Address

4.4.11.2. ALIAS

Is used to MASK the User’s userid.

4.4.11.3. INTERVAL (0,1,2,3,4,5,15,30)

Specifies the Notification day prior to password expiration. Values shown are the defaults.

4.4.11.4. SUBJECT 'EXPIRE NOTIFICATION'

Quoted string is the SUBJECT Default Value

4.4.11.5. FROM

May be any valid Email Address

4.4.12. ACTION .END

Required, ends the PSWDEXP Control Block Set.

4.5. NSEDETxx

Settings in the NSEDETxx Member defines the Daily, Weekly and Monthly intervals that function in conjunction matching NSEENSxx user and group email delivery settings. Working together they ensure that Administrative and Audit Interval Reports are prepared and delivered. This pairing notwithstanding NSEDETxx can work independently to create reports that are stored as Members in Registry Datasets and made viewable via the MFE Panel Interface.

4.5.1. MFEDETECDAY/WKS/MTH ON|OFF

Used to define the Administration Report Delivery Cycle

4.5.2. MFEDETAMDAY/WKS/MTH ON|OFF

Used to define the Auditor Report Delivery Cycle

4.5.2.1. CYCLE(DAILY) TIME(hh:mm) INTERVAL(1 - 12)

4.5.2.2. CYCLE(WEEKLY(MON,TUE,WED,THR,FRI,SAT,SUN)) TIME(hh:mm)

4.5.2.3. CYCLE(MONTHLY(DOM(day_number)EOM)) TIME(hh:mm)

An explanation of all Detector configuration parameters, Operational Keywords, Detector Identifiers, Sub-Keywords and Full Syntax can be found in the ICE Supplemental Detectors User Guide.

5.MFE Panel Interface

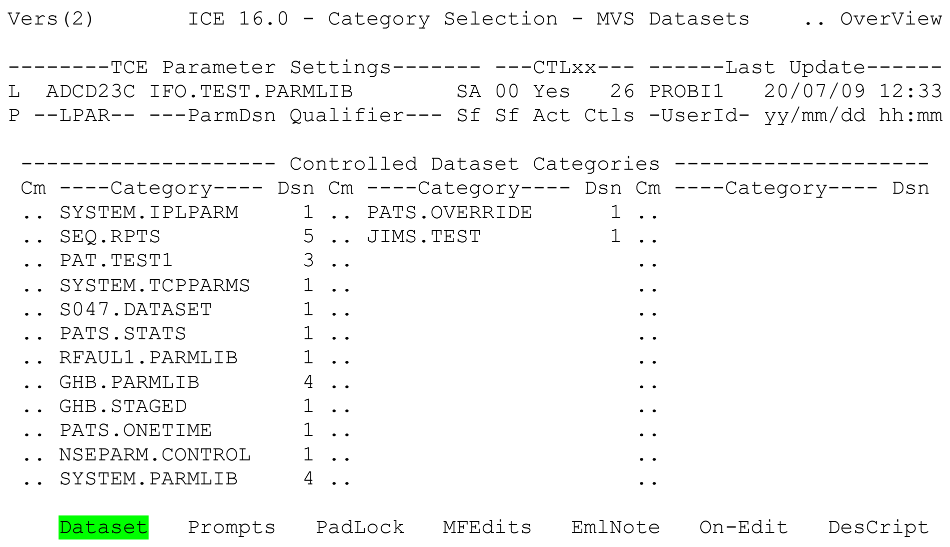
The MFE Panel Interface supports a collection of ISPF Dialogs that assist in:

1. Configuring MFE Category Profiles for Verification,
2. Configuring MFE Category Profiles for Certification,
3. Defining Users and Permitting them to MFE Profiles,
4. Access to Notification of various Notification Options,
5. Viewing of On-Line MFE Logs and Activity Reports,
6. Defining ADMIN and AUDIT Report Sets, and
7. Setting of Interval Reporting Delivery Timings.

Each will be explained in this section.

5.1. The MFE Primary Category Dialog

The MFE Primary Boundary Category Dialog may be reached via the ICE Primary Menu by selecting Controls and then Boundary and then Datasets, LoadLibs or USSFiles. If Datasets is selected, the following panel is displayed.



```
Vers(2)       ICE 16.0 - Category Selection - MVS Datasets    .. OverView

--------TCE Parameter Settings------- ---CTLxx--- ------Last Update------
L  ADCD23C IFO.TEST.PARMLIB        SA 00 Yes   26 PROBI1   20/07/09 12:33
P --LPAR-- ---ParmDsn Qualifier--- Sf Sf Act Ctls -UserId- yy/mm/dd hh:mm

 -------------------- Controlled Dataset Categories --------------------
 Cm ----Category---- Dsn Cm ----Category---- Dsn Cm ----Category---- Dsn
 .. SYSTEM.IPLPARM     1 .. PATS.OVERRIDE      1 ..
 .. SEQ.RPTS           5 .. JIMS.TEST          1 ..
 .. PAT.TEST1          3 ..                      ..
 .. SYSTEM.TCPPARMS    1 ..                      ..
 .. S047.DATASET       1 ..                      ..
 .. PATS.STATS         1 ..                      ..
 .. RFAUL1.PARMLIB     1 ..                      ..
 .. GHB.PARMLIB        4 ..                      ..
 .. GHB.STAGED         1 ..                      ..
 .. PATS.ONETIME       1 ..                      ..
 .. NSEPARM.CONTROL    1 ..                      ..
 .. SYSTEM.PARMLIB     4 ..                      ..

    Dataset   Prompts   PadLock   MFEdits   EmlNote   On-Edit   DesCript
```

Only one Boundary Type – Datasets, LoadLibs, USSFiles – may be managed at a time. If you wish to switch Types, PKF3 back to the Boundary Selection Menu.

Take note at the bottom of the panel ‘MFEdits’, cursor under it and press enter to reach the MFE Primary Dialog shown below.

```
Vers(2)       ICE 16.0 - Category Selection - Multi-Factor Edit

--------TCE Parameter Settings------- ---CTLxx--- ------Last Update------
L  ADCD23C IFO.TEST.PARMLIB        SA 00 Yes   26 PROBI1   20/07/09 12:33
P --LPAR-- ---ParmDsn Qualifier--- Sf Sf Act Ctls -UserId- yy/mm/dd hh:mm

 ----------------Controlled Dataset Category MFE Profiles---------------
 Cm ----Category---- Mfe Cm ----Category---- Mfe Cm ----Category---- Mfe
 .. SYSTEM.IPLPARM   --- .. PATS.OVERRIDE    (b) ..
 .. SEQ.RPTS         --- .. JIMS.TEST        (c) ..
 .. PAT.TEST1        --- ..                      ..
 .. SYSTEM.TCPPARMS  --- ..                      ..
 .. S047.DATASET     --- ..                      ..
 .. PATS.STATS       --- ..                      ..
 .. RFAUL1.PARMLIB   --- ..                      ..
 .. GHB.PARMLIB      (v) ..                      ..
 .. GHB.STAGED       (v) ..                      ..
 .. PATS.ONETIME     (c) ..                      ..
 .. NSEPARM.CONTROL  --- ..                      ..
 .. SYSTEM.PARMLIB   (b) ..                      ..

    Dataset    Prompts    PadLock    MFEdits    EmlNote    On-Edit    DesCript
```

5.2. Access Via the TSO/ISPF Command Line

This Dialog may also be reached directly from the native TSO/ISPF Command Line by entering:

TSO $CLI,*MYMFE

If USSFiles Categories are the target use:

TSO $CLI,*MYMFE,USS

If LoadLibs are the target

TSO $CLI,*MYMFE,LIB

5.3. Dialog Functional Description

Mulit-Factor Edit (MFE) is an extension of the control structures that surround a TCE Category. When used, it requires that a category be defined as an MFE Profile. To do this, select a Category with 'S' and press Enter. Categories with defined MFE Profiles are denoted on panel with (v)/(c)/(b). Once a Profile is defined, all access to associated Datasets, Files & Libraries is denied/warned unless users are specifically Permitted. Permitted users attempting access receive a required One-Time PassTicket to continue. All related actions invoke TCE Descriptor, Journaling and when '(c)' On-Edit Certification Detection. To Permit a user to a Category/Profile enter 'P' adjacent to the category name and press Enter. Cursor under MFEedit then press enter, shifts the panel to the ADMIN/AUDIT reporting view.

Text underlined and shown in white are point-and-shoot hot spots. Cursor under and press enter to drill-down to their supported feature. For example cursor under a Category Name and press enter to see the names of its Category Resources.

5.3.1. Text shown in the ‘Mfe’ Column indicates Category State

- *‘---’*

Indicates NO MFE Profile.

- *‘(v)’*

Indicates that the Category has a functional Verification Profile.

- *‘(c)’*

Indicates that the Category has a functional Certification Profile.

- *‘(b)’*

Indicates that the Category has both a Verification and Certification Profile.

5.3.2. To Create or Update an MFE Category Profile

Enter ‘S’ on the insertion point preceding the Category Name and press enter.

5.3.3. To Permit or Update User Permissions to a Category Profile

Enter ‘P’ on the insertion point preceding the Category Name and press enter.

5.3.4. Switching to Reporting Mode

To switch Dialog Mode so that Logs, Query and Reporting will be displayed, cursor under MFEdits and press enter. Depending on your MFE Role, ADMIN or AUDIT, the Option Line at the bottom of the panel will shift.

For ADMINs, it will look like this:

Profile Log   Permit Log   MFAdmin   MFE Events   MFE Monitor

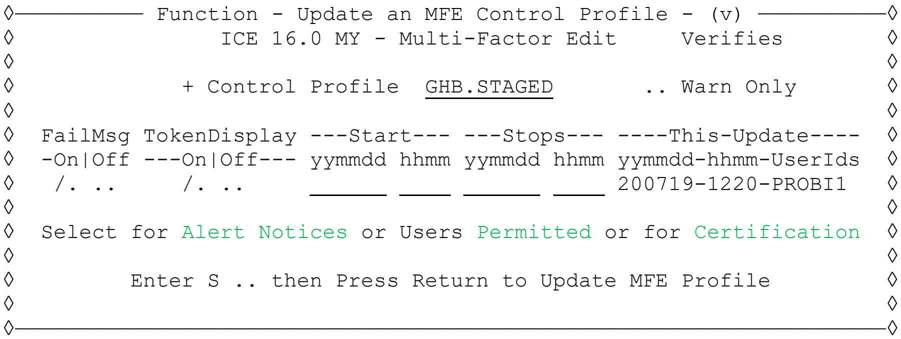
For AUDITs, it will look like this:

Profile Log   Permit Log   MFAudit   MFE Events   MFE Monitor

Cursor under MFAdmin/MFAudit and press enter to shift the Option Line back to its original state.

5.4. Configuring MFE Category Profiles for Verification

When ‘S’ is used to select a Category from the MFE Primary Menu the following dialog is displayed. Use the dialog to elevate a Category as a MFE Profile. By default, the Failed Message, Token Display and Deny Mode are ON. When a Category is also an active MFE Profile the panel will show ‘Verifies (v)’ in its upper right, ‘Certifies (c)’ if only a Certification Profile and ‘Veri/Cert (b)’ if both.



```
◊────────── Function - Update an MFE Control Profile - (v) ──────────◊
◊               ICE 16.0 MY - Multi-Factor Edit     Verifies         ◊
◊                                                                    ◊
◊             + Control Profile  GHB.STAGED       .. Warn Only       ◊
◊                                                                    ◊
◊  FailMsg TokenDisplay ---Start--- ---Stops--- ----This-Update----  ◊
◊  -On|Off ---On|Off--- yymmdd hhmm yymmdd hhmm yymmdd-hhmm-UserIds  ◊
◊   /. ..     /. ..     ______ ____ ______ ____ 200719-1220-PROBI1   ◊
◊                                                                    ◊
◊  Select for Alert Notices or Users Permitted or for Certification  ◊
◊                                                                    ◊
◊         Enter S .. then Press Return to Update MFE Profile         ◊
◊                                                                    ◊
◊────────────────────────────────────────────────────────────────────◊
```

5.4.1. Inserting an AUTHVFY Control Card

Selecting Update will add the AUTHVFY Control Card within CATEGORY Control Block of the selected Category as defined in the NSECTLxx ICE ParmLib Member. None of the Options described below are necessary as the key default values for FAILMSG, TOKENDISP and “DENY” will be taken when otherwise not specified. All MFE Update/Removal actions result in Profile Audit Log Records.

5.4.1.1. FailMsg

By Default ON to show Message when TOKEN entry fails.

5.4.1.2. TokenDisp

By Default ON to show visible area for entry of TOKEN. When OFF, TOKEN entry area is masked.

5.4.1.3. StartDate

Optional YY/MM/DD when MFE Controls become active. If not specified AUTHVFY takes effect upon activation.

5.4.1.4. StartTime

Optional (24) HH:MM when MFE takes effect. If no date, daily.

5.4.1.5. StopDate

Optional YY/MM/DD when MFE Controls become inactive. If not specified, AUTHVFY remain in effect indefinitely.

5.4.1.6. StopTime

Optional (24) HH:MM when MFE ceases. If no date, daily.

5.4.2. Updating, Removing a Profile

5.4.2.1. 'S'

Enter to create a new Profile or update an existing Profile.

5.4.2.2. 'R'

Enter to remove an existing Profile. This action is followed by a display of UserId(s) permitted to the profile, each of which may optionally be removed as well.

5.5. MFE Profiled Categories – ISPF Worksheet and Report

Cursor under the '±' shown in the upper left of the panel and press enter to display All Category Profiles and related settings.

```
 -NSIMRBX 0717- ICE 16.0 - MY MFE Category Profiles          Row 1 to 14 of 19
                                                             ---MFE Profiles---
------------------ 19 TCE Categories 10 MFE Defined Profiles ------------------
Row Selection: Show_Permitted_and_Unpermitted_UserIds_to_Selected_Category
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Line -----Control----- Usr ---Named Profiles--- ----Starts---- ----Stops-----

_ ____ ____ ____ ___ ___ ___ ____________________ ________ _____ ________ _____
S Numb Type Cntl Msg Tkn Ids -----Categories----- yy/mm/dd hh:mm yy/mm/dd hh:mm
_ 0001 DSNS None --- --- --- SYSTEM.IPLPARM       --/--/-- --:-- --/--/-- --:--
_ 0002 DSNS None --- --- --- SEQ.RPTS             --/--/-- --:-- --/--/-- --:--
_ 0003 DSNS None --- --- --- PAT.TEST1            --/--/-- --:-- --/--/-- --:--
_ 0004 LOAD None --- --- --- GHB.LOADMON          --/--/-- --:-- --/--/-- --:--
_ 0005 LOAD None --- --- --- PATS.PLAYLOAD        --/--/-- --:-- --/--/-- --:--
_ 0006 LOAD DVfy  On  On --- PAUL.PLAYLOAD        --/--/-- --:-- --/--/-- --:--
_ 0007 DSNS None --- --- --- SYSTEM.TCPPARMS      --/--/-- --:-- --/--/-- --:--
_ 0008 UNIX DVfy  On  On --- PATS.DIR5            --/--/-- --:-- --/--/-- --:--
_ 0009 DSNS None --- --- --- S047.DATASET         --/--/-- --:-- --/--/-- --:--
_ 0010 DSNS None --- --- --- PATS.STATS           --/--/-- --:-- --/--/-- --:--
_ 0011 DSNS None --- --- --- RFAUL1.PARMLIB       --/--/-- --:-- --/--/-- --:--
_ 0012 DSNS DVfy  On  On 002 GHB.PARMLIB          20/07/01 --:-- --/--/-- --:--
_ 0013 DSNS DVfy  On  On 002 GHB.STAGED           --/--/-- --:-- --/--/-- --:--
_ 0014 DSNS WCfy  On  On 002 PATS.ONETIME         20/08/04 --:-- --/--/-- --:--
```

This Worksheet presents a summary of MFE Profiles with specific information about Profiles Settings with direct access to UserIds permitted/not permitted to related Profiled resources. Enter Report on the Command Line and then press enter to View/Move/Copy related Profile Report(s).

5.5.1. Column Headings

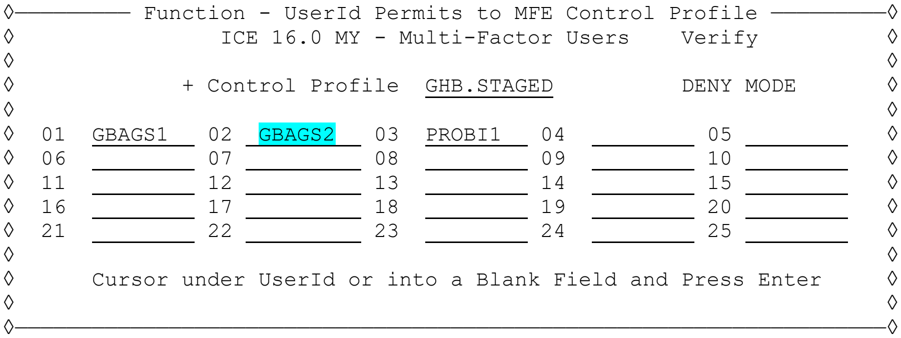
Numb: Worksheet Row Number.
Type: DSNS = Dataset, UNIX = UNIX File, LOAD = Library.
Cntl: Type of Control - None, Warn, Deny
Msg: If 'On' Fail Message Pop-Up on Token Entry Failures.
Tkn: If 'On' Token Entry Panel Shows View of Token Entry.
Ids: The Number of UserIds Permitted to the Profile.
Category: Category/Profile Name
yy/mm/dd: Year/Month/Day when Profile Became an Active Control.
hh:mm: Hour/Minute when Profile Became an Active Control.
yy/mm/dd: Year/Month/Day when Profile Becomes In-Active Control.
hh:mm: Hour/Minute when Profile Becomes In-Active Control.

5.5.2. Row Commands

‘S’ Present a Table of All MFE Active UserIds indicated by the Color turquoise, which are Permitted to the selected Profile.

5.6. Permitting User to MFE Category Profiles

Once a Category is Profiled users must be specifically permitted to it in order to gain resource access. The panel shown below is the focal point to this activity and can be reached directly from the MFE Primary Boundary Menu using the ‘P’ Category selection option or from the Profile Panel that will precede it when the ‘S’ option is used and then ‘Permitted’ is selected.



```
◊────────── Function - UserId Permits to MFE Control Profile ─────────◊
◊                 ICE 16.0 MY - Multi-Factor Users    Verify           ◊
◊                                                                      ◊
◊              + Control Profile  GHB.STAGED          DENY MODE        ◊
◊                                                                      ◊
◊  01  GBAGS1___  02  GBAGS2___  03  PROBI1__  04  ________  05  ________  ◊
◊  06  ________   07  _________  08  ________  09  ________  10  ________  ◊
◊  11  ________   12  _________  13  ________  14  ________  15  ________  ◊
◊  16  ________   17  _________  18  ________  19  ________  20  ________  ◊
◊  21  ________   22  _________  23  ________  24  ________  25  ________  ◊
◊                                                                      ◊
◊      Cursor under UserId or into a Blank Field and Press Enter       ◊
◊                                                                      ◊
◊──────────────────────────────────────────────────────────────────────◊
```

5.6.1. Selecting a Permitted UserId

All MFE Permitted UserIds must have a unique Access Profile. This panel presents all Permitted UserIds with the option of selecting and displaying their Access Profile - Token Delivery Information and the complete set of MFE Category Profiles they are permitted access to or not. Those UserIds shown in WHITE are not permitted to the Target Category selected in the prior panel(s). Those Highlighted in TURQUOISE are permitted. To select either and display their Delivery and Permit specifics, cursor under the UserId and press enter. In the panel that follows all Category Profiles are shown but only the Category Target will be accessible for update. Selecting the Target permits the User or deselecting the Target removes the user’s access permission.

5.6.2. Permitting a New UserId

New Users: To add a new User to a Category’s Permitted List, select an unused field, cursor into it, and press Enter. In the panel that follows, the UserId Field will appear at the Upper Left. If an existing user’s profile is being updated it cannot be altered. If a new user is being permitted entering the field will accept the target UserId. All Delivery Information fields are open as is the entry point preceding Category Target. Complete as needed. Permit to a Profile takes effect immediately upon exit (PFK3) from the panel.

5.7. *Defining the Users Permit Profile and Permissions*

Having selected a UserId the user's Permit Profile – Delivery Information and Permitted Categories – is displayed. Confirm the selected UserId as shown in the left of the panel. Update the user's delivery information as needed. Check '/' or Un-Check the Target Category as necessary to add or remove.

```
  -NSIMRBX 0717-  ICE 16.0 MY - Permit & Deliver - Email or /. NoEMail

Permit PROBI1   WAAddr prr@newera.com____________________________ /. Xp
Start Date ________ Time _____ End Date ________ Time ______ Day________
Designee-One .. WAAddr __________________________________________________
Designee-Two .. WAAddr __________________________________________________
Subject of Token Alert My MFE Token
 --- Check Either/Both Designee-One/Two to Denote 3rd-Party Delivery ---

 ----------------Controlled Dataset Category MFE Profiles---------------
 Cm ----Category---- Mfe Cm ----Category---- Mfe Cm ----Category---- Mfe
 .. SYSTEM.IPLPARM   --- /. PATS.OVERRIDE    (v) .. ________________ ___
 .. SEQ.RPTS         --- .. JIMS.TEST        (c) .. ________________ ___
 .. PAT.TEST1        --- .. ________________ ___ .. ________________ ___
 .. SYSTEM.TCPPARMS  --- .. ________________ ___ .. ________________ ___
 .. S047.DATASET     --- .. ________________ ___ .. ________________ ___
 .. PATS.STATS       --- .. ________________ ___ ..________________  ___
 .. RFAUL1.PARMLIB   --- .. ________________ ___ ..________________  ___
 .. GHB.PARMLIB      (v) .. ________________ ___ ..________________  ___
 .. GHB.STAGED       (v) .. ________________ ___ ..________________  ___
 .. PATS.ONETIME     (c) .. ________________ ___ ..________________  ___
 .. NSEPARM.CONTROL  --- .. ________________ ___ ..________________  ___
 /. SYSTEM.PARMLIB   (b) .. ________________ ___ ..________________  ___
```

5.7.1. *Delivery*

An MFE Token is dynamically generated and delivered when a Permitted UserId attempts to access a Profile Resource.

5.7.2. *Permit*

UserId Permitted Profile Access with Token received at Address. If no '@' in Address, value is assumed to be a valid UserId, WAEMAIL Lookup automatic.

5.7.3. *Designee*

One or Two possible alternate recipients of Token. When used, the UserId, a '/' and Email Address are required to signify that a 3rd Party will receive the Token. The Permitted user will not receive but is the only one who may use the token. Permitted user & Designee must cooperate.

5.7.4. *Permits*

If Targeted Category/Profile is checked '/', the user is permitted. Uncheck to remove the permission. If not checked, enter '/' to permit user to the Category/Profile. Only the Target may be altered in these ways.

5.7.5. Updates

Changes in either Delivery/Permits are monitored. If detected when you Exit/PFK3, all underlying control files & structures are automatically updated and activated.

5.8. All Permitted Users – ISPF Worksheet and Report

Cursor under the '+' shown in the upper left of the panel and press enter to display All Permitted Users and the Categories they may access.

```
-NSIMRBX 0717- ICE 16.0 - MY Active MFE Category Profiles   Row 1 to 12 of 12
----MFEPermits----
------------ 5 Active MFE Category Profiles Permit 3 Active UserIds -----------
Row Selection: Shows_UserId_MFE_Permit_Details View_UserId_Resource_Access_List
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Row -----Control----- -Permit- -Named Profiles- ----Starts---- ----Stops-----

_ ___ ____ ____ ___ ___ ________ ________________ ________ _____ ________ _____
S Num Type Cntl Msg Tkn -UserId- ---Categories--- yy/mm/dd hh:mm yy/mm/dd hh:mm
_ 001 DSNS DCfy  On  On GBAGS2   SYSTEM.PARMLIB   --/--/-- --:-- --/--/-- --:--
_ 002 DSNS DCfy  On  On PROBI1   SYSTEM.PARMLIB   --/--/-- --:-- --/--/-- --:--
_ 003 DSNS DCfy  On  On GBAGS1   SYSTEM.PARMLIB   --/--/-- --:-- --/--/-- --:--
_ 004 DSNS DVfy  On  On GBAGS2   GHB.PARMLIB      20/07/01 --:-- --/--/-- --:--
_ 005 DSNS DVfy  On  On GBAGS1   GHB.PARMLIB      20/07/01 --:-- --/--/-- --:--
_ 006 DSNS WCfy  On  On GBAGS2   PATS.OVERRIDE    20/07/01 --:-- --/--/-- --:--
_ 007 DSNS WCfy  On  On PROBI1   PATS.OVERRIDE    20/07/01 --:-- --/--/-- --:--
_ 008 DSNS WCfy  On  On GBAGS1   PATS.OVERRIDE    20/07/01 --:-- --/--/-- --:--
_ 009 DSNS WCfy  On  On GBAGS2   PATS.ONETIME     20/08/04 --:-- --/--/-- --:--
_ 010 DSNS WCfy  On  On GBAGS1   PATS.ONETIME     20/08/04 --:-- --/--/-- --:--
_ 011 DSNS DVfy  On  On GBAGS2   GHB.STAGED       --/--/-- --:-- --/--/-- --:--
_ 012 DSNS DVfy  On  On GBAGS1   GHB.STAGED       --/--/-- --:-- --/--/-- --:--
```

Worksheet presents a view of overall MFE Categories and users that are permitted to them. Cursor under a UserId and press enter to view users permitted resources.

5.8.1. Column Headings

Numb   Worksheet Row Number.
Type   DSNS = Dataset, UNIX = UNIX File, LOAD = Library.
Cntl   Type of Control - None, Warn, Deny
Msg   If 'On' Fail Message Pop-Up on Token Entry Failures.
Tkn   If 'On' Token Entry Panel Shows View of Token Entry.
Userid   The UserId Permitted to the MFE Category Profile.
Category   MFE Category/Profile Name
yy/mm/dd Start - Year/Month/Day when Profile Became an Active Control.
hh:mm   Start - Hour/Minute when Profile Became an Active Control.
yy/mm/dd Stop - Year/Month/Day when Profile Becomes an In-Active Control.
hh:mm   Stop - Hour/Minute when Profile Becomes an In-Active Control.

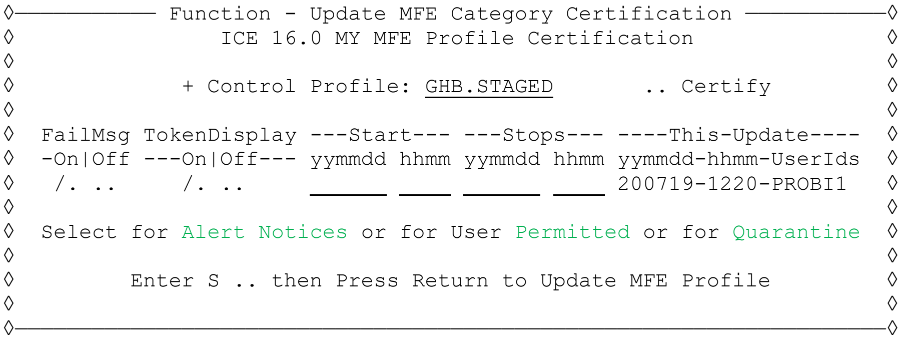
5.8.2. Row Commands

'S'   Shows the selected UserId Permit Profile Settings; Token Delivery specifics and Permitted MFE Categories.

'V'   View the Dataset, Libraies and Files that a UserId may Access as a result of Permission to an MFE Category.

5.9. Configuring MFE Category Profiles for Certification

Selecting the “Certification” option shown on the Control Profile Definition Panel, shown earlier, will display the Category Certification panel shown below. If the resources defined to the profile are be “Certified” Check ‘/’ Certify, enter ‘S’ and press return. Such an update returns to the prior panel, take note of the Verification/Certification indicator shown, upper right, of the Control Profile Definition panel. It will either show ‘Certify’ to indicate the Category resources are certified only or ‘Veri/Cert’ to indicate that they are both Verified and Certified.



```
◊─────────── Function - Update MFE Category Certification ───────────◊
◊                ICE 16.0 MY MFE Profile Certification                ◊
◊                                                                     ◊
◊             + Control Profile: GHB.STAGED       .. Certify          ◊
◊                                                                     ◊
◊  FailMsg TokenDisplay ---Start--- ---Stops--- ----This-Update----   ◊
◊  -On|Off ---On|Off--- yymmdd hhmm yymmdd hhmm yymmdd-hhmm-UserIds   ◊
◊   /. ..      /. ..    ______ ____ ______ ____ 200719-1220-PROBI1    ◊
◊                                                                     ◊
◊  Select for Alert Notices or for User Permitted or for Quarantine   ◊
◊                                                                     ◊
◊         Enter S .. then Press Return to Update MFE Profile          ◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

As is the case with the Control Profile Definition Panel all Profile definitions shown in this panel may be updated equally using this panel.

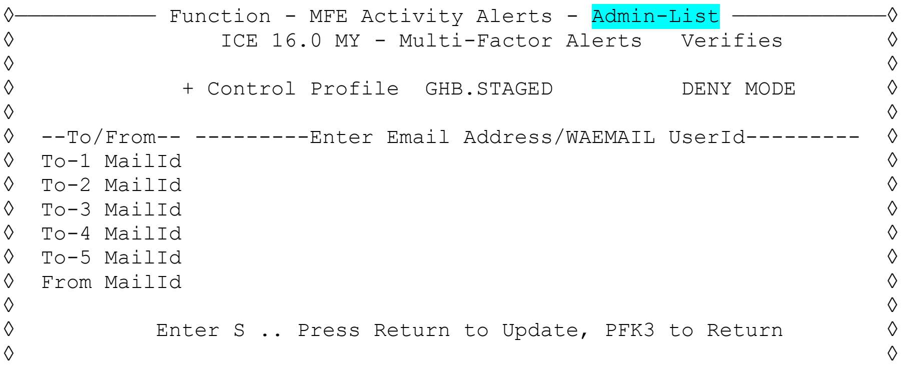
5.9.1. All Isolated Resources – ISPF Worksheet and Report

Cursor under the ‘+’ shown in the upper left of the panel and press enter to display All Isolated Resources.

5.9.1. Isolated

Curson under the white, underlined word Isolated to show a list of Isolated Resources in the selected Category.

5.10. Notification/Alerts of MFE Events and Actions



```
◊─────────── Function - MFE Activity Alerts - Admin-List ────────────◊
◊                ICE 16.0 MY - Multi-Factor Alerts   Verifies         ◊
◊                                                                     ◊
◊             + Control Profile  GHB.STAGED          DENY MODE        ◊
◊                                                                     ◊
◊  --To/From-- ---------Enter Email Address/WAEMAIL UserId---------   ◊
◊  To-1 MailId                                                        ◊
◊  To-2 MailId                                                        ◊
◊  To-3 MailId                                                        ◊
◊  To-4 MailId                                                        ◊
◊  To-5 MailId                                                        ◊
◊  From MailId                                                        ◊
◊                                                                     ◊
◊           Enter S .. Press Return to Update, PFK3 to Return         ◊
◊                                                                     ◊
```

The Notification Dialog allows up to five ADMIN and Five AUDIT Recipients to be added to the distribution list for MFE Email Alerts.

5.10.1. MFE Alerts Report on These Events

5.10.1.1. <ALLOW>

The edit was allowed to proceed because the user was permitted to the resource and proper edit token was received and properly entered.

5.10.1.2. <WARNS>

WARN mode was active and the access allowed to occur even without a proper Token.

5.10.1.3. <FAILS>

Did the MFE access attempt fail due to the edit token having reach timeout?
Did the MFE fail due to the entry of an incorrect MFE supplied token?

5.10.1.4. <3PART>

Did a Designee receive notification of an in process access attempt?

5.10.1.5. MFE Notification Alerts Contain

Day, Date, Time, UserId and an indication of one of the events described above and the impacted resource. All Alerts are Journaled.

5.10.1.6. Adding/Removing a Recipient

To add recipients to Alert List, cursor into available field & enter either fully qualified Email Address or a UserId & press enter. If UserId, call is made to ESM to extract address from WORKATTR Segment. On success, address is entered, if not, conditional message displayed.

5.11. *Viewing On-Line MFE Logs and Activity Reports*

All actions that impact a Category Profile and User Permissions are Logged and form the basis of on-line and interval Reports. The on-line worksheets are shown and explained below.

5.11.1. *Profile Log*

Profile Log   Permit Log   MFAudit   MFE Events   MFE Monitor

The Worksheet shown below shows Groups of Categories with access to their individual histories.

```
 -NSIMRBX 0717-  ICE 16.0 - MY MFE Category Profile Groups     Row 1 to 9 of 9
                                                                ---Audit Groups---
-------------------------- 9 Category Profile Groups --------------------------
Row Selection: List_the_Group_Records Displays_All_Current_Profile_Control_Info
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Row ----Profile Group---- ------Last Updated------ ---Controls--- ---Start---

_ ___ ___ _________________ ___ ______ ____ ________ ____ ____ ____ ______ ____
S Num Ttl ---MFECategory--- Act yymmdd hhmm -UserId- Mode Fail Tokn yymmdd hhmm
_ 001  13 JIMS.TEST         DEL 200717 1639   PROBI1 DCfy   On   On ------ ----
_ 002   7 PATS.OVERRIDE     UPD 200717 1610   PROBI1 WVfy   On   On 200701 ----
_ 003   3 SYSTEM.PARMLIB    UPD 200717 0539   PROBI1 DCfy   On   On ------ ----
_ 004  20 PATS.ONETIME      UPD 200714 1356   PROBI1 WCfy   On   On 200804 ----
_ 005   3 GHB.STAGED        UPD 200714 1208   GBAGS1 DVfy   On   On ------ ----
_ 006   7 GHB.PARMLIB       UPD 200709 1144   PROBI1 DVfy   On   On 200701 ----
_ 007   2 RFAUL1.PARMLIB    DEL 200609 1153   GBAGS2 DVfy   On   On ------ ----
_ 008   2 PATS.STATS        DEL 200609 0900   PROBI1 DVfy   On   On ------ ----
_ 009   1 DTCC.PAGENT       NEW 200609 0859   PROBI1 DVfy   On   On ------ ----
******************************* Bottom of data ********************************
```

A Profile Group is a collection of Profile Audit Records grouped by MFE Category Profile by UserId. The number in Permit Column reflects unique UserId Permits. L will List the Records by UserId. Record shown is Last update to the Profile. Enter REPORT on the command line and press enter to View/Move/Copy related Profile Report(s).

5.11.1.1. *Column Headings*

Permit: Number in Permit Group or UserId.
MFECat : MFE Category Profile Name.
Act: Last Action Taken - ADD, UPD, DEL.
Yymmdd: Year, Month, Day of Last Action.
hhmm: Hour, Minute of Last Action.
UserId: User taking the Last Action.
Mode: Profile Mode of Operation - Deny or Warn.
Fail: If On (Default) Message Pop-Up on Token Failed Entry.
Tokn: If On (Default) Token Entry Point shown in Panel.
Starts: Date Profile operational, if none, in operation now.

5.11.1.2. Row Commands

L List, by UserId, members of selected Profile Group.
D Displays full set of Defined Profile Controls.

5.11.2. Permit Log

Profile Log Permit Log MFAudit MFE Events MFE Monitor

The Worksheet below shows Groups of Permitted Users with access to their individual histories.

```
 -NSIMRBX 0717-  ICE 16.0 - MY MFE Category Permitted Groups Row 1 to 14 of 26
                                                             ---Audit Groups---
----------------------- 26 Category Permit UserId Groups ----------------------
Row Selection: List_the_Group_Records Display_UserId_Token_Delivery_Information
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Row ----Permit Category Groups---- ------Last Updated------ ----Designate----

_ ___ ___ ________ _________________ ___ ______ ____ ________ ________ ________
S Num Ttl -UserId- ---MFECategory--- Act yymmdd hhmm -UserId- -Desg01- -Desg02-
_ 001   6   PROBI1 JIMS.TEST         DEL 200717 1644   PROBI1  -------  -------
_ 002   7   GBAGS1 JIMS.TEST         ADD 200610 1513   PROBI1   PHARL1  -------
_ 003  16   PROBI1 SYSTEM.PARMLIB    UPD 200716 1120   PROBI1  -------  -------
_ 004   2   GBAGS2 SYSTEM.PARMLIB    ADD 200709 1006   PROBI1  --Yes--  -------
_ 005   2   GBAGS1 SYSTEM.PARMLIB    ADD 200709 1002   PROBI1  --Yes--  -------
_ 006  34   PROBI1 PATS.OVERRIDE     UPD 200714 1247   PROBI1  -------  -------
_ 007   1   GBAGS2 PATS.OVERRIDE     ADD 200709 1007   PROBI1  --Yes--  -------
_ 008   2   GBAGS1 PATS.OVERRIDE     ADD 200709 1001   PROBI1  --Yes--  -------
_ 009   6   GBAGS2 GHB.STAGED        UPD 200714 1234   GBAGS1  --Yes--  --Yes--
_ 010   2   GBAGS1 GHB.STAGED        DEL 200714 1105   GBAGS1  --Yes--  --Yes—
```

A Permit Group is a collection of MFE Permit Audit Records grouped together by UserId. The displayed record is the very last record for a unique UserId/Profile combination. Use the List function to expand the Group & List all the records. Use Display function to show full set of Token Delivery Info. Enter REPORT on command line and press enter to View/Move/Copy related Profile Report(s).

5.11.2.1. Column Heading

Ttl: Number of Profiles UserId is Permitted to Access.
UserId: Permitted UserId.
MFECat: MFE Category Profile Name.
Act: Last Action Taken - ADD, UPD, DEL.
yymmdd: Year, Month, Day of Last Action.
hhmm: Hour, Minute of Last Action.
UserId: User taking the Last Action.
Desg01: If 'Yes' Token is sent to Designate One and Not UserId.
Desg02: If 'Yes' Token is sent to Designate Two and Not UserId.

5.11.2.2. Row Commands

L List all the Update/Change Records in the Group.
D Displays the full set of UserId Delivery Information.

5.12. AdHoc TCE/MFE Journal Query

Profile Log   Permit Log   MFAudit   MFE Events   MFE Monitor

The Control Journal is a repository of ICE Managed/Controlled Events including all MFE Events. The panel shown below provides direct access to All Journal Records with options to define Data Characterization, Query/Search Range/Scope and Presentation Format.

```
◊───────── Function - Query & Display MFE Controlled Events ──────────◊
◊                ICE 16.0 MY - MFE Controlled Event Query               ◊
◊                                                                       ◊
◊  ---------------- Set the Data Characterization Profile ----------   ◊
◊                   by Category .. or by EventClass ..                  ◊
◊  --------------------- Set the Journal Query Range ---------------   ◊
◊  Begins with .. YY    MM    DD    & Ends with .. YY    MM    DD       ◊
◊  ---------------------- Check Presentation Format ----- .. NewOnly   ◊
◊    .. Active-Matrix  .. In-Summary  .. MetaDetail  .. FullDetail      ◊
◊                                                                       ◊
◊───────────────────────────────────────────────────────────────────────◊
```

Panel supports query against all Controlled Categories with or without MFE protection. When MFE Events are the target, it is best to select EventClass Characterization. If MFE events are within the scope of the query, they are preceded by MEDIT followed by /Classes Name.

5.12.1.1. ALLOW

MFE OK, token was sent and subsequently validated.

5.12.1.2. WARNS

MFE WARN was triggered; AUTHVFY WARN was specified and the edit would have otherwise been denied for either bad token, token entry timeout, or no MFEPERMT for userid/category.

5.12.1.3. DENYS

MFE failed; the dataset/file was in an AUTHVFY defined category with no WARN and the request to edit was failed for either a bad token, token entry timeout, or no MFEPERMT for userid/category.

5.12.1.4. SETUP

MFE passticket generation failed. This would indicate that the security product setup required to use the passticket generator most likely had not been done.

5.12.1.5. 3PART

Used to indicate a third party designation which would be same as ALLOW/WARNS except for 3RDPARTY MFEPERMT use.

5.12.2. EventClass Sample

```
            NSIMGBL 0618    ICE 16.0 - MY Controlled Event/Class Profiles
   0498
--------------- Control Dataset Versions - Event/Class Profiles ---------------
Cm Numb Event/Types Cm Numb Event/Types Cm Numb Event/Types Cm Numb ExcludeList
..  110 AUDIT/DTCNG ..                  ..                  ..
..  117 SAVED/CEDIT ..                  ..                  ..
..   68 AUDIT/DEDIT ..                  ..                  ..
..   25 ATMPT/AEDIT ..                  ..                  ..
..   59 MFEDT/ALLOW ..                  ..                  ..
..   12 OTHER/CEDIT ..                  ..                  ..
..   49 MFEDT/FAILS ..                  ..                  ..
..   24 MFEDT/WARNS ..                  ..                  ..
..    8 AUDIT/DTDEL ..                  ..                  ..
..    6 AUDIT/DTADD ..                  ..                  ..
..    4 SAVED/DELET ..                  ..                  ..
..    2 FIRST/DELET ..                  ..                  ..
..    2 ATMPT/AVIEW ..                  ..                  ..
..   10 SAVED/RSTOR ..                  ..                  ..
..    2 FIRST/CEDIT ..                  ..                  ..
..                  ..                  ..                  ..
..                  ..                  ..                  ..
..                  ..                  ..                  ..
```

As datasets are accessed/updated, the event and the class of event are recorded in the Control Journal along with related details - Metadata, Descriptor, Changes and/or the content of the dataset/member. The Panel reflects the classification/profiling of number of datasets specified in the prior panel. To view Datasets in a given profile, select the profile using an 'S' and press enter. In the worksheet that follows the individual Datasets Groups are shown. Using Row and Line Commands expand the groups, drill down into group detail and build/print reports.

5.12.3. Report Options

On the command line of this panel, enter command 'REPORT' and press return. This action will display a summary of all profiled events. Enter the command 'REPORT DETAIL' to display a report showing each event and detail. When you exit from a Summary or Detail Report, a standard Move/Copy Utility Panel is displayed. If the service is desired, pressing enter will transfer name of the temporary dataset to panel. Press enter to display the next panel where the desired copy dataset name is entered.

5.13. Joining an ADMIN and/or AUDIT Report Interval

Profile Log Permit Log MFAudit MFE Events MFE Monitor

5.13.1. Interval Monitor – Daily, Weekly, Monthly - Intervals

```
◊─────────── Function - MFE Monitor Intervals - TCE Admin ───────────◊
◊               ICE 16.0 MY - MFE Activity Monitor                   ◊
◊                                                                    ◊
◊   + Interval: HRS:06 MIN:49                      9                 ◊
◊     Delivery:   Ok Daily         No Weekly         Ok Monthly      ◊
◊                                                                    ◊
◊     ToEmlAdr: PRR@NEWERA.COM                                       ◊
◊                                                                    ◊
◊                      View Last Admin Report Set                    ◊
◊                                                                    ◊
◊────────────────────────────────────────────────────────────────────◊
```

This Panel serves multiple purposes. First, on entry it shows the status of MFE Interval Monitor, current execution Time and Days and below that the availability of a given interval for delivering a report.Second is to display the status of a provided email address. To do this, cursor into the address field and press enter. Once the status is shown, the target address may 'Joined'/'Leave' the selected delivery option. Entering a UserId as address will call the ESM to determine if it is known and if it has a corresponding WAEMAIL address. If address is known, it is displayed. If user is not known, condition noted.

5.13.2. View Last Report Set

Cursor under View Last Admin Report Set and press enter to show, by delivery option, the date of the last report for that delivery period. Cursor under the date & press enter to display the report. On exit from the report the system MOVE/COPY Utility will be displayed. To shift it back to its original state for the shown address, reselect or select the email address to redisplay its current delivery status by Day, Wks and/or Mth.

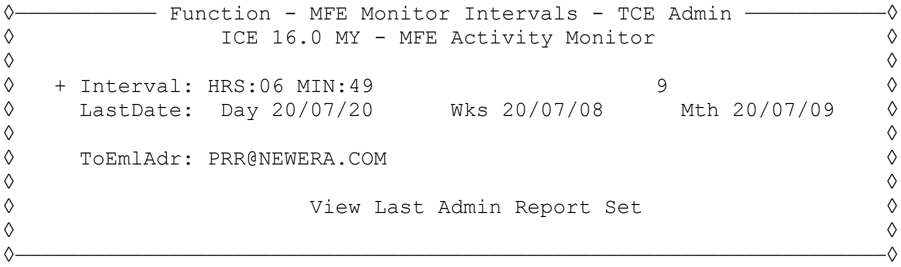
5.13.3. Interval Monitor – Daily, Weekly, Monthly – Users

Cursor under the Email Address to View the associated User's Current Delivery Schedule.

```
◊─────────── Function - MFE Monitor Intervals - TCE Admin ───────────◊
◊               ICE 16.0 MY - MFE Activity Monitor                   ◊
◊                                                                    ◊
◊   + Interval: HRS:06 MIN:49                      9                 ◊
◊     Delivery:  Stop Daily       Join Weekly       Stop Monthly     ◊
◊                                                                    ◊
◊     ToEmlAdr: PRR@NEWERA.COM                                       ◊
◊                                                                    ◊
◊                      View Last Admin Report Set                    ◊
◊                                                                    ◊
◊────────────────────────────────────────────────────────────────────◊
```

5.13.4. Interval Monitor – Daily, Weekly, Monthly – Views

Cursor under the white text “View Last Admin Report Set” and press enter to present the Date for the last Interval Report in each for Daily, Weekly and Monthly delivery. Cursor under the presented dates, if any, and press enter to display the Interval Report. Note that AUDIT and ADMIN Report Sets and Interval Delivery dates may differ.

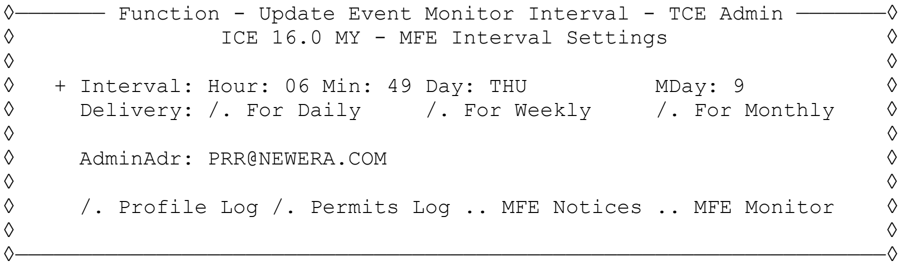


```
◊─────────── Function - MFE Monitor Intervals - TCE Admin ───────────◊
◊                ICE 16.0 MY - MFE Activity Monitor                   ◊
◊                                                                     ◊
◊   + Interval: HRS:06 MIN:49                        9                ◊
◊     LastDate:  Day 20/07/20      Wks 20/07/08      Mth 20/07/09     ◊
◊                                                                     ◊
◊     ToEmlAdr: PRR@NEWERA.COM                                        ◊
◊                                                                     ◊
◊                       View Last Admin Report Set                    ◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

5.13.1. Interval Monitor Settings

When the user is a TCE Admin or the MFEAuditor they cursor under the ‘+’ and press enter to reach the Interval Settings Panel shown next.

5.13.2. Intrerval Reporting Request and Delivery Timing.



```
◊─────── Function - Update Event Monitor Interval - TCE Admin ───────◊
◊                ICE 16.0 MY - MFE Interval Settings                  ◊
◊                                                                     ◊
◊   + Interval: Hour: 06 Min: 49 Day: THU           MDay: 9           ◊
◊     Delivery: /. For Daily     /. For Weekly      /. For Monthly    ◊
◊                                                                     ◊
◊     AdminAdr: PRR@NEWERA.COM                                        ◊
◊                                                                     ◊
◊     /. Profile Log /. Permits Log .. MFE Notices .. MFE Monitor     ◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

Here you define Interval Settings. First, the Hour(24), Day(s) -MON, TUE, WED, THU, FRI, SAT, SUN - Day(s) of Month (1-31) that define the Interval. Next, Check '/' one or more of the Delivery Options - Daily, Weekly, Monthly. On Exit(PFK3) changes, if detected, are activated. Entering a UserId as Email Address calls ESM to determine if known and has WAEMAIL. If so, Address is displayed.

5.13.2.1. Profile Log

The history of MFE Profile Adds, Deletes and Changes are recorded in the Profile Log. This report will show the specifics of Profile updates since the last report.

5.13.2.2. Permits Log

Like Profiles, changes to MFE User Permits are recorded in the Profile Log. This report will show the changes in individual Profiles since the last report.

5.13.2.3. MFE Notices

Both ADMIN & AUDIT users may be notified/alerted to MFE related Activity – Token generation/Token uses - in real time. This report lists those receiving these Emails.

5.13.2.4. MFE Monitor

Like Notices, ADMIN & AUDIT users may also be selected to receive the Interval Monitor reports defined from this panel. This report will list those recipients.

5.13.3. Interval Settings Report

To display a Worksheet that details Delivery Schedules for - DAY, WKS, MTH - and those individual Email Addresses that will receive the reports created, their Group – ADMIN, AUDIT – and Role – PRM, SEN – cursor under the '+' shown in the upper left of the panel and press enter.

```
/******************************************************************************/
/*                                                                            */
/*                 *MY/MFE - MFE Monitor - Interval Settings                  */
/*                                                                            */
/*         This Report Date:2020/07/20 - Time:08:50:21 - User:PROBI1          */
/*                                                                            */
/******************************************************************************/

 Row ------------Type,Role,Delivery------------- ------Schedule------ --Last--
 Num Class Job ----------Email Address---------- Frq hh:mm -Interval- yy/mm/dd
 --- ----- --- --------------------------------- --- ----- ---------- --------
 001 ADMIN PRM PRR@NEWERA.COM                    DAY 08:40 Daily      20/07/20
 002 ADMIN PRM PRR@NEWERA.COM                    MTH 08:40 9          20/07/09
 === ===== === ================================= === ===== ========== ========

/******************************************************************************/
/*                 RPTDSN:IFO.TEST.$TCETEMP.REPORTS($TEMPDSN)                 */
/******************************************************************************/
```

5.13.1. Interval Monitor – Daily, Weekly, Monthly – Reports

An Interval Monitor will include none or all four of the optional reports selectable from the panel. In addition, they will receive a Journaled MFE Activities and List of Recipients receiving the Interval Report Set.

```
/******************************************************************************/
/*                                                                            */
/*         *MY/MFE - Admin - Interval Monitor Report - Daily Delivery         */
/*                 TCE Prime Admin UserId Defined as - PROBI1                 */
/*               Date:2020/07/20 - Time:06:49:02 - User:PROBI1                */
/*                                                                            */
/******************************************************************************/

   <> MFE Profile Configuration - Most Recent Additions and/or Updates
      ----Group Listing--- ------Last Updated------ ---Controls--- ---Start---
      -- ---MFECategory--- Act yymmdd hhmm -UserId- Mode Fail Tokn yymmdd hhmm
      -- ----------------- --- ------ ---- -------- ---- ---- ---- ------ ----

   <> MFE Permits Configuration - Most Recent Additions and/or Updates
      -> Permitted MFE UserId:GBAGS1 EmlAddr:GHB@newera.com
      -- --Permit Category Groups-- ------Last Updated------ ----Designate----
      -- -UserId- ---MFECategory--- Act yymmdd hhmm -UserId- -Desg01- -Desg02-
      -- -------- ----------------- --- ------ ---- -------- -------- --------

   <> Journalled MFE Activities - New Events Starting 00:00 Y/M/D - 20/07/19
      -> 01 AUDIT/DTCNG 002 - Change from outside of TCE to Controlled Dsn/Mbr
      Typ TTLs mm/dd/year hh:mm:ss -Volume- -----------Dataset/File-----------
      --- ---- ---------- -------- -------- ----------------------------------

   <> MFE Activity Alerts - Current Recipients:

   <> MFE Interval Reports - Current Recipients:

   <> Recipient(s) of this Admin Report:
```

6.*MY Application Support of Permitted MFE Users

6.1. *MyWHO

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYWHO

The result is the display of the driving user's standing – General User, TCEPrime, TCEAdmin, MFEAuditor, MFEROAuditor. A sample is shown below:

```
◊─────────── You are TCEPRIME Admin & Senior MFE Auditor. ────────────◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

6.2. *MyHIS

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYHIS

The result is the display of the driving user's Journal History a sample is shown below:

```
 -NSIMCTL 0715-  ICE 16.0 - My UserId Event Group Worksheet   Row 1 to 14 of 15
                                                             ---UserId Group---
-------------------- 900 - Journal Entry Found for - PROBI1 -------------------
Row Selection: List_Journal_Entries_in_UserId_Group
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Row ---------------Related Journal Events for Target UserId---------------- >

___ ___ __ _____ _____ ________ ________ _____ _____ ________________________
S Row Ver JF Class Event -UserId- yy/mm/dd hh:mm Volume --Controlled Datasets--
_ 001 492 LS USERS ALLOW   PROBI1 20/07/25 16:53 --N/A- LGN.PWD.EVENTS
_ 002 184 MA OTHER CEACT   PROBI1 20/07/25 16:42 B2WRKD IFO.TEST.PARMLIB
_ 003 010 DE AUDIT DEDIT   PROBI1 20/07/24 14:36 C3RES1 SYS1.PARMLIB
_ 004 045 AE ATMPT PLOCK   PROBI1 20/07/24 14:35 C3RES1 SYS1.PARMLIB
```

6.3. *MyPIN

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYPIN

The result is the display of the driving user's PIN Permit Prefix Maintenance Dialog as shown below:

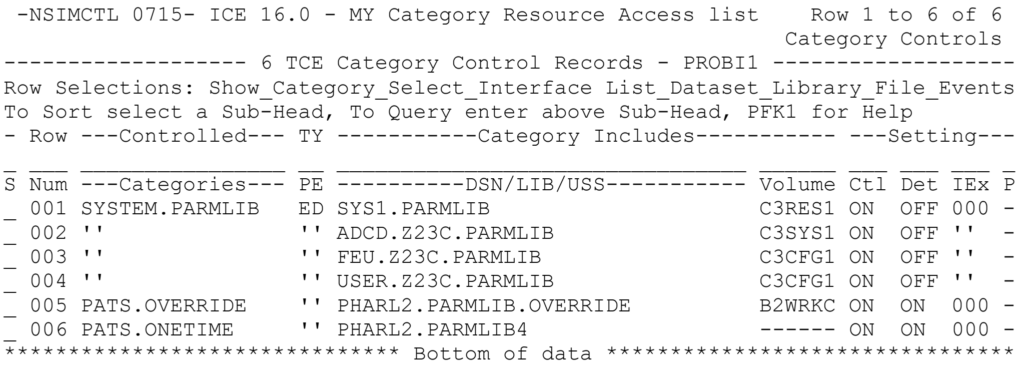
```
◊───────── Function - MFE UserId Permit Prefix Maintenance ──────────◊
◊               ICE 16.0 MY - MFE UserId Prefix Update               ◊
◊                                                                    ◊
◊  Old Prefix:          New Prefix:          Confirm New:            ◊
◊                                                                    ◊
◊          Enter 'S' .. and Press Enter to Update Prefix             ◊
◊                                                                    ◊
◊────────────────────────────────────────────────────────────────────◊
```

6.4. *MyPMT

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYPMT

The result is the display of the driving user's Permitted Profile(s) and their Protected Resources:



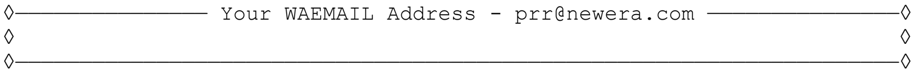
```
 -NSIMCTL 0715- ICE 16.0 - MY Category Resource Access list    Row 1 to 6 of 6
                                                             Category Controls
------------------- 6 TCE Category Control Records - PROBI1 -------------------
Row Selections: Show_Category_Select_Interface List_Dataset_Library_File_Events
To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help
- Row ---Controlled--- TY -----------Category Includes----------- ---Setting---
_ ___ _______________ __ ________________________________ ______ ___ ___ ___ _
S Num ---Categories--- PE ----------DSN/LIB/USS----------- Volume Ctl Det IEx P
_ 001 SYSTEM.PARMLIB   ED SYS1.PARMLIB                     C3RES1 ON  OFF 000 -
_ 002 ''               '' ADCD.Z23C.PARMLIB                C3SYS1 ON  OFF ''  -
_ 003 ''               '' FEU.Z23C.PARMLIB                 C3CFG1 ON  OFF ''  -
_ 004 ''               '' USER.Z23C.PARMLIB                C3CFG1 ON  OFF ''  -
_ 005 PATS.OVERRIDE    '' PHARL2.PARMLIB.OVERRIDE          B2WRKC ON  ON  000 -
_ 006 PATS.ONETIME     '' PHARL2.PARMLIB4                  ------ ON  ON  000 -
******************************* Bottom of data ********************************
```

6.5. *MyEML

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYEML

The result is the display of the driving user's WAEMAIL Status in a panel as shown below:



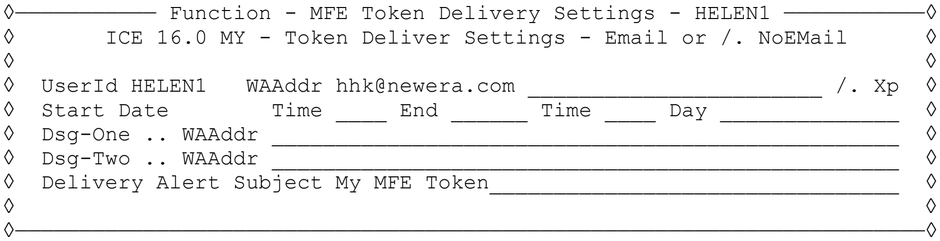
```
◊─────────────── Your WAEMAIL Address - prr@newera.com ───────────────◊
◊                                                                      ◊
◊──────────────────────────────────────────────────────────────────────◊
```

6.6. *MyDEL

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYDEL

The result is the display of the driving user's MFE Delivery Settings in a panel as shown below:



```
◊─────────── Function - MFE Token Delivery Settings - HELEN1 ───────────◊
◊       ICE 16.0 MY - Token Deliver Settings - Email or /. NoEMail      ◊
◊                                                                        ◊
◊  UserId HELEN1    WAAddr hhk@newera.com _______________________ /. Xp  ◊
◊  Start Date          Time ____ End ______ Time ____ Day ______________ ◊
◊  Dsg-One .. WAAddr ________________________________________________    ◊
◊  Dsg-Two .. WAAddr ________________________________________________    ◊
◊  Delivery Alert Subject My MFE Token_________________________________  ◊
◊                                                                        ◊
◊────────────────────────────────────────────────────────────────────────◊
```

6.7. *MyQRY

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYQRY

The result is the display of the TCE AdHoc Query panel as shown below:

```
◊─────────────── Function - TCE ADHOC Query & Display ────────────────◊
◊                ICE 16.0 MY - TCE Journalled Events                  ◊
◊                                                                     ◊
◊  ---------------- Set the Data Characterization Profile ----------  ◊
◊                    by Category .. or by EventClass ..               ◊
◊  --------------------- Set the Journal Query Range ---------------  ◊
◊  Begins with .. YY     MM     DD     & Ends with .. YY     MM     DD     ◊
◊  ---------------------- Check Presentation Format ----- .. NewOnly  ◊
◊    .. Active-Matrix  .. In-Summary  .. MetaDetail  .. FullDetail    ◊
◊                                                                     ◊
◊─────────────────────────────────────────────────────────────────────◊
```

6.8. *MyISO

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

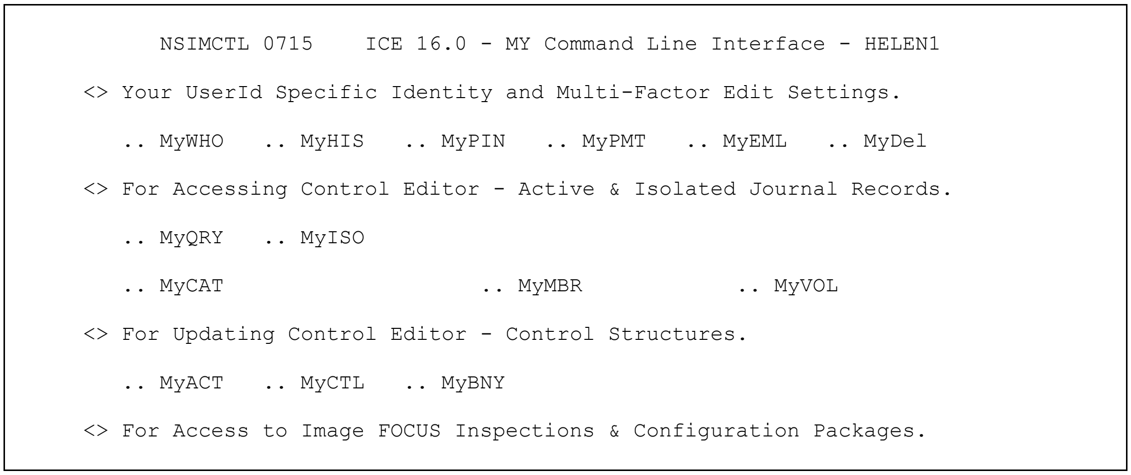
TSO $CLI,*MYISO

The result is the display of the Resources that were detected as non-conforming and therefore recorded in the Control Journal as Isolated. Such Isolated Resource Entries are not available of Restore operation and remain Isolated until they are Re-certified as Trusted:

6.9. *MyCLI

Enter the following Common String on the ICE/ISPF or TSO/ISPF Command Line and press enter:

TSO $CLI,*MYCLI



```
       NSIMCTL 0715    ICE 16.0 - MY Command Line Interface - HELEN1

 <> Your UserId Specific Identity and Multi-Factor Edit Settings.

    .. MyWHO   .. MyHIS   .. MyPIN   .. MyPMT   .. MyEML   .. MyDel

 <> For Accessing Control Editor - Active & Isolated Journal Records.

    .. MyQRY   .. MyISO

    .. MyCAT                     .. MyMBR            .. MyVOL

 <> For Updating Control Editor - Control Structures.

    .. MyACT   .. MyCTL   .. MyBNY

 <> For Access to Image FOCUS Inspections & Configuration Packages.
```

7. Technical Support Contact Information

NewEra Software, Inc.

Mailing Address:

18625 Sutter Boulevard, Suite 950
Morgan Hill, CA 95037

Phone:

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

FAX:

(888) 939-7099

Email Address:

support@newera.com

Web Site:

https://www.newera.com

Technical Support:

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