TECH TALKS

With Frontier Customer Support

Your Topics For Your Success

Today's Topic: Frontier Security

DEHN LODER | FRIEDMAN CORPORATION

The Details

- All participants are muted.
- Please post your questions in Chat or use the Q&A tab. We will answer them at the end of the presentation.
- This session is being recorded. The replay link will be sent to all registered customers.
- Presenter: Dehn Loder, Vice President of PowerPoint at Friedman Corp.

Agenda

- User Provisioning
  - Creating new IBM i user profiles for use with Frontier
  - Authorizing profiles to environments
- User Termination
  - Deactivating user profiles
- Creating New Frontier Security Groups in the UI
  - Try this one trick
- Can Frontier Security be Environment-Specific?
  - Considerations and recommendations

This Talk discusses topics which aren't entirely clear in the standard Security documentation.

We get a lot of questions about these topics.

User Provisioning (UP)

CREATING NEW USER PROFILES FOR USE WITH FRONTIER

UP: Before You Begin

- You need to have a user profile with *SECADM privileges
  - Avoid using QSECOFR
- The following procedure is for **day-to-day business** users
  - Programmers need some special authorities
- For **day-to-day business** Frontier users, know the following ahead of time
  - User profile name: 10 characters, alphanumeric
    - Check for duplicates first
  - Description: 50 characters
  - What Frontier environments will the user access?
    - DTA, PCM, TST, …?
  - Frontier group membership
    - Frontier application group(s), not IBM i group profile
  - Will the user need green-screen access?
    - What environment do they access via GS?
    - Affects choice of job description

UP: Create IBM i user profile: CRTUSRPRF (1/3)

CL command:

```
crtusrprf loder
```

F4=Prompt

```
                        Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . > LODER          Name
User password . . . . . A9E195U03V      Character value, *USRPRF...
Set password to expired . . . . *yes    *NO, *YES
Status . . . . . *ENABLED       *ENABLED, *DISABLED
User class . . . . . *USER      *USER, *SYSOPR, *PGMR...
Assistance level . . . . . *SYSVAL      *SYSVAL, *BASIC, *INTERMED...
Current library . . . . . *CRTDFT       Name, *CRTDFT
Initial program to call . . . . *NONE   Name, *NONE
  Library . . . . . _____       Name, *LIBL, *CURLIB
Initial menu . . . . . *SIGNOFF         Name, *SIGNOFF
  Library . . . . . _____       Name, *LIBL, *CURLIB
Limit capabilities . . . . . *YES       *NO, *PARTIAL, *YES
Text 'description' . . . . . 'Dehn Loder sample profile'
_____

                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

UP: Create IBM i user profile: CRTUSRPRF (1/3)

- User password (PASSWORD): pick a reasonably strong password
- Set password to expired (PWDEXP): ***YES**
  - Will force the user to choose a new password at next sign-on
- Initial program to call (INLPGM)
  - If no green-screen access required: ***NONE** (this is the default)
  - If green-screen access required: **FRNINTLPGM** in ***LIBL**
- Initial menu (INLMNU): ***SIGNOFF**
  - Prevents display of "system" menus after initial program runs
- Limit capabilities (LMTCPB): ***YES**
  - Prevents the direct entry of most CL commands by this user
- Text 'description' (TEXT): *please use this*

Password complexity rules governed by IBM I system values:

QPWDLMTAJC Limit adjacent digits in password
QPWDLMTCHR Limit characters in password
QPWDLMTREP Limit repeating characters in password
QPWDMAXLEN Maximum password length
QPWDMINLEN Minimum password length
QPWDPOSDIF Limit password character positions
QPWDRQDDGT Require digit in password
QPWDRQDDIF Duplicate password control
QPWDRULES Password rules

UP: Create IBM i user profile: CRTUSRPRF (2/3)

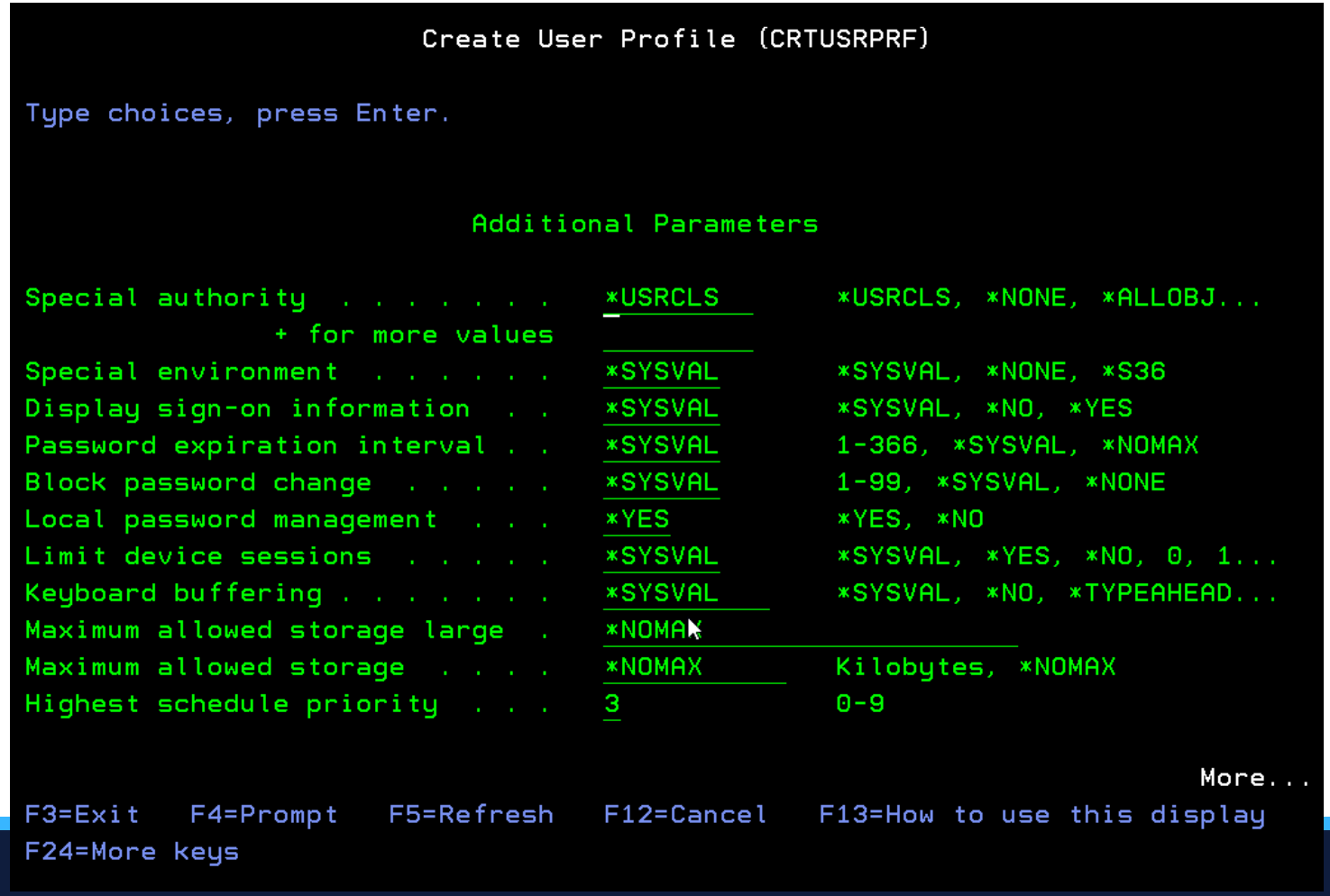
F10=Additional parameters

PageDown

For normal day-to-day users, **leave all parameters on this page at their default values.** Don't press ENTER yet!

There is another page, so

PageDown



UP: Create IBM i user profile: CRTUSRPRF (3/3)

```
                        Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Job description  . . . . . .   QDFTJOBD      Name
  Library  . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB
Group profile  . . . . . . . .   *NONE        Name, *NONE
Owner  . . . . . . . . . . . .   *USRPRF       *USRPRF, *GRPPRF
Group authority  . . . . . . .   *NONE        *NONE, *ALL, *CHANGE, *USE...
Group authority type . . . . .   *PRIVATE     *PRIVATE, *PGP
Supplemental groups  . . . . .   *NONE        Name, *NONE
              + for more values
Accounting code  . . . . . . .   *BLANK
Document password  . . . . . .   *NONE        Name, *NONE
Message queue  . . . . . . . .   *USRPRF      Name, *USRPRF
  Library  . . . . . . . . . .               Name, *LIBL, *CURLIB
Delivery . . . . . . . . . . .   *NOTIFY      *NOTIFY, *BREAK, *HOLD, *DFT
Severity code filter . . . . .   0            0-99
Print device . . . . . . . . .   *WRKSTN      Name, *WRKSTN, *SYSVAL

                                                                    More...
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

UP: Create IBM i user profile: CRTUSRPRF (3/3)

- Job description (JOBD)
  - If no green-screen access required *and using SSO*:
    QDFTJOBD in ***LIBL**
    - This is the default
    - The user will get almost nothing if logging in outside of the UI
  - If green-screen access required *or NOT using SSO*
    - Choose the **FRNBATCH** job description in the data library of the environment this use should be in after in green-screen sign on.
    - Typical examples:
      - Production environment — **FRNBATCH** in **FRNDTA040** (or FRNSYS040)
      - Test environment — **FRNBATCH** in **FRNTST040**

UP: Create IBM i user profile: CRTUSRPRF (3/3)

- Group profile (GRPPRF): ***NONE** (default)
  - For programmers that will compile RPGLE using CRTOBJ: **QPGMR**
- Owner (OWNER): ***USRPRF** (default)
  - For programmers that will compile RPGLE using CRTOBJ: ***GRPPRF**

ENTER

```
Object LODER type *MSGQ created in library QUSRSYS.
Special authorities granted *NONE.
Password longer than 8 characters.
Password does not meet all password rules.
User profile LODER created.
```

UP: Create IBM i user profile: CRTUSRPRF

- The CL command to provision a basic day-to-day Frontier user not requiring green-screen access:

```
CRTUSRPRF USRPRF(LODER)
          PASSWORD(X0O4NDOZYR)
          PWDEXP(*YES)
          INLMNU(*SIGNOFF)
          LMTCPB(*YES)
          TEXT('Dehn Loder (test profile)')
```

- Note: this won't get them into any Frontier environments. You need to edit the Frontier authority to the environment.
  - We'll talk about that

UP: Enable password change support for UI

- To enable the user password to be changed within the UI, **you must allow the FCADMINxxx profile to be able to modify the user profile**
  - The FCADMINxxx profile is the one that does password checking when the user logs on
  - FCADMIN profile named in an iProduct property
  - Forgetting this step means the user won't be able change their (expired) password in the UI!
- Use the following two Grant Object Authority commands:

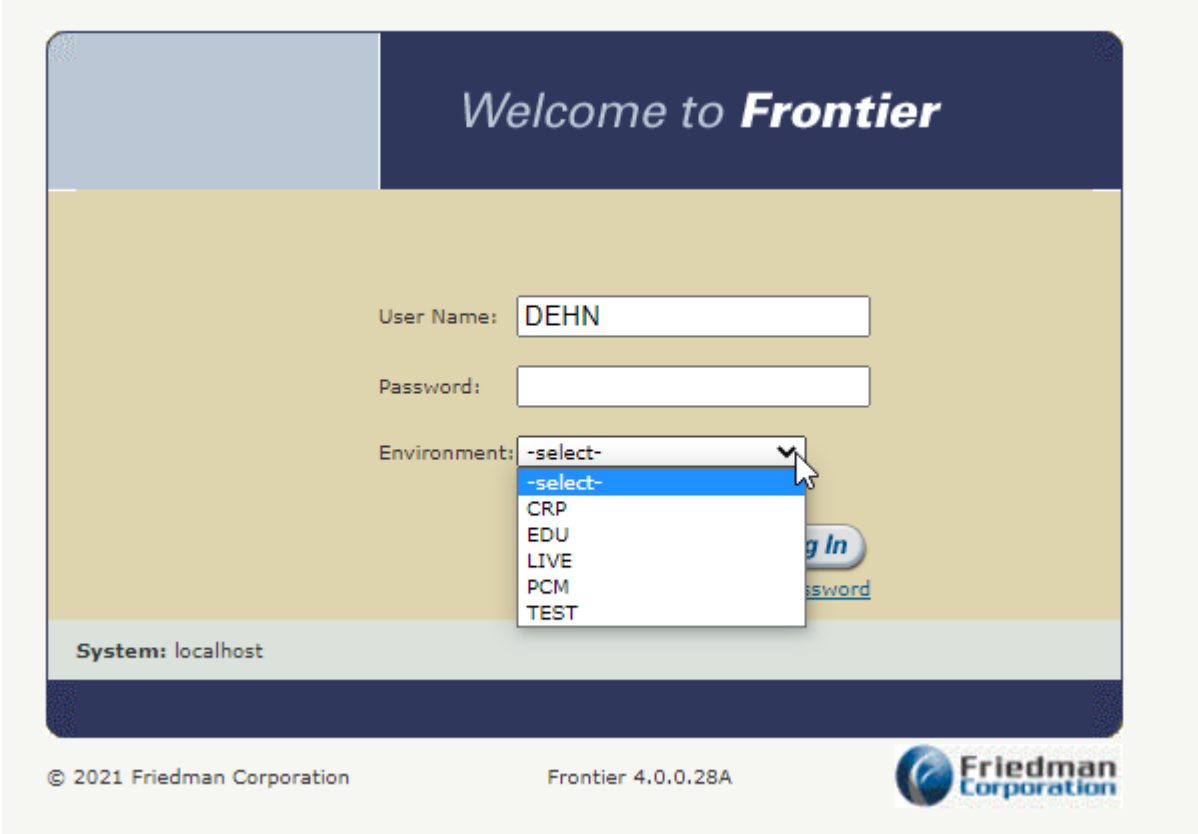
```
GRTOBJAUT OBJ(LODER) OBJTYPE(*USRPRF) USER(FCADMIN040) AUT(*OBJMGT)
```

and

```
GRTOBJAUT OBJ(LODER) OBJTYPE(*USRPRF) USER(FCADMIN040) AUT(*USE)
```

UP: Granting access to Frontier environment(s)

- SSO = “Single sign on”
  - Allows one user profile to be used across different environments **in the UI**



UP: Granting access to Frontier environment(s)

- Frontier environments are “named” in the **environments.xml** configuration file in WebSphere:

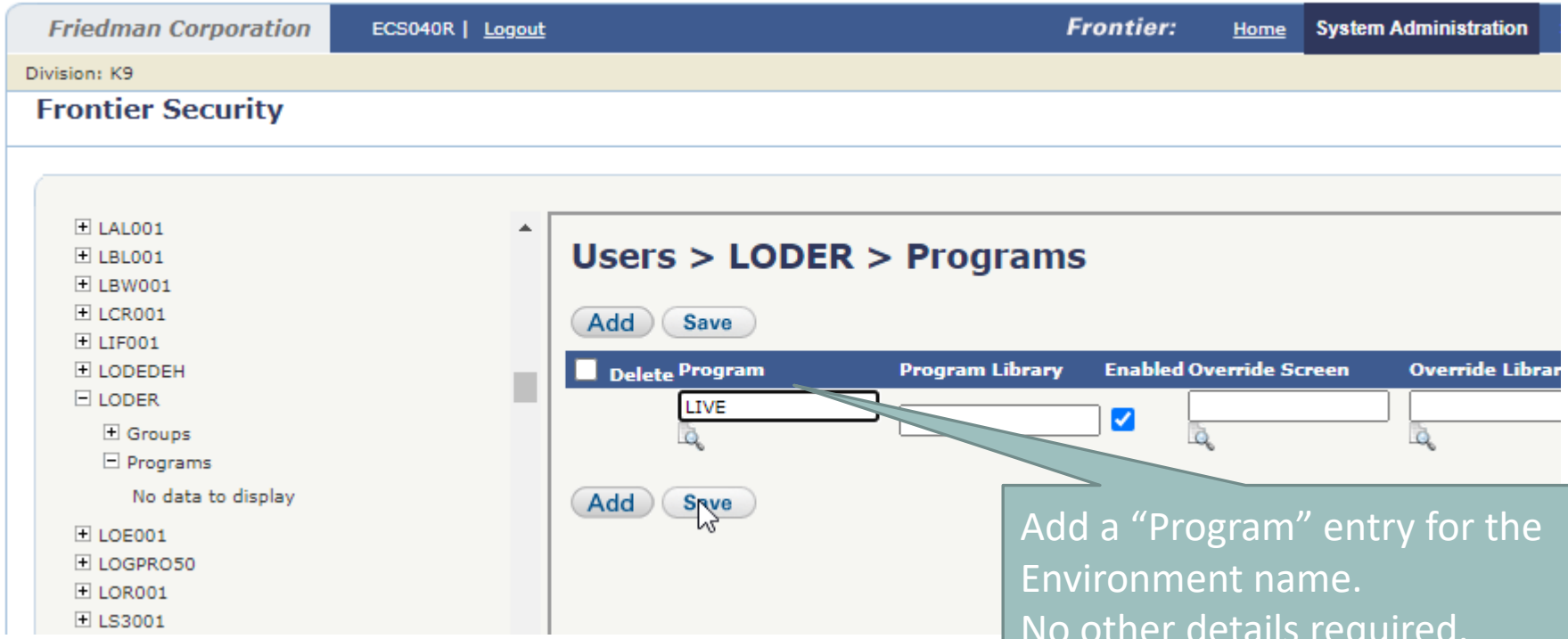
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<environments>
    <env name="LIVE"  user="FRN040"   pw="PRESENTING" />
    <env name="CRP"   user="CRP040"   pw="ISALOT" />
    <env name="EDU"   user="EDU040"   pw="OFFUN" />
    <env name="PCM"   user="PCM040"   pw="WOOTWOOT" />
</environments>
```

  - The environment definitions are created during installation, and normally maintained by the ad ministrator.

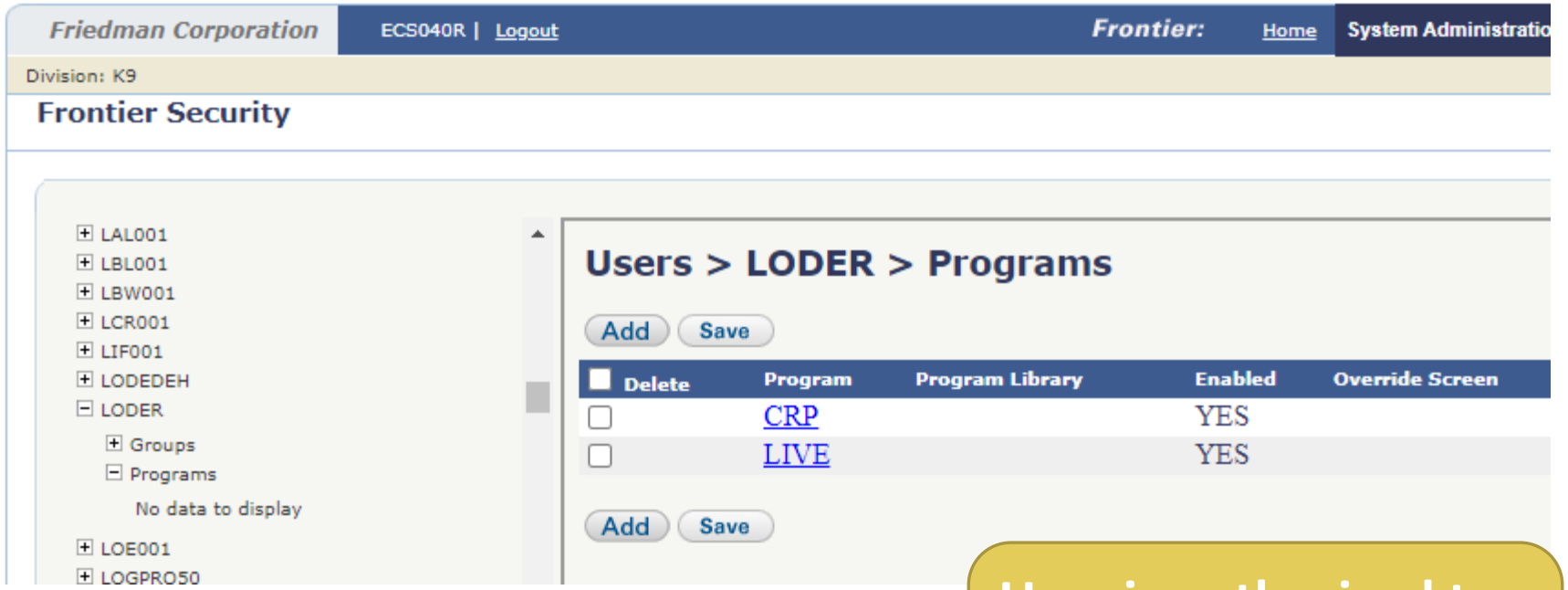
- A user profile (e.g. LODER) has to be granted access to one or more Frontier environments

UP: Granting access to Frontier environment(s)

UI:
System Administration > Security Administration
Users > *user* > Programs



UP: Granting access to Frontier environment(s)



User is authorized to environment names CRP and LIVE

UP: Detailed Frontier application access

- Once the IBM i profile has been created, Frontier security can reference the profile
- Likely, the user will be added to one or more **groups** in Frontier
- Do not confuse Frontier **groups** with IBM i **group profiles**

User Termination (UT)

WHAT TO DO WHEN EMPLOYEES LEAVE

User termination (UT)

- “Termination” = any reason to stop access to IBM i & Frontier
  - Won the lottery, perhaps?
- I recommend **disabling** user profiles (not deleting)
  - User profile names persist in database as matter of record
  - Prevents ambiguity later on
  - We’ll discuss this approach here
- **Delete** user profiles only when a profile was set up in error and never used for work in Frontier
  - DLTUSRPRF LODER

UT: Disabling IBM i user profiles: CHGUSRPRF

CL command:

```
chgusrprf loder
```

F4=Prompt

```
                        Change User Profile (CHGUSRPRF)

Type choices, press Enter.

User profile . . . . . > LODER          Name
User password . . . . . *none           Character value, *SAME, *NONE
Set password to expired . . . . *NO     *SAME, *NO, *YES
Status . . . . . *disabled      *SAME, *ENABLED, *DISABLED
User class . . . . . *USER      *SAME, *USER, *SYSOPR...
Assistance level . . . . . *SYSVAL      *SAME, *SYSVAL, *BASIC...
Current library . . . . . *CRTDFT       Name, *SAME, *CRTDFT
Initial program to call . . . . *NONE   Name, *SAME, *NONE
  Library . . . . . _____       Name, *LIBL, *CURLIB
Initial menu . . . . . *SIGNOFF         Name, *SAME, *SIGNOFF
  Library . . . . . _____       Name, *LIBL, *CURLIB
Limit capabilities . . . . . *YES       *SAME, *NO, *PARTIAL, *YES
Text 'description' . . . . . 'Dehn Loder (test profile) TERM 2020-07-13'

                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

UT: Disabling IBM i user profiles" CHGUSRPRF

- User password: ***NONE**
  - User can not sign on to a system where password is *NONE
- Status: ***DISABLED**
  - Not valid for sign on until an authorized user changes status to *ENABLED
- Text 'description'
  - Not required, but I'd recommend some sort of "terminated" note here.
  - Watch out for closing single quote

Enter

- Once processed, this user profile will be unable to start a new session until an authorized user changes the profile back.

UT: Disabling IBM i user profiles

- The basic CL command for disabling a user profile:

```
CHGUSRPRF USRPRF(LODER)
          PWD(*NONE)
          STATUS(*DISABLED)
          TEXT('Dehn Loder (test profile) TERM 2020-07-13')
```

UT: Re-enabling IBM i user profiles

- Re-enable a profile in the event of an error
  - Or perhaps this was a leave-of-absence?
- Change user profile (CHGUSRPRF)
  - Password — some new value
  - Set password to expired — *YES
  - Status — *ENABLED
  - Text ‘description’ — Back to user name only

```
CHGUSRPRF USRPRF(LODER)
          PASSWORD(P3WN44QPET)
          PWDEXP(*YES)
          STATUS(*ENABLED)
          TEXT('Dehn Loder (test profile)')
```

UT: Frontier application security clean-up

- There will still be records in Frontier application security for the disabled user profile. They won't do any harm – the profile can't sign on
- If desired, you can choose to either DELETE or OUT-DATE security records:

UT: Frontier application security clean-up

- System Administration > Security Administration
  - Users > *user* > Groups
    - Delete (or out-date) all records; removes user from all groups
  - Users > *user* > Programs
    - Delete (or out-date) all records; removes program/role authorities for user

- There is a way to do automated cleanup
  - Scary SQL to delete all security records where user profile is *DISABLED
  - Would need to be run on a recurring basis, perhaps nightly

Creating New Frontier Security Groups in the UI

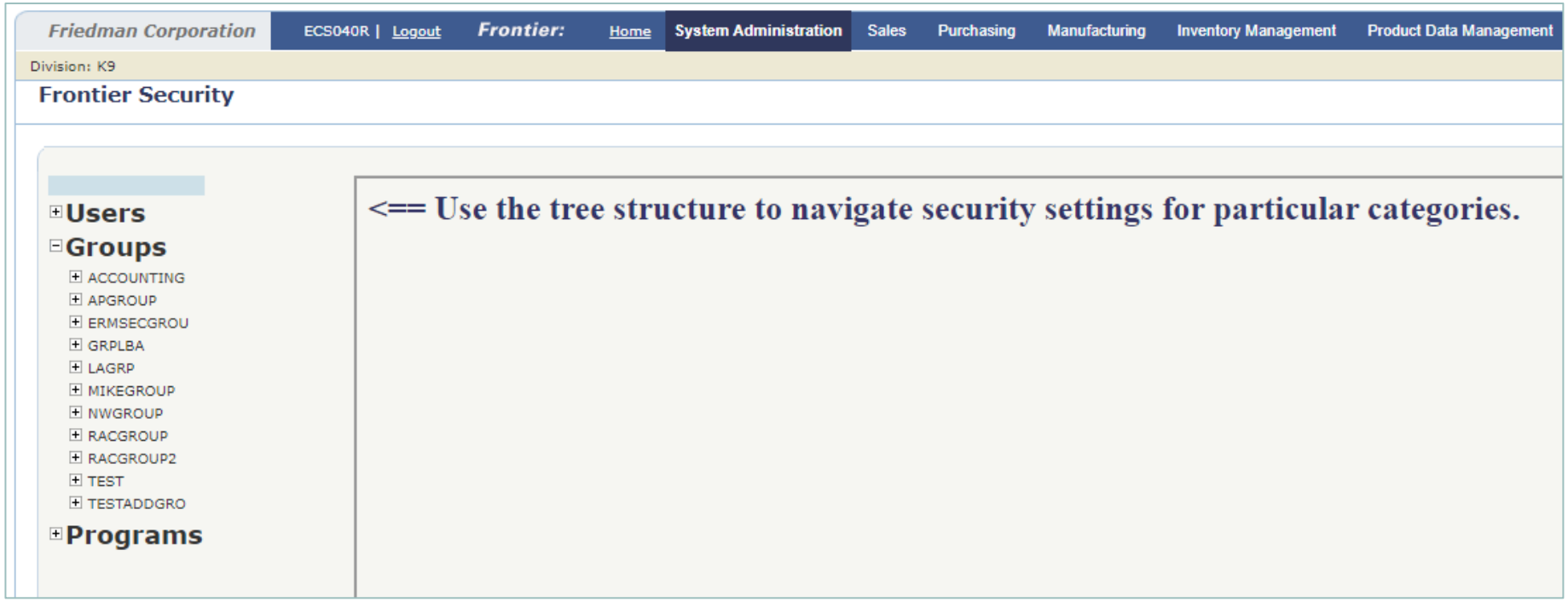
A BIT OF A WORKAROUND

Reminder

- Frontier **groups** are not the same as IBM i **group profiles**
  - Frontier groups are used solely to check application-level authorities
  - IBM i group profiles affect system-level object authorities

Creating a group in the UI

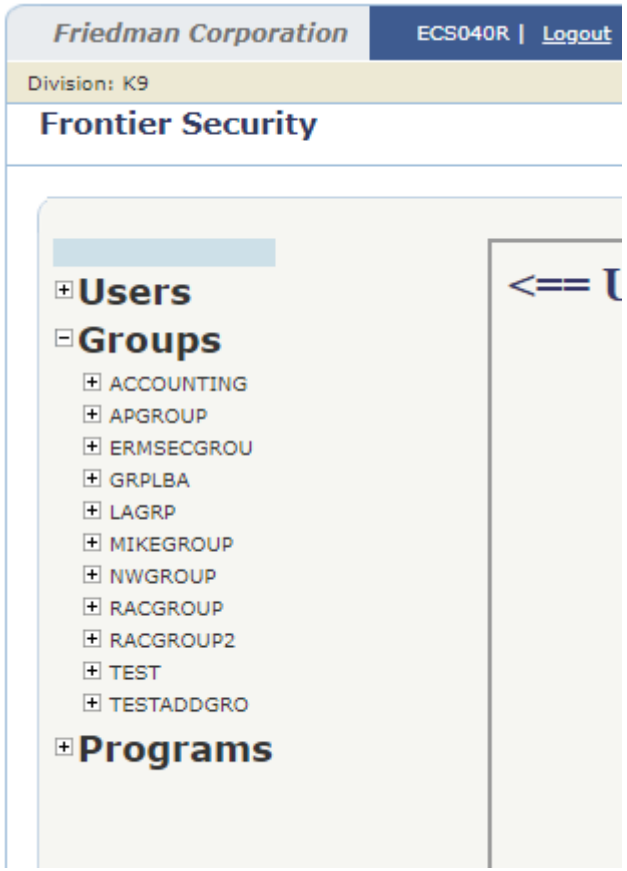
- QUESTION: How do I create a **group** in UI Security Maintenance?
  - There is no “add group” button?



Creating a group in the UI

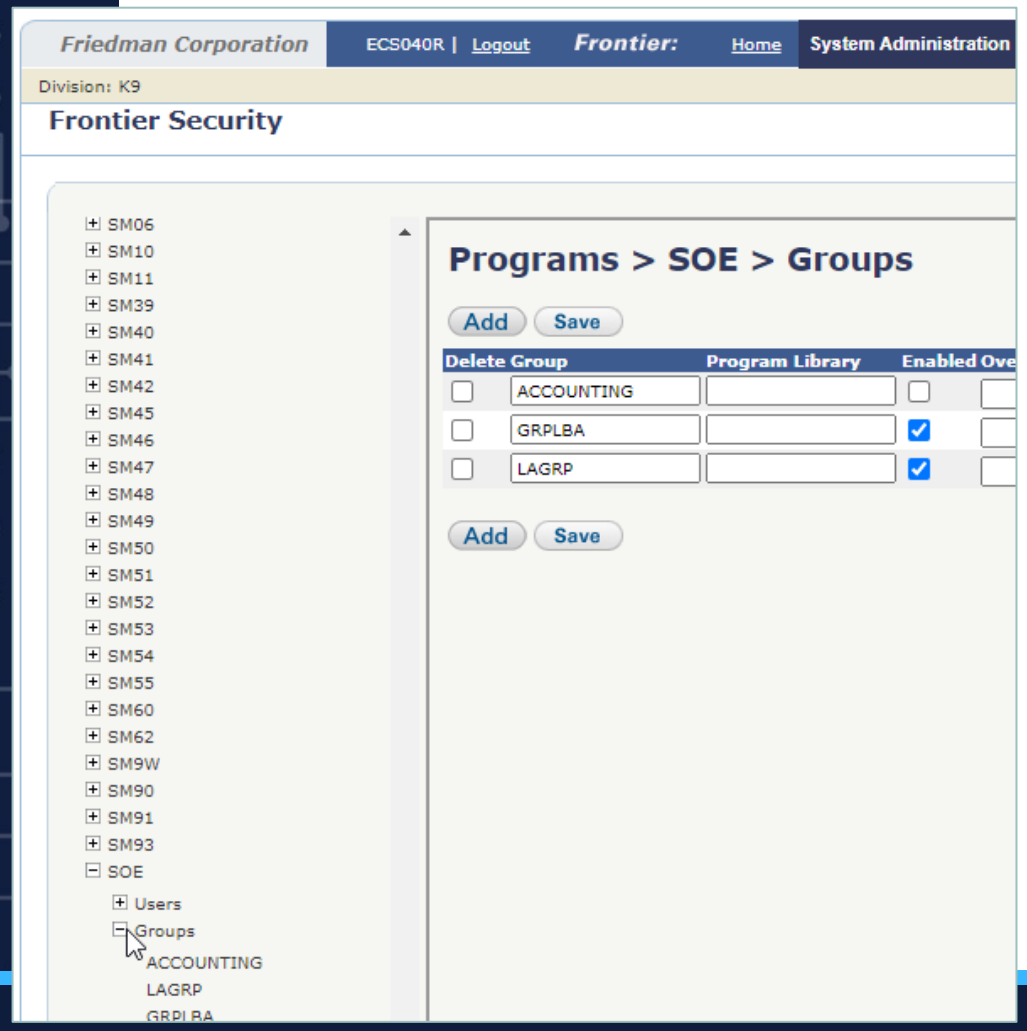
- ANSWER: Put at least one program into the new group to “create” the group
  - A group is defined by the programs listed in the group
  - If there are no programs in the group, it doesn’t exist
- You can pick any program or UI role you like
  - Consider using one that should be in the group anyway!
- For example, we want to create group **FOO_GROUP**
  - It should include UI role **SOE**, and maybe others

Creating a Group: Example procedure (1/4)



FOO_GROUP is not listed.
We want to create it.
We know we want UI role **SOE** in it.

Creating a Group: Example procedure (2/4)

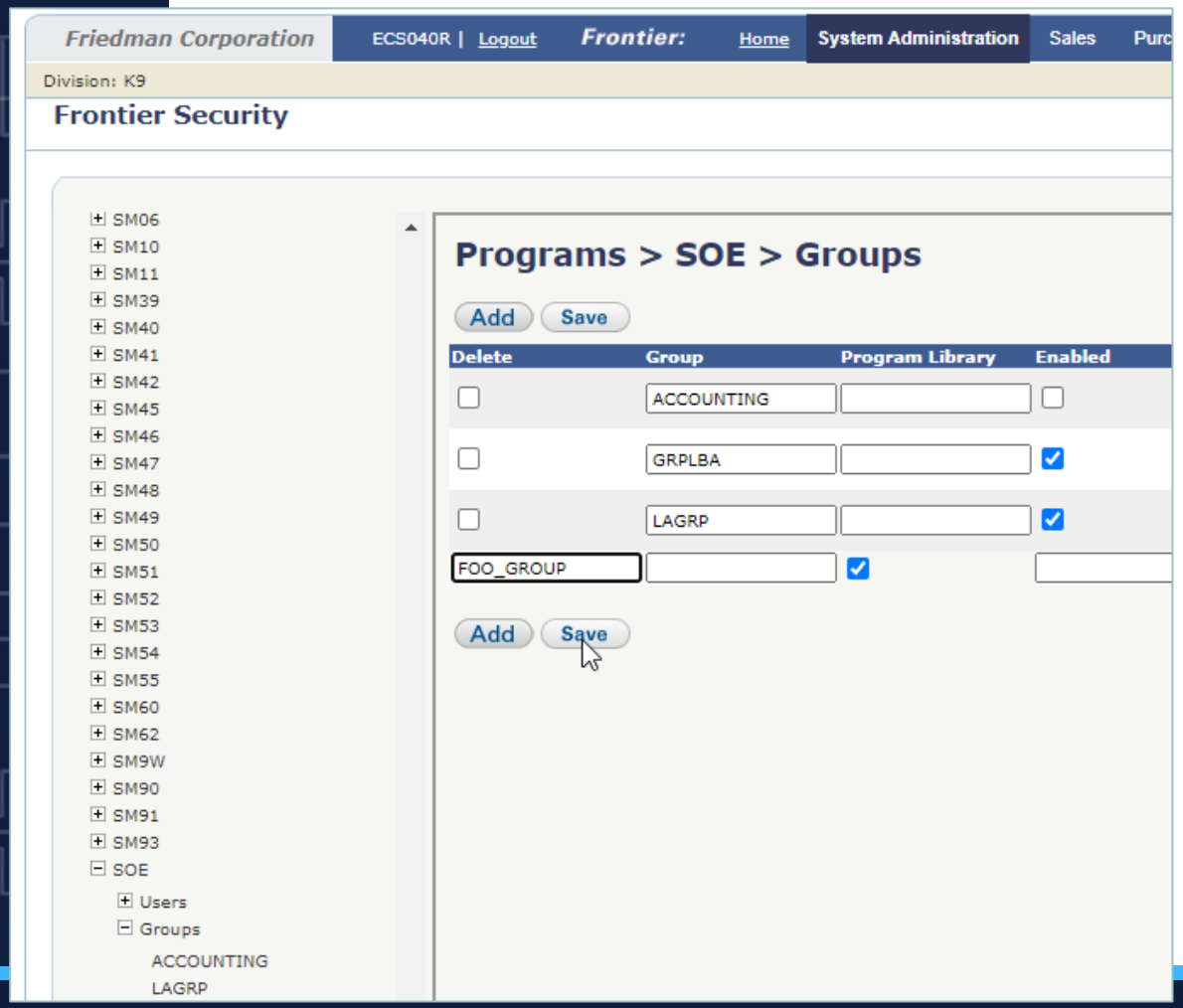


Navigate the tree to
Programs > **SOE** > Groups

Click [Add]:

we want to make UI role SOE
a member of FOO_GROUP

Creating a Group: Example procedure (3/4)



Type name of new group (**FOO_GROUP** in our example)

Click [Save]; list will update:

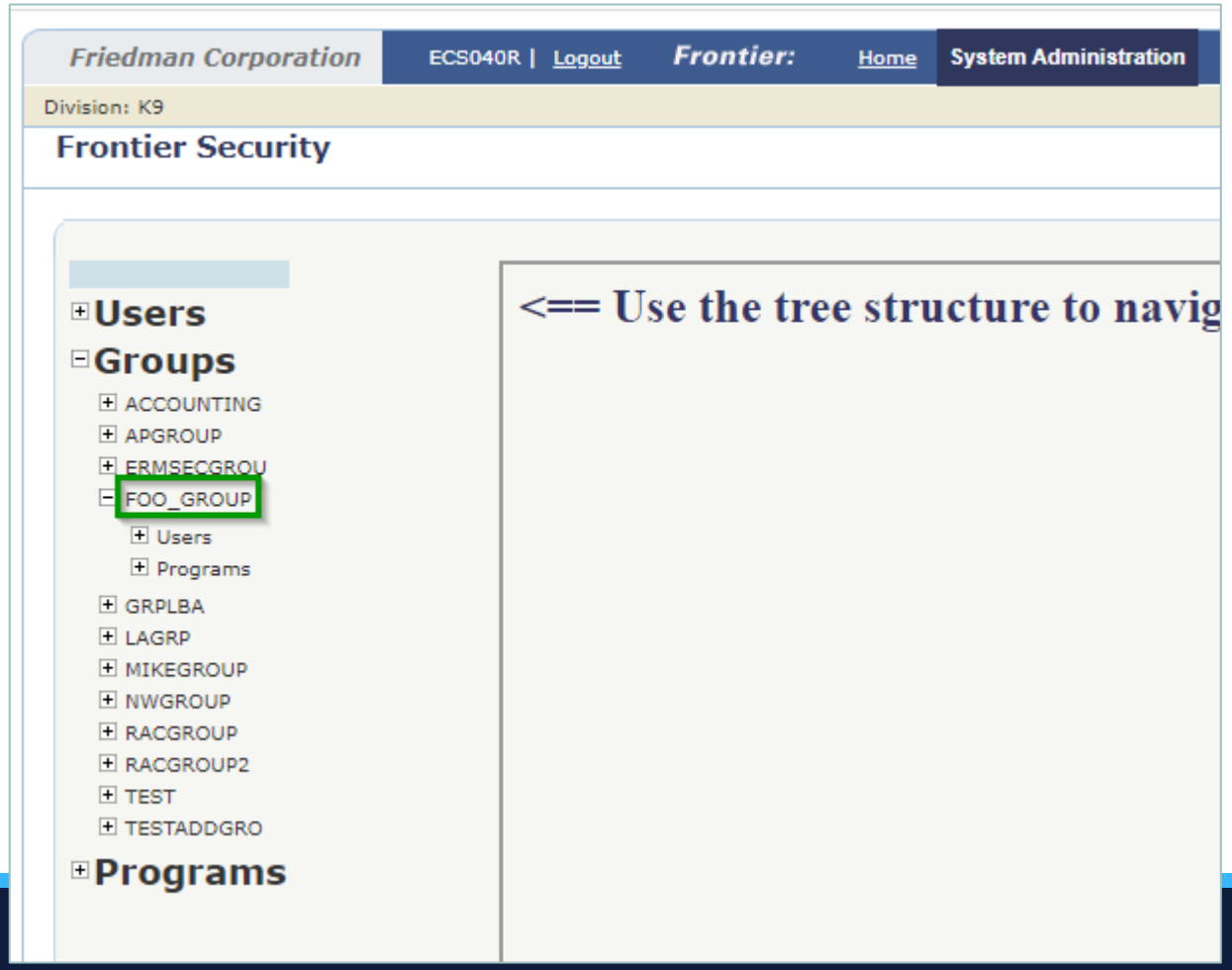
Creating a Group: Example procedure (4/4)

Click Refresh  on browser toolbar (or press F5).

Navigate to **Groups.**

Your new group will be shown;

You can now manipulate Users and Programs for that group



Can Security be Environment-Specific?

THE MECHANICS OF APPLICATION SECURITY AND SSO

Application Security: The Frontier Security Library

- **FRNnnnSEC** (nnn = release) e.g. FRN040SEC
- Used to perform application-level security checks
- Both code and data
  - Application calls programs in this library
- **Security data** in tables
  - TSYEP – Group exclusion
    - Defines “mutually exclusive” group memberships, for SOD compliance
  - TSYGP – Groups
    - User membership in group(s)
  - TSYP – Security master
    - User and/or group authorization to programs/UI roles

Intended to be a Shared Resource Across Environments

Friedman Corporation

- Original design point was to include the FRNnnnSEC library in any environment where security was desired
  - Implies exactly the same security setup for all environments
- Not a problem when everyone had 1 user profile per environment!
  - LODER → Production environment (DTA)m LODERTST → Test environment (TST), LODEREDU → Education environment etc
  - All of the above profiles would have different security records
- What happens with SSO?
  - LODER → Whatever environments are authorized
  - Implies exactly the same application security in *every* environment

How the UI Finds Security Data

- The UI does all kinds of queries against the TSY security tables to see if a user is valid for a role
  - UI Security maintenance also updates these tables
- **Where does it find these tables?**
- SPMENU 14,
  "Application System Info"
  - "iSecurity library"
  - **This is data area ISECLIB**

```
FRN040C              APPLICATION SYSTEM INFORMATION              7/14/20
                                                                 14:49:59

Asynchronous subsystem . . . . . ZASYNC
Batch job description  . . . . . FRNBATCH
  library  . . . . . . . . . . .   *LIBL
Batch output queue . . . . . . . FRNPRT
  library  . . . . . . . . . . .   *LIBL
Data object library  . . . . . . FRNCNS040



Frontier version . . . . . 040  Compatible with IBM OS V7R3M0
Cumulative upgrade level . . . . xxxxx

Number of decimal positions  . . . 3
Type of currency . . . . . S    (M = Multicurrency)
                                (S = Single Currency)

Stored procedures library  . . . . FRNPGM040C
iSecurity library  . . . . . . . . FRN040SEC


F3=Exit
```

How the UI Finds Security Data Finding ISECLIB

- Find the DATALIB data area in the current library list
  `*LIBL/DATALIB → 'FRNDTA040'`
- Use the DATALIB value to find the ISECLIB data area value
  `FRNDTA040/ISECLIB = 'FRN040SEC'`
- Use the ISECLIB data area value when querying or manipulating the security data tables:
  SQL> `select … from FRN040SEC.TSYP where..`

ISECLIB Data Area is by Environment

- The name of the security library is in data area ISECLIB,
  - which is in the library named by the DATALIB data area,
  - which is different for each environment.

- **SO, we could have a different security library for *each* Frontier environment if desired**
  - Duplicate the FRN040SEC library to as many distinct copies as you need
    - One per environment
  - In each environment, adjust SPMENU 14 “iSecurity library” to point to the distinct copy for that environment
    - Don’t forget to change the corresponding job description!
- But watch out when using SSO…

What About SSO?

- When using SSO, **we don't know the environment!**
  - We have to build a list of environments the user is authorized-to
  - User will then choose one
- Q: **What security library will we use?**
- A: **Whatever environment the FCADMINxxx profile defaults to!**
  - It is FCADMINxxx that queries the security database for each listed environment
  - We will look for DATALIB in FCADMINs library list
    - As set by FCADMIN's job description
  - From there, get ISECLIB data area, and query those tables

What About SSO?
Could be 2 Security Libraries Used

- With SSO, two different security libraries could be in play
  - One used by FCADMIN to check which environments are authorized
  - A different one once an environment has been chosen.

Recommendation

- **Use your PRODUCTION security library for environment authorization**
  - Production data library: FRNDTA040
  - SPMENU 14 iSecurity library: FRN040SEC
  - The FCADMINxxx profile should have FRNDTA040 in the library list
    - Will force system to find FRN040SEC
  - When provisioning new users, sign on to production (DTA environment) and add all environment names they are authorized to (DTA and otherwise)
    - And also detailed application authorities
- **Use cloned/duplicate security libraries for other environments**
  - Test data library: FRNTST040
  - SPMENU 14 iSecurity library FRN040SEC**T** (or whatever naming you prefer)
  - Must sign on to specific environment to grant detailed authorities for that environment

Recommendation (continued)

- You may still want to share security between some environments!
  - For example, CRP and DTA might share security
    - CRP needs to test security
    - CRP environment would use FRN040SEC library, same as DTA

- Want to clone FRN040SEC?
  - SAVLIB & RSTLIB works
  - Can also use CRTLIB, CRTDUPOBJ OBJTYPE(*ALL)

TECH TALKS

With Frontier Customer Support

Your Topics For Your Success

Security Topics
September, 2020

DEHN LODER| FRIEDMAN CORPORATION


Q&A