PennGroups countdown two step enrollment

Notes

This is our current "required to opt in" group: https://grouper.apps.upenn.edu/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.viewGroup&groupId=71626933689b4262b35a6a376991be3f

```
penn:isc:ait:apps:twoFactor:groups:requiredUsersStaff:twoFactorStaff
```

The job to populate the group currently runs hourly, and you will have to wait another hour for data to propagate to shib idp

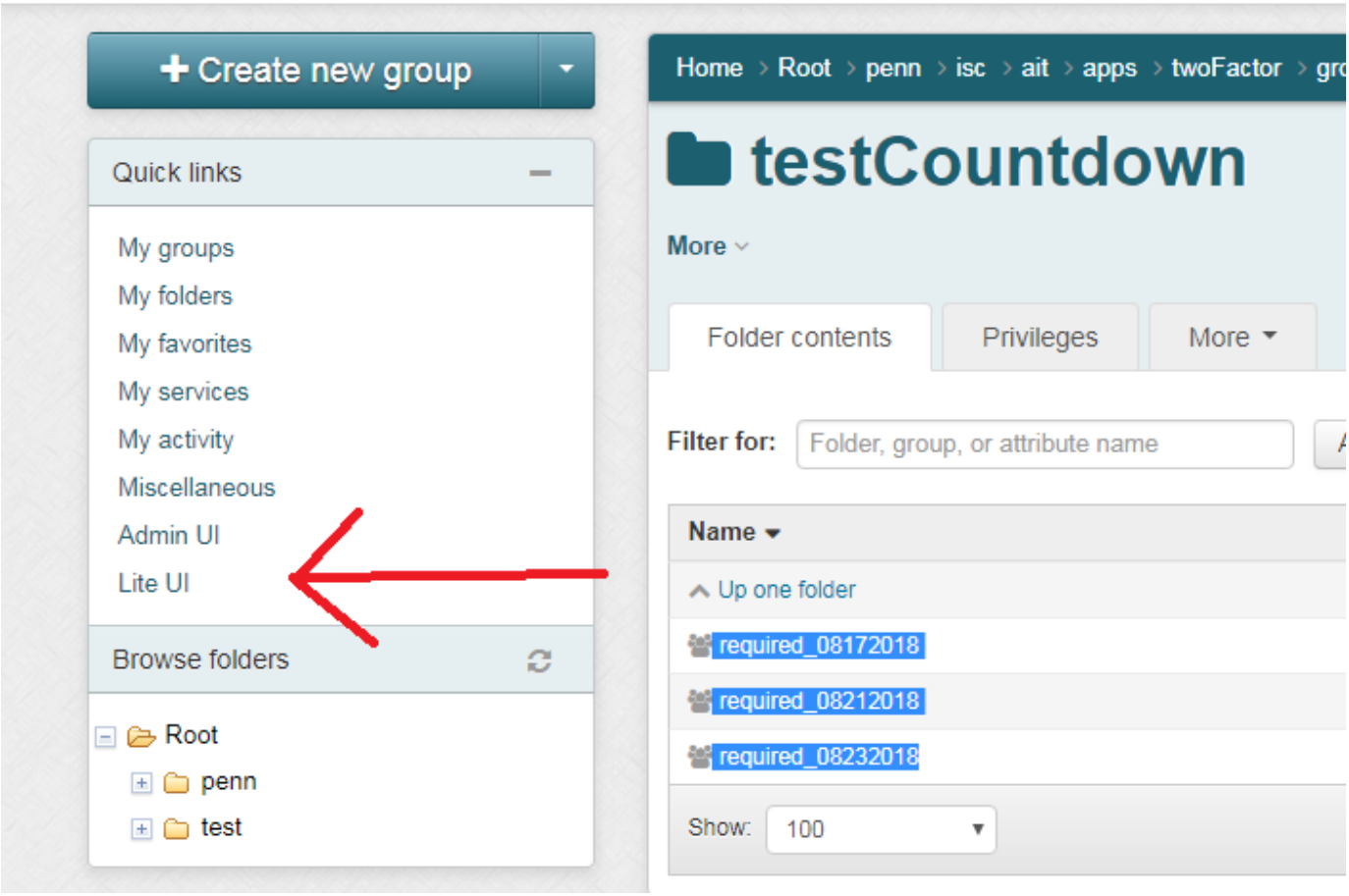
Assign a countdown

Go to a group in the two-step folder structure (or create one)

Note, do testing in this folder: https://grouper.apps.upenn.edu/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Stem.viewStem&stemName=penn:isc:ait:apps:twoFactor:groups:testCountdown

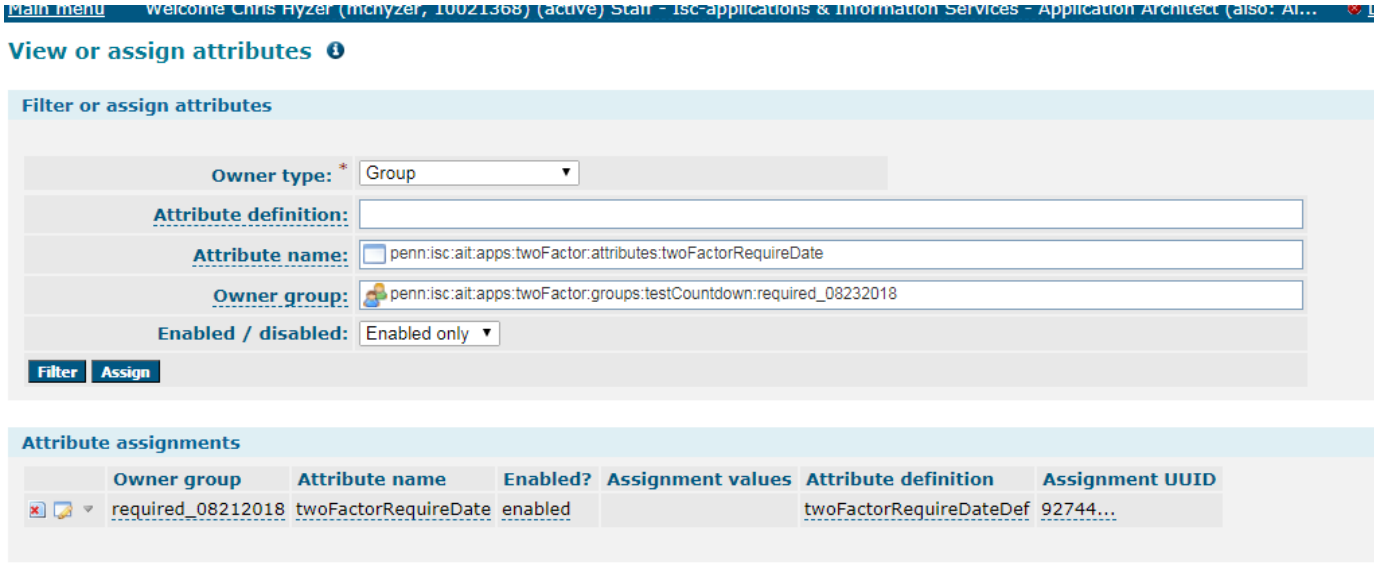
```
penn:isc:ait:apps:twoFactor:groups:testCountdown
```

Go to lite UI (its easier after we upgrade penngroups)

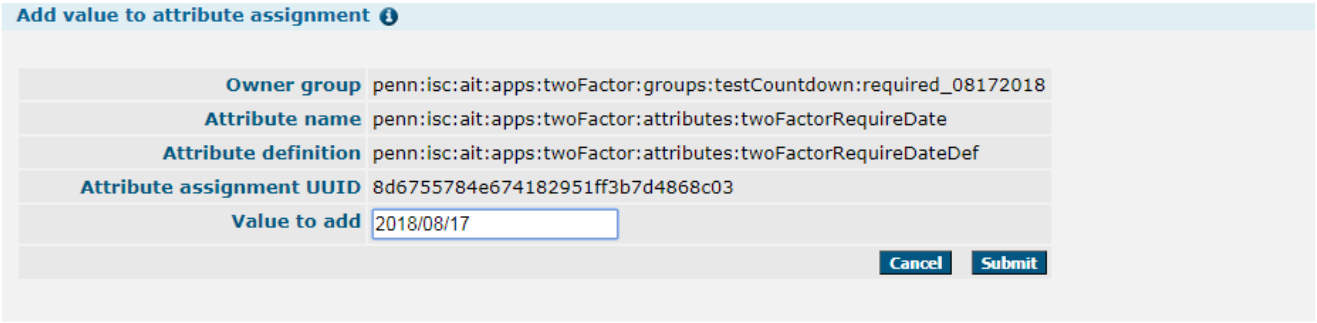


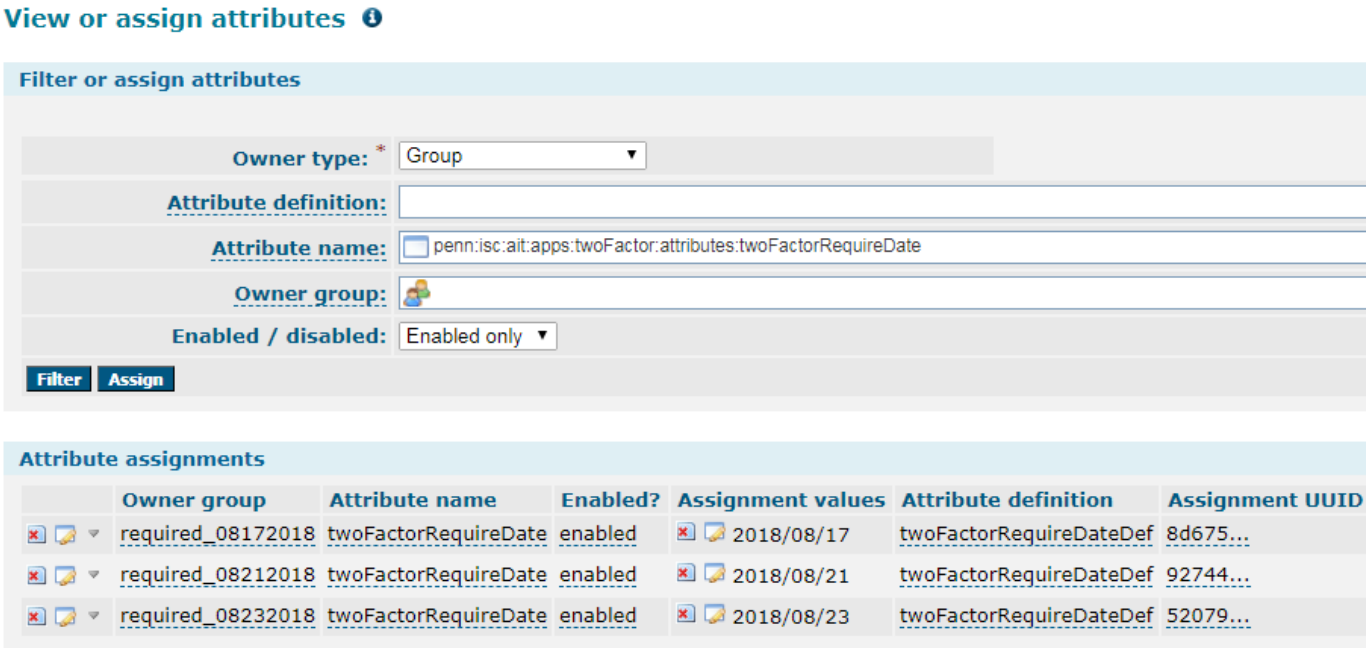
Manage attributes and permissions

View or assign attributes:



Assign value



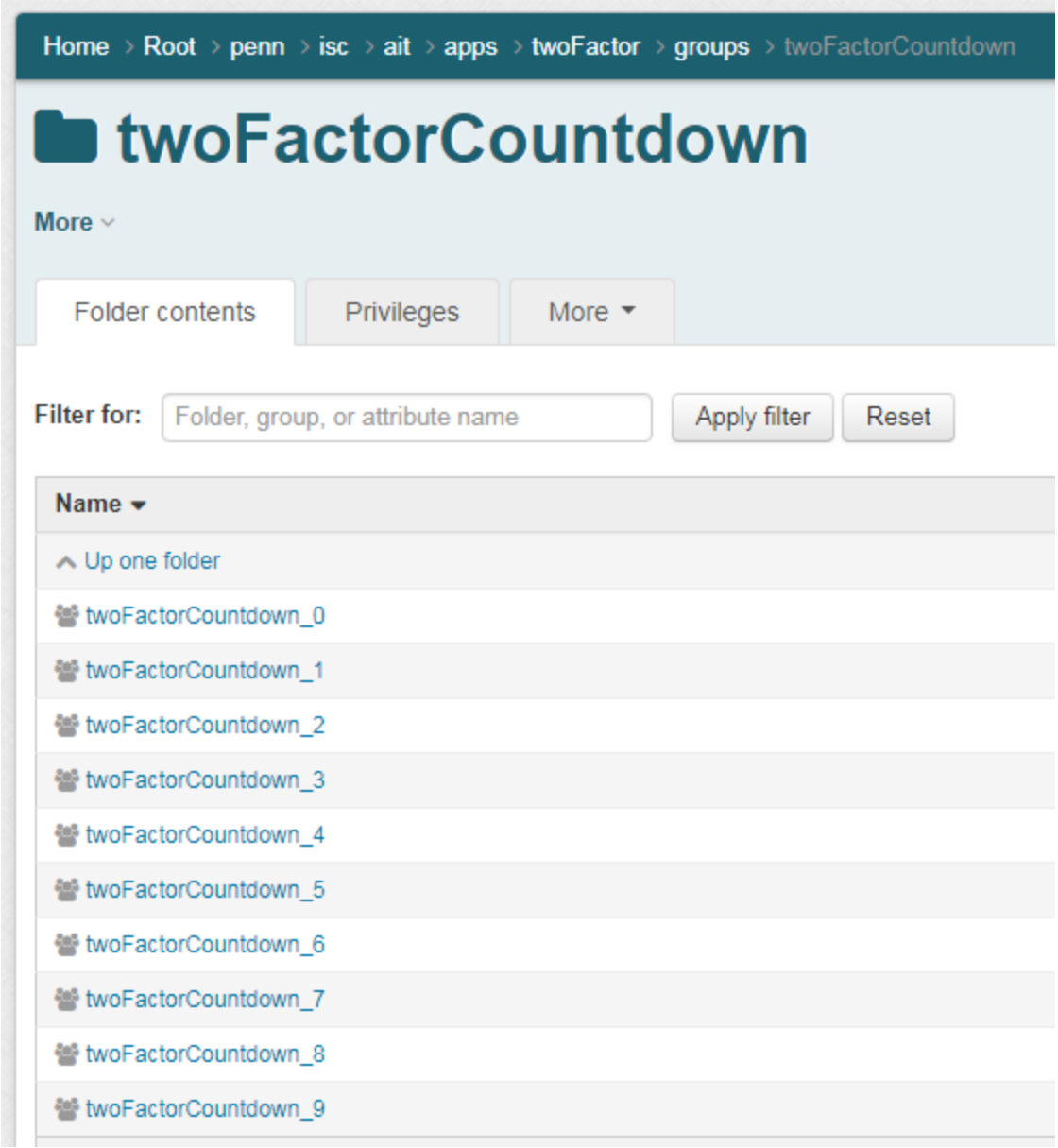


Group structure

Create a folder for these groups: penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown

Create 10 groups...

Group extension	meaning
twoFactorCountdown_0	required for two-step
twoFactorCountdown_1	required for two-step in 1 day
twoFactorCountdown_2	required for two-step in 1 days
twoFactorCountdown_n	required for two-step in n days
twoFactorCountdown_9	required for two-step in 9 days

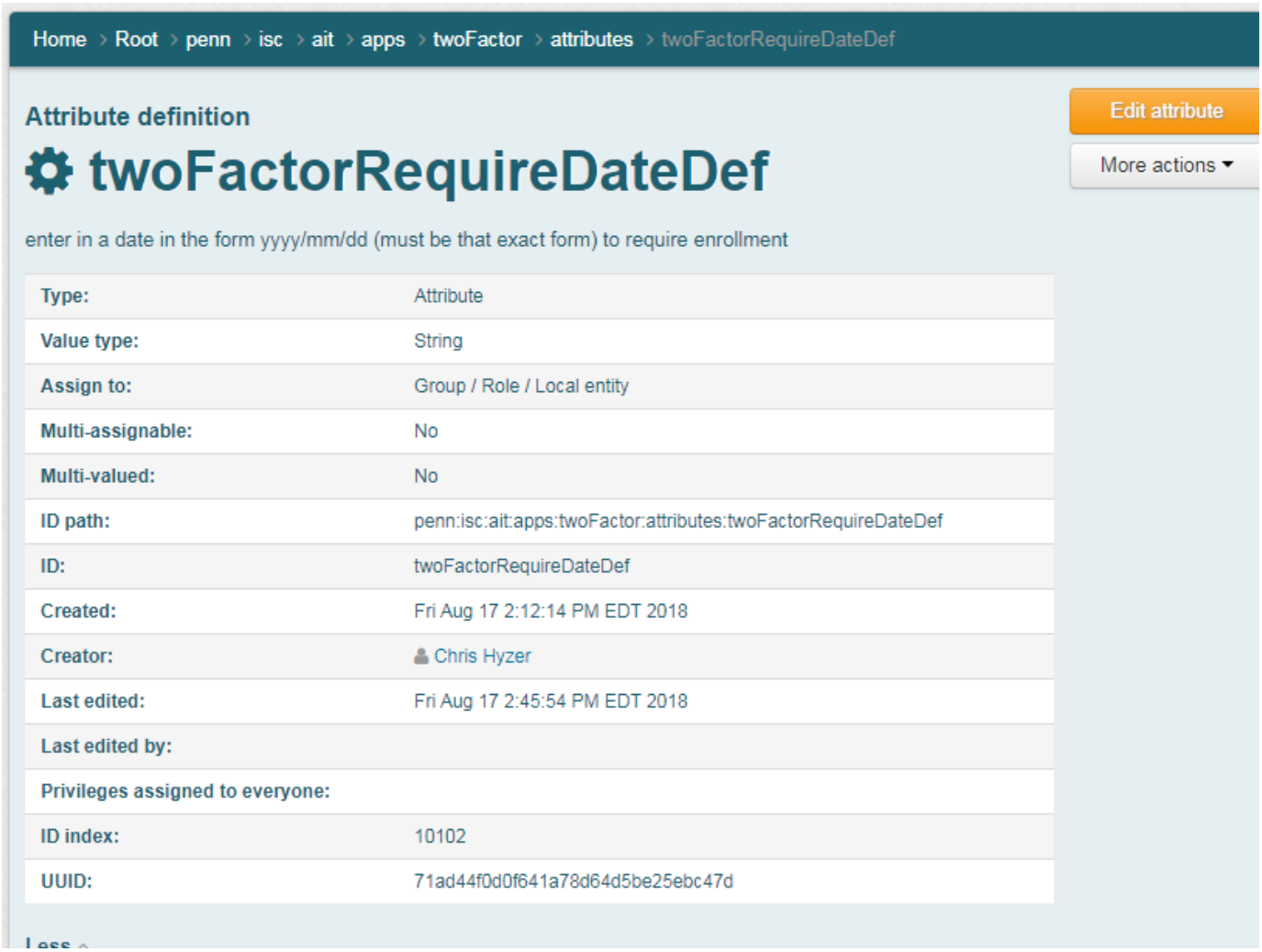


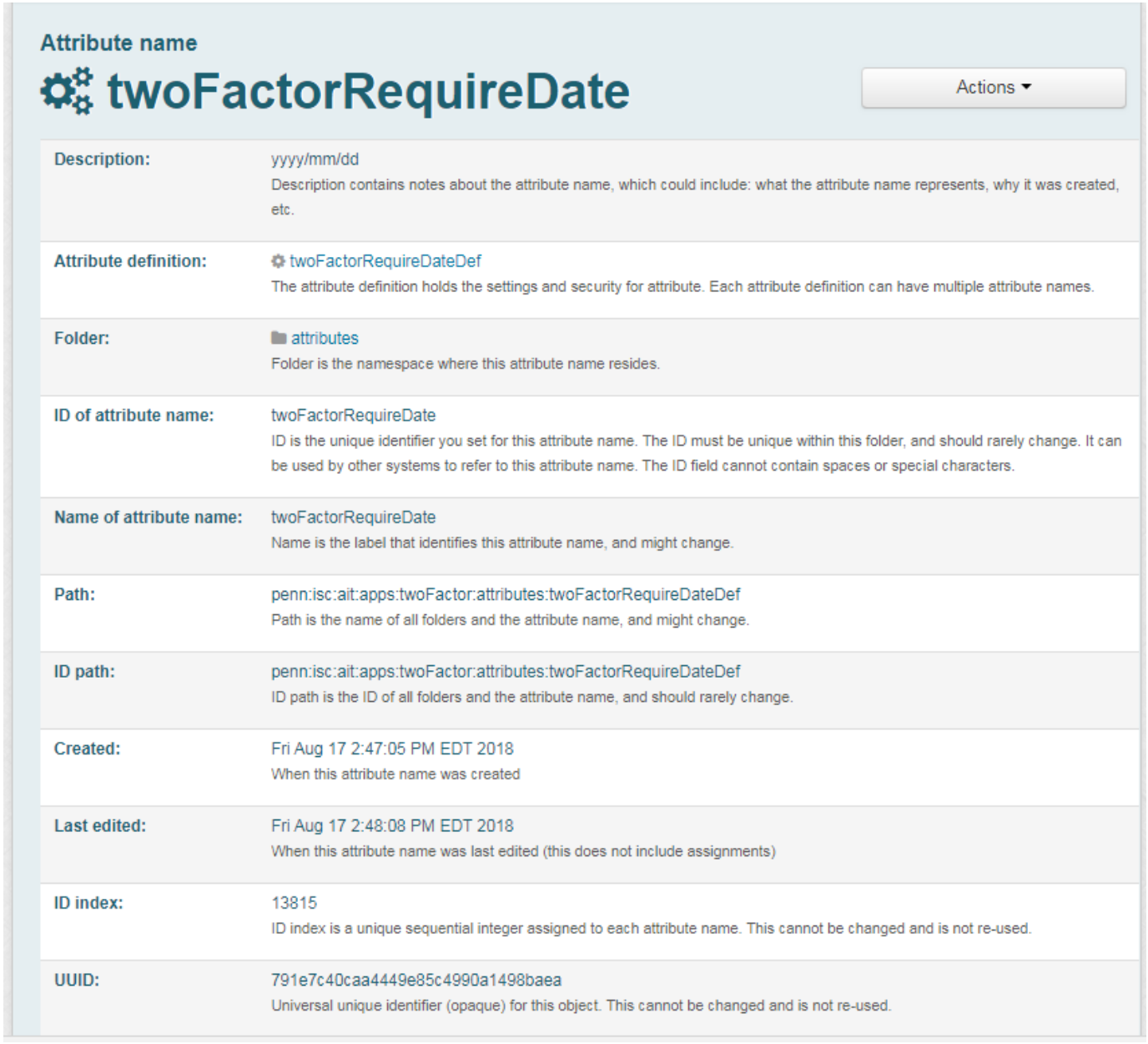
Release these groups to the IdP by allowing the shibdev service principal to READ on the folder inherited priv

Add the twoFactorCountdown_0 group to the two-step required group, so any members are required for two-step.

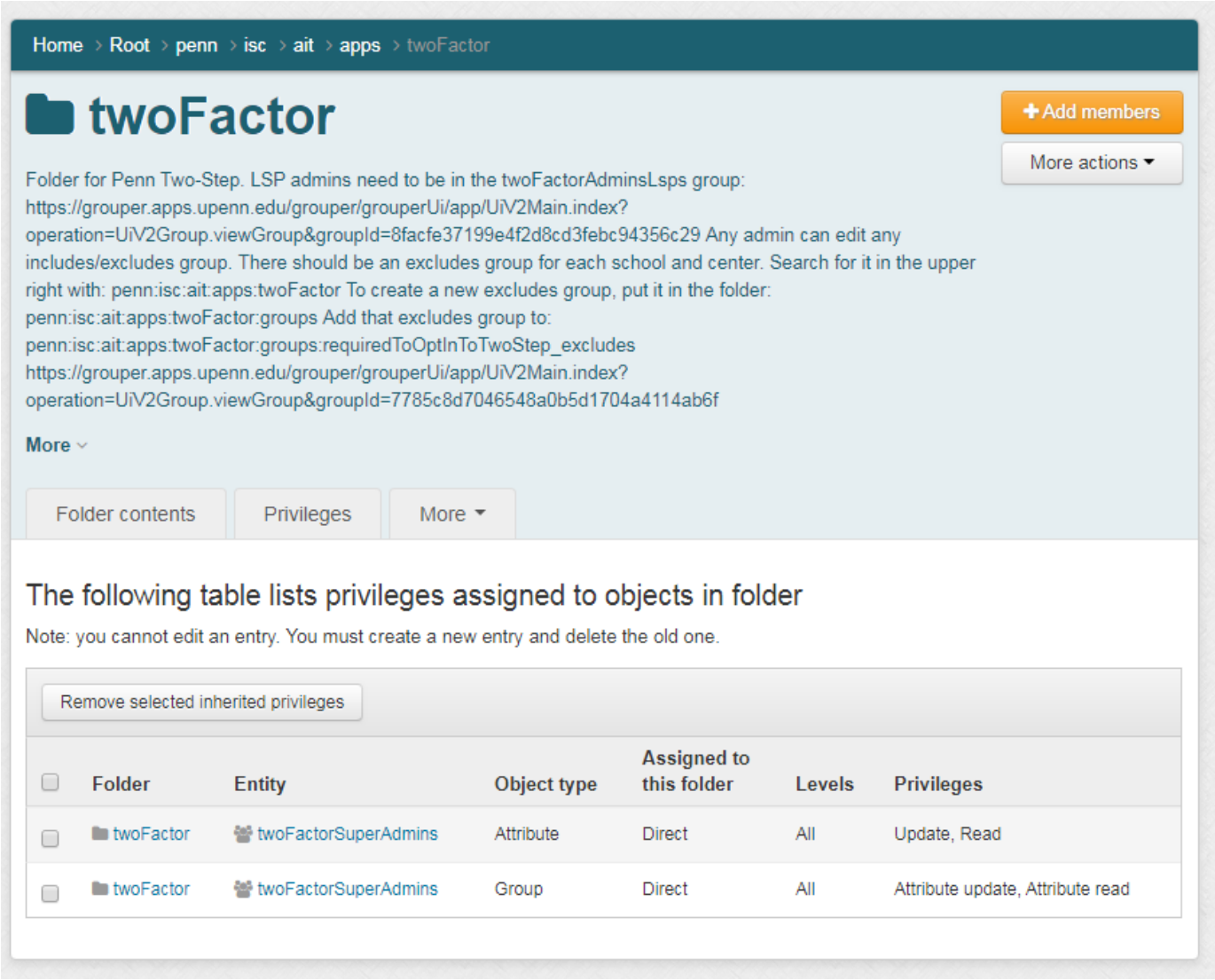
Attribute

Make a single assign attribute with single value string which is yyyy/mm/dd for the day that the group is required in two-step


Home › Root › penn › isc › ait › apps › twoFactor › attributes › twoFactorRequireDateDef
Attribute definition
twoFactorRequireDateDef
Edit attribute
More actions
enter in a date in the form yyyy/mm/dd (must be that exact form) to require enrollment
Type: Attribute
Value type: String
Assign to: Group / Role / Local entity
Multi-assignable: No
Multi-valued: No
ID path: penn:isc:ait:apps:twoFactor:attributes:twoFactorRequireDateDef
ID: twoFactorRequireDateDef
Created: Fri Aug 17 2:12:14 PM EDT 2018
Creator: Chris Hyzer
Last edited: Fri Aug 17 2:45:54 PM EDT 2018
Last edited by:
Privileges assigned to everyone:
ID index: 10102
UUID: 71ad44f0d0f641a78d64d5be25ebc47d
Less



Allow super admins of two-step to be able to assign that attribute



Views and loader

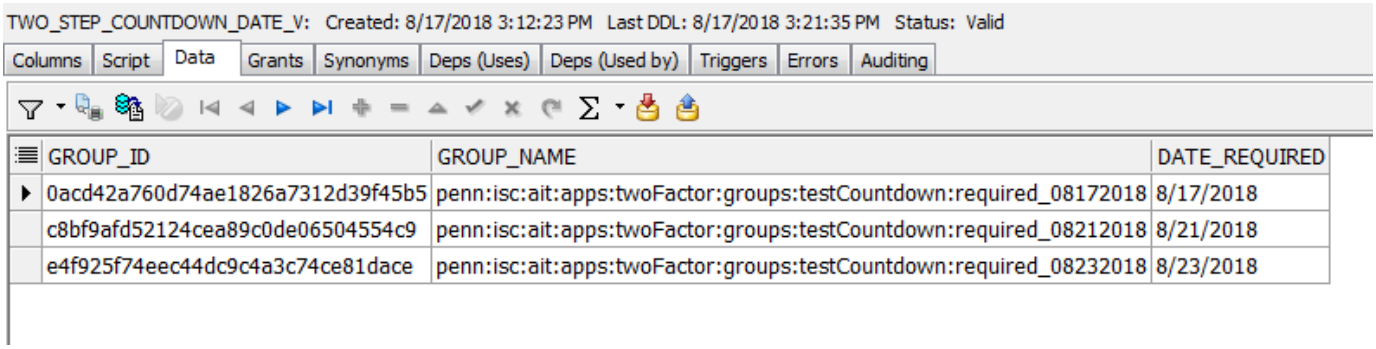
We need to do a lot of views and a loader job to make this easy to troubleshoot. Lets start with all groups with attributes in the right format

```
/* Formatted on 8/17/2018 3:08:54 PM (QP5 v5.252.13127.32847) */
CREATE OR REPLACE FORCE VIEW TWO_STEP_COUNTDOWN_GROUPS_V
(  group_id,
   GROUP_NAME,
   VALUE_STRING
)
   BEQUEATH DEFINER
AS
   SELECT group_id, group_name, value_String
     FROM GROUPER_AVAL_ASN_GROUP_V
    WHERE     attribute_def_name_name =

'penn:isc:ait:apps:twoFactor:attributes:twoFactorRequireDate'
          AND enabled = 'T'
          AND REGEXP_LIKE (value_string, '^\d\d\d\d/\d\d/\d\d$');
```

Lets convert that to a date

```
/* Formatted on 8/17/2018 3:21:16 PM (QP5 v5.252.13127.32847) */
CREATE OR REPLACE FORCE VIEW TWO_STEP_COUNTDOWN_DATE_V
(
   GROUP_ID,
   GROUP_NAME,
   DATE_REQUIRED
)
   BEQUEATH DEFINER
AS
   SELECT GROUP_ID, group_name, TO_DATE (value_String, 'yyyy/mm/dd')
     FROM TWO_STEP_COUNTDOWN_GROUPS_V;
```

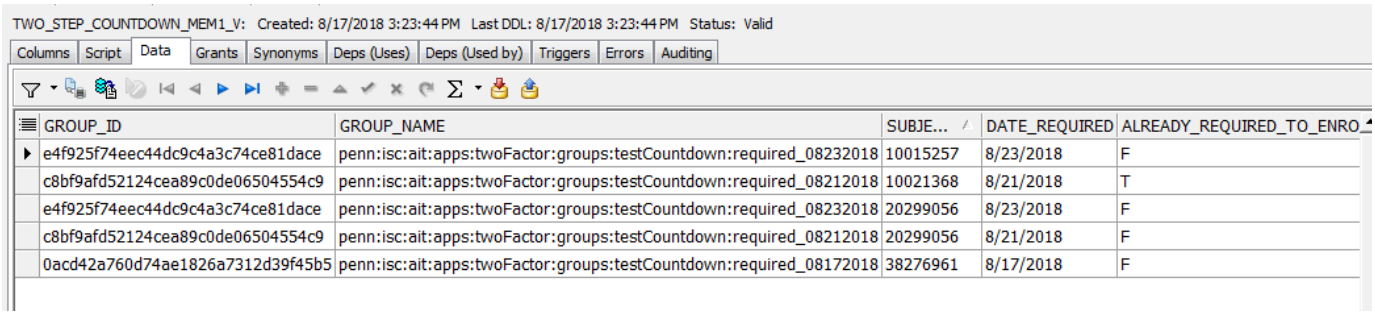


GROUP_ID	GROUP_NAME	DATE_REQUIRED
0acd42a760d74ae1826a7312d39f45b5	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08172018	8/17/2018
c8bf9afd52124cea89c0de06504554c9	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08212018	8/21/2018
e4f925f74eec44dc9c4a3c74ce81dace	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08232018	8/23/2018

Make a view of people with expire dates (can have dupes). Include if they are enrolled

```
/* Formatted on 8/17/2018 3:24:47 PM (QP5 v5.252.13127.32847) */
CREATE OR REPLACE FORCE VIEW TWO_STEP_COUNTDOWN_MEM1_V
(
   GROUP_ID,
   GROUP_NAME,
   SUBJECT_ID,
   DATE_REQUIRED,
   ALREADY_REQUIRED_TO_ENROLL
)
   BEQUEATH DEFINER
AS
   SELECT GMLV.GROUP_ID,
          gmlv.group_name,
          GMLV.SUBJECT_ID,
          TSCDV.DATE_REQUIRED,
          -- note we cache some memberships in this table to make
          -- subselects faster
          DECODE (
             (SELECT 1
                FROM penn_memberships_lw gmlv2
               WHERE     gmlv2.group_name =

'penn:isc:ait:apps:twoFactor:groups:requiredUsersStaff:twoFactorStaff'
                     AND gmlv2.member_id = gmlv.member_id
                     AND gmlv2.list_name = 'members'),
             1, 'T',
             'F')
             AS already_required_to_enroll
     FROM grouper_memberships_lw_v gmlv, TWO_STEP_COUNTDOWN_date_V tscdv
    WHERE     GMLV.GROUP_ID = TSCDV.GROUP_ID
          AND GMLV.LIST_NAME = 'members'
          AND GMLV.SUBJECT_SOURCE = 'pennperson';
```



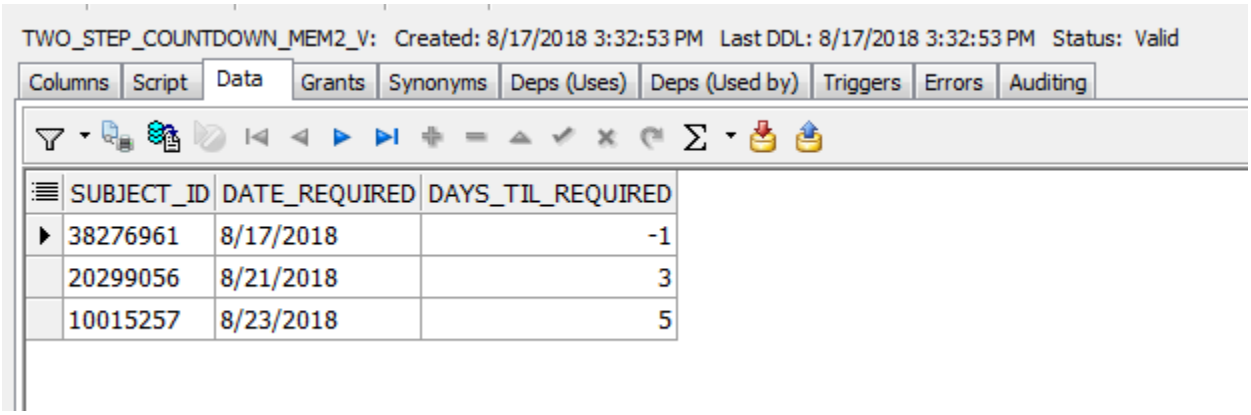
TWO_STEP_COUNTDOWN_MEM1_V: Created: 8/17/2018 3:23:44 PM Last DDL: 8/17/2018 3:23:44 PM Status: Valid

Columns | Script | Data | Grants | Synonyms | Deps (Uses) | Deps (Used by) | Triggers | Errors | Auditing

GROUP_ID	GROUP_NAME	SUBJE...	DATE_REQUIRED	ALREADY_REQUIRED_TO_ENRO...
e4f925f74eec44dc9c4a3c74ce81dace	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08232018	10015257	8/23/2018	F
c8bf9afd52124cea89c0de06504554c9	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08212018	10021368	8/21/2018	T
e4f925f74eec44dc9c4a3c74ce81dace	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08232018	20299056	8/23/2018	F
c8bf9afd52124cea89c0de06504554c9	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08212018	20299056	8/21/2018	F
0acd42a760d74ae1826a7312d39f45b5	penn:isc:ait:apps:twoFactor:groups:testCountdown:required_08172018	38276961	8/17/2018	F

Now make a view with one row per person for the 9 days, including the group names, this is what will be loaded

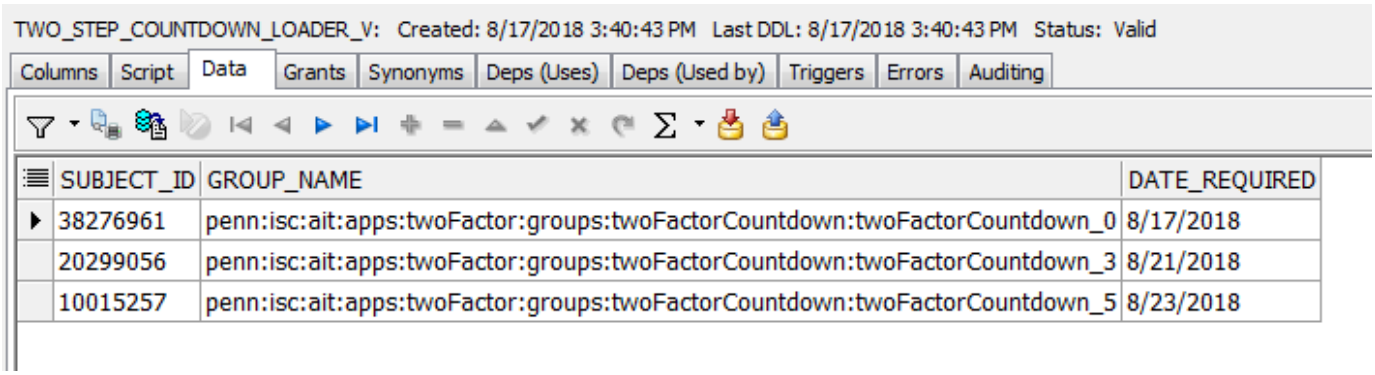
```
/* Formatted on 8/17/2018 3:33:05 PM (QP5 v5.252.13127.32847) */
CREATE OR REPLACE FORCE VIEW TWO_STEP_COUNTDOWN_MEM2_V
(
   SUBJECT_ID,
   DATE_REQUIRED,
   DAYS_TIL_REQUIRED
)
   BEQUEATH DEFINER
AS
   SELECT DISTINCT
          SUBJECT_ID,
          DATE_REQUIRED,
          ROUND (tscmv.DATE_REQUIRED - SYSDATE) AS DAYS_TIL_REQUIRED
     FROM TWO_STEP_COUNTDOWN_MEM1_V tscmv
    WHERE     tscmv.ALREADY_REQUIRED_TO_ENROLL = 'F'
          AND tscmv.DATE_REQUIRED =
                 (SELECT MIN (tscmv2.date_required)
                    FROM TWO_STEP_COUNTDOWN_MEM1_V tscmv2
                   WHERE tscmv.subject_id = tscmv2.subject_id);
```



SUBJECT_ID	DATE_REQUIRED	DAYS_TIL_REQUIRED
38276961	8/17/2018	-1
20299056	8/21/2018	3
10015257	8/23/2018	5

Now make the loader view

```
/* Formatted on 8/17/2018 3:40:55 PM (QP5 v5.252.13127.32847) */
CREATE OR REPLACE FORCE VIEW TWO_STEP_COUNTDOWN_LOADER_V
(
   SUBJECT_ID,
   GROUP_NAME,
   DATE_REQUIRED
)
   BEQUEATH DEFINER
AS
   SELECT subject_id,
          (
'penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:twoFactorCountdown_'
           || CASE
                 WHEN tcmv.DAYS_TIL_REQUIRED <= 0 THEN '0'
                 ELSE TO_CHAR (tcmv.DAYS_TIL_REQUIRED)
              END)
             AS group_name,
          date_required
     FROM TWO_STEP_COUNTDOWN_MEM2_V tcmv
    WHERE tcmv.DAYS_TIL_REQUIRED <= 9;
```



SUBJECT_ID	GROUP_NAME	DATE_REQUIRED
38276961	penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:twoFactorCountdown_0	8/17/2018
20299056	penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:twoFactorCountdown_3	8/21/2018
10015257	penn:isc:ait:apps:twoFactor:groups:twoFactorCountdown:twoFactorCountdown_5	8/23/2018

Add loader and schedule/run it

Loader settings

Loader actions

This group has loader configuration

Source type	SQL pull the members from a SQL database. Can be SQL or LDAP
Loader type	SQL_GROUP_LIST the SQL query loads the members of multiple groups. Can be SQL_SIMPLE or SQL_GROUP_LIST
Database name	grouper jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = orrcdbpr-clstr.seo.int)(PORT = 1521)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = pcom_svc1.world))) server ID that is configured in the grouper-loader.properties that identifies the connection information to the database server. Note: "grouper" means use the Grouper registry database connection.
SQL query	select group_name, subject_id, 'pennperson' as subject_source_id from TWO_STEP_COUNTDOWN_LOADER_V query for memberships. Since this is SQL_GROUP_LIST, the required GROUP_NAME column holds the group system name of the membership. the SUBJECT_ID or SUBJECT_IDENTIFIER or SUBJECT_ID_OR_IDENTIFIER column is required, and the SUBJECT_SOURCE_ID column is optional (but recommended for better performance). SUBJECT_ID has the best performance, and SUBJECT_IDENTIFIER and SUBJECT_ID_OR_IDENTIFIER are slower since they require subject API lookups. If the data has group names as members, it must be in a SUBJECT_IDENTIFER column.
Schedule type	CRON Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL
Schedule	0 0 * * * ? Every hour
Priority	this job has the default and middle priority of 5 (higher numbers have a higher priority)
Require members in other group(s)	
Group query (metadata on groups)	query (optional) for SQL_GROUP_LIST which should return cols: group_name, group_display_name (optional), group_description (optional). This should return all groups managed by this job. The name and display name are the full folder path. If there is a column named any of the following: readers, viewers, admins, updaters, optins, optouts, group_attr_readers, group_attr_updaters, then the data in the column (comma separated subjectId's or subjectIdentifers which can include group names) will be assigned to that group's privilege list. Note you can use inherited privileges on a folder instead.
Groups like sql part	sql like string (e.g. school:orgs:%org%_systemOfRecord), and the loader should be able to query group names to see which names are managed by this loader job. So if a group falls off the loader resultset (or is moved), this will help the loader remove the members from this

sdf