

Countdown groups for password reset requirement

Wiki Home	Grouper Release Announcements	Grouper Guides	Grouper Deployment Guide	Community Contributions	Internal Developer Resources
---------------------------	---	--------------------------------	--	---	--

We need a group that holds people who have not changed their password after Feb 2, 2021.

Those people should flow through count down group so our authn can give them a countdown warning to go and set their pass or they will be locked.

Setup the group is a simple LDAP loader. The match to get to the integer in AD that represents the date is the only trick



o365oneAdPasswordLastChanged

[More actions ▾](#)

holds people who havent changed their pass after Feb 15 2021

This group is managed by loader group o365oneAdPasswordLastChanged. It was last fully loaded on Fri Jan 22 17:46:57 EST 2021. Summary is: total: 47663 inserted: 47661 deleted: 0 updated: 0

[More ▾](#)[Members](#)[Privileges](#)[More ▾](#)

Loader settings

[Loader actions ▾](#)

This group has loader configuration

This group is managed by loader group o365oneAdPasswordLastChanged. It was last fully loaded on Fri Jan 22 17:46:57 EST 2021. Summary is: total: 47663 inserted: 47661 deleted: 0 updated: 0

State	ENABLED
Source type	LDAP pull the members from an LDAP server. Can be SQL or LDAP
Loader type	LDAP_SIMPLE loaded from LDAP filter which returns subject ids or identifiers. Can be LDAP_SIMPLE, LDAP_GROUP_LIST, or LDAP_GROUPS_FROM_ATTRIBUTES
Server ID	oneProdAd ldaps://azdc01.one.upenn.edu:636 server ID that is configured in the grouper-loader.properties that identifies the connection information to the LDAP server
LDAP filter	(&(employeeID=*)(pwdLastSet<=132578388000000000)) LDAP filter returns objects that have subjectIds or subjectIdentifiers
Subject attribute name	employeeID attribute name of the returned object the holds subject IDs or identifiers
Search base DN	OU=365Users,DC=one,DC=upenn,DC=edu location that constrains the subtree where the filter is applicable. Note, this is relative to the base DN in the ldap server config in the grouper-loader.properties for this server. This makes the query more efficient
Schedule	37 0 * * * ? At 37 seconds past the minute
Subject source ID	pennperson source ID from the sources.xml that narrows the search for subjects. This is optional though makes the loader job more efficient
Subject lookup type	subjectId can be either: subjectId (most efficient, default), subjectIdentifier (2nd most efficient), or subjectIdOrIdentifier
Search scope	SUBTREE_SCOPE how deep to search in LDAP. Can be OBJECT_SCOPE, ONELEVEL_SCOPE, or SUBTREE_SCOPE (default)
Priority	this job has the default and middle priority of 5 (higher numbers have a higher priority)
Subject expression	JEXL expression language fragment that processes the subject string before passing it to the subject API. e.g. \${loaderLdapEUtils.convertDnToSpecificValue(subjectId)}
Job name	LDAP_SIMPLE__penn:isc:ait:apps:O365:o365oneAdPasswordLastChanged__568ad895c45b45c091efa18b3a5424a9 used in the database in the grouper_loader_log table to identify records for this job


Now we need some queries to make countdown groups loader job. We want from 30 0 where 0 is March 14th, 2021

Group query: (probably a better way to do this, but this is quick and dirty)

```
create view authz_o365_countdown_names_v as
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_0' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_1' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_2' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_3' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_4' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_5' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_6' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_7' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_8' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_9' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_10' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_11' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_12' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_13' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_14' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_15' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_16' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_17' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_18' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_19' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_20' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_21' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_22' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_23' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_24' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_25' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_26' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_27' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_28' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_29' as group_name)
union all
(select 'penn:isc:ait:apps:0365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_30' as group_name)
```

Make the loader query

```
create view authz_o365_countdown_member_v as
select 'penn:isc:ait:apps:O365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_' || greatest(to_date('2021/03/14', 'yyyy/mm/dd') - current_date, 0) as group_name,
'penn:isc:ait:apps:O365:o365oneAdPasswordLastChanged' as subject_identifier, 'g:gsa' as subject_source_id
where to_date('2021/03/14', 'yyyy/mm/dd') - current_date <= 30
```

 **o365oneAdPasswordCountdown** More actions ▾

loader job to manage countdown groups

More ▾

MembersPrivilegesMore ▾

Loader settings Loader actions ▾

This group has loader configuration

State	ENABLED
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:postgresql://penngroupsproddb.cluster-clftu9idkcq8.us-east-1.rds.amazonaws.com:5432/mydb?sslmode=require 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_identifier, subject_source_id from authz_o365_countdown_member_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_IDENTIFIER column.
Schedule type	CRON Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL
Schedule	0 10 * * ? At 12:01 AM
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)	select group_name from authz_o365_countdown_names_v 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 subjectidentifiers 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	penn:isc:ait:apps:O365:o365oneAdPasswordLastChangedCountdown:oneAdCountdown_% 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 group. Note, if the group is used anywhere as a member or composite member, it won't be removed.
Grouper types applied to groups	comma separated GroupTypes which will be applied to the loaded groups. e.g. addIncludeExclude
Job name	SQL_GROUP_LIST__penn:isc:ait:apps:O365:o365oneAdPasswordCountdown__fc7e05bcc77a4e168ba1e850dc7b8043 used in the database in the grouper_loader_log table to identify records for this job

