Grouper attestation

Grouper attestation means marking a group or folder so that owners must review the membership list periodically. This is useful in ad hoc groups where deprovisioning is not automatic. Owners will be reminded by email to review the memberships. After reviewing the memberships, the group owner will click a button on the group indicating that it has been reviewed.

Attestation is available in a Grouper 2.3 patch and in Grouper 2.4 and above.

Note after installing the patches you should run from GSH:

```
loaderRunOneJob("OTHER_JOB_attestationDaemon");
```

Child pages:

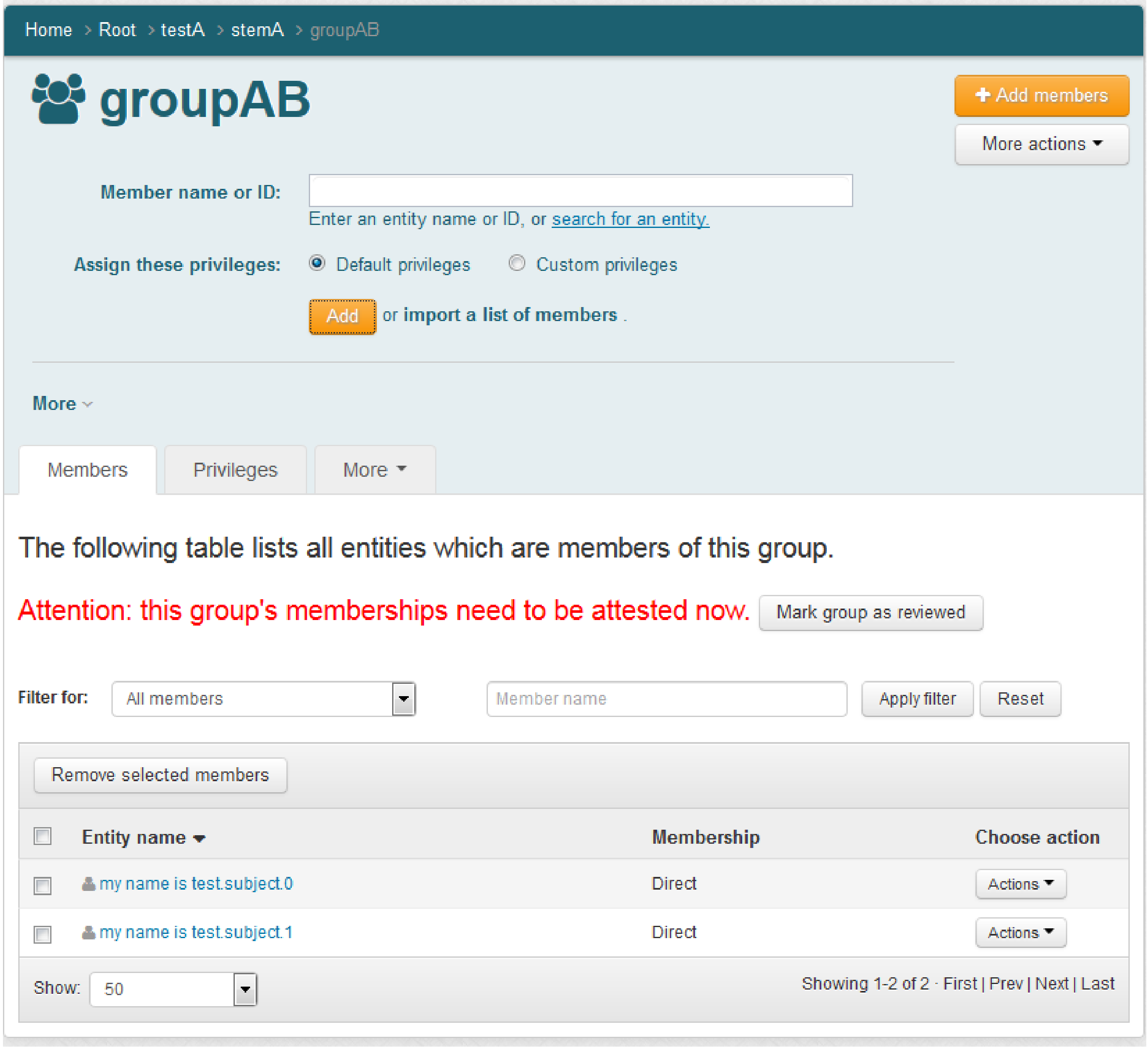
- Grouper attestation audit log
- Grouper attestation edit settings
- Grouper attestation folder level folders and groups with settings
- Grouper attestation folder level groups that need attestation
- Grouper attestation global folders and groups with settings
- Grouper attestation global groups that need attestation
- Grouper attestation testing
- Grouper attestation view settings
- Grouper automatic membership removal if not attested

Outline:

Attest a group as reviewed

When a group needs it memberships reviewed (either initially or when the attestation period has elapsed), you can attest the group on the membership screen or on the attestation screen

On the membership screen you will see a note and a button:



Member name or ID:

Enter an entity name or ID, or search for an entity.

Assign these privileges: ● Default privileges ○ Custom privileges

Add or import a list of members .

The following table lists all entities which are members of this group.

Attention: this group's memberships need to be attested now.

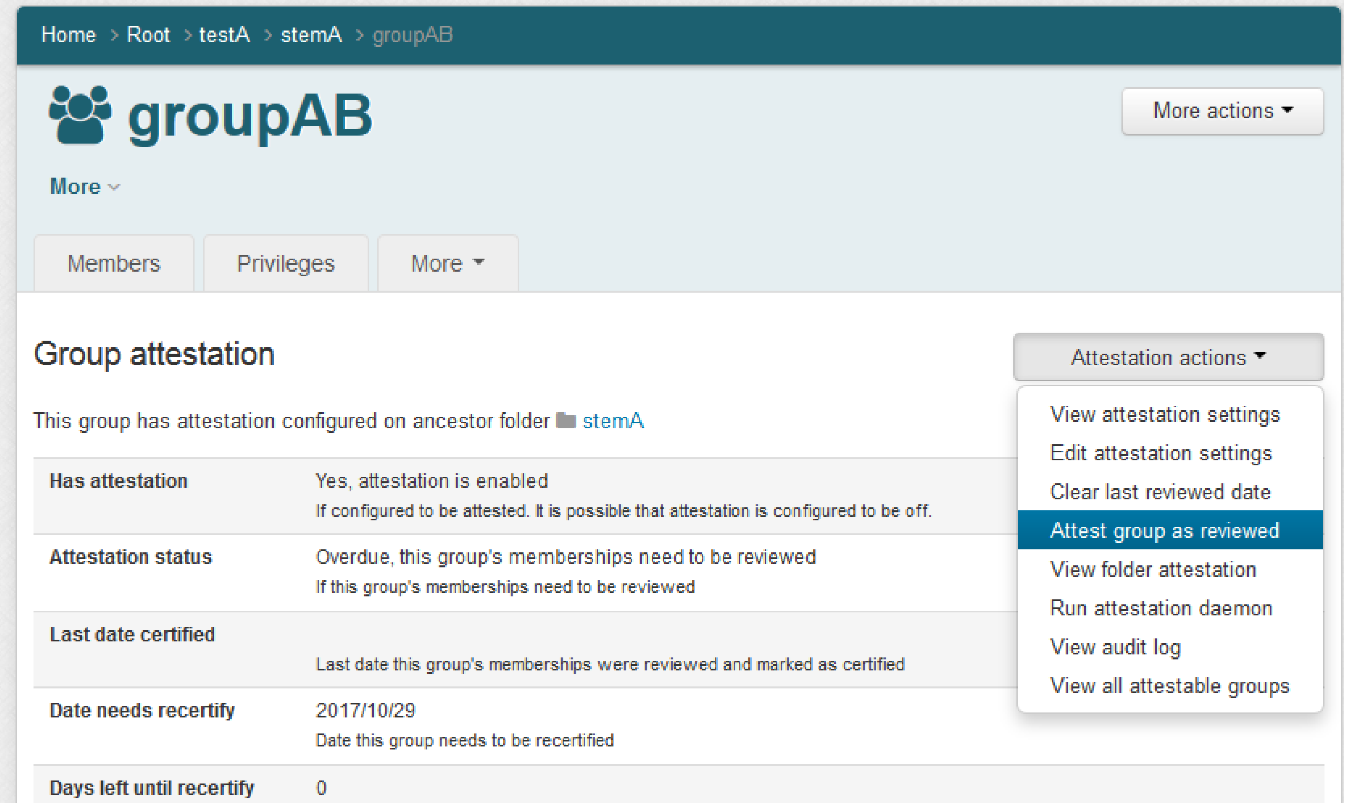
Filter for: All members | Member name

□	Entity name	Membership	Choose action
□	my name is test.subject.0	Direct	Actions
□	my name is test.subject.1	Direct	Actions

Show: 50

Showing 1-2 of 2 · First | Prev | Next | Last

If you are on the attestation screen, you will see a menu item Attestation actions Attest group as reviewed



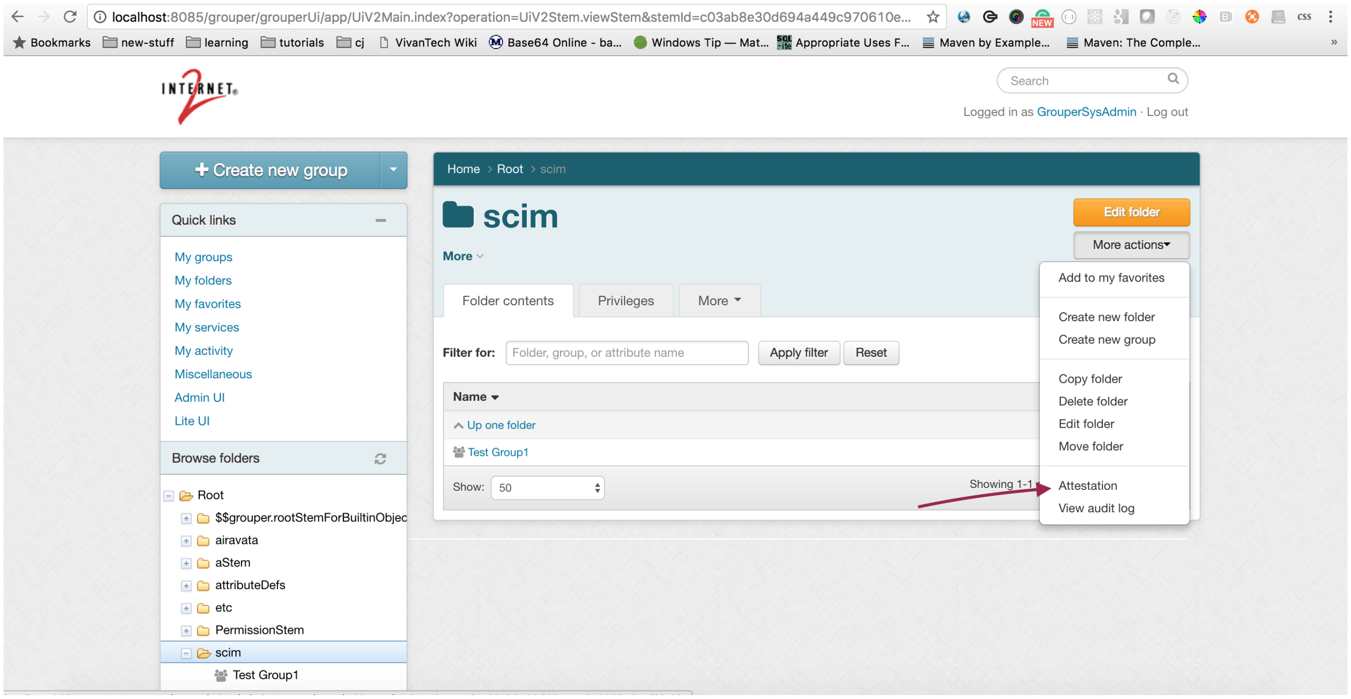
Group attestation

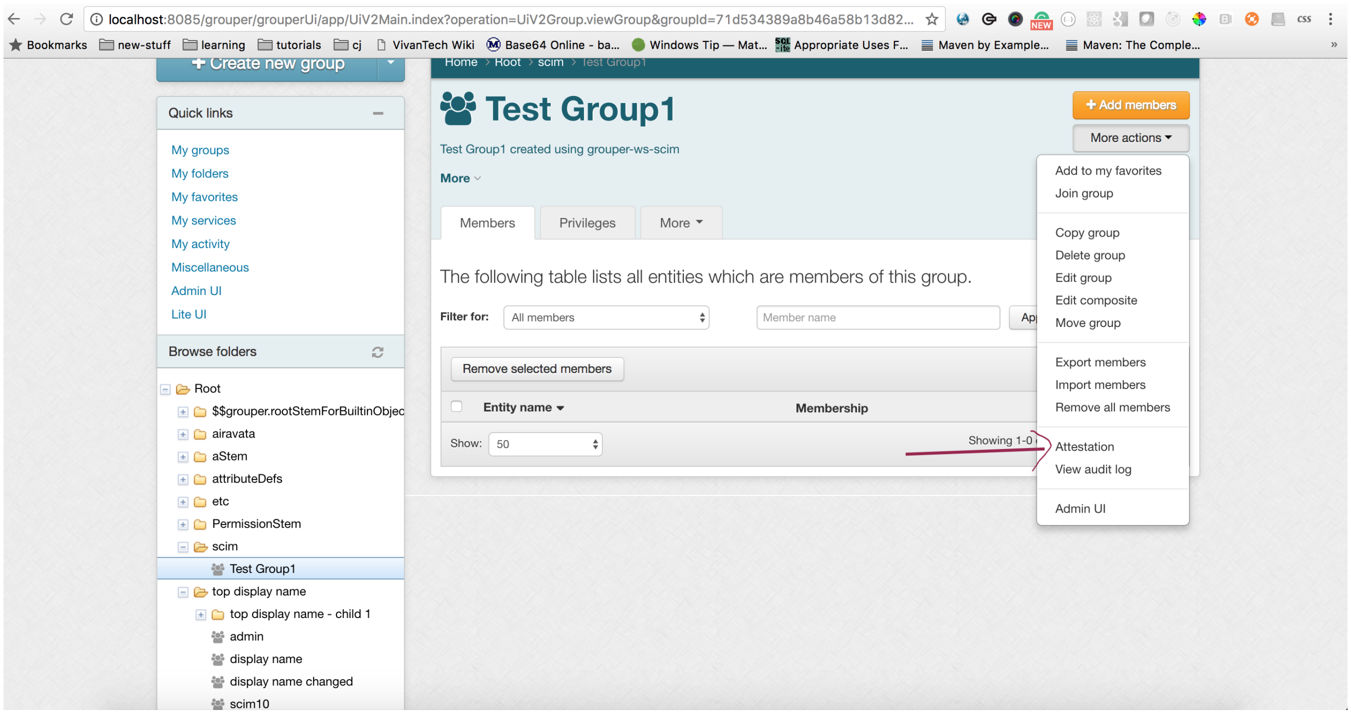
This group has attestation configured on ancestor folder stemA

Has attestation	Yes, attestation is enabled If configured to be attested. It is possible that attestation is configured to be off.
Attestation status	Overdue, this group's memberships need to be reviewed If this group's memberships need to be reviewed
Last date certified	Last date this group's memberships were reviewed and marked as certified
Date needs recertify	2017/10/29 Date this group needs to be recertified
Days left until recertify	0

Attestation menu

You will notice a new menu item Attestation in the More actions dropdown for groups and folders as shown in the screenshots:





Privileges

If you are a Grouper admin or if you have UPDATE or ADMIN privileges on a group, you can edit attestation.

If you can edit attestation or if you have READ on a group, you can READ the attestation.

NOTE: you dont need privileges on the attributes that configure the attestation.

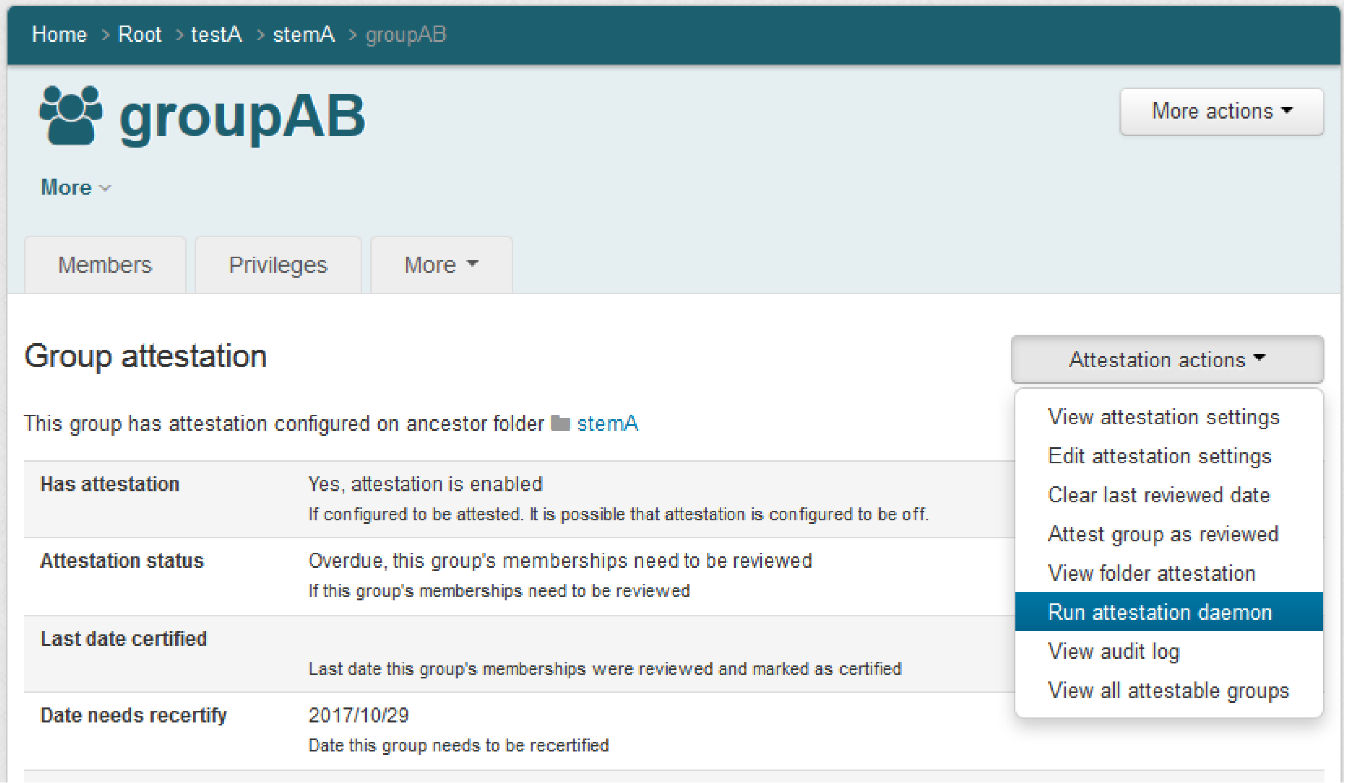
To run the daemon you need to be a Grouper admin

Daemon

There is a cron job which runs everyday (by default) in the Grouper daemon and it sends reminder emails to people configured in attestationEmailAddresses attribute or if there is no email address in that attribute, it picks up the emails from subject source email property of admins for the group. If no emails are found there either, then the job logs an error and move on to the next element. Note that the job doesn't send multiple emails to the same person on the same day even if you configure the cron to run the job multiple times on the same day.

attestationDaysBeforeToRemind attribute controls how many days before the current attestation expires, we are going to start sending emails. Or there is a default configured (default is 180 days)

Run daemon from UI: (you would only do this occasionally or for testing). There is a menu item for grouper admins to be able to kick off the daemon



Group attestation

This group has attestation configured on ancestor folder stemA

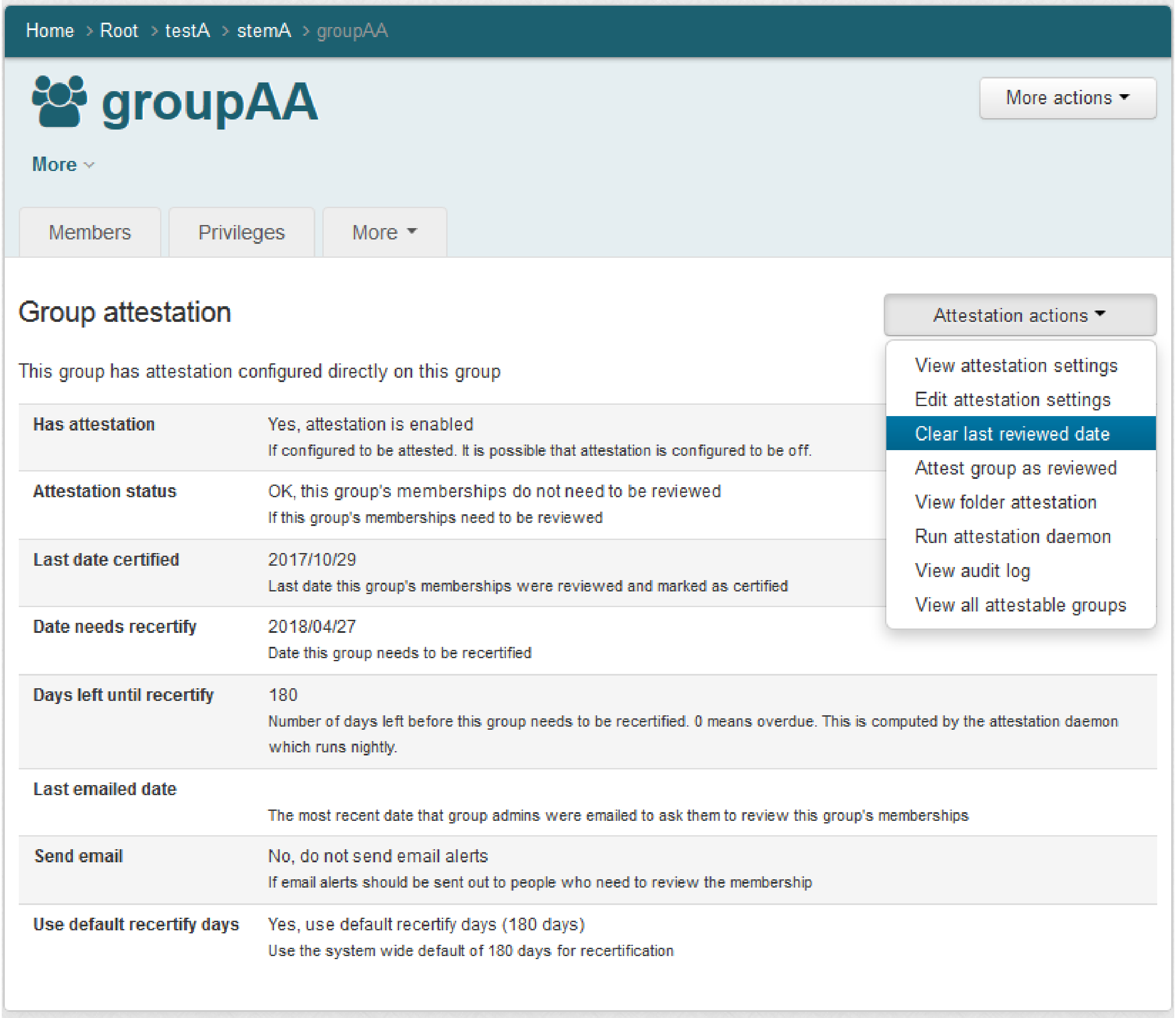
Has attestation	Yes, attestation is enabled If configured to be attested. It is possible that attestation is configured to be off.
Attestation status	Overdue, this group's memberships need to be reviewed If this group's memberships need to be reviewed
Last date certified	Last date this group's memberships were reviewed and marked as certified
Date needs recertify	2017/10/29 Date this group needs to be recertified

Run daemon from GSH:

```
loaderRunOneJob("OTHER_JOB_attestationDaemon");
```

Clear last reviewed date

If you want to mark a group to be reviewed again, you can "clear last reviewed date". While on the attestation screen for a group, click "Attestation actions Clear last reviewed date"



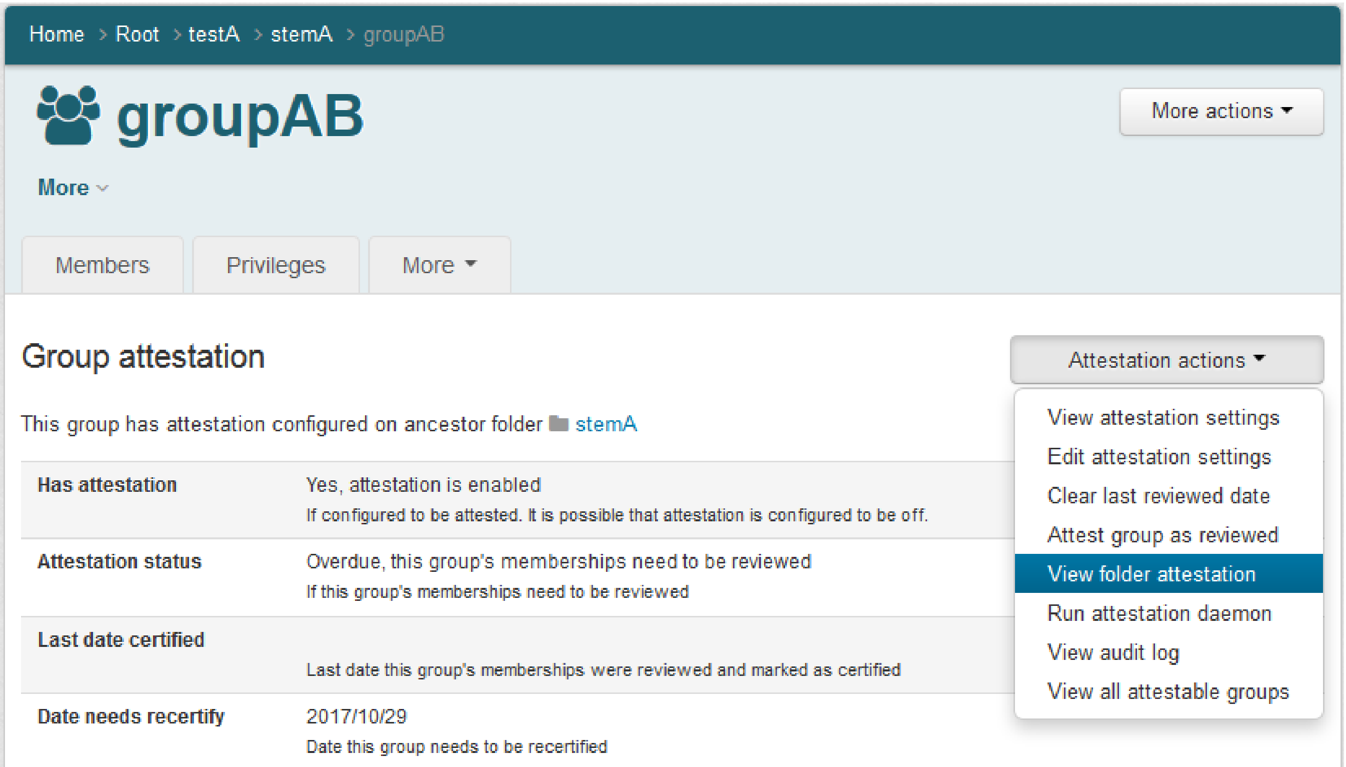
Group attestation

This group has attestation configured directly on this group

Has attestation	Yes, attestation is enabled If configured to be attested. It is possible that attestation is configured to be off.
Attestation status	OK, this group's memberships do not need to be reviewed If this group's memberships need to be reviewed
Last date certified	2017/10/29 Last date this group's memberships were reviewed and marked as certified
Date needs recertify	2018/04/27 Date this group needs to be recertified
Days left until recertify	180 Number of days left before this group needs to be recertified. 0 means overdue. This is computed by the attestation daemon which runs nightly.
Last emailed date	The most recent date that group admins were emailed to ask them to review this group's memberships
Send email	No, do not send email alerts If email alerts should be sent out to people who need to review the membership
Use default recertify days	Yes, use default recertify days (180 days) Use the system wide default of 180 days for recertification

View folder attestation

If a group inherits its attestation settings from an ancestor folder, there is a link from the group attestation menu: Attestation actions View folder attestation



Group attestation

This group has attestation configured on ancestor folder stemA

Has attestation	Yes, attestation is enabled If configured to be attested. It is possible that attestation is configured to be off.
Attestation status	Overdue, this group's memberships need to be reviewed If this group's memberships need to be reviewed
Last date certified	Last date this group's memberships were reviewed and marked as certified
Date needs recertify	2017/10/29 Date this group needs to be recertified

View all attestable groups

If you are in the folder or group "Attestation actions" menu, you can "View all attestable groups". This will go to the global view all attestable groups screen, that need attestation

Emails

- Daemon runs daily (via cron) and look for groups which have not been attested. Should group by email address. Send each user who get an email their own email with a list of groups and linked to be attested. Remind the user about clicking the button saying it is certified.
- Email logic: Take each email to each user (by email address), and only send one email to that user. If there are more than 100 (configured in grouper.properties) attestations, just show 100 in the message but say there are 5432 others so email isn't too big. Also, add at the bottom of each message who was CC'ed since you email will be sent directly to a person.

  e.g.

  school:groupA needs attestation: emails to: jsmith@school.edu, and bgreen@school.edu

  school:groupB needs attestation: emails to: jsmith@school.edu, and kwilson@school.edu

  send 3 emails:

  FIRST EMAIL: To jsmith@school.edu

  Subject: you have 2 grouper groups that require attestation.

  Body:

  You need to attest the memberships of the following groups:

  1. 1. school:groupA   (cc'd bgreen@school.edu)

  <link to membership>

1. 2. school:groupB (cc'd kwilson@school.edu)

<link to membership>

SECOND EMAIL: To bgreen@school.edu

Subject: you have 1 grouper groups that require attestation.

Body:

You need to attest the memberships of the following groups:

1. 1. school:groupA (cc'd jsmith@school.edu)

<link to membership>

THIRD EMAIL: To kwilson@school.edu

Subject: you have 1 grouper groups that require attestation.

Body:

You need to attest the memberships of the following groups:

1. 1. school:groupB (cc'd jsmith@school.edu)

<link to membership>

Configure for first time use

Set this in grouper.properties

```
#put the URL which will be used e.g. in emails to users.  include the webappname at the end, and nothing after
that.
#e.g. https://server.school.edu/grouper/
grouper.ui.url = http://localhost:8088/grouper/

#smtp server is a domain name or dns name.  set to "testing" if you want to log instead of send (e.g. for
testing)
mail.smtp.server = localhost

#this is the default email address where mail from grouper will come from
mail.smtp.from.address = noreply@school.edu


# OPTIONAL FOR ATTESTION, WILL BE BLANK IN PROD
#this is the subject prefix of emails, which will help differentiate prod vs test vs dev etc
mail.smtp.subject.prefix = DEV:
```

Note, might want to leave these as defaults. grouper.properties

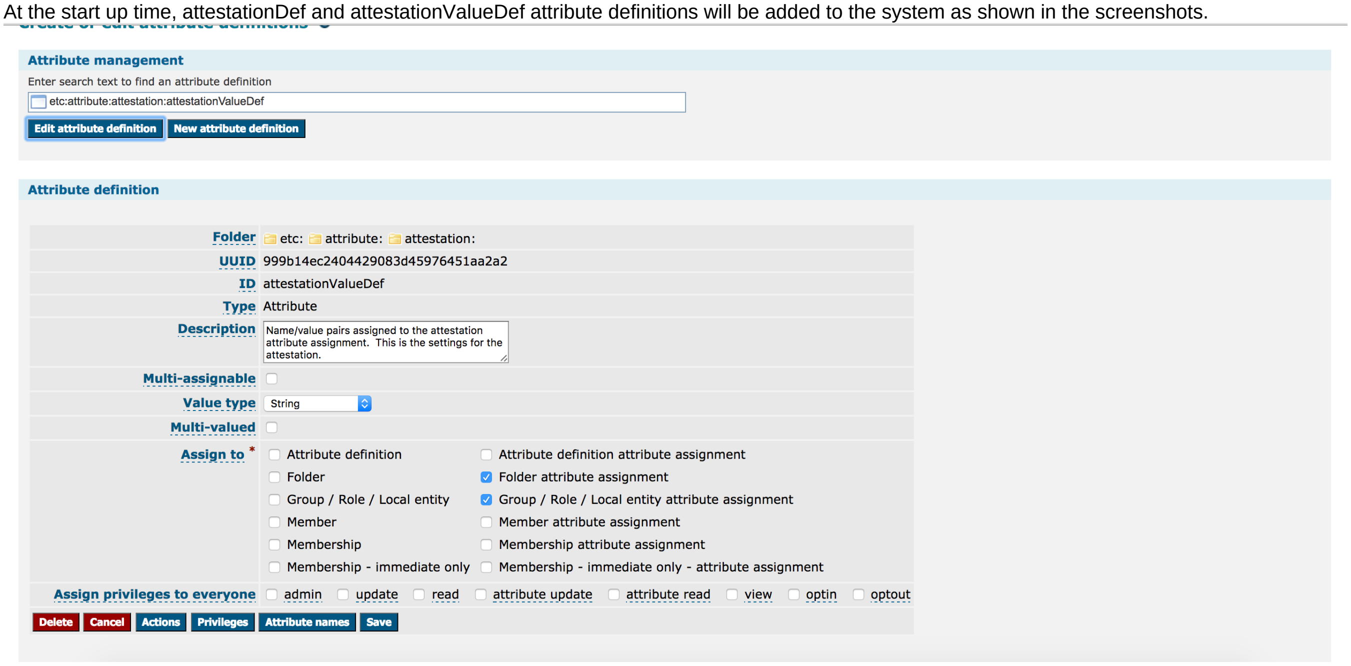
```
#############################################
## Attestation
#############################################

#default value of attestation days until recertify. Every group/folder can define their own days until
recertify value and if they don't provide, use the following one.
attestation.default.daysUntilRecertify = 180

#number of groups shown in the body of attestation email
attestation.email.group.count = 100

#attestation reminder email subject
attestation.reminder.email.subject = You have $objectCount$ groups that require attestation

#attestation reminder email body (links and groups are added dynamically)
attestation.reminder.email.body = You need to attest the memberships of the following groups.  Review the
memberships of each group and click: More actions -> Attestation -> Members of this group have been reviewed
attestation.reminder.email.body.greaterThan100 = There are $remaining$ more groups to be attested.
```

Configure in grouper-loader.properties (these are the defaults)

```
#####################################
## Atttestation Job
#####################################
otherJob.attestationDaemon.class = edu.internet2.middleware.grouper.app.attestation.GrouperAttestationJob
otherJob.attestationDaemon.quartzCron = 0 0 1 * * ?
```

Attributes

At the start up time, attestationDef and attestationValueDef attribute definitions will be added to the system as shown in the screenshots.



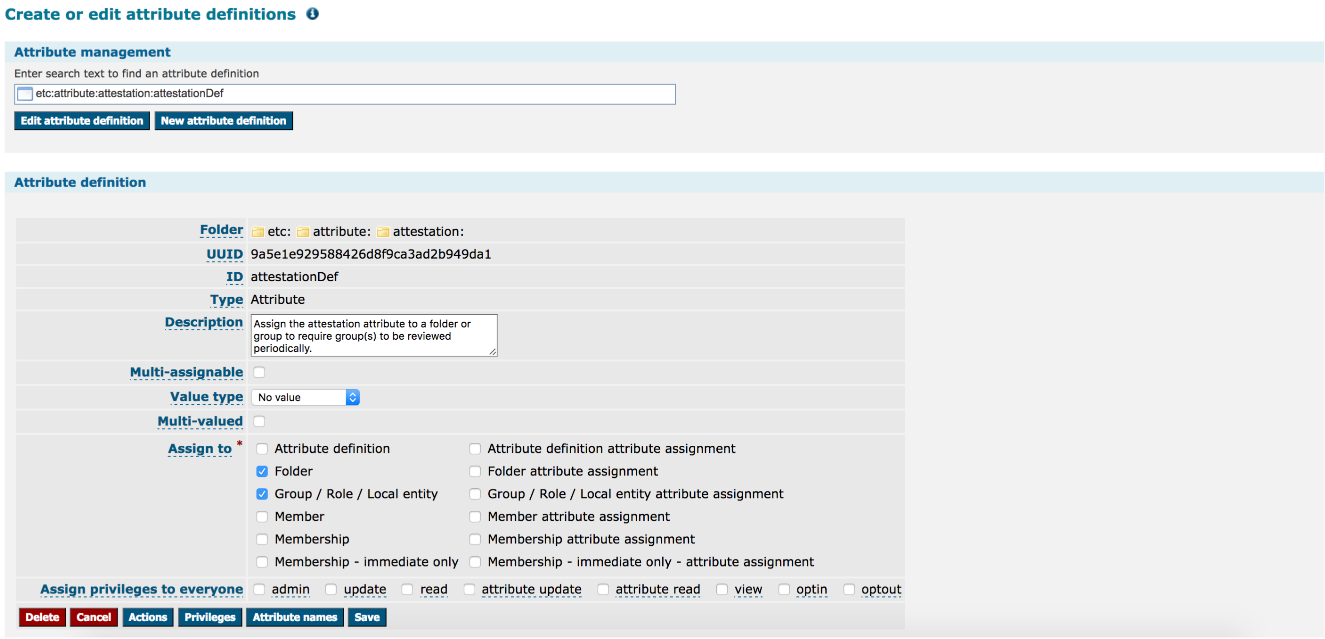
Attribute management

Enter search text to find an attribute definition

etc:attribute:attestation:attestationValueDef

Attribute definition

Folder	etc: attribute: attestation:
UUID	999b14ec2404429083d45976451aa2a2
ID	attestationValueDef
Type	Attribute
Description	Name/value pairs assigned to the attestation attribute assignment. This is the settings for the attestation.
Multi-assignable	□
Value type	String
Multi-valued	□
Assign to *	□ Attribute definition □ Folder □ Group / Role / Local entity □ Member □ Membership □ Membership - immediate only
	□ Attribute definition attribute assignment ☑ Folder attribute assignment ☑ Group / Role / Local entity attribute assignment □ Member attribute assignment □ Membership attribute assignment □ Membership - immediate only - attribute assignment
Assign privileges to everyone	□ admin □ update □ read □ attribute update □ attribute read □ view □ optin □ optout



Create or edit attribute definitions

Attribute management

Enter search text to find an attribute definition

etc:attribute:attestation:attestationDef

Attribute definition

Folder	etc: attribute: attestation:
UUID	9a5e1e929588426d8f9ca3ad2b949da1
ID	attestationDef
Type	Attribute
Description	Assign the attestation attribute to a folder or group to require group(s) to be reviewed periodically.
Multi-assignable	□
Value type	No value
Multi-valued	□
Assign to *	□ Attribute definition □ Attribute definition attribute assignment ☑ Folder □ Folder attribute assignment ☑ Group / Role / Local entity □ Group / Role / Local entity attribute assignment □ Member □ Member attribute assignment □ Membership □ Membership attribute assignment □ Membership - immediate only □ Membership - immediate only - attribute assignment
Assign privileges to everyone	□ admin □ update □ read □ attribute update □ attribute read □ view □ optin □ optout

Design

- Attributes on folders, groups: (two attributeDefs) (note, autocreate these attributeDefs and attributeNames on startup)
  - Note, edit these in the Grouper UI, do not edit them by hand
  - attestation (main flag, other attributes assigned to this assignment, no value, single assign)
    - attestationDirectAssignment (true | false) (on group only) default to false. If true then dont look at a folder for attestation attributes
    - attestationHasAttestation (true | false) (on groups and folders). If true then this group or folder has attestation assigned. On groups then it is directly or indirectly assigned. If on a folder, then it is directly assigned. i.e. if a folder doesnt have this, it doesnt mean that there isnt attestation inherited from a parent folder.
    - attestationSendEmail (String, true | false) default to true if not set
    - attestationEmailAddresses (String) comma separated email addresses to send reminders to. If not set, then get email addresses from list of Admins and Read/Update users. Note, we need a param (in the source) of which subject attribute is the email attribute. If none sent, log error, need either emails here or emails from admins
    - attestationDaysUntilRecertify (String) integer number of days until need to recertify from last certification. Can have a default in grouper.properties if not set. (180?)
    - attestationLastEmailedDate (String)(on group only) yyyy/mm/dd date that this was last emailed so multiple emails dont go out on same day
    - attestationDaysBeforeToRemind (String) Integer number of days before attestation to start sending emails about it.
    - attestationStemScope (String) one|sub (for folders only, scope one level or all levels). Default to all levels.
    - attestationDateCertified (String) (on group only) yyyy/mm/dd is the last date certified for this group. (only for groups, not stems)

Future scope

  - If attestation is not done in a certain amount of time, disable the memberships or group somehow

See Also

Presentation from Duke on Paranoid IAM, page 20