

User Deletion

When user are no longer desired on the AIM-managed server, they fall under the user deletion flow described here.

Deletion criteria

They are considered no longer desired if they are present in the root space of the organization, but they're not on the list of users who are supposed to be provisioned. In a GS-managed server this will only happen if a user was first added to the directory (and provisioned), and then removed from it.

Potential issues

If a user who was never part of the directory finds themselves in the company space somehow, they will be subject to the user deletion flow as well. This should never happen, as GS will not ever invite them to the root space by itself. However, a user with Admin (PL 100) permissions could invite them to the root space manually, which would make GS consider them a deletion candidate -- despite them never being part of a the directory and not being managed by GS before that point.

Configuration

User deletion can happen either instantly, or delayed by a configurable "grace period". In practice, the instant deletion is implemented the exact same way as the delayed deletion, but with grace period set to 0 seconds. It's controlled by the `user_soft_delete_period` parameter in the config, and leaving it unset is the same as setting it to `"0s"`.

```
userProvisioner:
```

```
  # Optional. Configure to enable user deprovisioning. Disabled by default.
```

```
deprovisioning:
```

```
  enabled: false
```

```
# Optional. When users get removed from the directory their accounts will only be deactivated,  
# but their erasure will be delayed by the specified time period, allowing them to be reactivated in the  
meantime.  
# The format is <amount><unit>, with amount being numeric and unit being one of: [s, m, h, d], for seconds,  
minutes,  
# hours or days respectively (for example: "24h", "31d" etc.).  
# The specified period will be translated into seconds, so won't account for things like DST, leap seconds etc.  
# Users will be deleted *no sooner* than that, but may be removed a bit later, depending on other Advanced  
Identity Management operations.  
# By default set to 30 days.  
soft_delete_period: '30d'
```

Actions performed instantly

When a user is found to be undesirable, their Matrix account is deactivated, preventing them from logging in. They are not being removed from any rooms though, and their permissions and power levels stay the same. It's equivalent to using a deactivate user Synapse API (with `erase` set to `false`).

If a grace period is configured and the user gets added back to the directory before they get deleted completely, their account will get reactivated.

The user then gets put on the "grace period" list.

NOTE: Historically Advanced Identity Management would reset the password for the user to a random value, but modern versions will just lock the account.

Actions performed after the grace period

Once the grace period expires for a user, they get erased from the server. This is done under the hood by the Synapse API deactivate user, with `erase` set to `true`.

Revision #4

Created 15 May 2025 09:26:07 by Gaël Goinvic

Updated 27 May 2025 06:42:01 by Gaël Goinvic