Configuring Matrix Authentication Service

See how to download example files from the helm chart here.

Configuration

For a quick setup using the default settings, see the minimal fragment example in `charts/matrix-stack/ci/fragments/matrix-authentication-service-minimal.yaml`.

Using Element Web ingress

If Element Web is deployed, you can use the ingress host to access the Matrix Authentication Service. To do so, you can skip configuring `matrixAuthenticationService.ingress`. The chart will automatically expose the Matrix Authentication Service on the same ingress as Element Web, under the path `/account`.

Configuring a postgresql database

If you want to use an external postgresql database, merge 2 files to `postgresql.yaml`:

- `charts/matrix-stack/ci/fragments/matrix-authentication-service-postgres.yaml`
- `charts/matrix-stack/ci/fragments/matrix-authentication-service-postgres-secrets-in-helm.yaml` or `charts/matrix-stack/ci/fragments/matrix-authentication-service-postgres-secrets-externally.yaml`

Credentials

Credentials are generated if possible. Alternatively they can either be provided inline in the values with `value` or if you have an existing `Secret` in the cluster in the same namespace you can use `secret` and `secretKey` to reference it.

If you dont want the chart to generate the secret, please refer to the following values fragments examples to see the secrets to configure.

Matrix Authentication Service requires `encryptionSecret`, `synapseSharedSecret` and `synapseOIDCClientSecret` secrets:

- `charts/matrix-stack/ci/fragments/matrix-authentication-service-secrets-in-helm.yaml`
- `charts/matrix-stack/ci/fragments/matrix-authentication-service-secrets-externally.yaml`

If you are using LDAP Authentication, this will also need to configure `dex.masClientSecret`.

Additional configuration

Additional Matrix Authentication Service configuration can be provided inline in the values as a string with

```
matrixAuthenticationService:
  additional:
    ## Either reference config to inject by:
    1-custom-config:
      config: |
        admin_contact: "mailto:admin@example.com"
    ## Either reference an existing `Secret` by:
    2-custom-config:
      configSecret: custom-matrix-authentication-service-config
      configSecretKey: shared.yaml
```

Disabling Matrix Authentication Service

Matrix Authentication Service is enabled for deployment by default can be disabled with the following values

```
matrixAuthenticationService:
  enabled: false
```

Enable user registration

To allow users registration, you will need to configure MAS with SMTP. To do so, follow the steps in Configuring Matrix Authentication Service to inject additional email configuration.

Here is a sample minimal MAS configuration that allows user registration. You are encouraged to look through the MAS documentation linked above and customise the options to your requirements.

```
matrixAuthenticationService:
  additional:
    user-config.yaml:
      config: |
        email:
          from: '"Company Ink" <noreply@example.com>'
          reply_to: '"Company Ink" <noreply@example.com>'
          transport: smtp
          mode: starttls
          hostname: "smtp.example.com"
          port: 587
          username: smtpuser
          password: secretsmtppassword
        account:
          password_registration_enabled: true
          password_recovery_enabled: true
          account_deactivation_allowed: true
          login_with_email_allowed: true
        policy:
          data:
            emails:
              allowed_addresses:
                suffixes: ["@example.com"]
        rate_limiting:
          account_recovery:
            per_ip:
              burst: 3
              per_second: 0.0008
            per_address:
              burst: 3
              per_second: 0.0002
          login:
            per_ip:
              burst: 3
              per_second: 0.05
            per_account:
```

```
            burst: 1800
            per_second: 0.5
          registration:
            burst: 3
            per_second: 0.0008
```

Enable the MAS Admin API

To enable the MAS Admin API, you need to add some additional MAS configuration. There are two modes to use the Admin API. You can enable either one on its own or both as per your requirements. Note you will need to generate valid ULIDs for the client IDs below using a ULID generator like for example https://ulidgenerator.com/

1. Using the Swagger UI provided with MAS. An example is available on the MAS documentation page at https://element-hq.github.io/matrix-authentication-service/api/index.html. However, we encourage you to instead use the one hosted by your MAS instance at `https://your-mas-domain.tld/api/doc/`. `ULID_Admin_Client_1` in the below example enables authentication for graphical MAS clients like the Swagger UI.
2. Manually calling the API using a rest client, for example cURL or Bruno. This is documented in this example in the MAS documentation. This is `ULID_Admin_Client_2` in the below example.

> Ensure you protect the Client IDs and Secrets as these grant full access to manage all accounts on your server.

Example configuration:

```
matrixAuthenticationService:
  additional:
    user-config.yaml:
      config: |
        policy:
          data:
            admin_clients:
              - ULID_Admin_Client_1
              - ULID_Admin_Client_2
            admin_users:
              - your-admin-user
        clients:
          - client_id: ULID_Admin_Client_1
```

```
    client_auth_method: client_secret_post
    client_secret: A-secret
    redirect_uris:
      - https://account.example.com/api/doc/oauth2-callback
  - client_id: ULID_Admin_Client_2
    client_auth_method: client_secret_basic
    client_secret: Another-secret
```

Synapse Admin API

Access tokens returned by the above MAS Admin API configuration cannot be used with the Synapse Admin API. Long term, we plan to implement Personal Access Tokens in MAS. However, until that feature has landed, the only way to get an access token for the Synpse Admin API is using `mas-cli`.

```
kubectl exec --container matrix-authentication-service --namespace ess \
    --stdin --tty deploy/ess-matrix-authentication-service \
    -- mas-cli manage issue-compatibility-token \
    --yes-i-want-to-grant-synapse-admin-privileges \
    your-username
```

This will return a response similar to this

```
2025-05-21T11:11:53.564226Z  INFO mas_cli::commands::manage:320 Compatibility
token issued: mct_secret compat_access_token.id=ZI1UZZKCNWFOBFUUOQEYZBSIU8
compat_session.id=9X1BFZGXOYXGG5MDHPODT3ER6Q compat_session.device=MI71UWHZLG
user.id=QZEMHAYQCYXS8AYYQ3QWTRMNJZ user.username=your-username
```

In this example, `mct_secret` is your admin access token.

> Ensure you protect the access token as this grants full access to manage your server.

Revision #15
Created 2025-05-21 10:35:59 UTC by Gaël Goinvic
Updated 2025-05-28 11:52:16 UTC by Gaël Goinvic