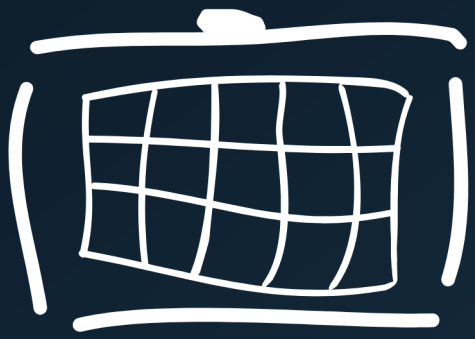


Radiator

CONFIGURATION GUIDE

EAP TLS Entra ID configuration guide

Date: 2026-11-16

Important notice

Before proceeding with this configuration guide, you must first complete the Microsoft Entra ID application creation process. This includes creating an app registration, configuring API permissions, generating client secrets, and handling the MFA exclusion.

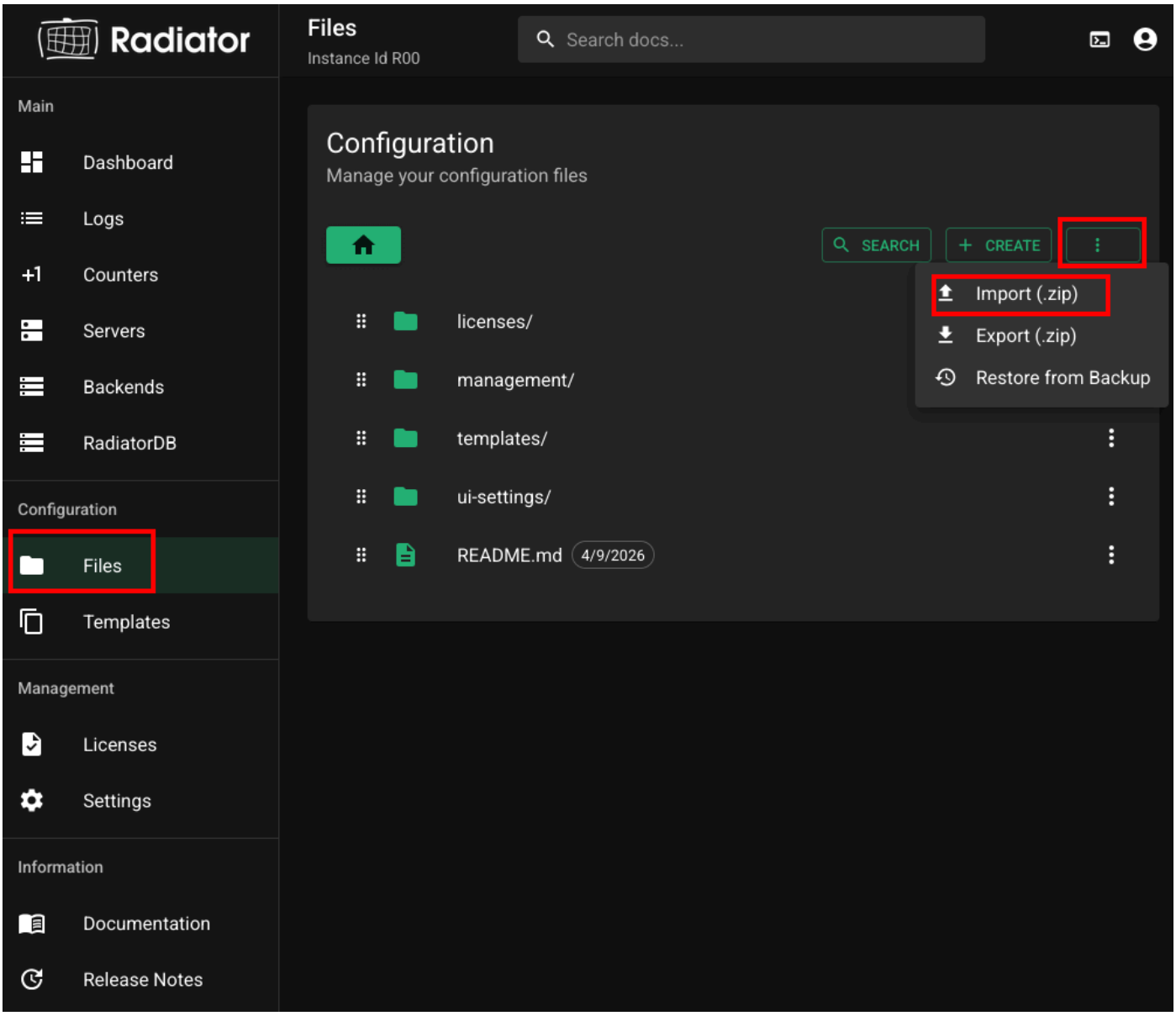
Please refer to the Microsoft Entra ID App creation for Radiator Policy Server authentication before continuing.

Example configuration setup

Radiator offers various Entra ID example configurations that demonstrate authentication with Microsoft Entra ID and optionally MFA support in the public radiator-radconfs repository.

A good starting point is the `eap-tls-entra-authz` configuration, which shows how to configure Microsoft Entra ID groups as an authorisation backend for EAP-TLS authentication.

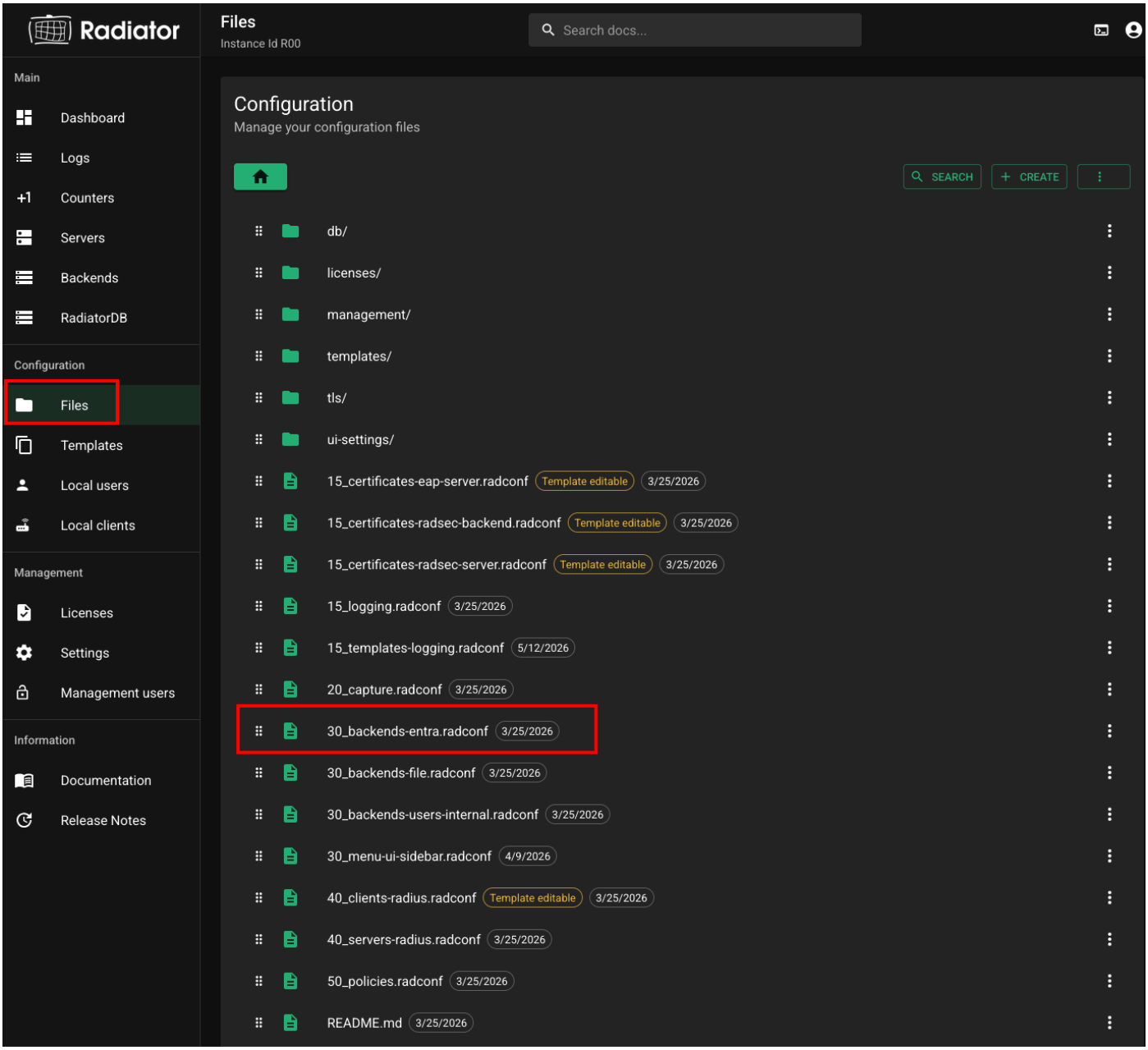
To get a working configuration, download the configuration zip from the radiator-radconfs repository and import it from the GUI by selecting **Files** > **Import (.zip)**



Please note that the imported configuration contains placeholder values that must be replaced with your actual Entra ID application information (covered in the following sections).

Updating the example configuration

After completing the previous steps as well as the Microsoft Entra ID App creation for Radiator Policy Server authentication guide, you will need to modify the example configuration from the first step to match your specific Entra ID application details. Start by locating `30_backends-entra.conf` in the GUI under **Files**

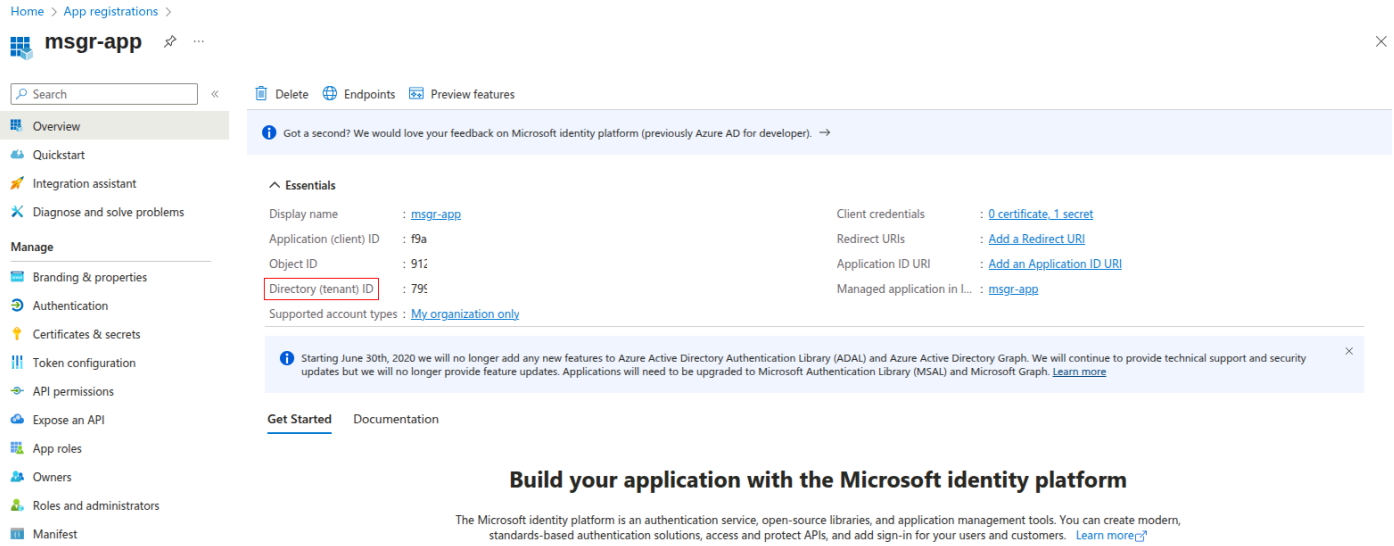


In `30_backends-entra.conf`, locate the http backend named "MS_CLIENT_CREDENTIALS" and navigate to the `authentication oauth2` block which looks something like this:

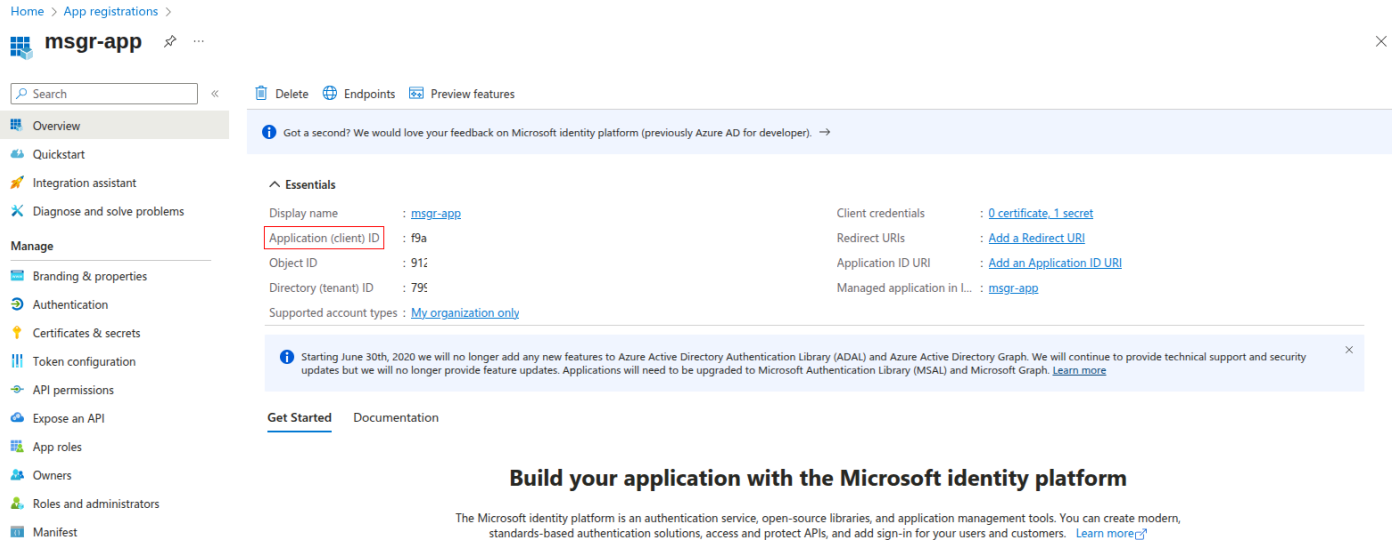
```
authentication oauth2 {
    token_url "https://login.microsoftonline.com/<Directory (tenant) ID>/oauth2/v2.0/token";
    client "<Application (client) ID>";
    secret "<Application secret>";
    # Entra ID client credentials flow scope is always this
    scope "https://graph.microsoft.com/.default";
}
```

In the authentication block, update the following values:

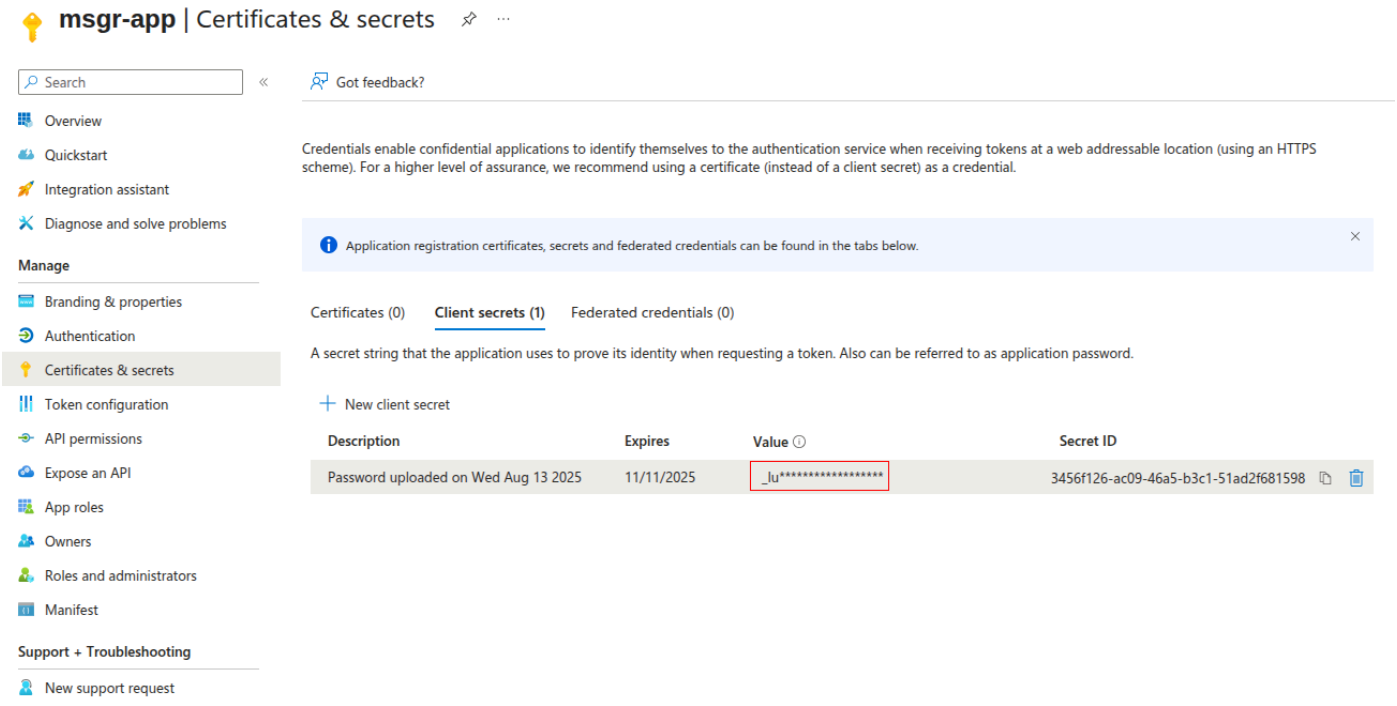
1. In token_url, replace `<Directory (tenant) ID>` with the Directory (tenant) ID. The Directory (tenant) ID is shown on the application Overview page:



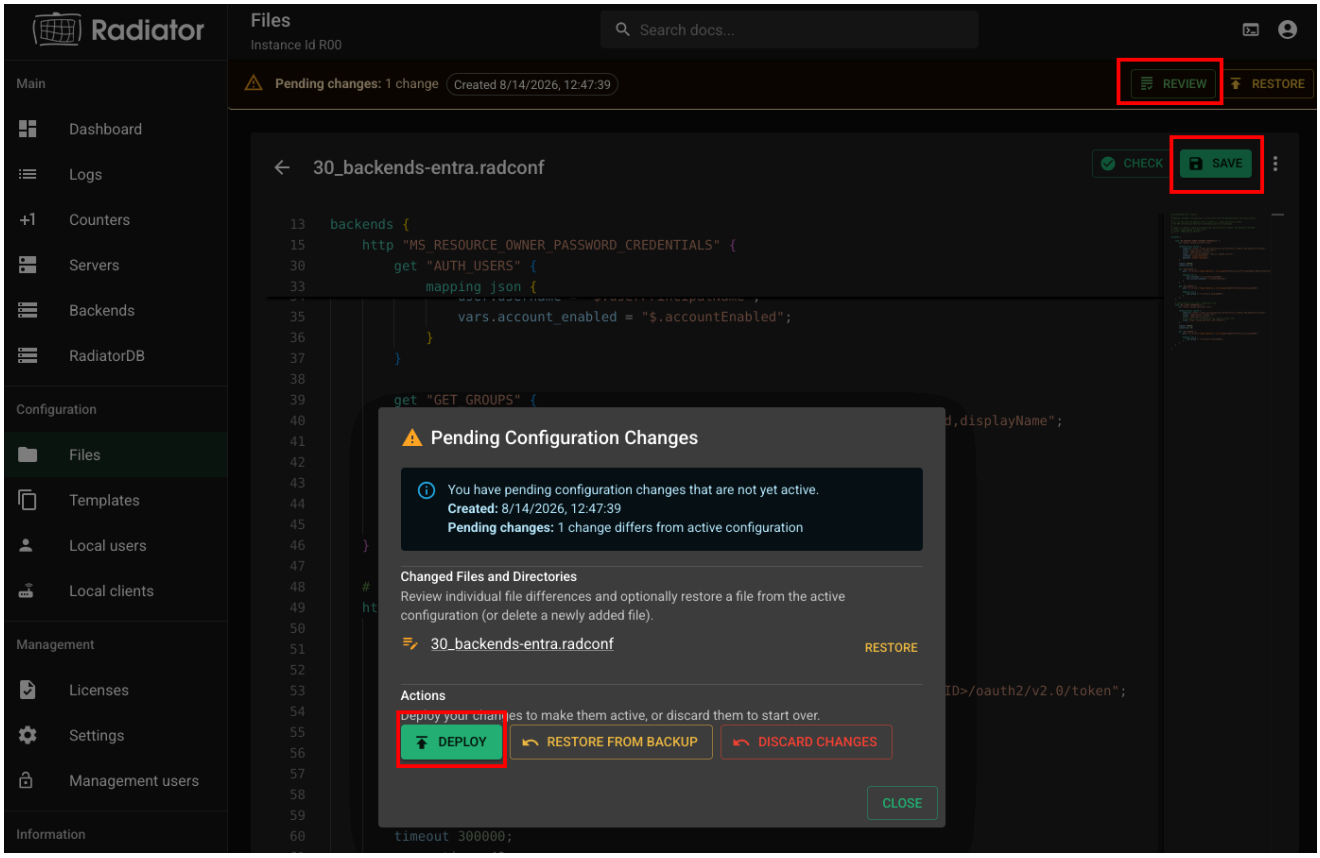
2. In client, replace `<Application (client) ID>` with the Application (client) ID. The Application (client) ID is shown on the application Overview page:



3. In secret, replace `<Application secret>` with the secret. The secret is shown on the application Certificates & secrets page right after creation:



4. Save the configuration file by selecting **Save**.
5. Deploy the changes by selecting **Review** > **Deploy** > **Deploy**



When making changes in the GUI, new configuration is automatically taken into use.

Testing

You can test the Entra ID authorisation using the eapol_test test client. The `eap-tls-entra-authz` configuration does EAP-TLS authentication with a certificate first, and then uses the emailAddress from the certificate with Microsoft Entra ID to determine which groups the user belongs to. Example eapol_test configurations are available in

`/opt/radiator/server/testutils/` and example certificates in `/var/lib/radiator/tls/`. Certificate files can also be viewed in the GUI in `tls` directory under the **Files** section.

eapol_test command for testing:

```
/opt/radiator/server/bin/eapol_test -s mysecret -c <eapol-test-configuration>
```

Note: Replace `mysecret` with your configured RADIUS client secret.