Realms API

Reference

Table of Contents

API Objective: Authenticate across different systems.

Realms are used to authenticate users across several different user access control systems.

There are seven realm types currently supported:

- Native, which uses Fusion itself to manage users and passwords.
- LDAP, which uses an LDAP server as the source of truth for usernames and passwords.
- Kerberos, where Fusion can be configured to use Kerberos for authentication.
- SAML, which uses the SAML 2.0 protocol to provide single sign-on.
- SSO Trusted HTTP, which can be configured to return a list of group names, and then map the groups to Fusion roles in the security realm definition.
- JSON Web Token (JWT), where you can configure Fusion to use a shared secret key to encrypt the JWT payload.
- OpenID Connect, which is an identity authorization layer that supplements the OAuth 2.0 protocol.

See Security Realms for more information about each realm type.

Authenticating users with an LDAP system creates a user record in Fusion, which includes a property for the realm the user belongs to. This Fusion user record is used by administrators to grant users access permissions for the UI or REST API services.

Create, Update, Delete or List Realms

The path for this request is:

```
/api/realm-configs/<id>
```

A GET request returns the configured realms. If ID is omitted, all realms will be returned.

A POST request creates a new realm. If the request is successful, a new ID will be generated.

A PUT request updates a realm.

A DELETE request removes the realm.

Input

Parameter	Description
name *Required*	The name of the realm. This name will appear on the login screen of the UI, and will appear in user records to identify the realm they belong to.
realmType *Required*	String value for realm type.
enabled *Required*	If **true**, the realm is available for users to use with system authentication.
ephemeralUsers	Prevents ephemeral users from being created in ZooKeeper during login. Enabling this property negates `config.autoCreateUsers`.
config.autoCreateUsers	Enables/disables the auto-creation of Fusion user accounts after users successfully authenticate for the first time.
roleNames	Indicates which roles are dynamically applied to users in the realm.

ADDITONAL PROPERTIES PER REALM TYPE

Each realm type requires additional properties for configuration, which should be specified within the `config` object field.

See the following documentation for each realm type:

- **Native**: Native is a preconfigured security realm and Fusion manages all authentication and permissions information directly.
- **LDAP**: Configure Fusion 5.x for LDAP
- **Kerberos**: Configure Fusion for Kerberos in Unix, Configure Fusion for Kerberos in Windows
- **SAML**: Configure Fusion for SAML
- **SSO Trusted HTTP**: Configure Fusion for SSO
- **JWT**: Configure Fusion for JWT

When creating a new realm, the output will include the properties for the realm just created, or an error to indicate a problem with the entry.

For a GET request, the output will include all defined properties of the realm.

For a DELETE or a PUT request, no output will be returned.

Examples

Get details of the default 'native' realm:

REQUEST

```
curl -u user:pass http://fusion-host:6764/api/realm-configs/86df9b5b-4a1c-4b0b-bc10-25aee55fef63
```

Copy

RESPONSE

```
{
    "enabled": true,
    "id": "86df9b5b-4a1c-4b0b-bc10-25aee55fef63",
    "name": "native",
    "realmType": "native"
}
```

Copy

Create a realm to support LDAP authentication:

REQUEST

```
curl -u user:pass -X POST -H 'Content-type: application/json' -d '{
    "realmType": "ldap",
    "name": "dev-ldap3",
    "enabled": true,
    "roleNames": ["developer","admin"],
    "config": {
```

🔍 [   ] ⌄

```
        "ephemeralUsers": false,
        "login": {
            "bindDnTemplate": "uid={},ou=users,dc=security,dc=example,dc=com"
        }
    }
}' http://fusion-host:6764/api/realm-configs
```

Copy

RESPONSE

```
{
    "realmType": "ldap",
    "id": "fd90a918-1e5c-4f27-952c-fd81a068ee85",
    "name": "dev-ldap3",
    "enabled": true,
    "createdAt": "2021-07-28T15:15:04Z",
    "config": {
        "autoCreateUsers": true,
        "host": "fusion-host",
        "ssl": true,
        "port": 10636,
        "ephemeralUsers": false,
        "login": {
            "bindDnTemplate": "uid={},ou=users,dc=security,dc=example,dc=com"
        }
    },
    "roleNames": [
        "developer",
        "admin"
    ]
}
```

Copy

API specification

Fusion Proxy API 5.4.0

api-controller

Basic system and user status information

o-auth-2-controller

Fusion OAuth2 endpoint

realm-controller

Realms' management

GET	/api/realm-configs	Obtain multiple realms

POST	/api/realm-configs	Create Realm

role-controller

Roles' management

suggestion-controller

Suggestion endpoint

user-controller

Fusion's Users management