

PART 2 API

Users

GET /user	Procure an authentication of User.
POST /user	Show user.
GET /user/:user	Procure his id.
PUT /user/:user	Add other users.
GET /user/:user/exists	Deconnect user.
POST /user/:user/authenticate	Show all authentication of users.
PUT /user/:user/password	Edit password.
PUT /user/:user/password-never-expires	The password never expire.
PUT /user/:user/password-expires	Add one password expire.
GET /user/:user/member-of/:group	Deconnect the group.
DELETE /user/:user	Delete a user.

:user is one example but you can put « /user/:Thomas » or other things.

Groups

GET /group	Procure an authentication of group.
POST /group	Show the group.
GET /group/:group	Procure its id.
GET /group/:group/exists	Deconnect the group.
POST /group/:group/user/:user	Show all user in the group.
DELETE /group/:group/user/:user	Delete user who's part of the group.
DELETE /group/:group	Delete the group.

:Projetfilrouge is one example but you can put « /user/:Projetfilrouge » or other things will be create.

Organizational Units

GET /ou	Procure an authentication of OU.
POST /ou	Show the OU.
GET /ou/:ou	Procure OU's ID.
GET /ou/:ou/exists	Deconnect OU who is part of the OU.
DELETE /ou/:ou	Delete the OU specific.

Difference between LDAP and LDAPS

LDAP : Lightweight Directory Access Protocol

LDAPS : Lightweight Directory Access Protocol Security

You will need to configure the domain controller as the Certificate Authority by setting up the Active Directory Certificate Services role.

If you connect to Active Directory via LDAP, it will refuse some write operations, including adding a user and changing a password.

And Windows Server doesn't support LDAPS out of the box.