

Configure FreeIPA LDAP User Authentication for PE and Foreman

- . First create a 'LookUp' FreeIPA account called '**ldapread**' (or it can be any name).
- . Do NOT assign this account to any user group so that if HostBasedAccessControl is setup it will not have any SSH connection policy to any server.
- . For PE: **Admin / Access Control / LDAP**

The screenshot shows the 'Access control' page in Puppet Enterprise. The 'LDAP' tab is selected. The 'Directory name' is 'ipa.example.local'. The 'Connection information' section shows 'Hostname' as 'ipa.example.local', 'Port' as '389', 'Lookup user' as 'ldapread', and 'Lookup password' as 'ldapread'. The 'Attribute mappings' section shows 'User login attribute' as 'uid', 'User email address field' as 'mail', 'User full name' as 'cn', 'Querying users' as 'cn=users,cn=accounts,dc=dev,dc=example,dc=local', 'User relative distinguished name' as 'cn=users', 'Querying groups' as 'cn=groups,cn=accounts,dc=dev,dc=example,dc=local', 'Group object class' as 'groupofnames', 'Group membership field' as 'member', 'Group name attribute' as 'cn', 'Group lookup attribute' as 'cn', 'Group relative distinguished name' as 'cn=groups', and 'Turn off LDAP_MATCHING_RULE_IN_CHAIN?' as 'no'. The 'Search nested groups?' checkbox is checked.

- . For Foreman: **Administer / Authentication Source**

1st tab: LDAP Server

Name: **FreeIPA**

Server: **ipa.example.local**

LDAPS: **unchecked**

Port: **389**

Server type: **FreeIPA**

The screenshot shows the 'Authentication Sources' page in Foreman. The 'LDAP server' tab is selected. The 'Name' is 'FreeIPA', 'Server' is 'ipa.example.local', 'LDAPS' is unchecked, 'Port' is '389', and 'Server type' is 'FreeIPA'. A 'Test Connection' button is visible.

2nd tab: Account

Account Username: **uid=ldapread,cn=users,cn=accounts,dc=dev,dc=example,dc=local**

Account Password: *********

Base DN: **cn=users,cn=accounts,dc=dev,dc=example,dc=local**

Group base DN: **cn=groups,cn=accounts,dc=dev,dc=example,dc=local**

Automatically Create Accounts in Foreman: **checked**

Usergroup Sync: **checked**

The screenshot shows the 'Account' tab in the 'Authentication Sources' page. The 'Account Username' is 'uid=ldapread,cn=users,cn=accounts,dc=dev,dc=example,dc=local', 'Account Password' is '*****', 'Base DN' is 'cn=users,cn=accounts,dc=dev,dc=example,dc=local', 'Groups base DN' is 'cn=groups,cn=accounts,dc=dev,dc=example,dc=local', 'Use Netgroups' is unchecked, 'LDAP filter' is empty, 'Automatically Create Accounts in Foreman' is checked, and 'Usergroup Sync' is checked.

3rd tab: Attribute mappings: take defaults for all fields.

4th tab: Location – **local**

5th tab: Organization - **example**

Back to 1st tab click **Test Connection**, if it is successful click **Submit** to save all tabs.

LDAP Authentication has now been complete, there are two methods to add FreeIPA accounts into PE or Foreman.

The 1st method is obviously preferred.

. 1st method: Admin to 'Pre-Add' the FreeIPA account(s), and grant the appropriate role(s).

For PE: **unfortunately there is no 'Pre-Add' option for 'External' (LDAP) user(s), it is only available for local users.**

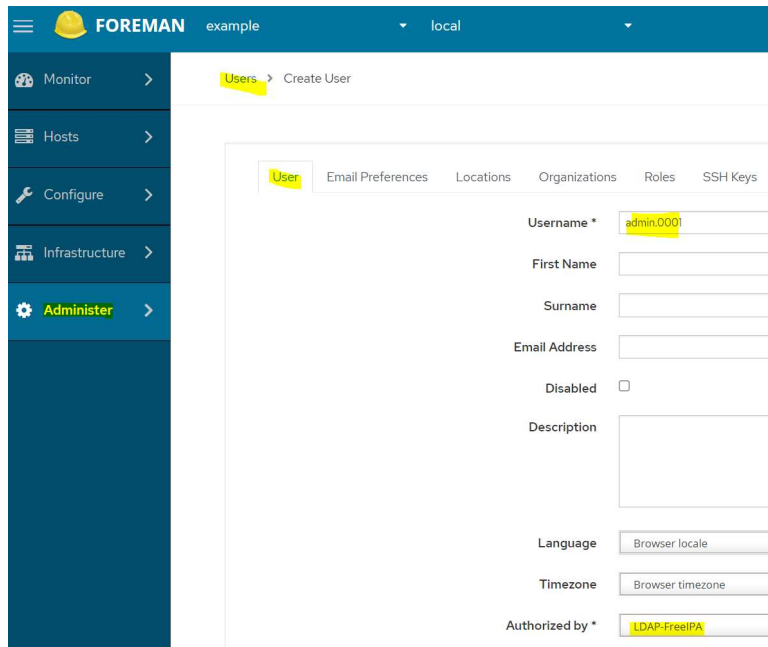
For Foreman: example add **admin.0001**

Note: there is no need to fill-in First Name, Surname and Email Address, as these will be populated when user logs in.

User tab:

Username: **admin.0001**

Authorized by: **LDAP FreeIPA**



The screenshot shows the Foreman Admin interface. On the left is a sidebar with navigation links: Monitor, Hosts, Configure, Infrastructure, and Administer (highlighted). The main content area is titled 'Create User' under the 'Users' section. There are tabs for 'User', 'Email Preferences', 'Locations', 'Organizations', 'Roles', and 'SSH Keys'. The 'User' tab is active, showing a form with the following fields: Username * (filled with 'admin.0001'), First Name, Surname, Email Address, Disabled (checkbox), Description, Language (dropdown with 'Browser locale'), Timezone (dropdown with 'Browser timezone'), and Authorized by * (dropdown with 'LDAP-FreeIPA').

Roles tab:

Administrator: **Checked** (if so there is no need to select individual role)

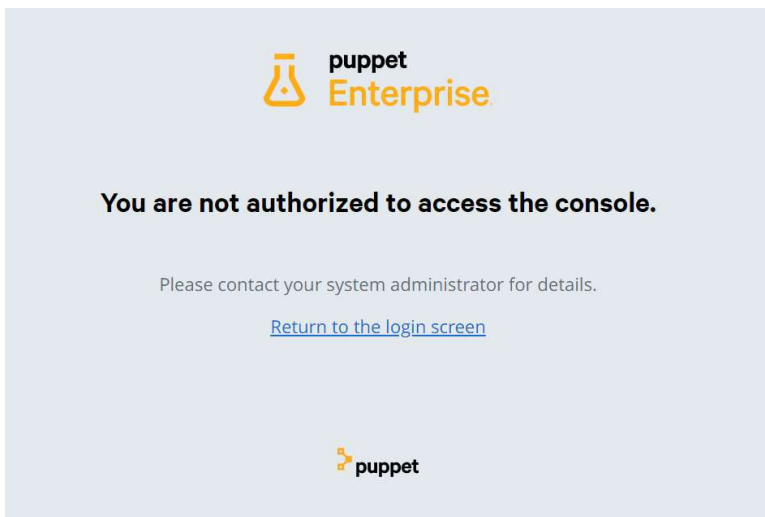
Click 'Submit'.

. 2nd Method: user to perform First Time Login using FreeIPA account, it will display the following screen, do NOT be alarmed.

. What this means the FreeIPA account has been created however the appropriate role(s) has/have not been assigned.

. User should then request PE / Foreman Admin to assign such roles so that subsequent login will be fine.

For PE: example 1st time login admin.0001 at PE GUI



PE Admin can check the AUTO-creation of account, example: admin.0001, and grant example: Admin role via Admin / Access Control / User Roles / Member users

For Foreman: example 1st time login admin.0001 at Foreman GUI.



Permission denied

You are not authorized to perform this action.

Please request one of the required permissions listed below from a Foreman administrator:

edit_authenticators

[Back](#)

Foreman Admin cat check the AUTO-creation of account, example admin.0001 and grant Admin role via Edit User.
Subsequent login by admin.0001 to PE or Foreman GUI will be fine.