

Integrate Windows AD on RHEL 8 using SSSD

474 Manu Chacko February 9, 2024 [Features & Functionalities](#) 6021

How can I integrate Windows AD on RHEL 8 using SSSD?

Ensure that the following ports on the RHEL host are open and accessible to the AD domain controllers.

DNS =53, LDAP =389, Kerberos 88 & 464, LDAP Global Catalog 3268,LDAPS 636 and NTP 123 (UDP)

Verify that the system time on both systems is synchronized. This ensures that Kerberos is able to work correctly.

Refer article to [correct server time in Centos, RHEL, Ubuntu, SUSE](#)

1. Login to Ezeelogin Web-GUI > open settings > Ldap

[How to find base DN and bind RDN](#)

Add the details of LDAP configurations.

The screenshot shows the Ezeelogin web interface. On the left is a red sidebar menu with options: Servers, Web Portals, Users, Access Control, Settings (selected), Cluster, Command Guard, Account, Help, and License. The 'Settings' menu is expanded, showing sub-options: General, Branding, Control Panels, Data Centers, API, LDAP (selected), SAML, RADIUS, and Server Fields. The main content area is titled 'LDAP Settings' and contains the following fields and controls:

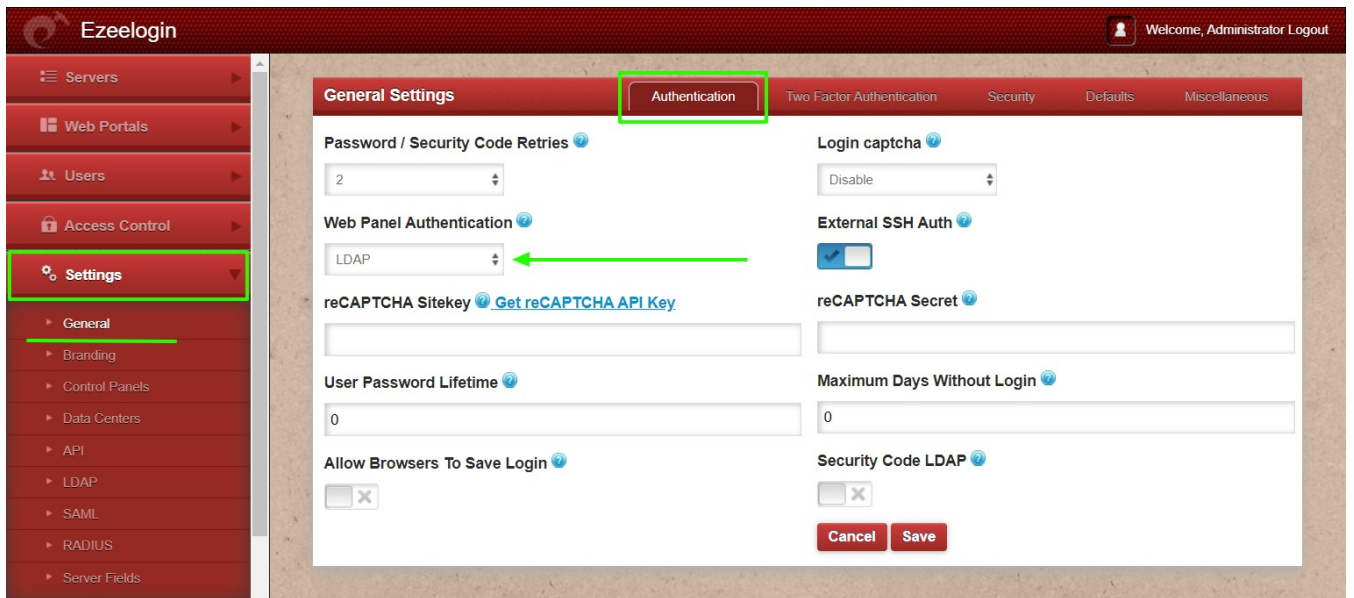
- Name:** ezad
- URI(s):** ldap://ezad.com
- Start TLS:** ☐
- Bind RDN:** CN=Administrator,CN=Users,DC=ezad,DC=com
- UID Attribute:** sAMAccountName
- First Name Attribute:** givenName
- Email Attribute:** mail
- Timeout:** 10
- Active:** ☒
- Verify Certificate:** ☐
- Base DN:** CN=Users,DC=ezad,DC=com
- Bind Password:** [masked with dots]
- Filter:** [empty]
- Last Name Attribute:** sn
- Group Attribute:** [empty]
- Rank:** 10
- Windows Active Directory:** ☒

At the bottom right of the form are 'Cancel' and 'Save' buttons. The footer of the sidebar says 'Powered by ezeelogin.com'.

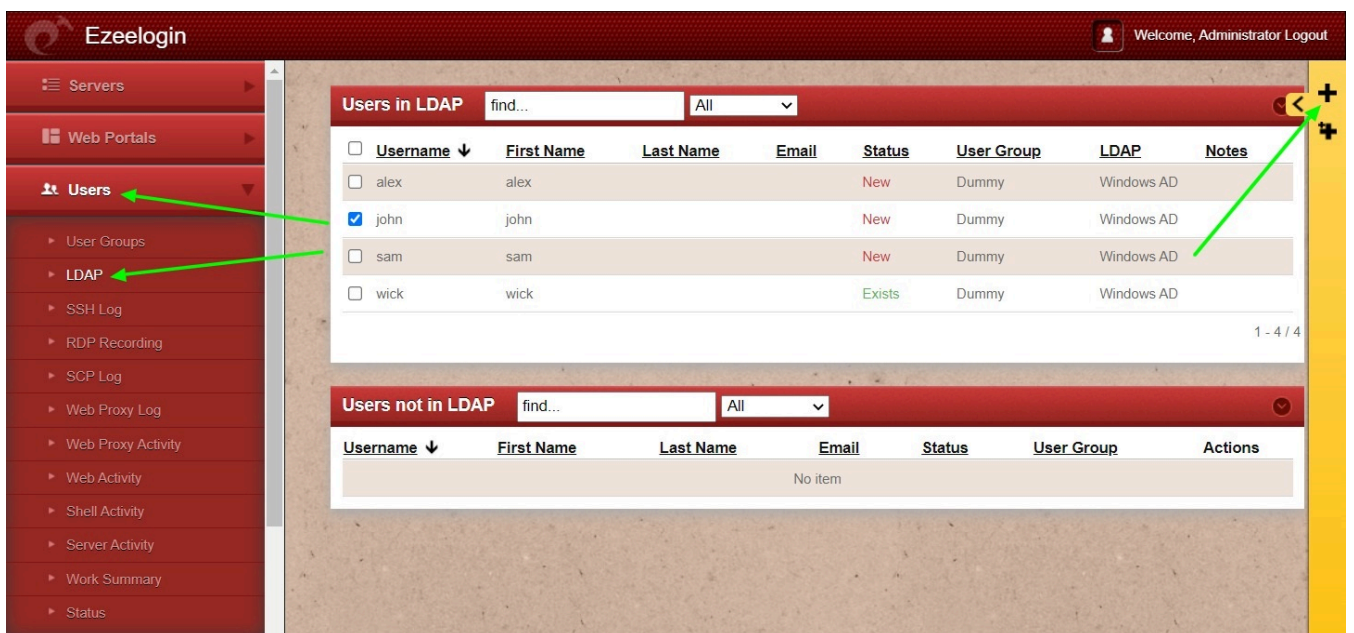
Verify Certificate feature is only available from **Ezeelogin version 7.35.0**.

Refer [article to upgrade Ezeelogin to the latest version](#).

2. Go to **Settings > General > Authentication** > change Web panel Authentication to LDAP

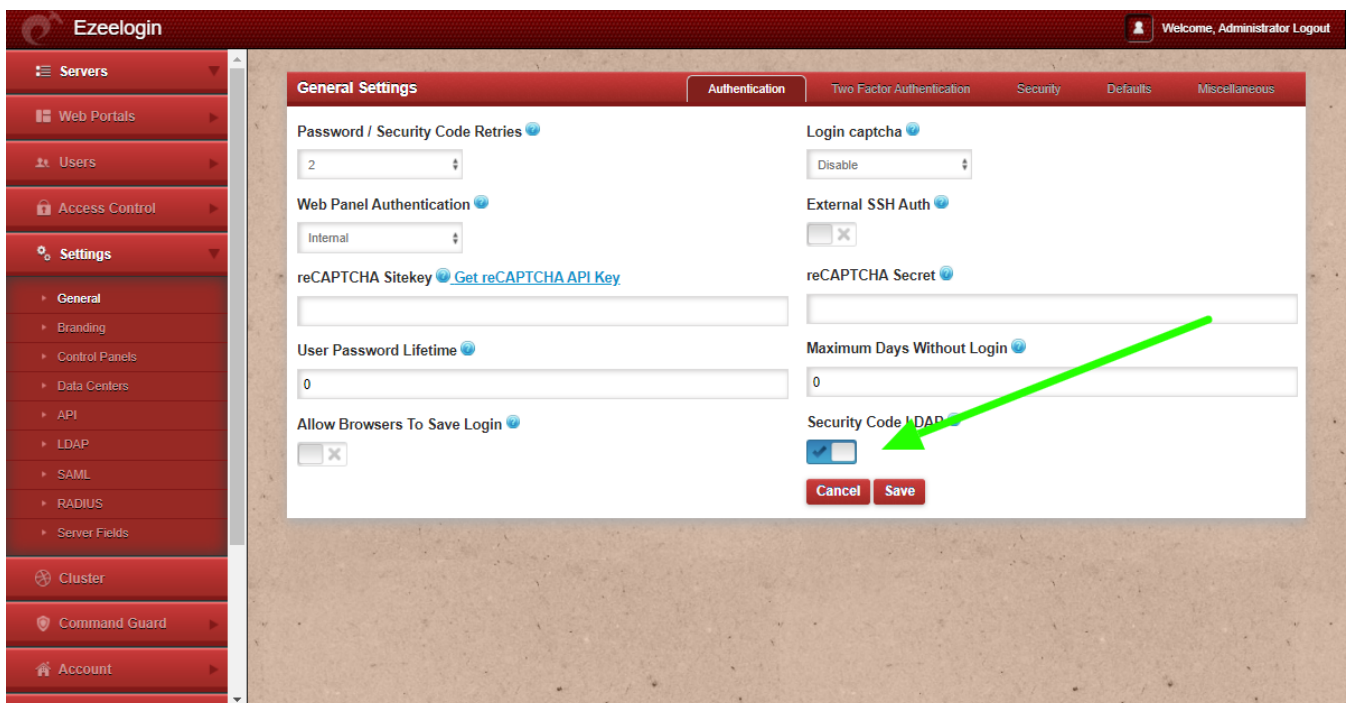


3. Select the LDAP users and click on the button to import users into Ezeelogin



You can confirm the imported LDAP users were listed in the Users tab in Ezeelogin GUI. You will be able to log in to Ezeelogin GUI with windows user credentials.

4. Enable Security code LDAP option from Settings > General > Authentication, if the user does not want to login to Ezeelogin GUI to set up a security code.



Backend configuration to integrate Windows with RHEL 8

1. Install the following packages:



Ensure that you are using the AD domain controller server for DNS.

2. Add the following to /etc/hosts file

```
root@gateway ~]# vi /etc/hosts

WindowsAD_server_ip windowsAD_domainname.com
windowsAD_domainname
```

3. Add in windows server IP /etc/resolv.conf to resolve and discover AD domain.

```
root@gateway ~]# vi /etc/resolv.conf

nameserver windows_ip
```

4. To display information for a specific domain, run realm discover and add the name of the domain you want to discover.

5. Configure RHEL with the Active Directory domain by the following command. Replace Administrator with Windows admin account.

```
root@gateway ~]# realm join ezad.com -U Administrator  
  
Password for Administrator :
```

6. You can verify by displaying AD user details, such as the administrator user:

7. After successful join, edit /etc/sss/sss.conf and change use_fully_qualified_names to **False** and append the following **override_shell = /usr/local/bin/ezsh**

```

root@gateway ~]# vim /etc/sss/sss.conf

[sss]
domains = ezad.com
config_file_version = 2
services = nss, pam

[domain/ezad.com]
ad_domain = ezad.com
krb5_realm = EZAD.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
  override_shell = /usr/local/bin/ezsh

```

8 . Restart sssd and nscd using the below commands.

```

root@gateway ~]# _____

```

9. Run `id username` / `getent passwd username` and see AD user details.

```

root@gateway ~]# id iohn
uid=170160110 0 8 (john) gid=1701600513(domain users) groups=1701600513(domain users)
root@gateway ~]# getent passwd iohn
john:*:170160110 8 :1701600513:john user:/home/john@ldap.ad.com:/usr/local/bin/ezsh

```

Now you will be able to log in with Windows AD credentials

```
john@johnpc:~$ ssh john@gateway-IP
```

```
Last login: Mon Jan 24 04:55:03 2022 from 123.43.233.223
```

```
root@gateway ~]#
```

Related Information

[Integrate Windows AD with Centos 8 using SSSD](#)

[Integrate OpenLdap with Centos 8 using SSSD](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-windows-ad-on-rhel-8-using-sssd-474.html>