Integrate Windows AD on RHEL 8 using SSSD

474 Manu Chacko March 27, 2025 Features & Functionalities 15360

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

Overview: This article provides a step-by-step guide to integrating Windows Active Directory (AD) with RHEL 8 using SSSD, covering package installation, domain configuration, user verification, and enabling AD authentication in Ezeelogin.

Note:

1. 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)

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

Refer to the article: correct server time in Centos, RHEL, Ubuntu, SUSE

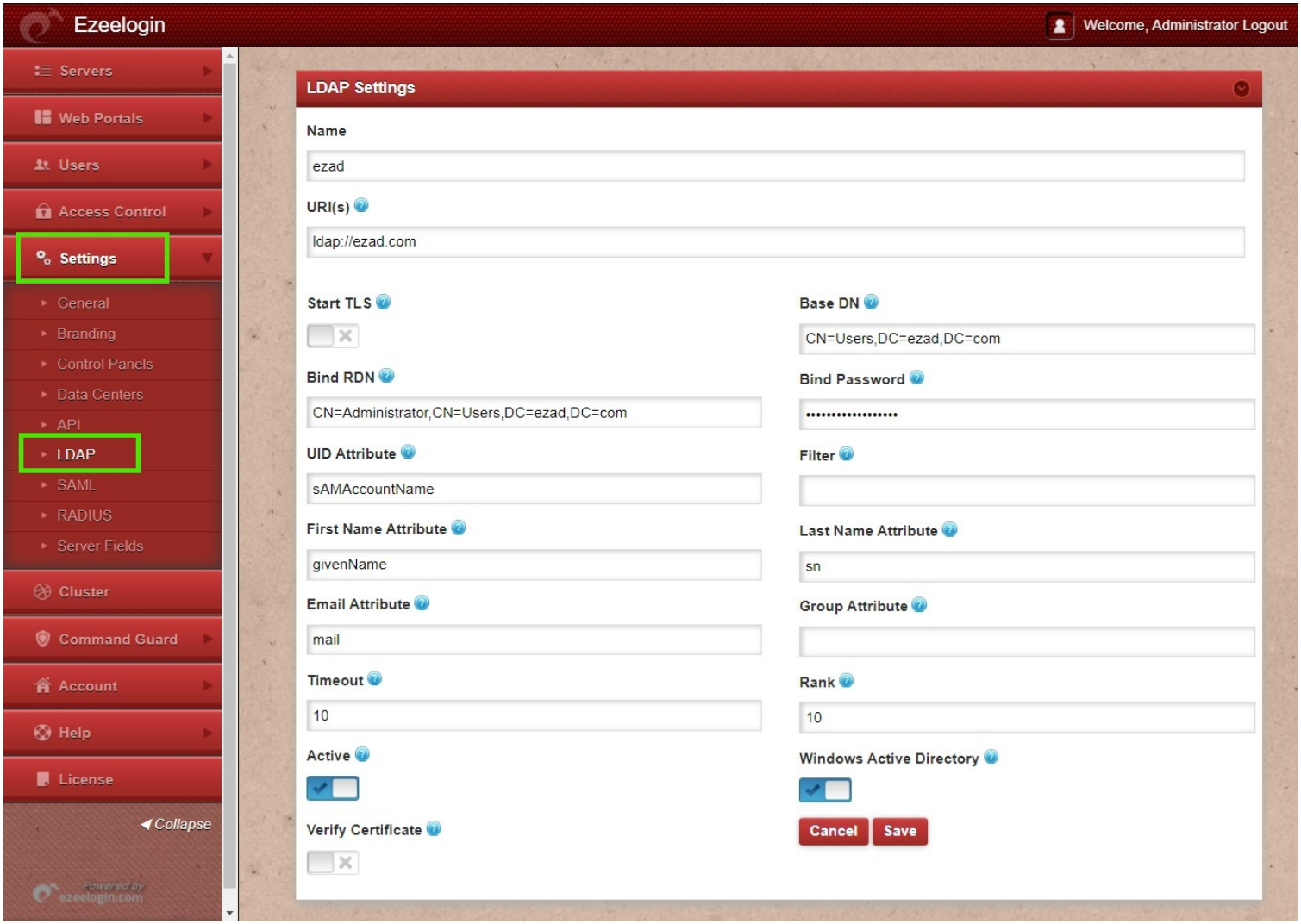
Step 1. Login to Ezeelogin Web-GUI -> open settings -> Ldap. Refer the article **How to find base DN and bind RDN**

Add the details of LDAP configurations.

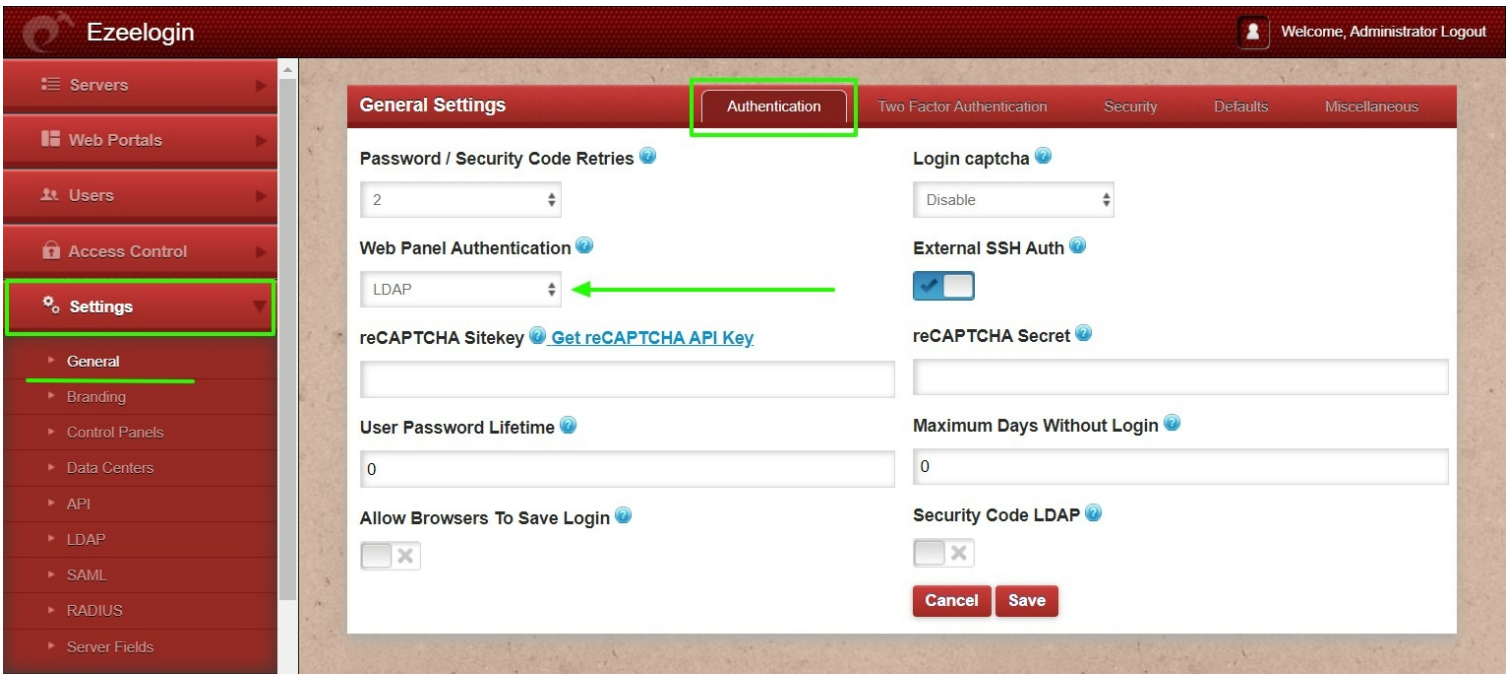
Multiple URIs or a list of URIs can be specified in the format:

- ldaps://host.com:636/ ldaps://host.com:636/

(Only the protocol, hostname, and port fields are allowed.)



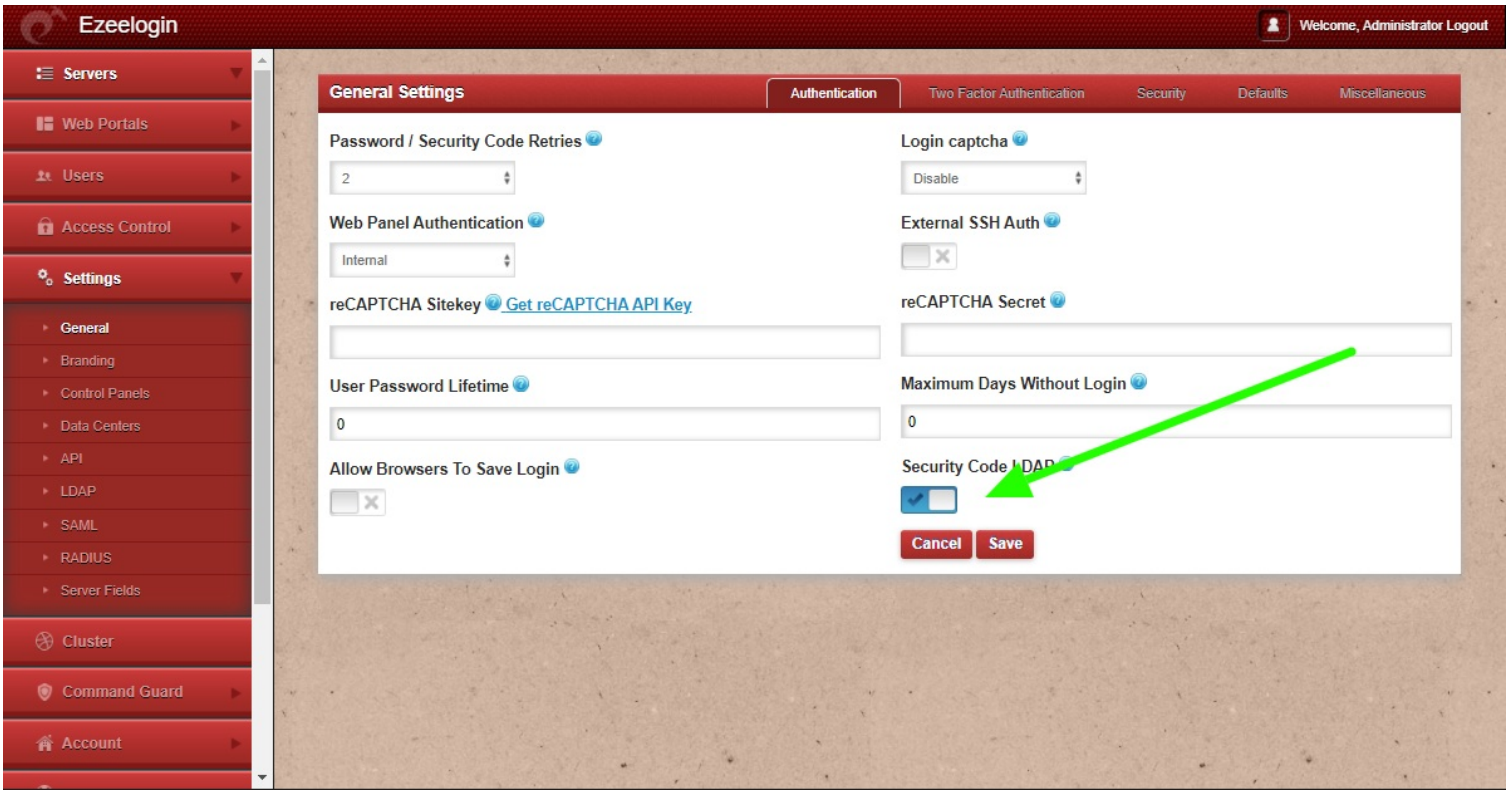
Step 2. Go to **Settings** -> **General** -> **Authentication** -> change Web panel Authentication to LDAP



Step 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.

Step 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

Step 1. Install the following packages:

```
yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation nscd
```

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

Step 2. Add the following to /etc/hosts file

```
vi /etc/hosts

WindowsAD_server_ip  windowsAD_domainname.com windowsAD_domainname
```

Step 3. Add in windows server IP /etc/resolv.conf to resolve and disc over AD do main.

```
vi /etc/resolv.conf

nameserver  windows_ip
```

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

```
realm discover ezad.com

ezad.com
type: kerberos
realm-name: EZAD.COM
domain-name: ezad.com
configured: no
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
```

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

```
realm join ezad.com -U  Administrator

Password for  Administrator :
```

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

```
getent passwd administrator@ezad.com

administrator@ezad.com:*:644600500:644600513:Administrator:/home/administrator@ezad.com:/bin/bash
```

Step 7. After successful join, edit /etc/sssd/sssd.conf and change use_fully_qualified_names **to False** and append the following **override_shell**

=/usr/local/bin/ezsh

```
vim /etc/sssd/sssd.conf

[sssd]
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
```

Step 8. Restart sssd and nscd using the below commands.

```
service sssd restart && service nscd restart
```

Step 9. Run id username /getent passwd username and s ee AD user de tails.

```
id john
uid=17016011 0 8 (john) gid=1701600513(domain users) groups=1701600513(domain users)

getent passwd john
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

```
tom@localhost :~$ ssh john@gateway-IP

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

root@gateway ~]#
```

Note: Verify Certificate feature is only available from Ezeelogin version 7.35.0.

Refer **article to upgrade Ezeelogin to the latest version**.

Related Articles:

Integrate Windows AD with Centos 8 using SSSD
Integrate OpenLdap with Centos 8 using SSSD

Integrate Windows AD with Ubuntu using SSSD