## Integrate Windows AD with CentOS using SSSD

430 Nesvin KN March 27, 2025 Productivity & Efficiency Features 7555

## How to integrate Windows AD with Centos 8 using SSSD

**Overview:** This article provides a comprehensive guide on integrating Windows AD with Ezeelogin and RHEL 8, covering steps for LDAP configuration, authentication setup, and backend integration.

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 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

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

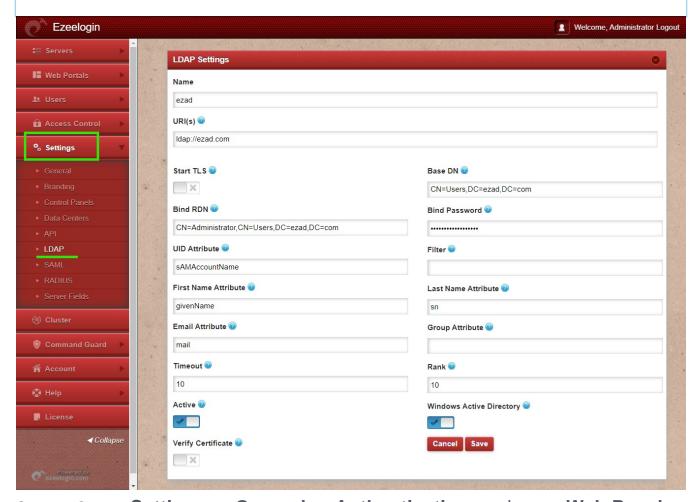
How to find base DN and bind RDN

Add the details of LDAP configurations.

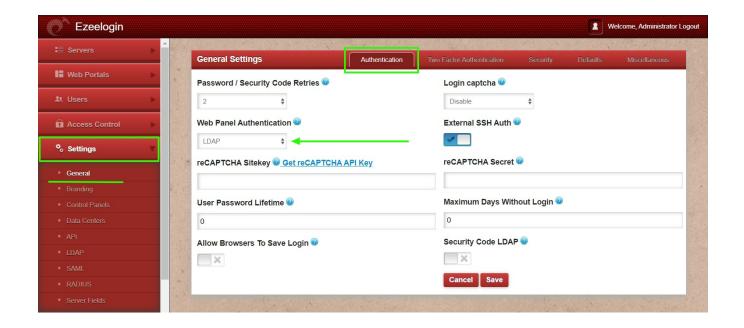
Multiple URIs or a list of URIs can be specified in the format:

• Idaps://host.com:636/ Idaps://host.com:636/

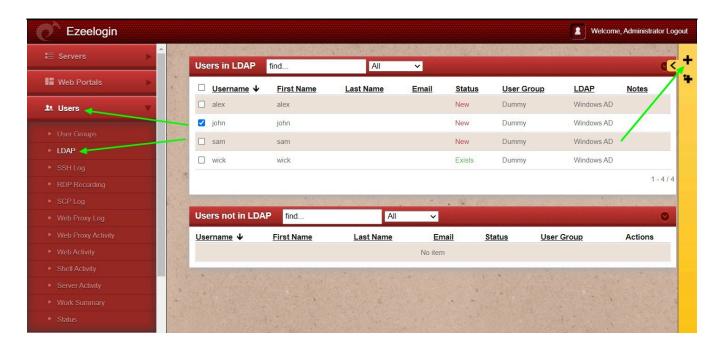
(Only the protocol, hostname, and port fields are allowed.)



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

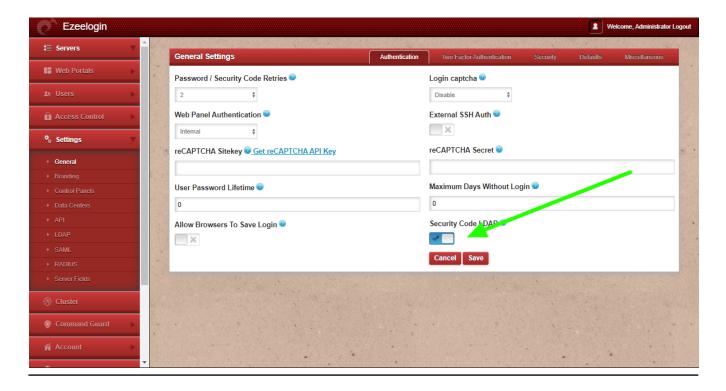


Step 3. Select the LDAP users and click on the button to import users into Ezeelogin



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 required packages.

root@gateway ~]# yum install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation authselect-compat nscd -y

## Step 2. Provide Windows IP and Windows domain name in hosts file.

```
root@gateway ~]# vim /etc/hosts
windows_ip windows_domain_name
```

Step 3. Provide Windows IP in resolv.conf to resolve and discover AD domain.

```
root@gateway ~]# vim /etc/resolv.conf
nameserver windows_ip
```

Step 4. Check if AD domain discovery is successful. Refer below example with Idapad.com

root@gateway ~]# realm discover ldapad.com

ldapad.com type: kerberos

realm-name: LDAPAD.COM domain-name: ldapad.com configured: kerberos-member 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

login-formats: %U@ldapad.com login-policy: allow-realm-logins

# **Step 5.** Join CentOS 8 in Active Directory domain. Replace Admininstrator with Windows admin account.

root@gateway ~]# realm join ldapad.com -U Administrator

Password for Administrator:

#### Step 6. Confirm joining successful with realm list. Refer below example.

root@gateway ~]# realm list

ldapad.com type: kerberos

realm-name: LDAPAD.COM domain-name: ldapad.com configured: kerberos-member 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

login-formats: %U@ldapad.com login-policy: allow-realm-logins

#### Step 7. After successful joining you will get below sssd.conf and you need to change use\_fully\_qualified\_names to False and shell to ezsh.

root@gateway ~]# vim /etc/sssd/sssd.conf [sssd] domains = ldapad.com config\_file\_version = 2 services = nss, pam [domain/ldapad.com] ad\_domain = ldapad.com  $krb5_realm = LDAPAD.COM$ 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.

root@gateway ~]# service sssd restart && service nscd restart

#### **Step 9.** Run id username /getent passwd username and see AD user details.

root@gateway ~]# id john uid=1701601108(john) gid=1701600513(domain users) groups=1701600513(domain users) root@gateway ~]# getent passwd john john:\*:1701601108:1701600513:john user:/home/john@ldapad.com:/usr/local/bin/ezsh

#### Note:

Use the below command to clear the cache of the user.

root@gateway ~]# sss\_cache -u username

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 RHEL 8 using SSSD

Integrate OpenLdap with Centos 8 using SSSD

Integrate Windows AD with Ubuntu using SSSD

Integrate OpenLdap with CentOS using SSSD

Online URL:

https://www.ezeelogin.com/kb/article/integrate-windows-ad-with-centos-using-sssd-430.html