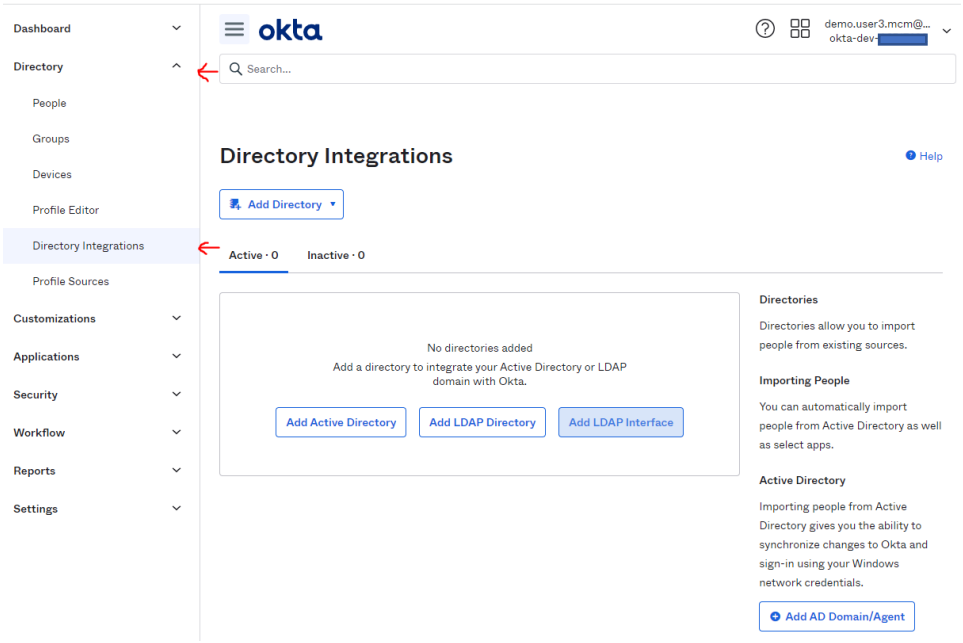
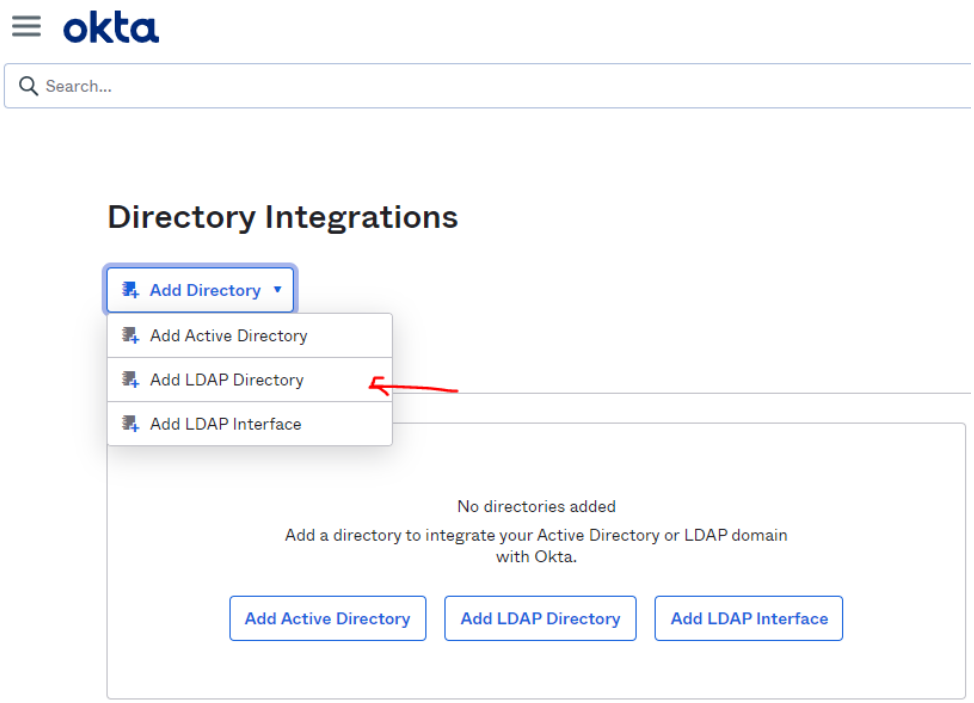
OKTA INTEGRATION WITH AWS LDAP SERVER

Please follow below steps for Okta agent installation and LDAP integration:-

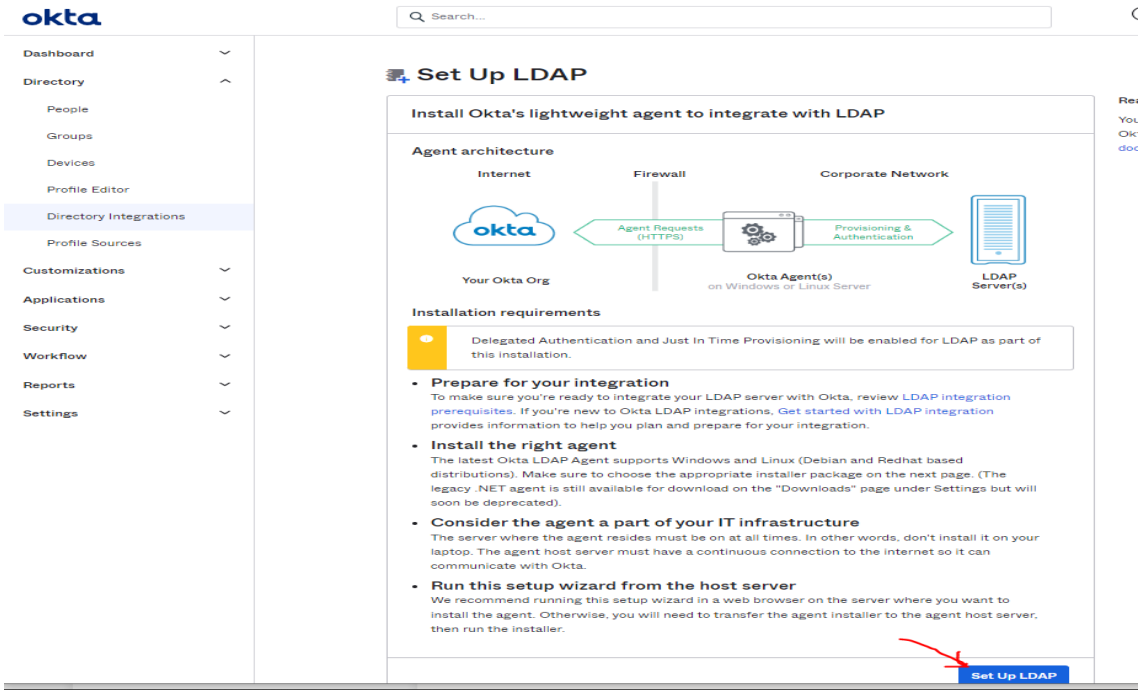
1. Login into okta admin console using administrator password. Navigate to Directory>>Directory Integration section.



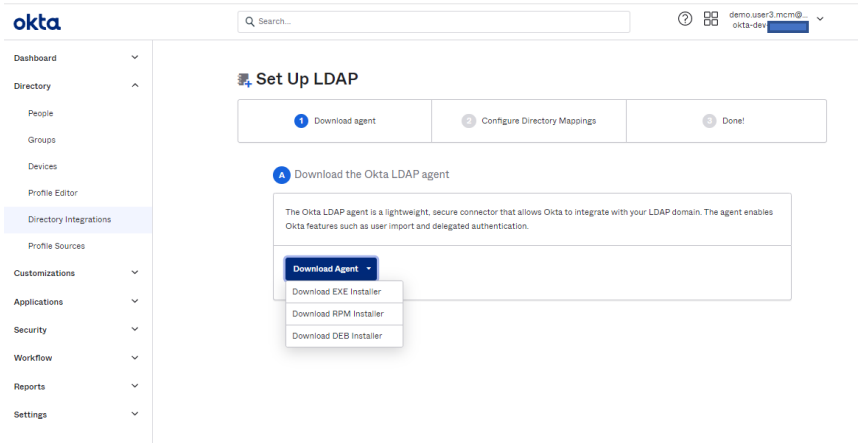
2. Select “Add LDAP Directory” from the options listed.



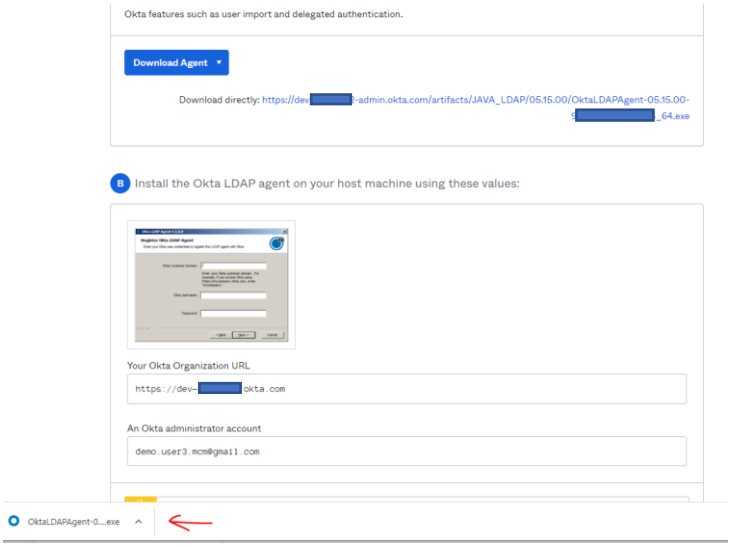
3. Click on “Set Up LDAP”



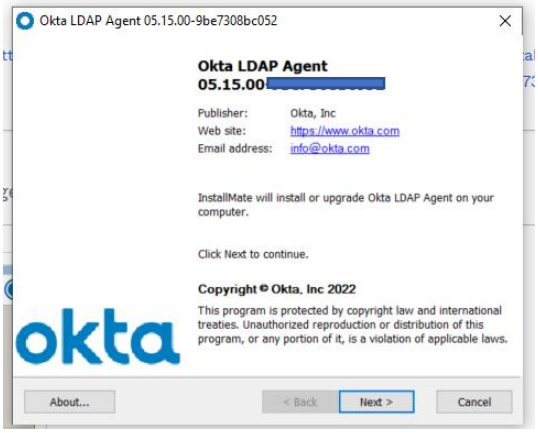
4. Set Up LDAP page is rendered on UI. From the drop down select appropriate package based on the environment okta agent is planned to be installed.
   Note:- This document covers the steps to install on Windows and Centos 7



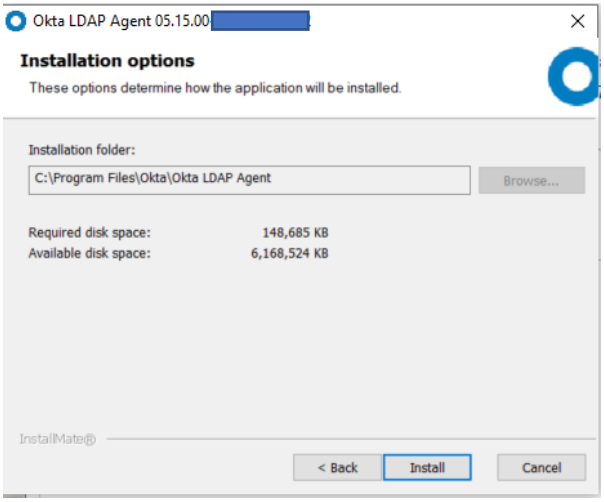
5. Once the installable is downloaded, “Okta Organization URL” is displayed. This URL and admin credentials will be needed while installing agent later.



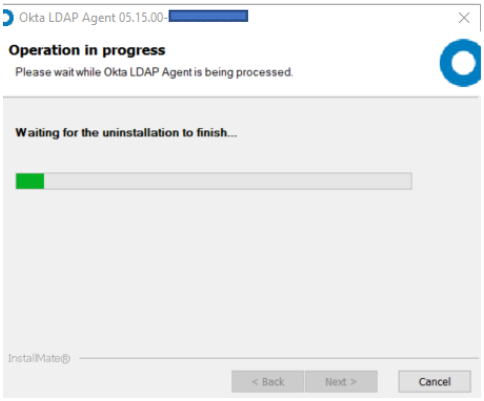
6. Steps to install okta agent on windows OS. Double click the exe to begin the installation. And installation prompt will be displayed. Click on “Next” to proceed.

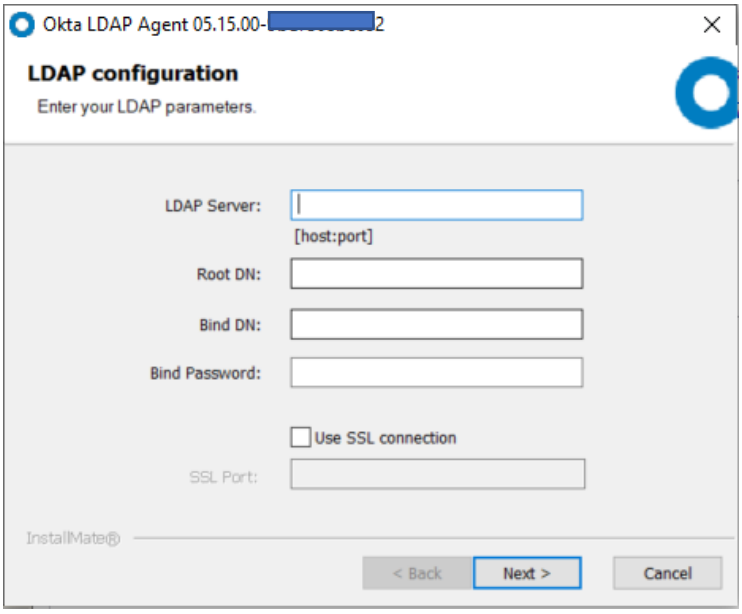


7. Click on install to proceed with installation in default location.

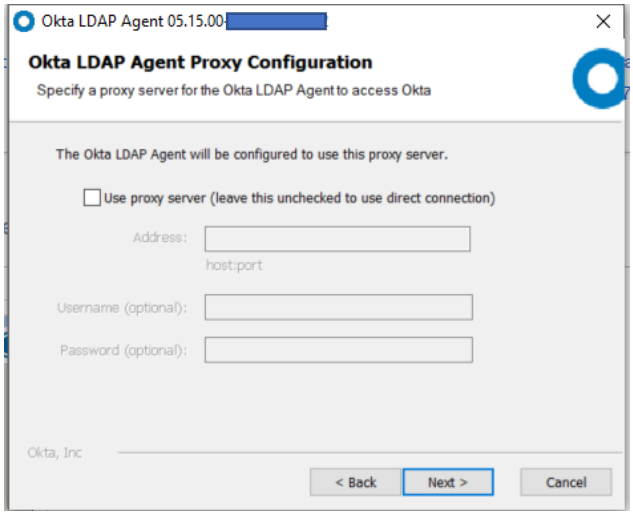


8. User will be prompted to enter LDAP credentials. Enter LDAP credentials accordingly.

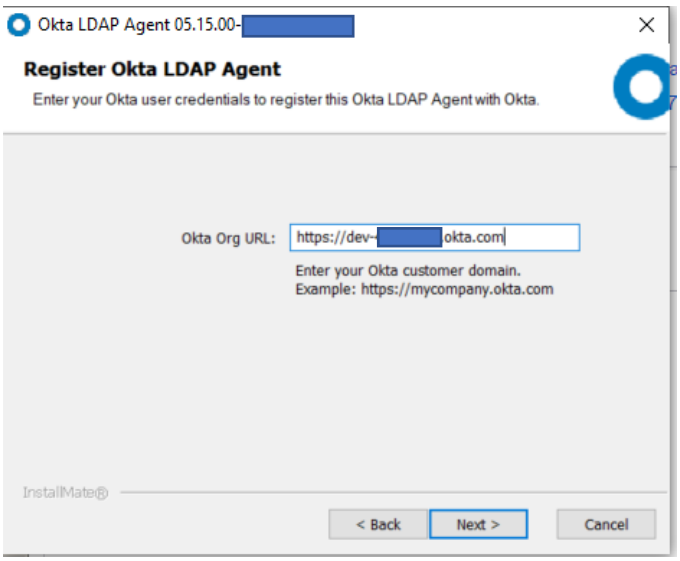




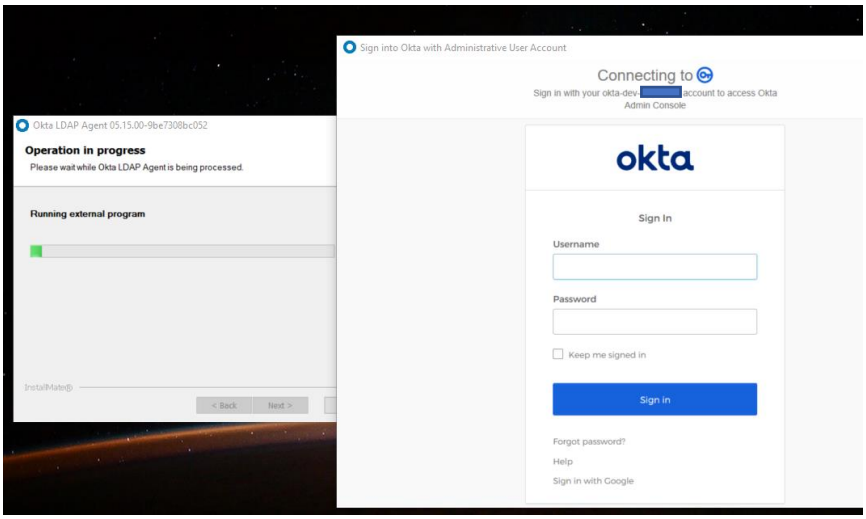
9. Click Next to continue



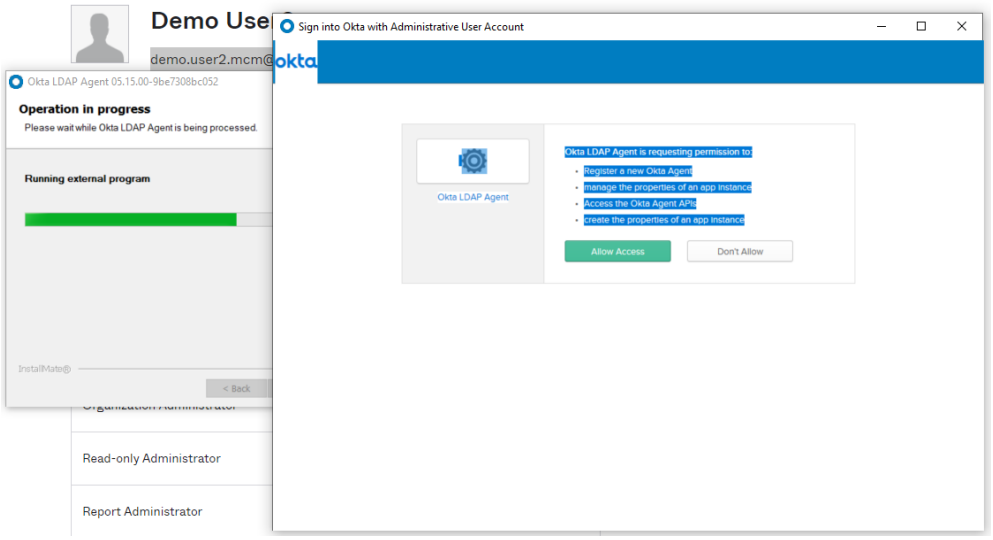
10. Enter the Okta Organizational URL that was displayed while downloading the installable.



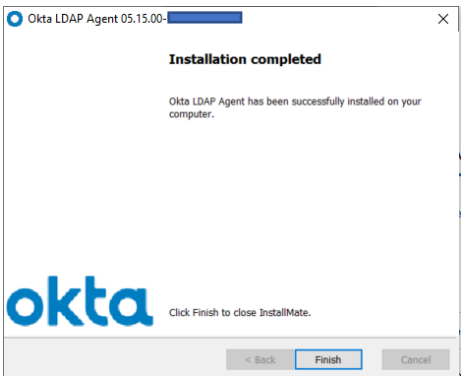
11. User will be promoted to enter Okta admin credentials.

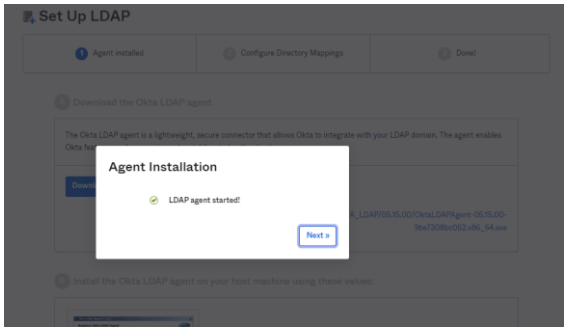


12. Once authenticated using admin credentials, Allow access to okta agent.

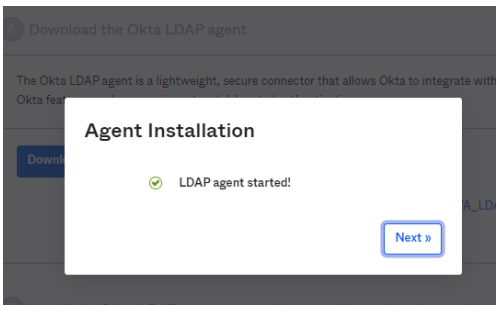


13. Okta agent installation is completed and user will be prompted to the UI page from where the exe was download for further configuration.

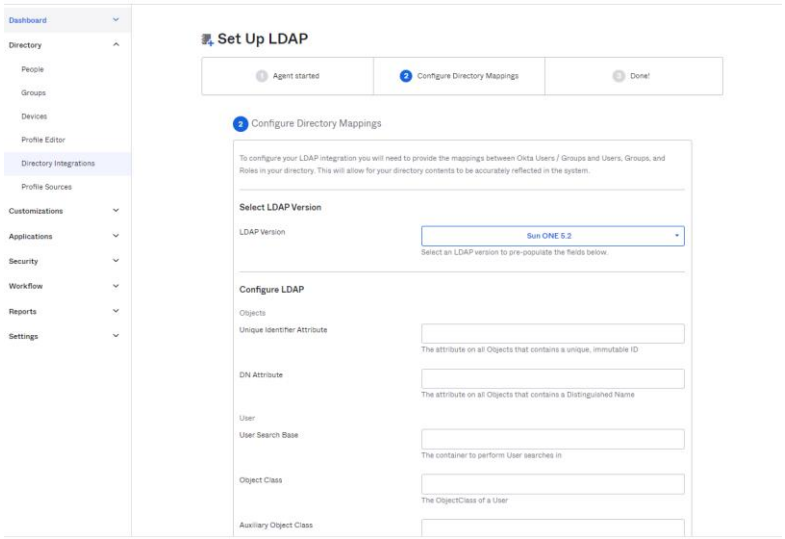




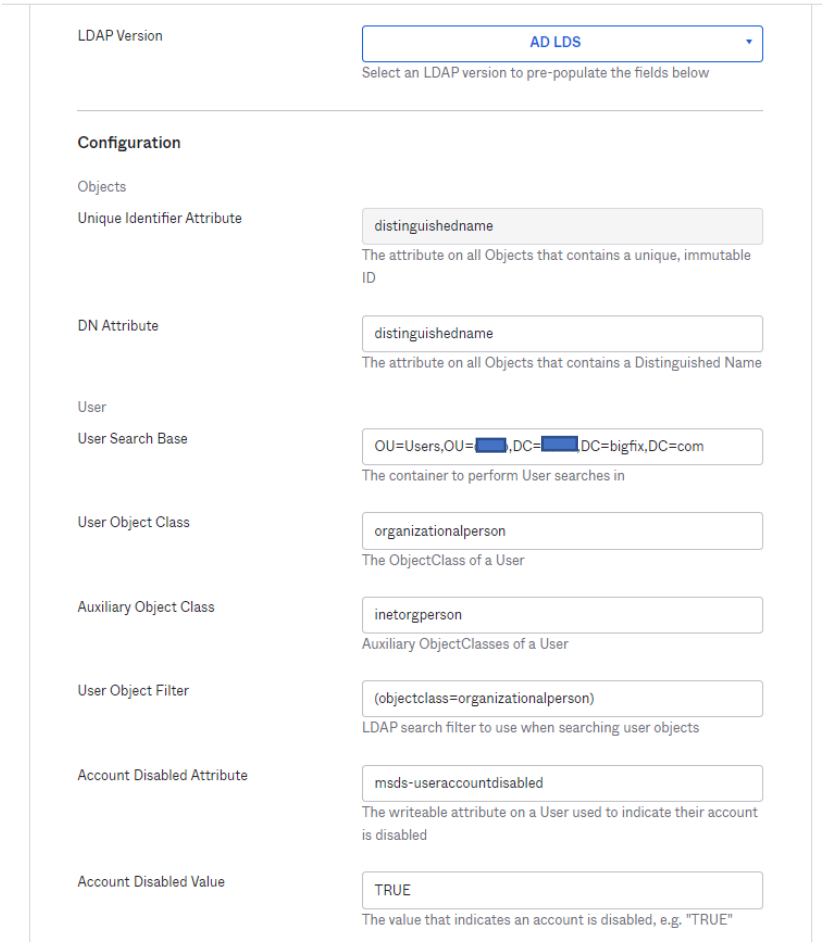
14. Click “Next” on the UI page. The user will be redirected to “Set-up LDAP” page.

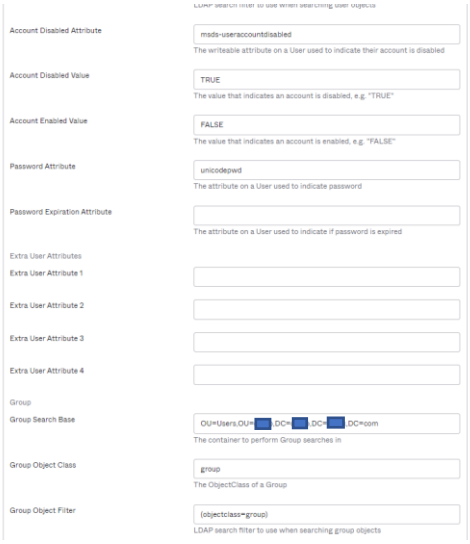


15. Choose “AD LDAP” from drop down for LDAP version.

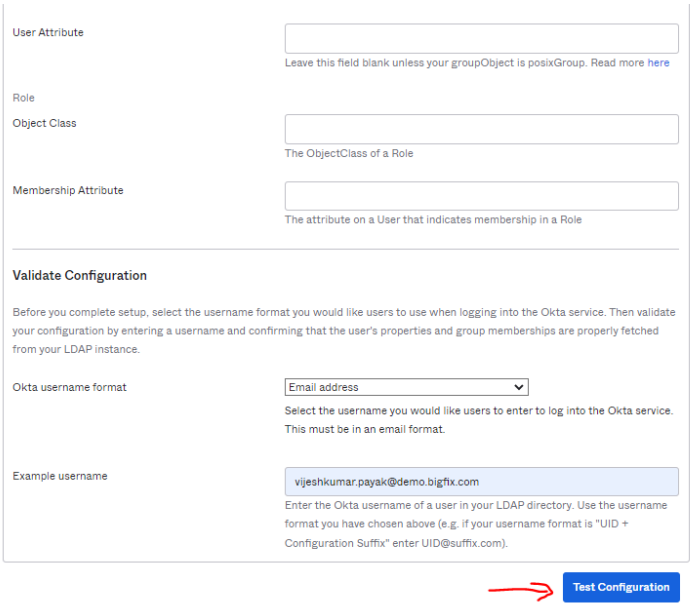


16. As per the LDAP to be connected add appropriate properties.
    Enter values as shown below to connect to LDAP.

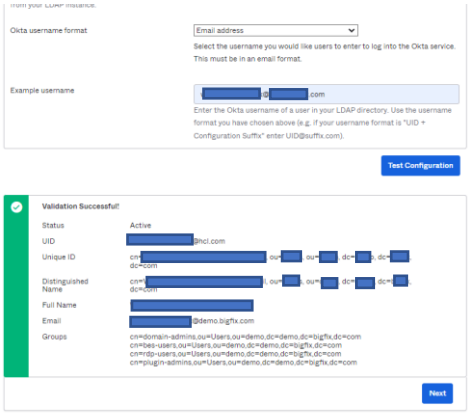




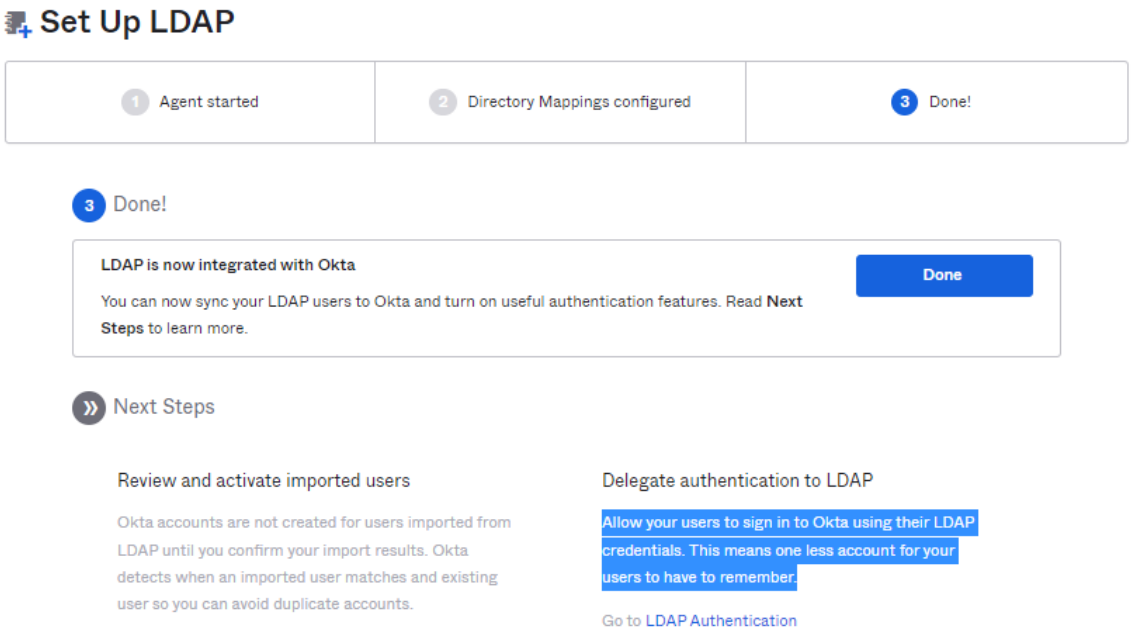
17. Once the values are entered, test the configuration using “Test configuration” button. Choose email and enter email address of any valid LDAP user.



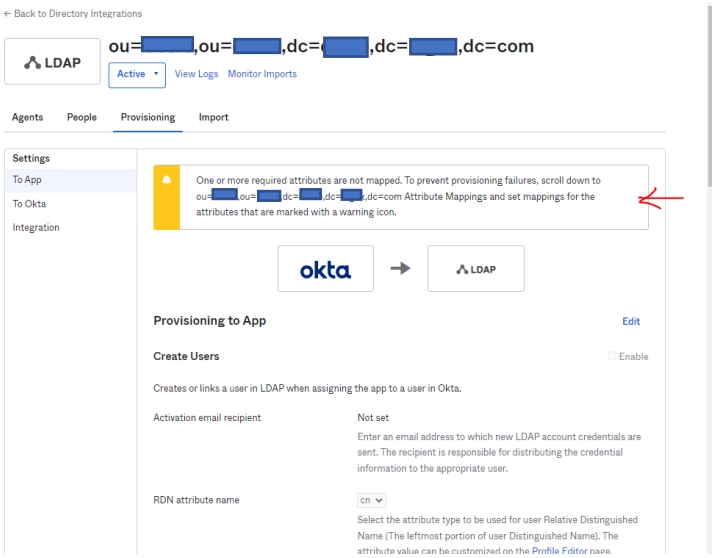
18. Okta agent will query the LDAP server and fetch user details if configuration is successful. Click “Next” to save the configurations.



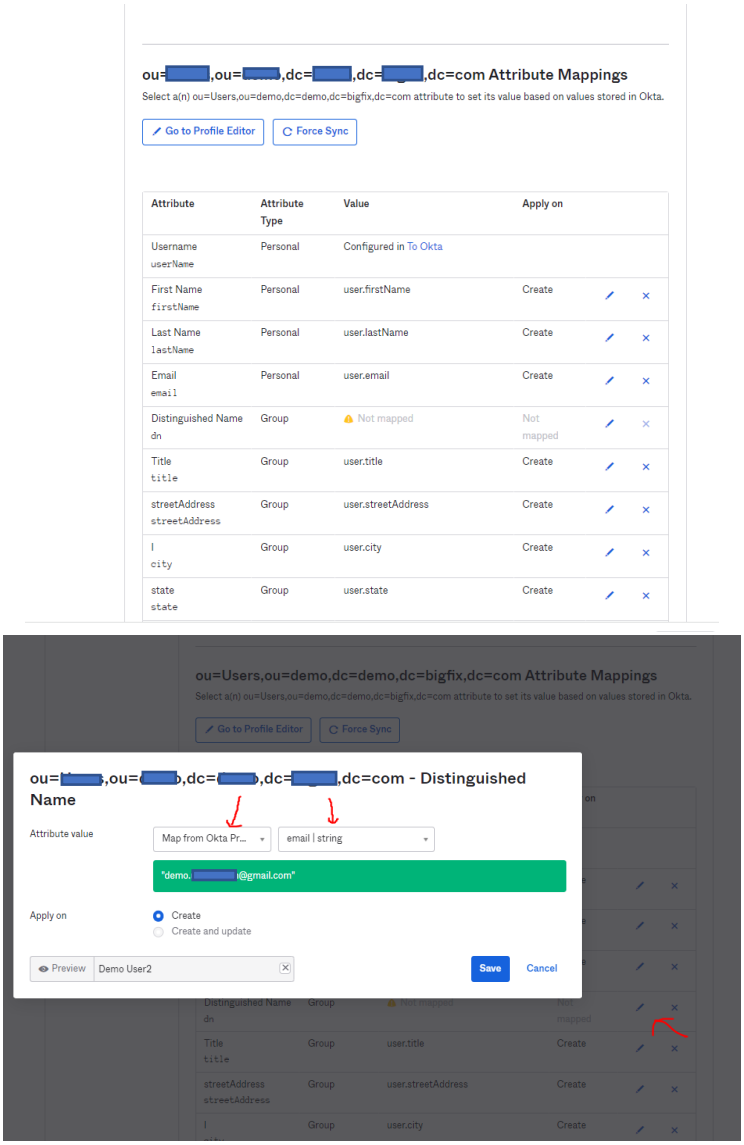
19. Click Done button.



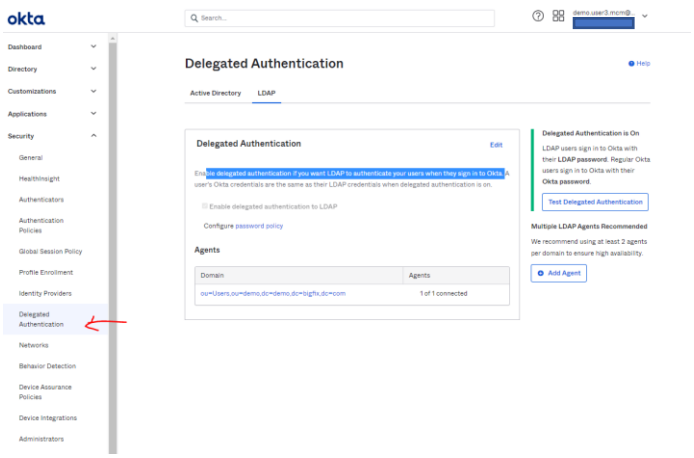
20. Once user clicks on “Done”, the user will be navigated to “Directory Integration” Page. The page will have a warning displayed.

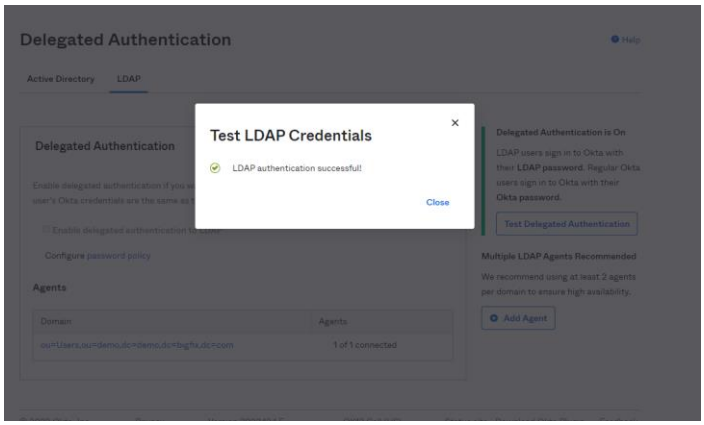


21. Scroll down to attribute mapping section on the same page. “Distinguished Name” will be shown as not mapped. Map the same as email.

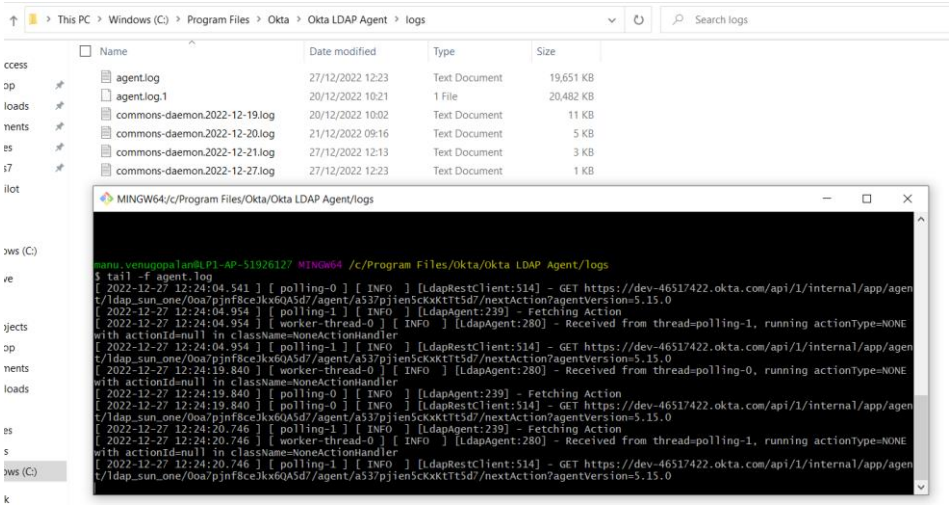


22. Navigate to Security>>Delegated Authentication. Click on “Test Delegated Authentication” and enter AWS user credentials and test the set-up.





23. Agent logs will be available in the below path on the machine agent is installed.



24. Okta logs will be available on the admin console under Reports>>System Log