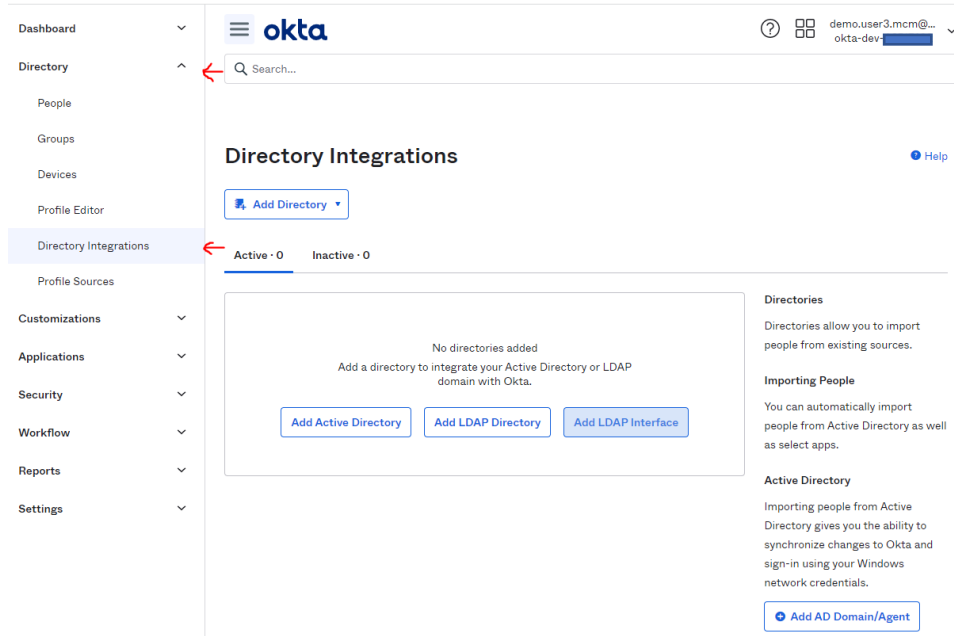




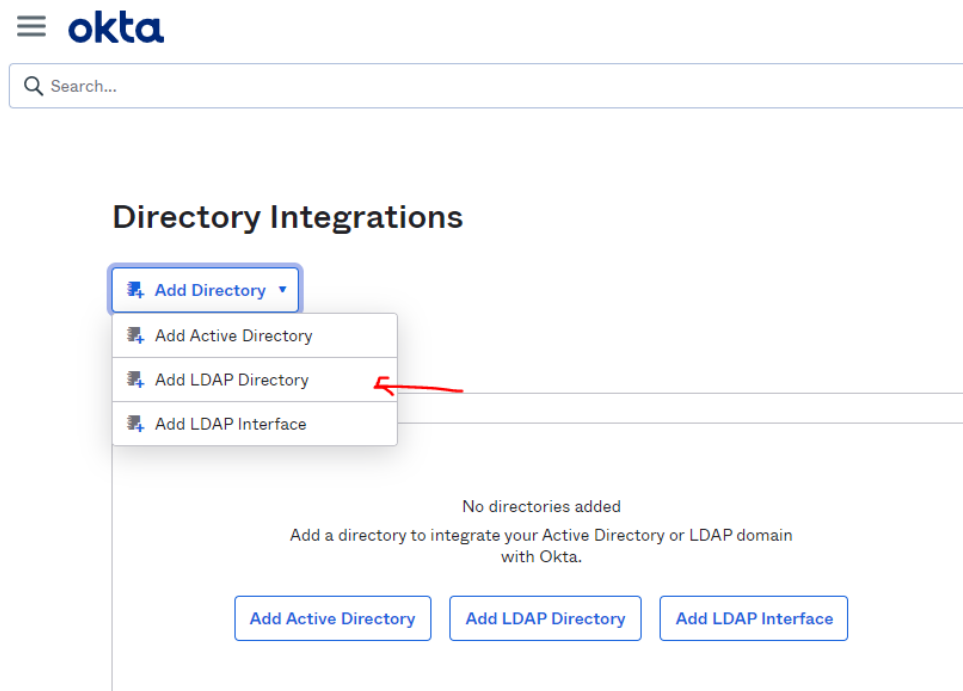
OKTA INTEGRATION WITH AWS LDAP SERVER

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”

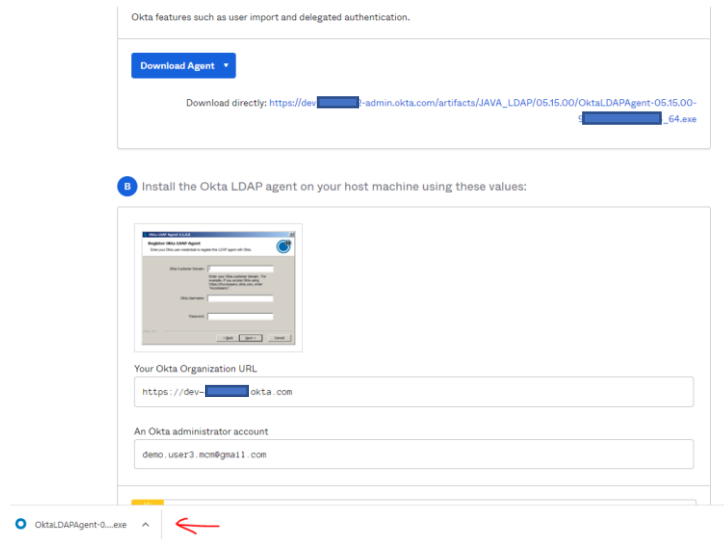
The screenshot shows the Okta administration console interface. On the left is a navigation menu with 'Directory Integrations' selected. The main content area is titled 'Set Up LDAP' and contains a diagram of the 'Agent architecture' showing the flow between 'Your Okta Org' (Internet), 'Okta Agent(s) on Windows or Linux Server' (Firewall), and 'LDAP Server(s)' (Corporate Network). Below the diagram are 'Installation requirements' and a list of steps: 'Prepare for your integration', 'Install the right agent', 'Consider the agent a part of your IT infrastructure', and 'Run this setup wizard from the host server'. A red arrow points to a 'Set Up LDAP' button at the bottom right of the content area.

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.

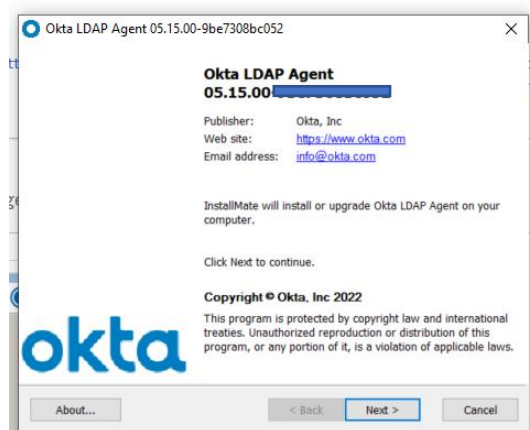
Note:- This document covers the steps to install on Windows and Centos 7

This screenshot shows the 'Set Up LDAP' page at the 'Download agent' step. A progress bar at the top indicates three steps: '1 Download agent', '2 Configure Directory Mappings', and '3 Done!'. The main content area is titled 'Download the Okta LDAP agent' and includes a description of the agent. A 'Download Agent' button has been clicked, opening a dropdown menu with three options: 'Download EXE Installer', 'Download RPM Installer', and 'Download DEB Installer'.

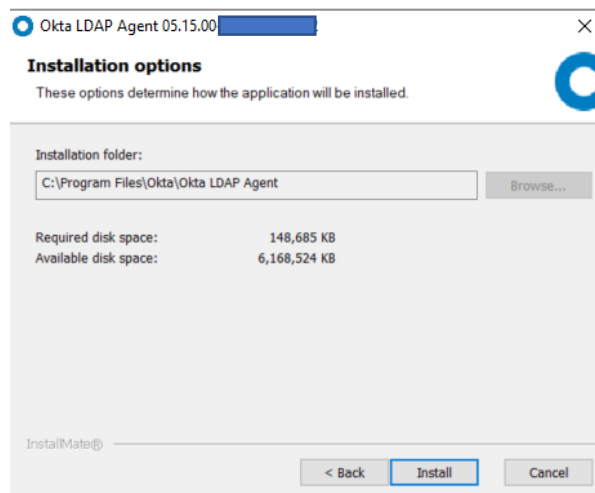
- Once the installable is downloaded, “Okta Organization URL” is displayed. This URL and admin credentials will be needed while installing agent later.



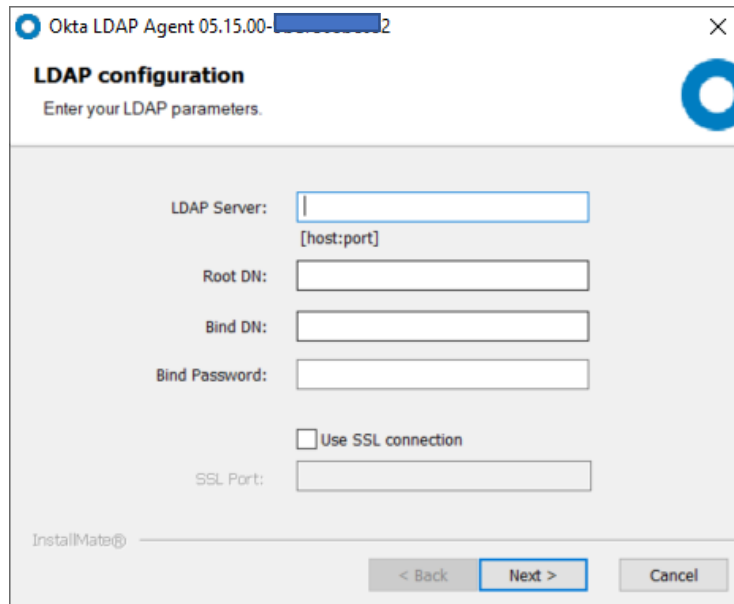
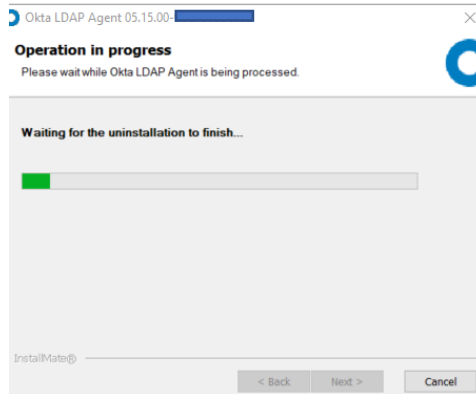
- Steps to install okta agent on windows OS. Double click the exe to begin the installation. And installation prompt will be displayed. Click on “Next” to proceed.



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



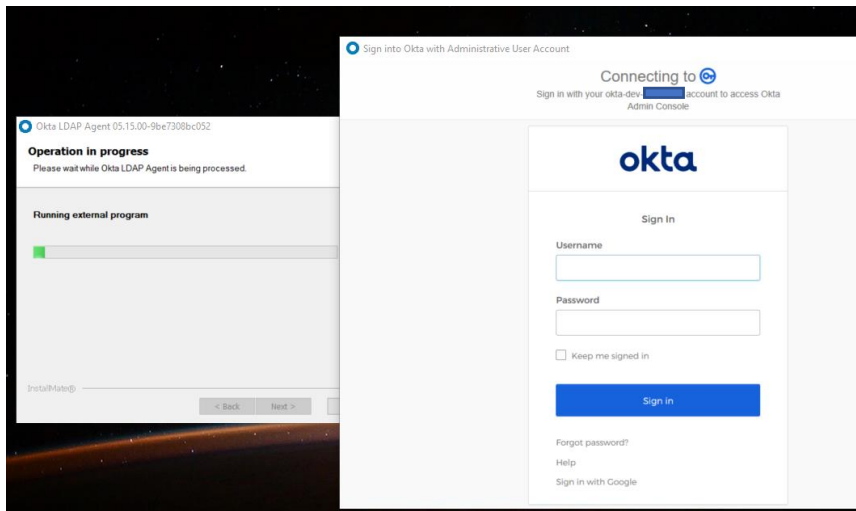
8. User will be prompted to enter LDAP credentials. Enter LDAP credentials accordingly.



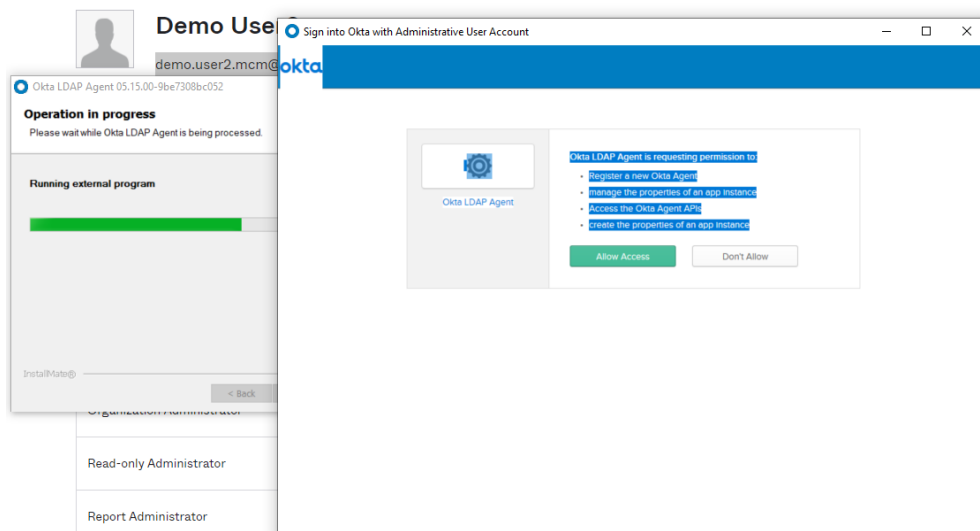
9. Click Next to continue

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

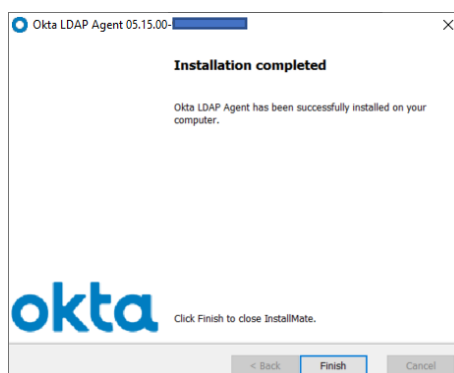
11. User will be prompted to enter Okta admin credentials.

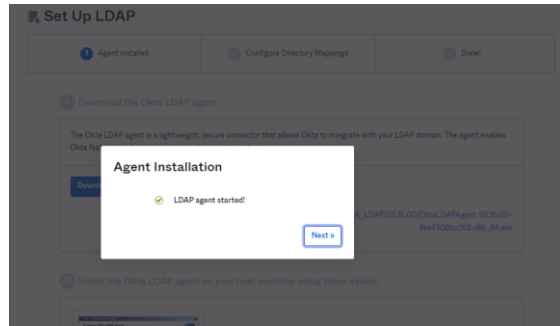


12. Once authenticated using admin credentials, Allow access to okta agent.

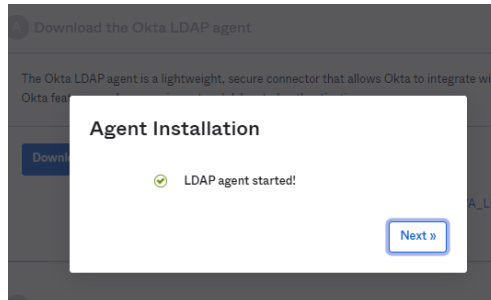


13. Okta agent installation is completed and user will be prompted to the UI page from where the exe was download for further configuration.

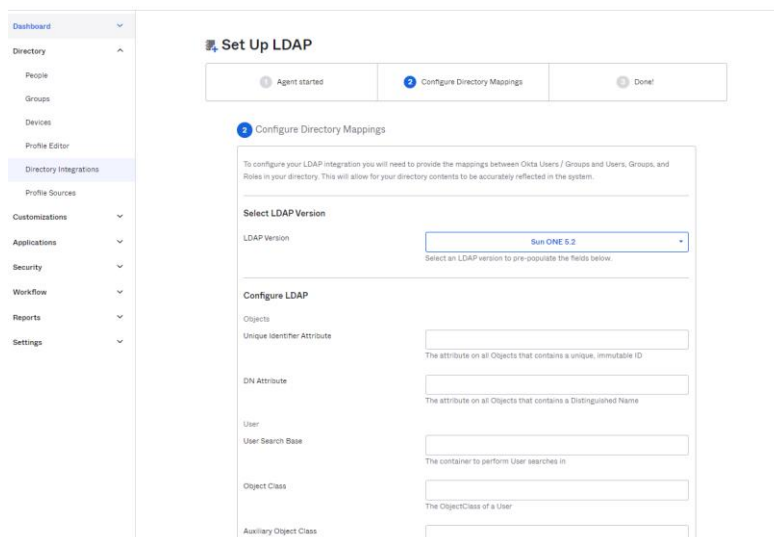




14. Click “Next” on the UI page. The user will be redirected to “Set-up LDAP” page.



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.

LDAP Version
 Select an LDAP version to pre-populate the fields below

Configuration

Objects

Unique Identifier Attribute
 The attribute on all Objects that contains a unique, immutable ID

DN Attribute
 The attribute on all Objects that contains a Distinguished Name

User

User Search Base
 The container to perform User searches in

User Object Class
 The ObjectClass of a User

Auxiliary Object Class
 Auxiliary ObjectClasses of a User

User Object Filter
 LDAP search filter to use when searching user objects

Account Disabled Attribute
 The writeable attribute on a User used to indicate their account is disabled

Account Disabled Value
 The value that indicates an account is disabled, e.g. "TRUE"

LDAP SEARCH FILTER TO USE WHEN SEARCHING USER OBJECTS

Account Disabled Attribute
 The writeable attribute on a User used to indicate their account is disabled

Account Disabled Value
 The value that indicates an account is disabled, e.g. "TRUE"

Account Enabled Value
 The value that indicates an account is enabled, e.g. "FALSE"

Password Attribute
 The attribute on a User used to indicate password

Password Expiration Attribute
 The attribute on a User used to indicate if password is expired

Extra User Attributes

Extra User Attribute 1

Extra User Attribute 2

Extra User Attribute 3

Extra User Attribute 4

Group

Group Search Base
 The container to perform Group searches in

Group Object Class
 The ObjectClass of a Group

Group Object Filter
 LDAP search filter to use when searching group objects

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

User Attribute
Leave this field blank unless your groupObject is posixGroup. Read more [here](#)

Role
The ObjectClass of a Role


Membership Attribute
The attribute on a User that indicates membership in a Role

Validate Configuration

Before you complete setup, select the username format you would like users to use when logging into the Okta service. Then validate your configuration by entering a username and confirming that the user's properties and group memberships are properly fetched from your LDAP instance.

Okta username format
Select the username you would like users to enter to log into the Okta service. This must be in an email format.

Example username
Enter the Okta username of a user in your LDAP directory. Use the username format you have chosen above (e.g. if your username format is "UID + Configuration Suffix" enter UID@suffix.com).

 [Test Configuration](#)

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

verify your LDAP instance.

Okta username format
Select the username you would like users to enter to log into the Okta service. This must be in an email format.

Example username
Enter the Okta username of a user in your LDAP directory. Use the username format you have chosen above (e.g. if your username format is "UID + Configuration Suffix" enter UID@suffix.com).

[Test Configuration](#)

Validation Successful!

Status	Active
UID	[redacted]@demo.bigfix.com
Unique ID	cn=[redacted], ou=[redacted], ou=[redacted], dc=[redacted], dc=com
Distinguished Name	cn=[redacted], ou=[redacted], ou=[redacted], dc=[redacted], dc=com
Full Name	[redacted]
Email	[redacted]@demo.bigfix.com
Groups	cn=admins, ou=Users, ou=demo, dc=demo, dc=bigfix, dc=com cn=bes-users, ou=Users, ou=demo, dc=demo, dc=bigfix, dc=com cn=reg-users, ou=Users, ou=demo, dc=demo, dc=bigfix, dc=com cn=plugin-admins, ou=Users, ou=demo, dc=demo, dc=bigfix, dc=com

[Next](#)

19. Click Done button.

Set Up LDAP

1 Agent started 2 Directory Mappings configured 3 Done!

3 Done!

LDAP is now integrated with Okta

You can now sync your LDAP users to Okta and turn on useful authentication features. Read [Next Steps](#) to learn more.

Done

» Next Steps

Review and activate imported users

Okta accounts are not created for users imported from LDAP until you confirm your import results. Okta detects when an imported user matches and existing user so you can avoid duplicate accounts.

Delegate authentication to LDAP

Allow your users to sign in to Okta using their LDAP credentials. This means one less account for your users to have to remember.

[Go to LDAP Authentication](#)

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

← Back to Directory Integrations

LDAP ou=,ou=,dc=,dc=,dc=com

Active View Logs Monitor Imports

Agents People Provisioning Import

Settings

To App

To Okta

Integration

One or more required attributes are not mapped. To prevent provisioning failures, scroll down to ou=,ou=,dc=,dc=,dc=com Attribute Mappings and set mappings for the attributes that are marked with a warning icon.

okta → LDAP

Provisioning to App Edit

Create Users Enable

Creates or links a user in LDAP when assigning the app to a user in Okta.

Activation email recipient Not set

Enter an email address to which new LDAP account credentials are sent. The recipient is responsible for distributing the credential information to the appropriate user.

RDN attribute name cn

Select the attribute type to be used for user Relative Distinguished Name (The leftmost portion of user Distinguished Name). The attribute value can be customized on the Profile Editor page.

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

ou=,ou=,dc=,dc=,dc=com Attribute Mappings

Select a(n) ou=Users,ou=demo,dc=demo,dc=bigfix,dc=com attribute to set its value based on values stored in Okta.

[Go to Profile Editor](#) [Force Sync](#)

Attribute	Attribute Type	Value	Apply on
Username userName	Personal	Configured in To Okta	
First Name firstName	Personal	user.firstName	Create / x
Last Name lastName	Personal	user.lastName	Create / x
Email email	Personal	user.email	Create / x
Distinguished Name dn	Group	⚠ Not mapped	Not mapped / x
Title title	Group	user.title	Create / x
streetAddress streetAddress	Group	user.streetAddress	Create / x
l city	Group	user.city	Create / x
state state	Group	user.state	Create / x

ou=Users,ou=demo,dc=demo,dc=bigfix,dc=com Attribute Mappings

Select a(n) ou=Users,ou=demo,dc=demo,dc=bigfix,dc=com attribute to set its value based on values stored in Okta.

[Go to Profile Editor](#) [Force Sync](#)

ou=,ou=,dc=,dc=,dc=com - Distinguished Name

Attribute value:

"demo. @gmail.com"

Apply on: Create Create and update

[Preview](#) Demo User2 [Save](#) [Cancel](#)

Attribute	Attribute Type	Value	Apply on
Distinguished Name dn	Group	⚠ Not mapped	Not mapped / x
Title title	Group	user.title	Create / x
streetAddress streetAddress	Group	user.streetAddress	Create / x
l city	Group	user.city	Create / x

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

okta

Search...

demo user3 emp@

Dashboard

Directory

Customizations

Applications

Security

General

Health Insight

Authentications

Authentication Policies

Global Session Policy

Profile Enrollment

Identity Providers

Delegated Authentication

Networks

Behavior Detection

Device Assurance

Policies

Device Integrations

Administrators

Delegated Authentication

Active Directory LDAP

Delegated Authentication [Edit](#)

Enable delegated authentication. If you want LDAP to authenticate your users when they sign in to Okta, user's Okta credentials are the same as their LDAP credentials when delegated authentication is on.

Enable delegated authentication to LDAP

[Configure password policy](#)

Agents

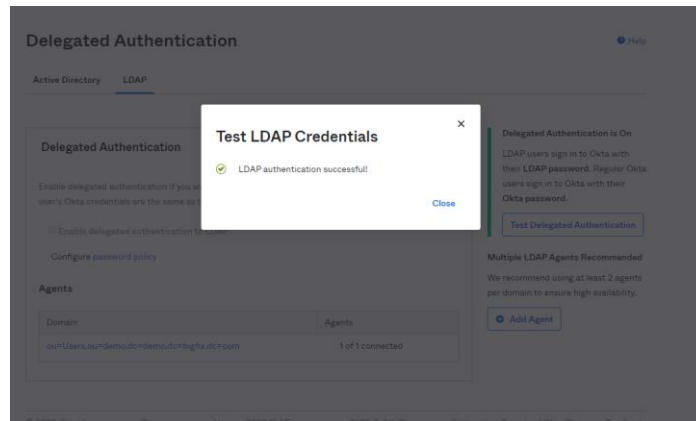
Domain	Agents
ou=Users,ou=demo,dc=demo,dc=bigfix,dc=com	1 of 1 connected

Delegated Authentication is On
LDAP users sign in to Okta with their LDAP password. Regular Okta users sign in to Okta with their Okta password.

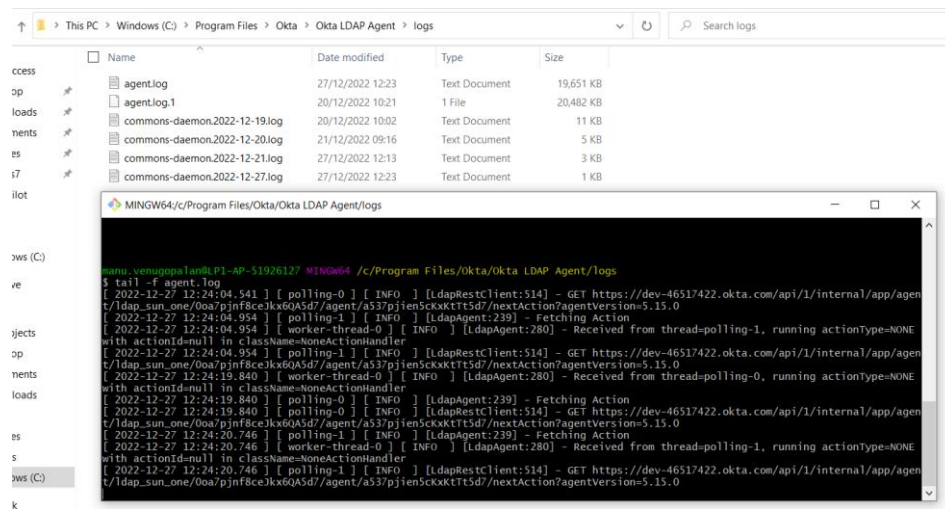
[Test Delegated Authentication](#)

Multiple LDAP Agents Recommended
We recommend using at least 2 agents per domain to ensure high availability.

[Add Agent](#)



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

