KONICA MINOLTA

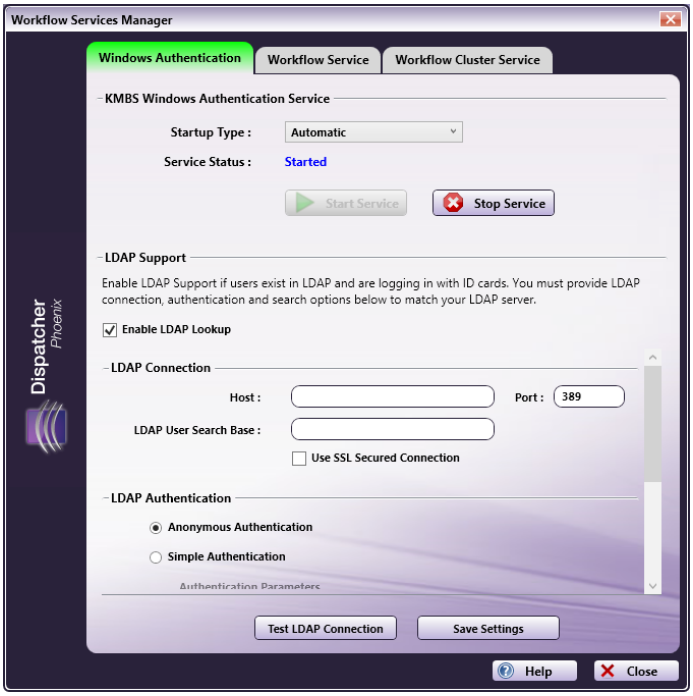
Dispatcher Phoenix

Configuring for LDAP Authentication

To scan to a personalized location, such as a user's home directory, users must first be identified at time of scanning. One common method for this is to authenticate through LDAP, the Lightweight Directory Access Protocol that is a standard for user authentication and storage of user profile data.

Dispatcher Phoenix can connect to LDAP to determine user attributes for scanning to home directories ({user:home}) and email addresses ({user:email}), etc. To configure for LDAP authentication within Dispatcher Phoenix, you must use the Workflow Services Manager, a tool that can be accessed from the Windows Start Menu (**All Programs > Konica Minolta**). You can also perform a Windows search on "Workflow Services Manager" to find this tool.

The Workflow Services Manager resembles the following illustration:



Using the **Windows Authentication** tab, do the following:

1. Enable support for LDAP (Lightweight Directory Access Protocol) by checking the **Enable LDAP Lookup box**. Once enabled, connection, authentication, and search options must be entered to match the LDAP server.
2. Under the **LDAP Connection** area, do the following:
   - In the **Host** field, enter the name of the server where the Active Directory (AD) server is hosted.
   - In the **Port** field, enter the AD server port.
   - In the **LDAP User Search Base** field, enter your search starting point in the LDAP server tree structure.
   - To enable SSL connections to the LDAP server, check the **Use SSL Secured Connection** box.

Configuring for LDAP Authentication, continued

3. Under the **LDAP Authentication** area, do the following:
   - Select the **Anonymous Authentication** radio button to specify that the connection should be made without passing credentials, or select the **Simple Authentication** button to specify that basic authentication should be used on the connection. If Simple Authentication is selected, the Bind DN and Password fields will be enabled.
   - In the **Bind DN** field, enter the user on the external AD server who is permitted to search the LDAP directory within the defined search base. Note that the {user}@{domain} variables will be replaced with information coming from the MFP and are necessary to perform the search.
   - In the **Password** field, enter the bind password.
4. Under the **LDAP Search Options** area, do the following:
   - In the **Default Search** field, configure the search attributes.
   - In the **Fallback Search** field, enter additional search strings.
5. Test the search setting by selecting the **Test LDAP Connection** button.
6. Update the Windows Authentication Service by selecting the **Save Settings** button.

Note the following:

- LDAP changes will not take effect until the KMBS Windows Authentication Service is stopped and started again.
- When a user first logs into Dispatcher Phoenix at the MFP, Active Directory and LDAP information is cached until the user logs out of Dispatcher Phoenix by exiting the app. The next time the user logs in, LDAP information will be obtained again from the Active Directory and/or LDAP.