# Windows SSO

Single Sign-On allows users to access their  Agiloft knowledgebase with a hyperlink. The link, which is verified against LDAP, uses the user's Windows session login to access the system.

This feature uses an Active X control, so the following conditions are required:

- Use the required browser, Internet Explorer 5.0+
- Server must be included in the browser's list of trusted sites
- The user's Windows login name must be the same as their  Agiloft login

If these conditions met, the user can instantly login using the following URL: http://SERVER:8080/gui2/sso.jsp?autoLogin=true&project=KB_NAME&State=Main

# System Setup

1. Click the **Setup** gear in the top-right corner and go to **Access > Single Sign-On**.
2. Set Enable LDAP Single Sign-On to Yes.
3. Select and configure either a domain name or IP address range:
    - Enter the trusted domain name, so that users coming from this domain can use single sign-on. This option is most useful if the system is within your firewall.
    - Enter a range of trusted IP-addresses, so that users coming from these addresses can use single sign-on. This option is very useful if you are accessing the system from across a firewall / NAT since, from the perspective of the system, all your users will appear to come from a single IP address. It can also be used if the system is within your firewall.
4. Select any groups you want to exclude from single-sign on. Usually, this is used to make sure users with extensive permissions, such as administrators, are always manually authenticated.
5. Select an authentication method.
6. If desired, select the option to validate the login password against the password in the Active Directory database.

If you want to use Windows SSO when users click hyperlinks from within an email, complete these steps as well:

1. Go to **Setup > System > Manage Global Variables**.
2. Go to the Variables with Default Values tab.
3. Edit the Hotlink Type global variable.
4. Set the Global Variable Value to OTHER_SSO.

# Force SSO Login

Finally, to make sure users log in with SSO after the transition, manually set new passwords for users who should use SSO instead. To do so:

1. Go to the People table and select every user who should use SSO from this point on.

   > Don't select every single user in your system. It's best to leave at least one administrator unchanged, if not the whole admin team, in case you encounter SSO issues in the future that prevent users from logging in with SSO.

2. Click Mass Edit, or Edit Fields, in the action bar.
3. Select the Password field, then click Next to proceed to the Update tab.
4. Select the formula option and enter random_password(15). This will call the random_password(15) function to randomly generate a new 15-character password for everyone you selected.
5. Click Next, then Finish.
6. Now, go to Setup Employees and go to the Layout tab. If you will use SSO for every user in the system, including external users, go to Setup People instead.
7. Remove the Password field from the layout. This prevents users from manually setting a new password and potentially using it to log in instead of SSO.

Next, go to **Setup > System > Manage Global Variables** and check the Customized Variables tab for the Hotlink Type variable. If it has been customized, edit it and reset it to the default value of STANDARD.

You might also notice a setting in the People table called SSO Authentication Method. This field is set automatically by the system when you enable SSO, and should not be modified.