This document describes how to configure CAREWare 6 to authenticate users using the OpenID Connect authentication standard, which is based on the OAuth 2.0 protocol.

Configure CAREWare OIDC setup options

To configure the information that CAREWare needs to communicate with the OpenID Connect provider in the CAREWare user interface:

1. Click Administrative Options.
2. Click Advanced Security Options.
3. Click OpenID Connect Configuration Settings.

Status: *On* means that users are authenticated by specified OIDC server.
OIDC Identity Provider(s): A read-only list of OIDC provider names that have been configured.

OpenID Connect provider configuration

The details of configuring single sign on for CAREWare with an OpenID Connect provider differs depending on which provider you use. You will most likely need to configure users with the OIDC provider. After a user logs into the OIDC provider, their OIDC user account will be matched with their CAREWare user account using one or more values that will be returned from the OIDC provider after the user signs in.

To configure a provider, click the “OIDC Identity Provider(s)” link from the main OpenID Connect Configuration Settings screen. The following settings must be configured for each OIDC provider used by CAREWare:

Name: The name this OpenID Connect provider will be known by
OAuth2 Authorization URL: The authorization URL of the OpenID Connect provider
Client ID: A string identifying the single sign on application. Azure Active Directory refers to this as the “Application ID”.
Client Secret: A secret known only to the CAREWare instance and to the Open ID Connect provider
Match ‘name’ claims key: When checked, the ‘name’ value returned from the OIDC provider is used to find the authenticated CAREWare user. This may be an insecure option if the OIDC provider allows users to change the ‘name’ value for their OIDC user account.
Match ‘name’ claims key on usr_oidc_alias field: When this and the above option are both checked, the ‘name’ value returned from the OIDC provider is matched with the CAREWare user’s record on the OIDC alias field rather than the user’s username.
Match ‘sub’ claims key: When checked, the ‘sub’ value returned from the OIDC provider is used to find the authenticated CAREWare user. The ‘sub’ value is guaranteed to be static and unique among the OIDC provider’s users. This is the most secure matching option.
Save ‘sub’ key if missing in cw_user record: When checked, CAREWare automatically saves a ‘sub’ value returned from the OIDC provider in the user record if the authenticated user can be matched using another field.
Match ‘email’ claims key: When checked, the ‘email’ value returned from the OIDC provider is used to find the authenticated CAREWare user. This may be an insecure option if the OIDC provider allows users to change the ‘email’ value for their OIDC user account.

After changing any Open ID Connect settings:

1. Stop the CAREWare Business Tier.
2. Stop the CAREWare HTTP Server.
3. Start the CAREWare Business Tier.

4. Start the CAREWare HTTP Server.

When Open ID Connect is enabled, all users who log in to CAREWare are authenticated using the OpenID Connect protocol, and all normal logins using a CAREWare username and password are disabled.

To enable normal logins and disable OpenID Connect authentication:

1. Set the *Status* setting to *Off.*
2. Click *Save*.
3. Stop the CAREWare Business Tier.
4. Stop the CAREWare HTTP Server.
5. Start the CAREWare Business Tier.
6. Start the CAREWare HTTP Server.

If OpenID Connect is enabled but configured incorrectly, you may not be able to log back into CAREWare in order to change the configuration. If this happens, normal logins can be re-enabled by setting the "OpenIDConnectAuthEnabled" common storage setting to "OFF".