



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

intelligent Workload Distribution

oauth Section

oauth Section

- `base.uri`
- `client_id`
- `enabled`
- `password`
- `redirect.uri`

base.uri

Default Value:

Valid Values: A fully qualified URI for the OAuth service endpoint; e.g.: `http://localhost:8095/auth/v3`

Changes Take Effect: After restart

Base URI of authorization server that will be accessed during authentication. Locations constructed with this URI will look like: `<base_uri>/oauth/authorize`, `<base_uri>/sign-out`, etc. Expected format for GWS Auth: `<protocol>://<host>:<port>/auth/v3` ; e.g.: `http://localhost:8095/auth/v3` .

client_id

Default Value:

Valid Values: OAuth2 client ID

Changes Take Effect: After restart

Client Identifier required to authenticate IWD manager on authorization server (GWS Auth).

enabled

Default Value: false

Valid Values: true or false

Changes Take Effect: After restart

Enable OAuth based authentication

password

Default Value:

Valid Values: OAuth 2 client secret
Changes Take Effect: After restart

Client Secret required to authenticate IWD manager on authorization server (GWS Auth).

redirect.uri

Default Value: Empty
Valid Values: A fully qualified URI for the iWD Manager endpoint
Changes Take Effect: After restart
Discontinued: 9.0.016.06

After authentication is done, the authorization server redirects users back to iWD Manager using the provided URI.

For example: `http://localhost:8090/iwd_manager`