# Configuration Options

## Glossary

<table>
<thead>
<tr>
<th>Option</th>
<th>Type</th>
<th>Description</th>
<th>Platforms</th>
<th>conf_version</th>
<th>Valid Settings</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>string</td>
<td>The version of the IDP API being used</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>v1, v2.</td>
<td>v2 -&gt; For fixes of CP-418. This value is recommenced to be used</td>
</tr>
<tr>
<td>platform</td>
<td>string</td>
<td>The platform this configuration is for.</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>windows, mac</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The backend this installation is targeting (IdP, CA, etc.)</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>idp, ca</td>
<td>ca is not currently supported</td>
</tr>
<tr>
<td>api_id</td>
<td>string</td>
<td>Deprecated The API ID used to authenticate to the backend.</td>
<td>Windows /Mac</td>
<td>1</td>
<td>cannot be empty</td>
<td></td>
</tr>
<tr>
<td>api_secret</td>
<td>string</td>
<td>Deprecated The API Secret used to authenticate to the backend</td>
<td>Windows /Mac</td>
<td>1</td>
<td>cannot be empty</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Deprecated The host URL used to connect to the backend.</td>
<td>Windows /Mac</td>
<td>1</td>
<td>cannot be empty</td>
<td></td>
</tr>
<tr>
<td>apis</td>
<td>array</td>
<td>List of idp instances, will be list of the following parameters</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>cannot be empty</td>
<td></td>
</tr>
<tr>
<td>access_level</td>
<td>integer</td>
<td>Controls local versus remote access bypass (typically used when an admin wants 2FA on remote logons only).</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>0 (always on), 1 (local only), 2 (remote only), 3 (always off), 4 (sspr only, 2fa off; Only valid for Windows)</td>
<td></td>
</tr>
<tr>
<td>multiple_user</td>
<td>boolean</td>
<td>Controls whether to show cached user names (typically used for server environments where a large number of people are logging in).</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>true, false</td>
<td></td>
</tr>
<tr>
<td>idm_ssrp_url</td>
<td>string</td>
<td>The host URL used to invoke the self service password reset workflow in the browser</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>idm_ssrp_label</td>
<td>string</td>
<td>Deprecated</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>alternate_providers</td>
<td>string array</td>
<td>List of GUIDs of other credential providers allowed to exist on the system</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>array of valid GUIDs</td>
<td></td>
</tr>
<tr>
<td>group_bypass</td>
<td>string array</td>
<td>List of AD group names that can bypass 2FA</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>group name or domain\groupname (e.g. “BypassGroup”, “DOMAIN\BypassGroup”)</td>
<td></td>
</tr>
<tr>
<td>allow_self_signed</td>
<td>boolean</td>
<td>Controls if we allow self signed certificates on the server side</td>
<td>Windows /Mac</td>
<td>1 and higher</td>
<td>true, false</td>
<td></td>
</tr>
<tr>
<td>conf_version</td>
<td>int</td>
<td>Login for Endpoints Configuration version</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>1, 2, 3, 4 (will be empty on version 1)</td>
<td>Added since 19.06</td>
</tr>
<tr>
<td>enabled_on_uac</td>
<td>boolean</td>
<td>Enabled credential provider on Run As Administrator</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>true, false (empty on version 1)</td>
<td>Added since 1.0.4</td>
</tr>
<tr>
<td>adaptive_enabled</td>
<td>boolean</td>
<td>Enable adaptive login</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>true, false (empty defaults to true)</td>
<td>Since 19.06</td>
</tr>
<tr>
<td>bypass_interval</td>
<td>integer</td>
<td>Value in seconds. 0 means disabled.</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>Any positive number</td>
<td>Since 19.06</td>
</tr>
<tr>
<td>store_seeds</td>
<td>boolean</td>
<td>Enable/Disable seeds cache. If cache is disabled users are not going to be able to log in while being offline.</td>
<td>Windows /Mac</td>
<td>2 and higher</td>
<td>true, false (empty defaults to true)</td>
<td>Since 19.06</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>custom_error_message</td>
<td>string</td>
<td>Text to display to the user if there was an error during the login process.</td>
<td>Windows</td>
<td>2 and higher</td>
<td></td>
<td>Since 19.06</td>
</tr>
<tr>
<td>legacy_http_communication</td>
<td>boolean</td>
<td>If present and set on true, the client will switch to the old HTTP library, only use as last resource, not recommended. This library behavior is not homogeneous among different OS versions and have some bugs. <em>Will be deprecated soon. Internal / troubleshooting use only, should not be used on production environments</em></td>
<td>Windows /Mac</td>
<td>3 and Higher</td>
<td>true, false, non_present defaults to false</td>
<td>Since 19.09</td>
</tr>
<tr>
<td>hide_retry_option</td>
<td>boolean</td>
<td>Enable/Disable the retry option to connect to idp</td>
<td>Windows</td>
<td>3 and Higher</td>
<td>true, false, non_present defaults to true</td>
<td>Since 19.09</td>
</tr>
<tr>
<td>lang_locale</td>
<td>string</td>
<td>Language code to display strings in UI</td>
<td>Windows /Mac</td>
<td>3 and Higher</td>
<td>lang code, default value &quot;en_US&quot;</td>
<td>Since 19.09. Currently at 19.09 en_US is the only valid value. to be extended on the future</td>
</tr>
<tr>
<td>passwordless_enabled</td>
<td>boolean</td>
<td>Enable/Disable passwordless functionality</td>
<td>Windows</td>
<td>3 and Higher</td>
<td>true, false</td>
<td>Since 19.09</td>
</tr>
<tr>
<td>login_attempts</td>
<td>int</td>
<td>Number of login attempts that the user has to login without 2fa. 0 means disabled.</td>
<td>Windows /Mac</td>
<td>4 and Higher</td>
<td>Any positive number</td>
<td>Since 20.03</td>
</tr>
</tbody>
</table>

Sample version 4 (since 20.03)

```
{
    "access_level": 0,
    "adaptive_enabled": true,
    "apis": [
        {
            "host": "https://endpoint01.gosecureauth.com/SecureAuth19",
            "id": "50b8bd3c9b8b4edf8b8335b180fcccbb",
            "secret": "de141d3f532be6035c3206083df6c8d1b64522094705aaa3ff9765b0a1a81e"
        }
    ],
    "bypass_interval": 0,
    "conf_version": 4,
    "login_attempts": 3,
    "custom_error_message": "",
    "enabled_on_uac": true,
    "group_bypass": "\\\Administrators",
    "hide_retry_option": false,
    "idm_sspール_label": "2. L4W SSPR",
    "idm_sspール_url": "https://endpoint01.gosecureauth.com/SecureAuth29",
    "multiple_user": false,
    "alternate_providers": [],
    "passwordless_enabled": true,
    "platform": "windows",
    "store_seeds": true,
    "type": "idp",
    "version": "v2"
}
```

Sample version 3 (since 19.09)
Mac Sample

```json
{
  "access_level": 0,
  "adaptive_enabled": true,
  "apis": [
    {
      "host": "https://localhost/SecureAuth3",
      "id": "000860c9324d4c79817d1edeece8ff",
      "secret": "e29e3f4f8a3150f579ea14bde65c9012aac65859ee1404d70c0ed655842b194b"
    }
  ],
  "bypass_interval": 300,
  "conf_version": 3,
  "custom_error_message": "For assistance, please contact Acme helpdesk at 949-555-1212, help@acme.co.com, or https://helpdesk.acme.co.com.",
  "enabled_on_uac": false,
  "group_bypass": ["BypassGroup", "DOMAIN\BypassGroup", ".\Administrators"],
  "hide_retry_option": false,
  "idm_ssp_label": "2. L4W SSPR",
  "idm_ssp_url": "https://localhost/SecureAuth2",
  "lang_locale": "en_US",
  "legacy_http_communication": false,
  "multiple_user": false,
  "passwordless_enabled": true,
  "platform": "windows",
  "store_seeds": true,
  "type": "idp",
  "version": "v2"
}
```

Sample version 2 (since 19.06)

```json
{
  "access_level": 0,
  "adaptive_enabled": true,
  "apis": [
    {
      "host": "https://localhost/SecureAuth3",
      "id": "000860c9324d4c79817d1edeece8ff",
      "secret": "e29e3f4f8a3150f579ea14bde65c9012aac65859ee1404d70c0ed655842b194b"
    }
  ],
  "bypass_interval": 300,
  "conf_version": 3,
  "custom_error_message": "For assistance, please contact Acme helpdesk at 949-555-1212, help@acme.co.com, or https://helpdesk.acme.co.com.",
  "enabled_on_uac": false,
  "group_bypass": ["group1", ".\Administrators", ".myDomain\DomainAdmins"],
  "platform": "mac",
  "store_seeds": true,
  "type": "idp",
  "version": "v2"
}
```
Sample version 1 (deprecated) (1.0.4 and earlier)

```json
{
  "version": "v1",
  "platform": "windows",
  "type": "idp",
  "api_id": "111860c9724d4c79817d1edbbccelaa",
  "api_secret": "119e3f4f8b3150f679ea14bde6589012aac65857ee1404d70c1ed655842b19aa",
  "host": "https://localhost/secureauth3",
  "access_level": 0,
  "multiple_user": false,
  "idm_ssp_url": "https://localhost/secureauth2",
  "alternate_providers": 
    
  "group_bypass": ["BypassGroup", ".\Administrators"]
}
```