Recast

Zones

Last Modified on 2026-11-11

Configure a Zone

This should be the URL with the FQDN where the targeted Application Workspace Zone is reachable.

```
{
   "zone": "https://company.liquit.com/"
}
```

For instructions on moving an agent from one zone to another, see Migrate an Application Workspace Agent to a Different Zone.

For steps to configure a custom domain, see Set Up a Custom Domain for a Zone.

Configure a Prompt Zone

This key controls the display of the Zone Prompt window where the user can configure the zone URL. The value entered in the dialog box is saved in the `zone` key.
This feature works only if there is no URL configured in the `zone` key.

Available options:

- Disabled: User is NOT prompted to enter the zone URL, even if it is not configured
- Show: User is prompted to enter the zone URL, if none is configured. This is the default value of the key.

```
{
   "promptZone": "Show"
}
```

Register a Device in a Zone

Registration creates a device in the Application Workspace zone. Typically, you will only need to complete the registration once per device. After successful registration, the device will get a Liquit Agent Authentication certificate that is tied to the device object in the Application Workspace. The device will then log into the Workspace using the certificate.

For a detailed description of registration options within Application Workspace, see Device Registration.

There are four methods to register a device within the Application Workspace. All methods apply to devices running the Application Workspace Agent.

User Account registration

For this registration method, the user account can be LOCAL or Microsoft Entra ID.

To register the device using the user account:

1. Install the Application Workspace Agent.

2. Modify the `Agent.json` file as in the following example:

```
{
   "registration": {
      "type": "User"
   }
}
```

3. Log into the Application Workspace and navigate to **Manage** > **System** > **Access policies**.

4. Assign the user an access policy that has the 'Register device' privilege. By default, the predefined **User** access policy grants this permission.

When the user logs in for the first time to the Application Workspace, the device is automatically registered.

Agent Credentials registration

To register the device using agent credentials:

1. Install the Application Workspace Agent.

2. Modify the `Agent.json` file as in the following example:

```
{
   "registration": {
      "type": "Credentials",
      "username": "local\\wksimport",
      "password": "P@ssw0rd"
   }
}
```

3. Log into the Application Workspace and navigate to **Manage** > **Identities** > **Users**.

4. Create a user with the LOCAL identity source. For example, "username": "local\wksimport" and "password": "P@ssw0rd"

5. Assign the user an access policy that has the 'Register device' privilege. By default, the predefined **User** access policy grants this permission.

The specified credentials will be used to register the device.

Agent Certificate registration

1. Choose one of three ways to complete the registration:
   - Place the certificate in the certificate repository of the Windows/Mac operating system on the device/user profile, install the Application Workspace Agent and then modify the `Agent.json` file as in the following example:

     ```
     {
        "registration": {
           "type": "Certificate"
        }
     }
     ```

   - Place the certificate in the device certificate store, install the Application Workspace Agent and then specify the `certificateThumbprint` in the `Agent.json` file as in the following example:

```
{
  "registration": {
    "type": "Certificate",
    "certificateThumbprint": "69f4db57b74e13415cd103323331d95022d840c1"
  }
}
```

- Place the certificate in the device certificate store, install the Application Workspace Agent, and then specify the `certificateIssuer` in the `Agent.json` file.

2. Log into the Application Workspace and navigate to **Manage** > **System** > **Device registration**.

3. Create a **Certificate** type registration.

4. Create or upload a certificate with a private key.

Agent Certificate Enrollment registration

1. Choose one of two ways to complete the registration:
   - Place the enrolled certificate which must have a private key on the device/user profile, install the Application Workspace Agent and then specify the `certificateThumbprint` in the `Agent.json` file.
   - Place the enrolled certificate which must have a private key on the device/user profile, install the Application Workspace Agent and then specify the `certificateIssuer` in the `Agent.json` file as in the following example:

```
{
  "registration": {
    "type": "CertificateEnrollment",
    "certificateIssuer": "Sectigo RSA Domain Validation Secure Server CA"
  }
}
```

2. Log into the Application Workspace and navigate to **Manage** > **System** > **Device registration**.

3. Create a **Certificate enrollment** type registration.

4. Select an intermediate certificate or the root CA in a certificate chain. It does not need a private key.

5. (Optional) Specify an OID, for example, to limit the number of valid certificates.

Agent certificate location

If you choose to certificate the device, the certificate must be placed in:

- Windows: Local machine certificate store (under the HKEY_LOCAL_MACHINE root).
- macOS: /Library/Keychains/System.keychain

If you choose to certificate a user, the certificate must be placed in:

- Windows: Current user certificate store (under the HKEY_CURRENT_USER root)
- macOS: ~/Library/Keychains/login.keychain-db

Keys

Key	Description	Default

Recast

Key	Description	Default
type	• *User* – The user that is currently logged on will be used to register the device with the server. • *Credentials* – The specified credentials will be used to register the device with the server. • *Certificate* – The system uses a certificate to register the device. • *Certificate Enrollment* – The system uses an erolled certificate to register the device. See Device Registration for more information.	User
username	When *type* key is set to *Credentials*, this username is used to register the device.	
password	When *type* key is set to *Credentials*, this password is used to register the device.	
certificateThumbprint	The hexadecimal string that uniquely identifies the certificate, for example: ea7f07211fddc0df73bac1437a3ff932ce*	
certificateIssuer	The authority that issued the certificate.	

When **type** key is set to 'Certificate' or 'Certificate Enrollment', the `certificateThumbprint` and `certificateIssuer` are optional settings to verify the certificate.

If the value of `certificateThumbprint` is not specified, the certificate must persist on the device in the following locations:
Windows: %ProgramData%\Liquit\Agent\AgentRegistration.cer
macOS: /Library/Application Support/com.liquit.Agent/AgentRegistration.cer
In this case, the certificate which matches the value and persists on the device, will be installed in the Windows Certificate Store or macOS Keychain and the certificate file will be removed from the device.

If the value of `certificateThumbprint` is specified, the Windows Certificate Store or macOS Keychain will be checked for a certificate with the specified value.