Recast

Settings

Last Modified on 04.16.26

The 🔧 **Settings** screen of the Application Workspace Satellite Server allows you to configure the following options that are used for all zones:

URL – This URL is used by the Application Workspace Servers to connect to this Application Workspace Satellite Server. When pairing, this URL is registered within the `Server` object of the Application Workspace zone.
Name – The default name of the Application Workspace Satellite Server that will be used when pairing a zone. It can be changed anytime after pairing within the zone.
Use ACME for automatic certificate renewal – With the Automatic Certificate Management Environment (ACME) client you can automatically request and maintain TLS certificates. If the option is enabled, additional options are displayed:
Provider – At this moment, only "Let's Encrypt" and "Google Trust Services" are supported. The requested certificate is valid for 90 days. After 60 days, a new certificate will be requested.
External Account Binding Key ID – The API key, a component of the EAB secret that enables your certificate requests to be associated with your Google Domains account.
External Account Binding HMAC Key – The hash-based message authentication code, a component of the EAB secret that enables your certificate requests to be associated with your Google Domains account.

> Google Trust Services
> For more information about Google Trust Services and how to generate the EAB keys, see Google Cloud documentation.

Contact email addresses – The email addresses of the ACME account where ACME errors will be mailed.

Request certificate – It becomes available once you finish filling in all the mandatory fields on this screen and click **Save**. The certificate status details are automatically displayed after you refresh the session.

The **Check ACME certificates** predefined scheduled task checks every day if the ACME certificates need to be renewed.

The ACME client uses a certificate itself for authenticating against a provider, this certificate can be found under **Settings** after the first certificate has been requested. The requested certificates including the chain are stored at the same place.

Important notes
The provider will check if the zone name belongs to the requester. For this check to be successfully completed, the following requirements must be met:

- The DNS name of the domain must be resolvable on the internet to the Application Workspace System. By default, it uses the local IP.
- The Application Workspace System must be accessible over port 80 from the internet.
  Redirects from HTTP port 80 to HTTPS port 443 are allowed when the redirects include the original request path. For example: *http://workspace.liquit.com/.well-known/acme-challenge/[token]* redirects to *https://workspace.liquit.com/.well-known/acme-challenge/[token]*. HTTPS port 443 is not required to have a valid SSL certificate, the ACME challenge mechanism will not validate any certificate.
- If HTTPS is configured but no certificate is found (and no ACME certificate is available), the system will automatically generate a self-signed certificate and assign it to the server.
- A success or failure message will be displayed upon certificate request or renewal.