Recast

Domains

Last Modified on 04.16.26

Domains allow you to configure additional domains (Virtual Hosts) to be accepted by a single zone. This allows custom branding of the portal based on the domain that is used to connect to the zone. This is also useful in case of company name changes to accept both the new and old during a migration period.

The default domain is always present and cannot be removed.

> Changing the virtual host of the default domain
> The virtual host of the default domain can only be changed with system permissions.
> The license will become invalid after changing the default domain and will cause downtime until the license has been updated with the new domain.

Here you also add the HTTPS Webserver certificates for your non-primary zones.

Domains list

This list displays all domains currently added to the Application Workspace System.

Selecting multiple rows from the table

- To select multiple adjacent rows, click on the first row, then hold down the Shift key and click on the last row in the range; all rows between will be selected.
- To select multiple non-adjacent rows, hold down the Ctrl key (or "Command" on Mac) and click on each row you want to select individually.
- To select multiple adjacent rows using the mouse only, click and hold the left mouse button on the first row, then drag the cursor up or down across the rows to highlight the desired ones.
- Selecting rows using only the keyboard is not possible.

Table toolbar

To add a new domain, click on the **Add** button; to view the details of a domain or edit it, double-click its entry or select the domain and click the **Edit** button.

The **Request certificate** button is available only for domains that have the **Use ACME for automatic certificate renewal** option enabled. It gives you the possibility to directly renew the certificate throught ACME, if you don't want to wait for the designated scheduled task to run and check for new certificates.

Edit domain dialog box

Details tab

Default – When checked, this is the default domain of the Zone.
Enabled – Whether or not the domain is enabled and usable.
Virtual host – Virtual host of the domain.
Description – Detailed description of the domain.

Certificate tab

Transport Layer Security (TLS) secures the connection between the user and the workspace.

You can have trouble reaching a zone if a zone certificate expires andHTST is enabled. Consult your browser documentation to learn how to remove the HSTS state in the browser for the zone domain.

You can select only a certificate that contains a private key. While not necessarily, it is best practice to only use certificates which have the full certificate chain imported. By default, HTTP.sys (part of the Windows OS) allows the usage of insecure/obsolete protocols, cyphers, key exchange algorithms and hashes for maximum compatibility. As this allows a wide range of browsers to interact with the web server, it also opens potential opportunities for TLS attacks. For hardening the TLS security, see: TLS Hardening.

ACME client

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, seeGoogle Cloud documentation.

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

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**Manage** > **System** > **Certificates** after the first certificate has been requested. The requested certificates including the chain are stored at the same place.

Requirements for ACME usage
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.
- 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.

Certificate

If the **Use ACME for automatic certificate renewal** option is not selected, then the**Certificate** field is displayed where you can select a certificate to secure the webserver. When you click on the browse button ... at the right of the lookup field, the **Certificate** dialog box opens, where you can view all the certificates available. If the certificate is not present in the list, you can add it by following the steps described in the Certificates article.

Auditing tab

Recast

View a comprehensive log of changes to this domain, displaying the identity behind each modification.
This screen is available only if the auditing is enabled in the Database Event Collector. For more information, see Auditing.

Further reading

Use your own company domain name as virtual host
How to configure SSO with Microsoft Entra ID (Azure AD)