Application Workspace Satellite

Last Modified on 2026-06-30

Install Application Workspace Satellite Server

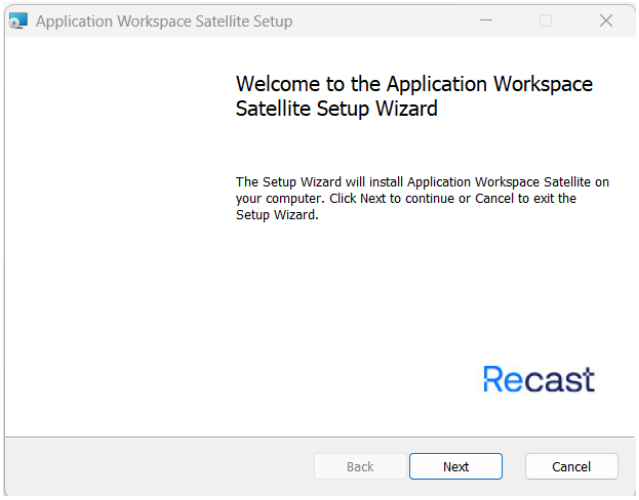
The Application Workspace Satellite Server is distributed as a Microsoft Installer (MSI) which you can find on our Downloads page.

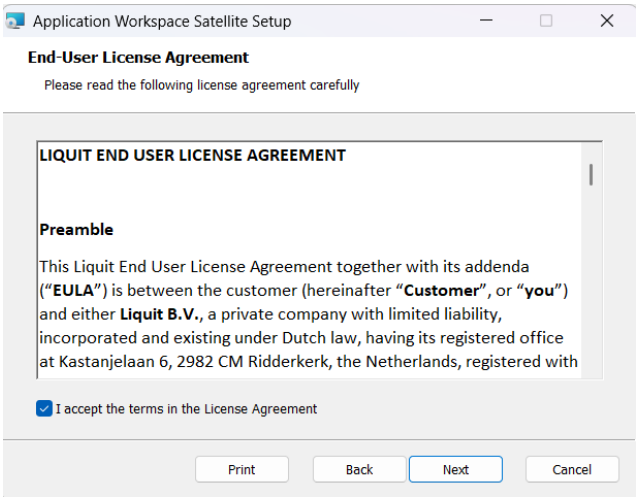
Prerequisites

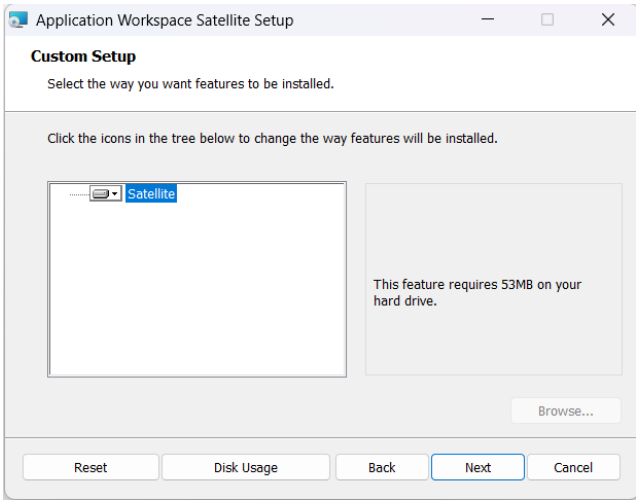
Note that Application Workspace Satellite Server is a web server and any existing services running on port 80 or 443 will cause conflicts.
To guarantee that the web version and Application Workspace Launcher of the Application Workspace work properly, a certificate supplied by Recast must be installed on the local PC. See HTTPS (Webserver certificates) for more information.

To install an Application Workspace Satellite Server:

1. Run the Application Workspace Satellite Setup Wizard, clicking **Next** in the Intro, End-User License Agreement, and Custom Setup windows.



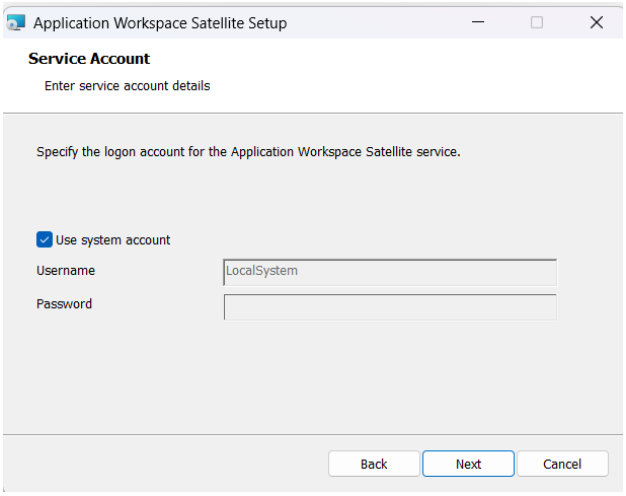




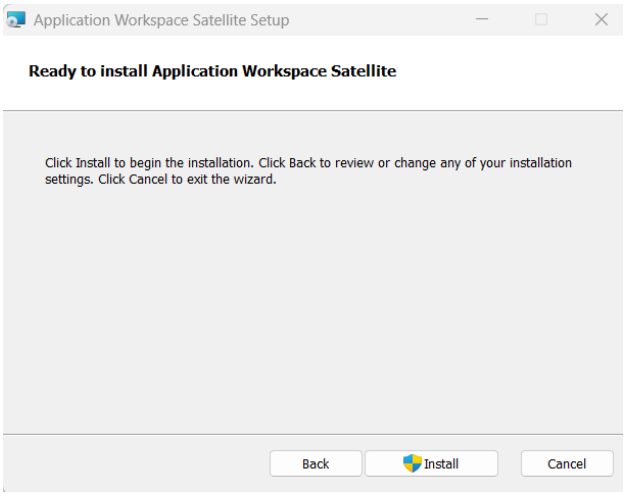
2. In the **Service Account** window, provide the credentials for the Application Workspace Satellite Server Service, which will be used for database connectivity and/or for securing access to the Content Store.

You can choose to use Windows Authentication or insert your credentials.

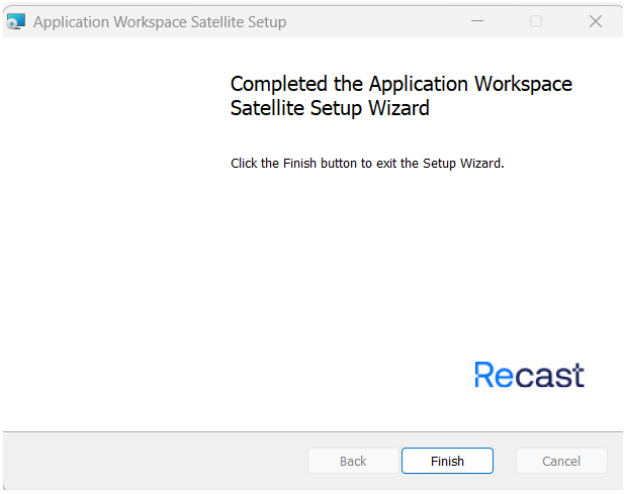
> If you provide custom logon account credentials, make sure that this account has “Log on as a service” rights as described in Add the Log on as a service Right to an Account | Microsoft Learn



3. In the **Ready to install Application Workspace Satellite Server** window, click **Install**.



4. After the installation is successfully completes, click **Finish** to exit the Setup Wizard.



Now that the Application Workspace Satellite Server is installed, you can access it using a web browser on `http://localhost/`

For more information about how to access the Application Workspace Satellite Server for the first time and how to start using it, see Configure Application Workspace Satellite.

Silent install of Application Workspace Satellite Server

Syntax

```
msiexec /i Application-Workspace-Satellite.msi /qn
```

MSI installation properties

The following MSI installation properties are supported (all property names should be in upper case):

Property	Description	Values
CONTENTS_PATH	Sets the path in the `Contents` section of the `Satellite.json` file. The path is used by the Liquit Content Store to store the contents.	By default it is `C:\ProgramData\Liquit Workspace\Satellite\Content`

Property	Description	Values
SERVICE_SYSTEM	Use system account.	0 – FALSE 1– TRUE
SERVICE_USERNAME	In case you provide a logon account, the username of that account.	
SERVICE_PASSWORD	In case you provide a logon account, the password of that account.	

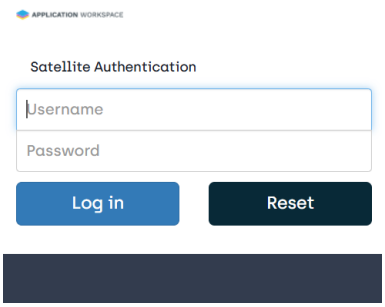
If you provide custom logon account credentials, make sure that this account has “Log on as a service” rights as described in Add the Log on as a service Right to an Account | Microsoft Learn

Configure Application Workspace Satellite

Default user

After installing the Application Workspace Satellite Server, you can access it using a web browser on `http://localhost/`.

The following login screen will be displayed:



The default username is 'admin' with an empty password.

Connectivity

All Application Workspace Servers that belong to a zone need to be able to directly connect to an Application Workspace Satellite Server. We recommend you set up the connectivity using a DNS record. By default, the Application Workspace Satellite Server will register itself with its local IP address. To change this, the URL can be reconfigured on the Settings page to include a proper DNS name instead of an IP address.

Pair zone

A zone can be paired after configuring the SSL certificate and theconnectivity URL for the Application Workspace System.
See Zones for more information on how to pair an Application Workspace System so it can be used by connectors.

Recast

Satellite JSON

`Satellite.json` is the configuration file of the Application Workspace Satellite Server.

It's default location path is `C:\Program Files (x86)\Liquit Workspace\Satellite`

The config file is always specific to a single server so we recommend you do not copy it to another server unless you want to migrate an existing Application Workspace Satellite Server installation to a new server.

> The values in a JSON file should always be escaped. For example, `C:\temp` should be `C:\\temp`.

Example of a complete Satellite.json configuration

```
{
  "log": {
     "level": "Info",
     "path": "Satellite.log",
     "rotateCount": 5,
     "rotateSize": 5242880
   },
  "redirect": true,
  "database": {
     "path": "Satellite.db",
     "compress": true
  },
  "contents": {
     "enabled": true,
     "cache": true,
     "replication": true,
     "concurrent": 8,
     "interval": 5,
     "path": "Content"
  },
  "listeners": [
  {
     "required": true,
     "address": "*",
     "port": 80,
     "offloadingPort": 443
  },
  {
     "required": true,
     "secure": true,
     "certificate": "Satellite",
     "address": "*",
     "port": 443
  }
  ]
}
```

Example of objects you can use in a Satellite.json config file

Log

Recast

The Application Workspace Satellite Server logs events that are initiated.

```
"log": {
   "level": Info,
   "path": "Satellite.log",
   "rotateCount": 5,
   "rotateSize": 5242880
  }
```

Property	Description	Default value
level	Defines the level of logging: • **None** Nothing will be logged to the log file • **Critical** only critical errors will be logged to the log file. • **Error** Only errors and critical errors will be logged to the log file. • **Warning** Only warnings, errors and critical errors will be logged to the log file. • **Info** Basic information and warnings, errors and critical errors will be logged to the log file. • **Debug** Detailed information will be logged to the log file about all actions. You can use this information when troubleshooting.	Info
path	You can define an alternate path of the Agent log files here.	C:\ProgramData\Liquit Workspace\Satellite\Logs
rotateCount	The number of log files that will be archived.	5
rotateSize	The limit of log file size in bytes. When this limit is reached, a new log file will be created and the old file will be archived.	5242880

Redirect

When set to true, the server will redirect incoming insecure requests to the secure port (by default 443), as configured within the listeners. When set to false, the server will NOT redirect insecure requests.

```
"redirect": true
```

Database

```
"database": {
   "path": "Satellite.db",
   "compress": true
  }
```

Property	Description	Default
Path	The path to the database.	Satellite.db
Compress	If enabled, the database is compressed in the gzip format.	true

Contents

Defines how the Application Workspace Satellite Server should handle its content.

```
 "contents": {
   "enabled": true,
   "cache": true,
   "replication": true,
   "concurrent": 8,
   "interval": 5,
   "path": "Content",
}
```

Property	Description	Default
cache	Defines whether or not the content of files that are smaller than 1 MB should be cached in memory.	true
replication	Enables the replication of the local server content across Application Workspace Satellite Servers.	true
Concurrent	Nr of workers to replicate content (how many files can be synched in parallel.	5
interval	The number of seconds between idle checks performed to see if any content needs to be replicated.	5
path	The path where contents are stored. The path is relative, but can be absolute.	C:\ProgramData\Liquit Workspace\Server\Content

Listeners

The listeners property defines which IP and/or ports Application Workspace will receive and handle requests.

```
"listeners": [
   {
    "required": true,
    "secure": true,
    "certificate": "Satellite",
    "address": "*",
    "port": 443
   }
 ]
```

Property	Description	Default
required	When the required value is set to true, the Application Workspace Satellite Server will not continue to start up when it can't be registered	false
secure	This option is overruled by the certificate option, if a certificate is set then this option will be handled as being set to true. Only required/needed if customers uses TLS Termination / Offloading	
certificate	The friendly name of the certificate Application Workspace Satellite Server should use. SSL/TLS is only used when this property has a value set.	
address	The address of the Application Workspace Satellite Server. Wildcards (*) are permitted.	*
port	The port used by the Application Workspace Satellite Server to receive and handle requests..	80
offloadingPort	Indicates that the listener is HTTPS offloaded (TLS termination). The webserver will use an HTTP listener but will handle incoming traffic as secure.	0

Zones

Recast

The **Zones** screen allows you to create and manage zone registrations within the Application Workspace Satellite Server.

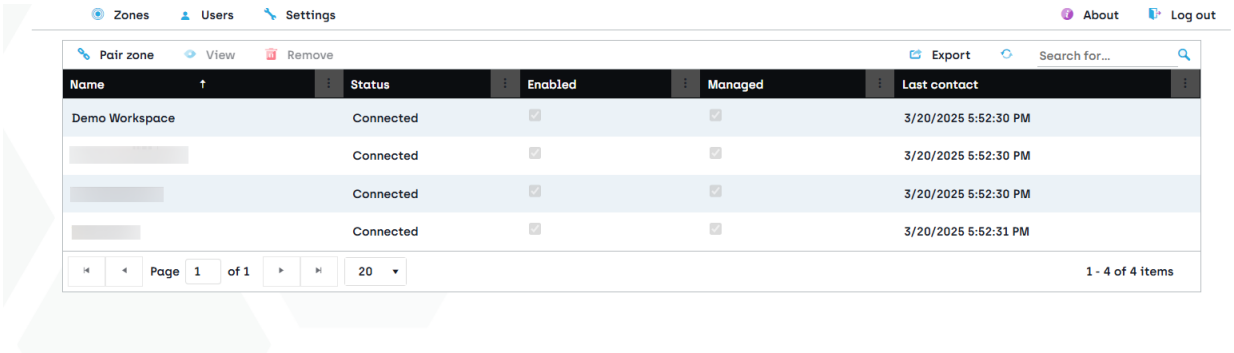
Zones list

This table displays all the zones to which the current satellite server is paired and the following information:

Status – The current state of the zone paired with the satellite server.

- *Registered* – The pairing of the satellite server is pending and it can't be used for the moment.
- *Paired* – The satellite server is paired, but no connection is established between this satellite server and servers within the zone.
- *Connected* – 1 or more servers are currently connected to this satellite server.

Enabled – Shows if the access of the satellite server to the zone is enabled or not. To change it select the desired zone and click **View**.
Managed – If the checkbox is selected, then the zone is allowed to modify system settings on the satellite server. For example, this is required to allow the installation of satellite server updates.
Last contact – The last time when a server within the zone has established a connection to this satellite server.



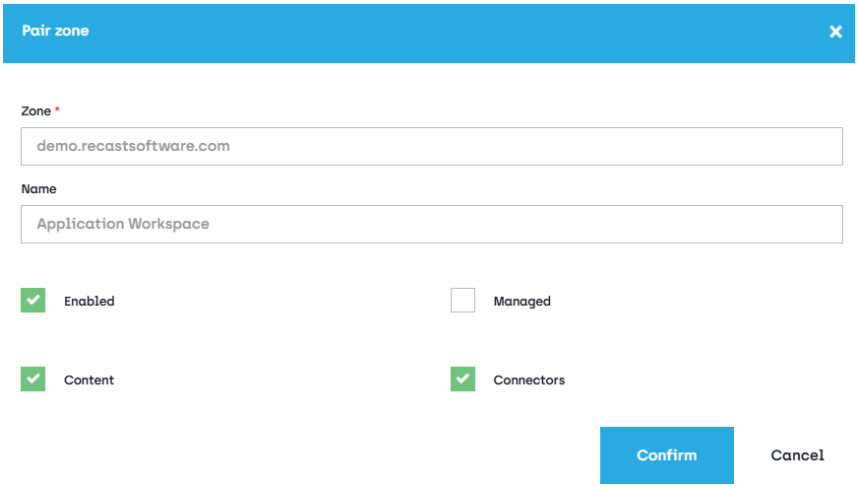
From the table toolbar, you can access the **Pair zone** or **View** all of which are described in the following sections.

Pair zone

You need to pair the Application Workspace Satellite Server to a zone, to use the satellite server in the respective zone.

The following options are available:

Zone – The URL of the zone to pair with, for example `https://demo.recastsoftware.com`. This is used to register the local satellite server within the specified zone.
Name – The name used to identify the zone paired with the local satellite server.
Enabled – When enabled, the zone can use the local satellite server after pairing.
Managed – If enabled, administrators within the zone are allowed to update the local satellite server from within the Application Workspace Portal.
Content – If enabled, the local satellite server can be used for hosting content for the zone.
Connectors – If enabled, the local satellite server can be used for hosting connectors for the zone.



View

Opens the detailed view of the selected zone, with the following screens:

Zone screen

Here you can change the name of the zone, enable/disable it or enable/disable the**Managed** option.

Servers screen

Displays an overview of servers that host the remote zone and are known by the satellite server. Only servers that are currently or have been previously connected are listed here. The satellite server's functionality doesn't depend on knowing all servers.

Content screen

Displays an overview of usage and statistics for content replication for the zone to which the satellite server is paired. These results are also replicated periodically in the zone where this information is accessible as well.

Replication mode – Shows how the content is replicated from a primary server to the satellite:

- **Disabled** – Files related to the current zone are removed from the satellite server.
- **On-demand** – Content is downloaded from primary servers to the satellite server when an Agent requests it. When multiple Agents request the same content, the satellite server will download it once and immediately stream it to all the Agents.
- **Synchronized** – All zone content is replicated periodically. If content is no longer available within the current zone, it is also removed from the satellite server. During synchronization, the on-demand feature is also enabled, giving the highest priority to the agents' requests.

Total – The total number of content entries needed by the server.
Queued – The number of content files that are queued to be downloaded to this server.
Progress – The number of content files currently being downloaded to this server.
Available – The number of content files that are available for use on this server.
Unavailable – The number of content files that failed to download. The server will re-attempt to download them at the next synchronization.
Total size of local content – The total size of local content that is available for use.
Total size of needed content – The total size of local content that is required to be replicated to this server.

Notes
The content stored on the local satellite server is deduplicated among zones.
To learn more about how content replication can be further configured and controlled from within the zone,

> see Servers.
> Use the Content Access feature to configure Agents to connect to the satellite server for content distribution.

Connectors screen

An overview of the connectors hosted by the satellite server for this zone.

Further reading

How to pair a zone

Users

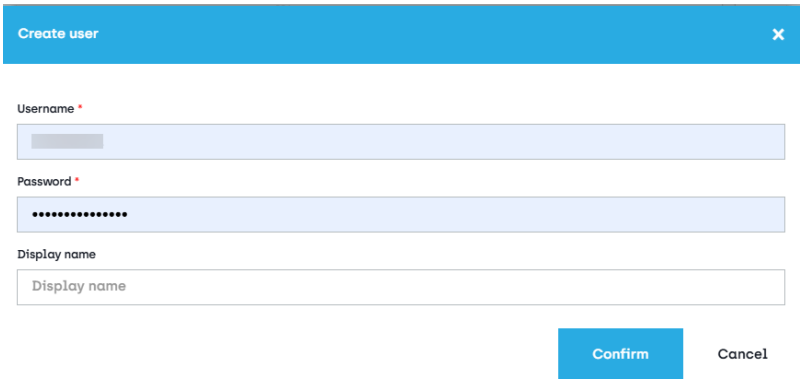
The **Users** screen displays all the existing users within the Application Workspace Satellite Server and allows you to manage them or create new ones.

To edit or disable a user, select it and then click **View** in the table toolbar.

Create user dialog box

The following basic options are displayed:

Username – The name used to authenticate the user.
Password – The password used to authenticate the user.
Display name – A friendly name used to identify the user.



Settings

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.

HTTP.sys Logfiles

Application Workspace uses the HTTP.sys web server of the Microsoft Windows operating system for handling the incoming HTTP(s) requests. By default, HTTP.sys logs errors in the `%windir%\System32\LogFiles\HTTPERR` folder. You need to have administrative rights to access the log files.

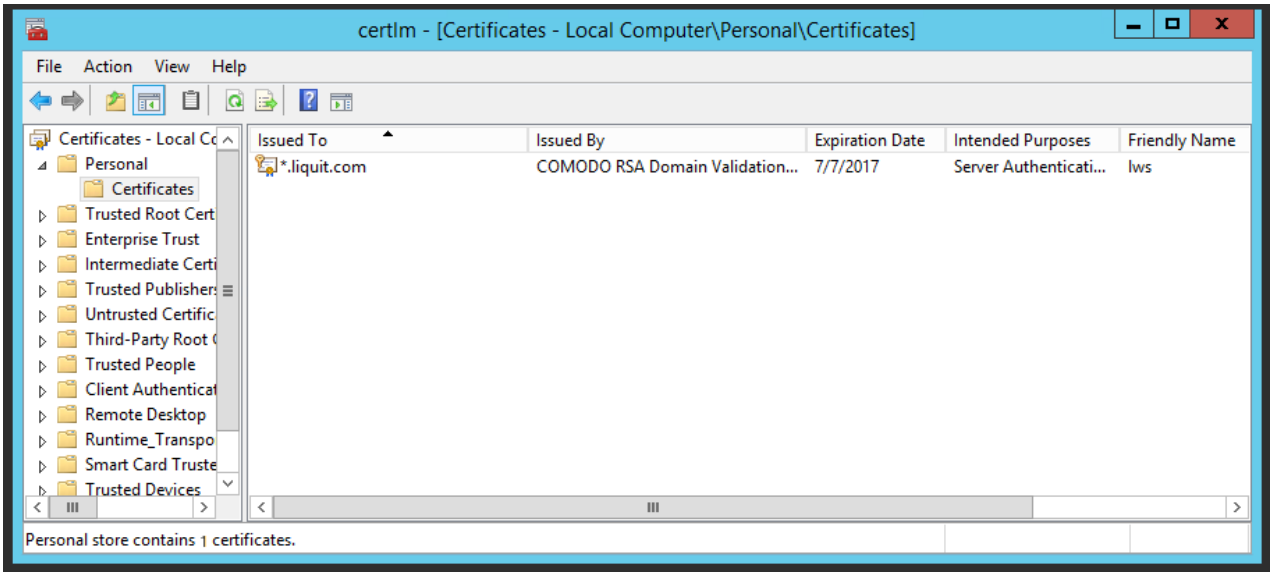
For more information about configuring the HTTP server API error logging, see Microsoft documentation.

HTTPS (Webserver certificates)

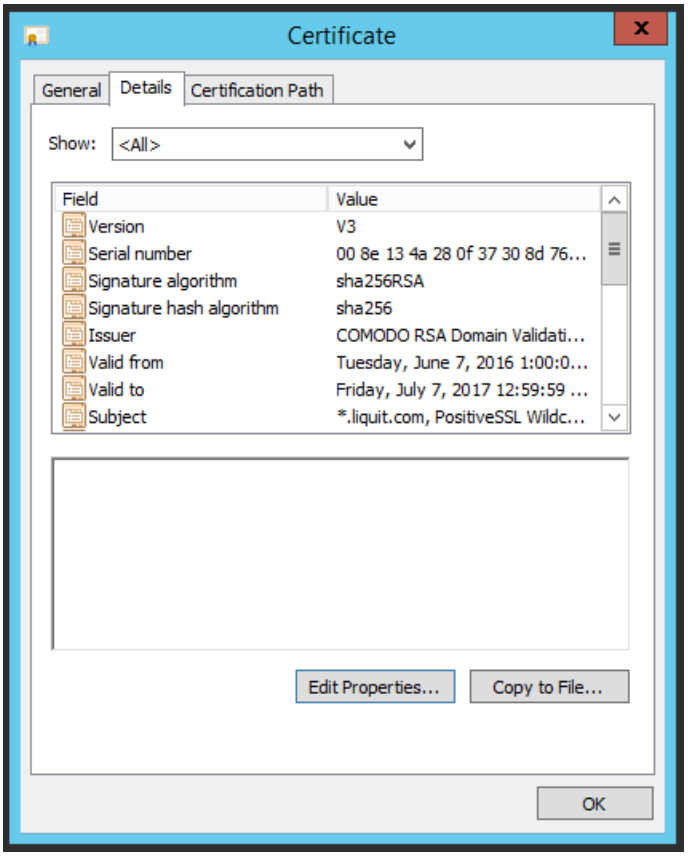
To ensure the correct operation of Application Workspace' web version and Launcher, it is essential to have your own certificate on the local machine.
This article describes the steps of adding this certificate to your primary zone. For non-primary zones and domains, the corresponding certificates can be added via Application Workspace, in Domains.

For the purpose of this example, we will use a `*.liquit.com` certificate.

1. Import the certificate in the personal folder of the local machine on Windows (certlm.msc).

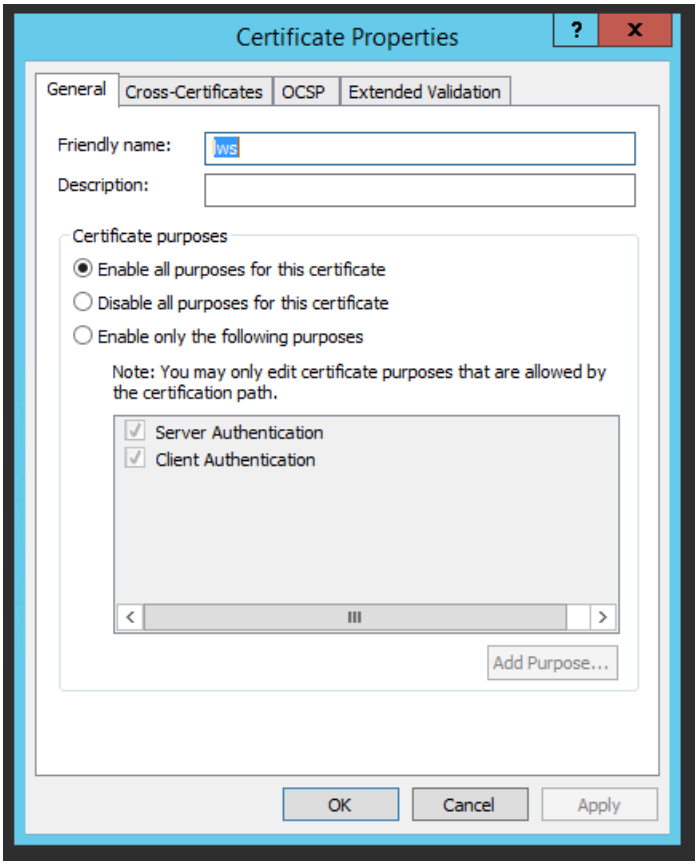


2. Open the certificate and navigate to the **Details** tab.



3. Click **Edit Properties**.

4. In the **General** tab, edit the value of the **Friendly name** field to "lws". This way Application Workspace can automatically select it on startup of the Application Workspace Server service and activate SSL support.



5. Restart the Application Workspace Server service to apply the SSL certificate.

Application Workspace Satellite Server Logging

Log file locations

Application Workspace Satellite Server logs are located at `C:\ProgramData\Liquit Workspace\Satellite\Logs`.

Enabling debug logging

In case of troubleshooting, you need to enable the debug logging feature by modifying the `Satellite.json` configuration file.
This config file is located in the `C:\Program Files (x86)\Liquit Workspace\Satellite` folder.
Within the `Satellite.json` configuration file, change the `level` key of the `log` object from "Info" to “Debug”:

```
"log":{
   "level":"Debug"
}
```

Restart the Application Workspace service to activate the debug logging.
After restart, check the `Satellite.log` file to verify if the log level is set to debug.

Anti-Virus recommendations

The following paths (including their subfolders) should be excluded from file scanning and on-access scanning:

`%ProgramFiles(x86)%\Liquit Workspace\Satellite\`

Recast

`%ProgramData%\Liquit Workspace\Satellite\`

Our recommendation arises from the following consideration: this component's actions are characteristic of legitimate and malicious software. Consequently, antivirus software may misinterpret these legitimate operations as potential threats, leading to unnecessary alarms and performance degradation.

Firewall settings

The built-in Web Server running on port 80/443 (default) needs to be accessible externally.

Application Workspace also supports direct access to get content directly from the Azure Blob storage. In case your Application Workspace System is hosted on Recast Software's cloud infrastructure and you configured an on-premise Application Workspace Satellite Server you need to configure the firewall to allow the content URIs. To see theURIs, navigate to **User Portal** > **Device** > **Content Access.**