Recast

Known Issues

Last Modified on 2026-11-10

Known issues with suggested workarounds, where available

Apps greyed out after Edge update

Starting with Microsoft Edge version 143, which introduced the Local Network Access feature, when accessing the Application Workspace URL you may see a prompt stating: '[domain] wants to look for and connect to any device on your local network.

If you **Block** access, applications in Application Workspace appear as greyed out.

Selecting **Allow** resolves the issue and adds the URL to Edge's allowed list under **Privacy, search, and services** > **Site permissions** > **All permissions** > **Local network access**.

You can also configure this setting via Intune using a configuration profile. For more details, see Configure Microsoft Edge policy settings with Microsoft Intune and LocalNetworkAccessAllowedForUrls.

Favorite icon disappears after sorting

When adding a new icon to your favorites and then sorting the list, the newly added icon may disappear due to a sync delay with the server. This behavior is a known issue, and a fix will not be provided due to system limitations.

AW fails to run on macOS 15

Currently, when trying to run Application Workspace on a device with macOS version 15, the following error message appears in the debug log:
"Failed to update current trust settings, exit code: 255"

Workaround
You can import the certificate manually, as a root certificate through an MDM solution.

Agent update package loop on macOS

When creating an update package to upgrade the Application Workspace Agent on macOS using an action set with frequency "Once per device" and an action to install the uploaded .pkg file, the agent updates successfully but does not record the installation status.

Because an external process restarts the Agent during installation, the Agent does not recognize that the update was completed. This can cause the update package to run repeatedly, resulting in an indefinite loop.

Status
The issue is under investigation. Currently, there is no workaround.

Recast

Options are visible when they should not be

Because device-based filters configured at the context level can take longer to apply, options that should not be visible can be visible, although the access policy is applied correctly.

Workaround
To update the interface, refresh the page.

Environment variables not updated in real-time

Application Workspace will use environment variables and their value from the start of the Universal Agent (Application Workspace Service) and will not update the values while running. If filters, actions, and processes use environment variables Application Workspace will use the startup values and not the current values. Only environment variables and the value changed with the actions "Set environment variable" or "Unset environment variable" will be updated. New environment variables that did not exist during the start will be picked up.

Error when viewing dashboards in AW Launcher

Known Issue:

When you view the dashboards in the Application Workspace Launcher, you are prompted to upgrade to a different browser.

Workaround:
For the best experience, we recommend accessing dashboards using a web browser.

FaultException Invalid user session

Possible cause: A session that is stuck in the database.
A session object may become stuck, which could prevent a user from logging in.

Workaround:

> This workaround will delete all user sessions and all the users will be logged out forcibly.

1. In Application Workspace, navigate to **Automation** > **Scheduled Tasks** and open the *Clean Sessions* task.
2. Navigate to the **Settings** screen. Set the number of hours to 0 (zero).
3. Navigate to the **Schedule** screen. Delete the default interval of 5 minutes.
4. Run the task. You will be logged out while the task runs because also the current user session is being deleted.
5. Log back into Application Workspace and navigate back to the *Clean Sessions* task.

6. Navigate to the **Settings** screen. Set the number of hours back to 8, the default value.

7. Navigate to the **Schedule** screen. Add an interval of 5 minutes. This is the default value.

Firefox unable to communicate with Recast Agent

Firefox is unable to communicate with the Recast Agent, Cross-Origin-request blocked

Possible cause: Firefox doesn't trust the certificate of the Agent.
Firefox doesn't use the Windows Certificate Store for validating certificates. This could cause Firefox to not trust the Agent certificate.

Workaround 1: Import the Agent certificate in Firefox.

The location of the certificate on Windows is:

- Workspace Agent: `C:\Program Files (x86)\Liquit Workspace\Agent\Agent.pfx`
- Universal Agent: `C:\Program Files\Liquit Universal Agent\Resources\Agent.pfx` .

The password for this file is "agent" without quotes. It is also available in the Windows Certificate Store under the friendly name "LWA".

Workaround 2: Create the following registry key `HKEY_LOCAL_MACHINE\Software\Policies\Mozilla\Firefox\Certificates\ImportEnterpriseRoots` with DWORD value of "1" to let Firefox automatically import the trusted certificate roots from the Windows Certificate Store. This is supported by Firefox starting version 60 and later.

Installation files not cleaned after failed install

Workaround
You have to manually clean the Windows temporary directory or create a package with the `${TempDir}` that cleans it for you.

NTLM/Kerberos does not work

Possible cause 1: The integration with Active Directory will use the Identity Source name as a realm.
The realm name for NTLM/Kerberos must match the Active Directory NetBIOS name before single sign-on could work.

Workaround: Make sure the Identity Source for Active Directory name is matching the NetBIOS name of Active Directory.

Possible cause 2: Internet Explorer will only engage an NTLM/Kerberos handshake if the visited site is listed in the trusted zone list.

Workaround: Make sure the Application Workspace Zone is listed in the trusted zone list of Internet Explorer.

Possible cause 3: The Kerberos token exceeds the allowed size.
Note: Application Workspace makes use of the HTTP.sys that is provided with Windows.

Workaround: Follow the steps in HTTP 400 Error Responses to HTTP Requests – Internet Information Services | Microsoft Learn.

Recast

Satellite Server UI Unresponsive

Summary

The satellite server user interface (UI) may become unresponsive or fail when invalid or broken inputs are entered on the Settings page during ACME configuration.

Symptoms

• Error dialogs appear during or after configuration.
• Login functionality stops working after the user logs out.
• In severe cases, the satellite UI becomes inaccessible.

Root Cause

This issue occurs when certain input values are entered in the ACME settings, which can corrupt configuration files and impact the satellite's ability to interact with its database.

Impact

• Users may be unable to log back in after logging out.
• The satellite server may require a full reinstallation, including its database.

Resolution

Report this issue to Support immediately for assistance.

Include the following details in your report:

• Steps taken before the issue occurred.
• Screenshots of error dialogs.
• Any relevant logs from the satellite server.

> Do not attempt manual fixes unless instructed by Support, as this may worsen the problem.

Server installation ends prematurely

This generally indicates that there was an issue while trying to upgrade the database schema.
To assist us in finding the issue where this problem occurred, we need the debug logging of the installation.

Workaround:
After restoring the database, re-install the Application Workspace Server with the following command-line prompt:

```
msiexec /i Liquit-Workspace-Server.msi /l*v setup.log
```

Send the resulting `setup.log` file to the Recast support department, so we can investigate what is causing the installation to end prematurely.

Recast

SharePoint: Embedding content not allowed

Users may receive the following message when they try to add an iframe containing Application Workspace to SharePoint: "Embedding content from this website isn't allowed."

Workaround:
Allow embedding content from a specific list of sites:

- Browse to the root site of your site collection.
- Click on the settings gear > click **Site Information** link > **View all site settings**.
- On the **Site settings** page, under **Site Collection Administration**, click **HTML Field Security**.
- Select one of the following options:
  Allow contributors to insert iframes from any domain
  Allow contributors to insert iframes only from the following domains (if you choose this option you need to add the Application Workspace URI to the list).
- Click **OK**

Unexpected database error during login

Possible cause: The Application Workspace Server is unable to reach the database.
It is important that all Application Workspace Servers have a reliable network connection to the database to perform correctly.

Workaround

- Check the `connectionString` parameter in the `Server.json` file.
- Ping the address specified in the `connectionString` parameter with the name "Data Source".
- Check the server log files for database errors.

Possible cause: The event table has reached the maximum amount of records supported.
Application Workspace affected versions: 3.0 and later

Especially in older versions with the Application Workspace Server, it is possible that the event table in the database has reached the maximum amount of records supported. This can happen if the task for cleaning events hasn't run or is configured to retain too many days of events. We recommend for large deployments to not set the retention period for more than 30 days.

Workaround

> This workaround will delete all existing events.

- Log into the Application Workspace database using an SQL client, like Microsoft SQL Server Management Studio.
- Execute the following SQL query on the database:

```
TRUNCATE TABLE [Events];
```

UserHost not found for session

Possible cause 1: The UserHost is not running.

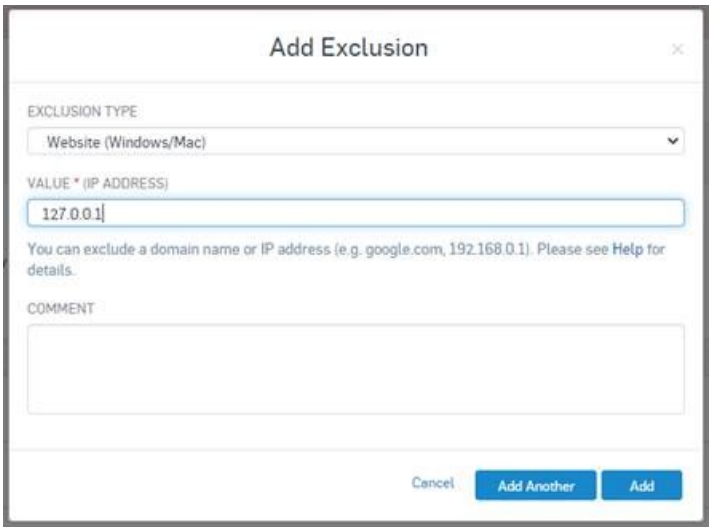
Workaround: Make sure the UserHost is running correctly and is not elevated.

Possible cause 2: Firewall software intercepts all localhost connections.

symptoms:

- The specified session is 0 (system)
- In the agent debug log files the origin process is 'swi_fc' (Sophos endpoint security)

Workaround: Make sure that the firewall software doesn't intercept lost host connections. For Sophos endpoint security, you can add a global exclusion for IP address 127.0.0.1:



For more recommended settings, see Anti-Virus recommendations.

User settings color slide issue

Click twice on the color slider and the number will stay if you click away fast.