Common Privilege Manager Issues

Last Modified on 05.23.23

Use these generic troubleshooting steps to detect and resolve common Privilege Manager issues.

Client troubleshooting

1. Verify that **Gateway address** and **Computer domain** (computer domain must be computer NETBIOS name for workgroup or Azure AD joined computers and DNS name of the on-premises AD for AD joined computers) are correct in following registry locations (first location available is used by the client):
    - HKLM\SOFTWARE\Policies\Recast\Agent
    - HKCU\SOFTWARE\Policies\Recast\Agent
    - HKLM\SOFTWARE\Recast\Agent
    - HKCU\SOFTWARE\Recast\Agent
2. If the **Gateway Address** or **Computer domain** are not correct then correct values must be set by manually editing registry or by modifying GPO targeted to computer.
3. Verify using the browser **Gateway Address** URL from step 1 can be accessed.
4. If the **Gateway address** cannot be opened by browser verify DNS name resolving and network connection to URL.
5. Check if errors are logged to the Windows Event Log under Application logs from the client.

IIS server troubleshooting

1. Verify that **IIS** is up and running and all web sites and application pools are running.
2. Check logs on App_data folders of Recast Agent Gateway and management portal websites for error reason.
3. Verify **ConnectionString** setting from web.config files in root of Recast Agent Gateway and management portal websites.
4. Verify that the connection to SQL database configured in ConnectionString setting can be opened from the server (DNS name resolving and TCP/IP connectivity check).

SQL instance troubleshooting

1. If **ConnectionString** setting in step 3 of Perform on IIS Server is configured to use SQL authentication then verify that the specified SQL login can access the SQL instance, otherwise verify that user account running IIS application pools on step 1 of Perform on IIS server can access the SQL instance.
2. Check the SQL server instance logs for the connection error reason.
3. Verify that the database is up and running.
4. Verify that the SQL login from step 1 has the user in the database and they have a Portal role and/or roleGateway roles.