Proficy Plant Applications 2022

Troubleshooting Guide

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Contents

Chapter 1. Troubleshooting Guide

Introduction

This Troubleshooting Guide is intended for operators, supervisors, administrators, and other users of Plant Applications.

This guide helps the user to troubleshoot the issues related to Plant Applications Installation, Plant Applications Web Client, and Plant Applications Administrator. It includes the information on how to diagnose and troubleshoot various common issues the user may encounter in Plant Applications.

This guide has the following sections:

Prerequisites

Refer to Plant Applications Server and Client Requirements *(on page)* before you attempt to troubleshoot an issue.

Troubleshooting Install Issues

Issue: SSL Certificate not updated

An SSL certificate allows you to access Enterprise Edition Web Client using HTTPS. You can either use a self-signed certificate or get a trusted certificate from a Certificate Authority (CA).

You must use `utility.sh` located at `plantapps-enterprise-webclient-<buildno>` folder to apply the certificate. If the certificate is not updated correctly, navigate to `<Install file path>/plantapps-enterprise-webclient<buildno>/log/ansible.log` to see the log files.

Refer to the below table, for issues related to certificates and corresponding resolutions.

Issue	Reason	Resolution
If utility fails	Not a valid path	1. Verify if the path for the below parameters mentioned in **silentinstaller.yml** are correct: • `SSL_CERT_PEM_PATH: ""` • `SSL_KEY_PEM_PATH: ""`

Issue	Reason	Resolution
		2. Ensure that the certificates are copied to the path mentioned in **silentinstaller.yml** 3. Restart `utility.sh`. **Note:** If the Certificate is signed by Enterprise CA, then it should contain all certificate levels: the Root CA, the Intermediate Enterprise Certificate, and the Server Certificate.
	Expired certificate	Replace the expired certificate with the new certificate. If UAA certificate is expired, refer to: Replace the Public Keys of Remote Services *(on page)*. If Web Client certificate is expired, refer to: Replace the SSL Certificate of Enterprise Edition Web Client *(on page)*.
Certificate not reflecting in the Web Client	Self-signed certificate is not updated, or the certificate is expired	This issue is fixed in PA2022. The `PApamymachinesservice` stack was not removed which prevented the certificates to be configured properly. You must remove the `PApamymachinesservice` stack by running the command: `sudo docker stack rm PApaMymachinesservice` For more information, refer to: Replace the Public Keys of Remote Services *(on page)* and Replace the SSL Certificate of Enterprise Edition Web Client *(on page)*.
Un-authorization error	Proficy server certificate failed	Access the **access control service** and check for the PKIX errors, if found:

Issue	Reason	Resolution
		• Run the command: `sudo docker service logs PAAccesscontrolService_accesscontrolservice` • Restart `utility.sh` to trust the certificate.
HAProxy error	Web Client application not accessible	To verify the logs, run the command: `sudo docker service logs PAHapoxy_haproxy` and check for the HAProxy error: *[ALERT] (8) : config : parsing [/usr/local/etc/haproxy/haproxy.cfg:34] : 'bind *:5059': No Private Key found in '/usr/local/etc/haproxy/haserver.pem.key'* To troubleshoot the HAProxy error: 1. Update the following parameters in **silentinstaller.yml** : • `SSL_CERT_PEM_PATH:"/docker/pathto/server_crt.pem"` • `SSL_KEY_PEM_PATH:"/docker/pathto/server_key.pem"` **Note:** You should not provide the path of the entire chain of the certificate. You must only provide the server certificate and server key path. 2. Ensure that the certificates are copied to the path mentioned in **silentinstaller.yml**. 3. Restart `utility.sh`.

Issue: Unable to access the Enterprise Edition Web Client

Plant Applications Enterprise Edition Web Client is installed only on a Linux machine. After successful installation, application is not accessible and Haproxy service logs display the following errors:

[NOTICE] (6) : haproxy version is 2.5.1-86b093a

[NOTICE] (6) : path to executable is /usr/local/sbin/haproxy

*[**ALERT**] (6) : [haproxy.main()] Cannot raise FD limit to 8251, limit is 1024*

> **Note:**
> This issue is specific to the Web Client that runs on Amazon Linux OS.

Follow the below steps to troubleshoot the issue:

1. Modify the following parameter at: `/etc/sysconfig/docker`

   ```
   OPTIONS="--default-ulimit nofile=1024:4096"
   ```

   Replace with

   ```
   OPTIONS="--default-ulimit nofile=10000:15000"
   ```

2. Restart the docker.

Troubleshooting Web Client Applications

Issue: History of Work Order Manager Stops Working

In the Standard Plant Applications Web Client, if the **History** section does not display the events associated with the work order, or if the work order history stops working, you must verify Tomcat Web Application Manager to check the running state of Kafka dependent services. If the Kafka dependent services are down (indicated by **false** in the **Running** column of Tomcat Web Application Manager), it implies that there is an issue with Kafka log message, or that the message broker is down and stopped:

The issue with the Kafka broker may be due to the following reasons:

- PA web client Master control did not start **GE PlantApps Zookeeper** and **GE PlantApps Kafka** in a specific order or, there was a delay in starting Kafka after Zookeeper started.
- Kafka\Kafka-logs is in crash state.

To troubleshoot the issue, follow the below steps:

1. Open the **Services** window from the search box.
2. Stop **GE PlantApps Zookeeper** and **GE PlantApps Kafka** services.
3. Delete Kafka log messages from:
    - `C:\Kafka\kafka-logs` and
    - `C:\Kafka\logs`.
4. Restart **GE PlantApps Zookeeper** and then **GE PlantApps Kafka** services.

> **Note:**
> There should not be any waiting time or time delay, after you restart **GE PlantApps Zookeeper**.

5. Verify Tomcat Web Application Manager to ensure that the below mentioned Kafka dependent services are up and in running state.
    - approval-cockpit-service
    - comment-app-service
    - erp-export-service
    - labor-service
    - operator-app-service
    - plant-execution-service
    - supervisor-app-service
    - work-order-history-service

Result: The Kafka dependent services that were down, will restart now (indicated by **true** in the **Running** column of Tomcat Web Application Manager). This indicates the Kafka broker is working as expected.

Issue: Time Booking records cannot be modified

In the Security application, the **Moderate time booking records** role enables you to edit the time booking records of other users using the Time Booking application, and this permission is only applicable at a Site/Plant level resource.

As a supervisor or an operator, if you are not able to modify labor records in Time Booking even if you have the required permissions, it means that the role assignment is not done at Site/Plant level resource.

Follow the below steps to troubleshoot the issue:

1. Navigate to the Security application.
2. Select the **Roles** tab and select  against the required role (the role that was assigned to the user who is not able to modify time records).

3. Select the **Time Booking** tab from **ROLE CATEGORY** and ensure that the **Moderate time booking records** toggle is enabled.

   > **Note:**
   > If the user is not given permission at a Site/Plant level resource from the Security application, you will not be permitted to change the user capabilities even if the **Moderate time booking records** permission is enabled for that specific user.

4. Select **Assignments** tab and select the assignment you want to edit (the assignment that includes the user who is not able to modify time booking records).
5. From the **Resources** tab, add the required Site/Plant level resource to that assignment.

Result: In the Time Booking application, you will be able to modify the user capabilities, when you select **Change User** located below your username.

> **Note:**
> In the Security application, each permission has a lowest level of resource that should be added to an assignment. For more information, refer to **About the Security Application** topic in Plant Applications Help.

Issue: Cannot create raw material lots in PA2022

After upgrading to PA2022 from 8.1 or 8.2 version, user may have issues in creating raw material lots. This is because, in 8.1 or 8.2 version the lowest resource level that should be added to the assignment was the unit at which the produced material was executing. In PA2022, the lowest resource level that should be added to the assignment is the unit at which the raw material is stored.

To troubleshoot this issue, the assignment for the user (for creating raw material lots) must be changed from the unit at which the produced material was executing to the unit at which the raw material is stored.

For more information on how to modify an assignment, refer to **Modify an Assignment** topic in Plant Applications Help.

Issue: Cannot find the serial/lot no. or work order or operation added to Work Queue

In the earlier versions of Plant Applications, when you added a new serial/lot no. or work order or operation to Work Queue application, it was added to the first row of the grid.

In PA2022, the content of the grid is sorted based on the ascending alphabetical order of the WORK ORDER column. Hence, you can locate the newly added serial/lot no. or work order or operation based on the alphabetical order of the WORK ORDER column.

Issue: Cannot create Work Order or Clock on

Even if the user has enabled with the required permissions in the Security application to **Create a work order** and to **Execute a work order**, the user may receive "you cannot create a work order" or "you cannot clock on" error message. The following are the prerequisites to create a work order or execute a work order:

- The user must have **Create a work order** permission at the line level, or higher, for creating a work order and **Execute a work order** permission at the unit level, or higher, for executing a work order.
- The user must have permission to **Add Security** permission to **Create a work order** and **Edit Security** permission to **Execute a work order** in display view of PA thick client (Plant Applications Administrator).

Follow the below steps to troubleshoot the issue:

In **Plant Applications Web Client**:

1. Select  against the required role (the role that was assigned to the user).
2. Select **Work Order Management** tab from **ROLE CATEGORY** and ensure that **Create a work order** toggle is enabled.
3. Select **Work Order Execution** tab from **ROLE CATEGORY** and ensure that **Execute a work order** toggle is enabled.
4. Select **Assignment** and from **Resources** tab ensure that you include required resource level for that assignment or assigned role. Also, ensure that the user is member of the group added to the assignment.

In **Plant Applications Administrator**:

1. On the left side of the main screen expand **Plant Model** tree and select your line, and then right-click the line to select **Route Enable<...>**.

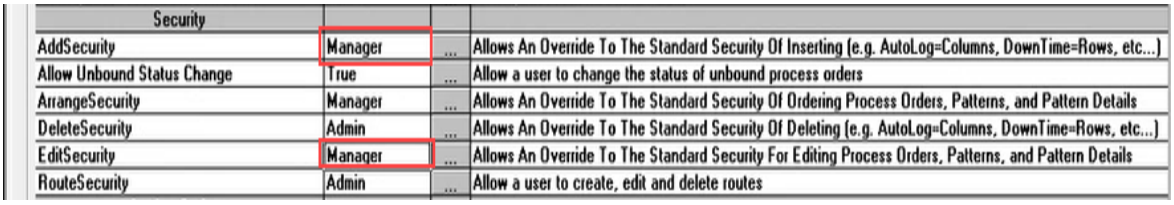
   > **Note:**
   > When you route enable the line, a display view is created for the work orders with naming convention **RESchedVw<...>**.

2. Expand **Client Management**, and from **Displays** tree, expand the line name.
3. Right-click **Change <> Security**.
   - If you have a security group, make a note of it.
   - If you have **<No Security Group>** continue.

4. Right-click **RESchedVw<...>**, and then select **Edit RESchedVw<...>**. The **Edit display** window appears.
5. Select **Display Options** and navigate to **Security** section.
    - Referencing the Security group from step 3, only the users with at least the role specified in **AddSecurity** can create work orders.
    - Referencing the Security group from step 3, only the users with at least the role specified in **EditSecurity** can execute work orders.
    - If step 3 had **<No Security Group>**, the value of the user role must be less than **Admin**.

Example: If John wants to create or execute a work order, and if a group called **Leaders** is the security group in the display view of **RESchedVw<...>**, then:

- John must be member of the **Leaders** user group.
- John must be member of the group and have at least the level of access specified in **AddSecurity** and **EditSecurity** (Example: If **Manager** is selected for **AddSecurity** and **EditSecurity** then the user must be member of a group with at least **Manager** level permission).



Security			
AddSecurity	Manager	...	Allows An Override To The Standard Security Of Inserting (e.g. AutoLog=Columns, DownTime=Rows, etc...)
Allow Unbound Status Change	True	...	Allow a user to change the status of unbound process orders
ArrangeSecurity	Manager	...	Allows An Override To The Standard Security Of Ordering Process Orders, Patterns, and Pattern Details
DeleteSecurity	Admin	...	Allows An Override To The Standard Security Of Deleting (e.g. AutoLog=Columns, DownTime=Rows, etc...)
EditSecurity	Manager	...	Allows An Override To The Standard Security For Editing Process Orders, Patterns, and Pattern Details
RouteSecurity	Admin	...	Allow a user to create, edit and delete routes