

Known Issues for Oracle Blockchain Platform Enterprise Edition for Besu

Learn about the issues you may encounter when using Oracle Blockchain Platform and how to work around them.

- [Assertion Failed Error When Using Blockchain App Builder](#)
- [Deployed Application Not Accessible on Instances Created with Custom Third Party Certificates](#)
- [Access to Bundled Application Deployed Using Custom Ingress-Gateway Port Fails](#)
- [Cannot Create Wallet for Other Organizations](#)
- [OpenLDAP Group Names Not Displayed When Creating LDAP Users](#)
- [Identity Provider Configuration Using the API Does Not Work](#)
- [Stack Information UI Mentions Incorrect Hosts Entry](#)

Assertion Failed Error When Using Blockchain App Builder

If you use Blockchain App Builder for Besu on Microsoft Windows 11, the following error message is displayed when uploading manifests to the smart contract registry:

```
Assertion failed: !(handle->flags & UV_HANDLE_CLOSING), file  
src\win\async.c, line 94
```

This is a known issue for Node.js running on Microsoft Windows 11.

Workaround: You can ignore this error message. The manifests will still be published to the smart contract registry.

Deployed Application Not Accessible on Instances Created with Custom Third Party Certificates

If you create an instance by using a third party certificate and then deploy one of the bundled applications, you cannot access the application.

Workaround: Run the following Kubernetes commands to update the information and restart the deployment.

```
kubectl -n obp-samples get secret "${deployment}-trust-bundle" \
-o jsonpath='{.data.ca\.crt}' | base64 -d > "${work_dir}/existing-
ca.crt"

kubectl -n idcs1 get secret obp-instance-external-ca-tls-
cryptomaterial \
-o jsonpath='{.data.ca\.crt}' | base64 -d > "${work_dir}/external-
ca-chain.crt"

cat "${work_dir}/existing-ca.crt" "${work_dir}/external-ca-chain.crt"
\
> "${work_dir}/ca.crt"

kubectl -n obp-samples create secret generic "${deployment}-trust-
bundle" \
--from-file=ca.crt="${work_dir}/ca.crt" \
--dry-run=client -o yaml | kubectl apply -f -

kubectl -n obp-samples rollout restart deployment/"${deployment}"

kubectl -n obp-samples rollout status deployment/"${deployment}"
```

Access to Bundled Application Deployed Using Custom Ingress-Gateway Port Fails

If you use one-click deployment from Blockchain Platform Manager to deploy an application to an instance in an installation setup with a custom Istio ingress gateway port, the "Access the application **here**" link provided at the end of the process does not open the application. A server error is returned because the link does not include the custom port.

Workaround: Include the custom port in the link provided at the end of the one-click deployment process.

Cannot Create Wallet for Other Organizations

When using IDCS as the identity provider, an error is returned when you attempt to create a wallet for a user in a different organization.

Workaround: Complete the following steps to create user wallets in the other organization directly in Blockchain Platform Manager. Then return to the application, load the wallet, and complete the account creation workflow.

1. Identify the target organization, organization network, user ID, and wallet service instance that will be used for the new deposit token account.
2. In Blockchain Platform Manager, open the **Wallet** page and select the **Users** tab.
3. Check whether the target user already exists for the target organization.
 - If the user exists, confirm that the organization and user ID are correct and that the user status is **Active**.
 - If the user does not exist, select **Register User** and enter the required details.
4. Select **Register User**, then confirm that the new user is displayed in the **Users** list with an **Active** status.
5. Select the **Wallets** tab, and then select **Create Wallet**.
6. In the Create Wallet window, enter the details for the selected user.
7. Select **Create Wallet**. Confirm that the wallet is displayed under the target organization in the **Wallets** list and that its status is **Active**.
8. Return to the Deposit Token application and open **Create Bank Account** for the target organization.
9. Enter the same **Bank User ID**, select **Load wallets**, and choose the wallet that you created in Blockchain Platform Manager.
10. Select the required application group, configure the account limits, and then select **Create Account**.
11. Confirm that the deposit token account is created and that the user can select the expected wallet when signing in.

OpenLDAP Group Names Not Displayed When Creating LDAP Users

OpenLDAP group names are not displayed in the **Instance Access Group** list when you create LDAP users and select groups. Instead, roles corresponding to the groups are displayed in the **Instance Access Group** list.

Workaround: Enter the group names manually if you intend to use other custom groups created in OpenLDAP.

Identity Provider Configuration Using the API Does Not Work

You cannot add an identity provider by using the API.

Workaround: Use the GUI to add an identity provider.

Stack Information UI Mentions Incorrect Hosts Entry

The **Stack information** area of the installation UI incorrectly mentions `wrapperapi.<instance-name>.<instance-domain>` instead of `wrapper.<instance-name>.<instance-domain>` in the list of entries to add to the `hosts` file.

Workaround: Disregard the UI and use `wrapper.<instance-name>.<instance-domain>` instead.

Oracle Database Known Issues for Oracle Blockchain Platform F20798-13

Copyright © 2019, 2026, Oracle and/or its affiliates

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.