Oracle® Database

Known Issues for Oracle Blockchain Platform

F20798-09

June 2025

Known Issues for Oracle Blockchain Platform

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

Supported Versions and Functions for this Release

- Supported Hyperledger Fabric Version
- Supported Browsers
- Interoperability of Hyperledger Fabric Versions
- Unsupported Functionality From Previous Versions

New Known Issues in this Release

- Instance Termination Occasionally Fails

Issues Initially Reported in Earlier Releases

- Instance Creation Supports Only Bundled OpenLDAP
- Peer Discovery Fails During Certificate Validation
- Log Display Not Updated for a Node
- Custom Root CA Certificates Not Supported
- Upgrade From Previous Releases Not Supported
- Error Message When Using the Oracle Blockchain Platform XA Implementation
- Console Unresponsive When Logging In
- Cannot Reinstall a Chaincode That Failed to Install Previously
- The Network's Oracle Blockchain Platform Instances Can't Manage Revoked Certificates

Supported Hyperledger Fabric Version

Oracle Blockchain Platform 24.1.3 supports Hyperledger Fabric 2.5.7.

Supported Browsers

If the console isn't behaving as expected, then check that you're using the latest version of a supported browser.

Oracle Blockchain Platform supports the following browsers:

- Mozilla Firefox
- Google Chrome
- Safari
- Microsoft Edge / Internet Explorer

Interoperability of Hyperledger Fabric Versions

Oracle Blockchain Platform does not support the use of instances based on Hyperledger Fabric v1.4.7 and on Hyperledger Fabric v2.x in the same blockchain network.
Workaround: Do not attempt to run different major versions of Hyperledger Fabric on the same blockchain network.

Unsupported Functionality From Previous Versions

Previous versions of Oracle Blockchain Platform Enterprise Edition supported load balancers and hardware security modules. These are not supported by Oracle Blockchain Platform 24.1.3.

Instance Termination Occasionally Fails

If your instance fails to terminate cleanly, try the following procedure.

Workaround:

1. Obtain the instance UUID:

```
# Replace username:password with the instance's admin user
credentials
AUTH_BEARER=$(echo -n 'username:password' | base64)

curl -k --location 'https://<control-plane-url>/api/v1/
blockchainPlatforms/instances' \
--header "Authorization: Basic $AUTH_BEARER"
```

   The `id` returned by this API is the UUID.

2. Identify the component causing the termination to fail:

```
kubectl get namespace "<instance-namespace>" -o json \
  | tr -d "\n" | sed "s/\"finalizers\": \[[^]]\+\]/\"finalizers\":
[]/" \
  | kubectl replace --raw /api/v1/namespaces/<instance-namespace>/
finalize -f - | jq -r '.status'
```

   The `NamespaceContentRemaining` field may contain multiple resources depending on the state of the instance. These reveal the resources preventing the namespace from being terminated.

3. Restart `hlf-operator` and `obp-operator`, which will restart the deletion flow for the instance.

```
# Restart hlf-operator
kubectl rollout restart deployment -n obp-cp hlf-operator-
controller-manager

# Restart obp-operator
kubectl rollout restart deployment -n obp-cp obp-operator
```

4. The termination process will now be restarted. To see if the termination was successful, you can re-run the API used in step 2 to see which components are still active and the status of the termination. If the termination was successful, the API request will fail.

5. To confirm the instance namespace has been terminated, ensure the namespace is no longer listed:

```
kubectl get ns
```

If your instance is still listed in the Blockchain Platform Manager instance list, the initial termination request may have timed-out. Use the following API to clear the entry for the terminated instance:

```
# Replace username:password with the instance's admin user credentials
AUTH_BEARER=$(echo -n 'username:password' | base64)
```

```
curl -k --location --request DELETE 'https://<control-plane-
url>/api/v1/blockchainPlatforms/instances/<instance-uuid>' \
--header "Authorization: $AUTH_BEARER"
```

Instance Creation Supports Only Bundled OpenLDAP

When you create an Oracle Blockchain Platform instance, even though there are options to add LDAP configurations for different types of LDAP, you must use the default OpenLDAP that is bundled with the product.

Workaround: Synchronize the data from your external LDAP system to the default OpenLDAP that is bundled with Oracle Blockchain Platform and then continue with instance creation.

Peer Discovery Fails During Certificate Validation

If your client application uses the `fabric-sdk-go` module, your application might fail due to certificate validation during the peer discovery process because of an unsupported version of `fabric-sdk-go`.
To use the `fabric-sdk-go` module, update to the following version:

```
github.com/hyperledger/fabric-sdk-go
v1.0.1-0.20240123083657-5d6ca326e01b
```

Log Display Not Updated for a Node

In the console UI, if you view logs for a particular node, then navigate to a different pane, and then return to the logs for the initial node, the logs are not fetched again.

Workaround: Refresh the browser page to fetch the latest logs.

Custom Root CA Certificates Not Supported

The Hyperledger Fabric CA root CA certificates are self-signed. This release of Oracle Blockchain Platform does not support signing these certificates with root or intermediate CA certificates provided by the customer.

Upgrade From Previous Releases Not Supported

You cannot upgrade to Oracle Blockchain Platform Enterprise Edition 24.1 from Oracle Blockchain Platform Enterprise Edition 21.1 or Oracle Blockchain Platform Enterprise Edition 19.3.

Workaround: There is no workaround for this issue.

Error Message When Using the Oracle Blockchain Platform XA Implementation

If you download the Java library that implements the XA protocol and then use it in an environment where a Maven version later than 3.8.1 is installed, the following error message is displayed: `the artifact information is not valid and contains invalid characters.`

Workaround: The `.pom` file in the downloadable library has a placeholder for the version number. Update the `pom.xml` file and change the version number to `24.1.3`.

Console Unresponsive When Logging In

When you attempt to log in to the service console, the UI might be unresponsive.

This behavior is fixed by the following patch: ORACLE BLOCKCHAIN PLATFORM ENTERPRISE EDITION (OBPEE) - 24.1.3 - PATCHSET-1, which is patch number 36929129. For more information about installing the patch, see Patch Oracle Blockchain Platform.

Cannot Reinstall a Chaincode That Failed to Install Previously

If you try to reinstall a chaincode with the same name as a chaincode from a previously failed installation, the installation process fails again. This can happen when a pod with the chaincode name was created for the previous installation attempt and then not deleted.

This behavior is fixed by the following patch: ORACLE BLOCKCHAIN PLATFORM ENTERPRISE EDITION (OBPEE) - 24.1.3 - PATCHSET-1, which is patch number 36929129. For more information about installing the patch, see Patch Oracle Blockchain Platform.

The Network's Oracle Blockchain Platform Instances Can't Manage Revoked Certificates

If an Oracle Blockchain Platform network contains Hyperledger Fabric organizations and their certificates are revoked, then the revoked certificates aren't applied to, won't display in, and can't be revoked from the network's Oracle Blockchain Platform instances.

Workaround: Use the native Hyperledger Fabric CLI or SDK to import the organization's certificate revocation list (CRL) file.

Channel Creator Can't Update the Channel's Configuration

When you use the native Hyperledger Fabric CLI or SDK to create a channel, the Creator policy isn't included in the `configtx.yaml` file. Oracle Blockchain Platform requires the Creator policy to allow the channel creator to edit a channel's configuration.

Workaround: Manually edit the `configtx.yaml` file to add the Creator policy.

Peer Fails to Pull Private Data from Another Peer

A peer can fail to pull private data from another peer if a private data collection's `blocktolive` value is less than 10 and its maxPeerCount is less than the total number of peers, not including the endorsing peer. This value is set when you use the console to create a private data collection definition or use the native Hyperledger Fabric CLI or SDK.

Workaround: Confirm that the `blocktolive` value is set to greater than or equal to 10. Or confirm that the `maxPeerCount` is set to no less than the total number of peers, not including the endorsing peer. If needed, you can re-instantiate or upgrade the chaincode to reset these values.

Channel Creator Organization and Channel Policy Settings Inconsistency

You can use the console to create a channel and set your organization's ACL to ReaderOnly. After you save the new channel, you can't update this ACL setting from the channel's **Edit Channel Organizations** option.

However, you can use the console's **Manage Channel Policies** option to add your organization to the Writers policy, which overwrites the channel's ReaderOnly ACL setting.

Workaround: There is no workaround for this issue.

Exported and Imported File Incompatibility

You can't export and import files (CRLs, certificates, orderering service settings, and peers) between the console and the REST APIs.

Files exported by the console and REST APIs are only compatible for import with the same component. For example, if you export a peer using the console, then you can't import it with the REST API (you can only import it with the console). And if you export a peer with the REST API, then you can't import it with the console (you can only import with the REST API).

Workaround: There is no workaround for this issue.

Chaincode Name Requirements

The Oracle Blockchain Platform chaincode name and version requirements are different than the Hyperledger Fabric requirements. You must use the Oracle Blockchain Platform requirements when you deploy a chaincode from the console or the Hyperledger Fabric client. If you don't follow these requirements when deploying from the Hyperledger Fabric client, then the chaincode may be listed incorrectly in the console.

Workaround: Use the following rules when deploying a chaincode name and version.

- Use ASCII alphanumeric characters, dashes (-), and underscores (_).
- The name must start and end only with ASCII alphanumeric characters. For example, you can't use names like `_mychaincode` or `mychaincode_`.
- Dashes (-) and underscores (_) must be followed with ASCII alphanumeric characters. For example, you can't use names like `my--chaincode` or `my-_chaincode`.
- The name and version can each be up to 64 characters long.
- The chaincode version can also contain a period (.) and plus signs (+).

Date and Time Picker Behavior

The Oracle Blockchain Platform date and time picker doesn't behave as expected. You use the date and time picker to filter items such as log files or ledger activity.

Workaround: Use the following information to help you use the date and time picker.

- If you select a specific time period (for example, **Last day**) and then select it again to re-run the query, the query doesn't re-run. To get the latest information, click the refresh button.
- If you haven't set the time zone on your computer, then when you select the **Custom** option, you must specify the start time and end time in GMT. However, if you set the Timezone Setting to **GMT** in the Preferences (in the console select your instance name, then click Preferences, and then Timezone Setting), the timezone on the console automatically converts to GMT.

Documentation Accessibility

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.