



Tutorial B3: Enrolling with the network

Estimated time: 10 minutes

In the previous tutorial we authenticated ourselves with the IBM Blockchain Platform web console. However, until we have also enrolled with the Hyperledger Fabric network, our ability to use the console to work with DriveNet is limited.

In this tutorial we will:

- Complete the enrollment of your user with the Community Org CA
- Associate that user with the Community Org peer
- Browse the consortium of member organizations that comprise DriveNet

In order to successfully complete this tutorial, you must have first completed tutorial [B2: Discovering the network](#) in your web browser.

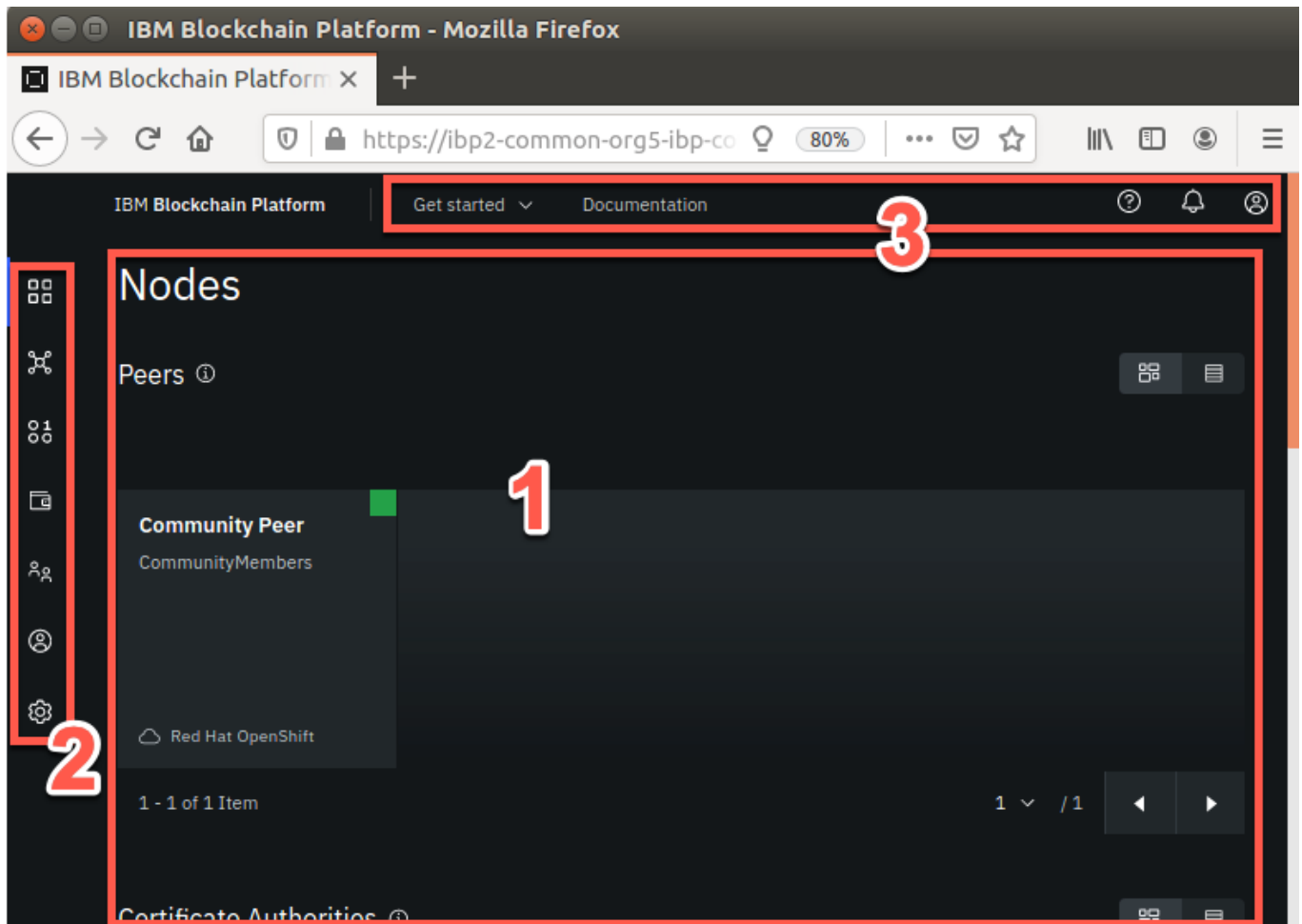
 **B3.1:** Expand the first section below to get started.

► Enroll with the certificate authority

In this section we will complete the enrollment process.

At the end of the previous tutorial we logged in to the IBM Blockchain Platform web console. Now take a look at the page you are shown. It consists of:

1. a **main view** (showing *Nodes* by default)
2. an **icon bar** on the left that allows you to select the type of Hyperledger Fabric object shown in the main view, and
3. a set of tabs along the top for **general information and settings**.



Nodes

In Hyperledger Fabric, a *node* is the general term for any component that helps run the network. There are three node types:

- peers, which hold ledgers and execute smart contracts
- certificate authorities, which manage identities for an organization
- orderers, which assert transaction order and build blocks.

If you scroll through the IBM Blockchain Platform Nodes view, you can see the DriveNet nodes we've gained access to: Community Peer, Community CA and DriveNet Ordering Service. A green square in the corner of each of the nodes confirms that they are running.

We used a locally installed peer in the previous set of tutorials, and will use the Community Peer extensively in this set. But for now let's look at the certificate authority (CA), as this will allow us to enroll with the network.

Enrollment is the process where we take the Fabric enrollment ID and secret that was previously registered and supplied to us, and use it to request a digital certificate from the CA that we can use to identify ourselves with the network.

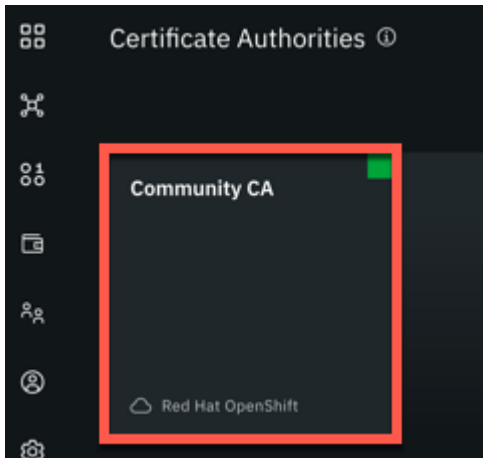
Registration vs. Enrollment

Note that while an organization's administrator will typically *register* a user, it is the end-user who will *enroll* it. This two stage process is deliberate; it ensures that the administrator cannot impersonate the

end-user by intercepting their certificate.

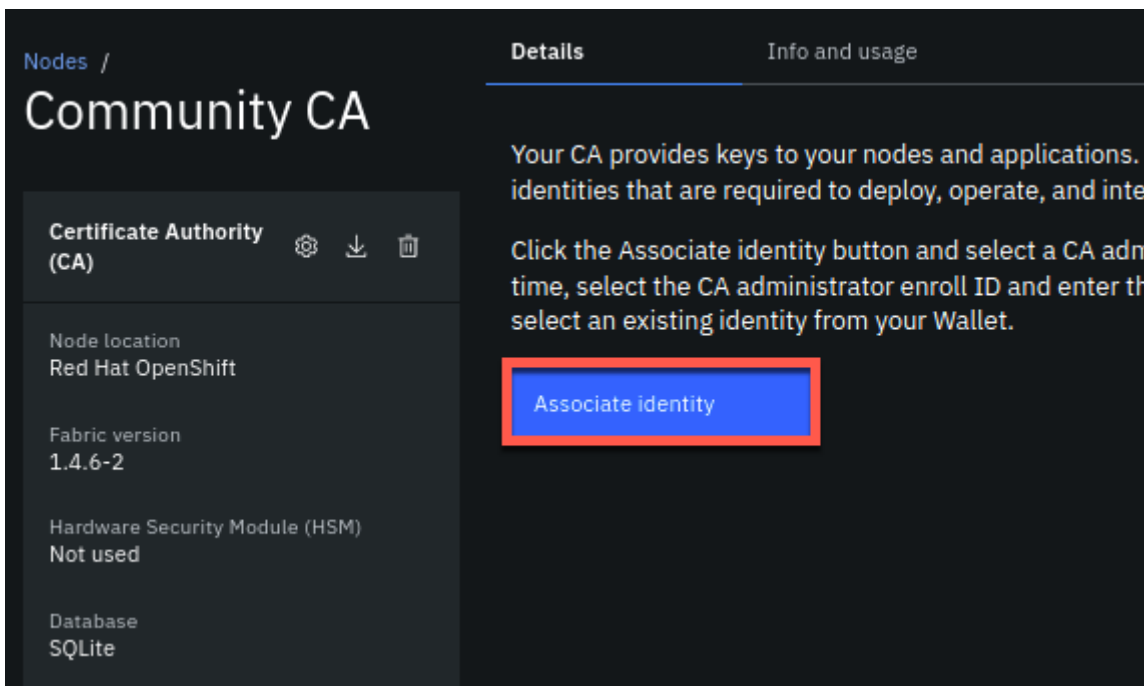
We will enroll our identity using the Community Org CA.

- B3.2: Scroll to the Certificate Authorities section of the Nodes view and click on 'Community CA'.



The view will change to show some information about the Community CA node.

- B3.3: Click 'Associate identity'.



- B3.4: In the side panel that appears, enter the Fabric enrollment user ID and secret that was supplied to you previously. Enter *student* as your identity display name, and when you're done, click 'Associate identity'.

Take particular care when entering your secret; use the eyeball icon to show what you're typing if necessary.

While it is possible to pick a different display name, we recommend sticking with *student* as it will be referenced throughout these tutorials.

×

Associate identity

An identity is required to operate this CA. You can use either the enroll ID and secret of your CA admin and add it to the Wallet by clicking Associate identity or select an existing identity from your Wallet.

Enroll ID

Existing identity

Enroll ID *

Enroll secret *

.....

👁

Identity display name *

student

You will now be enrolled onto the network and your certificate placed in your web browser's storage.

When completed, you might see an error that tells you that you cannot list the available users:

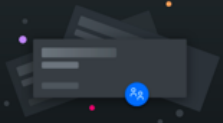
Enroll ID

Type

Affiliation

Unable to retrieve the list of users.

×



Unable to retrieve the list of CA users

You have entered an incorrect enroll ID or secret, or you do not have proper access to this list of users.
Click the settings icon for this CA to properly set the identity.

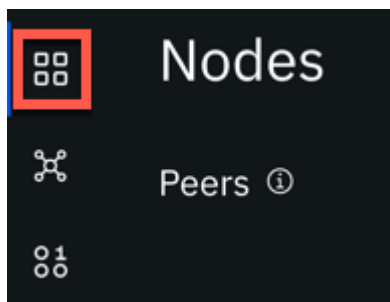
This is because your role as a network joiner does not allow you to list other users registered in the CA.

 B3.5: Expand the next section to continue.

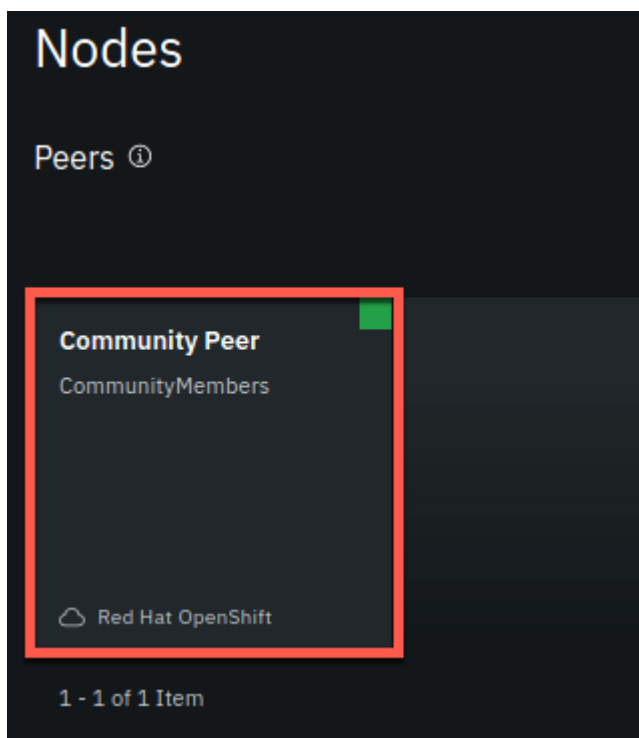
► Associate our identity with the peer

The final stage of enrollment is to make our new ID known to the Community Org peer.

 B3.6: Click the 'Nodes' icon in the icon bar to show the Nodes view.

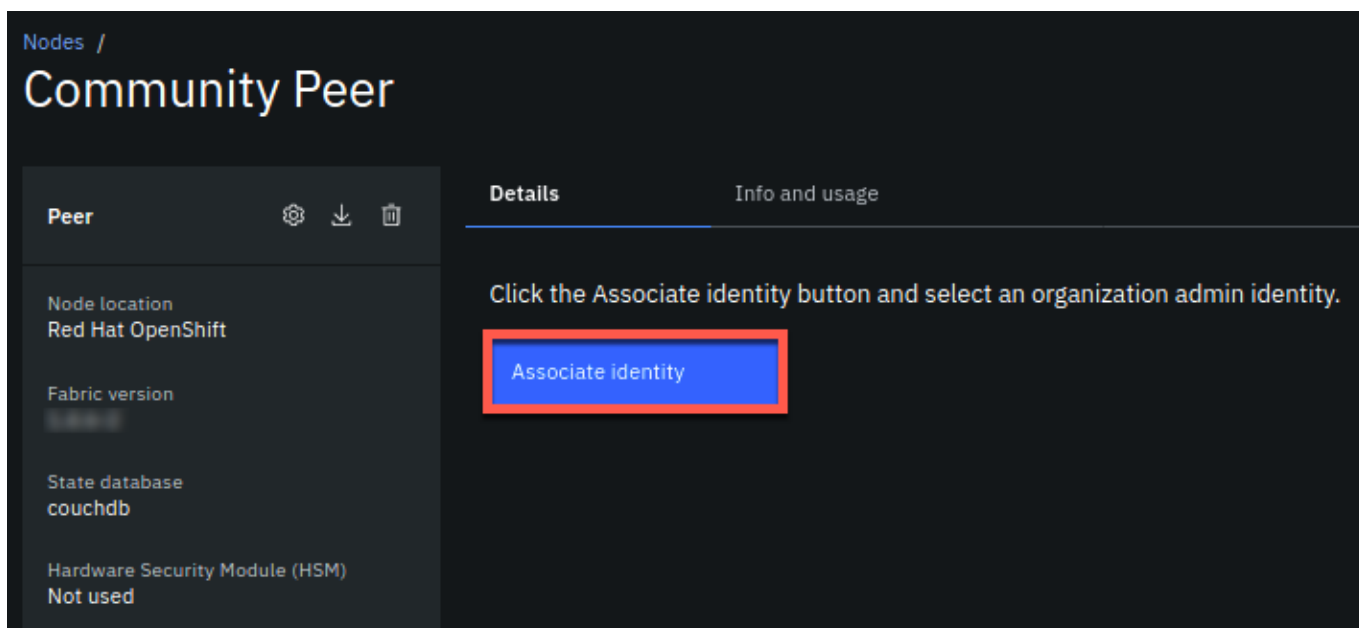


- B3.7: Select the Community Peer.

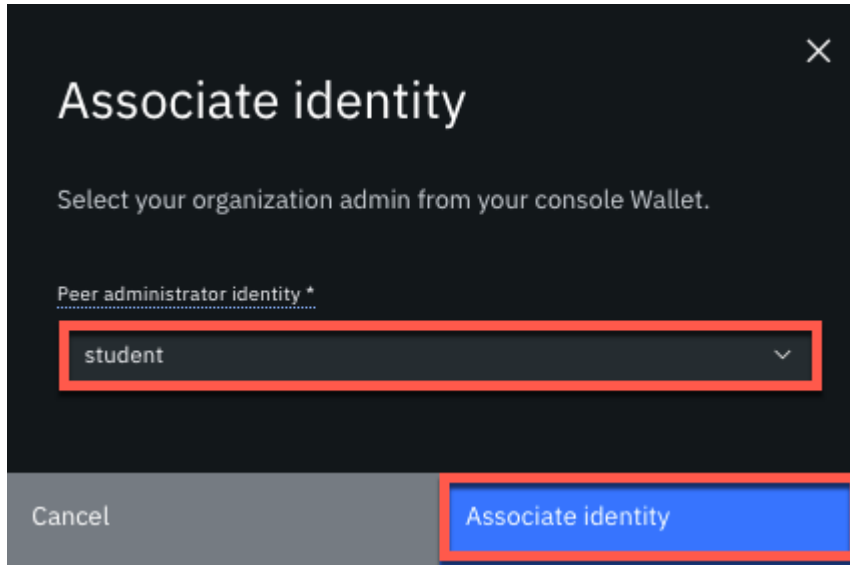


Similar to before, the view changes to show details on community peer.

- B3.8: Click 'Associate identity'.



B3.9: In the side panel that appears, select 'student' from the drop down list. Click 'Associate identity'.



► Browse the consortium

That completes our enrollment onto the DriveNet network.

Before we use the network, it's worthwhile to browse the consortium that makes up the network, as this confirms the organizations with whom we're going to share data. This is shown on the *Channels* view of the IBM Blockchain Platform web console.

Channels

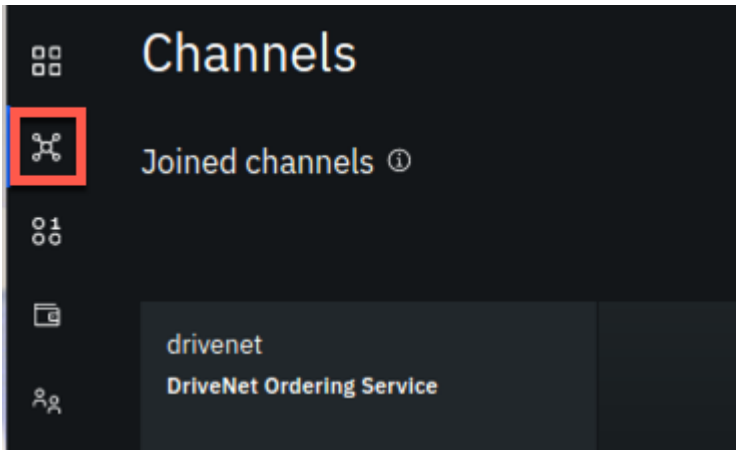
As we've seen, network channels, or channels, are the simplest and broadest way that Hyperledger Fabric scopes the sharing of transactions. DriveNet is an example of a channel.

By default, all organizations see the transaction details on the channel, but there are ways of restricting this. We'll see how in a later tutorial.

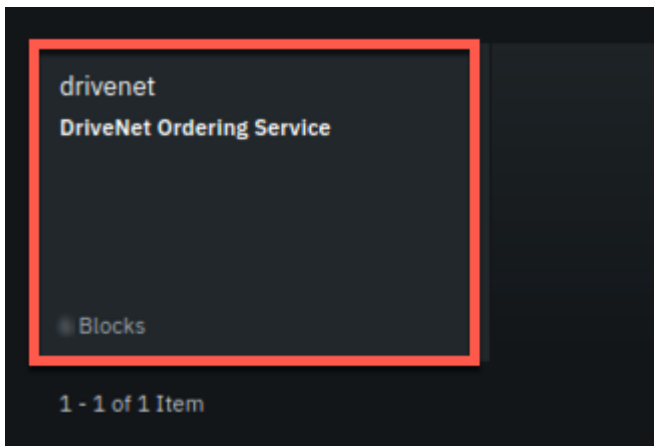
Each channel has a ledger, a set of member organizations, a set of participating nodes (e.g. peers) and a set of instantiated smart contracts.

We can browse all of these elements from the Channels view of the web console.

B3.10: Click the 'Channels' icon in the icon bar to show the Channels view.

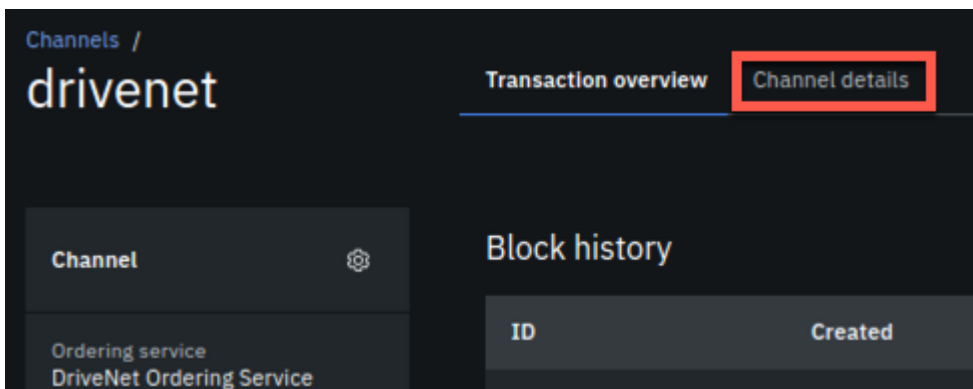


 B3.11: Click the 'drivenet' tile.



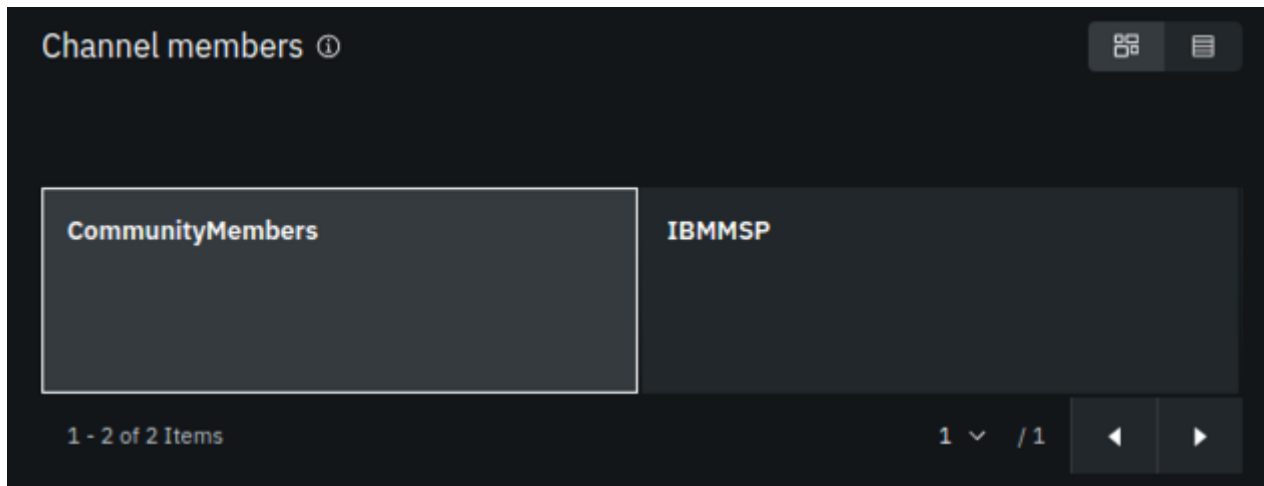
The DriveNet page shows a list of transactions by default, which we will investigate in more detail in the next tutorial. For now, we want to find out the DriveNet members, which are shown on the Channel details tab.

 B3.12: Click 'Channel details'.



This page describes all the components of the DriveNet network: for example, the nodes, channel members smart contracts.

If you scroll to the Channel members section you'll see the DriveNet member organizations.



These identifiers are called *Membership Services Provider identities*, or MSPIDs for short. MSP is a Hyperledger Fabric term that allows us to uniquely identify each organization in the network. DriveNet has two MSPs: *IBMMSP* and *CommunityMembers*; you're now a member of the latter.

Whenever we need to refer to an organization, for example, when creating a wallet, we must specify the MSPID.

Remember the *CommunityMembers* MSPID; we'll use it in the next tutorial.

Summary

In this tutorial we completed all the configuration steps necessary to onboard ourselves with the DriveNet network; we enrolled our user with the Community Org CA, and then we associated it with the Community Org peer.

Now that we have fully registered into the network, we can connect to it from our client applications. In order to do this we first need to get hold of the connection profile and identity files that allow external applications to connect. We'll do this in the next tutorial.

→ **B4: Acquiring network connection details**