

Moonshot Test Network

On this page you will find instructions on how to use the Moonshot Test Network which mirrors the actual Trust Router infrastructure.

Contents

- [1. The Moonshot Test Network](#)
 - [1.1. Domains and realms](#)
 - [1.2. Hosts](#)
 - [1.3. Firewall rules](#)
- [2. Registration for use](#)
- [3. How to use the network](#)



Use of the Moonshot Test Network

The usage of the Moonshot Test Network is subject to standard Terms and Conditions, including the right to terminate your access to this network prematurely.

1. The Moonshot Test Network

The Moonshot project has created a test network (kindly hosted by the Trust & Identity Directorate at Jisc) that demonstrates the functionality of the Moonshot technology. Free to use for piloting and testing, this network is designed to be the next step towards a full deployment and joining a Moonshot network. This test network includes an identity provider (to test your services with), two service providers (to test your identity provider with), and a trust router and APC.

1.1. Domains and realms

To demonstrate the difference between trust realms, identity realms, and the actual domain name system, and to avoid conflation of these concepts, the test network uses different values for each.

1.1.1. Trust realm

The trust realm suffix on the test network is `test.assent`. Each of the standard test network hosts in the network uses a different trust realm to everyone else, making each of these hosts a unique organisation in their own right. The trust realms are what entities on the network use to facilitate trust amongst themselves.

1.1.2. Identity realm

The only identity realm provided on (and by) the test network is `idp.test.assent`. While this realm includes the trust realm suffix, its name is different and does not match any other realms, including its own trust realm.

1.1.3. Communities of Interest (COI)

The only community of interest (COI) that currently exists on the test network is the APC community, `apc.test.assent`. All entities on the network belong to this COI. If you want to create a community of your own, please tell us, and we will create one for you. When we create test communities, we will use the realm suffix of `test.community`.

1.1.4. Domain names

The domain names for the standard network hosts are registered in the `moonshot-playpen.ti.ja.net` domain.

1.2. Hosts

1.2.1. The APC

The APC is `apc.moonshot-playpen.ti.ja.net`. It is the 'mother' community and identity provider for all the entities in the network as the organisation credentials are verified by the APC host. Its identity realm is `apc.test.assent`, which also is its trust realm and the name of the overarching community of interest. This is the only instance where the trust realm, community of interest and identity realms are identical.

1.2.2. The Trust Router

The Trust Router (TR) is `tr.moonshot-playpen.ti.ja.net`. It facilitates the trust amongst the different entities in the network.

1.2.3. The IdP

The Identity Provider (IdP) is `idp.moonshot-playpen.ti.ja.net`. It serves up the identity realm `idp.test.assent`. It serves three identities, `steve`, `bob`, and `hugh`.

1.2.4. The SP

The first Service Provider (SP) is `rp.moonshot-playpen.ti.ja.net`. This SP exposes an SSH service that has only one user: `moonshot`.

1.2.5. The web service

The second SP is `service.moonshot-playpen.ti.ja.net`. It exposes a web service both on HTTP and HTTPS. Visiting the root will give you access to four web scripts that expose information about your authentication request in different formats.

1.2.6. The portal

The Moonshot portal is `portal.moonshot-playpen.ti.ja.net`. Those wishing to test out Moonshot are given access to this portal to control the trust configuration for their services.

1.3. Firewall rules

Often test services are run in cloud infrastructures such as AWS, Azure or Google Cloud. They are also run in DMZ zones, or, in some instances, in private virtual infrastructures behind a firewall.

Here are sample firewall rules that establish incoming and outgoing rules to both the Test and Live (Jisc Assent) Moonshot trust router infrastructures. If you connect to another Trust Router, adjust these rules to suit:



IP Tables sample firewall rules (Jisc Assent)

```
-A INPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s 0/0 --dst <IdP/RP Proxy IP address> --dport 2083 -j ACCEPT
-A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s <IdP/RP Proxy IP address> --dst 0/0 --dport 2083 -j ACCEPT
-A INPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s 212.219.179.130,212.219.179.131,212.219.179.138,212.219.179.146 --dst <IdP/RP Proxy IP address> --dport 12309 -j ACCEPT
-A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s <IdP/RP Proxy IP address> --dst 212.219.179.130,212.219.179.131,212.219.179.138,212.219.179.146 --dport 12309 -j ACCEPT
```



IP Tables sample firewall rules (Test Network)

```
-A INPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s 0/0 --dst <IdP/RP Proxy IP address> --dport 2083 -j ACCEPT
-A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s <IdP/RP Proxy IP address> --dst 0/0 --dport 2083 -j ACCEPT
-A INPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s 13.79.134.211,13.79.128.103,52.169.31.104 --dst <IdP/RP Proxy IP address> --dport 12309 -j ACCEPT
-A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -m tcp -p tcp -s <IdP/RP Proxy IP address> --dst 13.79.134.211,13.79.128.103,52.169.31.104 --dport 12309 -j ACCEPT
```

2. Registration for use

To use this network, you must apply for an organisation credential. The credential must be used by all your services to identify them to the test network's trust router. To apply for such a credential, email trustrouter@jisc.ac.uk with details of your organisation, how long your pilot/testing will run, and your domain and host names. We will invite you to the portal where you are provided with a time-limited credential that will expire at the end of your pilot. If your credential needs to be extended, email us with an approximate extension, and we will adjust the expiry date.

Once your pilot is concluded and you decide to transition to a production network, see the list of [trust router operators](#) for one that suits you (currently just Jisc).

3. How to use the network

The network is designed to allow you to use both the services and the identity provider to test your own services and your own identity provider. If you are part of a group of organisations or services trying out Moonshot, you can also test your own services and identity providers amongst your group, using the test network as a facilitator.