# Install a Trust Router on Debian 7

On this page you will find instructions on how to set up a Trust Router on Debian 7.

**Contents**



# 1. System Preparation

## 1.1. Install Debian 7

The first thing that is required is a Debian 7 machine - this can be physical or virtual.

1. Install Debian 7 (Wheezy) via usual mechanism (e.g., netboot CD, ISO in VMware/VirtualBox or the DVD image.
2. Choose the following server install options: "Debian desktop, SSH server, Standard system utilities".
3. Create/choose a secure root password and an initial system user account.
4. Once installed, make sure you run an `apt-get update` and `apt-get upgrade` to ensure your system is fully up to date.

**Tip**
*We would recommend using LVM when disk partitioning to allow easier partition/disk expansion on a live system*.

**Warning**
After install, you will want to secure/lockdown the server as best practice dictates - for both the server and any extra software installed. This is beyond the remit of this guide but there are many guides available that provide information on securing your Debian servers and applications.

## 1.2. Configure Debian 7

Next, there are a few Debian configuration options that need to be set in advance.

### 1.2.1. Networking configuration

For production deployments, it is recommended that the machine be assigned a static IP address.

For Debian networking information please refer to the Debian documentation: https://wiki.debian.org/NetworkConfiguration

### 1.2.2. Firewall configuration

The following ports are required to be accessible from the outside world, both in the local firewall and in any external firewalls:

- 2083/tcp (for RadSec connections to other Moonshot entities)
- 12309/tcp (for Trust Router client connections - if using the Trust Router to broker trust relationships between entities)

These are sample firewall rules that establish incoming and outgoing rules to the Moonshot trust router infrastructure.

**IP Tables sample firewall rules**

```
-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 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
0/0 --dport 2083 -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
```

### 1.3. Add the Moonshot Repository

1. Add the Moonshot Debian Wheezy repository to your system. To do this, run the following command (as root, or using sudo):

```
$ echo "deb http://repository.project-moonshot.org/debian-moonshot
wheezy main" > /etc/apt/sources.list.d/moonshot.list
```

2. Install the Moonshot GPG key:

```
$ wget -O - http://repository.project-moonshot.org/key.gpg | apt-key
add -
```

> **Verifying the Moonshot GPG key**
> If you wish to verify the Moonshot GPG key's validity and integrity, please see the Packaging GPG Key for further details.

3. Update the apt cache with the new repository information:

```
$ apt-get update
```

## 2. Install Trust Router

We're now ready to install the Trust Router software and its required dependencies. Install the software by running the following command:

```
$ apt-get install moonshot-trust-router moonshot-ui
```

## 3. Configure Trust Router

Next, we need to configure the Trust Router.

### 3.1. RadSec

#### 3.1.1. APC TLS

First, you will need a copy of a client key and certificate (and appropriate CA) from the APC(s) that your Trust Router serves. Copy them onto the filesystem of your Trust Router.

You can put these files anywhere on the file system, but this guide assumes you put them in /etc/pki/tls. If you place them in a different location you will need to change the locations below as appropriate.

### 3.1.2. Connection to APC

Next, we need to configure the RadSec configuration for the APC. We do this by creating a file at `/etc/radsec.conf` with the following:

```
realm gss-eap {
 type = "TLS"
 cacertfile = "/etc/pki/tls/tr-ca.crt"
 certfile = "/etc/pki/tls/tr-client.pem"
 certkeyfile = "/etc/pki/tls/tr-client.key"
 disable_hostname_check = yes
 server {
  hostname = "apc.moonshot.ja.net"
  service = "2083"
  secret = "radsec"
 }
}
```

## 3.2. Trust Router

### 3.2.1. Daemon Configuration

Your Trust Router will need to have a few core configuration items set. To do this:

1. Open the default instance's main configuration file at `/etc/trust_router/conf.d/default/main.cfg` for editing.
    a. Change the hostname to the (fully qualified) hostname of your Trust Router.
    b. Change the port that it runs on, if necessary.

If the `/etc/trust_router` directory does not exist, you may need to create it yourself, along with the subdirectories mentioned.

### 3.2.2. Moonshot Configuration

Moonshot, you say? Yes, Trust Router uses Moonshot to authenticate and secure all communications between Trust Router clients and servers. So, you will need to configure the trust router user to make use of the Moonshot flatstore (i.e. telling Moonshot that this is a special system account, not a regular user account), and you will need to import a set of credentials for your Trust Router to use.

1. Enable the trustrouter user to use the Moonshot UI flatstore:

```
$ echo "trustrouter" >> /etc/moonshot/flatstore-users
```

2. Import it using the moonshot-webp command (as the trustrouter user):

```
$ su --shell /bin/bash trustrouter
$ unset DISPLAY
$ moonshot-webp -f [path to credential file]
```

The credentials file will be given to you by the administrator of the APC.

### 3.2.3. Shibboleth

Shibboleth, you say? Yes, Shibboleth is used by the Moonshot components to be able to deal with incoming SAML. However, this feature typically isn't used in Trust Router, but its logging will appear in your Trust Router's log files. So, to simplify your log files, it is recommended that you silence the Shibboleth logging. To do this:

1. Open `/etc/shibboleth/console.logger` for editing.
2. Change WARN to NONE on the first line, i.e.

```
log4j.rootCategory=NONE, console
```

### 3.2.4. Default Peer

> If your Trust Router is going to run in its own, standalone, trust network, then you can skip this step.

If your Trust Router is going to run in a wider trust network, then you can configure your Trust Router's default peer - i.e. the Trust Router it sends its clients to when they ask it to locate a Moonshot entity that your Trust Router doesn't know about. To do this:

1. Open `/etc/trust_router/conf.d/default/peering.cfg` for editing. Change the content as follows:

```
{
"default_servers": [
 "[hostname of trust router]"
 ]
}
```

**Example**
If you were configuring your default Trust Router peer to be Janet's Trust Router at tr1.moonshot.ja.net, its `peering.cfg` file would look like this:

```
{
"default_servers": [
 "tr1.moonshot.ja.net"
 ]
}
```

### 3.2.5. Configure your Trust Router

A trust router requires a trust configuration to function correctly. See the trust configuration file for more information.

Place an appropriate `trusts.cfg` file info the `/etc/trust_router` directory and symbolically link it into the default configuration directory:

```
# cd /etc/trust_router/conf.d/default
# ln -s ../../trusts.cfg
```

You can find a Trust Router configuration suitable for a Trust Router connecting to tr1.moonshot.ja.net at sample Trust Router Client configuration

### 3.2.6. Start your Trust Router

You are now ready to start your Trust Router and test it. To do this:

1. As trustrouter user, start the Trust Router:

```
$ trust_router
```

Debian currently has no initscript for trust_router so it needs to be run manually. We hope to fix this in the near future.

# 4. Testing

To test your trust router, you should attempt a TIDC request on a Moonshot service connected to your trust router. The TIDC request will take a little longer, but it should succeed.

If it fails, please contact us.

# 5. Next Steps

At this point, you now have a Trust Router. Blimey.