Required Platform Configuration

Contents:

This section contains a set of configuration steps required to enable basic functionality in the Trifacta® platform, as well as the methods by which you can apply the configuration.

> **Before you begin any configuration or modification to a working configuration, you should back up the `/opt/trifacta/conf` directory.**

Admin Settings page: If the software has been installed and the databases have been initialized, you should be able to start the platform and access the Admin Settings page. For more information, see *Platform Configuration Methods*.

> **Tip:** Whenever possible, you should use the Admin Settings page of the application for platform configuration.

Configuration by file: If the application is not available, you can perform configuration changes using the platform files. See below.

Configuring by File

> **Please make backups of any configuration files that you modify and apply changes with caution.**

> **Tip:** If you have not used a Linux text editor, please enter one of the following strings at the command line to see which is available in your environment. nano may be the easiest to use:
>
> - `vi`
> - `vim`
> - `emacs`
> - `nano`

The Trifacta configuration files are stored in the following directory:

```
/opt/trifacta/conf
```

Filename	Description
`hadoop-site/*`	(Hadoop only) Directory for configuration files from the Hadoop cluster to which the platform connects. See *Prepare Hadoop for Integration with the Platform*.
`nginx.conf`	Configuration of the platform's HTTP access.

`trifacta-conf.json`	Most customer-facing configuration and product options for all components are stored here.

NOTE: After saving your changes to the config files, you must restart the Trifacta platform to apply them. See *Start and Stop the Platform*.

Required Platform Configuration Steps

Review Self-Registration

By default, any visitor to the Login page can create an account in the Trifacta platform.

If the Trifacta platform is available on the public Internet or is otherwise vulnerable to unauthorized access, unauthorized users can register and use the product. If this level of access is unsatisfactory, you should disable self-registration.

Disabling self-registration means that a Trifacta administrator must enable all users. For more information, see *Configure User Self-Registration*.

Configure Shared Secret

To manage cookie signing, the platform deploys a shared secret, which is used for guaranteeing data transfer between the web client and the platform.

At install time, the platform inserts a default shared secret. The default 64-character shared secret for the platform is the same for all instances of the platform of the same version. This secret should not be used across multiple deployments of the platform.

NOTE: If your instance of the platform is available on the public Internet or if you have deployed multiple instances of the same release of the platform, cookies can become insecure across instances when the secret is shared across instances. You should get in the habit of changing this value for each installation of the platform.

Please complete the following steps to change the shared secret.

Steps:

1. You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.
2. Locate the following parameter:

```
"sharedSecret": <64_character_value>
```

3. Modify the current value. The new value can be any 64-character string.
4. Save your changes.

Other Required Configuration

The following configuration steps must be reviewed and completed for all deployments of the Trifacta platform:

NOTE: You must define and configure your backend datastore before the platform is operational.

NOTE: If High Availability is enabled on the cluster, it must be enabled on the Trifacta platform, even if you are not planning to rely on it. Do this step after completing the preceding steps. See *Enable Integration with Cluster High Availability*.