Configure Security

Contents:

This section provides an overview of security features of the Trifacta® platform and links to configuration workflows for each area.

Harden Trifacta node

The following sections cover how to enhance security for the Trifacta node.

User Access

Configure Password Criteria

By default, the Trifacta application enforces very limited requirements on password strength.

> **By default, a password can be a single character with no other requirements. Please configure password requirements.**

For more information, see *Configure Password Criteria*.

Change Admin Password

> **As soon as the Trifacta platform is operational, you should change the password on the admin account.**

See *Change Admin Password*.

Single Sign-On

The Trifacta platform can integrate with Active Directory at the KDC/Kerberos level or directory level.

> **NOTE:** SSO integration requires set up of an Apache server as a reverse proxy. Instructions are provided in the link below.

See *Configure SSO for AD-LDAP*.

Disable User Self-Register

Whether you use SSO or not, you should consider disabling user self-registration. When self-registration is disabled, an admin must provision individual users. See *Configure User Self-Registration*.

Application Timeouts

As needed, you can review and modify various application timeouts, which may need modification to meet your enterprise standards. For more information, see *Configure Application Limits*.

Client Security

Enable HTTP Strict-Transport security headers

HTTP Strict-Transport security headers force web browsers to use secure communications when interacting with the server and prevent any communications over insecure HTTP protocol.

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. Set the following setting to true:

```
"proxy.securityHeaders.httpsHeaders": true,
```

3. Save changes and restart the platform.

Enable Secure cookies

The web application requires use of cookies. Set the following flag to ensure use of secure cookies.

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. Set the following setting to true:

```
"webapp.session.cookieSecureFlag": true,
```

3. Save changes and restart the platform.

Enable SSL

Deploy Platform SSL Certificate

To enable HTTPS communications with the web application of the Trifacta platform, you must create and install an SSL certificate for use by the platform.

> **NOTE:** After you have deployed an SSL certificate, you can enable secure headers and secure cookies to be used by the web application.

See *Install SSL Certificate*.

SSL for SMTP Server

If the platform is integrated with an SMTP email server, by default it assumes that the server supports SSL. If not, this capability must be disabled.

> **NOTE:** Access to SMTP server is required for password reset communications.

See *Enable SMTP Email Server Integration*.

Session timeouts

For more information on these parameters, see *Configure Application Limits*.

Access logs

For some access logs, you can configure the fields that are included, which permits you to remove sensitive information like IP addresses. For more information, see *Configure Logging for Services*.

Databases

SSL for Trifacta databases

You can apply SSL secure access for connections to the Trifacta databases. For more information, see *Enable SSL for Databases*.

Configure Secure Access for Relational Connections

If you are enabling connections to relational databases, you must create and deploy a key file containing the credentials to use for your JDBC sources. These credentials are then used for encrypted access.

> **NOTE:** Encrypted authentication with your JDBC resources is required.

- For more information on enablement, see *Relational Access*.
- For more information on security, see *Configure Security for Relational Connections*.

Enhance Cluster Security

These options security options enhance the security of communications between the Trifacta node and the integrated cluster.

Configure for secure impersonation

Secure impersonation enables users to securely access the Hadoop cluster through a dedicated user or set of users, which enables use of cluster security features and permissions structures.

> **NOTE:** Secure impersonation requires Kerberos applied to the cluster.

See *Configure for Secure Impersonation*.

Configure for Kerberos Integration

If user access on your Hadoop cluster is secured via Kerberos, you can configure the platform to leverage this cluster security feature.

See *Configure for Kerberos Integration*.

Configure for KMS

Hadoop supports the use of encrypted transport to and from the cluster KMS system. Depending on the software distribution, configuration steps may vary.

> **NOTE:** If KMS is enabled on the cluster, you must configure KMS for the Trifacta platform regardless of other security features enabled on the cluster.

See *Configure for KMS*.

Enable SSL for HttpFS

Optionally, you can enable SSL connections between the Trifacta platform and the cluster's instance of HttpFS. See *Enable HttpFS*.

Enable SSL for Hive

You can configure SSL access to Hive. See *Configure for Hive*.