Admin console security

Redis Enterprise comes with a web-based user interface known as the admin console. The admin console provides the following security features:

- Encryption-in-transit using TLS/SSL
- User authentication using LDAP
- Role-based access control

We recommend the following practices:

- **Integrate with an external identity provider**: Redis Enterprise uses LDAP integration to support external identity providers, such as Active Directory.

- **Implement standard authentication practices**: If your organization does not support LDAP, you can still use Redis Enterprise’s user account security. Features include basic password complexity requirements, password expiration, and user login lockouts.

- **Limit session timeouts**: Session timeouts, also known as automatic sign out, help prevent unauthorized access. Admin console sessions are allowed to idle for a period of time before users are required to re-authenticate.

  By default, users are signed out after 15 minutes of inactivity. You can set the timeout period.

- **Require HTTPS for API endpoints** - Redis Enterprise comes with a REST API to help automate tasks. This API is available in both an encrypted and unencrypted endpoint for backward compatibility. You can disable the unencrypted endpoint with no loss in functionality.

- **Configure Transport Layer Security (TLS)** - A common compliance requirement is to set a minimum version of TLS. This helps to make sure that only secure versions of TLS are allowed when accessing the cluster.

- **Install your own certificates** - Redis Enterprise comes with self-signed certificates by default; however, many organizations require that you use specific CA signed certificates.

Updated: April 15, 2022