



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Deployment Guide

Cassandra Security

12/15/2025

---

## Contents

- 1 Cassandra Security
  - 1.1 Securing Access Interfaces

# Cassandra Security

This article describes how to tune secure access from your Co-browse Server to external Cassandra. Starting from 8.5.1, you can secure the following when using external Cassandra:

- [Secure the access interfaces](#) using authentication and authorization.
- Secure network traffic using TLS.

## Securing Access Interfaces

You can secure your access interfaces based on an authentication and authorization scheme. In other words, Cassandra needs to know:

- **Authentication**—who is trying to access the system?
- **Authorization**—is the user allowed to access the system and what data can the user access?

With the default setup, anybody can access any data. To secure access interfaces from Co-browse Server to external Cassandra, you must:

1. [Turn on authentication and authorization in your Cassandra configuration.](#)
2. [Set up a new Cassandra user to access the Co-browse keyspace.](#)
3. [Specify Cassandra user settings in the Resource Access Point configuration.](#)

## Configure Cassandra to Use Authentication and Authorization

Configure Cassandra by editing **<Cassandra installation directory>/conf/cassandra.yaml**.

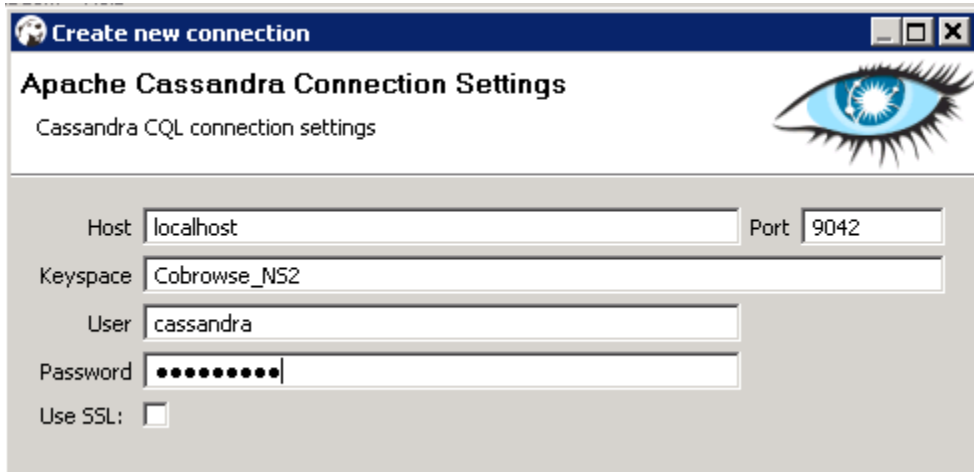
1. Set the **authenticator** option to PasswordAuthenticator. It's set to AllowAllAuthenticator by default.
2. Set the **authorizer** option to CassandraAuthorizer. It's set to AllowAllAuthorizer by default.
3. Optionally, tune your **system\_auth** keyspace replication according to the [DataStax system\\_auth documentation](#). Note that the validity period for permissions caching is 2000 ms. For more information about Cassandra permissions, see the [DataStax Object permissions documentation](#).
4. Restart your Cassandra node.

## Set Up a New Cassandra User

To set up a new Cassandra user, use a Cassandra client tool like **dbeaver** or **cqlsh**:

1. Start by connecting to Cassandra using the default superuser name and password, **cassandra/cassandra**. The following examples use dbeaver and cqlsh as examples but you can use a different Cassandra client:
  - **dbeaver:**

Navigate to **New connection > Cassandra CQL > Apache Cassandra Connection Settings**. Specify the **Host** and **Keyspace**. Use your superuser login for **User** and **Password**.



- **cqlsh:**

Start cqlsh using the default superuser name and password:

```
./cqlsh -u cassandra -p cassandra
```

2. Use the **CREATE USER** CQL statement to create another superuser. For example:

```
CREATE USER IF NOT EXISTS <new_cobrowse_user> WITH PASSWORD 'new_password' SUPERUSER
```

3. Use the **GRANT** CQL statement to grant access permissions. For example:

```
GRANT ALL PERMISSIONS ON <cobrowse_keyspace> TO <new_cobrowse_user>
```

CQL also supports the authorization statements **GRANT**, **LIST PERMISSIONS**, and **REVOKE**.

## Deactivate Default Superuser

Optionally, you can now deactivate the default superuser **cassandra**:

1. Login as your new superuser.
2. Change the password for the **cassandra** user.
3. Turn off the superuser status for the **cassandra** user.

## Configure Resource Access Point

Use the login information of the **superuser you created** to configure the Cassandra Resource Access Point:

1. Open or create a **cassandraClient** configuration options section.
2. Set the **userName** and **password** to your superuser's login.

The screenshot shows the Genesys Administrator web interface. The top navigation bar includes the Genesys logo, the title "Genesys Administrator", a tenant dropdown set to "Environment", and links for "New Window", "Log out", and a settings icon. Below this is a main navigation bar with tabs for "MONITORING", "PROVISIONING", "DEPLOYMENT", and "OPERATIONS". The "PROVISIONING" tab is active, and the breadcrumb trail shows "PROVISIONING > Environment > Applications > CasRAP\_2".

On the left is a "Navigation" sidebar with a search bar and a tree view containing "Environment", "Alarm Conditions", "Scripts", "Application Templates", "Applications" (highlighted), "Hosts", "Switching", "Routing/eServices", "Desktop", "Accounts", "Voice Platform", and "Outbound Contact".

The main content area is titled "CasRAP\_2 - \Applications\Co-browse\External C\* cluster\". It features a toolbar with buttons: "Cancel", "Save & Close", "Save", "Save & New", "Reload", "Uninstall", "Start", "Stop", and "Graceful Stop". Below the toolbar are tabs for "Configuration", "Options" (selected), "Permissions", "Dependencies", "Alarms", and "Logs".

Under the "Options" tab, there are buttons for "New", "Delete", "Export", and "Import", and a "View: Advanced View (Options)" dropdown. A table with columns "Name", "Section", "Option", and "Value" displays the configuration. A "Filter" row is present above the data rows.

Name	Section	Option	Value
cassandraClient (3 Items)			
cassandraClient/password	cassandraClient	password	*****
cassandraClient/transportCompression	cassandraClient	transportCompre...	LZ4
cassandraClient/userName	cassandraClient	userName	cobrowse_user
resource (1 Item)			
resource/type	resource	type	cassandra

At the bottom, there is a pagination bar showing "Page 1 of 1" and a refresh icon. On the right, it says "Displaying objects 1 - 4 of 4".