Configure ISE 3.2 Data Connect Integration with Splunk

Contents

Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) 3.2 integration with Splunk over Data Connect to retrieve reporting data from the ISE database directly. You can create your own queries and craft your own reports thanks to it.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

1. Cisco ISE 3.2
2. Basic knowledge about Oracle queries
3. Splunk

Components Used

The information in this document is based on these software and hardware versions:

1. Cisco ISE 3.2

2. Splunk 9.0.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

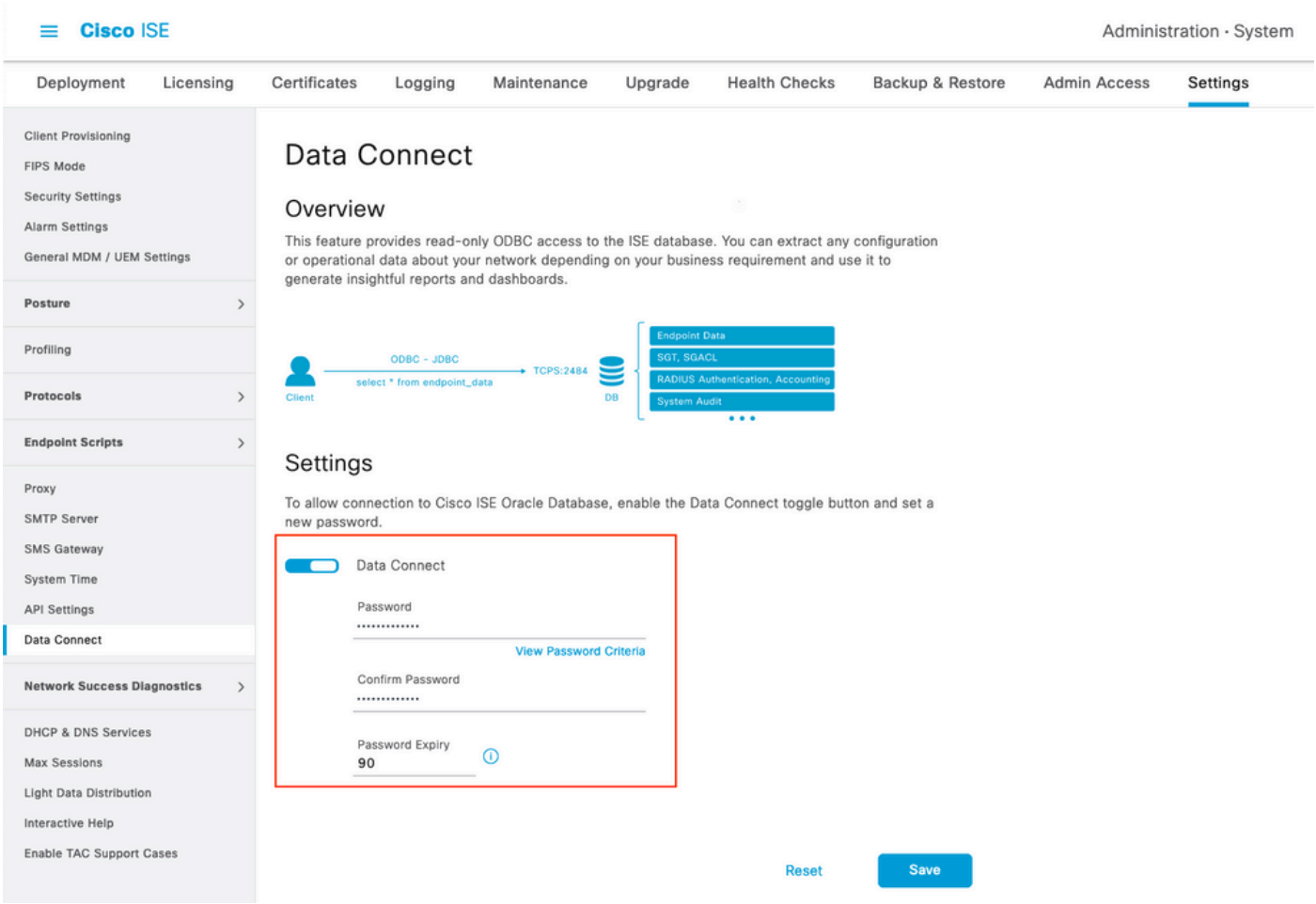
Configure

Configurations

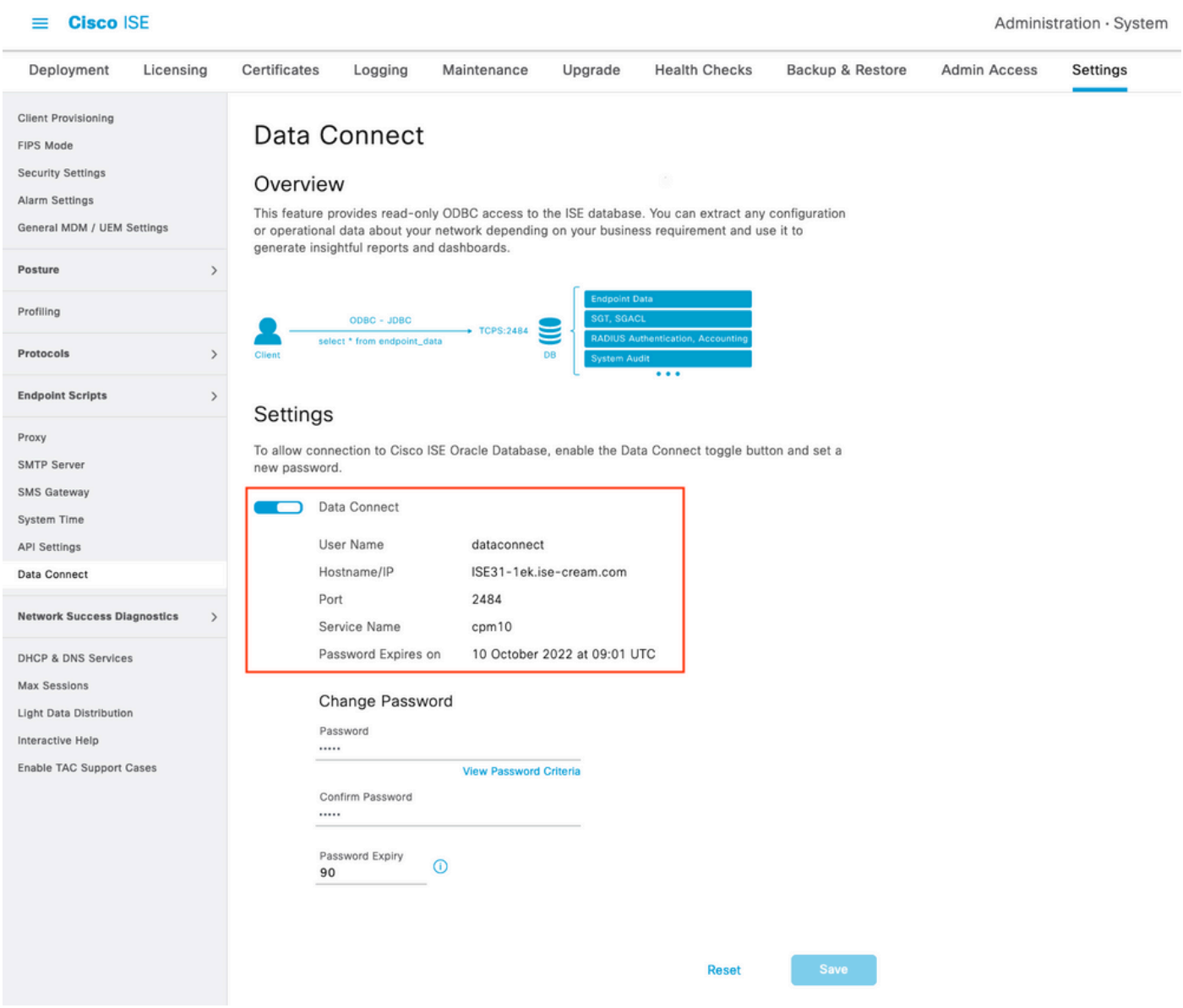
Step 1. Configure ISE Data Connect Settings

1. Enable Data Connect

On ISE, navigate to **Administration > System > Settings > Data Connect**and toggle the button against **Data Connect**. Enter the password and click on **Save** .



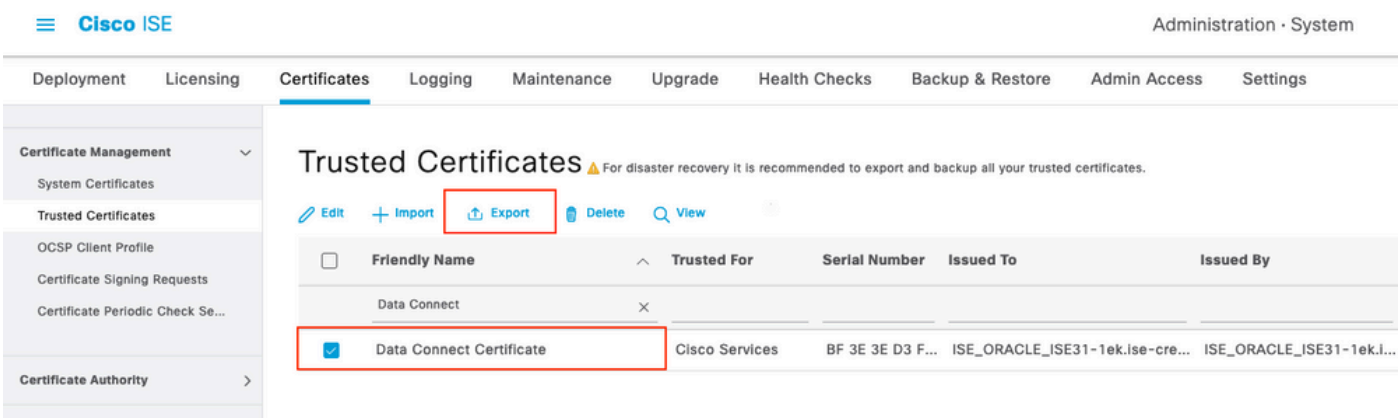
Make a note of Data Connect settings, which include **User Name, Hostname, Port, and Service Name** .Data Connect by default is enabled on Secondary MNT in a distributed deployment, more information about failover scenarios can be found in the Administrator Guide.



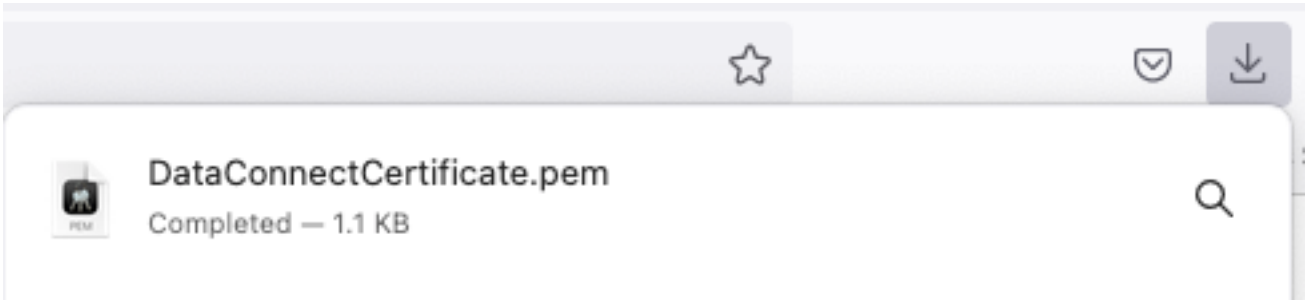
2. Export Data Connect Certificate

Operation in **Step 1.**triggered the creation of the Data Connect Certificate. It needs to be trusted by the clients who query ISE over Data Connect.

In order to export the certificate, navigate to **Administration > System > Settings > Cetificate Management > Trusted Certificates**,select Certificate with **Data Connect Certificate** Friendly Name and click on **Export** .



The certificate is exported in PEM format.

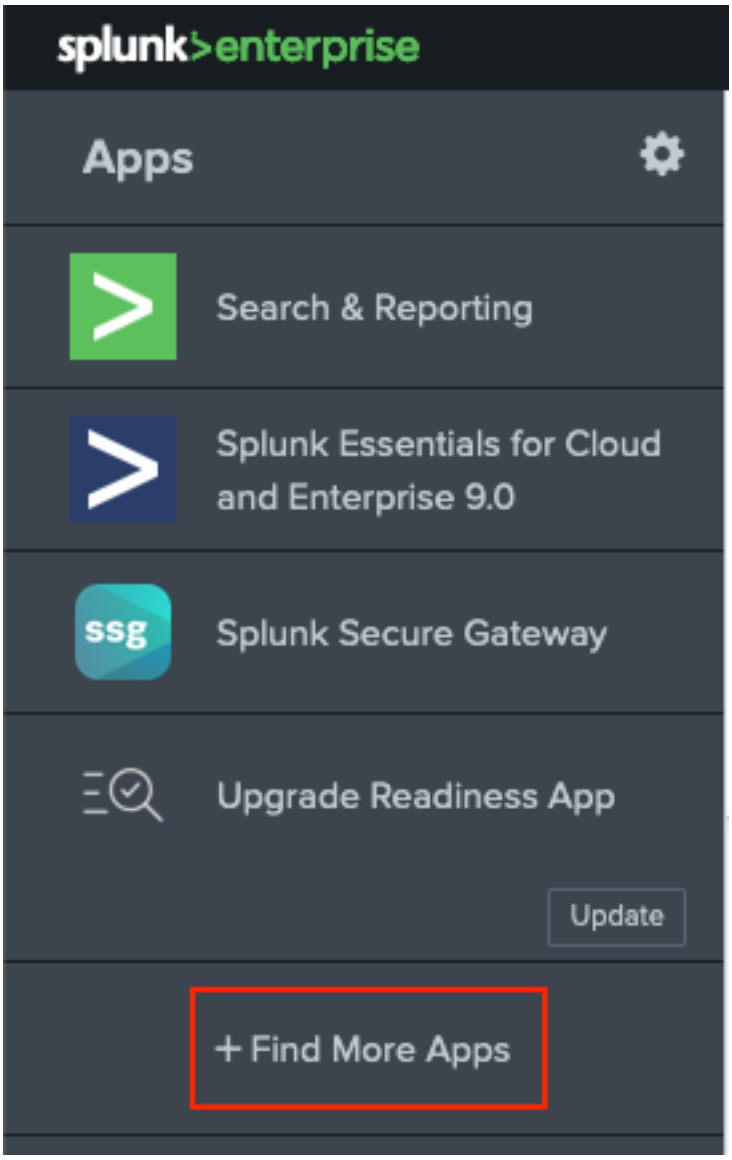


Step 2. Configure Splunk

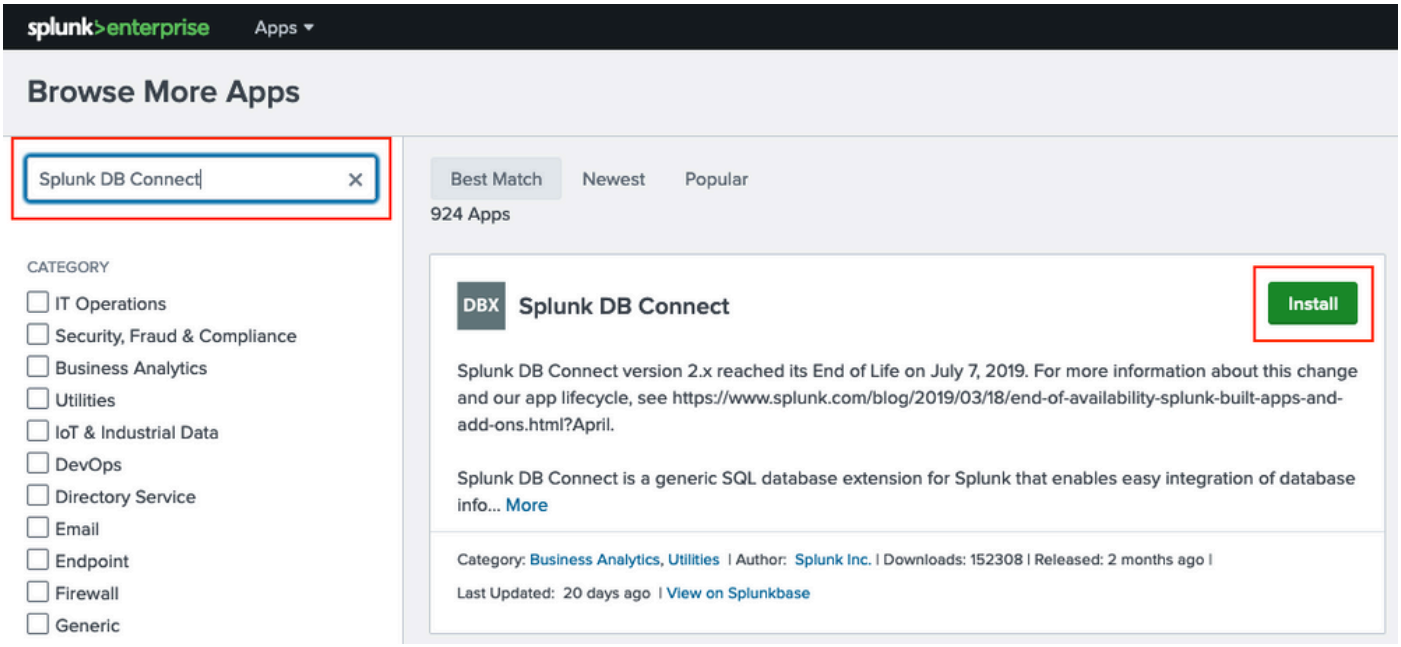
> **Note:** Splunk installation is outside the scope of this document.

1. Install Splunk DB Connect App

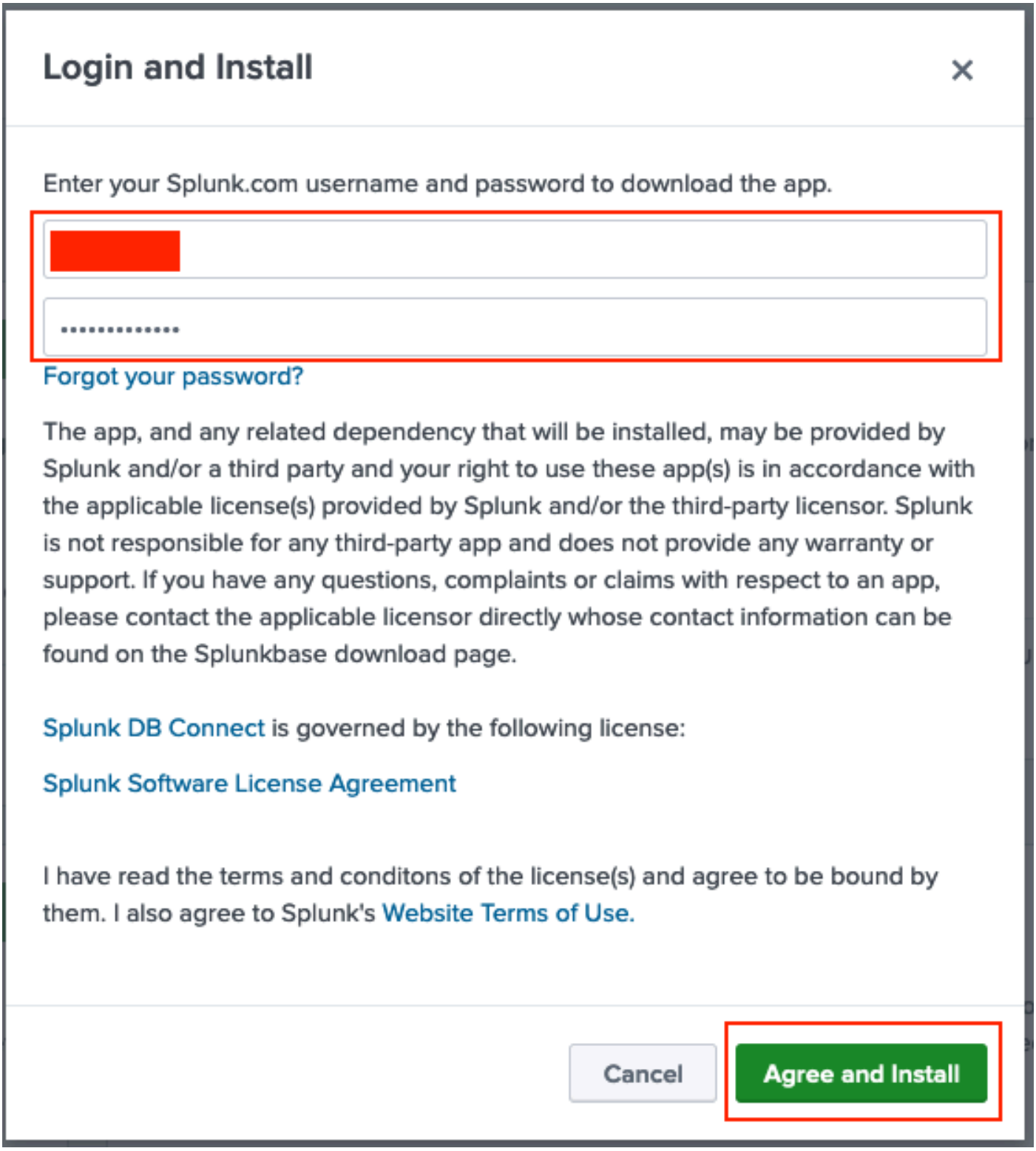
Click on **+ Find More Apps** from the main menu.



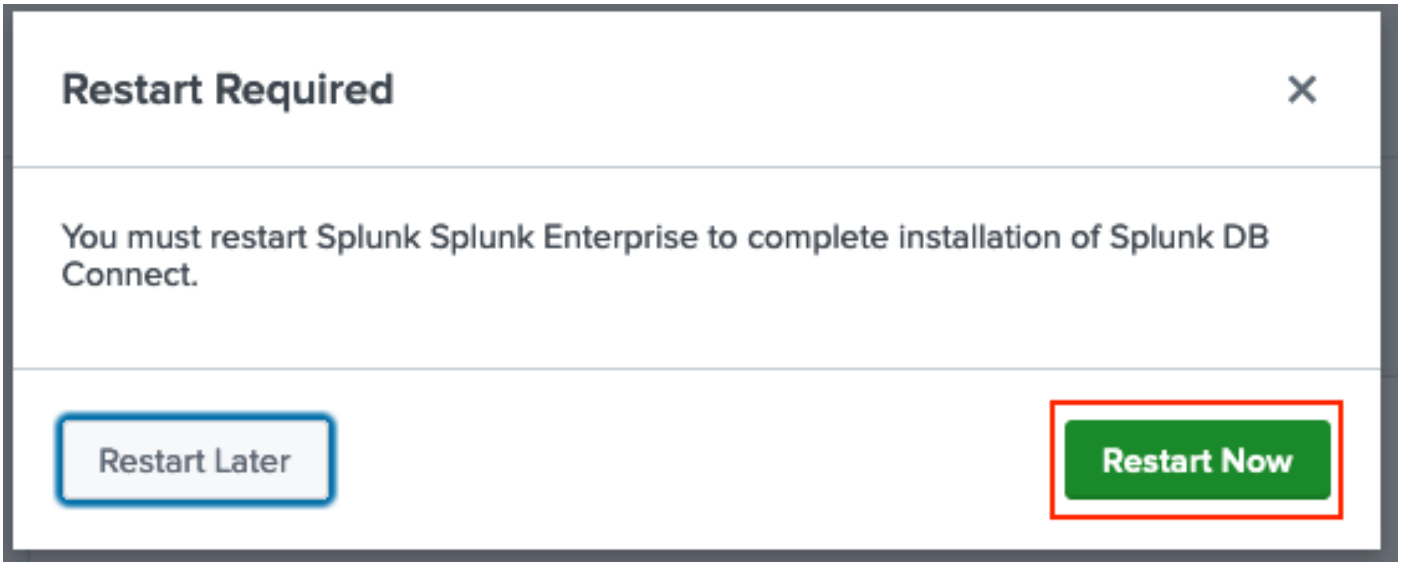
Enter **Splunk DB Connect** in the search menu and click on **Install**against **Splunk DB Connect** App as shown in the image.



Enter Splunk credentials in order to install the App. Click on **Agree and Install** as shown in the image.



App Installation requires the restart, click on **Restart Now**.



2. Install Oracle Drivers

As per Splunk Documentation, JDBC drivers must be installed. Install the Oracle driver through the Splunk add-ons for DB Connect. Click on **Login to Download** as shown in the image.

Click on **Download**.

From the Home menu, click on the Gear icon next to **Apps** as shown in the image.