

Configure ISE 3.2 Data Connect Integration with Splunk

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configurations](#)

[Step 1. Configure ISE Data Connect Settings](#)

[1. Enable Data Connect](#)

[2. Export Data Connect Certificate](#)

[Step 2. Configure Splunk](#)

[1. Install Splunk DB Connect App](#)

[2. Install Oracle Drivers](#)

[3. Configure Splunk DB Connect App Identity](#)

[4. Configure Splunk DB Connect App Connection](#)

[5. Configure Splunk DB Connect Inputs](#)

[Verify](#)

[Troubleshoot](#)

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**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration - System' and various menu items like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar lists various configuration categories, with 'Data Connect' selected. The main content area is titled 'Data Connect' and has an 'Overview' section. Below the overview is a diagram showing a 'Client' connected to a 'DB' (Database) via 'ODBC - JDBC' with the query 'select * from endpoint_data'. The database contains tables for 'Endpoint Data', 'SGT, SGACL', 'RADIUS Authentication, Accounting', and 'System Audit'. The 'Settings' section below the diagram contains a toggle for 'Data Connect' which is turned on. Below the toggle are fields for 'Password', 'Confirm Password', and 'Password Expiry' (set to 90). A red box highlights the 'Data Connect' toggle and the password fields. At the bottom right, there are 'Reset' and 'Save' buttons.

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.

- Client Provisioning
- FIPS Mode
- Security Settings
- Alarm Settings
- General MDM / UEM Settings
- Posture**
- Profiling
- Protocols
- Endpoint Scripts
- Proxy
- SMTP Server
- SMS Gateway
- System Time
- API Settings
- Data Connect**
- Network Success Diagnostics
- DHCP & DNS Services
- Max Sessions
- Light Data Distribution
- Interactive Help
- Enable TAC Support Cases

Data Connect

Overview

This feature provides read-only ODBC access to the ISE database. You can extract any configuration or operational data about your network depending on your business requirement and use it to generate insightful reports and dashboards.



Settings

To allow connection to Cisco ISE Oracle Database, enable the Data Connect toggle button and set a new password.

Data Connect

| | |
|---------------------|------------------------------|
| User Name | dataconnect |
| Hostname/IP | ISE31-1ek.ise-cream.com |
| Port | 2484 |
| Service Name | cpm10 |
| Password Expires on | 10 October 2022 at 09:01 UTC |

Change Password

Password
.....

[View Password Criteria](#)

Confirm Password
.....

Password Expiry ?
90

Reset

Save

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 > Certificate Management > Trusted Certificates**, select Certificate with **Data Connect Certificate Friendly Name** and click on **Export**.

- Certificate Management**
- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...
- Certificate Authority

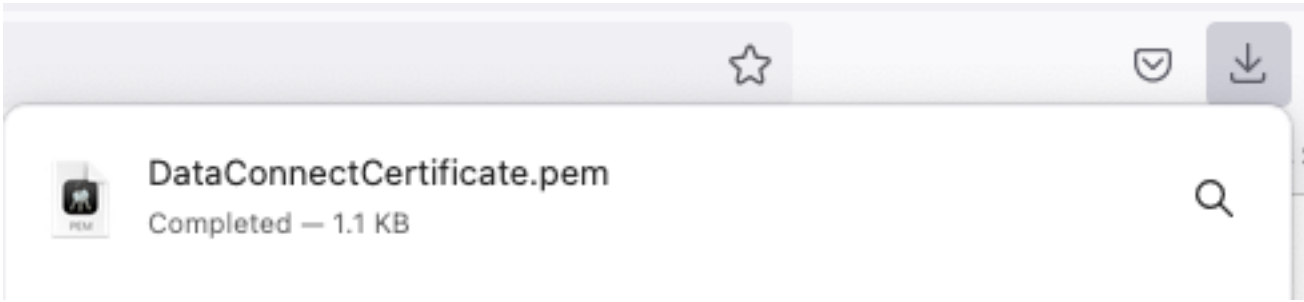
Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

[Edit](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

| <input type="checkbox"/> | Friendly Name | Trusted For | Serial Number | Issued To | Issued By |
|-------------------------------------|--------------------------|----------------|------------------|---------------------------------|---------------------------|
| <input type="checkbox"/> | Data Connect | X | | | |
| <input checked="" type="checkbox"/> | Data Connect Certificate | Cisco Services | BF 3E 3E D3 F... | ISE_ORACLE_ISE31-1ek.ise-cre... | ISE_ORACLE_ISE31-1ek.i... |

The certificate is exported in PEM format.

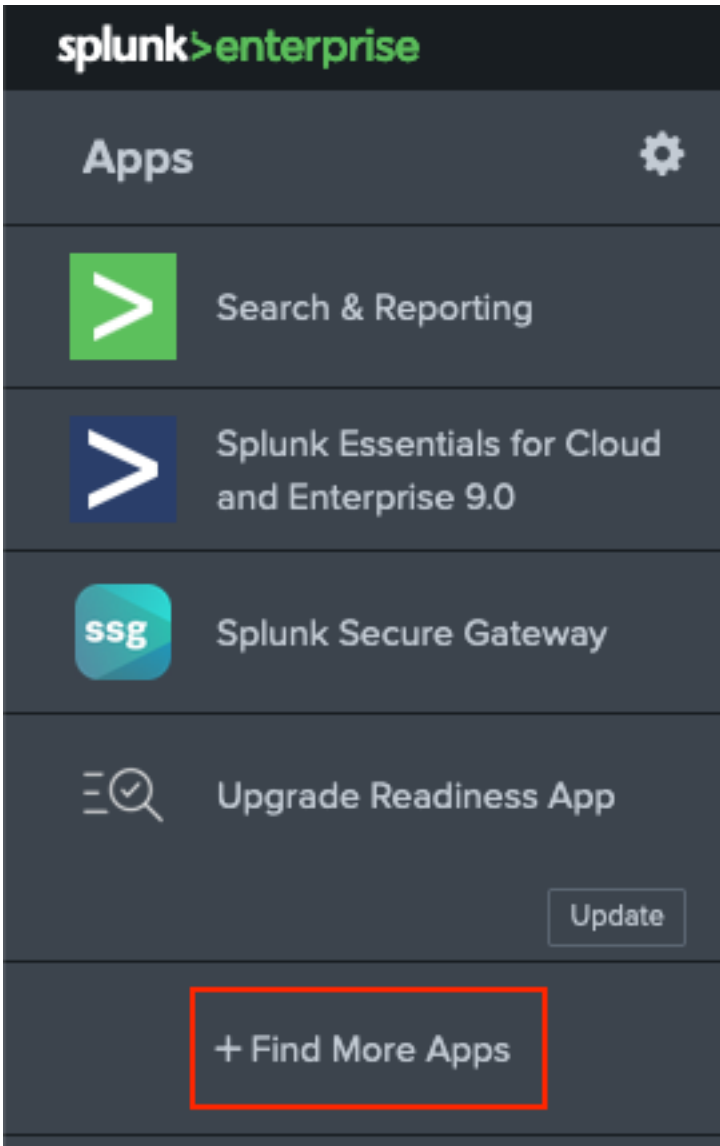


Step 2. Configure Splunk

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.

Browse More Apps

Splunk DB Connect ×

Best Match Newest Popular

924 Apps

CATEGORY

- IT Operations
- Security, Fraud & Compliance
- Business Analytics
- Utilities
- IoT & Industrial Data
- DevOps
- Directory Service
- Email
- Endpoint
- Firewall
- Generic

DBX Splunk DB Connect

Install

Splunk DB Connect version 2.x reached its End of Life on July 7, 2019. For more information about this change and our app lifecycle, see <https://www.splunk.com/blog/2019/03/18/end-of-availability-splunk-built-apps-and-add-ons.html?April>.

Splunk DB Connect is a generic SQL database extension for Splunk that enables easy integration of database info... [More](#)

Category: [Business Analytics](#), [Utilities](#) | Author: [Splunk Inc.](#) | Downloads: 152308 | Released: 2 months ago |

Last Updated: 20 days ago | [View on Splunkbase](#)

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

Login and Install



Enter your Splunk.com username and password to download the app.

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app and does not provide any warranty or support. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

[Splunk DB Connect](#) is governed by the following license:

[Splunk Software License Agreement](#)

I have read the terms and conditions of the license(s) and agree to be bound by them. I also agree to Splunk's [Website Terms of Use](#).

Cancel

Agree and Install

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

Restart Required ×

You must restart Splunk Splunk Enterprise to complete installation of Splunk DB Connect.

[Restart Later](#) [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.

SPLUNK

AddOn+ **Splunk DBX Add-on for Oracle JDBC**

★★★★★ 0 rating

Splunk Cloud Splunk Built

Overview Details

JDBC driver for Oracle Database provides Oracle Database JDBC driver. Drivers can be use by others Splunk apps like DB Connect.

Release Notes

Version 2.1.0 March 1, 2022

1,003 Downloads

LOGIN TO DOWNLOAD

VERSION
2.1.0 ▾

Click on **Download**.

SPLUNK



Splunk DBX Add-on for Oracle JDBC

★★★★★ 0 rating

Splunk Cloud Splunk Built

Overview

Details

JDBC driver for Oracle Database provides Oracle Database JDBC driver. Drivers can be use by others Splunk apps like DB Connect.

Release Notes

Version 2.1.0 March 1, 2022

1,003

Downloads

Download

Rate this App

VERSION

2.1.0 ▾

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

