

使用Splunk配置ISE 3.2資料連線整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[組態](#)

[步驟1.配置ISE資料連線設定](#)

[1.啟用資料連線](#)

[2.匯出資料連線證書](#)

[步驟2.配置Splunk](#)

[1.安裝Splunk DB Connect App](#)

[2.安裝Oracle驅動程式](#)

[3.配置Splunk DB Connect應用標識](#)

[4.配置Splunk DB Connect應用連線](#)

[5.配置Splunk DB連線輸入](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)3.2與Splunk over Data Connect的整合，以便直接從ISE資料庫檢索報告資料。藉助它，您可以建立自己的查詢並編寫自己的報告。

必要條件

需求

思科建議您瞭解以下主題：

1. Cisco ISE 3.2
2. 有關Oracle查詢的基本知識
3. 斯普倫克

採用元件

本文中的資訊係根據以下軟體和硬體版本：

1. Cisco ISE 3.2
2. Splunk 9.0.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

組態

步驟1.配置ISE資料連線設定

1.啟用資料連線

在ISE上，導航至 **Administration > System > Settings > Data Connect**並將按鈕切換為 **Data Connect**.輸入密碼並按一下 **Save** .

The screenshot shows the Cisco ISE Administration console interface. 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' highlighted. The main content area is titled 'Data Connect' and includes an 'Overview' section explaining the feature's purpose. Below the overview is a diagram showing a 'Client' connecting to a 'DB' (Database) via 'ODBC - JDBC' using the query 'select * from endpoint_data'. The database contains tables for 'Endpoint Data', 'SGT, SGACL', 'RADIUS Authentication, Accounting', and 'System Audit'. The 'Settings' section contains a toggle for 'Data Connect' (which is turned on), a 'Password' field with a 'View Password Criteria' link, a 'Confirm Password' field, and a 'Password Expiry' field set to '90'. At the bottom right, there are 'Reset' and 'Save' buttons.

記下資料連線設定，包括 **User Name, Hostname, Port, and Service Name** .分散式部署中的輔助MNT上預設啟用資料連線，有關故障轉移方案的詳細資訊，請參閱《管理員指南》。

- 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. 匯出資料連線證書

中的操作 Step 1.已觸發資料連線證書的建立。需要通過資料連線查詢ISE的客戶端需要信任它。

若要匯出證書，請導航至 Administration > System > Settings > Certificate Management > Trusted Certificates，選擇證書 Data Connect Certificate 友好名稱並按一下 Export。

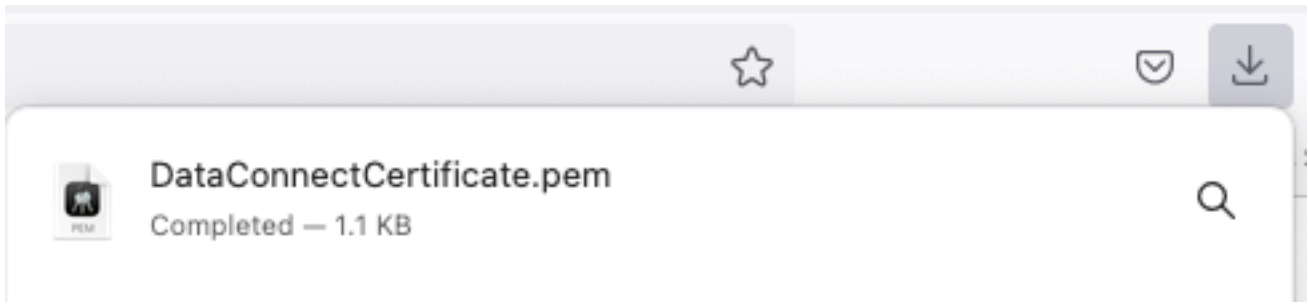
- Certificate Management**
- System Certificates
- Trusted Certificates**
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...
- Certificate Authority

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... |

證書將以PEM格式匯出。

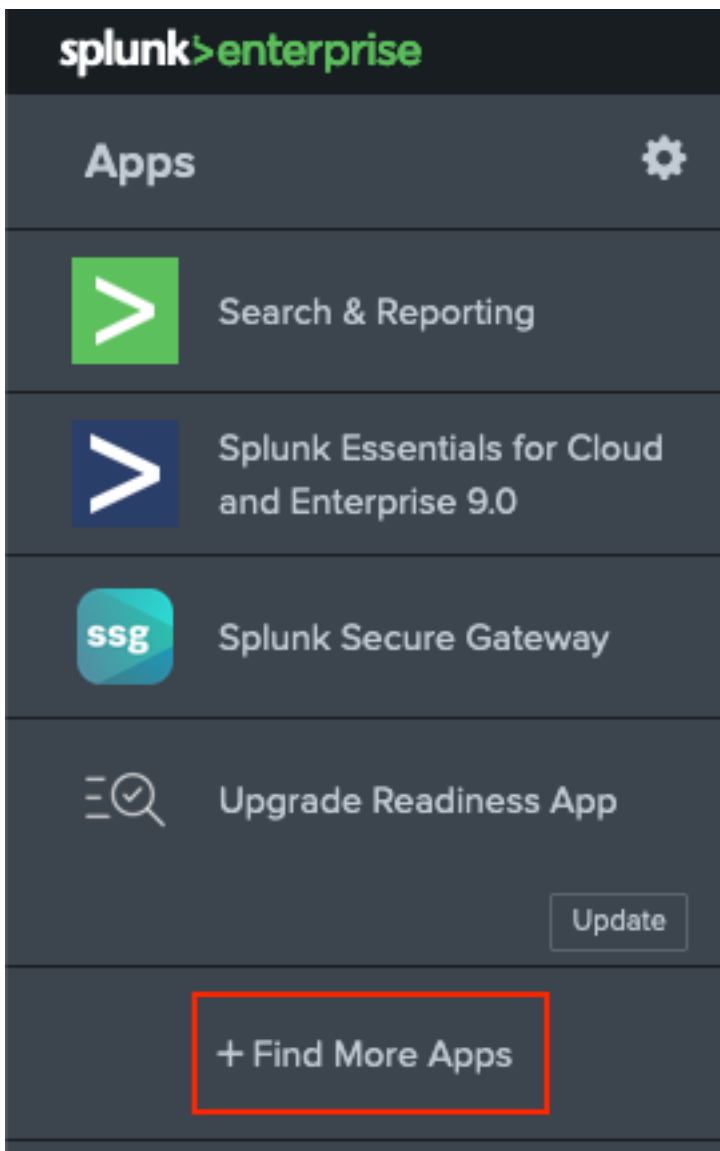


步驟2. 配置Splunk

附註： Splunk安裝不在本檔案的範圍之內。

1. 安裝Splunk DB Connect App

按一下 + Find More Apps 從主選單。



輸入 Splunk DB Connect 在「搜尋」選單中，按一下 Install 對 Splunk DB Connect App (如圖所示)。

Browse More Apps

 X

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](#)

輸入Splunk憑據以安裝應用。按一下 **Agree and Install** 如下圖所示。

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:

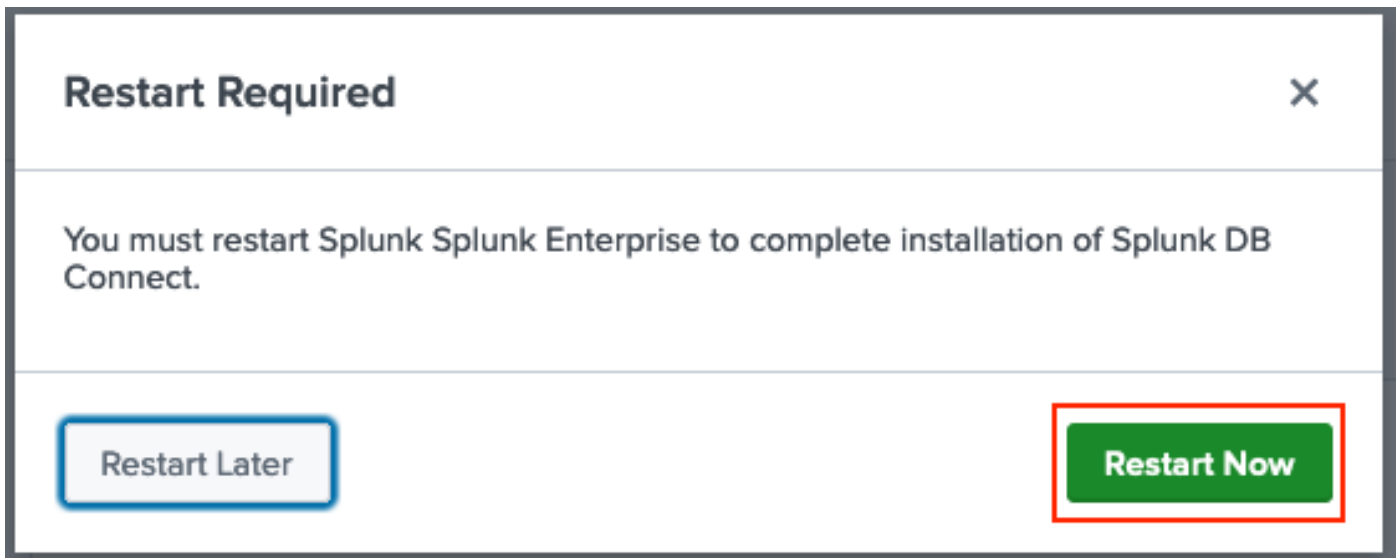
[Splunk Software License Agreement](#)

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

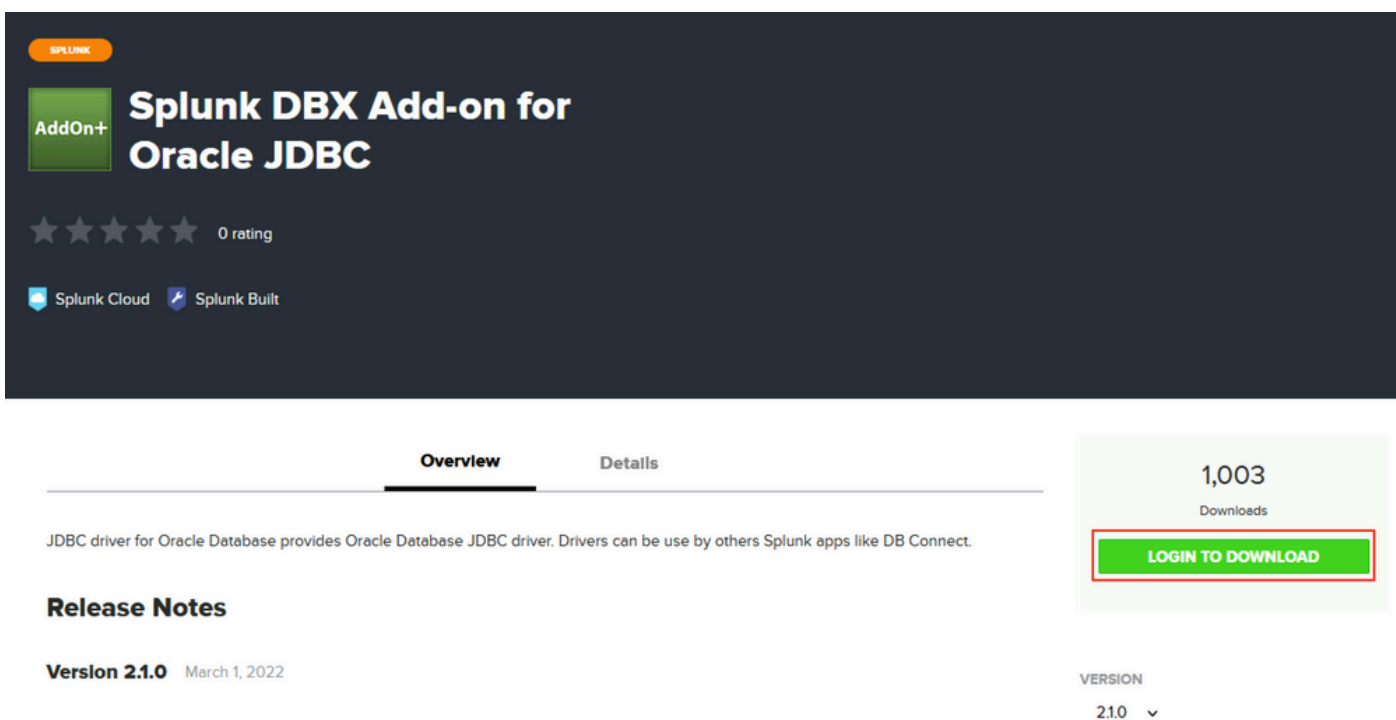
Agree and Install

應用程式安裝需要重新啟動，請按一下 **Restart Now**。



2.安裝Oracle驅動程式

根據[Splunk文檔](#)，必須安裝JDBC驅動程式。通過用於[DB Connect](#)的Splunk載入項安裝Oracle驅動程式。按一下 [Login to Download](#) 如下圖所示。



按一下 [Download](#).

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

Download Rate this App

VERSION
2.1.0 ▾

在「首頁」(Home)選單中，按一下旁邊的「齒輪」(Gear)圖示 Apps 如下圖所示。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。