

使用Splunk配置ISE 3.2数据连接集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[步骤1.配置ISE数据连接设置](#)

[1.启用数据连接](#)

[2.导出数据连接证书](#)

[步骤2.配置Splunk](#)

[1.安装Splunk DB Connect应用](#)

[2.安装Oracle驱动程序](#)

[3.配置Splunk DB Connect应用标识](#)

[4.配置Splunk DB Connect应用连接](#)

[5.配置Splunk DB连接输入](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何配置思科身份服务引擎(ISE)3.2与Splunk over Data Connect的集成，以直接从ISE数据库检索报告数据。您可以创建自己的查询，并创建自己的报告。

先决条件

要求

Cisco 建议您了解以下主题：

1. 思科ISE 3.2
2. 有关Oracle查询的基本知识
3. Splunk

使用的组件

本文档中的信息基于以下软件和硬件版本：

1. 思科ISE 3.2
2. Splunk 9.0.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

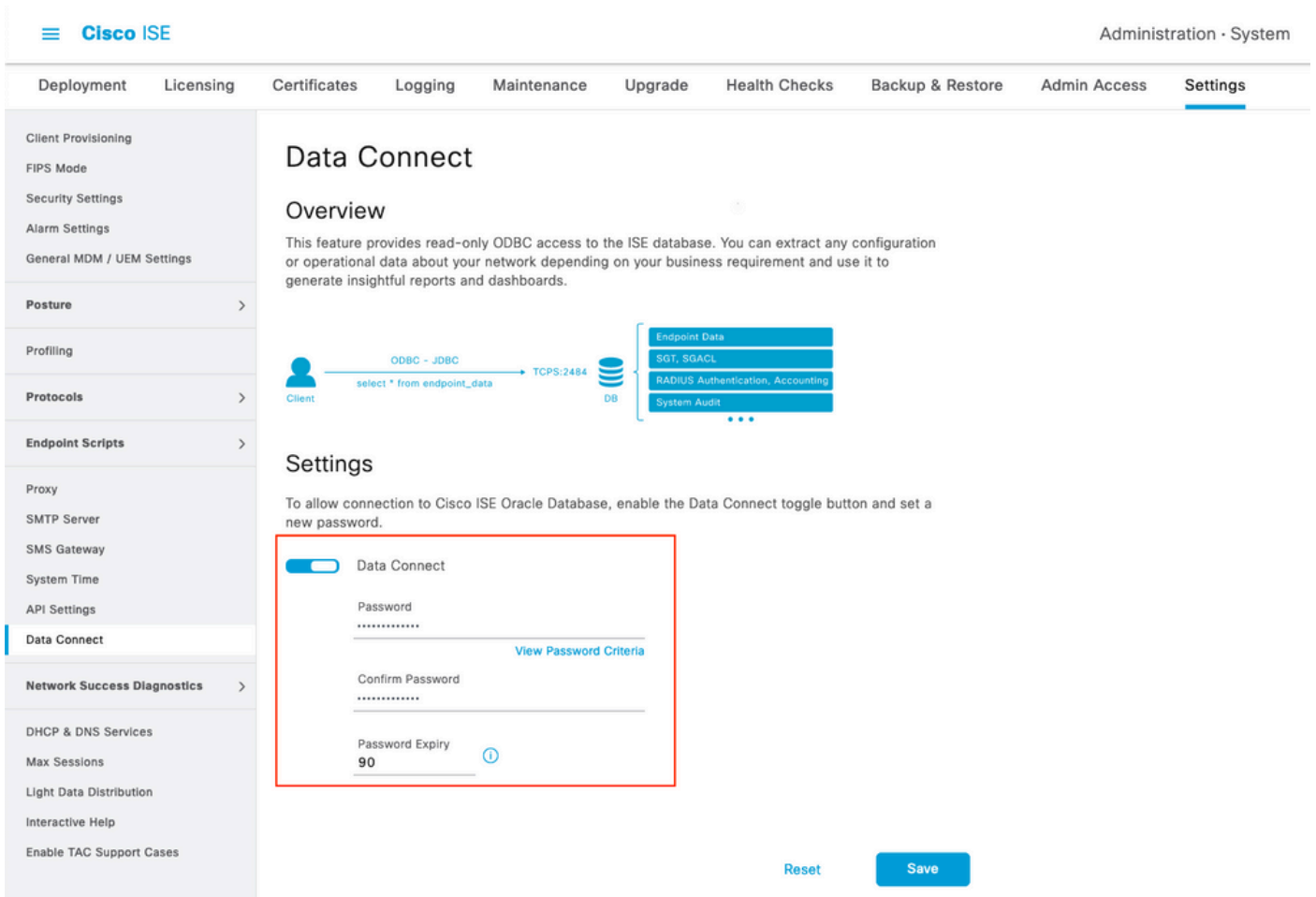
配置

配置

步骤1.配置ISE数据连接设置

1.启用数据连接

在ISE上，导航至 **Administration > System > Settings > Data Connect**并切换按钮 **Data Connect**.输入密码并单击 **Save** .



记录Data Connect设置，包括 **User Name, Hostname, Port, and Service Name** .默认情况下，在分布式部署中的辅助MNT上启用Data Connect，有关故障转移方案的详细信息，请参阅《管理员指南》。

- 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.导出数据连接证书

中的操作 Step 1.已触发数据连接证书的创建。它需要由通过数据连接查询ISE的客户端信任。

要导出证书，请导航至 Administration > System > Settings > Certificate Management > Trusted Certificates，选择 Certificate with Data Connect Certificate 友好名称并单击 Export。

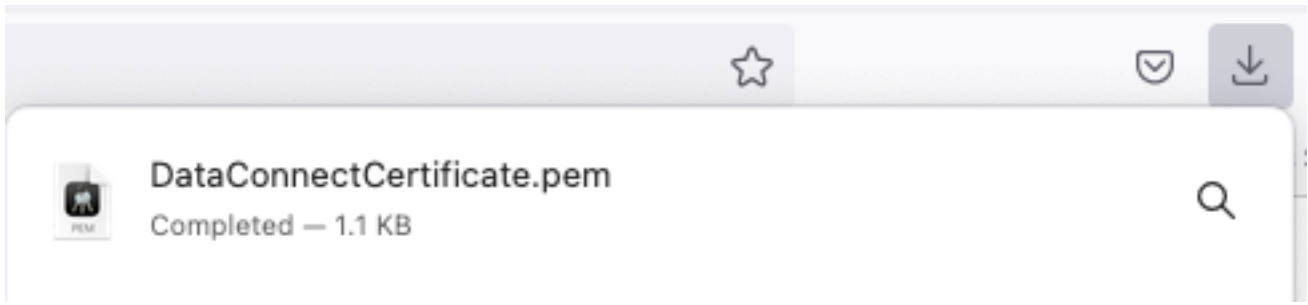
- Certificate Management**
 - System Certificates
 - Trusted Certificates**
 - OCSF Client Profile
 - Certificate Signing Requests
 - Certificate Periodic Check Se...
- Certificate Authority

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...

证书将以PEM格式导出。

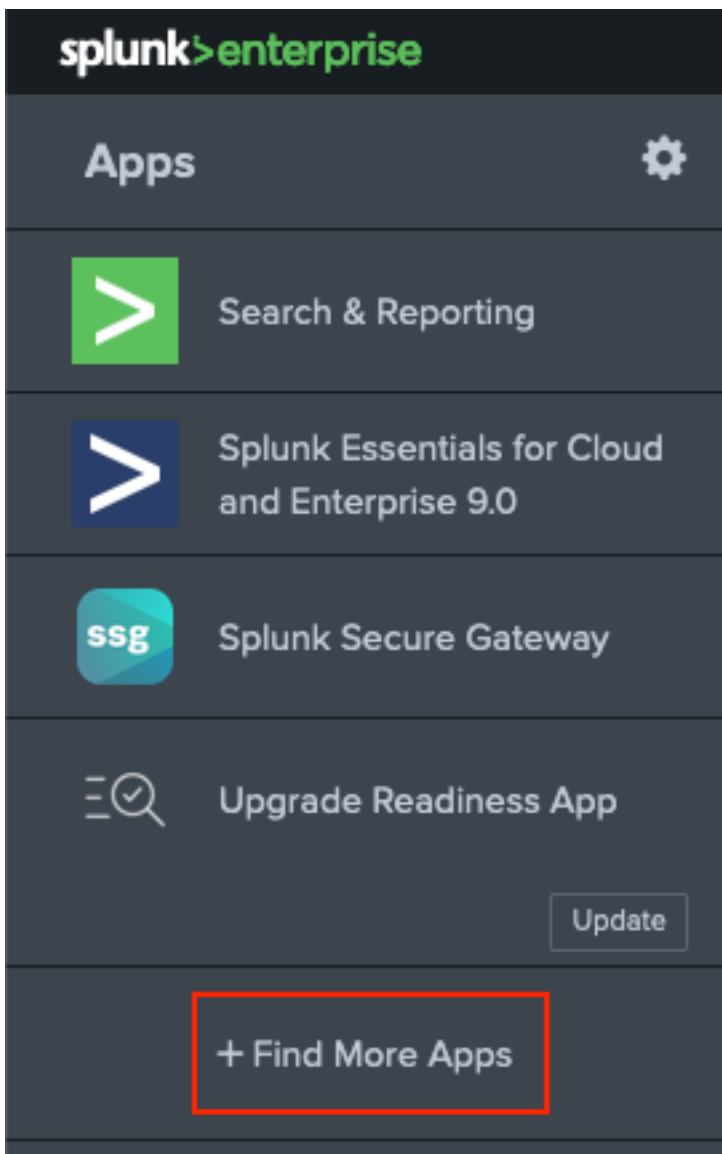


步骤2.配置Splunk

注意：Splunk安装不在本文档的讨论范围之内。

1.安装Splunk DB Connect应用

点击 + Find More Apps 从主菜单。



输入 Splunk DB Connect 在“搜索”菜单中并单击 Install针对 Splunk DB Connect 如图所示。

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](#)

输入Splunk凭据以安装应用。点击 **Agree and Install** 如图所示。

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:

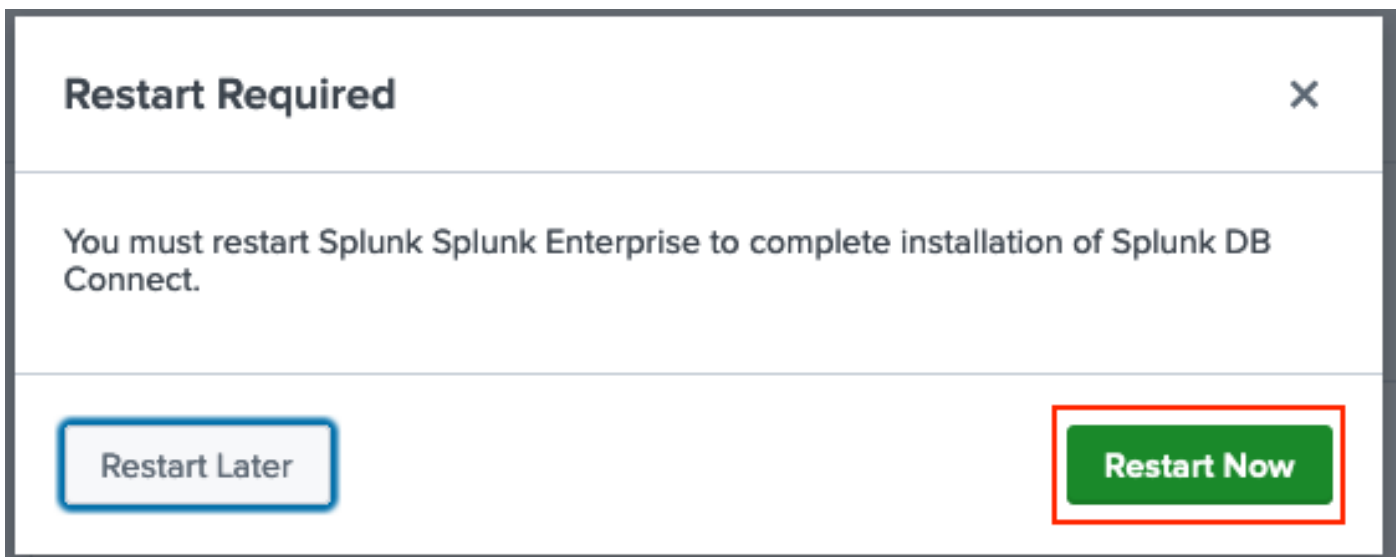
[Splunk Software License Agreement](#)

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

应用安装需要重新启动，请单击 **Restart Now**。



2.安装Oracle驱动程序

根据[Splunk文档](#)，必须安装JDBC驱动程序。通过用于DB Connect的Splunk加载项安装[Oracle驱动程序](#)。点击 [Login to Download](#) 如图所示。

A screenshot of the Splunk Add-on marketplace page for "Splunk DBX Add-on for Oracle JDBC". The page header includes the Splunk logo and "AddOn+". The product title is "Splunk DBX Add-on for Oracle JDBC". Below the title, there are five stars and "0 rating". It is marked as "Splunk Cloud" and "Splunk Built". The page has two tabs: "Overview" (selected) and "Details". The description states: "JDBC driver for Oracle Database provides Oracle Database JDBC driver. Drivers can be use by others Splunk apps like DB Connect." On the right side, there is a box showing "1,003 Downloads" and a green "LOGIN TO DOWNLOAD" button. Below the description, there is a "Release Notes" section with "Version 2.1.0" dated "March 1, 2022". At the bottom right, there is a "VERSION" dropdown menu currently set to "2.1.0".

点击 [Download](#).

The screenshot shows the Splunk App Store interface for the 'Splunk DBX Add-on for Oracle JDBC'. At the top left, there is a 'SPLUNK' logo and an 'AddOn+' badge. The main title is 'Splunk DBX Add-on for Oracle JDBC'. Below the title, there are five stars and the text '0 rating'. At the bottom left, there are icons for 'Splunk Cloud' and 'Splunk Built'. The page has two tabs: 'Overview' (selected) and 'Details'. A description states: 'JDBC driver for Oracle Database provides Oracle Database JDBC driver. Drivers can be use by others Splunk apps like DB Connect.' Under the 'Release Notes' section, 'Version 2.1.0' is listed with the date 'March 1, 2022'. On the right side, there is a green box containing '1,003 Downloads', a red-bordered 'Download' button, and a 'Rate this App' button. Below this, a 'VERSION' dropdown menu is set to '2.1.0'.

在“主页”(Home)菜单中，点击旁边的“齿轮”(Gear)图标 Apps 如图所示.

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。