

# Jira Cloud

Guia de implementação

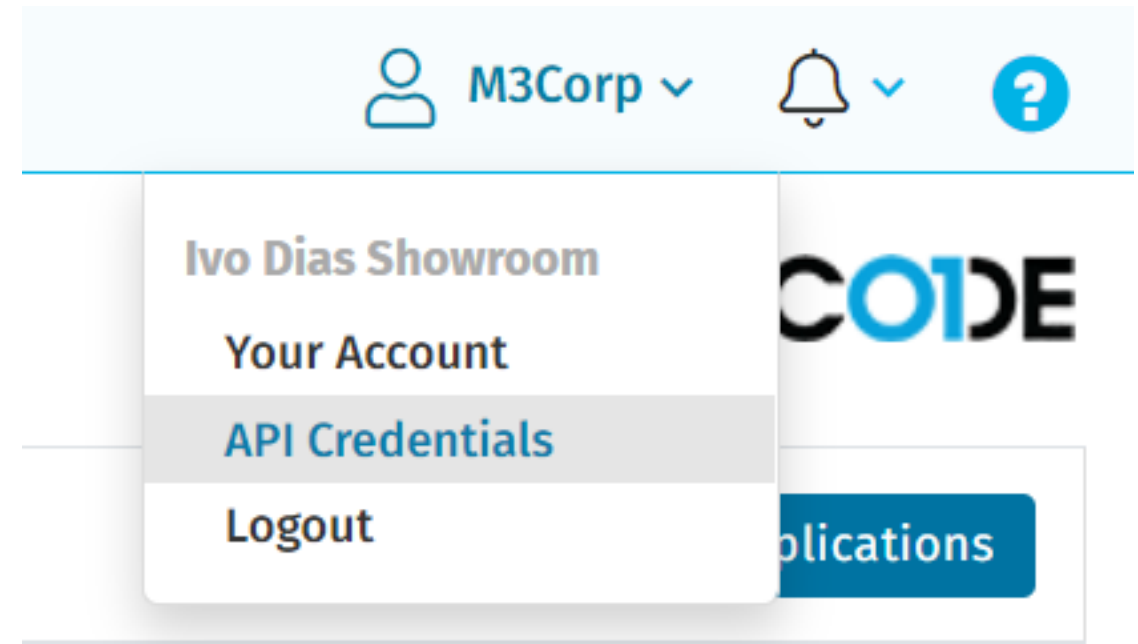
VERACODE



# Credenciais API



- Nosso primeiro passo é obter as credenciais no portal da Veracode
- O recomendado é a criação de um usuário API específico para essas integrações
  - Detalhes:  
<https://www.youtube.com/watch?v=juNzhEsytw>
- Conforme a imagem ao lado, precisamos apenas clicar no nosso usuário no canto superior esquerdo e selecionamos a opção de credenciais



# Credenciais API



- Vamos precisar do ID e da Secret Key para fazer as integrações
- Por padrão, essas credenciais duram 1 ano, mas conforme a imagem é possível revoga-las a qualquer momento

## Credentials Details

[Generate API Credentials](#)[Revoke API Credentials](#)**ID:**

\*\*\*\*\*

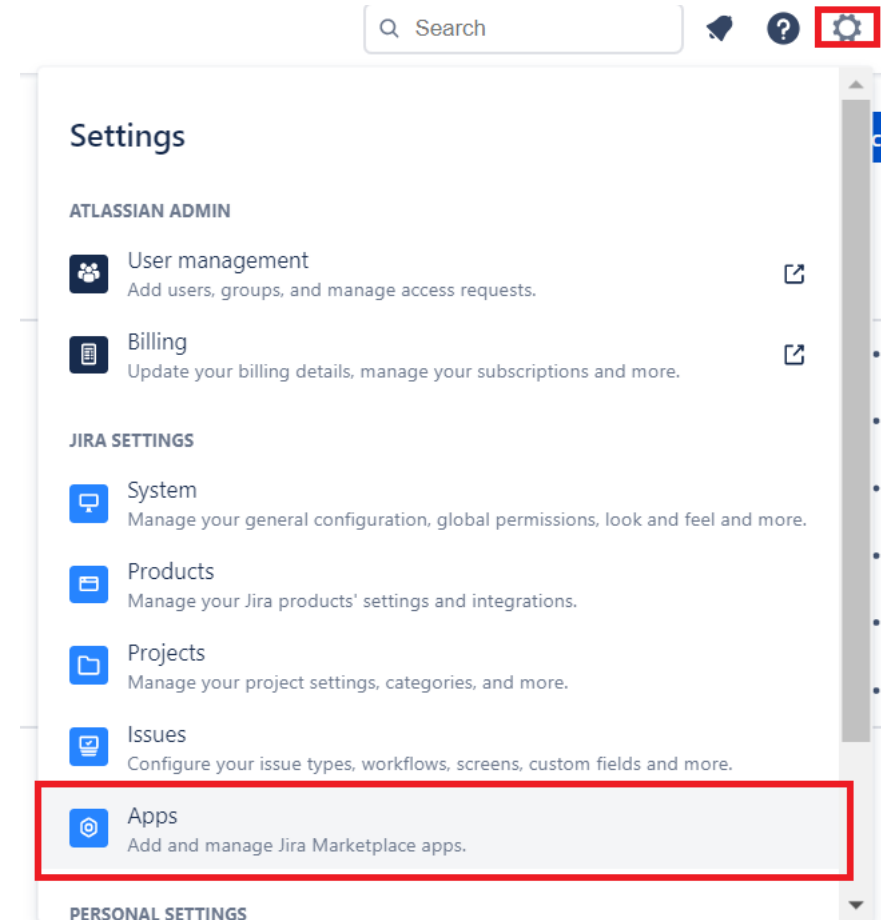
**Secret Key:**

\*\*\*\*\*

**Created:** 13 Jul 2021 @ 9:21 am EDT**Expires:** 13 Jul 2022 @ 9:21 am EDT

# Instalando plugin Veracode

- Em sua conta do Jira Cloud, logado como administrador, vá até **Settings** > **Apps** para acessar a área de marketplace do Jira



# Instalando plugin Veracode



- Na área de pesquisa, digite: **veracode**, selecione o plugin conforme a imagem ao lado
- Ao acessar, clique em **Install** para iniciar a instalação

Jira / Marketplace apps

## Discover apps and integrations for Jira

Sort ▾

☐ Free for all teams

More Filters ▾

Categories ▾

1 results



### Veracode Integration for Jira Cloud

Manage **Veracode** security findings from within Jira Cloud so you can develop secure software faster

Integrations, Security



ADDED

# Adicionar credenciais API

- Navegar: **Jira Cloud > Settings > Apps > Veracode Integration > Login Credentials**
- Adicionar **API ID** e **API KEY**, gerados na página 2 desse documento, nos respectivos campos
- Após adicionar, clicar em **Test credentials** para checar se está tudo OK

The screenshot shows the Jira Software interface for configuring Veracode integration. The top navigation bar includes 'Jira Software', 'Your work', 'Projects', 'Filters', 'Dashboards', 'People', 'Apps', and a 'Create' button. The left sidebar lists various app management options under 'Apps', including 'Find new apps', 'Manage apps', 'App requests', 'Promotions', 'OAuth credentials', and 'Veracode Integration' (which is expanded to show 'Login Credentials'). The main content area is titled 'Veracode Login Credentials' and contains two input fields: 'API ID:\*' and 'API Key:\*'. Below these fields is a warning message: 'JIRA and JIRA Cloud administrators have access to all user credentials.' There are three buttons: 'Test Credentials' (disabled), 'Save' (disabled), and 'Create' (active in the top bar).

# Adicionar Key project



- No seu projeto do Jira Cloud, identificar qual é a **KEY** dele. Geralmente é uma abreviação de 2 ou 3 letras do nome do seu projeto.
- Adicionar essa mesma KEY nos metadados do perfil da aplicação cadastrada na Veracode.
- Para adicionar:  
**Veracode > Applications > Selecionar o perfil de aplicação > Metadata > Custom Fields > Adicionar a KEY do projeto do Jira Cloud em um dos custom fields > Save**

**Name\***  
Java-VeraDemo

**Key\***  
JV ⓘ

**Application: Java-VeraDemo**

**Basics**

Origin: Not Specified

Industry: Not Specified

Application Purpose: Other Development Tools

Deployment Method: Not Specified

**Custom Fields**

Custom fields store organization-defined metadata. Ask your Veracode administrator to add more custom fields or change existing field names.

Custom 1: JV

Custom 2:

# Configurar importação de resultados



- Navegar em: Jira Cloud > Settings > Issues > Custom Fields
- Após acessar a tela, digitar na barra de pesquisa por **veracode**
- Irá aparecer 2 opções: **Veracode Link** e **Mitigation Status and Comments**. Nessas duas, iremos repetir o seguinte passo a passo:
  - Clicar no botão [...] > **Associate to Screens**

Custom fields

You currently have 49 active custom fields [Create custom field](#)

Active Trashed

veracode

Name	Type	Screens and contexts	Last used
<b>Mitigation Status and Comments</b> Contains text about the mitigation proposed for a flaw imported from the Veracode Analysis Center.	Text Field (multi-line)	12 screens, 1 context	No information
<b>Veracode APP ID</b>	Labels	7 screens, 1 context	No information
<b>Veracode Link</b> <small>LOCKED</small> Links the issue to Veracode Analysis Center.	Veracode Link	13 screens, 1 context	Not tracked

This configuration item is locked by Jira or one of its plugins. You are not allowed to alter its configuration.

[View field information](#)

[Associate to Screens](#)



# Configurar importação de resultados



- Identificar os seu projetos do Jira Cloud que irão estar associados esses **Custom Fields** da Veracode
- Após identificar, basta selecionar as checkboxes para que esses Custom Fields sejam associados ao seus projetos e depois finalizar clicando no **Update**

DVWA: Software Development Bug Screen

Field Tab ☒

DVWA: Software Development Default Issue Screen

Field Tab ☒

Default Screen

Field Tab ☒

JV: Software Development Bug Screen

Field Tab ☒

JV: Software Development Default Issue Screen

Field Tab ☒

KEN: Software Development Bug Screen

Field Tab ☐

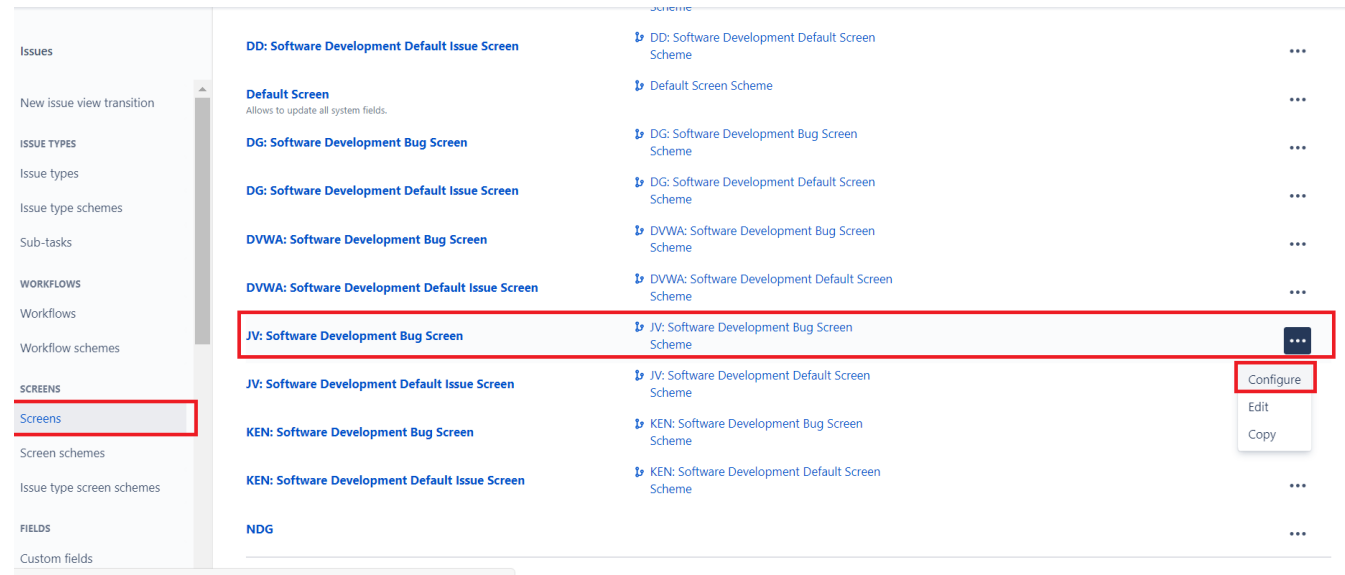
KEN: Software Development Default Issue Screen

Field Tab ☐

# Configurar importação de resultados



- Em todos os projetos que você quiser importar os resultados da Veracode, deverá ter algumas **screens** adicionais associadas aos projetos
- Navegar em:
  - Jira Cloud > Settings > Issues > Screens > clicar no botão [...] do projeto > Configure



# Configurar importação de resultados



- Selecionar esses 3 campos:

- Veracode link
- Environment
- Mitigation Status and Comments

The screenshot shows a configuration interface for importing results. It features a list of fields with a grid icon to the left of each field name. The fields are: 'Veracode Link', 'Environment', and 'Mitigation Status and Comments'. Below the list is a dropdown menu with the text 'Select Field ...' and a downward arrow. At the bottom of the interface, there is a small instruction: 'Select a field to add it to the screen.'

- Essas são screens padrões que contém informações que estarão contidas nos findings importados da Veracode

# Configurar importação de resultados

- Caso os Fields **Mitigation Status** and **Comments** e/ou **Environment** não estejam disponíveis ou criados, devemos criar um Custom Field para cada do tipo **Paragraph**
- Depois de criado, devemos associar eles as screens dos projetos que iremos fazer a integração

The screenshot displays the 'Custom fields' configuration page. On the left, a list of existing fields is shown, including 'Approvers', 'Arquivo da vulnerabilidade', 'Atlas project key', 'Atlas project status', 'Category', 'Change completion date', 'Change reason', and 'Change risk'. The 'Select a Field Type' panel on the right offers several options: 'Date Time Field', 'Labels', 'Number Field', 'Paragraph (supports rich text)', and 'Radio Buttons'. The 'Paragraph (supports rich text)' option is currently selected and highlighted in blue. At the bottom right, there are 'Next' and 'Cancel' buttons.



# Configurar plugin da Veracode

- Navegar em:
  - Jira Cloud > Settings > Apps > Veracode Integration > Findings Import
- Selecionar os campos desejados conforme sua necessidade
- Exemplo: Para importar resultados dos scans SAST, DAST e SCA, basta selecionar os 2 primeiros checkboxes, conforme a imagem ao lado
- Na opção **Filter Import By**, temos opções para importar: Os resultados dos últimos scans, somente que afetam as políticas de segurança, etc...
- Mais informações detalhadas:

[https://docs.veracode.com/r/t\\_jira\\_cloud\\_findings\\_import](https://docs.veracode.com/r/t_jira_cloud_findings_import)

## Veracode Import Results Settings

- Import: ☒ Static, dynamic, and manual findings  
☒ SCA findings  
☐ Sandbox static findings  
☐ Sandbox SCA findings
- Filter Import By: ☒ All findings  
☐ Only findings from the most recent scan  
☐ All unmitigated findings  
☐ Only unmitigated findings from most recent scan  
☐ All findings that affect policy  
☐ All unmitigated findings that affect policy

# Configurar plugin da Veracode

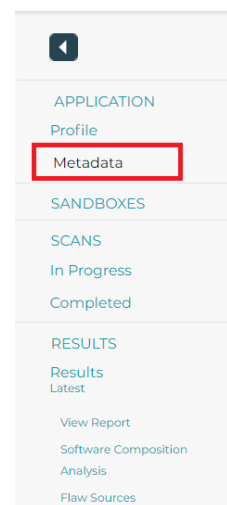


- Selecione o Issue Type para aplicar a cada resultado importado da Veracode, no nosso exemplo seccionamos Bug
- Em Import Issues Into: selecione o Custom Field do projeto da Veracode que contém o project Key do Jira, conforme configuramos anteriormente na página 7 desse documento
- Essa configuração nos permite ter diversos projetos do Jira atreladas a diferentes aplicações cadastradas no Veracode. Assim, os issues de cada aplicação estarão associadas aos respectivos projetos no Jira Cloud

Import Static and Dynamic Findings As:

Import Issues Into: ☐ JIRA project

☒ JIRA project using the value from the Veracode Platform custom field  ⓘ



## Application: Java-VeraDemo

### Basics

Origin:

Industry:

Application Purpose:

Deployment Method:

### Custom Fields

Custom fields store organization-defined metadata. Ask your Veracode administrator to add more custom fields or change existing field names.

Custom 1:

Custom 2:

Name\*

Java-VeraDemo

Key\*

JV ⓘ

# Configurar plugin da Veracode



- Seleccionamos os checkboxes **CWE and CVE** as **label**, e também **Severity** as **label**, para facilitar no tracking das issues criadas
- Caso desejar, você também pode adicionar outras labels digitando no campo **String as label**
- Por fim, em **Automated Issue Management**, você pode escolher entre as duas opções: **Fechar o ticket** ou **não fechar os tickets** em casos que houverem mitigações (medidas paliativas para evitar explorações) para as falhas

Add Values To Issues:

- ☒ CWE and CVE as label
- ☒ Severity as label
- ☐ String as label:
- ☐ Assign to next fix version

Automated Issue Management:

- ☒ Automatically close issues for mitigated findings ⓘ
- ☐ Manually manage issues for mitigated findings

JIRA User:

Enter the JIRA user you want to be able to create and modify the issues. This user must already have the necessary permissions for the JIRA projects that the findings are importing into.

# Configurar plugin da Veracode

- Agora deveremos colocar o Jira User ID no campo **JIRA User**
- Para localizar o User ID basta:
  - Clicar no botão do perfil de usuário > Profile > e na URL identificar a string do JIRA User ID
- Feito isso, no plugin da Veracode, podemos clicar em **Test JIRA User** para checar se está funcionando corretamente

Automated Issue Management: ☒ Automatically close issues for mitigated findings ⓘ  
☐ Manually manage issues for mitigated findings

JIRA User:

Enter the JIRA user you want to be able to create and modify the issues. This user must already have the necessary permissions for the JIRA projects that the findings are importing into.

Test JIRA User

Search

UPGRADE

Try the Standard plan **FREE 14-DAY TRIAL**

JIRA

Personal settings

LUCAS SANTOS FERREIRA

Profile

Account settings

Log out

View all

Vulnerability

https://lucasferreiram3.atlassian.net/jira/people/



# Mapeando os campos

- Para fazer o mapeamento dos campos de informações da Veracode para o Jira Cloud, navegamos por:
  - Jira Cloud > Apps > Veracode Integration > Field Mappings**
  - Aqui teremos todos os campos de informações e metadados da Veracode disponíveis e que podem estar presentes nos tickets criados para ter mais detalhes sobre as vulnerabilidades.
  - Basta associá-los aos campos disponíveis ou criados por você no Jira, selecionando o campo da Veracode e o respectivo campo do Jira Cloud.
  - Mais detalhes:  
[https://docs.veracode.com/r/t\\_jira\\_cloud\\_custom\\_mapping](https://docs.veracode.com/r/t_jira_cloud_custom_mapping)

Select			Component/s	
COMMON FIELDS	STATIC FIELDS	SCA COMPONENTS	SCA VULNERABILITIES	CUSTOM FIELDS
Application Name	Build ID	Added Date	CVE ID	Custom 1
Business Owner	CWE ID	Component ID	CVE Link	Custom 2
Business Unit	CWE Link	Component Path	CVSS Score	Custom 3
Current Policy	CWE Name	Description	Description	Custom 4
Scan Name	Category ID	File Name	Mitigation	Custom 5
Veracode App ID	Category Name	Library	Policy Compliance	Custom 6
	Date First Occurrence	License Name	SCA Detection Date	Custom 7
	Description	Max CVSS Score	Severity	Custom 8
	Exploit Level	New		Custom 9
	Flaw Category	Vendor		Custom 10
	Flaw ID	Version		
	Function Prototype			
	Function Relative Location			
	Grace Period Expire			
	Issue ID			
	Line Number			
	Mitigation Status Description			
	Mitigation Status			
	Module			
	Note			
	OWASP			
	PCI Related			
	Remediation Effort			
	Remediation Status			
	SANS25			
	Scope			
	Severity			
	Source File Name			
	Source File Path			
	Type			

# Importando as issues

- Navegar: Jira Cloud > Settings > Apps > Veracode Integration:

- O Plugin te possibilita fazer 3 tipos de importações:

1. One Time Import - Importação por demanda. Você pode inclusive selecionar quantas issues/tickets serão importados de uma vez
2. Selective Import - Selecione quais vulnerabilidades dos projetos você deseja importar
3. Veracode Automated import - Você seleciona o horário, frequência e quantidade de issues/tickets serão criadas

Start a one-time import from the Veracode Platform.

Import Limit:  Findings per application ⓘ

Override by Application: ☐ Use the value in the Veracode custom field  to set an import limit specific to an application.

Start a selective import from the Veracode Platform.

Import Limit:  Findings per application ⓘ

Override by Application: ☐ Use the value in the Veracode custom field  to set an import limit specific to an application.

Flaws Per Page:  Displaying flaws 1 to 10 of 121 →

Select	Flaw ID	Priority	CWE ID & Name	Application	Sandbox	Scan Name	Module
<input type="checkbox"/>	24	Medium	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Java-VeraDemo		2022-02-25 12:20:27 UTC - 15	verademo.war
<input type="checkbox"/>	7	Medium	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Java-VeraDemo		2022-02-25 12:20:27 UTC - 15	verademo.war

## Veracode Import Automation

Automate Flaw Import: ☒ Yes  
Select Yes to automatically schedule the flaw import.

Frequency: ☐ Hourly ☐ Daily ☒ Weekly

Day:

Time:

Import Limit:  Findings per application ⓘ

Override by Application: ☐ Use the value in the Veracode custom field  to set an import limit specific to an application.

# Verificando o ticket aberto



- Assim que a opção de importação for escolhida, basta aguardar e analisar o ticket/issue criada dentro do projeto que você configurou

Issues

Share Export issues Go to advanced search LIST VIEW DETAIL VIEW

Search issues Project: Java-VeraDemo Type Status Assignee More + Save filter BASIC JQL

Created

Veracode Flaw (static): Cross-Site Scripting (XSS), Java-VeraDemo, Build Number 12 commit 73d0339e3c1804921a24cfb4097b54f6e22b7145, Flaw 5

JV-53

Veracode Flaw (static): Cross-Site Scripting (XSS), Java-VeraDemo, Build Number 12 commit 73d0339e3c1804921a24cfb4097b54f6e22b7145, Flaw 36

JV-52

1-12 of 12

Give feedback

JV-53

Veracode Flaw (static): Cross-Site Scripting (XSS), Java-VeraDemo, Build Number 12 commit 73d0339e3c1804921a24cfb4097b54f6e22b7145, Flaw 5

Attach Create subtask Link issue

Description

**CWE:** 80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

**Module:** verademo.war

**Source:** feed.jsp:92

**Attack Vector:** javax.servlet.jsp.JspWriter.print

LF Add a comment...

Pro tip: press M to comment

To Do

Details

Assignee Unassigned

Reporter LF Lucas Santos Ferreira

Development Create Branch

Labels CWE\_80 Java-VeraDemo Sev3\_Medium

Data da primeira ocorrência Jun 24, 2021, 1:49 PM

Designado (Usuario) None

Source\_Path None

Arquivo da WEB-INF/views/


# Mais informações



- Para mais detalhes sobre Jira Cloud acessar os links abaixo:

Documentação: [https://docs.veracode.com/r/c\\_jira\\_cloud\\_about](https://docs.veracode.com/r/c_jira_cloud_about)

Tutorial em vídeo: <https://www.youtube.com/watch?v=si53GRvTM7g&t=207s>



Entre em contato com a nossa  
equipe para mais detalhes:  
[prevendas@m3corp.com.br](mailto:prevendas@m3corp.com.br)

SECURING THE SOFTWARE  
THAT POWERS YOUR WORLD

---

**VERACODE**