

The Continuous Dynamic Plugin for Jira[®] Data Center

Black Duck Software, Inc.

2025-04-14

Table of Contents

1.	Continuous Dynamic Plugin for Jira Data Center	1
	1.1. Prerequisites	1
2.	Installing the Continuous Dynamic Plugin for Jira Data Center	2
	2.1. Installing the Plugin from the Atlassian Marketplace for JIRA	2
3.	Configuring the Continuous Dynamic Plugin for Jira Data Center	4
	3.1. Configure Global Settings	5
	3.2. Configure DAST or SAST Settings	1
	3.3. Configure API Settings	8
	3.4. Configure MAST Settings	4
	3.5. Continuous Dynamic Workflow Settings	8
	3.6. Continuous Dynamic Integration 43	3
	3.7. Sample Workflow	8
4.	The Issues Page with the Continuous Dynamic Plugin for Jira Data Center	1
	4.1. Enable Vulnerability Management	1
	4.2. Adding a Note or Tag	1
	4.3. Ask a Question	4
	4.4. View Vulnerability Trace	7
5.	Troubleshooting the Continuous Dynamic Plugin for Jira Data Center	3
6.	Updating the Continuous Dynamic Plugin for Jira Data Center	4
	6.1. Download the new Plugin	4
	6.2. Update Process	4
	6.3. Plugin Update FAQ	7

Chapter 1. Continuous Dynamic Plugin for Jira Data Center

The Black Duck® Continuous Dynamic[™] Plugin for Jira Data Center is designed to integrate the Continuous Dynamic Portal with Jira® Data Center edition. The Plugin provides a seamless interface within Jira that will sync vulnerabilities from the Portal to your Jira application.

As vulnerabilities are discovered and listed in the Portal, they are pulled into Jira and issues are created to get those vulnerabilities into the hands of the individuals responsible for remediation. The vulnerability can be retested and developers can use the Portal's **Ask A Question** feature directly from the issue in Jira as though they were in the Portal.

1.1. Prerequisites

Note the following prerequisites:

- The Continuous Dynamic Plugin for Jira Data Center is compatible with Jira Data Center LTS versions 10.3.0 10.3.5.
- You must be logged in as a Jira Administrator with global permissions to install or configure the plugin.

Chapter 2. Installing the Continuous Dynamic Plugin for Jira Data Center

You can install the **Continuous Dynamic Plugin for Jira Data Center** directly from the **Atlassian Marketplace for JIRA** page in Jira Data Center. We strongly recommend installing the plugin this way rather than from the public Atlassian Marketplace website (where the Data Center Plugin is available to download as a .jar file).

2.1. Installing the Plugin from the Atlassian Marketplace for JIRA

Perform the following steps:

- 1. Log in to your Jira instance as an admin.
- 2. From the Jira Administration menu, select **Manage apps**. The **Atlassian Marketplace for JIRA** page is displayed.
- 3. Select **Find new apps** and then search the marketplace for **Black Duck**® **Continuous Dynamic**[™].



- 4. Click Install.
- 5. In the **Confirm app Installation** dialog, click **Accept & install**.
- 6. Select **Manage apps** in the left-hand menu; the plug-in is visible under **User-installed apps**. If necessary, refresh the page to display it.
- 7. Once this process is complete, new configuration options are added to the **Manage apps** page:

Manage apps	You can install, update, enable, and disable apps here. Find	new apps.	
BLACK DUCK CONTINUOUS DYNAMIC PLUGIN	Filter visible apps T User-installed	~ t	\pm Upload app $+$ Build a new app
Configure Global Settings	User-installed apps		
Configure DAST Settings	> 🔀 Atlassian Troubleshooting and Support Tools	٥	IPDATE AVAILABLE Update
Configure API Settings Configure MAST Settings	> 🕘 Automation for Jira	۵	Update Update
Configure Workflow Settings Configure Continuous Dynamic	› 📲 Jira Cloud Migration Assistant	C	IPDATE AVAILABLE Update
integration	> 🔯 SSO for Atlassian Data Center	C	IPDATE AVAILABLE Update
	 Black Duck Continuous Dynamic Plugin 		
	This is the Black Duck Continuous Dynamic plugin for A Uninstall Disable	Atlassian JIRA(r).	
	Manada Anama Paga Manada Manada Ma Manada Manada	Version: 5.1.0 Vendor: Black Duck Software, Inc. Support: Supported by vendor App key: com.whitehatsecurity.jira.plug s.sentinel2jirav5	Marketplace listing Documentation EULA Data security and privacy in Support and issues + 27 of 27 modules enabled

Chapter 3. Configuring the Continuous Dynamic Plugin for Jira Data Center

After installing the Continuous Dynamic Plugin for Jira Data Center, new configuration options are added to the **Manage apps** page in Jira, as shown below. Refreshing the **Manage apps** page may be necessary to see these options.

💠 Jira Software 🛛 🛛 🛛	shboards • Projects • Issues • Boards • Plans • Create Q Search	🕂 😲 🗘 🜔
Administration ۹	iearch Jira admin	ď
Applications Projects Issues	Manage apps User management Latest upgrade report System	
ATLASSIAN MARKETPLACE Find new apps Manage apps	Atlassian Marketplace for JIRA Discover powerful apps compatible with your JIRA version via the Atlassian Marketplace. Manage apps.	
ADVANCED ROADMAPS FOR JIRA Advanced Roadmaps permissions	The base URL configuration of your instance does not match the URL in your browser. This can prevent operations on this page from working correctly. See UPM documentation for more details about this error.	
Advanced Roadmaps license details		
Hierarchy configuration Dependencies Advanced Roadmaps early access features	Requirements & Test Management for San Device San Device San Devic	
BLACK DUCK CONTINUOUS DYNAMIC PLUGIN Configure Global Settings	Requirements Images and testing have Images and testing have never been easier Images and testing	
Configure DAST Settings		
Configure API Settings		
Configure MAST Settings	Search the Marketplace Q Staff-picked V All categories V All paid & free V	
Configure Workflow Settings	Jira Charting Plugin	
Configure Continuous Dynamic Integration	Atlassian Labs + Unsupported + Data Center 5,980 installations CUSTOM FIELDS DASHBOARD GADGETS PROJECT MANAGEMENT Free	

NOTE

There are seven possible configurations displayed. For the Plugin to function, the **Global Settings**, **Workflow Settings**, **Continuous Dynamic Integration**, and at least one asset type (**DAST Settings**, **SAST Settings**, **API Settings**, or **MAST Settings**) must be configured.

- Configure Global Settings: Configure the connections between the Plugin and Continuous Dynamic. Also configure how basic issues will be handled.
- Configure DAST Settings: Configure the interactions between the Plugin and Continuous Dynamic DAST services.
- Configure SAST Settings: Configure the SAST interactions between the Plugin and Sentinel Source SAST services.
- Configure API Settings: Configure the interactions between the Plugin and the Continuous Dynamic API services.
- Configure MAST Settings: Configure the interactions between the Plugin and Continuous Dynamic Mobile services.
- Configure Workflow Settings: Configure the Jira workflow to define how issues will be created, reopened and closed.

- Configure Continuous Dynamic Integration: Start and stop the integration, or view the Plugin log files.
- **NOTE** In the existing version of the Plugin, if a user has DAST configured for a group in the Continuous Dynamic Portal that contains DAST, API, or Mobile assets, then if a vulnerability is created for any of those assets, a ticket is created in JIRA. For users migrating to the new version of the Plugin, if DAST is configured for that same group, only the DAST assets would sync with JIRA. API and Mobile assets must now be configured separately.

Once this process is complete, the <u>Issues</u> page displays vulnerability information and key Continuous Dynamic features.

3.1. Configure Global Settings

To configure the Continuous Dynamic Plugin for Jira Data Center perform the following steps:

1. From the Jira System Dashboard click the gear icon.



- 2. Click Manage apps.
- 3. Log into an Admin account to manage the apps installed on Jira.

♦ Jira Software Dashboa	rds × Projects × Issues × Boards × Create Sea	arch Q 📌 0 🗘 🕗
ſ		
	Administrator Access	
	▲ If you were sent to this page from a link obtained from an untrusted source please proceed with caution or validate the link source before continuing.	
	You have requested access to an administrative function in Jira and are required to validate your credentials below.	
	Username Not You?	
	Password Confirm Cancel	

4. Click Manage apps.

	oards - Projects - Issues - Create Search	n 🔍 🤲 🖗 🔘
Administration Q Se Applications Projects Issues	arch Jira admin Manage apps User management Latest upgrade report System	♥ ➡ Back to project: Test-1
ATLASSIAN MARKETPLACE Find new apps Manage apps WHITEHAT SENTINEL Configure Global Settings Configure DAST Settings	Manage apps You can install, update, enable, and disable apps here. Find new apps. Filter visible apps V User-installed • User-installed apps	1 the two sets th
Configure API Settings Configure MAST Settings Configure Workflow Settings Configure Sentinel Integration	 Atlassian Troubleshooting and Support Tools Atlassian Universal Plugin Manager Plugin O WhiteHat Sentinel Plugin Audit log JIRA update check Settings Enter safe mode The Universal Plugin Manager (v4.0.8) by Atlassian 	UPDATE AVAILABLE Update UPDATE AVAILABLE Update

5. Select **Configure Global Settings** to configure the plugin connection to Continuous Dynamic. The following page is displayed.

💠 Jira Software 🛛 Dashboards 🗸	Projects Y Issues Y Create Search Q 🎺 😗 🗘 🌔
Administratio	Q Search Jira admin
Applications Projects Issues	Manage apps User management Latest upgrade report System
ATLASSIAN MARKETPLACE Find new apps Manage apps	WhiteHat Sentinel Plugin WhiteHat Global Settings SECURITY.
WHITEHAT SENTINEL Configure Global Settings Configure DAST Settings Configure API Settings Configure MAST Settings Configure Workflow Settings Configure Sentinel Integration	Authenticate WhiteHat Sentinel Credentials * Select Server US EU Other API Key Muthenticate Use outbound proxy server Configure Tickets Reopen tickets if Sentinel updates corresponding vulnerability's status Yes No Close tickets if corresponding vulnerabilities are closed in Sentinel Yes No
	Configure Vulnerability Content 8 Show vulnerability response from WhiteHat TRC team, retest status, and attack vectors • • • Yes No Configure Notification Settings Receive alerts when • • Plugin fails to create tickets • Plugin has Sentinel API issues 10 Advanced Configurations Save 11 Next
	WhiteHat Sentinel Plugin v5.0.0. See terms of license.

6. Authenticate Continuous Dynamic Credentials.

Authenticate WhiteHat Sentinel Credentials *

Select Server
API Kev 🕄
Se outbound proxy server
Proxy host
Proxy port 0
Username
Password
Authenticate

- a. Select a US, EU, or Other server.
- b. Enter your API key.

NOTE A valid API key must be entered before the plugin can be used.

To learn how to generate an API key in the Continuous Dynamic Portal, see Your Continuous Dynamic Portal Profile.

- c. To use an outbound proxy server, click the radio button.
- d. Type in the **Proxy Host** name and the **Proxy Port** number.
- e. Type in your **Username** and **Password** to log into the proxy server.
- f. Click Authenticate to check your connection.
- 7. Optionally, **Configure Jira Tickets**. Select the relevant radio buttons to configure default updates for your tickets.
 - a. To reopen closed tickets whenever a vulnerability's status is updated in the Portal.

Configure Tickets
Reopen tickets if Sentinel updates corresponding vulnerability's status 3 Yes No
Close tickets if corresponding vulnerabilities are closed in Sentinel 🚯
Yes NO

b. To close your existing tickets automatically if corresponding vulnerabilities are closed in the Portal.

8. Optionally, configure the **Vulnerability Content**.

Additionally, you can configure your tickets to view the retest status and notes or tags associated with a vulnerability.

a. Select the relevant radio button to show responses from the Black Duck TRC, when your team members ask questions about a vulnerability.



- 9. Optionally, configure Notification Settings.
 - a. Select the relevant radio button to determine when alerts should be sent.



- b. Then enter a comma-delimited list of the emails that should receive alerts.
- 10. Optionally, make changes to the **Advanced Configurations**.

WARNINGEach of the following actions can cause the Plugin to consume more systemWARNINGresources to the expense of the Jira server and its other components or
plugins:

- Setting too small a syncing interval.
- Setting too high a value for the maximum number of worker threads for the Continuous Dynamic API.
- Setting too high a limit on total vulnerabilities returned per API request.
- Setting too small a time interval between ticket updates.
- Setting too high a maximum character limit for issue fields.
 - a. Select the Advanced Configurations checkbox.

	Advanced Configurations a
	Set syncing interval (in minutes) 🚯
	360 D
	Pause syncing for time interval 1 Start: 8 End: 9 30 C
	Pause syncing for time interval 2 Start: 16 End : 17 45 C
	Set maximum number of worker thread for Sentinel API 🟮
	5 🧧
f	Ignore certificates for Sentinel API
	Set limit on total vulnerabilities returned per API request 3
	15 g
	Set time interval between ticket update by Sentinel API (in milliseconds)
	20 h
	Maximum character limit for issue fields 3
	∠ Z Configure Logging
	Set Logging level 3
	INFO 🗳
	Set log buffer size (lines) 🚯
	1000 k

- b. **Set Synching Interval (in minutes)** set the interval at which Continuous Dynamic and Jira will be synched.
- c. **Pause Synching for time interval** set one or two daily time intervals during which synching will be paused. Select the **Pause syncing for time interval 1** checkbox, to see the start and end time boxes for the first and, optionally, second period during which you want to pause synchronization.
- d. To pause synchronization between 8:30 and 9:30 a.m. and between 4:45 and 5:45 p.m., your entry should look like this.

NOTE

Each start and end time should be entered in hours (0-23) and minutes (0-59).

- e. **Set Maximum Number of Worker Threads** cap the number of API requests that can be in process at once.
- f. **Ignore Certification for Continuous Dynamic API** allows you to ignore any cert issues between your server and Continuous Dynamic.

WARNINGDo not enable the option to Ignore Certification for ContinuousWARNINGDynamic API, unless troubleshooting connectivity issues with the
Continuous Dynamic server.

- g. **Set Limit on Total Vulnerabilities Returned per API Request** limit the number of tickets that can be created from a single request.
- h. **Set Time Interval Between Ticket Updates** set the minimum interval (in milliseconds) between ticket updates from the Continuous Dynamic API.
- i. Maximum character limit for issue fields set a maximum character length for your Summary, Description, and Comments fields. Tick the checkbox to set your preferred maximum. The default value for this field will match **Jira's** global character limit, which is stored in 'jira.text.field.character.limit' and can be accessed from Administration>System>Advanced Settings. If you customize this value, it must be set to a value between zero and the maximum character limit set in 'jira.text.field.character.limit'.
- j. **Configure Logging** set the Logging level to the detail level desired from:
- INFO
- **DEBUG**
- TRACE
 - a. Log buffer size (lines) set the number of lines that will be retained in the log buffer.



The **Configure Logging** default values are a **Logging Level** of INFO and a **log buffer size** of 1000 lines.



11. When you have completed the **Global Configuration** process, click **Save**.

3.2. Configure DAST or SAST Settings

Select **Configure DAST Settings** or **Configure SAST Settings** to set your default reporter and assignee, map assets or groups to Jira projects, and map ticket priority to Continuous Dynamic ratings. The settings for each are broadly comparable, but some specifics will be called out where relevant.

1. To **Configure DAST/SAST Settings** select **Enable DAST integration** or **Enable SAST integration**.

NOTE Until the radio button is set to **Yes**, no other configuration options will be available.

♦ Jira Software Dashboards ◄	Projects v Issues v Create	Search Q 🎺 🖓 🗘 🌔
Administratio	Q Search Jira admin Manage apps User management Latest upgrade report System	♥ ← Back to project: Test-1
ATLASSIAN MARKETPLACE Find new apps Manage apps	WhiteHat Sentinel Plugin DAST (Sites) Settings	WhiteHat SECURITY.
WHITEHAT SENTINEL Configure Global Settings Configure DAST Settings Configure SAST Settings	Basic Configurations Enable DAST integration Yes 2 • No	
Configure API Settings Configure WAST Settings Configure Workflow Settings Configure Sentinel Integration	Save Cancel WhiteHat Sentinel Plugin v5.0.1. See terms of	Back Next

- 2. Select the **Yes** radio button. Once you have selected **Yes**, you will see the configuration settings. This will allow you to:
 - $\circ~$ Set the default Reporter for Jira tickets generated by the Plugin
 - Set the default Assignee for Jira tickets generated by the Plugin based on asset-and-project combinations
 - Map Vulnerability Ratings to Jira Priorities
 - Configure Jira Tickets

3.2.1. Basic Configuration

NOTE This shows the screen for selecting **Sites** using DAST. If configuring SAST, you have the option to select **Applications**.

1. Type the name or email of your default reporter in the search bar provided and then select your default reporter.

Basic Config	gurations		
Enable DAST • Yes	integration 🚯 No		
Set default re Type here to Set default a • Sites (DAS	search by username of search by username of ssignee Tassets) Sentinel Groups		
Add			
Remove	Sentinel sites	Projects	Username
	agrove asset1 Asset_20190625_us Asset_20190627_us confluence Created Step 1	Test-1	Type here to search by username of Unassigned

- 2. Set the default Jira assignee for a given asset (site or application) and associated Jira project. (This will map these assets to the Jira project(s) in question.) To set default assignees by group rather than asset, select the **Continuous Dynamic Groups** radio button. In this case, all assets in a group will be associated to the Jira project selected.
- 3. Select the asset from the list of **Continuous Dynamic sites**.
- 4. Select a project from the **Projects** list to assign.
- 5. Type the name or email of your default assignee in the search bar provided and then select them from the list.
- 6. To create additional default assignees and asset-to-project mappings, click Add.

NOTE Only one user can be selected as the default reporter in Jira. Only one user can be set as the default assignee to any given asset-project mapping. If **Unassigned** is selected for the **Username** field, any tickets generated will show the default assignee for that project.

Reporter Permissions Required

A reporter must have the following privileges for the project:

- Assign Issue
- Close Issue
- Create Issue
- Edit Issue
- Modify Reporter

- Resolve Issue
- Transition Issue
- Comment Issue

If you attempt to assign a user as reporter who does not have these permissions for the appropriate project, you will receive an error message.

3.2.2. Mapping Vulnerability Ratings to Jira Priorities

Vulnerability ratings for Source (SAST) vulnerabilities will all automatically use the **Advanced Rating Methodology**, which is based on **OWASP** ratings. Vulnerability ratings for Dynamic (DAST) Vulnerabilities may use either the **Advanced Rating Methodology** or the **Legacy Methodology**.

1. Select the vulnerability rating to use for DAST configuration.



For more information on choosing Legacy Ratings or Advanced Ratings, see Understanding the Rating Methodologies.

- 2. The default mapping will associate the most severe rating with the highest Jira priority. You can change this mapping using the drop-down lists.
- 3. Select the vulnerability ratings that should (checked) or should not (unchecked) be used to create Jira tickets.

Jira tickets will now be created for vulnerabilities rated **Critical**, **High**, or **Medium**. **Critical** vulnerabilities will receive the **Highest** Jira priority, **High** risk vulnerabilities will receive a Jira priority of **High**, and **Medium** risk vulnerabilities will receive a Jira priority of **Medium**. Jira tickets will not be created for vulnerabilities with a rating of **Low** or **Note**. In addition it is also possible to limit vulnerabilities that will result in Jira tickets based on the Continuous Dynamic tags associated to the vulnerability.

4. Click Add under Allow vulnerabilities that have these tags:

Allow vulnera	pility that have these tags
Remove	Vuln Tag Name

- 5. Type the tag name in the Vuln Tag Name text field.
- 6. To remove tags, click the checkbox next to the tag in question.

If you select any tags to be used to create Jira tickets, only vulnerabilities that have at least one of the listed tags in the Continuous Dynamic Portal will be used to create Jira issues.

3.2.3. Set Vulnerability Viewing Authorizations for Dynamic (DAST) Vulns

You can authorize Jira groups to view content from the vulnerabilities discovered via dynamic (DAST) testing, including retest status, notes and tags, and Black Duck Threat Research Center team responses to questions.

1. Select the relevant radio buttons to configure the type of vulnerability information that is visible to specific groups.

Authorize Groups to View	ulnerability Content	
View vulnerability information	from Sentinel in ticket 🧯	Add note and tag
Select Groups jira-administrators jira-software-users All	2 ~	

2. Select a group from the **Select Groups** table.

NOTE This information will appear in the summary section of your tickets.

3.2.4. Set Vulnerability Viewing Authorizations for Static (SAST) Vulns

You can authorize Jira groups to view content from the Portal vulnerabilities discovered via static (SAST) testing, including notes and tags, and Black Duck Threat Research Center team responses to questions.

1. Select the relevant radio buttons to configure the type of vulnerability information that is visible to specific groups.

Authorize Groups to View Vulnerability Content



2. Select a group from the **Select Groups** table.

NOTE This information will appear in the summary section of your tickets.

3.2.5. Configure Jira Tickets

1. To import closed vulnerabilities select the Import closed vulnerabilities checkbox.

Configure Tickets
Customize ticket summary 3
\${SEVERITY_LEVEL} Severity Vulnerability found on Sentinel Site \${LABEL}
Vulnerability ID: \${VULNERABILITY_ID} Type: \${VULNERABILITY_CLASS} Severity: \${SEVERITY_LEVEL} Threat: \${CLUPEAT_LEVEL}
Score: \${SCORE} CVSS: \${CVSS_SCORE} Date Found: \${DATE_FOUND}
Date Closed: \${DATE_OLOSED} Date Opened: \${DATE_OPENED} Status: \${STATUS}
Description: \${DESCRIPTION}
Solution: \${SOLUTION}
\${ATTACK_VECTOR_DETAILS}
Vulnerability details can be found at: \${SENTINEL_SERVER_URL}/site_vuln_detail.html? site_id=\${SITE_ID}&vuln_id=\${VULNERABILITY_ID}
See customization parameters

- 2. To customize the ticket summary select the **Customize ticket summary** checkbox.
- 3. To customize the ticket description select the **Customize ticket description** checkbox.
- 4. Optionally, to see customization parameters, check the checkbox next to **See Customization Parameters**

Custom Parameter	Description		
ATTACK_VECTOR_DETAILS	DAST Vulnerabilities have a notion of an attack vector. These are the unique name and values used when creating a vulnerability. It is possible for a single vulnerability to have more than one attack vectors. In most cases it is important to include this information.		
CVSS_SCORE	The CVSS score is a Common Vulnerability Scoring System designed to provide an open an standardized method for rating a vulnerability		
DATE_CLOSED	When a vulnerability is closed the time stamp of that time is held in this variable		
DATE_FOUND	When a vulnerability is first found a timestamp of that time is held in this variable		
DATE_OPENED	When a vulnerability is opened the time stamp of that time is held in this variable		
DESCRIPTION	Any time a vulnerability is found a description of that vulnerability is provided. This variable ho that value		
IMPACT	This value is similar to the severity found in DAST. What the criticality of a vulnerability could b This is the number value (0 to 9) or Low, Medium, or High		
IMPACT_READABLE	This is the text value representation of the 0 to 9 number of the impact.		
LABEL	Every asset has a label associated to it. For sites it is usually the host and for applications it cavary		
LIKELIHOOD	This value is similar to the threat found in DAST. What the likelihood or ease of an exploit of a vulnerability could be. This is the number value (0 to 9)		
LIKELIHOOD_READABLE	This is the text value representation of the 0 to 9 number of the likelihood.		
RISK	The risk is the product of the Impact * Likelihood. This is the number value. (1 to 5)		
RISK_READABLE	The risk is the product of the Impact * Likelihood. This is human readable text value. (Note, Lo Medium, High, Critical)		
SCORE	A DAST vulnerability gets a number of values that help to assign importance to vulnerability. T is a threat, severity, and priority. The sum of these values is the score		
SEVERITY	This holds the number value of a severity of a DAST vulnerability. (1 to 5)		
SEVERITY_LEVEL	This holds the severity level of a DAST vulnerability		
SOLUTION	Any time a vulnerability is found a solution of how to fix that vulnerability is provided. This van holds that value		
STATUS	This holds status of a vulnerability. (open,close)		
THREAT	This holds the number value of a threat of a DAST vulnerability. (1 to 5)		
THREAT_LEVEL	This holds the threat level of a DAST vulnerability		
VULN_RETEST_STATE	DAST vulnerabilities can be uniquely requested for retests. Therefore, it is possible for the stat a vulnerability to be different. This value holds the state of a vulnerability in regards to its retest		
VULN_URL	For DAST vulnerabilities a vulnerability is associated with a URL to where the vulnerability exist This variable holds that value		
VULNERABILITY_CLASS	This holds the vulnerability class of a vulnerability		
VULNERABILITY_ID	This holds the unique ID each vulnerability is assigned with upon creation		



Back Next

5. When you have completed configuration for **DAST** or **SAST** settings according to your preferences, click **Save**.

NOTE

If you've set a **Custom Asset ID** for this site or application (from the **Overview** tab in the Portal), it will appear as a field in the ticket **Details**.

3.3. Configure API Settings

Select **Configure API Settings** to set your default reporter and assignee, map assets or groups to Jira projects, and map ticket priority to Continuous Dynamic ratings.

- 1. To Configure API Settings, select Enable API integration.
 - **NOTE** Until the radio button is set to **Yes**, no other configuration options will be available.



- 2. Select the **Yes** radio button. Once you have selected **Yes**, you will see the configuration settings. This will allow you to:
 - $\circ~$ Set the default Reporter for Jira tickets generated by the Plugin
 - \circ Set the default Assignee for Jira tickets generated by the Plugin based on asset-and-project combinations
 - Map Vulnerability Ratings to Jira Priorities
 - Configure Jira Tickets

3.3.1. Basic Configurations

1. Enter the name or email of your default reporter in the search bar, then select your default reporter.

Basic Confi	gurations		
Enable API in • Yes •	ntegration 🚯 No		
Set default n Type here to	eporter * 3		
Set default a • API assets Add	ssignee 3 Sentinel Groups		
Remove	Sentinel API	Projects	Username
	API Production Check Individual 05/ API Production Check Individual 22/ API Production Check Upload 05/06 API Production Check Upload 22/05 ASVDEBITCARDPAYMENTS Clone Aug5_api	Test-1	Type here to search by username or Unassigned

- 2. Set the default Jira assignee for a given API and associated Jira project. (This will map these assets to the Jira project(s) in question.) To set default assignees by group rather than asset, select the **Continuous Dynamic Groups** radio button. In this case, all assets in a group will be associated to the Jira project selected.
- 3. Select the asset from the Continuous Dynamic API list.
- 4. Select a project from the **Projects** list to assign.
- 5. Type the name or email of your default assignee in the search bar provided and then select them from the list.
- 6. To create additional default assignees and asset-to-project mappings, click Add.

NOTE Only one user can be selected as the default reporter in Jira. Only one user can be set as the default assignee to any given asset-project mapping. If **Unassigned** is selected for the **Username** field, any tickets generated will show the default assignee for that project.

Reporter Permissions Required

A reporter must have the following privileges for the project:

- Assign Issue
- Close Issue
- Create Issue
- Edit Issue

- Modify Reporter
- Resolve Issue
- Transition Issue
- Comment Issue

If you attempt to assign a user as reporter who does not have these permissions for the appropriate project, you will receive an error message.

3.3.2. Mapping Vulnerability Ratings to Jira Priorities

Vulnerability ratings for API vulnerabilities will all automatically use the **Advanced Rating Methodology**, which is based on **OWASP** ratings. Vulnerability ratings for API vulnerabilities may use either the **Advanced Rating Methodology** or the **Legacy Methodology**.

1. Select the vulnerability rating to use for API configuration.

Map Vulnerability Legacy o	ulnerability ratings to your priorities () acy o Advanced (based on OWASP rational context of the set of the s	atin
Select item	ct item Vulnerability rating system Critical High Medium Low Note Vulnerability that have these tags 1 dd	Priority Highes High Mediur Low Lowest

For more information on choosing Legacy Ratings or Advanced Ratings, see Understanding the Rating Methodologies.

- 2. The default mapping will associate the most severe rating with the highest Jira priority. You can change this mapping using the drop-down lists.
- 3. Select the vulnerability ratings that should (checked) or should not (unchecked) be used to create Jira tickets.

Jira tickets will now be created for vulnerabilities rated **Critical**, **High**, or **Medium**. **Critical** vulnerabilities will receive the **Highest** Jira priority, **High** risk vulnerabilities will receive a Jira priority of **High**, and **Medium** risk vulnerabilities will receive a Jira priority of **Medium**. Jira tickets will not be created for vulnerabilities with a rating of **Low** or **Note**. In addition it is also possible to limit vulnerabilities that will result in Jira tickets based on the Continuous Dynamic tags associated to the vulnerability.

4. Click Add under Allow vulnerabilities that have these tags:

Allow vulnera	ability that have these tag	js 🕄
Remove	Vuln Tag Name	-5 _

- 5. Type the tag name in the **Vuln Tag Name** text field.
- 6. To remove tags, click the checkbox next to the tag in question.

If you select any tags to be used to create Jira tickets, only vulnerabilities that have at least one of the listed tags in the Continuous Dynamic Portal will be used to create Jira issues.

3.3.3. Set Vulnerability Viewing Authorizations for API Vulnerabilities

You can authorize Jira groups to view content from the vulnerabilities discovered via API testing, including retest status, notes and tags, and Black Duck Threat Research Center team responses to questions.

1. Select the relevant radio buttons to configure the type of vulnerability information that is visible to specific groups.

Authorize Groups to View Vulnerability Content						
Viev Viev	v vulnerability information from Sentinel in ticket Retest status 🛛 WhiteHat TRC team responses	 ☑ Add note and tag 				
:	Select Groups					
	jira-administrators					
	jira-software-users					

2. Select a group from the **Select Groups** table.

NOTE This information will appear in the summary section of your tickets.

3.3.4. Configure Jira Tickets

1. To import closed vulnerabilities, select the **Import closed vulnerabilities** checkbox.

Configure Tickets Import closed vulnerabilities
Customize ticket summary 3
\${RISK_READABLE} Risk Vulnerability found on Sentinel API \${LABEL}
- Customize ticket description
Type: \${VUI NERABILITY_CLASS}
Severity: \${SEVERITY LEVEL}
Threat: \${THREAT_LEVEL}
Score: \${SCORE}
CVSS: \${CVSS_SCORE}
Date Found: \${DATE_FOUND}
Date Closed: \${DATE_CLOSED}
Date Opened: \${DATE_OPENED}
Status: \${STATUS}
Description:
\${DESCRIPTION}
Solution:
\${SOLUTION}
\${ATTACK_VECTOR_DETAILS}
Vulnerability details can be found at: \${SENTINEL_SERVER_URL}/asset-management/api-site-
summary/\${SITE_ID}/findings/\${VULNERABILITY_ID}
See customization parameters

- 2. To customize the ticket summary select the **Customize ticket summary** checkbox.
- 3. To customize the ticket description select the **Customize ticket description** checkbox.
- 4. Optionally, to see customization parameters, check the checkbox next to **See Customization Parameters**

Custom Parameter	Description	
ATTACK_VECTOR_DETAILS	API Vulnerabilities have a notion of an attack vector. These are the unique name and values us when creating a vulnerability. It is possible for a single vulnerability to have more than one attac vectors. In most cases it is important to include this information.	
CVSS_SCORE	The CVSS score is a Common Vulnerability Scoring System designed to provide an open and standardized method for rating a vulnerability	
DATE_CLOSED	When a vulnerability is closed the time stamp of that time is held in this variable	
DATE_FOUND	When a vulnerability is first found a timestamp of that time is held in this variable	
DATE_OPENED	When a vulnerability is opened the time stamp of that time is held in this variable	
DESCRIPTION	Any time a vulnerability is found a description of that vulnerability is provided. This variable ho that value	
IMPACT	This value is similar to the severity found in API. What the criticality of a vulnerability could be. This is the number value (0 to 9) or Low, Medium, or High	
IMPACT_READABLE	This is the text value representation of the 0 to 9 number of the impact.	
LABEL	Every asset has a label associated to it. For APIs it is usually the host and for applications it cavary	
LIKELIHOOD	This value is similar to the threat found in API. What the likelihood or ease of an exploit of a vulnerability could be. This is the number value (0 to 9)	
LIKELIHOOD_READABLE	This is the text value representation of the 0 to 9 number of the likelihood.	
RISK	The risk is the product of the Impact * Likelihood. This is the number value. (1 to 5)	
RISK_READABLE	The risk is the product of the Impact * Likelihood. This is human readable text value. (Note, Medium, High, Critical)	
SCORE	A API vulnerability gets a number of values that help to assign importance to vulnerability. The a threat, severity, and priority. The sum of these values is the score	
SEVERITY	This holds the number value of a severity of a API vulnerability. (1 to 5)	
SEVERITY_LEVEL	This holds the severity level of a API vulnerability	
SOLUTION	Any time a vulnerability is found a solution of how to fix that vulnerability is provided. This vari holds that value	
STATUS	This holds status of a vulnerability. (open,close)	
THREAT	This holds the number value of a threat of a API vulnerability. (1 to 5)	
THREAT_LEVEL	This holds the threat level of a API vulnerability	
VULN_RETEST_STATE	API vulnerabilities can be uniquely requested for retests. Therefore, it is possible for the state vulnerability to be different. This value holds the state of a vulnerability in regards to its retest	
VULN_URL	For API vulnerabilities a vulnerability is associated with a URL to where the vulnerability exists This variable holds that value	
VULNERABILITY_CLASS	This holds the vulnerability class of a vulnerability	
VULNERABILITY ID	This holds the unique ID each vulnerability is assigned with upon creation	



Back Next

5. When you have completed configuration for **API** settings according to your preferences, click **Save**.

NOTE

If you've set a **Custom Asset ID** for this API (from the **Overview** tab in the Portal), it will appear as a field in the ticket **Details**.

3.4. Configure MAST Settings

Select **Configure MAST Settings** to set your default reporter and assignee, map assets or groups to Jira projects, and map ticket priority to Continuous Dynamic ratings.

1. To Configure MAST Settings, select Enable MAST integration.

NOTE Until the radio button is set to **Yes**, no other configuration options will be available.



- 2. Select the **Yes** radio button. Once you have selected **Yes**, you will see the configuration settings. This will allow you to:
 - $\circ~$ Set the default Reporter for Jira tickets generated by the plugin
 - Set the default Assignee for Jira tickets generated by the plugin based on asset-and-project combinations
 - Map Vulnerability Ratings to Jira Priorities
 - Configure Jira Tickets

3.4.1. Basic Configurations

1. Enter the name or email of your default reporter in the search bar, then select your default reporter.

Basic Configurations	
Enable MAST integration 3 • Yes O No	
Set Default Reporter * Type here to search by username or Set default assignee • Applications (MAST assets) • Sentinel Groups	
Remove Sentinel applications Pro 00 Test-1 0000007 0007MobileTest 001MobileDemo 003MobileTest 007MobileAppTest	jects Username 5 Type here to search by username or Unassigned

- 2. Set the default Jira assignee for a given application and associated Jira project. (This will map these assets to the Jira project(s) in question.) To set default assignees by group rather than asset, select the **Continuous Dynamic Groups** radio button. In this case, all assets in a group will be associated to the Jira project selected.
- 3. Select the asset from the list of **Sentinel applications**.
- 4. Select a project from the **Projects** list to assign.
- 5. Type the name or email of your default assignee in the search bar provided and then select them from the list.
- 6. To create additional default assignees and asset-to-project mappings, click Add.

NOTE Only one user can be selected as the default reporter in Jira. Only one user can be set as the default assignee to any given asset-project mapping. If **Unassigned** is selected for the **Username** field, any tickets generated will show the default assignee for that project.

Reporter Permissions Required

A reporter must have the following privileges for the project:

- Assign Issue
- Close Issue
- Create Issue
- Edit Issue

- Modify Reporter
- Resolve Issue
- Transition Issue
- Comment Issue

If you attempt to assign a user as reporter who does not have these permissions for the appropriate project, you will receive an error message.

3.4.2. Mapping Vulnerability Ratings to Jira Priorities

1. The default mapping will associate the most severe rating with the highest Jira priority. You can change this mapping using the drop-down lists.

p Vulnerabilit	ty ratings to your priorities 🕄	
Select item	Vulnerability rating system	Priority
∞ <mark>2</mark>	Critical	Highest 🗘
	High	(High 🗘
2	Medium	(Medium 🗘
	Low	Low 🗘
	Note	Lowest \$

For more information on choosing Legacy Ratings or Advanced Ratings, see Understanding the Rating Methodologies.

2. Select the vulnerability ratings that should (checked) or should not (unchecked) be used to create Jira tickets.

Jira tickets will now be created for vulnerabilities rated **Critical**, **High**, or **Medium**. **Critical** vulnerabilities will receive the **Highest** Jira priority, **High** risk vulnerabilities will receive a Jira priority of **High**, and **Medium** risk vulnerabilities will receive a Jira priority of **Medium**. Jira tickets will not be created for vulnerabilities with a rating of **Low** or **Note**. In addition it is also possible to limit vulnerabilities that will result in Jira tickets based on the Continuous Dynamic tags associated to the vulnerability.

3.4.3. Set Vulnerability Viewing Authorizations for MAST Vulnerabilities

You can authorize Jira groups to view content from the vulnerabilities discovered via MAST testing, including vulnerability notes and tags.

1. Select the relevant radio buttons to configure the type of vulnerability information that is visible to specific groups.



2. Select a group from the **Select Groups** table.

NOTE This information will appear in the summary section of your tickets.

3.4.4. Configure Jira Tickets

1. To import closed vulnerabilities select the **Import closed vulnerabilities** checkbox.



- 2. To customize the ticket summary select the **Customize ticket summary** checkbox.
- 3. To customize the ticket description select the **Customize ticket description** checkbox.
- 4. Optionally, to see customization parameters, check the checkbox next to **See Customization Parameters**

Custom Parameter	Description		
CLASS_READABLE	This is a readable format of the MAST vulnerability class for a vulnerability.		
COMPLIANCE	MAST vulnerabilities have a notion of compliance. If your organization create a policy in Sentinel th value will hold whether this vulnerability makes you compliant or not compliant.		
DATE_CLOSED	When a vulnerability is closed the time stamp of that time is held in this variable.		
CVSS_SCORE	The CVSS score is a Common Vulnerability Scoring System designed to provide an open and standardized method for rating a vulnerability		
DATE_FOUND	When a vulnerability is first found a timestamp of that time is held in this variable.		
DATE_OPENED	When a vulnerability is opened the time stamp of that time is held in this variable.		
DESCRIPTION	Any time a vulnerability is found a description of that vulnerability is provided. This variable holds that value.		
IMPACT	MAST vulnerabilities have a notion of impact. This value is similar to the severity found in DAS What the criticality of a vulnerability could be. This is the number value (0 to 9)		
IMPACT_READABLE	This is the text value representation of the 0 to 9 number of the impact.		
LABEL	Every asset has a label associated to it. For sites it is usually the host and for applications it car vary.		
LIKELIHOOD	MAST vulnerabilities have a notion of likelihood. This value is similar to the threat found in DAST What the likelihood or ease of an exploit of a vulnerability could be. This is the number value (0		
LIKELIHOOD_READABLE	This is the text value representation of the 0 to 9 number of the likelihood.		
LOCATION This is the absolute path to the vulnerable file in MAST.			
RISK_READABLE	The risk is the product of a Mobile application Impact * Likelihood. This is a text value. (Note, Low, Medium, High, Critical)		
SOLUTION	Any time a vulnerability is found a solution of how to fix that vulnerability is provided. This variable holds that value.		
STATUS	This holds status of a vulnerability. (open,close)		
VULNERABILITY_CLASS	This holds the vulnerability class of a vulnerability.		
VULNERABILITY ID	This holds the unique ID each vulnerability is assigned with upon creation.		



Back Next

5. When you have completed configuration for **MAST** settings according to your preferences, click **Save**.

NOTE

If you've set a **Custom Asset ID** for this mobile application (from the Overview tab in the Continuous Dynamic Portal), it will appear as a field in the ticket **Details**.

3.5. Continuous Dynamic Workflow Settings

This section will define how issues will be created, reopened and closed. The workflow scheme in Jira is highly configurable, and it can be difficult to account for all possible statuses and transitions created by an organization. This section allows you to define what each status should do based on the action of creating, closing, or reopening an issue in Jira.

You must use the Jira workflow that is associated to your projects (as defined in **DAST**, **SAST**, **API** and **MAST** configurations) and define the pertinent information. You must be using a single workflow, and that workflow must be associated to all your projects.

1. Select Configure Workflow Settings.



2. Optionally, select **show more...** to view the following information regarding creating a custom workflow and configuration parameters.

3.5.1. About

Use this section to configure the conditions that will create, reopen, or close your tickets. Using your custom workflow, you can define the actions that a status can perform whenever a ticket is created, closed, or reopened.

- 1. Select the workflow associated with your projects (defined in DAST and/or SAST configurations).
- 2. Create an XML file and add required configuration parameters. See the table below to learn about these parameters.
 - NOTEThe workflow scheme in is an advanced configuration and therefore you must be
aware of all the possible statuses and transitions between these statuses before you
configure your custom workflow.

See configuration parameters:

Parameter	Description
<workflow></workflow>	Define the workflow so that Continuous Dynamic add-on can create tickets.
<transition_action id=""></transition_action 	In order to transition into another status you must define the transition ID. The workflow provides you a list of all transitions for a given status when you use the workflow editor in text view.
<transition type=""></transition>	Define the type of transition for ticket. For example, you can define whether you want to close, reopen, or create the issue on a given transition.
<status_map></status_map>	Use this tag to define the state of each status within your workflow. The state can be either Opened or Closed. This allows the Continuous Dynamic add-on to make appropriate transition based on the ticket's status.
<status <br="" name="">state=""></status>	Define the name of the status and the state your ticket to be considered Opened or Closed.
<projects></projects>	Define each project that you want to associate within a workflow. This tag must be defined inside the tag.
<project <br="" name="">key=""></project>	Define the name and key for the project.
<issue_type id=""></issue_type>	Define the ID to use whenever new tickets are created by the Continuous Dynamic add-on. To find this ID, go to Administration \rightarrow Issues \rightarrow Issue Types. Hover over the Related Schemes column for that issue. This should show you the scheme ID for that issue. This is the ID that you will use for the issue_type tag.
<field <br="" name="">value=""></field>	In some cases certain fields are required to be filled in order to transition a ticket. Any required fields can be hard-coded values that will be filled in on making the transition defined by the parent tags.

3.5.2. Configure Workflow

To configure your workflow perform the following steps:

1. Click **Build Default Workflow Template** button to generate a generic template workflow XML file. This will generate a default XML workflow template that you can customize to match your chosen workflow. The XML will be generated under the XML Workflow Configuration section, and will be a starting point for the workflow configuration.

Configure Workflow 🔮	
Build Default Workflow Template	
VAL Modelieu Ocefermetice	
XML Workflow Configuration	7
Save Cancel	Back Next

Configure Workflow 3	
Build Default Workflow Template	
XML Workflow Configuration	
<workflows></workflows>	
<workflow name="JIRA Workflow (jira)"></workflow>	
<projects></projects>	
<project key="projectkey" name="projectname"></project>	
<issue_type id="1"></issue_type>	
<status_map> <status name="Open" state="Open"></status></status_map>	
<status name="Reopened" state="Open"></status>	
<status name="Resolved" state="Closed"></status>	
<status name="Closed" state="Closed"></status>	
<status name="In Progress" state="Open"></status>	
<status name="Create Issue (Integration Defined)"></status>	
<transition type="Create"></transition>	
<pre><ualisluon_action id="1"> </ualisluon_action></pre>	
<status name="Open"></status>	
<transition type="Close"></transition>	
<transition_action id="5"></transition_action>	
<field name="" values="" >	
<td></td>	
<transition type="Close"></transition>	
<transition action="" id="5"></transition>	
<field name="" values="" >	
<status name="Resolved"></status>	
<transition type="ReOpen"></transition>	
<transition_action id="3"></transition_action>	
<td></td>	
<status name="Closed"></status>	
<transition type="ReOpen"></transition>	
<transition_action id="3"></transition_action>	
<pre><!-- <field name="" values=""-->> </pre>	
<status name="In Progress"></status>	
<transition type="Close"></transition>	
<transition_action id="5"></transition_action>	
<field name="" values="" >	
<td></td>	
	11
Save Cancel	Back Next

2. In the **XML Workflow Configuration**, provide a **Workflow Name**, **Project Name**, and **Key values**. This will be the name of the Jira workflow you are using and the name and key of the Jira project where the issues will be created. An example of this is shown below:

```
<workflows>
  <workflow name="DEMO:Simple Issue Tracking Workflow">
    <projects>
        <project name= "DEMO" key= "DEMO"></project></project>
```

Locating your Project Name and Key in Jira

1. From the Jira **System Dashboard** click the gear icon.



- 2. Click Projects.
- 3. Log into an Admin account to manage the projects on Jira.

♦ Jira Software Dashboa	rds ~ Projects ~ Issues ~ Boards ~ Create Sea	rch Q 🐔 🛛 🔍
	Administrator Access	
	If you were sent to this page from a link obtained from an untrusted source please proceed with caution or validate the link source before continuing.	
	You have requested access to an administrative function in Jira and are required to validate your credentials below.	
	Username Not You?	
	Confirm Cancel	

4. Click Projects.

♦ Jira Software Dasht	boards ~ Projects ~ I	ssues - Boards -	Create	Search	Q	+ 0 C 🕓
Administration QS	Search Jira admin			Ú	←Back to	project: Test-1
Applications Projects	Issues Manage apps	User management	atest upgrade report System			
Projects Project categories Archived projects	Projects Q Search					Create project
	Project †	Key Project	Project Project lead category	Last issue update	Issues	Actions
	Test-1	TEST 0	neil.anderso No category			

- 5. The **Project Name** is shown here.
- 6. The **Key** is shown here.

3.5.3. Issue Type ID

Define the issue type IDs to be used for Jira tickets, based on Continuous Dynamic Portal vulnerability data. The Issue Type is available in Jira.

<issue_type id="5"></issue_type>

The issue type ID in Jira can be located by performing the following steps:

1. From the Jira System Dashboard click the gear icon.



- 2. Click Issues.
- 3. Click Issue types.

♦ Jira Software Dashl	boards - Projects - Issues - Boar	ds ~ Create	Search	م	4 €	00	0
Administration QS	Search Jira admin		ą	←Back	to proj	ject: Test	t-1
Applications Projects	ssues Manage apps User manage	ment Latest upg	rade report System				
ISSUE TYPES	Issue types			А	dd iss	ue type	?
Issue type schemes	Name	Type Rela	ated Schemes	Actions	;		
Sub-tasks	D Bug	Standard • T	EST: Scrum Issue Type Scheme	Edit D	elete	Translat	e
BROWSE AND EXPORT	A problem which impairs or prevents the functions of the product.			4			
Archived issues	Demo-1 test-1	Standard • D	efault Issue Type Scheme	Edit D	elete	Translat	e
WORKFLOWS	🚱 Epic	Standard • D	efault Issue Type Scheme	Edit D	elete	Translat	e
Workflows	Created by Jira Software - do not	• TI	EST: Scrum Issue Type Scheme				
Workflow schemes	user story that needs to be						
SCREENS	broken down.						
Screens	Story	Standard • D	efault Issue Type Scheme	Edit D	elete	Translat	е
Screen schemes	edit or delete. Issue type for a	• 11	EST. Scrum issue Type Scheme				
Issue type screen schemes	user story.						
FIELDS	✓ Task A task that needs to be done.	Standard • TI	EST: Scrum Issue Type Scheme	Edit D	alete	Translat	e
Custom fields	Sub-task	Sub-Task • D	efault Issue Type Scheme	Edit D	elete	Translat	e
Field configurations	The sub-task of the issue	• TI	EST: Scrum Issue Type Scheme				
Field configuration schemes							
Custom fields optimizer							

- 4. Click **Edit** on any of the **Issue types**.
- 5. To view the issue type ID click the URL.

					/accura/ad	min/Ed	:+ (* 5		
					/secure/adi	min/Ea			//
								>>	+
A You have temporary ad to the documentation.	ccess to administra	tive functio	ns. Drop acces	ss if you	no longer req	uire it. F	or more inf	ormation, refe	r
💠 Jira Software Dasł	nboards 🛩 Projects	s 👻 Issues	 Boards 	Creat	e	Search	Q	* 0 0	
Administration a	Search Jira admin					Q	←Back to	project: Test-´	1
Applications Projects	Issues Manage a	pps User	management	Latest	upgrade repor	t Syste	em		
ISSUE TYPES	Edit Issue Type	: Demo-1							
Issue types	Namo*	Domo 1							
Issue type schemes	Name	Demo-1							
Sub-tasks	Description	test-1							
BROWSE AND	Issue Type*	o select in	nage						
EXPORT	Avatar	Undata	Canaal						
Archived issues		Opdate	Cancer						
WORKFLOWS									
Workflows									
Workflow schemes									
SCREENS									
Screens									
Screen schemes									
Issue type screen schemes									
FIELDS									
Custom fields									
Field configurations									
Field configuration schemes									
Custom fields optimizer									
PRIORITIES									
Priorities									
Priority schemes									
ISSUE FEATURES									
Time tracking									
Issue linking									

6. The issue type ID is shown at the end of the URL.



3.5.4. Status Names & Transition ID's

Define the statuses that an issue can belong to, every status state must be defined in the workflow. The status names can be found in Jira.

```
<status_map>
<status name="To Do" state="Open"></status>
<status name="In Progress" state="Open"></status>
<status name="Done" state="Closed"></status>
</status_map>
```

NOTE

The status names given here are case sensitive and must exactly match the status name given in Jira.

The status names in Jira can be located by performing the following steps:

1. From the Jira **System Dashboard** click the gear icon.

Image: troduction Im	tem Dasł	nboard		JIRA ADMINISTRATION Applications
Welcome to JIRA Not sure where to start? Check out the Jira 101 guide and Atlassian training course. You can customize this text in the Administration section. You can customize this text in the Administration section.	troduction	2 ² ····	Assigned to Me	Projects
Welcome to JIRA Manage apps Not sure where to start? Check out the Jira 101 guide and Atlassian training course. You can customize this text in the Administration section. Activity Stream User management Your Company Jira System No activity was found No activity was found			You currently have no issues assi	gn Issues
Activity Stream User management You can customize this text in the Administration section. Your Company Jira System No activity was found No activity was found System		Welcome to JIRA		Manage apps
You can customize this text in the Administration section. Your Company Jira No activity was found		101 guide and Atlassian training course.	Activity Stream	User management
No activity was found	You can cus	stomize this text in the Administration section.	Your Company Jira	Latest upgrade report System
			No activity was found	

- 2. Click Issues.
- 3. Click Workflows.

♦ Jira Software Das	hboards ~ Projects ~ Issues ~ Boar	ds 🖌 Create Search	Q 🤲 🛛 🔍
Administration _c	Search Jira admin	ų	←Back to project: Test-1
Applications Projects	Issues Manage apps User manage	ment Latest upgrade report Sys	tem
ISSUE TYPES	Issue types		Add issue type ⑦
Issue type schemes	Name	Type Related Schemes	Actions
Sub-tasks	Bug A problem which impairs or	Standard • TEST: Scrum Issue Type Scheme	Edit Delete Translate
BROWSE AND EXPORT	prevents the functions of the product.		
Archived issues	o Demo-1 test-1	Standard • Default Issue Type Scheme	Edit Delete Translate
WORKFLOWS	Epic	Standard • Default Issue Type	Edit Delete Translate
Workflows	Created by Jira Software - do not	Scheme	
Workflow schemes	edit or delete. Issue type for a big user story that needs to be	TEST: Scrum Issue Type Scheme	
SCREENS	broken down.		
Screens	Created by Jira Software - do not	Standard • Default Issue Type Scheme	Edit Delete Translate
Screen schemes	edit or delete. Issue type for a	TEST: Scrum Issue	
lssue type screen schemes	user story.	Type Scheme	
FIELDS	☑ Task A task that needs to be done.	Standard • TEST: Scrum Issue Type Scheme	Edit Delete Translate
Custom fields	₅ Sub-task	Sub- Default Issue Type	Edit Delete Translate
Field configurations	The sub-task of the issue	Task Scheme • TEST: Scrum Issue	
Field configuration schemes		Type Scheme	
Custom fields optimizer			
PRIORITIES			
Priorities			
Priority schemes			

4. Click the **View** link on any workflow.

♦ Jira Software Das	hboards - Projects - Issues - Boards	~ Create	Search	Q	≁⁵ 🕜	o (
Administration c	χSearch Jira admin		ę	←Back to	o project: 7	ſest-1
Applications Projects	Issues Manage apps User manageme	ent Latest upgrad	de report System			
ISSUE TYPES Issue types	Workflows		Ac	ld workflo	w Import	i • (
lssue type schemes Sub-tasks	• To delete a workflow, you must fir	st unassign it fron	n all workflow schemes and	draft worl	cflow sche	mes.
BROWSE AND	Active					
EXPORT	Name	Last modified	Assigned Schemes	Steps	Actior	L
Archived issues	Software Simplified Workflow for	23/Mar/21	TEST: Software	3	View E	lit
WORKFLOWS	Project TEST Generated by JIRA Software version		Workflow Scheme		Сору	
Workflows	8.5.0-DAILY20190920183006. This					
Workflow schemes	workflow is managed internally by Jira Software. Do not manually					
SCREENS	modify this worknow.					
Screens						
Screen schemes	Inactive					
lssue type screen schemes						
FIELDS						
Custom fields						
Field configurations						
Field configuration schemes						
Custom fields optimizer						
PRIORITIES						
Priorities						
Priority schemes						

5. Click **Text** to see the list of statuses contained in the workflow.

💠 Jira Software Das	hboards 🖌 Projects 🗸	lssues 👻 Boards 🛩	Create Search	q 🤲 🛛 🗘 🜔
Administration c	Search Jira admin		Ģ	←Back to project: Test-1
Applications Projects	Issues Manage apps	User management	Latest upgrade report S	System
ISSUE TYPES Issue types Issue type schemes Sub-tasks BROWSE AND EXPORT	Workflows Software Simplifie Generated by JIRA S managed internally k This workflow w Diagram Text	d Workflow for Proje oftware version 8.5.0- by Jira Software. Do no as last edited by you a Export ~	ct TEST ACTIVE USED DAILY20190920183006. ot manually modify this wo at 23/Mar/21 10:34 AM.	BY 1 PROJECT Edit This workflow is ⑦ orkflow.
Archived issues	Step Name (id)	Linked Status	Transitions (id)	Actions
WORKFLOWS Workflows Workflow schemes SCREENS	To Do (1)	ΤΟ DO	To Do (11) >> To Do In Progress (21) >> In Progress Done (31) >> Done	View Properties
Screens Screen schemes Issue type screen schemes FIELDS	In Progress (6)		To Do (11) >> To Do In Progress (21) >> In Progress Done (31) >> Done	View Properties
Custom fields Field configurations Field configuration schemes Custom fields optimizer	Done (11)	DONE	To Do (11) >> To Do In Progress (21) >> In Progress Done (31) >> Done	View Properties
PRIORITIES Priorities Priority schemes ISSUE FEATURES				

- 6. The **Jira Workflow** has a list of all transitions that are possible for a given Status.
 - a. **Transitions (id)** shows each possible transition out of that state with the transition ID in parentheses. The transition ID for moving from a status of **To Do** to a status of **Done** is **31**.
 - b. Step Name (id) and Linked Status show each status and its status ID in parentheses.
- 7. Define the transition_action id for each relevant status change in the workflow. Every status will include a transition type and transition_action id, any required fields must be included.

For example, to move a Jira ticket from a state of **To Do** (as shown above) to a state of **Done**, your XML may look like this:

```
<status name="To Do">
  <transition type="Close">
        <transition_action id="31">
        </transition_action>
        </transition>
</status>
```

If any transition has a required field, that field must be included in the XML for the transition. If the transition above had a required field called **Resolved**, and you want to configure the field value to be **Yes**, the XML above would become:

```
<status name="To Do">
<transition type="Close">
<transition_action id="31">
<field name="Resolved" values="Yes"></field>
</transition_action>
</transition>
</status>
```

3.5.5. The Create Issue (Integration Defined) Status

The default XML Workflow includes the status **Create Issue (Integration Defined)** which is a custom status for the Continuous Dynamic to Jira integration.

1. If any custom fields are required to create an issue, include them here. Otherwise please do not edit the **Create Issue (Integration Defined)** status.



2. When you have defined the XML workflow configuration, click **Save**.

For an example of a completed XML Workflow configuration, please see Sample Workflow.

3.6. Continuous Dynamic Integration

This page allows an admin user to start and stop the Continuous Dynamic Plugin for Jira Data Center integration or view the plugin log files. Once all fields are populated correctly and the previous settings are saved, integration can begin.

NOTE If any changes to the settings of the Plugin are made while integration is running, you will need to stop the integration and re-start it to reflect the changed values.

To begin the initial integration process, perform the following steps:

1. From the Jira System Dashboard click the gear icon.



2. Click Manage apps

3. Log into an Admin account to manage the apps installed on Jira.

♦ Jira Software Dashboards × Projects	s ~ Issues ~ Boards ~	Create	Search	Q 📌	0 O	
Adminis	trator Access					
If you from a cautic contin	were sent to this page fr an untrusted source pleas on or validate the link sou nuing.	om a link obtained se proceed with rce before				
You have r function in credentials	requested access to an ac a Jira and are required to s below.	dministrative validate your				
Usern	ame Not	You? 3				
Passy	word	Ý				
	Confirm Cancel					

4. Click Configure Continuous Dynamic Integration.



5. Ensure the **Delta Sync** box is **unchecked**.

NOTE Enabling this option only integrates new changes to the existing Plugin configuration, since the last successful integration.



- 6. Click **Start Integration** to begin Continuous Dynamic Portal data syncing with Jira. This runs on the interval specified by the user.
 - **NOTE** Once the initial integration is complete, optionally Delta Sync may be turned on. This will enable the synchronization to be run only for items that have changed since the last successful synchronization. To run a full integration again, Delta Sync will need to be disabled.
- 7. To view the log files, click **Refresh Log**. This will display the latest one thousand lines of the log, and will automatically take you to the most recent portion of the log.

Projects × Issues × Create	Search	Q 📌	0 O	
Q Search Jira admin		🗣 😁 Back to	project: Te	est-1
Manage apps User management Latest upgrade report	System			
Manage apps User management Latest upgrade report Contine Integration Image apps Image apps Contine Integration Image apps Image apps	System jira.plugins.Sentinel 12 jira.plugins.Sentinel provide for Project TEST jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel ira.plugins.Sentinel ira.plugins.Sentinel ira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel jira.plugins.Sentinel	JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang GiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang JiraDataExchang	White secure ger] ger] ger] ger] ger] ger] ger] ge	Hat
Back				
	Projects Visues Create Image apps User management Latest upgrade report Manage apps User management Latest upgrade report Control Integration Start Integration Start Integration Start Integration Colspan="2">Colspan="2" <colspan="2">Colspan="2"<colspan="2"<colspan="2"<colspan="2"<colspan="2"<colspan="2"<colspan="2"<col< th=""><th>Project V Issues V Create Search Project V Issues V Create Search Image apps User management Latest upgrade report System Image apps Start Integration Start System Image approximation Image approxima</th><td>Projects v Issues v Create Search Q A • Search Jira admin • Search Jira admin • • • • • • • • • • • • • • • • • • •</td><td>Projects v tsuss v Create Search Q A A Q A A Q A</td></colspan="2"<colspan="2"<colspan="2"<colspan="2"<colspan="2"<colspan="2"<col<></colspan="2">	Project V Issues V Create Search Project V Issues V Create Search Image apps User management Latest upgrade report System Image apps Start Integration Start System Image approximation Image approxima	Projects v Issues v Create Search Q A • Search Jira admin • Search Jira admin • • • • • • • • • • • • • • • • • • •	Projects v tsuss v Create Search Q A A Q A A Q A

8. If necessary, use the **Stop Integration** button to stop your integration. Any vulnerabilities that have been added to Jira will be available to you in Jira, but no further vulnerabilities will be added unless and until you start a new integration process.

3.7. Sample Workflow

The following is a sample Plugin XML Workflow Configuration designed to work with the Jira **DEMO:** Simple Issue Tracking Workflow.

3.7.1. Sample Plugin XML Workflow Configuration

```
<workflows>
<workflow name="DEMO: Simple Issue Tracking Workflow">
 <projects>
 <project name="DEMO" key="DEMO"></project></project>
 </projects>
 <issue_type id="3"></issue_type>
 <status_map>
 <status name="To Do" state="Open"></status>
 <status name="In Progress" state="Open"> </status>
 <status name="Done" state="Closed"></status>
 </status_map>
 <status name="Create Issue (Integration Defined)">
 <transition type="Create">
    <transition_action id="1">
    </transition action>
 </transition>
 </status>
 <status name="To Do">
 <transition type="Done">
    <transition action id="21">
    <field name="Resolved" values="Yes"></field>
    </transition action>
 </transition>
 </status>
 <status name="In Progress">
 <transition type="Done">
    <transition_action id="41">
    <!-- <field name="" values=""></field> -->
    </transition action>
 </transition>
 </status>
 <status name="Done">
 <transition type="To Do">
    <transition action id="51">
    </transition_action>
 </transition>
 </status>
</workflow>
</workflows>
```

3.7.2. Jira DEMO: Simple Issue Tracking Workflow

This table shows the following issue types IDs:

Туре	Label	ID
Step	To Do	1
Step	In Progress	2
Step	Done	3
Transition	From To Do to Done	21
Transition	From In Progress to Done	31
Transition	From Done to To Do	51

The XML must reflect the terminology in Jira exactly, including letter case and spacing if any.

Chapter 4. The Issues Page with the Continuous Dynamic Plugin for Jira Data Center

The **Issues** page of every vulnerability created by the Continuous Dynamic Plugin for Jira Data Center has now integrated key Continuous Dynamic features, allowing users to get the information they need to remediate vulnerabilities without leaving Jira.

Continuous Dynamic's vulnerability data is presented in the description section of the Issue. At the bottom of every Issue you will see the **Continuous Dynamic - Vulnerability Management** section.

NOTE

In order to see this information, you must have configured your Global Settings appropriately. For more information, see Configure Global Settings / Configure Vulnerability Content. For troubleshooting help, see Troubleshooting.

4.1. Enable Vulnerability Management

To enable Vulnerability Management, perform the following:

1. When completing the **Configure Global Settings**, select the **Yes** radio button.

Configure Vulnerability Content

Show vulnerability response from WhiteHat TRC team, retest status, and attack vectors 3
• Yes

2. Select Save.

4.2. Adding a Note or Tag

To add a **Note** or **Tag** using the **Vulnerability Management** functions perform the following steps:

1. From the Jira system Dashboard, select Issues.

		1							
Jira Software	Dashboards 🖌 Projects 🖌	Issues 🗸 Boards 🗸	Create	Search	۹	4 €	0	٥	
System Dashb	oard	Current search Search for issues							
Introduction		Archived issues		e				e ⁿ	•
	Welcome to JIRA	RECENT ISSUES		2/e no issues assign	ed to y	ou. E	njoy	you	r
	Not sure where to start? Cl Jira 101 guide and Atlassian	 TEST-159 High Ris TEST-73 Critical R 	sk Vulner isk Vuln	m				27	•
11 - 24	course.	TEST-74 Critical R	isk Vulne	lira					
		TEST-38 Critical R	isk Vuln	Jia					-
		TEST-12 test 3						_	
		more		igh Risk Vulnerability fo	cre ound on	eated Senti	TES nel	1-	
		Import Issues from C	SV	tion 3-24-21 test Loggin	۱h				
		FILTERS		ability ID: 2166733	et Http (Body			
		My open issues		8.8	et.mtp.i	bouy			
		Reported by me		d In:		Horola	a o i o h		
		Manage filters		ssons/DBCrossSiteScr	ipting/E	ditPro	file.js	we sp	
			Date F	Found: 2021-03-24T22:1	4:12Z				
			Read	more »					
			4 c	lays ago Comment					
			158 - Applic	High Risk Vulnerability fo ation 3-24-21 test Loggir	cre ound on oh	eated Senti	TES nel	Т-	
			Vulnei Vulnei	rability ID: 2166736 rability Class:		4			
			Crypto CVSS	ography.Persist.Ccn.Une : 5.9	ncrypte	d			
			http://i a/org/	ed in: repo.sca.dev.whs/git/web owasp/webgoat/lessons/	goat.git	t/src/n or/Rol	nain/j leBas	av sed	
			Acces Date Read	sControl/UpdateProfile_1	.java				
			4 d	lays ago Comment					

2. Select an Issue.

3. Click **Continuous Dynamic - Vulnerability Management** to expand the section.

♦ Jira Software Dashboar	ds ~ Proje	cts 👻 Issues 🗸	Boards 🗸	Create			Searc	h (۹ 🕈	?	o 📀
Test-1	Pres Hig 3-	at-1 / TEST-159 gh Risk Vuln 24-21 test L	erability ogginh	/ found o	n Sen	itinel Applica	ation				
∭ TEST board ✓							-				
🖶 Backlog	🖋 Edit	Q Comment	Assign	More 🗸	To Do	In Progress	Done	Admin	•		
Active sprints									~	🔥 Exp	port 🗸
📤 Releases	 Details 						⊻ Pe	eople			
🗠 Reports	Type:	🖸 Bu	ıg	Status:		TO DO	As	ssignee:	3)	
☑ Issues	Priority	: <u>~</u> Hi	gh	Resolution		(View Workflow	()		U d	nassigi	ne
பி Components	Version	/s:	5	Fix Version	n/s:	None	_		Α	ssign t	o me
PROJECT SHORTCUTS	Labels:	Non	9				Re	eporter:	F)	
Add a link to useful information for your whole	> Descrip	otion									
team to see.	 Activity 	1					Vo	otes:	(
+ Add link	All C	omments Wor	k Log H	istory Ac	tivity		VV	atchers:	w	Stop atching	o g this
	There a	re no comments	s yet on th	ils issue.					is	sue	
							~ D	ates			
	QComm	ient					C	reated:	4	days a	igo
	WhiteH	at Sentinel - Vu	Inerabilit	y Manager	nent		U	pdated:	4	days a	igo
							~ A	gile			
							Vi	ew on Boa	rd		
							~ H	ipchat dis	cussio	ns	
							De	o you wan sue? Conn	t to dis ect to	cuss t Hipcha	his at.
							0	Connect	Dismi	SS	

a. Optionally, to retest this Issue select **Vulnerability Retest**.

Retest	
Jpdate Vulnerability with a Tag or Note	
Vulnerability 52554029	
Update type Note	
Attack vector 123584964 🗬	
Message	

b. Select from the drop down menu which update type you want to add.

c. Select from the drop down menu which attack vector the note or tag will be added to.

NOTE For **SAST** and **MAST** assets, the option to select an **Attack vector** is unavailable.

- d. Type the **Note** or **Tag** in the text field.
- e. Click Submit.
- 4. If the **Note** or **Tag** is successfully added, the following message is displayed.

♦ Jira Software	Dashboards 🗸	Projects 🗸	Issues 🗸	Boards 🗸	Create	Search	Q	, ≜ [£]	?	٥	(]
						.4					
		The i	nformation	was successf	ully updated.	T					
			Re	eturn To Issue							

4.3. Ask a Question

To ask a question using the **Vulnerability Management** functions, perform the following steps:

1. From the Jira system Dashboard, select **Issues**.

		1							
Jira Software	Dashboards 🖌 Projects 🖌	Issues 🗸 Boards 🗸	Create	Search	۹	4 €	0	٥	
System Dashb	oard	Current search Search for issues							
Introduction		Archived issues		e				e ⁿ	•
	Welcome to JIRA	RECENT ISSUES		2/e no issues assign	ed to y	ou. E	njoy	you	r
	Not sure where to start? Cl Jira 101 guide and Atlassian	 TEST-159 High Ris TEST-73 Critical R 	sk Vulner isk Vuln	m				27	•
11 - 24	course.	TEST-74 Critical R	isk Vulne	lira					
		TEST-38 Critical R	isk Vuln	Jia					-
		TEST-12 test 3						_	
		more		igh Risk Vulnerability fo	cre ound on	eated Senti	TES nel	1-	
		Import Issues from C	SV	tion 3-24-21 test Loggin	۱h				
		FILTERS		ability ID: 2166733	et Http (Body			
		My open issues		8.8	et.mtp.i	bouy			
		Reported by me		d In:		Horola	a o i o h		
		Manage filters		ssons/DBCrossSiteScr	ipting/E	ditPro	file.js	we sp	
			Date F	Found: 2021-03-24T22:1	4:12Z				
			Read	more »					
			4 c	lays ago Comment					
			158 - Applic	High Risk Vulnerability fo ation 3-24-21 test Loggir	cre ound on oh	eated Senti	TES nel	Т-	
			Vulnei Vulnei	rability ID: 2166736 rability Class:		4			
			Crypto CVSS	ography.Persist.Ccn.Une : 5.9	ncrypte	d			
			http://i a/org/	ed in: repo.sca.dev.whs/git/web owasp/webgoat/lessons/	goat.git	t/src/n or/Rol	nain/j leBas	av sed	
			Acces Date Read	sControl/UpdateProfile_1	.java				
			4 d	lays ago Comment					

2. Select an Issue.

3. Click **Continuous Dynamic - Vulnerability Management** to expand the section.

💠 Jira Software 🛛 Dashboar	ds ~ Proje	cts - Issues -	Boards	~ Create			Searc	h (۹ 📌	?	0	0
est-1	Pres Hi 3-	st-1 / TEST-159 gh Risk Vuln 24-21 test L	erability ogginh	y found o	n Sen	tinel Applica	ation					
🔟 TEST board 🗸 🗸	-		55									
🖨 Backlog	🖋 Edit	Q Comment	Assign	More ~	To Do	In Progress	Done	Admin	•			
Active sprints									«	фEx	port	~
📤 Releases	 Details 						× P€	eople				
🗠 Reports	Type:	D B	ug	Status:		TO DO	As	ssignee:	?			
☑ Issues	Priority	: A H	igh o	Resolution		(View Workflow)		Ui d	nassig	ne	
公 Components	Version	/s:	0	Fix Version	ı/s:	None			As	sign	to me	Э
PROJECT SHORTCUTS	Labels:	Non	e				Re	eporter:	(F.	9		
Add a link to useful information for your whole	> Descrip	otion										
team to see.	Activity	/					Vo	otes:	C			
+ Add link		omments wo	rk Log H	listory Act	ivity		VV	atchers:	W	atchin	p g thi	s
	There a	ire no comment	s yet on tr	his issue.					is	sue		
							Y Da	ates				
	Q Comn	nent			9		Сг	reated:	4	days	ago	
	WhiteH	lat Sentinel - Vu	ulnerabilit	ty Managem	nent		U	pdated:	4	days	ago	
							~ Ag	gile				
							Vi	ew on Boa	rd			
							≚ Hi	ipchat dis	cussio	ns		
							Do	o you wan sue? Conn	to dis ect to	cuss Hipch	this iat.	
Ma							(Connect	Dismis	S		

- a. From the drop down menu, select the **Category** that your question belongs to.
- b. Type your question in the text field.
- c. Select **Submit** to send your question to the Black Duck support team.



4. If the question is successfully submitted, the following message is displayed.

♦ Jira Software Das	hboards 🖌 Projects 🗸	Issues 🛩 Boa	rds Y Create	Search	۹	₹ £	?	0
	Thank you, A	WhiteHat TRC En	gineer will answer	vour question shortly.	4			
			.	,				
		Re	urn To Issue					

5. Previous questions and responses can be reviewed in the **Ask a Question** section of the **Vulnerability Management** functions.

NOTE The **Retest** and **Add Tag or Note Vulnerability Management** functions are only available for **DAST** Issues.

4.4. View Vulnerability Trace

To view vulnerability traces for Continuous Dynamic issues with a description and solution, perform the following steps:

1. From the Jira system Dashboard, select Issues.



2. Select an Issue.

3. At the bottom of the **Description**, click the link for **More information**. This includes the vulnerability traces, description and solution.

 QAProject / QAP-172 Medium Risk Vulnerability found on Sentinel Application 3-6 Sa upload 	ast EE Cloud	
Edit Q Add comment Assian More Y To Do In Progress Workflow Y Admin Y		< 🔥 Export 🗸
Details	✓ People	
Type: ✓ Task Status: TO DO (View Workflow)	Assignee:	Unassigned
Priority: – Medium Resolution: Unresolved	-	Assign to me
Labels: None	Reporter:	QA
✓ Description	Votes: Watchers:	0 1 Stop watching this issue
Vulnerability ID: 1405043 Vulnerability Class: Error.Handler.Global		
CVSS: 5.3	✓ Dates	
Date Found: 2020-03-06T20:43:05Z	Created:	13/Sep/21 12:22 AM
Date Opened: 2020-03-06120:43:112 Date Closed:	Updated:	13/Sep/21 12:22 AM
Status: Open Risk: Medium	✓ Agile	
Likelihood: Medium Impact: Medium	View on Board	
Description:		
The application fails to make sufficient use of a global error handling mechanism. Analysis of the deployment descriptor either noted a lack of or an incorrect use of the error-page directive. Failure to leverage a global error handling mechanism increases the risk that verbose implementation details will be revealed to attackers through a stack trace. Developers not using this mechanism are required to implement their own global error handling mechanism.		
Solution: Ensure the application deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the application. Such practice will significantly minimize the risk of disclosing sensitive implementation details through error messages.		
In Java:		
The web.xml should include error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all":		
<pre></pre>		
> Attachments		
> Activity		
Q Add comment		
WhiteHat Sentinel - Vulnerability Management		

4. This table displays the **Vector ID**, **Line Number** and code **Snippet** relating to this vulnerability.

WhiteHat Sentinel Plugin



SAST Vuln View

Vulnerability Class Application Misconfiguration: Global Error Handling Disabled

Vulnerability Id 1405043

T :	
Vector ID Numbe	Snippet
, tunioe	
96445318-1	
FileReference 1	Path: sample.war/WEB-INF/web.xml
	1 xml version="1.0" encoding="ISO-8859-1"? /*FileReference*/
	2 <web-app <="" td="" xmlns="http://java.sun.com/xml/ns/j2ee"></web-app>
	3 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
	xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-
	$app_2_4.xsd"$
	6
	7 <display-name>Hello, World Application</display-name> 8 <description></description>
	9 This is a simple web application with a source code organization
	10 based on the recommendations of the Application Developer's Guide.
	12
	13 <servlet></servlet>
	15 <servlet-class>mypackage.Hello</servlet-class>
	16
escription	
0	andling mechanism.
Solution	landling mechanism.
Solution Ensure the application application. Such prac	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by t ice will significantly minimize the risk of disclosing sensitive implementation details through error messa
Solution Ensure the application upplication. Such prac	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by t tice will significantly minimize the risk of disclosing sensitive implementation details through error messa
Solution Ensure the application application. Such prac in Java: The web.xml should in	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the company of the declaration that catches all uncaught exceptions thrown by the company of the declaration of the de
Solution Ensure the application application. Such prac in Java: The web.xml should in cerror-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment descriptor declares an error page declaration that catches all uncaught exceptions thrown by the deployment declares an error page declaration that catches all uncaught exceptions thrown by the deployment declares an error page declaration that catches all uncaught exceptions thrown by the deployment declares an error page declaration that catches all uncaught exceptions thrown by the deployment declares and the declares an error page declaration that catches all uncaught exceptions thrown by the declares and the declares an error page declares and the declares an error page declares and the declares and the declares an error page declares and the decla
Solution Ensure the application pplication. Such prac n Java: The web.xml should in <error-page> <error-code>403<td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all":</td></error-code></error-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all":
Solution Ensure the application application. Such prac in Java: The web.xml should in <error-page> <error-code>403<location>/error.jsp<!--<br--></location></error-code></error-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all":
Solution Ensure the application application. Such prac in Java: The web.xml should in <error-page> <error-code>403<location>/error.jsp<!--<br--></location></error-code></error-page> <error-page></error-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all":
Solution Ensure the application pplication. Such prac in Java: The web.xml should in cerror-page> <error-page> <error-page> <error-page> <error-code>404<location>/error.jsp<!--<br-->docation>/error.jsp<!--</td--><td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location></td></location></error-code></error-page></error-page></error-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location>
Solution Ensure the application pplication. Such prac in Java: The web.xml should in <error-page> <error-code>403<location>/error.jsp<!--<br--></location></error-code></error-page> <error-code>404<location>/error.jsp<!--<br--></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the component descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the component of the component of the component of the catches all uncaught exceptions thrown by the component of the catches all uncaught exceptions thrown by the component of the catches all uncaught exceptions thrown by the catches all uncaught exceptions through error messand even of the catches all uncaught exceptions throw and a "catches" and a "catch
Solution Ensure the application application. Such prace in Java: Fhe web.xml should in <error-page> <error-code>403<location>/error.jsp<!--<br--></location></error-code></error-page> <error-code>404<location>/error.jsp<!--<br--> <error-page> <error-page> <error-page> <error-code>500<td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code></td></error-code></error-page></error-page></error-page></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code>
Solution Ensure the application pplication. Such prac in Java: The web.xml should in <error-code>403<location>/error jsp<!--<br--> <error-page> <error-code>404<location>/error jsp<!--<br--></location></error-code></error-page> <error-code>500<location>/error jsp<!--</td--><td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location></td></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location>
Solution Solution Solution. Such prac n Java: The web.xml should in cerror-code>403 <location>/error.jsp<!--/cerror-page--> <error-code>404<location>/error.jsp<!--/cerror-page--> <error-code>500<location>/error.jsp<!--/cerror-page--> <error-code>500 <error-code>500</error-code></error-code></location></error-code></location></error-code></location>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location>
Solution Solution Solution. Such prac n Java: The web.xml should in <arror-page> <arror-code>403<arror-page> <arror-page> <arror-code>404<arror-page> <arror-code>404<arror-page> <arror-code>500<arror-page> <arror-code>500<arror-page> <arror-page> <arror-page> <arror-code>500<arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-page> <arror-< td=""><td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location></td></arror-<></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-page></arror-code></arror-page></arror-page></arror-page></arror-code></arror-page></arror-code></arror-page></arror-code></arror-page></arror-code></arror-page></arror-page></arror-code></arror-page>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location>
Solution Solution Solution. Such prac In Java: The web.xml should in cerror-page> <error-code>403<location>/error.jsp<!--/<br-->c/error-page> <error-code>404<location>/error.jsp<!--/<br-->c/error-page> <error-code>500<location>/error.jsp<!--/<br-->c/error-page> <error-code>500<location>/error.jsp<!--/<br-->c/error-page> <ercor-code>500<location>/error.jsp<!--/<br-->c/error-page> <ercor-type>java <location>/error.jsp<!--/</td--><td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location></td></location></ercor-type></location></ercor-code></location></error-code></location></error-code></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location>
olution nsure the application pplication. Such prac h Java: he web.xml should in error-page> <error-code>403<location>/error.jsp<!--/error.jsp<//error-page--> error-page></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location>
olution insure the application pplication. Such prac 1 Java: the web.xml should in error-page> <error-code>403<location>/error.jsp<!--/<br-->/error-page> <error-code>404<location>/error.jsp<!--/<br-->/error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page> error-page></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> or-code> location> loca
olution nsure the application pplication. Such prac h Java: he web.xml should in error-page> <error-code>403<location>/error.jse<!--<br--><error-page> er</error-page></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> lang.Throwable location>
Solution Solution Solution. Such prac n Java: The web.xml should in terror-page> <error-code>403<location>/error.jsp<!--/<br-->/error-page> <error-code>404<location>/error.jsp<!--/<br-->/error-page> <error-code>500<location>/error.jsp<!--/<br-->/error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> <error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </error-page> </location></error-code></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messan clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> lang.Throwable location> set the custom error mode to "on", define a defaultRedirect page, and include redirect pages for 403, 404, 404, 404, 404, 404, 404, 404,
isolution insure the application pplication. Such prac h Java: 'he web.xml should in error-page> <error-code>403<location>/error;jsp<!--/<br-->/error-page> <error-code>404<location>/error;jsp<!--/<br-->/error-page> <error-code>500<location>/error;jsp<!--/<br-->/error-page> <erception-type>java <location>/error;jsp<!--/<br-->/error-page> <erception-type>java <location>/error;jsp<!--/<br-->/error-page> <acception-type>java <location>/error;jsp<!--/<br-->/error-page> <acception-type>java <location>/error;jsp<!--/<br-->/error-page> <acception-type>java <location>/error;jsp<!--/<br-->/error-page> a C#: he web.config should customErrors mode='</location></acception-type></location></acception-type></location></acception-type></location></erception-type></location></erception-type></location></error-code></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by t ice will significantly minimize the risk of disclosing sensitive implementation details through error messa clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> lang.Throwable location> set the custom error mode to "on", define a defaultRedirect page, and include redirect pages for 403, 404, On" defaultRedirect="error.html">
isolution insure the application pplication. Such prac h Java: the web.xml should in terror-page> <error-code>403<location>/error,jsp<!--/error-page--> <error-code>404<location>/error,jsp<!--/error-page--> <error-code>500<location>/error,jsp<!--/error-page--> <error-code>500<location>/error,jsp<!--/error-page--> <erception-type>java <location>/error,jsp<!--/error-page--> <ercor-page> <ercorton= error,jsp<="" error-page=""> <ercor-page> <location>/error,jsp<!--/error-page--> <location>/error,jsp<!--/error-page--> <location>/error,jsp<!--/error-page--> <location>/error,jsp<!--/error-page--> <location>/error,jsp<!--/error-page--> a C#: The web.config should customErrors mode=' </location></location></location></location></location></ercor-page></ercorton=></ercor-page></location></erception-type></location></error-code></location></error-code></location></error-code></location></error-code>	deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by t icice will significantly minimize the risk of disclosing sensitive implementation details through error messa clude error pages for 403, 404, 500, java.lang.Throwable, and a "catch-all": or-code> location> or-code> location> lang.Throwable location> location> set the custom error mode to "on", define a defaultRedirect page, and include redirect pages for 403, 404, On" defaultRedirect="error.html"> 500" redirect="error.btml"> 500" redirect="error.btml"
Solution Solution Solution. Such prac n Java: The web.xml should in terror-page> <error-code>403<location>/error.jsp<!--/<br-->/error-page> <error-code>404<location>/error.jsp<!--/<br-->/error-page> <error-code>500<location>/error.jsp<!--/<br-->/error-page> <erception-type>java <location>/error.jsp<!--/<br-->/error-page> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor-roage> <ercor catch-all":="" or-code="" statuscode="</td><td>deployment descriptor declares an error-page declaration that catches all uncaught exceptions thrown by the tice will significantly minimize the risk of disclosing sensitive implementation details through error messa clude error pages for 403, 404, 500, java.lang.Throwable, and a "> location> or-code> location> or-code> location> lang.Throwable location> location> set the custom error mode to "on", define a defaultRedirect page, and include redirect pages for 403, 404, 404, 404, 404, 404, 404, 404,</ercor></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></ercor-roage></location></erception-type></location></error-code></location></error-code></location></error-code>	

- 5. The **Description** tab offers a description of the vulnerability class in question.
- 6. The **Solution** tab will offer an approach to resolving the vulnerability in question.

For troubleshooting help, please see [^top].

Chapter 5. Troubleshooting the Continuous Dynamic Plugin for Jira Data Center

The most common issue encountered is when, after starting the integration, no **Issues** are generated.

In most cases, this is caused by the selected **Assignee** not having adequate privileges to create that issue. To verify this, you can manually create an example issue in the Jira project.

For easy troubleshooting of other issues, the Plugin has been set up to generate verbose debugging. This can be viewed by going to the Jira log folder and pulling data from the atlassian-jira.log file. The verbosity of the log files generated can be configured in the Jira log configurations.

Chapter 6. Updating the Continuous Dynamic Plugin for Jira Data Center

6.1. Download the new Plugin

The latest version of the Continuous Dynamic Plugin for Jira Data Center is available to download from:

• The Atlassian Marketplace.

6.2. Update Process

To update the Continuous Dynamic Plugin for Jira Data Center from v4.0.1 to the latest version, perform the following steps:

1. From the Jira System Dashboard click the gear icon.



2. Click Manage apps.

3. Log into an Admin account to manage the apps installed on Jira.



4. Click Manage apps.



- 5. Click **Upload app**.
- 6. Click the **Choose File** option.



7. Select the latest WHS JIRA Plugin .jar file.



- 8. Click Choose for Upload.
- 9. Click Upload.



11. If necessary, refresh the **Manage apps** page to display the updated Plugin.

	/plugins/servlet/upm?source=side		1 O
♦ Jira Software Dashbo	aards ~ Projects ~ Issues ~ Create	Search Q 📌	o o 📀
Administration Q Se	arch Jira admin	🗣 😁 Back to	project: Test-1
Applications Projects Issues	Manage apps User management Latest upgrade report Syster	n	
ATLASSIAN MARKETPLACE Find new apps	Manage apps		
Manage apps	Filter visible apps V) Upload app _+	Build a new app
	User-installed apps		
	> 🔀 Atlassian Troubleshooting and Support Tools	UPDATE AVAILABLE	Update
	> 🔟 Atlassian Universal Plugin Manager Plugin	UPDATE AVAILABLE	Update
	 Ø WhiteHat Sentinel Plugin 		
	This is WhiteHat Security Sentinel plugin for Atlassian JIRA(r). Uninstall Disable		
	Loading screenshots Version: 5.0.1 Vendor: White Secur App key: com.v	III 27 of 27 modu enabled Hat ity vhitehatsec ira.plugins.	iles
	Audit log JIRA update check Settings Enter safe mode	el2jirav5	

12. Once this process is complete, the Plugin has been successfully updated.

6.3. Plugin Update FAQ

- 1. How do I access the Customer Support Portal ? Log in to the Black Duck Community.
- How do I install the new Plugin ? Follow the install process detailed in Installing the Continuous Dynamic Plugin for Jira Data Center for more information.
- 3. **Can I download the Plugin from the Atlassian Marketplace ?** Yes, currently the Plugin is available to download from The Atlassian Marketplace.
- Do I need to reconfigure the Plugin ? When you update from 4.0.1 or earlier versions to 5.0.1 and above, you don't need to reconfigure the Plugin.
- 5. What will happen to Jira issues already created ? Issues created by the prior Plugin will be recognized and handled appropriately by the updated Plugin.
- 6. Previously, I manually created tickets for each vulnerability in the Continuous Dynamic Portal. Will the Plugin create duplicates when syncing ?

Unfortunately the Plugin will not be able to recognize and properly synchronize or transition Jira issues not created by our Plugin.

7. How do I contact the support team?

You can log in to the Community Portal and contact Customer Support by creating or responding to a case. If you do not have Community Portal access you can email support@whitehatsec.com.