Edgescan Jira Plugin User Manual

Introduction

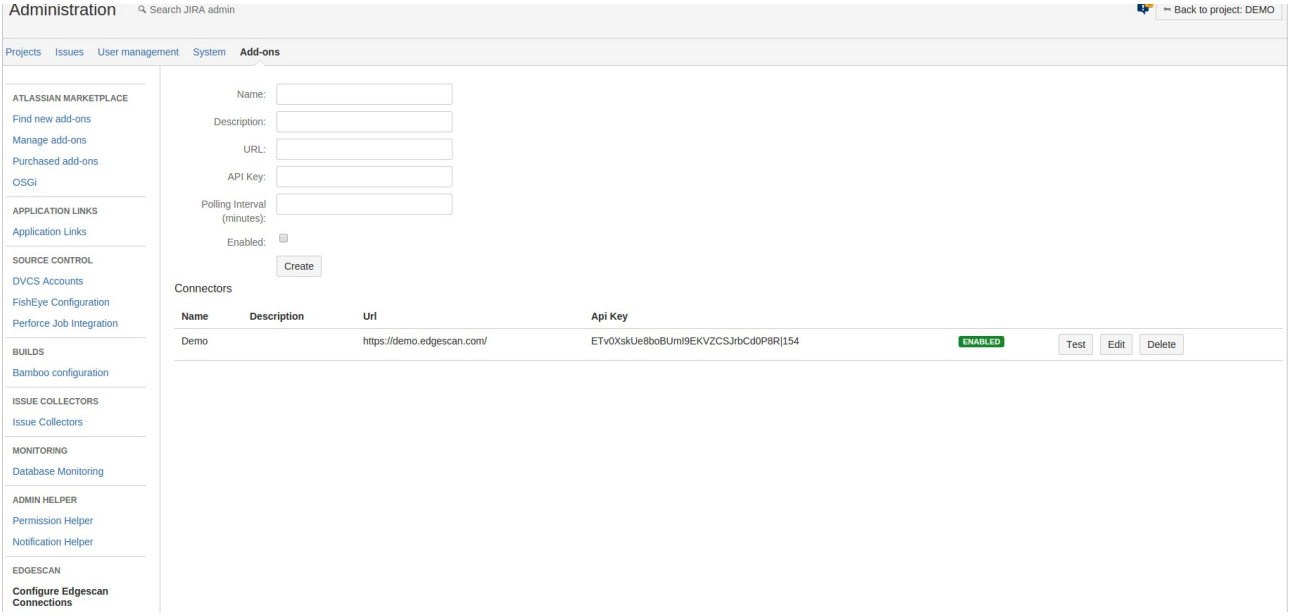
The Edgescan Jira plugin provides a means to link Edgescan assets to Jira projects. It can be configured to pull vulnerability data from the Edgescan API, opening a Jira issue for each new vulnerability, and automatically closing issues when the linked vulnerability is closed.

This manual assumes familiarity with the concepts and configuration used by both Edgescan and Jira.

There are two types of configurable component in the plugin:

- An ***Edgescan connection*** models a connection between Jira and Edgescan.
- *A **project link*** models a link between a Jira project and one or more Edgescan assets, and allows for configuration of how Jira issues are created by the plugin. Each project link must be associated with an edgescan connection.

Configuring Edgescan Connections



Screenshot 1: Edgescan Connection Configuration screen

The connection configuration screen can be found in the Jira admin portal under **Add Ons > Edgescan > Edgescan Connection Configuration.**

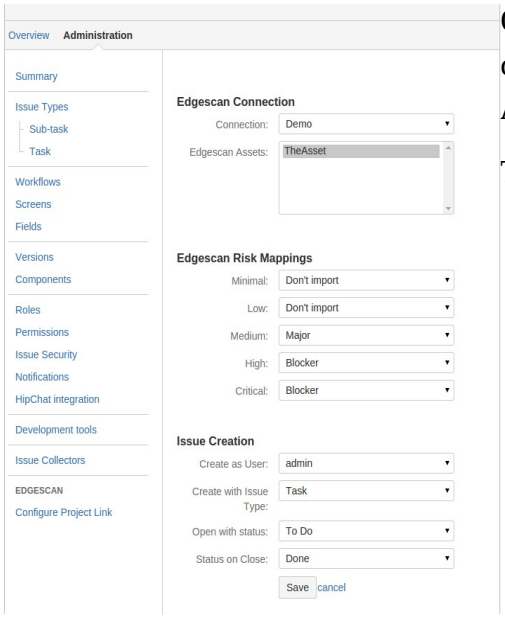
The fields that can be configured in this screen are:

- *Name* – the name of the connection
- *Description* – an optional description of the connection
- *URL* – the url through which edgescan may be accessed. The protocol must be specified and the url must end with a trailing '/' e.g. https://demo.edgescan.com/
- *API key* – the edgescan API key, see the edgescan user documentation for instruction on how to generate one. Note that API keys are accorded the same access rights as the user that

creates them.
- *Polling interval* – the frequency (in minutes) with which edgescan will be checked for updates to vulnerabilities.

Once created a connection may be tested using the button marked 'Test'. The test will pass if the connection to edgescan is successful and one or more assets are retrieved.

Configuring Project Links



Screenshot 2: Project Link form

One project link may be configured for each Jira project. The configuration screen can be found under **Project Administration > Edgescan > Configure Project Link.**

The configuration options for project links are as follows:

- *Connection* – the edgescan connection to be used
- *Edgescan Assets* – one or more assets must selected from those visible through the selected connection
- *Edgescan Risk Mappings* – Each Edgescan risk rating may be mapped to a Jira priority. Issues created from a vulnerability with a particular risk rating will have the mapped priority. If a risk rating is set to 'Don't Import', vulnerabilities of that risk will be ignored during imports.
- *Create As User* – the user account the plugin will use to open and close issues.
- *Create with Issue Type* – the type of created issues.

  Note: at present, the Sub-Task type is not supported by the plugin.
- *Open with Status* – the status of issues created by the plugin.
- *Status on Close* – the status to transition to when the linked vulnerability closes. The plugin assumes that there will always be a transition to this status available. If issues will be transitioned manually by Jira users, please configure the workflow to ensure that this is the case.

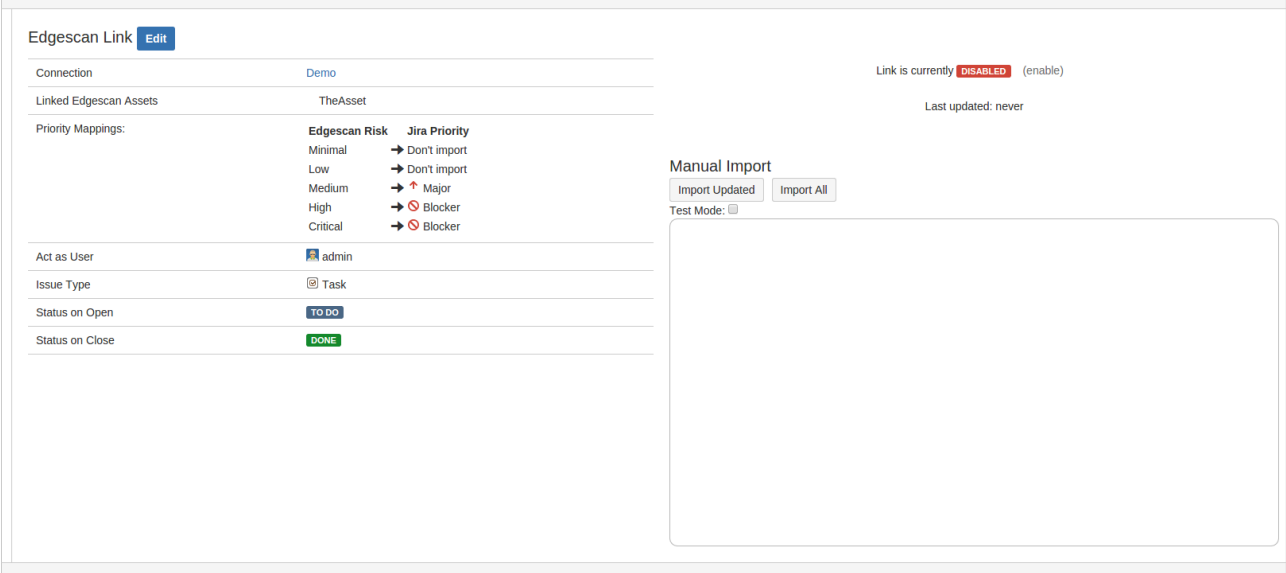
Importing Vulnerabilities from Edgescan

Once a project link is configured, vulnerabilities can be imported from Edgescan. Imports may be triggered manually or automatically. If automatic imports are enabled, the plugin will perform imports periodically, with the polling interval defined in the connection configuration.

Manual imports are triggered using the buttons on the configuration screen. Once a manual import finishes, the results are displayed to the user showing the number of vulnerabilities found/opened/closed etc., along with a breakdown for each risk rating. The results also include any errors encountered during the import, which may be useful for troubleshooting.

There are two possible import modes:

Import All: all vulnerabilities are retrieved from Edgescan. For each open vulnerability, if a linked issue exists it is updated, otherwise a new one is created. For each closed vulnerability the linked issue, if any, is transitioned to the configured 'Status on Close'. This mode may only be triggered manually.



Screenshot 3: Project Link Screen

Import Updated: vulnerabilities created/updated since the last successful import are retrieved from Edgescan. The open/update/close semantics are the same as the Import All case. All automatic imports are performed in this mode.

Important points:

- If the project link settings are changed – e.g if the priority mapping for a risk rating is changed – the import updated mode will not update existing issues accordingly. Therefore it is recommended that an import all be run after editing the link configuration.
- If the priority mapping for a risk is changed to 'Don't Import', any issues linked to vulnerabilities of that risk rating will be closed.
- A ***test mode*** is available for the manual imports to allow import results to be previewed. When test mode is active all checks relating to issue operations is performed, but no changes are committed to Jira.