# Acunetix Plugin

| Plugin Information |
| --- |
| View Acunetix on the plugin site for more information. |

Older versions of this plugin may not be safe to use. Please review the following warnings before using an older version:

- SSRF vulnerability
- Credentials stored in plain text

## Plugin Information

This plugin allows you to trigger automated Acunetix scans as part of your web application's build process inside of Jenkins.

## Description

Acunetix is an automated web application security testing and vulnerability management platform. Acunetix automatically crawls and scans off-the-shelf and custom-built websites and web applications for over 3000 web vulnerabilities to help organizations shore up their web security.
The Acunetix Jenkins Plugin enables you to:

1. Trigger Acunetix scans from within Jenkins upon each build
2. Trigger Acunetix scans with built-in or custom Scan Types to only scan for specific vulnerabilities
3. Configure Jenkins to fail a build (and optionally abort the scan) as soon as a specific threat-level (high, medium or low severity) is reached
4. Automatically generate reports

After setting up the Acunetix Jenkins Plugin, you can configure any Jenkins job with a build step action to trigger an Acunetix scan. When an Acunetix scan is triggered, Jenkins will launch a scan against a Target you specify and is scanned with settings configured in Acunetix. Jenkins will pass or fail the build based on criteria you provided.

**Note** – The Acunetix Jenkins Plugin requires an Acunetix API key, which is only available in *Acunetix Enterprise*.

## Installation

To install the Acunetix Jenkins Plugin:

1. In Jenkins, navigate to *Manage Jenkins > Manage Plugins* and select the *Available* tab
2. Search the Jenkins Plugin Index for *Acunetix*
3. Select *Install without restart* or *Download and install after restart*. Jenkins will install the plugin based on your preference

## Configuration

To configure the Acunetix Jenkins Plugin:

1. Make Acunetix reachable from hosts other than localhost
2. Add the Acunetix Root CA Certificate to Jenkins
3. Obtain an Acunetix API key
4. Modify the Jenkins Content Security Policy (optional)

## Usage

1. In Jenkins, navigate to the job you wish to run an Acunetix scan in, and select *Configure* in the sidebar
2. In the *Build* section, select *Acunetix* from the *Add build step* drop-down menu
3. You will then be presented with the options outlined below.
    a. **Scan Type** – Choose a *Scan Type* with which you want the scan to run. *Scan Types* are used to reduce the scope of the tests the scanner runs during the scan.

    b. **Scan Target** – Choose a *Scan Target* you wish to scan. *Scan Targets* are obtained from Acunetix, with the exception of Targets requiring Manual Intervention. Targets contain part of the Target description for distinguishability between Targets that have the same URL.
    c. **Fail build if threat level is** – Choose at which threat level to fail the Jenkins build based upon the scan's threat level (High severity, Medium severity or Low Severity).
    d. **Stop the scan when build fails** – Check this checkbox if you would like to abort the scan when the fail condition in *Fail build if threat level is* is met. This is setting is enabled by default.
    e. **Generate Report** – Choose to a report to generate upon completion of the scan. The report will be accessible inside of Acunetix and a download link will be provided within console output log
4. Click *Save*

# FAQs

1. **Which edition of Acunetix do I need to use the Acunetix Jenkins Plugin?**

The Acunetix Jenkins Plugin requires access to the Acunetix API and API key, which is only available in *Acunetix Enterprise*.

1. **The Target I have set-up in Acunetix is not showing in drop-down list inside Jenkins.**

The Acunetix Jenkins Plugin will display all Targets in an Acunetix installation, with the exception of Targets requiring Manual Intervention as part of their Login Sequence. Please make sure that the Target you wish to select does not make use of Manual Intervention.

1. **How can I differentiate between multiple Targets with the same URL?**

If you have multiple Targets with the same URL, it is advised that you enter a description in the Target's settings to be able to differentiate between them. The Target's description will show up in Jenkins if one is available.

1. **Why does a scan take long for to start?**

When Jenkins attempts to start a scan, the scan is placed in a scan queue. If the scan queue is empty, then the scan will start immediately. However, if the maximum number of scans (including scheduled scans) in the scan queue is reached, the scan will wait in the queue until other scans finish processing. This also means that the Jenkins build will not finish processing until the scan is complete.

1. **What happens to the scan if I abort the Jenkins build?**

Aborting the Jenkins build will also abort the scan. You may still view partial results inside of Acunetix. Reports will not be automatically generated if the Jenkins build is aborted (you can manually generate reports from within the Acunetix UI).

1. **What happens if I stop an Acunetix scan from outside Jenkins?**

If a scan that was started by Jenkins is stopped from the Acunetix UI or via the Acunetix API, the Jenkins build will also be aborted. Reports will not be automatically generated if the scan is stopped (you can manually generate reports from within the Acunetix UI)

1. **What kind of reports can be generated from Jenkins?**

All *Standard* reports can be generated from Jenkins (Affected Items, Developer, Executive Summary and Quick reports). Compliance reports (PCI DSS, OWASP Top 10, ISO 27001…) for the scans run by Jenkins may be generated from within the Acunetix UI.

1. **What happens to reports generated from Jenkins?**

Reports generated from Jenkins are generated on the main application and a download link is provided in the console output

1. **How do I disable or remove the Acunetix Jenkins Plugin**

Please refer to this Jenkins article on disabling and removing Jenkins plugins and associated plugin data

# Changelog

## Version 1.0.0 (March 15, 2017)

1. Initial release
2. New features
    a. Trigger Acunetix scans from within Jenkins upon each build
    b. Trigger Acunetix scans with built-in or custom Scan Types to only scan for specific vulnerabilities
    c. Configure Jenkins to fail a build (and optionally abort the scan) as soon as a specific threat-level (high, medium or low severity) is reached
    d. Automatically generate reports and save them within Jenkins
3. Improvements
    a. N/A
4. Bugfixes
    a. N/A

## Version 1.1.0 (October 24, 2018)

Improvements: Use Jenkins credentials for storing the API Key

## Version 1.2.0 (October 25, 2018)

Improvements: Better exception handling like situations when configured target or profile have been deleted in main application

Bug fixes:

- Plugin retrieve only first 100 targets
- Scans can now be executed on the online version of the scanner
- Reports cannot be downloaded. Now links to the reports will be provided on the output.

## Version 1.2.1 (January 10, 2019)

Bug fixes:

- Fixed 429 error when pairing with online build

## Version 1.2.2 (January 18, 2019)

Bug fixes:

- Fixed 429 error for reports

## Version 1.2.3 (February 06, 2019)

Bug fixes:

- Saved API URL is not loaded and shown in Jenkins system page