Jenkins Plugin for Qualys WAS

The Qualys WAS Jenkins plugin empowers DevOps teams to build application vulnerability scans into their existing CI/CD processes. By integrating scans in this manner, application security testing is accomplished earlier in the SDLC to catch and eliminate security flaws.

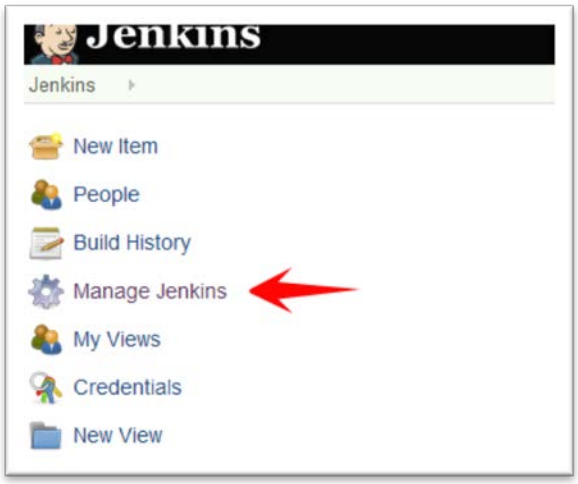
We'll help you: Install the Plugin | Configure the Plugin | Protect Your Qualys API Credentials

Install the Plugin

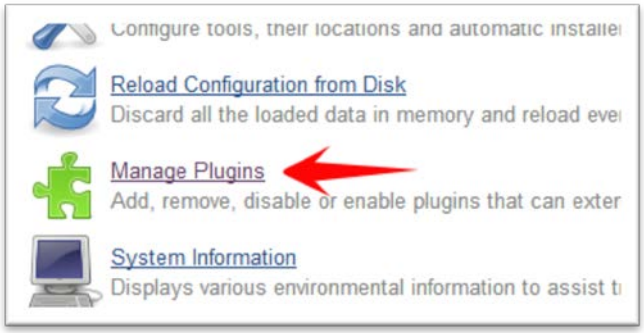
To install the Jenkins plugin for Qualys WAS into your Jenkins instance, you must first download the plugin from Qualys. The plugin comes in the form of a .hpi file. You can find it under Top Resources at https://community.qualys.com/community/web-application-scanning.

At this time, the plugin is not listed under the Available tab within Jenkins or in the plugin store at https://plugins.jenkins.io/.

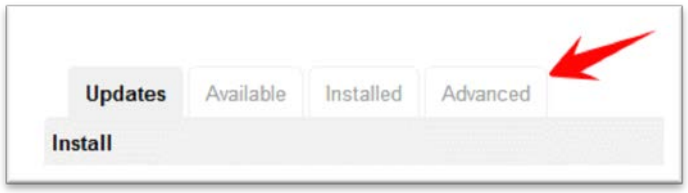
Once you have the .hpi file, log into your instance of Jenkins and click Manage Jenkins.



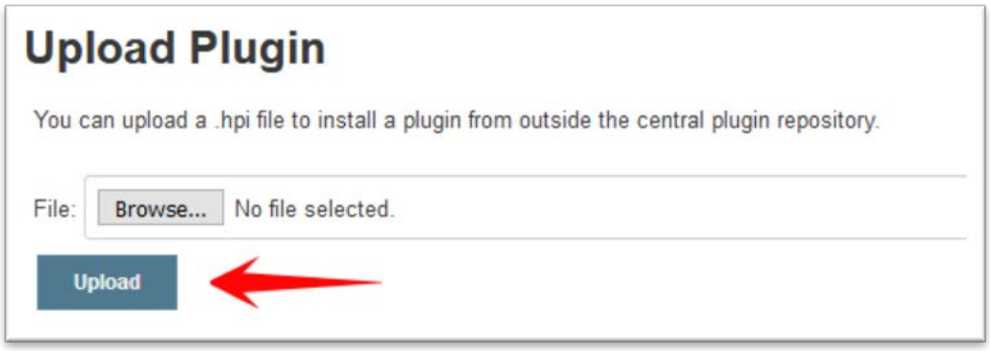
Next, click Manage Plugins.



Go to the "Advanced" tab.



Browse to select the .hpi file you downloaded and click the Upload button.



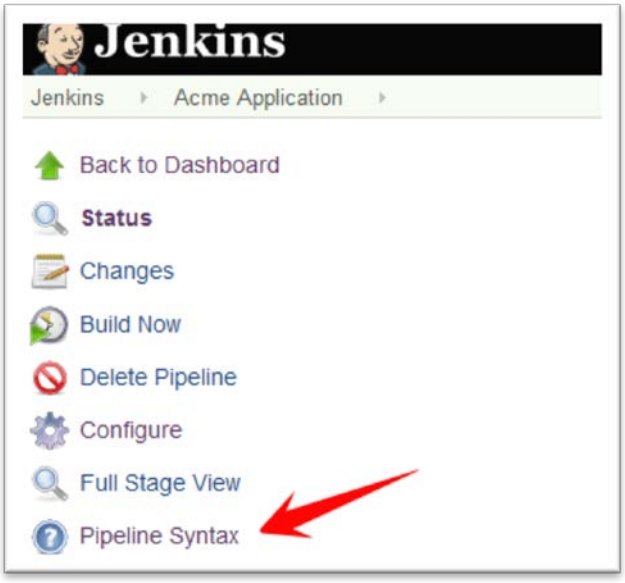
Confirm that the Success message appears. Click the link “Go back to the top page”.

That’s it! The installation is now complete. Read on to learn about configuring the plugin.

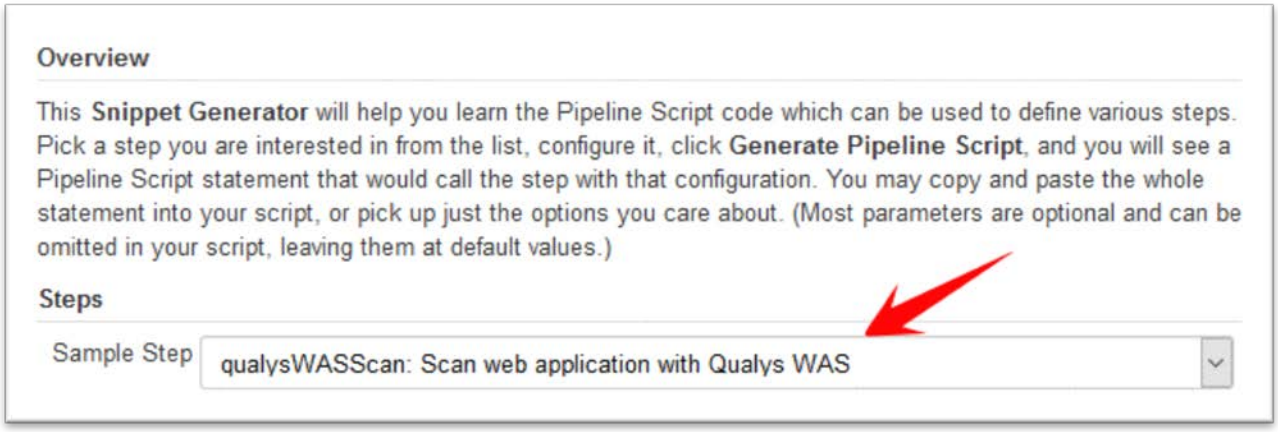
The first thing you’ll need to do is enable proxy on your browser. Then, on the browser where you enabled proxy, make a request to the RESTful API service, as shown below.

Configure the Plugin

Open your application's pipeline project and click "Pipeline Syntax" to enter the Snippet Generator.



Select "qualysWASScan" from the drop-down menu.

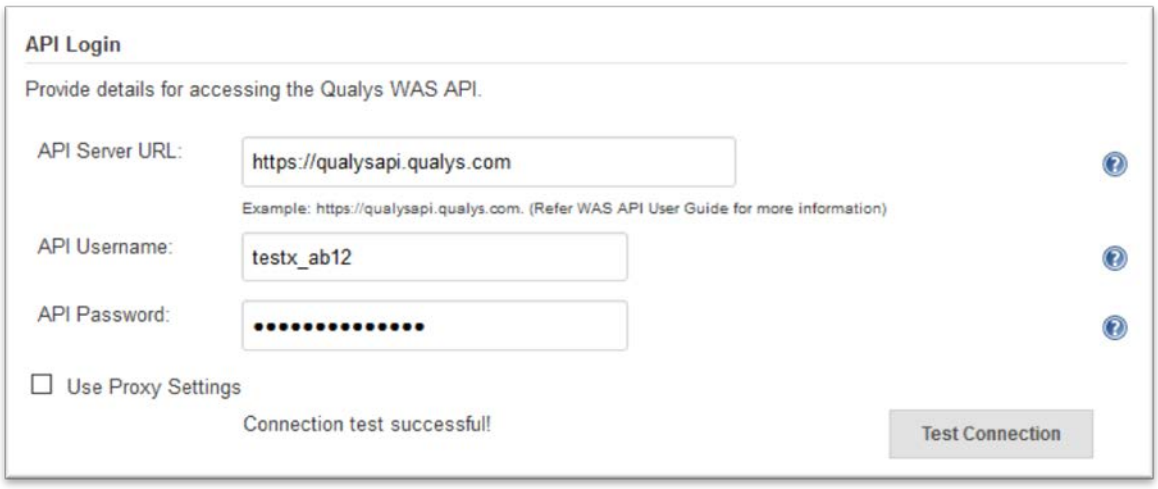


Now you are ready to configure the plugin. The first step is to confirm that Jenkins can communicate to the Qualys Cloud Platform via the WAS API. You'll need valid account credentials for an active Qualys WAS subscription. The account must have API access enabled as well as a role assigned with all necessary permissions. Qualys recommends using a service account restricted to API access only (no UI access) and having the least privileges possible.

Enter your Qualys API Server base URL. What you enter here depends on the particular Qualys platform your organization is using. Learn more

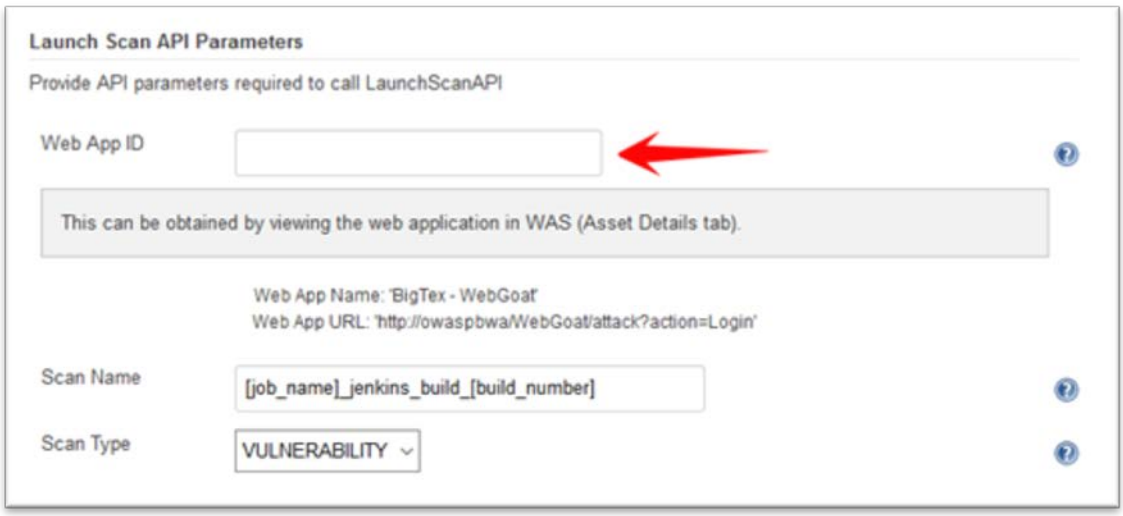
If your Jenkins instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" checkbox and enter the required information.

Enter the username and password for authenticating to the WAS API and click the "Test Connection" button.



Assuming you have entered the correct URL for your subscription and the credentials are valid, you will see the message "Connection test successful!".

Next, enter the ID for the web application in Qualys WAS that is associated with this application.



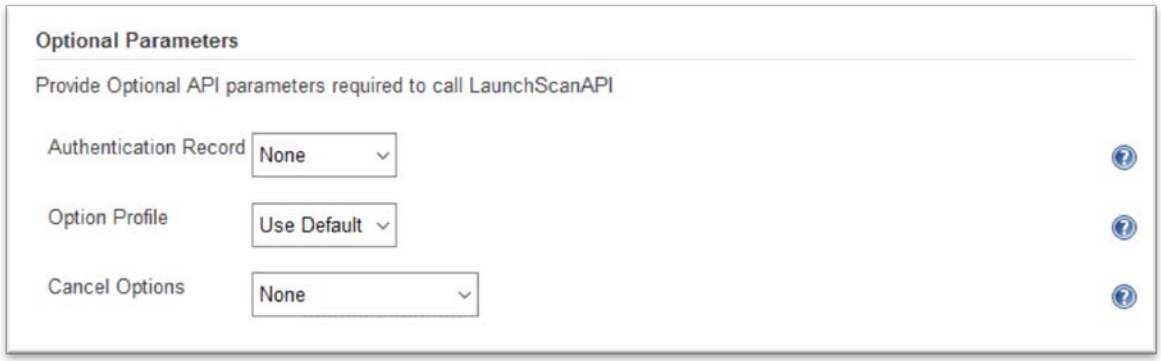
Notice that when you tab or click out of the Web App ID field, an API call is performed to retrieve the web app name and web app URL for the ID entered. Confirm the name and URL are what you expect.

By default, the WAS scan name will be:
`[job_name]_jenkins_build_[build_number] + timestamp`

You can edit the scan name as desired, but a timestamp will automatically be appended regardless.

You can choose to run a Discovery scan or Vulnerability scan. The default is Vulnerability scan.

Next, configure optional scan parameters.

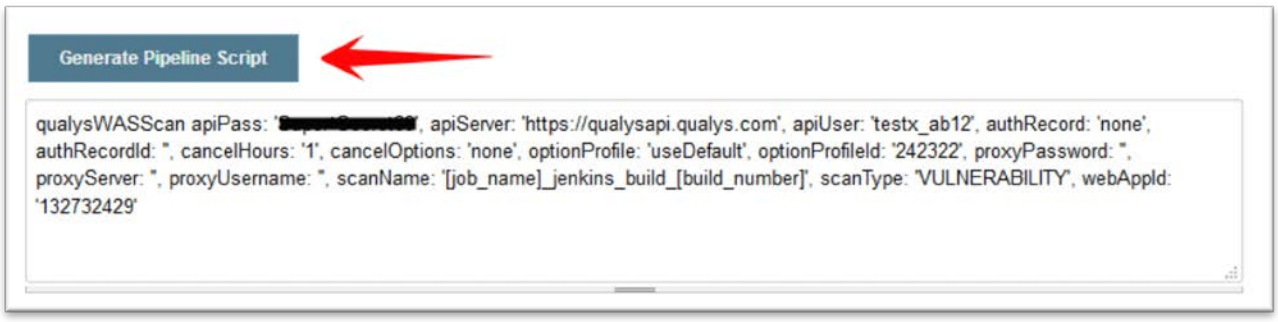


Authentication Record – You can choose to run the scan without authentication (the default) but keep in mind the scanner will not be able to log into the web application and test the authenticated surface area of the application in that case. You may instead want to select "Use Default", in which case the default authentication record for the web app in WAS (if any) will be used. You can also choose to enter a specific authentication record ID if desired.

Option Profile – The option profile contains the various scan settings such as the vulnerability types that should be tested (detection scope), scan intensity, error thresholds, etc. Selecting "Use Default" will use the default option profile for the web app in WAS. This is the recommended setting, however you can also choose to enter a specific option profile ID if desired.

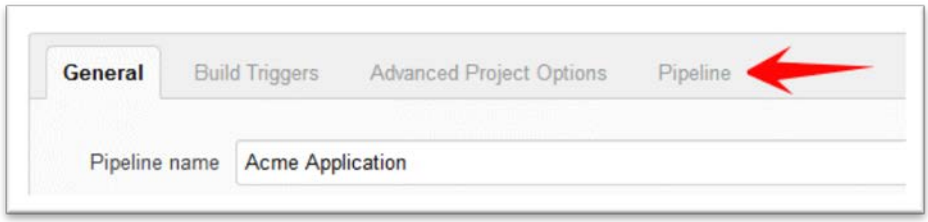
Cancel Options – The default is not to cancel the scan, in which case the scan will run to completion. However, you can choose to the cancel the scan after a set number of hours. Keep in mind you may not get any results if the scan is cancelled before finishing.

Next, click "Generate Pipeline Script". This is your pipeline snippet for launching a WAS scan.



The pipeline snippet is now ready to be plugged into your pipeline script. To prevent exposure of the Qualys API credentials in the script, follow steps in the next section.

Under your project configuration, click "Pipeline".

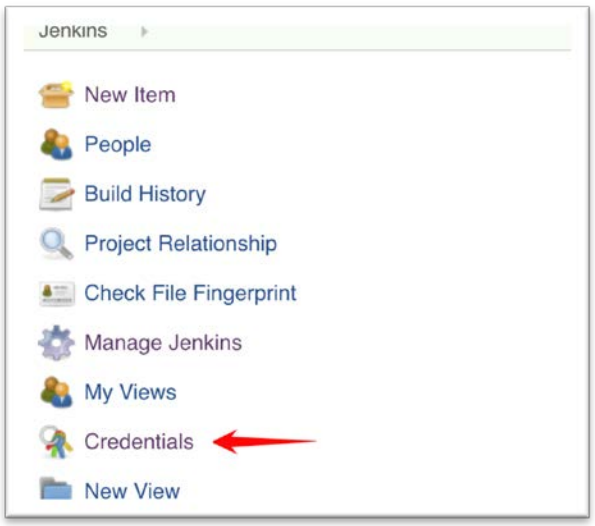


Create a new stage called "QualysWASscan" (or something similar). Follow the steps in the next section to protect the API credentials, then paste into the pipeline script here.

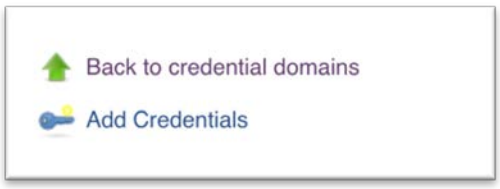
Protect Your Qualys API Credentials

Qualys strongly recommends using the built-in Jenkins Environment Variables functionality to store the Qualys API username and password. This will prevent exposure of the credentials in the pipeline script.

Jenkins can store credentials and other secrets as variables to protect them from disclosure in scripts. To store credentials in Jenkins, select "Credentials" from the main page.

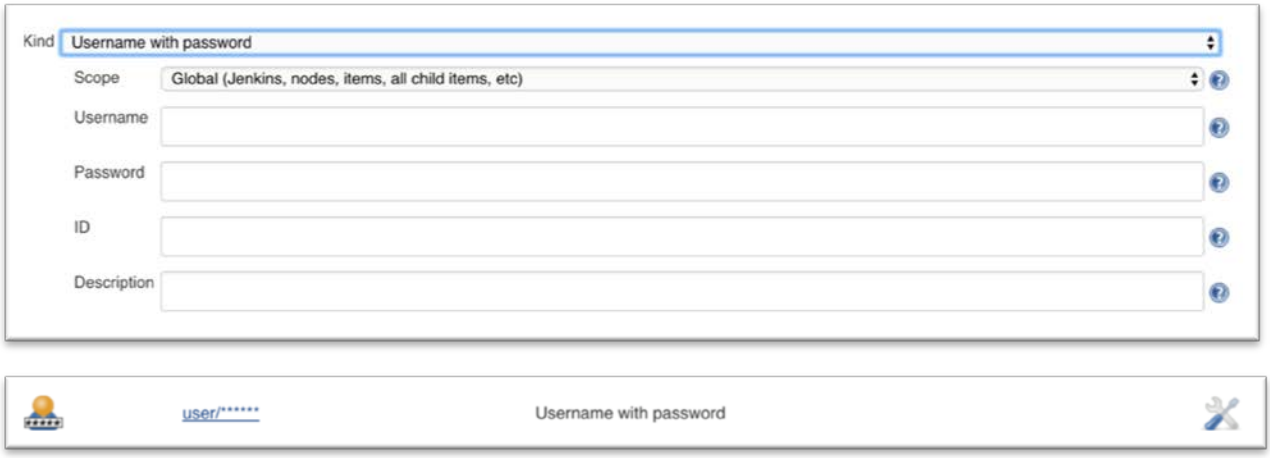


Select "Add Credentials".



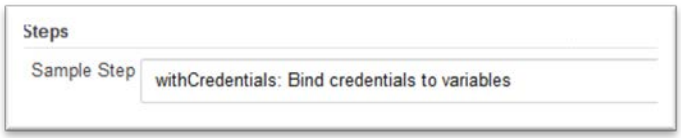
Choose the type of credentials. For the Qualys WAS plugin, choose "Username with password".

Enter your credentials and choose an ID for the credentials.

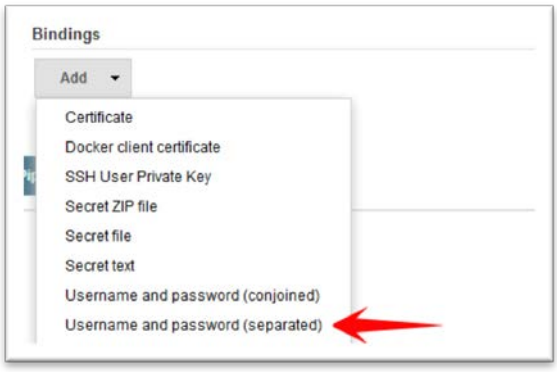


Once the record is added, it is ready to use in your scripts.

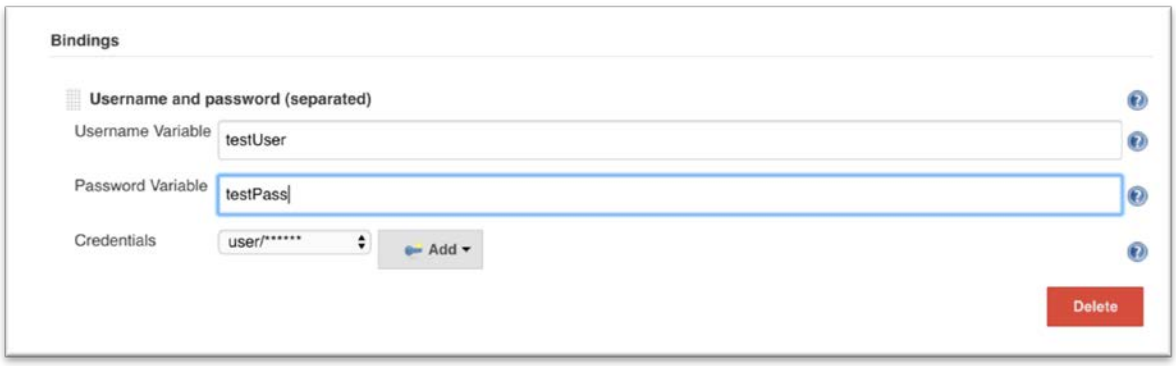
Click "Pipeline Syntax" to enter the Snippet Generator. From the drop-down, select "withCredentials : Bind credentials to variables".



Under Bindings, select "Username and Password (separated)".



Enter variable names for your username and password



Once entered, select "Generate Pipeline Script". It should look similar to this:

```
withCredentials([usernamePassword(credentialsId: 'Test Credentials ',
passwordVariable: 'testPass', usernameVariable: 'testUser')])  {
    // some block
}
```

Paste the above into your pipeline build script.

To access the variables in your generated pipeline snippet for WAS, the syntax is:

```
(env.testUser)
(env.testPass)
```

Replace the Qualys API credentials in the generated pipeline snippet for WAS with these variables. The final result will look something like this:

```
qualysWASScan apiPass: (env.testPass), apiServer:
'https://qualysapi.qualys.com', apiUser: (env.testUser), authRecord:
'useDefault', authRecordId: '', cancelHours: '1', cancelOptions: 'none',
optionProfile: 'useDefault', optionProfileId: '', proxyPassword: '',
proxyServer: '', proxyUsername: '', scanName:
'[job_name]_jenkins_build_[build_number]', scanType: 'VULNERABILITY',
webAppId: '132732429'
```

URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysapi.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysapi.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysapi.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

Last updated: April 25, 2018