

# Black Duck Scanning for Baker Hughes

This work performed under contract to:

[Baker Hughes]

**For more information contact:**

Cindy Xu  
**Manager Client Services**

[Mike Acosta]  
**Client Services Engineer**

Status:	Draft
Version:	1.1
Date:	11/18/2022



## Proprietary Statement

© 11/20/22 Synopsys, Inc. All rights reserved worldwide. No part or parts of this documentation may be reproduced, translated, stored in any electronic retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the copyright owner. Synopsys, Inc. retains the exclusive title to all intellectual property rights relating to this documentation.

The information in this documentation is subject to change without notice and should not be construed as a commitment by Synopsys, Inc. Synopsys, Inc. makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user's customers), that may be suffered by the user.

Synopsys and the Synopsys logo are trademarks of Synopsys, Inc. Other brands and products are trademarks of their respective owner(s).

### **Synopsys, Inc.**

185 Berry Street, Suite 6500  
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193

International Sales: +1 415.321.5237

Email: [sig-info@synopsys.com](mailto:sig-info@synopsys.com)

**[www.synopsys.com/software](http://www.synopsys.com/software)**

# Table of Contents

<b>1</b>	<b>Black Duck Console.....</b>	<b>5</b>
1.1	How to login to the console? .....	5
1.2	How to get access to the console? .....	5
1.2.1.	For Active Directory Group .....	5
1.2.2.	For DL Membership Management .....	6
1.3	How to get a role assigned to your BD User Account.....	7
<b>2</b>	<b>Manual Scanning.....</b>	<b>7</b>
2.1	Process To Scan .....	7
2.2	Scanning Properties .....	7
2.3	Scanning Tools .....	8
2.3.1	Downloading Detect (For Manual Scanning) .....	8
2.3.2	Downloading Signature Scanner .....	10
2.4	Configuring UI Detect Desktop.....	10
2.4.1	Generating an Access Token .....	10
2.4.2	Connecting the UI Detect to the BD Console .....	11
2.5	Scanning with UI Detect Desktop.....	12
2.5.1	Configuring The Scan .....	12
2.5.2	Rapid vs. Full/Intelligent Scanning.....	13
2.5.3	Naming Convention .....	13
2.5.4	Running The Scan.....	14
2.5.5	Additional Configuration for Build Tools .....	14
<b>3</b>	<b>Scanning with CI/CD .....</b>	<b>16</b>
3.1	Service Account for CI/CD.....	16
3.2	Jenkins.....	16
3.2.1	Freestyle .....	17
3.2.2	Pipeline .....	18
3.2.3	Execute Windows Batch Command.....	19
3.2.4	<i>Troubleshooting the Signature Scanner via Jenkins</i> .....	20
3.3	Github Actions .....	20
3.3.1	Set Up Workflow.....	20
3.3.2	Setting Up The Job.....	21
3.3.3	Confirming the Action .....	22
3.3	Azure Devops .....	23
3.3.1	Using the Plugin .....	23
3.3.2	Configuring the Plugin .....	24
3.3.3	Using Powershell.....	25
3.3.4	Using Variables .....	26
3.3.5	Confirming a Successful Run .....	27

<b>4</b>	<b>Viewing Results in Black Duck .....</b>	<b>28</b>
4.1	Navigating the UI to your Scanned Project/Version .....	28
4.1.1	Using a Direct Link to Project/Version.....	28
4.1.2	Using the Black Duck Console.....	29
4.2	Understanding your Results (BOM – Bill of Materials).....	30
<b>5</b>	<b>Additional Resources .....</b>	<b>33</b>
5.1.	Troubleshooting.....	33
5.2.	External Links.....	33

## 1 Black Duck Console

Baker Hughes has 2 Black Duck environments (PROD/DEV). Logging into either console is done through Okta and requires you to get access.

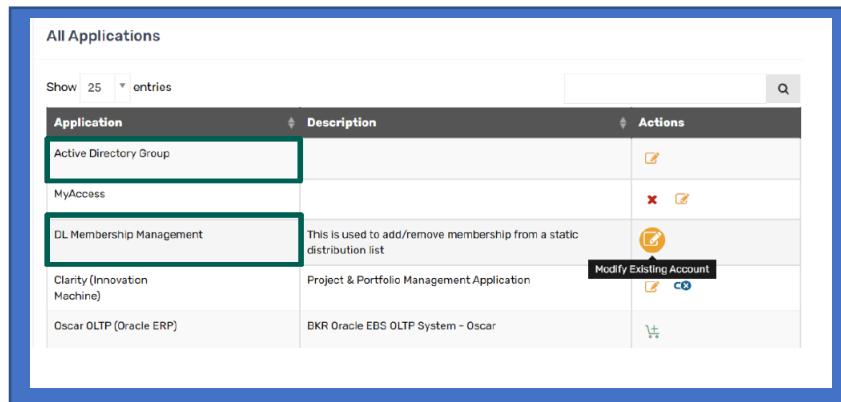
### 1.1 How to login to the console?

Dev: <https://bakerhughes-test.app.blackduck.com>

Prod: <https://bakerhughes.app.blackduck.com>

### 1.2 How to get access to the console?

- 1) Submit a MyAccess Request by navigating to <https://myid.bakerhughes.com>
- 2) Locate and click the chiclet titled “MyAccess”
- 3) Click “Request Access”
- 4) Locate Active Directory Group & DL Membership Management under All Applications
- 5) Under Actions select “Modify Existing Account” to add to cart



- 6) If prompted, select your domain login for which account name.

#### 1.2.1. For Active Directory Group

- 1) Under “Available Groups”, locate the group name “myid\_blackduck\_preprod ” and “ myid\_blackduck\_prod ”

**See Next Page**

## CONT'D For Active Directory Group

1 Select System 2 Select Access

Item #1 OF 1

Security System: Active Directory Group Endpoint: Active Directory Group

Available Groups

Show 5 entries

myid\_blackduck\_preprod

Groups	Description	Action
myid_blackduck_preprod	Members of this group receive access into BlackDuck Dev	+

Showing 1 to 1 of 1 entries

2) Under Actions, click the blue “+” to Add to Cart

### 1.2.2. For DL Membership Management

- 1) Under “Available Groups”, locate the group name “bh\_oss-tool-users”
- 2) Under Actions, click the blue “+” to Add to Cart

Item #1 OF 1

Security System: DL Membership Management Endpoint: DL Membership Management

Available Distribution List

Show 5 entries

bh\_oss

Distribution List	Description	Action
bh_oss-tool-users		+

Showing 1 to 1 of 1 entries

- 3) Next, select “Checkout”
- 4) Once you have reviewed your selections, click “Submit”

### 1.3 How to get a role assigned to your BD User Account

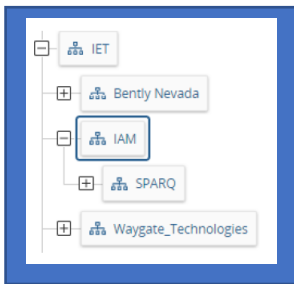
To be assigned your role in BlackDuck, send an email to:  
ApplicationSecurity@bakerhughes.com using the following template:

Hello,

Please assign Project Creator role to "Insert Your Name" to "Insert Your Team Name".

My business hierarchy is as follows....

**Note:** Provide your business hierarchy as noted below. I.E. (OFSE -> IMS -> Team)



## 2 Manual Scanning

Scanning in Black Duck is done through CI/CD tools or through Manual Scanning using the BlackDuck UI or the CLI

### 2.1 Process To Scan

A new team should get comfortable with how the tool works, which is why we recommend you do your initial scan to the DEV console. Once you get comfortable and understand the results and the different ways to scan, you can then simply change the BlackDuck URL parameter to point to PROD.

### 2.2 Scanning Properties

Regardless of what method you wish to scan, you must use, at minimum, the following properties for each scan:

- detect.project.name
- detect.project.version.name
- detect.project.group.name
- detect.project.user.groups

For more information on which project group or user group you belong in, please reach out to [OSSAdmin@bakerhughes.com](mailto:OSSAdmin@bakerhughes.com)

All the properties you can append to the tools can be found on this link:

[https://community.synopsys.com/s/document-item?bundleId=integrations-detect&topicId=properties/all-properties.html&\\_LANG=enus](https://community.synopsys.com/s/document-item?bundleId=integrations-detect&topicId=properties/all-properties.html&_LANG=enus)

**NOTE:** Not all the properties are available via the UI Tool.

## 2.3 Scanning Tools

Black Duck uses 2 tools to scan under the hood:

- Detect
- Signature Scanner

The Detect tool scans for package managers while the Signature Scanner scans each file in the source provided. An example of scanning with Detect is that the tool might find a `build.gradle` file and it will be smart enough to know that this is a Gradle project and check for direct and transitive dependencies. The signature scanner doesn't care what build tool it used because it will scan file by file and try to match it against our KnowledgeBase (KB).

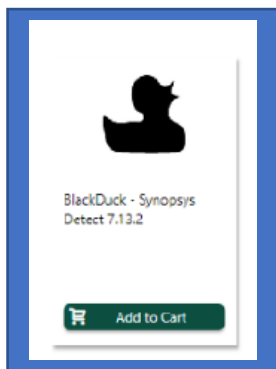
By default, both tools are used but you do have the option of using one or the other, even though we recommend using both.

**NOTE:** The initial scan, manual or via a pipeline, will download the Signature Scanner tool.

### 2.3.1 Downloading Detect (For Manual Scanning)

To download Black Duck Synopsys, visit the TechHub Baker Hughes website:

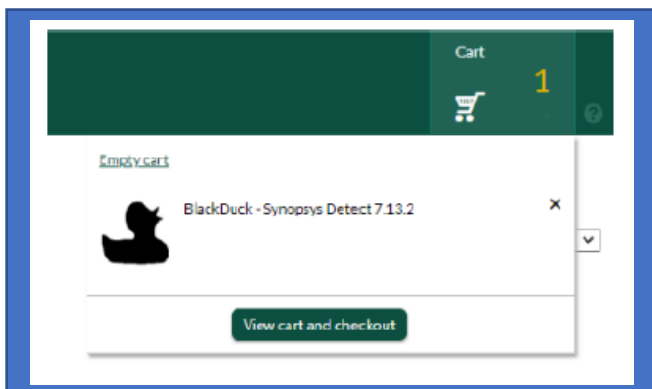
1. Log in to <https://techhub.ent.bhicorp.com/esd>
2. Using the "Search Catalog" bar, type in "BlackDuck", then select the following icon to "Add to Cart"



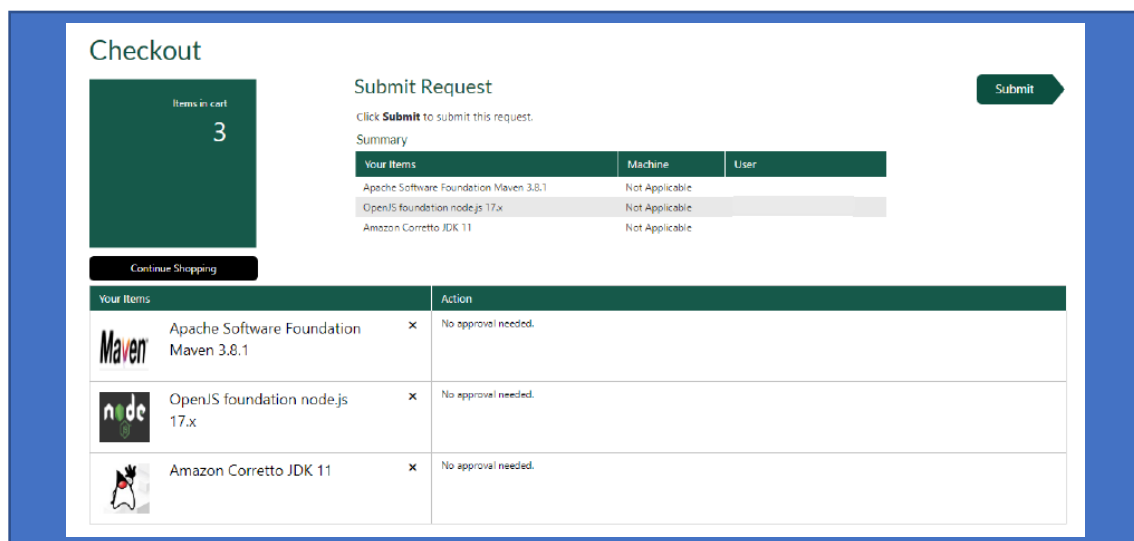


## CONT'D Downloading Detect (For Manual Scanning)

3. In the top right corner, click “Cart” and scroll down to “View cart and checkout”



4. Review and confirm your selections, then click “Submit.”



5. Once you have submitted your request, you should receive an email from TechHub. This email should include the links to download the submitted prerequisites.

### 2.3.2 Downloading Signature Scanner

There may be a situation where the Signature Scanner fails to download during the initial scan run (when you run Detect for the first time). If this is the case, you will need to manually download the Signature Scanner.

You can find that location here:

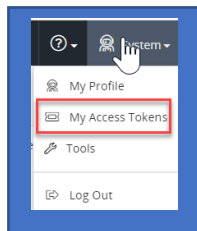
[https://bakerhughes-my.sharepoint.com/:f:/p/far-han\\_syed/EmitYg4fGBtClyeR2gXIeHEB94aAF8g5YNqafKwHQWHycA?e=bRhea3&OR=Teams-HL&CT=1668792715512&clickparams=eyJBCbHBOYW1lLjojVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiNy8yMjEwLmJgWzlwMCIslkhhc0ZIZGVyYXRIZFVzZXliOmZhbHNlfQ%3D%3D](https://bakerhughes-my.sharepoint.com/:f:/p/far-han_syed/EmitYg4fGBtClyeR2gXIeHEB94aAF8g5YNqafKwHQWHycA?e=bRhea3&OR=Teams-HL&CT=1668792715512&clickparams=eyJBCbHBOYW1lLjojVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiNy8yMjEwLmJgWzlwMCIslkhhc0ZIZGVyYXRIZFVzZXliOmZhbHNlfQ%3D%3D)

## 2.4 Configuring UI Detect Desktop

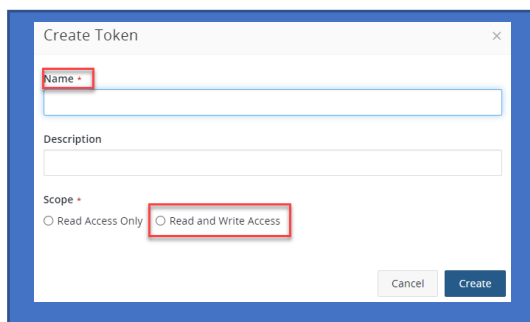
When manually doing a scan, you need to first configure the UI. The first thing you need to do is generate an API token using your OWN user account, via the Black Duck console. Service Accounts should not be used for Manual Scanning.

### 2.4.1 Generating an Access Token

- 1) Log into the BD Console
- 2) Click on your name at the upper right side and select My Access Tokens



- 3) Click on Create Token and make sure to give it a name and select the Read and Write Access Scope option.



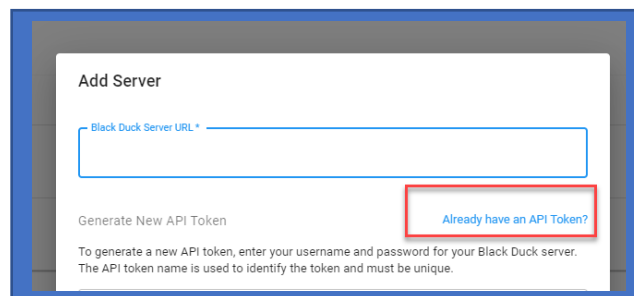
4) After you click create, make sure you save that API token as you'll need to add it in the UI Detect Scanning tool.

### 2.4.2 Connecting the UI Detect to the BD Console

Open the UI Detect software and click on the top right icon to access the Server Configuration:

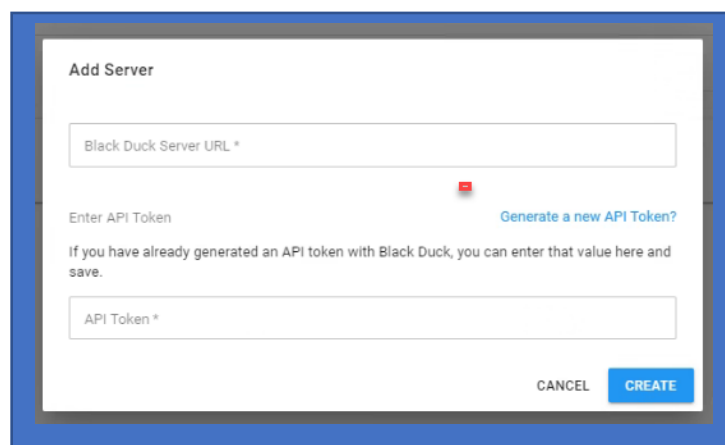


This will take you to this screen where you will need to click the Add Server button.

A screenshot of a web application window titled "Add Server". It contains a text input field labeled "Black Duck Server URL \*". Below the field, there is a section titled "Generate New API Token" with instructions: "To generate a new API token, enter your username and password for your Black Duck server. The API token name is used to identify the token and must be unique." To the right of this section, there is a red-bordered box containing the link "Already have an API Token?".

Click on the **Already have an API Token?** link.

You will get the following screen where you will enter the API token you generated earlier and the BD (PROD/DEV) URL of the console

A screenshot of the same "Add Server" dialog box. The "Black Duck Server URL \*" field is now empty. Below it, there is a section titled "Enter API Token" with a red error icon and the text "Generate a new API Token?". Below this, there is a text input field labeled "API Token \*". At the bottom right, there are two buttons: "CANCEL" and "CREATE".

A successful connection will look like the one below:

Server Configuration

In order to connect with a Black Duck server, you will need to generate an API token.

☒ Ignore validation for invalid or insecure TLS Certificates (Not Recommended)

This is a potentially unsafe operation. It should only be used if you must connect to a system with an insecure or self-signed certificate. Changing this setting will require you to restart the application.

**ADD SERVER**

Server	Version
https://bakerhughes.app.blackduck.com	2022.7.1
https://bakerhughes-test.app.blackduck.com	2022.7.1

Under Server you should see the URL of the console as well as what version of the console you are running.

**NOTE:** If it fails, click on the upper left checkmark (Ignore Validation) and repeat the same process.

## 2.5 Scanning with UI Detect Desktop

To scan with UI Detect, you would click on the “NEW SCAN” button at the top left of the screen.

### 2.5.1 Configuring The Scan

Complete the following on the left side of the screen:

**SELECT SOURCE DIRECTORY**

**CHOOSE BETWEEN FULL SCANNING OR RAPID SCANNING**

**CHOOSE THE PATH OF THE CODEBASE YOU WANT TO SCAN**

**Project Settings**

Project Name

Version Name

Project User Groups

Project Group Name

**Scan Settings**

Offline Mode

**RESET**

**Project Settings**

Project Name

Version Name

Project User Groups

Project Group Name

**Allow Project Level Adjustments**

If set, created projects will be created with the value of this property. For updates, see detect.project.version.update. (Default Value: true)

**Application ID**

Gets the Application ID project setting.

**Clone Latest Project Version**

If set to true, detect will attempt to use the latest project version as the clone for this project. The project must exist and have at least one version. (Default Value: false)

**Clone Project Categories**

## CONT'D Configuring The Scan

Click on the ADD button under Project Settings and find the 4 ones that were mentioned earlier by scrolling down the list and putting a check mark next to them.

They are:

- **Project Name**
- **Version Name**
- **Project User Groups**
- **Project Group Name**

Be sure to add value to each field.

### 2.5.2 Rapid vs. Full/Intelligent Scanning

One of the options for Scan Mode is Rapid or Full. Below is some information that let's you know the difference between each:

Black Duck's Rapid Scanning provides a way for developers to quickly determine if the versions of open source components included in a project violate corporate policies surrounding the use of open source. Using Synopsys Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Use Rapid Scanning when you need quick feedback and when persisting the data in Black Duck is not necessary.

Intelligent Scanning, also referred to as Full Scanning, does the same thing that the Rapid Scanning does with the exception of pushing the results into the Black Duck server database and creating a BOM (Bill of Materials) that allows you to see the results.

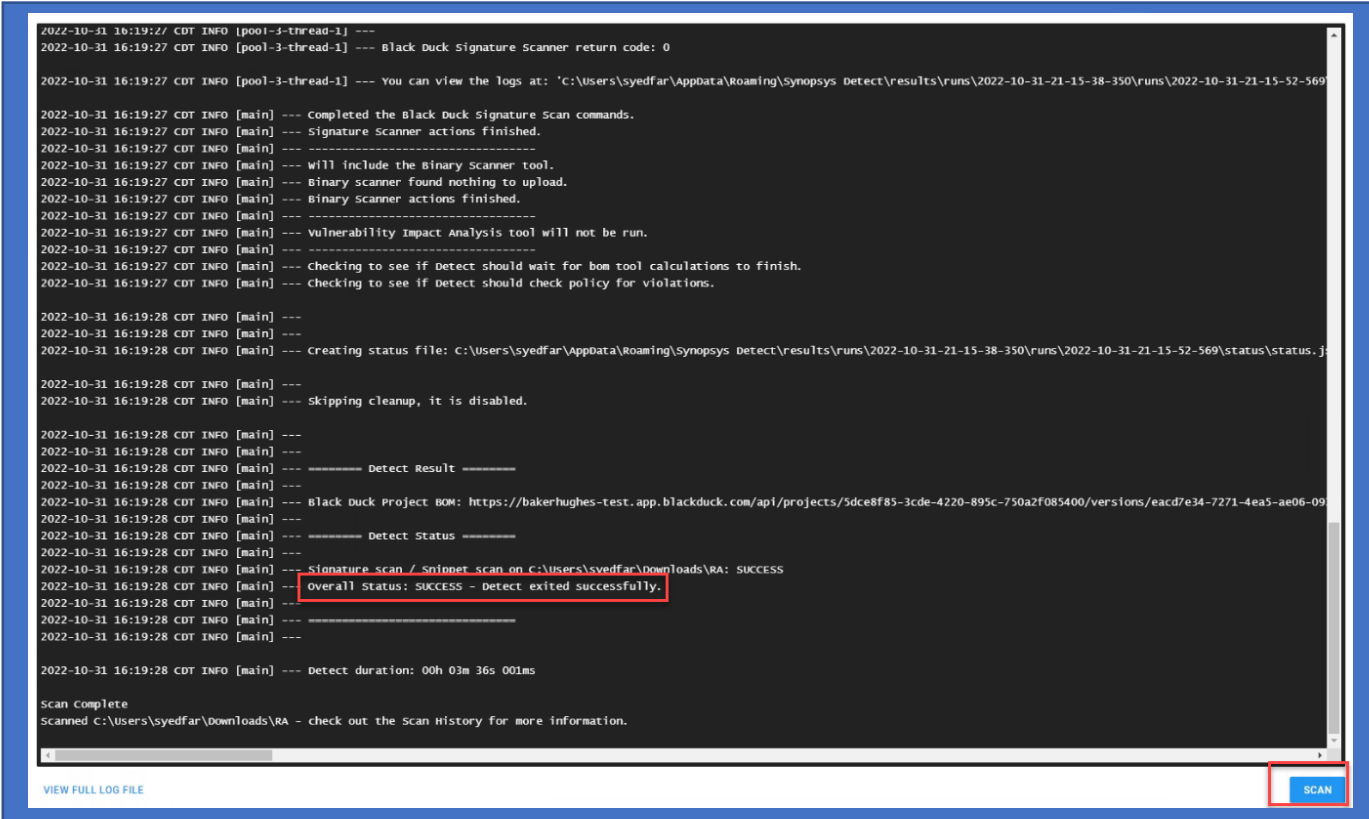
### 2.5.3 Naming Convention

Baker Hughes has a naming convention that you will be using for each application you onboard. The value of this naming convention goes in the field of **Project Name**

The naming convention is: `ApplicationCI_ApplicationProjectName`

## 2.5.4 Running The Scan

The last step after everything is configured is to click the SCAN button at the bottom right of the application.



```

2022-10-31 16:19:27 CDT INFO [pool-3-thread-1] ---
2022-10-31 16:19:27 CDT INFO [pool-3-thread-1] --- Black Duck Signature Scanner return code: 0
2022-10-31 16:19:27 CDT INFO [pool-3-thread-1] --- You can view the logs at: 'C:\Users\syedfar\AppData\Roaming\Synopsys Detect\results\runs\2022-10-31-21-15-38-350\runs\2022-10-31-21-15-52-569
2022-10-31 16:19:27 CDT INFO [main] --- Completed the Black Duck Signature Scan commands.
2022-10-31 16:19:27 CDT INFO [main] --- Signature Scanner actions finished.
2022-10-31 16:19:27 CDT INFO [main] ---
2022-10-31 16:19:27 CDT INFO [main] --- Will include the Binary Scanner tool.
2022-10-31 16:19:27 CDT INFO [main] --- Binary scanner found nothing to upload.
2022-10-31 16:19:27 CDT INFO [main] --- Binary Scanner actions finished.
2022-10-31 16:19:27 CDT INFO [main] ---
2022-10-31 16:19:27 CDT INFO [main] --- Vulnerability Impact Analysis tool will not be run.
2022-10-31 16:19:27 CDT INFO [main] ---
2022-10-31 16:19:27 CDT INFO [main] --- Checking to see if Detect should wait for bom tool calculations to finish.
2022-10-31 16:19:27 CDT INFO [main] --- Checking to see if Detect should check policy for violations.
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- Creating status file: C:\Users\syedfar\AppData\Roaming\Synopsys Detect\results\runs\2022-10-31-21-15-38-350\runs\2022-10-31-21-15-52-569\status\status.j
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- Skipping cleanup, it is disabled.
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- ===== Detect Result =====
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- Black Duck Project BOM: https://bakerhughes-test.app.blackduck.com/api/projects/5dce8f85-3cde-4220-895c-750a2f085400/versions/eacd7e34-7271-4ea5-ae06-09
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- ===== Detect Status =====
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- Signature scan / Snippet scan on C:\Users\syedfar\Downloads\RA: SUCCESS
2022-10-31 16:19:28 CDT INFO [main] --- Overall Status: SUCCESS - Detect exited successfully.
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] ---
2022-10-31 16:19:28 CDT INFO [main] --- Detect duration: 00h 03m 36s 001ms
2022-10-31 16:19:28 CDT INFO [main] ---
Scan Complete
Scanned C:\Users\syedfar\Downloads\RA - check out the Scan History for more information.

```

VIEW FULL LOG FILE

SCAN

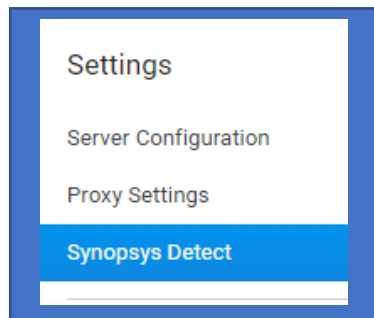
The message you want to see which is located at the bottom is:  
**OVERALL STATUS SUCCESS**, meaning everything scanned without any issues and sent the data over the Black Duck.

## 2.5.5 Additional Configuration for Build Tools

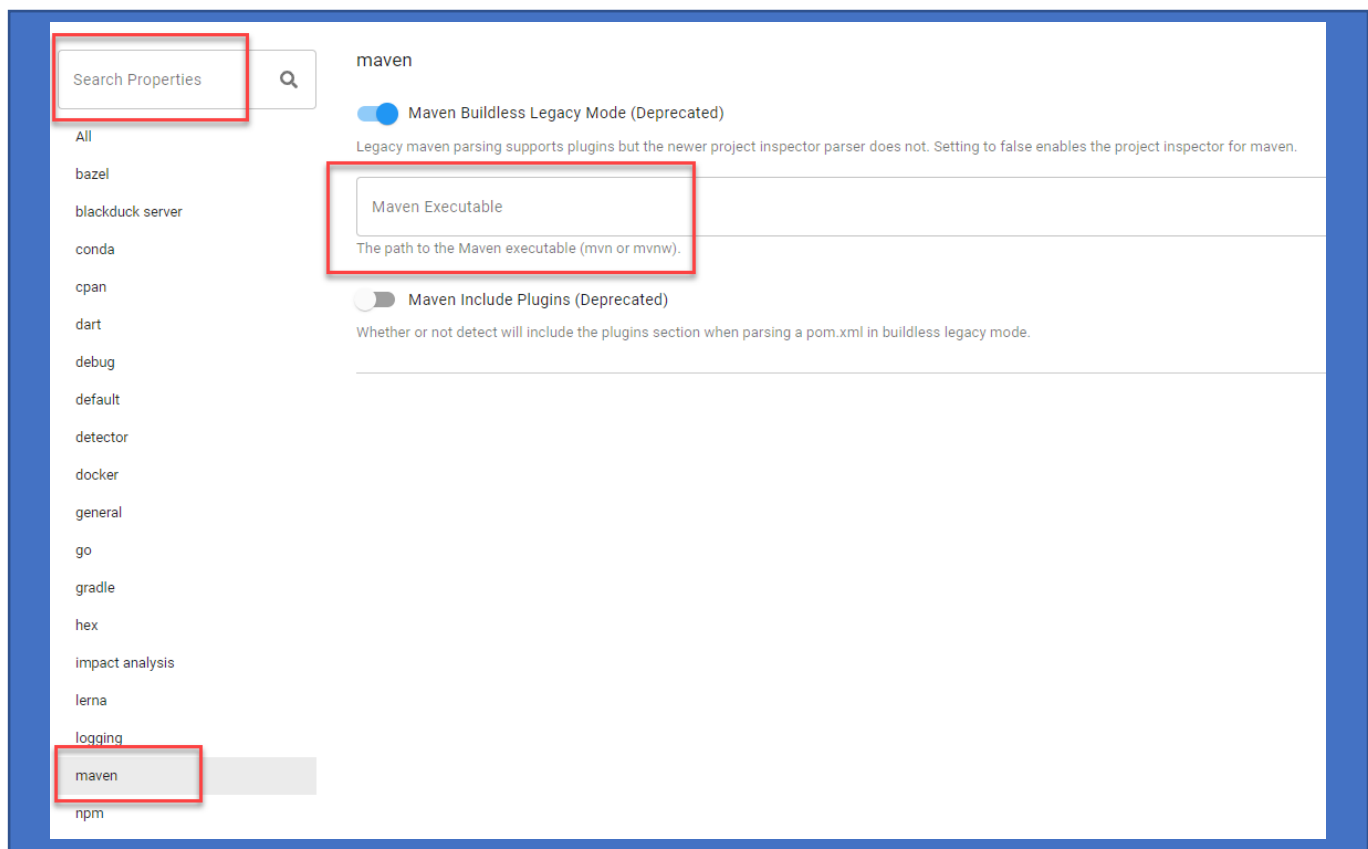
If you know in advance you are using a Maven or Gradle project for example, there is some additional configuration you need to do to scan for dependencies.

Back at the SETTINGS section, click on **Synopsys Detect** under Settings.

## CONT'D Additional Configuration for Build Tools



In this example, we will use Maven:



Select MAVEN from the left side or search for MAVEN via “Search Properties” text field at the top left.

Under Maven Executable, you will see a little folder icon on the right side that allows you to find the path to Maven. Click on that and find the executable path to Maven.

## CONT'D Additional Configuration for Build Tools

Now when you scan a Maven project, the Detect tool is smart enough to know if it finds a `pom.xml` file, that the project was built using Maven and run specific Maven commands (such as `tree` commands) to find the direct and transitive dependencies.

## 3 Scanning with CI/CD

Black Duck was configured to integrate with Jenkins, Github Actions, and Azure Devops. This section provides the configuration methods and how to scan using these tools.

### 3.1 Service Account for CI/CD

If you have an existing service account and would like to access BlackDuck with contact SOLV and have submit a ticket to have it be added to Active Directory group that you had joined via MyAccess.

If you are creating a service account for the first time click [here](#).

### 3.2 Jenkins

We successfully configured Black Duck with Jenkins using three different ways: Freestyle, Pipeline, Windows Batch Executable during the Batch.

Depending on the version of Jenkins, you may or may not be able to use the Black Duck Plugin. For more information on the requirements, please see the following link:

<https://synopsys.atlassian.net/wiki/spaces/INTDOCS/pages/824311829/Requirements+for+Synopsys+Detect+Plugin>

To download the plugin for Jenkins, follow the steps below (after verifying your requirements are met)

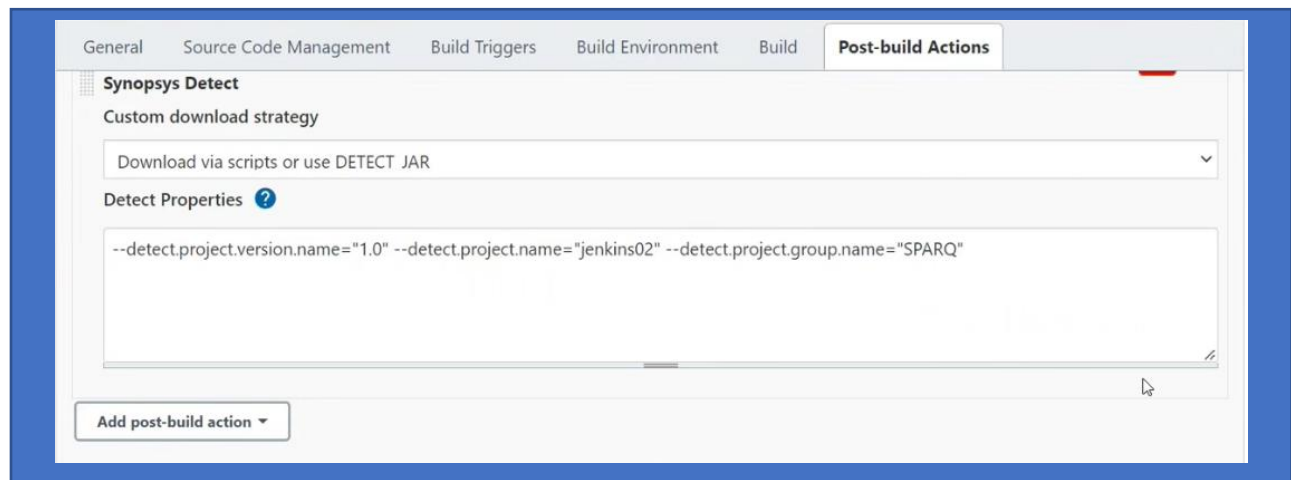
1. To install the Synopsys Detect for Jenkins plugin, do the following steps:
2. Navigate to Manage Jenkins > Manage Plugins.
3. Select the Available tab. Note that if the plugin is already installed, it does not appear in the Available list.



4. Select Synopsys Detect.
5. Click Download now and install after restart. This is the Synopsys recommendation for installing the plugin.
6. After restarting Jenkins, confirm that the plugin is successfully installed by navigating to Manage Jenkins > Manage Plugins > Installed, and verify that Synopsys Detect displays in the list.

### 3.2.1 Freestyle

The Freestyle workflow is the easiest one. Under the “Add Post-Build Action” simply select Synopsys Detect.



As you can see in this example, the only thing you need to do is add the 4 required properties that were listed earlier:

- `detect.project.name`
- `detect.project.version.name`
- `detect.project.group.name`
- `detect.project.user.groups`

In the screenshot you'll notice the last one is missing (`detect.project.user.groups`), but it is still required. Add the 2 dashes before each property and double quotes after each value, example:

```
--detect.project.name="test"
```

Leave the Custom Download Strategy as you see it.

### 3.2.2 Pipeline

A pipeline script is very similar to a Freestyle, when using the plugin, because you can leverage the plugin object with the name **synopsys\_detect**

```

61 stage('black_duck_test')
62 {
63     steps{
64         synopsys_detect '' --blackduck.url='https://bakerhughes-test.app.blackduck.com'
65     }
66 }

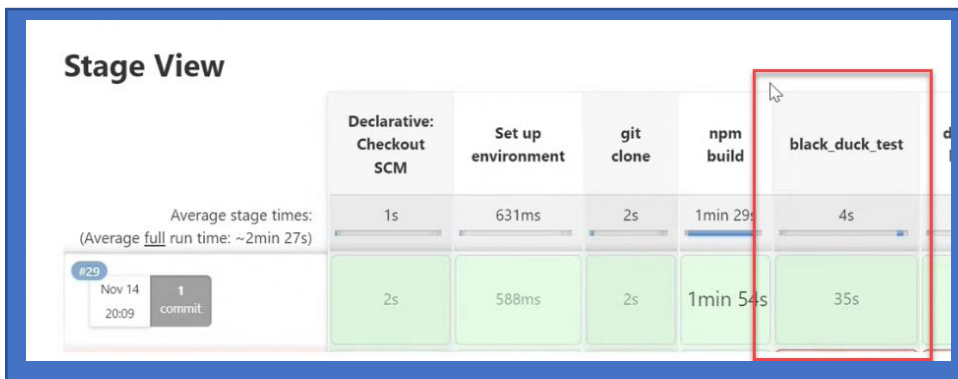
```

You would need to include additional properties when using this method:

- blackduck.url
- blackduck.api.token

These are not necessary when using the Freestyle method.

Once you run it, you can now see it in stages and you will see the outcome via the Stage View



In addition, you can always look at the output in realtime:

Confidential  
Proprietary

```

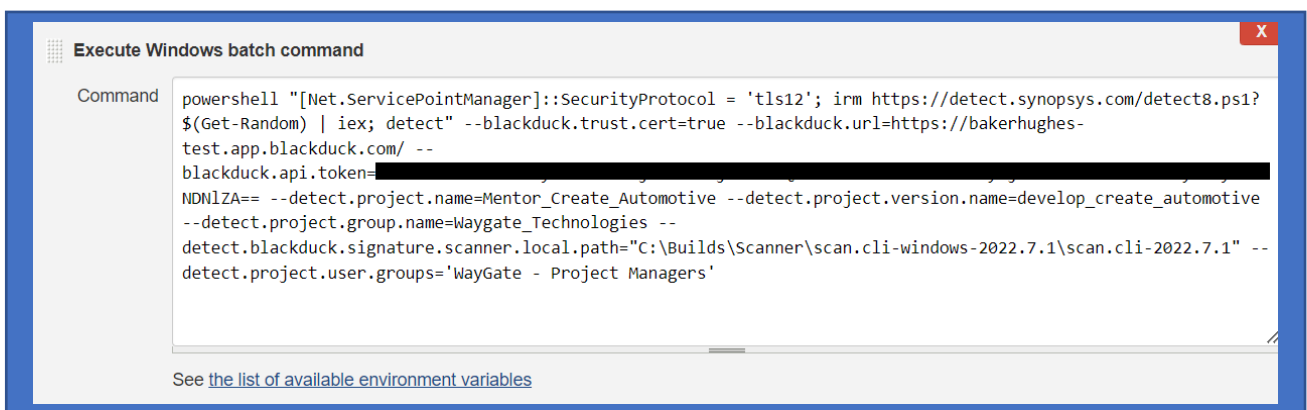
DEV  ▸ SPS-Analytics-ui-App-Black-Duck-Testing  ▸ #29
2022-11-14 14:42:03 UTC INFO [main] ---
2022-11-14 14:42:03 UTC INFO [main] --- ===== Detect Status =====
2022-11-14 14:42:03 UTC INFO [main] ---
2022-11-14 14:42:03 UTC INFO [main] --- GIT: SUCCESS
2022-11-14 14:42:03 UTC INFO [main] --- NPM: SUCCESS
2022-11-14 14:42:03 UTC INFO [main] ---
2022-11-14 14:42:03 UTC INFO [main] --- Signature scan / Snippet scan on /home/jenkins/workspace/MTC_Jobs/SPS/DEV/SPS
Analytics-ui-App-Black-Duck-Testing: SUCCESS
2022-11-14 14:42:03 UTC INFO [main] --- Overall Status: SUCCESS - Detect exited successfully.
2022-11-14 14:42:03 UTC INFO [main] ---
2022-11-14 14:42:03 UTC INFO [main] --- =====
2022-11-14 14:42:03 UTC INFO [main] ---
2022-11-14 14:42:03 UTC INFO [main] --- Detect duration: 00h 00m 26s 256ms
Result code of 0, exiting

```

Once you see the SUCCESS status, your scan was successful.

### 3.2.3 Execute Windows Batch Command

Another way method we used, on an older version of Jenkins (2.7.4) which doesn't support the plugin, required us to make sure of the Windows Batch Command.



An example of the command above is:

```
powershell "[Net.ServicePointManager]::SecurityProtocol = 'tls12'; irm https://detect.synopsys.com/detect8.ps1?$(Get-Random) | iex; detect" --blackduck.url=https://blackduck.mydomain.com --blackduck.api.token=myaccesstoken
```

You would simply copy and paste that and add the 4 required properties, in addition to the ones I have highlighted above.

**NOTE:** When using powershell, it is important to use SINGLE QUOTES when the value of your property has blank character spaces. Not the last line in the screenshot above.

### 3.2.4 Troubleshooting the Signature Scanner via Jenkins

If the Signature Scanner doesn't run, you will have to manually install it in your build server. In the example above, you noticed that we had to include an additional parameter: `detect.blackduck.signature.scanner.local.path=""`

This task requires your to download the signature scanner from the sharepoint site shared above in the document and unzip it in a path.

## 3.3 Github Actions

You can richly integrate Synopsys Detect into GitHub action workflows. To get the most out of this action, we recommend using RAPID scan-mode for all Pull Requests.

To download the plugin, use this link: <https://github.com/marketplace/actions/detect-rapid-scan-action>

### 3.3.1 Set Up Workflow

The first step is to create a workflow. An example workflow used by one of the teams in Baker Hughes is shown below:

```
- name: Run OSS Scan - BackDuck
  uses: synopsys-sig/detect-action@v0.3.3
  continue-on-error: true
  env:
    DETECT_PROJECT_NAME: "${{ github.event.repository.name }}"
    DETECT_PROJECT_VERSION_NAME: "${{ github.ref }}"
    DETECT_PROJECT_VERSION_LICENSE: "Baker Hughes Proprietary License"
    DETECT_PROJECT_GROUP_NAME: "System 1 APM"
    DETECT_PROJECT_TAGS: "BentlyNevada,GitHub"
    DETECT_DETECTOR_SEARCH_DEPTH: 10
    DETECT_DETECTOR_SEARCH_CONTINUE: true
    DETECT_DIAGNOSTIC: true
  with:
    scan-mode: "${{ steps.oss-scan-mode.outputs.selected-mode }}"
    github-token: ${{{ secrets.GITHUB_TOKEN }}}
```

Confidential and  
Proprietary

```
detect-version: 8.2.0
blackduck-url: ${ secrets.BLACKDUCK_URL }
blackduck-api-token: ${ secrets.BLACKDUCK_TOKEN }
```

Notice that they are using variables (highlighted above) which is the recommended approach, and within those variables, the API Token and the Black Duck URL are required.

The Github Token must be provided by the Git Hub Administrator.

The one property missing above is: `DETECT_PROJECT_USER_GROUP`: which should include the user group you are in.

NOTE: By default scan mode is RAPID but you can change that to Intelligent scanning by adding the following property:

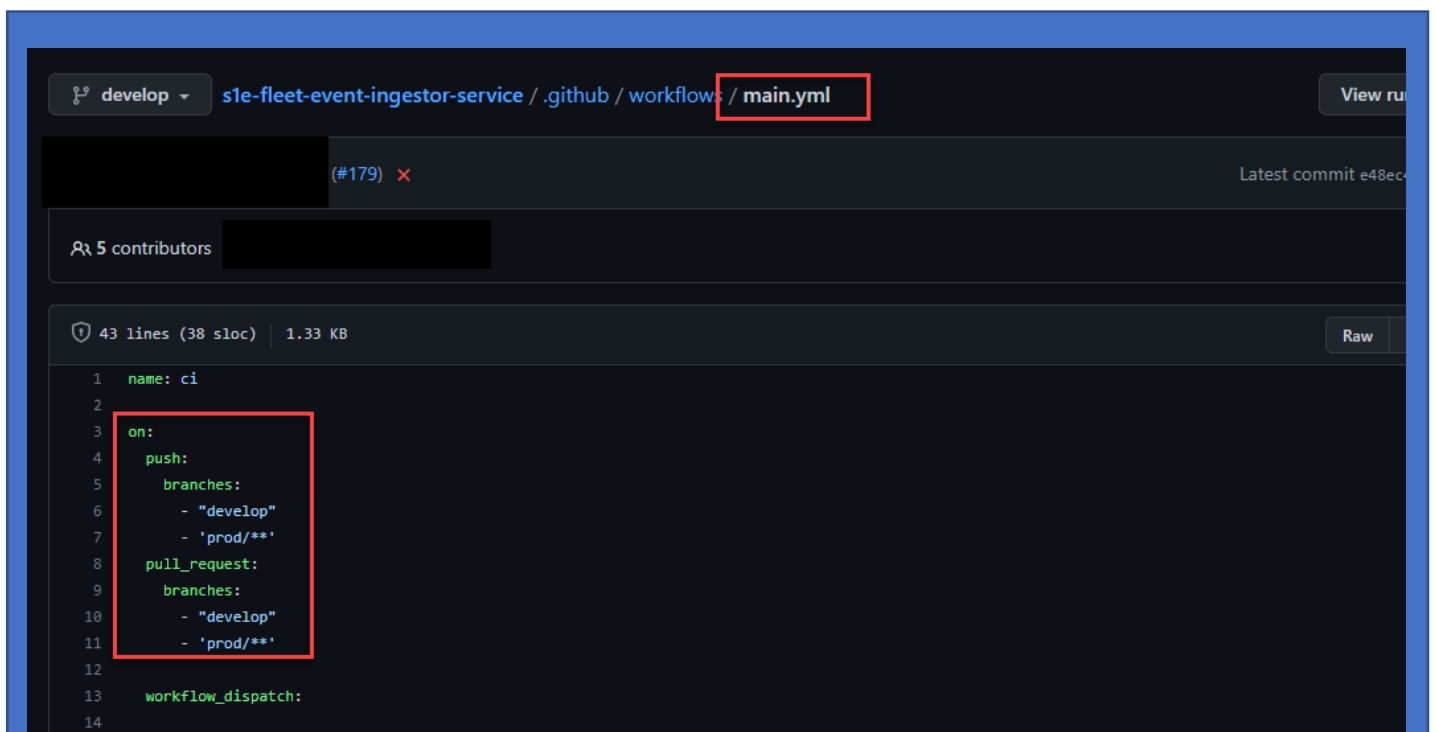
```
scan-mode: INTELLIGENT
```

In the code above, they are using custom logic to select what type of scan mode they want, which is an optional way of doing it.

### 3.3.2 Setting Up The Job

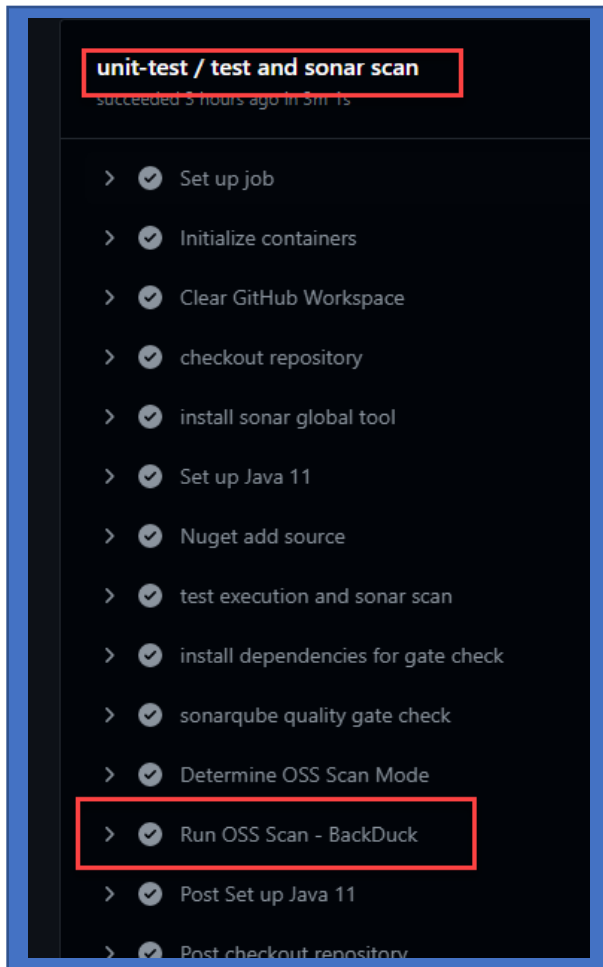
The code from the Workflow above was placed in a file called `dotnet-test-sonar.yaml`

In the screenshot below, the job is configured in such a way (our best practice approach), where if a push or pull request happens, it will trigger the action on `dotnet-test-sonar.yaml` which has our code, as shown in the previous step.



### 3.3.3 Confirming the Action

After the job completes, you can see that the BlackDuck step has been completed successfully.



### 3.3 Azure Devops

The Synopsys Detect for Azure DevOps plugin is architected to seamlessly integrate Synopsys Detect with Azure DevOps build and release pipelines. Synopsys Detect makes it easier to set up and scan code bases using a variety of languages and package managers.

The Synopsys Detect plugin for Azure DevOps supports native scanning in your Azure DevOps environment to run Software Composition Analysis (SCA) on your code.

As a Synopsys and Azure DevOps user, Synopsys Detect Extension for Azure DevOps enables you to:

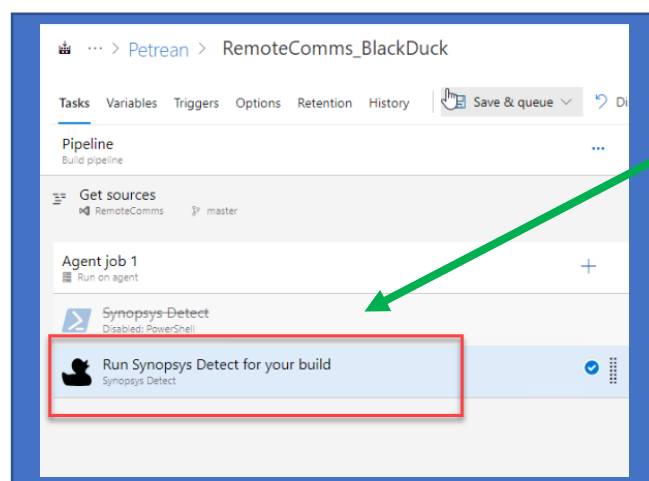
Run a component scan in an Azure DevOps job and create projects and releases in Black Duck through the Azure DevOps job.

After a scan is complete, the results are available on the Black Duck server (for SCA).

Using the Synopsys Detect Extension for Azure DevOps together with Black Duck enables you to use Azure DevOps to automatically create Black Duck projects from your Azure DevOps projects.

#### 3.3.1 Using the Plugin

The easiest way to integrate Azure with Blackduck is to use our plugin, which can be found on the marketplace. You can get the Synopsys Detect for Azure DevOps plugin at VisualStudio Marketplace: <https://marketplace.visualstudio.com/items?itemName=synopsys-detect.synopsys-detect>



In your Pipeline, add the “Run Synopsys Detect for your build” and select it.

### 3.3.2 Configuring the Plugin

On the right side of the screen, after selecting the plugin from the Pipeline Page, you will need to configure what is boxed in below:

Synopsys Detect ⓘ

Link settings View YAML Remove

Version 7.\* ▾

Display name \*

Run Synopsys Detect for your build

Black Duck Service Endpoint \* ⓘ | Manage

Synopsys BlackDuck ▾ ↻ + New

Black Duck Proxy Service Endpoint ⓘ | Manage

Detect Run Mode ⓘ

☒ Use Default Script ☐ Use Air Gap

Detect Arguments ⓘ

--detect.project.name=RemoteComms --detect.project.version.name=master --detect.project.group.name='3500' --blackduck.trust.cert=true --blackduck.api.token=\$(BlackDuckKey) --blackduck.url=\$(BlackDuckUrl) --detect.project.user.groups="Bently Nevada - Users"

☒ Add Detect Task Summary ⓘ

Detect Version \* ⓘ

latest

Detect Folder ⓘ

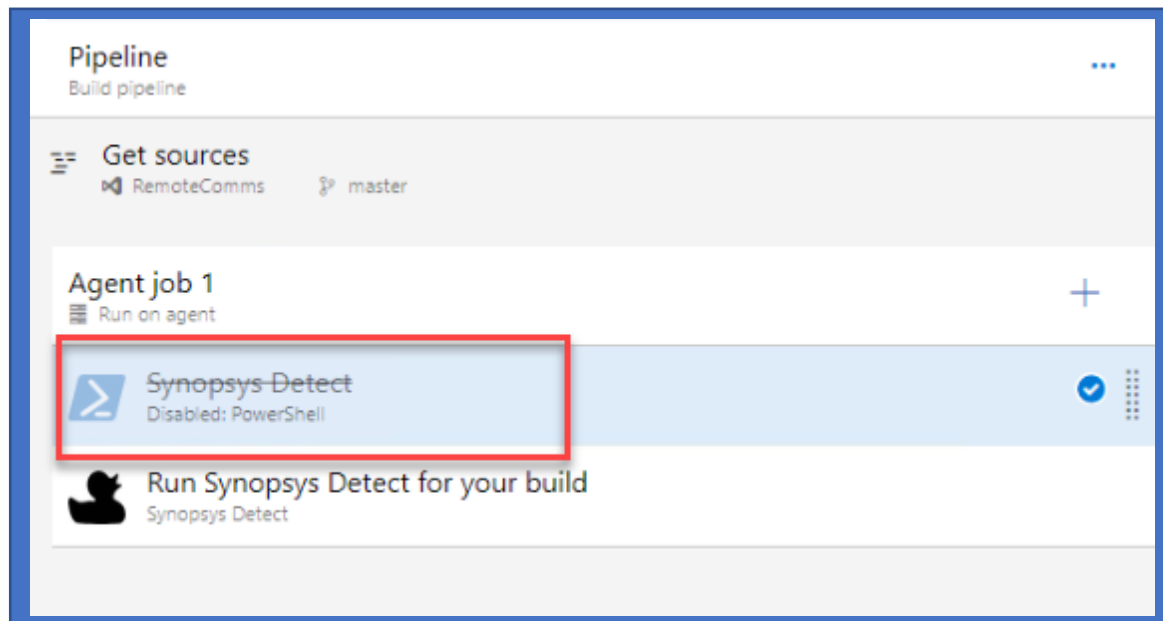
- Display name could be whatever you want.
- Black Duck Service Endpoint requires you to Manage it before adding it
  - Click+ New to add a new Black Duck Service Endpoint and then configure the details.
- Detect Run Mode, keep it in Default, which allows you to connect to the Knowledge Base
- Detect Arguments are the properties we spoke about earlier, but in the example above.
  - Notice that you can use variables, which is best practice.
- Detect Version, whatever your team wants to give it.



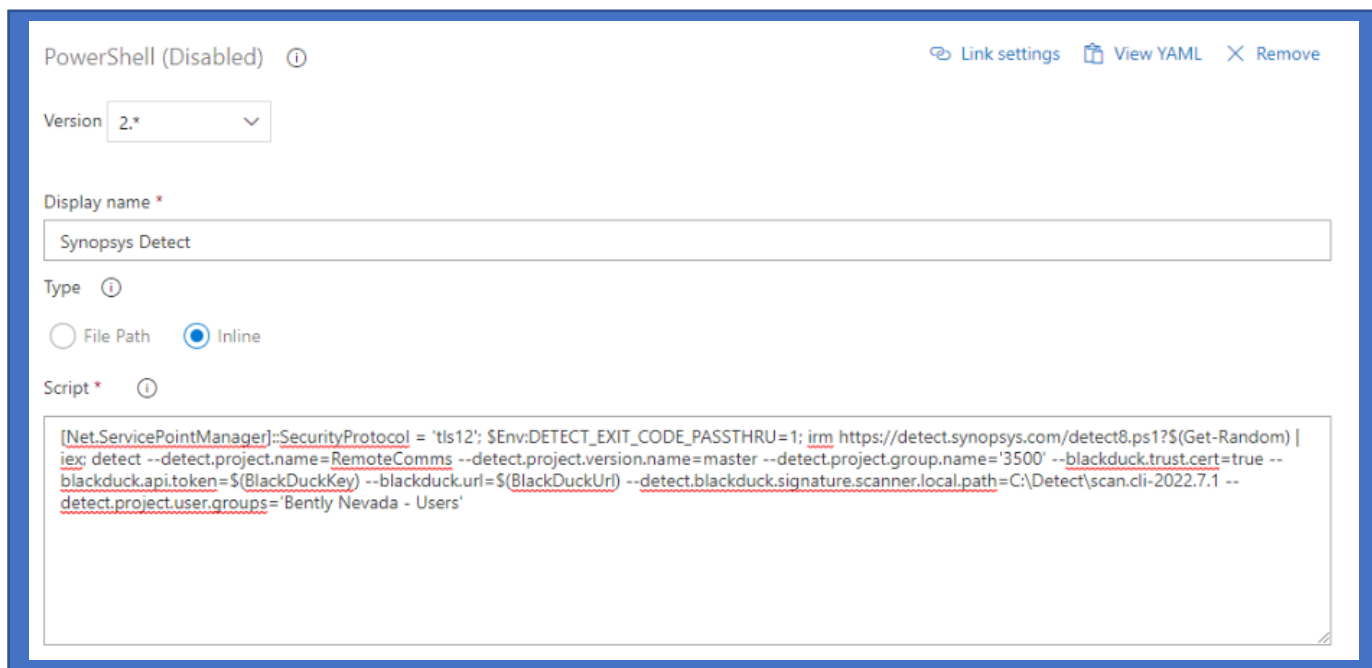
### 3.3.3 Using Powershell

If the plugin won't be utilized, you can run Azure Devops using Powershell:

Add a Powershell step to your Pipeline:



On the right side, you will add the powershell command:



Give the Display Name (required field): Synopsys Detect

For the actual script, use the following:

```
[Net.ServicePointManager]::SecurityProtocol = 'tls12';  
$Env:DETECT_EXIT_CODE_PASSTHRU=1; irm  
https://detect.synopsys.com/detect8.ps1?$(Get-Random) | iex; detect --  
detect.project.name=RemoteComms --detect.project.version.name=master --  
detect.project.group.name='3500' --blackduck.trust.cert=true --  
blackduck.api.token=$(BlackDuckKey) --blackduck.url=$(BlackDuckUrl) --  
detect.blackduck.signature.scanner.local.path=C:\Detect\scan.cli-2022.7.1
```

The highlighted portion above are the additional properties that one must add to it.

Notice the following on the last line: `--`

```
detect.blackduck.signature.scanner.local.path=C:\Detect\scan.cli-2022.7.1
```

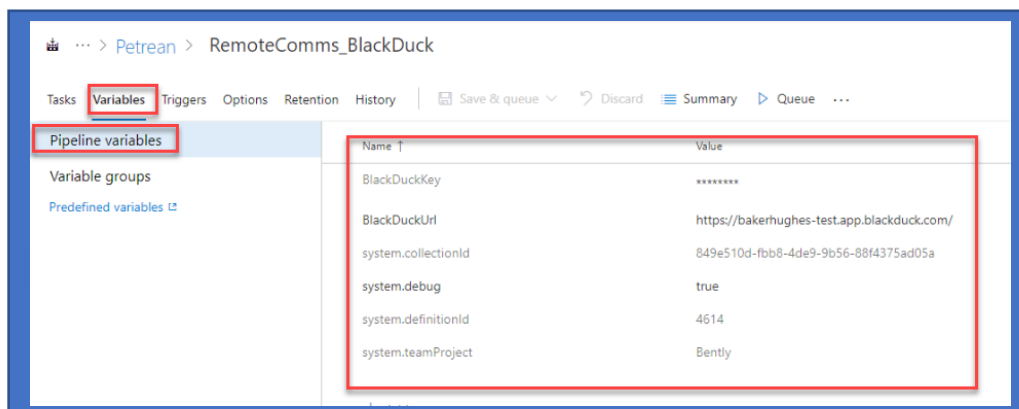
The Signature Scanner was moved from the default download location path to a different path: C:\Detect\

There could be 2 reasons for this, the user manually moved it and if that's the case, that property must be added so the scanner tool knows where it is located. OR the tool itself, for X amount of reasons, could not download it automatically and it had to be downloaded manually. Instructions for that are located in the beginning of this guide. Either way, when the signature scanner is not in the default path, that property must be added.

### 3.3.4 Using Variables

You probably noticed that some of the commands have variables in there:

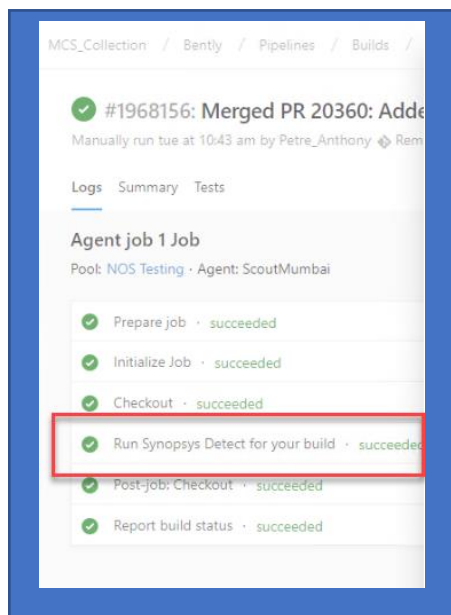
```
--blackduck.url=$(BlackDuckUrl)
```



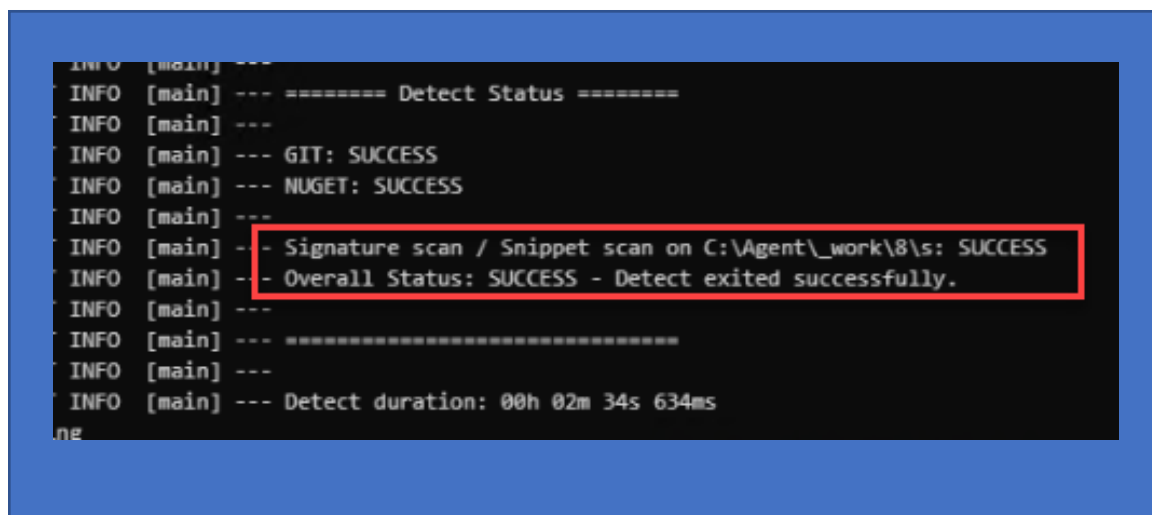
By clicking on Variables and the Pipeline Variables, you'll be able to add variables using the key:value format that will allow you to make use of them across the board. This is another best practice approach.

### 3.3.5 Confirming a Successful Run

Once your job starts, depending on how you named your stage, you can search for the step in the LOGS. The green checkmark confirms you ran a successful build.



In addition, selecting that stage to see the console output can you show the overall success of the run which confirms it was successful with this message



## 4 Viewing Results in Black Duck

Once you finish scanning, you'll want to view your results in the console. This only applies if you scanned with a Full/Intelligent Scan mode, which sends the data to the Black Duck server database. If you scanned with a Rapid scan mode, you will only see results on the console output.

### 4.1 Navigating the UI to your Scanned Project/Version

Every project in Blackduck consists of a Version. There are several ways to find your project/version.

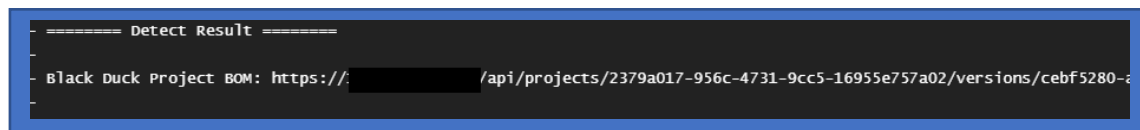
#### 4.1.1 Using a Direct Link to Project/Version

If your project was successful, you will get an URL listing the BOM (Bill of Materials) in your console output.

Example:

```
2022-10-18 16:28:01 EDT INFO [main] --- ===== Detect Result
=====2022-10-18 16:28:01 EDT INFO [main] ---2022-10-18 16:28:01
EDT INFO [main] --- Black Duck Project BOM:
https://XXX.XXX.XXX.XXX/api/projects/2379a017-956c-4731-9cc5-
16955e757a02/versions/cebf5280-a0c8-49ff-ae19-
361d5d6d27d2/components2022-10-18 16:28:01 EDT INFO [main] ---
2022-10-18 16:28:01 EDT INFO [main] --- ===== Detect Status
=====2022-10-18 16:28:01 EDT INFO [main] ---2022-10-18 16:28:01
EDT INFO [main] --- Signature scan / Snippet scan on
C:\Users\Mike\Documents\VM Shared\protex_tutorial: SUCCESS2022-10-
18 16:28:01 EDT INFO [main] --- Overall Status: SUCCESS - Detect
exited successfully.202
```

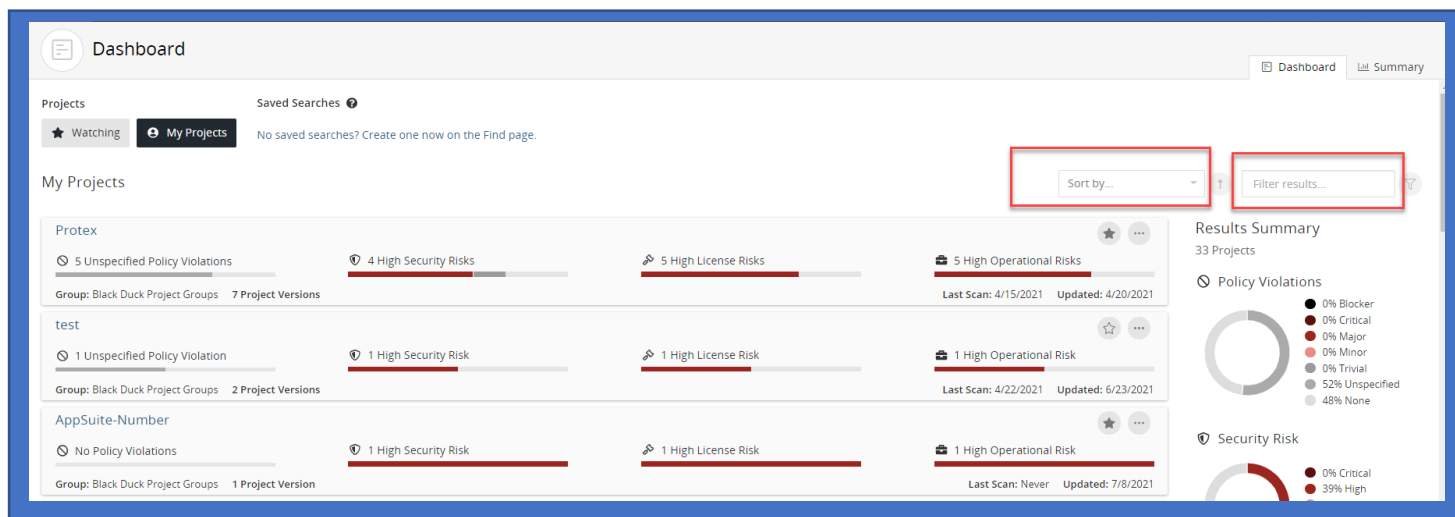
I highlighted the portion above, but it's laid out easier on the console output:



```
----- Detect Result -----
Black Duck Project BOM: https://. /api/projects/2379a017-956c-4731-9cc5-16955e757a02/versions/cebf5280-a0c8-49ff-ae19-361d5d6d27d2/components
```

### 4.1.2 Using the Black Duck Console

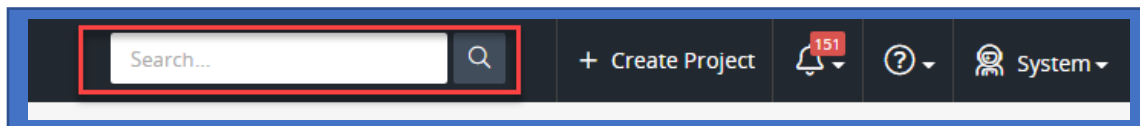
Assuming you have access, you will be able to see all the projects that you scanned (and those from others in your teams via the user groups role) via the Dashboard:



A couple of things to note here:

- This is the default page you land when you access the Black Duck (Dashboard)
- Top right side you can SORT BY with several different values OR you can filter results by typing the NAME of your project in there.
- Lastly, you can simply just scroll down the list until you find it.

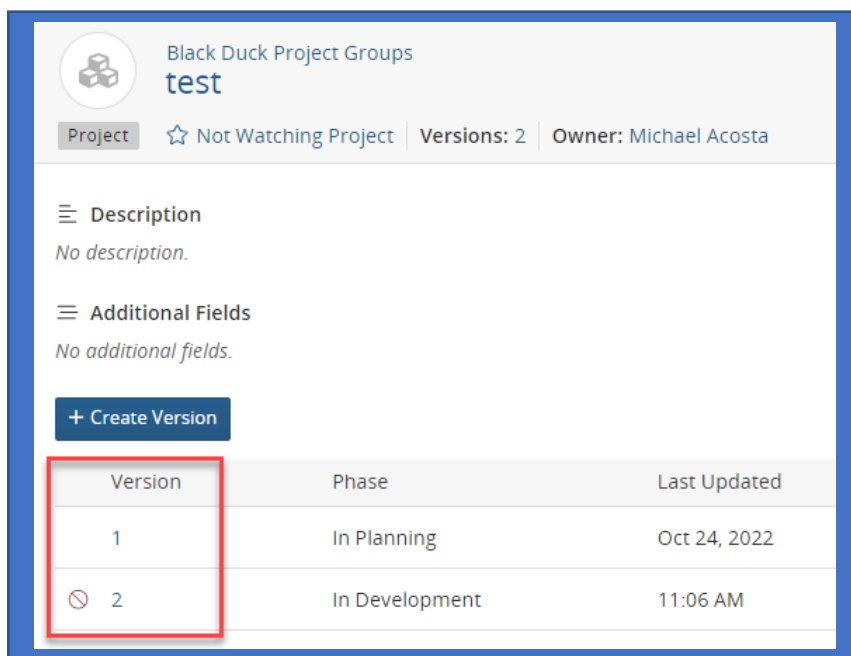
In addition to those methods, you can also use the global search option to find the project:



- This would just be an extra step because it would take you an another page, but nevertheless, the ability to search for your project can be found there and will be useful if you're not in the Dashboard page.

Once you find the project, click on the name of it and it will show you a list of the versions associated to it:

## CONT'D Using the Black Duck Console



As stated above, clicking the project (once you find it) will bring up this screen that lists all the versions associated to the project. By default, you will have a limited of 10 versions per project, but in the event you need more than 10, you can reach out to [OSSAdmin@bakerhughes.com](mailto:OSSAdmin@bakerhughes.com) with your use case and they can open a support ticket on your behalf for more versions.

Once you find the version, you will **simply click on it** and that will take you to the BOM (Bill of Materials).

**NOTE:** Notice in the screenshot above that there is a little red circle next to Version 2. This means that a global policy was violated in this scan.

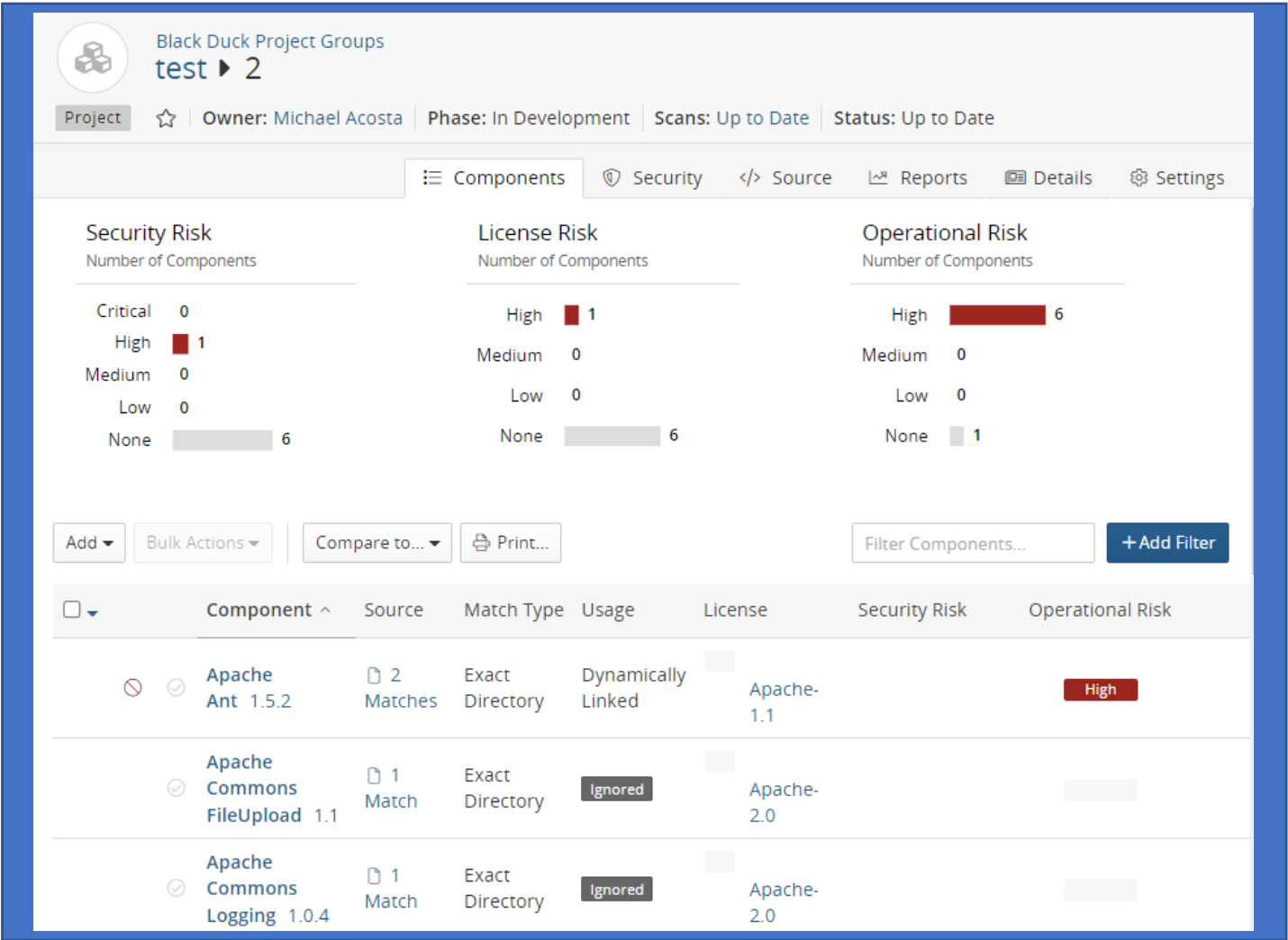
### 4.2 Understanding your Results (BOM – Bill of Materials)

The Bill of Materials is the results of the scan. Anything that was matched against our Knowledgebase will appear here categorized by risks with different categories such as (none, low, level, medium, high, critical).

By default, you will be dropped on the Components Tab that details everything.

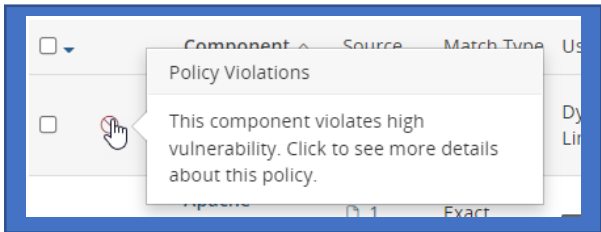
See next page for example:

CONT'D Understanding your Results (BOM – Bill of Materials)



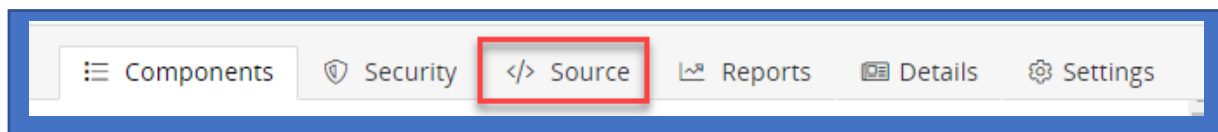
This will list the Security Risk, License Risk, and Operational Risk for each.

In this example, you can see which policies were violated by looking at the little red circle on the left side of the component name. If you hover your mouse over it, you will see which Policy was triggered:



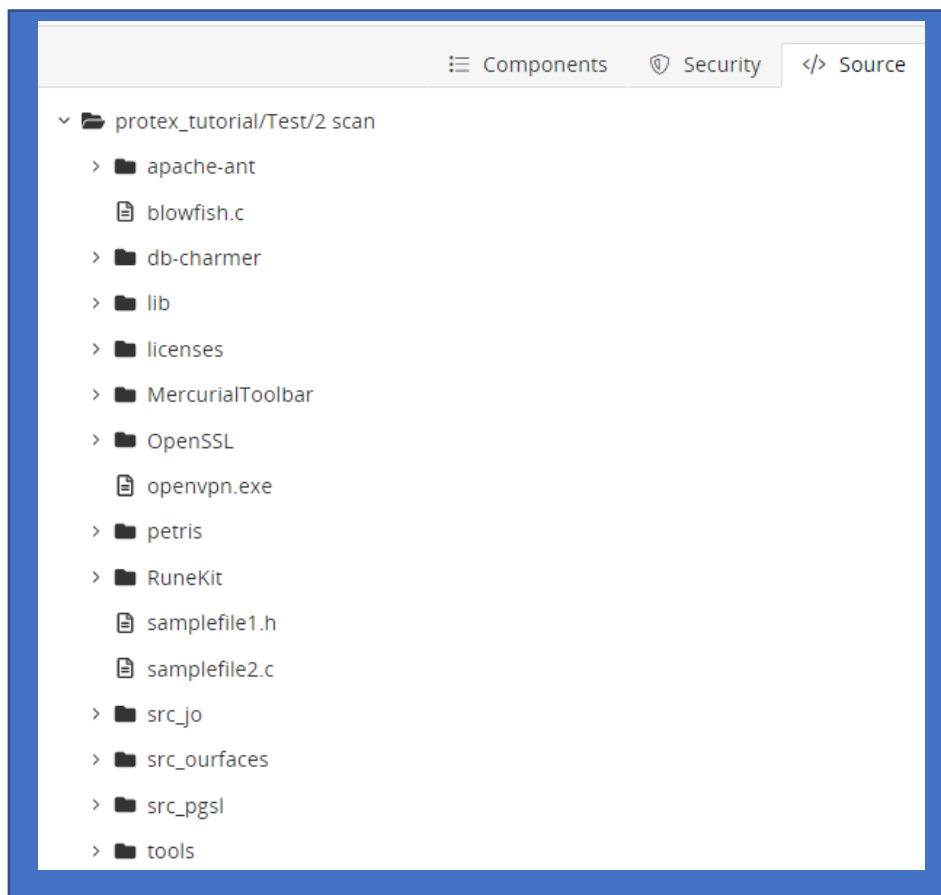
In this case, there was a policy that will be triggered if it finds ANY component with a high vulnerability.

For Policy Violations, you will have to follow internal procedures into remediating them. Reach out to [OSSAdmin@bakerhughes.com](mailto:OSSAdmin@bakerhughes.com) for any questions regarding them.



The tabs on the top right give you additional information about your scan.

The **SOURCE** tab will allow you to view your results in a tree-like structure:



The **SECURITY** tab will allow you to view your vulnerabilities while the **REPORTS** tab will allow you to generate specific reports to your version.



## 5 Additional Resources

The following information will help you through the scanning process.

### 5.1. Troubleshooting

Any questions, any scanning errors, anything that you feel should work or isn't working you should be addressed to: [OSSAdmin@bakerhughes.com](mailto:OSSAdmin@bakerhughes.com)

Please include the console output in the event it was a scanning error and provide screenshots with detailed explanations of the issue

### 5.2. External Links

The following external links provides additional more in-depth information that was covered in here. Reach out to these guides if you want additional information on what was mentioned.

- Black Duck Detect Getting Started Buck
  - [https://github.com/blackducksoftware/hub/blob/master/docs/en\\_US/getting\\_started.pdf](https://github.com/blackducksoftware/hub/blob/master/docs/en_US/getting_started.pdf)
- Black Duck for Jenkins
  - <https://synopsys.atlassian.net/wiki/spaces/INTDOCS/pages/71106939/Synopsys+Detect+for+Jenkins>
- Black Duck for GitHub Actions
  - <https://synopsys.atlassian.net/wiki/spaces/PARTNERS/pages/151093290/Synopsys+Detect+GitHub+Action>
- Black Duck for GitHub Actions
  - <https://synopsys.atlassian.net/wiki/spaces/INTDOCS/pages/622618/Synopsys+Detect+for+Azure+DevOps>
- Black Duck Detect Scanning Tool
  - <https://community.synopsys.com/s/document-item?bundleId=integrations-detect&topicId=introduction.html& LANG=enus>