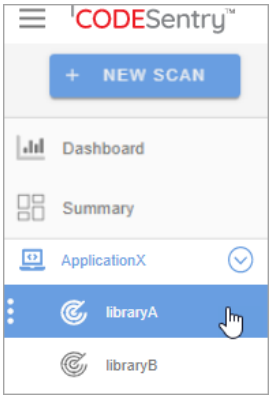
Summary Page

This page provides an overview of the results available on the CodeSentry instance, and provides links to full details for each scan.

The Summary page is displayed when you first open the CodeSentry user interface. You can also navigate to the Summary page at any time by selecting **Summary** at the top of the menu panel.



Page Contents

- There are two badges at the top of the page.
  - *Applications*: the total number of applications on the CodeSentry instance.
  - *Scans*: the total number of scans across all projects.
- There are three tabs. **Scans**, **Components**, and **Vulnerabilities**.
  - The main content of the **Scans** tab is a table of scans on your instance.
    - There is a search box with 4 filter options (**All**, **Application**, **Scan**, and **Artifact**) and a search term field.
      - **All** : retrieve all applications, scans, and artifacts that match the search term.
      - **Application** : retrieve all applications that match the search term.
      - **Scan** : retrieve all scans that match the search term.
      - **Artifact** : retrieve all artifacts that match the search term.
  - The **Components** tab is a table of components on your instance.

- There are three search fields on the **Components** tab. Search fields use exact matching on search terms, are case insensitive, and you can use '%' to match wildcard characters.
  - **Search component name** : search for a specific component by name, across all scans on the instance.
  - **Search component version** : search for a specific component version, across all scans on the instance.
  - **Search component vendor** : search for a specific vendor across all scans on the instance.

- The **Vulnerabilities** tab is a **table of vulnerabilities** on your instance.
  - There is a date selector, which allows you to search for new or updated vulnerabilities since a specific date.
  - There is a search box, via which you may search for a vulnerability by its `CVE ID` or `Vulnerability ID` .
  - There are optional filters:
    - **Filter by severity**
    - **Filter by remediation**
    - **Filter by location**

Scans Tab

The table contains one row for every scan on the CodeSentry instance, including scans that are still in progress and scans that failed.

Click on any row to navigate to the corresponding Scan Results page.

Click a column header to sort the table by that column; click again to reverse the sort order. When the table is sorted an up arrow ("ascending") or down arrow ("descending") is displayed to the right of the corresponding column header. Sorting is chronological for the **Scan Created** column and lexicographic for the **Scan Name** and **Application Name** columns.

The table has the following columns.

- **Scan Name**.
- **Application Name**. The application to which the scan belongs.
- **Artifact Name**. The basename of the artifact that was uploaded and scanned for the scan. The table cannot be sorted by this column.
- **Scan Created**. The UTC timestamp at which the CodeSentry instance received the new scan command.

Components Tab

The **Components** table contains one row for every application and scan on the CodeSentry instance, including scans that are still in progress and scans that failed. Search the inventory of scans performed by CodeSentry to determine if any of the scanned artifacts contain a specific component. This page displays results in alphabetical order, sorted by component name.

Search by component *name*, *version*, or *vendor*. Filter the table by *Pass/Fail* status or *license risk*.

Note that as you apply filters and searches on the **Components** tab, the query parameters in the URL update, making it possible to share links to specific views.

The table has the following columns.

- **Pass/Fail**
- **Application/Scan** name
- **Component Name**
- **Component Version**
- **Component Vendor**
- **Target Path**
- **License**
- The **Link to Scan** icon. Click to navigate to the corresponding Scan Results page.

The **Pass/Fail**, **Application/Scan**, **License** and **Component Name** columns are sortable. Click a column header to sort the table by that column; click again to reverse the sort order. When the table is sorted, an up arrow ("ascending") or down arrow ("descending") is displayed to the right of the corresponding column header.

Vulnerabilities Tab

The **Vulnerabilities** table contains one row for every vulnerability on the CodeSentry instance. Search the inventory of scans performed by CodeSentry to determine if any of the scanned artifacts contain a specific vulnerability.

This page displays results, sorted by Severity from highest to lowest.

The table has the following columns.

- Severity
- Vulnerability ID
- **Vulnerability Title**
- **Component Name**
- **Component Version** - Note that versions are sorted alphanumerically as strings.
- **Match**
- CVE ID(s)
- **Updated At** - The time in UTC of the most recent vulnerability database update.
- **Target Path**
- Status
- The **Link to Scan** icon. Click to navigate to the corresponding Scan Results page.
- Annotate

All columns except for **CVE ID(s)**, **Status**, **Link to Scan**, and **Annotate** are sortable. Click a column header to sort the table by that column; click again to reverse the sort order. When the table is sorted, an up arrow ("ascending") or down arrow ("descending") is displayed to the right of the corresponding column header. Note that versions are sorted alphanumerically as strings.

Use the date selector to check for new or updated vulnerabilities since a specific date. This feature can help identify whether specific vulnerability data has changed since the date specified via the date selector.

Select a date and one or more of the following options:

- **Updated Vulnerability** - select to find any new vulnerability information for any scans on the instance, since the selected date.
- **Updated Remediation** - select to find any new *remediation* information for any scans on the instance, since the selected date.
- **Updated Exploit** - select to find any new *exploit* information for any scans on the instance, since the selected date.
- **New Vulnerability** - select to find any newly-reported vulnerabilities in any scans on the instance, since the selected date.

To deselect the chosen date and any selected options, click the **Clear** button.

Example use cases

- You may choose to search your instance upon hearing about a new vulnerability. In this case, you would select a recent date on the date selector, and the **New Vulnerability** checkbox. Upon clicking **Apply**, the **Vulnerabilities** tab will refresh and list only newly-found vulnerabilities, if any are present on your instance.
- A second use case might be periodic checks on whether a remediation has been found for a specific vulnerability you know exists in your instance. Select the date of the last time you checked for updates, and select **Updated Remediation** to check for potential updates that would then allow your team to utilize the new remediation for the known vulnerability.
- A third use case might be periodic checks on whether any vulnerability information has changed on your instance. Select the date of the last time you checked for updates, or if doing this for the first time, a reasonable date such as the date of the most recent scan on the instance, and select all 4 checkboxes. This provides a quick way to view any new vulnerability data since your last scan.

Note: For internet-connected On-Premise installations, you must configure your system to receive updates and synchronize with the database.

Footer

The page footer indicates the CodeSentry *Edition* enabled on your instance.

Edit, Modify, or Annotate CodeSentry Findings

You can modify CodeSentry findings in a variety of ways.

- You can modify a **bill of materials**: *exclude* components, *include* components (for example, to include formerly excluded components), and add notes to individual components.
- You can annotate **licenses** as **Approved**, **Not Approved**, or **In Review** (note that **In Review** is the default state) and **bulk annotate** licenses.
- You can **add components** to the Bill of Materials.
- You can annotate **N-Day Finding information**: change the originally reported **CVSS Score**, assign a **Status** (*Under Investigation*, *Affected*, *Not Affected*, *Fixed*), and add comments.

  Note that updates to the Bill of Materials and N-Day Findings sync every 60 seconds. If another user modifies the Bill of Materials or N-Day Findings, it may take up until one minute to see the updated data.

Annotate Bill of Materials

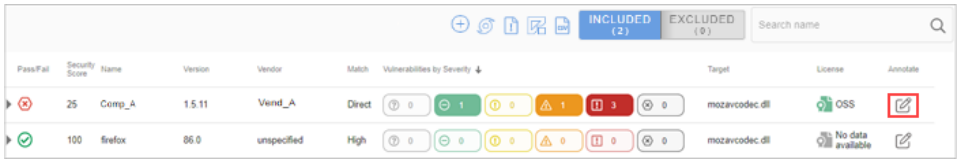
The following sections illustrate how a user might leverage *Component Annotation* functionality.

- Identify a potential false positive result.
- Exclude this result from the Bill of Materials and note why the finding is being excluded.
- Re-include the result after determining that is a valid finding.
- Generate a Scan Report that includes the annotation for this component.

See the **API Guide** for instructions on performing these operations via the API.

Exclude a Component

1. Identify a finding, `Comp_A` in this example, suspected of being a false positive.
2. Click the **Annotate** button in the `Comp_A` row to open the **Annotate Component** window.



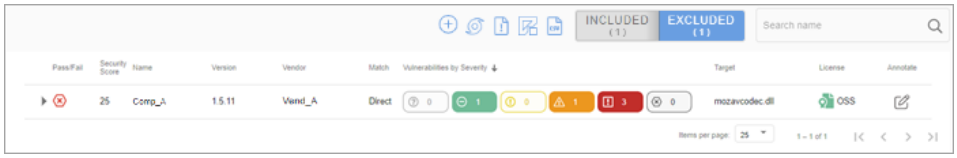
3. Set the **State** to **Exclude** and add a comment explaining the reason for excluding the component.

4. Click **Update** to apply the annotation.

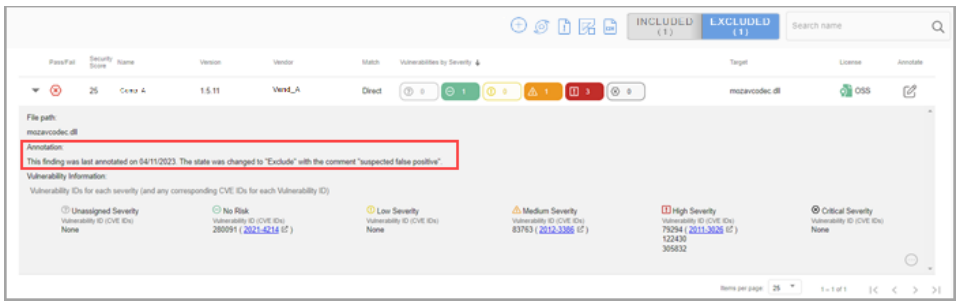
5. Note that the Bill of Materials tab default view of **Included Components** no longer shows `Comp_A` .

Include a Component

1. Click the **Excluded Components** button. `Comp_A` is listed here.

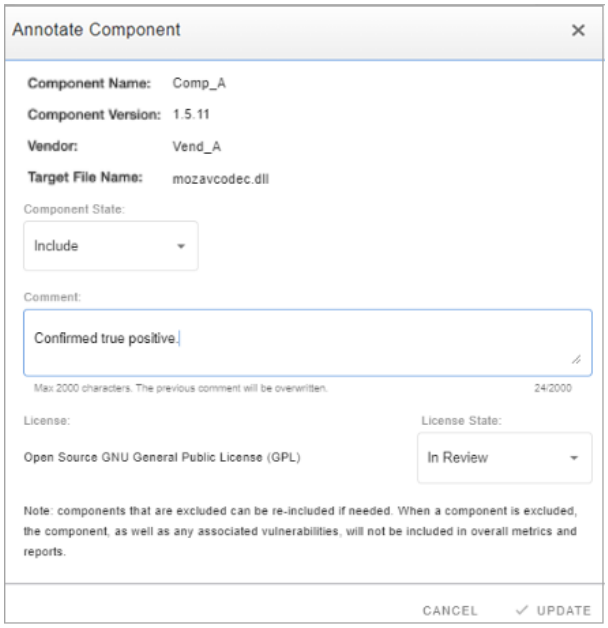


2. Expand the `Comp_A` row, and note that the annotation information is displayed.



3. Click the **Annotate** button in the `Comp_A` row of the Bill of Materials to open the **Annotate Component** window.

4. Set the **State** to **Include**, and update the **Comment** to describe the result of investigation.



5. Click **Update** to apply the annotation.

6. Note that the **Excluded Components** page shows no results.

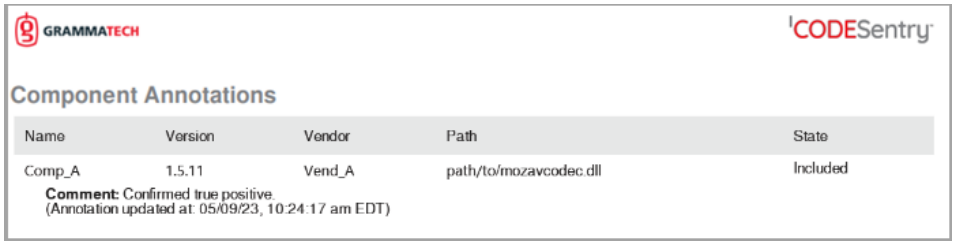
7. Click **Included Components** to see `Comp_A` restored to the Bill of Materials.

Include Annotations in a Scan Report

1. Click the **Scan Report** tab.

2. Select the **Component Annotations** checkbox, then click **Download Report**.

3. Open the newly-generated Scan Report, and scroll to the **Component Annotations** section. `Comp_A` is displayed, along with the contents of the latest comment.


GRAMMATECH
CODESentry

Component Annotations

Name	Version	Vendor	Path	State
Comp_A	1.5.11	Vend_A	path/to/mozavcodec.dll	Included

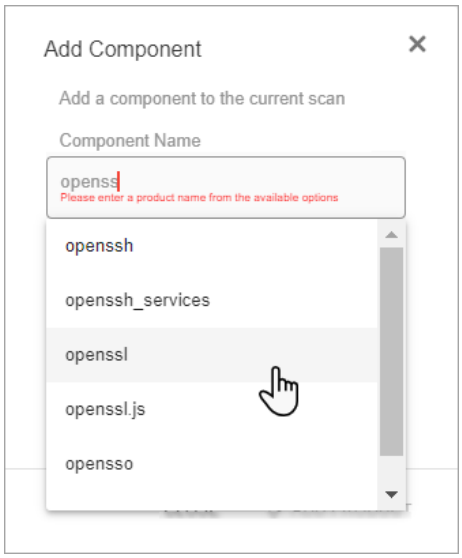
Comment: Confirmed true positive.
(Annotation updated at: 05/09/23, 10:24:17 am EDT)

Add Component

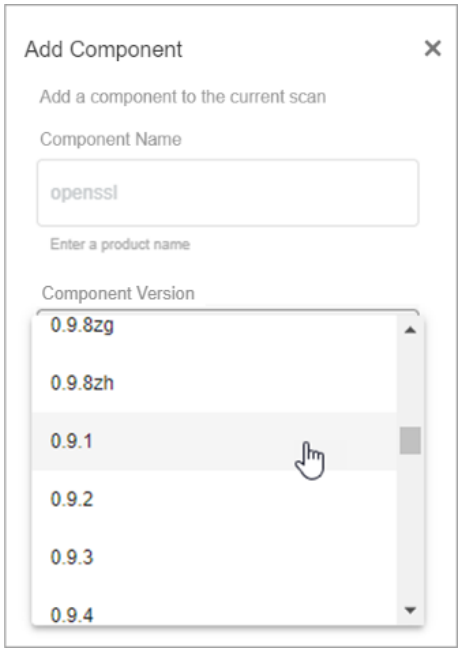
Directly Add a Component

The procedure for directly adding a component to a specific scan is as follows.

1. Navigate to the Scan Results page for the scan.
2. Click the blue + icon to open the Add Component dialog.
3. Enter the component name in the **Component Name** field. A drop down menu will list the available completion options for the current field contents.

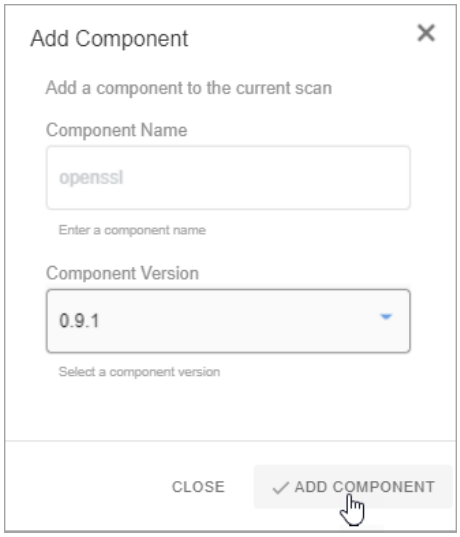


4. Select the component version from the **Component Version** drop down menu. The listed version numbers correspond to available database entries for your selected **Component Name**.

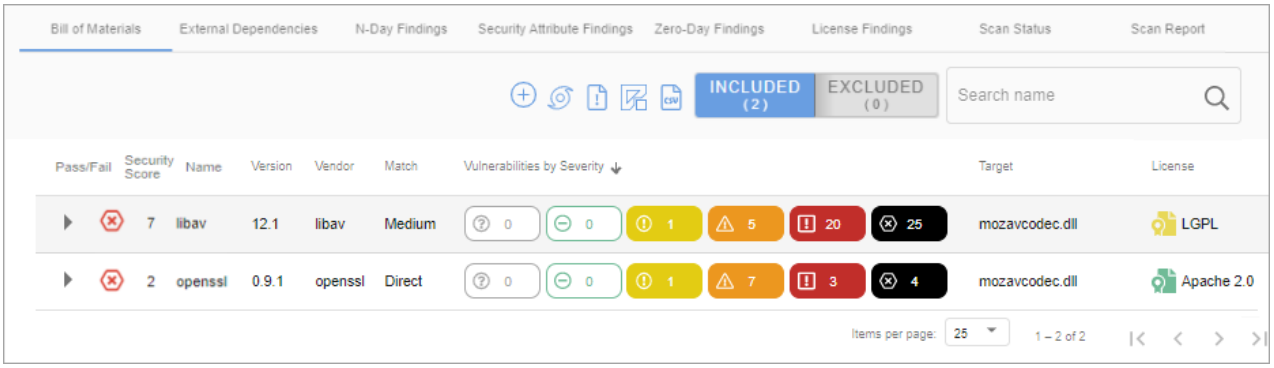


The **Component Version** field is not active until a **Component Name** has been selected.

5. Click **Add Component**.



The Scan Results page will refresh to show the **Bill of Materials tab** with the newly added component included in the table of components.



- In some cases there are multiple vendors of components with the same name and version. When this occurs, information about *all* matching components is added to the results stored for the scan and you will see multiple new rows in the **Bill of Materials table**.
- The **Match Level** for directly added components is always **Direct**.
- If the table of components is large and has been paginated, the new rows may not be displayed on the first page. You can change to a later page or search to see the new rows. You can also sort in decreasing order by *Match Level*, so that all directly-added components are displayed at the top of the table.

Viewing Information for Directly Added Components

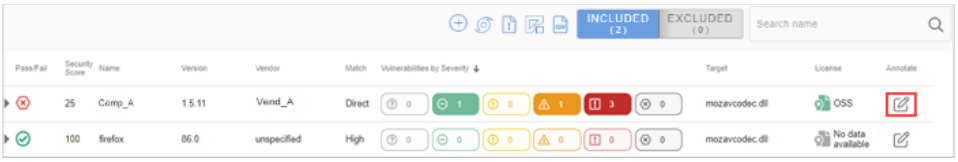
- **Bill of Materials tab**: One row for each directly added component in the **BoM table**.
- **N-Day Findings tab** One row for each **vulnerability** directly associated with each directly added component.
- **Scan Status tab** Component lookup jobs are not shown in the Scan Status tab.
- Downloaded files
  - Bill of Materials (CSV): One row for each **vulnerability** directly associated with each directly added component.
  - **Scan Report**: Each directly added component, and each vulnerability associated with a directly added component, is included in the counts in the **N-Day Vulnerabilities** section of the **Executive Summary**. There is a row for each directly added component in the Bill of Materials. There is an entry for each directly added component in the **N-Day Findings** section, organized under the **artifact** with which the corresponding lookup job was associated. The **N-Day finding details** and **Zero-Day finding details** sections include an entry for every **vulnerability** associated with a directly added component.
- **API**
  - When there are directly added components, their information is included in results for queries about components and their N-Day vulnerabilities. Vendor information is provided in the `vendor` column.

Annotate License Information

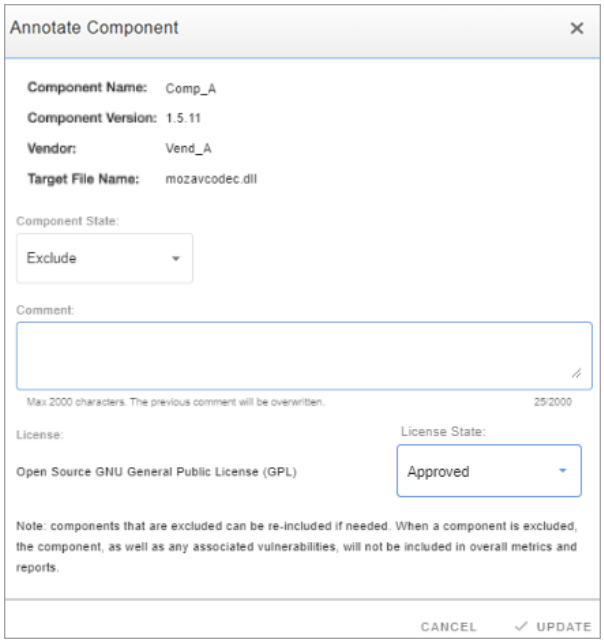
Use the **Annotate Component** feature, accessible on both the **Bill of Materials tab** and the **License Findings tab**, to define if the license or licenses belonging to a component or set of components are *In Review*, *Approved*, or *Not Approved*.

Annotate a Component's License

1. Identify a finding, `Comp_A` in this example, with an associated *License Type* that is approved by your organization.
2. Click the **Annotate** button in the `Comp_A` row to open the **Annotate Component** window.



3. Set the **License State** to **Approved**.



4. Click **Update** to apply the updated **License State**.

5. Note that the license icon in the Bill of Materials tab changed from **In Review**  to **Approved**  .

Bulk Annotate

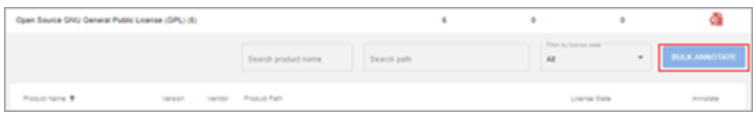
1. Navigate to the License Findings tab.

2. Expand one of the **License Name** rows. *Open Source GNU General Public License (GPL)* is used for this example.

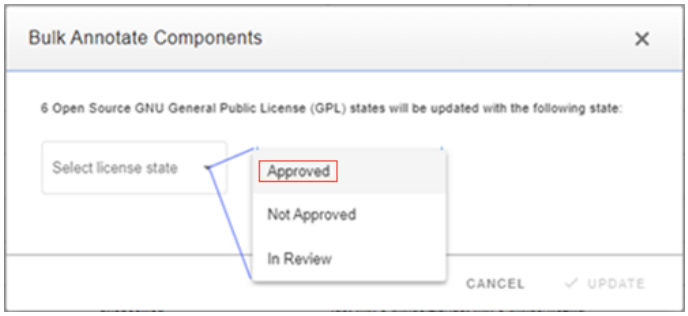
3. Set the **Filter by license state** dropdown to **In Review**. This will update the table to list all components with *Open Source GNU General Public License (GPL)* licenses that have not yet been reviewed.

   Note that bulk annotation applies to the currently-filtered list. For example, you can filter by a specific **Path**, and then apply a state such as **Approved** to all licenses belonging to components on the filtered **Path**.

4. Click the **Bulk Annotate** button.



   The **Bulk Annotate Components** dialog will open.



5. Select **Approved** in the dropdown list.
6. Click **Update**.

   The **Bulk Annotation Complete** dialog will open, confirming the details of the licenses just updated.
7. Click **Close** to dismiss the **Bulk Annotation Complete** dialog.

Annotate N-Day Finding Information

- Annotate one finding:
  - Identify a vulnerability that should have a **Status** other than its default status of **Under Investigation**.
  - Change the vulnerability **Status** to **Affected** and add a comment to explain the reason the vulnerability that was **Under Investigation** is now **Affected**.
  - Change the **Score** from its default value and add a comment to explain the score change.
- Modify an annotation.
- Delete comments and reset the **Status** and **Score** to their default values.
- Annotate a set of findings:
  - Identify a set of vulnerabilities that should all have their **Status** and or **Score** changed to the same values.
  - Change the **Status** and **Score** for the entire selection of vulnerabilities.
- Modify comments from multiple previously annotated vulnerabilities.
- Delete comments from multiple previously annotated vulnerabilities.
- Delete all annotations (restore all **Status** and **Score** values to their originally discovered values, and remove related comments).

See the API Guide for instructions on performing these operations via the API.

Annotate One Finding

1. On the N-Day Findings tab, click to select a finding in the **Annotate** column.
2. Click the 3 dots in the column header, then click **Annotate (1 Finding)** to open the **Annotate Vulnerability** dialog.

- Get Zero-Day CWE Weaknesses

Get N-Day Analysis Results

A GraphQL query for obtaining N-Day analysis results associated with the canonical path stored in `RESULTS_PATH` path is shown below.

```graphql
query {
  visible_components(
            where: {
              job: {
                org_node: {
                  path: {
                    _like: \\\"${RESULTS_PATH}/%\\\"
                    }
                  }
                }
              },
            limit: 20
            offset: 0
            order_by: [
              { confidence: asc }
              { component_name: asc }
              { analysis_worker: asc }
              { id: asc }
            ]
            ) {
  component_name
  vendor
  version
  confidence
  }
}
```

The `visible_components` query retrieves a list, so we must specify a `limit` (coordinated with `offset` and `order_by`) in order to avoid database timeouts on large queries. A future version of CodeSentry will add explicit enforcement for this requirement.

You can specify any sequence of `order_by` terms for visible_components, sorting `asc` or `desc` by any of the following: `id`, `component_name` and `version`, `created_at`, `updated_at`.

1. Set up a GraphQL query to retrieve information about the first 20 detected components (with respect to the specified ordering).

```bash
GQL="query { visible_components(where: \
              { job: { org_node: { path: { _like: \\\"${RESULTS_PATH}/%\\\" } } } }, \
                limit:20,offset:0 \
                order_by:[{component_name:asc},{version:asc},{id:asc}]) \
      { component_name, vendor, version, confidence }}"
```

   - If there are fewer than 20 detected components, all components will be retrieved.

2. Issue the query and direct the output to a file for further investigation.

```bash
curl -X POST -H "Authorization: Bearer ${ACCESS_TOKEN}" \
    -d "{\"query\":\"${GQL}\"}" ${URL}/api/results/v1/graphql \
    -o component_results.json
```

3. Use `jq` to pretty-print the output.

```bash
jq <component_results.json
```

You should see a pretty-printed rendering of the scan results in JSON format.

- You may like to compare this information to that available in the various tabs of the Scan Results page for the same scan.

How Many Components Were Found?

It can be useful to know how many components were found before starting to retrieve the results. For example, you can use this total to parameterize a retrieval loop, or to present as summary information while full details are collected.

```graphql
query {
  metrics(id: "${SCAN}") {
    results {
      components_found
    }
  }
}
```

1. Set up a GraphQL query to retrieve the number of components detected.

```bash
GQL="query { metrics(id: \\\"${SCAN}\\\") {  results { components_found } } }"
```

2. Issue the query and extract the resulting count to store in variable `COMPONENT_COUNT`.

```bash
COMPONENT_COUNT=$(curl -X POST \
  -H "Authorization: Bearer ${ACCESS_TOKEN}" \
  -d "{\"query\":\"${GQL}\"}" ${URL}/api/results/v1/graphql \
  | jq -r .data.metrics.results.components_found)
```

3. Check the value of `COMPONENT_COUNT`

```bash
echo $COMPONENT_COUNT
```

Which N-Day Findings Are Highest Priority?

It can be useful to query the 20 top vulnerabilities designated as **Findings to Fix**. These are findings with a **Public** or **Undisclosed** *Exploit*, a **Remote / Network Access** or **Location Unknown** *Location*, and a known *Remediation*.

```graphql
query {
  nDayExploitsToFix: instance_nday_exploits(
    limit: 20,
    where: {
      solution_status: {_eq: true}
    }
  ) {
    component_name
    db_id
    job_id
    path
    severity_label
    solution
    solution_status
    title
    component_version
    component_vendor
  }
}
```

1. Set up a GraphQL query to retrieve information about the first 20 vulnerabilities.

```bash
GQL="query {\
nDayExploitsToFix: instance_nday_exploits(\
 limit: 20,\
 where: {\
   solution_status: {_eq: true}\
 }\
) {\
 component_name\
 db_id\
 job_id\
 path\
 severity_label\
 solution\
 solution_status\
 title\
 component_version\
 component_vendor\
```

CodeSentry Release Notes

Current Version

CodeSentry 6.0.2 Release Notes

- **Large Scan Load Performance Improvement**
  - The load time of large scans has been improved.
- **Bug Fix**
  - An issue related to CodeSentry Vulnerability Updater Service has been fixed. A small number of components recently gained a many updated vulnerabilities, which had been causing an internal query to hit a memory limit in the Vulnerability Database.

Previous Versions

CodeSentry 6.0 Release Notes

- **User Interface Changes**
  - The N-Day Findings tab now includes an **Annotate** option which provides functionality for changing vulnerability **Status** and modifying **CVSS Score** values. See Edit or Modify a Bill of Materials for examples of this new functionality. Note that this functionality is also available on the Vulnerabilities tab.
    - If you apply vulnerability annotations, the Bill of Materials tab expanded details view now organizes vulnerabilities by **Status**.
  - Search filters applied on the Summary page are now applied to the URL, making URLs with specific search results easy to share.
  - The N-Day Findings tab now includes a **Match Level** filter.
  - The Components tab now includes **Pass/Fail** status and **License Risk** filters.
  - The **Dashboard** and **Summary** links in the Menu panel are now fixed in place to improve ease of navigation.
  - Widgets on the Dashboard have been updated to be more interactive. Clicking certain elements on the dashboard now open the appropriate view on the Components tab and Vulnerabilities tab.
  - The user interface now displays file size in base-2 format.
  - Several error messages have been made more informative.
  - To improve security:
    - User messaging related to an incorrect username or password no longer specifies which value is incorrect, and has been changed to say that one of the values is incorrect.
    - Idle and max session lifetimes have been reduced to conform to security best practices.

Scope	Port Numbers
On primary node for HTTPS communication	443
Admin UI	8800
Prometheus	30900
Grafana	30902
Alertmanager	30903
Kubernetes API TCP connection *	6443
Weave *	6783
Logs *	10250

* = Optional. Ports required for adding worker nodes.

Existing Kubernetes note

Ensure that your server does not have Kubernetes installed. The following installation procedures include a Kubernetes installation. An existing version could cause compatibility issues.

Install from the Internet

You will receive the following information from GrammaTech:

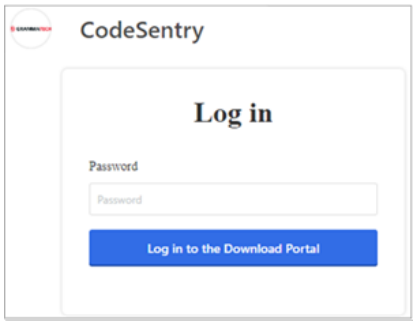
- a URL to a download portal
- a unique password to log into the download portal
- a pre-signed URL to the vulnerability database
- a command to install Replicated Kubernetes, of the form

```
curl -sSL https://kurl.sh/<build_name>
```

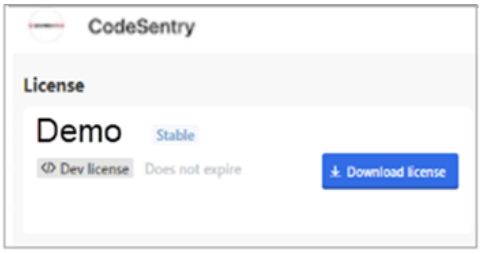
where `<build_name>` is unique to your installation. This will be a name such as `codesentry-man-v5-0-0` or similar.

You will use this command later in the installation process.

1. Navigate to the *Replicated Customer Download portal* URL provided by GrammaTech.



2. Enter the password provided by GrammaTech to log in to the *Replicated Customer Download portal*.



3. Click **Download License** and save the file. You will need to access this file at a later step.

4. Use `ssh` to connect to your instance.

5. Run the Replicated Kubernetes installation command provided by GrammaTech.

```
curl -sSL https://kurl.sh/<build_name> | sudo bash
```

where `<build name>` is the release name provided by GrammaTech.

6. Take note of the terminal output at the end of the installation. Copy the output from the `KOTSADM` entry through the end of the output, and paste this block of text to a file named `install_log.txt`. You will refer to various elements in this file in later steps.

```
Kotsadm: http://172.31.19.139:8800
Login with password (will not be shown again): HjP4uM%sr
This password has been set for you by default. It is recommended that you change this password; this can be done with the following command:
 kubectl kots reset-password default


To access the cluster with kubectl:

    bash -l
Kurl uses /etc/kubernetes/admin.conf, you might want to unset KUBECONFIG to use .kube/config:

    echo unset KUBECONFIG >> ~/.bash_profile


Node join commands expire after 24 hours.

To generate new node join commands, run cat ./tasks.sh | sudo bash -s join_token airgap on this node.

To add worker nodes to this installation, copy and unpack this bundle on your other nodes, and run the following:

    cat ./join.sh | sudo bash -s airgap kubernetes-master-address=172.31.19.139:6443 kubeadm-token=gqkjfq.65nlu994omjgcyxn kubeadm-token-ca-
hash=sha256:060c22da5077dbb2a7cf91ceca3dfca69fba2350e1b58190e5f5e59d0d22c624 kubernetes-version=1.21.14 docker-registry-ip=10.96.3.74 prima
y-host=172.31.19.139
```

7. Verify that Kubernetes is running properly by entering the following commands.

```
bash -l
```

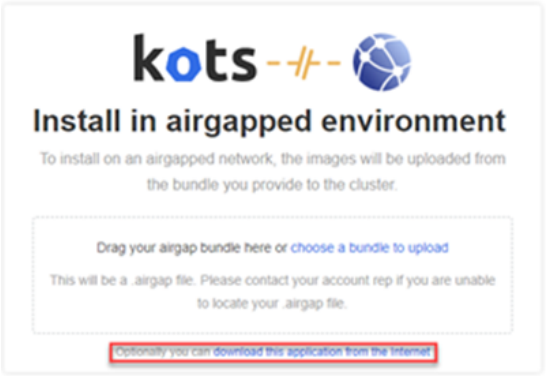
and

```
kubectl get pods -A
```

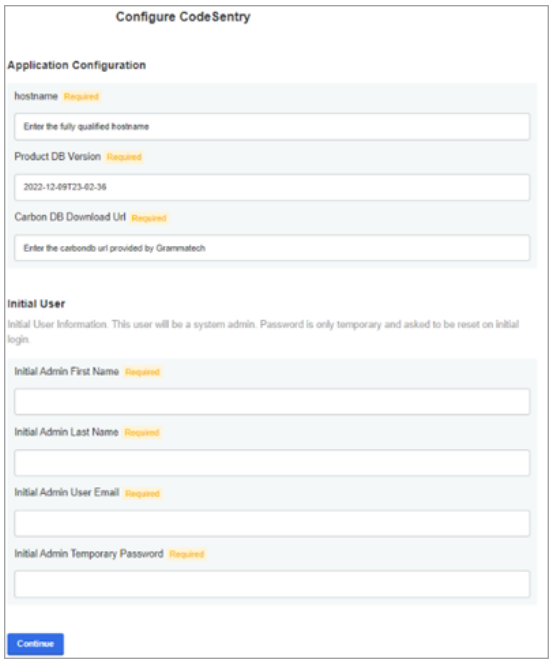
The **STATUS** column should say "Running" for all rows of output in the previous commands.

8. Open `install_log.txt` and navigate to the URL listed here (this was printed at the end of the Kubernetes installation) to access the **Replicated Admin Console**.
9. Click the **Continue to Setup** button.
10. Optional-follow the prompts in the user interface to configure TLS.
11. Optional-click **Skip & continue** to proceed without configuring TLS.
12. Enter the password listed in `install_log.txt` (this was printed at the end of the Kubernetes installation) on the **Log in to CodeSentry** screen.

13. Click **Log in**.
14. Upload your license file.
15. Click **download CodeSentry from the Internet**.



16. Populate the **Configure CodeSentry** screen with information for the initial user, who will also be the administrator.



17. Enter the **hostname**. Note that this value cannot be an IP address, and must be a fully qualified **hostname** that is stable across machine restarts. Note that default EC2 instance hostnames do not meet this criteria.
    - If the FQDN/**hostname** needs to be updated, login into the **Admin Console**, navigate to the **Configuration Options** screen, update the **hostname** field, and redeploy the application.
18. Leave the **Product DB Version** as default. This may change in a future release.
19. Enter the vulnerability database pre-signed URL in the **Carbon DB Data Directory** field. Note that you should wrap this URL in quotes.
20. Enter the Admin user's first name, last name, and email address.
21. Enter a temporary password for the Admin user. You will be prompted to change this password upon signing in to CodeSentry. Note the password must meet the CodeSentry password policy.
22. Click **Continue**. You should see the **Preflight checks** page while the preflight checks are running.