FOSSID

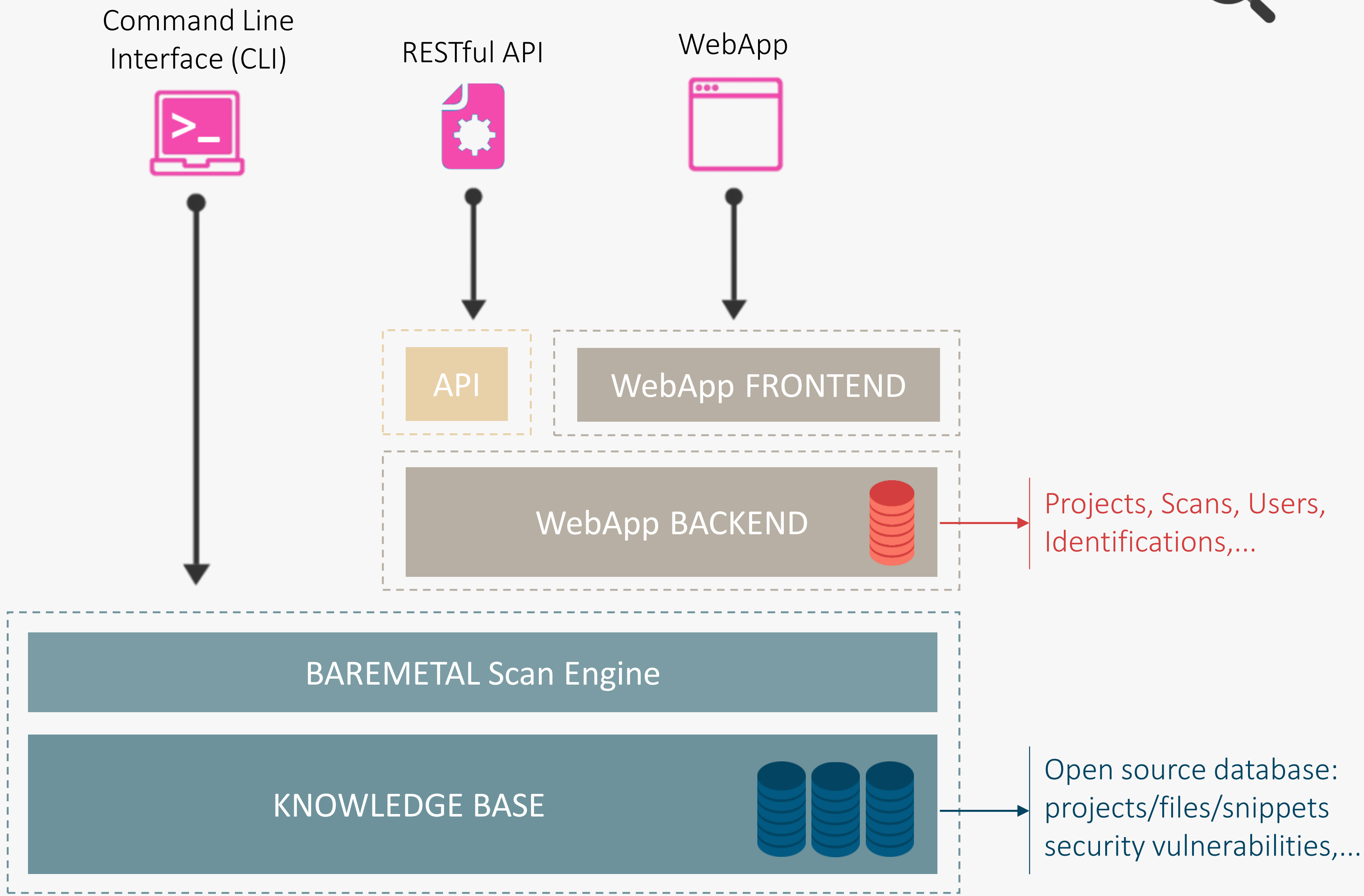
# Open source compliance process using FOSSID tools and services

# Contents

- FOSSID Tools - Architectural View
- Customer A
  - Continuous Scanning (CLI)
- Customer B
  - Continuous Scanning (WebApp)
  - API calls

# FOSSID Tools - Architectural View

# FOSSID Technology
## Architectural View

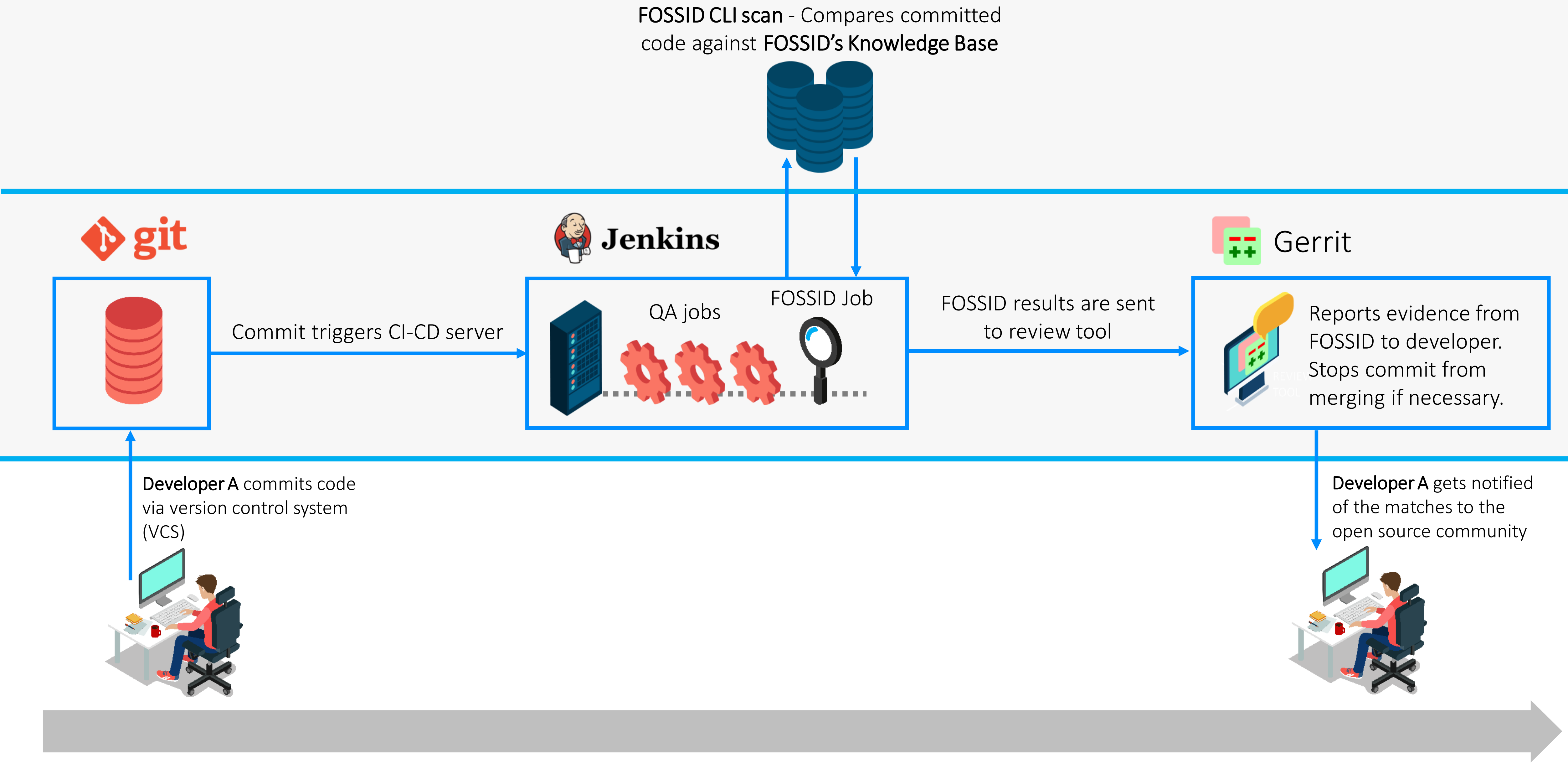


Projects, Scans, Users, Identifications,...

Open source database: projects/files/snippets security vulnerabilities,...

# Customer A

# Customer A – Continuous Scanning (CLI)



**FOSSID CLI scan** - Compares committed code against **FOSSID's Knowledge Base**

Commit triggers CI-CD server

QA jobs

FOSSID Job

FOSSID results are sent to review tool

Reports evidence from FOSSID to developer. Stops commit from merging if necessary.

**Developer A** commits code via version control system (VCS)

**Developer A** gets notified of the matches to the open source community

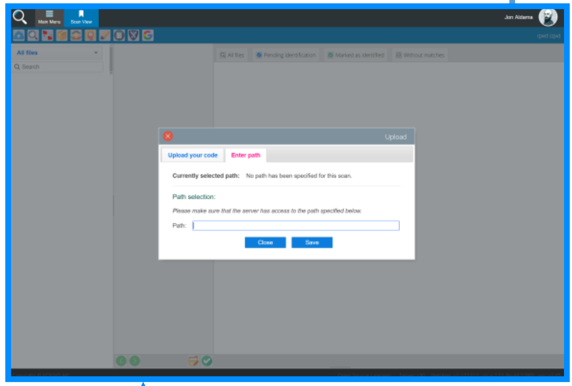
# Customer B

FOSSID

# Customer B – Continuous Scanning (WebApp)

**FOSSID WebApp scan** - Compares codebase snapshot against **previous knowledge** as well as **FOSSID's Knowledge Base**

Scan is triggered nightly via API



Upload your code | Enter path

**Currently selected path:** No path has been specified for this scan.

Path selection:

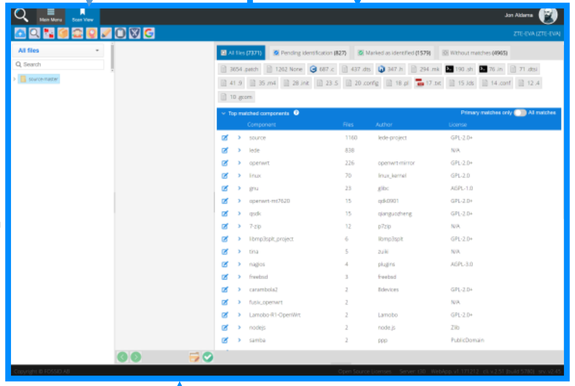
*Please make sure that the server has access to the path specified below.*

Path:

Close | Save

Scan target path

Refresh file tree every night



All files (7371) | Pending identification (827) | Marked as identified (1579) | Without matches (4965)

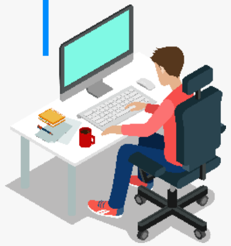
3654 .patch | 1262 None | 687 .c | 437 .dts | 347 .h | 294 .mk | 190 .sh | 76 .in | 71 .dtsi | 41 .9 | 35 .m4 | 28 .init | 23 .5 | 20 .config | 18 .pl | 17 .txt | 15 .lds | 14 .conf | 12 .4 | 10 .gcom

Top matched components — Primary matches only / All matches

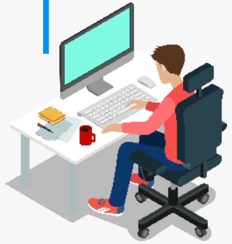
| Component | Files | Author | License |
|---|---|---|---|
| source | 1160 | lede-project | GPL-2.0+ |
| lede | 838 | | N/A |
| openwrt | 226 | openwrt-mirror | GPL-2.0+ |
| linux | 70 | linux_kernel | GPL-2.0 |
| gnu | 23 | glibc | AGPL-1.0 |
| openwrt-mt7620 | 15 | qdk0901 | GPL-2.0+ |
| qsdk | 15 | qianguozheng | GPL-2.0+ |
| 7-zip | 12 | p7zip | N/A |
| libmp3splt_project | 6 | libmp3splt | GPL-2.0+ |
| tina | 5 | zuiki | N/A |
| nagios | 4 | plugins | AGPL-3.0 |
| freebsd | 3 | freebsd | |
| carambola2 | 2 | 8devices | GPL-2.0+ |
| fusic_openwrt | 2 | | N/A |
| Lamobo-R1-OpenWrt | 2 | Lamobo | GPL-2.0+ |
| nodejs | 2 | node.js | Zlib |
| samba | 2 | ppp | PublicDomain |

Open Source Licenses Server: t30 WebApp: v1.171212 cli: v.2.51 (build 5780) srv: v2.45

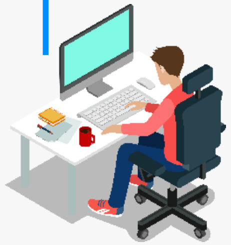
**Open source officer** creates a scan via WebApp that point a git repository



**Developers** commit code via version control system (VCS) regularly

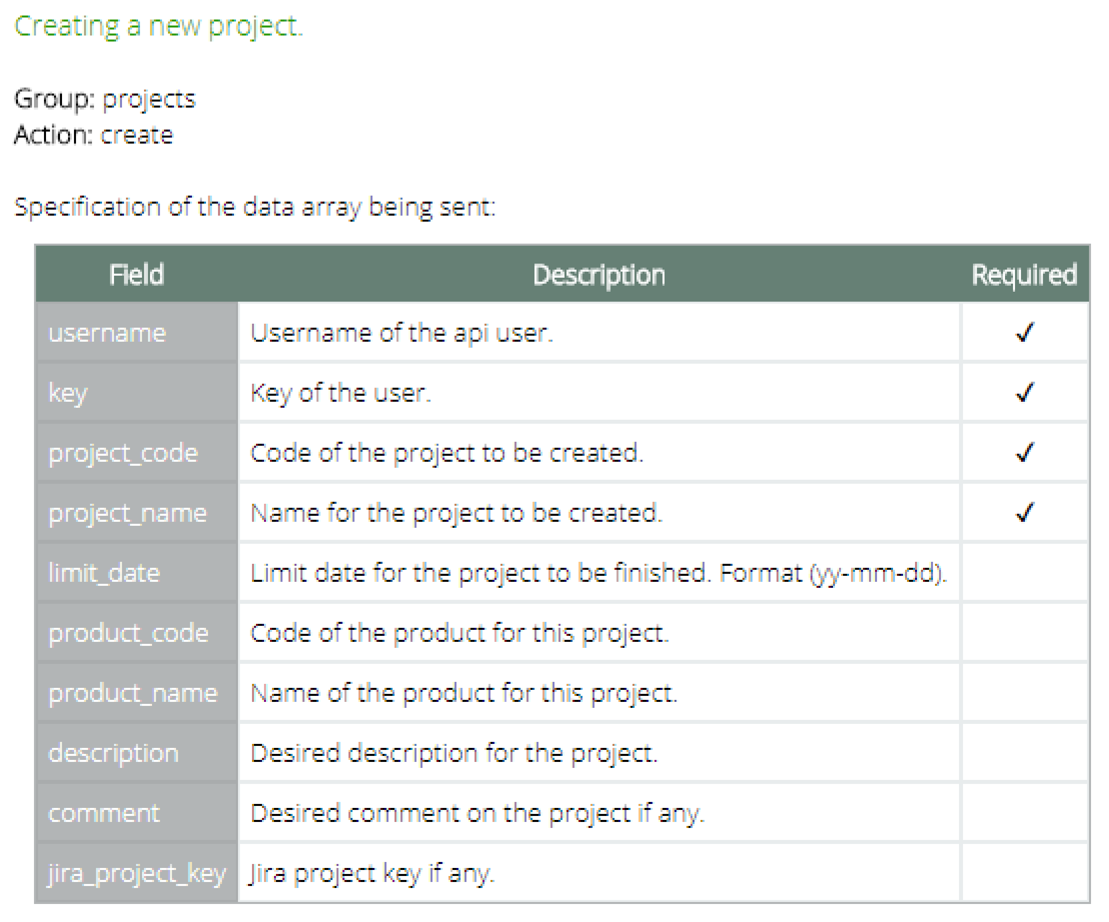


**Open source officer** reviews delta scan results daily and generates reports when necessary.



# API calls

*Create a new **project** and **scan**.*

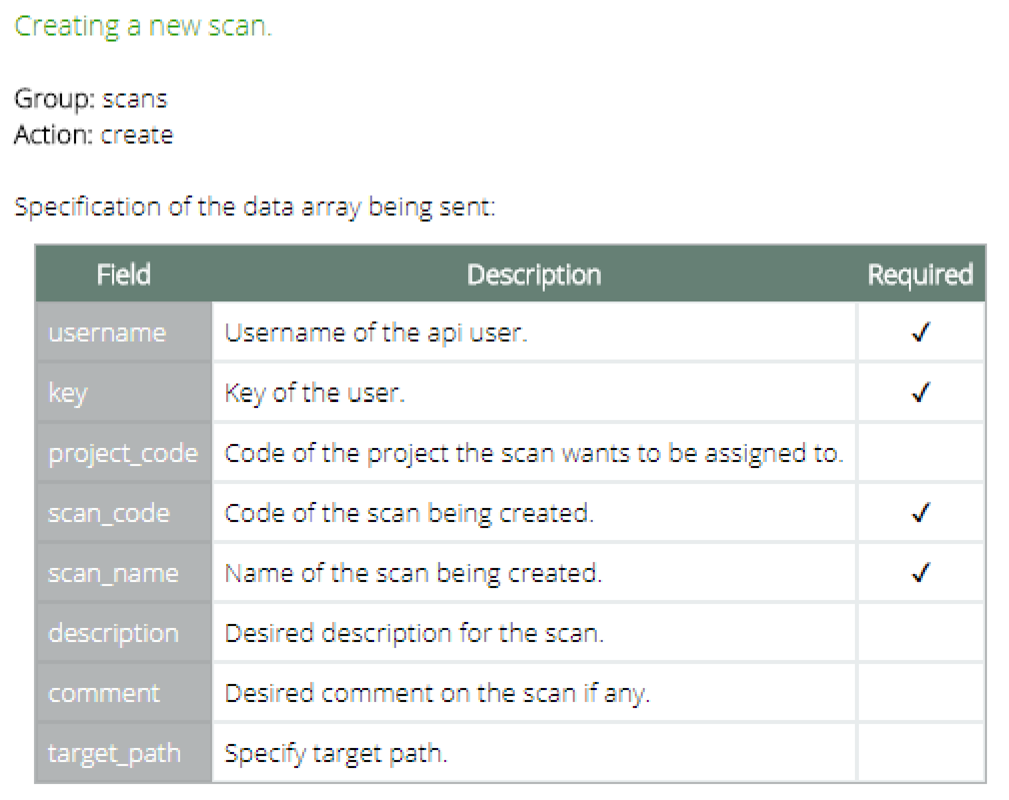


Creating a new project.

Group: projects
Action: create

Specification of the data array being sent:

| Field | Description | Required |
|---|---|---|
| username | Username of the api user. | ✓ |
| key | Key of the user. | ✓ |
| project_code | Code of the project to be created. | ✓ |
| project_name | Name for the project to be created. | ✓ |
| limit_date | Limit date for the project to be finished. Format (yy-mm-dd). | |
| product_code | Code of the product for this project. | |
| product_name | Name of the product for this project. | |
| description | Desired description for the project. | |
| comment | Desired comment on the project if any. | |
| jira_project_key | Jira project key if any. | |



Creating a new scan.

Group: scans
Action: create

Specification of the data array being sent:

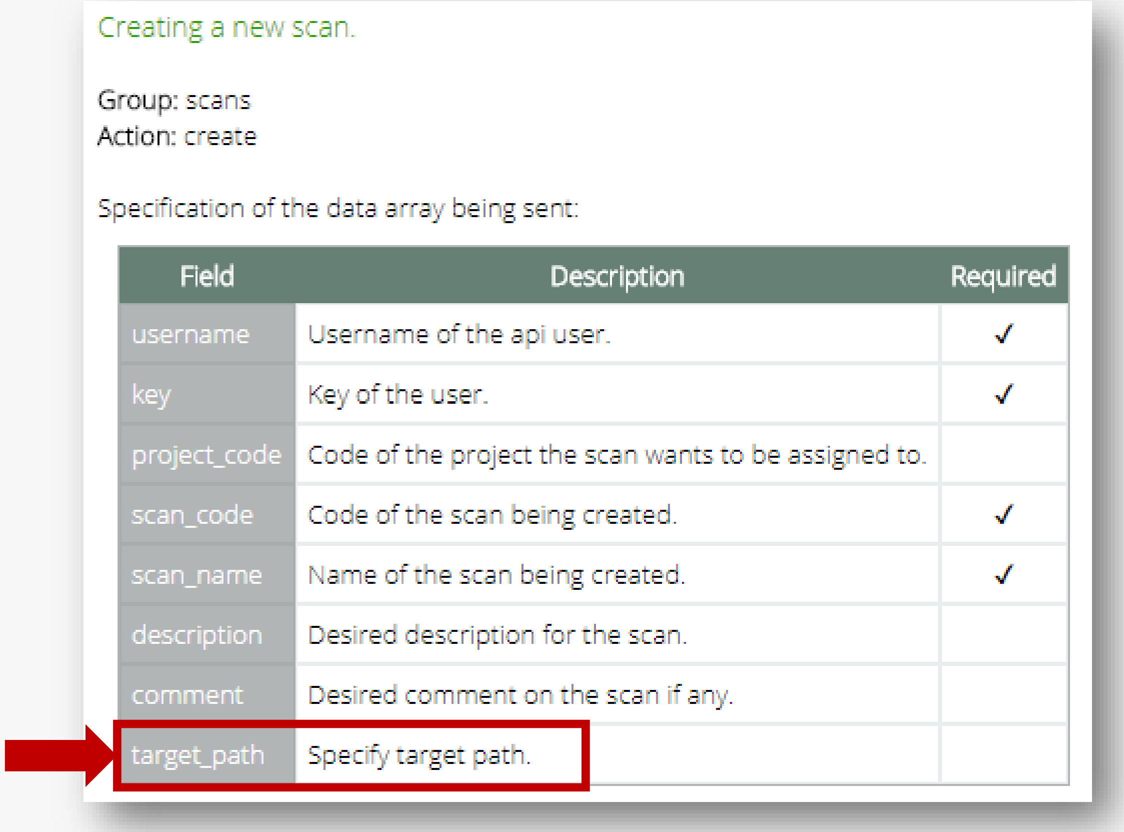
| Field | Description | Required |
|---|---|---|
| username | Username of the api user. | ✓ |
| key | Key of the user. | ✓ |
| project_code | Code of the project the scan wants to be assigned to. | |
| scan_code | Code of the scan being created. | ✓ |
| scan_name | Name of the scan being created. | ✓ |
| description | Desired description for the scan. | |
| comment | Desired comment on the scan if any. | |
| target_path | Specify target path. | |

*You can run **remote scans** via API (**target_path**).*

*This functionality allows you start a scan without uploading the code by pointing at the location where the target code resides. Note that the location needs to be accessible from the server where the WebApp runs.*

*Examples of usage:*

*- **Copy locally** the files you want to scan via scp or similar (for git repositories, do a **git clone**)*
*- Alternatively, you can also **mount remote file systems** (useful for repository managers)*
*- Monitor remote scans, trigger regular scans*



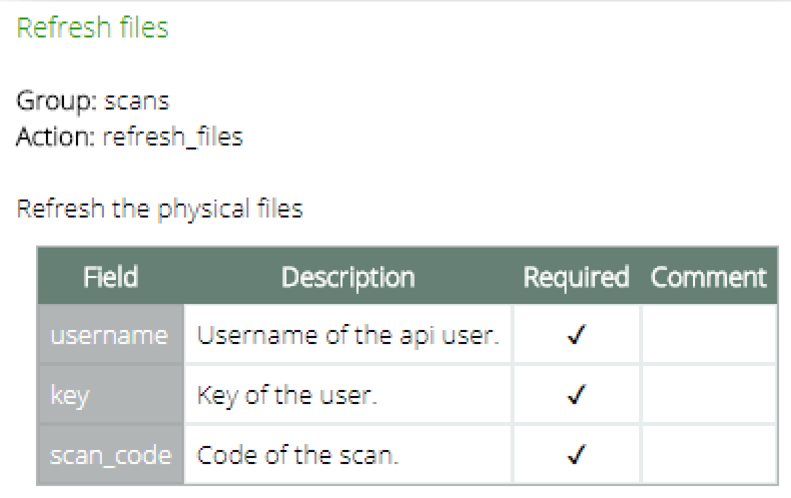
Creating a new scan.

Group: scans
Action: create

Specification of the data array being sent:

| Field | Description | Required |
|---|---|---|
| username | Username of the api user. | ✓ |
| key | Key of the user. | ✓ |
| project_code | Code of the project the scan wants to be assigned to. | |
| scan_code | Code of the scan being created. | ✓ |
| scan_name | Name of the scan being created. | ✓ |
| description | Desired description for the scan. | |
| comment | Desired comment on the scan if any. | |
| target_path | Specify target path. | |

*__Refresh target path__ before re-scan:*



Refresh files

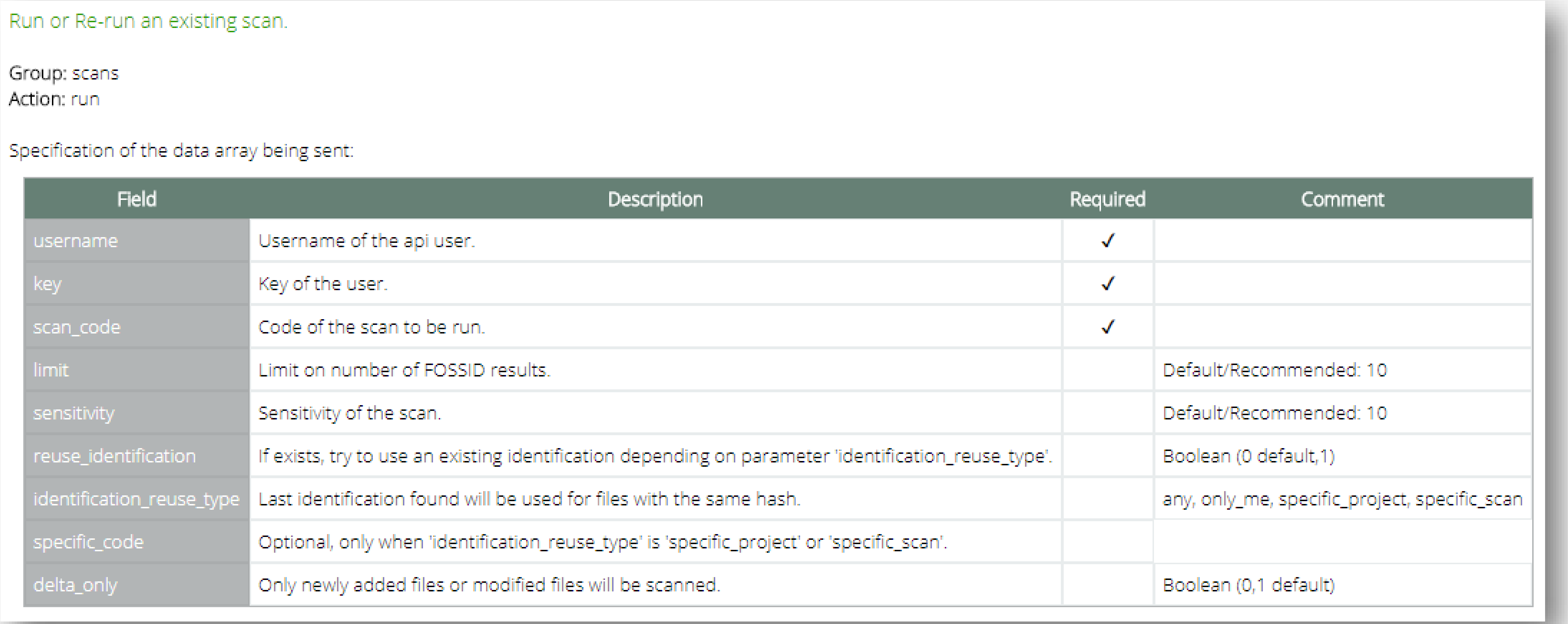
Group: scans
Action: refresh_files

Refresh the physical files

| Field | Description | Required | Comment |
|---|---|---|---|
| username | Username of the api user. | ✓ | |
| key | Key of the user. | ✓ | |
| scan_code | Code of the scan. | ✓ | |

*You can use* ***scan or re-scan options****:*

- *Limit & sensitivity*
- *Identification re-use options: based on specific project, scan, user…*
- *Use* ***delta only*** *option to scan the files that have changed from the previous iteration (re-scan)*



Run or Re-run an existing scan.

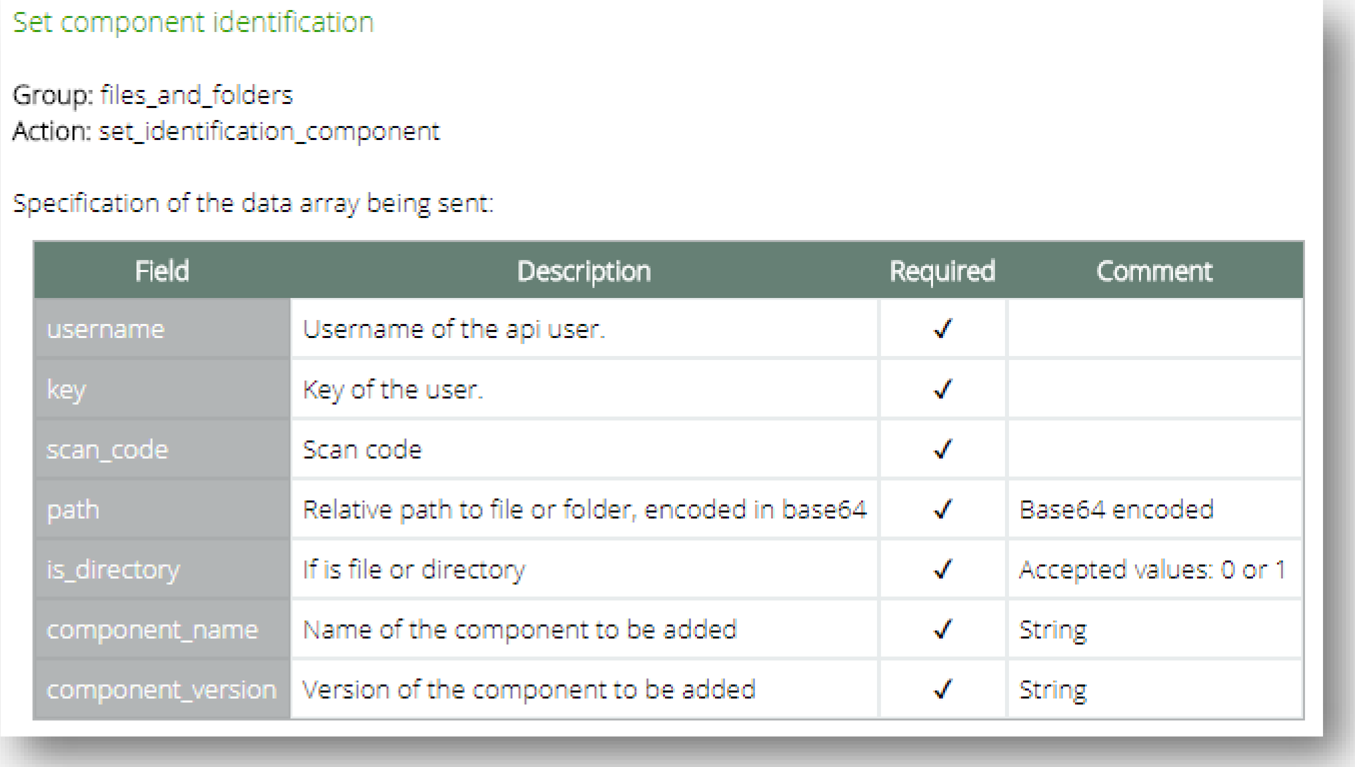
Group: scans
Action: run

Specification of the data array being sent:

| Field | Description | Required | Comment |
|---|---|---|---|
| username | Username of the api user. | ✓ | |
| key | Key of the user. | ✓ | |
| scan_code | Code of the scan to be run. | ✓ | |
| limit | Limit on number of FOSSID results. | | Default/Recommended: 10 |
| sensitivity | Sensitivity of the scan. | | Default/Recommended: 10 |
| reuse_identification | If exists, try to use an existing identification depending on parameter 'identification_reuse_type'. | | Boolean (0 default,1) |
| identification_reuse_type | Last identification found will be used for files with the same hash. | | any, only_me, specific_project, specific_scan |
| specific_code | Optional, only when 'identification_reuse_type' is 'specific_project' or 'specific_scan'. | | |
| delta_only | Only newly added files or modified files will be scanned. | | Boolean (0,1 default) |

*Perform* ***identifications*** *(build your own pedigree database):*

- *On file or folder level*
- *Reuse identifications in future scans (do not annotate a file twice)*
- *Saved in transparent MySQL database*



Set component identification

Group: files_and_folders
Action: set_identification_component

Specification of the data array being sent:

| Field | Description | Required | Comment |
|---|---|---|---|
| username | Username of the api user. | ✓ | |
| key | Key of the user. | ✓ | |
| scan_code | Scan code | ✓ | |
| path | Relative path to file or folder, encoded in base64 | ✓ | Base64 encoded |
| is_directory | If is file or directory | ✓ | Accepted values: 0 or 1 |
| component_name | Name of the component to be added | ✓ | String |
| component_version | Version of the component to be added | ✓ | String |

# THANK YOU

www.fossid.com