Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

Sign in

powered by Stoplight

Access Management Service Phase 1

Export

v1.0.0

▸ **{Base_URL}/api/access-management**

> This section relates to Phase 1 of the new Access Management feature, which is being rolled out gradually for customers. Documentation for Phase 2 is available here. Please contact your Checkmarx account agent to verify whether this is supported yet for your account.

The Access Managent APIs are used for managing access to specific resources in your tenant account. An admin user can use the POST `Create an assignment` API to create an "asignment". An "assignment" specifies one or more "entities" (user, usergroup or OAuth Client) and grants them permission to access specific "resources" (tenant, application or project). These APIs also enable you to access detailed information about all assignments in your account.

> Currently, the set of actions that a user can take on each resource is determined by the permissions that they have accross the tenant account. In a later phase, it will be possible to assign granular permissions relative to specific resources.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Sign in

powered by Stoplight

Access Management Service Phase 2

Export

v1.0.0

▸ **{Base_URL}/api/access-management**

> This section relates to Phase 2 of the new Access Management feature, which is being rolled out gradually for customers. Documentation for Phase 1 is available here.

The Access Managent APIs are used for managing access to specific resources in your tenant account. A user with `update-assignments` permission can use the POST `Create an assignment` API to create an "asignment". An "assignment" specifies one or more "entities" (user, usergroup or OAuth Client) and grants them permission to access specific "resources" (tenant, application or project). You can also specify "roles" that designate the permissions for this assignment. If not specified, then each user has the permissions specified in his "base role".
Each role comprises a series of permissions that specify the precise actions that he is authorized to take. The system comes with a set of preconfigured (out-of-the-box) "System Roles". In addition you can create custom roles based on the granular permissions that are available in the system.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Sign in

powered by Stoplight

All Scanners Results Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/results**

Overview

Get detailed results for each of the scanners that ran in a specific scan (by scan ID). This API returns full details about each vulnerability detected, including vulnerability details, history, compliance, affected nodes etc. Results from the following scanners are included in the results: SAST, SCA, IaC Security (kics) and Container Security (containers), Secret Detection (sscs-secret-detection) and Scorecard sscs-scorecard (sscs-scorecard).

Workflow

1. Use `POST /api/scans` to create a scan, generating a “scan id”.
2. Use the “scan id” with `GET /api/results` to get the results of that SAST scan.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Application Risk Management

Sign in

powered by Stoplight

Analytics REST API

Export

v1.0.0

▸ **{Base_URL}/api/data_analytics**

Overview

This API provides seamless access to the Checkmarx platform's Analytics DB, providing the following benefits:

- Enable customers to integrate their preferred Business Intelligence (BI) tools for customizable data analysis and reporting.
- Offer internal CXone services a unified access method for consuming analytics data.
- Streamline data access by replacing multiple real-time data retrieval processes with a singular, robust API, reducing integration complexity and points of failure.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

> The token needs to be generated by a user who has either the `ast-admin` role or the following combination of roles and permissions: `manage-project` (Role) + `manage-application` (Role) + `view-risk-management` (Permission) + `import-`

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Application Risk Management

Sign in

powered by **Stoplight**

`findings-external-platforms` (Permission).

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Application Risk Management REST API

Export

v1.0.0

Overview

These APIs enable users to easily identify the riskiest applications and the most severe risks in each application. You can also manage the remediation process by changing the state of risks to indicate that they have been analyzed or are currently being processed. See complete documentation of this feature here.

Permissions

The permissions required for using these APIs are documented here.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Applications Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/applications**

Overview

An Application in Checkmarx One is a logical entity that represents a group of related Projects. This enables you to view aggregated data for all of the related Projects. The Application configuration includes defining “rules” that determine which Projects are associated with that Application. For example, you can assign all Projects that either have the tag “demo” or have “demo” as part of their name to a particular Application.

> Scanning is done on the project level. Applications are only relevant for viewing scan results.

Projects are not required to be assigned to an Application. You can perform all CRUD actions on Applications and Application “rules” via API.

> You can create rules within the POST Application API call. It is not necessary to create rules separately using the Application rule APIs.

Authentication

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Applications Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Create an application	POST	/applications	Create a new Checkmarx One application, which is used for organizing projects.
Get list of applications	GET	/applications	Get a list of all applications in your account.
Get list of application tags	GET	/applications/tags	Get a list of all tags that have been applied to applications in your account. Tags can be simple strings or key:value pairs.
Get application info	GET	/applications/{application_id}	Get detailed info about a particular application.
Update an application	PUT	/applications/{application_id}	Update the configuration of a application.
Delete an application	DELETE	/applications/{application_id}	Delete an application.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Applications Rules Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Create an application rule	POST	/applications/{application_id}/project-rules	Create a new rule for a particular application.
Get list of application rules	GET	/applications/{application_id}/project-rules	Get a list of all rules for a particular application.
Get info about an application rule	GET	/applications/{application_id}/project-rules/{rule_id}	Get info about a particular application rule.
Update an application rule	PUT	/applications/{application_id}/project-rules/{rule_id}	Update the configuration of an application rule.
Delete an application rule	DELETE	/applications/{application_id}/project-rules/{rule_id}	Delete an application rule.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Audit Trail Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/audit**

Audit Trail API

Introduction

This API enables users to get a complete log of events that occurred in their account. Events are recorded for user management activities such as creation or deletion of users and roles. In addition, events are recorded for several other Checkmarx One services.

> ⓘ Event info is stored in CloudEvents format.

Events for the current day are given as a json object with a record for each event. Events for previous days are given as links that are used to download the json for that day's events.

> ⓘ Events are available for the previous 365 days.

List of Logged Events

The following list shows the events that are currently logged by this service.

- ▸ cx-iam events (user management)
- ▸ Other Checkmarx One services

Checkmarx

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Workflow

Use `GET /api/audit` to get the events for the current day as well as URL links for events on previous days.

For each previous day, use `GET \<URL>` to get the events for that day.

> You need to submit your JWT token with each request.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

Authentic API

Description

This API generates a JWT (JSON Web Token) access token which is used for authentication with all Checkmarx One APIs.

> The access token is valid for a 30 minute session.

There are two methods that can be used to generate an access token:

> **API Key** - If you have an API Key, you can submit it with this API in order to receive an access token. To learn how to generate an API Key, see Generating an API Key.

Authentication API
Description
Method
Workflow
URL
Curl Sample - Refresh Tok...
Curl Sample - OAuth2 Client
Media Type (header)
Parameters
Success Response
Sample Success Response
Error Response

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

After the initial call, there is an option to submit a Refresh Toke (valid for 8 hours) in place of the API Key, to generate ne access toke A refresh token is returned as part of the response fo the Authenticat API, see below.

OAuth2 Client - If you have an OAuth2 Client for Checkmarx One, you can submit your **Client ID** and **Secret** with this API in order to receive an access token. To learn how to generate an OAuth2 Client, see Creating an Oauth2 Client.

The access token

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

inherits whichever roles (permission are assigne to the OAuth2 Client.

Method

POST

Workflow

1. Use the Authentication API to generate an access token
2. Use the access token for authentication of all APIs

URL

US Environment - https://iam.checkmarx.ne auth/realms/{tenant_account_ protocol/openid-connect/token

US2 Environment - https://us.iam.checkmarx auth/realms/{tenant_account_

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

protocol/
openid-
connect/token

EU
Environment -
https://
eu.iam.checkmarx
auth/realms/
{tenant_account_
protocol/
openid-
connect/token

EU2
Environment -
https://
eu-
2.iam.checkmarx.
auth/realms/
{tenant_account_
protocol/
openid-
connect/token

DEU
Environment -
https://
deu.iam.checkma
auth/realms/
{tenant_account_
protocol/
openid-
connect/token

Australia &
New Zealand -
https://
anz.iam.checkmar
auth/realms/
{tenant_account_
protocol/
openid-
connect/token

India - https://
ind.iam.checkmar
auth/realms/
{tenant_account_
protocol/

openid-connect/token

Singapore - https://sng.iam.checkmar auth/realms/{tenant_account_ protocol/openid-connect/token

UAE - https://mea.iam.checkma auth/realms/{tenant_account_ protocol/openid-connect/token

Curl Sample - Refresh Token

```
curl --request POST
  --data "grant_type
  --data "client_id=
  --data "refresh_to
```

Curl Sample - OAuth2 Client

```
curl --request POST
  --header 'Content-
  --header 'Accept:
  --data-urlencode '
  --data-urlencode '
  --data-urlencode '
```

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

Media Type (header)

Accept: application/ json

Parameters

PARAMETER	REQUIRED
grant_type	Yes
client_id	Yes
refresh_token	Required grant_typ `refresh_t`
client_secret	Required grant_typ `client_cr`

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

Success Response

Code: 200
Authenticated

ATTRIBUTE	TYPE
access_token	strin
expires_in	integ
refresh_expires_in	integ
refresh_token	strin
token_type	strin

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

ATTRIBUTE	TYPE
not-before-policy	integ
session_state	strin
scope	strin

Sample Success Response

```
{
        "access_toke
        "expires_in"
        "refresh_exp
        "refresh_tok
        "token_type"
        "not-before-
        "session_sta
        "scope": "ia
    }
```

Error Response

Status Code: 400

Message: `Grant type`

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

`must be one of the following values: client_credentials`

Message: `Token is a required field`

Status Code: 401

Message: `Not Authorized: Provided token is not valid`

Status Code: 405

Message: `Method Not Allowed`

Status Code: 500

Message: `Internal Server Error`

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Bring Your Own Results (BYOR) Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/byor**

Overview

This API is used to import vulnerability results that adhere to SARIF version 2.1.0 format from third-party security tools and services.
These imported results are integrated into the Application Risk Management feature, providing organizations with a unified view of their application risk profile and enabling them to make informed decisions to secure their end-to-end application lifecycle.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

> The token needs to be generated by a user who has either the `ast-admin` role or the following combination of roles and permissions: `manage-project` (Role) + `manage-application` (Role) + `view-risk-management` (Permission) + `import-findings-external-platforms` (Permission).

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Workflow

The following procedure explains the E2E workflow for importing SARIF results into Checkmarx One via API.

1. Create one or more SARIF files, following the specifications described in SARIF File Specification and SARIF File Limitations. If you are importing multiple files, create a zip archive.
2. Use `POST /api/projects` to create a new Project, taking note of the Project ID. (Alternatively, you can use an existing Project.)

> In order to view results in Checkmarx One, you must ensure that the Project is assigned to an Application, see here.

1. Use `POST /api/uploads` to generate an upload link.
2. Use `PUT /{uploadLink}`, specifying the path to your SARIF file or zip archive, to upload your results.
3. Use `POST /api/imports`, specifying the Project ID and upload link, to import the results.
4. Retrieve the imported results together with your overall Application Risk Management results in Checkmarx One using `GET /api/risk-management/summary`. You can also, retrieve the risk management results for this specific Application using [GET api/risk-management/{applicationId}/results].

Alternatively, you can view the results on the Application Risk Management screen of the Checkmarx One web application (UI), see Application Risk Management.

> The imported results are only shown in the context of the Application Risk Management feature, they are not integrated with the scan results on the Project page.

Checkmarx

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by **Stoplight**

Checkmarx One API Endpoints Summary

The Checkmarx One external APIs are grouped into the following categories:

API CATEGORY	DESCRIPTION
All Scanners Results	This API is used for retrieving comprehensive results for the vulnerabilities identified by all scanners (SAST, IaC Security, SCA) in a specific scan.
API Security Scan Results	This API is used for retrieving comprehensive results for API Security scans run in your account.
Application Risk Management	These APIs enable users to easily identify the riskiest applications and the most severe risks in each application.
Applications	These APIs are used for performing all CRUD activities on Applications. They are also used to get various types of data about the Applications in your account. There are also APIs for CRUD activities on “rules” which define how Projects are associated with Applications.
Audit Trail	This API is used for retirieving a list of all events that occurred in your tenant account.
Authentication	Uses your *Refresh Token (i.e., API Key)* or username and password to obtain an *Access Token* which is used for authentication of your Checkmarx One API calls during the current session.
Bring Your Own Results (BYOR)	This API is used for importing vulnerability results that adhere to

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by **Stoplight**

API CATEGORY	DESCRIPTION
	SARIF version 2.1.0 format from third-party security tools and services.
Code Repository Project Conversion	This API is used for converting (migrating) existing Checkmarx projects to Code Repository projects.
Code Repository Project Import	This API is used for creating code repository import projects in Checkmarx. This is done by setting up an integration with your SCM and creating a Checkmarx One project for each repo that you would like to scan.
DAST Results	These APIs are used for viewing information about results (risks) that were identified by DAST scans run in your account.
DAST Scans	These APIs are used for creating and managing DAST Environments as well as for running and managing DAST scans.
IaC Secrurity Results	This API enables you for retrieving comprehensive results for the vulnerabilities identified by the IaC Security scanner in a specific scan.
IaC Security Results Predicates	These APIs are used for managing vulnerabilities identified by IaC Security throughout your SDLC.
Policy Management	This API retrieves results for all policies that apply to the specified scan of a project.
Projects	These APIs are used for performing all CRUD activities on projects. They are also used to get various types of data about the projects in your account.
Projects Overview	These APIs are used for retrieving an overview of data for projects in your tenant account, including a summary of results from the latest scan of each project.
Query Editor	These APIs are used for managing queries in your account.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by **Stoplight**

API CATEGORY	DESCRIPTION
Reports	This API enables users to generate Reports with info about the applications, projects and scans in their account.
Reports - Customized	This API enables users to generate scan reports with detailed information about the risks identified by each of the scanners. This report is more comprehensive than the standard scan report and the PDF output has an improved look and feel.
Results Overview	DEPRECATED
	This API enables you to get an overview of data for the projects in your account.
Results Summary	This API enables you to get a summary (counters) of the scan results for one or more scans.
SAST Metadata	These APIs are used to get information about the running of a scan. This includes detailed info about how incremental scans were executed.
SAST Results	This API enables you to get comprehensive results for the vulnerabilities identified by the SAST scanner in a specific scan.
Sast Results Predicates	These APIs enable you to manage vulnerabilities identified by SAST throughout your SDLC.
SAST Results Summary	These APIs enable you to get aggregated data about SAST vulnerabilities identified in the projects in your account.
Scan Configuration	These APIs are used to configure global settings for the tenant account as well as settings for specific Checkmarx One projects and scans.
Scans	These APIs are used to run, cancel or delete scans. They are also used to get various types of data about scans

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

API CATEGORY	DESCRIPTION
	that have been run in the account.
SCA File Analysis	These APIs enable you to upload a supported type of report file for SCA analysis, and retrieve results.
Uploads	These APIs are used for uploading zip archives to the cloud for scanning.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Checkmarx SCA File Analysis Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/sca/analysis/requests**

Overview

These APIs enable you to upload a supported type of report file for SCA analysis, and retrieve results. The results include detailed info about the packages specified in the file as well as all associated vulnerabilities, supply chain risks and license info.

> This service currently supports SBOMs in CycloneDx (v1.0-1.6) and SPDX (v2.2) formats. It is mandatory to include the Package URL (purl) for each package in the SBOM. For more information about purl syntax, see here.

> This API does not run a full SCA scan of your project. To run a full SCA scan, use the `/scans/` endpoint.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Code Repository Management REST API

Export

v0.0.1

▸ **{Base_URL}/api/repos-manager**

Overview

These APIs are used to retrieve data about the Code Repository integrations configured in your Checkmarx One account.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Code Repository Project Conversion Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/repos-manager**

Overview

Checkmarx One enables you to convert (migrate) existing Checkmarx projects to Code Repository projects. Checkmarx manual projects are used to trigger scans of zip files or code repository paths via the Checkmarx One platform. When migrating a manual project to a Code Repository based project, the following modifications take place:

> Webhooks are created for the organization and repository.
>
> The scan trigger changes to push events and pull requests, initiated from the repository itself.
>
> The entire scanning process is automated.

The migrated project retains its scan history, and all pre-configured scan rules remain unchanged.

The migration process is supported for GitHub, GitLab, Bitbucket, and Azure DevOps - Cloud-hosted / Self-hosted. For detailed information about required permissions for each SCM, see Code Repository Integrations.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Project Conversion Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Convert a project	POST	/project-conversion	Migrate (convert) one or more projects to Code Repository projects.
Retrieve project conversion status	GET	/project-conversion	Retrieve the status of a project conversion process.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Code Repository Project Import Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/repos-manager/scm-projects**

Code Repository Project Import API

Overview

Checkmarx One enables you to create code repository import projects in Checkmarx. This is done by setting up an integration with your SCM and creating a Checkmarx One project for each repo that you would like to scan. A code repository import project differs from a manual project in the following ways:

> Webhooks are created for the organization and repository.
>
> Scans are triggered by push events and pull requests, initiated from the repository itself.
>
> The entire scanning process is automated.

For detailed information about required permissions, see Code Repository Integrations.

Limitations

> This API is currently supported only for GitHub repos. For other SCMs, you can create manual projects and then use the Project Conversion API to convert them into code repository

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

projects.

There is a maximum of three branches that can be "protected" (scanned) for each project.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Project Conversion Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Create a project	POST	/scm-projects	Create Code Repository projects in Checkmarx by importing repos from your SCM.
Retrieve project creation status	GET	/scm-projects	Retrieve the status of an import process.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

Sign in

powered by **Stoplight**

Generating an API Key

You can generate an API Key in the Checkmarx One web application (UI), using the procedure described in Generating an API Key.
The roles (permissions) assigned to the API Key are inherited from the user account that generates the key. Therefore, make sure that you are using an account with the appropriate permissions. The minimum required roles for running an end-to-end flow of scanning a project and viewing results are the out-of-the-box composite role `ast-scanner` as well as the IAM role `default-roles, see Managing Roles.

> Whenever you update your Checkmarx One license (e.g., adding a new scanner) all existing API Keys become invalid. You will need to generate new API Keys to replace those that are used in your integrations and plugins.

Checkmarx

Search Checkmarx One API Reference Guide...

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Improved Reports Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/reports/v2**

Overview

This API enables users to generate various types of reports based on the data in their Checkmarx One account. These reports are more comprehensive than the standard reports generated using `/reports` (v1) APIs, and the PDF output has an improved look and feel. Learn more about the new report format here. This API also enables report customization by specifying the sections to include and applying filters to the data. You can retrieve the reports via API or by specifying email recipients. The success response returns a `reportId` which can be used to download the report using `GET reports/{reportId}/download`.

> **Project Report** - gives detailed info about one or more projects, including aggregated statistics about the vulnerabilities detected in the project broken down by state, severity, technology etc.
>
> **Scan Report** - gives detailed info about a particular scan of a project in your account, including info about the vulnerabilities detected by each of the scanners. This report is more comprehensive than the standard scan report and the PDF output has an improved look and feel. Learn more about the new report format here.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by **Stoplight**

Introduction

You can access the full functionality of Checkmarx One using our REST APIs. You can use APIs to perform CRUD actions on Checkmarx One projects and applications, run scans, and view scan results. You can also use APIs to manage vulnerabilities and create webhooks.

Checkmarx One requires JWT (JSON Web Token) access tokens for authentication of all API calls. Access tokens are generated using the Authentication API).

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Projects Overview Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/projects-overview**

Overview

Use this API to get an overview of data for projects in your tenant account, including a summary of results from the latest scan of each project. You can limit the results by using pagination and/or setting filters.
Note: This API replaces the Results Overview API which will soon be deprecated.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Projects Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/projects**

Overview

A Project in Checkmarx One is a logical entity that represents a source repository, such as a component, microservice, etc. which you intend to scan for vulnerabilities. Each time that you run a scan on the source repository you do so under the same project, enabling you to track vulnerabilities in Checkmarx One throughout your SDLC. When you create a project, you configure the project settings, including specifying Groups for access control.

> When scanning from a zip archive, you must first create a project in your account before you can run the scan. When scanning from a Git repository, there is an option of running a scan without a preconfigured project. In this case, a project is automatically generated and it is given the name of the repo.

Projects can be assigned to applications, together with other related projects. This enables you to view aggregated data for all of the related projects.

You can perform all CRUD actions on projects via API.

> Once you have created a project you can

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

run a scan of that project using the Scan APIs.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Pagination

GET `projects`, `last-scan` and `branches` use pagination. By default they return the first 20 results. Use `limit` to adjust the maximum number of results to return and `offset` to specify the number of results to skip before starting to return results. You can use `offset=0` and `limit=0` to get all results.

Projects Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Create a project	POST	/projects	Create a new Checkmarx One project.
Get list of projects	GET	/projects	Get a list of all projects in your account.
Get list of tags	GET	/projects/tags	Get a list of all tags that have been applied to projects in your account. Tags can be simple strings or key:value pairs.
Get last scan list	GET	/projects/last-scan	Get a list of the most recent scans of each project (based on applied filters), with the scan IDs mapped

API	METHOD	ENDPOINT	DESCRIPTION
			out to the corresponding project IDs.
Get list of branches	GET	/projects/branches	Get a list of all branches of a particular project.
Get project info	GET	/projects/{project_id}	Get detailed info about a particular project
Update a project	PUT	/projects/{project_id}	Update the configuration of a project.
Delete a project	DELETE	/projects/{project_id}	Delete a project.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Reports Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/reports**

Overview

This API enables users to generate Reports with info about the applications, projects and scans in their account. The API can be used to generate the following types of reports:

Application List Report - gives a list of applications in your account, with detailed info about each application.

Project List Report - gives a list of projects in your account, with detailed info about each project.

Scan List Report - gives a list of scans run on a particular project, with detailed info about each scan.

Project Report - gives detailed info about a particular project, including aggregated statistics about the vulnerabilities detected in the project broken down by state, severity, technology etc.

Scan Report (NEW) - gives detailed info about a particular scan of a project in your account, including info about the vulnerabilities detected by each of the scanners. This report is more comprehensive than the standard scan report and the PDF output has an improved look and feel. Learn more about the new report format here.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Legacy Scan Report - gives detailed info about a particular scan of a project in your account, including info about the vulnerabilities detected by each of the scanners.

Reports can be generated in various formats (PDF, CSV, JSON) depending on the type of report being generated. Reports can be sent via email or downloaded using the download API.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Create Report	POST	/api/reports	Generate a new report.
Report Status	GET	/api/reports/{reportId}	Check the status of a report.
Download Report	GET	/api/reports/{reportId}/download	Download a report that has been generated. The API redirects to the download URL and automatically initiates the download to your local machine.

Standard Workflow

To generate a report and download it:

Use `POST /api/reports` to generate a report, and record the Report ID that is returned.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Use `GET /api/{reportId}`, specifying the Report ID of the desired report, to monitor the status of the report.

Once the report is completed, use `GET /{reportId}/download`, specifying the Report ID of the desired report, to download the report.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Results Overview Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/results-overview**

> This API will soon be deprecated. It is being replaced by Projects Overview.

Overview

Use this API to get an overview of data for projects in you tenant account.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Results Summary Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/scan-summary**

Overview

This API enable you to get aggregated data (counters) for various types of vulnerabilities identified in one or more scans. If you would like to get detailed info about individual vulnerabilities that were detected, use (Scanners Results)[AllScannersResults.yaml].

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Sast Metadata Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/sast-metadata**

Overview

These APIs get detailed information about how a SAST scan was run.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Endpoints Summary

The following is a list of Checkmarx One APIs that relate to SAST Metadata:

API	METHOD	ENDPOINT	DESCRIPTION
GET Scan Metadata	GET	/api/sast-metadata/	Get SAST scanner metadata for one or more scans.
GET (Specific) Scan Metadata	GET	/api/sast-metadata/{scan-id}	Get SAST scanner metadata for a specific scan.
GET (Specific)	GET	/api/sast-metadata/	Get the SAST scanner metrics

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

API	METHOD	ENDPOINT	DESCRIPTION
Scan Metadata Metrics		{scan-id}/metrics	for the specified scan. This includes info about memory usage as well as aggregated statistics for succesfully scanned items (broken down by language).

Workflow

1. Use `POST /api/scans` to run a scan.
2. Use the “scan id” with `GET /api/sast-metadata` to get the metadata of that scan. You can include more than one scan id in your request.
3. Use the “scan id” with `GET /api/sast-metadata/{scan-id}/metircs` to get the metrics of that scan.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

SAST Results Predicates API

Export

v1.0.0

▸ **{Base_URL}/api/sast-results-predicates**

Overview

Recurrent Vulnerabilities

Checkmarx One tracks vulnerabilities throughout your SDLC by assigning a `similarityId` to each vulnerability instance in your scan. This enables Checkmarx One to track that particular instance in future scans. This means that after the initial scan of a project, if the **identical** vulnerability is detected in subsequent scans it is automatically marked as a **Recurrent** vulnerability.

> A **Recurrent** vulnerability is defined as a vulnerability with the identical Source Node and Sink Node as well as the identical Attack Vector elements. If even minor changes were introduced to any of these elements (even though the nature of the threat is the same), the `similarityId` will be different, causing the vulnerability to be identified as a **New** vulnerability.

Each vulnerability has a “Predicate” associated with it, which is comprised of the following attributes, **state**, **severity** and **comments**. After reviewing the results of a scan, you have the ability to triage the results by changing these predicates. If a subsequent scan discovers a vulnerability with the identical

`similarityId`, its **status** will be marked as **Recurrent**, and the **state**, **severity** and **comments** from the previous scan will be applied to the new scan. Each time that you modify the **state**, **severity** or **comments** associated with a vulnerability's `similarityId`, a new predicate is created, with an associated unique predicate id. For more information about triaging results, see Managing (Triaging) Vulnerabilities.

Endpoint Summary

The following is a list of Checkmarx One APIs that relate to Results Predicates:

API	METHOD	ENDPOINT	DESCRIPTION
Change a SAST predicate	POST	`/sast-results-predicates`	Creates a new predicate
Update a SAST preidcate	PATCH	`/sast-results-predicates`	Update the comment for a SAST predicate
Retrieve a SAST predicate	GET	`/sast-results-predicates/{similarityId}`	Retrieve the predicates for a specific vulnerability instance
Retrieve latest SAST predicate	GET	`/sast-results-predicates/{similarityId}/latest`	Retrieve the details of the latest predicate that was created for a particular vulnerability instance
Delete a SAST predicate	DELETE	`/sast-results-predicates/{similarityId}/{projectID}/{predicateID}`	Delete a specific predicate

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

SAST Results Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/sast-results**

Overview

Get comprehensive results for each of the vulnerabilities detected in a specific SAST scan (by scan ID). This API returns full details about each vulnerability detected, including vulnerability details, history, compliance, affected nodes etc. You can also compare results for two different scans.

> ⓘ If you would like to get the SAST results together with results from the other scanners run on the scan, use `GET /api/results`.

Workflow

1. Use `POST /api/scans` to create a scan (specifying to run the SAST scanner), generating a “scan id”.
2. Use the “scan id” with `GET /api/sast-results` to get the results of that SAST scan.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

SAST Scan Results Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Get SAST scan results	GET	/sast-results	Get detailed results from the SAST scanner for a specific scan.
Compare SAST scan results	GET	/sast-results/compare	Compare SAST results from two different scans.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Sast Results Summary Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/sast-scan-summary**

Overview

These APIs enable you to get aggregated data about SAST vulnerabilities identified in the Projects in your account. If you would like to get detailed info about individual SAST vulnerabilities that were detected, use SAST Results.

> These APIs replace the `/scan-summary` endpoints, which have been deprecated.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Results Summary Endpoints

API	METHOD	ENDPOINT	DESCRIPTION
Retrieve aggregated SAST scan results	GET	/api/sast-scan-summary/aggregate	Get summary of aggregated SAST results for the specified scan. You can

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

API	METHOD	ENDPOINT	DESCRIPTION
			customize the groupings and filters. An AND operator is applied between filters, and an OR operator is applied to multiple values for each filter.
Retrieve aggregated SAST compared results	GET	/api/sast-scan-summary/compare/aggregate	Get summary of aggregated SAST results for the comparison between two scans. You can customize the groupings and filters. An AND operator is applied between filters, and an OR operator is applied to multiple values for each filter.

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Scan Configuration Service

Export

v1.0.0

▸ **{Base_URL}/api/configuration**

Overview

The Checkmarx One Scan Configuration APIs enable users to view and configure global settings for their tenant account as well as settings for specific Checkmarx One projects and scans. Checkmarx One configuration applies the following hierarchy: Tenant -> Project -> Config as Code -> Scan. If there is a conflict between the configuration settings, then the lower level (more specific) takes precidence. However, if a parameter is set at a higher level as 'don't allow override', then the higher level setting is always applied.

Configuration Parameters

The following is a list of config parameters by category:

▸ SAST
▸ SCA
▸ GIT
▸ IaC Security
▸ CONTAINER SECURITY
▸ PLUGINS

Learn more about the configuration options here.

Compliance Filtering

The `scan.config.sast.compliance` parameter is used to filter which compliance standards are included in the scan results.
By default, all supported compliances are returned. If you would like to limit the compliances returned, you can set this parameter and specify an array of compliances to **include**. This filter applies to the results shown in the UI on the Project Overview page as well as to the results returned in the Results Summary API. This can be configured on the tenant level or on the project level for a specific project.
You can enter the value as "All" for all compliances or "[]" for no compliances

▸ Supported compliance standards

Sample Request Body Tenant Level

```
[
  {
    "key": "scan.config.sast.compliance",
    "name": "compliance",
    "category": "sast",
    "originLevel": "Tenant",
    "value": "[\"ASD STIG 4.10\", \"CWE top 25\", \
    "valueType": "Multi",
    "allowOverride": true
  }
]
```

Sample Request Body Project Level

```
[
  {
    "key": "scan.config.sast.compliance",
    "name": "compliance",
    "category": "sast",
    "originLevel": "Project",
    "value": "[\"ASD STIG 4.10\", \"CWE top 25\", \
    "valueType": "Multi",
    "allowOverride": false
  }
]
```

Checkmarx

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Scans Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/scans**

Overview

Checkmarx One scans identify vulnerabilities in your source code. You can specify which scanners to run for each scan (SAST, SCA, IaC Security and API Security). Each scan is run on a project (a logical entity representing a source code repository).

The **scans** endpoints enable you to run scans, get info about scan that have run in your account and check their status. You can also cancel and delete scans.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Workflow

The following are examples of standard workflows for using the scans APIs together with other Checkmarx One APIs to run scans and retrieve scan results.

> You must first create a project in your account either using the the Checkmarx One web portal or using the `POST /api/projects` API before you can run the scan.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

To scan source code from a zip archive:

1. Use `POST /api/projects` to generate a Project ID.
2. Use `POST /api/uploads` to generate an upload link.
3. Use `PUT /{uploadLink}` , specifying the path to your zip archive, to upload your file.
4. Use `POST /api/scans`, specifying the Project ID and upload link, to scan the zip file.
5. Use `GET /api/scans/{scanId}` to check the status of the scan.
6. View the results using `GET /api/results`, specifying the Scan ID.

Alternatively, you can view the results in the Checkmarx One web application (UI), see Scan Results.

To scan from a Git repo:

1. Use `POST /api/projects` to generate a Project ID.
2. Use `POST /api/scans`, specifying the Git repo URL and Project ID to scan the Project.
3. Use `GET /api/scans/{scanId}` to check the status of the scan.
4. View the results using `GET /api/results`, specifying the Scan ID.

Alternatively, you can view the results in the Checkmarx One web application (UI), see Scan Results.

Workflow for API Security Scanner

The API Security Scanner identifies API security risks using two types of data sources: your project's source code and the Swagger file. In order to harness the full capabilities of the API Scanner it is recommended to submit both types of data sources. Analysis of the source code is accomplished by running the `sast` scanner together with the `apiSec` scanner.

To run a comprehensive API Security scan from zip archives:

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

1. Use `POST /api/projects` to generate a Project ID.
2. Use `POST /api/uploads` to generate an upload link for the source code.
3. Use `POST /api/uploads` to generate a second upload link for the Swagger file.
4. Use `PUT /{uploadLink}` , specifying the path to your source code zip archive, to upload your source code file.
5. Use `PUT /{uploadLink}` , specifying the path to your Swagger zip archive, to upload your Swagger file.
6. Use `POST /api/scans`, specifying the following:
    1. The project ID
    2. The `handler` object that includes the property `uploadUrl` with the upload link of your source code
    3. The scanner types, specifying `sast` and `apiSec`
    4. The `apiSec` scanner object including a `value` with a property `uuid` with the upload link for the Swagger file.

▸ Example of the request body

Scans Endpoints Summary

API	METHOD	ENDPOINT	DESCRIPTION
Run a scan	POST	/scans	Run a scan from a zip archive or Git repo.
Retrieve list of scans	GET	/scans	Get a list of scans, with detailed information about each scan. You can limit the results by using pagination

API	METHOD	ENDPOINT	DESCRIPTION
			and/or setting filters.
Retrieve scan details	GET	/scans/{id}	Get details about a specific scan, including the current status of the scan.
Cancel a scan	PATCH	/scans/{id}	Cancel a scan.
Delete a scan	DELETE	/scans/{id}	Delete a scan.
Retrieve scan workflow	GET	/scans/{id}/workflow	Get a detailed workflow, listing the tasks performed for a specific scan.
Retreive scan status summary	GET	/scans/summary	Get a summary of the status of the scans in your account.
Retrieve templates	GET	/scans/templates	Get the list of the available config-as-code template files that are under the dedicated directory.
Retrieve template file	GET	/scans/templates/{file-name}	Get a config-as-code template file.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

API	METHOD	ENDPOINT	DESCRIPTION
			Example: '/templates/config.yml'
Retrieve tags	GET	/scans/tags	Get a list of all scan tags used in your account. Tags can be simple strings or key:value pairs.
Update scan tags	PUT	/scans/{id}/tags	Update tags applied to a scan.
Retrieve values for fields	GET	/scans/fieldValues	Get a list of all values in your tenant account for specific fields (e.g., project name, scan ID etc.).
Run scan recalculation	POST	/scans/recalculate	Run a recalculation of the results for the specified project branch.
Flag a scan as needing recalculation	PUT	/scans/need-recalculation	Flag a project branch for which changes have been made that require a recalculation of the scan results.

Checkmarx

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

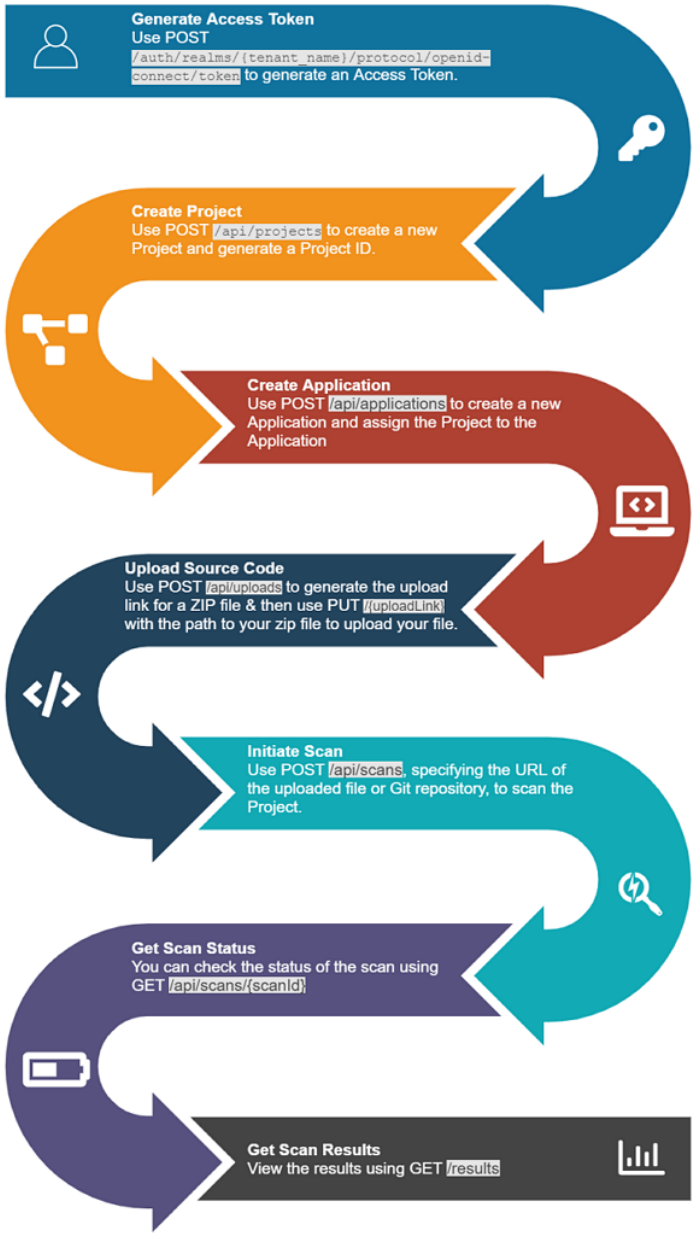
IaC Security Results

Sign in

powered by Stoplight

Scan Workflow

The following diagram represents a standard workflow for creating a new project, running a scan on that project and viewing results. For additional scan workflow details, see here.



Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

SCA Scanner - Export Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/sca/export**

Overview

This API enables you to export reports of the data identified by a Checkmarx SCA scan. This includes detailed info about the open source packages in your project and the risks associated with them. This API can be used to generate the following types of reports:

> **Scan Report** - shows an overview of the security of your project as well as specific vulnerabilities, legal risks, and outdated versions identified by the scan. Scan Reports can be generated in JSON, XML, PDF or CSV format.
>
> **Software Bill of Materials (SBOM)** - SBOMs can be generated in either CycloneDX v1.6 or SPDX v2.2 format. SPDX SBOMs are output in JSON format. For CycloneDX, there is an option to output the data as JSON or XML.
>
> **Remediated Manifest File** - A replacement manifest file that contains the recommended versions for each of your packages. You can download the remediated manifest file and use it to update your project. This feature is currently supported only for npm manifest files and this remediation method is relevant only for direct dependencies.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

> Each API call generates a report in a single format. If you would like to generate reports in multiple formats, then you need to send a separate API call for each report.

What's in a scan report?

The report shows an overview of the security of your project as well as specific vulnerabilities, legal risks, and outdated versions identified by the scan. Reports can be generated in pdf, xml, json, or csv format.

Reports show data divided into the following sections:

> **Packages** - shows info about the open source packages used by your project that contain risks, including: security vulnerabilities, license violations, and outdated versions. The info is separated into a direct packages table and a transitive packages table.
>
> **Vulnerabilities** - shows info about all of the security vulnerabilities that were identified in the open source packages used by your project, including: severity level, CVE references, remediation recommendations etc. Results are shown also for Supply Chain risks (i.e., suspected malicious packages).
>
> **Licenses** - shows the licenses that you have for the packages in your project and the legal risks associated with those packages.
>
> **Policy Violations** - shows any security Policies which the Project violates.

When you generate a report, by default all sections are included in the report. You can specify any sections that you would like to exclude from the report.

What's in an SBOM?

Software Bill of Materials (SBOM), in simple words, is a list of all ingredients (i.e., components) of a software

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

product. Just like you would check the ingredients of a food product before eating it, so too you should know what's in your software before using it. Checkmarx SCA leverages our existing infrastructure for identifying vulnerabilities as well as license and supply chain risks to supplement the standard SBOM info. This creates an SBOM that provides real insight into the risks associated with your 3rd party components. This API enables creation of SBOMs in two popular formats:

> **CycloneDX** - CycloneDX is a lightweight SBOM standard for application security contexts and supply chain component analysis, used primarily for OWASP compliance.
>
> **SPDX** - SPDX is formed with the intent of creating a common data exchange format for information related to software packages for sharing and collection among developers.

Workflow

1. Create a project and run a scan. Take note of the `scanId`.
2. Use `POST /requests`, specifying the `scanId`, and `fileFormat` to generate a report. Take note of the `exportId`.
3. Use `GET /requests`, specifying the `exportId` as a query parameter, to check the status of the report and to get the `fileUrl` for downloading the file.
4. Once the report is complete, use the `fileUrl` to download the report file.

Authentication

Authentication for all Checkmarx One endpoints is done using JWT (JSON Web Token) access token. Access tokens are generated using the Authentication API.

Checkmarx

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

SCA Scanner - Management of Risk REST API

Export

v1.0

COMING SOON
These APIs are not yet fully supported in all environments.

▸ **{Base_URL}/api/sca/management-of-risk**

Overview

These APIs enable you to manage risk by triaging specific vulnerability results. You can also manage packages by ignoring vulnerable packages.

Management of Risk

Checkmarx SCA assigns a profile (predicate) to each risk instance (i.e., vulnerability or Supply Chain (i.e., Suspected Malware) risk), consisting of state, risk score and comments. This enables users to prioritize remediation activity and manage risks throughout the SDLC. You can change the state and risk score for a particular risk instance. A "Risk Instance" is defined as a specific risk that is associated with a particular package. So that, if a particular risk affects several packages that are used in your project, each instance will have its own profile.
For each action, you must add a comment explaining the rational behind the action. You also need to specify one or more projects for which the change will take effect.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

> A unique risk is identified based on: packageName, packageVersion, packageManager and vulerabilityId (or supplyChainRiskId).

Changing the State

Each instance of a risk identified by SCA has a state assigned to it. Possible states are: To Verify, Not Exploitable, Confirmed, Urgent and Proposed Not Exploitable. All new risks are initially marked as To Verify, meaning that the threat from this risk has not yet been verified and needs to be assessed by your appsec team. During the onboarding process (and subsequent result reviews), if you determine that a risk isn't vulnerable to exploitation, e.g., the package isn't used or the source code doesn't call the vulnerable method, then you can mark it as Proposed Not Exploitable or Not Exploitable. If you determine that it does pose a threat, then you can mark it as Confirmed or Urgent.

Changing the Risk Score

Checkmarx intially designates the risk score based on the most recent available version of the NVD CVSS (Common Vulnerability Scoring System) for that vulnerability. You can change the Severity for a particular risk instance according to your team's AppSec analysis.

Management of Packages - Muting/Snoozing Packages

If you determine that a particular package should be used in your project despite the vulnerabilities associated with it, you can mute the package. Vulnerabilities associated with a muted package won't be counted in the risk summary and the vulnerabilities won't be shown in the scan results.There is also an option to mute a package temporarily by marking it as

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

"snooze". When you "snooze" a package, you need to specify the end time until which it will be "snoozed". Once that time passes it will automatically revert back to being "monitored" in subsequent scan results and a new scan will run automatically in order to update the results.
For each action, you must add a comment explaining the rational behind the action. You also need to specify the project for which the change will take effect.

> A unique package is identified based on: packageName, packageVersion and packageManager.

Authentication

Authentication is done using a JWT (JSON Web Token) access token.

Permissions

For Management of Risk, the following permissions are applicable:

- update-result (can update all result states and severities except Not exploitable state)
- update-result-state-not-exploitable (can change to this state only)
- update-result-state-propose-not-exploitable (can change to this state only)
- update-result-states (can change all states except not-exploitable; can’t change the severity)
- update-result-severity (can change only severities)

> For additional details about triage permissions, see here.

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by **Stoplight**

For Management of Packages, the following permissions are applicable:

- update-package-state-mute (can mute packages)
- update-package-state-snooze (can snooze packages)

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Schedules

Export

v1.0.0

▸ **{Base_URL}/api/projects/schedules**

Overview

These APIs are used to create scan schedules, which trigger scans of your Checkmarx One projects based on the specified recurring schedule.

Current Limitations

- The only activities that can be scheduled are scans
- There can only be one project per schedule and one schedule per project (one-to-one)
- Current recurrence options are either once a day or weekly, on one or more specific days of the week
- Currently, only supports triggering the following scanners: sast, sca and kics (IaC Security)
- Maximum 1k schedules allowed per tenant account
- Scheduled scans may be delayed by up to 15 minutes from the specified time, depending on the pending queue

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

Generating an API Key

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management

User Management

Schemas

Access Management (PHASE 2)

Access Management

User Management

Base Roles

Roles and Permissions

Schemas

All Scanners Results

Retrieve scan results - all scanners GET

Schemas

Analytics

Retrieve Analytics KPI data POST

Schemas

API Security Scan Results

Scan

Sign in

powered by Stoplight

Uploads Service REST API

Export

v1.0.0

▸ **{Base_URL}/api/uploads**

Overview

Use this API to upload a zip archive to a preconfigured storage location. You will then be able to run a scan on the source code contained in the zip archive.

> ⓘ If you are scanning the source code directly from a Git repo, then this procedure is not needed. Use `POST /api/scans` to run a scan on the source code in the repo.

Workflow

1. Use `POST /api/uploads` to generate an upload link.
2. Use `PUT /{uploadLink}`, specifying the upload link and path to your ZIP file, to upload your file.
3. Use `POST /api/scans`, specifying the `projectId` and upload link, to scan the ZIP file.
4. Use `GET /api/scans/{scanId}` to check the status of the scan.
5. View the results using `GET /api/results`, specifying the `scanId`. Alternatively, you can view the results in the Checkmarx One web portal (UI), see Scan Results.

Uploads Endpoints Summary

The following is a list of Checkmarx One APIs that relate to Uploads:

API	METHOD	ENDPOINT	DESCRIPTION
Generate upload link	POST	/api/uploads	Generate a pre-signed upload URL to be used for scanning a zip archive. This returns an upload link which is used in `PUT /{uploadLink}` and `POST /api/scans`.
Upload file	PUT	/{uploadLink}	Upload the zip file to Checkmarx One. The Path parameter is the link you generated using `POST /api/uploads`. The Body parameter is the path to the zip archive on your local machine.

Upload File

After generating the uploadLink, use `PUT /{uplpadLink}` to upload the zip file with your source code. Use the upload link (`url`) that that you generated using `POST /api/uploads` as the path parameter, and specify the path to the zip archive as a --data-binary body parameter. The following is an example of a cURL for this API.

```
curl --location --request PUT '"https://<YOUR_UPLOA
--header 'Content-Type: application/zip'\
--header 'Authorization: Bearer <<TOKEN>>'\
--data-binary '@/X:/Projects/SupportProject-master.
```

Home

Checkmarx One API Reference Guide

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by Stoplight

Using SCA APIs

Several of the SCA external (REST) APIs are available for use by Checkmarx One users. Checkmarx One users access these endpoints by replacing the SCA base URL with `<Checkmarx_One_Base_URL>/api/sca`. The following are the APIs that are available and the links to the documentation in our main documentation portal.

Export Service (Reports) - This API is used for generating SBOMs and SCA Scan Reports.

> This API replaces the old `Scan Report and SBOM` APIs, which will be **deprecated on September 30**. For more info, feel free to contact your Technical Account Manager.

Management of Risk - These APIs are used for triaging risk by changing the state of risks and adding comments.

> This API replaces the `IgnoreVulnerability` and `UnignoreVulnerability` APIs which use the old risk-management service. Those APIs will be **deprecated on July 7**. For more info, feel free to contact your Technical Account Manager.

Management of Package Licenses - If you are aware of a license that is relevant for a particular package that was not identified by Checkmarx, you can use this API to add the license manually to the package.

File Analysis - These APIs enable you to upload a supported type of report file for SCA

ABOUT CHECKMARX ONE (REST) APIS

Introduction

API Endpoints Summary

Scan Workflow

Using SCA APIs

Authentication API

API Parity Between Checkmarx One and Leg...

Try it out in Swagger

REST API REFERENCE GUIDE

Access Management (PHASE 1)

Access Management (PHASE 2)

All Scanners Results

Analytics

API Security Scan Results

Application Risk Management

Applications

Audit Trail

Bring Your Own Results (BYOR)

Cloud Connections

Cloud Insights

Code Repository Management

Code Repository Project Conversion

Code Repository Project Import

Custom States

DAST Results

DAST Scans

Feedback Apps

IaC Security Results

Sign in

powered by **Stoplight**

analysis, and retrieve results.

Running scans and Scan Recuaculation for the SCA scanner are done using the relevant Checkmarx One APIs.
Authentication is done using the standard Checkmarx One JWT access token.