CodeArts Check

Service Overview

Issue 01

Date 2025-11-03

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 What Is CodeArts Check?

CodeArts Check is a cloud-based service that checks code. With years of experience in automatic static check and enterprise application, CodeArts Check provides rich check services on code style, common quality, cyber security, and other elements. It also includes professional scan reports, convenient bug handling, and many other efficient, easy-to-use functions for enterprises to effectively improve code quality.

The cloud service and IDE plug-in are two forms of CodeArts Check. In addition, it provides an enhanced package with in-depth security check.

CodeArts Check Functions

Table 1-1 CodeArts Check functions

Function	Description
Coding issue check	Use rule sets to check issues in your own code.
Code security check	Use rule sets to check code security risks and issues.
Code style check	Use rule sets to check whether your code matches the selected style.
Code health score	A comprehensive metric. It is related to the issue impact, quantity, and code quantity. The code health score is automatically calculated.
Issue management	Handle issues found in code checks based on issue descriptions, statuses, check rules, file paths, source code, and fix suggestions.
Cyclomatic complexity	Evaluate code quality risks based on the code cyclomatic complexity report.
NBNC (non-blank non-comment)	Number of valid lines of code (LOC) excluding blank lines and comment lines.

Function	Description
Duplication rate	Evaluate code quality risks based on the duplication rate report.
Scheduled check	Use the function of scheduling code checks every week and every day to balance rest and coding.
Check result notification	After the check is complete, the messages are sent to notify related personnel of the check results so that they can handle issues in time.
Check in multiple languages	Check code in Lua, Rust, Shell, Kotlin, Java, C++, JavaScript, Go, Python, C#, TypeScript, CSS, HTML, and PHP.

IDE Plug-in of CodeArts Check

It is a powerful assistant for developers to protect the code quality.

- Provides industry standard (including Huawei Cloud) check, one-click code style formatting, and automatic code fixing, adhering to the concepts of simplicity, high speed, and real-time monitoring.
- Checks code accurately and efficiently, and builds three-layer protection during coding, merging, and version release with cloud services jointly.
- Displays all built-in lightweight IDE rules that are a subset of cloud rules in the cloud, implements security scan shifting left, and covers 30+ defect categories.
- Supports Java, C, C++, and Python. The IDE plug-in has been rolled out on four mainstream IDE platforms: VSCode IDE, IntelliJ IDEA, CodeArts IDE, and Cloud IDE.

Enhanced Package of CodeArts Check

The security check feature in this package is highly valuable as it thoroughly identifies code security risks and vulnerabilities. It also includes security scenarios that are not found in other packages, such as value errors, encryption issues, and data verification issues. Moreover, it enhances security check and analysis for vulnerability detection items in the industry (such as cross-function check, cross-file check, taint analysis, and semantic analysis).

Currently, the package contains 284 rules (Java: 61; C++: 199; Go: 8; Python: 16).

The enhanced package provides the following items:

- Supports vulnerability check that complies with the taint propagation model, such as command injection, SQL injection, path traversal, and information disclosure.
- Covers common security vulnerability detection items, such as LDAP injection, SQL injection, open redirect, value processing, and information disclosure.
- Checks hard-coded passwords, API keys, and access tokens.

- Checks access key leakage.

After a tenant purchases an enhanced package, the tenant and their IAM accounts can use the package.

The number of parallel tasks of the package is limited. 1 package: 1 task; 2 packages: 2 parallel tasks; *N* (max. 100) packages: *N* (max. 100) parallel tasks. For details about how to purchase, see **Purchasing a Value-Added Feature**.

To purchase the enhanced package, **purchase CodeArts Pro or Enterprise Edition**. The enhanced package cannot be used after the CodeArts package expires.

2 Service Features

2.1 Huawei-developed Code Check Engine

Comprehensively Evaluating the Seven Characteristics of Code Quality

The core of CodeArts Check lies in engine, which helps you efficiently and accurately detect code issues at the early stage of development, and improves development efficiency and product quality.

- Stems from the collaboration of 40+ PhDs in China, 50+ experts in global research centers, and 10+ teachers in China and abroad, continuously improved by 150,000+ Huawei developers, with an average of 50 billion lines of code scanned per day.
- Covers mainstream development languages in the industry, and comprehensively analyzes code in terms of readability, maintainability, security, reliability, testability, efficiency, and portability.
- Integrates years of continuous thinking, exploration, and practices in code quality and trustworthiness improvement, and accumulates various check rules.

2.2 Five Mainstream Industry Standards and Huawei Programming Guidelines

Improved Code Compliance Driven by Mainstream Standards and Guidelines

Quality issues of software products often lead to unacceptable operational risks or high costs. It is important to establish standards for quality detection at the source code level, such as the ISO/IEC 5055 and CERT coding specifications.

- Checks the code quality comprehensively.
- Filters identified coding specification issues, provides knowledge association between specifications and standards, helps you understand the issue type, severity, and details. In this way, you can quickly analyze and make rectification plans as required.

- Complies with ISO 5055, CERT, CWE, OWASP top 10 and CWE/SANS top 25.

2.3 Mainstream Programming Languages

Multiple Programming Languages and 3,000+ Built-in Check Rules for Out-of-the-Box Usability

CodeArts Check supports more than 10 mainstream programming languages, such as Lua, Rust, Shell, Kotlin, Java, C++, JavaScript, Go, Python, C#, TypeScript, CSS, HTML, and PHP., for embedded, web, and mobile application development.

- Built-in open-source tools, self-developed engines, and 3,000+ check rules.
- 10+ rule sets, including those for comprehensive, critical, mobile field, and Huawei codestyle specification check.
- Custom rule sets based on rule library for various check needs

2.4 Tens of Billions of LOC Scanned per Day

Hyperscale Code Check for Large Enterprises

CodeArts Check excels at high-concurrency processing. It provides high-frequency code check services for more than 150,000 Huawei software developers, and daily scheduled check for all code repositories, scanning tens of billions lines of code per day.

- It has a series of high availability (HA) features, such as cross-AZ disaster recovery (DR), cross-region multi-active DR, overload protection, and service dependency and isolation, to provide reliable support for self-detection, self-isolation, and self-recovery of service faults.
- Fluctuating code check demands are well taken care of by the powerful elastic scheduling that allocates resources whenever needed and aims to achieve zero waiting time.

2.5 One-stop Issue Fixing

One-stop Issue Fixing with Higher Efficiency

Developers are tired of tools that are not easy to understand, issue distribution that is time-consuming and labor-intensive, and repeated handling of the same alarm in multiple versions. These lead to difficulties in issue analysis and fixing, affecting the initiative for tool use.

CodeArts Check provides the following capabilities to help developers efficiently and smoothly check code.

- Code defects are detected by line and fixed quickly according to the provided guides, including built-in coding specifications, compliant and noncompliant examples, and fix suggestions. Developers do not need to retrain specifications and fix skills.

- Issue owners are automatically matched based on the code commit information, improving the issue distribution efficiency, and enhancing specification and quality awareness of developers.
- The ignored issues that have been handled are automatically synchronized. Therefore, all same false positives in a repository only need to be handled once.

The preceding capabilities improve the efficiency of issue analysis and fixing during practices.

2.6 Three-Layer (Coding, Merging, and Version Release) Protection

Three-Layer Protection Against Issues to Improve Both Efficiency and Quality

To improve code quality, code check should be integrated into the development phase, including automatic audit during coding and committing, and daily programming specification and code quality check.

- This is recommended by many excellent development modes, such as SDL (security development lifecycle) and DevSecOps.
- CodeArts Check provides various APIs, including those for task creation, setting, scanning, and report analysis. It allows you to seamlessly integrate CodeArts Check into self-built CI/CD or CodeArts. Check data can be displayed in customers' boards, making code quality visible and manageable.
- Flexible task management allows you to set excluded catalogs to avoid invalid scanning. CodeArts Check supports check in hybrid languages, simplifies deployment, and obtains comprehensive quality reports of whole version.

2.7 Enhanced Security Checks

The security check feature in the enhanced package is highly valuable as it thoroughly identifies code security risks and vulnerabilities. It also includes security scenarios that are not found in other packages, such as value errors, encryption issues, and data verification issues. Moreover, it enhances security check and analysis for vulnerability detection items in the industry (such as cross-function check, cross-file check, taint analysis, semantic analysis).

Currently, the package contains 284 rules (Java: 61; C++: 199; Go: 8; Python: 16).

Table 2-1 Differences between the enhanced package and common editions

Item	OWASP Top	CWE Top	Description	Basic	Professional / Enhanced Package
Command injection	Yes	Yes	Attackers use external input to construct system commands and use applications that can invoke system commands to perform unauthorized operations.	Yes	Yes
Path traversal	No	Yes	Attackers use the vulnerabilities of applications to access data or directories without obtaining authorization, thereby causing data leak or tampering.	No	Yes
SQL injection	Yes	Yes	Attackers use pre-defined query statements and construct additional sentences through external input to implement unauthorized operations.	Yes	Yes
Uncontrolled format string	No	Yes	Attackers use the format string vulnerability to control programs and cause information leakage.	No	Yes
Cross-site scripting (XSS) attack	Yes	Yes	Attackers insert malicious code to the links from websites or emails to steal user information.	No	Yes
LDAP injection	Yes	Yes	Unauthorized lightweight directory access protocol (LDAP) queries are generated based on the parameters entered by users to steal user information.	No	Yes
Insecure reflection	Yes	Yes	Attackers use external input to bypass access control paths such as identity authentication and perform unauthorized operations.	No	Yes
Open redirection vulnerability	No	Yes	Attackers change the redirection address to a malicious website to initiate phishing, fraud, or steal user credentials.	No	Yes

Item	OWASP Top	CWE Top	Description	Basic	Professional / Enhanced Package
XPath injection	Yes	Yes	Attackers use external input with malicious query code for privilege escalation.	Yes	Yes
Incorrect array index	No	Yes	Out-of-bounds memory read occurs, which may cause information leakage or system breakdown.	No	Yes
Null pointer dereference	No	Yes	Unpredictable system errors may occur, resulting in system breakdown.	Yes	Yes
Information leakage in logs	No	Yes	Information leakage in server logs and debug logs	No	Yes
Information leakage in messages	No	Yes	Information leakage caused by error messages	Yes	Yes

2.8 Flexible Matching of User Scenarios

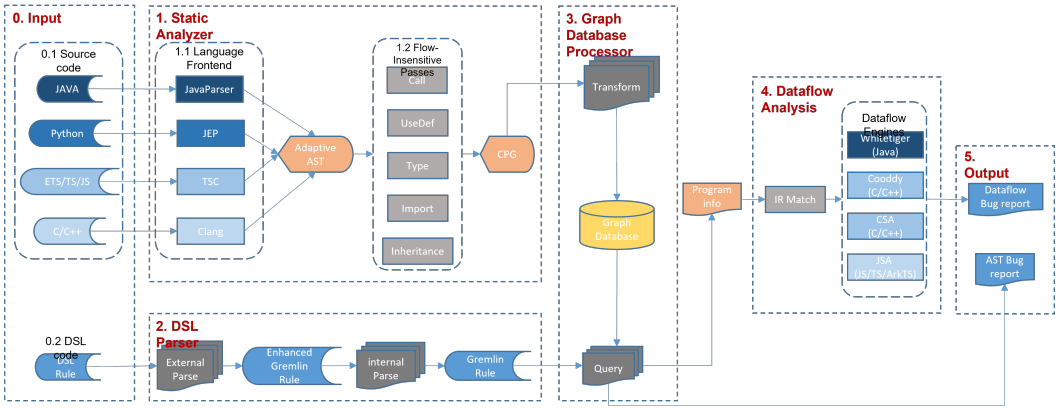
Custom Rules for Various Scenarios

In software development, maintaining code quality presents several challenges: varying team standards (such as naming conventions and comment styles), intricate service-specific logics, and integrating best practices into new frameworks. The built-in rules of code check tools target common issues such as syntax compliance and null pointers but struggle with industry-specific demands, service logics, or customized team needs.

Therefore, Huawei Cloud CodeArts Check allows users to create custom rules for flexible scenario adaptation.

During the rule management phase of CodeArts Check, you can use a domain-specific language to create custom rules tailored to specific issues, add these rules to your custom rule set, and enable them. **Figure 2-1** shows how a domain specific language works.

Figure 2-1 Working Principles of a domain-specific language



3 Advantages

Professional

- Provides more than 3,000 check rules.
- Provides multi-dimensional quality statistics reports, such as quality gates.

Accurate

- Locates reported defects under fix guidance.
- Enables you to customize check rule sets to target at issues that you pay more attention to.

Comprehensive

- Supports multiple mainstream development languages, such as Lua, Rust, Shell, Kotlin, Java, C++, JavaScript, Go, Python, C#, TypeScript, CSS, HTML, and PHP..
- Supports code guideline, security, code repetition rate, and cyclomatic complexity checks.
- Supports CWE, Huawei, OWASP top 10, ISO 5055, SANS top 25, CERT, and MISRA security standards.

Easy to Use

- Checks code in hybrid languages.
- Allows you to run configured tasks by one click, filter issues in batches, and quick handle issues by severity or category.

Code Security Check

Scenarios

- Checks code quality and security issues automatically in the software development phase, supports built-in security guidelines, requirements, and software production workflows, helps enterprises secure software production.
- Provides in-depth code security check capabilities to help government cloud operators and large enterprises manage and control ISV software security quality and build a supply chain security system.

Capabilities

- Analyzes taints and checks across functions and files.
- Checks for top security vulnerabilities, such as injection and access key leakage.
- Supports programming guidelines and is compatible with CWE, Huawei, OWASP top 10, ISO 5055, SANS top 25, CERT, and MISRA standards.

4 Application Scenarios

Web Applications

- Application: Use rule sets of web development languages to check code, provide fix suggestions for developers, such as location, system, language, module, and engine.
- Characteristics: Web services are oriented to the Internet and are vulnerable to DDoS attacks or information leakage.
- Scenario: Accept security levels during Internet service delivery.

Project Quality Control

- Application: Control risks in real time based on the code complexity, repetition rate, and quality score during delivery.
- Characteristics: Project managers agree that they should **secure quality from the front end in daily delivery**. However, there is often no effective tool platform. Currently, most quality work depends on backend testing.
- Scenario: Project managers control iteration delivery quality.

5 Functions

This section describes main functions of CodeArts Check. You can check if a certain function is available in your region on the console.

Code Check

CodeArts Check is a cloud-based service that checks code. The service offers advanced capabilities for checking code style, quality, and cybersecurity risks. It delivers comprehensive quality reports and streamlined issue resolution processes that empower businesses to efficiently manage their code quality and drive success. For details, see **Creating a Task** and **Executing a Task**.

Rule Set Configuration

By default, CodeArts Check supports rule sets in Lua, Rust, Shell, Kotlin, Java, C++, JavaScript, Go, Python, C#, TypeScript, CSS, HTML, and PHP.. Each language corresponds to multiple rule sets.

You can also customize rule sets. After customization, use the custom rule set for a code check task.

For details, see **Configuring a Preset Rule Set** and **Configuring a Custom Rule Set**.

Task Settings

You can modify a task name, switch the default branch, and delete a task.

You can also configure check rule sets, permissions, ignored files, quality gates, execution plans, notifications, logo states, integration and services, execution history, and advanced options. For details, see **Configuring a Task**.

API

CodeArts Check provides Representational State Transfer (REST) style APIs, allowing you to call APIs using HTTP/HTTPS requests to create, execute, delete, query, and stop check tasks, as well as manage bugs and rule sets. For details, see **API Overview**.

6 Security

6.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 6-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 6-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 6-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

6.2 Authentication and Access Control

Authentication

You can access CodeArts Check using its UI, APIs, and SDKs. Regardless of the access mode, your requests are sent through REST APIs provided by CodeArts Check.

CodeArts Check APIs can be accessed only after requests are authenticated. Code check supports two authentication modes:

- Token: Requests are authenticated using tokens. By default, token authentication is required to access the CodeArts Check console.
- AK/SK: Requests are encrypted using an AK/SK. This method is recommended because it provides higher security than token-based authentication.

  For more authentication details and how to obtain tokens and signatures, see **Authentication**.

Access Control

CodeArts Check controls user operations in the following ways:

- Role permission control: Roles and permissions are required for adding, deleting, modifying, and querying check tasks and rule sets, viewing rules, creating, importing, and exporting service orders.
- Fine-grained permission control: Operations such as querying tenant projects, setting project creators, and managing tenant project member lists require fine-grained authorization from IAM.

6.3 Data Protection Technologies

CodeArts Check takes different methods and features to keep data secure and reliable.

Measure	Description	Reference
Transmission encryption (HTTPS)	To secure data transmission, CodeArts Check uses HTTPS.	**Making an API Request**
Personal data protection	CodeArts Check controls access to data and records logs for operations performed on the data.	**Permission Management**
Privacy protection	Sensitive data is encrypted for storage when the database account information of users needs to be stored.	-

Measure	Description	Reference
Data clearing	Sensitive data during task execution is checked and cleared immediately after the check is complete.	-
Data backup	User data can be backed up.	-

6.4 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record management and data traces of CodeArts Check for auditing.

For details about how to enable and configure CTS, see **Enabling CTS**.

6.5 Service Resilience

CodeArts Check uses multi-active stateless cross-AZ deployment and inter-AZ data disaster recovery (DR) to enable service processes to be quickly started and recovered if a fault occurs, ensuring service reliability.

To achieve this, an isomorphic DR cluster is provided for CodeArts Check in a separate AZ. In the event of a natural disaster affecting the production cluster's location, the DR cluster can take over.

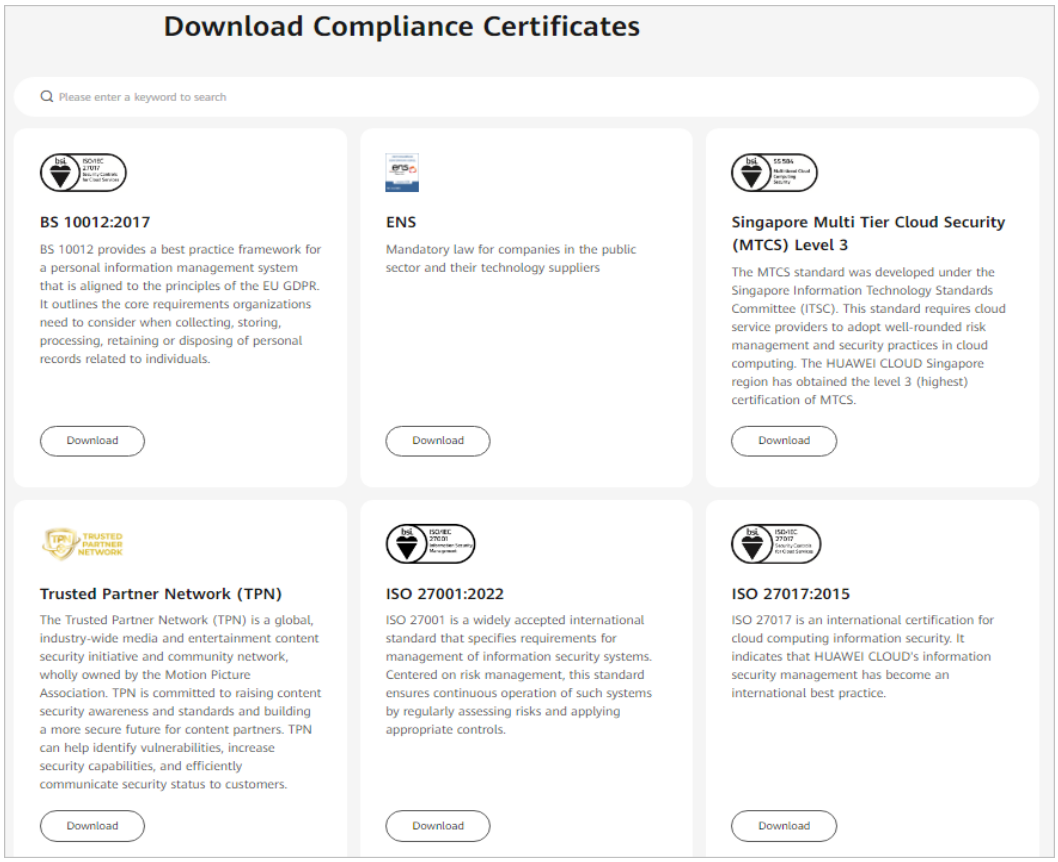
If the production cluster fails due to internal faults, it cannot handle read and write requests. In such cases, the DR cluster assumes the role of the production cluster.

6.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

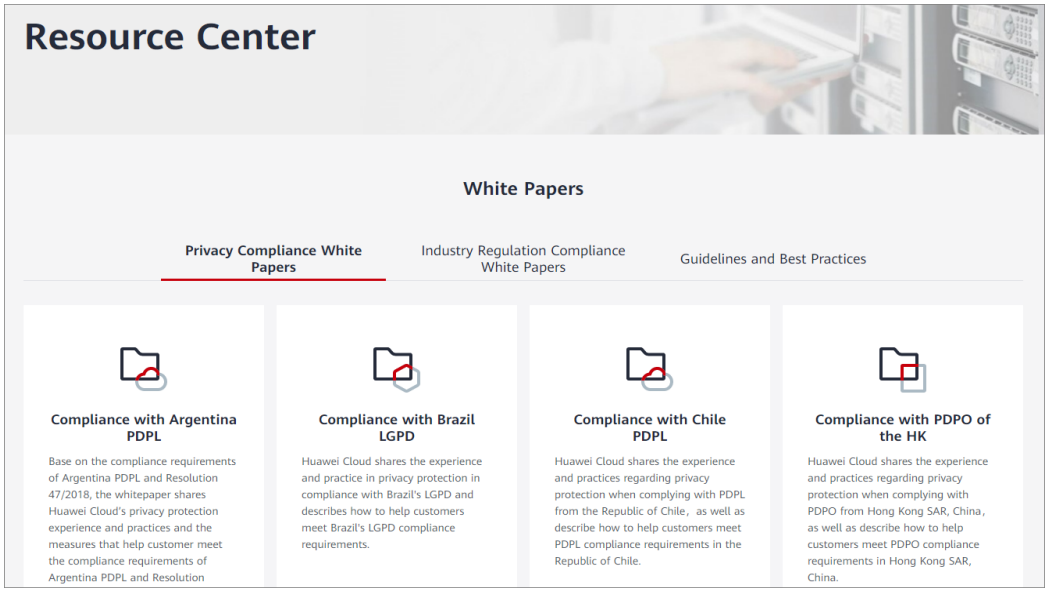
Figure 6-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 6-3 Resource center



7 Constraints

Naming

Item	Description
Task name	Enter 1 to 128 characters: letters, digits, underscores (_), hyphens (-), and periods (.).
Rule set name	Enter 1 to 128 characters: letters, digits, underscores (_), hyphens (-), and periods (.).

Specifications

Item	Limit
Code issues detected at a time	Max. 300,000
Custom rule sets	Max. 1,000
Code check tasks per tenant	Max. 50,000
Duration per code check task	Max.12 hours
Browser	The following browsers are supported: • Chrome: The latest three stable versions are supported and tested. • Firefox: The latest three stable versions are supported and tested. • Microsoft Edge: Windows 10 uses Microsoft Edge by default. The latest three stable versions are supported and tested. **Chrome and Firefox are recommended.**
Resolution	1280 × 1024 or higher is recommended.

8 Glossary

Table 8-1 CodeArts Check glossary

Glossary	Definition
Duplication rate	Formula: Duplication rate = Number of duplicate lines of code/ Number of lines of code ×100% Duplicate lines of code: identical code in multiple locations within a program. Duplicate blocks: Java: 10 consecutive lines; others: 100 consecutive characters in 10 lines.
Rule	Rules are used to check code, including code issue impact and fix suggestions.
Rule set	A set of check rules defined for specific languages to improve code quality.
Cyclomatic complexity	Formula: Average cyclomatic complexity = Loop complexity/ Number of functions A metric used to indicate the code complexity. It has an impact on the code maintainability and testability. A high cyclomatic complexity indicates a high possibility of code errors. Categorization of cyclomatic complexity: ● 1–5: little risk ● 6–10: moderate risk ● 11–20: medium risk ● 21–50: high risk ● 51+: extremely high risk ● NA: not supported language
SDLC	Software development life cycle.
Issue display	A function showing the lines of code where issues are found. Users can view and fix code issues online.

Glossary	Definition
Deferral period	The upgraded check engines may detect new issues. These new issues will be counted if not fixed or masked during a 60-day buffer period.
Execution plan	An automatic triggering mode of check tasks for more flexible, easy to use, and automated check.

