



IBM Cloud Services Agreement

IBM Cloud Service Description: IBM Sterling Supply Chain Visibility

The following is the Service Description for your Order:

1. Cloud Service

The Cloud Service offering including the base offering and available optional features is described below and as selected in an Order Document. The Order Document will consist of the Quotation that is provided and the Proof of Entitlement (PoE) you will receive confirming the start date and term of the Cloud Services and when invoicing will commence.

1.1 IBM Sterling Supply Chain Visibility

IBM Sterling Supply Change Visibility (SCV) tracks and alerts the status of modeled purchase order life cycle events from purchase to payment (SCV-Inbound) and order to cash (SCV-Outbound). You can upload order related information and data, including hypertext markup language files, purchase order related B2B transaction files, and EDI files that are created, provided, or transferred by your or any user authorized by you ("Content").

The Cloud Service includes:

- a. Order Search and Details which provide visibility into order status and activity.
- b. Shipment Search and Details which provide visibility into the status of shipments and supporting activity.
- c. Process modeling which provides the ability to configure multiple order flows for various supply chain paths.
- d. Event management which monitors and provides alerts regarding business processes that are nearing or have exceeded configured tolerances.
- e. Analytics and Reporting which tracks performance and enables fulfillment analysis using key performance indicators (KPI's).

1.2 Optional Features

1.2.1 Vendor Compliance

Vendor Compliance is an add-on to SCV and subject to a separate Service Description, which allows you to collaborate with your suppliers to help manage their fulfillment performance and automate the calculation and issuance of non-compliance financial penalties.

2. Security Description

2.1 Security Policies

IBM maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. We have an information security team. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

2.2 Access Control

Access to client data is allowed only by authorized IBM support representatives according to principles of segregation of duties. IBM staff use two-factor authentication to an intermediate "gateway" management host. All connections are encrypted channels when accessing client data. All access to client data and transfer of data into or out of the hosting environment is logged. WIFI use is prohibited within the IBM data centers that support this Cloud Service.

2.3 Service Integrity & Availability

Modifications to operating systems and application software are governed by IBM's change management process. Changes to firewall rules are also governed by the change management process and are reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus,

intrusion detection, vulnerability scanning, and intrusion prevention) systems are used in all IBM data centers. IBM's data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Physical Security

IBM maintains physical security standards designed to restrict unauthorized physical access to IBM data center. Only limited access points exist into the IBM data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

2.6 Compliance

IBM certifies its privacy practices annually as consistent with the U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. IBM performs industry standard SSAE 16 audits (or their equivalent) annually in production data centers. IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. IBM employees and vendor employees complete workforce security and awareness training annually. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations annually.

3. Service Level Commitment

IBM provides the following availability service level agreement ("SLA") for the IBM Sterling Supply Chain Visibility portion of the Cloud Service. The component to which the SLA applies will be known as the "Service" throughout this section that describes the SLA. You understand that the SLA does not constitute a warranty to you.

3.1 Definitions

- a. "Availability Credit" means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the Service.
- b. "Claim" means a claim submitted by you to IBM pursuant to the SLA that a Service Level has not been met during a Contracted Month.
- c. "Contracted Month" means each full month during the term of the Service measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.
- d. "Downtime" means a period of time during which production system processing for the Service has stopped and your users are unable to use all aspects of the Service for which they have permissions. Downtime does not include the period of time when the Service is not because of:
 - A scheduled outage for the purpose of maintenance.
 - Events or causes beyond IBM's control (e.g., natural disaster, internet outages, etc.).
 - Problems with your applications, equipment or data, or a third party's applications, equipment or data.

- Your failure to adhere to required system configurations and supported platforms for accessing the Service.
 - IBM's compliance with any designs, specifications, or instructions that you provide to IBM or a third party provides to IBM on your behalf.
- e. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.
- f. "Service Level" means the standard set forth below by which IBM measures the level of service it provides in this SLA.

3.2 Availability Credits

- a. To submit a Claim, you must log a Severity 1 support ticket (as defined below in the Technical Support section) for each Event with the IBM technical support help desk, within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the Service. You must provide all necessary detailed information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event.
- b. You must submit your Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month in which the Claim arose.
- c. Availability Credits are based on the duration of the Downtime measured from the time you report that you were first impacted by the Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based on the achieved Service Level during each Contracted Month, as shown in the table below. IBM will not be liable for multiple Availability Credits for the same Event in the same Contracted Month.
- d. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed 10 percent (10%) of one twelfth (1/12th) of the annual charge paid by you to IBM for the Service.

3.3 Service Levels

Availability of Service during a Contracted Month

Availability during a Contracted Month	Availability Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
<99.0%	2%
<97.0%	5%
<95.0%	10%

Availability is calculated as: (a) the total number of minutes in a Contracted Month (minus the minutes of Planned System Downtime), minus (b) the total number of minutes of non-scheduled Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month (minus the minutes of Planned System Downtime), with the resulting fraction expressed as a percentage.

Example: 500 minutes total non-scheduled Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month 200 minutes of Planned System Downtime – 500 minutes Downtime = 42,500 minutes	= 2% Availability Credit for 98.8% Achieved Service Level
<hr style="width: 50%; margin: 0 auto;"/> 43,200 total minutes (-200 minutes of Planned System Downtime) in a 30 day Contracted Month =43,000 minutes	

3.4 Other information about this SLA

This SLA is made available only to IBM's clients and does not apply to claims made by your users, guests, and participants of the Service or to any beta or trial services that IBM provides. The SLA only applies to the production Services, so it does not apply to non-production environments, including but not limited to test, disaster recovery, quality assurance, or development.

4. Entitlement and Billing Information

4.1 Charge Metrics

The Cloud Services are made available under the following charge metric as specified in the Order Document:

Purchase Order Lines is a unit of measure by which the Cloud Service can be obtained. A Purchase Order Line is a record that represents an item being purchased on a purchase order. Sufficient entitlements must be obtained to cover the highest number of Purchase Order Lines processed during the measurement period specified in the Proof of Entitlement or Order Document.

4.2 Charges and Billing

The amount payable for the Cloud Service is specified in the Order Document.

4.3 Partial Month Charges

The partial month charge is a pro-rated daily rate. The partial month charges are calculated based on the remaining days of the partial month starting on the date you are notified by IBM that your access to the Cloud Service offering is available.

4.4 Overage Charges

If your actual usage of the Cloud Service during the measurement period exceeds the entitlement stated on the PoE portion of the Order Document, then you will be invoiced for the overage, as set forth in the Order Document.

4.5 Set-Up

Set-up charges will be either (a) specified in the Order Document, or (b) included in a statement of work that will be issued under the Cloud Services Agreement and agreed upon by the parties.

4.6 On-Demand

On-Demand options will be invoiced in the month the on-demand option is employed by you at the rate set forth in the Order Document.

4.7 Remote Services (Human Based)

Any additional remote services will be invoiced in accordance with the fee contained in a statement of work issued under the Cloud Services Agreement and agreed upon by the parties.

5. Term and Renewal Options

5.1 Term

The term of the Cloud Service begins on the date that IBM notifies you that you have access to the Cloud Service, as described in the Order Document. The PoE portion of the Order Document will confirm the exact date of the start and end of the term. You are permitted to increase your level of use of the Cloud Service during the term by contacting IBM or your IBM Business Partner. We will confirm the increased level of usage in the Order Documents.

5.2 Cloud Services Term Renewal Options

Your Order Document will set forth whether the Cloud Service will renew at the end of the term, by designating the term as one of the following:

5.2.1 Automatic Renewal

If your Order Document states that your renewal is automatic, you may terminate the expiring Cloud Service term by written request, at least ninety (90) days prior to the expiration date of the term that is set forth in the Order Document. If IBM or an IBM Business Partner does not receive such termination notice by the expiration date, the expiring term will be automatically renewed for either a one year term or the same duration as the original term as set forth in the PoE portion of the Order Document.

5.2.2 Continuous Billing

When the Order Document states that your billing is continuous, you will continue to have access to the Cloud Service and will be billed for the usage of the Cloud Service on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, you must provide IBM or your IBM Business Partner with ninety (90) days written notice requesting that your Cloud Service be cancelled.

Upon cancellation of your access, you will be billed for any outstanding access charges through the month in which the cancellation took effect.

5.2.3 Renewal Required

When the Order Document states that your renewal type is “terminate”, the Cloud Service will terminate at the end of the term and your access to the Cloud Service will be removed. To continue to use the Cloud Service beyond the end date, you must place an order with your IBM sales representative or IBM Business Partner to purchase a new subscription term.

6. Technical Support

Technical support for the Cloud Service is available during the subscription period. The standard technical support may be enhanced with the Premium Support Services options, described in Section 1 above.

Regular Phone and Email Support Hours of Operation are as follows:

8:00 a.m. – 11:00 p.m. Eastern Standard Time zone, U.S., Monday – Friday

After Hours Support:

After Hours Support (outside of the regular operating hours stated above) is available only for Severity 1 issues on business days, weekends, and holidays.

Support Hotline: 1-888-558-7509

Email: sterlingsaas_support@us.ibm.com

Support web portal: <https://support.ibmcloud.com>

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Within 1 hour	24x7
2	Significant business impact: A service business feature or function of the service is severely restricted in its use or you are in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours
4	Minimal business impact: An inquiry or non-technical request	Within 1 business day	M-F business hours

7. Description of Integration, Configuration and Customer Services

7.1 Implementation Services

You may obtain implementation services for this Cloud Service as defined by a separate SOW issued under the CSA. Typical implementation steps may include creation of the customer account and on boarding to the application, document integration, document testing, document error track and trace education, solution training, orientation and access to tutorials, solution design documentation, move from test environment to production, and transition to customer support.

8. Additional Information

IBM may copy data to a non-production server within the Cloud Services environment for the exclusive purpose of testing and improving the quality of IBM’s offerings.

8.1 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) you identify as receiving benefit of the Cloud Services. IBM will apply taxes based upon the business address listed when ordering a Cloud Service as the primary benefit location unless you provide additional information to IBM. You are responsible for keeping such information current and providing any changes to IBM.