

IBM Technology

A glowing blue cube is positioned in the center of the image. The cube's faces are covered in a grid of small, glowing blue squares. Two of the visible faces of the cube feature a glowing blue cloud icon. The cube is resting on a complex circuit board with various components and traces. The background is a dark, textured surface with a grid-like pattern.

G-Cloud 15 IBM – IBM Concert Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Contents

TABLE OF CONTENTS	2
OVERVIEW	3
Service Description	3

Service Description

IBM Concert

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Concert Standard

IBM Concert Standard helps Client to understand its application landscape and enabling Client to discover the connections, dependencies, gaps, and opportunities in its application architecture, including by providing generative AI insights. The Cloud Service may be hosted on IBM Cloud or AWS infrastructure, and includes the following features:

- **Vulnerability Management** helps Client with detection, prioritization, and remediation of vulnerabilities risks across Client's specified environments.
- **Resilience** provides Client visibility into application and infrastructure resilience.
- **Certificate Management** helps Client to centralize and automate Client's certificate health monitoring.
- **Concert Workflows** help with integration and orchestration of tools, data, devices, and existing automation across domains.
- **Data App** helps Client to build data visualization.
- **Compliance** provides visibility, continuous monitoring, and automated evidence validation of Client's specified controls, in support of Client's alignment with standards like NIST, SOC 2, and PCI.
- **Power Infrastructure Risk Management** helps Client to unify fragmented operational data from their Power environment to deliver insights, prioritized recommendations, and automated recommended remediation actions for vulnerabilities of its application architecture.

1.1.2 IBM Concert Trial

The IBM Concert Trial provides Client a subset of the IBM Concert Standard plan functionality to be used for evaluation purposes only. The Trial plan automatically expires after 30 days, with no option for renewal, and with no option to initiate a second trial from an account that previously completed a trial. All data is deleted after the trial ends and cannot be recovered. Features from the Standard plan may be offered with limitations. This Trial plan is offered at no charge under the terms of the Preview Cloud Services section defined in the IBM Cloud Services Agreement or an equivalent agreement for Cloud Services.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

<https://www.ibm.com/terms/?id=66D5E192289B467AAD3CA6B8769AB1EB>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of



minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at <https://www.ibm.com/support/pages/node/731179>.

Availability	Credit (% of monthly subscription fee*)
Less than 99.8%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

3.2.1 Optional Support Offerings

Additional support options are available for this Cloud Service. If Client selects to order an optional support offering, the terms defined in the Optional Support Offerings Service Description at <https://www.ibm.com/terms/?id=i126-9789> will apply to the support offering specified in Client's TD.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Resource Unit is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service. For this Cloud Service, the Resources counted are:
 - Base charge – 1 RU per hour per instance
 - Connected Applications
 - Vulnerability Management – 0.1 RU per Connected Application per hour
 - Resilience – 0.025 RU per Connected application per hour
 - Certificates – 1 RU per 100 certificates managed per hour
 - Activated Workflows – 2 RUs per deployed workflow per hour
 - Compliance
 - Enabled IT Compliance Framework – 500 RUs per month
 - Application related to the IT Compliance Framework – 0.5 RU per Application per hour
 - Permanently Activated Power Processor Cores (PPC) - 0.01 RU per PPC per hour

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Definitions

- Connected Application is any uniquely named software program that is separately installable on a computing device, interfaces with, connects to, or otherwise uses the Cloud Service to perform operations or exchange data.

- Certificate is any cryptographic key pair or digital credential, such as an SSL/TLS certificate, code signing certificate, or authentication token, used to secure, encrypt, or validate data and communications.
- Workflows are a logical arrangement of action blocks (pre-defined, reusable set of jobs that perform specific tasks) created using the IBM Concert workflow editor or downloaded from the Automation Library “designed/defined” to perform executable processes.
- Data App is the capability to build data visualization using data sourced from the Cloud Service or other related tools.
- IT Compliance Framework is a structured set of guidelines, policies, and procedures such as SOC 2, ISO 27001, or HIPAA, organizations may follow.
- Processor Core is a functional unit within a computing device that interprets and executes instructions. A Processor Core consists of at least an instruction control unit and one or more arithmetic or logic units. With multi-core technology, each core is considered a Processor Core.

5.2 AI Technology Terms

a. Foundation and Embedding Models

The Cloud Service may include generative AI foundation models and/or embedding models as described in the documentation for the Cloud Service. Each foundation model and embedding model included in the Cloud Service will contain a model information document that provides information about that model (“Model Information”), including details on the model provider. The available IBM-developed foundation models and embedding models are considered part of the IBM Cloud Service.

Client is prohibited from extracting the Model Weights. “Model Weights” means the numerical values associated with the parameters of the training, optimization and performance of a model.

All Client inputs to any model, including by inferencing or prompting the model, and any content provided by Client for further training of a model, including fine-tuning or prompt-tuning are Client Content. Except as set forth in Section (c) (“Output Indemnity”) below, Client is solely responsible for any Output and its subsequent use. IBM does not claim to have ownership rights to the Output that is not based on IBM’s content. Unless separately authorized by Client through a voluntary feedback submission, IBM will not use Client Content or model Output to train the foundation models or embedding models.

b. AI Use Restrictions

This Cloud Service is not intended for use in a high risk context as defined under the EU AI Act or other applicable regulations. If Client chooses to use it in such, please contact ChiefPrivacyOffice@ca.ibm.com.

c. Output IP Indemnity

IBM’s obligation to protect Client against third party claims as set forth in the applicable agreement includes third party claims that the result generated by the Covered Model in response to a Client’s prompt or other input (collectively, “Output”) infringes that third party’s patent or copyright provided that (in addition to the exclusions and Client obligations provided in the relevant base agreement):

- (1) Client has a paid subscription to the Cloud Service or the Covered Model at the time Client generates the Output.
- (2) Client enables all available filters and logging features recommended by IBM in the product documentation or delivered with the Cloud Service or the Covered Model, and Client supplies information collected by such filters and features as requested by IBM in connection with a third party claim;
- (3) If applicable, Client was using a supported version of the Covered Model
- (4) the Output at issue was generated in connection with an Indemnified Use Case;
- (5) Client takes mitigating actions reasonably requested by IBM, which may include ceasing use of the allegedly infringing Output; and

- (6) Client had no reasonable basis to know that the Content or Output was infringing or likely to cause an infringement.

“Covered Model” means: an IBM developed foundation model provided with the Cloud Service (“IBM Covered Model”); and a third-party foundation model provided with the Cloud Service and identified in the product documentation as being an indemnified third party model (“Third Party Covered Model”)

“Indemnified Use Cases” means use within Client’s enterprise of an IBM Cloud Service in a manner consistent with the Cloud Service’s intended use as described in its published documentation.

All other terms of ‘(a) Foundation and Embedding Models’ and of the Liability and Intellectual Property Protection terms in the base agreement remain in effect.

5.3 Preview Features

If a feature is provided to Client as a “preview,” then, (i) the terms related to “preview” in the applicable base agreement apply, (ii) any indemnitees do not apply to this preview, and (iii) in exceptional circumstances it may be necessary for IBM to take steps to suspend or limit unreasonable use by Client of the preview.

5.4 Client Use of Output

Based on the Client’s input, the Cloud Service will provide suggested tasks and other materials as generated outputs. All Client inputs to the Cloud Service and any content provided by Client for further training of the Cloud Service, including fine-tuning or prompt-tuning, are Client Content. IBM does not claim to have ownership rights to any generated output. Client is solely responsible for outputs generated by the Cloud Service and Client should exercise discretion and evaluate whether outputs generated from the model are appropriate for the Client’s environment. Unless separately authorized by the Client through a voluntary feedback submission, IBM will not use the Client Content or generated outputs to train the Cloud Service.





IBM Technology



G-Cloud 15 IBM – IBM Instana Observability SAAS Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Contents

TABLE OF CONTENTS	2
OVERVIEW	3
Service Description	3

Service Description

Instana Observability SaaS

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

Instana Observability SaaS offers an application performance monitoring and observability solution with capabilities to manage the performance of complex and modern cloud-native applications, no matter where they reside.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 Instana Observability SaaS Application Performance Monitoring

An enterprise-grade observability platform for IBM with multi-cloud capabilities that supports cloud native infrastructure and full-stack application visibility.

1.1.2 Instana Observability SaaS Infrastructure Quality Monitoring

Infrastructure Quality Monitoring discovers all relevant components with their configuration and ensures that the data is current. This offering provides monitoring for cloud and infrastructure components, including platforms, databases, custom metrics, cloud services, and container monitoring. This offering excludes application performance management, tracing, end user management, and unbounded analytics.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

Please note that despite offering name differences, the Data Sheets linked below apply equally to the corresponding named Data Sheet as identified in this SD.

Instana Observability SaaS Application Performance Monitoring

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=E7505A603A3611EBA94E77C5BC708D24>

Instana Observability SaaS Infrastructure Quality Monitoring

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=241998003A9411EBA94E77C5BC708D24>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Managed Virtual Server is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications managed by the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Serverless Monitoring

Support for monitoring of serverless function workloads is included in Instana Observability SaaS Application Performance Monitoring. If the environment to be monitored is comprised only of serverless functions, then entitlement for a minimum of 50 Managed Virtual Server (MVS) is required to use serverless functions monitoring.

The serverless functions supported are listed below. Details of the support is described in the IBM Observability by Instana documentation:

- AWS Lambda
- ASW Fargate (AWS ECS with the launch type Fargate)
- Google Cloud Run

5.2 Consuming data from existing, deployed offerings

Support for ingesting IBM Cloud Application Performance Management (Cloud APM) resource metric monitoring data is supported. As a technical preview, support for ingesting IBM Tivoli Monitoring (ITM) and IBM Tivoli Composite Application Manager for Applications (ITCAM for Applications) resource metric monitoring data is also supported. Entitlement for a minimum of 50 Managed Virtual Servers (MVS) of Instana Observability SaaS Application Performance Monitoring is required to use the ingesting capability. Current subscription entitlement to Cloud APM SaaS is required if ingesting data from Cloud APM SaaS. Current Subscription and Support entitlement to on-prem Cloud APM, ITM and ITCAM for Applications is also required. Details of the support is described in the IBM Observability by Instana documentation.

5.3 Enabling Software

The Cloud Service contains the following Enabling Software:

- Host Agent
- Instana Cloud Service Agents



- Instana Serverless Agents
- Instana Web and Mobile Agents



IBM Technology

A glowing blue cube is positioned in the center of the image. The cube's faces are covered in a grid of small, glowing blue squares. Two of the visible faces of the cube feature a glowing blue outline of a cloud. The cube is resting on a complex, dark circuit board with numerous gold-colored pins and traces. The background is a dark, textured surface with a grid-like pattern.

G-Cloud 15

IBM – Noname Advanced API Security as a
Service for IBM

Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Table of Contents

1. Cloud Service	3
1.1 Offerings	3
1.2 Optional Services	3
2. Data Processing and Protection Data Sheets	4
3. Service Levels and Technical Support	4
3.1 Service Level Agreement	4
3.2 Technical Support	4
4. Charges	4
4.1 Charge Metrics	4
5. Additional Terms	5
5.1 Obfuscation of Sensitive Information / PII	5

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or an equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 Noname Advanced API Security as a Service for IBM

This service provides additional security capabilities for APIs, which complement and extend the traditional security capabilities provided by API gateways and web app firewalls. This solution provides posture management, API discovery and behavioral threat detection with AI. Clients can: discover unmanaged APIs, using data classification and context-aware analysis; analyze and assess APIs for misconfigurations, vulnerabilities, and alignment to best practices, with suggested remediation steps; and detect abnormal API traffic in real-time and intelligently block malicious traffic. Each Instance of this Cloud Service includes 50 Managed Endpoints.

1.1.2 Noname Advanced API Security as a Service for IBM Active Testing

While in a test environment, this service ensures that APIs configured are tested for key vulnerabilities. APIs will only be published if they have been cleared of security vulnerabilities. Access to this Cloud Service includes 50 Managed Endpoints.

1.2 Optional Services

1.2.1 Noname Advanced API Security as a Service for IBM Managed Endpoint

This service provides additional Managed Endpoints for Noname Advanced API Security as a Service for IBM.



1.2.2 Noname Advanced API Security as a Service for IBM Active Testing Managed Endpoint

This service provides Clients with the ability to acquire additional Active Testing Managed Endpoint entitlements. For Clients with entitlement to Noname Advanced API Security as a Service for IBM, Client may acquire entitlement to activate the Active Testing capability.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=6229D216258F4A90A94C6191F63E2204>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at <https://www.ibm.com/support/pages/node/731179>.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 98.5%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document. The following charge metrics apply to this Cloud Service:

- Instance is each access to a specific configuration of the Cloud Services.
- Access is the right to access functionality of the Cloud Services.
- Resource Unit is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service. One Resource is a Managed Endpoint. One Managed Endpoint is the combination of a Method, a Host, and a Uniform Resource Identifier (URI). A Method is the operation used to invoke the API, such as an HTTP GET. A Host is defined to be the hostname of the API gateway through which the API is exposed. A URI is the path by which the API is referenced.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Obfuscation of Sensitive Information / PII

The Cloud Service provides the capability to obfuscate sensitive information that it might process, including PII; however, these capabilities are not enabled by default and require configuration by the Client in order to be used. Client agrees to enable the obfuscation capability in the Cloud Service, as required by applicable regulations or laws.



IBM Technology



G-Cloud 15 IBM – IBM Turbonomic SAAS Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Contents

TABLE OF CONTENTS	2
OVERVIEW	3
Service Description	3

Service Description

IBM Turbonomic SaaS

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or an equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Turbonomic

IBM Turbonomic is an AI-powered software that provides analytics which dictate what actions to take to maintain optimal levels of application performance, as well as automate the execution of those actions. IBM Turbonomic monitors performance, makes near-real time decisions, and applies the appropriate resources at the right time to maintain maximum levels of performance.

1.1.2 IBM Turbonomic Cloud Optimization Essentials

IBM Turbonomic Essentials uses AI and automation to match application demands with appropriate cloud resources, such as CPU, memory, storage and network at the lowest cost while maintaining performance and meeting business level objectives. Turbonomic Essentials only supports optimizing applications and entities running in a cloud. An Instance of the Cloud Service is limited to optimizing applications up to an annual cloud spend of \$2 million. Turbonomic Essentials does not support managing applications or entities running in on-premises datacenters and does not support Enterprise Single Sign-On (SSO).

1.1.3 IBM Turbonomic Standard

IBM Turbonomic Standard ("Standard") is a Cloud Service that helps Clients understand and implement cost effective application performance and resource utilization through intelligent automation. This Standard edition only supports optimizing applications running in a cloud. Standard edition is intended for Clients with an annual cloud spend of more than \$2 million. The Standard edition allows Client to use SaaS reporting.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

IBM Turbonomic SaaS on AWS

<https://www.ibm.com/terms/?id=908399A6938347E9892E586A24E4923E>

IBM Turbonomic SaaS on Google Cloud

<https://www.ibm.com/terms/?id=B9ACF8A0517F11ECB7241FF603469C11>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Instance is each access to a specific configuration of the Cloud Services.
- Managed Virtual Server is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications managed by the Cloud Services.
- Monitored Costs are all fees from third-party cloud providers as reflected in Client's billing data including, without limitation, discounted public pricing constructs (e.g., reserved instances, savings plans or analogous products), support, taxes, and prior to the application of any one-time or recurring credits, discounts, refunds, and third-party marketplace fees. In the event Monitored Costs and Cloud Service fees are in different currencies, IBM will convert Monitored Costs at an applicable exchange rate. Each quantity measurement is equal to USD 100,000 Monitored Costs.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

5.2 AI Technology Terms

a. Foundation and Embedding Models

The Cloud Service may include generative AI foundation models and/or embedding models as described in the documentation for the Cloud Service. Each foundation model and embedding model included in the Cloud Service will contain a model information document that provides information about that model ("Model Information"), including details on the model provider. The available IBM-developed foundation models and embedding models are considered part of the IBM Cloud Service.

Client is prohibited from extracting the Model Weights. "Model Weights" means the numerical values associated with the parameters of the training, optimization and performance of a model.

All Client inputs to any model, including by inferencing or prompting the model and any content provided by Client for further training of a model, including fine-tuning or prompt-tuning, are Client Content. Except as set forth in Section (c) ("Output Indemnity") below, Client is solely responsible for

any Outputs and their subsequent use. IBM does not claim to have ownership rights to the Output that is not based on IBM's content, unless the Output is based on IBM's content.

b. **AI Use Restrictions**

This Cloud Service is not intended for use in a high-risk context as defined under applicable regulations, including the EU AI Act.

c. **Output IP Indemnity**

IBM's obligation to protect Client against third party claims as set forth in the applicable agreement includes third party claims that the result generated by the Covered Model in response to a Client's prompt or other input (collectively, "Output") infringes that third party's patent or copyright provided that (in addition to the exclusions and Client obligations provided in the relevant base agreement):

- (1) Client has a paid subscription to the Cloud Service at the time Client generates the Output.
- (2) Client enables all available filters and logging features recommended by IBM in the product documentation or delivered with the Cloud Service or the Covered Model, and Client supplies information collected by such filters and features as requested by IBM in connection with a third party claim;
- (3) If applicable, Client was using a supported version of the Covered Model;
- (4) the Output at issue was generated in connection with an Indemnified Use Case;
- (5) Client takes mitigating actions reasonably requested by IBM, which may include ceasing use of the allegedly infringing Output; and
- (6) Client had no reasonable basis to know that the Content or Output was infringing or likely to cause an infringement.

"Covered Model" means an IBM developed foundation model provided with the Cloud Service ("IBM Covered Model"); and a third-party foundation model provided with the Cloud Service and identified in the product documentation as being an indemnified third party model ("Third Party Covered Model").

"Indemnified Use Cases" means use within Client's enterprise of an IBM Cloud Service in a manner consistent with the Cloud Service's intended use as described in its published documentation or the Model Information or other Transaction Documents (such as license information or program specifications).

All other terms of '(a) Foundation and Embedding Models' and of the Liability and Intellectual Property Protection terms in the base agreement remain in effect.

d. **Previews**

If this generative AI feature is provided to Client as a "preview," then, (i) the terms related to "preview" in the applicable base agreement apply, (ii) any indemnitees do not apply to this preview, and (iii) in exceptional circumstances it may be necessary for IBM to take steps to suspend or limit unreasonable use by Client of the preview.

e. **Feedback**

IBM may provide Client opportunities to voluntarily provide feedback in connection with the use of this generative AI feature, which IBM may use for any purpose, except for training generative AI models.

6. **Overriding Terms**

6.1 **Data Use**

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM may however use Content and other information that results from Content in the course of managing and providing the Cloud Service provided that any data subject to applicable privacy regulations will be rendered into a form that no longer constitutes personal data. IBM will use Client's Content and other information that results from Content, excluding personal data, only for research, testing, and offering development. IBM may share threat identifiers and other security information embedded in Client personal data for threat detection and



IBM Technology



G-Cloud 15
IBM – Verify

Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Service Description

IBM Verify

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

IBM Verify provides Single Sign-On (SSO), multi-factor authentication (MFA) and identity lifecycle controls for internal (workforce) and external (customer) user types. Client Instances have a maximum aggregated transaction rate limit of 400 Transactions per second (TPS) for each Production Instance and 100 TPS for each Non-Production Instance. Scenarios, such as user login and MFA, performed by this service may consist of multiple transactions.

Performance and load testing on any Client instance is permitted only when the Client submits a request via a support ticket at least one week prior to the planned testing period and IBM confirms in writing the test time and planned traffic volume. IBM will advise Client of the maximum aggregated transaction rate limit ("Test Rate Limit") applicable during testing as part of the written confirmation. The Test Rate Limit will not be less than the maximum aggregated transaction rate limit set out in a Transaction Document or Client's maximum growth projections as previously disclosed to IBM for the test. IBM reserves the right to not allow performance and load testing during the requested period, and in such event, IBM will provide an alternative test time. Notwithstanding anything to the contrary in this section, IBM is not obligated to permit the performance and load testing if the parties cannot agree on the parameters or other details pertaining to the proposed performance and load testing.

The data obtained from Client's performance and load testing (collectively "Testing Data") is IBM confidential information (governed under s. 5.3 below) and can only be used for Client's internal testing and validation purposes. Client cannot disclose Testing Data without IBM's prior written consent.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Verify (SaaS)

IBM Verify helps Clients secure user productivity with cloud-delivered, Single Sign-On (SSO), multi-factor authentication, lifecycle management, adaptive authentication, and identity governance under a single part number. This Cloud Service also supports access to thousands of popular cloud service applications, and in-house applications, with hundreds of pre-built templates for faster integration.

- **Single Sign-On**
This Cloud Service delivers Single Sign-On (SSO) via SAML and Open ID Connect (OIDC), Authentication as a Service for cloud-based API authorization, an application launchpad, administrator reporting and an analytics dashboard. This Cloud Service connects users to applications using modern standards-based authentication and federation protocols, including hundreds of connectors to common applications. This Cloud Service includes the IBM Verify Application Gateway software program, as enabling software, to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. It also tightly integrates with the separately licensed, on-premises IBM Verify Identity Access software program.
- **Multi-Factor Authentication**
This Cloud Service provides multi-factor authentication for applications protected by IBM Verify Identity Access on prem, or via direct API invocation, and for other enforcement points including RADIUS clients, Unix/Linux PAM servers and Windows servers to verify identities when accessing a digital service. Second factors enabled by the Cloud Service include, but are not limited to, email, SMS and voice call, time based one-time passwords, and mobile biometrics powered by the IBM Verify Authenticator App for Mobile (iOS and Android). The SMS and voice call factors are not included as part of the Cloud Service and can be added by obtaining the IBM Verify SMS and Voice One-time Password optional add-on service. This Cloud Service integrates with the separately

licensed, on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications.

- **Adaptive Access**

This Cloud Service uses a combination of Threat Intelligence and Artificial Intelligence (AI) to help organizations accurately differentiate between malicious and true users, when user is trying to access an application protected by the service. The service consumes insights on users, their devices, and behavior patterns to determine in real-time a risk-mitigating action: allow access, enforce authentication, or block access. The service uses hundreds of data points and contextual information collected from the end-user's device to fingerprint the device and calculate a holistic risk level of the session. Risk-based access rules defined in the access policy uses the session risk level with additional parameters for determining the system's action. This service is tightly connected with the Verify administrator reports, access policy rules editor and the multi-factor authentication service.

- **Lifecycle Management and Governance**

This Cloud Service tightly integrates with the separately licensed, on-premises IBM Verify Identity Governance Enterprise software program, to provide a solution for Clients to support their line-of-business demands for identity governance spanning both their on-premises and cloud applications. This Cloud Service provides organizations advanced identity lifecycle management capabilities within the cloud that includes account synchronization, application access request workflow, access certification, provisioning to cloud and on-premises applications.

1.1.2 IBM Verify Dedicated

IBM Verify Dedicated provides a highly available cloud instance for workforce, consumer, citizen, and classroom enterprises that provides single sign on, multi-factor authentication and lifecycle management with dedicated transaction rates that exceed the maximum aggregated transaction rate limit of 400 TPS for Production Instances, with the dedicated transaction rate to be specified in a transaction document.

1.1.3 IBM Verify Hybrid

This Cloud Service delivers flexibility through its entitlement to both on-premises and cloud solutions to let organizations approach hybrid deployments and cloud migration appropriately.

Verify Hybrid is a Dual Entitlement offering that provides simultaneous use of the Cloud Services and use of the identified Programs in a Client computing environment. The identified Programs are IBM Verify Identity Access Enterprise Edition, IBM Verify Identity Governance Enterprise Edition and IBM Directory Suite Enterprise Edition which may be used simultaneously with IBM Verify (SaaS) Single Sign-On, Multi-Factor Authentication and Lifecycle Management and Governance Cloud Services.

1.1.4 IBM Cloud Identity Connect

This Cloud Service delivers Single Sign-On (SSO) and Open ID Connect (OIDC), Authentication as a Service for cloud-based API authorization, an application launchpad, administrator reporting and an analytics dashboard. This Cloud Service connects users to applications using modern standards-based authentication and federation protocols, including hundreds of connectors to common applications. This Cloud Service tightly integrates with the on-premises IBM Verify Identity Access software program, which is included as enabling software, to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications.

1.1.5 IBM Cloud Identity Connect for ISAM

This Cloud Service tightly integrates with the on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. This Cloud Service requires the Client to have an active Software Subscription and Support (S&S) entitlement for the IBM Verify Identity Access program, and the S&S must remain active for the duration of Client's Cloud Service subscription. Client's entitlement to this Cloud Service must be equivalent to the Client's on-premises IBM Verify Identity Access license entitlement. Discontinuation of Client's S&S will also discontinue this Cloud Service. Access to the enabling software defined in Section 5.1 is not included with this Cloud Service.

1.1.6 IBM Cloud Identity Essentials

This Cloud Service provides Clients with Single Sign-On (SSO) and Multi-Factor Authentication (MFA) capabilities to the various IBM and public cloud applications they are using. This Cloud Service can be coupled with IBM MaaS360 to provide additional levels of security controls, such as conditional access.

1.1.7 IBM Cloud Identity Verify

This Cloud Service provides multi-factor authentication for applications protected by Cloud Identity Connect, or via direct API invocation, and for other enforcement points including RADIUS clients, Unix/Linux PAM servers and Windows servers in order to verify their identities when accessing a digital service. This includes mechanisms such as email, SMS and time based (software token) one-time passwords, and push based mobile biometrics authentication powered by IBM Verify. This Cloud Service integrates with the on-premises IBM Verify Identity Access software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. It is available standalone, or to compliment Cloud Identity Connect, Cloud Identity Connect for IBM Verify Identity Access and Cloud Identity Essentials.

1.1.8 IBM Cloud Identity Govern

This Cloud Service tightly integrates with the separately licensed, on-premises IBM Verify Identity Governance Enterprise software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premises and cloud applications. This Cloud Service provides organizations advanced identity lifecycle management capabilities within the cloud that includes application access request workflow.

1.1.9 IBM Cloud Identity Connect and Verify

This Cloud Service provides Client with the functionality of IBM Cloud Identity Connect and IBM Cloud Identity Verify as a single offering.

1.1.10 IBM Cloud Identity Adaptive Access

This Cloud Service uses Artificial Intelligence (AI)-powered contextual insights on users, their devices, and behavior patterns to help organizations enforce the correct authentication policies.

1.1.11 IBM Cloud Identity Connect Verify and Govern

This Cloud Service provides Client with the functionality of IBM Cloud Identity Connect, IBM Cloud Identity Verify, and IBM Cloud Identity Govern as a single offering.

1.2 Optional Services

1.2.1 IBM Verify Non-Production

IBM Verify Non-Production Environment on Cloud is a separate instance of the IBM Verify platform that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces. This Cloud Service has the option to include an availability service level agreement (SLA), subject to the terms in Section 3 Service Levels and Technical Support. This Cloud Service has a maximum aggregated transaction rate limit of 100 Transactions per second.

1.2.2 IBM Verify Vanity Domain

A vanity domain (one domain or sub-domain) allows for the Client to use a domain owned by, and more relevant to their organization, rather than using the default tenant domain that is provided by the platform out of the box. An SSL certificate will be maintained by IBM for the single domain and will be renewed on an annual basis.

1.2.3 IBM Verify Hosted Application Gateway

The application gateway provides an IBM managed and hosted light-weight appliance for Clients looking to support non-standard, or legacy, based single sign-on mechanisms. These mechanisms include LTPA and HTTP header-based authentication. Ongoing monitoring and maintenance are managed by IBM.

1.2.4 IBM Verify SMS and Voice One-time Password

This optional service provides voice call and SMS delivered one-time passwords, as a second factor authentication mechanism.

1.2.5 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud is a separate instance of the IBM Cloud Identity platform that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces. This Cloud Service has the option to include an availability service level agreement (SLA), subject to the terms in Section 3 Service Levels and Technical Support. This Cloud Service has a maximum aggregated transaction rate limit of 100 Transactions per second.

1.2.6 IBM Cloud Identity Vanity Domain

A vanity domain (one domain) allows for the Client to use a domain owned by, and more relevant to their organization, rather than using the default tenant domain that is provided by the platform out of the box. An SSL certificate will be maintained by IBM for this domain and will be renewed on an annual basis.

1.2.7 IBM Cloud Identity Application Gateway Hosted

The application gateway provides an IBM managed and hosted light-weight appliance for Clients looking to support non-standard, or legacy, based authentication mechanisms. These mechanisms include LTPA and HTTP header-based authentication. Ongoing monitoring and maintenance is managed by IBM.

1.3 Acceleration Services

Acceleration Services are expert services, as described in this SD, and are provided remotely to Client. For the purpose of this SD, if Client's base agreement references Cloud Services, then all such references apply to Acceleration Services, as applicable.

These remotely delivered services, for purposes of this Service Description, are referred to as the "Service". The Service provides Client access to subject matter expertise (SME) resources and supporting information for the IBM Verify product family.

Through coaching, mentoring and knowledge transfer, the Service is designed to aid Client in the construction and management of business solutions built using Verify Software products. Client must have an active entitlement to Verify virtual or physical appliance product. The Service is applicable to generally available Verify products, not "deprecated", "experimental" or "beta" products.

A list of supported product families can be viewed at the following webpage:

<https://www.ibm.com/security/security-expert-labs>

The Service is delivered in English language only, unless mutually agreed with Client.

The Service does not replace the role of the IBM Support organization which should continue to be the point of contact for technical problems.

1.3.1 IBM Expert Labs Assess Verify (10 hours)

This Service provides up to ten (10) hours in one or more of the following focus areas:

- A trusted advisor to help organizations achieve benefits and value from their Verify investment.
- Enhancements to the organization's capability to help develop a broad range of skills that span full process implementation of a Verify subscription.
- Regular check points during the implementation project to address challenges or architectural design decisions.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

IBM Security Verify:

www.ibm.com/terms/?id=735E5650E26711E69CCD7F0385C6524D

During service provisioning of IBM Verify, Client may select preferred region for Hosting Processing Activities from this list:

- Australia
- Canada

- Europe Region
- Japan
- United States

IBM Common Service Mesh (IBM Covered Model):

<https://www.ibm.com/terms/?id=503882A8505045C1802C09E0B315F6CC>

IBM Common Service Mesh is a common service that enables the generative AI functionality contained in the Cloud Service.

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month, and is specific to the region impacted and number of subscribed users in the region. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.99%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.1.1 Other Information about this SLA

During the first sixty (60) days of Client's term ("Burn-In Period"), Client shall not be entitled to any credit due to failure of the Cloud Service environment to achieve the minimum 99.99% Uptime Percentage under this Agreement. If prior-to or during the Burn-In Period IBM identifies existing Client configurations, policies, data, or code ("Pre-Existing Components") intended to be migrated to the Cloud Service that would prohibit the Cloud Service from successfully achieving the Uptime Percentage within this Agreement, IBM shall reserve the right to notify Client of such Pre-Existing Components and exempt them at IBM's sole discretion, from the provisions of the SLA. Should IBM notify Client of any exempted Pre-Existing Components, IBM shall be responsible for presenting to Client a remediation plan, to the extent possible, which enables such exempted components to meet the Uptime Percentage of this Agreement. Client shall be solely responsible for the cost of any such remediation unless otherwise agreed-upon by both parties.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

3.2.1 Optional Support Offerings

Additional support options are available for this Cloud Service. If Client selects to order an optional support offering, the terms defined in the Optional Support Offerings Service Description at <https://www.ibm.com/terms/?id=i126-9789> will apply to the support offering specified in Client's TD.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Services.

- For Verify SMS and Voice One-time Password, an Event is a voice call or SMS delivered one-time password. SMS sent for user management operations are not considered in this calculation.
- For IBM Verify (SaaS), IBM Verify Dedicated, IBM Verify Hybrid, and Cloud Identity Connect, an Event is an http request against the Cloud Service.
- For IBM Verify (SaaS), IBM Verify Dedicated, IBM Verify Hybrid, and Cloud Identity Verify, an Event is any multi-factor method being invoked via the Cloud Service.
- Authorized User is a unique user authorized to access to the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.
- Employee is a unique person employed in or otherwise paid by or acting on behalf of Client's Enterprise, whether or not given access to the Cloud Services.
- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
- Instance is each access to specific configuration of the Cloud Services.
- Resource Unit is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service.
 - Graduated Tiers is a cumulative pricing model, the Client is required to step through the tiers by purchasing the quantities in Tier 1, then Tier 2, etc.
 - Monthly Active User is a unique person who accesses the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means measured monthly.
 - Usage of each functional capability requires the specified number of Resource Unit entitlements to this Cloud Service subscription:

Maximum Monthly Active Users:

Graduated Tier	Maximum Monthly Active Users	Functional Capability in weighted Resource Units required per Active User		
		Single Sign-On	Multi-factor Authentication	Adaptive Access
1	500	0.1	0.1	0.1
2	5,000	0.08	0.08	0.08
3	10,000	0.06	0.06	0.06
4	100,000	0.008	0.008	0.008
5	500,000	0.0025	0.0025	0.0025
6	1,000,000	0.002	0.002	0.002
7	5,000,000	0.0015	0.0015	0.0015
8	10,000,000	0.0015	0.0015	0.0015
9	50,000,000	0.001	0.001	0.001
10	999,999,999	0.0005	0.0005	0.0005

Maximum Total Users:

Graduated Tier	Maximum Total Users	Functional Capability in weighted Resource Units required per Total User
		Lifecycle Management and Governance
1	500	0.29
2	5,000	0.075

		Functional Capability in weighted Resource Units required per Total User
Graduated Tier	Maximum Total Users	Lifecycle Management and Governance
3	10,000	0.05
4	100,000	0.005
5	500,000	0.002
6	1,000,000	0.001
7	5,000,000	0.0005
8	10,000,000	0.0002
9	50,000,000	0.0001
10	999,999,999	0.0001

Note: All calculations will be rounded up to a whole number.

4.2 Remote Services Charges

A remote service will expire 90 days from purchase regardless of whether the remote service has been used.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Enabling Software

Enabling Software is provided to Client under the following terms:

Enabling Software	Applicable License Terms (if any)
IBM Verify Antenna	https://www.ibm.com/terms/?id=L-RVFP-9ZCQEW
IBM Verify Bridge	https://www.ibm.com/terms/?id=L-DDVG-SXWNMK
IBM Verify Authenticator App for Mobile	https://www.ibm.com/terms/?id=i125-5589
IBM Verify SDK (iOS)	
IBM Verify SDK (Android)	
IBM Verify SDK for JavaScript	
IBM Verify Bridge for Directory Sync	https://www.ibm.com/terms/?id=L-PLRN-678SAZ
IBM Application Gateway	https://www.ibm.com/terms/?id=L-SVRZ-CLFGHV
IBM Verify Gateway for Windows Login	https://www.ibm.com/terms/?id=L-ZALG-B7F9GL
IBM Verify Gateway for AIX PAM	https://www.ibm.com/terms/?id=L-LKMK-TRZC7Z
IBM Verify Gateway for Linux PAM	https://www.ibm.com/terms/?id=L-ELDJ-JK7M9F
IBM Verify Gateway for RADIUS	https://www.ibm.com/terms/?id=L-CNEM-X5UCHT
IBM Verify Identity Governance Infrastructure Adapters (Class A)	https://www.ibm.com/terms/?id=L-UDUG-X3CFM6
IBM Verify Identity Governance Application Adapters (Class B)	https://www.ibm.com/terms/?id=L-NHKM-NPLA8A
IBM Verify Directory Integrator	https://www.ibm.com/terms/?id=L-CNWH-KN4EVN

The following enabling software may only be used with the IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify, and IBM Cloud Identity Connect Verify and Govern Cloud Services:

Enabling Software	Applicable License Terms (if any)
-------------------	-----------------------------------

IBM Verify Identity Access Virtual Enterprise Edition	Container: https://www.ibm.com/terms/?id=L-UGYM-JBJAL3 Software: https://www.ibm.com/terms/?id=L-MAZZ-49RVWE
---	---

5.2 Client Reference

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

5.3 Confidentiality

Testing Data, as well as any information or materials created, in any form or format, using the Testing Data, or any feedback about the Testing Data Client provides to IBM in any form or format, is considered to be IBM confidential information ("Information").

Client will use the Information only for the purpose set forth in this Service Description and for the benefit of IBM, and will use reasonable care to avoid disclosure of the Information other than to Client's:

- a. employees and employees of any legal entity that it controls, controls it, or with which it is under common control, who have a need to know. Control means to own or control, directly or indirectly, over 50% of voting shares; or
- b. subcontractors, financial and legal advisors, and then only to those who have a need to know.

Before disclosure to any party in (a) or (b), Client will have a written agreement with such party sufficient to require that party to treat Information substantially the same as described in this Agreement.

If required to disclose Information by law or court order, Client will endeavor to give IBM prompt notice to allow IBM a reasonable opportunity to obtain a protective order.

Client may disclose, disseminate, and use Information that is already in its possession without obligation of confidentiality, developed independently, obtained from a source other than IBM without obligation of confidentiality, publicly available when received or subsequently becomes publicly available through no fault of the Client, or disclosed by IBM to another without obligation of confidentiality. Client's obligations with respect to the Information will continue for a period of five years from its disclosure.

Notwithstanding the existence of any confidentiality or other agreement Client may have with IBM pertaining to confidential information, the preceding paragraphs govern with respect to the Testing Data.

5.4 Output IP Indemnity

IBM's obligation to protect Client against third party claims as set forth in the Cloud Services Agreement includes third party claims that the result generated by the Covered Model in response to a Client's prompt or other input (collectively, "Output") infringes that third party's patent or copyright provided that (in addition to the exclusions and Client obligations provided in the relevant base agreement):

- a. Client has a paid subscription to the Cloud Service at the time Client generates the Output.
- b. Client enables all available filters and logging features recommended by IBM in the product documentation or delivered with the Covered Model or in the Cloud Service, and Client supplies information collected by such filters and features as requested by IBM in connection with a third party claim;
- c. the Output at issue was generated in connection with an Indemnified Use Case;
- d. Client takes mitigating actions reasonably requested by IBM, which may include ceasing use of the allegedly infringing Output; and
- e. Client had no reasonable basis to know that the Content or Output was infringing or likely to cause an infringement.

"Covered Model" means an IBM developed generative model provided with the Cloud Service ("IBM Covered Model").

"Indemnified Use Cases" means use within Client's enterprise (a) of an IBM Covered Model in a manner consistent with such model's intended use as described in its published Model Information or other Transaction Documents (such as license information or program specifications).

Except for IBM's obligation set out above relating to third party claims, Client is solely responsible for Output generated by the Cloud Service.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM may however use Content and other information that result from Content as part of the Cloud Service for the purpose of managing and improving the Cloud Service. IBM may share threat identifiers and other security information embedded in Client personal data for threat detection and protection.

IBM Technology



G-Cloud 15 IBM – Verify Identity Protection Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Service Description

IBM Verify Identity Protection

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

IBM Verify Identity Protection is a cloud-based service that helps to protect the identity fabric of an organization against identity-focused attacks, by providing end-to-end visibility into security gaps and potentially risky user accesses across identity systems in a hybrid-cloud environment. The identity fabric consists of all cloud and local systems used in managing human and non-human identities and their access to the organization's resources, including user directories, application gateways, identity access providers and entitlement management systems.

The service employs both identity security posture management (ISPM) and identity threat detection and response (ITDR) methodologies to identify and alert on system blind spots, misconfigurations, and access-based attacks as they unfold.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Verify Identity Protection

This Cloud Service helps organizations identify and remediate identity posture issues and threats for managed and unmanaged identities across multi-cloud, SaaS and on-premise environments. The solution helps provide visibility, contextual observability, end-to-end identity security posture management (ISPM) functionality, and real-time identity threat detection and response (ITDR) capabilities. It contains over 70 risk logics ("playbooks") for detecting various identity risk postures such as absence of multifactor authentication (MFA), bypassing of critical security controls like Zero Trust Network Access (ZTNA), or the use of shadow identity systems such as unapproved password managers.

Available ISPM features include, but are not limited to:

- Identity activity observability, for all service and human accounts
- Identity & access blind spots
- Identity infrastructure exposures

Available ITDR features include, but are not limited to:

- Identity infrastructure threats,
- Suspicious identity accesses
- Threat investigations and response with identity context

Entitlements for the Cloud Service are calculated based on Entity IDs across the company which will be tracked on a monthly basis.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

<https://www.ibm.com/terms/?id=6EAFCBAC38014EAFA3BABF75AC43A7FE>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total

number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at <https://www.ibm.com/support/pages/node/731179>.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Entity ID is a unique identifier for any entity identified within the Cloud Services.
For the purposes of this Cloud Service, an Entity ID is defined as a human user accessing the systems of the company, for example, an employee, a contract, or a business partner. Each Entity ID may have up to 10 assigned identities, such as user accounts or service accounts. In the event an Entity ID has more than 10 assigned identities, Client must purchase additional Entity ID entitlements to cover the additional identities.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Enabling Software

The Cloud Service contains the following Enabling Software:

- Network Access Flow Collector
- Directory Collector

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM and IBM's supplier Authmind, Inc. may however use Content and other information that result from Content as part of the Cloud Service for the purpose of managing and improving the Cloud Service and other Cloud Services that utilize the same underlying technology. IBM may share (including to IBM's supplier Authmind Inc.) threat identifiers and other security information embedded in Client personal data for threat detection and protection purposes. The provisions of this section will survive the termination or expiration of the transaction.

IBM Technology



G-Cloud 15 IBM – Verify Privilege Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Service Description

IBM Security Verify Privilege

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Security Verify Privilege Cloud Service consists of the following 4 offerings, each includes one production environment:

IBM Security Verify Privilege Vault

Privilege Vault is a solution that allows Clients to:

- Establish a Secure Vault – Store privileged credentials in an encrypted centralized vault.
- Discover Privileges – Identify all services, applications, administrators, and root accounts.
- Manage Secrets – Provision & deprovision, ensure password complexity and rotate credentials.
- Delegate Access – Set up RBAC, workflow for access requests and approvals for third parties.
- Control Sessions – Implement session launching, proxies, monitoring and recording.

IBM Security Verify Privilege Manager

Privilege Manager is a solution that allows Clients to:

- Deploy a Single Agent – Discover application usage with admin rights, even on non-domain machines.
- Define Flexible Policies – Elevate, allow, deny, and restrict applications in just a few clicks with a policy wizard.
- Discover and Inventory – Find the most important applications that need to be addressed by Client's policies.
- Manage and Remove Local Admin Rights – Create rules to permanently define local group membership and automatically rotate credentials for non-human privileged accounts.
- Elevate Applications – Allow trusted applications to run, while maintaining a least privilege model.
- Improve IT Productivity – Automate bulk or repeatable operations. Reduce help desk tickets.
- Support Business Users – Allow people to access apps and systems they need automatically.

IBM Security Verify Privilege DevOps Vault

Privilege DevOps Vault helps Clients to protect privileges and reduce secret sprawl across cloud attack surface by:

- Establish a Secure DevOps Vault – Store privileged credentials in an encrypted, centralized SaaS-based vault in minutes.
- Centralize Secrets – Eliminate disparate vault instances with a platform-agnostic solution that enforces secure secrets access and provides complete auditing.
- Automate and Scale – Choose Client's automated interface (CLI and API) built for the speed and scale of DevOps pipelines and RPA deployments and tools.
- Manage Secrets for IaaS – Remove standing access to critical infrastructure with dynamic secrets for AWS, Azure and Google Cloud Platform.
- Issue Certificates – Issue X.509 and SSH certificates, which enables automated certificate signing and distribution.

IBM Security Verify Privilege Account Lifecycle Manager

IBM Security Verify Privilege Account Lifecycle Manager helps Clients automate the service account lifecycle. Some capabilities include:

- Discover Hidden Accounts – Find service accounts and understand their purpose.
- Establish Workflows – Delegate ownership with role-based permissions.

- Provision Accounts – Set up accounts seamlessly and automatically.
- Enforce Governance – Establish ownership and accountability for accounts.
- Decommission Accounts – Remove accounts without causing disruption.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Security Verify Privilege Vault for Business Users

IBM Security Verify Privilege Vault for Business Users offering is used to manage accounts not considered Privilege. These accounts can include individual or team application accounts and credentials. Examples of accounts not considered Privilege include email login, social media password, or productivity software credentials.

Privilege Vault provides the following entitlement per tenant:

- Storage of 4 TB
- Single Sign On and Multi Factor Authentication from the IBM Security Verify offering.
- A limit of 10,000 secrets, otherwise known as privileged credentials.
- 10 IBM Security Verify Privilege Vault Sites.
 - Each IBM Security Verify Privilege Vault Site includes 10 IBM Security Verify Privilege Vault Engines. Engine is a Windows Service which does discovery, password changing, and heartbeat. Each Engine belongs to a Site. Sites are logical groupings of work items. Every managed secret will have one Site. The Engine pulls work items from the Site for processing.

1.1.2 IBM Security Verify Privilege Vault for Privilege Users

IBM Security Verify Privilege Vault for Privilege Users offering is used to manage Privilege accounts; such as database server credentials, security appliance passwords, Cloud Service root keys, or any other IT infrastructure credentials.

Privilege Vault provides the following entitlement per tenant:

- Storage of 4 TB
- Single Sign On and Multi Factor Authentication from the IBM Security Verify offering.
- A limit of 10,000 secrets, otherwise known as privileged credentials.
- 10 IBM Security Verify Privilege Vault Sites.
 - Each IBM Security Verify Privilege Vault Site includes 10 IBM Security Verify Privilege Vault Engines. Engine is a Windows Service which does discovery, password changing, and heartbeat. Each Engine belongs to a Site. Sites are logical groupings of work items. Every managed secret will have one Site. The Engine pulls work items from the Site for processing.

1.1.3 IBM Security Verify Privilege Manager for Managed Client

The number of entitlements required for IBM Security Verify Privilege Manager for Managed Client is determined by the number of individual endpoint computers that the endpoint agent can be actively installed on.

1.1.4 IBM Security Verify Privilege Manager for Managed Server

The number of entitlements required for IBM Security Verify Privilege Manager for Managed Server is determined by the number of servers that the endpoint agent can be actively installed on.

1.1.5 IBM Security Verify Privilege DevOps Vault Production Subscription per Record

The number of entitlements required for IBM Security Verify Privilege DevOps Vault Production is determined by the number of passwords, encryption keys, digital certificates or other credentials stored in the production instance of IBM Security Verify Privilege DevOps Vault.

1.1.6 IBM Security Verify Privilege Account Lifecycle Manager for Users

The IBM Security Verify Privilege Account Lifecycle Manager offering is used to manage and automate the service account lifecycle.

Privilege Account Lifecycle Manager provides the following entitlement per tenant:

- One Account Lifecycle Manager Engine. This engine is a Windows Service that runs on the Client's hardware. It manages interactions between the Account Lifecycle Manager Cloud Service and the Client's Microsoft Active Directory.

1.1.7 IBM Security Verify Privilege Cloud Suite

IBM Security Verify Privilege Cloud Suite is a software-as-a-service (SaaS)-based solution that secures privileged access for servers in multi-cloud environments. It allows humans and machines to authenticate, enforcing least privilege with just-in-time privilege elevation, increasing accountability, and helps to reduce administrative access risk.

Security Verify Privilege Cloud Suite provides the following three core services:

- Cloud Authentication Service simplifies user authentication to servers from any directory service, including Active Directory, OpenLDAP, and other cloud directories, such as Azure AD. This enables secure access to Linux and Microsoft Windows virtual systems and containers and enforces adaptive multifactor authentication (MFA) for stronger identity assurance. This includes:
 - Multidirectory brokering
 - Machine identity, delegated machine credentials, and credential management
 - Authentication policy management
 - MFA at system login
- Cloud Privilege Elevation Service enforces the principle of least privilege across multi-cloud workloads to minimize the risk of a security breach. Administrators can request just-in-time privilege elevation for a limited time. This includes:
 - Consistent, dynamic, and automated security policy management
 - Just-in-time privilege
 - MFA at privilege elevation
- Cloud Audit and Monitoring Service helps with compliance and incident response by providing auditing features and tying activities to an individual identity. It identifies abuse of privilege, helps to counter attacks, and assists with regulatory compliance by providing a detailed audit trail and video recordings that capture all privileged activity. This includes:
 - Advanced, host-based session recording, auditing, and reporting
 - Gateway session recording, monitoring, and control

1.2 Optional Services

The Client may select from the following available add-ons.

1.2.1 IBM Security Verify Privilege Vault Sites

IBM Security Verify Privilege Vault Sites add-on is used to expand the number of Sites included in the Cloud Service.

1.2.2 IBM Security Verify Privilege Vault Engines

IBM Security Verify Privilege Vault Engines add-on is used to expand the number of Engines included in the Cloud Service.

1.2.3 IBM Security Verify Privilege Vault Analytics

IBM Security Verify Privilege Vault Analytics provides risk-based user behavior alerts for activity within IBM Security Verify Privilege Vault. This Service can be configured to perform various response actions when an alert occurs.

1.2.4 IBM Security Verify Privilege Vault for Business Users Non-Production

IBM Security Verify Privilege Vault for Business Users Non-Production offering is a separate instance of the IBM Security Verify Privilege Vault for Business Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.5 IBM Security Verify Privilege Vault for Privileged Users Non-Production

IBM Security Verify Privilege Vault for Privileged Users Non-Production offering is a separate instance of the IBM Security Verify Privilege Vault for Privileged Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.6 IBM Security Verify Privilege Manager Non-Production for Managed Client

IBM Security Verify Privilege Manager Non-Production for Managed Client offering is a separate instance of the IBM Security Verify Privilege Manager for Managed Client offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.7 IBM Security Verify Privilege Manager Non-Production for Managed Server

IBM Security Verify Privilege Manager Non-Production for Managed Server offering is a separate instance of the IBM Security Verify Privilege Manager for Managed Server offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.8 IBM Security Verify Privilege DevOps Vault Non-Production Subscription per Record

The number of entitlements required for IBM Security Verify Privilege DevOps Vault Non-Production is determined by the number of passwords, encryption keys, digital certificates or other credentials stored in the non- production instance of IBM Security Verify Privilege DevOps Vault.

1.2.9 IBM Security Verify Privilege Account Lifecycle Manager Engines

The Account Lifecycle Manager Engine is a Windows Service that runs on a machine in the Client's environment. The Engine service manages interactions between the Account Lifecycle Manager Cloud Service and the Client's Microsoft Active Directory. This add-on is used to enable High Availability or an additional Microsoft Active Directory domain.

1.2.10 IBM Security Verify Privilege Account Lifecycle Manager Non-Production for Users

The IBM Security Verify Privilege Account Lifecycle Manager Non-Production for Users offering is a separate instance of IBM Security Verify Privilege Account Lifecycle Manager for Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.11 IBM Security Verify Privilege Vault Additional Secrets (Pack of 1000 Secrets)

IBM Security Verify Privilege Vault Additional Secrets (Pack of 1000 Secrets) enables a Client using IBM Security Verify Privilege Vault offerings to add secrets when the limit of 10,000 is insufficient for the Client's organization.

1.2.12 IBM Security Verify Privilege Cloud Suite Non-Production

IBM Security Verify Privilege Cloud Suite Non-Production offering is a separate instance of the IBM Security Verify Privilege Cloud Suite offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=4B8D1F20C00511E9908EB999AAEAE31E>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

Non-production Cloud Service instances are not eligible for Service Level Agreements (SLA).

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

3.2.1 Technical Support for All Non-Production Instances

Support for non-production instances is available from 8 AM to 8 PM in any of the following four home regions: Washington, DC, London, United Arab Emirates, and the Philippines. In addition, severity levels and response times as laid out in the IBM Cloud Service overview will not be applied to Non-Production Instance support cases.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Authorized User is a unique user authorized to access to the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device, or application server) through any means.
- Instance is each access to a specific configuration of the Cloud Services.
- Managed Client Device is any device that requests or receives execution commands, procedures or applications from a server environment managed by the Cloud Services.
- Managed Server is a physical computer or device (such as a blade or rack-mounted device) that is comprised of processing units, memory and input/output capabilities, and that executes requested procedures, commands or applications for users or Client devices managed by the Cloud Services.
- Record is a set of unique attributes for a specific item that is managed by, processed by, or related to the use of the Cloud Service. Unique attributes can include secrets, passwords, encryption keys, digital certificates, or any other credential stored in the Cloud Service.
- Virtual Server is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications made available to the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

IBM Technology



G-Cloud 15 IBM – webMethods Hybrid Integration Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Table of Contents

1.	<i>Cloud Service</i>	3
1.1	<i>Offerings</i>	3
2.	<i>Data Processing and Protection Data Sheets</i>	3
a.	<i>IBM webMethods Hybrid Integration SaaS [Generation 2]</i>	4
b.	<i>IBM webMethods SaaS [Generation 1]</i>	4
3.	<i>Service Levels and Technical Support</i>	4
3.1	<i>Service Level Agreement</i>	4
3.2	<i>Technical Support</i>	5
4.	<i>Charges</i>	5
4.1	<i>Charge Metrics</i>	5
5.	<i>Additional Terms</i>	8
5.1	<i>Configuration Requirements</i>	9
5.2	<i>Connectors to access third party offerings</i>	9
5.3	<i>Trademarks and logos</i>	9
5.4	<i>Enabling Software</i>	9
5.5	<i>Restrictions and Fair Usage Policy</i>	10
5.6	<i>Tech Preview Features</i>	10
5.7	<i>Client Use of Output</i>	10
5.8	<i>AI Use Restrictions</i>	11
6.	<i>Overriding Terms</i>	11
6.1	<i>Data Use</i>	11

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at <http://www.ibm.com/terms/csa> (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM webMethods Hybrid Integration SaaS Trial

This trial Cloud Service is provided for 30-days at no charge after which access to the service will be discontinued. This trial Cloud Service does not include the service level agreement or technical support described in this document and it is not intended for production use.

1.1.2 IBM webMethods Hybrid Integration SaaS [Generation 2 infrastructure]

This Cloud Service is an Integration Platform-as-a-Service (iPaaS) that enables clients to automate tasks by connecting apps and services and the automated tasks into your own applications. The Cloud Service provides Enterprise-wide connectivity options for integration needs. The platform is composed of Application Integration, API Management, B2B, Value-Added Network (VAN), Managed File Transfer and Event Endpoint Management as well as a Hybrid Control Plane providing end-to-end monitoring, runtime management and usage analytics.

1.1.3 IBM webMethods Hybrid Integration – Hybrid Control Plane

This offers the SaaS Hybrid Control Plane capability only. Including end-to-end monitoring, runtime management and usage analytics.

1.1.4 IBM webMethods SaaS [Generation 1 infrastructure]

This Cloud Service is an Integration Platform-as-a-Service (iPaaS) that enables Clients to automate tasks by connecting apps and services and the automated tasks into Client's applications with Client's branding and user experience. The Cloud Service provides enterprise-wide connectivity options for integration needs. The platform is composed of Integration, API Management, B2B, and Managed File Transfer.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.



a. IBM webMethods Hybrid Integration SaaS [Generation 2]

- IBM webMethods Hybrid Integration SaaS
<https://www.ibm.com/terms/?id=78622B695AFF41F18E94AA86225A6263>
- IBM Sterling B2B Integration Value-Added Network
<https://www.ibm.com/terms/?id=38BF2400B93711E7A5A50513C295686A>

If Generation 2 infrastructure is not available in the desired region, then Client may deploy in Generation 1 infrastructure regions as below:

b. IBM webMethods SaaS [Generation 1]

For the following Data Sheets, IBM does not commit to fully comply with the requirements included within the IBM Data Security and Privacy Principles, as referenced in the base Cloud Service Terms and the Data Processing and Protection Data Sheet.

- IBM webMethods Integration SaaS
<https://www.ibm.com/terms/?id=55F789E2F9F84C2696E835538D9FCC9D>
- IBM webMethods API Management SaaS
<https://www.ibm.com/terms/?id=9E7E196E479A4F2D92A68520949B4EA6>
-
- IBM webMethods B2B SaaS
<https://www.ibm.com/terms/?id=71E19E70C52848D09A1EC3F630CA11F1>
- IBM webMethods Managed File Transfer SaaS
<https://www.ibm.com/terms/?id=F110C54E3F9546ECA5C3142BE6C205C2>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
--------------	---

Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.1.1 SLA Eligibility

SLA credits for the Cloud Service are limited to Service Down related to components deployed and managed by the Cloud Service, subject to the following limitations:

- Any Client-initiated API target service endpoint(s) must be implemented, available, and responding according to their specifications. Any misconfigurations or outages related to Client-initiated API target service endpoints are not eligible for SLA credits. To the extent Client leverages any other services or runtimes related to its APIs, those respective SLAs shall apply (that is, for the avoidance of doubt, there shall be no duplication of SLA credits).
- Cloud Service management APIs are not eligible for SLA credits.
- Usage analytics, AI Agents and AI Assistants are not eligible for SLA credits.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

3.2.1 Optional Support Offerings

Additional support options are available for this Cloud Service. If Client selects to order an optional support offering, the terms defined in the Optional Support Offerings Service Description at <https://www.ibm.com/terms/?id=i126-9789> will apply to the support offering specified in Client's TD.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document. The following charge metrics apply to this Cloud Service:

- Resource Unit is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service. For the purpose of this Cloud Service, the resources measured are Instances, Transactions, API Calls, GraphQL

API Calls, Events, Integration Runtime Instances, and API Gateway Instances.
The following defines each resource type, and the corresponding Resource Units (RU) required:

(1) Instance is each access to a specific configuration of the Cloud Services. Client must obtain appropriate RU entitlements for each Instance provisioned during a 12 month period:

- (a) 1 webMethods Integration Instance = 60 RU per month
- (b) 1 App Connect Enterprise (ACE) Instance = 60 RU per month
- (c) 1 B2B Instance = 60 RU per month
- (d) 1 Managed File Transfer Instance = 60 RU per month
- (e) 1 webMethods API Instance = 50 RU per month
- (f) 1 API Connect Instance = 50 RU per month
- (g) 1 Event Endpoint Management Instance = 50 RU per month
- (h) 1 API Connect for GraphQL Instance = 15 RU per month

(2) Additional Hosted Integration Runtime within an existing environment

- (a) 1 Additional Hosted Integration Runtime = 5 RU per month

(3) Transactions

Client must obtain sufficient RU entitlements for the Transactions processed by the Cloud Service during a 12 month period as follows:

(a) An Integration Transaction occurs when an event triggers a flow to execute any one or more nodes in the flow. An execution that takes more than 60 seconds to complete is counted as an additional transaction for each additional 60 seconds (or part thereof). An Integration Transaction can occur in a SaaS Integration runtime or an Edge Integration runtime.

- 100,000 webMethods Integration Transactions = 4 RU for the first 100M Transactions per year
- 100,000 webMethods Integration Transactions = 1 RU for Transactions greater than 100M Transactions per year
- 100,000 ACE Integration Transactions = 4 RU for the first 100M Transactions per year
- 100,000 ACE Integration Transactions = 1 RU for Transactions over 100M per year

(b) A Managed File Transfer (MFT) Transaction is an initiation of an inbound file transfer or an initiation of an outbound file transfer.

- A file more than 5 megabytes will be counted as an additional MFT Transaction for each additional 5 megabytes rounded up to the nearest increment.
- 100,000 MFT Transactions = 4 RU for the first 100M Transactions per year
- 100,000 MFT Transactions = 1 RU for Transactions greater than 100M Transactions per year

(c) A B2B Transaction is the exchange of any electronic document (e.g., purchase order, purchase order acknowledgment, invoice, ASN) with another entity in any EDI or non-EDI standard format (e.g., EDI, XML, csv).

- A single document sent or received by the platform is counted as a B2B Transaction.
- For batch transactions, each single B2B transaction contained within the batch is counted.
- A document more than 5 kilobytes will be counted as an additional B2B Transaction and each additional 5 kilobyte will be rounded up to the nearest increment.
- 100,000 B2B Transactions = 4 RU for the first 100M Transactions per year
- 100,000 B2B Transactions = 1 RU for Transactions greater than 100M Transactions per year

(d) Value-Added Network (VAN) Transactions

-
- A single document sent or received by the VAN capability is counted as a VAN Transaction.
- For batch transactions, each single VAN Transaction contained within the batch is counted.
- A document more than 5 kilobytes will be counted as an additional VAN Transaction. Each additional 5 kilobytes will be rounded up to the nearest increment.
- 10,000 VAN Transactions = 30 RU for the first 1M Transactions per year
- 10,000 VAN Transactions = 10 RU for Transactions greater than 1M Transactions per year

(4) API Call is the invocation of the Cloud Services through a programmable interface. Specifically, each inbound API Call to an API Gateway or microgateway component will be counted as an API Call. Client must obtain sufficient RU entitlements for the API Calls processed by the Cloud Service during a 12 month period as follows:

(a) webMethods API Calls

- 1,000,000 webMethods API Calls = 3 RU for the first 1B API Calls per year

- 1,000,000 webMethods API Calls = 2 RU for API Calls greater than 1B API Calls per year

(b) API Connect API Calls

- 1,000,000 API Connect API Calls = 3 RU for the first 1B API Calls per year
- 1,000,000 API Connect API Calls = 2 RU for API Calls greater than 1B API Calls per year

(5) GraphQL API Call is an API call to the GraphQL Endpoint.

(a) A single API Call to an API Connect for GraphQL Endpoint will consume 1 GraphQL API Call as long as the GraphQL API is not invoking another service hosted by API Connect for GraphQL.

(b) A single API Call to an API Connect for GraphQL Endpoint that is federated across 3 subgraphs hosted by API Connect for GraphQL would consume 4 GraphQL API Calls assuming the subgraphs GraphQL APIs are not invoking another service hosted by API Connect for GraphQL in Client's account.

(c) An Endpoint is a physical device that connects to and exchanges information with API Connect for GraphQL.

- 1,000,000 GraphQL API Calls = 5 RU for the first 1B GraphQL API Calls per year
- 1,000,000 GraphQL API Calls = 3 RU for GraphQL API Calls greater than 1B API Calls

(6) Events

Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Services. For this Cloud Service, an Event is a message published or received through an Event Gateway. Client must obtain sufficient RU entitlements for the Events processed by the Cloud Service during a 12 month period as follows:

(a) A message exceeding 200 kilobytes will be counted as an additional Event. Each additional 200 kilobytes will be rounded up to the nearest increment.

- 1,000,000 Events = 3 RU for the first 1B Events per year
- 1,000,000 Events = 2 RU for Events greater than 1B Events per year

(7) Integration Runtime/API Gateway (IR/API GW) in the Hybrid Control Plane

(a) Each remote Integration Runtime Instance (IR) and each remote API Gateway Instance (API GW) will be counted and requires RU allocation as follows:

- 1 IR/API GW = 2 RU per month for the first 100 IR/API GW per year
- 1 IR/API GW = 1 RU per month for IR/API GW greater than 100 IR/API GW per year.

5. Additional Terms



For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Configuration Requirements

- a. VAN functionality requires the use of webMethods B2B
- b. webMethods B2B requires the use of Integration for full data mapping and transformation capabilities
- c. For the Hybrid Control Plane, use of the Event Gateways, DataPower Gateway and webMethods Integration Edge Runtimes Enabling Software programs will be excluded from RU calculations. The RUs consumed for the Hybrid Control Plane is measured as the high-water mark for the calendar month.
- d. Not all capabilities for these Cloud Services are available in all regions.

5.2 Connectors to access third party offerings

This Cloud Service provides connectors that allow clients to connect to third-party applications or external data sources, by entering client's access credentials into the Cloud Service to execute the connection. Client's connectivity to such third-party applications or external data sources via a connector relies on the availability of such third-party applications or external data sources' APIs to IBM. Client must obtain its own license (and access credentials) from such providers of third-party applications or data sources and is responsible to comply with such third parties' terms and conditions. IBM may modify and/or limit use of the connectors if so required by the providers of the third-party applications or data sources.

5.3 Trademarks and logos

The trademarks and logos included on this site are owned by third parties. They are being displayed for the sole purpose of assisting Client in locating an IBM connector that integrates to a third party product or service of interest to you. Such display in no way implies any affiliation, sponsorship or endorsement from the third party trademark owners of the IBM connectors or any other IBM product or service.

5.4 Enabling Software

The Cloud Service contains the following Enabling Software:

Enabling Software	Applies when	Applicable License Terms (if any)
IBM App Connect Enterprise Evaluation Edition	Using the App Connect capability as part of IBM webMethods Hybrid Integration SaaS	https://www.ibm.com/terms/?id=L-LDLB-B6JT36
IBM App Connect Enterprise Secure Agent 12.0.0	Using the App Connect capability as part of IBM webMethods Hybrid Integration SaaS	https://www.ibm.com/terms/?id=L-ADZA-EU8EWD
Event Gateway	Using the Event Endpoint Management Capability of IBM webMethods Hybrid Integration SaaS	License terms are as defined in the Enabling Software section of the base Agreement.

webMethods Integration Edge Runtime	Using the webMethods Integration Capability of either IBM webMethods Hybrid Integration SaaS or webMethods SaaS.	License terms are as defined in the Enabling Software section of the base Agreement.
DataPower Gateway Virtual Edition	Using the DataPower Gateway as a remote Gateway using the API Connect capability as part of IBM webMethods Hybrid Integration SaaS	License terms are as defined in the Enabling Software section of the base Agreement.

Additional restrictions for use of the Enabling Software are:

- IBM App Connect Enterprise Evaluation Edition may only be used for the following purposes:
- To develop flows using the provided App Connect Enterprise Toolkit

In the event of a conflict with the license terms accompanying the Enabling Software, this Service Description will prevail.

5.5 Restrictions and Fair Usage Policy

The Cloud Service is designed to run certain Flows as soon as a defined trigger event occurs, however IBM does not warrant that this will occur within a set period of time.

In exceptional circumstances it may be necessary for IBM to take steps to stop or remove unreasonable Client Flows which are adversely impacting other users or overall system performance.

5.6 Tech Preview Features

Some features within capabilities are labeled as “tech preview”. Any tech preview feature is excluded from available service level agreements and may not be supported. IBM may change or discontinue a tech preview feature at any time and without notice.

5.7 Client Use of Output

Based on the Client's input, the Cloud Service will provide suggested tasks and other materials as generated outputs. All Client inputs to the Cloud Service and any content provided by Client for further training of the Cloud Service, including fine-tuning or prompt-tuning, are Client Content. IBM does not claim to have ownership rights to any generated output. Client is solely responsible for outputs generated by the Cloud Service (including obligations related to third party licenses referenced in outputs) and Client should exercise discretion and evaluate whether outputs generated from the model are appropriate for the Client's environment. The generated outputs will likely require modifications by the Client. Unless separately authorized by the Client through a voluntary feedback submission, IBM will not use the Client Content or generated outputs to train the Cloud Service.

5.8 AI Use Restrictions

Client agrees not to, and not to direct or allow third parties, use the Cloud Service: (i) for mass surveillance, racial profiling, or any use that violates or encourages the violation of basic human rights or other applicable laws and regulations; (ii) to distribute false, misleading, disparaging or obscene information or content; (iii) to provide fully automated decision making in connection use cases involving critical processes or the risk of loss of life, property or impact on an individual's legal rights; (iv) in a manner that impersonates another for deceptive purposes or conceals the fact a user is interacting with AI; or (v) to distribute or intentionally generate malware or other harmful code. This Cloud Service is not intended for use in a high-risk context as defined under the EU AI Act or other applicable regulations. If Client chooses to use it in such, please contact ChiefPrivacyOffice@ca.ibm.com.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM may however use Content and other information that results from Content in the course of managing and providing the Cloud Service provided that any data subject to applicable privacy regulations will be rendered into a form that no longer constitutes personal data. IBM will use Client's Content and other information that results from Content, excluding personal data, only for research, testing, and offering development. IBM may share threat identifiers and other security information embedded in Client personal data for threat detection and protection purposes. The provisions of this section will survive the termination or expiration of the transaction.

IBM