

Service Description

IBM Cloud Identity

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

1. Cloud Service

IBM Cloud Identity provides Single Sign-On (SSO), multifactor authentication and identity lifecycle controls for internal (employees) and external user types.

1.1 Offerings

The Client may select from the following available offerings, all of which have an Event capacity of 400 events per second.

1.1.1 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-premise IBM Security Access Management (ISAM) 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-premise and cloud applications.

1.1.2 IBM Cloud Identity Connect for ISAM

This Cloud Service tightly integrates with the on-premise IBM Security Access Management (ISAM) software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premise and cloud applications. This Cloud Service requires the Client to have an active Software Subscription and Support (S&S) entitlement for the IBM Security Access Management (ISAM) 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-premise ISAM license entitlement. Discontinuation of Client's S&S will also discontinue this Cloud Service. Access to the enabling software defined in Section 5.2 is not included with this Cloud Service.

1.1.3 IBM Cloud Identity Essentials

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

1.1.4 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-premise IBM Security Access Management (ISAM) software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premise and cloud applications. It is available standalone, or to compliment Cloud Identity Connect, Cloud Identity Connect for ISAM and Cloud Identity Essentials.

1.1.5 IBM Cloud Identity Govern

This Cloud Service tightly integrates with the on-premise IBM Governance and Intelligence (IGI) 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-premise and cloud applications. This Cloud Service provides organizations advanced identity lifecycle management capabilities within the cloud, and includes application access request workflow.

1.1.6 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.

1.1.7 IBM Cloud Identity Analyze

This Cloud Service augments existing IBM solutions, such as IBM Security Identity Governance and Intelligence (IGI) and IBM Security Identity Manager (ISIM), to provide a holistic risk profile of managed users. This Cloud Service includes an on-premises, multi-purpose analytics engine that processes activity and entitlement data from a variety of sources, which provide a 360-degree view of access risks with the ability to take action based on those risk insights.

1.1.8 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.

1.1.9 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 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 100 Events per second capacity.

1.2.2 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.

1.2.3 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

1.3.1 IBM Cloud Identity Connect Solution Planning

This service provides one (1) week of professional services during which IBM will perform some or all of the following:

- Establish single sign-on for cloud-based SaaS applications
- Configure a launch pad for easy application location
- Connect applications with ready-made connectors
- Solution planning, architecture and guidance
- IBM recommended approach and practices

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

This service provides a three (3) day professional services workshop, focused on multi-factor authentication challenges and securing a Client's applications using IBM Cloud Identify Verify. The workshop will cover some or all of the following:

- Embed familiar authentication into all digital and in person interactions where authentication is required
- Enable an application to enforce strong authentication using developer friendly REST API

- Provide industry best practice recommendations on identity security
- Streamlined user experience and adoption on all form factors – phones, tablets and laptops

1.3.3 IBM Cloud Security Strategy and Planning

This service provides a three (3) week professional services workshop on how to apply cloud security best practices, with a focus on infrastructure and application security. The workshop will cover some or all of the following:

- Establish single sign-on for cloud-based SaaS applications
- Configure a launch pad for easy application location
- Connect applications with ready-made connectors
- Solution planning, architecture and guidance
- Insights on emerging trends in cyber security
- IBM recommended approach and practices

1.3.4 IBM Cloud Identity Expert On Demand

This service provides twenty (20) hours of professional services, delivered in two (2) hour sessions within thirty (30) days of start. The services will provide a Cloud Identity architect to answer questions and provide guidance and recommendations on, but not limited to:

- Technical skills to augment a Client's Cloud Identity solution implementation
- Architectural and implementation questions on a Client's Cloud Identity solution
- Guidance on a Client's Cloud Identity solution and/or strategy

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 provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at <http://ibm.com/dpa/dpl> apply.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D>

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 SaaS support overview at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9 %	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 IBM Cloud Identity environment to achieve the minimum 99.9% 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 IBM Cloud Identity

Service that would prohibit the IBM Cloud Identity 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/>.

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.
- 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 a specific configuration of the Cloud Services.
- Engagement is a professional or training service related to the Cloud Services.
- Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Services.
 - For Cloud Identity Connect, an Event is an http request against the Cloud Service.
 - For Cloud Identity Verify, an Event is any multi-factor method being invoked via the Cloud Service.

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 Client Reference

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

5.2 Enabling Software

The Cloud Service contains the following Enabling Software:

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:

- IBM Security Access Manager Virtual Enterprise Edition

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

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

The following enabling software may only be used with the IBM Cloud Identity Analyze Service:

- IBM Cloud Identity Analyze on-premises analytics engine

5.3 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.