

## IBM Cloud Identity

본 서비스 명세서는 본 클라우드 서비스에 대해 설명합니다. 관련 주문 서류에서는 고객의 주문에 대한 가격 책정과 추가적인 세부사항을 제공합니다.

### 1. 클라우드 서비스

#### 1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

##### 1.1.1 IBM Cloud Identity Connect

이 클라우드 서비스는 인에이블링 소프트웨어로 포함된 온프레미스 IBM Security Access Management(ISAM) 소프트웨어 프로그램을 강력하게 통합하여 온프레미스와 클라우드 애플리케이션 모두에 걸쳐서 액세스 관리에 대한 LOB(line-of-business) 요구를 지원하기 위해 고객에게 필요한 솔루션을 제공합니다.

##### 1.1.2 IBM Cloud Identity Connect for ISAM

이 클라우드 서비스는 온프레미스 IBM Security Access Management(ISAM) 소프트웨어 프로그램을 강력하게 통합하여 온프레미스와 클라우드 애플리케이션 모두에 걸쳐서 액세스 관리에 대한 LOB(line-of-business) 요구를 지원하기 위해 고객에게 필요한 솔루션을 제공합니다. 이 클라우드 서비스를 사용하기 위해서는 고객은 IBM Security Access Management (ISAM) 프로그램에 대해 유효한 Software Subscription and Support (S&S) 권한이 있어야 하며 S&S는 고객의 클라우드 서비스 사용등록 기간 동안 유효한 상태를 유지해야 합니다. 고객의 S&S가 중단되면 이 클라우드 서비스도 중단됩니다. 5.2항에 정의된 인에이블링 소프트웨어에 대한 액세스 권한은 이 클라우드 서비스에 포함되어 있지 않습니다.

##### 1.1.3 IBM Cloud Identity Essentials

이 클라우드 서비스는 고객이 사용 중인 다양한 IBM 및 공용 클라우드 애플리케이션에 대한 싱글 사인온(SSO) 기능을 고객에게 제공합니다. 조건부 액세스와 같이 추가 보안 제어 레벨을 제공하는 IBM MaaS360과 함께 이 클라우드 서비스를 사용할 수 있습니다.

##### 1.1.4 IBM Cloud Identity Verify

이 클라우드 서비스는 온프레미스 IBM Security Access Management(ISAM) 소프트웨어 프로그램을 통합하여 온프레미스와 클라우드 애플리케이션 모두에 걸쳐서 액세스 관리에 대한 LOB(line-of-business) 요구를 지원하기 위해 고객에게 필요한 솔루션을 제공합니다. 이 클라우드 서비스는 디지털 서비스 액세스 시 신원 확인을 위해 사용자에게 2차 인증 요소를 요구하는 기능을 제공합니다. Cloud Identity Connect 및 Cloud Identity Essentials에서 사용 가능하며 액세스 보안 및 싱글 사인온 목적으로 해당 플랫폼을 사용하는 애플리케이션에 대한 2차 인증 요소를 제공하는 데 사용됩니다.

##### 1.1.5 IBM Cloud Identity Govern

이 클라우드 서비스는 인에이블링 소프트웨어로 포함된 온프레미스 IBM Governance and Intelligence (IGI) 소프트웨어 프로그램을 강력하게 통합하여 온프레미스와 클라우드 애플리케이션 모두에 걸쳐서 액세스 관리에 대한 LOB(line-of-business) 요구를 지원하기 위해 고객에게 필요한 솔루션을 제공합니다. 이 클라우드 서비스는 조직에게 클라우드 내의 고급 ID 라이프사이클 관리 기능을 제공하며 애플리케이션 액세스 요청 워크플로우를 포함합니다.

##### 1.1.6 IBM Cloud Identity Connect and Verify

IBM Cloud Identity Connect와 IBM Cloud Identity Verify의 번들 오퍼링입니다.

### 1.1.7 IBM Cloud Identity Connect Verify and Govern

IBM Cloud Identity Connect, IBM Cloud Identity Verify 및 IBM Cloud Identity Govern 의 번들 오퍼링입니다.

## 1.2 선택적 서비스

### 1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud 는 고객이 테스트, 성능 조정, 결함 진단, 내부 벤치마킹, 스테이징 품질 보증 활동 및/또는 공개된 API(Application Programming Interfaces)를 사용하여 내부적으로 사용되는 추가 기능 또는 확장 기능의 개발을 포함하여(단, 이에 한하지 않음) 내부 비프로덕션 활동 용도에 한해서만 사용할 수 있는 IBM Cloud Identity Platform 의 별도 인스턴스입니다. 이 클라우드 서비스에는 제 3 조 서비스 레벨 및 기술 지원 조항에 준하여, 가용성 서비스 레벨 계약(SLA)를 포함시킬 수 있는 옵션이 있습니다.

## 1.3 Acceleration 서비스

### 1.3.1 IBM Cloud Identity Connect Solution Planning

본 서비스는 IBM 이 다음 중 일부 또는 전체를 수행하는 1 주간의 전문 서비스를 제공합니다.

- 클라우드 기반 SaaS 애플리케이션을 위한 싱글 사인온 설정
- 애플리케이션 위치를 쉽게 지정할 수 있도록 런치 패드 구성
- 사전 제작된 커백터로 애플리케이션 연결
- 솔루션 계획, 아키텍처 및 지침
- IBM 이 권장하는 접근법 및 관행

### 1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

본 서비스는 3 일 동안 IBM Cloud Identity Confirm 을 사용하여 다단계 인증 문제를 해결하고 고객의 애플리케이션을 보호하는 데 초점을 맞춘 전문 서비스 워크샵을 제공합니다. 이 워크샵에서는 다음 사항의 일부 또는 전체를 다룹니다.

- 인증이 필요한 모든 디지털 및 직접 상호작용에 친숙한 인증 포함
- 애플리케이션에서 개발자 친화적인 REST API 를 사용하여 강력한 인증 적용
- ID 보안에 대한 업계 우수 사례 권장사항 제공
- 전화, 태블릿, 랩탑 등 모든 폼 팩터에서 사용자 환경 및 채택 간소화

### 1.3.3 IBM Cloud Security Strategy and Planning

이 서비스는 3 주 동안 인프라 및 애플리케이션 보안을 중심으로 클라우드 보안 우수 사례를 적용하는 방법에 대한 전문 서비스 워크샵을 제공합니다. 이 워크샵에서는 다음 사항의 일부 또는 전체를 다룹니다.

- 클라우드 기반 SaaS 애플리케이션을 위한 싱글 사인온 설정
- 애플리케이션 위치를 쉽게 지정할 수 있도록 런치 패드 구성
- 사전 제작된 커백터로 애플리케이션 연결
- 솔루션 계획, 아키텍처 및 지침
- 사이버 보안의 새로운 동향에 대한 통찰력
- IBM 이 권장하는 접근법 및 관행

### 1.3.4 IBM Cloud Identity Expert On Demand

본 서비스는 20 시간의 전문 서비스를 제공하며, 시작 후 30 일 이내에 두 시간 세션으로 제공됩니다. 이 서비스는 Cloud Identity 설계자가 질문에 답하고 다음 사항에 대한 지침과 권장사항을 제공합니다(단, 이에 한하지 않음).

- 고객의 Cloud Identity 솔루션 구현을 강화하기 위한 기술
- 고객의 Cloud Identity 솔루션에 대한 아키텍처 및 구현 질문
- 고객의 Cloud Identity 솔루션 및/또는 전략에 대한 지침

## 2. 데이터 처리 및 보호 데이터 시트

IBM 데이터 처리 부칙(Data Processing Addendum: DPA)(<http://ibm.com/dpa> 참조) 및 아래 링크의 데이터 처리 및 보호 데이터 시트(Data Processing and Protection Data Sheet(s))(데이터 시트(들) 또는 DPA 별표(들)로 참조됨)는 클라우드 서비스에 대한 추가적인 데이터 보호 정보와 처리할 수 있는 콘텐츠의 유형, 관련 처리 활동, 데이터 보호 기능 및 콘텐츠의 보관 및 반환 정보와 관련한 옵션을 제공합니다. DPA는 콘텐츠에 포함된 개인 데이터에 i) European General Data Protection Regulation (EU/2016/679)(GDPR) 또는 ii) <http://www.ibm.com/dpa/dpl> 에 명시된 기타 데이터 보호법이 적용되는 경우 그 범위에 한 해 적용됩니다.

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

## 3. 서비스 레벨(Service Levels) 및 기술 지원

### 3.1 SLA(Service Level Agreement)

IBM은 다음 가용성 "서비스 레벨 계약"(이하 SLA)을 고객에게 제공합니다. IBM은 아래 표와 같이 누적 클라우드 서비스 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 가용률은 약정 월의 총 시간(분)에서 약정 월의 총 Service Down(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다. Service Down의 정의, 클레임 절차, 서비스 가용성 문제에 관한 IBM 문의 방법은 IBM SaaS 지원 개요([https://www.ibm.com/software/support/saas\\_support\\_overview.html](https://www.ibm.com/software/support/saas_support_overview.html))에서 확인할 수 있습니다.

가용성	크레딧 (월별 사용등록료*의 %)
99.9% 미만	10%

\* 사용등록료는 클레임 대상이 되는 해당 월의 약정 요금입니다.

#### 3.1.1 SLA에 대한 기타 정보

고객은 최초 60일 기간("번인(Burn-in) 기간") 동안 IBM Cloud Identity 환경의 최소 99.9% 업타임 백분율 미달성에 따른 크레딧을 제공받을 수 없습니다. IBM이 번인 기간(Burn-In Period) 동안이나 그 이전에 IBM Cloud Identity Service로 마이그레이션되는 기존의 고객 구성, 정책, 데이터 또는 코드("기존 구성요소") 중, IBM Cloud Identity Service에서 본 계약에 지정된 업타임 백분율을 달성하지 못하게 하는 구성요소를 식별하는 경우 IBM은 해당 기존 구성요소에 대해 고객에게 통지하고 IBM의 재량으로 SLA의 조항에서 해당 구성요소를 면제할 수 있습니다. IBM이 면제된 기존 구성요소에 대해 고객에게 통지하는 경우 면제된 구성요소가 본 계약의 업타임 백분율을 충족할 수 있는 정도의 구제책을 고객에게 제공해야 할 책임은 IBM에게 있습니다. 양 당사자가 달리 합의하지 않는 한, 그러한 구제책의 비용은 전적으로 고객이 부담해야 합니다.

### 3.2 기술 지원

지원 문의 상세 정보, 심각도 레벨, 가용성 지원 시간, 응답 시간 및 기타 지원 정보와 절차를 포함하여, 클라우드 서비스에 대한 기술 지원은 IBM 지원 안내서(<https://www.ibm.com/support/home/pages/support-guide/> 참조)에서 클라우드 서비스를 선택하면 확인할 수 있습니다.

## 4. 요금

### 4.1 청구 체계

클라우드 서비스에 대한 과금 체계는 거래서류에 명시됩니다.

이 클라우드 서비스에는 다음 청구 체계가 적용됩니다.

- 승인된 사용자(Authorized User)는 어떠한 방법, 어떠한 형태로든(예, 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스에 액세스하도록 권한이 부여된 고유한 사용자를 의미합니다.
- 직원이란 클라우드 서비스에 대한 액세스 권한 유무에 관계 없이, 고객의 기업집단에 채용되거나 고객의 기업집단이 임금을 지불하거나 고객의 기업집단을 대신하여 업무를 수행하는 고유한 개인을 의미합니다.
- 적격 참여자(Eligible Participant)는 클라우드 서비스에서 관리하거나 추적하는 서비스 제공 프로그램에 참여할 수 있는 개인이나 법인을 의미합니다.
- 인스턴스는 클라우드 서비스의 특정 구성에 대한 각 액세스를 의미합니다.
- 인게이지먼트(Engagement)는 클라우드 서비스들과 관련된 프로페셔널 서비스 또는 트레이닝 서비스입니다.

## 5. 추가 조항

2019년 1월 1일 이전에 작성된 클라우드 서비스 계약들(또는 동등한 기본 클라우드 계약들)에는 <https://www.ibm.com/acs>에서 제공한 조건들이 적용됩니다.

### 5.1 고객 참조

고객은 IBM 이 매스컴이나 마케팅 통신문에서 고객을 클라우드 서비스의 가입자로 공개적으로 언급할 수 있다는 데 동의합니다.

### 5.2 인에이블링 소프트웨어(Enabling Software)

클라우드 서비스에는 다음 인에이블링 소프트웨어가 포함됩니다.

다음 인에이블링 소프트웨어는 IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify 및 IBM Cloud Identity Connect Verify and Govern 클라우드 서비스와 함께 사용되어야만 합니다.

- IBM Security Access Manager Virtual Enterprise Edition

다음 인에이블링 소프트웨어는 IBM Cloud Identity Govern 및 IBM Cloud Identity Connect Verify and Govern 클라우드 서비스와 함께 사용되어야만 합니다.

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

### 5.3 데이터 수집 및 처리 권한

클라우드 서비스는 고객이 고객의 보안 환경과 데이터를 개선하는 것을 지원하기 위해 설계되었습니다. 일부 지역의 경우 클라우드 서비스는 개인 정보로 간주될 수 있는 정보를 단독 또는 결합 형태로 승인된 사용자로부터 수집합니다. 수집하는 데이터에는 사용자 소스 IP 주소, 사용자 ID, 고객 지원을 위한 IBM 접촉 목적으로 제공된 사용자 이름(성 및 이름), 전화번호, 비밀번호 및 이메일 주소가 포함될 수 있습니다. 데이터 수집 및 처리 실무는 클라우드 서비스의 기능을 개선하기 위해 업데이트될 수 있습니다. 필요에 따라 데이터 수집 및 처리 실무에 대해 자세하게 기술한 문서(데이터 처리 안내서 참조)를 업데이트하며 고객이 요청하는 경우 이를 제공합니다. 고객은 IBM 이 데이터 처리 및 EU 데이터 개인정보 보호정책 조건에 따라 정보를 수집하고 처리할 수 있도록 필요한 권한을 부여합니다.

### 5.4 Cloudflare

본 클라우드 서비스는 고객 콘텐츠에 대한 재처리자의 하나로 Cloudflare, Inc.를 이용합니다. Cloudflare 는 클라우드 서비스의 제공을 최적화하기 위해 암호화되지 않은 양식으로 콘텐츠를 처리합니다. Cloudflare 는 레벨 1 서비스 공급자로 PCI 를 준수하며 ISO 27001 및 SOC 2 준수를 위해 노력하고 있습니다. (즉, 본 전반적인 클라우드 서비스는 PCI 준수 제품이 아닙니다.)