

IBM Security AppScan Mobile Analyzer

Die Nutzungsbedingungen bestehen aus diesen IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen (nachfolgend „SaaS-spezifische Angebotsbedingungen“ genannt) und einem Dokument mit dem Titel IBM Nutzungsbedingungen – Allgemeine Bedingungen (nachfolgend „Allgemeine Bedingungen“ genannt), das unter der folgende Adresse zu finden ist: <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

Im Falle eines Widerspruchs haben die SaaS-spezifischen Angebotsbedingungen Vorrang vor den Allgemeinen Bedingungen. Durch die Bestellung von IBM SaaS, den Zugriff darauf oder die Nutzung von IBM SaaS erklärt der Kunde sein Einverständnis mit diesen Nutzungsbedingungen.

Die Nutzungsbedingungen unterliegen dem IBM International Passport Advantage Vertrag, dem IBM International Passport Advantage Express Vertrag oder dem IBM Internationalen Vertrag über ausgewählte IBM SaaS-Angebote (nachfolgend „Vertrag“ genannt) und bilden zusammen mit dem jeweils anwendbaren Vertrag die vollständige Vereinbarung.

1. IBM SaaS

Die vorliegenden SaaS-spezifischen Angebotsbedingungen gelten für das folgende IBM SaaS-Angebot:

- IBM Security AppScan Mobile Analyzer

2. Gebührenmetriken

IBM SaaS wird unter der folgenden Gebührenmetrik entsprechend der Angabe im Auftragsdokument verkauft:

- „Anwendungsinstanz“ ist eine Maßeinheit für den Erwerb von IBM SaaS. Für jede Instanz einer Anwendung, die mit IBM SaaS verbunden wird, muss eine Berechtigung erworben werden. Besteht eine Anwendung aus mehreren Komponenten, die jeweils einem bestimmten Zweck und/oder einer bestimmten Benutzerschaft dienen und mit IBM SaaS verbunden oder von IBM SaaS verwaltet werden können, dann wird jede dieser Komponenten als separate Anwendung betrachtet. Ferner werden Test-, Entwicklungs-, Staging- und Produktionsumgebungen für eine Anwendung als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Mehrere Anwendungsinstanzen in einer einzelnen Umgebung werden als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Der Kunde muss ausreichende Berechtigungen erwerben, um die Anzahl der Anwendungsinstanzen abzudecken, die während des Abrechnungszeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, mit IBM SaaS verbunden werden.

3. Gebühren und Abrechnung

Der für IBM SaaS zu bezahlende Betrag ist im Auftragsdokument angegeben.

3.1 Nutzungsabhängige Gebühren (Pay as you Go)

'Pay as you Go'-Optionen werden in dem Monat nach der Inanspruchnahme des Service zu dem im Auftragsdokument angegebenen Gebührensatz in Rechnung gestellt.

4. Technische Unterstützung

Technische Unterstützung für IBM Security AppScan Mobile Analyzer wird in zwei Varianten erbracht:

4.1 Supportforum

Alle Kunden erhalten Unterstützung über ein Supportforum, das regelmäßig von IBM Supportmitarbeitern und Entwicklern überwacht wird.

- Fragen können über die folgende Adresse gestellt werden:
<https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer>
- Aktuelle Beiträge können über die folgende Adresse eingesehen werden:
<https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/>

4.2 Standardunterstützung

Standardunterstützung wird in dem Zeitraum erbracht, in dem beim Kunden 'Pay as you Go'-Gebühren anfallen. Die Kunden können Support-Tickets direkt im Cloud-Service einstellen oder eine Chatsitzung öffnen, um Unterstützung zu erhalten. Weitere Informationen über Supportverfahren sind im IBM Support-Webportal unter <https://support.ibmcloud.com> oder im IBM SaaS Software Support Handbook unter http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf zu finden.

Fehlerklasse	Definition der Fehlerklasse	Angestrebte Reaktionszeiten	Deckungszeiten
1	Kritische Auswirkung auf den Geschäftsbetrieb/Serviceausfall: Geschäftskritische Funktionen sind nicht funktionsfähig oder eine kritische Schnittstelle ist ausgefallen. Dies betrifft normalerweise eine Produktionsumgebung und weist darauf hin, dass der Zugriff auf die Services nicht möglich ist, mit kritischen Auswirkungen auf betriebliche Abläufe. In diesem Fall ist eine sofortige Lösung erforderlich.	Innerhalb von 1 Stunde	24x7
2	Erhebliche Auswirkung auf den Geschäftsbetrieb: Die Nutzung eines geschäftsrelevanten Service-Features oder einer Servicefunktion ist stark eingeschränkt, oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann.	Innerhalb von 2 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
3	Geringe Auswirkung auf den Geschäftsbetrieb: Der Service oder die Funktionalität kann genutzt werden und das Problem hat keine kritische Auswirkung auf betriebliche Abläufe.	Innerhalb von 4 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
4	Minimale Auswirkung auf den Geschäftsbetrieb: Eine Anfrage oder eine Frage nicht technischer Art.	Innerhalb 1 Arbeitstages	Mo-Fr zu den Geschäftszeiten

4.3 Zugriff auf Kundendaten

IBM kann zur Diagnose von Problemen mit dem Service und um die Prüfung von Kundenanwendungen mithilfe des Service zu vereinfachen, auf Kundendaten zugreifen. Der Datenzugriff erfolgt ausschließlich zum Zwecke der Fehlerbehebung oder zur Unterstützung von IBM Produkten oder Services.

5. Zusätzliche Bedingungen für die IBM SaaS-Angebote

Der Cloud-Service ist für die Erkennung einer Vielzahl potenzieller Sicherheits- und Compliance-Probleme in mobilen Anwendungen und mobilen Web-Services ausgelegt. Es werden weder alle Sicherheitslücken oder Compliance-Risiken überprüft noch fungiert der Service als Schutz vor Sicherheitsattacken. Da sich Sicherheitsbedrohungen, Regelungen und Standards ständig ändern, kann der Service nicht alle Änderungen berücksichtigen. Die Sicherheit und Compliance der mobilen Anwendung des Kunden, seiner Systeme und Mitarbeiter sowie alle Abhilfemaßnahmen liegen in der alleinigen Verantwortung des Kunden. Der Kunde entscheidet alleine über die Nutzung der vom Service bereitgestellten Informationen.

5.1 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für IBM SaaS über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der IBM SaaS-Nutzung im Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität von IBM SaaS erfassen, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder die Interaktionen mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholt oder eingeholt hat, damit IBM die erhobenen personenbezogenen Daten für die vorstehenden Zwecke innerhalb von IBM, durch andere IBM Unternehmen und deren Unterauftragnehmer in allen Ländern, in denen sie geschäftlich tätig sind, in Übereinstimmung mit der geltenden Gesetzgebung verarbeiten darf. IBM wird den Anforderungen der Mitarbeiter und

Auftragnehmer des Kunden nachkommen, die sich auf den Zugriff, die Aktualisierung, die Korrektur oder die Löschung ihrer personenbezogenen Daten beziehen.

5.2 Bevorzugte Standorte

Soweit möglich, basieren die Steuern auf dem Standort, den der Kunde als bevorzugten Standort für IBM SaaS angibt. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung von IBM SaaS als primärer Standort angegeben wird, es sei denn, der Kunde stellt IBM zusätzliche Informationen bereit. Der Kunde ist dafür verantwortlich, diese Informationen auf dem aktuellen Stand zu halten und IBM über Änderungen zu informieren.

Anhang A

1. Allgemeine Beschreibung des IBM SaaS-Angebots

IBM Security AppScan Mobile Analyzer

Dieser Service identifiziert Sicherheitsprobleme auf der Codeebene mobiler Android-Anwendungen. Mit diesem Service kann ein Entwickler nach Sicherheitslücken suchen, ohne dass der Anwendungscode bereitgestellt werden muss. Bei Abschluss des Scans wird ein Sicherheitsbericht generiert, der Einzelheiten über erkannte Sicherheitslücken, die dadurch verursachten potenziellen Sicherheitsrisiken für die mobile Anwendung und Vorschläge zur Behebung der Sicherheitslücken enthält.