# IBM Watson Campaign Automation (WCA) Engage
# Security & Operations Overview

IBM Watson Campaign Automation (“WCA”, formerly Marketing Cloud / Silverpop) Engage is a web-based, multi-tenant, software-as-a-service (SaaS) digital-marketing platform designed to be a data-driven self-service solution with a flexible data schema that allows clients to determine the data elements to be stored, collected, and processed; typical use cases include the means of contacting recipients (email address, mobile number for SMS messaging, and/or App ID for Mobile Push Notification), first names and other elements desired for the personalization of messages, and data elements needed to segment contact lists into target groups. The application segregates client data with logical keys and performs multiple checks to ensure users can access only their organization’s data as provisioned by their organization’s designated application administrators.

### Security Governance and Human Resources

The WCA security program adheres to standard IBM security policies as outlined in the Data Security and Privacy Principles for IBM Cloud Services. The WCA Engage service has been certified as compliant with the ISO/IEC 27001:2013 framework.

IBM conducts extensive background screening, as permitted by law, on all personnel prior to employment. All IBM personnel are required to provide written acknowledgement of security, confidentiality, data privacy, and non-disclosure requirements, as well as complete Cybersecurity and Business Conduct Guidelines training courses during on-boarding and again annually. Human Resources sends notifications of terminations and job transfers to a distribution list of administrators and stakeholders to ensure timely revocation of access.

### Privacy and Compliance

IBM’s business practices comply with applicable laws and regulations in the jurisdictions in which it conducts business. IBM’s Online Privacy Statement and Software and Services Privacy Statement are published online. The WCA Engage service is certified to be compliant with the EU-US Privacy Shield Framework, processes personal data as instructed by clients, and offers standard EU Model Clauses.

The WCA platform provides features to enable clients to comply with laws and regulations related to commercial messaging and data privacy such as CAN-SPAM (US), CASL (Canada), the Data Protection Directive (EU), Privacy and Electronic Communications (EC Directive) Regulations (UK), and the DPA (UK). Features include: logging of opt-in/opt-out activity; support for confirming opt-ins and one-click opt-outs; optional enforcement of double opt-ins; optional enforcement of explicit consent to use browser cookies; web forms to allow recipients to manage their information and preferences; integrated spam scoring; and support for email-authentication frameworks (SPF, DKIM, DMARC).

### Security Testing, Monitoring, Investigations, and Incident Response

A Web Application Security Assessment (WASA) that incorporates external standards such as the OWASP Top Ten and CWE/SANS Top 25 is performed on every major release by IBM ethical-hacking personnel, and at least one per year is performed by an independent third party. The platform infrastructure and network are subject to attack-and-penetration testing and vulnerability scans by IBM personnel at least quarterly and by an independent third party at least annually. All findings from security testing are presented to the appropriate stakeholders for analysis to determine validity and potential risk exposure, then those that present a risk exposure that warrants remediation are prioritized, placed in the schedule accordingly (subject to timing considerations), and tracked through verification of remediation.

In addition to a 24x365 Application Delivery Response Team (ADRT), IBM has personnel dedicated to security in the WCA Security Operations Center (SOC) and the WCA Information Security team, which is independent of Operations; these teams coordinate to design, implement, operate, and monitor overlapping layers of security. WCA Information Security manages and coordinates all investigations and incident response related to security and privacy, engaging other internal teams and resources, including the broader IBM Computer Security Incident Response Team (CSIRT), as appropriate given the nature of the situation. If an investigation indicates that the security or privacy of any client data or accounts may have been compromised, IBM will engage the client to provide the relevant information and solicit participation in the investigation.

### Hosting (Data Center) and Processing Locations

The IBM WCA production infrastructure is colocated within dedicated cages or hosted in a cloud service (depending on the specific instance) within Tier 3 (or higher) facilities that employ physical-security and environmental controls, with redundancy, that meet or exceed industry standards, as evidenced by the SSAE-16 SOC Type II attestation reports and ISO 27001 certifications for the facilities. WCA Engage clients may select from the offered hosting geographies, which are published in the IBM Data Hosting and Other Processing Locations for IBM Cloud Services.

### Platform Architecture, Performance, Reliability, and Monitoring

The IBM WCA Engage platform is based on a highly scalable multi-tier architecture with clusters of load-balanced servers for most key components, providing resilience such that issues with one component rarely affect the platform's availability; each key component that cannot have a load-balanced cluster has a failover server in place. The application automatically manages client programs to ensure resources are efficiently allocated to support all tenants; if monitoring indicates a client program is adversely affecting performance, Support will engage the client to provide assistance in troubleshooting and optimizing the program for better performance. IBM’s 24x7 monitoring and support ensure sufficient capacity, high reliability, and enterprise-class performance are delivered even during seasonal peak periods. The platform’s monthly reliability statistics are published on a rolling 12-month basis on a public website (currently https://www.ibm.com/watson/marketing-automation/reliability).

### Infrastructure Security

In addition to the physical-security controls related to the data centers, the IBM WCA platform incorporates multiple, overlapping layer of infrastructure-security controls and technologies, including:

- Firewalls and load balancers isolating the production environments from all other environments;
- All structured (“contact list”) data are encrypted at rest (on disk);
- Host-based intrusion-detection systems (HIDS) on production servers;
- A Security Information and Event Management (SIEM) system that automatically aggregates infrastructure-security logs, performs data analysis, and alerts security personnel to anomalous activity;
- Anti-virus/anti-malware (AV/AM) solutions; and
- DDoS mitigations implemented at upstream providers.

The SOC and Information Security teams perform ongoing research and conduct proofs of concept to identify opportunities to enhance the platform’s overall security.

### Access to Client Data

No IBM personnel, other than any Services personnel to whom the client has provisioned application-user accounts to assist in operating their campaigns, have regular access to client data through the application. To facilitate troubleshooting, the “Become User” feature, the use of which must be explicitly authorized by the user from within the user account, allows Client Support to temporarily view the account “through the user’s eyes” without requiring the user’s password or allowing the export of data; use of this feature is automatically logged in a secure database table and included in reports sent to Information Security daily for review.

Direct access to client data (at the database layer) is restricted to authorized IBM personnel whose regular job responsibilities require such access and is reviewed by management and Information Security on a quarterly basis to ensure the access remains current and appropriate. Access to the infrastructure in the production environments hosting client data is restricted to authorized personnel and requires a secure VPN with two-factor (software token) authentication. To access production servers, which are configured to deny direct logins, administrators must use SSH to connect to a bastion host and authenticate using LDAP credentials that are independent of those used to access the corporate network; access to network devices is restricted and controlled via TACACS. Policy prohibits the export of client data from the platform without explicit authorization from the client or Information Security. No third parties have access to client data except as required for the delivery of specific optional services authorized in advance by the client.

**Application Security**

The IBM WCA platform offers multiple layers of security and authentication controls, including:

- **Secure connections & data transfers.** All client-user connections to the platform, including the web-based user interface, file transfers, and the suite of APIs, are via the public Internet through standard secure (encrypted) Internet protocols (HTTPS/TLS, SFTP/SSH).
- **Role-based access.** The client's designated application administrators ("Org Admins") provision user accounts, assigning each a standard role (Org Admin, Standard, or Reporting Only), and access to data sets and specific functionality can be provisioned or restricted by role or on an individual, granular basis.
- **Password length & complexity.** The application requires passwords to be at least eight (8) characters in length with, by default, characters from at least three of four categories (upper case letters, lower case letters, numeric digits, and special characters/symbols). Org Admins can strengthen the complexity requirements to meet their organization's standards by requiring up to five (5) characters from each category, and by doing so effectively increase the minimum-length requirement.
- **IP Address Validation.** The application tracks every IP address from which each user has successfully authenticated. If a user submits valid credentials from an IP address that has not previously been validated for the user account, the application sends to the notification email address defined in the user's profile a unique validation code that the user must enter to authenticate and gain access to the application. This feature provides the flexibility of allowing the user to access the application from any Internet connection while still providing reasonable assurance of the user's identity.
- **IP Address Restriction.** The client's Org Admins can configure IP Restriction to explicitly define ("whitelist") the authorized IP addresses and ranges from which individual or all user accounts may access the application. Access attempts originating from unauthorized IP addresses will be denied.
- **Token-based multi-factor authentication (optional service).** The platform offers multi-factor authentication through software-based tokens that generate user-specific transient validation codes that must be verified by an authentication service before access is granted.
- **Limit on invalid login-attempts** is configurable: 3 to 10 invalid login attempts triggers account lockout.
- **Password-reuse restriction** is configurable: 0 to 15 previous passwords cannot be used.
- **Password-expiration frequency** is configurable: 30, 45, 90, 120, or 180 days.
- **Password-expiration warning** is configurable: 3, 7, 14, 21, or 30 days.
- **Inactive-session expiration period** is configurable: 30 minutes; 1, 2, 4, or 8 hours.
- **Self-service password resets with emailed validation code.** Users are able to reset their passwords by clicking on a Reset Password link, entering the unique validation code sent to the notification-email address in their user profile, and then setting their new password.
- **Email notifications for key security events.** A notification is sent to the previously defined email address in the user's profile when any change is made to their user ID, password, or notification email.
- **Security-event logging & monitoring.** The application logs security events, including every login attempt (capturing the time/date, user ID, source IP, and other parameters), and reports of key events are automatically compiled and sent to Information Security daily for review.
- **Storage of user passwords in encrypted form.** User passwords are stored in an encrypted form generated by a strong, salted, one-way hashing algorithm that is highly resistant to cracking.

### Change Management Process, Maintenance Windows, and Downtime

All changes to the WCA platform, including software and infrastructure, are implemented according to a formal Change Control process. Every change is documented in a Change Control Request (CCR) that is reviewed by the Change Control Committee (CCC) for the business justification, potential impact, and completeness of required activities (e.g., applicable testing). Application source code is maintained in a code-repository/version-control tool; system and application builds are maintained in a deployment-automation system that monitors systems for compliance. Approved changes are implemented during scheduled maintenance windows by the Configuration Management and Operations teams using automation tools.

The Engage application operates on a highly customized and integrated platform, therefore all vendor-supplied patches and reported vulnerabilities or control deficiencies are evaluated on a case-by-case basis for applicability and potential risk exposure, prioritized, and placed into the schedule accordingly (subject to timing considerations). Non-emergency patches and fixes are included a full cycle of development and testing to ensure they do not adversely impact the system's operations and performance.

IBM reserves weekly maintenance windows during off-peak hours (e.g., Sunday midnight-04:00 US Eastern for US-hosted clients) for the WCA platform, but maintenance is typically performed no more than once in any 30-day period for a given instance of the platform and rarely involves downtime. IBM announces new releases at least 14 days in advance and planned maintenance at least 48 hours in advance in the Scheduled Maintenance area of the Client Support Portal and/or a splash page displayed upon login, and while access to the application may be limited during maintenance, all recipient-facing activities (e.g., opens, click-throughs, image renders, bounces, etc.) are captured and the transactional-email service remains available.

### Disaster Recovery, Business Continuity, and Data Backups

IBM maintains detailed Disaster Recovery (DR) Plans (as applicable) and an Incident Response (IR) Plan, which contemplates business-continuity (BC) scenarios defined by the availability of key personnel, locations, and resources; these plans are designed to ensure the continuation of the service even for a disruption outside of IBM’s control. As the platform operates on a 24x7x365 basis, support personnel can, and routinely do, work remotely to provide support and maintain continuous service.

For the WCA Engage platform, IBM has implemented a sophisticated, multi-tier backup architecture that utilizes native database features to create multiple backups of the hosted client data per day. Where available, replication of the backups is performed multiple times per day, via a secure encrypted tunnel, directly to disk in a secure secondary data center offering geographic diversity to ensure maximum availability for recovery in the case of a disaster or major outage at the primary site. Portable media (e.g., tapes) are not used for client data. Application source code, system builds, and application builds are backed up.

Due to the WCA platform being a high-volume multi-tenant SaaS environment, IBM does not support the restoration of data for individual clients; platform backups are intended to optimize recovery of the entire multi-tenant instance of the platform from a disaster. The WCA Engage application provides clients with functionality to easily export templates and data in standard file formats for backup and archival purposes. Large files are written to SFTP folders for retrieval. Clients who choose to integrate the platform with their systems can have their data automatically synchronized to ensure their local copy remains current at all times.

### Data Deletion

Clients manage and may delete or overwrite their data at any time while their service is active. Upon deletion of data from the database, the database and underlying storage reclaim the space and overwrite it with other data, rendering the deleted data unrecoverable. As client data are stored exclusively on disk, all copies are purged as backups the replication process overwrites backups. After service termination, the platform retains any remaining data according to the terms of the Services Agreement. Any data-storage devices that are decommissioned or otherwise removed from service are secured until physically destroyed to ensure data cannot be recovered.