CommCare's Security Capabilities

Data Security Overview

Data on CommCare mobile is stored encrypted-at-rest (symmetric AES256) by keys that are secured by the mobile user's password. User data is never written to disk unencrypted, and the keys are only ever held in memory, so if a device is turned off or logged out the data is locally irretrievable without the user's password.

Data is transmitted from the phone to the server (and vis-a-versa) over a secure and encrypted HTTPS channel.

On CommCare's server, your data is hosted in the cloud at an enterprise-grade ISO 27001-compliant data center (AWS). Data is secured with at-rest AES256 encryption, regular offsite backups, intrusion monitoring, biometric physical access security, in addition to other best-practice security measures.

For more details on our security practices, please see Dimagi's **Data Confidentiality & Security Overview**.

GDPR Compliance

CommCare is fully compliant with GDPR. General Data Protection Regulation (GDPR), went into effect on May 25, 2018. GDPR significantly enhances the protection of personal data of EU Data Subjects and increases the obligations on organizations (like us). We wanted to provide such a high standard of data protection to all our customers--regardless of where you are.

GPPR Compliance is only applicable to organizations who plan on collecting data on GDPR Data Subjects. We require such organizations to sign our GDPR Data Processing Agreement. We have signed such **DPAs** with several of our customers.

An important stipulation under GDPR is on collecting clear Consent from EU Data Subjects. CommCare apps allow you to easily collect such consent via Signatures, Initials or via explicit Voice Recordings

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) was established to ensure that patients' protected health information is kept secure and private. CommCare satisfies HIPAA requirements.

All relevant policies and procedures have been fully implemented to provide HIPAA compliance, and we also offer HIPAA business associate agreements (BAAs) to our partners.

SOC 2 Compliance

Dimagi's CommCare solution is certified SOC 2 compliant and our SOC 2 Type 2 Report is now available to your compliance team upon request.

CommCare by dimagi

Key Security Features of CommCare Mobile

1 CONFIGURE YOUR APP'S OFFLINE DATA POLICY

Collected form data is discarded from mobile devices immediately after it is submitted to the server. You may decide to configure certain data elements called Case Data to be available offline only if you need to.

This flexible model allows organizations to design offline data policies aligned with the last mile use cases and security scenarios at hand.

2 ENFORCE STRONG LOGOUT POLICIES

CommCare's mobile apps can be forced to **automatically log out the user** based on a configurable length of time.

3 UTILIZE SECURITY CAPABILITIES OFFERED BY THE ANDROID ECOSYSTEM

The Android ecosystem comes with **many security features** which can be utilized to further optimize your needs for security in volatile environments. Further, **certain third-party apps** can be used by mobile workers to wipe data from their mobile devices during an emergency situation.

4 REMOTE DATA WIPE

Our new Mobile Device Management product, **Focus**, allows you to remotely wipe data from mobile devices in situations when the device is lost or stolen.

Key Security Features of CommCareHQ

1 SSO

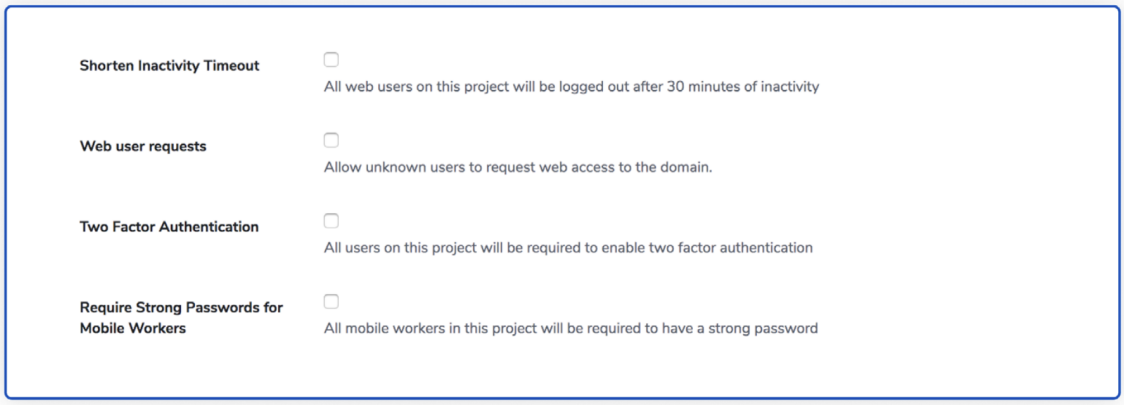
Enforce your security policies by having your users log-in to CommCareHQ using their organizational credentials.

2 RESTRICT WEB USER ACCOUNTS BY THEIR LOCATION

CommCare's Locations feature allows you to **assign a web user account to a given location**, thus making sure a given web user account can only access data collected by mobile workers from their assigned location. Such a setup significantly reduces the potential exposure of sensitive data

3 SECURE WEB USER ACCOUNTS

Project Admins can enforce the following advanced security measures on all web users of their project space:

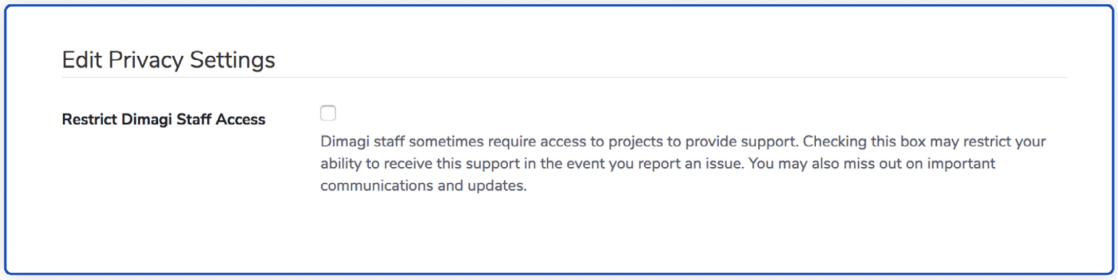


4 SETUP ROLE BASED ACCESS

Using CommCareHQ, project admins can create **custom project roles** and give these roles the desired permissions for accessing parts of your project space. For example, you create a special role for App Builders, Field Implementors and Data Consumers. Such a setup allows admins to provision access on a need to basis.

5 BLOCK DIMAGI'S ACCESS TO YOUR PROJECT SPACES

From your project space's privacy settings, you can disable our access to your project space:



Data Security is of utmost importance to our partners who trust us with their data, and so it is for us. Not only do we use state-of-the-art measures to protect your data, but also as a certified B Corp, we meet the highest standards of verified social and environmental performance, public transparency, and legal accountability to balance profit and purpose.

B Corporation recognized Dimagi on its 2019 Best For the World List in two categories: **Customers** and **Governance**. For the second year in a row, Dimagi was awarded for both our dedication to supporting underserved populations and promoting public benefit, as well as our impact-driven and transparent organizational structure. Please refer to **this blog** for thoughts from our CEO and COO.

Please reach out to us at **info@dimagi.com** if you have any further questions.