DIONA

How it Works

A Strong Foundation

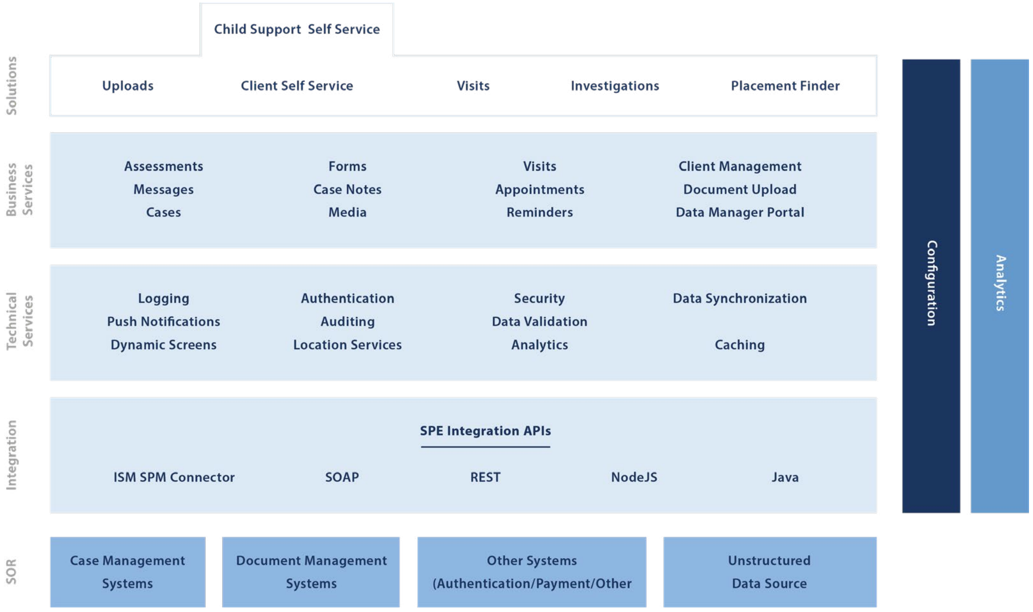
Diona solutions are delivered through a core set of services provided by the Diona Server. With common data adapters, auditing, logging, notifications, assessments infrastructure, hook points, and Mobile Device/Endpoint Management integration, each solution is part of a robust and flexible framework for delivering and managing apps.

Mobile-First Design

Diona recognizes that mobile devices are a transformative technology that is changing every aspect of how work is done and information is shared. Many projects characterized as "mobile" merely involve using mobile devices as a channel for information. Our strategy is different, we fully commit to the potential in mobile devices as a system of engagement to connect users to back-end systems and processes. That's why we build native applications for Android, iOS, and Windows. Native code is the only way to get the level of precision necessary to make great solutions. That's a strong statement, but we stand by it. We exhausted other methods such as hybrid development before accepting that there are no shortcuts to great user experiences.

A Strong Foundation Based on Open Standards

The Diona Server is the engine that facilitates communication between the mobile app and the various systems of record found within a Health and Human Services enterprise architecture. The Diona Server leverages best in breed, open technologies including Node.js® and MongoDB®. These infrastructure components are widely supported and massively scalable which helps ensure that our customers are served well from initial deployment through to future upgrades and requirements changes.



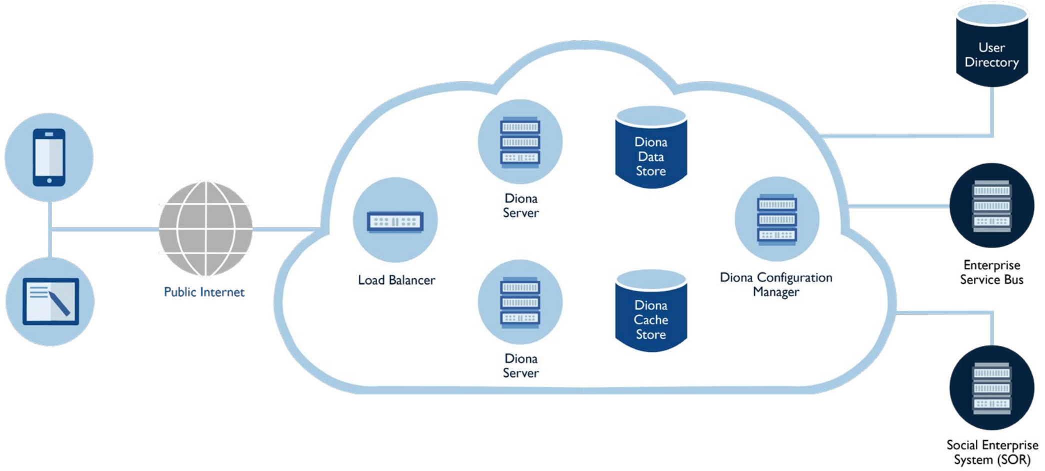
Child Support Self Service

Solutions	Uploads	Client Self Service	Visits	Investigations	Placement Finder
Business Services	Assessments Messages Cases	Forms Case Notes Media	Visits Appointments Reminders	Client Management Document Upload Data Manager Portal	
Technical Services	Logging Push Notifications Dynamic Screens	Authentication Auditing Location Services	Security Data Validation Analytics	Data Synchronization Caching	
Integration	SPE Integration APIs				
	ISM SPM Connector	SOAP	REST	NodeJS	Java
SOR	Case Management Systems	Document Management Systems	Other Systems (Authentication/Payment/Other	Unstructured Data Source	

Configuration

Analytics

Diona Solution Architecture



Diona Deployment Architecture

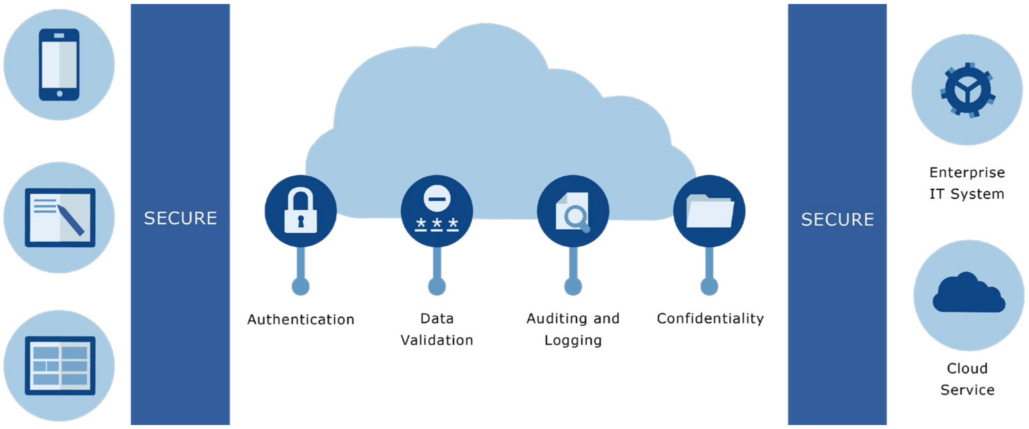
Back-End Diplomacy

Diona solutions are highly interoperable and easy to integrate with existing systems of record out-of-the-box. Through an API-based approach (including REST, SOAP and Java options), integration with multiple back-end systems can be tied in quickly. Each API can be pointed to a different system of record turning Diona solutions into tools to pull essential information from across an agency's different systems.

Diona solutions can also communicate with popular services such as Apache Camel and enterprise service buses.

The Diona Server is architected to allow mobile apps participation in an SOA based Health and Human Services IT ecosystem. Each Diona solutions exposes a set of interfaces that define the required interactions with the various systems of record that store information to be used within the mobile apps. The data adapter layer controls how the Diona Server integrates with these external systems, allowing the end point and transport method to be configured per each interface.

Diona solutions also offers integration to popular cloud-based storage services such as Dropbox and Google.



Diona Security Components

Secure By Design

As Health and Human Services agencies around the world accelerate the deployment of systems of engagement for the mobile channel, one of the most important concerns is security. By nature, mobile solutions have more areas where security risks can manifest themselves than traditional server-oriented solutions like enterprise web applications. To manage the risks, Diona solutions provide secure data storage and transmission using the highest encryption standards.

Device Security

All data held on the device is encrypted using best practice encryption algorithms and techniques. The secret key for encrypting the data is generated by the server and sent to the mobile app during login. The secret key returned from the server is also held in memory while the user is logged into the solution and is used both as the password for the encrypted database and decrypting attachments held on the device.

When the user logs out, is timed out or the solution is closed, the secret key is deleted from memory. For offline login support, the secret key is also encrypted using the user's password as the encryption password and stored in private shared preferences. The user's password is not held anywhere on the device. With each online login, the key is retrieved from the server and used for accessing the encrypted device database and encrypted files.

For offline login (where a server connection is not available) the user's password is used to decrypt the encrypted key held in private shared preferences. This ensures that the key is never stored on the device in plain text format.

Online Login

The credentials supplied by the user are passed to the configured authentication provider. The authentication provider is responsible for determining if the credentials supplied are valid. If the credentials are not valid, a server session is not created and the user is informed that access was denied to the system. For security reasons, the message displayed to the user does not provide any information that could be used to help a malicious user determine valid credentials. If valid credentials are provided, a server session is created.

To support automatic re-connection (when a connection is dropped), the credentials are encrypted on the server using a secret key and a randomly generated salt. The encrypted credentials are sent to the mobile app and held in memory while the user is logged into the device. If the user logs out, is timed out or the app is closed, the encrypted credentials are deleted.

On completion of the login process, the app determines the data that must be uploaded to the server. This will include data re-corded while offline. If such data is present, the app invokes the data upload process to send the data to the server.

Authentication

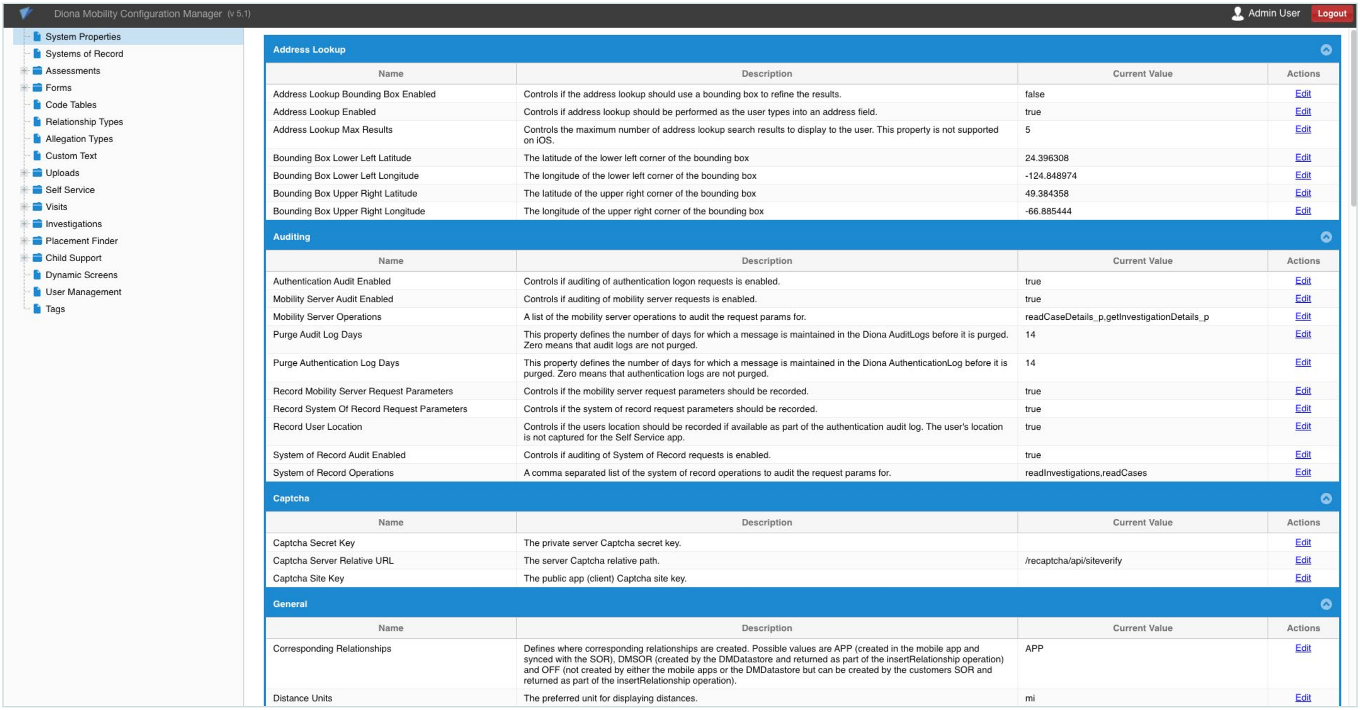
Diona solutions support anonymous usage (no authentication) for certain solutions (Diona Uploads) and credential linked usage for others (Diona Self Service, Diona Visits, Diona Placement Finder, Diona Child Support and Diona Investigations). Access to the credential based solutions requires that the user provide a valid username and password. These credentials must be issued to the user by the organization that has deployed the solution and are typically the same credentials that are used to access the agency's other systems.

Offline Login

When required, Diona solutions support offline usage. The user can continue to use features of these solutions even though their device is not connected to the server. Offline login is an important element of this support. Even though the user's device is not connected to the Internet, the user can still securely log in to the solution. In order to log in offline, the user must have successfully completed at least one online login that day. After each successful online login, a one-way hash of the username and password is created using a randomly generated salt value. For increased security a different salt value is used for each successful login. The hashing algorithm used is SHA-256.

The hashed credentials and salt are stored as private shared preferences and are accessible only via the Diona solution in use. When a user attempts to log in while offline, the username and password are hashed using the stored salt value. The hashed value is then compared to the stored hash in shared preferences. If the values match, the user is able to gain access to the solution.

Unlike online login, offline login does not refresh the locally stored data. The user must work with the data stored on the device from the last online download. The message "You are working offline" is displayed in the title bar. If Internet connectivity is established, the user will remain disconnected from their backend server or system of record. In other words, the user will remain offline until the user logs out of the solution and logs back in again while connected to the Internet.



Address Lookup

Name	Description	Current Value	Actions
Address Lookup Bounding Box Enabled	Controls if the address lookup should use a bounding box to refine the results.	false	Edit
Address Lookup Enabled	Controls if address lookup should be performed as the user types into an address field.	true	Edit
Address Lookup Max Results	Controls the maximum number of address lookup search results to display to the user. This property is not supported on iOS.	5	Edit
Bounding Box Lower Left Latitude	The latitude of the lower left corner of the bounding box	24.396308	Edit
Bounding Box Lower Left Longitude	The longitude of the lower left corner of the bounding box	-124.848974	Edit
Bounding Box Upper Right Latitude	The latitude of the upper right corner of the bounding box	49.384358	Edit
Bounding Box Upper Right Longitude	The longitude of the upper right corner of the bounding box	-66.885444	Edit

Auditing

Name	Description	Current Value	Actions
Authentication Audit Enabled	Controls if auditing of authentication logon requests is enabled.	true	Edit
Mobility Server Audit Enabled	Controls if auditing of mobility server requests is enabled.	true	Edit
Mobility Server Operations	A list of the mobility server operations to audit the request params for.	readCaseDetails_p,getInvestigationDetails_p	Edit
Purge Audit Log Days	This property defines the number of days for which a message is maintained in the Diona AuditLogs before it is purged. Zero means that audit logs are not purged.	14	Edit
Purge Authentication Log Days	This property defines the number of days for which a message is maintained in the Diona AuthenticationLog before it is purged. Zero means that authentication logs are not purged.	14	Edit
Record Mobility Server Request Parameters	Controls if the mobility server request parameters should be recorded.	true	Edit
Record System Of Record Request Parameters	Controls if the system of record request parameters should be recorded.	true	Edit
Record User Location	Controls if the users location should be recorded if available as part of the authentication audit log. The user's location is not captured for the Self Service app.	true	Edit
System of Record Audit Enabled	Controls if auditing of System of Record requests is enabled.	true	Edit
System of Record Operations	A comma separated list of the system of record operations to audit the request params for.	readInvestigations,readCases	Edit

Captcha

Name	Description	Current Value	Actions
Captcha Secret Key	The private server Captcha secret key.		Edit
Captcha Server Relative URL	The server Captcha relative path.	/recaptcha/api/siteverify	Edit
Captcha Site Key	The public app (client) Captcha site key.		Edit

General

Name	Description	Current Value	Actions
Corresponding Relationships	Defines where corresponding relationships are created. Possible values are APP (created in the mobile app and synced with the SOR), DMSOR (created by the DMDatastore and returned as part of the insertRelationship operation) and OFF (not created by either the mobile apps or the DMDatastore but can be created by the customers SOR and returned as part of the insertRelationship operation).	APP	Edit
Distance Units	The preferred unit for displaying distances.	mi	Edit

Diona Configuration Manager

Configuration

Diona solutions provides flexibility and control from the first day of implementation through the complete life-cycle of the solution. Through configuration, changes in business requirements can be accommodated without a need to re-code the solution.

All Diona solutions are configurable through the Diona Configuration Manager. The Diona Configuration Manager gives agency IT administrators the ability to tailor their enterprise mobility solutions to suit the requirements of their system, process, and users.

Administrators are able to change diverse elements such as launch screens, menus, fields, screen images, contents and flow of assessments and forms, content of notifications, multiple language support, system logging, and security and authentication.

Both back-end and front-end parameters can be set through a graphical interface.

Different sets of configuration details can be implemented at three stages in the lifecycle of implementing the solution: Installation, Build Time, and Run Time. A configuration-based approach to software management offers three benefits:

1. Changes can be made rapidly and safely without touching the code.
2. The user interface on an installed app can be changed on the fly without re-installation.
3. The administrator has a clear and unified view of how a solution has been configured and which parameters they can change.

Sophisticated Data Handling for Sophisticated Data

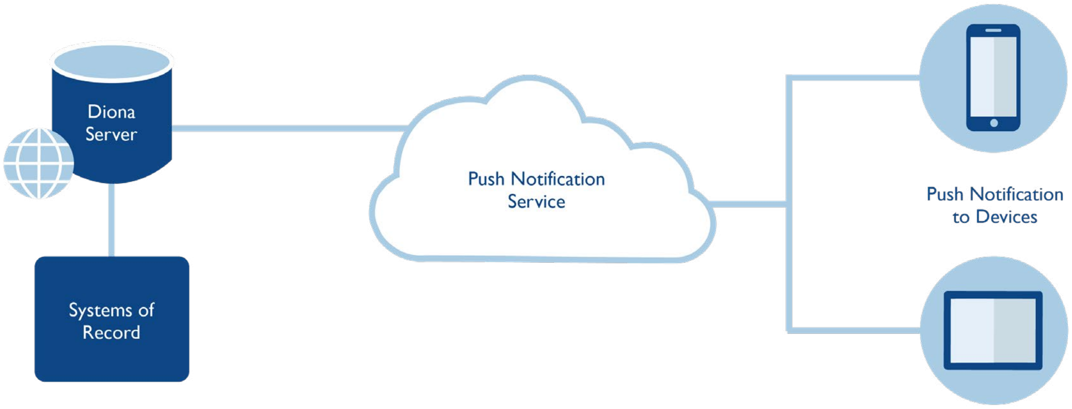
The rise of mobile solutions is paralleled by the rise of richer content in larger sets of data such as video. This can be a challenge for agencies managing back-end systems and systems of record that were implemented long ago. Diona solutions provide a secure supplemental database that acts as a sidecar to agency systems of record. New media types and data options can be supported without re-inventing the back-end.

Assessments and Forms Infrastructure

Assessments and forms are the backbone for much of the work done by Health and Human Services agencies. The Diona assessments and forms infrastructure provides agencies with the ability to rapidly configure and deploy mobile assessments and forms without any special tools or coding. The assessments and forms are integrated with Diona solutions such as Diona Investigations and Diona Visits. With a simple and intuitive user interface including swipe and wipe gesture support and inking support, social workers can navigate and complete their assessments and forms easily and quickly while staying focused on the visit or investigation.

Notifications

Push notifications are an important part of all mobile applications. The Diona Server exposes a set of interfaces that facilitate the distribution of the notifications to mobile devices. To send a notification, the system of record makes a call out to the Diona Server, which looks up the set of devices that should receive the notification based on the message type, application ID and username. A push notification service such as Google Cloud Messaging (GCM) is used to distribute the notification to the appropriate mobile devices. Upon receipt of the notification, the user taps on the message and is taken to the appropriate location in the app to view the details of the message.



Diona Notifications