



OrthoWeb: Cloud and Application Security

Overview of security architecture, features, and administration

Contents

Overview.....	2
Architecture	2
User Management and Authentication	4
Session Security.....	5
Data Access and Transmission.....	5
Auditing.....	5
Application and Database Security	5
Data Storage	6
Sharing and Collaboration	6
TraumaCad®	8
VoyantLink™	9
Notices.....	9

OrthoWeb™ Security

Overview

OrthoWeb™ is a highly secure, web-based service designed to give surgeons convenient access to their orthopedic surgical cases from wherever they need them. The OrthoWeb system provides users with easy-to-use tools for securely transferring data to and from their cloud-based account, and TraumaCad® for planning fracture treatment, joint replacement, and deformity correction procedures.

Voyant Health is dedicated to the security and integrity of our customer’s data. All of our systems and applications are designed from the “ground up” for security, reliability, and scalability. This document describes the architecture and security features of the OrthoWeb system and its applications.

Architecture

OrthoWeb and other cloud-based services from Voyant Health are built on VoyantWeb™, our robust and scalable cloud infrastructure. A suite of integrated cloud technologies, VoyantWeb leverages industry-leading cloud platforms from Salesforce.com and Amazon. These cloud services were selected for their known scalability, reliability, security and established trust among large organizations in healthcare, finance, and other sectors.



Figure 1 – OrthoWeb and VoyantWeb architecture

VoyantWeb’s major components are Storage Services (file storage on Amazon S3), Web Services (integration services hosted on Amazon EC2), and Data Services (application logic and database hosted on Force.com).

Applications such as TraumaCad and VoyantLink™ Desktop connect to OrthoWeb through SSL-secured web services hosted on VoyantWeb Web Services. When accessing or uploading case data (such as uploading DICOM files using VoyantLink Desktop or saving planning data using TraumaCad), these integration services communicate within the secured cloud environment with the VoyantWeb Storage Manager. The VoyantWeb Storage Manager relays all storage commands to VoyantWeb Storage Services for saving or retrieving images.

Users access case data stored within VoyantWeb’s Data Services through the OrthoWeb web application hosted on Force.com, while applications access case data through a VoyantWeb Data Services Proxy which provides secured access to case data through a combination of encoded session IDs and SSL encryption.

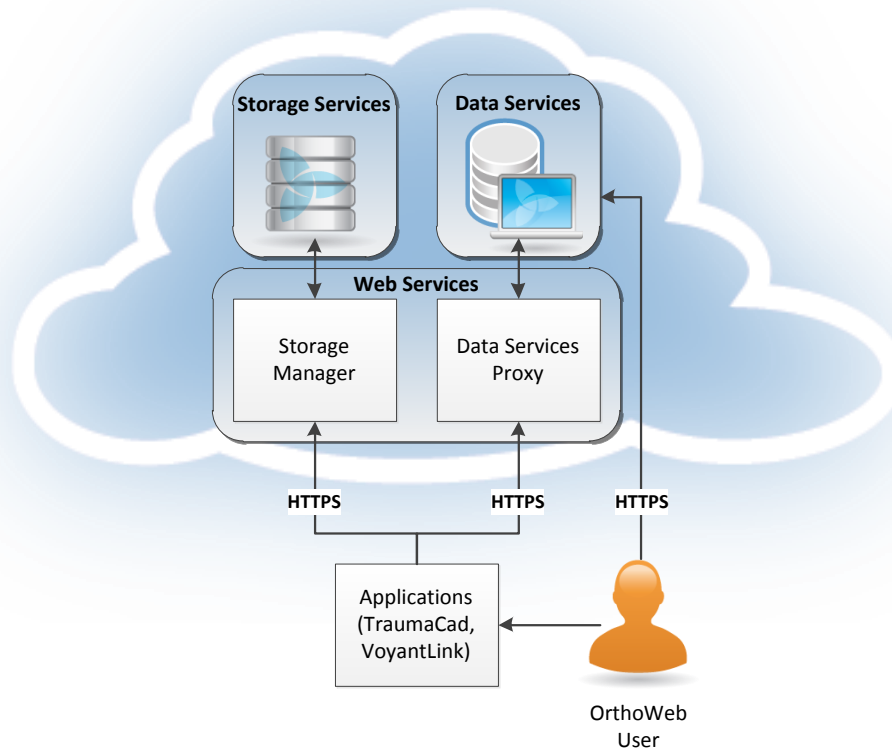


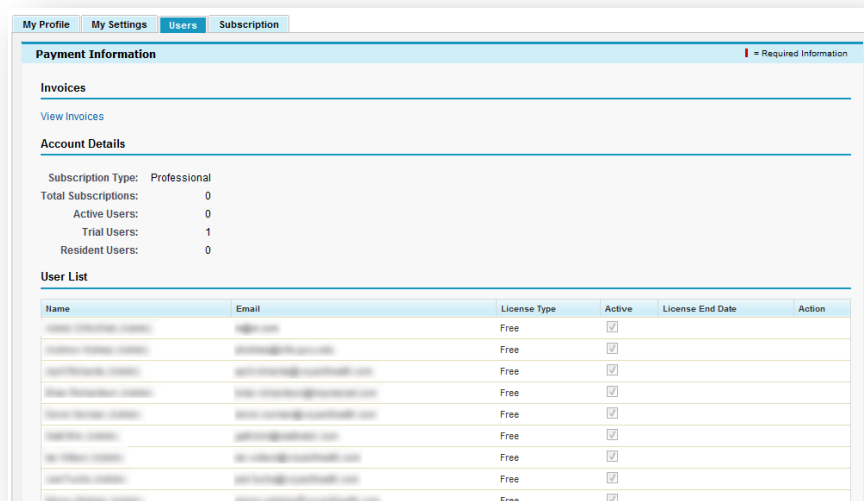
Figure 2 - VoyantWeb Infrastructure



User Management and Authentication

OrthoWeb users are defined as belonging to either the standard or administrator roles. In addition to standard user functions, Administrators (for Professional accounts only) can perform the following functions:

- Add or remove (disable) users
- Enable/disable case auto-sharing¹
- Access audit trail data and reports²



The screenshot shows the 'Users' tab in the OrthoWeb interface. It includes sections for 'Payment Information', 'Invoices', 'Account Details', and a 'User List' table.

Payment Information					
Invoices					
View Invoices					
Account Details					
Subscription Type: Professional					
Total Subscriptions:	0				
Active Users:	0				
Trial Users:	1				
Resident Users:	0				
User List					
Name	Email	License Type	Active	License End Date	Action
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		
[Redacted]	[Redacted]	Free	<input checked="" type="checkbox"/>		

Figure 3 - Account User Management

To access OrthoWeb, users must be assigned a unique user name (email address). When a new user is added to an account, the user receives a notification email with a link to verify their email address and prompt the user to set their password. Users may reset their password by using the “Forgot Password?” link on the OrthoWeb home page to send a password reset link to their registered email address.

Users must log into OrthoWeb through the OrthoWeb.com web site, TraumaCad, or VoyantLink using valid OrthoWeb credentials prior to accessing data stored in their account or shared with them by other users. After logging in, users have access to applications and data to which they have been granted access, based on their account, role and subscription type.

¹ Feature available in Spring 2011 release

² Reports available upon request. Admin user access to reports planned for Summer 2011 release.



Session Security

Upon logging in, a user session is created. User sessions remain active until the user logs out but are also subject to a timeout period. If the user is inactive for a period of time, he/she will be automatically logged out.

A session “cookie” is created to record encrypted authentication information for the duration of the session. The “cookie” contains the encoded session ID, but does not contain the usernames, passwords, or other confidential information.

All user sessions are secured using industry-standard 128-bit SSL encryption.



Data Access and Transmission

In order to access data within the OrthoWeb system, the user must have authenticated and created a valid user session (described above). To access file data stored within OrthoWeb, the user must have a valid session and have been explicitly granted permissions to access the case data.

All data uploaded to or downloaded from OrthoWeb is transferred over a secured connection. All OrthoWeb.com web pages, web services, and communications with applications such as TraumaCad and VoyantLink are always secured using HTTPS (128-bit SSL) connections.



Auditing

User logins to OrthoWeb.com (including user’s IP address) are recorded and maintained for 6 months. User access to all cases, applications, and files within OrthoWeb as well as user actions such as editing case details and sharing cases are recorded in the audit trail.

Audit trail reports can be generated by date/time, user, or patient³.



Application and Database Security

OrthoWeb is built on the Force.com cloud platform from Salesforce.com. Prior to publishing an application on Force.com, developers must submit their code to Salesforce.com for a thorough security evaluation. This evaluation includes auditing of the code for security vulnerabilities, as well as the security of any systems and applications the code interacts with. Salesforce.com is SAS 70 Type II, SysTrust, and ISO 27001 certified.

All services and applications hosted by OrthoWeb are maintained within datacenter facilities located in the United States only.

³ Reports available upon request. Admin user access to reports planned for Summer 2011 release.

Additional information about Force.com security can be found at:
http://wiki.developerforce.com/index.php/Secure_Private_Trustworthy_Force.com_Whitepaper



Data Storage

OrthoWeb file data is stored within Amazon S3, a robust storage service designed for 99.999999999% durability. S3 stores data redundantly on multiple devices across multiple facilities to ensure availability, and uses Content-MD5 checksums and cyclic redundancy checks (CRC) to ensure data integrity. Amazon is ISO 27001, SAS 70 Type II, PCI DSS Level 1, and FISMA certified and accredited. All files stored within the OrthoWeb system are encrypted using the AES symmetric-key encryption standard with a 256-bit key.

All data stored and processed by OrthoWeb is maintained within datacenter facilities located in the United States only.

Additional information about Amazon Web Services can be found at
<http://aws.amazon.com/security>



Sharing and Collaboration

OrthoWeb's case sharing functionality allows users to provide shared access to cases for their colleagues. Users can select OrthoWeb colleagues to share a specific case with. When sharing a case, users select the OrthoWeb user to share the case with, and then select permissions for shared case access. Users can permit their colleagues read-only access, or allow editing of the case (for example, adding a TraumaCad-templated image).

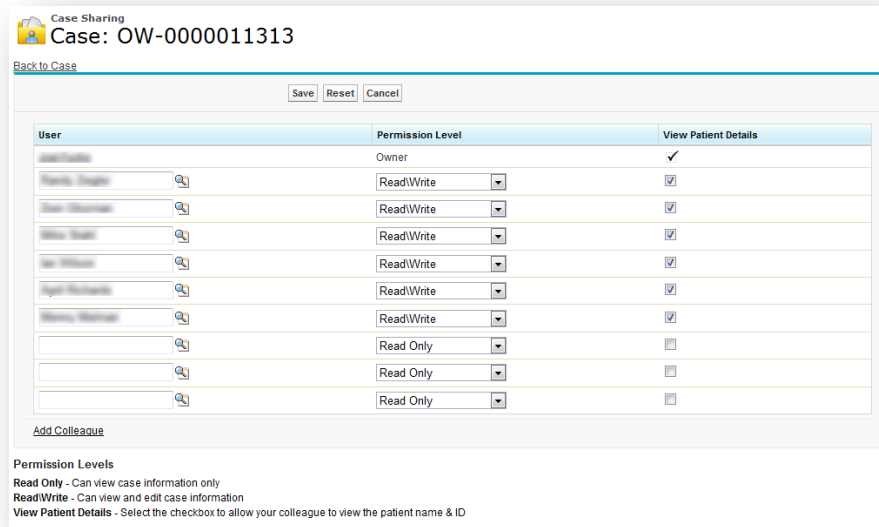


Figure 4 - Case Sharing Setup

Users can also choose whether to share patient-specific details with their colleague by showing or hiding (anonymizing) protected health information (PHI) within the case.

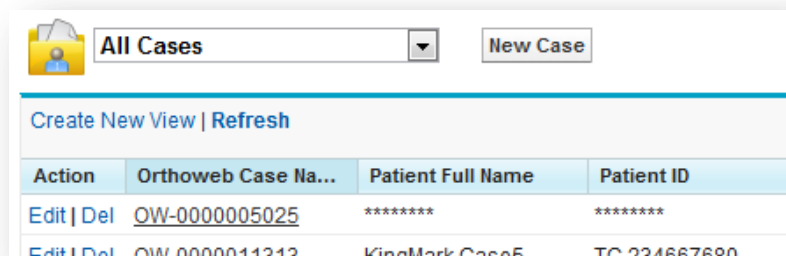


Figure 5 - Case shared without patient details

In addition to manual case sharing, account administrators can configure automatic sharing rules using the same permission structure to create sharing groups for their users. All case sharing takes place within the secured OrthoWeb environment between registered users. Users must authenticate using valid OrthoWeb credentials before viewing case data.

Shared cases can be “followed” by members of the sharing group. Users can post comments on the case, and members of the sharing group can view comments and notifications of case updates in their OrthoWeb home page’s news feed. Only colleagues added to the sharing group by the user or administrator can access case information, including viewing case comments.



TraumaCad®

TraumaCad users can open images from their OrthoWeb cases, and save planning data back to their OrthoWeb account. When launching TraumaCad from OrthoWeb, the user's session data is securely passed to TraumaCad, allowing the user to work with OrthoWeb data within TraumaCad without the need for re-authentication.

When launching a standalone or server-based version of TraumaCad, users can log in using their OrthoWeb account credentials. Once authenticated, users can search for and open images from their account. When ready to save their planning data, authenticated users can save the data back to their OrthoWeb account. All communication, including authentication and image transfer takes place over a secured, industry-standard 128-bit SSL connection.



Figure 6 - My OrthoWeb Account Login

While TraumaCad is a Windows-based application, OrthoWeb users on the Mac OS X platform can access TraumaCad through a hosted Citrix environment. When accessing OrthoWeb using their Mac's web browser, TraumaCad will be launched within a Citrix session. Citrix sessions are generated automatically and are unique to each authenticated user's OrthoWeb session ID. Sessions are secured using Citrix's ICA encryption, and user authentication data is passed to TraumaCad entirely within the secured OrthoWeb environment.



VoyantLink™

VoyantLink is a desktop application provided to OrthoWeb users for uploading images from their PACS or local computer to their OrthoWeb account, or for downloading images from their OrthoWeb™ account for local or PACS-based storage.

Like all other OrthoWeb applications, all communication including user authentication and data transfer is done over 128-bit SSL-encrypted connections. Users must authenticate using valid OrthoWeb credentials before accessing data stored within their OrthoWeb account. When launched from within an authenticated user's OrthoWeb account, the user's session data is securely passed to VoyantLink.

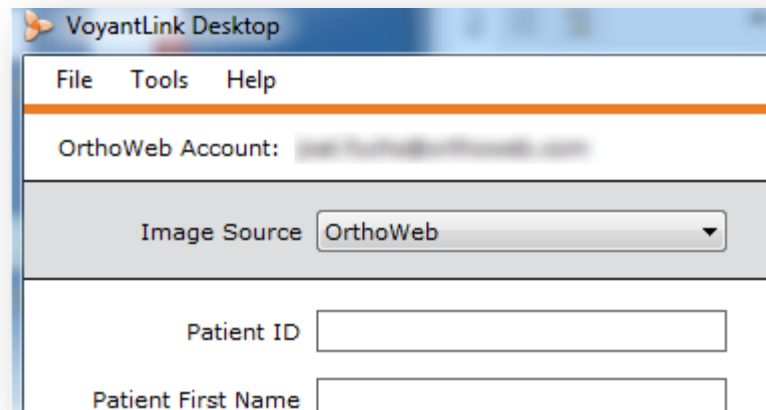


Figure 7 - User logged into VoyantLink using OrthoWeb account credentials

Notices

© 2011 Voyant Health, Ltd., or its affiliates. This information is provided for informational purposes only. The information furnished in this material is believed to be accurate at the time of distribution; however, Voyant Health, Ltd. assumes no responsibility for its use. Voyant Health, Ltd. reserves the right to alter this information at any time without notice