SOUND BUSINESS SYSTEMS

Winscribe

Security and Encryption

sales@soundbusiness.co.nz

New Zealand
phone: 0800 342828
+64 9 3003030
soundbusiness.co.nz

Sound Business Systems
Unit 3, 62 Paul Matthews Road, Rosedale
Auckland 0632, New Zealand

Australia
phone: 1300 83 08 02
soundbusiness.au

Contents

Introduction

This document outlines the different methods of authentication, authorization and encryption utilized by the Winscribe Digital Dictation, Text, and Mobility products. It is intended for network administrators with a good understanding of network topology and transport protocols.

Winscribe Digital Dictation

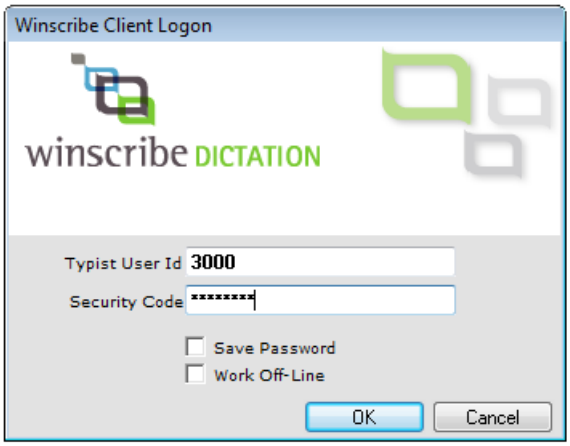
Authentication

Winscribe Digital Dictation (Winscribe DD) offers two methods of authenticating users as valid Winscribe users. These two methods are:

- Winscribe Authentication
- Active Directory Authentication

Winscribe Authentication

Winscribe Authentication is a simple process of entering a valid Winscribe user id and password combination. When starting a Winscribe client application, the Winscribe login dialog is displayed, prompting the user to enter their user ID and password.



Where security is less important, users can tick the *Save Password* check box in order to retain their login credentials for the next login.

Password Policy

Administrators can define a facility-specific password policy that can:

- Force users to change their password after a defined period
- Prevent users from re-using their most recent passwords
- Lockout users for a defined period following three failed login attempts
- Define a minimum password length
- Force users to change password at their first logon
- Force passwords to comply with complexity requirements
- Prevent users from saving their passwords on the logon dialog

Active Directory Authentication

Winscribe DD also supports user authentication by integrating with Active Directory (AD). Winscribe users who wish to use this option are associated with an AD user allowing the AD user properties (contact details) to be synchronized with the Winscribe user database.

When an AD integrated user starts Winscribe, they are not prompted to login with the standard Winscribe login dialog. Instead, their current Windows login credentials are used for authentication. If the credentials do not match an AD integrated Winscribe user, the user is prompted to enter a valid domain, login id, and password to continue.

Certificates and IP Restrictions

Because Winscribe DD client applications utilize IIS and HTTP(S) to communicate with the server, standard security restrictions available through IIS operate transparently within Winscribe. Examples of additional security measures that can be employed are:

- Client Certificates:

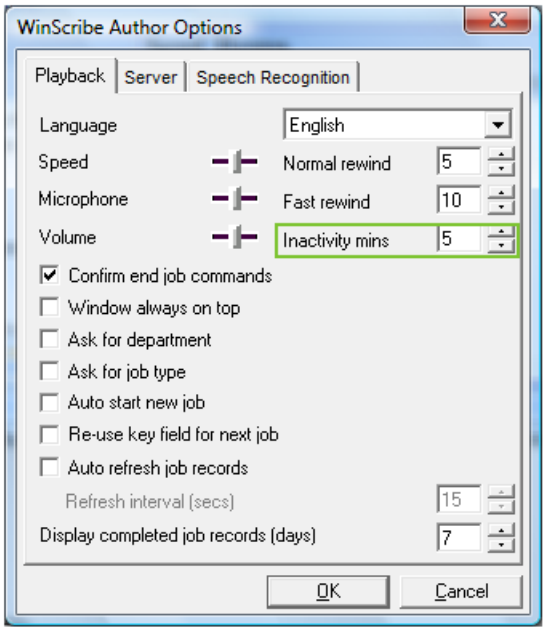
  To confirm client identity, a client certificate can be requested when Winscribe connects to the server. Only clients with a valid client certificate will be able to connect.

- IP Address Restrictions:

  IP address ranges can be specified to ensure only selected devices can utilize the Winscribe server services.

Automatic Logoff

To maintain security when users forget to logoff, Winscribe DD can be set to perform an auto logoff after a defined period of inactivity.

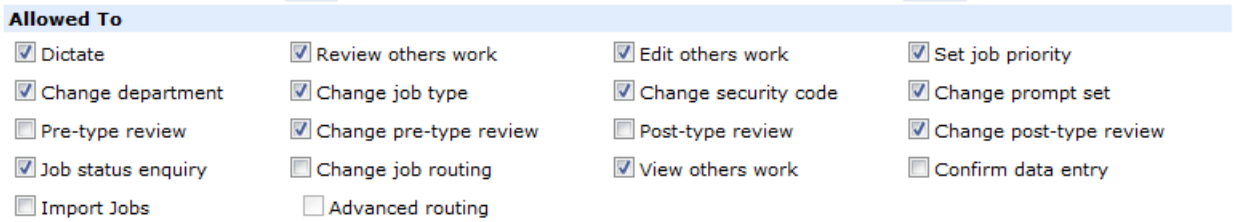


Authorization

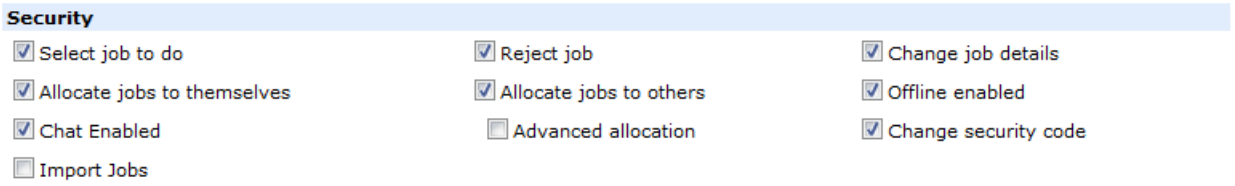
Winscribe DD allows detailed control over the information available to a user based on his/her role within the system. Authorization permissions can be set on a per-user basis through the Winscribe management interface.

By setting appropriate permissions, managers can limit access to specific database entities and categories of data within these entities, as well as applying filters to limit the records visible to specific departments.

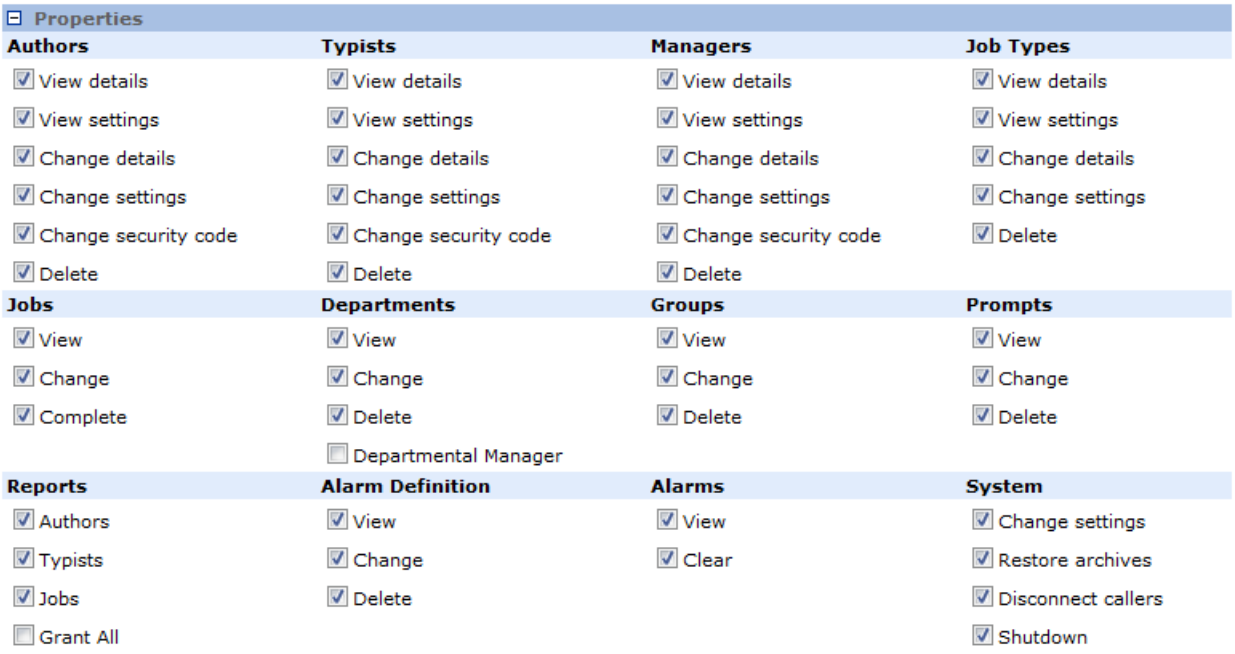
Author's security settings



Typist's security settings



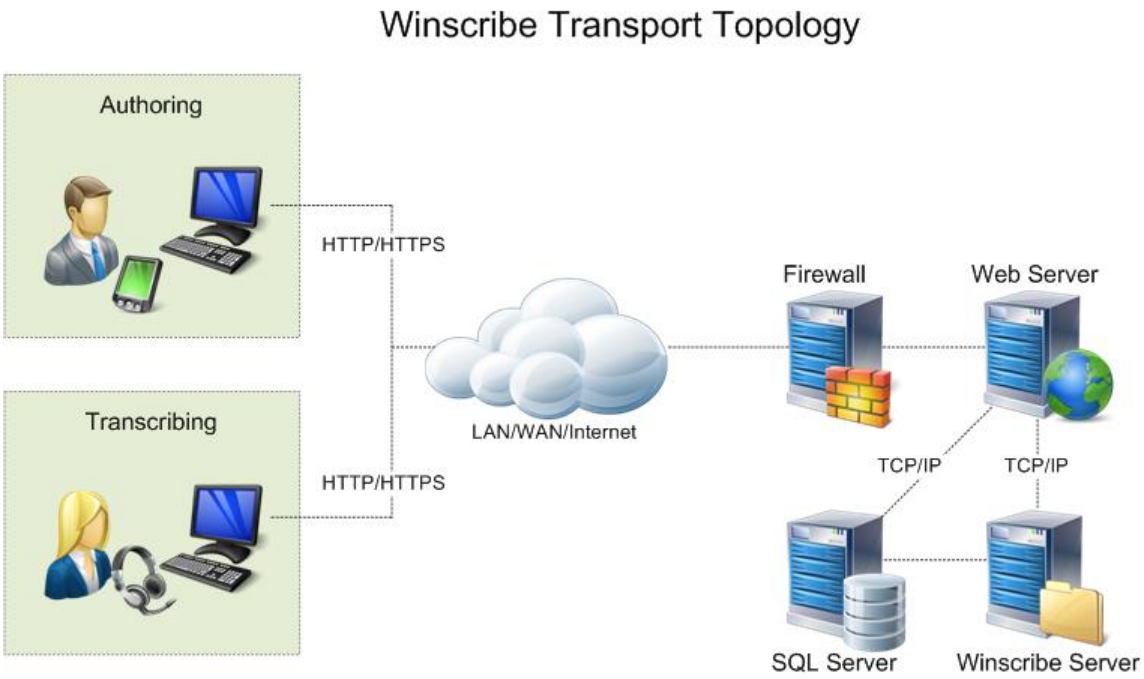
Manager's security settings



Transport

The Winscribe client applications utilize the HTTP or HTTPS protocol to transport audio and data to the Winscribe server. Microsoft's Internet Information Server (IIS) is employed as the enabling technology for this protocol. Data and audio are uploaded using standard HTTP POST, PUT and GET commands.

Options are available for changing the default TCP/IP port used to communicate with the server, as well as throttling bandwidth used by the server connection.



Encryption

Winscribe DD employs two types of encryption to ensure the security of data transferred between, and stored on, client and server machines. These two types are:

- Winscribe Encryption
- HTTPS Encryption

Winscribe Encryption

Winscribe clients can operate offline, so dictation information must be stored on local machines to facilitate this feature. For this reason, all dictation audio is immediately encrypted (using 32-bit private key encryption) before being written to the local hard disk. The voice files remain encrypted for the entire duration of the job, only being unencrypted in memory prior to its use. This includes when the voice files are being transported via HTTP or HTTPS protocols and also when stored on the Winscribe Servers hard disk drives(s).

HTTPS Encryption

When HTTPS is employed as the transport protocol, all data is encrypted prior to transmission, and unencrypted on receipt. HTTPS ensures that any data intercepted during transmission cannot be unencrypted (in a reasonable time frame) by using a public/private key pair which is not transmitted with the data.

Data and File Storage

Winscribe DD uses Microsoft SQL Server (including MSDE) technology for the storage and security of all the data associated with the Winscribe system, with the exclusion of the voice files. The SQL Server user id and password settings control the level of security imposed on the programs accessing the Winscribe data. All Winscribe programs use an encrypted SQL user id and password, which is stored in the registry and is decrypted in memory before being used.

The voice files are stored on the Winscribe Servers HDD system and remain encrypted at all times. Access to these files is controlled by the Winscribe Share permissions and these can be limited to the Winscribe Web Components PC, the Web Manager PC, the Dictation Server PCs and the Exporter PC, which may be the same PC in many cases.

Voice file storage is in a separate directory for each facility thus maintaining the physical separation of the voice files for each facility. Voice file storage can also be at a separate physical location to the data storage, thus reducing bandwidth requirements for accessing voice files.

Mobility for Winscribe Digital Dictation

Encryption

iPhone

Dictation

- Winscribe MD
- Winscribe Professional

Recorded audio is password encrypted with a proprietary scheme, prior to being stored on the device.

Jobs sent to the server as .wav files are not encrypted. SSL(HTTPS) should be enabled for the IIS virtual folder (Winscribe WSPPCServer or Winscribe MD WSMobService) to ensure security and encryption of these files.

Storage

- Winscribe Professional — No patient fields exist, however, the user may voluntarily store patient IDs in the internal database. Database is not encrypted.
- Winscribe Medical — Stores patient information in the internal database (all the fields the user sees on-screen). Database is not encrypted.

Android / BlackBerry 10

- Winscribe MD
- Winscribe Professional

Recorded audio is password encrypted with a proprietary scheme, prior to being stored on the device.

Jobs sent to the server as .wav files are not encrypted. SSL (HTTPS) should be enabled for the IIS virtual folder (Winscribe WSPPCServer or Winscribe MD WSMobService) to ensure security and encryption of these files.

Summary

The following table summarizes the status of the encryption available in the Winscribe Professional and MD apps, from the following aspects (with a quick summary provided below the table):

- Storage of data on device, i.e., local database
- Transmission of data between device and server
- Storage of recorded audio on device

Question	iPhone PRO	iPhone MD	Android PRO	Android MD
Data encrypted on device	No, but is stored in an isolated storage area on the phone. Security relies on this isolation and protection that Apple make available to the user such as password enabled devices.			
If yes, what format?	-			
Data transmitted with encryption	Yes, when transmitted via HTTPS.			
If yes, what format?	The transport is 256 bit encrypted by virtue of the fact that IIS handles 256 bit SSL encryption at a communication protocol level (https).			
Audio Encrypted on the device	No, but is stored in an isolated storage area on the phone.		Recorded audio is password encrypted with a proprietary scheme, prior to being stored on the SD card.	

In essence, we encrypt audio files on Android devices because these files are stored on a removable SD card. This problem does not occur on iPhone devices as the audio is stored in an un-accessible location (sand box).

On both Android and iPhone devices, the database is stored in an inaccessible location (sand box).

Encryption of the audio to the iPhone apps was made available with v1.1.9 in March, 2013.

We currently do not add encryption to the database on any device.

Data in Transit

Both the Winscribe Professional and MD apps allow dictation to be sent directly to a Winscribe server through a secure HTTPS transmission to meet the requirements for secure client data transmission.

Secure data transmission via HTTPS over Wi-Fi and Cellular connections. The SSL layer adds an additional 128 or 256-bit encryption with 2048-bit asymmetric cryptography on top of the already encrypted file to ensure patient data is transmitted securely to the server. The actual encryption depends on the cipher suite negotiated by the device and server, the cipher suites specified on the receiving server, and the strength of the SSL Certificate used. Our mobile apps can use whatever SSL certificate is installed on the server: TLS 1.2 RSA, DHE and AES 128/ 256 SHA-1 (until 01/01/17) and SHA-2.

Data at Rest

All audio files are password encrypted with a proprietary scheme ensuring files are secure at all stages of the dictation process.

In addition to encryption to the server ID, both the Winscribe Professional and MD apps encrypt data to the device ID, so that in the unlikely event the files are obtained from the device, these would not be decipherable. This is in addition to any security and encryption already provided by the phone itself.

Inactivity Timeout

Both the Winscribe MD and Professional apps include a configurable inactivity timeout requiring the user to enter the password, should the app be suspended and accessed at a later time.

One Way

Both the Winscribe Professional and MD apps cannot download audio from previous sessions, only audio that is recorded on the device can be played back. Once the file is removed from the device, it cannot be downloaded from the server for playback.

MDM Software

While the Winscribe Professional and MD apps are not specifically programmed to work with MDM software (as of yet), some of the security features and settings can be applied to the device and will work effectively with the apps: remote wipe, secure tunneling, etc.

Winscribe Text

Desktop Security Considerations

Winscribe Desktop was designed in conjunction with the healthcare industry, where environment, patient safety, and data security are at the forefront of concerns.

Authentication

Winscribe Text offers two methods of authenticating users as valid Winscribe users. These two methods are:

- Winscribe Authentication
- Single Sign-On Authentication

Winscribe Authentication

Winscribe Text uses unique user ids and security codes, as well as multilevel access to ensure only authorized access to confidential information and reports is maintained at all times.

Winscribe Authentication is a simple process of entering a valid Winscribe user id, and password combination. When starting a Winscribe client application, the Winscribe login dialog is displayed, prompting the user to enter their user id and password.

Single Sign-On Authentication

Winscribe Text supports single sign-on, i.e. bypassing the Winscribe Desktop login screen by using the AD credentials of the current Windows session.

To enable single-sign-on from the Desktop, both the Corridor, and Desktop, must be marked for **Enable single sign on** during installation, and the Corridor web server (IIS) must have *SSL* enabled.

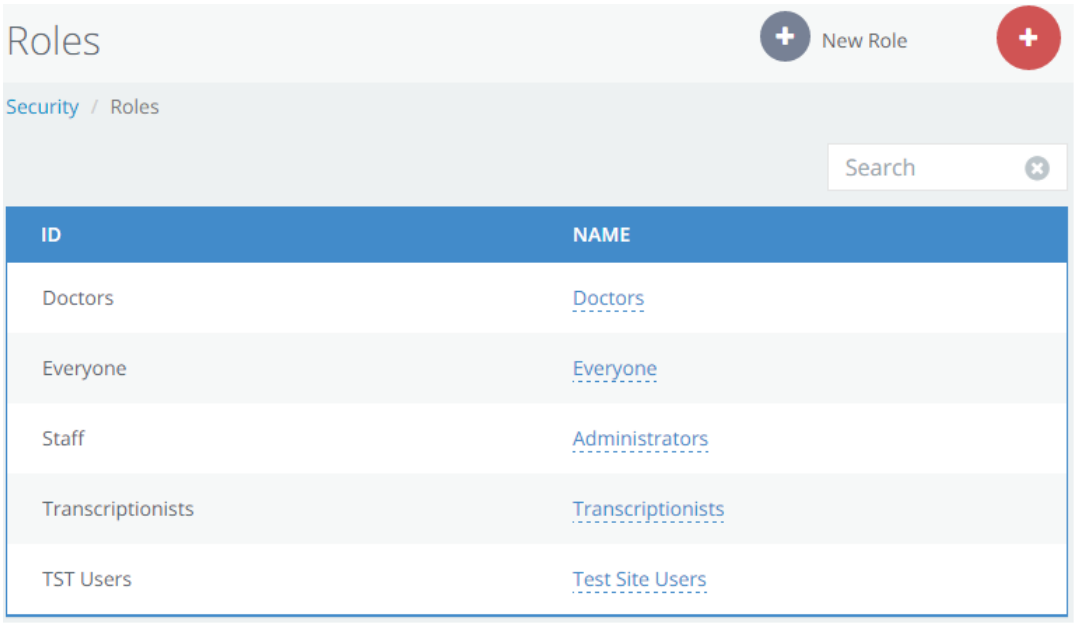
During Desktop single-sign-on, failure to authenticate will result in the login dialog being displayed, where the user may specify credentials.

Authorization

Winscribe Text features a **Security** section (in the **Web Admin**), where the system's *User Roles* are configured. Roles are the permission sets that govern what each user may do (and not do) within the system. This facility gives administrators detailed control over the information available to each user based on his/her role within the system.

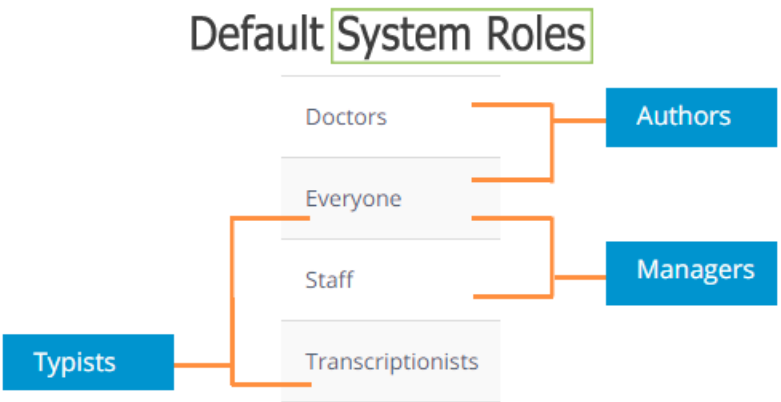
There are two types of role:

- System Role
- Custom Role

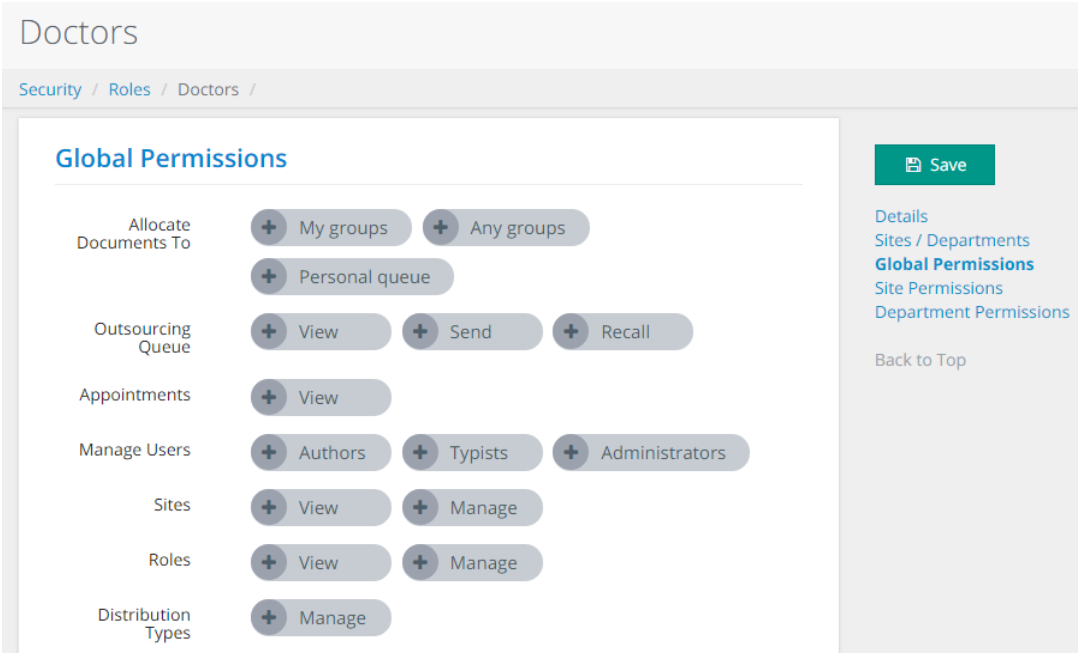


System Roles

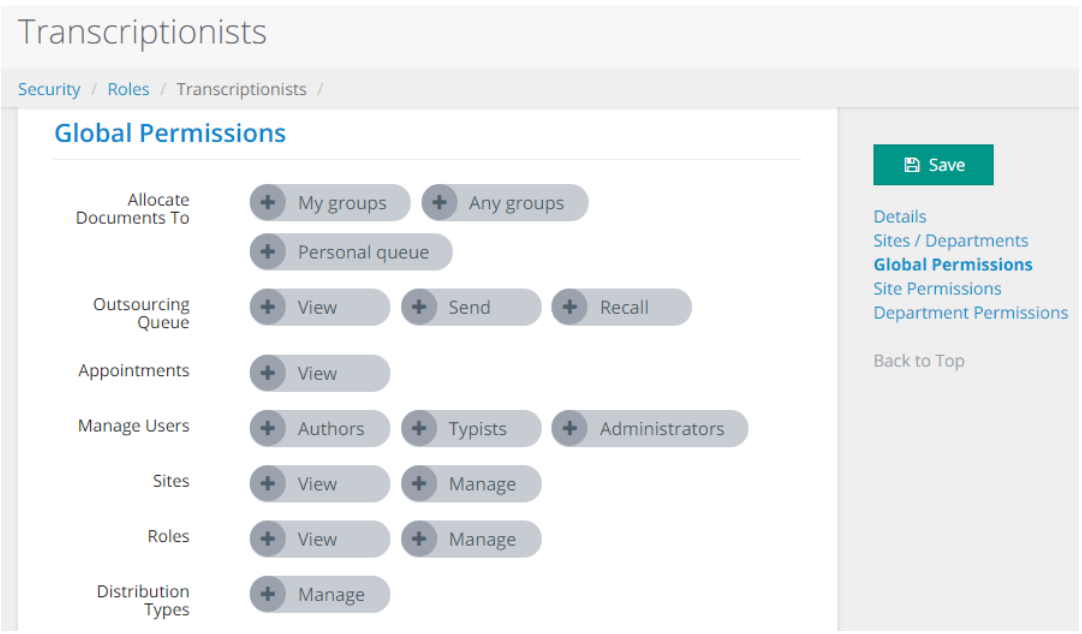
Each user in Winscribe Text (authors, typists, staff) has two default System Roles: *Everyone* plus that of his/her user type:



Doctors' Role

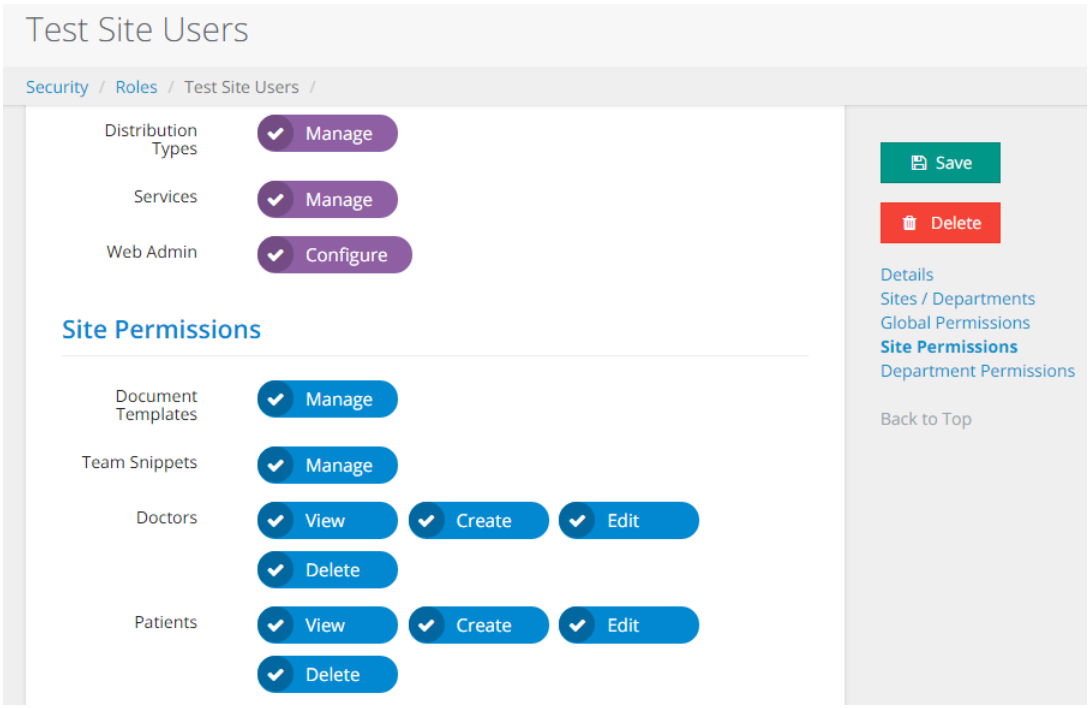


Transcriptionists' Role



Custom Roles

Custom Roles define which sites and departments a user may access, and what he/she may do in these. Users may be assigned multiple custom roles.



Transport

The Winscribe Text client applications utilize the HTTP or HTTPS protocol to transport audio and data to the Winscribe server. Microsoft's Internet Information Server (IIS) is employed as the enabling technology for this protocol. Data and audio are uploaded using standard HTTP POST, PUT and GET commands.

Options are available for changing the default TCP/IP port used to communicate with the server, as well as limiting network traffic.

Encryption

Winscribe Text employs two types of encryption to ensure the security of data transferred between, and stored on, client and server machines. These two types are:

- Winscribe Encryption
- HTTPS Encryption

Winscribe Encryption

All dictation audio is encrypted using 32-bit proprietary scheme (the Text app stores audio in native iOS formats, and converts it to encrypted VOX while it is in the Outbox). Voice files remain encrypted for the duration of the job, only being unencrypted in memory prior to its use; this includes when the voice files are being transported via HTTP or HTTPS protocols and also when stored on the Winscribe Servers hard disk drives(s).

HTTPS Encryption

When HTTPS is employed as the transport protocol, all data is encrypted prior to transmission, and unencrypted on receipt. HTTPS ensures that any data intercepted during transmission cannot be unencrypted (in a reasonable time frame) by using a public/private key pair, which is not transmitted with the data.

Data and File Storage

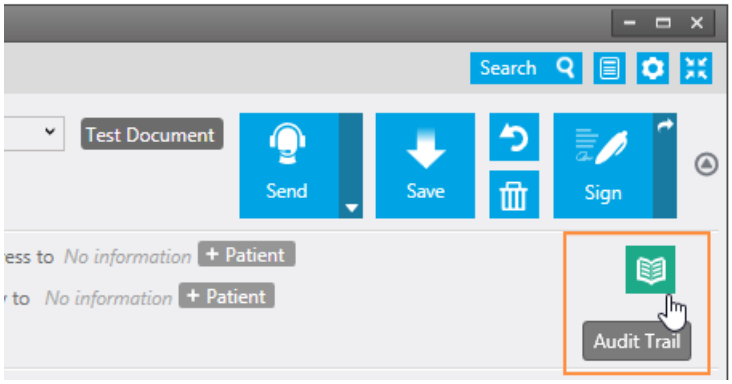
Winscribe Text uses Microsoft SQL Server technology for the storage and security of all the data associated with the Winscribe system with the exclusion of the voice files. The SQL Server user id and password settings control the level of security imposed on the programs accessing the Winscribe data.

- Text Desktop stores the connection string an in encrypted configuration file
- Text for iOS stores its internal database password in the iOS Keychain

The voice files stored on the Winscribe Servers HDD system remain encrypted at all times. Access to these files is controlled by the Winscribe Share permissions.

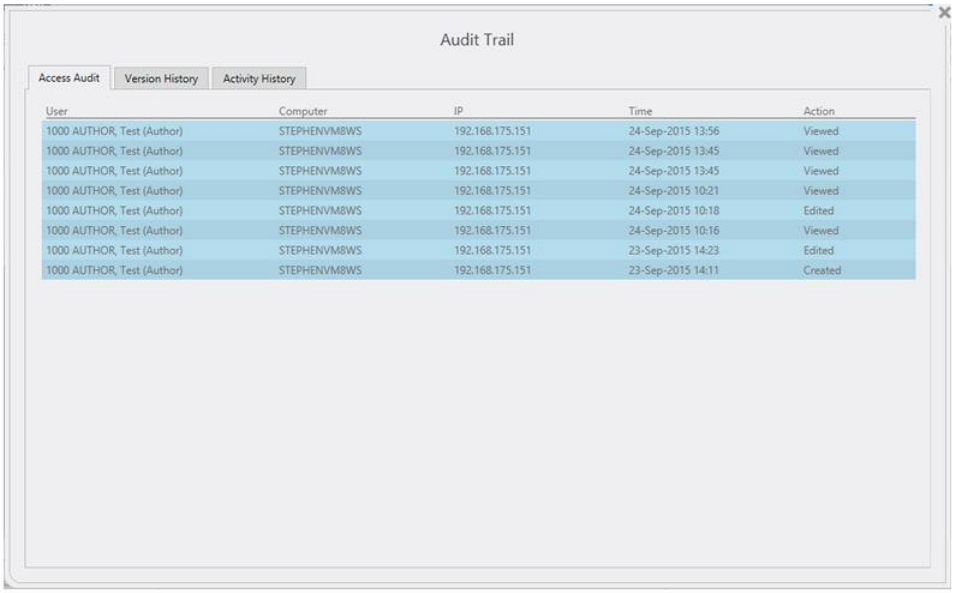
Data Tracking and Auditing

Winscribe Desktop features an **Audit Trail** function that enables users to examine a document's history.



The Audit Trail provides three tabulated windows of information for each document:

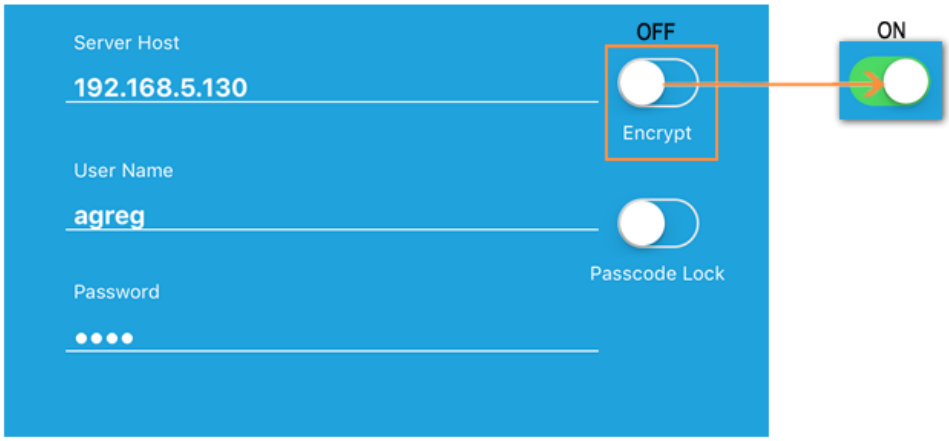
- **Access Audit** — details about the users who have accessed the document and the actions they performed
- **Version History** — details the document's versions, with a facility to open a read-only version of each)
- **Activity History** — details about the users who have worked on the document



Mobility for Winscribe Text

Encryption

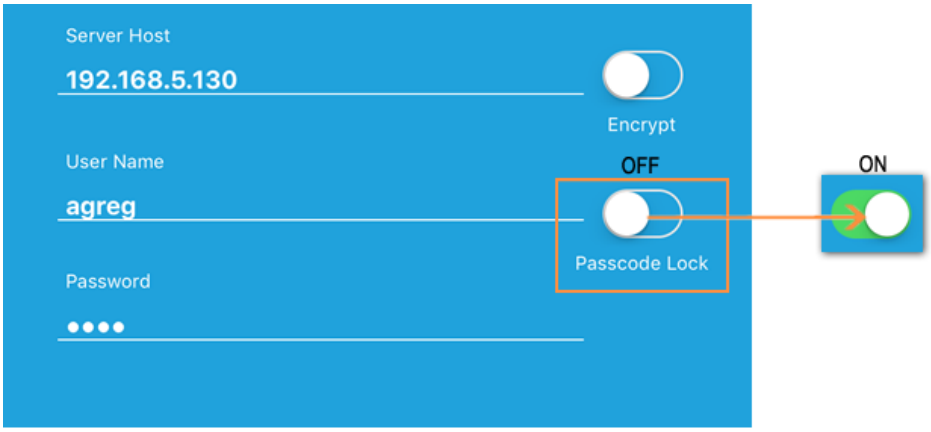
The Winscribe Text iOS app enables the user to toggle between *HTTP* and *HTTPS*, as desired:



- Toggle *ON* if the server URL uses SSL and starts with **HTTPS**
- Toggle *OFF* if the server URL starts with **HTTP**

Passcode Lock

For security and privacy, and a measure against loss or theft of the device, the requirement of a **passcode** can be invoked, when returning to the Winscribe Text iOS app after 30+ seconds.



Device Backup

The Winscribe Text iOS app does not backup data to the device's *iCloud* backup service or to *iTunes*. In the event the device is restored at any time from a backup, then any drafts saved to the app will be lost.

Data Storage

Patient information is stored in the device's internal database, which can include patient name, doctor name, dates and times, department name, document type.

- AES256 bit encrypted database, key stored in keychain.