HTH Engineering, Inc.
825 Cypress Trails Dr, Tarpon Springs, FL 34688
Tel: (727) 939-8853 Fax: (810) 821-6940
Web: http://www.startstop.com

Security Features of the Olympus DS-7000 & DS-3500 Digital Voice Recorder

21 Jan 2015

Security Features of the Olympus DS-7000 Digital Voice Recorder
By: Justin Parker

Keeping Your Files Secure

Whether it's for reasons related to your industry, or because you want to protect your work, you've likely given some thought to data security. But have you extended that thought to your dictations?

Whether you currently use professional dictation hardware, or are curious about what options are available, we think you'll find this a helpful rundown. What follows are the significant security and data loss prevention measures that Olympus features in their flagship line of digital voice recorders, the DS-3500 and the DS-7000.

We'll go over each these in brief, so that you can get an overview of how either device can help you protect your data. Keep in mind that most of this functionality is enabled and configured via the Olympus *software* that pairs with these recorders, ODMS R6. In most cases, this software is included in the sale of the device.

File Lock

Essentially, when you lock a dictation file, you are protecting it from being recorded over or modified, and preventing it from being deleted. There are some limitations to this feature, though:

- Anyone who has access to the device can simply unlock the file.
- Files do not stay locked on the computer—they are only locked on the device.
- A locked dictation can be deleted from the recorder, once connected to a computer.

The "File Lock" feature is one the few that can be set on the device itself. And it won't prevent the file from downloading as it would normally. Do note that if you have your Olympus dictation software configured to delete files after download, locked dictations won't be deleted.

PRO TIP: To change this, check the "Delete locked file(s)" box, located in the software, under *Tools* > *Options* > *Workflow* > *Download.*

Folder Autolock

Setting a "Folder Autolock" is very similar to locking an individual file. All of the same behaviors and limitations apply, except that any dictation recorded into an auto-locked folder will also be locked.

This feature is only configurable in the Olympus dictation software.

Data Loss Prevention

This failsafe is only available for users who have the administrative version of ODMS installed. It turns the voice recorder into a read-only device *when connected to the computer*. This prevents files from being added, modified, or deleted unintentionally.

See more here.

Hold Switch (DS-3500 Only)

If you turn your DS-3500 over, you'll see a switch with two positions: "Hold" and "Power." It's obvious that pressing down will turn the device on, but what happens when you flick the switch into the upper position?

That engages the "Hold" function, which freezes all of the buttons on the device. Might come in handy for when you put the recorder in your pocket, or if you just want to send the message, "Do not touch."

Disabling Buttons

There's a pretty surefire way to prevent changes from being made to the files on your handheld recorder—as well as changes to its settings.

Within the Device Settings menu in ODMS, you can configure it so that the [Erase] and/or [Menu] buttons are disabled. That would prevent anyone, including yourself, from deleting files or accessing anything in the File, Recording, Sound, or Device menus.

Again, as soon as the device is connected to a computer, all bets are off. The files can be accessed, downloaded, modified, or deleted, and settings can be changed.

PIN Code Lock

Now we're talking about real security. Setting a PIN code lock shuts out anyone who doesn't have the code. Period. The device is useless without it. And, even if the recorder is connected to a computer, it won't be recognized unless the PIN has been entered.

- The PIN code is enabled and configured in the Olympus software.
- The device can be set to lock when turned off, and also when going to standby.
- You may configure the maximum number of attempts at the PIN before the recorder goes into a 10 minute "halt" mode, which is essentially a complete lockdown.

PRO TIP: If you've reached this lockdown and you can't remember your PIN code, your Olympus dealer should be able to help you.

On-Device Encryption

Perhaps the most effective security feature available on the DS-3500 and DS-7000 recorders is file encryption. We're talking Advanced Encryption Standard (AES), 128 or 256 bit. You know, the good stuff.

Encrypting your files will keep them from being played outside of the device—unless you have the encryption code that was used in the first place. This means that if the files are downloaded, they will need to be decrypted before they can be transcribed. If the SD card is ever removed and placed in an unauthorized recorder, the encrypted files will not play.

EXCEPTION: If that memory card were placed in a device using the same encryption password, the dictations *would* play.

File encryption on the device is configured in the Olympus software, and works on a folder-by-folder basis. That means that individual folders are set for encryption, and only dictations recorded in those folders get encrypted. Moving the dictations after that will not “undo” the encryption, but any dictation created in a non-encrypted folder will not be encrypted.

Please note that encryption is only supported when using the DSS Pro (.DS2) audio format. Also ensure you are running the latest firmware for your device when using this feature.