

## STEGOSTIK™ ENTERPRISE SECURITY PARAMETERS

The table shows the different security parameters available for StegoStik™ Enterprise devices.

The column headed 'Default' shows the setting used if you do not supply custom options. The 'Custom options' column shows the alternatives that can be specified using the StegoStik™ Toolkit.

Note we no longer accept written requests for custom options. You must set up the desired parameters in the StegoStik™ Toolkit and email the file StegoDefaults.dat to sales@stegostik.co.uk.

StegoStik Limited  
Empire House  
175 Piccadilly  
London W1J 9TB

t: 0870 116 0 117  
f: 0870 116 0 118

[www.stegostik.co.uk](http://www.stegostik.co.uk)

### Security parameters: Defaults and custom options

Subject	Parameter	Default	Custom options
Passphrase	Minimum length	8 characters	.... characters (1-20)
	Character types	2 types	.... types (1-4)
	Mandatory types	Lower case, numeric	<input type="checkbox"/> Lower case <input type="checkbox"/> Upper case <input type="checkbox"/> Numeric <input type="checkbox"/> Punctuation
Timeout	Inactivity period	30 minutes	No timeout / .... minutes (5-60)
	Silent timeout	No	Yes / No
File shredding	Default method	Standard	Standard / Shred
	User can change	Yes	Yes / No
Encryption	AES key size	256-bit	128-bit / 192-bit / 256-bit
Administrator passphrase		None	None / .dat file supplied
Lockout	Failed attempts	Disabled	Disabled / .... failed attempts
	Action on lockout	N/a	Allow reset / Block reset / Shred index
User information	Editable fields	All editable	<input type="checkbox"/> Name <input type="checkbox"/> Address 1 <input type="checkbox"/> Company <input type="checkbox"/> Address 2 <input type="checkbox"/> Phone <input type="checkbox"/> Address 3 <input type="checkbox"/> Mobile <input type="checkbox"/> Comment
	Show on bad p/p	Yes	Yes / No
Temporary unencrypted workspace	Max. unencrypted	0 MB	.... MB
	User can activate	No	Yes / No
	Default randomise	Fast	Standard / Fast
	User can change	N/a	Yes / No
Temporary directory	Default location	N/a	C: / Workspace
	User can change	N/a	Yes / No

## STEGOSTIK SECURITY PARAMETERS

---

For software version 2.2.0. Updated April 2008.

Customising the security parameters for your StegoStik devices provides the security you need while leaving users as much freedom as possible, which promotes compliance.

While many organisations simply adopt the default configuration, each of the features below has been requested by our customers, so might be useful for your situation.

### Passphrase

A strong user passphrase is essential to prevent brute force attacks on a device. Three parameters allow you to specify the minimum strength:

- ❑ *Minimum length*: Minimum number of characters in a passphrase. While the lowest allowed value is 1, most applications will require at least eight characters.
- ❑ *Minimum character types*: Minimum number of character types in a passphrase, out of lower case, upper case, numeric and punctuation. A higher value expands the alphabet to be tested in a brute force attack.
- ❑ *Mandatory character types*: Tick none, one, or more character types to require the passphrase to contain the character type(s). Forcing a numeric and/or punctuation character to be included ensures the passphrase is not a real word.

### Timeout

Closing the StegoStik software interface after a period of inactivity reduces the risk of a security breach where the user has left a StegoStik device unattended. Specify:

- ❑ *Inactivity period for timeout*: Minutes of inactivity that causes the program to restart, forcing the passphrase to be re-entered. Set to 'None' for no timeout.
- ❑ *Display warning message*: Normally 'Yes'. Specify 'No' for stealth applications.

### File shredding

Shredding a file (overwriting with random numbers) is more secure, but slower than standard deletion (leaving the encrypted version on the device). Specify:

- ❑ *Default file deletion method*: Which method is used when the software starts.
- ❑ *User can change method*: Normally 'Yes' unless default is 'shred'.

### AES key size

The default key size is 256-bit for maximum security. Selecting 192-bit or 128-bit key size yields a slight performance improvement. A 128-bit key is roughly as strong as a passphrase comprising 20 random characters.

### Administrator passphrase

If enabled, every time the user resets the passphrase, the derived AES key is encrypted with an RSA public key, so that the device can also be accessed by the private key.

- ❑ *Use admin passphrase*: Whether the feature is activated.
- ❑ *RSA key size*: Select 1024-, 2048- or 4096-bit.
- ❑ *RSA public key*: The public key, which is stored on the device. This can be generated using the toolkit and is best supplied using the StegoDefaults.dat file.

### Lockout after failed passphrase attempts

Since StegoStik is a software implementation, it is possible to circumvent the lockout. Moreover, the point of enforcing a strong passphrase is that it is resistant to brute force attacks. However, lockout can serve as a deterrent or defence against opportunists.

- ❑ *Failed attempts*: Either disabled, or how many failures activate lockout.
- ❑ *Action on lockout*: Options are user can reset passphrase, administrator must reset device or shred file index.

## User information

Storing user information on a StegoStik device can help with telling devices apart, and may enable a lost device to be returned. However, some customers choose to restrict this capability, for example so their company name cannot be stored. Specify:

- ❑ *Editable fields*: Tick none, one or more field names to let the user edit that field.
- ❑ *Field contents*: Specify any pre-loaded text, eg. a help desk phone number.
- ❑ *Show on bad passphrase*: This may prompt the realisation that the wrong device has been inserted. Normally 'Yes' if there are any editable or pre-loaded fields.

## Temporary unencrypted workspace

Normally, forcing all data to be encrypted is exactly what customers need. However, there are some specialised situations where a *limited* amount of unencrypted workspace can be useful. Firstly, if the user may need to work with non-Windows machines: many such PCs will be able to read an unencrypted copy although they won't be able to run the software. Secondly, if you want users to be able to display or edit files without storing an unencrypted copy on the hard drive (eg. at third party sites), then it can make sense to make this temporary copy on the StegoStik device. Settings:

- ❑ *Maximum unencrypted workspace (MB)*: Set to zero for no unencrypted workspace, or an integer to specify the largest workspace permitted, in megabytes. The workspace specified reduces the space for encrypted files.
- ❑ *User can activate workspace*: Normally 'No' if workspace zero, otherwise 'Yes'.
- ❑ *Default randomise speed*: When removing the workspace by overwriting with random numbers, the 'Fast' option is suitable for most (non-stealth) situations.
- ❑ *User can change speed*: Normally 'Yes' if default is 'Fast', otherwise 'No'.

## Temporary directory

When StegoStik decrypts files in order to copy or open them, it creates a decrypted copy in a temporary directory. Normally, this is in the standard Windows Temp directory (usually on C:). If workspace has been specified, there is the option for StegoStik to create its temporary directory there. If workspace is non-zero, you can specify:

- ❑ *Default location for temporary files*: Either 'C:' (meaning standard Windows Temp directory), or the StegoStik 'Workspace'.
- ❑ *User can change location*: Normally 'Yes' if default is 'C:', otherwise 'No'.

## StegoStik toolkit

The StegoStik toolkit provides the IT department with additional capabilities that can be helpful, particularly in a multi-user environment. A special activation file ensures that each customer can only manipulate the StegoStik devices that they have purchased. The key toolkit capabilities are:

- ❑ *Change security parameters*: All the security parameters described above can be adjusted for individual devices where users have particular needs.
- ❑ *Load/save default settings*: To simplify management. The StegoDefaults.dat file can be sent to StegoStik for use in the production of your purchase orders.
- ❑ *Preset user information*: By setting user information fields and disabling the user's ability to edit them, you can embed messages such as an IT contact number.
- ❑ *Generate RSA key pairs*: Create the public/private administrator keys.
- ❑ *Prevent reset passphrase*: An alternative to the administrator's passphrase to access a user's files. Simply set the passphrase then disable the ability to reset it.
- ❑ *Prevent file deletion*: Ensures a user can only add files, not delete or overwrite them. Combine with 'Prevent reset passphrase' as this would remove all data.
- ❑ *Upgrade software*: The repair utility will also switch to the latest software version.
- ❑ *Repair device*: If a user deletes one or both of the pre-loaded StegoStik files, the device can be repaired immediately. A reformatted device requires an updated StegoDevices.dat file to be requested.

*If you have any questions, please do not hesitate to get in touch  
on 0870 116 0 119 or support@stegostik.co.uk.*