Security OpenPGP tab

Related Topics

- security admin

Overview

Use this tab to configure Tiki to use OpenPGP.

To Access

From the Security Admin page, click the **OpenPGP** tab.

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences

Option	Description	Default
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg

Option	Description	Default
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/

Option	Description	Default
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled

Option	Description	Default
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. ☝ *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Documentation for Tiki OpenPGP support - developing issues here: https://dev.tiki.org/OpenPGP