

iLink 3

Release Notes

Version 1.3.2 – April 26th 2023

Overview

Version 1.3 introduces optional support for configuration file encryption to enhance security. This release also includes various other enhancements and bug fixes.

New Features / Enhancements

- Support for optional encryption of device configuration files. (Jira iLINK-35)
- Improved form behavior when Windows display scaling is greater than 100% (Jira iLINK-41)
- iRIS270 FTP - MIS file type. Support auxiliary logging catalog codes (Jira iLINK-38)
- iRIS270 FTP - MIS file type. Catalog code validation (length and duplicates) (Jira iLINK-32)
- iRIS270 & UC. Completion check for clear configuration operation. (Jira iLINK-33)
- iRIS270 & UC. Add Modbus address validation. (Jira iLINK-51)

Bug Fixes

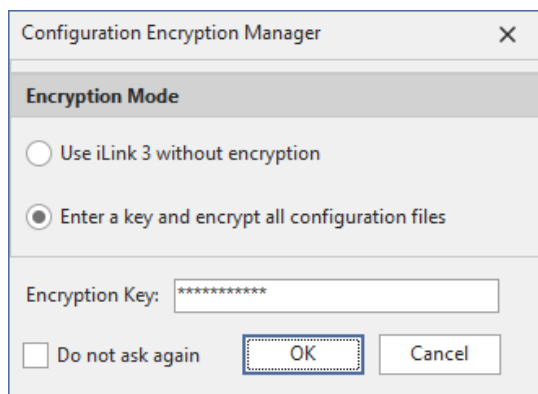
- Samples graph and table view is very slow to load larger datasets. (Jira iLINK-52)
- iRIS270 Configuration version N/A after loading existing configuration from disk (Jira iLINK-10)
- iRIS270 – If only one TCP server is configured, enforce the primary must be used. (Jira iLINK-28)
- Remove software options as not relevant for iRIS270/UC program/auto upgrade. (Jira iLINK-17)
- Disable access to Polarity and Schedule when DIO is in input mode. (Jira iLINK-53)
- Wi-Fi connectivity ping check may fail with socket error 10013 on some machines. (Jira iLINK-54)

Configuration Encryption

This release enables configuration files to be saved in an encrypted state. This eliminates the potential vulnerability of exposing sensitive settings, such as communication details including API credentials.

Enabling encryption

When iLink 3 starts for the first time after the upgrade, it will prompt for an encryption mode.



The screenshot shows a dialog box titled "Configuration Encryption Manager" with a close button (X) in the top right corner. The dialog has a section titled "Encryption Mode" with two radio button options: "Use iLink 3 without encryption" (which is unselected) and "Enter a key and encrypt all configuration files" (which is selected). Below this, there is a text input field labeled "Encryption Key:" containing a series of asterisks. At the bottom of the dialog, there is a checkbox labeled "Do not ask again" which is unchecked, and two buttons: "OK" and "Cancel".

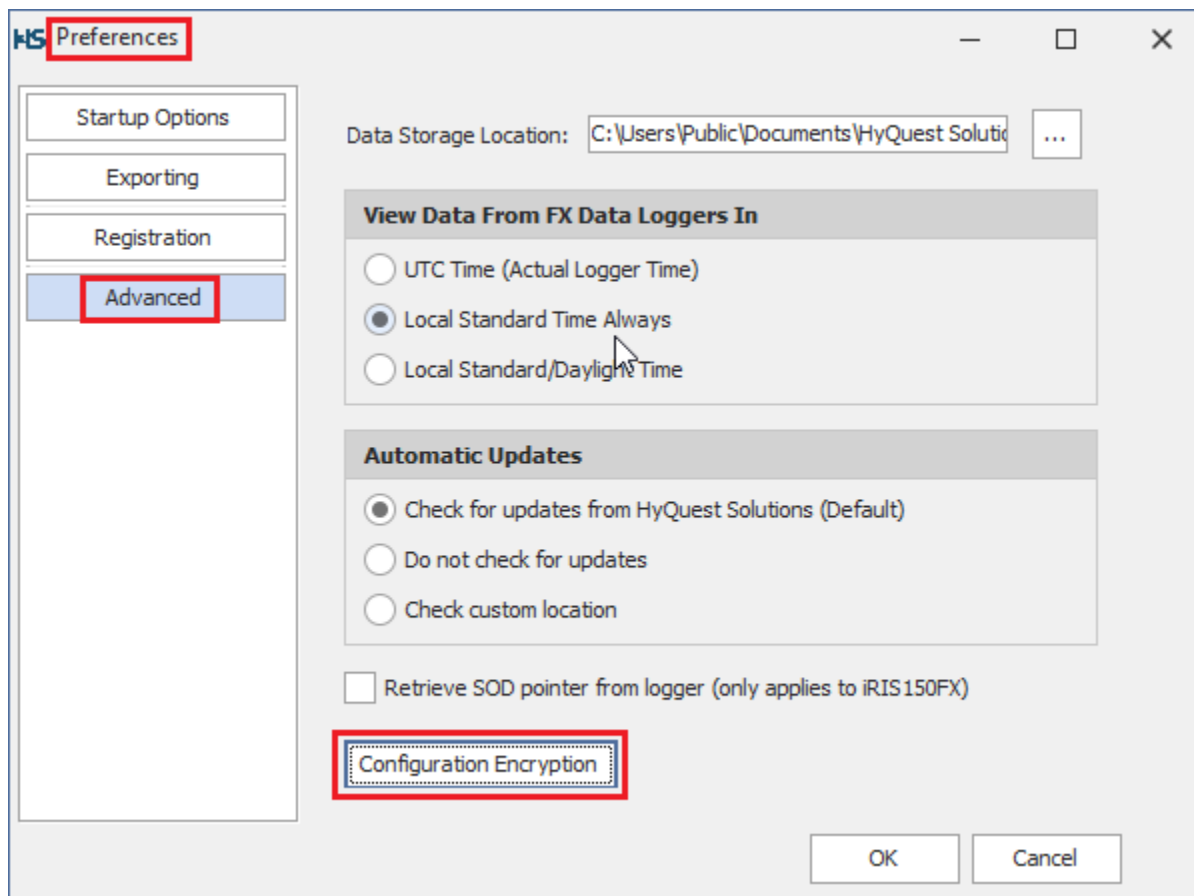
If encryption is enabled (default), a suitable encryption key string must then be entered. The key can comprise any mix of characters and can be between 4 and 32 characters in length.

iLink 3 will then encrypt all existing configuration files, on the computer (including archived files) and their file names will be changed to include an 'E' suffix. This indicates the file is encrypted using the internal iLink encryption key string. After this step, users will not notice any difference, unless manually loading or saving configuration files. See below for more details.

If "Use iLink 3 without encryption" is selected and the "Do not ask for this again" checkbox is also enabled, iLink 3 will continue using standard configuration files and will not prompt again on start up.

Disabling encryption or changing key

At any time, the associated encryption key can be changed or encryption mode disabled. This is done using the Encryption Manager form described above. Use Preferences->Advanced->Configuration Encryption to invoke it.



Changing the encryption key

Enter a new key string. On clicking Ok, iLink will securely process the configuration files sequentially, using the previous key string to decrypt, then re-encrypt the files using the new key string.

Disabling encryption

Change the mode to "Use iLink 3 without encryption". On clicking Ok, iLink will unencrypt all configuration files using the current encryption key and also remove the 'E' file name suffix.

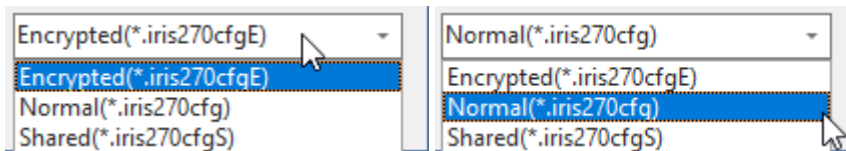
Manually Loading or Saving Configuration Files

Even if encryption is not enabled in iLink 3 as described earlier, it is possible to create encrypted files for sharing with a user defined key string.

WARNING: If the encryption string is forgotten, a shared file cannot be used.

Saving and Loading Files

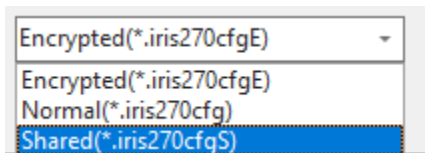
Either encrypted or standard files can be loaded and saved by selecting the appropriate file type. Encrypted files use the current iLink 3 encryption key string.



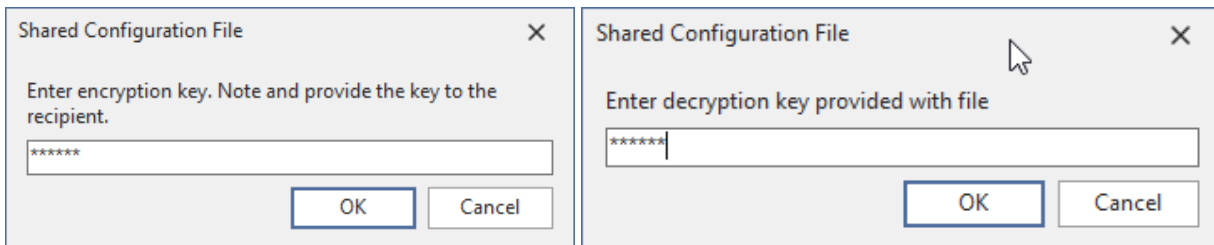
Sharing Encrypted Files

iLink 3 can also save and load files for sharing, using a one-off encryption key. This is possible, even if encryption has not been enabled as described earlier. This avoids the need for the internal iLink 3 encryption string to be disclosed when sharing configuration files outside an organisation for example.

To do this, select the Shared option in the file type options.



A prompt to either create a key (saving) or to enter the supplied shared key (loading) will appear.



WARNING: If the one-off encryption string used for sharing files is forgotten, it is impossible to use any shared file that was encrypted using it.