Windward Security FAQ

Last Updated: 19 June 2019

We try in this FAQ to answer any questions you have around Windward and security. If anything is not answered, please ask us:

Q: Does Windward see my data?

A: The company Windward does not have access to your data.

Q: Does the Windward program write anything to my data?

A: The Windward program only reads from your data, with the following caveat. A user can write any select for a tag and that tag could include a command to change the datasource. Therefore we recommend that you provide read-only credentials to any datasource you pass to Windward to enforce this restriction.

Q: Do I need to worry about SQL injection attacks.

A: With SQL and OData (JSON & XML are read-only files so not an issue) there are three modes you can specify for setting parameter values. 1) Always use the connector setParameter() call – which precludes any injection attack. 2) Always use string substitution – which will allow an injection attack. 3) Mixed mode where parameter names starting with an _ like _var are string substitution and the rest are setParameter(). The default is the third mode which assumes the template designers will use _var carefully and appropriately.

Q: How do you save the datasource connection credentials in the designer?

A: The designer stores the credentials to each datasource in the template one of three ways. 1) In clear text (uuencoded, but no encryption). 2) They are encrypted for the logged in user using System.Security.Cryptography.ProtectedData and on subsequent use decrypted, only for that same user. 3) They are not stored and have to be re-entered each time the template is opened. The default is mode 1 which assumes designers point to a sample datasource.

Q: What security vulnerabilities exist in the program

A: First if you turn on verbose logging, that will include template and data content. And even error or fatal logging can include template content and/or data in the exception information logged. The logging does try to scrub passwords from the info logged, but it works based on expected patterns for a password (i.e. "password=secret"). Second, the XPath 1.0 libraries are susceptible to XXE attacks. Always use the XPath 2.0 (Saxon) libraries for XPath datasources.

Q: Is Windward GDPR compliant?

A: We believe so (is anyone 100% sure?). We do this by not seeing or touching your data in any way.

Q: How do we keep your data secure?

A: We never have access to your data. The Windward program runs on your system and the data it reads is merged into the generated report – and that's it.

Note: When we say "we never see your data" we mean the company Windward never sees your data. Obviously, the Windward program does see your data as it merges it into the generated report.