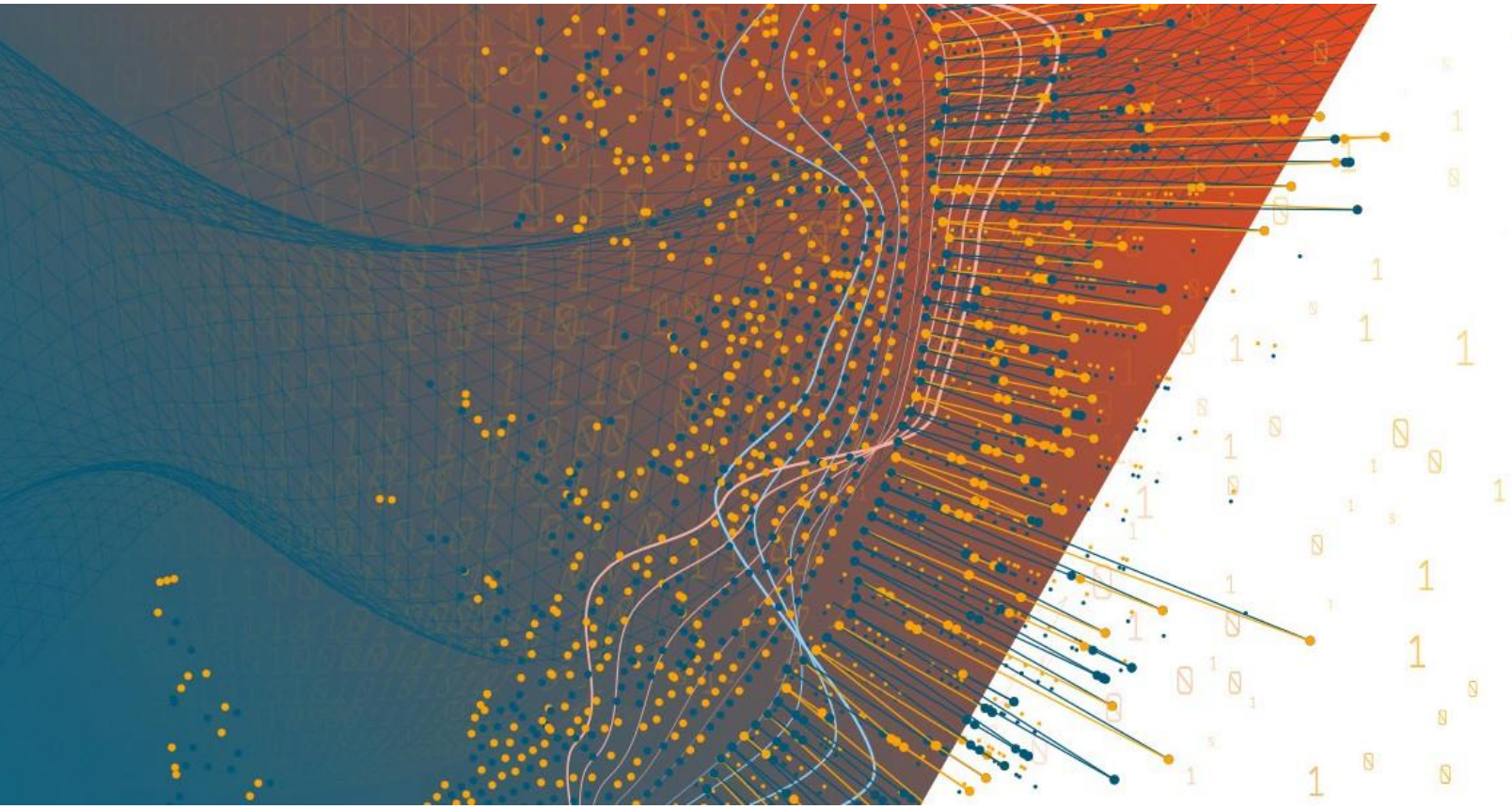


ALTAIR

Altair® Monarch® v2021.1.1

MONARCH SERVER CONTENT SECURITY ENHANCEMENTS GUIDE

TABLE OF CONTENTS

INTRODUCTION

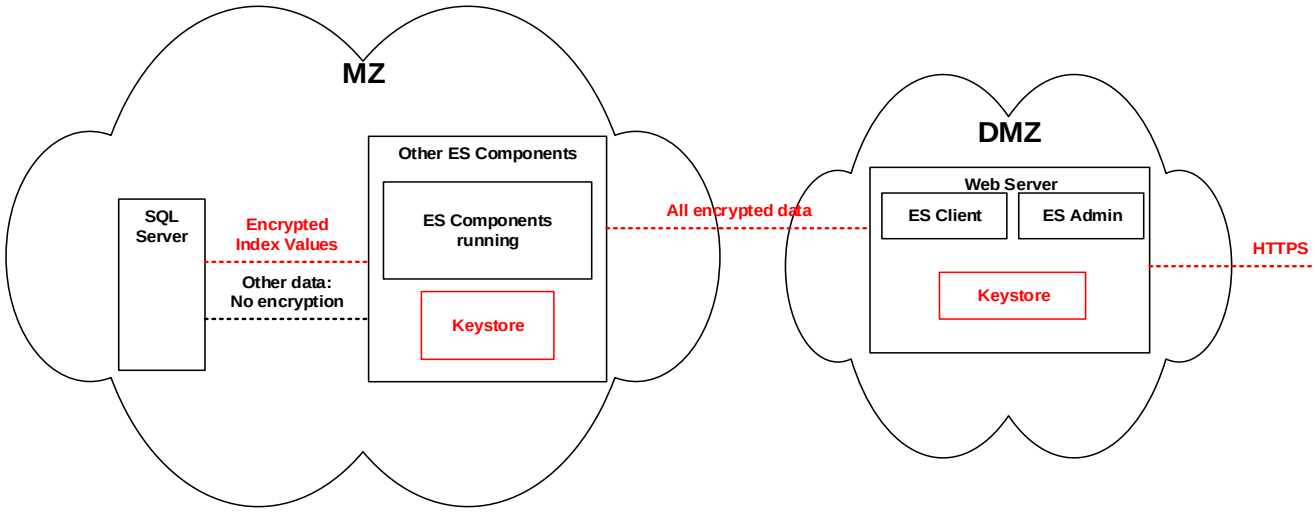
To enhance security of the Monarch Server application, you can use the Security Enhancements features. These features are an optional Monarch Server functionality that is available under license.

The Monarch Server Security Enhancements Guide gives an overview of the Security Enhancements features and explains how to use them with Monarch Server.

This Guide is intended for Monarch Server consultants, customers, and system administrators who will use the Security Enhancements features.

ABOUT MONARCH SERVER SECURITY ENHANCEMENTS

The Monarch Server Security Enhancements help reduce the risks of unauthorized data access. Each enhancement affects a separate part of the Monarch Server system, as illustrated in the following diagram:



MZ stands for “militarized zone” and includes the network segment that is well protected against intrusions, i.e. unauthorized data access, from the outside network by appropriate tools (e.g., firewalls). However, data on the database server requires additional protection.

DMZ stands for “demilitarized zone” and includes the network segment open to the outside network. DMZ usually comprises the corporate Web server that is the most exposed component in the system because it has to be accessible to Monarch Server end users.

To improve the security of your Monarch Server system, you can use the following Security Enhancements:

- Web Services Security Certificates
- Database Server Protection with Encrypted Index Values
- Key Generation
- Encrypting and Decrypting Existing Data

NOTES

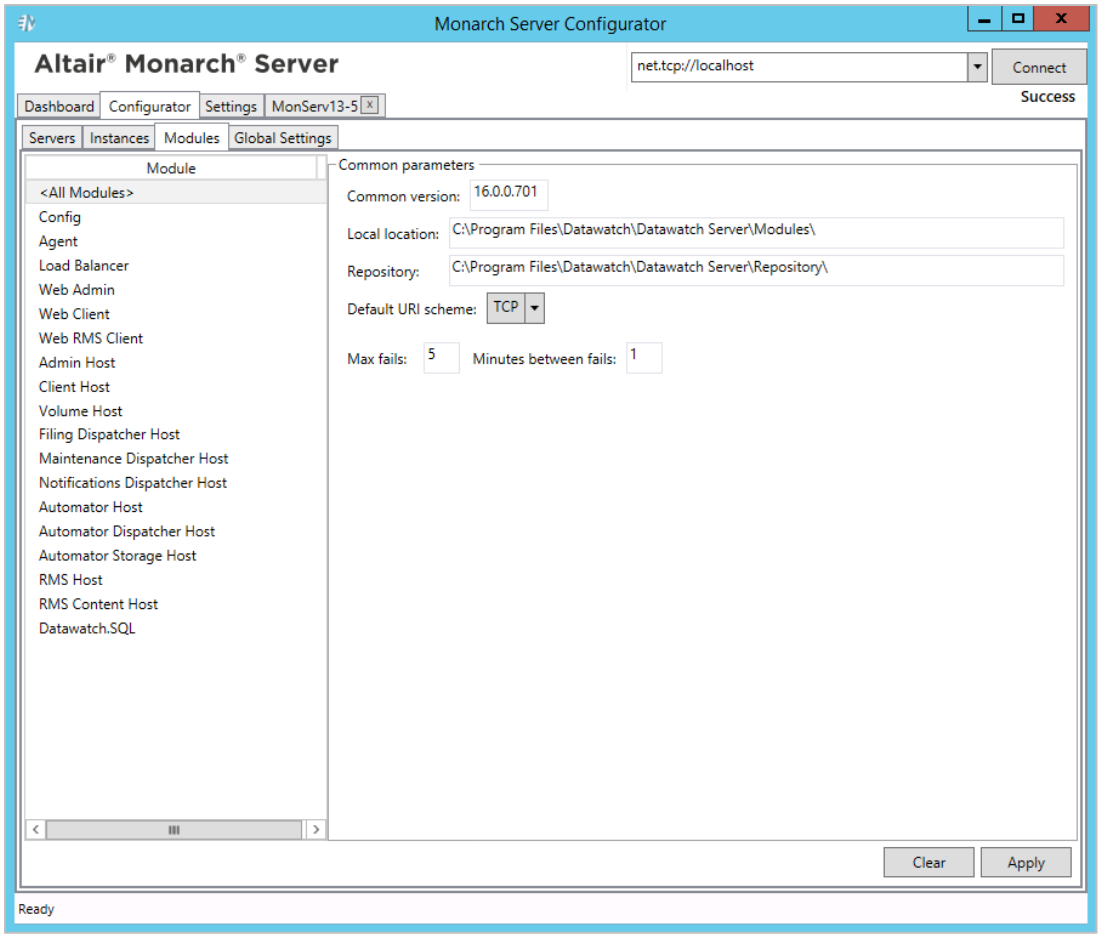
The **SecurityModule** license component is required to enable Security Enhancements.

WEB SERVICES SECURITY CERTIFICATES

With Monarch Server Security Enhancements, you can encrypt messages that services and Web servers exchange. To do this, you can use the Security Enhancements certificates feature.

To use a certificate

1. Install the required certificate on all machines that will run the services.
2. Run Monarch Server Configurator.
3. Select the **Configurator** tab, and then select the **Modules** tab.



4. For each module, set the default URI scheme to SecuredHTTP and to a unique port.
5. In Datawatch.ModulesManagement.Agent.exe.config, set the URL to **Config**.
6. In `Web.config` of the Admin and Client Web applications, set the URL to **Config**.
7. Edit the `config.xml` file. In the *Modules* section of the file, enter the certificate name: **DefaultCertificateSubjectName =<subjectName>**

8. Restart the Config and Agent Services of Monarch Server.

NOTES

The certificate must have a private key.

DATABASE SERVER PROTECTION WITH ENCRYPTED INDEX VALUES

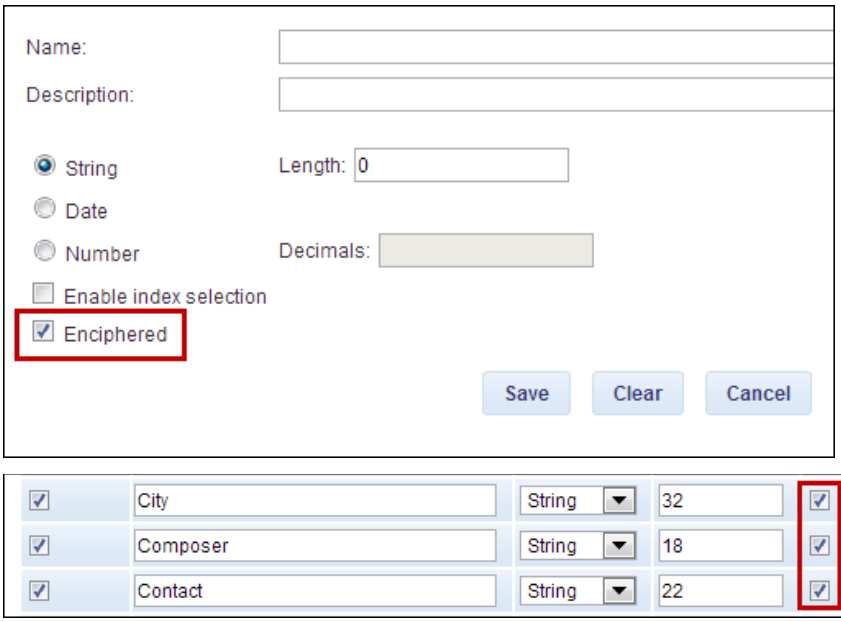
Although the Monarch Server database server runs in the well-protected MZ, you can achieve an even higher level of data protection by encrypting string index values.

String index values retrieved from ingested reports are stored inside the database. After finding a way to access the database, an intruder (i.e., a person intending to get unauthorized access to data) is able to read the information. To decrease the risk of such a scenario, the data are encrypted using the AES encryption algorithm.

Using the AES algorithm, you can encrypt those data items that are dependent on encrypted index values, for example, document names, report names, and search and security criteria.

With Monarch Server Security Enhancements, you can encrypt index values selectively via the index field.

Index values are encrypted for those index fields that you choose to be encrypted when creating them or importing from a model:



After an index field is created, you can decrypt or encrypt (whichever is applicable) its index values with the help of another Security Enhancements application — Database Encryptor. For more information, see Using Database Encryptor.

There are three limitations in using encrypted index fields when specifying search or security criteria:

- It is not possible to see a list of values to choose.
- It is not possible to set compare symbols other than “=” and “<>”.
- It is not possible to use masks for these fields.

Inside the database, the index values of selected index fields and each search or security criterion containing a value for the field are encrypted.

KEY GENERATION

You can generate keys used for data encryption and decryption by using the Key Generation application. A key is stored in a file in the keystore, i.e., in a dedicated directory on a disk.

The system administrator must ensure that the keys are protected by means of the operating system, i.e., a key file should be accessible only to the user account under which Monarch Server services run.

You can generate seven types of keys with the Key Generator:

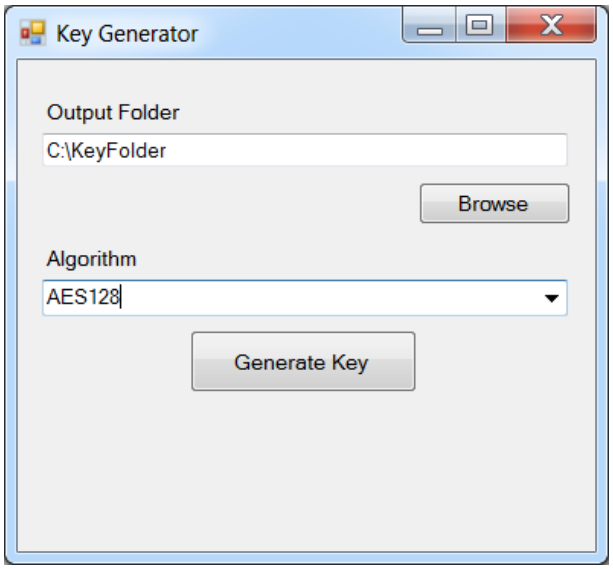
- AES128
- AES256
- Rijndael
- Blowfish
- DES
- RSA
- DSA

NOTES

For all Security Enhancements to work, you need to first generate the AES key used to encrypt database information.

To generate a key

1. Run Key Generator.exe.
2. Specify an output folder, i.e., the folder in which the keys will be stored.
3. Select an encryption algorithm.



4. Click **Generate Key**. A file with a key is generated. The file name is displayed in the Key Generator window.

NOTES

You can store up to 100 keys generated with one algorithm in one folder.

ENCRYPTING AND DECRYPTING EXISTING DATA

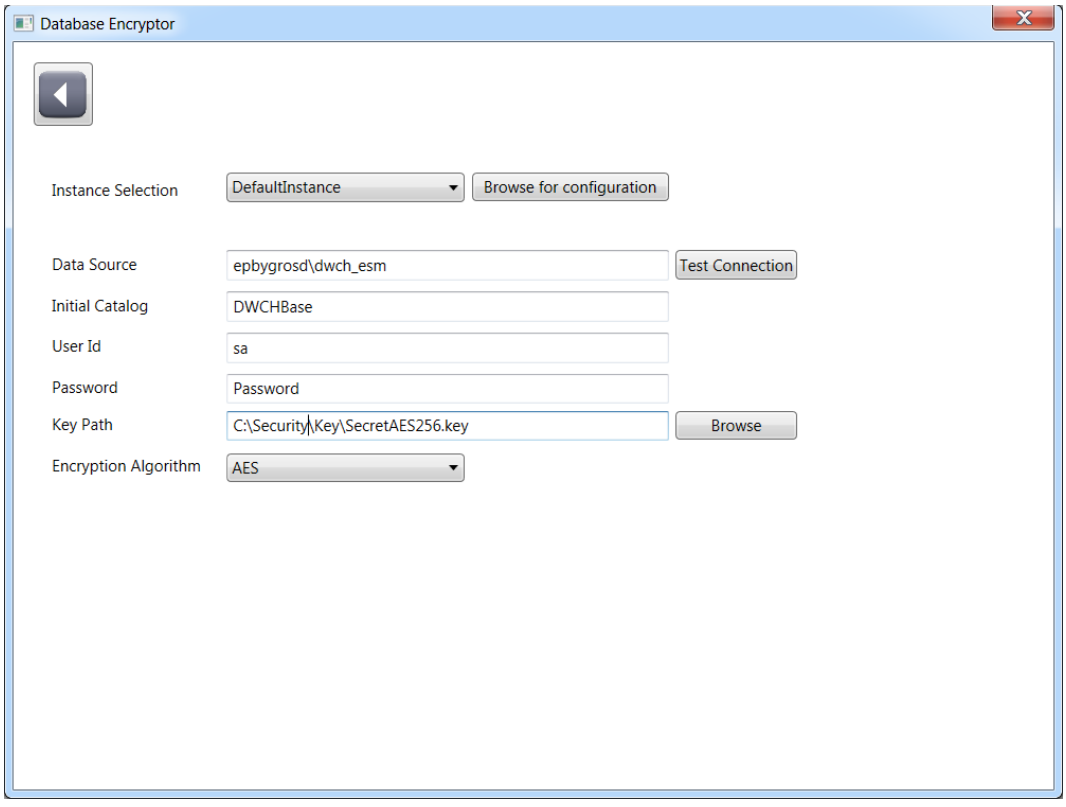
If you want to encrypt (and decrypt thereafter) already loaded data, i.e., index values, on a working system, you can only do so by using the Database Encryptor application.

USING DATABASE ENCRYPTOR

To encrypt or decrypt index values, you first configure the database parameters and then specify the fields to be encrypted or decrypted.

To encrypt or decrypt data

1. Stop all Monarch Server services.
2. Run **DatabaseEncryptor.exe**. The *Database Encryptor* configuration window appears.

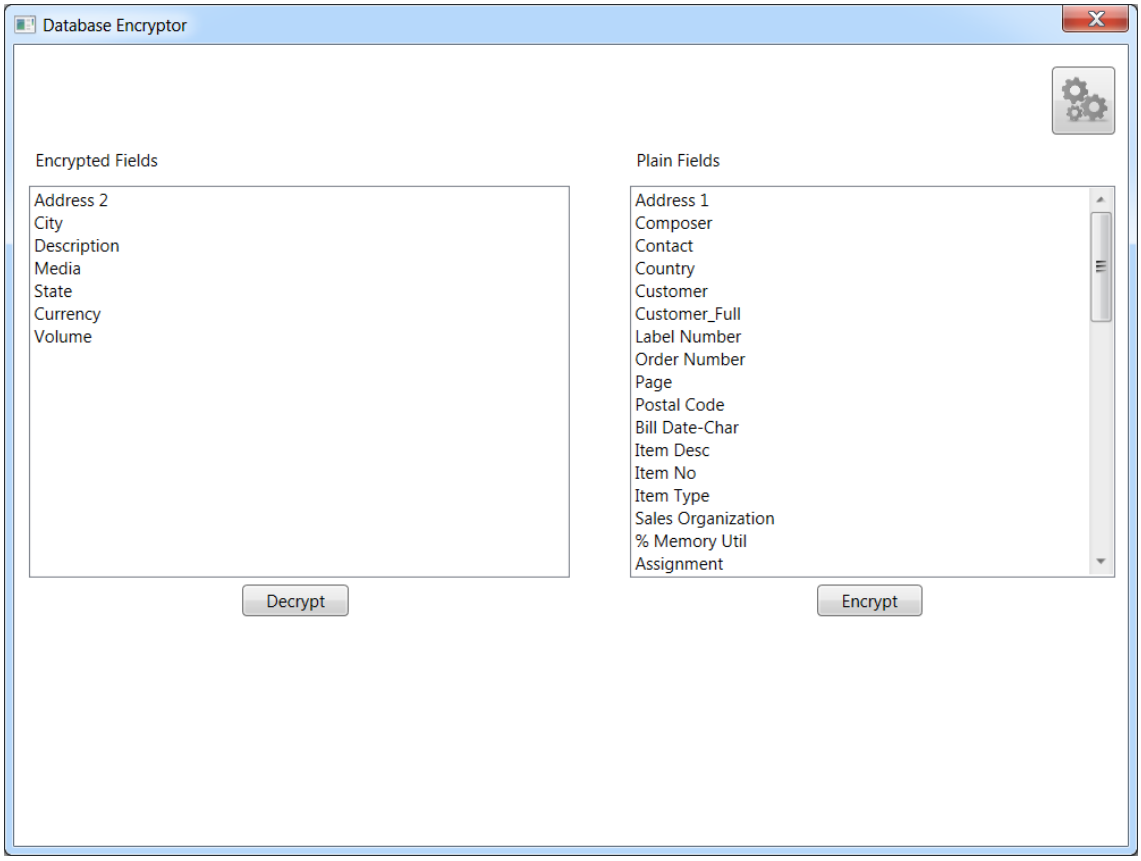


3. If you want to configure the database parameters automatically, click **Browse for configuration**.
4. Select the config.xml file. The database-related fields (**Data Source**, **Initial Catalog**, **User Id**, and **Password**) are filled in automatically.

NOTES

Make sure the **Encryption Enabled** field value is set to "true" and the path to the key is specified in config.

5. If the selected config has several instances, the **Instance Selection** drop-down list is populated with the available instances. Select the required instance from the list. Go to Step 8.
6. If you want to configure the database parameters manually, enter the required values in the fields **Data Source**, **Initial Catalog**, **User Id**, and **Password**.
7. If you want to verify the specified parameters, click **Test Connection**. Information about successful or failed connection to the database server will be displayed.
8. Click **Browse** and specify the key path. For more information about encryption keys, see Key Generation.
9. Select an encryption algorithm. Currently, Monarch Server uses the AES algorithm only.
10. After configuration is completed, click the arrow button in the upper left corner of the Database Encryptor window. The left pane of the application window displays the encrypted fields, and the right pane displays the plain fields.



11. To encrypt fields, select the required ones in the **Plain Fields** pane (hold Ctrl or Shift for multiple selections), and click **Encrypt**.
12. To decrypt fields, select the required ones in the **Encrypted Fields** pane (hold Ctrl or Shift for multiple selections), and click **Decrypt**.

CONTACT US

GET IN TOUCH

We'd love to hear from you. Here's how you can reach us.

SALES CONTACT INFORMATION

Portal: Contact Altair

US: + 1.800.445.3311

International: + 1.978.441.2200

SUPPORT CONTACT INFORMATION

Customer Portal: https://community.altair.com/community
Email: dasupport@altair.com
US: +1 800.988.4739
Canada: +1 978.275.8350
Europe, Middle East, Africa: +44 (0) 8081 892481