# XML Encryption

This topic explains how to configure and apply the XML Encryption tool in SOAtest and Virtualize. This tool encrypts XML documents for security purposes.

Sections include:



## Understanding XML Encryption

In order to securely send data across the Internet during a Web service transaction, security standards must be put in place to ensure that outside parties cannot view or read any of the private transaction data. The XML Encryption standard recommended by the W3C defines a process that allows any data in XML documents to be encrypted and decrypted. It specifies the data to be encrypted, as well giving information about the cipher or key used to encrypt the data.

The XML Encryption tool supports the W3C XML Encryption standard and the WS-Security standard from OASIS. The XML Encryption Tool allows you to encrypt and decrypt data to be sent as Web service transactions. The XML Encryption tool also allows you to encrypt individual elements of the XML document, or the entire document itself. This feature is especially useful for Web service transactions that are performed between multiple partners or endpoints. For example, a credit card transaction can be encrypted where the user's name and address are visible, but the user's credit card number is encrypted.

## Configuring the XML Encryption Tool

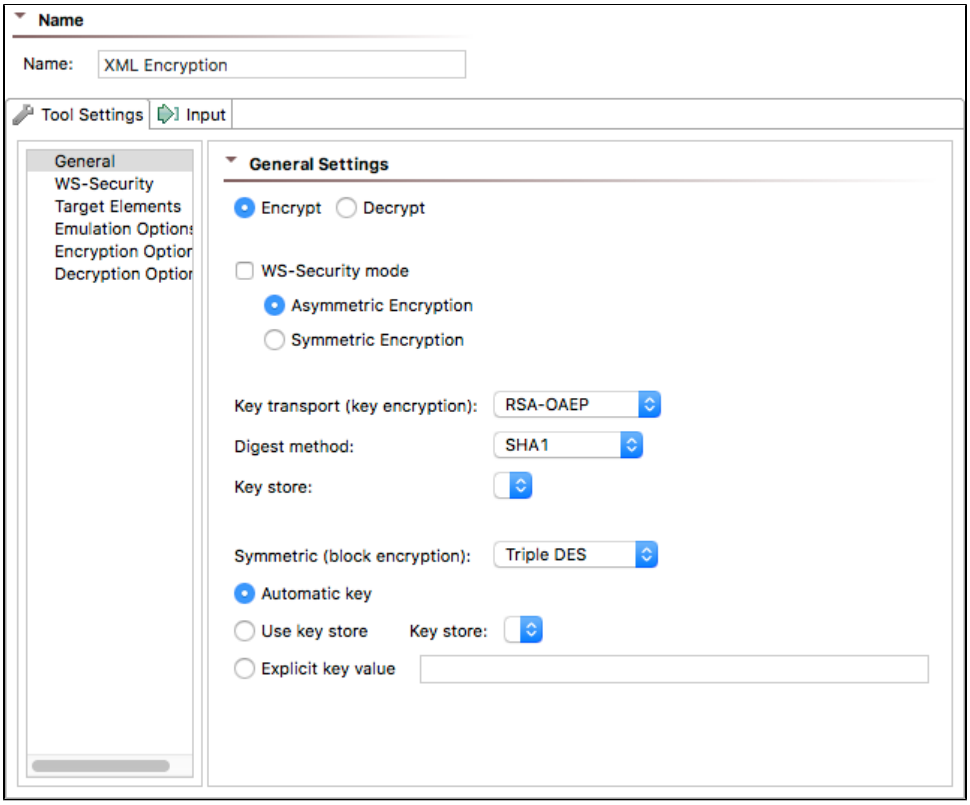
The XML Encryption Tool allows you to either Encrypt or Decrypt data. Depending on the **Encryption Mode** you select, the options for **Encrypt** mode and **Decrypt** will vary.

> **Note**
>
> Before using the XML Encryption Tool, you must download the Unlimited Strength Java Cryptograpy Extension. For more information, see Unlimited Strength Java Cryptography Extension.

### Tool Settings

The following options display in the left pane of the Tool Settings tab:

- General
- WS-Security
- Target Elements
- Emulation Options
- Encryption Options
- Decryption Options




## General

When selecting **General** from the left pane of the Tools Settings tab, the following options are available:

- **Encrypt** or **Decrypt**: Select the appropriate radio button to encrypt or decrypt data.
- **WS-Security Mode:** Enables OASIS WS-Security 1.0 for encrypting SOAP messages. Enable this option and the **Encrypt SOAP Body (WS-Security Mode) or Entire Document (non WS-Security mode)** option to automatically encrypt the content of the Body element. WS-Security Mode uses asymmetric encryption but does not allow use of key stores or explicit key values.
- **Asymmetric (non-WS-Security):** Enables the use of a symmetric key to encrypt the data and an asymmetric key to encrypt the block encryption key. You may also choose to use a key store or an explicit key value.
- **Symmetric (non-WS-Security):** Enables the use of only one secret, shared, symmetric key to encrypt the data directly.
- **Key Transport (Key Encryption):** Specifies the unique algorithm used to encrypt the key.
- **Digest method**: Choose a message digest algorithm for encrypting the data. Supported algorithms are SHA1, SHA256, SHA384, and SHA512. This option is enabled only when the **Key Transport (key encryption)** option is set to RSA-OAEP.
- **Key Store:** Specifies the key store for the key-encryption key. The Key Stores available in this menu are dependent on the Key Stores you added at the test or Responder suite level. For more information on adding Key Stores, see Global Key Stores.
- **Symmetric (Block Encryption):** Specifies the unique algorithm used to encrypt the data.
- **Automatic Key:** Enables automatic block encryption key generation.
- **Use Key Store:** Specifies the key store used for the Symmetric (Block Encryption) key. The Key Stores available in this menu are dependent on the Key Stores you added at the test or Responder suite level.For more information on adding Key Stores, see Global Key Stores.
- **Explicit Key Value:** Enter an explicit key, depending on the Algorithm you selected from the Symmetric (Block Encryption) menu.

## WS-Security

When selecting **WS-Security** from the left pane of the Tools Settings tab, the following options are available—if **Encrypt** and **WS-Security** are selected in the **General** tab:

- **Form:** Choose the appropriate form to specify the key and certificate used for encryption.
- **Actor:** Enter a value to specify a SOAP actor.
- **Add mustUnderstand="1" attribute:** Specifies whether or not the receiver must recognize and decrypt the message. If this option is enabled, a SOAP fault will be sent back if the receiver does not know how to decrypt and deserialize the message.
- **Add timestamp:** Select to add a timestamp to the message. When this option is enabled, the following are available:
  - **Sign timestamp:** Select to provide a digital signature with the timestamp.
  - **Add expiration:** Select to enter an expiration value in the **Time to Live** field.

## Target Elements

When selecting **Target Elements** from the left pane of the Tools Settings tab, the following options are available—if **Encrypt** is selected in the **General** tab:

- **SOAP body/entire document:** Select to encrypt the entire SOAP body or entire XML document.

- Click the **Add** button (only available if **SOAP body/entire document** is unselected) to specify an XPath and encrypt a specific element within the XML document. After clicking the Add button, a row will appear in the **Element Selection** list. The **Element Selection** list consists of the following two columns:
    - **XPath Expression:** Allows you to enter the desired XPath you would like encrypted.
    - **Target:** Allows you to choose either **Entire Element** or **Content Only**.
      Selecting **Entire Element** will encrypt the entire XPath.
      Selecting **Content Only** will encrypt only the text content.

### Emulation Options

When selecting **Emulation Options** from the left pane of the Tools Settings tab, the following options are available:

> **Note**
>
> The following options are available only if **WS-Security Mode** is selected in the **General** tab.

- **Emulate:** Select the application server you are using to automatically configure the emulation options. You can also select the appropriate version number of your application server from the **Version** drop-down menu.
    - To manually configure the emulation options, select **Custom** from the **Emulate** drop-down menu. The following options will be available for you to manually configure:
        - **wsse URI:** Select the namespace URI of the WS-Security specification used.
        - **wsu URI:** Select the utility namespace URI of the WS-Security specification used.
        - **Qualify signed element ID attribute:** Select to qualify signed element ID attribute.
        - **Qualify BinarySecurity Token attributes:** Select to qualify binary security token attributes with the wsse namespace.
        - **Prefix BinarySecurity Token attribute values:** Select to prefix binary security token attributes with the wsse URI.

### Encryption Options

With **Encryption Options** selected in the left pane of the Tools Settings tab, the following options are available:

- **Security Header Layout:** This property indicates which layout rules to apply when adding items to the security header. The following options are available:
    - **Lax:** Items are added to the security header in any order that conforms to WSS: SOAP Message Security
    - **LaxTimestampFirst:** Same as Lax, except that the first item in the security header MUST be a wsse:Timestamp
    - **LaxTimestampLast:** Same as Lax, except that the last item in the security header MUST be a wsse:Timestamp
    - **Strict:** Items are added to the security header following the numbered layout rules described below according to a general principle of 'declare before use'.

### Decryption Options

With **Decryption Options** selected in the left pane of the Tools Settings tab, the following options are available:

> **Note**
>
> The following options are available only if the **Decrypt** radio button is selected in the **General** tab.

- **Signature verification:** This setting allows you to specify whether you'd like to perform a Signature verification when decrypting the XML message.
- **Key Store:** Specifies the key store used to verify the signature. The Key Stores available in this menu depend on the Key Stores you added at the test or Responder suite level.For more information on adding Key Stores, see Global Key Stores.

    - **Decrypt all known WSS headers:** Select to decrypt WSS header formats.
    - **Decrypt specific header formats:** Select to decrypt specific header formats.

## Input Type Tab

The **Input Type** tab is only available if the XML Encryption tool is added as a standalone tool and not chained to another tool. The following options are available from the Input Type tab:

- **Text:** Use this option if you want to type or copy the XML document into the UI. Select the appropriate **MIME type**, enter the XML in the text field below the **Text** radio button.
- **File:** Use this option if you want to use an existing file. Click the Browse button to choose a file.
    - Check the **Persist as Relative Path** option if you want the path to this file to be saved as a path that is relative to the current configuration file. Enabling this option makes it easier to share tools across multiple machines. If this option is not enabled, the test or Responder suite will save the path to this file as an absolute path.

# Usage Notes

You can use the XML Encryption tool as a stand-alone tool at the test suite level by right-clicking the main test suite node and selecting **Add New> Test** fro m the shortcut menu and then selecting **XML Encryption** from the dialog that opens.

You can also chain the XML Encryption tool to a tool by right-clicking the desired tool node and selecting **Add Output** from the shortcut menu and then selecting **XML Encryption** from the dialog that opens. The tool will use the transformed XML.

You can chain the XML Encryption tool and the XML Signer tool to a messaging tool to perform both encryption and XML signature on a message. For more information on the XML Signer tool, see XML Signer.

You can also chain any tool, such as an Edit or Browse tool, to the **XML Encryption Tool** by right-clicking the desired **XML Encryption Tool** node and selecting **Add Output** from the shortcut menu and then selecting **XML Encryption** from the dialog that open

## Unlimited Strength Java Cryptography Extension

> **Important**
>
> In order to perform security operations using the XML Signature Verifier, XML Signer, or XML Encryption tools, or if using Key Stores, you will need to download and install the Unlimited Strength Java Cryptography Extension. For details, see JCE Prerequisite.

# Related Tutorials

The following tutorial lesson demonstrates how to use this tool:

- WS-Security