|  |  |
| --- | --- |
| January 19, 2011 |  |
|  | Security Framework |
| Version 1.1 |  |
| Processor user's guide | |



Table of Contents

[1 Introduction 3](#_Toc282069681)

[2 Configuration files structure 3](#_Toc282069682)

[2.1 SubsystemProperties 3](#_Toc282069683)

[2.2 Processor configuration file structure 4](#_Toc282069684)

[2.2.1 Engines 4](#_Toc282069685)

[2.2.2 Rules 5](#_Toc282069686)

[3 Example configuring engine of processor. 10](#_Toc282069687)

# Introduction

This document describes the processor subsystem. It allows to create mechanisms for the client application protection. These mechanisms are based on the individual parts of the functionality of various subsystems.

# Configuration files structure

Configuration is a set of XML documents. Each Security Framework subsystem has a separate configuration file. There is a root configuration file - MtSfConfigurationLoader.xml that references all subsystem’s configuration files.

Please see the section “2.1. Security Monitor configuration reference” in the Security Monitor user’s guide for the root configuration file reference.

The Processors configuration file structure at high level is shown below:

|  |
| --- |
| <SubsystemProperties IsRuntimeApiEnabled="true" IsRuntimeApiPublic="true" IsControlApiEnabled="true" IsControlApiPublic="true">  <EnginesProps>  <Engine />  <Engine />  </EnginesProps>  </SubsystemProperties> |

The following sections describe attributes, elements, and child elements.

## SubsystemProperties

Root element. It’s not required but recommended do not change the element’s name. It matches with name of the class that takes the configuration properties when it is loading.

There are the following child elements and attributes under the root.

Attributes:

| Attribute | Description |
| --- | --- |
| IsRuntimeApiEnabled | Required attribute.  Indicates whether the Security Monitor API is enabled. Prevents the API from initializing if set to **false**.  **Recomended value is «true».** |
| IsRuntimeApiPublic | Required attribute.  Indicates whether the Security Monitor API is exposed to public access.  **Recomended value is «true».** |
| IsControlApiEnabled | Required attribute.  Indicates whether the Security Monitor control API is enabled. Prevents the control API from initializing if set to **false**. *For future use*.  **Recomended value is «true».** |
| IsControlApiPublic | Required attribute.  Indicates whether the Security Monitor control API is exposed to public access. *For future use*.  **Recomended value is «true».** |

Elements:

| Element | Description |
| --- | --- |
| Engines | Required element.  Defines available engines and their properties. |

The element’s structure is described below.

## Processor configuration file structure

The Processor configuration file structure at high level is shown below:

|  |
| --- |
| <SubsystemProperties IsRuntimeApiEnabled="true" IsRuntimeApiPublic="true" IsControlApiEnabled="true" IsControlApiPublic="true">  <Engines>  <Engine>  <Rules>  <Rule/>  <Rule>  <Cases>  <Case />  <Case />  </Cases>  </Rule>  <Rule/>  </Rules>  </Engine>  <Engine>  <Rules>  <Rule/>  <Rule/>  </Rules>  </Engine>  </Engines>  </SubsystemProperties> |

The following sections describe attributes, elements, and child elements.

### **Engines**

Contains elements with processor engine properties. Each engine of processor contains chain of rules for handling data.

<SubsystemProperties>

<Engines>

|  |
| --- |
| <Engine Id="<Processor\_Engine\_ID>" Category="<Category\_name>" IsDefault="True|False" IdFirstRule="<Start\_rule\_ID>" RealType="MetraTech.SecurityFramework.ProcessorEngine" MaxExecution="<Integer\_value>">  <Rules>  …  </Rules>  </Engine> |

Child elements and attributes for properties of engine are described below:

| Element | Description |
| --- | --- |
| Rules | Required element.  Rules collection. These rules process the input data. Default type for elements is **«MetraTech.SecurityFramework.SequenceRule».** If it's necessary to determine another rule type indicate it in **RealType** attribute. |

| Attribute | Description |
| --- | --- |
| Id | Required attribute.  Defines a unique item ID. Uses internally. |
| RealType | Required attribute.  Defines a rule type. Must be “**MetraTech.SecurityFramework.ProcessorEngine**”. |
| IsDefault | Optional attribute.  Specifies whether the engine is default for its category. Default value is «false». |
| Category | Required attribute.  Sets category name for current engine. |
| IdFirstRule | Required attribute.  Rule Id. This rule starts processing. |
| MaxExecution | Required attribute.  Sets default value maximum executions count for rules in current engine. This value sets in rule, if this parameter in rule is not overrides. **Recomended value for this attribute is «5».** |

### Rules

This section contains rules collection for processor pipeline. Each rule handles data in processor chain. Rule types for processor pipeline are described below.

| Rule type | Description |
| --- | --- |
| SequenceRule | This rule type processes data and result is transferred to the following rule in chain of processor. This rule type is default. If it's necessary to determine another rule type indicate it in **RealType** attribute. |
| SwitchRule | This rule type used for determination next element handling input data in chain of processor. Next rule determined by comparing input data with template. Element **Cases** contains collection templates. |
| StitchRuleEx | This rule type combines functional of **SwitchRule** and **SequenceRule**, i.e. current rule handling input data and determination next element handling input data in chain of processor. Next rule determined by comparing handling result with template. Element **Cases** contains collection templates. |
| StopRule | This rule type used for declaring end processor chain. |

#### SequenceRule

Configuring section attributes for rules of type **SequenceRule**.

<SubsystemProperties>

<EnginesProps>

<Engine>

|  |
| --- |
| <Rules>  <Rule Id="Rule\_ID" RealType="MetraTech.SecurityFramework.SequenceRule" MaxExecution="<Unsigned\_value>" Subsystem="<Current\_subsystem\_Id>" IdNextRule="<Next\_rule\_Id>" IdEngine="<Current\_engine\_Id>" IdExceptionRule="<Exception\_rule\_Id>" >  </Rules> |

Contains elements with rule properties. Child elements and attributes for properties of rule are described below:

| Attribute | Description |
| --- | --- |
| Id | Required attribute.  Sets id for current rule. This property must be unique for current chain of processor. |
| RealType | Optional attribute.  Defines a rule type. Must be “**MetraTech.SecurityFramework.SequenceRule**”. |
| Subsystem | Required attribute  Sets subsystem name for current engine. This engine is handler for input data. |
| IdEngine | Required attribute  Sets current id engine. This engine is handler for input data. |
| IdNextRule | Required attribute  Sets id next rule, if current rule completed work without errors. This rule must be declared in current chain of processor. |
| IdExceptionRule | Required attribute  Sets id next rule if data handling throw exception. |
| MaxExecution | Optional attribute  Sets maximum executions count for current rule. If current rule executed count more than this value, processor subsystem throw exception. **Default value for this attribute is «5».** |

#### SwitchRule.

Configuring section attributes for rules of type **SwitchRule**.

<SubsystemProperties>

<EnginesProps>

<Engine>

|  |
| --- |
| <Rules>  <Rule Id="Rule\_ID" RealType="MetraTech.SecurityFramework.SwitchRule" MaxExecution="<Unsigned\_value>" DefaultIdRule="<Default\_rule\_Id>" IdExceptionRule="<Exception\_rule\_Id>">  <Cases>  . . .  </Cases>  </Rule>  </Rules> |

Contains elements with rule properties. Contains collection cases for processing output data and choice next rule in rules chain.

Child elements and attributes for properties of rule are described below:

| Element | Description |
| --- | --- |
| Cases | Required element  Sets collection conditions for choices next rule. If these cases do not work, id next rule defines by the **IdDefaultRule** parameter of current rule. |

| Attribute | Description |
| --- | --- |
| Id | Required attribute.  Sets id for current rule. This property must be unique for current chain of processor. |
| RealType | Required attribute.  Defines a rule type. Must be “**MetraTech.SecurityFramework.SwitchRule**”.  Optional attribute |
| DefaultIdRule | Required attribute  Sets id next rule, if current rule completed work without errors. This rule must be declared in current chain of processor. |
| IdExceptionRule | Required attribute  Sets id next rule if data handling throw exception. |
| MaxExecution | Sets maximum executions count for current rule. If current rule executed count more than this value, processor subsystem throw exception. **Default value for this attribute is «5».** |

#### SwitchRuleEx.

Configuring section attributes for rules of type **SwitchRuleEx**.

<SubsystemProperties>

<EnginesProps>

<Engine>

|  |
| --- |
| <Rules>  <Rule Id="Rule\_ID" RealType="MetraTech.SecurityFramework.SwitchRuleEx" MaxExecution="<UInt\_value>" Subsystem="<Current\_subsystem\_Id>" IdEngine="<Current\_engine\_Id>"  DefaultIdRule="<Default\_rule\_Id>" IdExceptionRule="<Exception\_rule\_Id>">  <Cases>  . . .  </Cases>  </Rule>  </Rules> |

Contains elements with rule properties. Contains collection cases for processing output data and choice next rule in rules chain.

Child elements and attributes for properties of rule are described below:

| Element | Description |
| --- | --- |
| Cases | Required element  Sets collection conditions for choices next rule. If these cases do not match, **IdDefaultRule** parameter of current rule defines id next rule. |

| Attribute | Description |
| --- | --- |
| Id | Required attribute.  Sets id for current rule. This property must be unique for current chain of processor. |
| RealType | Required attribute.  Defines a rule type. Must be “**MetraTech.SecurityFramework.SwitchRuleEx**”. |
| Subsystem | Required attribute  Sets subsystem name for current engine. This engine is handler for input data. |
| IdEngine | Required attribute  Sets current id engine. This engine is handler for input data. |
| DefaultIdRule | Required attribute  Sets id next rule, if current rule completed work without errors. This rule must be declared in current chain of processor. |
| IdExceptionRule | Required attribute  Sets id next rule if data handling throw exception. |
| MaxExecution | Optional attribute  Sets maximum executions count for current rule. If current rule executed count more than this value, processor subsystem throw exception. **Default value for this attribute is «5».** |

#### StopRule.

Configuring section attributes for rules of type **StopRule**.

<SubsystemProperties>

<EnginesProps>

<Engine>

|  |
| --- |
| <Rules>  <Rule Id="<Rule\_ID>" RealType="MetraTech.SecurityFramework.StopRule"/>  </Rules> |

Contains elements with rule properties. Child elements and attributes for properties of rule are described below:

| Attribute | Description |
| --- | --- |
| Id | Required attribute.  Sets id for current rule. This property must be unique for current chain of processor. |
| RealType | Required attribute.  Defines a rule type. Must be “**MetraTech.SecurityFramework.StopRule**”. |

#### Cases.

Configuring section of elements for rules of type **SwitchRule** and **SwitchRuleEx**.

<SubsystemProperties>

<EnginesProps>

<Engine>

<Rules>

|  |
| --- |
| <Rule>  <Cases  <Case CompareValue="<String\_or\_Regex>" IdNextRule="<Unique\_rule\_Id\_1>" OperationType="None|Equal|NotEqual|Contain|NotContain|RegexIsMatch| RegexIsNotMatch|IsInputOutputEqual|IsInputOutputNotEqual IdEngine="<Engine\_Id>" Subsystem="<Subsystem\_name>"/>  </Cases>  </Rule> |

Has the following attributes:

| Attribute | Description |
| --- | --- |
| CompareValue | Required attribute.  Template for comparison with the result of data processing. |
| IdNextRule | Required attribute.  Rule id. Works if the malicious code is detected. |
| OperationType | Required attribute.  Sets comparison type. |
| Subsystem | Optional attribute.  Sets subsystem name for result handler. This engine is handler for input data. If set this attribute, attribute **IdEngine** is required. |
| IdEngine | Optional attribute.  Sets engine id for result handler. If set this attribute, attribute **Subsystem** is required. |

Enum «**OperationType**» contain type of comparing operation. Can take values:

| Value | Description |
| --- | --- |
| None | This value is default. Always return «false». |
| Equal | Return «true» if input value well value in **CompareValue** attribute, else return «false». |
| NotEqual | Return «true» if input value do not well value in **CompareValue** attribute, else return «false». |
| Contain | Return «true» if a string specified in the attribute **CompareValue** contained in the input data, else return «false». |
| NotContain | Return «true» if a string specified in the attribute **CompareValue** not contained in the input data, else return «false». |
| RegexIsMatch | Return «true» if input data is match regular expression in **CompareValue** attribute, else return «false». |
| RegexIsNotMatch | Return «true» if input data is don't match regular expression in **CompareValue** attribute, else return «false». |
| IsInputOutputEqual | Return «true» if input data is match output data in current rule, else return «false».  This value always return "true" for **SwitchRule**. |
| IsInputOutputNotEqual | Return «true» if input data is don't match output data in current rule, else return «false».  This value always return "false" for **SwitchRule**. |

# Example: processor engine configuration.

Below describe example for processor "Processor.Default " configuration.

<Engines>

|  |
| --- |
| <Engine Id="Processor.Default" MaxExecution="10"  Category="General" IsDefault="true"  IdFirstRule="Default.Start.Rule"  RealType="MetraTech.SecurityFramework.ProcessorEngine">  <Rules>  <!--Configuring sequence rules-->  <Rule Id="Decoder.Url.Default.Rule"  MaxExecution="30" Subsystem="Decoder"  IdEngine="Url.V1" IdNextRule="Detector.Xss.Default.Rule"  IdExceptionRule="Processor.Default.Stop.Rule"/>  <Rule Id="Detector.Xss.Default.Rule"  MaxExecution="1" Subsystem="Detector"  IdEngine="Xss.Default" IdNextRule="Processor.Default.Stop.Rule"  IdExceptionRule="Processor.Default.Stop.Rule"/>  <!--Configuring switch rule-->  <Rule Id="Default.Start.Rule"  MaxExecution="1" RealType="MetraTech.SecurityFramework.SwitchRule"  DefaultIdRule="Detector.Xss.Default.Rule"  IdExceptionRule="Processor.Default.Stop.Rule">  <!--Configuring cases-section-->  <Cases>  <Case CompareValue="%"  IdNextRule="Decoder.Url.Default.Rule"  OperationType="Contain"/>  </Cases>  </Rule>    <Rule Id="Processor.Default.Stop.Rule"  RealType="MetraTech.SecurityFramework.StopRule" />  </Rules>  </Engine> |

Sheme of work for processor «Processor.Default» see at Pict.1.



Pict.1 Scheme of work for processor «Processor.Default»