

IBM Security Verify Access  
Version 10.0.3  
December 2021

*Federation Auditing*





---

# Contents

**Tables..... V**

**Chapter 1. Federation auditing events..... 1**

**Chapter 2. IBM\_SECURITY\_AUTHN\_events.....5**

**Chapter 3. IBM\_SECURITY\_AUTHN\_TERMINATE event..... 9**

**Chapter 4. IBM\_SECURITY\_ENCRYPTION events..... 11**

**Chapter 5. IBM\_SECURITY\_FEDERATION events..... 13**

**Chapter 6. IBM\_SECURITY\_MGMT\_AUDIT events.....19**

**Chapter 7. IBM\_SECURITY\_MGMT\_POLICY events..... 23**

**Chapter 8. IBM\_SECURITY\_RUNTIME events (Runtime start)..... 43**

**Chapter 9. IBM\_SECURITY\_RUNTIME events (SAML2 message transmission)..... 45**

**Chapter 10. IBM\_SECURITY\_TRUST events.....47**

**Chapter 11. Deploying pending changes..... 51**

**Index..... 53**



---

# Tables

1. Attributes and elements of the ContextDataElements element.....	1
2. Attributes for the SourceComponentId element.....	2
3. Attributes for the Situation element.....	3
4. Attributes for the Outcome element.....	4
5. Elements for an IBM_SECURITY_AUTHN event.....	5
6. Elements for an IBM_SECURITY_AUTHN_TERMINATE event.....	9
7. Elements for an IBM_SECURITY_ENCRYPTION event.....	11
8. Elements for an IBM_SECURITY_FEDERATION event.....	13
9. IBM_SECURITY_FEDERATION action-dependent additional attributes.....	15
10. Elements used in IBM_SECURITY_MGMT_AUDIT events.....	19
11. Elements for an IBM_SECURITY_MGMT_POLICY event.....	23
12. XPaths for shredding and staging attributes.....	25
13. Policy information attributes for a SAML20 self profile.....	26
14. Policy information attributes for a SAML20 partner profile.....	33
15. Elements for an IBM_SECURITY_RUNTIME event.....	43
16. Elements for an IBM_SECURITY_RUNTIME event.....	45
17. Elements for an IBM_SECURITY_TRUST event.....	47



# Chapter 1. Federation auditing events

This section lists the audit elements that are available for each audit event type.

Use the instructions in [Configuring auditing on the appliance](#) to configure auditing on the appliance.

Federation supports the following auditing events:

- IBM\_SECURITY\_TRUST
- IBM\_SECURITY\_RUNTIME

This section describes the available elements for each event type.

## Common elements for all events

The following elements are included with all security events:

- ContextDataElements
- SourceComponentIdelements
- Situation
- Outcome

## ContextDataElements

The contextId value, which is specified on the type attribute, is included in the ContextDataElements element to correlate all events that are associated with a single transaction.

Attribute	Value
name	Security Event Factory The XPath is: <code>CommonBaseEvent/contextDataElements/@name</code>
type	eventTrailId The XPath is: <code>CommonBaseEvent/contextDataElements/@type</code>
contextId	This element is a container element for the eventTrailId value; it does not have an XPath value.
eventTrailId	The event trail identifier value, for example, FIM_116320b90110104ab7ce9df3453615a1+729829786 The XPath is: <code>CommonBaseEvent/contextDataElements/[@type='eventTrailId']/contextId</code>

The following are XML-formatted examples of CBE event headers containing entries for the ContextDataElements element. These entries illustrate how separate events are correlated for a single transaction.

```
<CommonBaseEvent  
  creationTime="2007-01-31T20:59:57.625Z"  
  extensionName="IBM_SECURITY_TRUST"  
  globalInstanceId="CE4454A122E10AB044A1DBB16E020E1D80"
```

```

sequenceNumber="1" version="1.0.1">
<contextDataElements name="Security Event Factory" type="eventTrailId">
  <contextId>FIM_79f4e4c801101db5aba48cd8e0212be7+656317861</contextId>
</contextDataElements>
...
</CommonBaseEvent>

```

```

<CommonBaseEvent
  creationTime="2007-01-31T20:59:57.765Z"
  extensionName="IBM_SECURITY_TRUST"
  globalInstanceId="CE4454A122E10AB044A1DBB16E02213050"
  sequenceNumber="2" version="1.0.1">
  <contextDataElements name="Security Event Factory" type="eventTrailId">
    <contextId>FIM_79f4e4c801101db5aba48cd8e0212be7+656317861</contextId>
  </contextDataElements>
...
</CommonBaseEvent>

```

## SourceComponentId element

The SourceComponentId is an identifier that represents the source that generates the event.

Table 2. Attributes for the SourceComponentId element	
Attribute	Value
application	IBM Security Verify Access The XPath is: <code>CommonBaseEvent/sourceComponentId/@application</code>
component	The XPath is: <code>CommonBaseEvent/sourceComponentId/@component</code>
componentIdType	ProductName The XPath is: <code>CommonBaseEvent/sourceComponentId/@componentIdType</code>
componentType	<code>http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes</code> The XPath is: <code>CommonBaseEvent/sourceComponentId/@componentType</code>
executionEnvironment	<code>&lt;OS name&gt;#&lt;OS Architecture&gt;#&lt;OS.version&gt;</code> The XPath is: <code>CommonBaseEvent/sourceComponentId/@executionEnvironment</code>



Table 2. Attributes for the SourceComponentId element (continued)

Attribute	Value
location	<p>&lt;hostname&gt;</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='registryInfo']/children [@name='location']/values</pre>
locationType	<p>FQHostname</p> <p>The XPath is:</p> <pre>CommonBaseEvent/sourceComponentId/ @locationType</pre>
subComponent	<p>&lt;classname&gt;</p> <p>The XPath is:</p> <pre>CommonBaseEvent/sourceComponentId/ @subComponent</pre>

### Situation element

The Situation element describes the circumstance that caused the audit event.

Table 3. Attributes for the Situation element

Attribute	Value
categoryName	<p>ReportSituation</p> <p>The XPath is:</p> <pre>CommonBaseEvent/situation/ @categoryName</pre>
reasoningScope	<p>INTERNAL</p> <p>The XPath is:</p> <pre>CommonBaseEvent/situation/situationType/ @reasoningScope</pre>
reportCategory	<p>SECURITY</p> <p>The XPath is:</p> <pre>CommonBaseEvent/situation/situationType/ @reportCategory</pre>

### Outcome element

The Outcome element is the result of the action for which the security event is being generated.

Table 4. Attributes for the Outcome element

Attribute	Value
failureReason	The XPath is:  <code>CommonBaseEvent/extendedDataElements [@name='outcome']/children [@name='failureReason']/values</code>
majorStatus	The XPath is:  <code>CommonBaseEvent/extendedDataElements [@name='outcome']/children [@name='majorStatus']/values</code>
result	The XPath is:  <code>CommonBaseEvent/extendedDataElements [@name='outcome']/children [@name='result']/values</code>

**Note:** Federation does not use the **ReporterComponentId** field.

## Chapter 2. IBM\_SECURITY\_AUTHN\_events

This event type is generated by the authentication service when it authenticates a user accessing a protected resource.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_AUTHN event. All elements are included in the output, unless indicated otherwise.

Element	Description
action	<p>Optionally specifies the HTTP method on the requested resource or the operation that is performed by the provider of the authentication service.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='action']/values</pre>
authnProvider	<p>The provider of the authentication service.</p> <p>Sample data: com.tivoli.am.fim.authsvc.protocol.delegate.AuthSvcDelegate com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAuthenticator</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='authnProvider']/values</pre>
authnScope	<p>Optionally specifies the transaction identifier of the authentication policy.</p> <p>Sample data: 94434b2a-748e-42fe-af3d-67db04aa4ba0</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='authnScope']/values</pre>
authnType	<p>The URI identifier of the authentication policy.</p> <p>Sample data: urn:ibm:security:authentication:asf:password_hotp</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='authnType']/values</pre>
partner	<p>The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as 'Not Available'.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='partner']/values</pre>

Table 5. Elements for an IBM\_SECURITY\_AUTHN event (continued)

Element	Description
progName	<p>Optionally specifies the URL of the requested resource.</p> <p>Sample data: http://www.example.com</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='progName']/values</pre>
tokenType	<p>The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as 'Not Available'.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='tokenType']/values</pre>
trustRelationship	<p>The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as 'Not Available'.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='trustRelationship']/values</pre>
userInfo.appUserName	<p>Optionally specifies information about the user who is authenticating.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='userInfoList']/children[1]/children [@name='appUserName']/values</pre>
userInfo.attributes	<p>Optionally specifies the following types of additional information about user data that are audited during authentication:</p> <p><b>licenseFileMetadata</b> Metadata that is defined in the license agreement.</p> <p><b>licenseFileName</b> The license file name.</p> <p><b>userAction</b> The action that the user takes when the End-User License Agreement authentication mechanism presents the license agreement. The user can accept the license agreement or decline the license agreement.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='userInfoList']/children [@name='userInfo'] /children [@name='attributes']/children</pre>
xmlTokenType	<p>The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as 'Not Available'.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='xmlTokenType']/values</pre>

## Sample of an IBM\_SECURITY\_AUTHN event

The following example shows one event generated by the runtime for a two-factor authentication policy requiring both username password and one-time password authentications:

```
<CommonBaseEvent
  creationTime="2014-02-15T18:50:05.026Z"
  extensionName="IBM_SECURITY_AUTHN"
  globalInstanceId="FIM36e24f6301441708947ceef443526"
  sequenceNumber="2"
  version="1.1">
  <contextDataElements
    name="Security Event Factory"
    type="eventTrailId">
      <contextId>FIM_36e24f62014415f59913eef443526e68+1246005647</contextId>
    </contextDataElements>
  <extendedDataElements name="userInfoList" type="noValue">
    <children name="userInfo" type="noValue">
      <children name="registryUserName" type="string">
        <values>Not Available</values>
      </children>
      <children name="appUserName" type="string">
        <values>test_user</values>
      </children>
    </children>
  </extendedDataElements>
  <extendedDataElements name="tokenType" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <extendedDataElements name="authnProvider" type="string">
    <values>com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAAuthenticator</values>
  </extendedDataElements>
  <extendedDataElements name="action" type="string">
    <values>verify</values>
  </extendedDataElements>
  <extendedDataElements name="authnType" type="string">
    <values>urn:ibm:security:authentication:asf:password_hotp</values>
  </extendedDataElements>
  <extendedDataElements name="outcome" type="noValue">
    <children name="result" type="string">
      <values>SUCCESSFUL</values>
    </children>
    <children name="majorStatus" type="int">
      <values>0</values>
    </children>
  </extendedDataElements>
  <extendedDataElements name="trustRelationship" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <extendedDataElements name="progName" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <extendedDataElements name="authnScope" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <sourceComponentId
    application="IBM Security Verify Access"
    component="Authentication and Federated Identity"
    componentIdType="ProductName"
    executionEnvironment="Linux[amd64]#2.6.32-279.14.1.30.iss7_3.x86_64"
    location="example"
    locationType="FQHostname"
    subComponent="com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAAuthenticator"
    threadId="Default Executor-thread-60"
    componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
  <situation categoryName="ReportSituation">
    <situationType
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="ReportSituation"
      reasoningScope="INTERNAL"
      reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>
```



## Chapter 3. IBM\_SECURITY\_AUTHN\_TERMINATE event

This audit event is generated when a user is logged off.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_AUTHN\_TERMINATE event.

Element	Description
action	The operation that caused the termination of the authentication to occur - log off The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='action']/values</code>
authnProvider	The provider of the authentication service. The default is WebSEAL. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='authnProvider']/values</code>
authnType	The type of authentication that is used by the user - trustRelationship. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='authnType']/values</code>
terminateReason	The reason the session was terminated. For example, the user logged off. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='terminateReason']/values</code>
userInfo.appUserName	Information about the user who is logging off. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='userInfoList']/children[1]/children[@name='appUserName']/values</code>

### Sample of a IBM\_SECURITY\_AUTHN\_TERMINATE event

The following example shows an IBM\_SECURITY\_AUTHN\_TERMINATE event:

```
<CommonBaseEvent
  creationTime="2006-04-19T18:13:15.916Z"
  extensionName="IBM_SECURITY_AUTHN_TERMINATE"
  globalInstanceId="CE11DACFD02C005F20EE33FA70BA750567"
  sequenceNumber="10"
  version="1.0.1">
  <extendedDataElements name="authnType" type="string">
    <values>trustRelationship</values>
  </extendedDataElements>
  <extendedDataElements name="action" type="string">
```

```

    <values>logout</values>
  </extendedDataElements>
  <extendedDataElements name="outcome" type="noValue">
    <children name="majorStatus" type="int">
      <values>0</values></children>
      <children name="result" type="string">
        <values>SUCCESSFUL</values></children>
      </extendedDataElements>
    <extendedDataElements name="terminateReason" type="string">
      <values>UserLoggedOut</values>
    </extendedDataElements>
    <extendedDataElements name="authnProvider" type="string">
      <values>webseal</values>
    </extendedDataElements>
    <extendedDataElements name="userInfoList" type="noValue">
      <children name="userInfo" type="noValue">
        <children name="appUserName" type="string">
          <values>me_elain</values></children>
          <children name="registryUserName" type="string">
            <values>Not Available</values></children>
          </children>
        </extendedDataElements>
      </children>
    </extendedDataElements>
  <sourceComponentId
    application="IBM Security Verify Access"
    component="Authentication and Federated Identity"
    componentIdType="ProductName"
    executionEnvironment="Linux[x86]#2.4.21-4.EL"
    location="fimtest.au.ibm.com"
    locationType="FQHostname"
    subComponent=
      "com.tivoli.am.fim.saml20.protocol.actions.SAML20LocalLogoutAction"
    threadId="WebContainer : 0"
    componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
  <situation categoryName="ReportSituation">
    <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="ReportSituation"
      reasoningScope="INTERNAL"
      reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>

```



## Chapter 4. IBM\_SECURITY\_ENCRYPTION events

This event is generated whenever data is encrypted.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_ENCRYPTION event.

Element	Description
action	The operation that is being performed, either encryption or decryption. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='action']/values</code>
keyInfo	The key used to perform the action. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='keyInfo']/values</code>
msgInfo	The pertinent parts of the SOAP messages. The XPath is: <code>CommonBaseEvent/extendedDataElements[@name='msgInfo']/values</code>

### Sample of a IBM\_SECURITY\_ENCRYPTION event

The following example shows an IBM\_SECURITY\_ENCRYPTION event:

```
<CommonBaseEvent
  creationTime="2006-04-18T18:02:09.824Z"
  extensionName="IBM_SECURITY_ENCRYPTION"
  globalInstanceId="CE11DECF0574918190EA65C3F4A1F4E637"
  sequenceNumber="23"
  version="1.0.1">
  <extendedDataElements name="keyInfo" type="string">
    <values>DefaultKeyStore_testkey</values>
  </extendedDataElements>
  <extendedDataElements name="action" type="string">
    <values>Encrypt</values>
  </extendedDataElements>
  <extendedDataElements name="outcome" type="noValue">
    <children name="majorStatus" type="int">
      <values>0</values></children>
    <children name="result" type="string">
      <values>SUCCESSFUL</values></children>
    </extendedDataElements>
  <extendedDataElements name="msgInfo" type="string">
    <values>[{}urn:oasis:names:tc:SAML:2.0:protocol}Response[0]
      {http://www.w3.org/2000/09/xmldsig#}Signature[0]}</values>
  </extendedDataElements>
  <extendedDataElements name="userInfo" type="noValue">
    <children name="appUserName" type="string">
      <values>Not Available</values></children>
    <children name="registryUserName" type="string">
      <values>Not Available</values></children>
    </extendedDataElements>
  <sourceComponentId
    application="IBM Security Verify Access"
    component="Authentication and Federated Identity"
    componentIdType="ProductName"
    executionEnvironment="Linux[x86]#2.4.21-4.EL "
```

```
location="fimtest.au.ibm.com"
locationType="FQHostname"
subComponent=
"com.tivoli.am.fim.kess.service.jks.worker.impl.KessServiceJksWorkerImpl"
threadId="WebContainer : 1"
componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
<situation categoryName="ReportSituation">
  <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="ReportSituation"
    reasoningScope="INTERNAL"
    reportCategory="SECURITY"/>
</situation>
</CommonBaseEvent>
```

## Chapter 5. IBM\_SECURITY\_FEDERATION events

This event type is generated when a federation event occurs.

An IBM\_SECURITY\_FEDERATION event is generated by the following actions:

- When a user identity mapping is created, that is, when a user is federated.
- When a user consents to federate.
- When a user identity mapping is deleted, that is, when a user is de-federated.
- When a user mapping is updated, for example, an RNI operation.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_FEDERATION event.

Element	Description
action	The type of federation action: CreateMapping ConsentToFederate DeleteMapping UpdateMapping  The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='action']/values</pre>
messageAction	The type of action that is associated with the message.  The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='messageAction']/values</pre>
partner	The partner that sends or receives the message.  The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='partner']/values</pre>
profile	The profile within the federation.  The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='profile']/values</pre>
protocolName	The type of federation protocol.  The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='protocolName']/values</pre>

Table 8. Elements for an IBM\_SECURITY\_FEDERATION event (continued)

Element	Description
role	The role that the audit generating component takes. The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='role']/values</pre>
userInfo.appUserName	Information about the user who is performing this operation. The XPath is: <pre>CommonBaseEvent/extendedDataElements [@name='userInfoList']/children[1]/children[ @name='appUserName']/values</pre>

### Action-dependent additional attributes

Depending on the type of federation event action, the following attributes are available:

Table 9. IBM\_SECURITY\_FEDERATION action-dependent additional attributes

Action	Additional attributes	Description
CreateMapping	selfAlias	<p>If a self alias is set for the user, then this attribute shows that value.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'consentToFederate')] /../../children [@name='value']/values</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'selfAlias')] /../../children [@name='value']/values</pre>
	partnerAlias	<p>If a partner alias is set for the user, then this attribute shows that value.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'partnerAlias')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'partnerAlias')] /../../children [@name='value']/values</pre>
ConsentToFederate	ConsentToFederate	<p>This attribute specifies whether the user consented to federate. This event applies to Liberty and SAML20 protocol flows.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'consentToFederate')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'consentToFederate')] /../../children [@name='value']/values</pre>

Table 9. IBM\_SECURITY\_FEDERATION action-dependent additional attributes (continued)

Action	Additional attributes	Description
DeleteMapping	None	None
UpdateMapping	selfAlias	<p>If a self alias is set for the user, then this attribute shows the updated value.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'consentToFederate')] /../../children [@name='value']/values</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'selfAlias')] /../../children [@name='value']/values</pre>
	partnerAlias	<p>If a partner alias is set for the user, then this attribute shows the updated value.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'partnerAlias')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='attributes']/ children [@name='attribute']/children [@name='name']/values [contains(., 'partnerAlias')] /../../children [@name='value']/values</pre>

### Sample of a IBM\_SECURITY\_FEDERATION event

The following example shows an IBM\_SECURITY\_FEDERATION event:

```
<CommonBaseEvent
creationTime="2006-04-05T20:09:41.983Z"
extensionName="IBM_SECURITY_FEDERATION"
globalInstanceId="CE11DAC4E01E4BBF50E69681063F1AA1AF"
sequenceNumber="7"
version="1.0.1">
<extendedDataElements name="action" type="string">
<values>DeleteMapping</values>
</extendedDataElements>
<extendedDataElements name="partner" type="string">
<values>https://sp:444/FIM/sps/saml20-sp/saml20</values>
</extendedDataElements>
<extendedDataElements name="relayState" type="string">
<values>Not Available</values>
</extendedDataElements>
<extendedDataElements name="outcome" type="noValue">
<children name="majorStatus" type="int"><values>0</values></children>
```

```

    <children name="result" type="string"><values>SUCCESSFUL</values></children>
  </extendedDataElements>
  <extendedDataElements name="clientInfo" type="boolean">
    <values>>false</values>
  </extendedDataElements>
  <extendedDataElements name="role" type="string">
    <values>IP</values>
  </extendedDataElements>
  <extendedDataElements name="messageAction" type="string">
    <values>RECEIVED</values>
  </extendedDataElements>
  <extendedDataElements name="profile" type="string">
    <values>urn:oasis:names:tc:SAML:2.0:profiles:SSO:nameid-mgmt</values>
  </extendedDataElements>
  <extendedDataElements name="protocolName" type="string">
    <values>urn:oasis:names:tc:SAML:2.0:protocol</values>
  </extendedDataElements>
  <extendedDataElements name="userInfoList" type="noValue">
    <children name="userInfo" type="noValue">
      <children name="appUserName" type="string"><values>Elain</values></children>
      <children name="registryUserName" type="string">
        <values>Not Available</values></children>
      </children>
    </extendedDataElements>
  </extendedDataElements>
  <sourceComponentId
    application="IBM Security Verify Access"
    component="Authentication and Federated Identity"
    componentIdType="ProductName"
    executionEnvironment="Linux[x86]#2.4.21-4.EL"
    location="fimttest.au.ibm.com"
    locationType="FQHostname"
    subComponent=
    "com.tivoli.am.fim.saml20.protocol.actions.nimgmt.
    SAML20ProcessManageNameIDMessageAction"
    threadId="WebContainer : 1"
    componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
  <situation categoryName="ReportSituation">
    <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="ReportSituation"
      reasoningScope="INTERNAL"
      reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>

```





---

## Chapter 6. IBM\_SECURITY\_MGMT\_AUDIT events

This event type provides information about changes to the auditing settings; for example, if auditing is enabled or disabled or if auditing is set for specific transactions.

IBM\_SECURITY\_MGMT\_AUDIT events are generated when the audit configuration is modified. Changes to the following data are audited:

- User name
- Action
- Domain
- Audit configuration properties:
  - Enable auditing
  - Enable auditing for specific audit event types. Event types are shown in the following table under the mgmtInfo element.
  - Audit log location
  - Maximum number of audit files
  - Maximum audit file size
  - Disk cache location
  - Web service SSL keystore
  - Enable Web service basic authentication
- Disable auditing:
  - User name
  - Action

The following table lists the elements that can be displayed in the output of an IBM\_SECURITY\_MGMT\_AUDIT event.

<b>Element</b>	<b>Description</b>
action	<p>The type of action that occurred against the audit settings. Possible values are Modify and Disable.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='action']/values</pre>

Table 10. Elements used in IBM\_SECURITY\_MGMT\_AUDIT events (continued)

Element	Description
mgmtInfo	<p>Information about the auditing operation. The supported items and values are:</p> <p>EnableAudit=true   false            Domain=<i>domain_name</i>            AuditLogLocation=<i>path</i>            CacheLocation=<i>path</i>            WebServiceBasicAuthUsername=<i>username</i>            WebServiceBasicAuthPassword=<i>password</i>            WebServiceKeyIdentifier=<i>keyname</i>            WebServiceURL=<i>URL</i>            MaxAuditFiles=<i>number</i>            AuditFileSize=<i>number</i>            UseWebServiceBasicAuth=true   false            WebServiceKeystore=<i>keystore_name</i>            AuditSecurityAuthnEvents=true   false            AuditSecurityAuthnTerminateEvents=true   false            AuditSecurityEncryptionEvents=true   false            AuditSecuritySigningEvents=true   false            AuditSecurityFederationEvents=true   false            AuditSecurityTrustEvents=true   false            AuditSecurityMgmtPolicyEvents=true   false            AuditSecurityMgmtAuditEvents=true   false</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='mgmtInfo']/children [@name='command']/values</pre>
userInfo	<p>Information about the user who is performing the operation.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='userInfo']/children [@name='appUserName']/children [@name='registryUserName']/values</pre>
type	<p>Always set to the audit value.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='type']/values</pre>

### Sample of an IBM\_SECURITY\_MGMT\_AUDIT event

The following example shows an IBM\_SECURITY\_MGMT\_AUDIT event:

```
<CommonBaseEvent
  creationTime="2007-04-25T07:01:51.726Z"
  extensionName="IBM_SECURITY_MGMT_AUDIT"
  globalInstanceId="CEFA81F627EBCFC5DFA1DBF2FAD8573020"
```

```

sequenceNumber="1"
version="1.0.1">
<contextDataElements name="Security Event Factory" type="eventTrailId">
  <contextId>FIM_278bcbef011213a9865f8a816f9717a6+1969112872</contextId>
</contextDataElements>
<extendedDataElements name="mgmtInfo" type="noValue">
  <children name="command" type="string">
    <values>EnableAudit=true;
      Domain=mydomain-server1;
      AuditLogLocation=audit_location;
      AuditFileSize=10;
      MaxAuditFiles=100;AuditAuthnEvents=true;
      AuditAuthnTerminateEvents=true;
      AuditFederationEvents=true;
      AuditTrustEvents=true;
      AuditSigningEvents=true;
      AuditEncryptionEvents=true;
      AuditMgmtPolicyEvents=true;
      AuditMgmtAuditEvents=true;
    </values>
  </children>
</extendedDataElements>
<extendedDataElements name="type" type="string">
  <values>audit</values>
</extendedDataElements>
<extendedDataElements name="userInfo" type="noValue">
  <children name="appUserName" type="string">
    <values>unauthenticatedUser</values>
  </children>
  <children name="registryUserName" type="string">
    <values>Not Available</values>
  </children>
</extendedDataElements>
<extendedDataElements name="action" type="string">
  <values>Modify</values>
</extendedDataElements>
<extendedDataElements name="outcome" type="noValue">
  <children name="result" type="string">
    <values>SUCCESSFUL</values>
  </children>
  <children name="majorStatus" type="int">
    <values>0</values>
  </children>
</extendedDataElements>
<sourceComponentId
  application="IBM Security Verify Access"
  component="Authentication and Federated Identity"
  componentIdType="ProductName"
  executionEnvironment="Linux[x86]#2.6.9-34.ELsmp"
  location="fimfun2.austin.ibm.com"
  locationType="FQHostname"
  subComponent="com.tivoli.am.fim.mgmt.fim.FIMManagementImpl"
  threadId="SoapConnectorThreadPool : 0"
  componentType=
    "http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
<situation categoryName="ReportSituation">
  <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="ReportSituation"
    reasoningScope="INTERNAL"
    reportCategory="SECURITY"/>
</situation>
</CommonBaseEvent>

```



## Chapter 7. IBM\_SECURITY\_MGMT\_POLICY events

This event type is generated by federation runtime management calls.

An IBM\_SECURITY\_MGMT\_POLICY event is generated by the following actions:

- When a new federation is created.
- When an existing federation is modified.
- When a federation is deleted.
- When a partner is added to a federation.
- When a partner is deleted from a federation.
- When the properties of a partner are modified.
- When a Web Service partner is created.
- When a Web Service partner is modified.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_MGMT\_POLICY event.

Element	Description
action	<p>The type of operation that is being performed. The supported operations are:</p> <ul style="list-style-type: none"><li>• create</li><li>• delete</li><li>• modify</li></ul> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='action']/values</pre>
mgmtInfo.command	<p>Information about the management operation. The supported management operations are:</p> <ul style="list-style-type: none"><li>• CreateFederation</li><li>• ModifyFederation</li><li>• DeleteFederation</li><li>• CreateFederationPartner</li><li>• ModifyFederationPartner</li><li>• DeleteFederationPartner</li><li>• CreateWebServicePartner</li><li>• ModifyWebServicePartner</li></ul> <p><b>Note:</b> Modifying or deleting a Web service partner generates a ModifyWebServicePartner operation.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='mgmtInfo']/children [@name='command']/values</pre>

Table 11. Elements for an IBM\_SECURITY\_MGMT\_POLICY event (continued)

Element	Description
policyInfo.attributes	<p>The different attributes for this policyInfo object. See the tables in “Attributes determined by policy profile type” on page 24 for attributes that might be present in the event. Each attribute consists of a name and a value.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='value']/values</pre>
policyInfo.name	<p>The name of the federation, the name of the partner, or the name of the Web service partner.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='name']/values</pre>
policyInfo.type	<p>Information about the policy object. The type can be either federation or partner.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='type']/values</pre>
userInfo.appUserName	<p>Information about the user who is performing this operation.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='userInfoList']/children[1]/children [@name='appUserName']/values</pre>

### Attributes determined by policy profile type

Depending on the type of profile used, policyInfo contains different attributes. These attributes can be shredded or extracted for custom reports.

**Note:** Different partner attributes are specified as *partner id\_attribute name*, where *partner id* is the uuid assigned to a partner and *attribute name* is an attribute from the following tables.

### Shredding and staging attributes

This example shows how the data can be shredded by using the contains keyword. It requires an XPath for each attribute.

To stage the following name-value pairs for FederationName, FederationId and SAML1.SigningKey Identifier from the attributes fields of a policyInfo, use the following XPaths:

Table 12. XPathS for shredding and staging attributes

Field	XPath
policyInfo attributes FederationId	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'FederationId')]</pre>
policyInfo attributes FederationId value	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'FederationId')] /../../children [@name='value']/values</pre>
policyInfo attributes FederationName	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'FederationName')]</pre>
policyInfo attributes FederationName value	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'FederationName')] /../../children [@name='value']/values</pre>
policyInfo attributes SAML1.SigningKeyIdentifier	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML1.SigningKeyIdentifier')]</pre>
policyInfo attributes SAML1.SigningKeyIdentifier value	<pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML1.SigningKeyIdentifier')] /../../children [@name='value']/values</pre>

### SAML20 self attributes

The following table lists the SAML20 self attributes that are audited in profiles for service providers and identity providers.

Table 13. Policy information attributes for a SAML20 self profile.

Common attributes for service providers and identity providers	Definitions
SAML2.SigningKeyIdentifier	<p>The identifier for the key used to sign outgoing messages.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SigningKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SigningKeyIdentifier')] /../../children [@name='value']/values</pre>
SAML2.DecryptionKeyIdentifier	<p>The pointer to the private key used to decrypt the symmetric encryption key in encrypted messages from a partner.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.DecryptionKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.DecryptionKeyIdentifier')] /../../children [@name='value']/values</pre>



Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.EncryptionKeyTransportAlgorithm	<p>The algorithm used to encrypt the symmetric encryption key.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2. EncryptionKeyTransportAlgorithm)]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2. EncryptionKeyTransportAlgorithm')] /../../children [@name='value']/values</pre>
SAML2.SignArtifactRequest	<p>The indicator for whether the provider signs outgoing artifact requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignArtifactRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignArtifactRequest')] /../../children [@name='value']/values</pre>

Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SignArtifactResponse	<p>The indicator for whether the provider signs outgoing artifact responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignArtifactResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignArtifactResponse')] /../../children [@name='value']/values</pre>
SAML2.SignLogoutRequest	<p>The indicator for whether the provider signs outgoing logout requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignLogoutRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignLogoutRequest')] /../../children [@name='value']/values</pre>

Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SignLogoutResponse	<p>The indicator for whether the provider signs outgoing logout responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignLogoutResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignLogoutResponse')] /../../children [@name='value']/values</pre>
SAML2.SignNameIDManagementRequest	<p>The indicator for whether the provider signs outgoing name identifier management requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignNameIDManagementRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignNameIDManagementRequest')] /../../children [@name='value']/values</pre>

Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SignNameIDManagementResponse	<p>The indicator for whether the provider signs outgoing name identifier management responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignNameIDManagementResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignNameIDManagementResponse')] /../../children [@name='value']/values</pre>
SAML2.PresentFederationConsent	<p>The indicator for whether the identity provider presents a consent to federate page when the federation occurs.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.PresentFederationConsent')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.PresentFederationConsent')] /../../children [@name='value']/values</pre>
<b>Additional self attributes for service providers only</b>	

Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SignAuthnRequest	<p>The indicator for whether the provider signs outgoing authentication requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignAuthnRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SignAuthnRequest')] /../../children [@name='value']/values</pre>
SAML2.WantAssertionsSigned	<p>The indicator for whether the provider wants to receive signed assertions.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.WantAssertionsSigned')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.WantAssertionsSigned')] /../../children [@name='value']/values</pre>
<b>Additional self attributes for identity providers only</b>	

Table 13. Policy information attributes for a SAML20 self profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.ValidateAuthnRequest	<p>The indicator for whether the provider validates incoming authentication requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateAuthnRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateAuthnRequest')] /../../children [@name='value']/values</pre>
SAML2.SignAuthnResponse	<p>The indicator for whether the provider signs authentication responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignAuthnResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SignAuthnResponse')] /../../children [@name='value']/values</pre>

### SAML20 partner attributes

The following table lists the SAML20 partner attributes that are audited in profiles for service providers and identity providers.

Table 14. Policy information attributes for a SAML20 partner profile.

Common attributes for service providers and identity providers	Definitions
SAML2.SoapRequestClientBasicAuth	<p>The indicator for whether client basic authentication is used for the SOAP backchannels.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SoapRequestClientBasicAuth')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SoapRequestClientBasicAuth')] /../../children [@name='value']/values</pre>
SAML2.SoapRequestClientCertAuth	<p>The indicator for whether client certificate authentication is used for the SOAP backchannels.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SoapRequestClientCertAuth')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.SoapRequestClientCertAuth')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SoapRequestServerCertAuth	<p>The indicator for whether server certificate authentication is used for the SOAP backchannels.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SoapRequestServerCertAuth')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2.SoapRequestServerCertAuth')] /../../children [@name='value']/values</pre>
SAML2. SoapRequestServerCertAuthKeyIdentifier	<p>The identifier for the key used when using server certificate authentication.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2. SoapRequestServerCertAuthKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (., 'SAML2. SoapRequestServerCertAuthKeyIdentifier')] /../../children [@name='value']/values</pre>



Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2. SoapRequestClientCertAuthKeyIdentifier	<p>The identifier for the key used when using client certificate authentication.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2. SoapRequestClientCertAuthKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2. SoapRequestClientCertAuthKeyIdentifier')] /../../children [@name='value']/values</pre>
SAML2.ValidateKeyIdentifier	<p>The identifier for the key used to validate signatures on incoming messages from a partner. This attribute is the signing public key of the partner.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateKeyIdentifier')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.EncryptionKeyIdentifier	<p>The identifier for the key used to encrypt outgoing messages to a partner. This attribute is the encrypting public key of the partner.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.EncryptionKeyIdentifier')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.EncryptionKeyIdentifier')] /../../children [@name='value']/values</pre>
SAML2.ValidateArtifactRequest	<p>The indicator for whether the provider validates incoming artifact requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateArtifactRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateArtifactRequest')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.ValidateArtifactResponse	<p>The indicator for whether the provider validates incoming artifact responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateArtifactResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateArtifactResponse')] /../../children [@name='value']/values</pre>
SAML2.ValidateLogoutRequest	<p>The indicator for whether the provider validates incoming logout requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateLogoutRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.ValidateLogoutRequest')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.ValidateLogoutResponse	<p>The indicator for whether the provider validates incoming logout responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.ValidateLogoutResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.ValidateLogoutResponse')] /../../children [@name='value']/values</pre>
SAML2. ValidateNameIDManagementRequest	<p>The indicator for whether the provider validates incoming name identifier management requests.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2. ValidateNameIDManagementRequest')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2. ValidateNameIDManagementRequest')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2. ValidateNameIDManagementResponse	<p>The indicator for whether the provider validates incoming name identifier management responses.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2. ValidateNameIDManagementResponse')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2. ValidateNameIDManagementResponse')] /../../children [@name='value']/values</pre>
SAML2.EncryptNameIdentifiers	<p>The indicator for whether name identifiers must be encrypted for the partner.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.EncryptNameIdentifiers')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.EncryptNameIdentifiers')] /../../children [@name='value']/values</pre>

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.BlockEncryptionAlgorithm	<p>The algorithm used to encrypt the data.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.BlockEncryptionAlgorithm')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.BlockEncryptionAlgorithm')] /../../children [@name='value']/values</pre>
<b>Additional partner attributes for service providers only</b>	
SAML2.WantAssertionsSigned	<p>The indicator for whether the provider wants to receive signed assertions.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.WantAssertionsSigned')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (.,'SAML2.WantAssertionsSigned')] /../../children [@name='value']/values</pre>
<b>Additional partner attributes for identity providers only</b>	

Table 14. Policy information attributes for a SAML20 partner profile. (continued)

Common attributes for service providers and identity providers	Definitions
SAML2.SignAssertions	<p>The indicator for whether the provider signs assertions.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.SignAssertions')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.SignAssertions') /../../children [@name='value']/values]</pre>
SAML2.EncryptAssertions	<p>The indicator for whether the provider encrypts assertions.</p> <p>The XPath for the attribute name is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.EncryptAssertions')]</pre> <p>The XPath for the attribute value is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='policyInfo']/children [@name='attributes']/children [@name='attribute']/children [@name='name']/values [contains (..,'SAML2.EncryptAssertions') /../../children [@name='value']/values]</pre>

### Sample of a IBM\_SECURITY\_MGMT\_POLICY event

The following is an example of a IBM\_SECURITY\_MGMT\_POLICY event:

```
<CommonBaseEvent
creationTime="2006-04-26T12:22:25.874Z"
extensionName="IBM_SECURITY_MGMT_POLICY"
globalInstanceId="CE11DAD51F526D53D0E30FDAA2C9637F07"
sequenceNumber="1"
version="1.0.1">
<extendedDataElements name="action" type="string">
<values>Create</values>
</extendedDataElements>
<extendedDataElements name="outcome" type="noValue">
<children name="majorStatus" type="int">
<values>0</values></children>
<children name="result" type="string">
```

```

    <values>SUCCESSFUL</values></children>
</extendedDataElements>
<extendedDataElements name="policyInfo" type="noValue">
  <children name="attributes" type="noValue">
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>saml11-ip</values></children>
      <children name="name" type="string">
        <values>FederationName</values></children>
    </children>
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>enabled</values></children>
      <children name="name" type="string">
        <values>State</values></children>
    </children>
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>saml11-ip</values></children>
      <children name="name" type="string">
        <values>FederationId</values></children>
    </children>
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>DefaultKeyStore_testkey</values></children>
      <children name="name" type="string">
        <values>SAML1.SigningKeyIdentifier</values></children>
    </children>
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>>true</values></children>
      <children name="name" type="string">
        <values>SAML1.SignArtifactResponse</values></children>
    </children>
    <children name="attribute" type="noValue">
      <children name="value" type="string">
        <values>SAML1_1</values></children>
      <children name="name" type="string">
        <values>FederationProtocol</values></children>
    </children>
  </children>
</children>
<children name="type" type="string">
  <values>federation</values></children>
<children name="name" type="string">
  <values>saml11-ip</values></children>
</extendedDataElements>
<extendedDataElements name="mgmtInfo" type="noValue">
  <children name="command" type="string">
    <values>CreateFederation</values></children>
</extendedDataElements>
<extendedDataElements name="userInfo" type="noValue">
  <children name="appUserName" type="string">
    <values>Not Available</values></children>
  <children name="registryUserName" type="string">
    <values>Not Available</values></children>
</extendedDataElements>
<sourceComponentId
  application="IBM Security Verify Access"
  component="Authentication and Federated Identity"
  componentIdType="ProductName"
  executionEnvironment="Linux[x86]#2.4.21-4.EL"
  location="localhost.localdomain"
  locationType="FQHostname"
  subComponent="com.tivoli.am.fim.mgmt.fim.FIMManagementImpl"
  threadId="SoapConnectorThreadPool : 1"
  componentType=
"http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
<situation categoryName="ReportSituation">
  <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="ReportSituation"
    reasoningScope="INTERNAL"
    reportCategory="SECURITY"/>
</situation>
</CommonBaseEvent>

```



## Chapter 8. IBM\_SECURITY\_RUNTIME events (Runtime start)

This event type is generated when the runtime is started.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_RUNTIME event.

Element	Description
Domain	The XPath is:  CommonBaseEvent/extendedDataElements [@name='Domain']/values
IsMgmtAudit	The XPath is:  CommonBaseEvent/extendedDataElements [@name='IsMgmtAudit']/values
nameInApp	The XPath is:  CommonBaseEvent/extendedDataElements [@name='resourceInfo']/children [@name='nameInApp']/values
nameInPolicy	The XPath is:  CommonBaseEvent/extendedDataElements [@name='resourceInfo']/children [@name='nameInPolicy']/values
type	The XPath is:  CommonBaseEvent/extendedDataElements [@name='resourceInfo']/children [@name='type']/values
uniqueID	The XPath is:  CommonBaseEvent/extendedDataElements [@name='resourceInfo']/children [@name='uniqueID']/values
action	The XPath is:  CommonBaseEvent/extendedDataElements [@name='action']/values

### Samples of IBM\_SECURITY\_RUNTIME events

The following example shows an events generated by a runtime request.

```
<CommonBaseEvent  
  creationTime="2016-09-20T03:45:55.838Z"  
  extensionName="IBM_SECURITY_RUNTIME"  
  globalInstanceId="FIM45b338ad015712f2ad5cd6c9d3998"
```

```

sequenceNumber="0" version="1.1">
<contextDataElements
  name="Security Event Factory"
  type="eventTrailId">
  <contextId>FIM_45b337ec01571ef29f4cd6c9d3998025+1092518090</contextId>
</contextDataElements>
<extendedDataElements name="Domain" type="string">
  <values>Not Available</values>
</extendedDataElements>
<extendedDataElements name="IsMgmtAudit" type="boolean">
  <values>>false</values>
</extendedDataElements>
<extendedDataElements name="action" type="string">
  <values>auditStart</values>
</extendedDataElements>
<extendedDataElements name="resourceInfo" type="noValue">
  <children name="nameInApp" type="string"><values></values>
  </children>
  <children name="nameInPolicy" type="string"><values></values>
  </children>
  <children name="type" type="string"><values>application</values>
  </children>
  <children name="uniqueId" type="long"><values>0</values>
  </children>
</extendedDataElements>
<extendedDataElements name="outcome" type="noValue">
  <children name="result" type="string"><values>SUCCESSFUL</values>
  </children>
  <children name="majorStatus" type="int"><values>0</values>
  </children>
</extendedDataElements>
<sourceComponentId
  application="IBM Security Verify Access"
  component="Authentication and Federated Identity"
  componentIdType="ProductName"
  executionEnvironment="Linux[amd64]#2.6.32-279.14.1.91.iss7_3.x86_64"
  location="isam.myidp.ibm.com"
  locationType="FQHostname"
  subComponent="com.tivoli.am.fim.audit.event.impl.RuntimeAuditAdapterImpl"
  threadId="Default Executor-thread-10"
  componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
<situation categoryName="ReportSituation">
  <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="ReportSituation"
    reasoningScope="INTERNAL"
    reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>

```

## Chapter 9. IBM\_SECURITY\_RUNTIME events (SAML2 message transmission)

This event type is generated when transmitting SAML2 authentication request and response messages.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_RUNTIME event.

Element	Description
type	The XPath is:  CommonBaseEvent/extendedDataElements [@name='resourceInfo']/children [@name='type']/values
action	The XPath is:  CommonBaseEvent/extendedDataElements [@name='action']/values
MessageContent	The XPath is:  CommonBaseEvent/extendedDataElements [@name='MessageContent']/values

### Samples of IBM\_SECURITY\_RUNTIME events

The following example shows an events generated by a runtime request.

```
<CommonBaseEvent creationTime="2016-09-13T02:54:22.612Z"
extensionName="IBM_SECURITY_RUNTIME" globalInstanceId="FIM2177819501571d34a705ed4ca920c"
sequenceNumber="10" version="1.1">
<contextDataElements name="Security Event Factory" type="eventTrailId">
<contextId>FIM_2177814701571a92875fed4ca920ca5a+1206972288</contextId>
</contextDataElements>
<extendedDataElements name="MessageContent" type="string">
<values><samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://sp-wga/isam/sps/saml20sp/saml20/login"
Destination="https://ip-wga/isam/sps/saml20ip/saml20/login"
ForceAuthn="false" ID="FIMREQ_217780c5-0157-1645-a617-f796a7dfc338"
IsPassive="false" IssueInstant="2016-09-13T02:54:22Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Version="2.0"><saml:Issuer Format="
urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
https://sp-wga/isam/sps/saml20sp/saml20</saml:Issuer>
<samlp:NameIDPolicy AllowCreate="false"
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
</samlp:NameIDPolicy></samlp:AuthnRequest></values>
</extendedDataElements>
<extendedDataElements name="action" type="string">
<values>Received</values>
</extendedDataElements>
<extendedDataElements name="resourceInfo" type="noValue">
<children name="nameInApp" type="string">
<values/>
</children>
<children name="nameInPolicy" type="string">
<values/>
</children>
<children name="type" type="string">
<values>Saml20AuthnRequest</values>
</children>
</extendedDataElements>
```

```
<extendedDataElements name="outcome" type="noValue">
<children name="result" type="string">
<values>SUCCESSFUL</values>
</children>
<children name="majorStatus" type="int">
<values>0</values>
</children>
</extendedDataElements>
<sourceComponentId application="IBM Security Verify Access"
component="Authentication and Federated Identity" componentIdType="ProductName"
executionEnvironment="Linux[amd64]#2.6.32-279.14.1.91.iss7_3.x86_64"
location="ip" locationType="FQHostname"
subComponent="com.tivoli.am.fim.saml20.protocol.actions.sso.SAML20ValidateAuthnRequestAction"
threadId="Default Executor-thread-61"
componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
<situation categoryName="ReportSituation">
<situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ReportSituation" reasoningScope="INTERNAL" reportCategory="SECURITY"/>
</situation>
</CommonBaseEvent>
```

## Chapter 10. IBM\_SECURITY\_TRUST events

This event type is generated by the trust server when it validates a token, issues a token, maps an identity, or authorizes a Web service call.

The following table lists the elements that can be shown in the output of an IBM\_SECURITY\_TRUST event.

Element	Description
accessDecision	<p>For the authorization module, it is the result of the authorization decision. This element is filled out only when the action is authorized.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='accessDecision']/values</pre>
action	<p>The action being performed. Possible actions are:</p> <ul style="list-style-type: none"><li>• authorize</li><li>• issue</li><li>• map</li><li>• validate</li></ul> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='action']/values</pre>
appliesTo	<p>The destination or resource that the request or token applies to.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='appliesTo']/values</pre>
issuer	<p>The party responsible for issuing the token.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='issuer']/values</pre>
moduleName	<p>The module in the STS module chain that the action is taken on.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='moduleName']/values</pre>
ruleName	<p>The rule name used for the mapping module. This element is filled out only when specified action is set to <i>map</i>.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='ruleName']/values</pre>

Table 17. Elements for an IBM\_SECURITY\_TRUST event (continued)

Element	Description
token	<p>The incoming token that the action is being taken on. Only the first 1024 characters of the token are set. When the action is set to <i>map</i>, this element represents the incoming principal.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='token']/values</pre>
tokenInfo	<p>The internal representation of the user information <i>after</i> changes are made by the module. Only the first 1024 characters of the token are set. When action is set to <i>map</i>, this element represents the outgoing principal. When the action is set to <i>authorize</i>, this element represents the principal for whom the access decision was made.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='tokenInfo']/values</pre>
tokenType	<p>The type of token the module is using.</p> <p>The XPath is:</p> <pre>CommonBaseEvent/extendedDataElements [@name='tokenType']/values</pre>

### Samples of IBM\_SECURITY\_TRUST events

The following example shows an event generated by a Trust request.

```
<CommonBaseEvent creationTime="2013-07-19T06:21:05.256Z"
extensionName="IBM_SECURITY_TRUST"
globalInstanceId="FIMf596c16e013f12d38eb0b66d4d925"
sequenceNumber="1" version="1.1">
  <contextDataElements name="Security Event Factory"
type="eventTrailId">
    <contextId>FIM_f596bda0013f188f9983b66d4d92542a+971185751</contextId>
  </contextDataElements>
  <extendedDataElements name="tokenType" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <extendedDataElements name="issuer" type="string">
    <values>/otpfed/otp/get/delivery/options/issuer</values>
  </extendedDataElements>
  <extendedDataElements name="token" type="string">
    <values>user1 [ Attribute 1 name [ value 1 user1 ] ]</values>
  </extendedDataElements>
  <extendedDataElements name="ruleName" type="string">
    <values>otp_get_methods.js </values>
  </extendedDataElements>
  <extendedDataElements name="moduleName" type="string">
    <values>com.tivoli.am.fim.trustserver.sts.modules.STSMapDefault</values>
  </extendedDataElements>
  <extendedDataElements name="appliesTo" type="string">
    <values>/otpfed/otp/get/delivery/options/appliesto</values>
  </extendedDataElements>
  <extendedDataElements name="action" type="string">
    <values>Map</values>
  </extendedDataElements>
  <extendedDataElements name="tokenInfo" type="string">
    <values>user1 [ Attribute 1 name [ value 1 user1 ] ]</values>
  </extendedDataElements>
</CommonBaseEvent>
```

```

<extendedDataElements name="outcome" type="noValue">
  <children name="result" type="string">
    <values>SUCCESSFUL</values>
  </children>
  <children name="majorStatus" type="int">
    <values>0</values>
  </children>
</extendedDataElements>
<sourceComponentId application="IBM Security Verify Access"
component="Authentication and Federated Identity"
componentIdType="ProductName"
executionEnvironment="Linux[amd64]#2.6.32-279.14.1.30.iss7_3.x86_64"
location="localhost" locationType="FQHostname"
subComponent="com.tivoli.am.fim.trustserver.sts.modules.STSMapDefault"
threadId="Default Executor-thread-6"
componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
  <situation categoryName="ReportSituation">
    <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ReportSituation" reasoningScope="INTERNAL" reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>

```





---

# Chapter 11. Deploying pending changes

Some configuration and administration changes require an extra deployment step.

## About this task

When you use the graphical user interface on the appliance to specify changes, some configuration and administration tasks take effect immediately. Other tasks require a deployment step to take effect. For these tasks, the appliance gives you a choice of deploying immediately or deploying later. When you must make multiple changes, you can wait until all changes are complete, and then deploy all of them at one time.

When a deployment step is required, the user interface presents a message that says that there is an undeployed change. The number of pending changes is displayed in the message, and increments for each change you make.

**Note:** If any of the changes require the runtime server to be restarted, the restart occurs automatically when you select **Deploy**. The runtime server will then be unavailable for a period of time until the restart completes.

## Procedure

1. When you finish making configuration changes, select **Click here to review the changes or apply them to the system**.

The **Deploy Pending Changes** window is displayed.

2. Select one of the following options:

Option	Description
<b>Cancel</b>	Do not deploy the changes now. Retain the undeployed configuration changes. The appliance user interface returns to the previous panel.
<b>Roll Back</b>	Abandon configuration changes. A message is displayed, stating that the pending changes were reverted. The appliance user interface returns to the previous panel.
<b>Deploy</b>	Deploy all configuration changes. When you select <b>Deploy</b> , a system message is displayed, stating that the changes were deployed. If any of the changes require the runtime server to be restarted, the restart occurs automatically when you select <b>Deploy</b> . The runtime server will then be unavailable for a period of time until the restart completes.



---

# Index

## A

audit  
    events [1](#)  
audit configuration event [19](#)  
audit configuration management  
    elements for [19](#)  
audit events  
    common elements [1](#)

## C

common elements  
    audit events [1](#)  
configuration management  
    elements for [23](#)

## D

deploying changes [51](#)

## E

encryption  
    elements [11](#)  
encryption event [11](#)  
events  
    audit configuration [19](#)  
    encryption [11](#)  
    IBM\_SECURITY\_ENCRYPTION [11](#)  
    IBM\_SECURITY\_FEDERATION [13](#)  
    IBM\_SECURITY\_MGMT\_AUDIT [19](#)  
    IBM\_SECURITY\_MGMT\_POLICY [23](#)  
    IBM\_SECURITY\_RUNTIME [43, 45](#)  
    IBM\_SECURITY\_TRUST [47](#)  
    management [23](#)

## F

federation events  
    name identifier management [13](#)

## I

IBM\_SECURITY\_AUTHN events [5](#)  
IBM\_SECURITY\_ENCRYPTION event  
    description [11](#)  
IBM\_SECURITY\_FEDERATION event  
    description [13](#)  
IBM\_SECURITY\_MGMT\_AUDIT event  
    description [19](#)  
IBM\_SECURITY\_MGMT\_POLICY event  
    description [23](#)  
IBM\_SECURITY\_RUNTIME  
    description [43, 45](#)  
IBM\_SECURITY\_TRUST

IBM\_SECURITY\_TRUST (*continued*)  
    description [47](#)

## N

name identifier management  
    elements [13](#)

## P

pending changes [51](#)

## S

security runtime  
    events [43, 45](#)  
security trust  
    events [47](#)





