

IBM Security Access Manager for Mobile
Version 8.0.0.1

Auditing Guide



IBM Security Access Manager for Mobile
Version 8.0.0.1

Auditing Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 33.

Edition notice

Note: This edition applies to version 8.0.0.1 of IBM Security Access Manager for Mobile (product number 5725-L52) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2013.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures v

Tables vii

About this publication ix

Access to publications and terminology ix

Accessibility x

Technical training. x

Support information. x

Statement of Good Security Practices x

Chapter 1. Configuring auditing 1

**Chapter 2. IBM Security Access Manager
for Mobile auditing events 5**

**Chapter 3. Elements for
IBM_SECURITY_TRUST events. 9**

**Chapter 4. Elements for
IBM_SECURITY_RUNTIME events 13**

**Chapter 5. Elements for
IBM_SECURITY_CBA_AUDIT_MGMT
events 15**

**Chapter 6. Elements for
IBM_SECURITY_CBA_AUDIT_RTE
events 21**

**Chapter 7. Elements for
IBM_SECURITY_RTSS_AUDIT_AUTHZ
events 25**

Chapter 8. Deploying pending changes 31

Notices 33

Index 37

Figures

Tables

1. Syslog server remote machine configuration values.	1	8. Elements for an IBM_SECURITY_RUNTIME event.	13
2. Audit tuning values	2	9. Elements used in IBM_SECURITY_CBA_AUDIT_MGMT events	15
3. Attributes and elements of the ContextDataElements element.	5	10. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events	21
4. Attributes for the SourceComponentId element	6	11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events	25
5. Attributes for the Situation element	7		
6. Attributes for the Outcome element	7		
7. Elements for an IBM_SECURITY_TRUST event	9		

About this publication

The *IBM Security Access Manager for Mobile Auditing Guide* explains how to configure auditing for IBM Security Access Manager for Mobile. The guide also provides descriptions of the events that can be audited.

Access to publications and terminology

This section provides:

- A list of publications in the “IBM Security Access Manager for Mobile library.”
- Links to “Online publications.”
- A link to the “IBM Terminology website.”

IBM Security Access Manager for Mobile library

The following documents are available online in the IBM Security Access Manager for Mobile library:

- *IBM Security Access Manager for Mobile Configuration Guide*, SC27-6205-00
- *IBM Security Access Manager for Mobile Administration Guide*, SC27-6207-00
- *IBM Security Access Manager Appliance Administration Guide*, SC27-6206-00
- *IBM Security Access Manager for Mobile Auditing Guide*, SC27-6208-00
- *IBM Security Access Manager for Mobile Troubleshooting Guide*, GC27-6209-00
- *IBM Security Access Manager for Mobile Error Message Reference*, GC27-6210-00

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security IBM Security Access Manager for Mobile library

The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central

IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center

The IBM Publications Center site (<http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss>) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. You can use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the IBM Accessibility website at <http://www.ibm.com/able/>.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

IBM Security Access Manager for Mobile Troubleshooting Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Configuring auditing

Use the Audit Configuration feature to enable logging of audit events.

Before you begin

Depending on the required audit configuration, you might need the following information to complete the auditing configuration:

- If you plan to use a syslog server on a remote machine, ensure that you have the information of the location of the syslog server.
- If you plan to use a TLS type protocol, ensure that the server certificate was imported into the chosen certificate database.
- If you plan to use client certificate to authenticate to the syslog server, ensure that the certificate is trusted by the syslog server. The certificate must be imported into the chosen certificate database.

About this task

IBM® Security Access Manager for Mobile provides the capability of collecting and processing system log (syslog) messages. Enable the feature by completing the steps in the audit configuration page to use a common auditing configuration that is used by all runtime components.

Procedure

1. From the top menu, select **Monitor Analysis and Diagnostics > Logs > Audit Configuration**.
2. Select **Enable audit log**.
3. Specify the location of the syslog server.

On this appliance

Audit events are sent to a syslog server on this appliance. If you select the local syslog server, no additional mandatory configuration is needed. If you want to tune the default configuration settings, proceed to step 5 on page 2.

Note: If you configure auditing to use a local syslog server, see the topic "Viewing application log files" in the *IBM Security Access Manager Appliance Administration Guide*, to view the audit logs.

On a remote machine

Audit events are sent to a syslog server on a remote machine. If you select a syslog server on a remote machine, you might need to specify some or all of the following information:

Table 1. Syslog server remote machine configuration values..

Field	Default Values	Description
Host	None	Specifies the host name of the syslog server.
Port	514	Specifies the port of the syslog server.

Table 1. Syslog server remote machine configuration values. (continued).

Field	Default Values	Description
Protocol	UDP Note: Though UDP is the default value, use TLS. TLS is the preferred protocol for production environments.	Specifies the type of transport protocol to use to transmit syslog messages.
Certificate database (truststore)	None	Specifies the truststore to use to validate the certificate of the syslog server. This field is enabled only when the transport layer protocol type selected is TLS.
Enable client certificate authentication	Disabled	If enabled, the client is able to do client certificate authentication during the SSL handshake upon server request.
Certificate database (keystore)	None	Specifies the keystore to use for client certificate authentication. This field is enabled only when the enable client certificate authentication is selected.
Certificate label	None	Specifies the personal certificate to use for client certificate authentication. This field is enabled only when the enable client certificate authentication is selected.
Enable disk failover	Disabled	If enabled, audit events are logged to a local disk file when an error occurs during the SSL connection to the remote syslog server. Note: If you enable disk failover the audit events are logged to local disk files that follow the naming pattern ISAMAudit0.log.nn , where nn is a number that uniquely identifies a local disk file. The local disk file can be viewed at the same location as the local syslog server audit logs.

4. If you choose to use default values for tuning, you can complete the configuration by clicking **Save**. Otherwise, proceed with the subsequent steps. If you want to discard the changes you made, click **Refresh**.
5. Optional: Click **Tuning**. Provide the following information:

Table 2. Audit tuning values.

Field	Default Value	Description
Event Queue Size	1000	Specifies the maximum number of audit events that the event queue can hold. Syslog messages are queued in the memory before they are sent to the syslog server.

Table 2. Audit tuning values (continued).

Field	Default Value	Description
Queue Full Timeout (seconds)	-1	Specifies the number of seconds to wait before an incoming event is discarded when the queue is full. A value of 0 indicates that new events are discarded immediately if the queue is full. A value of -1 indicates that new events wait perpetually for the queue to have a vacancy.
Sender Threads	1	Specifies the number of sender threads, which drain the audit events from the queue to send to the syslog server.
Error Retry Count	2	Specifies the number of times the syslog client tries to establish a connection with the server again if it fails in the first attempt.

6. Click **Save**. Otherwise, click **Refresh** to discard the changes you made.

Results

Notes:

- Audit events that are generated by IBM Security Access Manager for Mobile vary in size. Some events can exceed default sizes of some remote syslog server implementations. Ensure that remote syslog servers are configured to handle large events. Consider configuring the servers to accept audit records up to 6 kB in size. Truncation of audit events by the servers may occur if the limits are not sufficiently increased.
- When you choose a protocol, use TLS. TLS is the preferred protocol for production environments.

You can enable the inclusion of additional data in audit events. Such events are called verbose events.

1. Log in to the local management interface.
2. Click **Secure Mobile Settings**.
3. Under **Manage**, click **Advanced Configuration**.
4. Find the `audit.verboseEvents.enabled` property.
5. Click the edit button.
6. Select the **Enabled** box.

Note: The `audit.verboseEvents.enabled` property defaults to **false**.

7. Click **Save**.

Note: The administrator must refresh the auditing cache to fully enable the `audit.verboseEvents.enabled` property. To refresh the auditing cache, complete the following steps:

- a. Click **Manage System Settings**.
- b. Under **System Settings**, click **Restart or Shut down**.
- c. Click **Restart**.
- d. Click **Yes** when you are asked if you want to restart the appliance.
- e. Log back in to the local management interface after the appliance restarts.

What to do next

Deploy the configuration settings.

Related tasks:

Chapter 8, “Deploying pending changes,” on page 31

Some configuration and administration changes require an extra deployment step.

Chapter 2. IBM Security Access Manager for Mobile auditing events

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

Security Access Manager for Mobile supports the following auditing events:

- IBM_SECURITY_TRUST
- IBM_SECURITY_RUNTIME
- IBM_SECURITY_CBA_AUDIT_MGMT
- IBM_SECURITY_CBA_AUDIT_RTE
- IBM_SECURITY_RTSS_AUDIT_AUTHZ

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.

Table 3. Attributes and elements of the ContextDataElements element

Attribute	Value
name	Security Event Factory The XPath is: CommonBaseEvent/contextDataElements/@name
type	eventTrailId The XPath is: CommonBaseEvent/contextDataElements/@type
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: CommonBaseEvent/contextDataElements/[@type='eventTrailId']/contextId

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 4. Attributes for the SourceComponentId element

Attribute	Value
application	ITFIM#8.0.0 The XPath is: CommonBaseEvent/sourceComponentId/ @application
component	The XPath is: CommonBaseEvent/sourceComponentId/ @component
componentIdType	ProductName The XPath is: CommonBaseEvent/sourceComponentId/ @componentIdType
componentType	http://www.ibm.com/namespaces/autonomic/ Tivoli_componentTypes The XPath is: CommonBaseEvent/sourceComponentId/ @componentType
executionEnvironment	<OS name>#<OS Architecture>#<OS.version> The XPath is: CommonBaseEvent/sourceComponentId/ @executionEnvironment
location	<hostname> The XPath is: CommonBaseEvent/extendedDataElements [@name='registryInfo']/children [@name='location']/values

Table 4. Attributes for the SourceComponentId element (continued)

Attribute	Value
locationType	FQHostname The XPath is: CommonBaseEvent/sourceComponentId/ @locationType
subComponent	<classname> The XPath is: CommonBaseEvent/sourceComponentId/ @subComponent

Situation element

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

Table 5. Attributes for the Situation element

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

Outcome element

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

Table 6. Attributes for the Outcome element

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

Table 6. Attributes for the Outcome element (continued)

Attribute	Value
result	The XPath is: CommonBaseEvent/extendedDataElements [@name='outcome']/children [@name='result']/values

Note: Security Access Manager for Mobile does not use the **ReporterComponentId** field.

Chapter 3. Elements for 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.

Table 7. Elements for an IBM_SECURITY_TRUST event

Element	Description
accessDecision	For the authorization module, it is the result of the authorization decision. This element is filled out only when the action is authorized. The XPath is: CommonBaseEvent/extendedDataElements [@name='accessDecision']/values
action	The action being performed. Possible actions are: • authorize • issue • map • validate The XPath is: CommonBaseEvent/extendedDataElements [@name='action']/values
appliesTo	The destination or resource that the request or token applies to. The XPath is: CommonBaseEvent/extendedDataElements [@name='appliesTo']/values
issuer	The party responsible for issuing the token. The XPath is: CommonBaseEvent/extendedDataElements [@name='issuer']/values
moduleName	The module in the STS module chain that the action is taken on. The XPath is: CommonBaseEvent/extendedDataElements [@name='moduleName']/values
ruleName	The rule name used for the mapping module. This element is filled out only when specified action is set to <i>map</i>. The XPath is: CommonBaseEvent/extendedDataElements [@name='ruleName']/values

Table 7. Elements for an IBM_SECURITY_TRUST event (continued)

Element	Description
token	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. The XPath is: CommonBaseEvent/extendedDataElements [@name='token']/values
tokenInfo	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. The XPath is: CommonBaseEvent/extendedDataElements [@name='tokenInfo']/values
tokenType	The type of token the module is using. The XPath is: CommonBaseEvent/extendedDataElements [@name='tokenType']/values

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>
  <extendedDataElements name="outcome" type="noValue">
    <children name="result" type="string">
      <values>SUCCESSFUL</values>
    </children>
  </extendedDataElements>
</CommonBaseEvent>
```

```

</children>
<children name="majorStatus" type="int">
  <values>0</values>
</children>
</extendedDataElements>
<sourceComponentId application="ITFIM#8.0.0"
component="IBM Tivoli Federated Identity Manager"
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 4. Elements for IBM_SECURITY_RUNTIME events

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.

Table 8. Elements for 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="2013-07-19T06:20:18.361Z"
extensionName="IBM_SECURITY_RUNTIME"
globalInstanceId="FIMf5960a71013f15479e82b66d4d925"
sequenceNumber="0"
version="1.1">
  <contextDataElements name="Security Event Factory"
type="eventTrailId">
    <contextId>FIM_f5960938013f1eba8b40b66d4d92542a+1655973824</contextId>
  </contextDataElements>
  <extendedDataElements name="Domain" type="string">
    <values>Not Available</values>
  </extendedDataElements>
  <extendedDataElements name="IsMgmtAudit" type="boolean">
    <values>>false</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>application</values>
  </children>
  <children name="uniqueId" type="long">
    <values>0</values>
  </children>
</extendedDataElements>
<extendedDataElements name="action" type="string">
  <values>auditStart</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="ITFIM#8.0.0"
component="IBM Tivoli Federated Identity Manager"
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.audit.event.impl.RuntimeAuditAdapterImpl"
threadId="Start Level Event Dispatcher"
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. Elements for IBM_SECURITY_CBA_AUDIT_MGMT events

This event type identifies the security context-based management events, such as the creation of risk profiles.

The following table lists the elements that can be displayed in the output of a IBM_SECURITY_CBA_AUDIT_MGMT event. All elements are included in the output, unless indicated otherwise.

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_MGMT events

Element	Description
creationTime	Specifies the date and time when the event was issued. For example: 2013-09-11T19:18:04.140Z The letter Z in the sample that is shown indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
actionInfo	Provides information about the management action that is performed on a resource. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.

Table 9. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element	Description
action-id	Specifies the action that caused this management event. Possible actions include: ATTRIBUTE_CREATE_EVENT, ATTRIBUTE_DELETE_EVENT, ATTRIBUTE_SEARCH_EVENT, ATTRIBUTE_UPDATE_EVENT, ATTRIBUTE_MATCHER_CREATE_EVENT, ATTRIBUTE_MATCHER_DELETE_EVENT, ATTRIBUTE_MATCHER_SEARCH_EVENT, ATTRIBUTE_MATCHER_UPDATE_EVENT, AUTHENTICATION_RULE_CREATE_EVENT, AUTHENTICATION_RULE_DELETE_EVENT, AUTHENTICATION_RULE_IMPORT_EVENT, AUTHENTICATION_RULE_SEARCH_EVENT, AUTHENTICATION_RULE_UPDATE_EVENT, DEVICE_DELETE_EVENT, DEVICE_SEARCH_EVENT, DEVICES_FOR_USER_SEARCH_EVENT, DEVICE_USER_ID_SEARCH_EVENT, GEOLOCATION_DATA_CANCEL_IMPORT_EVENT, GEOLOCATION_DATA_IMPORT_EVENT, GEOLOCATION_DATA_STATUS_IMPORT_EVENT, HVDB_DELETE_ALL_DATA_EVENT, HVDB_DELETE_USER_DATA_EVENT , MAPPING_RULE_EXPORT_EVENT, MAPPING_RULE_IMPORT_EVENT , MAPPING_RULE_SEARCH_EVENT, MAPPING_RULE_UPDATE_EVENT, _CREATE_EVENT, OBLIGATION_DELETE_EVENT, OBLIGATION_SEARCH_EVENT, OBLIGATION_UPDATE_EVENT, OVERRIDE_CONFIG_SEARCH_EVENT, OVERRIDE_CONFIG_UPDATE_EVENT, PIP_INSTANCE_CREATE_EVENT, PIP_INSTANCE_UPDATE_EVENT, PIP_INSTANCE_DELETE_EVENT, PIP_INSTANCE_SEARCH_EVENT, PIP_TYPE_CREATE_EVENT, PIP_TYPE_UPDATE_EVENT, PIP_TYPE_DELETE_EVENT, PIP_TYPE_SEARCH_EVENT, POLICY_ATTACHMENT_CREATE_EVENT, POLICY_ATTACHMENT_DELETE_EVENT, POLICY_ATTACHMENT_PDADMIN_EVENT, POLICY_ATTACHMENT_POLICIES_SEARCH_EVENT, POLICY_ATTACHMENT_POLICIES_UPDATE_EVENT, POLICY_ATTACHMENT_PUBLISH_EVENT, POLICY_ATTACHMENT_SEARCH_EVENT, POLICY_ATTACHMENT_UNPUBLISH_EVENT, POLICY_ATTACHMENT_UPDATE_EVENT, POLICY_ATTACHMENT_UPDATE_PROPERTIES_EVENT, POLICY_CREATE_EVENT POLICY_DELETE_EVENT, POLICY_SEARCH_EVENT, POLICY_UPDATE_EVENT, POLICY_SET_CREATE_EVENT, POLICY_SET_DELETE_EVENT, POLICY_SET_POLICIES_SEARCH_EVENT, POLICY_SET_POLICIES_UPDATE_EVENT, POLICY_SET_SEARCH_EVENT, POLICY_SET_UPDATE_EVENT, RISK_PROFILE_CREATE_EVENT, RISK_PROFILE_DELETE_EVENT, RISK_PROFILE_SEARCH_EVENT, RISK_PROFILE_UPDATE_EVENT, RUNTIME_POLICY_DEPLOY_EVENT, RUNTIME_POLICY_IS_DEPLOYED_EVENT, RUNTIME_POLICY_SEARCH_EVENT, RUNTIME_POLICY_UNDEPLOY_EVENT. XPath: CommonBaseEvent/extendedDataElements /[@name= 'actionInfo']/children[@name='urn:oasis:names:tc:xacml:1.0:action:action-id']/values

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_MGMT events (continued)

Element		Description
outcome		Specifies the outcome of the action for which the security event is generated. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type
	failureReason	Provides more information about the outcome. This element is included in the output when the result is FAILURE. XPath: CommonBaseEvent/extendedDataElements /[@name='outcome']/children[@name='failureReason']/values
	result	Specifies the overall status of the event that is commonly used for filtering. The following values are possible for the status of this element: - FAILURE - SUCCESSFUL XPath: CommonBaseEvent/extendedDataElements /[@name='outcome']/children[@name='result']/values
userInfoList		Provides information about the user who accesses the resource. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
	appUserName	Specifies the name of the user. XPath: CommonBaseEvent/extendedDataElements /[@name='userInfoList']/children[@name='appUserName']/values
resourceInfo		Provides information about the resource that is accessed. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
	RESTInvocationURI	Specifies the URI of the REST interface that is accessed for this management event. XPath: CommonBaseEvent/extendedDataElements /[@name='resourceInfo']/children[@name='RESTInvocationURI']/values

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_MGMT events (continued)

Element		Description
	nameOfPolicy	Specifies the policies and policy sets that are associated with the policy attachment for the resource as specified by the nameOfResource property. This element is included in the output for policy attachment action-ids. XPath: CommonBaseEvent/extendedDataElements /[@name='resourceInfo']/children[@name='nameOfPolicy']/values
	nameOfResource	Specifies the name of the resource for a policy attachment. For example: /WebSEAL/security-default/index.html This element is included in the output for policy attachment action-ids. XPath: CommonBaseEvent/extendedDataElements /[@name='resourceInfo']/children[@name='nameOfResource']/values
restManagement		Provides optional information regarding the input JSON for this management request. This element is included in the output for some management audit events. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
	json	JSON for this management request. This element is included in the output for some management audit events. Note: To enable the inclusion of additional data in an audit event, the administrator must enable the audit.verboseEvents.enabled property, which sets the property to true. XPath: CommonBaseEvent/extendedDataElements /[@name='restManagement']/children[@name='json']/values
extensionName		Specifies the name of the event class that this event represents. The name indicates any additional elements that are expected to be present within the event. The value for context-based authorization management events is <i>IBM_SECURITY_CBA_AUDIT_MGMT</i>. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_MGMT events (continued)

Element		Description
globalInstanceId		Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example: f0c93637-ada2-4afb-9687-47a7ec1fa3a7 This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
msg		Specifies more information when the outcome is SUCCESSFUL. This element: • Is optional. • Is a container element. • Does not have a valid XPath. A valid XPath requires a values declaration. • Uses the children of the ComponentIdentification element type.
reporterComponentId		This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
	application	Specifies the name of the application that reports the event. For context-based authorization events, the value is set to <i>IBM Security Context-Based Authorization</i>.
	component	Specifies the logical identity of a component. For context-based authorization events, the value is set to <i>Context-Based Authorization</i>.
	componentIdType	Specifies the format and meaning of the component that is identified by this component identification. For example: <i>ProductName</i>
	location	Specifies the physical address that corresponds to the location of a component. For example: <i>host name, IP address, or MAC address</i>.
	locationType	Specifies the format and meaning of the value in the location property. For context-based authorization events, the value is set to <i>FQHostname</i>.
sourceComponentId		Identifies the component that is affected or was impacted by the event. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.

Table 9. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element		Description
	component	Specifies the logical identity of a component.
	componentIdType	Specifies the format and meaning of the component that is identified by this component identification. For example: <i>ProductName</i>
	location	Specifies the physical address that corresponds to the location of a component. For example: <i>host name, IP address, or MAC address.</i>
	locationType	Specifies the format and meaning of the value in the location property. For context-based authorization events, the value is set to <i>FQHostname</i> .

Related tasks:

Configuring auditing

Use the Audit Configuration feature to enable logging of audit events.

Chapter 6. Elements for IBM_SECURITY_CBA_AUDIT_RTE events

This event type identifies the security context-based authorization events, such as device registration.

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

Table 10. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events

Element		Description
creationTime		Specifies the date and time when the event was issued. For example: 2013-09-11T19:18:04.140Z The letter Z in the sample that is shown indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
actionInfo		Provides information about the management action that is performed on a resource. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
	action-id	Specifies the action that caused this event. Possible actions include: • CALCULATE_RISK_SCORE_EVENT • DEVICE_DELETION_EVENT • DEVICE_REGISTRATION_EVENT XPath: CommonBaseEvent/extendedDataElements /[@name= ' actionInfo']/children[@name=' urn:oasis:names:tc:xacml:1.0:action:action-id']/values
outcome		Specifies the outcome of the action for which the security event is generated. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type

Table 10. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events (continued)

Element	Description
failureReason	Provides additional information about the outcome. Included in the output when the result is FAILURE. XPath: CommonBaseEvent/extendedDataElements /[@name='outcome']/children[@name='failureReason']/values
result	Specifies the overall status of the event that is commonly used for filtering. The following values are possible for the status: - FAILURE - SUCCESSFUL XPath: CommonBaseEvent/extendedDataElements /[@name='outcome']/children[@name='result']/values
userInfoList	Provides information about the user who accesses the resource. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
appUserName	Specifies the name of the user. XPath: CommonBaseEvent/extendedDataElements /[@name='userInfoList']/children[@name='appUserName']/values
extensionName	Specifies the name of the event class that this event represents. The name indicates any additional elements that are expected to be present within the event. The value for context-based authorization runtime events is <i>IBM_SECURITY_CBA_AUDIT_RTE</i>. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
globalInstanceId	Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example: f0c93637-ada2-4afb-9687-47a7ec1fa3a7 This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.

Table 10. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events (continued)

Element	Description
msg	Specifies additional information when the outcome is SUCCESSFUL. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.

Chapter 7. Elements for IBM_SECURITY_RTSS_AUDIT_AUTHZ events

This event type identifies the authorization decision events for runtime security services.

Runtime security services generates an authorization decision event record if both of the following conditions occur:

- The runtime security services component is asked for an access decision
- Auditing is enabled

In addition to the base Common Base Event content, runtime security services authorization decision records contain authorization-specific properties. These authorization-specific properties are defined in the Common Base Event Extensions for Security Events specification with the ExtendedDataElement.

The following table lists the event properties that are included in the output of an IBM_SECURITY_RTSS_AUDIT_AUTHZ event record. All elements are included in the output, unless indicated otherwise.

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events

Element	Description and values
accessDecision	Present when the result is SUCCESSFUL This property specifies the decision of the authorization call. Possible element values include: • Permit • Deny • NotApplicable • Indeterminate If a Permit decision is returned with obligations, then a ConditionalPermit decision is recorded in the event.
accessDecisionReason	Present when accessDecision is DENY This property provides more information about the denial of the access decision.
action	Not always in output. This property specifies the action that caused the authorization event.
outcome	Specifies the outcome of the action for which the security event is being generated. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the outcomeType element type.
failureReason	Not always in output. This property provides more information about the outcome.

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
majorStatus	Specifies the major status code.
minorStatus	Not always in output. This property specifies the minor status code.
result	Specifies the overall status of the event. This element is also used for filtering. Element values are UNSUCCESSFUL if an error condition occurs that prevents standard processing. Element values are SUCCESSFUL when the error condition starts standard processing.
permissionInfo	Provides information about access permissions. This ExtendedDataElement element has no value declaration. This container element uses the children of the PermissionInfoType element type.
checked	Specifies permissions that are checked during the authorization call.
denied	Not always in output. This property specifies the permissions that are denied among the permissions that are requested.
granted	Not always in output. This property specifies permissions that are granted.
policyInfo	Not always in output. This property provides information about policies that are attached to the resource or the container of a resource. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the PolicyInfoType element type.
attributes	Not always in output. This property specifies attributes that are associated with a policy.
description	Not always in output. This property provides a description of the policy.
name	Not always in output. This property specifies the name of the policy.
type	Not always in output. This property specifies the type of the policy.

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
registryInfo	Not always in output. This property provides information about the registry that is involved in the authentication. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the RegistryInfoType element type.
serverLocation	Not always in output. This property specifies where the registry server is located.
resourceInfo	Provides information about the resource that is accessed. This ExtendedDataElement element has no a value declaration. This container element uses the children of the resourceInfoType element type.
attributes	Specifies the attributes for the resource.
nameInApp	Not always in output. This property specifies the name of the resource in the context of the application.
nameInPolicy	Specifies the name of the resource when it applies a policy to the resource.
type	Specifies the type of the resource.
userInfo	Provides information about each user in the delegation chain. This ExtendedDataElement element has no a value declaration. This container element uses the children of the UserInfoType element type.
appUserName	Present when the accessing subject is authenticated. This property specifies the name of a user within an application.
attributes	Not always in output. This property provides more user information.
callerList	Not always in output. This property specifies a list of names that represents the identities of a user.
location	Not always in output. This property specifies the location of the user.
locationType	Not always in output. This property specifies the type of location.
realm	Not always in output. This property specifies the registry partition to which the user belongs.

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
registryUserName	Not always in output. This property specifies the name of the user in the registry.
sessionId	Not always in output. This property specifies the ID for the session that belongs to the user.
uniqueId	Not always in output. This property specifies the unique identifier that belongs to the user within an application.
creationTime	Specifies the date and time when the event was issued. For example: 2008-09-11T19:18:04.140Z The letter Z in the example indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time.
contextDataElement	Specifies the ContextDataElement type, which defines the contexts that each event references. This element contains data that assists with problem diagnostic procedures by correlating messages or events that are generated during the execution of a unit of work.
type	Specifies the data type of the contextValue property.
name	Specifies the name of the application that created the contextDataElement.
contextValue	Specifies the value of the context regarding the implementation of the context.
extensionName	Specifies the name of the event class that the extensionName event represents. The extensionName event indicates more elements that are expected to be present within the event. The value for runtime security services is the following value: IBM_SECURITY_RTSS_AUDIT_AUTHZ
globalInstanceId	Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example:f5e6bcc5-d1e8-4638-8f84-3ba29ca950b2

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
msg	Provides the text that accompanies the event. This element is typically the resolved message string in human readable format that is rendered for a specific locale. The following example uses runtime security services data: Subject cn=wasadmin,c=us requests access to the http://localhost:9081/rtss/test/jaxws/echo/EchoService protected resource.
situation	Specifies the situation that caused the event to be reported.
categoryName	Specifies the category type of the situation that caused the event to be reported.
situationType	Specifies the type of situation that caused the event to be reported.
reportCategory	Specifies the category of the reported situation. This element is used if the value that belongs to the element is STATUS.
reasoningScope	Defines whether this situation has either of the following impacts: • Internal-only impact. • Potential external impact. This element is used if the element value is either of the following values: • INTERNAL • EXTERNAL
sourceComponentId	Identifies the component that is impacted by the event. This element has no a value declaration. This container element uses the children of the ComponentIdType element type.
application	Specifies the name of the application. The value that belongs to this element is the following: IBM runtime security services
component	Specifies the logical identity of a component.
componentIdType	Specifies the format of the component and meaning of the component that is identified by this componentIdentification. For example: ProductName
componentType	Specifies a well-defined name that is used to characterize all of the instances that belong to this component.
location	Specifies the physical address that corresponds to the location of a component. For example: Host name, IP address, or MAC address.

Table 11. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
locationType	Present if available. This property specifies the format and meaning of the value in the location property. For runtime security services, the value is set to Not available if the meaning of the location element value is not determined. The following is sample runtime security services data: ipAddress.
processId	Not always in output. This property identifies the process ID of the running component or subcomponent that generated the event.
subComponent	Not always in output. This property specifies a further distinction for the logical component property of the event.
version	Specifies a string that identifies the version of the event. The element value is 2.0.

Chapter 8. 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
Cancel	Do not deploy the changes now. Retain the undeployed configuration changes. The appliance user interface returns to the previous panel.
Roll Back	Abandon configuration changes. A message is displayed, stating that the pending changes were reverted. The appliance user interface returns to the previous panel.
Deploy	Deploy all configuration changes. When you select Deploy , 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 Deploy . The runtime server will then be unavailable for a period of time until the restart completes.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing, or distributing application programs that conform to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: <http://www.ibm.com/legal/copytrade.shtml>

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

A

- accessibility x
- audit
 - events 5
 - log 1
- audit events
 - common elements 5
 - IBM_SECURITY_CBA_AUDIT_RTE
 - events 21
- authorization events
 - IBM_SECURITY_CBA_AUDIT_RTE
 - events 21

C

- common elements
 - audit events 5
- configuration
 - audit 1

D

- deploying changes 31

E

- education x
- events
 - IBM_SECURITY_CBA_AUDIT_RTE
 - events 21
 - IBM_SECURITY_RUNTIME 13
 - IBM_SECURITY_TRUST 9

I

- IBM
 - Software Support x
 - Support Assistant x
- IBM_SECURITY_CBA_AUDIT_MGMT
 - events 15
- IBM_SECURITY_CBA_AUDIT_RTE
 - events 21
- IBM_SECURITY_RTSS_AUDIT_AUTHZ
 - events 25
- IBM_SECURITY_RUNTIME
 - description 13
- IBM_SECURITY_TRUST
 - description 9

N

- notices 33

O

- online
 - publications ix
 - terminology ix

P

- pending changes 31
- problem-determination x
- publications
 - accessing online ix
 - list of for this product ix

S

- security runtime
 - events 13
- security trust
 - events 9

T

- terminology ix
- training x
- troubleshooting x



Product Number: 5725-L52

Printed in USA

SC27-6208-01

