HP Select Audit Software

for the Windows®, HP-UX®, Solaris® and Linux® operating system

Software Version: 1.02

Select Audit Database Schema Guide

Document Release Date: July 2007
Software Release Date: July 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

HP provides third-party products, software, and services that are not HP Branded “AS IS” without warranties or representations of any kind from HP, although the original manufacturers or third party suppliers of such products, software and services may provide their own warranties, representations or conditions. By using this software you accept the terms and conditions.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

HP Select Audit includes software developed by third parties. The software HP Select Audit uses includes:

- ANTLR Copyright 2005 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- Install Anywhere, Copyright 2004 Zero G Software, Inc.
- Jasper Decisions Copyright 2000-2006 JasperSoft Corporation.
- JavaScript Tree, Copyright 2002-2003 Geir Landro.
- Legion of the Bouncy Castle developed by Bouncy Castle.
- log4J from the Apache Software Foundation.
- Microsoft SQL Server 2005 JDBC Driver
- OpenAdaptor from the Software Conservancy.
- Oracle JDBC Thin Driver
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.

Please check the `<install_dir>/3rd_party_license` folder for expanded copyright notices from such third party suppliers.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To find more information about HP Passport, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Select Audit Database Schema

This guide describes the HP Select Audit software database schema and views.

Tables Overview

The Select Audit database schema is made up of system tables and application-specific Fact tables. The Fact tables are used to store the data that is sent to Select Audit in log files. The system tables are used by Select Audit to store information about how to behave; which applications it knows about, how to parse the input data, signatures and verification data, and so on.

Messages types are sorted by the following:

- **Application:** The application logging the message (Select Audit, Select Identity).
- **Component:** The module within the larger application that has produced the message (Select Audit Config, Select Access Validator).
- **EventType:** The event being logged in the message (Log in, User Role Add).

For each EventType, the message is parsed in a specific way to extract the relevant data into Fact tables. This process is done through the application of a series of XPATH expressions to match the relevant data.

All tables are organized in a tree structure, with each entry containing a unique ID, and a reference to the ID entry in the parent table. For example, an entry in the Component table has a component ID and an application ID that associates the component with a given application. Each application has one or more components.

System Tables

The system tables create a gateway for incoming messages, sorting them into their respective Fact tables. The first set of tables contain XPATH expressions that define how to recognize certain message types, and how to parse the data in each type.

The Select Audit system tables are listed below:

- Application
- Component
- EventTypes
- ComponentEventTypes
- EventSummaryExp

The data in these tables does not change and is for internal Select Audit use only.

The Application table stores information about the applications from which Select Audit is configured to handle audit messages (Select Access, Select Identity, and so on). The Component table defines each module of an application. If you are only looking for messages from the Select Access Validator, you can filter by component. EventTypes list all defined events, including events that are common to all applications, such as Log in, and those that are only be used by a single application (for example, Validator LDAP Message). These EventTypes are shown alongside messages in reports.

Fact Tables

Fact tables are used to store the data that is logged from client applications in a normalized and easy to access way. There are two sets of Fact tables:

- common Fact tables
- application-specific Fact tables

The data types in the following tables are Oracle specific. In an SQL Server environment, the relevant SQL Server specific data types would apply.

Common Fact Tables

The common Fact tables are the Batch table, the Batch_Props table, and the AuditEvent table.

Batch Table

All batches, regardless of the application, are inserted into the Batch table on arrival. This table stores the raw XML messages without performing any parsing. It writes the raw XML in `gzip` compressed form into the Content column as a `BLOB`. The Batch table also stores various other details, such as the arrival time. When messages arrive at the Audit Server, they are automatically inserted into the Batch table.

Table 1 Batch Table

Column Name	Type	Sample Value	Description
ID	Integer	`96`	Sequential unique ID for this batch.
Arrival Time	Varchar2(24)	`2006-09-29 10:51:59`	Timestamp of when batch received by the Audit Server.
PrincipalName	Varchar2(255)	`Admin`	The user that authenticated the batch. This is set by the connector.
Content	BLOB	`<?xml …`	The compressed raw XML batch of multiple messages to be processed.
DigestUnique	Raw(64)	`3DDECB33E8583 ED5167416341C 2BEED428A2892 100D125A21A6D 951D8ADD09F2`	Used to ensure each batch is unique.

Table 1 Batch Table (cont'd)

Column Name	Type	Sample Value	Description
DigestMultiple	Raw(64)		Used to detect duplicate batches.
SignatureId	Integer	97	Link to signature of this batch. This column is present in every Fact table and will not be described each time.
ProcessFlag	Integer	2	Status of batch processing: 0 = not yet processed 1 = currently processing 2 = processing successful 3 = error occurred in processing
ActionTime	Varchar2(24)	2006-09-29 10:52:15	Timestamp of when processing begins on the batch.
ProcessTime	Integer	183202	The time in milliseconds taken to normalize the batch.

Batch_Props Table

Each batch has a number of properties associated with it, including where the batch came from, authentication type, and connector version. These are stored in the Batch_Props table.

Table 2 Batch_Props Table

Column Name	Type	Sample Value	Description
ID	Integer	2	The batch ID of the batch being described.
Name	Varchar(255)	remoteHost	The name of a property of the batch.
Value	Varchar(255)	auditconnector.can.hp.com	The value of the property.

AuditEvent Table

From the Batch table, batches are separated into messages and parsed into their corresponding Fact tables. For every message, regardless of application, an entry is created in the AuditEvent table. The AuditEvent table stores standard fields such as user name and target, but the way that these fields are extracted from the given message depends on which component EventType the message is. For example, in a Select Access admin message, the user would be the value in the <administrator> element, but in a Select Access workflow

message, the user is taken from the <user> element of the message. If the message cannot be recognized as any known EventType, the componenteventtypeid is set to -1, and the entire message is stored in the Message column.

Table 3 AuditEvent Table

Column Name	Type	Sample Value	Description
ID	Number	13	The unique ID of this message event.
BatchID	Number	7	The ID of the batch entry in the parent Batch table.
SignatureID	Number	5	As described in the Batch table.
ChainID	Number	2	Used for data verification.
Component EventTypeID	Number	93	The EventType matching this message. Corresponds with an entry in the ComponentEventTypes table.
BatchIndex	Number	4	The index of this message within the batch of messages.
ClientID	Varchar2(256)	SPEventPlugin	The client ID of the connector that sent this message.
Time_Stamp	Varchar2(24)	2006-09-29 10:52:15	The client time as logged by the connector.
UserName	Varchar2(512)	_System_	The user triggering the action to happen. It can be a user name, machine name, IP address, _System_, and so on.
Target	Varchar2(2048)	shrike.can.hp.com	The target of the event. It can be another user, a resource, a machine, and so on.
Message	CLOB	connection established to shrike.can.hp.com:9988	The text message within the XML log, or the entire XML message if it is unrecognized.

The AuditEvent table is the last table common to all logging applications. Past this table, the data is directed to the appropriate Fact tables for its application, based on the message type matching the application's XPATH expression. Each defined application has a top-level application-specific AuditEvent table. It may also have a deeper tree of Fact tables, depending on how detailed and varied the message parsing needs to be. The four default applications are Select Audit, Select Federation, Select Identity, and Select Access. Each of these will be discussed in turn.

Application-specific Fact Tables

The Select Audit schema contains application-specific Fact tables for Select Audit, Select Federation, Select Identity and Select Access.

Select Audit

Select Audit logs event messages to itself that keep records of configuration changes, report execution, and general events happening within the Audit Server.

SAudAuditEvent

Select Audit events are stored in the SAudAuditEvent table.

Table 4 SAudAuditEvent Table

Column Name	Type	Sample Value	CLOB
ID	Number	21	The unique ID of this message event.
AuditEventID	Number	13	The ID of the corresponding entry in the parent AuditEvent table.
LogType	Varchar2(255)	INFO	The level of logging the message was sent on.
Time_Stamp	Varchar2(24)	2006-09-29 10:52:15	Used for data integrity verification.
Event	Varchar2(64)	Access Control	The type of Select Audit event being logged.
Action	Varchar2(32)	LOGOUT	The specific action being logged.
Component	Varchar2(128)	Select Audit Portal	The module logging the message.
Host	Varchar2(128)	audit.myserver.com	The server that the log message was sent from.
UserName	Varchar2(64)	Admin	The user generating the event being logged.
Target	Varchar2(256)	http://audit.myserver.com/auditportal/logout.jsp	The location or resource that the event is being executed on.
Description	Varchar2(256)	User Admin Logged Out	A short description of the event.
Details	CLOB	<State><Status>201</status><Instance>0</Instance></State>	Event-specific details.

SAudServerConfig Table

If the Select Audit event being logged is a configuration change, an additional entry is created in the SAudServerConfig table. The type of configuration change will be captured in the above SAudAuditEvent table, through the event and component fields.

Table 5 SAudServerConfig Table

Column Name	Type	Sample Value	Description
ID	Number	4	The unique ID of this message event.
SAudAudit EventID	Number	21	The ID of the event entry in the parent SAudAuditEvent table.
Value	Varchar2(512)	10K	The new value of the configuration change.
OldValue	Varchar2(512)	13K	The previous value of the configuration item.

Select Federation

Messages that are identified as coming from a Select Federation application are entered into the SFAuditEvent table.

SFAuditEvent

The Select Federation messages are entered into the SFAuditEvent table.

Table 6 SFAuditEvent Table

Column Name	Type	Sample Value	Description
ID	Number	34	The unique ID of this message event.
AuditEventID	Number	13	The ID of the entry in the parent AuditEvent table.
Time_Stamp	Varchar2(24)	2006-09-29 10:52:15	Used for data integrity verification.
Event	Varchar2(255)	Logged Out	The type of action being logged.
AdminID	Varchar2(255)	Admin	The administrator executing this administrative task. Note: Either AdminID or UserID will be present, never both.
UserID	Varchar2(255)	UserA	The user executing this non-administrative action.
ProviderID	Varchar2(128)	myservername	The name of the partner server.

Table 6 SFAuditEvent Table (cont'd)

Column Name	Type	Sample Value	Description
RequestID	Varchar2(128)	`i6c449ffce0271f896f9e0a541d0d3e4589b7d834`	The unique identifier of this request (set by Select Federation).
Origin	Varchar2(128)	`Remote Site`	The type and ID of the originating machine.
OriginIP	Varchar2(128)	`16.254.11.685`	The IP address of the originating machine.
Details	CLOB	`<saml:assertion id="…`	Event-specific details.

Select Identity

All Select Identity (SI) messages are entered into the SIAuditEvent table, and depending on the message type, into one of its child Fact tables. Several entries in the Select Identity Fact tables are ID numbers that reference entries in the Select Identity system tables. These tables are described below in SI System Tables on page 19.

SIAuditEvent

The SIAuditEvent table contains all Select Identity messages.

Table 7 SIAuditEvent Table

Column Name	Type	Sample Value	Description
ID	Number	`34`	The unique ID of this message event.
AuditEventID	Number	`13`	The ID of the entry in the parent AuditEvent table.
AdminRole	Varchar2(255)	`End User`	The role of the user executing the event.
AuditType	Varchar2(32)	`20`	The ID of the event being logged.
AuditSubType	Varchar2(32)	`3`	The specific ID of the action being logged.
Time_Stamp	Varchar2(24)	`2006-09-29 10:52:15`	Used for data integrity verification.
Status	Varchar2(32)	`2`	The status of the event.
ServiceName	Varchar2(64)	`Service1`	The name of the service (if any).
AdminID	Varchar2(32)	`1110`	If the user is an administrator, their admin ID.

Table 7 SIAuditEvent Table (cont'd)

Column Name	Type	Sample Value	Description
AdminName	Varchar2(128)	Zhang	The user name of the administrator.
RequestMethod	Varchar2(32)	3	The SI request method ID. See SI_SYS_AuditRequestMethod Table on page 20 for descriptive name.
RequestType	Varchar2(32)	1	The SI request type ID. See SI_SYS_RequestTypes Table on page 20 for descriptive name.
RequestID	Varchar2(32)	11536	The unique ID of this request.
ParentRequestID	Varchar2(32)	11535	The ID of the parent request.
CauseByRequestID	Varchar2(32)	9748	The ID of the request generating this.
CTXVarName	Varchar2(255)	Company	The name of the service context identifier.
CTXVarValue	Varchar2(255)	HP	The value of the service context identifier.
CTXVarID	Varchar2(255)	8	The ID of the service context identifier.

SIAuditTarget Table

The SIAuditTarget table is used to store details about Select Identity Target entries in the logs. Every entry in the target table corresponds to an entry in the SIAuditEvent table. An Select Identity audit event may have multiple target/user/other entries in its subtables.

Table 8 SIAuditTarget Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this message event.
SIAuditEventID	Number	34	The reference to the entry for this message in the parent SIAuditEvent table.
TargetID	Varchar2(32)	3900	The ID of the target.
TargetName	Varchar2(255)	sf	The name of the target.
TargetType	Varchar2(255)	9	The predefined type of the target. See SI_SYS_AuditTargetTypes Table on page 19 table for the descriptive name.

SIAuditUser Table

The SIAuditUser table is used to store details about Select Identity audit users from the logs.

Table 9 SIAuditUser Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this message event.
SIAuditEventID	Number	34	The reference to the entry for this message in the parent SIAuditEvent table.
UserID	Varchar2(32)	3682	The unique identifier of the user.
Name	Varchar2(128)	Administrator	The user name.
PrimaryID	Varchar2(32)	5354	The primary ID is used with the PrimaryName to associate multiple accounts with a single user.
PrimaryName	Varchar2(128)	Admin	The name are used with the PrimaryID to associate multiple accounts with a single user.
Details	CLOB	<memberships> <OVSIAudit Membership> <membershipId> 1826</memb...	Used to hold any additional information specified about the user.

SIAuditSvcConfigChange Table

The SIAuditSvcConfigChange table is used to describe service configuration changes logged by Select Identity.

Table 10 SIAuditSvcConfigChange Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this service config change entry.
SIAuditEventID	Number	34	The reference to the entry for this message in the parent SIAuditEvent table.
SIType	Number	6	The Select Identity audit action being logged. See SI_SYS_AuditType Table on page 19 table for descriptive names.
ServiceID	Number	1626	The unique ID of the service being configured.

Table 10 SIAuditSvcConfigChange Table (cont'd)

Column Name	Type	Sample Value	Description
ServiceName	Varchar2(256)	`ExternalLDAP`	The name of the service being configured.
FieldID	Number	`1765`	The ID of the field being configured.
FieldName	Varchar2(256)	`View`	The name of the field being configured.
Details	CLOB	`<properties> <property name= "eventHandlers"> <add><entity key="1"/>…`	Additional properties describing the service configuration.

SIAuditConfigChange Table

The SIAuditConfigChange table is used to store information logged about configuration changes made within Select Identity.

Table 11 SIAuditConfigChange Table

Column Name	Type	Sample Value	Description
ID	Number	`48`	The unique ID of this configuration entry.
SIAuditEventID	Number	`34`	The reference to the entry for this message in the parent SIAuditEvent table.
SIType	Number	`15`	The type of Select Identity configuration change being logged. See SIType Values for corresponding names.
FieldID	Number	`9`	The ID of the field being configured.
FieldName	Varchar2(64)	`Workflow Template`	The name of the field being configured.
Details	CLOB	`<properties> <property name="admin AttributeView"> <add><value> <![CDATA[0]]…`	Additional details about the configuration.

SIType Values

```
TYPE_RESOURCE = 1;
TYPE_ADMIN_ROLE = 4;
TYPE_EXT_CALL = 5;
```

```
TYPE_SERVICE = 6;
TYPE_SERVICE_CTX = 7;
TYPE_SERVICE_ROLE = 8;
TYPE_SERVICE_VIEW = 9;
TYPE_ATTRIBUTE = 10;
TYPE_WORKFLOW = 11;
TYPE_RULE = 12;
TYPE_NOTIFICATION = 13;
TYPE_CONNECTOR = 14;
TYPE_CONFIG_ITEM_CFG = 15;
TYPE_SERVICE_ROLE_CREATE = 16;
TYPE_SERVICE_ROLE_DELETE = 17;
TYPE_SERVICE_ROLE_MODIFY = 18;
TYPE_SERVICE_CTX_CREATE = 19;
TYPE_SERVICE_CTX_DELETE = 20;
TYPE_SERVICE_CTX_MODIFY = 20;
TYPE_SERVICE_FORM_CREATE = 21;
TYPE_SERVICE_FORM_DELETE = 22;
TYPE_SERVICE_FORM_MODIFY = 23;
```

SIAuditUser Table

The SIAuditUser table is an index table that stores common user information for both the SIAuditUserMembership and the SIAuditUserAttrChange tables.

Table 12 SIAuditUser Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this user entry.
SIAuditEventID	Number	13723	References table SIAuditUser.
UserID	Varchar2(32)	1624	The Select Identity user ID of this user.
Name	Varchar2(128)	AWest	The Select Identity user name of this user.
PrimaryID	Varchar2(32)	1422	The primary ID is used with the PrimaryName to associate multiple accounts with a single user.
PrimaryName	Varchar2(128)	Adam29	The name are used with the PrimaryID to associate multiple accounts with a single user.
Details	CLOB	<memberships> <OVSIAudit Membership> <membershipId> 1109…	Used to store any additional information about this user.

SIAuditUserAttrChange Table

The SIAuditUserAttrChange table is used to store details about Select Identity user attribute changes.

Table 13 SIAuditUserAttrChange Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this user attribute change entry.
SIAuditUserID	Number	13723	Reference to the corresponding entry's ID in the parent SIAuditUser table.
AttrID	Number	8	The ID of the attribute type being changed.
AttrName	Varchar2(64)	Company	The name of the attribute being changed.
OpType	Number	2	The type of change being executed. See SI_SYS_AuditChangeOp Table on page 20 for descriptive names.
CLOB	Varchar2(512)	HP	The new value coming out of the change.
CLOB	Varchar2(512)	Compaq	The previous value of the attribute.
SensitiveLevel	Number	1	The level of sensitivity of the data. See SI_SYS_SensitiveLevel Table on page 21 for descriptive names.

SIAuditUserMembership Table

The SIAuditUserMembership table is used to store information about user membership changes logged by Select Identity.

Table 14 SIAuditUserMembership Table

Column Name	Type	Sample Value	Description
ID	Number	48	The unique ID of this user membership entry.
SIAuditUserID	Number	34	Reference to the corresponding entry's ID in the parent SIAuditUser table.
UserID	Number	4299	The user ID of the user membership being changed.
MembershipID	Number	1929	The ID of the membership being changed.

Table 14 SIAuditUserMembership Table (cont'd)

Column Name	Type	Sample Value	Description
Membership Operation	Number	1	The type of change being executed. 1 =Add, 2 =Delete.
MembershipType	Number	2	The Select Identity membership type. 1 =Resource, 2 =Service.
MembershipName	Varchar2(32)	chAdmin	The membership name being modified.

SI System Tables

SI System tables are used to define the unique identifiers used in Select Identity log messages. If you are building reports from Select Identity Fact tables, select from these tables to get descriptive names instead of ID numbers.

Table 15 SI_SYS_AuditTargetTypes Table

Column Name	Type	Sample Value	Description
TargetTypeID	Number	11	The unique ID of this Select Identity audit target.
TargetTypeName	Varchar2(32)	Workflow	The descriptive name of the audit target.

Table 16 SI_SYS_AuditType Table

Column Name	Type	Sample Value	Description
AuditTypeID	Number	34	The unique ID of this Select Identity audit type.
Action	Varchar2(64)	Add	The corresponding action name for this audit type.
Description	Varchar2(64)	Add New User	The descriptive name for the action.

Table 17 SI_SYS_AuditEventStatus Table

Column Name	Type	Sample Value	Description
StatusID	Number	5	The unique ID of this event status message.
StatusName	Varchar2(32)	Approved	The descriptive name of this status message.

Table 18 SI_SYS_AuditSubType Table

Column Name	Type	Sample Value	Description
SubTypeID	Number	`1`	The unique ID of this subject type.
SubTypeName	Varchar2(32)	`Approval`	The descriptive name of this subject type.

Table 19 SI_SYS_AuditChangeOp Table

Column Name	Type	Sample Value	Description
OpTypeID	Number	`1`	The unique ID of this operation type.
OpType	Varchar2(32)	`Add`	The descriptive name of this operation type.

Table 20 SI_SYS_RequestTypes Table

Column Name	Type	Sample Value	Description
RequestTypeID	Number	`5`	The unique ID of this request type.
RequestTypeName	Varchar2(32)	`System Request`	The descriptive name of this request type.

Table 21 SI_SYS_AuditRequestMethod Table

Column Name	Type	Sample Value	Description
RequestMethodID	Number	`3`	The unique ID of this request method.
RequestMethod	Varchar2(64)	`SOAP`	The name of this request method.
Description	Varchar2(64)	`Delegated WEBService`	The descriptive name of this request method.

Table 22 SI_SYS_AuditServiceType Table

Column Name	Type	Sample Value	Description
ServiceID	Number	`1`	The unique ID of this service type.
ServiceName	Varchar2(32)	`Admin Service`	The descriptive name of this service type.

Table 23 SI_SYS_SensitiveLevel Table

Column Name	Type	Sample Value	Description
SensitiveLevelID	Number	1	The unique ID of this data sensitivity level.
SensitiveLevel	Varchar2(32)	Clear Text	The descriptive name of this data sensitivity level.

Select Access

Select Access log messages are quite complex in nature. Therefore, the Select Access normalizer schema is more comprehensive than some of the other applications, with over a dozen Fact and details tables.

SAAuditEvent

All Select Access messages will have an entry in the top-level SAAuditEvent table.

Table 24 SAAuditEvent Table

Column Name	Type	Sample Value	Description
ID	Number	26	The unique ID of this message event.
AuditEventID	Number	13	The ID of the corresponding entry in the parent AuditEvent table.
Host	Varchar2(255)	16.98.124.281	The IP Address of the host machine.
Administrator	Varchar2(255)	Admin24	The username of the administrator, if this event is an admin action.
Time_Stamp	Varchar2(24)	2006-09-29 10:52:15	The time the event was logged.
EventLevel	Varchar2(32)	INFO	The log severity level of the message.
Channel	Varchar2(32)	LDAP	The source of the message.
EntryName	Varchar2(1024)	<entryName> cn=admin admin, ou=Victoria-Audit-Apr6, dc=can,dc=hp, dc=com </entryName>	The LDAP representation of the user.
Service	Varchar2(255)	jdbc://volcano.can.hp.com:7001	The service being requested.

Table 24 SAAuditEvent Table (cont'd)

Column Name	Type	Sample Value	Description
SAResource	Varchar2(255)	`/WebService/ WebService.asmx`	The resource being accessed.
SAResourceOld	Varchar2(255)	`Network/Sun ONE`	In a change, the resource previously in use.
SAUser	Varchar2(255)	`cn=admin admin, ou=victoria-audit-apr6, dc=can,dc=hp, dc=com`	The Select Access user performing the action.
Message	Varchar2(2048)	`ALLOW, source IP address 14.234.77.134`	A brief message describing the log.

SALogConfig Table

Once an entry has been inserted into the SAAuditEvent table, it may also reference one or more detail tables. For example, in a log configuration change message, the old value and the new value of the change are both inserted into the SALogConfig table.

Table 25 SALogConfig Table

Column Name	Type	Sample Value	Description
ID	Number	`6`	The unique ID of this entry.
SAAuditEventID	Number	`26`	The ID of the corresponding message entry in the parent SAAuditEvent table.
Type	Varchar2(10)	`Old`	Either `old` or `new`. The type of value being recorded.
Value	Varchar2(512)	`<old><logClient Config> <destination> <systemLog/> <channel level="ERROR" name="*"/> </destination> </logClient Config></old>`	Details the previous value of the setting, before the config change.

SALogDestination Table

Every SALogConfig entry has one or more destination entries in the SALogDestination table.

Table 26 SALogDestination Table

Column Name	Type	Sample Value	Description
ID	Number	6	The unique ID of this entry.
SALogConfigID	Number	8	The ID of the corresponding entry in the parent SALogConfig table.
Destination	Varchar2(255)	<destination> <logSAudServer host="127.0.0.1" port="9979"/> <channel level="INFO" name="*"/> </destination>	The destination the logger is logging to (for example. to a file, to a Select Audit connector).

SAComponentChange Table

The SAComponentChange table stores the new and old values for any configuration changes that are executed within Select Access.

Table 27 SAComponentChange Table

Column Name	Type	Sample Value	Description
ID	Number	11	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
Component	Varchar2(80)	Admin Server	The component logging the event.
Old	CLOB	<old><validator Config> <serverHost> alvafish.asia pacific.hpqcorp .net </serverHost> </validator Config></old>	The old value of the configuration change.
New	CLOB	<new><validator Config> <serverHost> alvafish.asia pacific.hpqcorp .net </serverHost> </validator Config></new>	The new value of the configuration change.

SAAttribute Table

The SAAttribute table stores the representation of a single attribute of a log message. Each message may have several attribute entries.

Table 28 SAAttribute Table

Column Name	Type	Sample Value	Description
ID	Number	13	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
Type	Varchar2(10)	Add/Remove	Tracks if the attribute is being added or removed.
Name	Varchar2(128)	UserPassword	The attribute name.
Value	Varchar2(512)	XXXXXXXX	The attribute value. Sensitive data is not available for access.

SAAccessRule Table

The SAAccessRule table describes a Select Access Access Rule definition.

Table 29 SAAccessRule Table

Column Name	Type	Sample Value	Description
ID	Number	9	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
Type	Varchar2(10)	Old/new	Marks if the details are describing the current value or previous.
AccessRuleName	Varchar2(32)	Logout	The name of the Access Rule.
AccessRuleType	Varchar2(32)	Rule	The type of Access Rule.
Details	CLOB	<ACCESSRULE NAME ="logout" TYPE="rule"> <COMPONENT CONDITION="begin" EVALUATOR="logout " NAME="Logout" TYPE="allow"/> </ACCESSRULE>	The details of the Access Rule defined.

SAComponent Table

The SAComponent table describes settings for authentication and decision plugins configured for Select Access.

Table 30 SAComponent Table

Column Name	Type	Sample Value	Description
ID	Number	`3`	The unique ID of this entry.
SAAuditEventID	Number	`26`	The ID of the corresponding message entry in the parent SAAuditEvent table.
Type	Varchar2(10)	`New`	`Old` or `New`. The type of component being described.
ComponentType	Varchar2(32)	`decision`	The type of component (`decision`, `authentication`).
Condition	Varchar2(32)	`Any`	Describes the condition set on the component.
Name	Varchar2(32)	`Authentication`	The name of the component being configured.
Authenticator	Varchar2(32)	`password`	The name of the authenticator used.
Method	Varchar2(32)	`password`	The type of authentication.
Evaluator	Varchar2(32)	`authentication`	The name of the evaluator used.
Configurator	Varchar2(128)	`com.hp.ov. selectaccess.rule builder.screens. AuthPropertiesDlg`	The class name of the configurator for this component.
Details	CLOB	`<COMPONENT CONDITION="any" CONFIGURATOR="com .hp.ov. selectaccess.rule builder.screens. AuthPropertiesDlg " DESCRIPTION= "Authenticate Users" EVALUATOR="authen tication" …`	All details about the component configuration.

SAMatrixDelegate Table

The SAMatrixDelegate table describes configuration of the Select Access matrix.

Table 31 SAMatrixDelegate Table

Column Name	Type	Sample Value	Description
ID	Number	4	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
Changetarget	Varchar2(20)	matrixChange	The type of change being executed.
NodeType	Varchar2(32)	Identity	The column type being configured in the matrix.
OldValue	Varchar2(32)	inherit	The old value of the change.
NewValue	Varchar2(32)	allow	The new value set by the change.
Details	CLOB	<matrixChange><administrator>Main Administrator</administrator><resource>Resource Access/volcano</resource><user>cn=victoria victoria,ou=Victoria-Audit-Apr6,dc=can,dc=hp,dc=com</user><nodeType>Identity</nodeType><OldValue>inherit</OldValue><NewValue>allow</NewValue><old>inherit</old><new>allow</new></matrixChange>	All details about the change.

SAUserSource Table

The SAUserSource table describes where Select Access users are provisioned from.

Table 32 SAUserSource Table

Column Name	Type	Sample Value	Description
ID	Number	`1`	The unique ID of this entry.
SAAuditEventID	Number	`26`	The ID of the corresponding message entry in the parent SAAuditEvent table.
userSource	Varchar2(128)	`SA Users - OpenLDAP on blowfish`	Describe where Select Access users are provisioned from (LDAP server, file system).
serverDN	Varchar2(128)	`ou=deb-identity -win2k3-zurich -apr27,dc=gdcc, dc=com`	
serverAddresss	Varchar2(128)	`access.hp.net`	
serverPort	Varchar2(16)	`342`	
serverSSL	Varchar2(16)	`True`	`True` or `False` if SSL is used on this server.
Old	Varchar2(256)	`Users5`	If the user source is changed, the old value of the source.
New	Varchar2(256)	`Users3`	If the user source is changed, the new value of the source.

SAPolicyDecision Table

The SAPolicyDecision table describes Validator policy decisions.

Table 33 SAPolicyDecision Table

Column Name	Type	Sample Value	Description
ID	Number	`19`	The unique ID of this entry.
SAAuditEventID	Number	`26`	The ID of the corresponding message entry in the parent SAAuditEvent table.
PolicyAction	Varchar2(32)	`AUTH`	The action being performed by the Validator (`Allow`, `Deny`, `Auth`).

Table 33 SAPolicyDecision Table (cont'd)

Column Name	Type	Sample Value	Description
EventType	Varchar2(32)	POST	The type of HTTP request sent to the Enforcer.
SrcIP	Varchar2(64)	15.211.119.84	The IP the request is originating from.
PolicyUser	Varchar2(256)	admin	The user name of the authenticated Select Access user executing the request.

SAPasswordResetConfig Table

The SAPasswordResetConfig table records the details of Select Access password reset settings.

Table 34 SAPasswordResetConfig Table

Column Name	Type	Sample Value	Description
ID	Number	6	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
Old	CLOB	<old><passwordReset><questions reset QuestionNumber="14" userQuestionNumber="14"><question>What is your mother's maiden name?</question>…	The old password reset settings, from before this change event.
New	CLOB	<new><passwordReset><questions reset QuestionNumber="1" userQuestionNumber="1"><question> What is your place of birth?</question>…	The current password reset settings, after this event.

SAWorkflowChange Table

The SAWorkflowChange table describes a Select Access workflow event.

Table 35 SAWorkflowChange Table

Column Name	Type	Sample Value	Description
ID	Number	5	The unique ID of this entry.
SAAuditEventID	Number	26	The ID of the corresponding message entry in the parent SAAuditEvent table.
WorkflowID	Varchar2(32)	1	The ID of the workflow being changed.
WorkflowDate	Varchar2(32)	20060308193910	The date that the workflow was initiated.
Action	Varchar2(10)	submitted	The action being performed on the workflow.
Submitter	Varchar2(128)	admin	The user ID of the user who initiated the workflow.
Description	Varchar2(256)	Create identity entry at "users/approver97 User".	A textual description of the change.
Reason	Varchar2(256)	Invalid Entry	The reason supplied when rejecting a workflow.

SAWorkflowAttribute Table

For each workflow change event logged, there is one or more attribute change logs in the SAWorkflowAttribute table, describing the old and new value of the change.

Table 36 SAWorkflowAttribute Table

Column Name	Type	Sample Value	Description
ID	Number	5	The unique ID of this entry.
SAWorkflow ChangeID	Number	5	The ID of the corresponding entry in the parent SAWorkflowChange table.
AttributeName	Varchar2(128)	telephoneNumber	The name of the attribute.
OldValue	CLOB	555-7717	The previous value, before the change.
NewValue	CLOB	555-7777	The new value, after the change.

Database Views

A number of views exist in the Select Audit database schema and the are used in different ways. Some views are used in the underlying SQL that make up the Select Audit default reports, for example, System Activity Report, Service Report. Other views are used during data filtering when Select Identity Integration is enabled, to simply the filtering process. Views are also used by the modeling component. The different views are listed below, categorized according to how they are used.

Views Used in Reports

AuditEventsView

This view forms the heart of the SQL used in the following Select Audit default reports:

- Account Change Report
- Account Events Report
- Administrator Report
- Configuration Report
- Password Management Report
- Security Events Report
- System Activity Report
- User Activity Report
- User Summary Report

The view collects together all the different audit event details needed for the above reports.

AuditEventsViewSISpecific

This view is designed specifically to be used in the Service Report. The Service Report involves the most complex SQL, compared with any of the other default reports. A specific view was created to simplify things and for performance.

The Service Report contains multiple joins and doesn't solely rely on this specific view.

WorkflowEventsView

This view is designed specifically to be used in the following two reports:

- Workflow Events Report
- Change History Report

EventTypesView

This view is used within the AuditEventsView and in the `.rdl` definition of the reports to return the list of actions that can be contained in a particular report.

Views Used in Select Identity Integration Data Filtering

The following views are used as part of the data filtering logic:

- SiAdminSiView
- SiAdminSfView
- SiAdminSaView
- SiAdminSaudView
- SiAdminAuditView
- SiAdminSaudGenView
- SiAdminEventTypesView
- SiAdminUserView
- SiAdminEventView
- SiAdminSVCCTXVALView
- NonSiReportEventTypesView
- SiReportTypeCompEventView
- Auditreportsipermissionview

Views Used in Modelling Component

The following views are used by the modeling component:

- auditeventview
- auditlist
- eventlist
- eventsummary
- eventview
- saattributeview
- sacompchangeview
- sacomponentview
- saeventview
- salogview
- samatrixview
- saruleview
- saseventview
- sausersourceview
- sawfview
- siconfigchangeview
- siservicechangeview
- siseventview

- sitargetview
- siuserattrview
- siusermembershipview
- siuserview
- siusrview

Other Views

This section lists views in the Select Audit database schema that are not included in the sections above:

- **Sa_wf_state_times** is used by the Workflow Scheduler in Workflow Attestation. The quartz timer reads this view to run the workflows.