



ISSO Users Guide

Broadsword Version 3.1

Prepared for:
AFC2ISRC/A26
Langley Air Force Base, VA 23665

Prepared by:
Air Force Research Laboratory, Rome Research Site
AFRL/IFEB
32 Brooks Road
Rome, NY 13441-4114

September 2002

Version Note

This document is the current version of the Broadsword 3.1 ISSO Users Guide, superceding the Broadsword 3.1 ISSO Users Guide dated 17 June, 2002. This document was updated to reflect the changes in functionality added with the 3.1.x patch to the 3.1 software.

Curriculum Schedule	1
1 Functionality Through the Interface	2
1.1 Audit Events	2
1.2 Archived Events	3
2 Audit Formats	4
2.1 Understanding the Audits	4
2.2 User and Producer Audits	4
2.2.1 Logging into the Gatekeeper	5
2.2.2 Performing Queries on Local Sources	5
2.2.3 Performing Product Requests on Local Sources	6
2.2.4 Cataloging a Product	7
2.2.5 Deleting a Queue Product	7
2.2.6 Modifying Metadata associated with a product on a Queue	8
2.2.7 Setting Site Specific Validation	8
2.2.8 Logging out of the Gatekeeper	8
2.3 Putting It All Together	9
2.3.1 An Example with Only Local Requests	9
2.3.2 Interpreting the Audits	12
2.3.3 An Example with Local and Remote Requests	12
2.4 Identifying Audit Anomalies	15
2.5 Administrative Audits - Configuring and Maintaining the System	16
2.5.1 Gatekeeper Maintenance	17
2.5.2 INK Maintenance	19
2.5.3 Global Registration/Maintenance	19
2.5.4 User Maintenance	24
2.5.5 Group Maintenance	25
2.5.6 Operations Maintenance	26
2.6 ISSO Audits	26

Curriculum Schedule

UNCLASSIFIED

1 Functionality Through the Interface

Broadsword provides significant functionality to ease the ISSO's job through its interface. Once the account has been created and the ISSO role granted by the Broadsword Administrator, the user will see the 'ISSO' menu appear in their top menu bar. This menu consists of Audit Events and Archived Events.

1.1 Audit Events

The Audit Events screen is used to retrieve audit records currently stored in the Sybase database, to delete records from the Sybase database, and/or to archive records from the Sybase database to the Unix file system. This is done through filling in the appropriate fields and the bottom buttons.

- Username field – Fill this in if you're looking for one specific user. If it is blank, which is the default, the search is not dependent on username.
- Start Date field – This field starts with the current date/time loaded into it. The format is YYYYMMDDhhmmss, where YYYY is the four-digit year, MM the numeric two-digit month, DD the numeric two-digit day, hh the two-digit hour, mm the two digit minute, and ss the two-digit seconds. Note that if the Start Date and End Date fields are identical (as is initially the case), the search of audit events is not dependant on time.
- End Date field – This field starts with the current date/time loaded into it. The format is YYYYMMDDhhmmss, where YYYY is the four-digit year, MM the numeric two-digit month, DD the numeric two-digit day, hh the two-digit hour, mm the two digit minute, and ss the two-digit seconds.
- Audit Event field – this dropbox starts with "All Events" selected. If the ISSO chooses, they may limit this search to one specific auditable event, or leave 'All Events' selected. If 'All Events' is selected, the search is not dependent on audit events. The various Audit Events are described in more detail below, in the Audit Formats section.
- Archive File Name field – this is only used when archiving information from the Sybase to the Unix file system. At any other time, it should remain blank. It is highly recommended that the ISSO develop a meaningful schema for these archived audits to prevent confusion later. One suggestion would be to start with which user, which audit event, start&end dates, the date the audits were archived, and the initials of the ISSO. Note that blank spaces are not acceptable, but periods and underscores are.

Bottom buttons:

- Archive File
The system will enable this button when a filename has been entered. The system will copy these records to the Unix file system for the query defined above.
- Delete Records
The system will remove all records which match the query defined. Note that there is no way to retrieve this information once 'Delete Records' has been clicked. Instead, Archive the records first and verify that the archive is valid through the ISSO -> Archived Events functionality before deleting records. Always ensure that the query is the one you expect before selecting the 'Delete Records' button.
- Get Audit Report
The system will process the query defined above and create a blue 'View Audit Report' link on the page, which will open a separate window and display the desired audit information. More information on the format of these reports will be found in Audit Formats, below.

UNCLASSIFIED

1.2 Archived Events

The Archived Events screen is used to retrieve audit records currently stored in the Unix file system or to delete records from the Unix file system. This is done through filling in the appropriate fields and the bottom buttons.

The first table is a listing of any and all archived audits currently stored in the Unix filesystem (typically /opt/bswd3.1/audit). It has, on its left-hand edge, a column of checkboxes. The ISSO may select one or more of these archived audits to query within. The middle column replicates the name given that set of audit records by the ISSO who archived them. The third column lists when the audits were archived.

The second table closely repeats the fields in the Audit Events functionality, as described above. The one difference in functionality is the lack of an 'Archive File Name field'. Again, if the Start and End date fields are identical, the archived files will be checked regardless to date.

Finally, the bottom button allows the ISSO to 'Get Audit Record' for the selected archived audits.

2 Audit Formats

2.1 Understanding the Audits

The Broadsword components work together to provide the ISSO with a comprehensive set of tools for a) identifying who has accessed what information and b) assisting in the identification of significant security events. Specific audits logged by each of the components are provided in the following sections. Since Broadsword is a distributed architecture, it is important for the ISSO to understand where the information to answer a specific question exists. This section examples of all of the Gatekeeper audits that can be generated by user actions in the Broadsword client. The audits are broken up into three categories:

(1) User and Producer Audits

- * Logging into the Gatekeeper
- * Performing Queries on Local Sources
- * Performing Product Requests on Local Sources
- * Cataloging a Product
- * Logging out of the Gatekeeper
- * An Example with Local and Remote Requests

(2) Administrative Audits - Configuring and Maintaining the System

- * Gatekeeper Maintenance
- * INK Maintenance
- * Global Registration/Maintenance
- * User Maintenance
- * Group Maintenance
- * Operations Maintenance

(3) ISSO Audits

2.2 User and Producer Audits

To begin, the user launches a web browser on their local workstation and types in the URL of the assigned Gatekeeper (a Gatekeeper to which they have a login and password). The Broadsword system returns the home page for that Gatekeeper which requests that the user types in their login and password. Once the user has clicked the Accept button, the audit trail begins.

The table below provides a summary of the possible audits collected during a session for a user who is neither an Administrator nor an ISSO. In the following sections we will provide samples for each of the audits and conclude this section with a sample user session.

User Security Audits		
Event Description	Event Name	Configuration
User Logged In	LOGIN	All
Query	QUERY	All
Transfer Request	REQUEST	All
Catalog Request	CATALOG	All
Initiate Stream Request	INITSTREAM	All
Terminate Stream Request	TERMINATESTREAM	All
Client Profile Management		Not Used By Client
Client Profile Queue Management		Not Used By Client

UNCLASSIFIED

Get Column Attributes		Not Used By Client
User Logged Out	LOGOUT	All
Delete Managed Queue Entry	DELETEDQENTRY	All
Set Metadata Element	SETMETADATA	All
Configure Site Catalog Element	SETSITECATELEM	All

Table 1 – User Security Audits

2.2.1 Logging into the Gatekeeper

The first audit record that is cut for any user (regardless of what function or roles they have) is the initiation of a session. When a user logs into or attempts to log into the Gatekeeper, an audit record is cut. To generate a report of user logins the ISSO can either request All Events or select only User Logged In under the Event popup list. Selecting All Events will display the entire log to include login, queries, results, and product pulls. Selecting only User Logged In will provide only a list of login attempts.

The login audit record contains two lines. The first provides the user login, the IP Address of the machine they are logging in from, the user's ID on that workstation, the Gatekeeper's IP Address they are logging into and a unique session identifier. The session identifier will be unique for each time the user is logged in. The second line of the example below shows a successful log in.

```
Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper
```

Example 1 - Sample Login Record (Successful Login)

The next example shows the audit that is cut when either an invalid login or password is entered.

```
Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Invalid Login from Daleth Gatekeeper
```

Example 2 - Sample Login Record (Invalid Login)

The user has a number of times in which they must correctly enter the login and password. If they do not, the account will be automatically disabled. The example below displays the audit record identifying that the account was disabled. Prior to this record would be a number of invalid login audit records (as shown in the example just above).

```
Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Login disabled from Daleth Gatekeeper
```

Example 3 - Sample Login Record (Login Disabled)

2.2.2 Performing Queries on Local Sources

There are many capabilities provided to the user once they have logged in. Most of the features of the client are for personalization and do not require auditing. From a security viewpoint, the majority of

UNCLASSIFIED

auditable events can be put into two categories: (1) queries or requests and (2) product pulls or deliveries. Queries or requests are presented to the Gatekeeper through its application programmers interface (API), are audited by the Gatekeeper, and routed to the appropriated plugin(s). For each source that the user has queried an audit record is written verifying that the request was sent to the plugin and is being processed. The plugin then processes the request and sends the translated request to the source itself. When the source responds, the plugin processes the results and passes them back to the Gatekeeper, who in turn writes an audit record identifying the specific items returned as a result of the request and the total number of hits.

To generate a report of queries the ISSO can either request All Events or select only Query under the Event popup list. The example below provides a sample query/response set of audits. The first audit provides a summary of the request. This includes the type of query (simultaneous or sequential), whether thumbnails were requested, the maximum number of hits requested, the request itself and the source(s). The second line provides a list of the hits returned and a total of the number returned.

```
QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y,  
MAX_HITS=5(0=ALL), BQS=IMG.SOURCE="TEST" from 5D at Titan via Daleth
```

```
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327205627650 from 5D at Titan via Daleth
```

```
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327211927560 from 5D at Titan via Daleth
```

```
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827081558206 from 5D at Titan via Daleth
```

```
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827082616003 from 5D at Titan via Daleth
```

```
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827083055386 from 5D at Titan via Daleth
```

```
QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth
```

Example 4 - Sample Query/Response Record

2.2.3 Performing Product Requests on Local Sources

Depending on the type of source, there are two possible mechanisms to pull a product through the Broadsword Client: (1) Pull to View and (2) Deliver to Destination(s). From the Gatekeeper's viewpoint both mechanisms are the same - the only difference being the destination directory. Once the imagery product is in the desired format and compression, the product is delivered to the specified destination(s). In the case of a "pull to view," the product is delivered into a directory so that the client can set the content type and stream the file to the browser. If the request was a "deliver to destination(s)," the product will be delivered to the destination(s) and directory(s) specified by the user through FTP. The client sends the request to the Gatekeeper, which in turn audits the request, creates a status record into the status log and routes the request through the plugin. The plugin, in turn, routes the request to the source.

To generate a report of product pulls the ISSO can either request All Events or select only Transfer Request under the Event popup list. The example on the next page shows the events generated whenever a user requests a product.

REQUEST @ 20000926105854 : Request Accepted from 5D at Titan via Daleth

REQUEST @ 20000926105910 : 26105854ZSep00.000095134512128123177001000010000004907
ACCESSID: FIVED08002021976808002021976819970827081558206 FORMAT: (ASIS) DEST IP
ADDRESS: 123.45.678.89 DESTLOGIN: bswdreg DESTPATH:
/opt/bswd3.1/client/PROTECTED/docs/session/4906/ FILENAME:
bswdreg.FIVED08002021976808002021976819980897081558206.NITF02.00 STATUS: Transfer
successful. from 5D at Titan via Daleth

Example 5 - Sample Product Request/Delivery

The first line of the request record identifies that the request was passed on to the source. The second line provides a unique identifier for the request (the last five characters will contain the user's session id), the specific product that was requested, the format, the IP Address of the delivery destination, its directory and file name. It also provides the status of the delivery.

2.2.4 Cataloging a Product

The Broadsword Interface also allows users to produce imagery into IPL datasources. Every time a producer sends a product to the IPL's input queue, an audit record is generated.

To generate a report of cataloged products the ISSO can either request All Events or select only Catalog Request under the Event popup list. The next example shows a product being sent to the IPL 2.5.1 at Saturn with the title of "BSWD PEND TEST LPA0."

CATALOG @ 20001005151630 : Catalog New Product Accepted, PRODUCT TITLE: BSWD PEND
TEST LPA0 from IPL 2.5.1 at Saturn

CATALOG @ 20001005151630 : Catalog New Product Ftp to IPA/IPL Successful. PRODUCT TITLE:
BSWD PEND TEST LPA0 from IPL 2.5.1 at Saturn

Example 6 – Catalog a new product into IPL 2.5.1

The first record identifies that the IPL 2.5.1 plugin has accepted the product. The second record indicates that the plugin initiated an FTP session with the appropriate IPL 2.5.1 and that it was successful. At this point there is no way to find out whether the product was successfully ingested into the IPL database. IPL itself does not provide back any status.

2.2.5 Deleting a Queue Product

The Catalog Manager has the ability to delete products in a queue. This is typically done if the product is incorrectly produced by a Managed Producer or placed in the Public Queue.

UNCLASSIFIED

DELETEQENTRY @ 20001212122922 : Managed Product Deleted: Source = IPL 3.0 at AFRL, Managed User = smoej, Managed Product Title = AlphaTest.ird, Managed Product File Name = smoej-1008159031, Managed Date/Time = 20001212121033 from IPL 3.0 at AFRL

Example 7 – Deleting a Product From a Queue

2.2.6 Modifying Metadata associated with a product on a Queue

The Catalog Manager may choose to modify the metadata associated with a product on one of the queue(s) which they manage.

SETMETADATA @ 20011212121934 : Managed Product Metadata Update Successful: Source = IPL 2.5.1 at AFRL, Managed User = smoej, Managed Product Title = IPA_site.specific_20161138Zdec2000_583548, Managed Product File Name = smoej-1007995489, Managed Date/Time = 20011210144452 from phobos Gatekeeper

Example 8 – Modifying Metadata

2.2.7 Setting Site Specific Validation

The Catalog Manager may tighten the validation filters on the IPLs they manage. This functionality is reached through the Catalog Manager -> Site Validation page.

SETSITECATELEM @ 20011211152319: Section IMG Element SENS MODE Changes: Required Adding to Data List from saturn Gatekeeper

Example 9 – Site Validation

2.2.8 Logging out of the Gatekeeper

The last audit that is possible during a user session, is the logout record. Upon successful logout, an audit record is written identifying that the session was terminated. To generate a report of user logouts the ISSO can either request All Events or select only User Logged Out under the Event popup list. This next example provides a sample of this audit.

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

Example 10 - Logout Record

The Broadsword system implements a deadman timeout. Since the Broadsword client uses a Web browser, it is possible for it to terminate abnormally or for the user to exit the browser without logging out. In either of these cases, the session process will stay around. To allow for a graceful termination of these unconnected processes and to provide these resources back to the system, a timeout has been implemented. If there is an extended period of inactivity in a user's session (default is 30 minutes) the session will be terminated automatically. On those occasions a different logout audit record will be written, as shown below

UNCLASSIFIED

LOGOUT @ 20000926110202 : Gatekeeper timed out from daleth Gatekeeper

Example 11 - Logout Record (user timed out)

2.3 Putting It All Together

In this next section we provide two audit reports. The first contains only local requests, while the second has both local and remote.

2.3.1 An Example with Only Local Requests

Our first example, as pictured in Figure 1, includes only one Gatekeeper. A Gatekeeper (Daleth, IP Address 123.45.678.89) is connected to three local sources: IPL 1.0, 5D and MIDB. The IPL 1.0 and 5D reside on the same server (Titan) while the MIDB resides on a second server (Hoth). The name of the MIDB has been augmented by its version name, Othello. For our example, the user workstation is using the IP Address 123.45.678.90 and the username "gen_user."

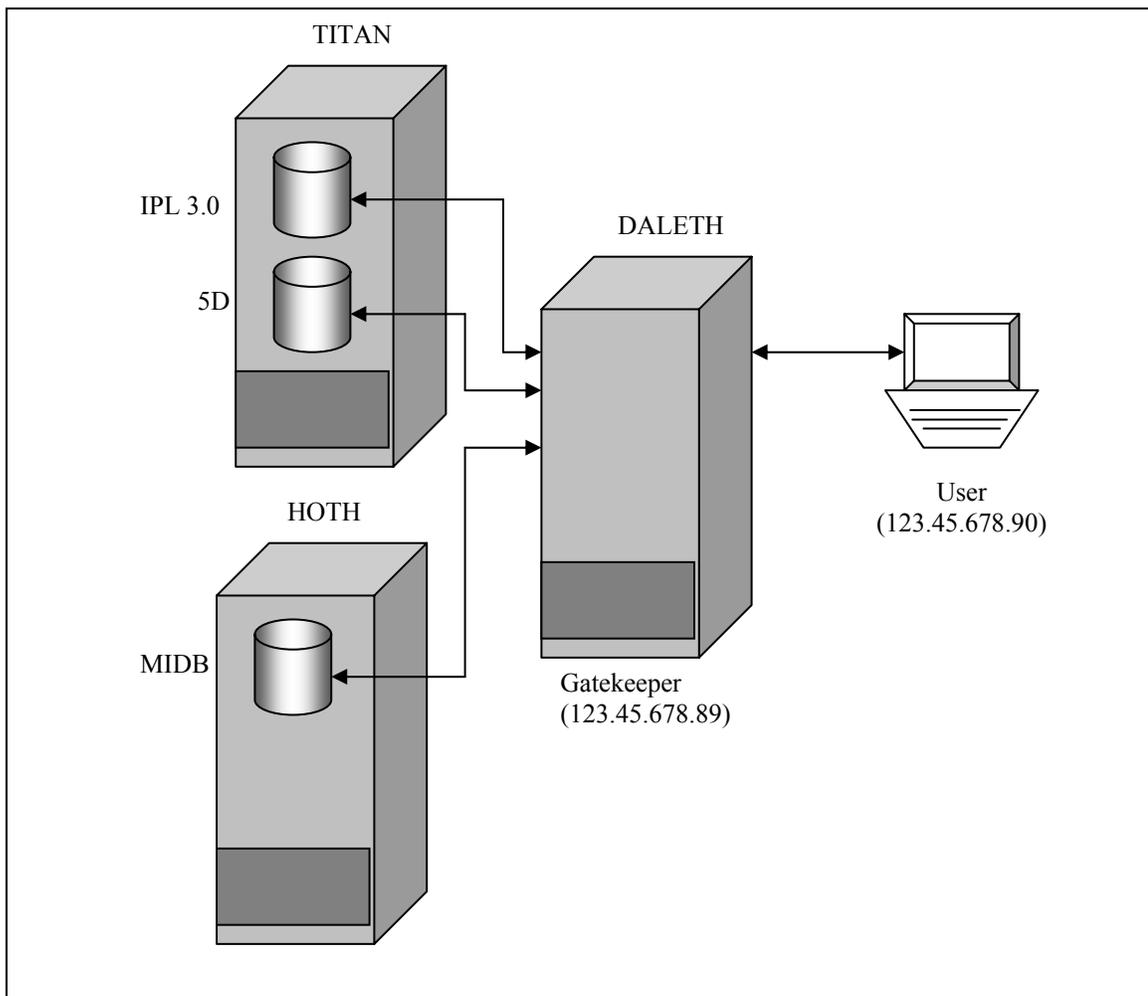


Figure 2.1 Performing a Local Request

UNCLASSIFIED

To view what the user has done, the ISSO would go to the Audit Log Maintenance page under the ISSO menu. This capability allows the ISSO to query the audit database. To continue with our example, the ISSO would enter the user name, "gen_user" and click on the Audit Report button. The Gatekeeper processes the request and an audit report will be generated. To view the report, the ISSO will next click on the "View Audit Report" anchor located in the middle of the page. The boxed figure below provides an example audit report.

Audit Report

User: gen_user For All Dates For All Events.

Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtpr: 123.45.678.89 Session Key: 4907
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULTANEOUS, THUMBNAIIS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Titan via Daleth

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAIIS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAIIS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from MIDB Othello at Hoth via Daleth

QUERY @ 20000926105619 : Unsupported Query Element: IMG.SOURCE for MIDB Othello at Hoth via
Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327205627650 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327211927560 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827081558206 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827082616003 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827083055386 from 5D at Titan via Daleth

QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204727486 from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204522533 from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204301083 from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204109470 from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826203915123 from IPL 3.0 at Titan via Daleth

QUERY @ 20000926105619 : 5 Hits from IPL 3.0 at Titan via Daleth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

Example 12 - Sample Audit Report (Request) for User "gen_user"

UNCLASSIFIED

2.3.2 Interpreting the Audits

The first line of the audit record indicates the beginning of a session. The Login identifies the user name of the person logged in. The IP is the IP address of the machine that the user has connected from. The Orig. Login is the username of that the user logged into the workstation with (if this information can be resolved). Gkpr is the IP address of the Gatekeeper the user has logged into. Session Key is a unique session identifier.

The second line identifies at what time the user attempted to login, the status of that login (Successful) and the name of the Gatekeeper that the user has logged into (Daleth Gatekeeper). The next set of records indicates that the user has initiated a query. Each record identifies what source the user has queried, what the user has queried for, the type of query (simultaneous or sequential), the number of hits to be returned from the source and, if supported, whether thumbnails have been requested or not. In this example, the 5D at Titan, IPL 3.0 at Titan and MIDB at Hoth were queried for up to five hits where IMG.SOURCE="TEST". At this point the Gatekeeper passes the query to the appropriate plugins and waits for their responses.

As each plugin returns, it provides status back to the Gatekeeper. The first response is from the MIDB plugin. The query submitted for the MIDB contained an element not supported (IMG.SOURCE) by MIDB and was blocked by the plugin.

The next set is from the 5D. Each record is uniquely identified using the Product's Access ID (PRD.ACCESSID). The last line of this set identifies that 5 hits (the maximum requested) were returned.

The last set of records is from the IPL30 plugin. Like 5D, each hit returned from the IPL is uniquely identified using the Product's Access ID. The last line again identifies the number of hits returned from the IPL. In our example, the IPL returned 5 hits. Since the user/client requested a maximum of 5 hits, only 5 are sent back. The last line of our example is the log out record. It identifies when the user logged out and that the connection with the Gatekeeper has been closed.

2.3.3 An Example with Local and Remote Requests

Our next example, as pictured in Figure 2, builds upon the previous example. It includes both our local Gatekeeper and an additional remote Gatekeeper with its own sources. The remote Gatekeeper (Beth, IP Address 987.65.43.210) has connected to it two sources, 5D and IPL 2.5.1.

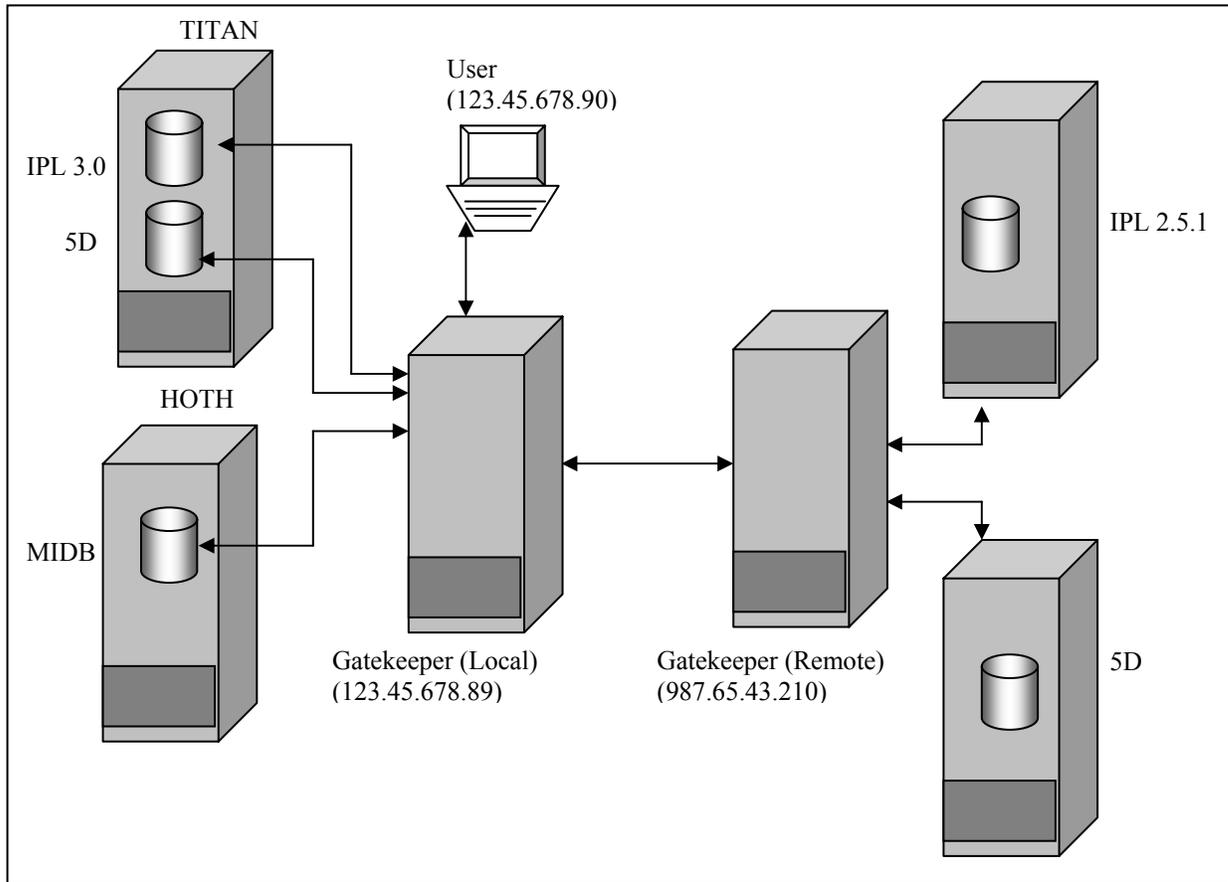


Figure 2.2 - Performing a Local & Remote Request

The local Gatekeeper continues to keep track of all requests and responses made by its local users. When the ISSO generates an audit report for a specific user at the Gatekeeper to which the user has logged in, all user activities are contained at that Gatekeeper. Remote Gatekeepers will also contain audit information for that portion of the request that they are responsible for.

In our example, the ISSO responsible for the given user (i.e. the local Gatekeeper's ISSO), through a similar query as with the previous example, will generate a single report for the given user including all requests/results from both the local and remote sources. If the ISSO performs a similar request (through the ISSO interface) on the remote Gatekeeper, the report will contain only information pertaining to that Gatekeeper's sources. The next page provides a sample of the reports generated from the local and remote Gatekeepers.

Reviewing the audit report, we see that the user logged in and queried a local 5D, a remote 5D, and a remote IPL 2.5.1. The request was sent to the respective sources, accepted and processed. The results were then returned and the user logged out.

Audit Report
User: gen_user For All Dates For All Events.

Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtkpr: 123.45.678.89 Session Key: 4907
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULT ANEIOUS, THUMBNAILS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Titan via Daleth
QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y
QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y

Q: How do I know this includes a remote query?
A: This is not the name of the local Gatekeeper.

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327205627650 from 5D at Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327211927560 from 5D at Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827081558206 from 5D at Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827082616003 from 5D at Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827083055386 from 5D at Titan via Daleth
QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826204727486 from IPL 2.1 at Saturn via Beth
QUERY @ 20000926105619 : Saturn IPA: 00001 Hit from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826204109470 from 5D at Neptune via Beth
QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826203915123 from 5D at Neptune via Beth
QUERY @ 20000926105619 : Saturn IPA: 00003 Hits from 5D at Neptune via Beth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

Audit Report
User: gen_user For All Dates For All Events.

Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtkpr: 123.45.678.89 Session Key: 4907
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Saturn via Beth
QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from IPL 2.1 at Neptune via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826204727486 from IPL 2.1 at Saturn via Beth
QUERY @ 20000926105619 : Saturn IPA: 00001 Hit from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826204301083 from 5D at Neptune via Beth
QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826204109470 from 5D at Neptune via Beth
QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:
FIVED80201de96719970826203915123 from 5D at Neptune via Beth
QUERY @ 20000926105619 : Saturn IPA: 00003 Hits from 5D at Neptune via Beth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

Example 13 – Local & Remote Audit Logs

2.4 Identifying Audit Anomalies

It is apparent, from reading the previous sections, that an audit report can contain extensive amounts of information. The question is what does the ISSO do with this information? What is the ISSO looking for? The ISSO is answering questions such as: Who is accessing the system? What is being accessed? Have there been any attempts to penetrate the system?

The last question is one that we are concerned with. The ISSO needs some way to identify that activity that might indicate attacks on the system. Such indicators can be invalid logins, bad MD5 seals, or unexpected system downtime. Broadsword provides an anomaly detection tool that allows an ISSO to easily identify malicious behavior.

The Broadsword Audit logs will highlight any audit records containing anomalous keywords, as demonstrated below.

```
Audit Report  
User: test Starting at: 20010216175029 and Ending at : 20010316175029 For All  
Events.  
  
LOGIN: test IP: 100.200.300.400 Orig.Login NotATest Gtkpr: 100.200.300.401  
Session Key: 54  
LOGIN @ 20010219181326: Successful Login from saturn Gatekeeper for bswd  
3.1  
LOGOUT @ 20010219171722: Connection close from saturn Gatekeeper for  
bswd 3.1  
Login: test IP: 100.200.300.400 Orig.Login NotATest Gtkpr: 100.200.300.401  
Session Key: 23104  
LOGIN @ 20010316142716 : Successful Login from saturn Gatekeeper for bswd  
3.1  
QUERY @ 20010316143211 : Query Accepted, QUERY  
TYPE=SIMULTANEOUS, THUMBNAIIS=Y,MAX_HITS=10 (0=ALL),  
BQS=TGT.CC="IZ" from IPL 2.5.1 at Ariel via SATURN LPA3 SDE  
QUERY @ 20010316143127 Could Not Connect to IPL 2.5 Database from IPL  
LOGOUT @ 20010316144102: Gatekeeper timed out from saturn Gatekeeper for  
bswd3.1
```

Anomaly highlight

Example 14 - Audit Report with Highlighted Anomaly

The ISSO may configure this utility by specifying new keywords and phrases to identify. To modify this list, the ISSO should edit the file `/opt/bswd3.1/client/etc/audit_anomalies.conf` on the Broadsword server. This file contains keywords to search for, one per line. To add a new key phrase to search for, merely add a new line to the file. The search phrases are not case sensitive. Once the phrase has been added, save the file and exit. The change will be reflected immediately; no process needs to be stopped or restarted.

2.5 Administrative Audits - Configuring and Maintaining the System

The Broadsword client provides the Administrator the ability to (1) configure/tailor the Broadsword system to a site's specific needs, (2) maintain the system and (3) obtain system status and statistics. Chapters 7 and 8 describe these capabilities. The purpose of this section is to describe the audits that are generated when the administrator performs a given function. An administrator is allowed to change only the information/configuration of the Gatekeeper that they are logged into. The following list provides a summary of the audits generated by the administrator.

User Security Audits		
Event Description	Event Name	Configuration
Gatekeeper Maintenance		
Added New Source	CREATESRC	ALL
Set Source Parameter	SETSRCPARAM	ALL
Set User Discretionary Access Control (DAC)	SETUSERDAC	ALL
Added Discretionary Access Control(DAC)	ADDDAC	ALL
Remove Source	DELETESRC	ALL
Remove Discretionary Access Control (DAC)		Not Used By Client
INK Maintenance		
Modified Element	MODELEMENT	ALL
Global Registration/Maintenance		
Register Our Gatekeeper with Keymaster	REGOURGKPR	ALL
New or Updated Gatekeeper Info	CONFIGUPDATE	ALL
Update Daemon Status	UPDATE_DAEMON	ALL
User & Group Maintenance		
Added User Privileges	ADDUSER	ALL
Remove User Privileges	DELUSER	ALL
Added Group Member	ADDGROUPMEMBER	ALL
Removed Group Member	DELGROUPMEMBER	ALL
Added Group	ADDGROUP	ALL
Modified Group	MODGROUP	ALL
Removed Group	DELGROUP	ALL
Operations		
Gatekeeper Started	GATEKEEPER STARTED	ALL
Gatekeeper Stopped	GATEKEEPER SHUTDOWN	ALL
Clear Statistics		Not Used By Client

Table 2 - List of Administrator Audits

The audit events described below are examples of typical audit records generated by an administrator. The specific auditable events include adding backside sources, configuring attributes, modifying users and registering the gatekeeper with the Keymaster.

UNCLASSIFIED

2.5.1 Gatekeeper Maintenance

The administrator has the ability to add or modify a backside source. Shown below are three examples of sources being added. Each source requires a number of parameters to be filled in. These parameters vary from source to source. The three examples show the different accesses that can be granted to a source: No Access, Local Access Only, and Local & Remote Access.

When a source is configured with No Access, by default no users have access to the source. In order to allow access to such a source, the administrator needs to grant that user access (see Chapter 4). Sources set to allow Local Access Only allow access only to those users logged into the given Gatekeeper. If the Gatekeeper is registered with a Keymaster, then any sources set to allow Local & Remote Access will allow all local users to access the source, and will also allow all users on other Gatekeepers in the Keymaster's domain to access the source.

This next example shows the creation of a new backside source. The source that was added was an IPL 2.1 to the Gatekeeper on Daleth.

```
CREATESRC @ 20001004054446 : IPL21 Source Created with Reference of  
8092cff8:970611035:IPL21:970616918 from Daleth Gatekeeper  
  
SETSRCPARAM @ 20001004054842 : Following parameters Changed For IPL 2.1 at AFRL: Query Max  
Hits, IPL 2.1 Host IP Address, IPL 2.1 TCP/IP Port, IPL 2.1 Site Name, IPL Host IP Address, IPL Order  
Status Port, IPL 2.1 Account, IPL 2.1 Sybase IP Address, IPL 2.1 Sybase Port, IPL21 Database Name, IPL  
2.1 SQS Sybase Server IP Address, IPL 2.1 SQS Sybase Server Port, IPL 2.1 Database Login, Access  
Permission Override, IPL 2.1 Password, IPL 2.1 Database Password from Daleth Gatekeeper  
  
SETUSERDAC @ 20001004054843 : ALL Allowed Access to IPL 2.1 at AFRL from Daleth Gatekeeper
```

Example 15 - Add an IPL 2.1 source and allow access to all users

The CREATESRC record was generated by the creation of the source. The SETSRCPARAM record shows a list of all of the source parameters set when the source was created. The SETUSERDAC record is generated when the client sets the list of users allowed access to the source to ALL. The example below shows the creation of a new IPL 1.0 source that has been made available to only local users.

```
CREATESRC @ 20001004054446 : IPL Source Created with Reference of  
8092aae7f2:935556478:IPL:972337212 from Daleth Gatekeeper  
  
SETSRCPARAM @ 20001004054842 : Following parameters Changed For IPL at AFRL: Query Max  
Hits, IPL Host IP Address, IPL TCP/IP Port, IPL Site Name, IPL Host IP Address, IPL Order Status Port,  
Harvest TCP/IP port, Format Conversion Flag, IPL Account, Access Permission Override from Daleth  
Gatekeeper  
  
ADDDAC @ 20001004054843 : None Allowed Access to 8092aae7f2:935556478:IPL:972337212 from  
Daleth Gatekeeper  
  
SETUSERDAC @ 20001004054843 : 8092aae7f2:935556478 Allowed Access to IPL at AFRL from  
Daleth Gatekeeper
```

Example 16 - Add an IPL 2.1 source and allow access to only local users

UNCLASSIFIED

In this example, the ADDDAC call is made to explicitly to allow no access to the source. Then the SETUSERDAC call adds 8092aae7f2:935556478 (Daleth's Gatekeeper Reference) to the access list. This allows all of Daleth's local users to access this source.

The next example shows the creation of a new 5D source that, by default, does not allow access to any users.

```
CREATESRC @ 20001004071517 : 5D Source Created with Reference of
8092cff8:970611035:5D:970622117 from Daleth Gatekeeper

SETSRCPARAM @ 20001004071520 : Following parameters Changed For 5D at AFRL: Query Max Hits,
Query Plugin Name, Request Plugin Name, 5D Sybase IP Address, 5D Sybase Port, 5D Database Name,
5D Catalog Directory, 5D Database
Login, IPL TCP/IP Port, IPL Order Status Port, IPL 2.0 Account, Access Permission Override from Daleth
Gatekeeper

SETUSERDAC @ 20001004054843 : ALL Denied Access to 5D at AFRL from Daleth Gatekeeper
```

Example 17 - Add a 5D source and deny access to all users

In this example, the SETUSERDAC call is made to deny access to all users.

There are two additional functions available for configuring sources. These are the modification of a parameter of a source and the removal of a source. The next two examples show the audit record that is written when a source attribute has been modified, and the audit record when the source has been removed.

```
SETSRCPARAM @ 20001101023601 : Following parameters Changed For John's IESS: Exploitation
Sybase Port, Imagery_Coverage Sybase Port from saturn Gatekeeper
```

Example 18 - Modification of a Source Parameter

```
DELETESRC @ 20001004054843 : Source IPL21 (IPL 2.1 at AFRL) Deleted With Reference of
8092cff8:970611035:IPL21:970616918 from Daleth Gatekeeper
```

Example 19 - Removal of a Source (IPL 2.1 at AFRL)

There are a number of system or gatekeeper parameters that were configured during the installation process. There may be a need to change this information. If any of this information is changed, it will be audited. This next example shows an audit record when the Point of Contact field was modified.

```
SETSRCPARAM @ 20001013113738 : Following parameters Changed for Daleth Gatekeeper: Point of
Contact from Daleth Gatekeeper
```

Example 20 - Modifying the Gatekeeper's Point of Contact

UNCLASSIFIED

2.5.2 INK Maintenance

Using the DE Configuration capability, the administrator can modify an existing attribute's name, help, and popdown values. The two following examples show the audits cut when the administrator has gone into the DE configuration page and selected the CLASS attribute under the PROD (Product) table. In the first, the administrator has removed an entry from the popdown list. In the second, the administrator has added a new entry to the popdown list.

MODELEMENT @ 20001006114746 : Section PRD Element CLASS Changes:
Display Name Data Help for Daleth Gatekeeper

MODELEMENT @ 20001006114748 : Section PRD Element CLASS Changes: Deleting From Data List
from Daleth Gatekeeper

Example 21 - Modifying the Gatekeeper's Point of Contact

MODELEMENT @ 20001006114746 : Section PRD Element CLASS Changes:
Display Name Data Help for Daleth Gatekeeper

MODELEMENT @ 20001006114748 : Section PRD Element CLASS Changes: Adding
To Data List Data List Help from Daleth Gatekeeper

Example 22 - Adding a new popdown

2.5.3 Global Registration/Maintenance

Broadsword v1.0 allowed a site to grant a single point of access to local data sources for all of the site's users. Broadsword v2.0 introduced the Keymaster. The Keymaster allows the creation of a virtual network between Gatekeepers. Each Gatekeeper has the ability to publish local data sources (this list is called the Gatekeeper's local map), thus allowing users at other sites to access these sources (recall Figures 3.6 and 3.7). The Keymaster maintains a global list of each Gatekeeper's local map (referred to as the global map). This table provides a list of Keymaster audit events.

Administrative Security Audits for Keymaster ONLY	
Event Description	Event Name
Accept Registration from Remote Gatekeeper	INITREG
New or Updated Gatekeeper Info	CONFIGUPDATE
Update Daemon Status	UPDATE_DAEMON
Unregister Gatekeeper	UNREGGKPR

Table 3 – Keymaster Audit Events

This diagram shows the sample environment that we will consider for the following examples:

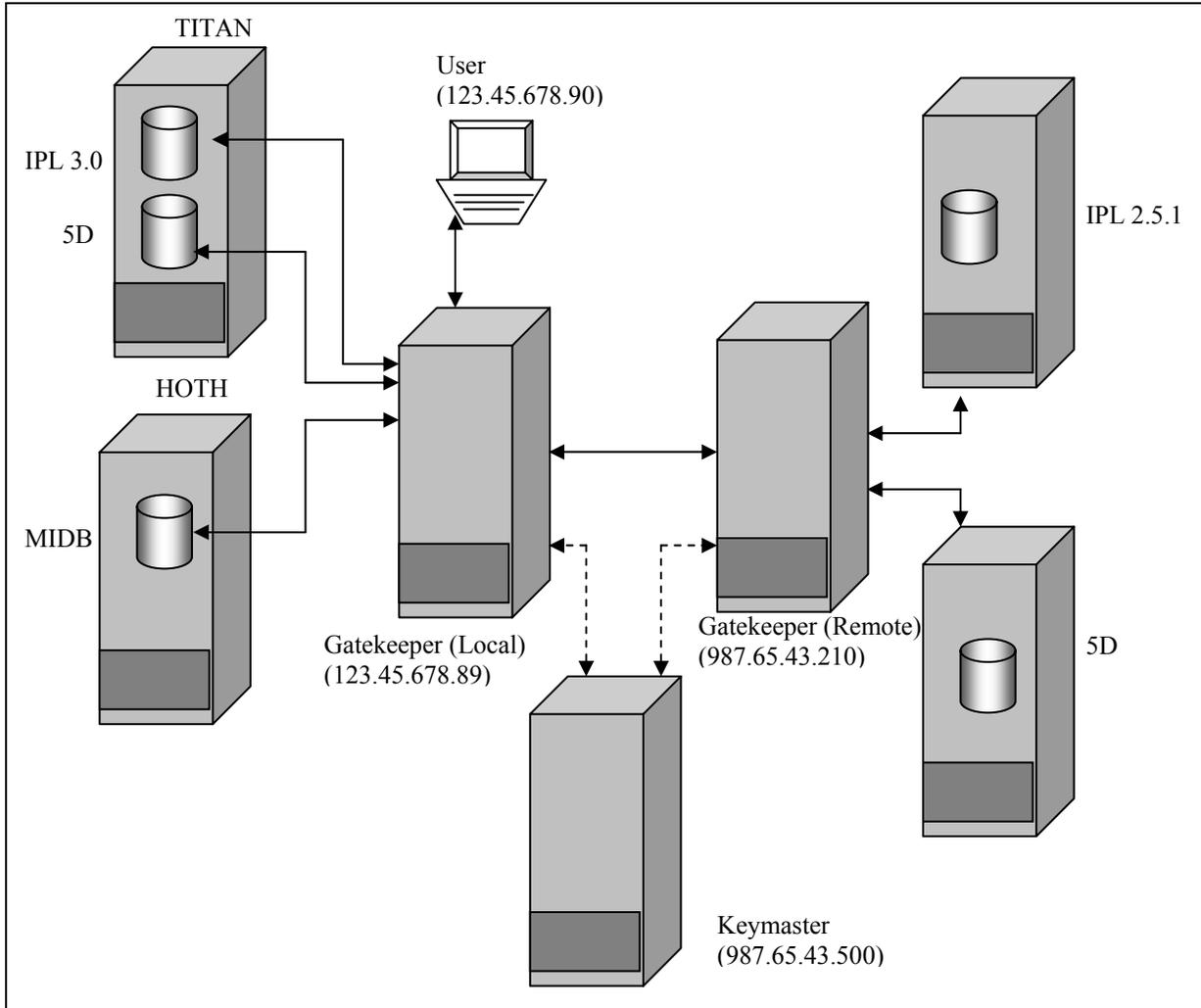


Figure 2.3 – Sample Environment Configuration

When a new Gatekeeper joins the network of Gatekeepers, it must first register itself with the Keymaster. The process begins when the system administrator of the new Gatekeeper calls the Keymaster Distribution Center. From the Keymaster administrator, a unique registration identifier will be generated for the new Gatekeeper. The system administrator of the new Gatekeeper will then enter this registration identifier, the port number of the Keymaster and the Keymaster's IP address into the Gatekeeper's registration screen. At this point the Gatekeeper will then generate a public/private key pair and send the Keymaster a message containing: (1) its public key, (2) the one time registration identifier and (3) a map identifying the sources to be made publicly available (set to Allow Local & Remote Access).

Once the Keymaster has processed the Gatekeeper's registration message, the Keymaster will respond with a message containing: (1) the Gatekeeper's digital certificate (a timestamp, the Gatekeeper's identification and the Gatekeepers public key) encrypted using the Keymaster's private key, (2) a second digital certificate describing the Keymaster, and (3) the world map of all other Gatekeepers and their publicly available (published) sources. The Keymaster will complete the registration process by alerting all other Gatekeepers to the existence of the new Gatekeeper. Once this is accomplished, a periodic background process checks for any map updates and, if necessary, sends each Gatekeeper a new map.

UNCLASSIFIED

In some circumstances it becomes necessary to remove a Gatekeeper from a Keymaster's community. The Keymaster administrator has the ability to remove a Gatekeeper from the community. This removes all global map and certificates from the removed Gatekeeper, and removes all references to that Gatekeeper from the other Gatekeepers' maps.

The next two figures provide example audit records from a successfully completed Gatekeeper registration, a map update, and the unregistration of a Gatekeeper, respectively.

Gatekeeper Logs (daleth)

Login: bswduser IP: 123.45.678.90 Orig.Login
bswduser Gtkpr: 123.45.678.89 Session Key 10484
LOGIN @ 20001204184746 : Successful Login
from daleth Gatekeeper
REGOURGKPR @ 20001204184955 :
Registration Successful, to Gkpr: 987.65.43.500,
Port: 5700, Desc: io Keymaster from daleth
Gatekeeper
LOGOUT @ 20001204185207 : Connection
closed from daleth Gatekeeper

Login: root IP: Orig. Login: Gtkpr: 987.65.43.500
Session Key: 10672
LOGIN @ 20001204184959 : Successful Login
from io Keymaster
LOGOUT @ 20001204185137 : Connect ion
closed from io Keymaster
CONFIGUPDATE @ 20001204185137 :
Configuration Update From io Keymaster, IP
Addr: 123.45.678.90 Was Successful from io
Keymaster

Unregister Gatekeeper

Map Updates

Keymaster Logs (io)

Login: keyadmin IP 987.65.43.500 Orig. Login:
keyadmin Gtkpr: 987.65.43.500 Session Key 672
LOGIN @ 20001204184358 : Successful Login
from io Keymaster
INITREG @ 20001204186438 : Gatekeeper
Registration Started from io Keymaster
INITREG @ 20001204184958 : Gatekeeper
Registration Compoleted For daleth Gatekeeper
from io Keymaster
LOGOUT @ 20001204190507 : Connection
closed from io Keymaster

Login: root IP: 987.65.43.500 Orig Login: root
Gtkpr: 987.65.43.500 Session Key 813
UPDATE_DAEMON @ 20001204184957 :
Update Daemon Started from io Keymaster
UPDATE_DAEMON @ 20001204185013 :
Successfully sent Configuration To (beth
Gatekeeper), with Ref (80aae5f1:987654123) from
io Keymaster
UPDATE_DAEMON @ 20001204185013 :
Successfully sent Configuration To (daleth
Gatekeeper), with Ref (80bac5f4:982434109) from
io Keymaster
UPDATE_DAEMON @ 20001204185138 :
Update_daemon Exiting from io Keymaster

Example 23—Register a New Gatekeeper

Gatekeeper Logs (daleth)

Login: root IP: Orig.Login: Gtkpr: 987.65.43.500
Session Key: 10672
LOGIN @ 20001204184959 : Successful Login
from io Keymaster
LOGOUT @ 20001204185137 : Connection
closed from io Keymaster
CONFIGUPDATE @ 20001204185137 :
Configuration Update From io Keymaster, IP
Addr: 123.45.678.90 Was Successful from io
Keymaster

Unregister Gatekeeper

Map Updates

Keymaster Logs (io)

Login: keyadmin IP: 987.65.43.500 Orig. Login:
keyadmin Gtkpr: 987.65.43.500 Session Key 8960
LOGIN @ 20001205143551 : Successful Login
from io Keymaster
UNREGGKPR @ 20001205143551 : daleth
Gatekeeper Unregistered With Reference of
80bac5f4:982434109 from io Keymaster
LOGOUT @ 20001205143851 : Connection
closed from io Keymaster

Login: root IP 987.65.43.500 Orig. Login: root
Gtkpr: 987.65.43.500 Session Key 813
UPDATE_DAEMON @ 20001204184957 :
Update Daemon Started from io Keymaster
UPDATE_DAEMON @ 20001204185013 :
Successfully sent Configuration to (beth
Gatekeeper), with Ref (80aae5f1:987654123) from
io Keymaster
UPDATE_DAEMON @ 20001204185013 :
successfully sent Configuration to (daleth
Gatekeeper) , with Ref (80bac5f4:982434109)
from io Keymaster

Example 24– Unregistering a Gatekeeper

UNCLASSIFIED

2.5.4 User Maintenance

Broadsword version 3.1 supports the way in which user access and authentication was performed in version 2.0. The site will continue to create user accounts through CSE-SS or AFDI and add privileges/accesses through the Broadsword administration interface.

Existing users can be deleted. Only the user's Broadsword-related files are removed. The user still has a valid UNIX login. To completely remove the user from the system, his or her account must be removed through the tool used to create it. If the account is not removed, the user will still be capable of logging into the Broadsword client and have all the default sources and privileges. This example displays the audit record that is written when a user account has been removed.

```
DELETEUSER @ 20001005150223 : gen_user Deleted As General User from da leth Gatekeeper
```

Example 25 - Removing an Existing User

Once the administrator has created the account using CSE-SS/AFDI/Sun Tools, the administrator can add/remove sources, add privileges or roles, and add the user to a group. For those sources that were configured to have the access flag set to Deny All, the administrator must individually grant a user access to those sources. When the administrator grants this access, an audit record (as shown in the example below) is written.

```
SETUSERDAC @ 20001101025620 : gen_user Allowed Access to IESS at AFRL from saturn Gatekeeper
```

Example 26 - Adding Source Access for a User

Likewise, when the administrator removes access to a given source an audit record (as shown below) is written.

```
SETUSERDAC @ 20001101025727 : gen_user Denied Access to IESS at AFRL from saturn Gatekeeper
```

Example 27 - Adding Source Access for a User

The administrator can add additional privileges to a user account. These privileges include Administrator, ISSO, and producer/catalog ability. The example below shows that the user "gen_user" was given the ability to catalog to an IPL 2.1 system.

```
ADDUSER @ 20001005150223 : gen_user Added To Producer List for Reference  
8092cff8:970611035:IPL21:970616918
```

Example 28 - Adding Role Privilege

UNCLASSIFIED

DELETEUSER @ 20001101032917 : bswduser Deleted From Producer List For Reference
80b40e1e:968967577:IPL:968969809 from saturn Gatekeeper

Example 29 - Removing Role Privilege

In addition to assigning privileges to an individual, the administrator can add the user to one or more groups that already have the appropriate privileges. The following two examples show a user being added and removed from a group, respectively.

ADDGROUPMEMBER @ 20001101033851 : bswduser Added To Group Test from saturn Gatekeeper

Example 30 - Adding a User to the Group 'Test'

DELGROUPMEMBER @ 20001101034300 : bswduser Deleted From Group Test from saturn Gatekeeper

Example 31 - Removing a User from the Group 'Test'

2.5.5 Group Maintenance

Users can belong to one or more groups. Groups allow the administrator to group a set of common accesses and privileges together. By doing this, the administrator does not have to add roles and sources to each user individually. For example, if the site wishes to grant several users the ability to catalog to one or more IPLs, the administrator can create a group, (i.e. DBM with Description of Data Base Managers) and assign one or more producer roles to the group. They can then go under users (under groups) and simply move each user over to become a member of the group. The following example shows the audit record written when the group is created.

ADDGROUP @ 20001006120814 : Added Group DBM, Description: Data Base Manager from Daleth Gatekeeper

Example 32 - Created Group Named 'DBM'

Once the group has been created, sources, roles and users can be assigned. For each source added to the group a SETUSERDAC event will be written. This record will look similar to the SETUSERDAC when a source is added to a specific user. When the group is granted additional roles or privileges, an ADDUSER event record is written and likewise as each user is added to the group under group membership an ADDGROUPMEMBER audit record is written. The example below provides an example of the record that is written when the group description is changed.

MODGROUP @ 20001006120814 : Modified Group DBM, Description: Data Base Managers from Daleth Gatekeeper

Example 33- Modified Description for Group Named 'DBM'

This next example provides an example of an audit record when a user is added to a group.

ADDGROUPMEMBER @ 20001006120814 : testact1 Added To Group DBM from Daleth Gatekeeper

Example 34 - Added User Named 'testact1' to Group Named 'DBM'

Next is an example of an audit record when a user is removed from a group.

DELGROUPMEMBER @ 20001228211835 : testact1 Deleted From Group DBM from Daleth Gatekeeper

Example 35 - Added User Named 'testact1' to Group Named 'DBM'

The following example provides an example of an audit record when the group is deleted.

DELGROUP @ 20001006120814 : Deleted Group DBM from Daleth Gatekeeper

Example 36 - Deleted Group Named 'DBM'

2.5.6 Operations Maintenance

Upon startup, the Gatekeeper cuts an audit record.

GATEKEEPER STARTUP @ 20001006120814 : Gatekeeper Server Startup Using Solaris BSM from daleth Gatekeeper

Example 37 - Gatekeeper Startup

2.6 ISSO Audits

All of the audits presented up to this point were retrieved through the ISSO interface in the Broadsword application. The ISSO can do more than just search the audit logs. The ISSO can also archive the audits to a file on the system, query these archives for specific events, and delete both these archives and the audit records. Each of these events is audited to provide full accountability. This next table provides a list of security audits that are generated in response to ISSO actions.

ISSO Security Audits		
Event Description	Event Name	Configuration
Audit Dump	DUMPAUDIT	All
Delete Audit	DELETEAUDIT	All
Got Audit Report	GETAUDITRPT	All

Table 4 – ISSO Audits

The next four examples give samples of the possible security audits that can be generated by an ISSO using the ISSO tools.

GETAUDITRPT @ 20001005100007 : Audit Report Generated for User gen_user From Date 20001005085925 To Date 20001005095925 For Event QUERY from Daleth Gatekeeper

Example 38 - Query Audit Records

DUMPAUDIT @ 20001101034832 : Audit Report Dumped for User gen_user To File johns_test from saturn Gatekeeper

Example 39- Generate an Audit Archive

GETAUDITRPT @ 20001101035016 : Audit Report Generated From Archive: File(s) johns_test from saturn Gatekeeper

Example 40- Query an Archive Record

DELETEAUDIT @ 20001013113608: Audit Deleted for User gen_user from Daleth Gatekeeper

Example 41- Delete an Audit Record

The first example provides the audit record generated by an ISSO querying the audits. In this case, the query was for any queries performed by gen_user over the last hour. In the second example, the ISSO generated an audit archive for the previous audit record. The third example shows the ISSO querying the archive record johns_test. Now that the admin has verified that the audit archive is complete, the admin deletes the audit record, as shown in the fourth example. DELETEAUDIT records apply to the preceding GETAUDITRPT records. For example:

GETAUDITRPT @ 20001005100007 : Audit Report Generated for User gen_user From Date 20001005085925 To Date 20001005095925 For Event QUERY from Daleth Gatekeeper

GETAUDITRPT @ 20001005100507 : Audit Report Generated for User gen_user From Date 20001005095925 To Date 20001005095925 For Event LOGIN from Daleth Gatekeeper

DELETEAUDIT @ 20001013113608: Audit Deleted for User gen_user from Daleth Gatekeeper

Example 42 - Delete an Audit Record

In this example, the ISSO deleted all LOGIN records for the user gen_user. The QUERY records are still in the database.