Administrator's User 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

UNCLASSIFIED

Version Note

This document is the current version of the Broadsword 3.1 Administrator's Guide, superceding the Broadsword 3.1 Administrator's 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 Overview 2
2 A Standard Gatekeeper 3
3 Keymaster Architecture 4
4 Trusted Transfer Agent Architecture 2
5 Functionality Through the Interface 3
5.1 System Status 3
5.1.1 Daemon Status 3
5.1.2 Set Debug Flags 3
5.1.3 Queue Maintenance 3
5.1.4 System & Log Info 3
5.1.5 Current Users 4
5.2 User & Group Maintenance 4
5.2.1 User Maintenance 4
5.2.2 Group Maintenance 5
5.3 System Statistics 5
5.3.1 Batch Jobs 5
5.3.2 Top Data Sources 5
5.3.3 Top Requests 5
5.3.4 Web Server 5
5.4 System Configuration 5
5.4.1 Data Elements 5
5.4.2 Reset Counter 6
5.4.3 System Parameters 6
5.4.4 Profile Notification 6
5.4.5 Gatekeeper 6
5.4.6 Backside Sources 7
5.4.7 Connected Sites 7
5.4.8 Register Gatekeeper 7
5.4.9 Add Map Data 8
6 Functionality at the Solaris Command Line 9
6.1 Starting Broadsword 9
6.2 Checking Broadsword's Status 9
6.3 Stopping Broadsword 10
6.4 Current Users 10
6.5 Message Queue 11
6.6 Miscellaneous System Checks 11
6.6.1 Logins: 11
6.6.2 System Configuration: 12
6.6.3 Backups and Recommended Patches: 12
6.7 Special Tasks 13
6.8 Changing Broadsword passwords (bswduser, cdimuser, bswd3user) 13
6.9 Changing Soft and Hard Database Limits 14
6.10 Clearing Broadsword's Database if overfull 14
7 Troubleshooting 16
7.1 Error Messages 16
7.1.1 "Cannot connect to…" error message 16
7.1.2 "Zero Hits" message 16
7.2 Common Errors 16
7.2.1 Cannot Log In to Broadsword 16
7.2.2 If nothing else works 17
8 Definitions of Terms 18

Curriculum Schedule

(To be determined)

1 Overview

Every day, people in organizations seek answers to complex questions. In many cases, the answers are difficult to find because they are scattered throughout various data sources. Relevant data often exists in various formats such as text, relational data, and video. It may be quite extensive, may exist on a number of platforms, and may reside across several geographical regions. How does an organization search large quantities of data to make informed decisions?

Air Force Research Laboratory, Rome Research Site has developed an innovative information integration software application called Broadsword that enables an organization to manage heterogeneous, distributed resources. With the assistance of Broadsword, an organization may tie together diverse information resources, perform intelligent searches, and visually display the results in a manner that aids and simplifies the decision making process.

In addition, the Broadsword software is designed to perform these tasks with minimal administrative oversight. Features that ease the administrator's task include:

- Administrator-defined groups to simplify adding roles and access to sources across broad ranges of users with similar need-to-know and job requirements
- Significant amounts of returnable data regarding all aspects of Broadsword's functionality
- A high degree of configurability to the Broadsword interface, allowing adaptation to changing environments and requirements
- An easily expanded architecture able to connect to many different datasources published across the security domain, as well as to query sources on a lower security domain if required.

2 A Standard Gatekeeper

The Broadsword Gatekeeper is the most commonly installed software portion of the Broadsword Architecture. The Gatekeeper is composed of two software elements: the client and the Gatekeeper.

The Broadsword Gatekeeper is the heart of the entire Broadsword architecture. It is a robust, thin layer of software which performs a variety of internal functions, including processing users' queries, auditing, communicating with various sources, interconnection with other Gatekeepers, maintaining system status, and collection/compilation of results.

The Broadsword client is a Web-based Graphical User Interface to access the Gatekeeper and local data sources. It supports multiple roles, which are assigned on an individual user or group basis. Each user's roles automatically include the General User Role (a.k.a. 'Searching' role), and may include one or more of the following: Producer, Managed Producer, Catalog Manager, Administrator, and/or ISSO.

The simplest architecture that Broadsword uses involves a single Gatekeeper, as shown below:

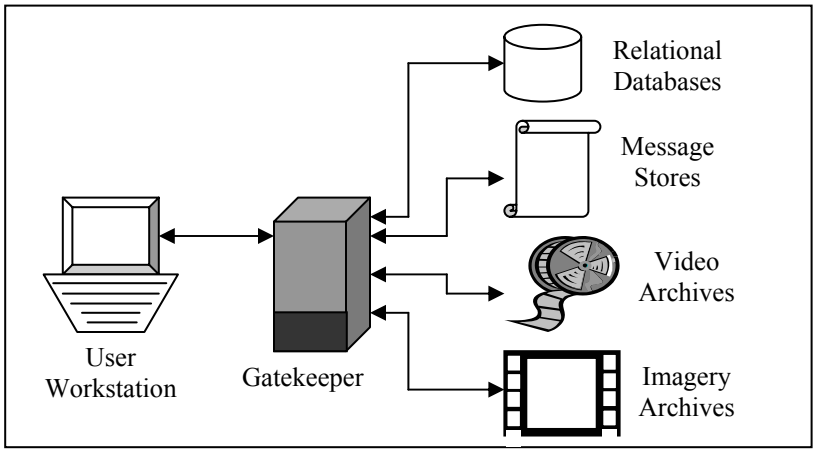

Figure 2.1 - Sample Gatekeeper Architecture

The user will log into the system from the main screen. Based on the user's login, the main screen will be tailored to the roles that have been assigned by the site System Administrator. The general functionality is described in detail in the Broadsword Student's Guide or in the online User's Guide, available on the Broadsword login page. The administration functionality will be discussed after the remaining architectures that Broadsword may use are described.

3 Keymaster Architecture

Sources at a site can be made available to other sites through the Gatekeeper to Gatekeeper connection. Gatekeepers have the ability to communicate with each other and their respective sources as long as each site has registered their Gatekeeper with a Keymaster. The Keymaster manages a list of all Gatekeepers and their sources that have registered with it. During the registration process, a Gatekeeper receives the global map. The global map identifies all other Gatekeepers and sources. Queries and product requests performed between the available Gatekeepers do not involve the Keymaster. Changes in a specific Gatekeeper's configuration are propagated up to the registered Keymaster and are then propagated back down to all other Gatekeepers. The figure below shows the simplest Keymaster architecture with two Gatekeepers and a Keymaster.

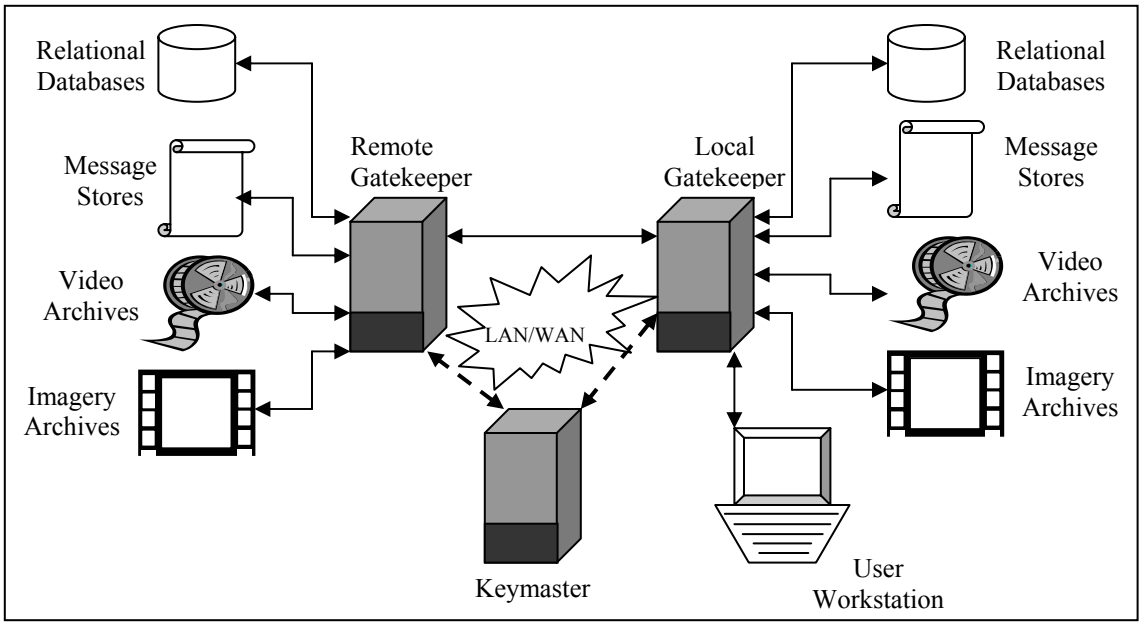

Figure 3.1 - Simple Keymaster Architecture

Please note that the Keymaster is only involved when registering a Gatekeeper, unregistering a Gatekeeper, or passing the map of published (world-accessible) sources between Gatekeepers. All queries, requests for products, etcetera pass from Gatekeeper to Gatekeeper.

This architecture can be set up to handle many more Gatekeepers, with equivalent increases in complexity.

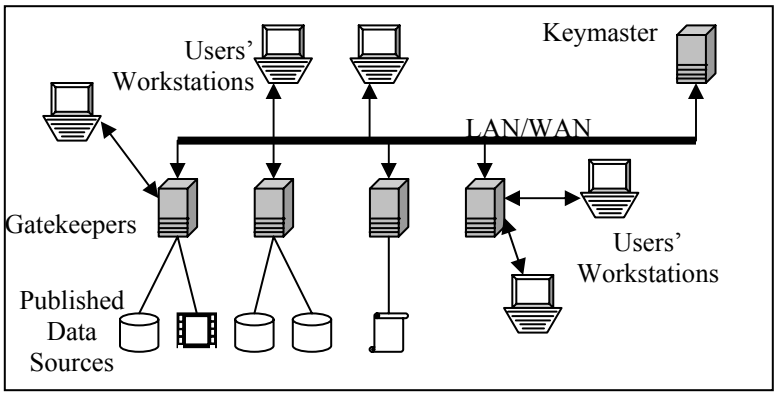

Figure 3.2 – A Complex Keymaster Architecture

4 Trusted Transfer Agent Architecture

The Gatekeeper and Keymaster provide a powerful infrastructure for the interconnection of information sources within a single Community of Interest (COI) and a single security domain. The Trusted Transfer Agent (TTA) brings together this powerful infrastructure and the multiple security level capability provided under the Information Support Server Environment (ISSE) Guard. TTA provides any authorized user logged into the high-side Gatekeeper the ability to access, query, and pull information from a low-side data source connected to a low-side Gatekeeper.

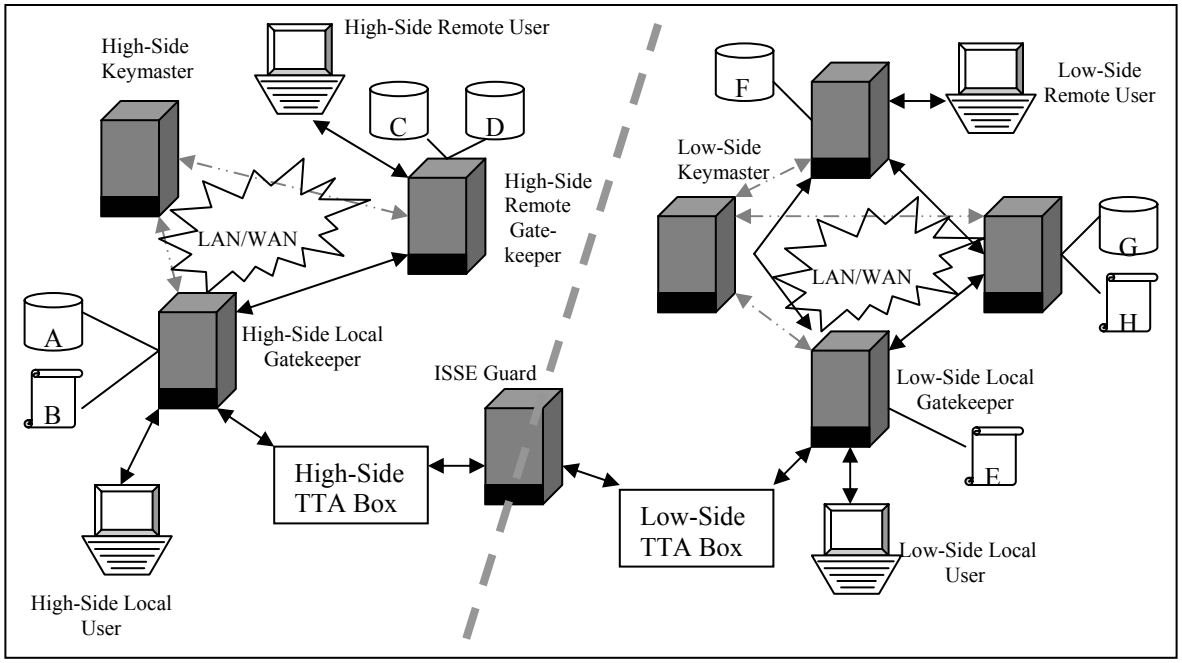

Figure 4.1 - A TTA Architecture Example

In the above example, the four users listed (High-Side Local User, High-Side Remote User, Low-Side Local User, and Low-Side Remote User) will see different sources available. The Low-Side users will both see sources E, F, G, and H. The High-Side Remote User will see sources A, B, C, and D. The High-Side Local User will see sources A, B, C, D, E, F, G, and H, as they can "see" the low-side sources through the TTA functionality.

5 Functionality Through the Interface

As previously mentioned, Broadsword has a significant amount of functionality available through the interface for the administrator. The four primary sections are: System Status, User & Group Maintenance, System Statistics, and System Configuration.

5.1 SYSTEM STATUS

5.1.1 Daemon Status

Daemon Status lists the current state of the core processes of Broadsword. Specifically, Conan, the 5 Gatekeeper processes (gatekeeper.SVR4, gatekeepermrs.SVR4, gatekeepermsl.SVR4, gatekeeperftp.SVR4, and gatekeeperreg.SVR4), jivacron, and any plugins which have been configured in the Administration -> System Config -> Backside Sources page. The remote_plugin.SVR4 will also be listed if the gatekeeper has been registered with a Keymaster, as this is the plugin which connects with other gatekeepers.

Note that this page automatically updates every thirty seconds.

5.1.2 Set Debug Flags

This page contains a large number of flags which can help trace problems with the system. As they do increase the traffic into log files, we recommend that they all be turned off unless the administrator is actively tracing a problem with the system. These flags do not affect the standard audits, just the amount of debugging information sent to log files.

5.1.3 Queue Maintenance

This page lists information regarding the message queue. The message queue is used by the Broadsword client to pass messages between the cgi-bin processes and Conan as needed. If users are not waiting for Broadsword's pages to finish loading, it is possible that messages may be orphaned on the queue. As there is an operating system-derived 4,096-byte limit to the message queue, this can become a problem. If the message queue fills to approximately 3,000 bytes, Broadsword may not be able to function properly, denying logins and/or other functionality.

The Administrator may prevent this from happening by ensuring first that the users have been properly trained to use Broadsword (e.g., they will wait for the interface to finish loading a page before clicking on button(s)), and by periodically monitoring this page to ensure that messages have not been orphaned on the queue. If a message has been orphaned, the Administrator may "pop" the message off the queue. This may be useful to help debug the problem with the assistance of the IDHS Help Desk.

WARNING: It is NOT recommended that the administrator simply remove any messages found on the queue! In the normal course of events, messages WILL be placed on the message queue for short periods of time by the software. It is only when messages are left on the message queue that there can be a problem. Thus, the administrator should double check that the number of messages on the queue remains greater than zero for at least a minute before popping messages off the queue.

Note that this page automatically updates every 10 seconds.

5.1.4 System & Log Info

This page lists several of the log files maintained by the client for debug purposes, their size, and the free space in the Broadsword directory structure (/opt/bswd3.1 or /h/bswd3.1, normally). The administrator also has the ability to purge these log files at this time, but due to system security requirements regarding maintaining a certain amount of log files, it is not recommended that the administrator use this functionality except in an emergency situation.

The administrator may update this page at will with the 'Update' button at the bottom.

5.1.5 Current Users

This page lists the users currently logged into the interface, what their session ID is, and the time/date stamp they logged in at. Note that a user may have a Broadsword window open, displaying data, and not be logged into the system as Broadsword automatically disconnects links with no auditable events after a half-hour. The user's browser may maintain the information on the current page, but when they attempt to access another page they receive a warning stating that their session has been timed out, and are returned to the Broadsword login page.

5.2 USER & GROUP MAINTENANCE

5.2.1 User Maintenance

The User Maintenance screens are designed to add, view, modify, and/or remove privileges from users on a user-by-user basis.

The first page in User Maintenance lists all the users who have either logged into this Broadsword or have been added by an administrator. The administrator may add more users one at a time by clicking in the 'New User' box, entering their username, and clicking the 'Add' button at the bottom of the page. This simply adds that username to the list, assuming that there is a UNIX account with that username accessible by the Broadsword Gatekeeper.

If an account must be removed, the administrator should select that username and click the 'Delete' button. This removes all Broadsword permissions except the General User privileges and destroys any user files stored in the Broadsword functionality. However, it does not prevent the user from logging back in to the Gatekeeper. To prevent this, the Administrator must disable the user's UNIX account, either through the AFDI or CSE-SS CISSO tools.

Alternately, the administrator may select a username from the list and click 'Modify', which takes the administrator to the next page. This page allows the administrator to add/modify/delete the user's roles, source access, and/or group membership.

The roles that are available for each user are General User (which all users have access to), ISSO, and Administrator. If one or more IPL datasources have been configured on the Gatekeeper, there will be a Catalog Manager, a Managed Producer, and a Producer role available for each IPL datasource. This is assuming the installer enabled the production capability when Broadsword was being installed. (See "Enabling Production Capability" below for process to enable such functionality if so desired.) The administrator simply selects the role(s) the user should have according to site rulings and need-to-know and clicks the << button to apply them to the user. Alternately, the administrator may select one or more granted roles and remove them by clicking the >> button.

Sources are handled much the same as roles are, above. When this page opens, the administrator sees all the data sources which have been configured to allow all local and/or all local & remote users to access them. Any sources that have been denied to local users will be in a configuration much like the roles, above. Simply select the denied sources the user needs and click the << button to add them to the user. Alternately, select the sources to be denied and click the >> button to remove them from the user.

Finally, the user may be added to or removed from one or more groups in the same fashion as sources or roles. Each group does have an administrator-defined text string that can be used to specify their usage. More information on groups can be found under the next heading.

5.2.2 Group Maintenance

Groups are an attempt to ease the administrator's configuration headaches. It allows the administrator the ability to set up one or more sets of privileges and add users to that group, instead of having to add each privilege (source or role) to each user.

The first page the administrator sees lists all current groups and their brief descriptions. The administrator may add to this list by entering a name and description and clicking the "New" button at the bottom of the page. Alternately, they may delete a group by selecting the name and clicking the "Delete" button at the bottom of the page.

Finally, the administrator can modify the privileges that the members of the groups have, as well as which users are members of the group, by selecting the group and clicking the "Modify" button at the bottom of the page.

When this happens, the administrator is brought to a new page from which they may add or remove roles, sources, or users from lists containing those currently active within the system, identical to the User Maintenance pages above.

5.3 SYSTEM STATISTICS

5.3.1 Batch Jobs

This page allows the administrator to check to see what batch jobs are currently pending on the system. Batch jobs are used by the users to gather information based on a saved query at some future time. Common usage is for the user to have a standing query that is run against relatively slow datasources once a day, scheduled so that the results are available when they start their shift.

5.3.2 Top Data Sources

This page uses the "Wusage" package to gather information on the sources available through the Gatekeeper. The top ten datasources queried are listed here, along with information on numbers of queries and when the last query was run against the source.

5.3.3 Top Requests

Again using the "Wusage" package, the Broadsword client returns information on the ten top requested products in the available datasources. It includes information on the number of times that each product has been accessed and the timestamp of the last time each was returned.

5.3.4 Web Server

A third aspect of the "Wusage" software offers information on web-based traffic through the Broadsword server. This includes the total number of bytes transferred and history graphs indicating periods of high usage.

5.4 SYSTEM CONFIGURATION

5.4.1 Data Elements

The administrator can use this page to alter the metadata acceptable to Broadsword in pop-down boxes in the short-form query, as well as modifying the help text associated with each element. When the administrator first loads this page, there is a list of all the metadata elements which Broadsword can access either as queryable and/or returnable elements from one or more datasources. When the administrator selects the element they choose to review and/or alter, they are brought to the next screen.

The second screen shows the administrator the rules associated with the data element – the minimum length, the maximum length, and the type of data acceptable (numeric, character, alpha, etc). The administrator may alter the help text associated with the element. Additionally, if there is a list of acceptable values (e.g. – country codes), that list will be displayed and the administrator may add or delete values, as well as their 'user-friendly' associated text. (E.g.- in a list of state codes, the value TX would have the associated text "Texas".)

In a few cases where there are many different values acceptable for a specific data element, Broadsword has categorized them into smaller groupings. These categories were developed based on different organizational needs, and Broadsword ships with all these elements enabled. However, if the administrator or site management require that their users limit their searches to a specific subset of acceptable values, this functionality greatly increases the ease with which it's accomplished.

Note – any changes to these values affect each and every user of this Gatekeeper.

5.4.2 Reset Counter

This page is simply there to allow the administrator to reset the counter on the initial login page.

5.4.3 System Parameters

This page allows the Broadsword administrator to alter the time it takes Broadsword to "give up" on a specific connection attempt. At sites with poor connectivity, this number may need to be greatly increased, while other sites with limited numbers of connections may wish to decrease this number.

Note that this number does not affect the client's browser's timeout. Internet Explorer has a default timeout of 20 minutes for an attempted load, as does Netscape.

5.4.4 Profile Notification

This page allows the Administrator to modify the period of time it takes for the Profile Notification screen to automatically reload. Note that it also lists the Minimum Interval time of 30 minutes, which is not modifiable through the interface.

5.4.5 Gatekeeper

The Gatekeeper page has quite a bit of functionality built into it. The first line defines the human-readable name for this Gatekeeper. We recommend that the Gatekeeper have a meaningful name indicating the site it is located at. Some examples would include "(unitname) Gatekeeper" or "Gatekeeper at (sitename)". This is especially important if the site has published datasource(s), as this is part of the name the remote users will see when they are querying the datasource(s).

Next comes the IP address and port number that this Gatekeeper is running at. This is one place where this information must be changed if the host machine must have its IP address changed. This is discussed more under Special Tasks in the subheading "Changing Broadsword's IP Address".

The next seven fields identify the primary administrator of this Gatekeeper. This is used in several ways through out the Broadsword interface, including shared with other Gatekeepers registered to the same Keymaster, as the email address used to report system problems or feedback from users, and the point of contact for the local users for administration tasks.

Next comes the client idle timeout. This allows the Broadsword administrator to alter the time it takes the Gatekeeper to "give up" on a specific connection to the client. At sites with poor connectivity, this number may need to be greatly increased, while other sites with limited numbers of connections may wish to decrease this number.

The Profile User account is used for the update profile functionality, and needs to be an account on the Broadsword server with its primary Unix group being the bswd group. It is typically configured to be "cdimuser".

The Alternate User Account is used as the initial Broadsword Administration account. It is typically configured to be "bswduser", and needs to have the bswd group be its primary Unix group.

The Gatekeeper Database Name and username are configured during installation and should not need to be adjusted. However, if the administrator needs to access the database through Sybase's isql functionality, this is one place they can come for this information.

The four LDAP fields are not currently supported until the DoDIIS profile and/or AFDI instate an LDAP solution, and therefore should remain untouched.

The Max User Login Failures can be adjusted to match the site's security requirements. It is normally set to 3 logins before the account is locked.

The User Password History, Minimum Number of Special Characters, Minimum and Maximum Password Length, and Dictionary fields are only used for the LDAP functionality, which is not supported in version 3.1

The various Password fields are for the appropriate Account fields previously mentioned.

The LDAP Bind password is only used for the LDAP functionality, which is not supported in version 3.1

NOTE: After any of these fields have been changed, the Administrator must stop and start Broadsword to prevent a mismatch between the client and the gatekeeper.

5.4.6 Backside Sources

Another large set of functionality is included under Backside Sources. This is how the Gatekeeper is configured to work directly with one or more datasource(s). When Broadsword is initially installed, it has no datasources configured. Once datasource(s) are configured, there will be one or more blue links in the rightmost column. These links bring the Administrator to the specific information for each specific datasource.

Additionally, the Administrator may remove one datasource at a time by selecting it and clicking the 'Delete' button at the bottom of the page.

Note that each type of datasource has needs for different information to make the connection. These are covered in more detail in the Trusted Facility Manual for Broadsword.

5.4.7 Connected Sites

Once the system has been registered with a Keymaster (see the next heading for information on how to do this), the page lists all the other Gatekeepers that are registered to the Keymaster. If the Administrator wishes, they may allow access to these sites to the general users by clicking the checkbox. As each checkbox is selected, any published sources from that site are listed with their own checkboxes. To allow access to the source, simply select the appropriate checkbox(s).

5.4.8 Register Gatekeeper

This page allows the Administrator to connect with a Keymaster. This is a time-sensitive process, requiring a near-real-time communications connection to the Keymaster Administrator.

The local Gatekeeper's Administrator must input the Keymaster IP address and port number as the Keymaster Administrator initializes their system to accept a Gatekeeper initial connection. As soon as the Keymaster is capable of accepting a Gatekeeper's registration request, it generates a one-time key. This key must be communicated - by secure means - to the Gatekeeper's Administrator, who enters it into the third field. The Gatekeeper then initializes a SSL connection to the Keymaster and passes along its information. In return, it gets a map to the published sources and information on the other Gatekeepers connected to the

Keymaster. It also will get an update message every 4 hours with changes in the published sources and registered Gatekeepers, if there are any.

5.4.9 Add Map Data

The Administrator can add any of the standard NIMA map formats (CADRG, CIB, DBDB5) to the Broadsword graphical map functionality through this screen. The user indicates the location that the information can be found at (typically /cdrom/cdrom0 or equivalent), the format of the information, and the unique title of the information. The destination directory is where the information will be copied to and accessed by the Broadsword system, and should remain the pre-filled default unless you've gained the IDHS help desk's assistance to move the information elsewhere.

The next page confirms that the information is where and what you told the interface, double checks that you have enough free storage, and asks you to confirm your choice. If the Administrator approves, the system will ingest the information. As this can be a fairly processor-intensive task, it is recommended that it be done off primary duty hours.

6 Functionality at the Solaris Command Line

6.1 STARTING BROADSWORD

Broadsword, as typically installed, should automatically start on boot. However, if for some reason the administrator needs to manually start Broadsword, it is a simple task.

Log into the Broadsword server and open a shell process, then follow the next section

```
% su - root
        (the root password will need to be entered at this point)

# cd /opt/bswd3.1/scripts

# ./startserver
        (answer "Y" to both questions.)
```

Example 6.1 – Starting Broadsword

After approximately 90 seconds, Broadsword should respond back with the output of a 'whoserver' script (see Checking Broadsword's Status, next).

6.2 CHECKING BROADSWORD'S STATUS

To determine from the command line if Broadsword is fully operational, the administrator should follow these steps:

Log into the Broadsword server and open a shell process following site-specific procedures.

```
% su - root
        (the root password will need to be entered at this point)

# cd /opt/bswd3.1/scripts

# ./whoserver
/opt/bswd3.1/bin/conan:                    running
/opt/bswd3.1/bin/gatekeeper.SVR4           running
/opt/bswd3.1/bin/gatekeeperftp.SVR4        running
/opt/bswd3.1/bin/gatekeepermrs.SVR4        running
/opt/bswd3.1/bin/gatekeepermsl.SVR4        running
/opt/bswd3.1/client/bin/jivacron           running
/opt/bswd3.1/bin/ipl25_plugin.SVR4         running
/opt/bswd3.1/bin/midb_plugin.SVR4          running
/opt/bswd3.1/bin/meta_plugin.SVR4          running
/opt/bswd3.1/bin/remote_plugin.SVR4        running
```

Example 6.2 – Checking Status

If one or more process is not operational, the "**running**" will be replaced with "**not running**". Additionally, the list of plugins that your system runs will vary depending on whether or not it is registered with a Keymaster (the 'remote plugin') as well as what data sources are configured in the Administration -> System Config -> Backside Sources page.

6.3 STOPPING BROADSWORD

It is recommended that, whenever possible, Broadsword be manually halted before system shutdown. There are two slightly different procedures used, depending whether or not the database is shared or not. The determination to share a database or not is made during the Broadsword installation.

If the database is shared, use the following procedure from within a shell process on the Broadsword server.

```
% su - root
        (the root password will need to be entered at this point)

# cd /opt/bswd3.1/scripts

# ./stopserver
        (answer the questions "N", "N", "Y", "Y")
```

Example 6.3a – Stopping a Shared-Database Broadsword

After approximately 90 seconds the system should return to the shell prompt.

Alternately, if the database is not shared, use the following procedure from within a shell process on the Broadsword server.

```
% su - root
        (the root password will need to be entered at this point)

# cd /opt/bswd3.1/scripts

# ./stopserver
        (answer the questions  "Y", "Y")
```

Example 6.3b – Stopping a Stand-Alone Broadsword

After approximately 90 seconds the system should return to the shell prompt.

6.4 CURRENT USERS

There are several ways to determine the number of users currently connected to Broadsword from the UNIX prompt. The simplest is done from within a shell prompt, and does not require root privilege:

```
% w | grep gkp
bennerj    gkp1    1223     11:05m        3      3   /opt/bswd3.1/bin/gatekeeper.SVR4
bswduser gkp2    2233     11:10am       2      3   /opt/bswd3.1/bin/gatekeeper.SVR4
tester     pty4    4110     12:20pm       3      2   grep gkp
```

Example 6.4 – Checking Users

Note that the user 'tester' is not actually logged into the Gatekeeper. Instead, the second and last columns should both show that the last line isn't a log-in to the Gatekeeper, but rather the process which determined which users ARE logged in.

6.5 MESSAGE QUEUE

As previously stated, the message queue may end up with messages orphaned within it. In the worst situations, this may even prevent log-in to Broadsword. The administrator may either stop and start the Broadsword server, or they may attempt to clear the message queue at the UNIX level and then restart Broadsword.

To clear the message queue, the following steps will need to be followed in a shell process on the Broadsword server:

```
% su - root
        (the root password will need to be entered at this point)

# ipcs -qa
IPC status from <running system> as of Mon Dec 14 10:03:40 2001
T      ID       KEY        MODE     OWNER     GROUP    CREATOR   CGROUP   CBYTES
QNUM  QBYTES  LSPID  LRPID   STIME   RTIME   CTIME
q      11     0x1234abcd  –Rrw-rw-rw-   root        root       root        root        3125
15        4096      1234     2345     7:40:20   6:51:01  12:13:54

        (note that the information has wrapped around the screen. IE – every two screen lines is one entry)
        (if the "CBYTES" is greater than 3,000 – in this case, 3125 bytes – then the message queue is
        excessively full.)

# ipcrm -q 11
```

Example 6.5 – Clearing the Message Queue

Remember, as well, that it is normal for messages to appear on the message queue temporarily. This process should only be followed when it has been determined that the message queue is definitely over full over a period of several minutes and several "ipcs –qa" checks.

Finally, once this has been done, the system will need to be restarted, as per the previous instructions.

6.6 MISCELLANEOUS SYSTEM CHECKS

The following commands may be of use to ensure the security of the system. We include them here as a grab-bag of techniques which may or may not apply to your situation, but have shown themselves to be of value at some Broadsword sites.

6.6.1 Logins:

- To determine which accounts are currently logged in to the system, use the following command:

  ```
  % w | more
  ```

  This particular command is useful in that it also differentiates between a standard login session (it will list as console or 'ptty' followed immediately by a number) or those authenticated and currently logged into the Gatekeeper (which will list 'gkp' followed immediately by a number).

6.6.2 System Configuration:

- We recommend that the Administrator periodically check the disk usage on the system:

```
% df -k
```

Ensure that no partition is approaching 100% usage. It is recommended that this check be done periodically, and the output be logged for future reference to determine if certain filesystems are approaching a dangerous size.
Additionally, the command

```
% du -dsk * | sort -n
```

will list the current directory's contents with sizes, including the sizes of any sub-folders.

6.6.3 Backups and Recommended Patches:

Due to Solaris being an operating system constantly in development by Sun, Inc, it is recommended by the Broadsword office that the Broadsword server periodically have the latest patch clusters applied. If the site has direction regarding patch clusters, please follow that, but if not, we recommend that patches be updated at least twice a month.

The patch clusters are available via anonymous FTP from ftp.sunsolve.sun.com, or through the web at http://sunsolve.sun.com. The ISMC also maintains reasonably recent patch clusters both at the Intelink and Intelink-S levels off of their web site, either http://www.ic.gov or http://www.ismc.sgov.gov.

We recommend that the Administrator back up the Broadsword server, as per the suggestions in the Broadsword Installation Guide or Trusted Facility Manual. After the backup has been completed, it would be a near-optimal time to download the patches and apply them as little if any data could be lost due to problems with patches – an extremely rare occurrence, but one to guard against regardless.

6.7 SPECIAL TASKS

This section is still in development at this time.

6.8 CHANGING BROADSWORD PASSWORDS (BSWDUSER, CDIMUSER, BSWD3USER)

In accordance with site policy, it may be required to change passwords required for the Broadsword system's functionality. These accounts are created during system installation, and are bswduser, bswdreg, and cdimuser accounts at the Unix level, and the bswd3user account at the Sybase level.

To change the Unix-level accounts, we recommend that the administrator follow these steps:

- change the passwords through the Administrator functionality (Administration -> System Config -> Gatekeeper, as described above)
- stop the Broadsword processes (as described above)
- change the passwords at the Unix level to those changed in the Gatekeeper page by the method required by the site
- restart the Broadsword processes (again, as described above).

To change the Sybase account, we recommend the administrator follow these steps:

- changes the password through the Administrator functionality (Administration -> System Config -> Gatekeeper, as described above)
- stop the Broadsword processes (as described above)
- change the password within Sybase (as follows)

```
% su - sybase
```
Password:

(the 'sybase' Unix account password will need to be entered at this point unless the user is currently root)

```
% setenv SYBASE /opt/SYBASE
```
(depending on your site's configuration, this may be a different directory other than /opt/SYBASE. You should be able to determine this by checking the /opt/bswd3.1/etc/bswd_settings file and searching for the line that starts with ' ')

```
% hostname
HOSTNAME
```
(the system responds with the system's hostname)

```
% setenv DSQUERY BSWD_HOSTNAME_SVR
```
(where "HOSTNAME" is replaced by the system's hostname as reported by the previous command)

```
% $SYBASE/bin/isql -Ubswd31_user
```
Password:

(the system will prompt you for the old bswd31_user password)

```
1> sp_passwd,oldpassword,newpassword
2> go
```
(where oldpassword is the last password and newpassword is what you wish to change the password to. Note that the password must start with an alphabetic character, and that there are no spaces on the line.)

```
1> exit
%
```
(the task has been successfully completed at this point)

Example 6.8 – Changing the bswd31_user Password

6.9 Changing Soft and Hard Database Limits

Broadsword has the capability to send email warning the administrator of the site if the audit logs are too full. By default, this is set to warn the administrator at 90% full and prevent further access at 98% full, also called a 'soft' limit and a 'hard' limit, respectively. While this configuration should work on any supported system, those with massive audit requirements or those with somewhat weaker processors may wish to limit this further to speed audit functionality.

This can be done by editing the file /opt/bswd3.1/etc/server_env_vars and adding two lines: (the numbers used are examples)

```
setenv BSWD_DB_FULL_THRESHOLD 75
setenv BSWD_DB_THRESHOLD 50
```

Example 6.9 – Lines to add

This file should have ownership of bswduser:bswd and have permission of 644.

If the file does not contain either of these lines, the system will assume the soft, 'warning' limit is set to 90% and the hard, preventative limit is set to 99%.

The above example 6.9 assumes that you want email sent to the administrator when the audit database is 50% full and the database to stop accepting connections when it is 75% full, preventing use of Broadsword at that point.

Note also that the email sent will be to the address given during installation for the Broadsword Administrator, and that this address may be changed on the Gatekeeper Config page (Administration -> System Config -> Gatekeeper), as discussed under that page's description previously in section 5.4.5.

These changes require a stopserver and startserver to be run to take effect, as described in sections 6.3 and 6.1, respectively.

6.10 Clearing Broadsword's Database if overfull

Broadsword adheres to the security premise of "By default, secure." What this means is that if the system is unable to retain its security, it shuts down. One way this may happen is if the auditing logs become full. If we are unable to write auditing information, we prevent any use of the application.

The system administrator should use the procedure in section 6.9 to reset the hard limit to at least one percent higher if possible, then using the interface to archive the information properly. This procedure is included only for emergency usage.

To re-enable the system, the administrator must remove the information in the audit logs. We recommend that the administrator archive this information as well, but there are situations where it is necessary to bring Broadsword back up swiftly and thus we will address how to simply remove the audit information as well. Please note that this WILL cause loss of log information, and therefore should not be attempted unless the situation requires it.

```
% su - sybase
        (the sybase account's password may need to be entered at this point)

> echo $DSQUERY $SYBASE
BSWD_sitename_SVR /opt/SYBASE
```

(doublecheck that the /opt/SYBASE directory exists, and that in the (in this case) /opt/SYBASE/interfaces file there is a 'BSWD_sitename_SVR' entry, or whatever is appropriate. If these are incorrect, find the correct values and set them as follows:
>setenv SYBASE /opt/SYBASE11.9.2
>setenv DSQUERY BSWD_SVR

```
> $SYBASE/bin/isql -Usa
```
(at this point, the sa password will need to be entered)
```
1> use bswd31_db
2> go
1> trunc table EVENT_AUDITS
2> go
1> trunc table EVENT_AUDITS_DETAILS
2> go
1> exit
>logout
%
```

Example 6.10 – Destructively Emptying the Broadsword Sybase Audits

7 Troubleshooting

7.1 ERROR MESSAGES

7.1.1 "Cannot connect to…" error message

This message may appear in the summary table on the results page, as generated by a query. This is an error message indicating that the Gatekeeper was unable to reach the datasource. This can be for several reasons, including but not limited to:

- The datasource being turned off, temporarily or otherwise.
- The network between the Gatekeeper and the datasource having errors, either temporary or otherwise.
- The appropriate plugin not being running on the Gatekeeper.

Of these, only the last one may be easily troubleshot. Follow the above procedure to "Check Broadsword's Status" and pay particular attention to the plugins. If the appropriate plugin is not running (IE, if you're having problems reaching an MIDB datasource and the midb_plugin.SVR4 process is showing as **Not Running** when the administrator runs the /opt/bswd3.1/scripts/whoserver command), the following steps should be performed:

1. Check for core files. Core files are usually left behind by the operating system if a process errors out. As root on the machine, type

   find /opt/bswd3.1/ -name core –type f –print | xargs ls –al

For each file that this turns up, check to see if the file date is since the last time the system was checked and found to be running properly. If so, make a copy of that file. While in the directory of the file in question, type the following command:

mv core OldCore.TodaysDate

2. Try to start the process with the startserver command. That is, as root, type

   /opt/bswd3.1/scripts/startserver

Answer 'y' to the two prompts, and the system will try to restart the failed plugin. The system will automatically run a whoserver command after starting. If the process still shows as being down, please contact the IDHS Help Desk at COM (315)330-4347 or CONUS DSN 587-1716 for further assistance.

3. Be certain to double check the process later in the day with the whoserver command.
4. If this is repetitious, please try to troubleshoot with your users and determine where in the Broadsword functionality this is erroring out, and contact the IDHS Help Desk.

7.1.2 "Zero Hits" message

This message may appear in the summary table on the results page generated by a query. It is actually not an error message – quite the opposite, it is a report that Broadsword was able to access the datasource normally, but that the datasource in question did not have data pertaining to the query generated.

The reason this is included here is that many users have been known to misread this message as an error, and to report it as an error to their local Administrator.

7.2 COMMON ERRORS

7.2.1 Cannot Log In to Broadsword

The typical order that the Broadsword System Administrators have developed to determine the problem is as follows:

- If the user cannot see the login page:
  - **A)** Determine that the user is accessing the right web address.
  - **B)** Try to connect to the same web address. If you are able to, it is probably likely that the user may have mistyped the address.
  - **C)** If you are unable to connect, telnet to the Broadsword server (assuming you are the administrator for that Gatekeeper) and check to see if Broadsword is running (See "Checking Broadsword's Status", above). If it is running properly, please contact a local network administrator to verify network connectivity between the user's workstation and the Gatekeeper. This connectivity should

include HTTP, SSL, and FTP access, and should doublecheck to see if there may be an issue with firewall(s).

D) If there is appropriate connectivity, please contact the IDHS Help Desk for additional assistance.

- If the user can see the login page, but cannot log in:
  - **A)** By logging into the Broadsword Gatekeeper at the UNIX level, check to see if the user's account has been locked using system standard techniques. (For AFDI or CSE-SS, the cisso account and the isso pallette contain this functionality. See the appropriate software manual(s) for specific direction on how to accomplish this.) If the user's account has been locked, confirm with the user that they tried and failed to log in at least 3 times in a row. If this is not the case, check with your security manager for local policy.
  - **B)** If the user's account is not locked, run a whoserver command as root to ensure that the processes are running as expected.(See "Checking Broadsword's Status," above). If they are running properly, yet the user is still having difficulty, please contact the IDHS Help Desk for additional assistance.

- If the user logs in, but is 'dumped' out of their browser Broadsword session:
  - **A)** Check to ensure that the user didn't leave the system unused for the timeout period (typically 30 minutes).
  - **B)** Check to ensure the Broadsword processes are running properly (See "Checking Broadsword's Status," above.)
  - **C)** Ask the user to repeat the actions just prior to their being 'dumped' from the system. Observe the results. If the user is 'rushing' the system, not waiting for the page to fully load, it is a known problem with Broadsword 3.1 that this can cause the system do 'dump' a user and leave messages stuck on the message queue. Please ask the user to wait for the page to load and double check the message queues (section 5.5, "Message Queues", above).
  - **D)** If the problem is intermittent, but occurs more than once, please open a helpdesk ticket with as much detail as possible with the IDHS Help Desk.

7.2.2 If nothing else works

Contact the IDHS Help Desk at (315)330-4347 or CONUS DSN 587-4347 for additional support.

8 Definitions of Terms

Administrator 1) The people authorized and required to fulfill the duties listed and described in DCID 6/3.

2) A specific role within Broadsword with capability to configure, maintain, and troubleshoot the software. Described in this document and the Trusted Facility Manual.

AFDI – Air Force DoDIIS Infrastructure. A program designed to secure computers and enhance their capabilities with a standardized set of software utilities. The descendant of the CSE-SS program.

Broadsword – 1) A program designed to offer the user a single interface to multiple disparate datasources. Consists of the Broadsword client, Gatekeeper, and potentially the Keymaster and/or Trusted Transfer Agent software.

2) Specifically, the client portion of the Broadsword effort, as differentiated from the Gatekeeper.

Catalog Manager – A specific role within Broadsword with the ability to review Public and Managed cataloging queues and validation rules for production, all versus a specific IPL datasource.

Cataloging – The process of preparing an electronic product for storage in an IPL datasource.

conan – The core process to the client portion of the Broadsword effort. It is a GUI-driven interface that expands the basic capabilities built into the Gatekeeper.

CSE-SS – A program designed to secure computers and enhance their capabilities with a standardized set of software utilities. The precursor to the AFDI program.

datasource – One of the repositories of information which Broadsword accesses. These may be databases, unsorted stores of information, or some combination thereof.

Gatekeeper – 1) The middleware portion of the Broadsword software which provides a single interface to various datasources for query, retrieval, and product request/delivery. It also provides a single point in which all users are authenticated and all actions audited.

2) A machine running an instance of the Broadsword middleware.

Group – 1) A Solaris operating system capability to gather together users who need access to certain software capabilities. All Broadsword users need to be part of the 'bswd' group, created during the installation of the Broadsword software. Also referred to as an "Unix-level group.

2) A collection of Broadsword users with identical access needs. Used to simplify the Administrator's task by reducing the amount of information that needs to be entered while creating a new account. Each group can consist of rights to access specific datasources and/or roles. Also referred to as a "Broadsword-level group."

IDHS Help Desk – The help desk available for Broadsword questions and problems not answered in the documentation. Phone (315) 330-4347 or DSN 587-4347.

ISSE – Information Support Server Environment. A program that acts as a multiple-security layer (MSL) gateway.

ISSO – Information System Security Officer. 1) The person(s) authorized and required to fulfill the duties listed and described in DCID 6/3.

2) A specific role within Broadsword with capabilities to audit Broadsword transactions, as well as archive audit information. Covered in the Broadsword Trusted Facility Manual and the ISSO User's Guide.

Keymaster – 1) Software designed to connect multiple Gatekeepers. Among other capabilities, it acts as a custom X509 certificate authority and an available-source map transmission facility. There is one Keymaster per security domain.

2) A machine running an instance of the Keymaster software.

Managed Producer – A specific role within Broadsword with the ability to prepare products for cataloging after passing through the Managed Queue for a specific IPL datasource.

Plugin – The specific module of Broadsword's Gatekeeper code which connects to external resources, be it datasource(s) and/or other Gatekeeper(s). Each translates between the format used within Broadsword and that particular datasource's format.

Producer – A specific role within Broadsword with the capability to prepare products for cataloging directly into a specific IPL datasource.

Queue – 1) The Solaris mechanism used in the Broadsword client to pass messages between separate internal processes. It can become "jammed" with information if there are system problems or if the users are not waiting for Broadsword pages to fully load.

2) The storage location for IPL Managed or Public products, as configured in the Administration -> System Config -> Backside Sources page.

Role – A specific set of functionality logically grouped together. The various types of roles available through the Broadsword interface are General User, Administrator, and ISSO. If the site chooses, they may also enable the Producer, Managed Producer, and Catalog Manager roles during installation of the Broadsword software.

Sybase – a relational database COTS product used by the Gatekeeper to maintain auditing information.

Trusted Transfer Agent (TTA) An effort jointly developed by Broadsword and ISSE to leverage both programs' strengths. TTA currently allows users at a higher security level to query and retrieve information from datasource(s) at a lower security level without a man in the loop.