



SYSTEM INSTALLATION & MAINTENANCE GUIDE FOR BROADSWORD VERSION 3.0



Prepared for:

497th INTELLIGENCE GROUP
INTELLIGENCE SYSTEMS DIRECTORATE (497IG/IND)
BOLLING AIR FORCE BASE
WASHINGTON, DC 20332-5000

Prepared by:

Air Force Research Laboratory, Rome Research Site
AFRL/IFED
32 Brooks Road
Rome, NY 13441-4114

January 2001

Points of Contact

Broadsword Program Office:

Unclassified email: strongc@rl.af.mil

Commercial Phone: (315) 330-4429

DSN: 587-4429

<http://www.if.afrl.af.mil/bsword>

Air Force POC: 497IG

Unclassified email: mishawkd@emh-497ig.bolling.af.mil

Commercial Phone: (202) 404-1780

DSN: 754-1781

Configuration Management:

Commercial Phone: (315) 330-2723/4209

<http://www.if.afrl.af.mil/programs/cm>

Mailing Address and Fax Number: AFRL/IFED

32 Brooks Road

Rome, New York 13441

37-3.0-SYIMG-01 01-G0
09 January 2001

Phone: (315) 330-4429 Fax: (315) 330-3913

This page left intentionally blank

POINTS OF CONTACT.....	I
FORWARD.....	VIII
CHAPTER 1 INTRODUCTION	1
1.1 INSTALLATION OVERVIEW	1
1.2 SYSTEM DESCRIPTION	3
1.2.1 <i>Gatekeeper</i>	4
1.2.1.1 User Services	4
1.2.1.2 Administration Services	5
1.2.1.2 Administration Services	6
1.2.1.3 Security Audit Review	7
1.2.2 <i>Keymaster</i>	8
1.2.3 <i>Access and Authentication Module (AAM)</i>	10
1.2.3.1 LDAP Replication	12
1.2.4 <i>The Broadsword Client</i>	13
1.2.4.1 General.....	14
1.2.4.2 Searching	14
1.2.4.3 Administration.....	16
1.2.4.4 ISSO	16
CHAPTER 2 GETTING STARTED.....	20
2.1 SERVER REQUIREMENTS.....	20
2.2 PREPARING YOUR SYSTEM.....	21
2.3 SITE CONFIGURATION WORKSHEET	24
CHAPTER 3 INSTALLATION.....	30
3.1 LOADING THE SOFTWARE AND STARTING THE SETUP SCRIPT	30
3.2 PROVIDING INSTALLATION CHOICES.....	34
3.2.1 <i>Providing CD-ROM Registration Information</i>	34
3.2.2 <i>Determining the Import Preference</i>	35
3.2.3 <i>Database Configuration</i>	35
3.2.3.1 Creating a New Data Server	36
3.2.3.2 Sharing an Existing Data Server.....	38
3.2.4 <i>Gatekeeper Configuration</i>	40
3.2.5 <i>Client Configuration</i>	41
3.2.6 <i>LDAP Configuration</i>	42
3.2.7 <i>POC Configuration</i>	43
3.3 CONFIRMING INSTALLATION CHOICES.....	44
3.4 INSTALLATION PROGRESS.....	46
3.5 INSTALLATION VERIFICATION.....	49
CHAPTER 4 SYSTEM CONFIGURATION.....	52
4.1 BACKSIDE SOURCES	52
4.1.1 <i>Backside Sources (both methods)</i>	57
4.1.2 <i>Pull to Destination</i>	57
4.2 GATEKEEPER CONFIGURATION	57
4.3 SYSTEM PARAMETERS.....	58
4.3.1 <i>Reset Home Page Access Counter</i>	59
4.3.2 <i>Set System Parameters</i>	59
4.3.3 <i>Set E-Mail Notification Parameters</i>	59
4.4 REGISTER GATEKEEPER.....	60
4.5 CONNECTED SITES.....	61
4.6 DATA ELEMENTS.....	62
4.7 ADD MAP DATA.....	66

CHAPTER 5 CLIENT REQUIREMENTS	67
5.1 HTML BROWSERS.....	67
5.2 IMAGE VIEWERS.....	68
5.3 SHOCKWAVE-FLASH PLAYERS.....	69
5.4 FTP SERVERS.....	69
CHAPTER 6 USER AND GROUP MAINTENANCE.....	70
6.1 USER MAINTENANCE IN A NON-ACCESS & AUTHENTICATION MODULE ENVIRONMENT	70
6.2 USER MAINTENANCE IN AN AAM ENVIRONMENT	73
6.3 ADDING/REMOVING SOURCES.....	77
6.4 ADDING/REMOVING ROLES.....	78
6.5 ADDING/REMOVING GROUPS.....	79
6.6 ADDING, MODIFYING, AND DELETING A GROUP	80
6.7 ADDING/REMOVING SOURCES.....	85
6.8 ADDING/REMOVING ROLES.....	85
6.9 ADDING/REMOVING USERS.....	85
CHAPTER 7 SYSTEM STATUS	90
7.1 DAEMON STATUS.....	90
7.1.1 Possible Problems/Solutions.....	92
7.2 QUEUE MAINTENANCE	92
7.2.1 Possible Problems/Solutions.....	93
7.2.2 Pop Message Info	94
7.3 SET DEBUG FLAGS.....	95
7.4 SYSTEM AND LOG INFORMATION.....	96
7.5 CURRENT USERS.....	97
7.6 DATABASE THRESHOLDS.....	98
7.6.1 Level-One Threshold	98
7.6.2 Level-Two Threshold.....	99
CHAPTER 8 SYSTEM STATISTICS	101
8.1 BATCH JOBS.....	101
8.2 TOP DATA SOURCES.....	102
8.3 TOP REQUESTS.....	102
8.4 WEB SERVER STATISTICS.....	103
CHAPTER 9 ISSO.....	108
9.1 AUDIT LOG MAINTENANCE AND ARCHIVING LOGS.....	108
9.2 UNDERSTANDING THE AUDITS.....	110
9.2.1 User and Producer Audits.....	111
9.2.1.1 Logging into the Gatekeeper.....	111
9.2.1.2 Performing Queries on Local Sources	112
9.2.1.3 Performing Product Requests on Local Sources	113
9.2.1.4 Cataloging a Product.....	114
9.2.1.5 Changing Passwords (LDAP Gatekeepers Only).....	114
9.2.1.6 Logging out of the Gatekeeper	116
9.2.2 Putting It All Together	116
9.2.2.1 An Example with Only Local Requests	116
9.2.2.2 What do the Audits Say?	118
9.2.2.3 An Example with Local and Remote Requests	119
9.2.3 Administrative Audits - Configuring and Maintaining the System.....	122
9.2.3.1 Gatekeeper Maintenance	122
9.2.3.2 INK Maintenance.....	124
9.2.3.3 Global Registration/Maintenance	125
9.2.3.4 User Maintenance.....	129
9.2.3.5 Group Maintenance	131
9.2.3.6 Operations Maintenance.....	132

9.2.3.7 Performing Regional User Maintenance 132
9.2.4 ISSO Audits 132

APPENDIX A - PLUGIN WORKSHEETS.....A-1

- AIR FORCE WEATHER (WX)
- AIR ORDER OF BATTLE DATABASE (AODB)
- AUTOMATED MESSAGE HANDLING SYSTEM (AMHS)
- COMMERCIAL SATELLITE IMAGERY LIBRARY (CSIL)
- IMAGE PRODUCT LIBRARY (IPL)
- IMAGERY PRODUCT LIBRARY VERSION 2.0 (IPL20)
- IMAGERY EXPLOITATION SUPPORT SYSTEM (IESS)
- INFORMATION EXTRACTION TOOL (IET)
- INTELINK (HYDRA)
- INTELINK (METASEARCH)
- INFOSPHERE MANAGEMENT SYSTEM (ISM)
- MILITARY EQUIPMENT PARAMETRIC AND ENGINEERING DATABASE (MEPED)
- MILITARY INTEGRATED DATA BASE (MIDB)
- NPIC DISSEMINATION SYSTEM (NDS)
- SPACE DATA BASE (SDB)

APPENDIX B – TEST CASES.....B-1

- BROADSWORD V3.0, GENERAL FUNCTIONS TESTING
- BROADSWORD V3.0, QUERY-LOCAL & REMOTE SOURCES
- BROADSWORD V3.0, SHOPPING CART & ORDER STATUS TESTING
- BROADSWORD V3.0, SAVED & BATCH QUERIES TEST
- BROADSWORD V3.0, LOCAL USER MAINTENANCE USING CSE-SS
- BROADSWORD V3.0, USER MAINTENANCE USING THE AAM
- BROADSWORD V3.0, SECURITY AUDIT REVIEW TOOLS

APPENDIX C – CHANGING DATABASE PASSWORD.....C-1

APPENDIX D – INSTALLING NETSCAPE DIRECTORY (LDAP) SERVER.....D-1

- LDAP SUPPLIER
- LDAP CONSUMER

APPENDIX E - UNINSTALLING BROADSWORD.....E-1

APPENDIX F - BROADSWORD FILE LISTING.....F-1

This page left intentionally blank

Forward

The following DRRs have been incorporated into this document:

DRR#	Short Description
4636.3	Changed screen capture; network types are SIPRNET, JWICS, and Internet
4888.3	Added Appendix F with the Broadsword file listing
69484.3	Spelling of the word “auditing”
69485.3	Grammar – The word “the” repeated
69486.3	Spelling – changed “Logger” to “Logged”
69487.3	Grammar – changed “table” to “tables”
69488.3	Numbers Instead of Bullets in Site Config. Worksheet
69497.3	Intelink Misspelled
69498.3	Missing Double Quote
69509.3	“Although” changed to “although”
69510.3	Bad Document Date
69511.3	Period missing
69512.3	Spelling of the word “the”
69513.3	Grammar – “an” should be “and”
69804.3	Spelling – changed “keymasterd3.0” to “keymaster3.0”
69806.3	Grouped commands in Step 4 for clarity
70103.3	Added POC List
70104.3	Added Browser Cache Recommendations
70105.3	Added note that necessary and approved browser plugins are available from the ISMC
70177.3	Noted That LDAP Server Must Be Co-Located With Broadsword
70178.3	Default SYBASE Username Defaults to ‘sybase’, not ‘Sybase’
70179.3	Added More Information on Executing ‘setup.sh’
70180.3	Full Paths to Devices Do Not Need Filenames
70183.3	Fixed Screen Capture in Figure 3.13
70184.3	A listing of plugins in Appendix A was added to the table of contents
70185.3	Added Help on the “Access Permission Override” option
70190.3	Fixed E-mail notification gif
70192.3	Added Instructions for Launching Broadsword the First Time
70208.3	Fixed Figure 4.3
70216.3	Added instructions for configuring access of a 5D/IESS through and IPL
70228.3	Fixed Broadsword Version Number
70229.3	Changed all occurrences of ‘/opt/Keymaster3.0’ to ‘/opt/keymaster3.0’
70230.3	Synchronized Site Configuration Worksheet numbering with instructions
70264.3	Keymaster must be installed before Gatekeeper registration
70265.3	Added more explicit instructions for sharing a dataserver
71339.3	Added a note about Sybase problem calculating free disk space

Chapter 1

Introduction

The purpose of the System Installation & Maintenance Guide is to provide detailed procedures to install a new copy of Broadword Version 3.0 or to upgrade an existing Version 2.0 system. It also provides configuration information and discussion on tools provided to maintain the system.

This document is divided into three parts: (1) Installation, (2) System Operations and (3) ISSO. The remainder of this chapter provides an overview of the Broadword system, its architecture and functionality and an overview of the installation process.

1.1 Installation Overview

The Installation of the system consists of two major sections: (1) installation and (2) configuration. An upgrade consists of three major sections: (1) installation, (2) configuration and (3) removal. The purpose of the installation process is to download the software, create the database and enter the necessary configuration information to bring up an initial copy of the system. The configuration process takes this initial system and configures it by adding site specific data. The configuration process adds local sources, allows editing of system and Gatekeeper values, registers the local Gatekeeper with the community, configures remote sources and tailors data elements. The upgrade process assumes that there is a previous version of the system already installed and operational. Provided as part of the upgrade process is the ability to remove the older version. This process is kept separate from the actual installation since it is believed that both versions will be run for some time until the site has the confidence that the new version has been successfully installed. At this time, the site can then execute the procedure provided in Appendix E.

Figure 1.1 provides an outline of the procedures that will be followed to perform the installation.

Preparing the System – Chapter 2

Installing the System – Chapter 3

Loading the System Software
 Providing Installation Choices
 Database Configuration
 Gatekeeper Configuration
 Client Configuration
Confirming Installation Choices
Installation Progress
Installation Verification

Configuring the System – Chapter 4

Server Configuration
 Configuring Backside Sources
 Editing/Modifying Gatekeeper Parameters
 Editing/Modifying System Parameters
 Tailoring Data Element Descriptions
 Registering with the Keymaster
 Viewing Connected Gatekeepers

Client System Requirements – Chapter 5

HTML Browsers
Image Viewers
MPEG Viewers
Shockwave-Flash Players
Audio Players
Document Viewers
FTP Servers

User and Group Maintenance – Chapter 6

Non-AAM environment
AAM environment



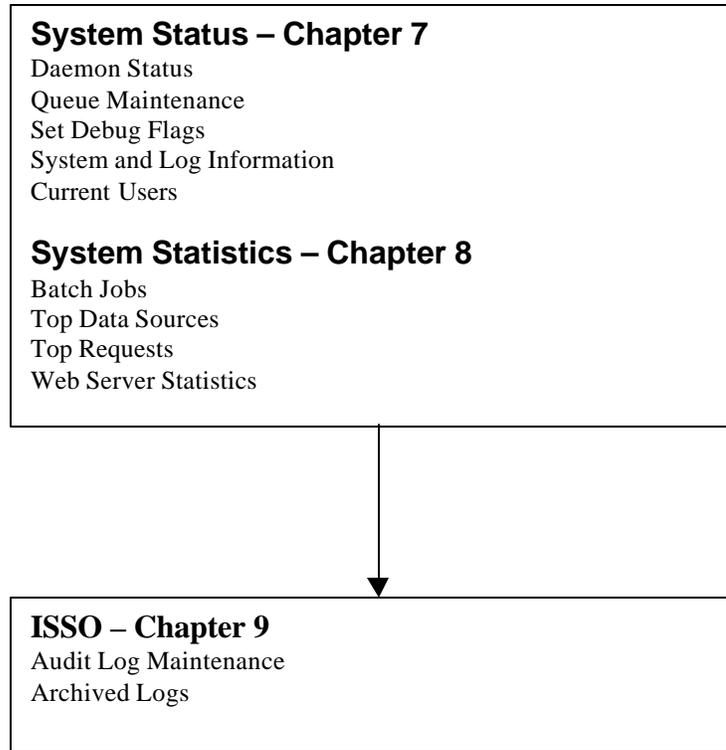


Figure 1.1 - Outline of Procedures for Installation

1.2 System Description

Broadsword implements a multi-tier architecture supporting a single, seamless interface that is secure and administratively manageable. The Broadsword architecture can be divided into five functional components. These components collectively act on behalf of all parties (ISSO, System Administrator and User) and are tailored to meet the connectivity requirements of the site. Table 1.1 provides an overview of each component.

Functional Component	Purpose
Gatekeeper	Provides single interface to various sources for query, retrieval, and product request/delivery. It also provides a single point in which users are authenticated and all actions audited.
Keymaster	Acts as a global map manager allowing for Gatekeepers and their sources to become accessible to others who register with the same Keymaster
Access and Authentication Module (AAM)	Provides a single place where all user access and authentication information is kept. This service is bundled with the

	Gatekeeper (for local administration) and is accessible by authorized Keymaster administrators (for regional administration). It also supports the creation of a “yellow page” lookup of users via the use of the Lightweight Directory Access Protocol (LDAP).
Broadsword Client	User interface which implements the Client/Gatekeeper API and provides ISSO, System Administrator and General Searching capabilities.

Table 1.1 – Summary of Broadsword Functional Components

1.2.1 Gatekeeper

The Gatekeeper component is the heart of the overall 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; interconnecting with other Gatekeepers; maintaining system status; and collection/compilation of results. The Gatekeeper supports a single Application’s Programmer’s Interface (API) for developers to access the functionality provided and to create applications. The API is based on a simple message passing mechanism and is divided into three sections: (1) User, (2) Administration and (3) ISSO. Figure 1.2, shows the overall architecture of the Gatekeeper.

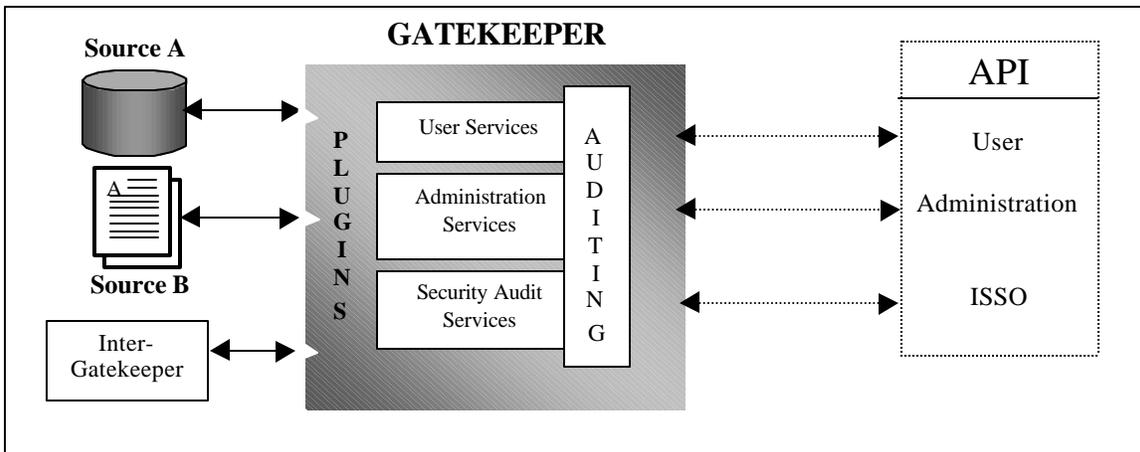


Figure 1.2 - The Overall Gatekeeper Architecture

1.2.1.1 User Services

The Gatekeeper provides support for the processing of user requests, collating the results, delivering products and converting/compressing supported imagery. User requests can be keyword, spatial or SQL based. The availability of request options is dependent upon the sources

connected and what each source supports. Once a request has been submitted, the Gatekeeper audits the request, forwards it to all appropriate sources via plug-ins and waits for each of the sources to respond. Upon receiving the results from each of the sources, the Gatekeeper combines the results into a single response, builds an audit record and forwards the response to requester. Figure 1.3 summarizes the major functionality provided by the Gatekeeper through the User Services portion of the interface.

Some of the sources that are connected to the Gatekeeper may support the ordering and delivery of products. Products include reports from database sources, messages, documents, video clips, maps and images. Delivery mechanisms from the individual sources include: (1) tasking for non-real-time mail order delivery, (2) tasking for FTP delivery and (3) near-real-time FTP delivery.

A number of the imagery sources provide varying degrees of conversion and compression support. As a minimum, each source stores imagery using the National Imagery Transfer Format (NITF) 2.0. This standard supports many levels of compression, bit sizes and storage formats. There are a number of commercial products that can view the full range of NITF storage options. To provide for a wider range of users (those who don't have nor wish to pay for a special application), the Gatekeeper provides conversion support to TIFF 6.0 and JPEG formats.

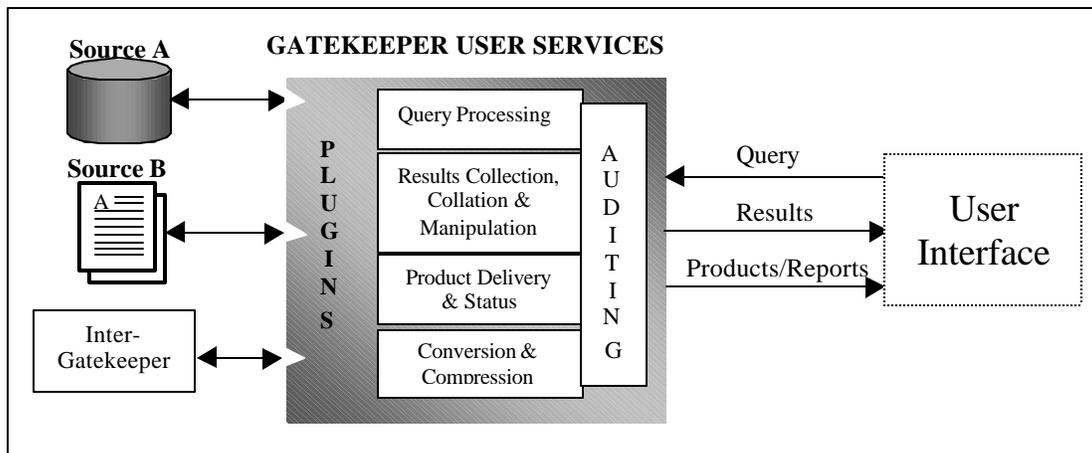


Figure 1.3 – User Services

1.2.1.2 Administration Services

Under Administration Services the Gatekeeper provides an interface for user maintenance, system statistics and system configuration. Access to the functionality provided by these services is limited to authorized users only. Under User/Group Maintenance, the system administrator creates and configures user accounts and groups. User accounts use one of two models. The first mode (used under Broadsword version 2.0) is a combination of Sun Tools/CSE-SS and the Broadsword Administrative Interface. User account creation and password maintenance is managed through CSE, while Broadsword roles and source accesses are maintained through the Broadsword Administration Interface. The problem identified with this approach is the fact that the System Administrator is required to go to two places to manage user accounts. To correct this situation and support the capability for regional administration, Broadsword version 3.0

introduced the Access and Authentication Module (AAM). The role that AAM plays in the architecture is described in more detail in section 1.2.3. Each user can be assigned to one or more groups and have access to various sources. Members of groups share sources and roles assigned to the group. Groups are created and configured through Group Maintenance.

System Statistics provides Gatekeeper statistics, includes a listing of the most frequently accessed products and the most frequently processed queries. In System Configuration, the system administrator configures the Gatekeeper, adds/removes backside sources, defines values for attributes and establishes connectivity with other Gatekeepers through registration with the Keymaster (described in section 1.2.2). Figure 1.4 summarizes the major functionality provided by the Administration Services.

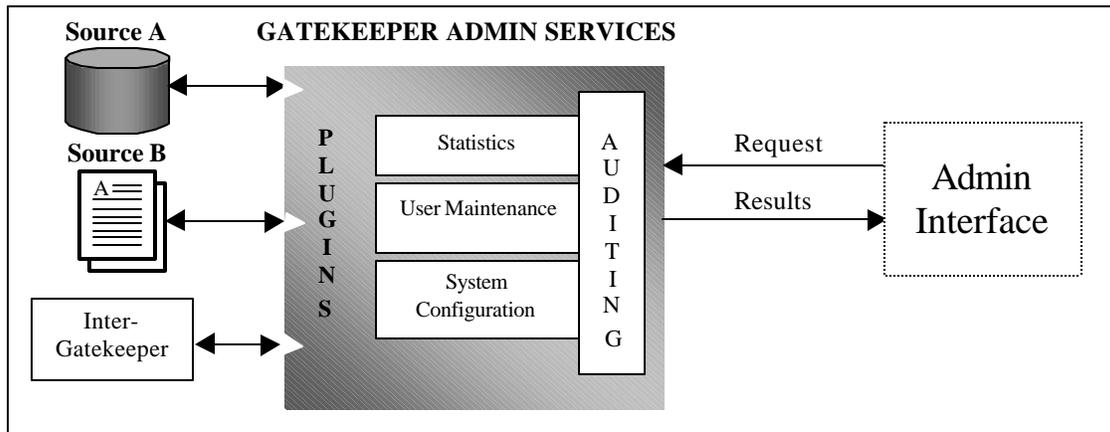


Figure 1.4 – User Services

1.2.1.2 Administration Services

Under Administration Services the Gatekeeper provides an interface for user maintenance, system statistics and system configuration. Access to the functionality provided by these services is limited to authorized users only. Under User/Group Maintenance, the system administrator creates and configures user accounts and groups. User accounts use one of two models. The first mode (used under Broadword version 2.0) is a combination of Sun Tools/CSE-SS and the Broadword Administrative Interface. User account creation and password maintenance is managed through CSE, while Broadword roles and source accesses are maintained through the Broadword Administration Interface. The problem identified with this approach is the fact that the System Administrator is required to go to two places to manage user accounts. To correct this situation and support the capability for regional administration, Broadword version 3.0 introduced the Access and Authentication Module (AAM). The role that AAM plays in the architecture is described in more detail in section 1.2.3. Each user can be assigned to one or more groups and have access to various sources. Members of groups share sources and roles assigned to the group. Groups are created and configured through Group Maintenance.

System Statistics provides Gatekeeper statistics, includes a listing of the most frequently accessed products and the most frequently processed queries. In System Configuration, the system administrator configures the Gatekeeper, adds/removes backside sources, defines values for

attributes and establishes connectivity with other Gatekeepers through registration with the Keymaster (described in section 1.2.2). Figure 1.4 summarizes the major functionality provided by the Administration Services.

1.2.1.3 Security Audit Review

The Security Audit Review Interface provides the ability to view, archive, and remove audit information. Those records that have been archived are also available for review. All audits are stored in a database. Broadword version 3.0 offers Sybase as the database engine during the installation. Security records can be filtered based on any one event, user name and/or time range. Table 1.2 provides a summary of the events that are audited by the Gatekeeper.

Gatekeeper Security Audits		
User Events:		
Catalog Request	Transfer Request	User Logged In
Query	User Change Password	User Logged Out
Administration Events:		
Accept Registration from Remote Gatekeeper	Gatekeeper Stopped	Removed Group
Added Discretionary Access Control (DAC)	Get Column Attributes	Removed Group Member
Added Group	Initiate Stream Request	Remove Source
Added Group Member	Modified Element	Remove User
Added New Source	New or Updated Gatekeeper Info	Set Source Parameter
Added User Privileges	Register Our Gatekeeper With Keymaster	Set User Discretionary Access Control (DAC)
Clear Statistics	Remove Discretionary Access Control (DAC)	Terminate Stream Request
Gatekeeper Started	Removed Remote Gatekeeper	Update Daemon Status
ISSO Events:		
Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 1.2 - Summary of Security Audits

The certifying authority uses the audit trail dumps, in conjunction with the system audit logs, to validate security-auditing requirements. There are three Sybase audit log formats used within Broadword. Table 1.3a shows a sample Audit Report. This report identifies the user, the client,

the date and time of the request, the destination address for product transfers, the type of action requested, the result of the action requested and the unique session identifier.

UserID	Client ID	Date/Time	Destination ID	Action	Result	Session Key
test01	128.132.888.888	950126 18:01		Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16		Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16	128.132.888.899	Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16	128.132.888.898	Query	Project Broadsword: 00085 Hits	5607

Table 1.3a – Sample Audit Report

Table 1.3b provides a sample Product Request Report. The Product Request Report provides information about a product transfer. In addition to the information provided on the original query, this report provides Server ID.

UserID	Client ID	Date/Time	Access ID	Server ID	Session Key
test01	128.132.999.999	950126 21:35	IPA_16193533ZNov94_061488	128.132.989.989	5607
test01	128.132.999.999	950126 21:38	IPA_16193533ZNov94_061488	128.132.989.989	5607
test01	128.132.999.999	950126 21:41	IPA_16193533ZNov94_061488	128.132.989.989	5607

Table 1.3b – Sample Product Request Audit Report

The Query Report provides information about data returned for individual hits. In addition to the information provided on the original query, this report provides the Access ID and the Server ID for the Server performing the query. Table 1.3c provides a sample of this report type.

UserID	Client ID	Date/Time	Access ID	Server ID	Session Key
test01	128.132.999.999	950126 20:33	IPA_19153415ZJan95_216672	128.132.999.888	5607
test01	128.132.999.999	950126 20:33	IPA_19153608ZJan95_213744	128.132.999.888	5607
test01	128.132.999.999	950126 20:33	IPA_19153611ZJan95_849	128.132.999.888	5607

Table 1.3c – Sample Query Response Audit Report

1.2.2 Keymaster

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.

Broadsword version 3.0 supports regional user maintenance. User accounts can be created and configured at the Keymaster for a specified registered Gatekeeper. Figure 1.5 shows the Broadsword architecture with two Gatekeepers and a Keymaster.

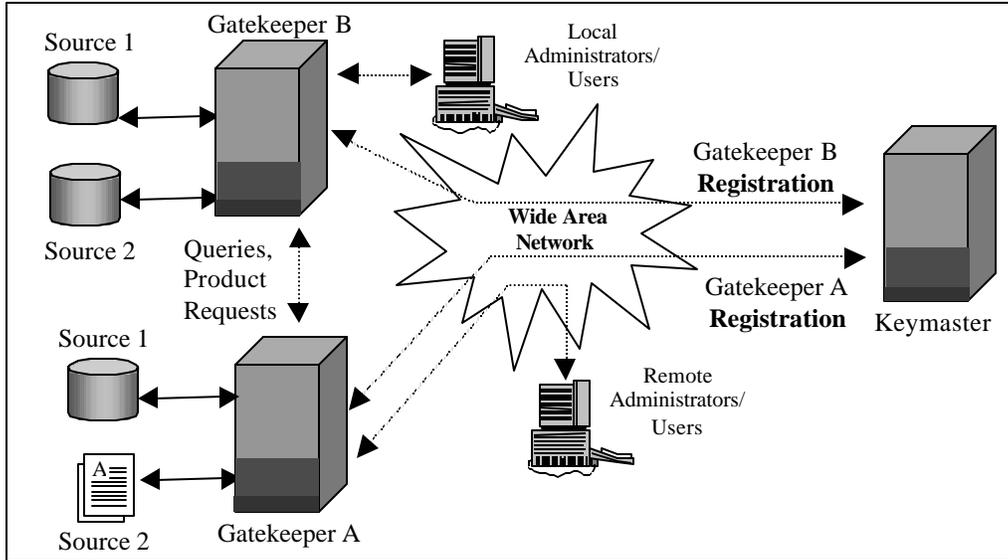


Figure 1.5 – Gatekeeper/Keymaster Architecture

The Keymaster uses a subset of the API libraries provided as part of the Gatekeeper. Specifically, it uses the login process, its associated user administration capability and ISSO functionality. Table 1.4 provides a list of auditable events within the Keymaster.

Keymaster Security Audits		
User Events:		
User Change Password	User Logged In	User Logged Out
Administration Events:		
Accept Registration From Remote Gatekeepers	Keymaster Stopped	Remove Remote Gatekeeper
Added Discretionary Access Control (DAC)	New or Updated Gatekeeper Info	Remove User Privileges
Added Group	Register Our Gatekeeper With Keymaster	Set User Discretionary Access Control (DAC)
Added Group Member	Removed Discretionary Access Control (DAC)	Set User Info
Added User Privileges	Removed Group	Update Daemon Status
Keymaster Started	Removed Group Member	
ISSO Events:		

Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 1.4 - Summary of Security Audits

1.2.3 Access and Authentication Module (AAM)

To create and configure a user within Broadsword version 2.0, the administrator must first create a user account through either the SUN operating system (SUN Tools) or through CSE-SS and then use the Broadsword administration tools to add privileges/sources. At best, this process is disjointed and requires the administrator to know/understand multiple interfaces and applications. To alleviate this problem and to implement additional user requirements, Broadsword version 3.0 has introduced the Access and Authentication Module (AAM). To support existing deployments of Broadsword 2.0, version 3.0 supports and is backward compatible with the current 2.0 user maintenance infrastructure.

The overall goal of the AAM is threefold. The first is to provide the Broadsword administrator a single interface to create and configure user accounts. The second goal of the AAM is to provide for regional user maintenance. Administrators are not available at all locations. There exists the requirement to create user accounts at a central location. The final goal is to automatically create a global directory service through which users can find information about other users. This capability must be compatible with the Lightweight Directory Access Protocol (LDAP) initiative being pursued by the Intelligence Community (IC) and DoD.

The trend within the IC and DoD is to use Netscape's LDAP to store all user information. The IC LDAP schema is designed as an on-line phone book or "yellow pages" directory service. It contains information describing the user. It does not contain the necessary information to maintain and manage user passwords. Data such as password history, account lock/unlock, and number of invalid login attempts are a few attributes that need to be maintained in order to provide an accreditable user authentication module. The AAM provides a single interface through which all user and system access information is accessed and maintained. The AAM is accessed through the Gatekeeper Administration API. The information required is divided into three parts; user information, password management and system configuration.

By separating user information from password management, each Gatekeeper will have a pure LDAP schema as defined by the IC as well as all of the necessary information to perform a reasonable level of authentication information and password management. The list of necessary information, and the requirements that dictated this list, was derived from the password and user authentication policies provided by CSE-SS. These include:

- Password Expiration
- Dictionary Attack
- Account Locking/Unlocking
- Bad Password Checking
- Password History

Tables 1.5a and b provides a list of those items that are stored and in which storage mechanism.

Gatekeeper Configuration File	Database
Number of bad Login attempts before account locked	User Identification
Number of days before password expires	User Identification password (Encrypted using CRYPT or MD5)
Minimum password size	Space delimited list of OLD PassWorDs (Encrypted using CRYPT or MD5)
Maximum password size	Last Date/Time of Password Changed (YYYYMMDDhhmmss)
Minimum number of special characters required in a password	Account locked (Y/N)
Number of passwords saved in user's password history	Number of bad login ATTEMPTS
LDAP Host IP	
LDAP Port	
LDAP root Distinguished Name	
LDAP root password (Encrypted)	

Table 1.5a – AAM Gatekeeper/Database Attributes

LDAP Schema		
Mandatory Attributes:		
Citizenship	Given Name	Name
Surname		
Policy-based Attributes:		
Employee Type	Intelligence Community Email	Telephone: Unclassified Voice Phone Number
Home Organization	PKI: Certificate	
Optional Attributes:		
Company Name	Physical Address	Phone: Secure Facsimile Number
Current Organization	Physical Building Name	Phone: Secure Telephone Number
Email: Internet Address	Physical City	Phone: Unclassified Fax Phone Number
Email: Niprnet Address	Physical State or Province	Title
Email: Siprnet Address	Physical Postal Code	User Identification
Grade	Physical Country Name	Expert Country
Mailing Address	PKI: Authority Revocation List	Expert Functional Area
Telephone: DSN Voice Phone Number	PKI: CACertificate	Production Manager
Telephone: Secure Facsimile Number	PKI: Certificate Revocation List	Language Proficiency
Middle Initials	Telephone: DSN Voice Phone Number	

Table 1.5b – AAM LDAP Attributes

All users will be assigned a specific Gatekeeper through which they will log into the system and perform all requests. The local system administrator can add user accounts to the Gatekeeper. Figure 1.6 provides an overall architecture.

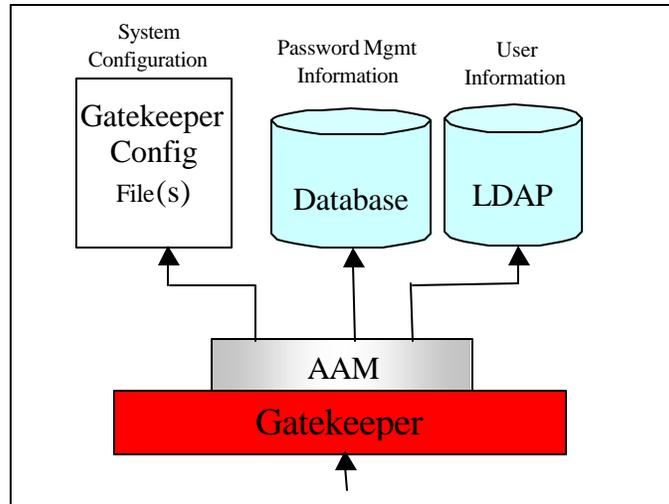


Figure 1.6 – Access & Authentication Module Architecture

The AAM also supports the ability to perform regional user maintenance. User accounts can be created/maintained remotely through the Keymaster and its interface. Keymaster administrators must be granted privilege from the local Gatekeeper administrator to allow not only the Keymaster but also the particular Keymaster administrator permission for remote access. Before the Keymaster client is permitted to access the AAM to create/modify a user account, the two components (Keymaster and Gatekeeper) must authenticate themselves.

1.2.3.1 LDAP Replication

Information stored in the Gatekeeper LDAP can be replicated (via Netscape's replication service) to any other registered LDAP server. LDAP servers can exist anywhere in the network. An LDAP server may reside on the same server as that of the Keymaster or exist on one of the servers that is part of the JIVA Enterprise. Registered LDAP servers must have valid Digital Certificates and be configured to communicate through the use of Secure Sockets Layer (SSL). Digital certificates will be obtained through the Intelink System Management Center's (ISMC) Certificate Authorities. Since Broadword's LDAP servers contain only user information as designed by the IC, it is acceptable to supply this information to other registered LDAP servers. Figure 1.7 provides a high-level architecture diagram illustrating a scenario where the AAM and LDAP servers exist.

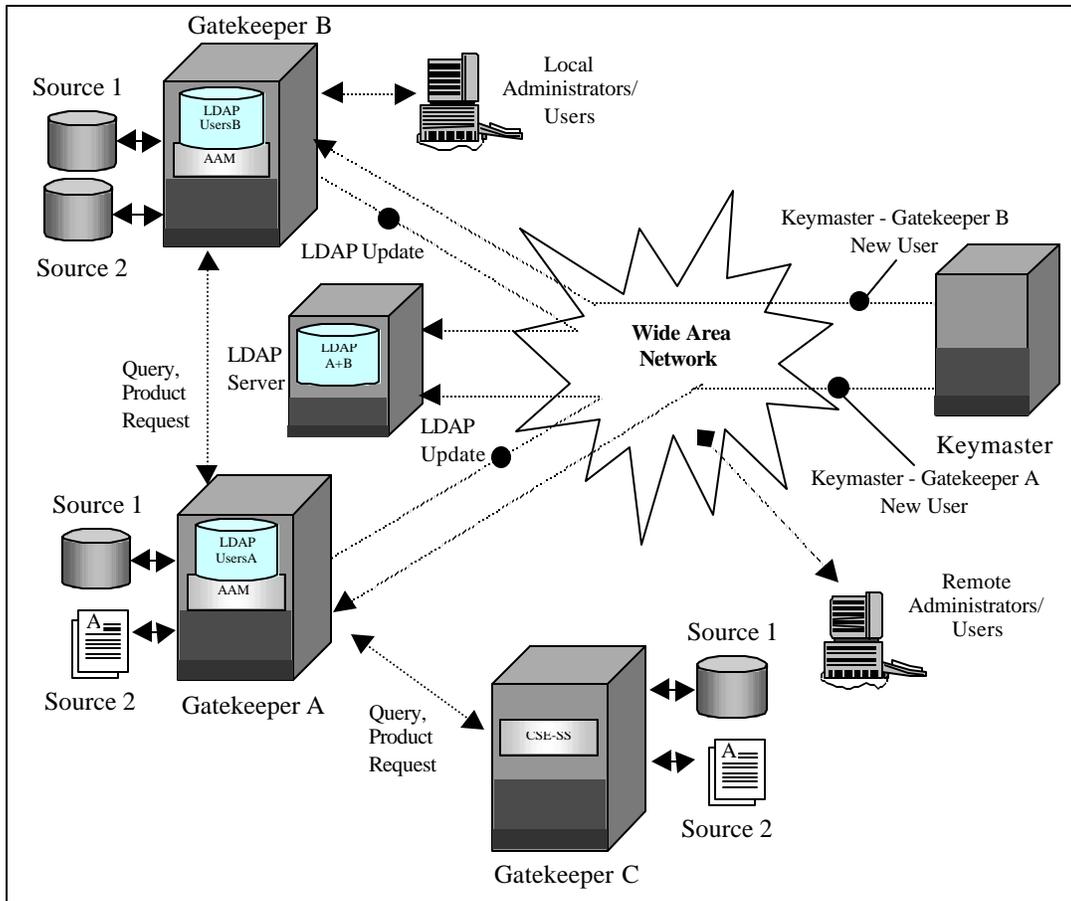


Figure 1.7 – Gatekeeper/Keymaster with LDAP Architecture

A Gatekeeper using the Broadword version 2.0 user maintenance will still be capable of registering with the Keymaster and participating with other Gatekeepers (both version 2.0 and 3.0), but will be unable to support regional user maintenance and LDAP user information.

1.2.4 The Broadword Client

Broadword provides a User Interface to access the Gatekeeper and local data sources. It is Web-based and supports multiple roles. Roles are assigned on an individual user basis and can include one or more functions: Searching, Administration and ISSO.

The user will log into the system from the main screen; based on the user's login, the main screen will be tailored to what roles that have been assigned by the site System Administrator. The following paragraphs provide an overview of the functionality supported through the client interface. Figure 1.9 shows the overall User Interface Architecture.

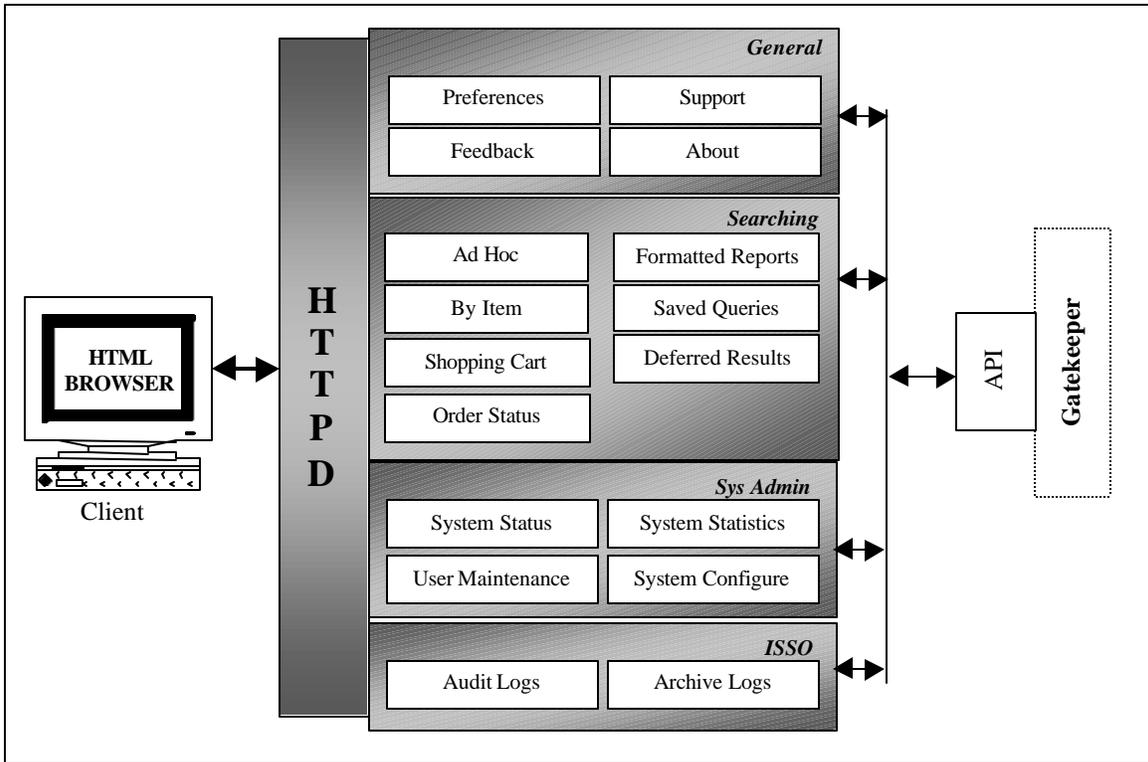


Figure 1.9 - Broadsword Client Architecture

1.2.4.1 General

The Preferences section allows the user to set up their default values and is split into six separate pages: (1) General Registration & Default First Page; (2) Information Support; (3) Delivery Options; (4) What and Where to Search and Search Utilities; (5) Attribute Configuration and (6) Remote Access. Users are able to define what their Search Tools page looks like, which data sources to search, and their preferred search mechanism. The Feedback page allows the user to provide on-line suggestions and comments about the interface. This form is pre-filled with information provided on the Preferences page. The Support page provides a listing of points of contact for requirements, help desk, site system administration, site ISSO and site Intelink officer. The About page provides the version number of the system, and whom the current copy is registered to. These capabilities are provided to all users regardless of their roles.

1.2.4.2 Searching

Under Searching, the user is provided with tools to discover, navigate and retrieve information across various sources. Searching capability is given to any user that has been given a login and password. Searching is divided into two functional capabilities: Ad Hoc and By Item.

Users are able to choose between an SQL form-based utility (Query) or a spatial tool (Geographic Search). In addition, users are able to combine these search tools and configure what method they prefer through the Define Search Page preference. This preference represents

the search mechanism they use the most, and that will be displayed. Should the user select search tools as their default first page, then this search mechanism will be displayed immediately after login. Thus, the Search Form page is a single user-selected page, tailored to each user's preference.

Provided off the spatial tool, is the ability to turn on broadcast feeds (e.g., TRAP/TRE). The user can use these feeds for tip off of potential activity within a given Area Of Responsibility (AOR) and request additional/available information of the area through the request mechanism.

The results page displays all records matching the user's query. There are two methods supported under searching; Ad Hoc and By Entity. Selecting Ad Hoc allows the user to search all sources simultaneously and return all hits from each source individually. This method is the one currently available under Broadword version 2.0 and is the method most users are familiar with when using such search engines as AltaVista, Yahoo, Lycos, etc.

The second method, new to Broadword version 3.0, is by Entity. This method limits the initial request to an MIDB and a single Imagery source. If the user has selected an MIDB and/or Imagery source through preferences, the first one in the list in each case will be selected. If one or neither of the sources has been chosen, the interface will default to the first one in the user's list of each type. If the user does not have access to both sources, then this search option will not be available.

The results are provided back in an aggregated view based on the requested item(s). The results window is then used as a portal providing suggested sources for additional information. The results can be displayed as a sorted/unordered list, timeline or on a map. From the results page, the records can be examined further, products pulled, or products ordered. Frequently used queries can be saved through either the Search Form page or Results Page. Each source dictates the display and/or retrieval of its products.

Currently Broadword supports ordering CSIL, IPL, 5D and IDEX products. There is a different process for requesting IDEX products, pulling IPL/5D products to a destination, and ordering CSIL products. Users are able to choose several products of differing types and put them into a "shopping cart". The ordering attributes for any product placed in the cart can be modified while in the cart. Items placed in the cart can be saved from session to session and across multiple queries. At any time the user can order the items in the cart by clicking the order button. The user can find out the status of any orders that they have placed by clicking on the Order Status capability. This function provides information as to whether the product has been successfully delivered or has been shipped out (depending on the source).

Formatted reports provide the ability for the user to generate a set of predefined reports. Specific report types and the attributes available to generate them are based on the source and type. Reports can be ordered to a specified destination or available on-line.

The Saved Queries page provides the user with a list of all queries, which the user saved through the Search Tools or Results Page, as well as functionality to process the queries in different ways. A saved query can be used interactively by the user, producing immediate results, as well as by background processing, producing deferred results. Interactive use of saved queries includes immediate execution of the query and loading of the query for display modification. Background processing of saved queries is done by the E-mail Notification and Batched Query utilities. E-mail Notification Processing periodically informs the user of new and updated products that

match the saved query. Batched Query Processing allows the user to schedule the query to be executed at a later time. The results generated by the background processing utilities are viewed through the Deferred Results Page. The Deferred Results capability not only allows viewing of E-mail and Batched results, but also deletion of these results. For viewing, the standard display format is used to present product information.

1.2.4.3 Administration

The System Administration (SA) section for the Gatekeeper provides system status, user/group maintenance, system statistics and system configuration. System Status provides the status of all processes associated with the Project Broadsword system, the ability to turn on debug flags and maintenance for Broadsword log files.

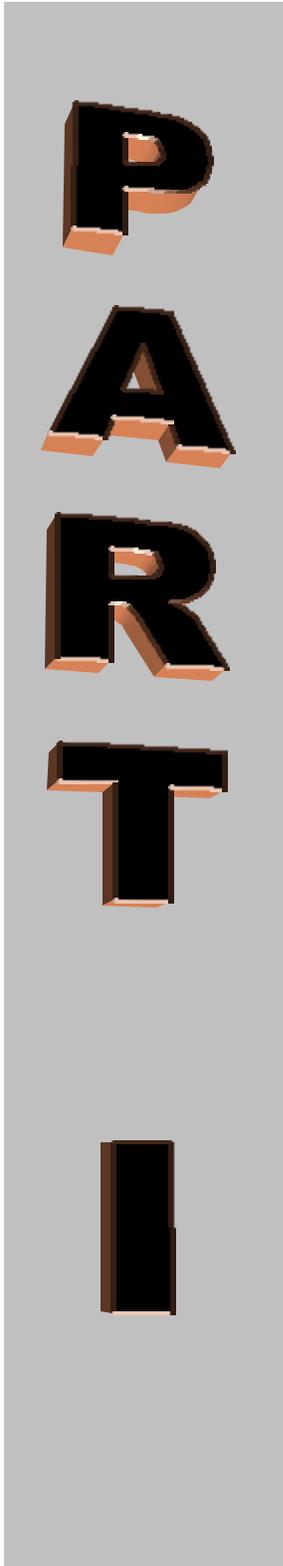
Under User Maintenance, the system administrator grants additional privileges (i.e., system administrator, and ISSO) and access to various sources. System Statistics provides Web, Gatekeeper and Batched jobs statistics. Web statistics is based on Web Usage and provides such information as the amount of bytes transferred, the top number of pages accessed and the total number of accesses. Gatekeeper statistics include a listing of the top 10 frequently accessed products and the top 10 frequently issued queries.

The System Configuration section, allows the system administrator to modify or change the configuration information of the Gatekeeper, add/remove sources, define values for attributes (used for pop-downs as part of the short form) and establish connectivity with other Gatekeepers through registration with the Keymaster.

1.2.4.4 ISSO

The ISSO Interface provides the ability to view, archive, or remove audit information from the Broadsword Sybase Database based on users(s), date/time and audit event. It also allows the ISSO to retrieve previously archived audits.

This page left intentionally blank



The purpose of this part is to provide detailed information to install a new version or to upgrade an existing one.

Topics covered in this part:

Getting Started

- Server Requirements
- Preparing your system
- Site Configuration Worksheet

Installation

- Loading the System Software
- Providing Installation Choices
 - Database Configuration
 - Gatekeeper Configuration
 - Client Configuration
- Confirming Installation Choices
- Installation Progress
- Installation Verification

System Configuration

Client Requirements

User & Group Maintenance

This page left intentionally blank

Chapter 2

Getting Started

The purpose of this chapter is to prepare your system for installation and to gather all the required information you'll need beforehand. At the end of this chapter is a "Site Configuration Worksheet." You should have this worksheet filled out before continuing to Chapter 3. It contains all the questions the installation script will be asking. You may want to detach it from this document to have it handy during the installation. The topics in this chapter include:

- Requirements
- Preparing Your System
- Site Configuration Worksheet

2.1 Server Requirements

Broadsword can be installed on a dedicated Solaris system, or it can share a system with another Sybase application. Your system must be operating with at least the following hardware/software in order to successfully install and use the Broadsword Interface:

Software	Hardware
<ul style="list-style-type: none">• Sybase SQL OR Sybase Adaptive Server• Solaris v2.6• An HTML v4.0+ compliant web browser, such as Netscape 4.7+ or Internet Explorer 4.0+ (refer to Chapter 5 for more information)• CSE-SS or an LDAP Server already preloaded• X-Window Environment (if running CSE-SS)	<ul style="list-style-type: none">• CD ROM Drive• At least 2 GB free disk space for Broadsword database• At least 1 GB free disk space for Broadsword software• At least 1 GB free disk space for map data• At least 2 processors• 1GB/2 GB recommended memory (imagery products)

For CSE-SS Option:

1. No special CSE-SS audit flags are needed for Broadword; the CSE-SS minimum audits will suffice, as Broadword utilizes its own auditing scheme.
2. No additional operating system packages and subsets are required for Broadword, except those required to support CSE-SS version 1.3/1.4.
3. No special steps are required to install Broadword in a CSE-SS environment.

2.2 Preparing your System

This section provides a list of things to do *before* installing the system.

Note: You must be user **root** at this point to perform each of the following steps (unless specified otherwise).

1 Partition Broadword Database Devices

You must partition disk space to use for the Broadword database, transaction log, and temp device. Use whichever utility program you normally use to partition disks, such as 'format' or 'SparcStorage Array Volume Manager', if using a Sun Sparc Disk Storage Array. The standard partition sizes are as follows, but can be made larger:

- Master Device Path: 30MB (**60MB for Sybase adaptive server**) {Worksheet #10}
- Sysprocs Device Path: 30MB(**60MB for Sybase adaptive server**) {Worksheet #11}
- TempDevice: 100MB {Worksheet #14-15}
- Database: 2000 MB {Worksheet #17-18}
- Transaction Log: 500MB {Worksheet #19-20}

You can use either raw or UNIX file system partitions for these Sybase devices, however, Sybase, Inc. recommends raw partitions. In either case, make sure that the raw device path (or UNIX directory) is owned and writeable by the Sybase user. Also be sure there is enough space available on each partition. You will be prompted during the installation for the location of these free space partitions.

Sybase licensing requires an SQL Server site license to create multiple Sybase dataservers. If your site does not have this site license, you CANNOT create multiple dataservers on this system. If this is the case, you MUST answer the question for 'Sybase Dataserver Name' (Worksheet #8) with your existing dataserver name. This will allow Broadword to 'share' this existing dataserver. If your site does have the site license, the installation will create a new Sybase dataserver if desired. If in question, contact your local Sybase Administrator or Sybase, Inc. at 1-800-8-SYBASE.

Note: If you decide to share with an existing dataserer, be sure to choose one that has a sort order of "case - insensitive dictionary sort order." Broadsword will not function correctly otherwise (i.e., 5D cannot be shared with because it's dataserer is case sensitive. To verify this, execute the "sp_helpsort" system stored procedure inside the dataserer in question to confirm the sort order is set as described above.

Also, if you decide to share with an existing dataserer, you will not need to partition space for a Master Device, Sysprocs Device, or Temp Device. These will be used in the existing dataserer being shared with.

2 Determine Available Disk Space

The standard location to install Broadsword is /opt/bswd3.0. Enter the following to determine if the /opt partition has adequate free space (1 GB for Software, 1 GB for Map Data):

```
df -k /opt <cr>
```

There should be at least 1GB available on the /opt partition. The distribution media accounts for only a fraction of this 1GB; the rest is to allow for product & thumbnail caching. If the /opt partition doesn't contain at least 1GB of free space, you should utilize a partition that is large enough, and create a symbolic link called /opt/bswd3.0 that points to it. For example, if the /opt partition is not large enough, but there's an /opt1 partition that is, the following commands could be used:

<pre>/usr/bin/mkdir /opt1/bswd3.0<cr></pre>	(Makes new directory to store Broadsword)
<pre>/usr/bin/chmod 755 /opt1/bswd3.0<cr></pre>	(Sets permissions)
<pre>/usr/bin/ln -s /opt1/bswd3.0 /opt/bswd3.0 <cr></pre>	(Creates a symbolic link, called /opt/bswd3.0 that "points to" /opt1/bswd3.0)

3 Make sure *sendmail* is running on your system

In order for the Feedback and Profile Notification functions to work properly, the host on which you are installing the Interface must have *sendmail* set up. Use the following command to check if it's running:

```
/bin/ps -ef|grep sendmail|grep -v grep<cr>
```

If you get output returned by the system, *sendmail* is already running, and you may proceed to the next step. If you get no output, type the following (as user root) to start *sendmail*:

```
sh /etc/init.d/sendmail start <cr>
```

4 Perform system kernel modification, if necessary

These lines are needed by the Sybase dataserver. If the following lines don't already exist in the file `/etc/system`, you must append them (as user root):

```
set shmsys:shminfo_shmmax=1310720000
set shmsys:shminfo_shmseg=32
set maxusers=512
```

and issue the following commands:

```
touch /reconfigure <cr>
```

Note: Before issuing the following shutdown command, you must shutdown any Database Servers that are currently running to avoid any possible database corruption.

```
/usr/sbin/shutdown -y -g60 -i6 <cr>
```

(to reboot the system and make the new values take effect)

5 Choose Broadsword Group

Choose an existing UNIX group on the system to use for Broadsword, or create a new one (i.e. `bswd`). All users connecting to the Broadsword Interface must be in this group. For example, if your server already has an "ipa" group defined, and this same group of users will be allowed to connect to Broadsword, you can simply use "ipa" as your group name. Be sure to write the group chosen in Field (31) in the Site Configuration Worksheet below.

6 Create Broadsword System Administration User

Create a new UNIX user on the system, using your normal means, called `bswduser`. This user is used as the Broadsword System Administrator. Add this user to the Broadsword group chosen or created above.

7 Create Broadsword CDIM User

Create a new Broadsword user on the system, using your normal means, called `cdimuser`. This user is used for Profile Notification operations. Add this user to the Broadsword group chosen or created above.

8 Create Broadsword Registered User

Create a new UNIX user on the system, using your normal means, called `bswdreg`. This user is used for Broadsword Registered Server Functions. Add this user to the Broadsword group chosen or created above.

9 Allow X Server Connections

On the system, open up a new xterm window on the **console** and allow X server access:

```
/usr/openwin/bin/xterm & <cr>
```

And in the new xterm window:

```
/usr/openwin/bin/xhost <hostname> <cr>
```

10 Complete the Site Configuration Worksheet (below)

After correctly completing the above steps, fill out the **ENTIRE** worksheet below, as you will refer to it during the installation process in Chapter 3.

2.3 Site Configuration Worksheet

The following section previews all the configuration questions that will be asked during the installation process. You are encouraged to write in your answers on this page so that you have them handy during installation. (The numbers adjacent to the Field Names are referred to throughout this guide.)

Note: For completeness, password fields are listed here. However, it is advisable NOT to write down any passwords on this sheet. You should remember them.

Field Number	Field Name	Your Answer	Description
1	CD Registration name		Registration name as shown on the Broadword distribution CD-ROM.
2	CD Serial Number		Serial number as shown on the Broadword CD-ROM
3	Import Selection		Answer "Yes" to import various items from a previous Broadword version (Default: YES)
4	Broadword Previous Version Path		Path to previous version of Broadword. Asked only if Import selection is Yes.
5	Dataserver Creation Method		Dataserver Creation Method (Default: Create New)
6	Sybase Username		Sybase UNIX username associated with version of Sybase being used for Broadword. (Default: sybase)
7	Sybase Home Dir Path		Home directory path of Sybase SQL Server or Sybase Adaptive server.
8	Sybase Dataserver Name		The dataserver name to create or share for Broadword Sybase server.

37-3.0-SYIMG-01 01-G0
09 January 2001

Field Number	Field Name	Your Answer	Description
			(Default: BSWD_<hostname>_SVR)
9	Sybase Dataserver Port Number		UNIX port to be used by the Broadsword Sybase server. Asked only if creating a new dataserver. (Default: 2503)
10	Sybase Dataserver Master Device Path		System location to place Broadsword dataserver master device. Can either be a raw device (i.e. /dev/rdisk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Must be at least 30MB free on path (60 MB for Sybase Adaptive Server). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. master.dev) at the end of the path. The filename will be added automatically.
11	Sybase Dataserver Sysprocs Device Path		System location to place Broadsword dataserver systemprocs device. Can either be a raw device (i.e. /dev/rdisk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Must be at least 30MB free on path (60 MB for Sybase Adaptive Server). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. master.dev) at the end of the path. The filename will be added automatically.
12	Sybase B/U Server Create?		Create new Sybase Backup Server? Asked only if creating a new dataserver. If a Sybase Backup Server already exists on this system, you may click "No".
13	Sybase B/U Server Port #		UNIX port to be used by the Sybase Backup Server. Asked only if creating a new dataserver, and "Yes" is answered to question # 12 above.
14	Broadsword TempDevice Path		System location to place Broadsword TempDevice. Can either be a raw device (i.e. /dev/rdisk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. master.dev) at the end of the path. The filename will be added automatically.
15	Broadsword TempDevice Size		Size to make the Broadsword TempDevice. Asked only if creating a new dataserver. (Default: 100MB)
16	Sybase Administrator Password	(don't write here)	The password for the Sybase System Administrator (sa). Asked only if sharing an existing dataserver.
17	Broadsword Data Device Path		System location to place Broadsword database. Can either be a raw device (i.e. /dev/rdisk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices.

37-3.0-SYIMG-01 01-GO
09 January 2001

Field Number	Field Name	Your Answer	Description
			Note: Do not include the device filename (e.g. master.dev) at the end of the path. The filename will be added automatically.
18	Broadsword Data Device Size		Size to make the Broadsword database. (Default: 2000 MB)
19	Broadsword Log Device Path		System location to place Broadsword database transaction log. Can either be a raw device (i.e. /dev/rdisk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Note: Do not include the device filename (e.g. master.dev) at the end of the path. The filename will be added automatically.
20	Broadsword Log Device Size		Size to make the Broadsword database transaction log. (Default: 500 MB)
21	bswduser Account Password	(don't write here)	UNIX password for 'bswduser' account created in Chapter 2.
22	cdimuser Account Password	(don't write here)	UNIX password for 'cdimuser' account created in Chapter 2.
23	Existing IPA/IPL on this machine?		Click "Yes" if there is a co-located IPA or IPL 1.0 on THIS server.
24	Path to existing IPA/IPL?		If "Yes" is answered to question above, enter UNIX directory path to IPA or IPL 1.0. (Default: /opt/ipl10)
25	Server Type		Server type for this Broadsword Installation. (Choices: Protected or Both Protected and Registered)
26	Protected HTTP port #		UNIX port to be used by the Protected HTTP daemon.

This field is required for a Registered Server only.

27	Registered HTTP port #		UNIX port to be used by the Registered HTTP daemon. Asked only if "both" is answered to question above.
----	------------------------	--	---------------------------------------------------------------------------------------------------------

This field is required for LDAP and Registered Servers only.

28	bswdreg Account Password	(don't write here)	UNIX password for 'bswdreg' account created in Chapter 2.
----	--------------------------	--------------------	-----------------------------------------------------------

29	Network host machine is on		Network type host machine is connected to. (Choices: SIPRNET, JWICS, or Internet) (Default: SIPRNET)
30	Additional network classification label (optional)		Any additional caveats or compartments that should be added to the security banner (e.g. - SI/TK) Default: Blank
31	SIPRNET Project Broadsword Program Office IP Address		IP Address (on SIPRNET only) of Project Broadsword Program Office homepage. Asked only if network type is SIPRNET. If this address is unknown contact the Broadsword Program

37-3.0-SYIMG-01 01-GO
09 January 2001

Field Number	Field Name	Your Answer	Description
			Office at (315) 330-4429.
32	Group Name		UNIX group to use for Broadsword
33	Broadsword Homepage Logo Image File		Site chosen image to be displayed in upper left corner of Broadsword homepage. Must be path to a GIF or JPEG image; recommended size 159x150 pixels. For no logo (default), just leave blank.
34	Log Rolling Count		Number of previous Broadsword log files to keep and archive (as compressed tar files), for example, if set to 10 (default), only 10 will be kept and the oldest will be overwritten.
35	Activate Cataloging Capability?		Click "Yes" if this server will be used for imagery production purposes (cataloging to an IPL 1.x/2.x) (Default: No).
36	Use Access & Authentication Module?		Whether to use the AAM, if installed at the site. Requires an LDAP server co-located on the Broadsword machine (Default: No).

These fields are required only if the answer to the previous question is Yes.			
37	LDAP Server		Hostname of an LDAP server accessible on the Broadsword machine. Asked only if "Yes" is answered to question #34 above.
38	LDAP Port #		Port # of the LDAP server specified above (Default: 389). Asked only if "Yes" is answered to question #34 above.
39	LDAP Bind DN		Bind DN of the LDAP server specified above (Default: cn=Directory Manager). Asked only if "Yes" is answered to question #34 above.
40	LDAP Bind Password	(don't write here)	LDAP Bind password for LDAP server specified above. Asked only if "Yes" is answered to question #34 above.
41	Migrate Solaris/CSE-SS Accounts?		Whether to migrate Solaris or CSE-SS user accounts into Broadsword. Asked only if "Yes" is answered to question #34 above (Default: No).

42	System Admin Name		System Administrator name (MANDATORY)
43	System Admin Branch		System Administrator branch (MANDATORY)
44	System Admin Organization		System Administrator organization (MANDATORY).
45	System Admin Address1		System Administrator address (MANDATORY).
46	System Admin Address2		System Administrator address (MANDATORY).
47	System Admin Phone		System Administrator UNCLASSIFIED phone number (MANDATORY).
48	System Admin FAX		System Administrator FAX (MANDATORY)
49	System Admin E-mail		System Administrator E-mail (MANDATORY)
50	System Admin City		System Administrator City (MANDATORY)
51	System Admin		System Administrator State/Locality

37-3.0-SYIMG-01 01-G0
09 January 2001

Field Number	Field Name	Your Answer	Description
	State/Locality		(MANDATORY)
52	System Admin Country Code		System Administrator Country Code (MANDATORY)
53	ISSO Name		ISSO name.
54	ISSO Branch		ISSO branch.
55	ISSO Organization		ISSO organization.
56	ISSO Address1		ISSO address.
57	ISSO Address2		ISSO address.
58	ISSO Phone		ISSO UNCLASSIFIED phone number.
59	ISSO Fax		ISSO fax number.
60	ISSO Email		ISSO email address.
61	Intelink Site Info Manager Name		Intelink Site Information Manager name.
62	Intelink Site Info Manager Branch		Intelink Site Information Manager branch.
63	Intelink Site Info Manager Organization		Intelink Site Information Manager organization.
64	Intelink Site Info Manager Address1		Intelink Site Information Manager address.
65	Intelink Site Info Manager Address2		Intelink Site Information Manager address.
66	Intelink Site Info Manager Phone		Intelink Site Information Manager UNCLASSIFIED phone number.
67	Intelink Site Info Manager Fax		Intelink Site Information Manager fax number.
68	Intelink Site Info Manager Email		Intelink Site Information Manager email address.

Table 2.1 Site Configuration Worksheet

This page left intentionally blank

Chapter 3

Installation

The purpose of this chapter is to provide detailed procedures to install the basic server software. It covers both a new install and an upgrade to an existing one. If this is a new install, make sure you have completed Chapter 2 first. After completing the instructions provided within you must proceed to Chapter 4 to configure and tailor the system. Specific topics covered include:

- Loading the Software and Starting the Setup Script
- Providing Installation Choices
- Confirming Installation Choices
- Configuration Progress
- Installation Verification
- Uninstalling the System (Current or Previous Version)

3.1 Loading the Software and Starting the Setup Script

1 Start a terminal window (xterm shell):

At the command line type:
/usr/openwin/bin/xterm <cr>

or launch a Terminal window off the desktop. You may want to launch two windows just in case you might want to monitor some part of the process or need to look something up during the process.

2 Within this new window login as super-user on the machine you wish to install:

su - root <cr>

3 Insert the distribution CD into the CD-ROM drive.

At the shell prompt, enter:
cd /cdrom/cdrom0 <cr>

4 Execute the setup script.

- *./setup.sh*

The setup script will prompt for the type of installation. The available options are Full and Upgrade. Figure 3.1 shows this screen.

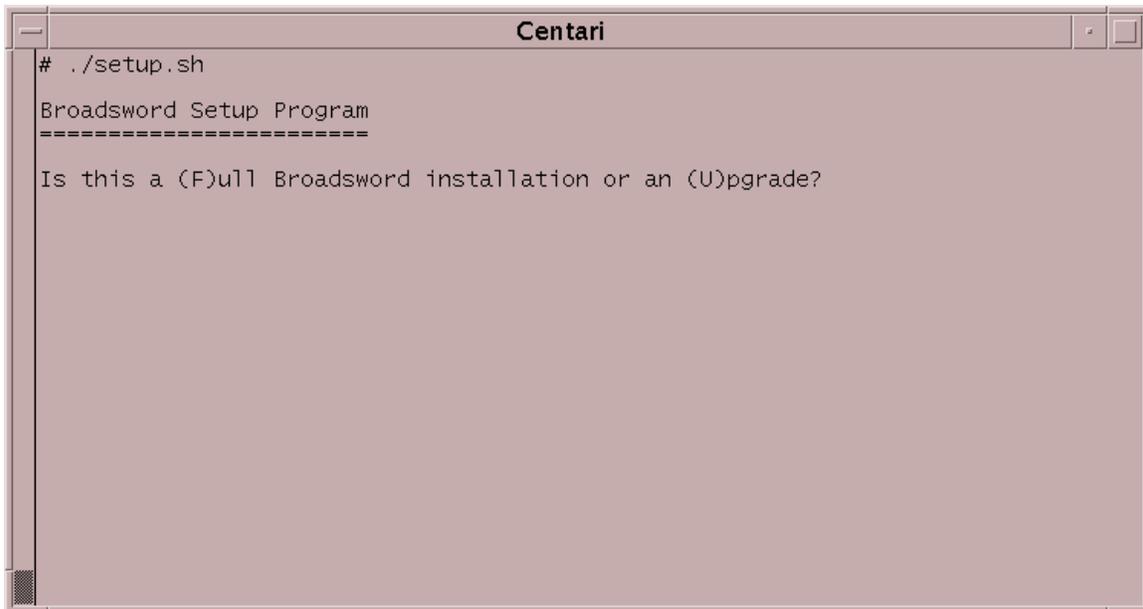


Figure 3.1 - Setup Script (Installation Type)

Note: Defaults are shown in square brackets [] and may be chosen by pressing "Enter."

In the case of a full installation, the user will be prompted for the X display name on which to launch the installer GUI (e.g. – adonis:0.0). Figure 3.2 shows this screen.

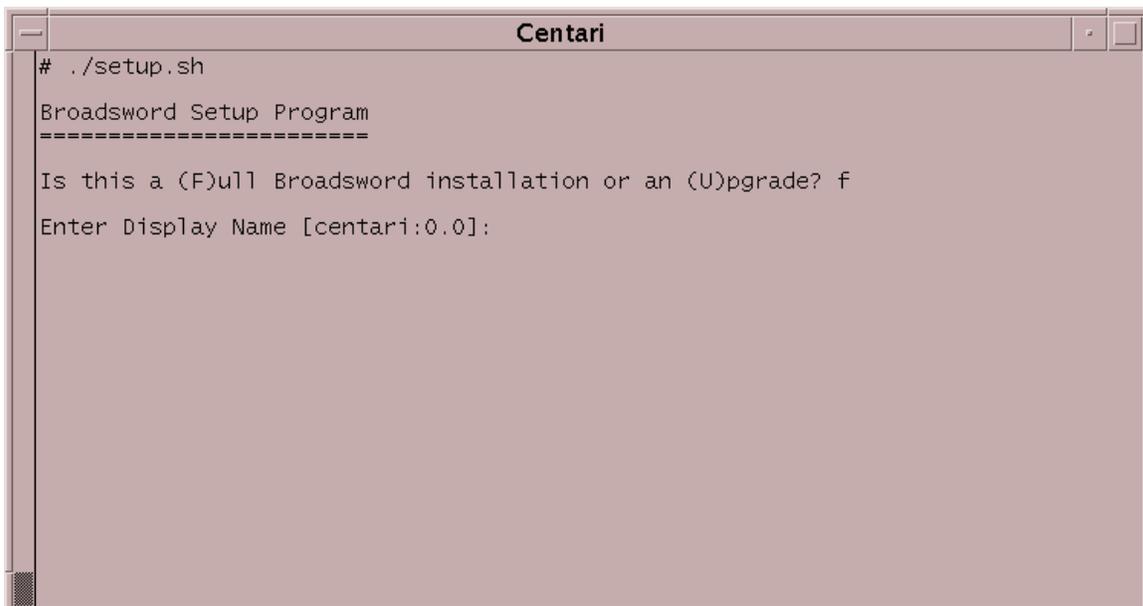
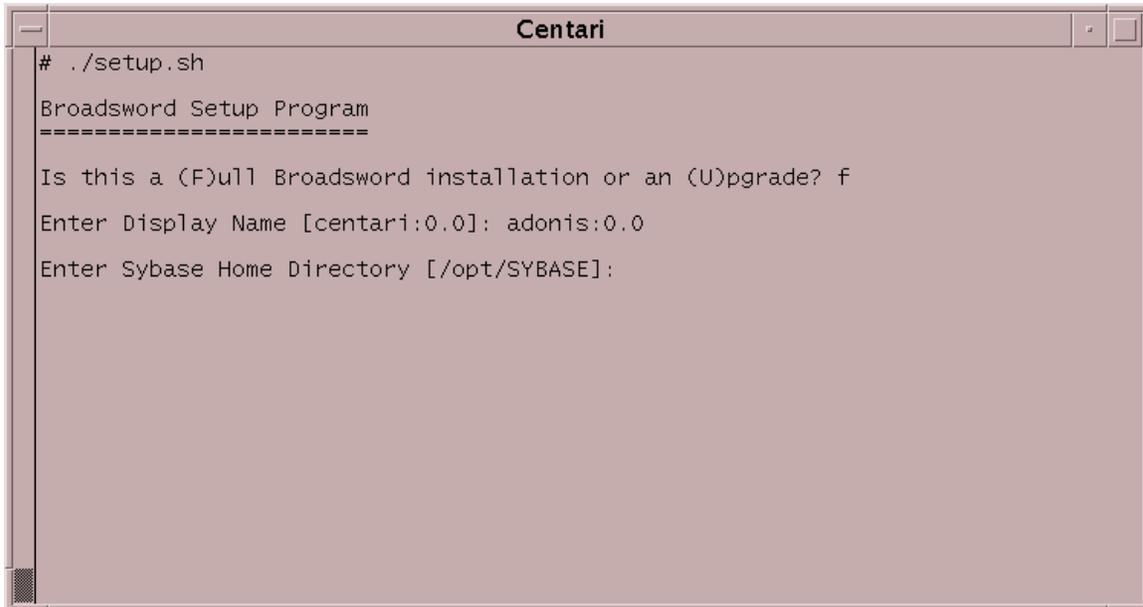


Figure 3.2 - Setup Script (X display Setup)

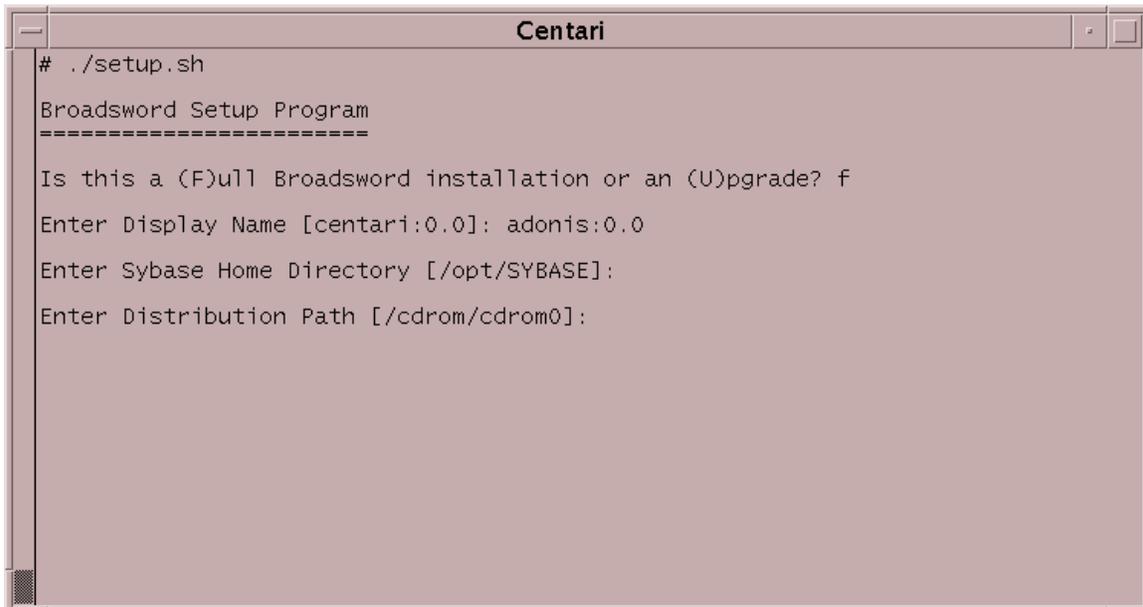
Next, the user will be prompted for the directory on the server where the Sybase product is located (refer to Worksheet #7 in the previous chapter). Figure 3.3 shows this screen.



```
Centari
# ./setup.sh
Broadsword Setup Program
=====
Is this a (F)ull Broadsword installation or an (U)pgrade? f
Enter Display Name [centari:0.0]: adonis:0.0
Enter Sybase Home Directory [/opt/SYBASE]:
```

Figure 3.3 – Setup Script (Sybase directory)

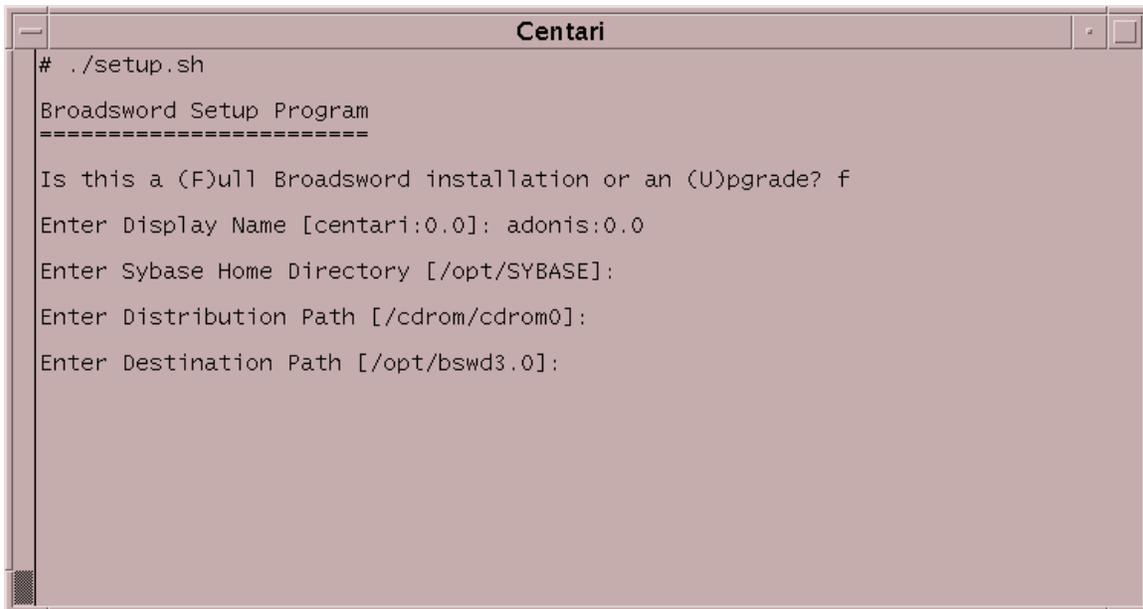
Next, the user is prompted for the directory in which the Broadsword distribution tar files are stored. In general, this will be the distribution CD. Figure 3.4 shows this screen.



```
Centari
# ./setup.sh
Broadsword Setup Program
=====
Is this a (F)ull Broadsword installation or an (U)pgrade? f
Enter Display Name [centari:0.0]: adonis:0.0
Enter Sybase Home Directory [/opt/SYBASE]:
Enter Distribution Path [/cdrom/cdrom0]:
```

Figure 3.4 – Setup Script (Distribution Path)

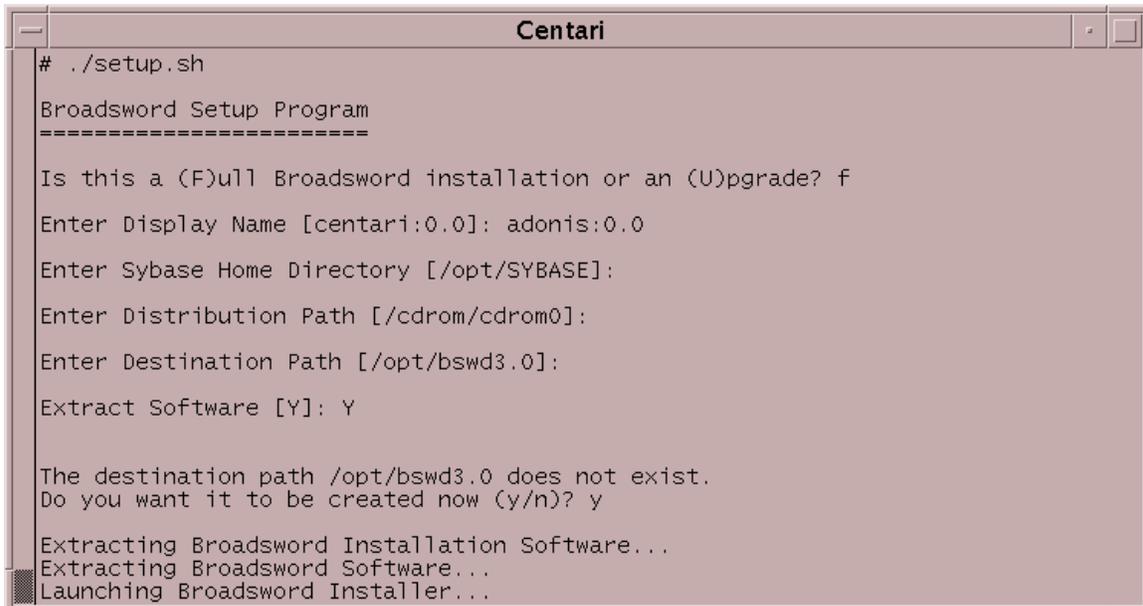
Next, the user is prompted for directory in which the Broadsword software should be installed. Figure 3.5 shows this screen.



```
Centari
# ./setup.sh
Broadsword Setup Program
=====
Is this a (F)ull Broadsword installation or an (U)pgrade? f
Enter Display Name [centari:0.0]: adonis:0.0
Enter Sybase Home Directory [/opt/SYBASE]:
Enter Distribution Path [/cdrom/cdrom0]:
Enter Destination Path [/opt/bswd3.0]:
```

Figure 3.5 – Setup Script (Destination Path)

Finally, the user will be asked to confirm extraction of the Broadsword installation. This should always be answered 'Y', unless the software has already been extracted fully. After confirming this, if the user has not created the install directory already, he will be prompted to create it at this time. Figure 3.6 shows this screen.



```
Centari
# ./setup.sh
Broadsword Setup Program
=====
Is this a (F)ull Broadsword installation or an (U)pgrade? f
Enter Display Name [centari:0.0]: adonis:0.0
Enter Sybase Home Directory [/opt/SYBASE]:
Enter Distribution Path [/cdrom/cdrom0]:
Enter Destination Path [/opt/bswd3.0]:
Extract Software [Y]: Y

The destination path /opt/bswd3.0 does not exist.
Do you want it to be created now (y/n)? y

Extracting Broadsword Installation Software...
Extracting Broadsword Software...
Launching Broadsword Installer...
```

Figure 3.6 – Setup Script Completion

After all questions above have been answered, the setup script will launch either the Installation or Upgrade script, whichever is appropriate. The remainder of this chapter explains the details of the Installation process. If performing an Upgrade, the Upgrade script will take over the remainder of the Upgrade process, prompting for any additional information, if required.

Note: Currently, upgrades cannot be performed between major releases (i.e. 2.0-->3.0). A full installation must be run instead, since during this process a new, separate audit database is created, thereby allowing both versions of Broadsword to coexist. However, the installer is still given the opportunity to import various items from the previous Broadsword version (i.e. Users' preferences, Cataloging Templates, Profiles, Data Elements, and Backside sources). If unsure whether an upgrade is possible, select the Upgrade option from the setup script initially - this will be determined automatically.

Backside source information that is imported from a previous version should be verified by the system administrator, as several of the sources may require additional configuration information to function properly.

3.2 Providing Installation Choices

After the install script has successfully extracted the two tar files, it will launch the graphical portion of the install process. This portion will take the installer step by step through the remainder of the installation process. Figure 3.7 shows the initial screen.



Figure 3.7 - Initial Installation Screen

3.2.1 Providing CD-ROM Registration Information

After clicking the "OK" button the installer needs to enter the Registration Name and serial Number found on the Broadsword distribution CD-ROM. This information is found in Worksheet #1 and #2 in the previous chapter. If a valid combination is not entered the installation will not continue. After the installation is completed, this information is placed on the Broadsword "About" page for future reference. Refer to Figure 3.8 for this screen.



Figure 3.8 - Registration Screen

3.2.2 Determining the Import Preference

After clicking the “Next” button the installer is asked whether they would like to import various items from a previous version or Broadword. Figure 3.9 shows this screen. If “No” is selected the import path will be ignored.

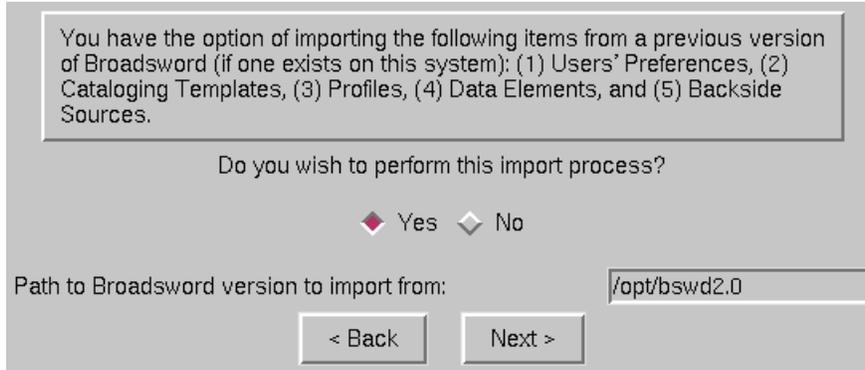


Figure 3.9 - Import Screen

FIELDS VALIDATED	
Import Path (Previous version)	File <Path Entered>/client/bin/conan EXISTS

Table 3.19 - Fields Validated

Note: If importing from a previous version, or if Broadword was previously installed on this server, the following commands need to be executed as root on the Broadword server:

```
# cd /etc/rc3.d  
# mv SS99zstart_bswd2 old.SS99zstart_bswd2
```

3.2.3 Database Configuration

After clicking the “Next” Button, the install script asks whether the database will exist as a separate Data Server or share an existing server. Each Data Server requires an individual license. If a site has a site license for Sybase, then both options are available to the site.

Note: The existence of Sybase licenses is **NOT** determined automatically by the installer; it is up to the site personnel to determine this. If the site has only a single server license, the only option available to the site is to install the Database under the existing Data Server. The disadvantage of using a shared Data Server is that if it goes down for some reason, all the Databases running under the Data Server will go down. This becomes a reliability concern.

Note: During this installation, there are several points at which device names and sizes are requested (e.g. – TempDevice, MasterDevice, etc.). It is

possible that an error will occur stating that there is insufficient disk space to create the device. If the amount of unused space on the disk is greater than 2 gigabytes, the amount of free space detected by Sybase will be incorrect. This is a known Sybase problem. In order to fix this problem, the system administrator must temporarily fill the extra space on the file system until the free space is just slightly less than a multiple of 2 gigabytes. For example, if the partition in question had 4,299,162 Kbytes (about 4.1 Gbytes) free, then filling up an additional 104,900 Kbytes (just over .1 Gbytes) will fix the problem.

3.2.3.1 Creating a New Data Server

Figure 3.10 provides a sample of this screen. The default option is to “Create new”. If the “Share existing” option is picked, skip to Section 3.2.3.2.

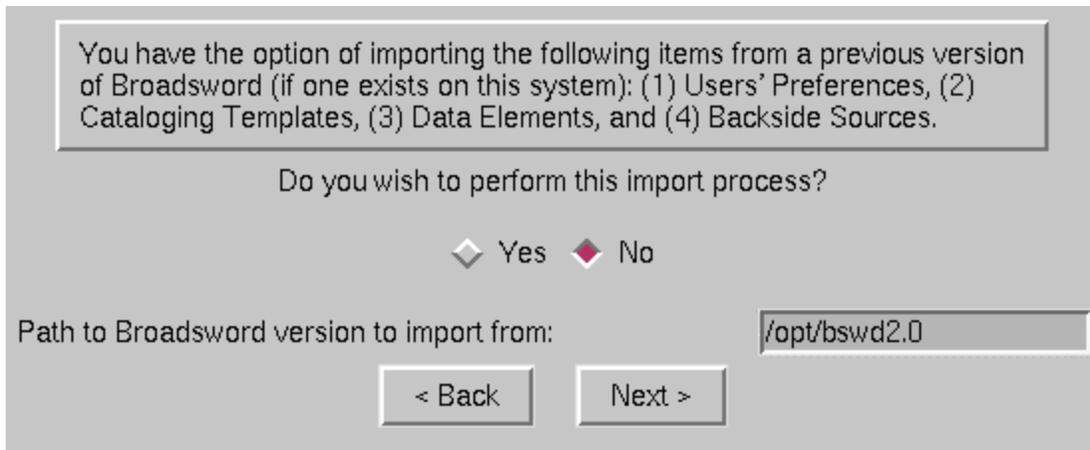


Figure 3.10 - “Creating the Data Server” Screen

If the “Create new” option is chosen (as shown in Figure 3.11), the installation process will next ask for information required to configure the Data Server.

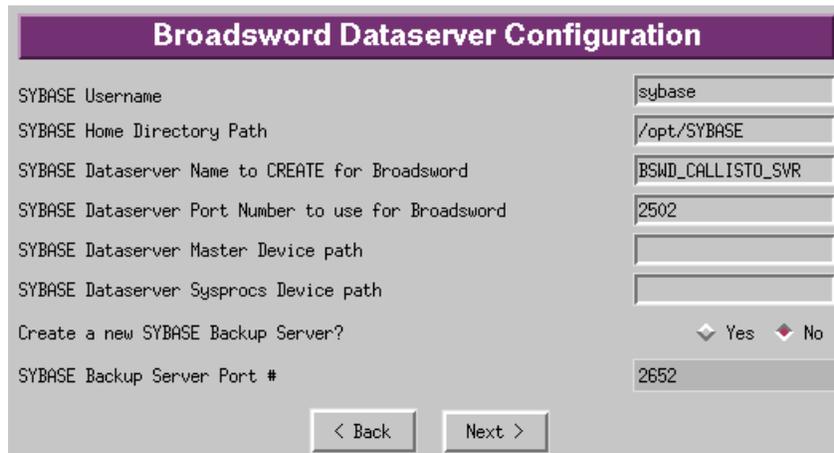


Figure 3.11 - Initial Database Configuration Screen

Note: The *SYBASE Dataserver Name* can contain only letters, numbers, and underscores. In addition, it must begin with a letter.

A number of the default values have been entered. The installer must verify these values along with entering the additional requested information. The additional requested information specifically identifies where Sybase will physically write its data. The device path can be either the full path to a raw partition or the full path to a file system. Figure 3.12 shows the sample screen with the device paths filled in and the creation of a SYBASE Backup Server.

Note: The new dataserver created will have an administrator (sa) password that is empty. To set a password, please refer to Appendix C.

Figure 3.12 - Example Database Configuration Screen

FIELDS VALIDATED	
Sybase Username	Username entered exists on system.
Sybase Home Directory Path	File <Path Entered>/bin/dataserver EXISTS.
Sybase Dataserver Name	Name entered is a currently defined dataserver (when in sharing mode). Also, when in sharing mode, verifies that dataserver entered is running.
Sybase Administrator Password	Installer enters it twice AND password is verified by doing test login into dataserver.
Dataserver Port #	Port number is not already in use.
Master Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (30 or 60 MB).
Sysprocs Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (30 or 60 MB).
Backup Server Port #	Port number is not already in use.

Table 3.2 - Fields Validated

After entering the requested information and pressing the “Next” button, the install process asks for information to configure the temporary device for Sybase. Figure 3.13 provides an example of this screen with both the path and size entered.

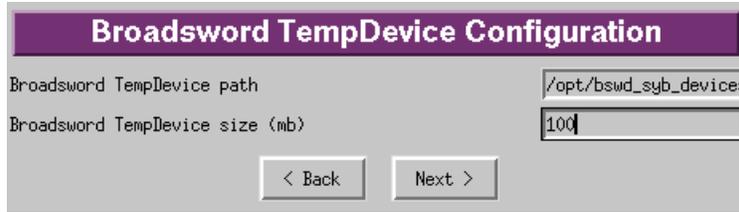


Figure 3.13 - Sample “TempDevice Configuration” Screen

The next step in the installation process is to configure the Sybase Data and Log Devices. Similar information as with the Temporary Device portion is requested. Figure 3.14 provides an example of this screen.



Figure 3.14 - Sample “Database Configuration” Screen

FIELDS VALIDATED	
Data Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device.
Log Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device.

Table 3.3 Fields Validated

At this point all the necessary information to configure the Data Server is complete. The installation process will next request information needed to configure the Gatekeeper. Skip to section 3.2.4, below to proceed with the installation.

3.2.3.2 Sharing an Existing Data Server

If the “Share existing” option is chosen, as shown in Figure 3.15, the installation process will next ask for information required to configure the Database.

Note: The Master, Sysprocs, and Temp device information are not required when sharing an existing dataserver. These values will be the same as the those specified for the original dataserver.



Figure 3.15 - "Sharing an Existing Data Server" Screen

A number of the default values have been entered. The installer must verify these values along with entering the additional requested information. The additional requested information specifically identifies where Sybase will physically write its data. Figure 3.16 provides the initial, default screen, while Figure 3.17 shows the sample screen with the device paths filled in.

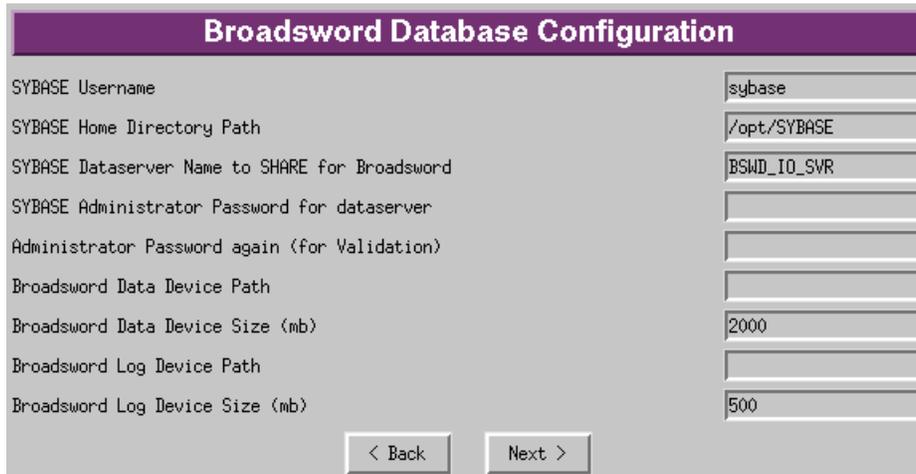


Figure 3.16 - Initial Database Configuration Screen

Sybase can use either raw partitions or files for the data and log devices. The example that is provided in Figure 3.17 uses raw partitions for both the data and log devices. It also changes the sizes of each of these devices. After filling in all the blanks, press the "Next" button. At this point the information provided is validated and checks whether the dataserver (i.e. SYBASE) is running. If not, a warning message is presented, providing the procedure to bring it up. After successfully starting the server the process can continue.

Figure 3.17 - Example Database Configuration Screen

FIELDS VALIDATED	
Sybase Username	Username entered exists on system.
Sybase Home Directory Path	File <Path Entered>/bin/dataserver EXISTS.
Sybase Dataserver Name	Name entered is a currently defined dataserver (when in sharing mode). Also, when in sharing mode, verifies that dataserver entered is running.
Sybase Administrator Password	Installer enters it twice AND password is verified by doing test login into dataserver.
Data Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (entered by installer).
Log Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (entered by installer).

Table 3.4 - Fields Validated

3.2.4 Gatekeeper Configuration

The next part of the installation process is to provide information necessary to configure the Gatekeeper. This section provides the initial login (always 'bswduser') and password for the administrator to log into the interface and further configure the system. It also identifies whether the system will be co-located with an existing IPL 1.0. Figure 3.18 provides a sample of the Broadsword Gatekeeper Configuration Screen.

Broadsword Gatekeeper Configuration

'bswduser' Account Password

'bswduser' Account Password again (for Validation)

'cdimuser' Account Password

'cdimuser' Account Password again (for Validation)

Are you currently running an IPA or IPL 1.0 on THIS MACHINE? Yes No

Path to IPA/IPL 1.0 software on THIS MACHINE

< Back Next >

Figure 3.18 - Broadsword Gatekeeper Configuration Screen

FIELDS VALIDATED	
'bswduser' Password	Installer enters it twice.
'cdimuser' Password	Installer enters it twice.
IPA/IPL 1.0 S/W Path	File <Path Entered>/ipadirs EXISTS.

Table 3.5 - Fields Validated

3.2.5 Client Configuration

After clicking on the "Next" button the configuration information is processed and validated. If successful, the installation process will continue with the configuration of the Broadsword Client. In this section, the determination as to whether both a protected and a registered server will be configured, their respective HTTPD ports, the network, the IP address of the Broadsword Program Office Home Page and the location of the GIF image used to personalize the Client Home Page. Figure 3.19 displays this page.

Figure 3.19 - Broadsword Client Configuration Screen

FIELDS VALIDATED	
Client Protected HTTP Port #	Port number is not already in use.
Client Registered HTTP Port #	Port number is not already in use.
'bswdreg' Password	Installer enters it twice.
SIPRNET Broadsword Program Office IP Address	If Network Type selected is SIPRNET, this field cannot be empty.
System Group Name	Group name EXISTS on system.
Homepage Logo File	File entered EXISTS AND has gif, jpg, or jpeg extension.
Log Rolling Count	Must be greater than or equal to zero.

Table 3.6 Fields Validated

3.2.6 LDAP Configuration

The next part of the installation process is to provide information necessary to configure the Access & Authentication Module (AAM), if its use is desired, and there is an LDAP server currently accessible on this server. Refer to Figure 3.20 for the necessary information. If the AAM is used, you can optionally migrate your Solaris or CSE-SS user accounts into Broadsword.

Figure 3.20 - LDAP Configuration

FIELDS VALIDATED	
LDAP Port #	If AAM use is desired, this field cannot be empty.
LDAP Bind DN	If AAM use is desired, this field cannot be empty.
LDAP Bind Password	Installer enters it twice.
Current Organization	If AAM use is desired, this field cannot be empty.

Table 3.7 Fields Validated

3.2.7 POC Configuration

The final portion of the installation process is to configure the Support Page. This page provides the necessary site's Points of Contacts (POCs) for System Administration, ISSO and Intelink Site Manager. The System Administration fields are mandatory. Figure 3.21 provides an example of the POC screen.

System Administrator		ISSO	
Note: These fields are mandatory:			
Name	<input type="text"/>	Name	<input type="text"/>
Branch	<input type="text"/>	Branch	<input type="text"/>
Organization	<input type="text"/>	Organization	<input type="text"/>
Address1	<input type="text"/>	Address1	<input type="text"/>
Address2	<input type="text"/>	Address2	<input type="text"/>
Phone	<input type="text"/>	Phone	<input type="text"/>
FAX	<input type="text"/>	FAX	<input type="text"/>
Email	<input type="text"/>	Email	<input type="text"/>
City	<input type="text"/>		
State/Locality	<input type="text"/>		
Country Code	US		

Intelink Site Info Manager	
Name	<input type="text"/>
Branch	<input type="text"/>
Organization	<input type="text"/>
Address1	<input type="text"/>
Address2	<input type="text"/>
Phone	<input type="text"/>
FAX	<input type="text"/>
Email	<input type="text"/>

Figure 3.21 - Point of Contact Information Screen

Note: The email address in the *System Administrator* area of this screen is the address that receives all system status messages. It is suggested that at sites with more than one administrator, this email address is set to **root**, and that all of the administrators are aliased to receive **root** mail.

3.3 Confirming Installation Choices

Upon entering the POC information, the process continues by providing a screen that displays the configuration information that has been entered thus far. At this point, clicking the “Install” button will continue the installation process. If changes are desired, use the “Back” button to proceed to the screen in which that item was configured. Figure 3.22 is an example of how a new data server confirmation screen and Figure 3.23 is an example of a shared data server confirmation screen.

Broadsword will be configured with these settings:

Import Mode:	Yes
SYBASE User Name:	sybase
SYBASE Home Directory:	/opt/SYBASE
SYBASE Dataserver Name:	BSWD_EUROPA_SVR
SYBASE Dataserver Port:	2503
SYBASE Dataserver Master Path:	/opt/bswd_syb_devices
SYBASE Dataserver Sysprocs Path:	/opt/bswd_syb_devices
SYBASE Backup Server Port:	2653
Broadsword TempDevice Path:	/opt/bswd_syb_devices
Broadsword TempDevice Size:	100
Broadsword Data Device Path:	/opt/bswd_syb_devices
Broadsword Data Device Size:	100
Broadsword Log Device Path:	/opt/bswd_syb_devices
Broadsword Log Device Size:	25
IPA/IPL Path:	N/A
Client Protected HTTP Port #:	80
Client Registered HTTP Port #:	N/A
Network:	Intelink-S
Group Name:	bswd
Logo File:	/opt/bswd3.0/client/docs/gifs/callisto.gif
Rolling Log Count:	10
Use AAM:	No
LDAP Server (if using AAM):	europa
LDAP Port # (if using AAM):	389
LDAP Bind DN (if using AAM):	cn=Directory Manager
Current Organization (if using AAM):	
Migrate Solaris/CSE-SS Accounts (if using AAM):	No

If these settings are correct click Install to start the installation or click Back to make any corrections.

< Back Install

Figure 3.22 - Sample Based on New Data Server Confirmation Screen

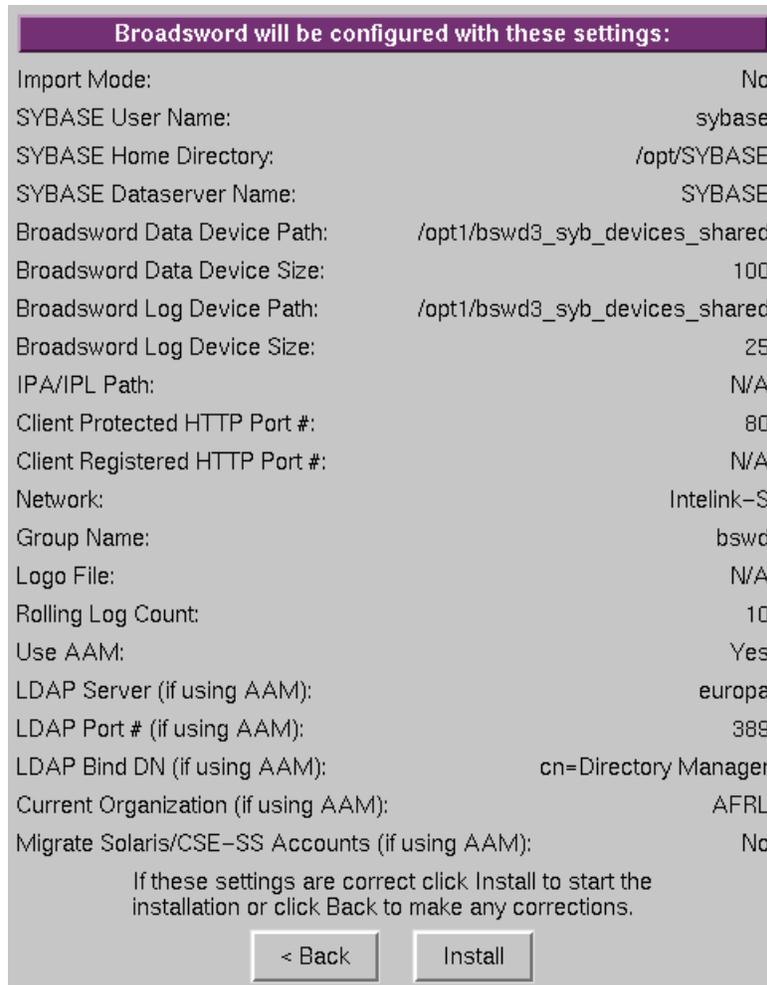


Figure 3.23 - Sample Based on Shared Data Server Confirmation Screen

3.4 Installation Progress

After clicking on the “Install” button, the installation process will continue to make the necessary changes. Two windows will appear to allow for monitoring of the progress. The first is a progress gauge that provides for the percent of the total installation complete, while the second line indicates the percent complete of that specific part. Figure 3.24 provides an example of this screen.

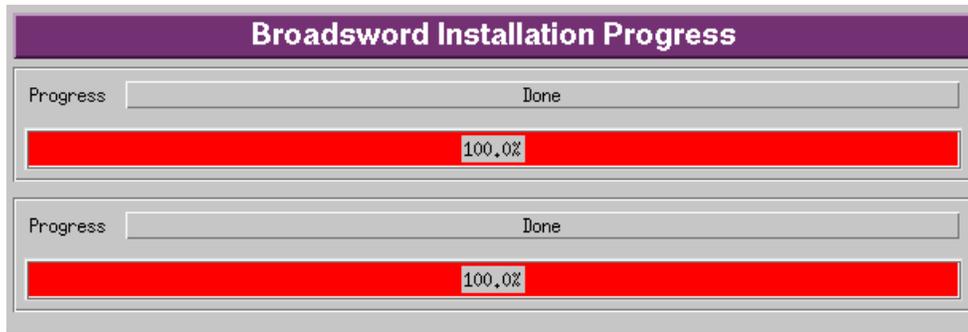


Figure 3.24 - Example of the Progress Gauge

The second screen provides a log of the process. Figure 3.25 provides a sample log screen. The information contained on the screen is also saved into a file for later reference. Also the configuration information is saved and if the installation process is restarted, it will read the saved file.



```
->Initialize Install
->Broadsword Dataserver Configuration
->Broadsword Database Configuration
--->Loading Schema
--->Loading Indexes
--->Loading Stored Procedures
->Configuring Broadsword Server
--->Updating Configuration Files
--->Encrypting Configuration Files
->Configuring Broadsword Client
--->Updating Configuration Files
--->Configuring Homepages
--->Configuring POC Page
--->Installing Logo File
--->Installing Initial Statistics Page
Initialize: /opt/bswd3.0/etc/local.gkpr.conf.template from "def" files in: /opt/bswd3.0/client/etc/dataelements/local
Gkpr Config Files Updated Successfully!
Gkpr Config Files Updated Successfully!
->Starting Broadsword Processes
--->

Default BSWD startup? (Y/N/Q) [Y]: You have chosen the following BSWD startup options:
  Start Sybase ..... Yes
  Start BSWD background APs..... Yes
  BSWD executables..... /opt/bswd3.0/bin
Start these portions of BSWD? (Y/N/Q) [Y]: Starting Sybase...
SYBASE SQL Server is already running
SYBASE Backup Server is already running

Checking validity of DISPLAY.
Testing...

DISPLAY = europa:0.0 is valid.

Starting Background APs...
  Starting /opt/bswd3.0/client/bin/conan
  Starting /opt/bswd3.0/bin/gatekeeper.SVR4
  Starting /opt/bswd3.0/bin/gatekeeperftp.SVR4
  Starting /opt/bswd3.0/bin/gatekeepermrs.SVR4
  Starting /opt/bswd3.0/bin/gatekeepermsl.SVR4
  Starting /opt/bswd3.0/bin/jivacron
Wait 5 seconds, then tickle MSL

Broadsword 3.0 Process Status (Thu May  4 14:37:34 EDT 2000):

running  /opt/bswd3.0/bin/gatekeeper.SVR4
running  /opt/bswd3.0/bin/gatekeeperftp.SVR4
running  /opt/bswd3.0/bin/gatekeepermrs.SVR4
running  /opt/bswd3.0/bin/gatekeepermsl.SVR4
running  /opt/bswd3.0/bin/jivacron
running  /opt/bswd3.0/client/bin/conan

->Cleaning up
->Done
--->Done
```

Figure 3.25 - Sample Log Screen

When the installation is complete, the last screen displayed will be the “Installation Complete” screen (as shown in Figure 3.26).

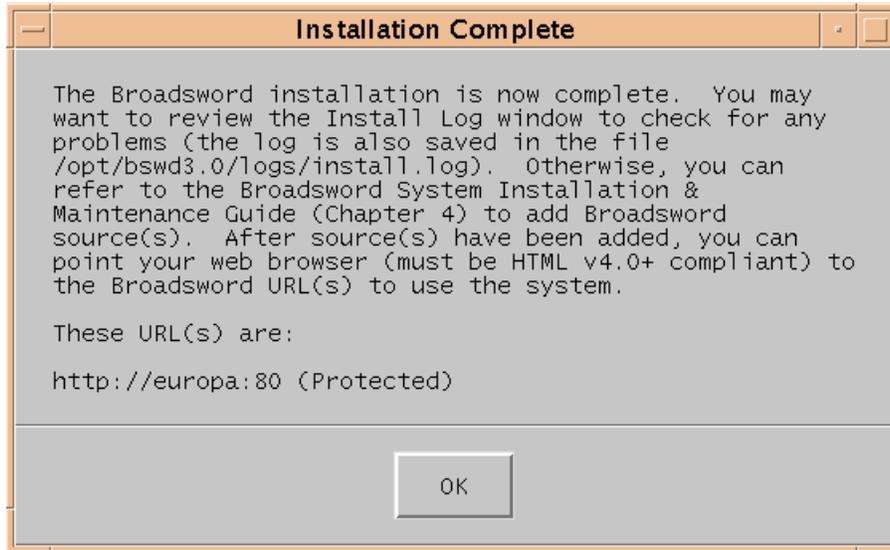


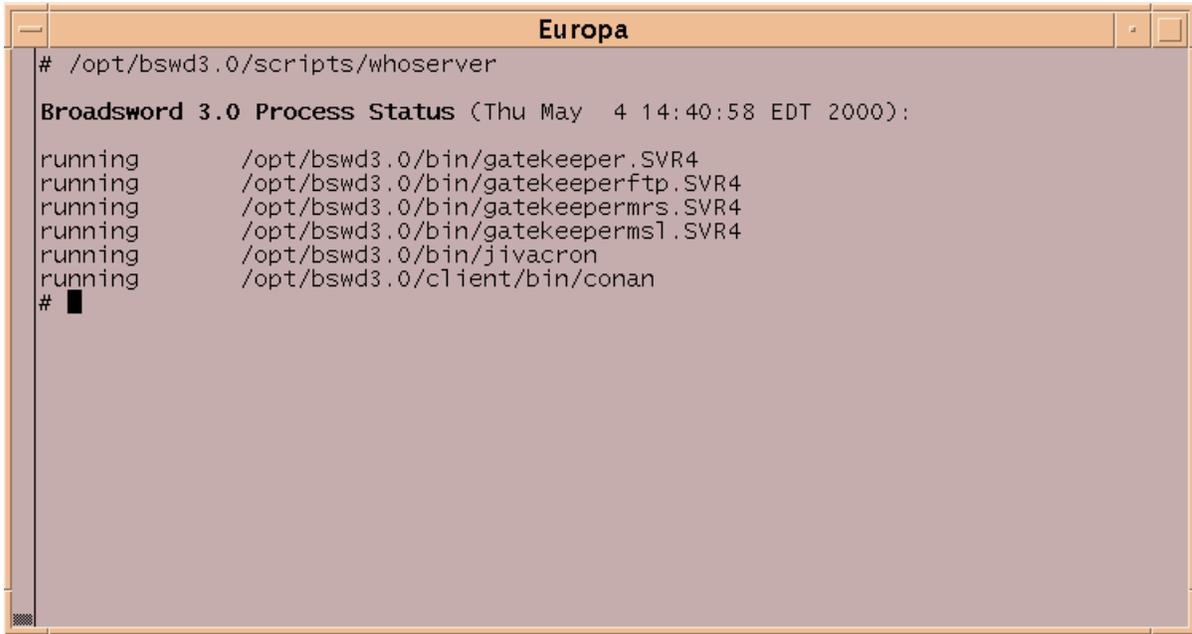
Figure 3.26 - Installation Complete

3.5 Installation Verification

At this point the installation process is complete. To verify the installation has completed correctly, the following command may be executed:

`/opt/bswd3.0/scripts/whoserver`

If all processes are shown to be running, the installation most likely has succeeded. Figure 3.27 provides a sample listing of the processes that should be running. If one or more of the processes are not running, check the log window (or the log file) for any obvious problems during the installation. If the problem cannot be fixed at this point contact the Broadsword help desk, otherwise continue to Chapter 4 – System Configuration.



```
# /opt/bswd3.0/scripts/whoserver  
Broadsword 3.0 Process Status (Thu May  4 14:40:58 EDT 2000):  
running      /opt/bswd3.0/bin/gatekeeper.SVR4  
running      /opt/bswd3.0/bin/gatekeeperftp.SVR4  
running      /opt/bswd3.0/bin/gatekeepermrs.SVR4  
running      /opt/bswd3.0/bin/gatekeepermsl.SVR4  
running      /opt/bswd3.0/bin/jivacron  
running      /opt/bswd3.0/client/bin/conan  
# █
```

Figure 3.27 - Sample Listing of Processes Running

This page left intentionally blank

Chapter 4

System Configuration

Once the installation of the basic system is completed, site specific configuration must be performed. This chapter provides details on how to add local sources, modify system and Gatekeeper parameters, register the Gatekeeper with others, set up access to remote sources and tailor data element values. To begin, start your web browser and type the URL of the newly installed Broadsword system (e.g. – <http://callisto:80>) in the Location field. When the login screen appears, enter bswduser as the username. Also enter the bswduser account password as entered during the installation process (Section 3.2.4), and click the “Accept” button. By selecting the System Configuration item (under the Administration pop down menu), the administrator is presented with a set of options as shown in figure 4.1.

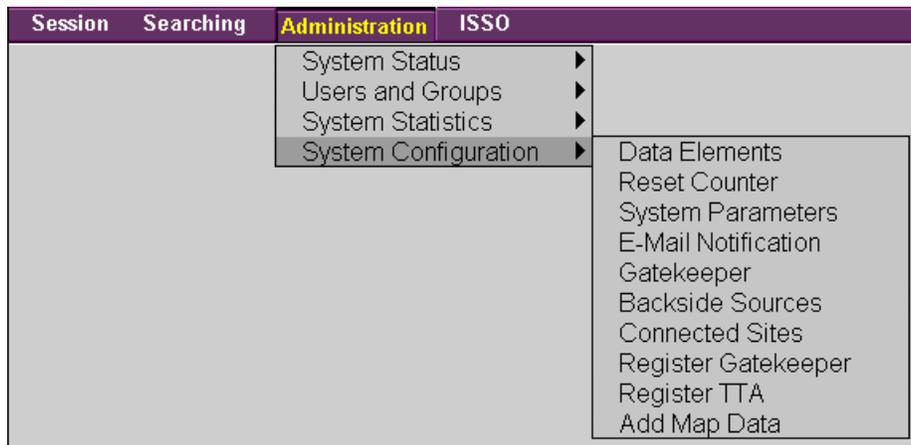


Figure 4.1 System Configuration Tools

4.1 Backside Sources

After the initial installation, there will be no sources configured; to configure new sources select the “Backside Sources” option. If there are no backside sources to configure, proceed to section 4.2 (Gatekeeper Registration). The page shown in Figure 4.2 will appear. Configuration of sources is usually done by the system administrator or by anyone assigned system administration privileges. Once the desired browser is started, Netscape or Internet Explorer, users can either enter the Gatekeeper’s IP in the URL location of the browser or the name of the Gatekeeper machine. The Broadsword login screen will then appear and the user would log in as normal, entering their username and password, and then selecting the accept button.

After logging in, the user would, as illustrated in Figure 4.1, the user would select the menu item under the **Administration -> System Configuration -> Backside Sources**.

Installed Sources			
Add	Server Type	Remove	Source Description
<input type="radio"/>	IPL		
<input type="radio"/>	IPL20		
<input type="radio"/>	5D		
<input type="radio"/>	AMHS		
<input type="radio"/>	CSIL		
<input type="radio"/>	IESS		
<input type="radio"/>	INT		
<input type="radio"/>	MEPED		
<input type="radio"/>	META		
<input type="radio"/>	MIDB		
<input type="radio"/>	SDB		
<input type="radio"/>	WX		
<input type="radio"/>	AODB		
<input type="radio"/>	ISM		
<input type="radio"/>	IET		

Reset Form Remove Marked Add Source

Figure 4.2 Sample “Backside Sources” Screen

To add a source, select the desired *Server Type* radio button in the Add column, and click the *Add Source* button in the bottom bar (the Add Source button will become sensitive when a source has been selected). A second page will be displayed providing configuration items for that specific source. Figure 4.3 provides an example screen for adding an IPL source. Appendix A provides screens for each of the supported sources.

Note: Sybase will not accept a name that begins with a numeric digit. For example, use FIVED not 5D.

Note: Both AODB and FIRES are backside sources that that require configuration in addition to that provided in the “Backside Sources” section of the interface. After adding the FIRES or AODB source, telnet into the Broadsword server, su to *root* and execute the following:

```
% cd /opt/bswd3.0/odbc/oracle7/network/admin/tnsnames.ora
```

```
% vi tnsnames.ora
```

In this file, there will be a record for the FIRES or AODB source. The IP address and port number listed should be the same as the IP and port

numbers listed on the source's server. For more information on how to get this information from the source's server, contact your local administrator for that data source.

Note: For the backside sources (5D)Demand Driven Direct Digital Dissemination and (IESS) Imagery Exploitation Support System, the following fields need to be filled out ONLY if they are accessed through an IPL:

- IPL Host IP Address
- IPL TCP/IP Port
- IPL Site Name
- IPL Host IP Address
- IPL Order Status Port
- IPL 1.0 Account for IEISS or IPL 2.0 Account for 5D
- IPL 1.0 Password for IEISS or IPL 2.0 Account for 5D

Add New IPL Source		
Configuration Item	Value	Item Description
IPL Description	<input type="text" value="IPL 1.0 Source"/>	This field describes the IPL. This will appear in the preferences section of the client.
Query Max Hits	<input type="text" value="0"/>	This field specifies the max number of hits to return for a query. If zero, then there is no limit.
IPL Host IP Address	<input type="text"/>	This field specifies the IP address the ipl_plugin will use to connect to the IPL "pcr" process.
IPL TCP/IP Port	<input type="text" value="5004"/>	This is the TCP/IP port that the ipl_plugin will use to connect to the IPL "pcr" process.
IPL Site Name	<input type="text"/>	This is the site name of the IPL to query. This should match the IPL Site Name as configured in the IPL download file.
IPL Host IP Address	<input type="text"/>	This is the IP address of the IPL to query. This should match the IPL IP Address as configured in the IPL download file.
IPL Order Status Port	<input type="text" value="5007"/>	This is the port that IPL will send status messages to after a order request.
Harvest TCP/IP port	<input type="text" value="8501"/>	This is the TCP/IP port that the Harvest daemon is using.
Format Conversion Flag	<input type="text" value="N"/>	If this field is set to Y, then Broadsword will perform all conversion/compression.
IPL Account	<input type="text" value="ipamngr"/>	This is the IPL account Broadsword uses to connect to IPL.
Access Permission Override	<input type="text" value="Don't Override"/>	This field is used to temporarily override source access that was granted to users via the User/Group Privileges Administrator functions.
IPL Password	<input type="text"/>	This is the IPL password Broadsword uses to connect to IPL.
Access Control:	<input type="text" value="No Access"/>	This denotes whether to allow no users, only Local users, or All users access to this source.

Figure 4.3 Sample "Add New IPL Source" Screen

Note: Several of the sources accessed through Broadword require an account with which to access the source (MIDB, IESS, etc.). These accounts have a set of minimal source/database accesses that the source must support for all of the Broadword functionality to work properly. For information on a specific source, see Appendix A.

After submitting a valid source configuration, the new source will be added to the list of installed sources. You can configure multiple sources per type. Refer to Figure 4.4.

The values provided under the “Access Control” configuration item define user access to the source, the three options are **No Access**, **Local Access Only**, and **Local & Remote Access**. During the registration process with a Keymaster, the local map will be sent to the Keymaster and further distributed to all other Gatekeepers. If the “Access Control” is set to **Local & Remote**, then that source will be available to remote Gatekeepers. This setting may be overridden by editing the source later and utilizing the “Access Permission Override” option. The “Access Permission Override” option allows the system administrator to selectively allow or not allow temporary access to a particular source. Permission to access a source is done through the User and Group Privileges.

The “Access Control” configuration item determines whether the source is available by default to users. If “No Access” is chosen, then no local or remote users will have access by default. If “Local Access Only” option is selected then only local users to the Gatekeeper will have default access to that source. If “Local & Remote Access” option is selected then all users, both local and remote, will have default access to that source.

Table 4.1 summarizes the possible options.

Access Control	Don't Override	Deny Access To All Users	Deny Access To All Remote users
No Access	As Is	No Access	No Access
Local Access Only	Access to all local users	Users must be added individually	Access to all local users
Local & Remote Access	Access to all users	No remote users, local access must be individually granted.	Access to all local users

Table 4.1 Summary of Remote Access Controls

Installed Sources			
Add	Server Type	Remove	Source Description
<input type="radio"/>	IPL	<input type="checkbox"/>	IPL 1.0 at Sun via Saturn
		<input type="checkbox"/>	IPL 1.0 at Titan
		<input type="checkbox"/>	Roger Dummy IPL10
<input type="radio"/>	IPL20	<input type="checkbox"/>	IPL 2.1 Source at Orion via Saturn ODBC Version
		<input type="checkbox"/>	IPL 2.1.2 at aerial via SATURN 3.0
<input type="radio"/>	5D	<input type="checkbox"/>	5D at Saturn via Saturn
		<input type="checkbox"/>	5D at 480ig Via Saturn
		<input type="checkbox"/>	5D at Titan via Saturn
<input type="radio"/>	AMHS	<input type="checkbox"/>	AMHS at Elara via Saturn
<input type="radio"/>	CSIL	<input type="checkbox"/>	CSIL at DIA via Saturn
<input type="radio"/>	IESS	<input type="checkbox"/>	IESS at IESS0 via Saturn
<input type="radio"/>	INT	<input type="checkbox"/>	Intelink-Hydra Search via Saturn
<input type="radio"/>	MEPED	<input type="checkbox"/>	MEPED via Saturn
<input type="radio"/>	META	<input type="checkbox"/>	Intelink-Meta Search via Saturn
<input type="radio"/>	MIDB	<input type="checkbox"/>	MIDB at Hoth via Saturn
		<input type="checkbox"/>	MIDB Source
		<input type="checkbox"/>	MIDB Source
		<input type="checkbox"/>	MIDB Source

Figure 4.4 Sample “Backside Sources” Screen with Sources Configured

To change an existing source configuration, click on the *Source Description* for the one you wish to update. The system will display the same list of fields used to initially add that source, along with the current configuration. The fields may be edited and resubmitted. If the original “Access Control” was set to **No Access**, then the value listed under “Access Control” will be either **No Change (No Access)** or **No Change (User List)**. If no users have been granted access to the source, then the value will be either **No Change (No Access)**. If at least one user has been granted access to the source through the **Users and Groups** section of the interface, then the value will be **No Change (User List)**.

To remove an existing source, check the appropriate box(es) in the *Remove* column immediately to the left of the *Source Description*. Then click the *Remove Marked* button in the bottom bar.

Note: TCP wrappers on the workstation can cause difficulty in pulling products. There are two different ways to pull products: “Pull to view” and “Pull to destination.” It is important to understand how these two different methods work. “Pull to view” will pull the product to the Broadword server and display it to the user via the browser. “Pull to destination,” (when a valid choice for the source selected) will cause the Broadword server to ftp the product to a destination computer specified by the user. For both methods, connected backside IPL, 5D, IDEX and NDS sources must be able to ftp to the Broadword server. For the “Pull to

destination” method, the Broadword server must be able to ftp to the workstation or other system specified by the user.

4.1.1 Backside Sources (both methods)

If you are running CSE-SS on the Broadword server, see the “Network Management” section of the “Trusted User Training” manual for a description of how to configure TCP/IP wrappers to allow the IPL and IDEX servers to ftp to the Broadword server.

If you are running UNIX with TCP wrappers on the Broadword server but are not running CSE, be sure that the `/etc/hosts.allow` file is configured to allow ftp access from the IPL and IDEX servers. For example, the following line should appear in `/etc/hosts.allow` on the Broadword server (if the IP address of the IPL, IDEX or 5D server is 123.123.123.123):

in.ftpd: 123.123.123.123

It is okay to replace “in.ftpd” with “ALL” if you want to allow all the IPL, IDEX or 5D server to use all inetd services on the Broadword server. Review your tcpd manual page for more information.

4.1.2 Pull to Destination

If you are running CSE 1.3 or 1.4 on the destination workstation, see the “Network Management” section of the “Trusted User Training” manual for a description of how to configure TCP/IP wrappers to allow the Broadword server to ftp to the destination workstation.

If you are running UNIX with TCP wrappers on the workstation but are not running CSE, be sure that the `/etc/hosts.allow` file is configured to allow ftp access from the Broadword server. For example, on a Solaris workstation, the following line should appear in `/etc/hosts.allow` (if the IP address of the IPL or 5D server is 123.123.123.123):

in.ftpd: 123.123.123.123

It is okay to replace “in.ftpd” with “ALL” if you want to allow all the IPL or 5D server to use all inetd services. Review your tcpd manual page for more information.

If you are trying to pull to a Windows NT workstation, be sure that it is configured to allow the IPL or 5D server to ftp to it.

4.2 Gatekeeper Configuration

The “Gatekeeper” screen allows the administrator to modify various parameters of the local Gatekeeper. Figure 4.5 presents a sample “Gatekeeper” screen.

Configuration Item	Current Value	Help Description
Gatekeeper Description	Return Gatekeeper	This gives a name visible next to a gatekeeper (i.e. ACOV)
Gatekeeper IP Address		This is the IP Address of the Gatekeeper
Gatekeeper TCP/IP Port	5400	This is the TCP/IP port number the gatekeeper will wait for connections
Point Of Contact		This is the name of the person responsible for maintaining this gatekeeper. This name is also used for registration with a keymaster
POC Phone #		This is the unabbreviated phone number for the POC
POC Email		This is the email address (name@hostname) for the Point of Contact
Organization Name		This is the organization name where this gatekeeper resides
Country Code		This is the 3 character country code where this gatekeeper resides
State or Locality		This is the state or locality where this gatekeeper resides
City		This is the city where this gatekeeper resides
Idle Time Timeout	30	This is the time in minutes the gatekeeper waits for a port activity before closing the connection
Registered User Account	RegisteredUser	This is the name used to login to the Gatekeeper for Registered Users
Profile User Account	ProfileUser	This is the name used to login to the Gatekeeper by the Profile process
Alternate User Account	AlternateUser	This is the name used to login to the Gatekeeper by remote gatekeepers during alternate delivery of a product
Gatekeeper Database Name	BroadSyrbase	This is the name of the database the gatekeeper uses
Gatekeeper Database Account	BroadSyruser	This is the database account the gatekeeper uses to login into the database
LDAP Server IP Address		This is the IP address of the LDAP Server. This is only used in LDAP installations
LDAP Server TCP/IP Port		This is the TCP/IP port that the LDAP Server will wait for connections on. This is only used in LDAP installations
LDAP Bind DN		This is the Distinguished Name (DN) of a user with full access to the LDAP Server. This is only used in LDAP installations
Max User Login Failure	3	This is the number of times a log-in may fail before the user account is locked. This is only used in LDAP installations
User Password History Count	3	This is the number of old passwords remembered for a user. This is only used in LDAP installations
Minimum Number Of Special Characters Required In User Password	2	This is the number special characters required to be in a user's password. The special characters are ! @ # % ^ & * and ~. This is only used in LDAP installations
User Password Expiration		This is the max number of days a user's password is valid. This is only used in LDAP installations
Minimum User Password Length	6	This is the minimum number of characters required in a password. This is only used in LDAP installations
Maximum User Password Length	12	This is the maximum number of characters that can be in a password. This is only used in LDAP installations
Password Dictionary File		This is the fully qualified path to the dictionary file used for validating passwords. This is only used in LDAP installations
Registered User Password	*****	This is the password used to login to the Gatekeeper for Registered Users
Profile User Password	*****	This is the password used to login to the Gatekeeper by the Profile process
Alternate User Password	*****	This is the password used to login to the Gatekeeper by remote gatekeepers during alternate delivery of a product
Gatekeeper Database Password	*****	This is the database password the Gatekeeper uses to login into the database
LDAP Bind DN Password	*****	This is the Distinguished Name (DN) password of a user with full access to the LDAP Server. This is only used in LDAP installations

Figure 4.5 Sample “Gatekeeper” Screen

Several configuration items, their current (editable) values, and help text for each are presented. Select the field(s) of the items that require modification, enter their new value, and when complete, click the “Apply” button. You may click “Reset Form” to revert any changes you have been making to the page and start over.

**It is important to note that, if the Gatekeeper is configured running LDAP, that the Registered User account and Registered User Password data fields be entered with data (see arrows). This information is critical in order for users to pull products to view.*

Note: Apply button will not be sensitized until the user changes at least one value in top section and clicks outside the box.

Note: After applying any changes to this screen, Broadword must be restarted to force it to reread the configuration file. (see Section 7.1)

4.3 System Parameters

The “System Parameters” screen allows the administrator to add/modify site specific parameters. These items fall into three categories: (1) Resetting the Home Page Access Counter, (2) System Parameters and (3) E-mail Notification Parameters.

4.3.1 Reset Home Page Access Counter

The “Reset Home Page Access Counter” screen allows the administrator to reset the access counter that appears on the login screen (to zero). By clicking on the “Home Page Access Counter” checkbox, followed by clicking the “Apply” button that appears in the bottom button bar, the counter will be reset. Figure 4.6 provides a sample of the “Reset Home Page Access Counter” screen.

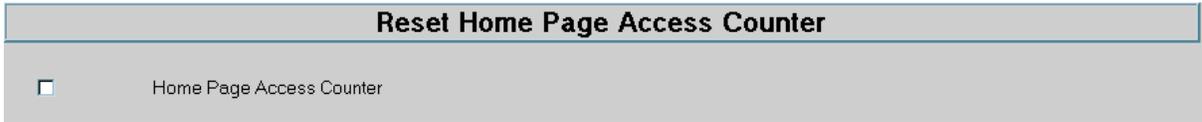


Figure 4.6 Sample “Reset Home Page Access Counter” Screen

4.3.2 Set System Parameters

The “Set System Parameters” section allows the administrator the ability to edit or modify the timeout values used by the client and the size reduction of the thumbnail. Figure 4.7 provides a sample of the “Set System Parameters” section.

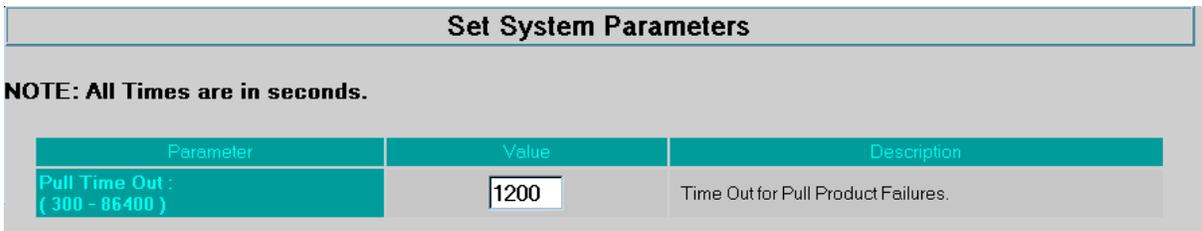


Figure 4.7 Sample “Set System Parameters” Screen

Table 4.2 provides a detailed description for each of these parameters:

Parameter	Description
Pull Time Out	Time Out for Pull Product Failures - The length of time to wait for a product to arrive at the server when pulling a product via the hit list. If the product does not arrive within this time, an error message results. VALID RANGE: 300 - 86400 seconds.

Table 4.2 Summary of Values

4.3.3 Set E-Mail Notification Parameters

The “Set E-Mail Notification Parameters” section allows the administrator to define the items associated with E-Mail or Profile Notification. Figure 4.8 provides a sample screen.

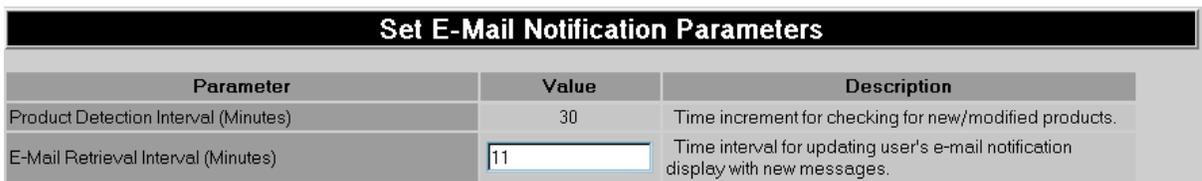


Figure 4.8 Sample “Set E-Mail Notification Parameters” Screen

By clicking on the “**Apply**” button, any changes made to any of the sections (Reset Home Page Access Counter, Set System Parameters, and Set E-Mail Notification Parameters) will be processed. Clicking on the “**Reset Form**” button will return the values to those that previously existed.

4.4 Register Gatekeeper

The power that Broadsword brings is not just the capability of accessing multiple local sources simultaneously, but the ability to also access other sources that are geographically separated. In order to provide this access, Gatekeepers have the ability to communicate with each other. In order for this to happen each Gatekeeper must register themselves with a Keymaster.

Note: A Keymaster must be installed and configured before a Gatekeeper can register to it. Refer to the Keymaster Installation and Maintenance Guide.

To begin this process, the administrator must contact the appropriate Keymaster administrator for a one-time registration identifier. After receiving this information, the Gatekeeper administrator will select the Register Gatekeeper item and will be presented with the screen shown in Figure 4.9.

Register Gatekeeper	
Keymaster IP Address	<input type="text"/>
Keymaster Port	<input type="text"/>
Registration ID	<input type="text"/>
Allow Remote User Administration	<input type="radio"/> Yes <input type="radio"/> No

Figure 4.9 Sample “Register Gatekeeper” Screen

After entering the information requested and clicking on the “Register Gatekeeper” button, all the necessary information is passed up to the Keymaster. Upon successful registration, the Keymaster will in turn pass back a Global Map (identifying other participating Gatekeepers and their sources) and a certificate used to authenticate itself with the other participating Gatekeepers.

Successful registration is indicated with a response back from the Keymaster that the registration process was successful.

The “Allow Remote User Administration” will only be displayed if the Gatekeeper is configured to use AAM for user administration. If the “Yes” radio button is selected, then the keymaster, which this Gatekeeper is registering to, will be granted admin permissions to administer the AAM entries for the local users to the Gatekeeper. If the “No” radio button is selected, then only local administration of users will be allowed. The response is shown in Figure 4.10.

Note: Once a Gatekeeper has selected to “Allow Remote User Administration”, the only way to change this setting is to unregister and then re-register this Gatekeeper with the Keymaster.



Figure 4.10 Registration Result

The local map, sent by the local Gatekeeper to the Keymaster, is automatically generated by the local Gatekeeper. As part of configuring each source, there is a configuration item entitled “Access Control” which is used to determine whether the source is to be made available to outside users. If it has a value of “Local and Remote”, the source will be included onto the local map.

Denying “Local & Remote Access” source access by outside users can be accomplished by bringing up that source’s configuration page through “Backside Sources” and setting the “Access Permission Override” value to “Deny Access To All Remote Users”. Changes will then be posted, sent to the Keymaster and automatically propagated to all other Gatekeepers.

4.5 Connected Sites

After registering your Gatekeeper with a Keymaster (See Register Gatekeeper Section), remote sources may be available as remote sources. The Connected Sites page allows the local Gatekeeper administrator to view these remote sources.

The screenshot shows a web interface titled "Connected Sites". It features a table with two columns: "GATEKEEPER" and "SOURCE". The table lists several gatekeepers and their associated sources, including "saturn Gatekeeper" and "saturn bswd3.0.Idap Gatekeeper".

KEYMASTER	
Registered to 'Saturn Keymaster' on (Zulu) Fri May 26 15:27:15 2000	
GATEKEEPER	SOURCE
saturn Gatekeeper	...
...	IPL 1.0 at Sun via Saturn
...	IESS at IESS0 via Saturn
...	5D at Saturn via Saturn
...	Elint Stream Via Saturn Baseline
saturn bswd3.0.Idap Gatekeeper	...
...	Roger All IPL Test

Figure 4.11 Sample “Connected Sites” Screen

4.6 Data Elements

The “Data Elements” screen provides the administrator the ability to tailor the information provided for each of the attributes described in the Information Navigational Keys (INK) document. Figure 4.12 provides a sample of the “Data Element Configuration” screen.

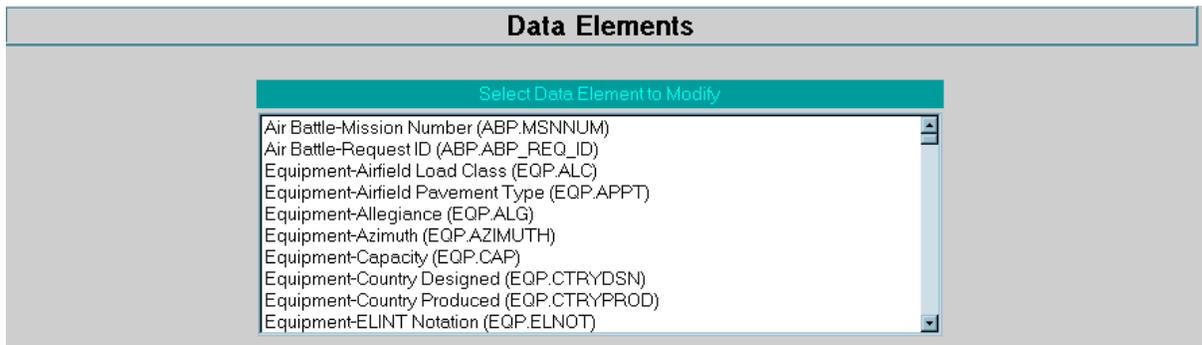


Figure 4.12 Sample “Data Element Configuration” Screen

Initially, the page presents the administrator with a scrolled list of all available Data Elements. To edit a particular element, select its name from the list and click the **‘Edit’** button. The **‘Reset Form’** button deselects your choice from the list. Figure 4.13 again displays the Data Element Page, with the Equipment Country Designed (EQP.CTRYDSN) element highlighted (selected).

IMPORTANT NOTE: The list of data elements available is a union of the elements for each source that the administrator has access to, NOT a union of the elements for all sources that the site has access to. To ensure that this list is complete make sure that the administrator account has access to all available local sources. To add sources to a specific user refer to Chapter 6 – User and Group Maintenance.

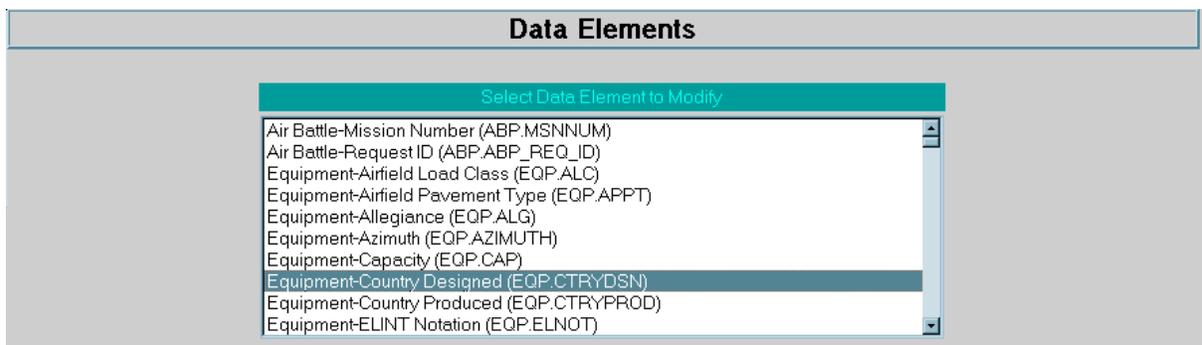


Figure 4.13 Data Element Page Example

Clicking on the Edit button, the administrator will be taken to the edit page for the Equipment Country Designed (EQP.CTRYDSN) element page (as shown in Figure 4.14).

Edit 'EQP.CTRYDSN' Element

Constant Element Attribute Values

Data List Constraints (If Any)	
Data Type	Character
Minimum Length	
Maximum Length	3

Step 1: Edit Data Element Attributes

Element Attribute	Value
Display Name	<input type="text" value="Country Designed"/>
Help Text	<input style="width: 95%;" type="text" value="Country Code of country designing the object."/>
Cataloging Mandatory Value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Step 2: Configure Data Element Groups

Select Global Default Group		Select Local Default Group
<p><i>No Global Default Groups Exist</i></p> <p>No Global Default Groups Exist for Data Element eqp.ctrydsn.</p>	<input type="button" value=">>>>"/> <input type="button" value="<<<<<"/> <input type="button" value="Reset"/>	<input type="checkbox"/> <input type="text" value="General"/>

Step 3: Edit Data Element Values

	EQP.CTRYDSN Data List Items
<p><i>Delete</i> Data List Items</p> <p><i>Add</i> Data List Item <input style="width: 30px;" type="text"/></p> <p>Help Text for New Item: <input style="width: 250px;" type="text"/></p>	<div style="border: 1px solid black; padding: 5px; min-height: 150px;"> AF (Afghanistan) AL (Albania) AG (Algeria) AQ (American Samoa) AN (Andorra) AO (Angola) AV (Anguilla) AY (Antarctica) AC (Antigua and Barbuda) AR (Argentina) </div>

Figure 4.14 Sample “Data Element Configuration” Screen

From this page, the administrator can modify the existing default values and descriptors for the element. Not all data elements have a predefined value list. An element may have none, one, or many predefined value list(s). When one (or many) exist, it/they are managed in Step 2 as shown in Figure 4.14. In this illustration there is one list available for EQP. CTRYDSN named general.

When a predefined value list is the select local Default group then its values populate the pop-down menu. As shown, general is selected as the local default group and therefore all the items in this list appear as Data Element Values in Step 3. To remove an entire list, click the check box next to the list name and select the left arrows button. General will then appear as a Select Global Default Group and the list in Step 3 will be empty. A table in the top and center of the edit element page provides the attribute definitions for the given data element. These attributes include:

The Type of Element Values (Character, Numeric, etc.)

The Minimum Length (in characters) the Value Can Be, if any defined

The Maximum Length (in characters) the Value Can Be

The Display Name allows for a translation to be made based on the actual element name to a user-friendly name. The help text provides for a description of the meaning or use of the element. There is no limit to the length of this description. The last item in this section is used for the site to determine whether the element is a mandatory field that must be entered when a new product is to be cataloged into an IPL. This option will only be shown if the element is available in an IPL.

Each data element may have a list of pre-defined values associated with it. These are the values the user sees in various pop-down menus on the short form.

If an element has a data list defined, the data list items are the only values it can take on. Therefore, when creating a list for an element that does not have one, the administrator should be sure to define all possible values the element can take on. The administrator can create new values or modify the acceptable values for a given data element list by using the add/delete functions provided in the lower half of the page.

To ADD a data item, enter the value of the new data item into the text input box labeled "Add Data List Item". If there was no previous value, i.e., then the data element value box (on the short form) will automatically be converted to a pop-down. If it was already a pop-down, the new value will be added to the existing list. There is also a Help Text field in which a user-friendly descriptor can be entered. To have this new value entered the "Save" button must be clicked. In this example we wish to add the country code "US" to the list. We also provide a user-friendly descriptor of "United States". After entering these values we click on the Save button for the changes to take effect (see Figure 4.15).

The screenshot shows a web interface titled "Step 3: Edit Data Element Values". At the top, there is a teal header bar with the text "EQP.CTRYDSN Data List Items". Below this, on the left, are three labels: "Delete Data List Items", "Add Data List Item", and "Help Text for New Item:". To the right of "Delete Data List Items" is a scrollable list box containing the following items: AF (Afghanistan), AL (Albania), AG (Algeria), AQ (American Samoa), AN (Andorra), AO (Angola), AV (Anguilla), AY (Antarctica), AC (Antigua and Barbuda), and AR (Argentina). To the right of "Add Data List Item" is a text input field containing "US". To the right of "Help Text for New Item:" is a text input field containing "United States".

Figure 4.15 Example of Adding a Data Item

To DELETE a data item, select the item to be deleted from the menu of current data list items titled “Delete Data List Items” and click the “Save” button. Figure 4.16 shows the removal of the data item “US” from the list.

The screenshot shows the same web interface as Figure 4.15. The teal header bar still says "EQP.CTRYDSN Data List Items". The scrollable list box now contains: TX (Turkmenistan), TK (Turks and Caicos Islands), TV (Tuvalu), UG (Uganda), UP (Ukraine), TC (United Arab Emirates), UK (United Kingdom), US (United States), UY (Uruguay), and UZ (Uzbekistan). The "US (United States)" item is highlighted with a blue background. The "Add Data List Item" and "Help Text for New Item:" input fields are now empty.

Figure 4.16 Example of Deleting a Data Item

In both cases, to cancel the process click on the “Cancel” button. This will cancel the current change and return to the Data Elements page. Clicking “Apply” has the same effect as clicking “Save”, although “Apply” does not return to the Data Elements page.

Note: The changes made to Data Elements will not be seen immediately. The modifications will only be seen on logins after the change has been made. The administrator who changes the element(s) should logout, and back in again to confirm the modifications have taken place correctly.

4.7 Add Map Data

The purpose of this section is to allow the administrator to add additional Map Data to the default set of map data which is included as part of the Broadsword installation CD-ROM. Currently, the following map data levels are supported: CADRG, CIB, WDBII, DBDB5, and DTED.

To add new maps you must have either a CD-ROM containing map data or an accessible file system containing the map data that you want copied for use by Broadsword.

The initial Add Map Data page consists of four text entry boxes and a drop down menu. The values entered into these fields define the location and the type of map data. The name and an explanation of each field is outlined in the following table:

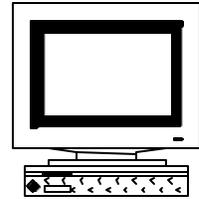
Field Name	Explanation	Example
Location of Map Data	Directory path to the map data.	/cdrom/vmap
Destination Directory	Directory path to where the data will be stored.	/opt/bswd3.0/client/mapdata
Map Data Type	Type of map data that will be copied	CADRG
Map Data Item	Unique name that helps to develop the directory structure.	5NINM0914
Map Data Base Name	Names the continent that contains the map data	Noamer

Table 4.3 Summary of Values

The administrator should note that Map Data Base Name corresponds to directory names and can be found by examining the CD-ROM or file system directory containing the map data.

After you have entered values for all of the fields on the initial Add Map Data page and are satisfied that the entries are correct, click on the apply button. Based on the information you have entered, the AddMap binary will confirm that the directory path and names are valid and that the data is accessible. The AddMap binary will also determine if there is enough disk space available for the new map data. If there is a problem with accessing the map data or if there is not enough disk space available, an error message will be displayed along with the initial page containing the values that you entered. This will give you an opportunity to correct any problems before again attempting to add new map data. If AddMap does not detect any problems, the Confirm Map Data Add page will be displayed. This page summarizes the data that you entered on the initial page. It also contains a summary of the current disk usage for the file system that the map data will be copied to and the amount of disk space required for the new map data.

After determining that the information is correct and that the map data will not consume a disproportionate amount of available disk space, click the Add Map Data button. This will initiate the copying of the map data.



Chapter 5

Client Requirements

The purpose of this chapter is to identify what software or application(s) that will be required to access the system. As a minimum, an HTML browser will be necessary. To view the narrated video clips provided within the interface, a Shockwave-Flash Plug-in or external viewer will also be required. Otherwise, any additional external application, plug-ins or viewers may be required depending on the sources and products that will be accessed. There is NO specific client software required to be loaded. Specific topics to be covered include:

- HTML Browsers
- Image Viewers
- MPEG Viewers
- Quicktime Viewer
- Shockwave-Flash Viewer
- Audio Players
- Document Viewers
- FTP Servers

Note: The applications listed here are only examples. Only approved software may be installed on the client workstations, as defined by site policy. For those sites with access to Intelink or Intelink-S, many of these applications are made available on the ISMC web pages.

5.1 HTML Browsers

Broadsword requires a web browser that supports the HTML 4.0 standard. The system uses Javascript and hence the Javascript and cascading style-sheet options need to be on. The interface is best viewed using Netscape 4.7x or Internet Explorer 4.0x.

If caching is enabled on either Internet Explorer or Netscape, it is possible to visit previously loaded pages without reloading them from the server on which they reside. If there are any form elements on these pages, all data previously entered will still be present. Thus it would be possible to complete a Broadsword session, and then return to the login page and connect without retyping one's password. This problem may be circumvented by making sure to exit the browser after logging out, or by clearing the cache after a session. Another option is disabling the cache (see Note below).

When using Netscape, resizing the browser window may cause the current page's data to be lost. The server will respond with a missing form data error. Reloading the form data will not return you to the expected page, since all of Broadsword's pages are created dynamically. In order to solve this problem, the user must enable the memory or disk cache under advanced preferences. This value should be suitably large (1000 K should work). For Netscape, user should, under **Edit-> Preferences-> Advanced -> Cache** select the **Every Time** radio button under the

Document is Compared to Document on Network heading. When using Internet Explorer, be sure to **View-> Internet Options** ->click on the **Settings** button under the **Temporary Internet files** heading and ensure that the **Every visit to the page** radio button is selected under the **Check for newer versions of stored pages**.

Operating System	Browser
Solaris 2.5.1	Netscape v4.7x
Windows 95/98/NT v4.0	Netscape v4.7x, Internet Explorer 4.01 SP2

Table 5.1 - Summary of Supported HTML Browsers

Project Broadsword has the ability to access virtually any type of product. Some product formats included are TIFF, NITF 1.1, NITF 2.0, MPEG, and Quicktime, to name a few. However, none of these formats are inherently supported by a Browser. Helper applications, also called external viewers, are software programs external to the Web browser that are used to open files of data types that the browser doesn't natively recognize.

The majority of these helper applications have setup utilities that automatically make the browser aware of their existence on PC and Macintosh platforms. However in some cases the user can configure the browser manually to make them aware of helper applications. Some examples of valid configurations are available on the Helper Configuration page.

IMPORTANT NOTE: Because of how fast Browsers are being released today, it's extremely difficult to keep up configuration issues. Please refer to the applicable browser documentation for configuration information.

5.2 Image Viewers

To view NITF 1.1, NITF 2.0, TIFF 6.0 and Sun Raster image files an external viewer will be necessary. Listed below are some Image Applications or viewers that can be launched from a browser, their platform and what formats they handle.

Platform	Application	Supported Formats
UNIX	5D Client	TIFF 6.0, Sun Raster, NITF 1.1, NITF 2.0
	EZView 1.0a	NITF 1.1, NITF 2.0 Level 6, PCX, PICT, TIFF, SunRaster, BMP, GIF, and JPEG
	MATRIX v4.0.2	NITFS (v1.1 & v2.0), TIFF, SunRaster
	Paragon ELT/7000	NITF 2.0
	xv v3.00,3.10	GIF, TIFF, JFIF (JPEG), SunRaster, PBM family, Multiple Formats
Windows 95 / 98 / NT 4.0	ACDSee 32 v2.21	BMP, GIF, JPEG, PCX, PNG, TGA, TIFF, and WMF
	Corel Photo-Paint 7.0	BMP, EPS, GIF, JPEG, PCX, PNG, TGA, WMF, Multiple formats
	LView v3.1, Lview Pro	BMP, GIF, JPEG, PCX, TGA, TIFF
	Northrop View,v3.1, Release 4	NITFS (v1.1 & v2.0), Multiple Formats
	Paint Shop Pro v4.0	BMP, EPS, GIF, JPEG, PCX, PNG, TGA, TIFF, WPG
	SENDS NDS, Image Manager, v2.02	NITFS (v1.1 & v2.0), Multiple Formats

Table 5.2 - Summary of Supported Imagery Viewers

5.3 Shockwave-Flash Players

The Video Clips provided as part of the On-Line Demonstrations are in Shockwave-Flash format and have both video and audio (with Closed Captioning). To play these video clips you must have a Shockwave-Flash plugin configured with any web browsers on the client machine.

Platform	Application	Notes
UNIX	Shockwave-Flash plugin	Packaged with Netscape Communicator 4.7x and Internet Explorer 4.0 SP2 or can be downloaded from www.macromedia.com
Windows	Shockwave-Flash plugin	Packaged with Netscape Communicator 4.7x and Internet Explorer 4.0 SP2 or can be downloaded from www.macromedia.com

Table 5.3 - Summary of Supported Shockwave-Flash Players

5.4 FTP Servers

A number of the potential sources provide support for products to be delivered to a specified destination. For this to happen, an FTP Server must exist on the Client Workstation and there must be a valid user name and password for the FTP Server. For a UNIX Based machine an FTP Server is included. For Windows Based machines there are many commercial packages that perform well. Some FTP Daemons available are Exceed Hummingbird and Vermillion FTP.

Note: In order for an FTP server to be compatible with IPL's product pull protocols, the server must support standard response messages, and must allow a user to execute an FTP 'bin' command before a user logs in.

Chapter 6

User and Group Maintenance

6.1 User Maintenance in a Non-Access & Authentication Module environment

The following section pertains to User Maintenance in a Non-AAM environment. If the administrator logs into a Broadsword server which has been configured with Non-AAM support, the user will be unable to create user accounts through the Broadsword interface. However, the Broadsword interface will allow the administrator to grant roles and sources. Rather, the process of creating an account will have to be done with the environment's appropriate software, i.e. CSE-SS, Sun Tools, or AFDI. The User Maintenance page is accessible by means of the top most menu bar. The user is able to navigate to the page by clicking on Administration → Users and Groups → User Maintenance. The following image (Figure 6.1) shows the initial page the administrator will see when they click on the User Maintenance sub menu.

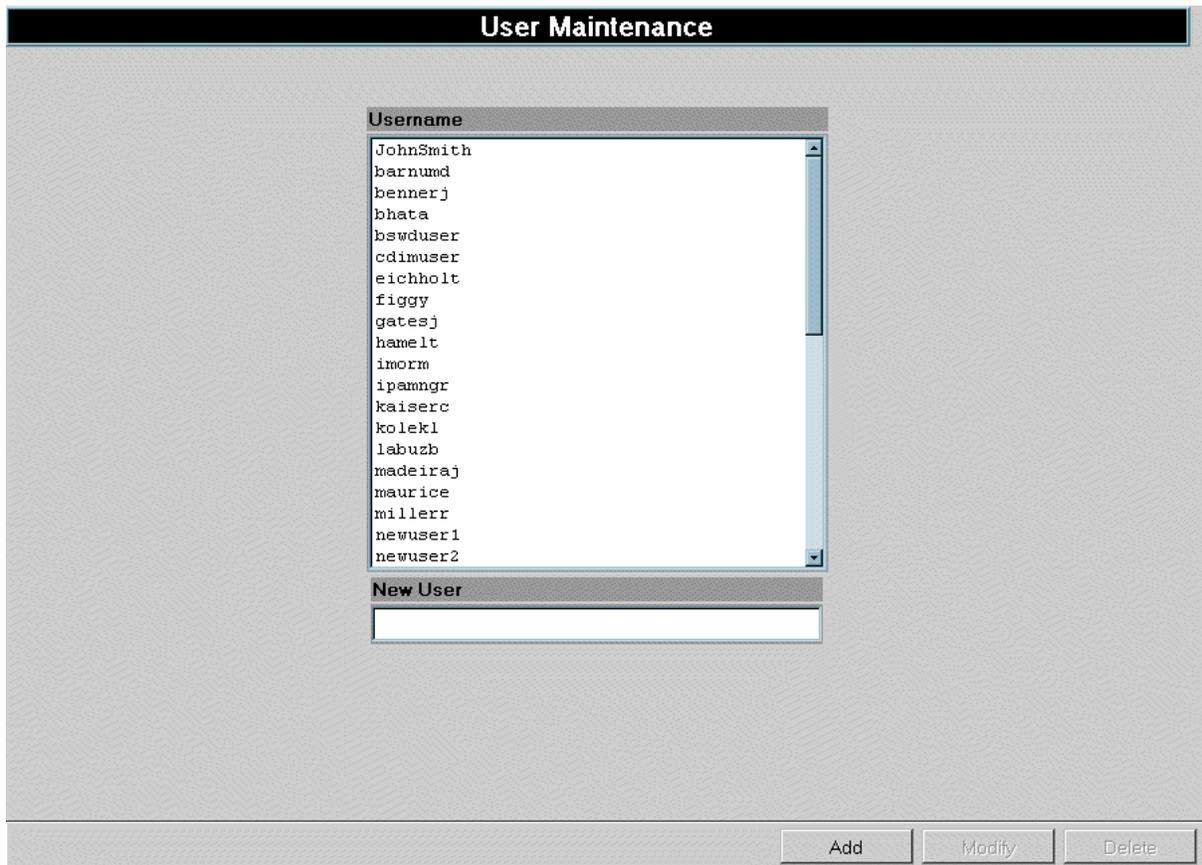


Figure 6.1 - User Maintenance

This page contains a list of users who are able to access log into Broadsword.

Note: The username list is created by reading a directory in which Broadsword profiles are kept. Thus, if a user has *not* logged into Broadsword in the past, their username will not appear in the username list.

If the administrator would like to add a user to the Username List, the administrator should type the username into the text box located below the Username List. After entering the username into the text box, the administrator should then click on the Add button. Once the Add button has been activated, the new username will appear in the Username List. Initially, when the administrator accesses the above page, the Modify/Delete buttons are not accessible. In order to activate the buttons, one must select a username from the Username list. Once they have selected a Username, the administrator is able to do one of two things, Modify the selected account or Delete it. Figure 6.2 shows a Username selected with the buttons activated.

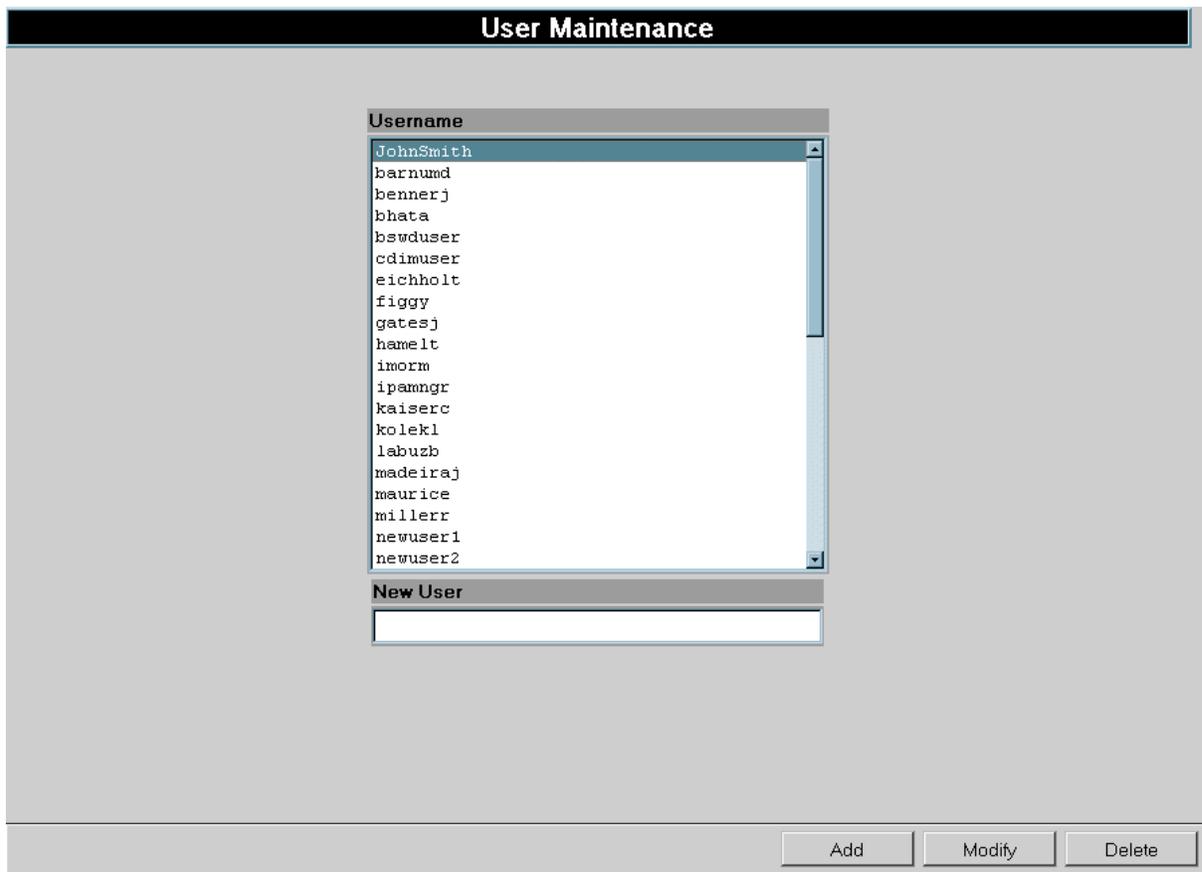


Figure 6.2 - User Maintenance (username selected)

For example, if the administrator chooses the Delete button, the administrator will be able to delete the selected Username.

Note: With a Non-AAM environment, deleting a user does *not* actually delete the user from the entire system. Rather, it deletes the user's relevant Broadsword files.

If the administrator clicks on the delete button, a dialog box will appear that will allow the user to choose whether or not they actually want to go through with the process.

The administrator may like to modify an existing account. Like the Delete button, the Modify button will only become "active" when a user has been selected from the Username list (Figure 6.2). If a user selects a Username and clicks on the Modify button, the following page will appear (Figure 6.3):

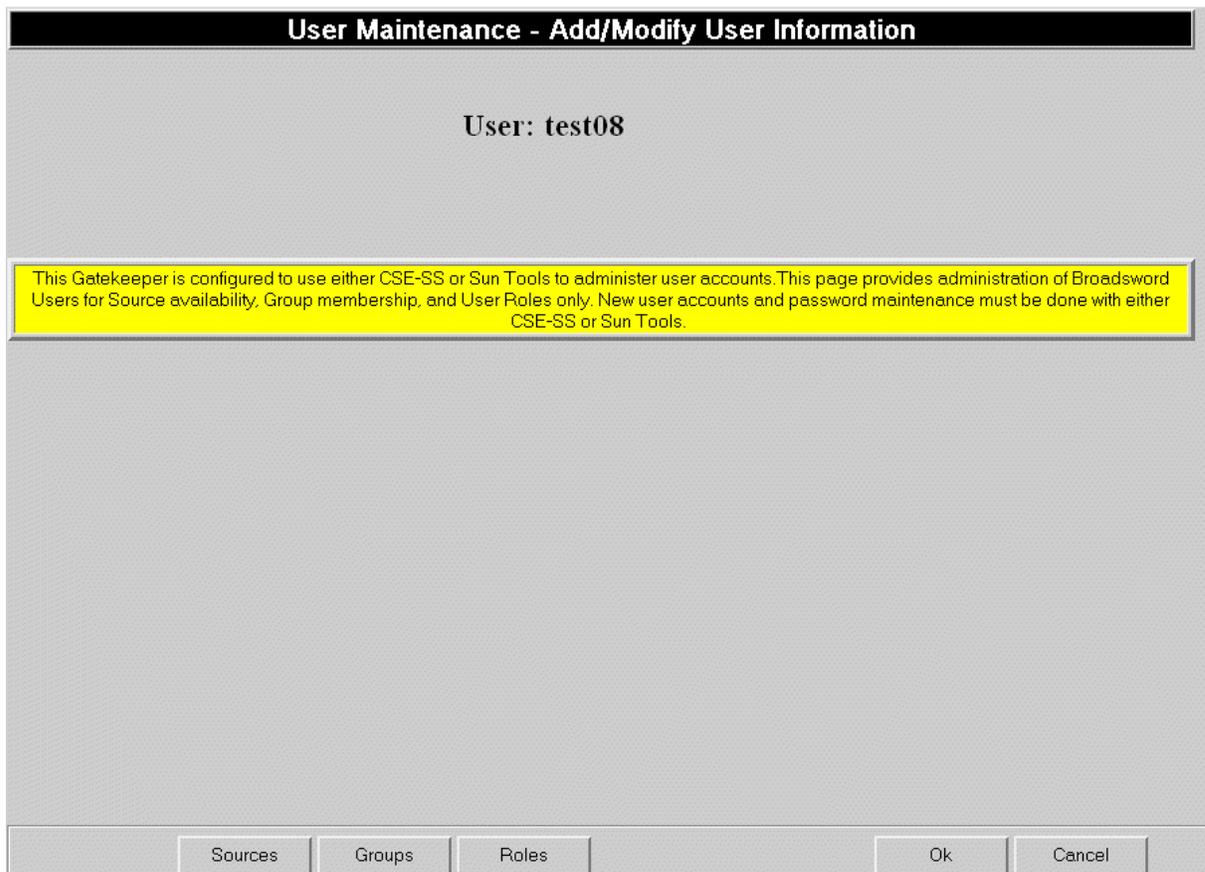


Figure 6.3 - User Maintenance (Modifying a user)

The Modify user page (Figure 6.3) contains a yellow banner in the middle of the page. Similar to adding a user, Broadsword is unable to modify user information in a Non-AAM environment. In order to modify the selected user, the environment's appropriate software must be used. If the user chooses either the Ok or Cancel Button, the user will be brought back to the main User Maintenance page (Figure 6.2). If the administrator selects the Sources, Groups or Roles button, the user will be brought to the button's relevant page. For information pertaining to these buttons (Sources, Groups, or Roles) reference section 6.3 of this manual.

6.2 User Maintenance in an AAM environment

The following section deals with User Maintenance in an AAM environment. If the administrator logs into Broadsword with AAM support, the administrator will be able to create user accounts using the Broadsword interface. The User Maintenance page is accessible by means of the top most menu bar. The user is able to navigate to the page by selecting on Administration → Users and Groups → User Maintenance. The following image (Figure 6.4) shows the initial page the user will see when they click on the User Maintenance sub menu:

Note: If the administrator is unable to login to the system as an administrator, it is possible that an account has been locked in the AAM. In order to unlock this account, the user must login to the Broadsword server as **root** and execute the following to unlock the account in the AAM:

```
% /opt/bswd3.0/bin/account_unlock <username>
```

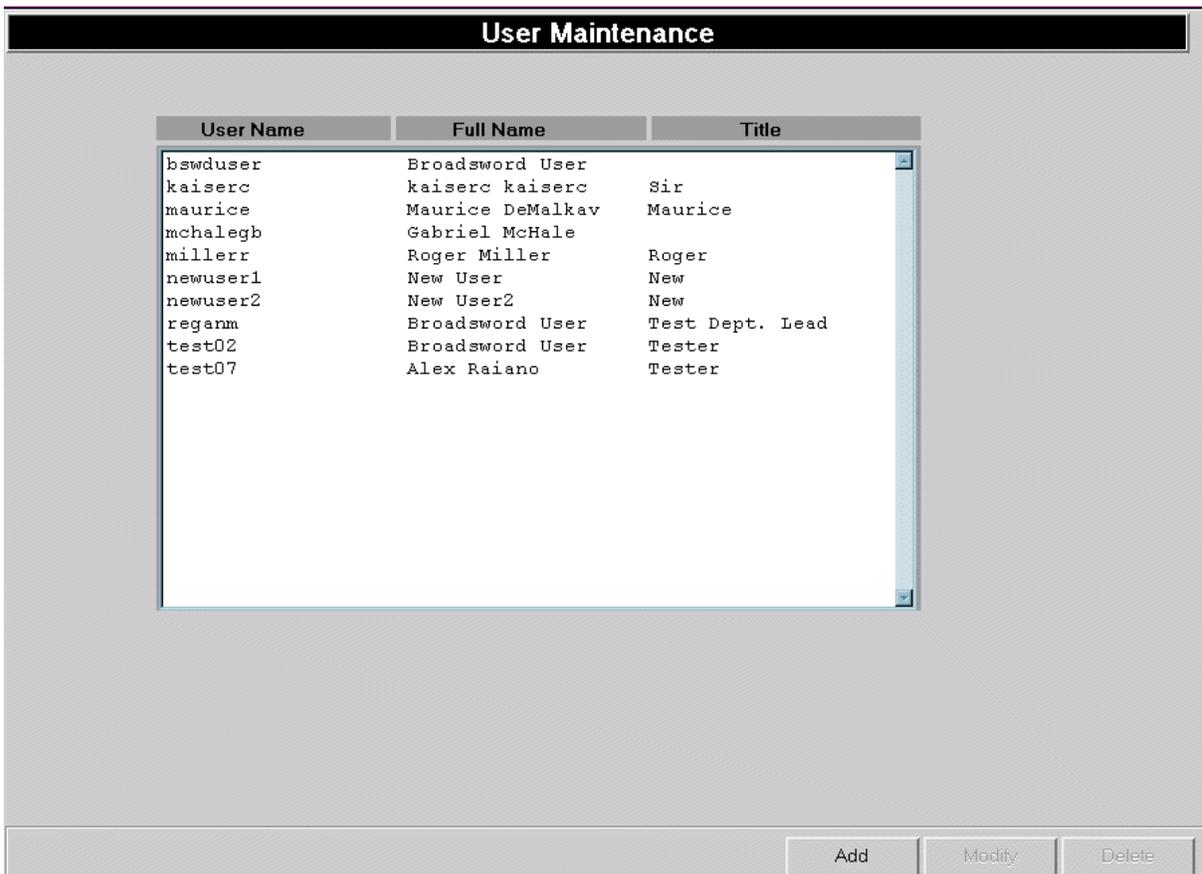


Figure 6.4 - User Maintenance

From this screen (Figure 6.4) the administrator is able to see all existing accounts. For each username, a full name and title is given. Along with the information about the users, this page also contains three buttons (Add, Modify, or Delete). The Add button allows you to create a new user. The Modify button provides the ability to change an already existing user. The Delete

button offers the ability to remove a user from the system. Upon initial entry into this page, note that the Modify and Delete buttons are disabled. In order to enable these buttons, the administrator must select an existing username from the list. Once the username has been selected, the Modify and Delete buttons will become active (Figure 6.5).

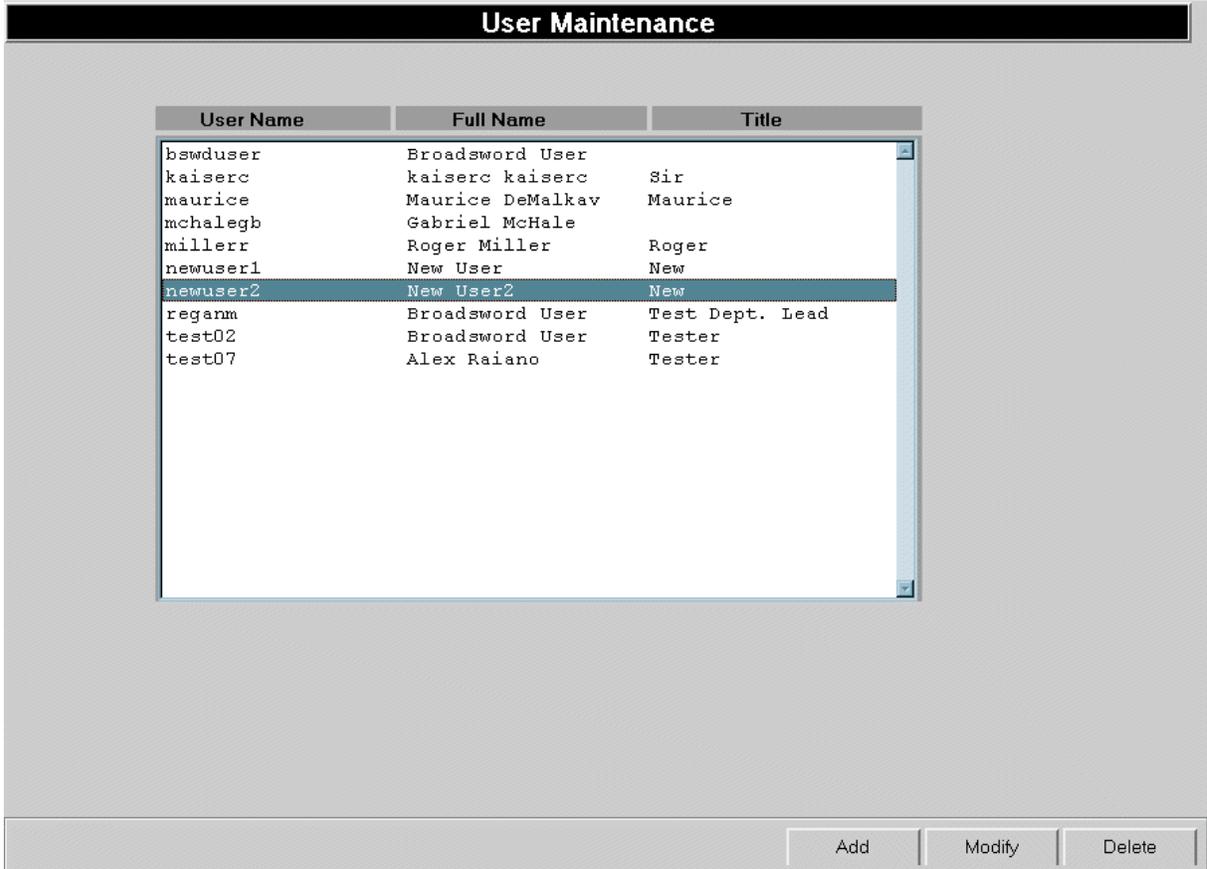


Figure 6.5 - User Maintenance (username selected)

If the administrator desires to add a new user to the system, all the administrator has to do is click on the Add button. The Add button brings up a page where the administrator is able to enter information about the new account that is going to be created (Figure 6.6).

Configuration Item	Value	Item Description
User ID	<input type="text"/>	This mandatory field is the user's ID.
Given Name	<input type="text"/>	This mandatory field contains the user's first name.
Middle Initial	<input type="text"/>	This mandatory field contains the user's middle initial.
Surname	<input type="text"/>	This mandatory field contains the user's last name.
Language Proficiency	RCL0, LCL0	Individual's evaluated ability to read, write, and speak a second language, other than english. Based on Defense Language Proficiency Test.
Citizenship	UNITED STATES (USA)	This mandatory field represents the countries that this user is a citizen of.
Home Organization	ACOM	This mandatory field contains the user's owning agency.
Account Locked?	N	This field indicates whether or not a user's account is locked.
Employee Type	USAF	Service Branch, Contractor, Civilian, FFRDC
Intelligence Community Email	<input type="text"/>	IC Email that operates across JWICS.
Telephone: Unclassified Voice Phone Number	<input type="text"/>	User's unclassified telephone number.
Company Name	<input type="text"/>	Company Name of the contractor.
Email: Internet Address	<input type="text"/>	Unclassified Internet Email

Sources Groups Roles Ok Apply Cancel

Figure 6.6 - Adding a User

Notice that initially, the Sources, Groups, and Roles buttons are not accessible. In order for these buttons to become active, the user must first fill-out the form and Apply the changes. When the form has been completely filled out, the administrator can create the account by pressing either the Ok or Apply buttons. If the user selects the Ok button and there are no errors, a new account will be created and the user will be brought back to the initial User Maintenance page (Figure 6.4). If the administrator selects the Apply button and there are no errors, a new account will be setup and the administrator will stay at the current page. If there are errors in the creation of the new account, the administrator will be brought to a page that allows them to fix what is causing the problem. Missing data in one of the required fields will most likely cause the problem(s). At any time during the process, if the administrator decides not to create a new account, the administrator can click on the cancel button which will bring them back to the User Maintenance (Figure 6.4) page without a new account created. After submitting the account with the Apply button, the administrator has the option of adding/removing Sources, Roles and Groups. For information pertaining to these pages reference sections 6.3, 6.4, or 6.5 respectively. The new account is activated as soon as it is submitted. The new user is now able to login to the system using the default password. Upon entering the system for the first time, the new user will be required to change their default password.

To modify an existing user account, select the username that needs to be modified and click on the Modify button (Figure 6.4). Upon clicking on the Modify button, the administrator will be brought to the User Modification screen shown below:

Configuration Item	Value	Item Description
Name	User.Broadsword.bswduser	This field contains the user's full name including agency unique identifier.
User ID	bswduser	This mandatory field is the user's ID.
User Password	<input type="password"/>	This field contains the password for this Broadsword user.
Given Name	<input type="text" value="Broadsword"/>	This mandatory field contains the user's first name.
Surname	<input type="text" value="User"/>	This mandatory field contains the user's last name.
Citizenship	<input type="text" value="UNITED STATES (USA)"/>	This mandatory field represents the countries that this user is a citizen of.
Home Organization	<input type="text" value="USAF"/>	This mandatory field contains the user's owning agency.
Current Organization	AFRL/RRS	This field contains the agency to which the user is currently delegated.
Account Locked?	<input type="text" value="N"/>	This field indicates whether or not a user's account is locked.
Number of Bad Login Attempts	0	This is the current count of failed logins.
Date of Last Password Change	20000504133335	This is the date on which the user's password was last changed.
Employee Type	<input type="text" value="USAF"/>	Service Branch, Contractor, Civilian, FFRDC
Intelligence Community Email	<input type="text"/>	IC Email that operates across JWICS.
Telephone: Unclassified Voice	<input type="text"/>	User's unclassified telephone number

Sources Groups Roles Ok Apply Cancel

Figure 6.7 - Modifying a User

From this screen the administrator is able to change any data about a user. Along with the data about the account, the administrator is also able to change the selected account's Sources, Groups and Roles. If the administrator selects the Ok button and there are no errors, the account will be changed with the modification(s) provided and the administrator will be brought back to the initial User Maintenance page (Figure 6.4). If the administrator selects the Apply button and there are no errors in the form, the account will be modified and the user will stay at the current page. If there are errors in the modification of the account, the administrator will be brought to a page that allows them to fix what is causing the problem. Missing data in one of the required fields will most likely cause the problem(s). At any time during the process, if the user decides not to modify the chosen account, the user can click on the Cancel button, which will bring them back to the User Maintenance page (Figure 6.4) without any modifications made.

To delete an existing account, select a user from the list and click on the Delete button (Figure 6.4). Once the administrator clicks on the Delete button, the administrator will be shown a dialog box, which confirms the deletion.

Note: When the user deletes an account the deletion actually removes the user from the system. The removal does *not* simply eliminate the users relevant Broadsword files.

6.3 Adding/Removing Sources

This section contains information on how to assign/remove Sources for both AAM and CSE-SS environments. Both the AAM and Non-AAM environments are the same in terms of their functionality when it comes to assigning/removing Sources.

To modify the sources available for a particular user account, the administrator must click on the Sources button located on one of the previously mentioned pages (AAM: Add User (Figure 6.6) or Modify User (Figure 6.7) Non-AAM: Modify user (Figure 6.3). Once the button has been clicked, the administrator will see the following page:

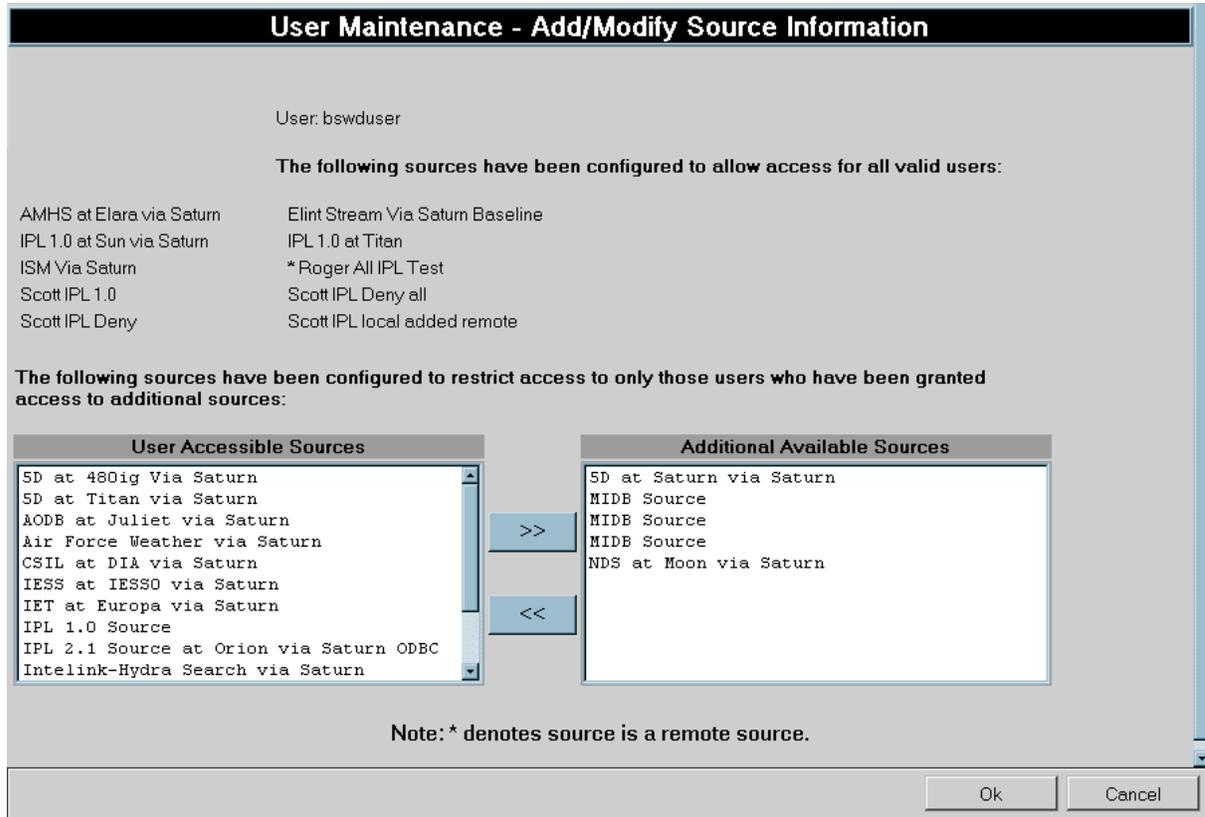


Figure 6.8 - Adding/Removing Sources

By using the list box and the appropriate arrows, the administrator is able to change which sources are available to the selected user. There are two types of sources, (1) sources which are given by default to all users whom have been granted access to the given Gatekeeper (2) sources which have been configured to restrict access and must be individually granted access to the user. To remove a source from a user, simply select it from the User Accessible Sources list and click on the right arrow. To add a source to a user, click on the source you want to add from the Additional Available Sources list and click on the left button.

Note: There can be source(s) that are available to all users. These “global” sources are located below the description that signifies them as such. Also note that remote sources are identified by an asterisk (*) before their name/description.

In order for the changes to take effect, the user must click on the Ok button, the user will then be brought back to the previous page. If the user clicks on the Cancel button, no changes will be made and the user will be brought back to the previous page.

6.4 Adding/Removing Roles

If the administrator would like to change a particular user’s Role(s), the administrator can click on the Roles button located on one of the relevant pages (AAM: Add User (Figure 6.6) or Modify User (Figure 6.7) Non-AAM: Modify user (Figure 6.3)). The Roles button brings up the following page:

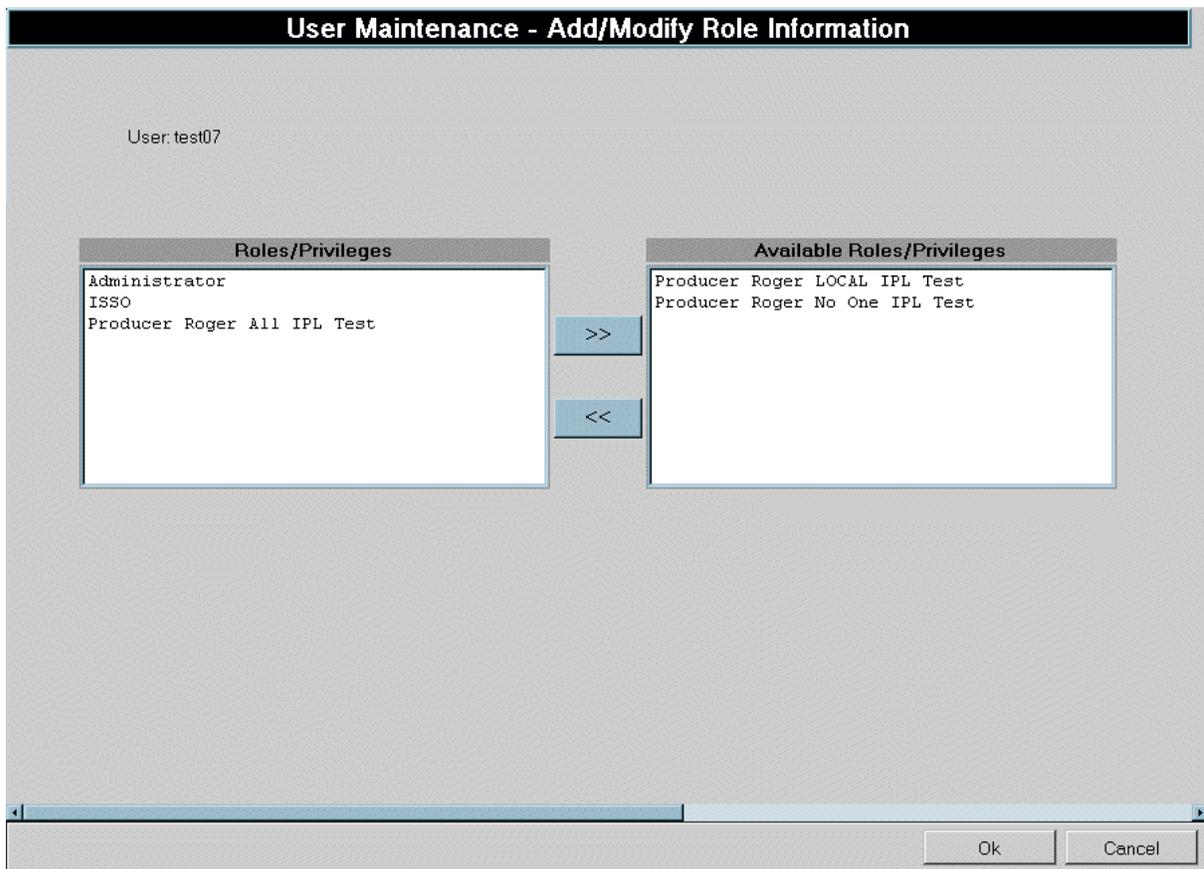


Figure 6.9 - Adding/Removing Roles

All of the user’s current Roles/Privileges appear in the leftmost list (Roles/Privileges). All other Available Roles/Privileges are located in the rightmost list. In order to remove/add a role(s) from

the selected user, simply select a list item and click on the relevant button. Once the Ok button has been clicked, all changes will take effect and the administrator will be placed back to the previous page. If at any time the administrator clicks the Cancel button, all changes will be discarded and the administrator will be brought to the previous page.

6.5 Adding/Removing Groups

This section contains information on how to assign/remove Groups from a particular user. If you are in an AAM setting, you can access the Groups buttons from either the Add User (Figure 6.6) or Modify User (Figure 6.7) pages. If you are in a Non-AAM environment, you will be able to get at the Groups button from the Modify user page (Figure 6.3). Both the AAM and Non-AAM environments are the same in terms of their functionality when it comes to assigning/removing Groups.

If the administrator would like to change the Groups, the administrator must click on the Groups button located on one of the following pages (AAM: Add User (Figure 6.6) or Modify User (Figure 6.7) Non-AAM: Modify user (Figure 6.3)).

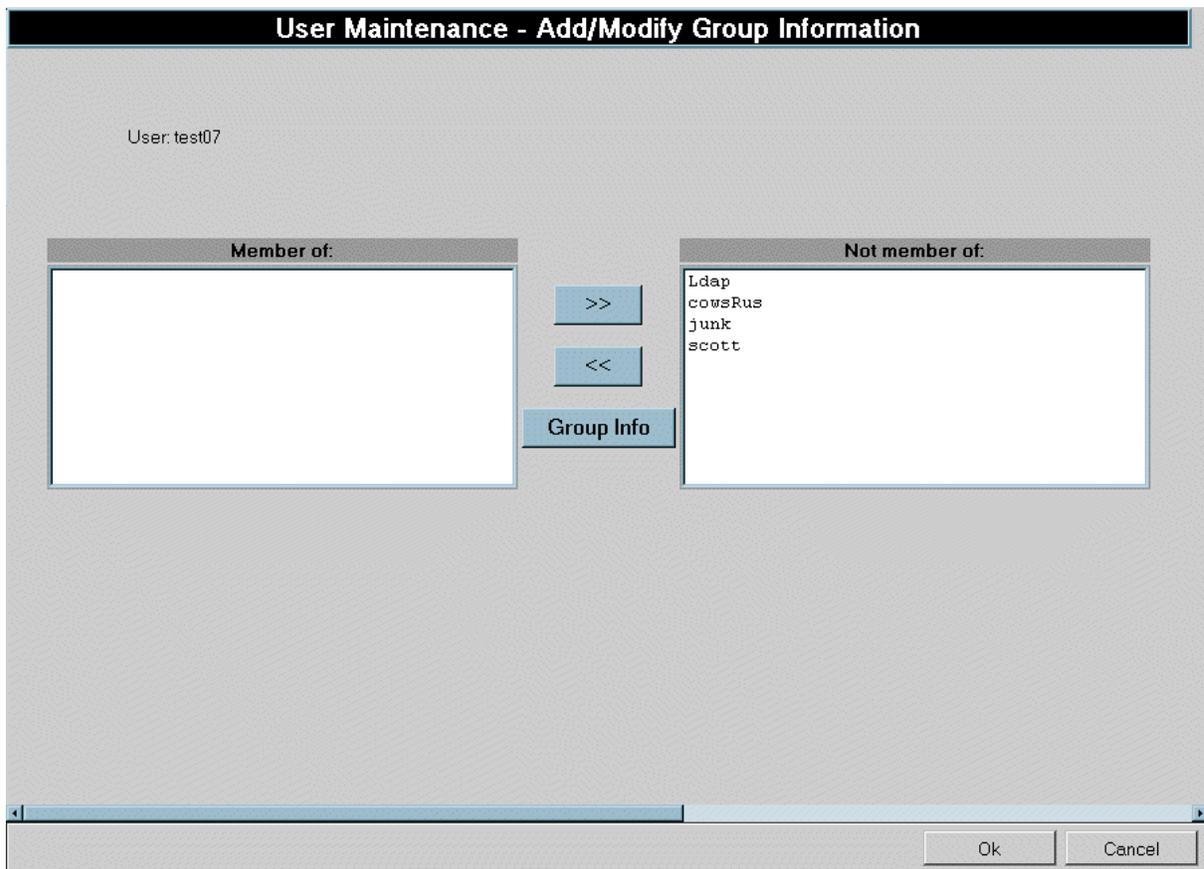


Figure 6.10 - Adding/Removing Groups

From this screen (Figure 6.9) the user can change a user's membership in a group(s). The left most box contains a list of group(s) that the user is currently a member of. The rightmost box

contains a list of groups that the user is not currently a member of. In order to remove/add a group(s) from the selected user, simply select a list item and click on the relevant button. Once the Ok button has been clicked, all changes will take effect and the user will be placed back to the previous page. If at any time the user clicks the Cancel button, all changes will be discarded and the administrator will be brought to the previous page. If the administrator would like to view a particular group's member(s), the administrator should select the group that he is interested and then click on the View Group Info button. The View Group Info button will popup a new window with what roles and source accesses have been assigned to the group and a list of users which have membership to the group.

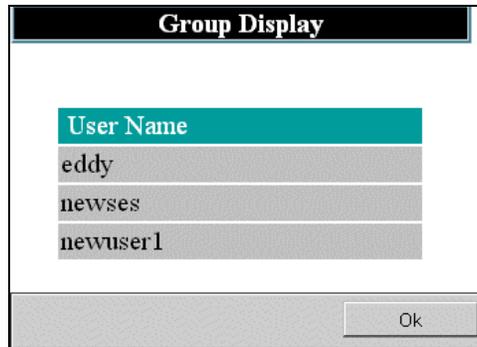


Figure 6.11 - Group Information

6.6 Adding, Modifying, and Deleting a Group

The following section pertains to Adding, Modifying and Deleting Groups. The Group Maintenance page is accessible by means of the top most menu bar. The user is able to navigate to the page by clicking on Administration → Users and Groups → Group Maintenance. The following image (Figure 6.12) shows the initial page the administrator will see when they click on the Group Maintenance sub menu.

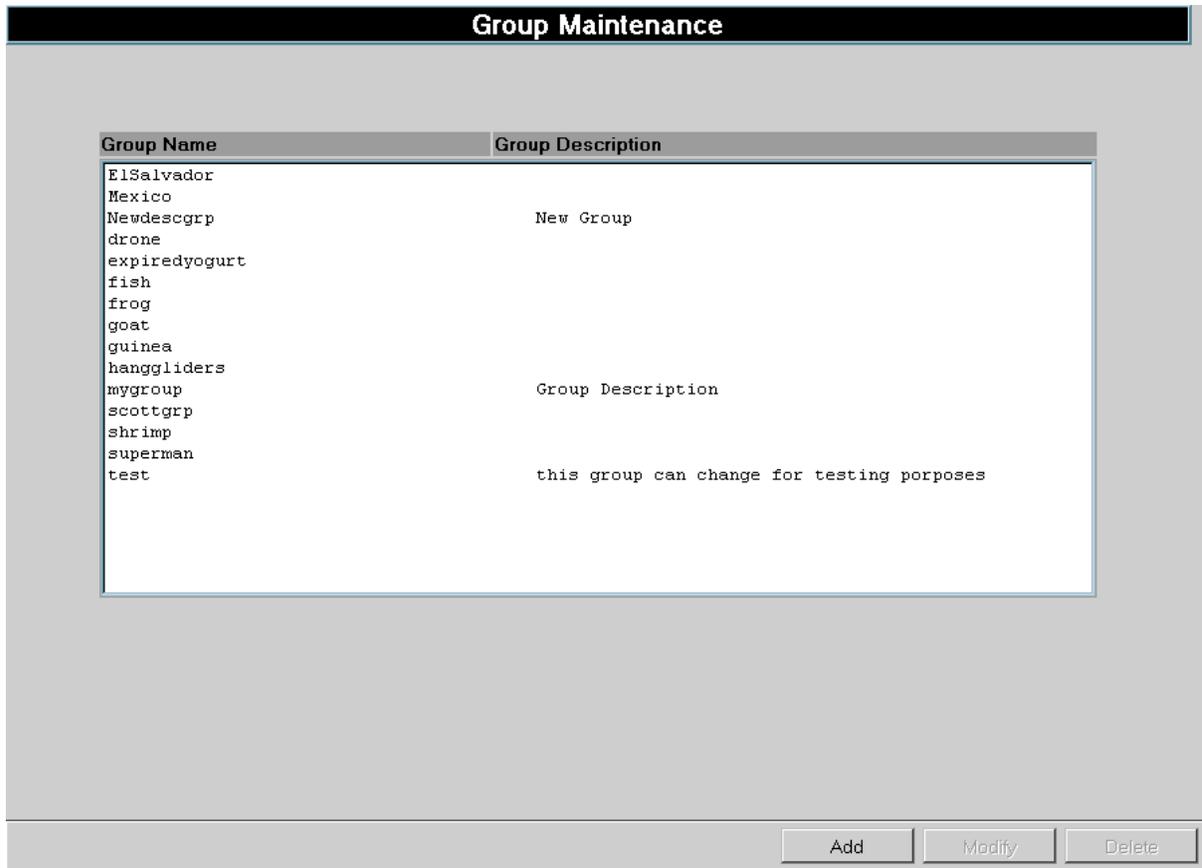


Figure 6.12 - Group Maintenance

From this screen (Figure 6.12) the administrator is able to see all existing Groups. For each Group Name, a Group Description can be given. Along with the information about the groups, this page also contains three buttons (Add, Modify, or Delete). The Add button allows you to create a new group. The Modify button provides the ability to change an already existing group. The Delete button offers the ability to remove a group from the system. Upon initial entry into this page, note that the Modify and Delete buttons are disabled. In order to enable these buttons, the administrator must select an existing group name from the list. Once the group name has been selected, the Modify and Delete buttons will become active (Figure 6.13).

Note: Groups are Broadword groups not UNIX groups

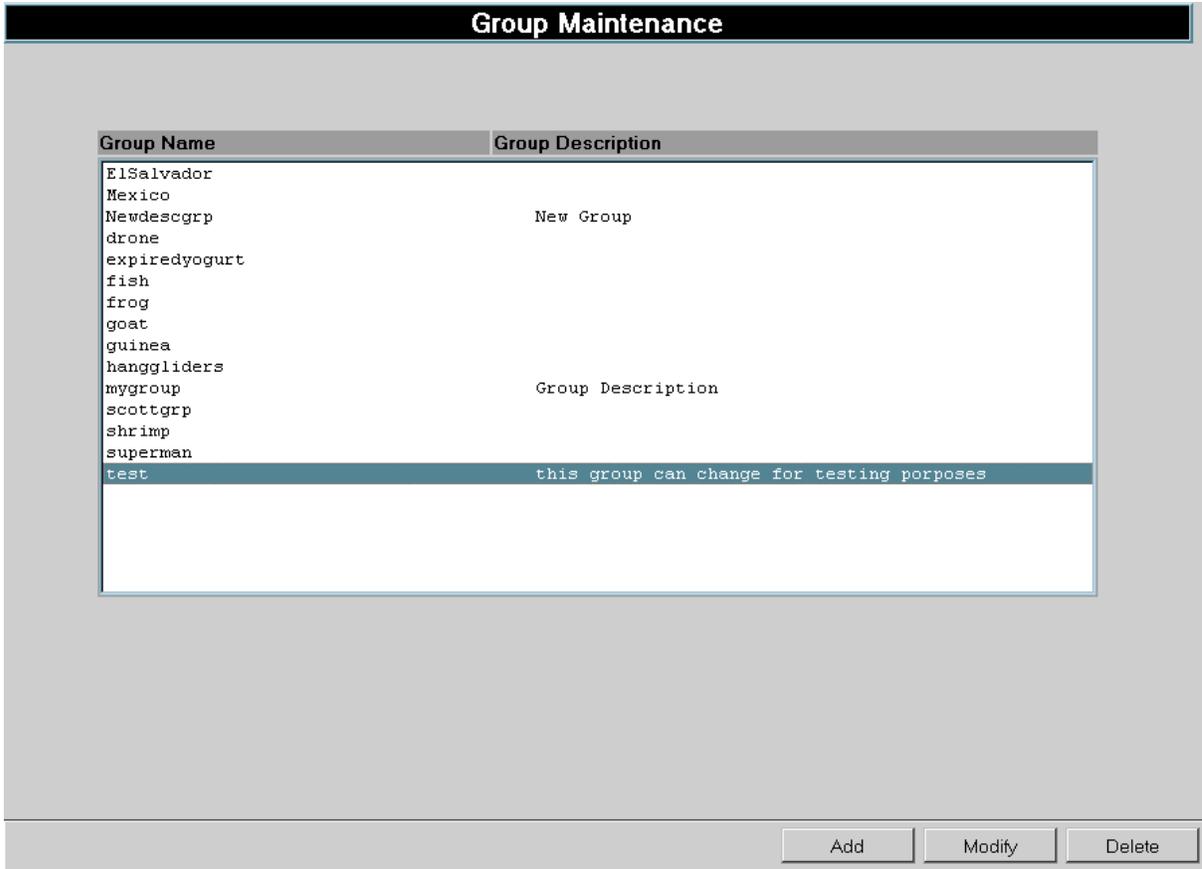


Figure 6.13 - Group Maintenance (group name selected)

If the administrator desires to add a new group to the system, all the administrator has to do is click on the Add button. The Add button brings up a page where the user is able to enter information about the new group that is going to be created (Figure 6.14).

The screenshot shows a web-based form titled "Group Maintenance - Add/Modify Group Information". The form contains two text input fields: "Group Name" and "Description". Below the form is a navigation bar with several buttons: "Sources", "Roles", "Users", "Ok", "Apply", and "Cancel". The "Sources", "Roles", and "Users" buttons are currently disabled (greyed out), while "Ok", "Apply", and "Cancel" are active.

Figure 6.14 - Adding a group

Notice that initially, the Sources, Groups, and Users buttons are not accessible. In order for the administrator to be able to access these buttons, the administrator must first fill out the form and then Apply the changes. When the form has been completely filled out, the administrator can create the group by pressing either the Ok or Apply buttons. If the administrator selects the Ok button and there are no errors, a new group will be created and the administrator will be brought back to the initial Group Maintenance page (Figure 6.12). If the admim selects the Apply button and there are no errors, a new group will be setup and the administrator will stay at the current page. If there are errors in the creation of the new group, the administrator will be brought to a page that allows them to fix what is causing the problem. Missing data in one of the required fields will most likely cause the problem(s). At any time during the process, if the administrator decides not to create a new group, the administrator can click on the cancel button which will bring them back to the Group Maintenance (Figure 6.12) page without a new group created. The new group is activated as soon as it is submitted. After submitting the Group with the Apply button, the administrator has the option of adding/removing Sources, Roles and Users.

To modify an existing group, select the Group Name that needs to be modified and click on the Modify button (Figure 6.12). Upon clicking on the Modify button, the administrator will be brought to the Group Modification screen shown below:

Group Maintenance - Add/Modify Group Information

Group Name test

Description this group can change for testing purposes

Sources Roles Users Ok Apply Cancel

Figure 6.15 - Modifying a Group

From this screen the administrator is able to change any data about a group. Along with the data about the group, the administrator is also able to change the selected group's Sources, Roles and Users. Reference section 6.3, 6.4 or 6.5 for information pertaining to these pages. If the administrator selects the Ok button and there are no errors, the group will be changed with the modification(s) provided and the administrator will be brought back to the initial Group Maintenance page (Figure 6.12). If the administrator selects the Apply button and there are no errors in the form, the account will be modified and the administrator will stay at the current page. If there are errors in the modification of the group, the administrator will be brought to a page that allows them to fix what is causing the problem. Missing data in one of the required fields will most likely cause the problem(s). At any time during the process, if the administrator decides not to modify the chosen group, the administrator can click on the Cancel button, which will bring them back to the Group Maintenance page (Figure 6.12) without any modifications made.

To delete an existing group, select a group name from the list and click on the Delete button (Figure 6.12). Once the administrator clicks on the Delete button, the administrator will be shown a dialog box, which confirms the deletion.

6.7 Adding/Removing Sources

Note: Reference section 6.3.

6.8 Adding/Removing Roles

Note: Reference section 6.4.

6.9 Adding/Removing Users

This section contains information on how to add/remove Users from a particular Group. If the administrator would like to modify the Users in a group, the administrator must click on the Users button located on one of the previously mentioned pages (Add Group (Figure 6.14) or Modify Group (Figure 6.15)). Once the button has been clicked, the administrator will see the following page:

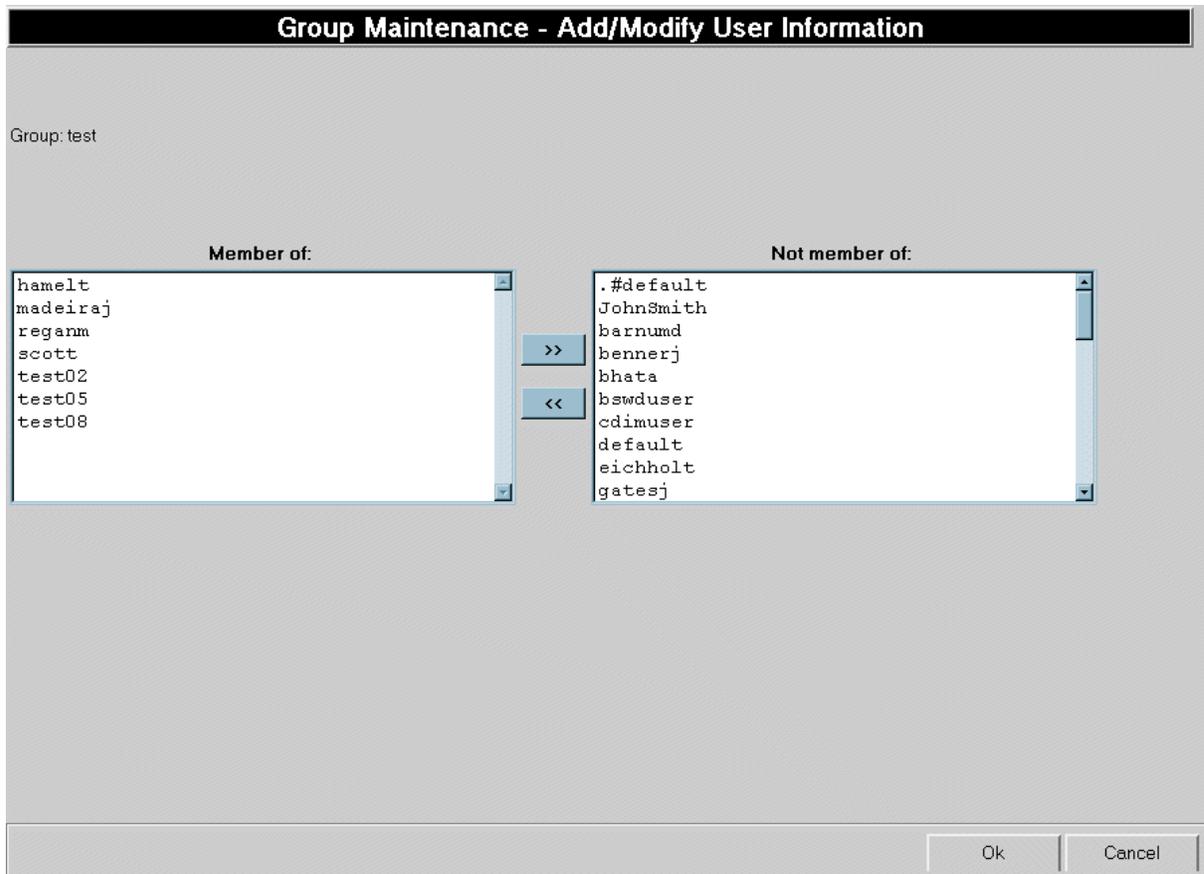


Figure 6.18 - Adding/Removing Users

All of the group's current Users appear in the leftmost list (Member of). All other Users are located in the rightmost list. In order to remove/add a user(s) from the selected group, simply select a list item and click on the relevant button. Once the Ok button has been clicked, all changes will take effect and the administrator will be placed back to the previous page. If at any time the administrator clicks the Cancel button, all changes will be discarded and the administrator will be brought to the previous page.

This page left intentionally blank

SYSTEM OPERATIONS

P A R T I I

The purpose of this part is to provide an overview of the system operations available. Sections covered in this part are:

System Status

- Daemon Status
- Queue Maintenance
- Set Debug Flags
- System and Log Information
- Current Users
- Database Thresholds

System Statistics

- Batch Jobs
- Top Data Sources
- Top Requests
- Web Server Statistics

This page left intentionally blank

Chapter 7

System Status

System Status provides the administrator the ability to manage the operations of the system. Tools are provided to show if all the necessary processes are running, the status of the message queues used for communication between the processes, management of the logs used by the system and available system space and the ability to turn on/off debug flags to assist in identifying problems. By selecting the System Status item (under the Administration pop down menu), the Administrator is presented with a set of options as shown in Figure 7.1.

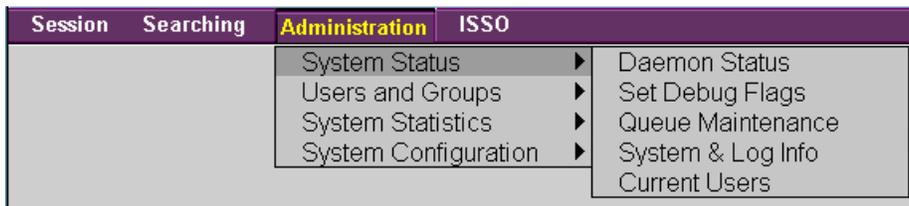


Figure 7.1 System Status Tools

7.1 Daemon Status

The “Daemon Status” screen provides the administrator with the status of the processes that are required to run the system, identifies possible problems and suggests solutions to these problems. Figure 7.2 provides a sample of the Daemon Status screen.

Daemon Status		
Daemon Name	Process ID	Status
conan	14291	running
gatekeeper	1245	running
gatekeeperftp	1250	running
gatekeepermrs	n/a	not running
gatekeepermsl	1260	running
jivacron	1265	running

Figure 7.2 Sample “Daemon Status” Screen

Note: Daemon Status is updated every 30 seconds automatically

The "Daemon Status " screen contains a table that shows the **Daemon Name** , **Process ID** and **Status** for each process. A description of each column follows:

Column Name	Contents
Daemon Name	Name of the daemon process. MANDATORY PROCESSES INCLUDE: conan, gatekeeper, gatekeeperftp, gatekeepermrs, gatekeepermsl, jivacron ADDITIONAL PROCESSES: local plugin(s) and remote_plugin (if remote connectivity is configured)
Process ID	Process ID of the corresponding daemon process. POSSIBLE ENTRIES: Integer value, n/a
Status	Status of the corresponding daemon process. POSSIBLE ENTRIES: running, not running,

Table 7.1 Summary of Values

Upon installation, only the mandatory processes (conan, Gatekeeper, Gatekeeperftp, Gatekeepermrs, Gatekeepermsl, jivacron) will appear in the process table. Each process will have a process ID and a status of **running**. Local plugins (Backside Sources) can be configured from the *Backside Sources* screen accessible within the *System Configuration* option under the *Administration* popdown menu. Access to remote sources is displayed within the *Connected Sites* option accessible through the same menu path.

It is not the purpose of this screen to start/stop the processes. It is not possible to provide this capability through the interface since two out of the six mandatory processes must be running for the interface to work. Thus, it would be possible to stop all processes through the interface, but not be able to start them (or even do anything else). Scripts are provided for the administrator to start, stop and find out whether system processes are running. These scripts are run from the command line.

Note: This page will automatically refresh every 30 seconds.

To Start/Stop the System

To **start** the Broadword processes, do the following:

```
/opt/bswd3.0/scripts/startserver <cr>
```

and press <cr> to accept the defaults.

To **stop** the Broadword processes, do the following:

```
/opt/bswd3.0/scripts/stopserver <cr>
```

and follow the prompts.

Also provided is a command line script which checks the status of the processes without having to log into the interface.

To **check** the Broadsword Server processes, do the following:

/opt/bswd3.0/scripts/whoserver <cr>

7.1.1 Possible Problems/Solutions

The process table should contain information on each of the mandatory processes. Also, any local plugins should also appear in the process table, if they were configured by the administrator. There are several problem conditions that may occur. Table 7.2 lists these conditions. For each problem condition the normal process id and status is shown, along with the process id and status that appears when there is a problem. A possible solution to the problem is also provided.

Condition	Normal		Problem		Possible Problem Solution
	Process ID	Status	Process ID	Status	
Process Should Be Running	integer value	running	n/a	not running	Check for existence of the Daemon Description file (binary). If binary exists, check its ownership and permissions. Also, check for a core file to determine if the process died.
Local Plugin does not Appear	-	-	-	-	Local plugin was not installed. Follow the instructions under Upon Installation to install the plugin.
Mandatory Process does not Appear	-	-	-	-	Contact Technical Assistance, which is identified on the Support screen.

Table 7.2 Summary of Potential Problems/Solutions

7.2 Queue Maintenance

The “Queue Maintenance” screen allows the administrator to perform periodic maintenance on or trouble shoot problems related to the state of the message queue. The message queue shows the message traffic that occurs between the session manager (conan) and client processes (cgi-bins). Figure 7.3 provides a sample of the Queue Maintenance screen.

Queue Maintenance							
Queue ID	Access Modes	Owner	Current Bytes	Current # of Messages	Max Bytes	Last Pid to Send	Last Pid to Receive
100	rw-rw-rw-	root	0	0	4096	20351	27271

Figure 7.3 Sample “Queue Maintenance” Screen

The "Queue Maintenance" screen contains a table that displays information about the current state of the message queue. A description of the information in this table follows:

Column Name	Contents
Queue ID	Identifier for the message queue. VALID VALUE: integer
Access Modes	Message queue access modes are nine characters interpreted as three sets of three bits each. Reading from left to right, the first set refers to the owner's permissions; the next to permissions of others in the user group of the message queue; and the last to all others. Within each set, the first character indicates permission to read, the second character indicates permission to write or alter the message queue, and the last character is currently unused. The permissions are indicated as follows: r Read permission is granted; w Write permission is granted; a Alter permission is granted; - The indicated permission is not granted. VALID VALUE: rw-rw-rw-
Owner	Login name of the owner of the message queue. VALID VALUE: root
Current Bytes*	Number of bytes in messages currently outstanding on the message queue. VALID VALUE: less than the value of Max Bytes
Current # of Messages*	Number of messages currently outstanding on the message queue. VALID VALUE: any number that allows the Current Bytes for these messages to not exceed Max Bytes
Max Bytes	Maximum number of bytes allowed in messages outstanding on the message queue. VALID VALUE: integer
Last Pid to Send	Process ID of the last process to send a message to the queue. VALID VALUE: integer
Last Pid to Receive	Process ID of the last process to receive a message from the queue. VALID VALUE: integer

Table 7.3 Summary of Queue Maintenance Values

Note: Current Bytes and Current # of Messages will appear in red when the Current # of Messages is greater than zero.

There is one button located on the bottom of the page: “Pop Message”. There are times when a message can get stuck in the queue. This can cause either an increase in response time or no response at all. Clicking on the “Pop Message” button allows the administrator to remove a message from the queue. Each click of the button will remove the message that is at the top of the queue.

Note: This page will automatically refresh every 10 seconds.

7.2.1 Possible Problems/Solutions

Problems that may be related to the state of the message queue and possible solutions to these problems are listed in the following table:

Problem Condition	Possible Solution
A user cannot log into Broadword or logins are taking an unusually long time	If the administrator cannot log into Broadword the session manager, conan, may not be running. At the UNIX level check to see if the process conan is running. If conan is not running, start it up by typing /opt/bswd<version_number>/bin/startconan. If conan is running, follow the instructions in the next problem solution.
<p>Response time is unusually long after clicking any action button</p> <p style="text-align: center;">- OR -</p> <p>Get no response after clicking any action button</p>	Messages may be stuck on the message queue or the Current Bytes on the queue may have exceeded the Max Bytes . If the Current Bytes and Current # of Messages are greater than zero and these entries don't go down after a few refreshes, then messages are stuck on the queue. Release stuck messages from the queue by clicking the " Pop Message " button (see the "Button Functions" section for a description). Upon clicking the " Pop Message " button, information on the message that was removed from the queue will appear in a table (see the "Pop Message Info" section). Try popping all the stuck messages from the queue and see if the problem goes away. If the problem remains contact Technical Assistance, which is identified on the "Support" screen, and refer to the " Pop Message Info " table when discussing the problem.

Table 7.4 Summary of Potential Problems/Solutions

7.2.2 Pop Message Info

The "**Pop Message Info**" table contains three types of information on the message that was popped from the message queue after clicking the "**Pop Message**" button. A description of these information types follow.

Information Type	Description
Receiving Process: OR Pid of Receiving Process:	Identifies the process that was to receive the message appearing in the queue. VALID VALUES: conan for Receiving Process , process id of client process for Pid of Receiving Process
Command:	The command that initiated the message that was put on the queue by the sending process. VALID VALUES (conan): Server Response, Server Administration VALID VALUES (client processes): User Login, Save Data Set, Retrieve Data Set, Save User Record to File, Retrieve User Record, Update User Record, User Logout, Make Query, Update User's Preferences, Pull Product, Update E-mail Notification Profiles, Remove Data Set, Update Data Set, E-mail Notification Query, Update Map Data, Failed Login, Message Queue Initialization Failed, Send Message Failed, Receive Message Failed, No Login, User's Session Folder not Found, User's Preferences Folder not Found, User Record not Found, User's Preferences data not Found, Bad Query Status, Unknown Command
Message:	The message that was put on the queue by the sending process. If the sending process was conan, the message is the outcome of a request performed by conan. If the sending process was a client process, the message is information needed by conan to perform a request of the client process.

Table 7.5 Summary of Messages

7.3 Set Debug Flags

The “Set Debug Flags” screen allows the administrator to set or clear debug flags prior to viewing a log file. The **Set Debug Flags** screen should be used when debugging a problem with the assistance of a technical support person. (Technical Assistance is identified on the **Support** screen.) Technical Assistance would instruct the administrator to set certain debug flags depending on the problem being addressed. The information sent to the log file depends on what debug flags are set. Figure 7.4 provides a sample of the Set Debug Flags screen.

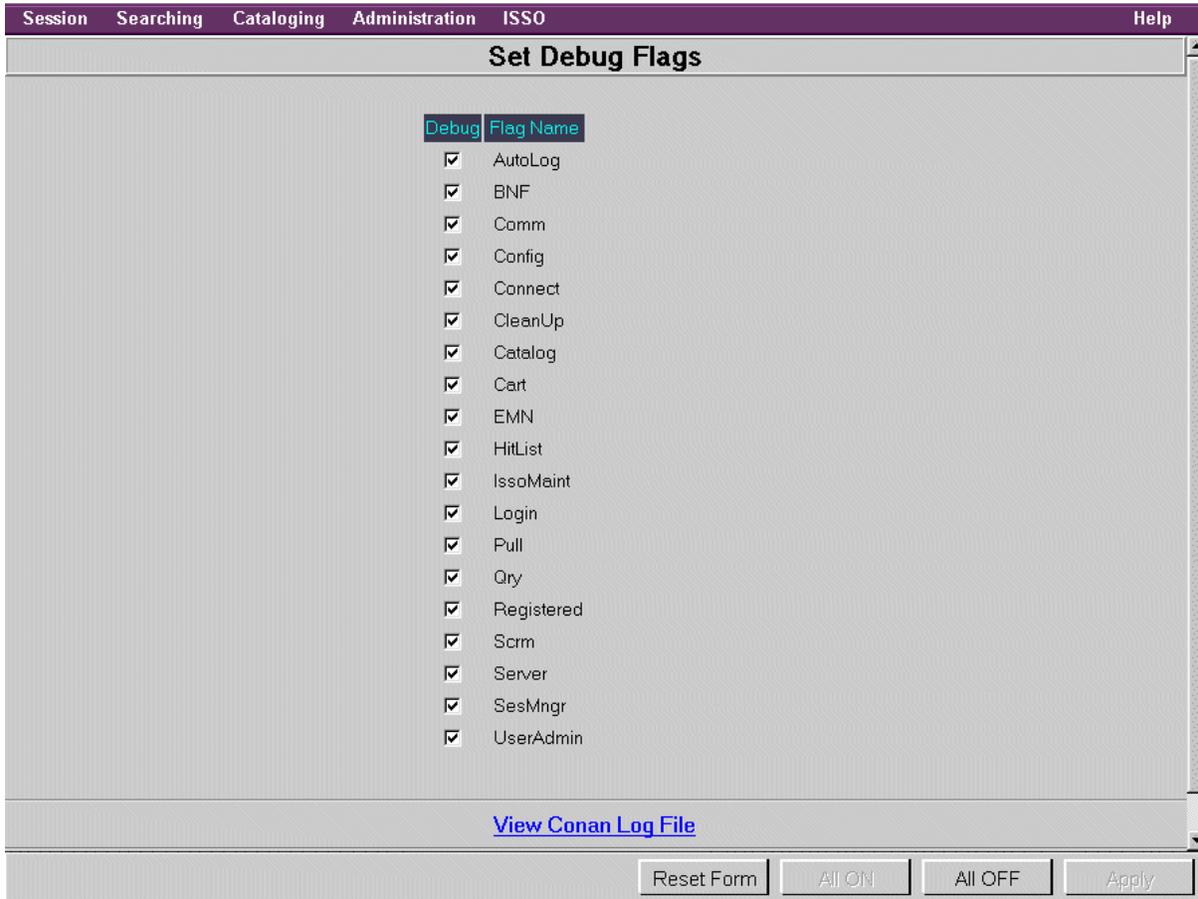


Figure 7.4 Sample “Set Debug Flags” Screen

The "Set Debug Flags" screen contains a table with two columns. These columns are described as follows:

Column Name	Contents
Debug	Checkbox for selecting the debug flag.
Flag Name	Name of debug flag. A AVAILABLE FLAGS: Autolog, BNF, Comm, Config, Connect, CleanUps, Cart, EMN, Hitlist, IssoMaint, Login, Pull, Qry, Registered, Scrm, Server,SesMngr, User Admin.

Table 7.6 Summary of Values

There are four buttons available on this page: (1) **Reset Form**, (2) **All ON**, (3) **All OFF**, and (4) **Apply**. Clicking on the **All ON** button will turn on all the available flags while clicking on the **All OFF** button will turn off all the flags. To select one or a subset of the available flags, click inside the box located next to the item and click on the **Apply** button. The **Reset Form** button will reset the form to those items that were checked upon entering the page.

The log file can be viewed by clicking on the anchor titled **View Conan Log File** located just above the button bar.

7.4 System and Log Information

The **System and Log Information** screen allows the administrator to monitor and/or free up disk space due to log files that are used by the system. Through the **System and Log Info** screen the administrator can select log files to be purged and monitor disk usage information on the file system where the system resides. Figure 7.5 provides a sample of the **System and Log Info** screen.

Select	Log File	Size in Bytes
<input type="checkbox"/>	error_P.log	301,856
<input type="checkbox"/>	access_P.log	27,402,993
<input type="checkbox"/>	agent_log	0
<input type="checkbox"/>	referer_log	0
<input type="checkbox"/>	error_R.log	5,718
<input type="checkbox"/>	access_R.log	91,094
<input type="checkbox"/>	conan.log	179,002,001
<input type="checkbox"/>	pid.log	0
<input type="checkbox"/>	jvacronlog	789,353
<input type="checkbox"/>	cgi_debug.log	967,468

File System	Total Kilobytes	Used	Available	Capacity
/opt/bswd3.0/client	33,452,032	31,272,960	2,179,072	93%

Reset Form Update Purge Marked

Figure 7.5 Sample **System and Log Info** Screen

The **System and Log Info** screen contains two sections. The top section contains the log file information while the bottom section contains the disk usage information. The administrator

should use the information from these two sections to determine if it is necessary to free up disk space due to the log files. The log file information is presented in a table with three columns, which are described as follows:

Column Name	Contents
Select	Checkbox for selecting the log file.
Log File	Name of log file. ACCESSIBLE LOG FILES: see Figure 7.5
Size in Bytes	Size of the log file.

Table 7.7 Summary of Values

The purpose of the accessible log files are described as follows:

Log File	Purpose
error_P.log	Logs httpd error information.
access_P.log	Logs httpd activity information.
agent_log	Logs browser identification information.
refer_log	Logs browser URL/page information.
conan.log	Logs session and client activity information.

Table 7.8 Summary of Log Files

Note: There may be additional Log Files that appear in this screen.

There are two buttons on this page: (1)“Reset Form”(2) “Update” and (3)“Purge Marked”. The “Update” button allows the administrator to display the latest information about the sizes of the log files. Since the table represents a snapshot in time and does not automatically update itself, it is necessary to initiate the update. This is done by clicking the “Update” button. To remove or purge the log files, the administrator must identify the file by clicking in the box next to the log file name and pressing the “Purge Marked” button. The table in the bottom section of the "System and Log Info" screen contains the disk usage information. The contents of this table are described as follows:

Column Name	Contents
File System	Name of file system that contains the log files.
Total Kilobytes	File system's total capacity in kilobytes.
Used	Amount of file system's total capacity that has been used, in kilobytes.
Available	Amount of file system's currently available capacity, in kilobytes.
Capacity	Percentage of file system's capacity that has been used.

Table 7.9 Summary of Values

7.5 Current Users

The “Current Users” screen allows the administrator to monitor the currently logged-in users. Figure 7.6 provides a sample of the “Current Users” screen.

Current Users as of 2000 May 24, 14:31:16		
Username	Conan PID	Time of Log-in
reganm	16052	2000 May 24, 12:16:22
parkerr	16900	2000 May 24, 12:39:15
madeiraj	17898	2000 May 24, 12:54:10
hamelt	18159	2000 May 24, 12:56:30
nickl	19379	2000 May 24, 13:02:38
reganm	21260	2000 May 24, 13:09:47
reganm	21327	2000 May 24, 13:12:21

Figure 7.6 Sample "Current Users" Screen

The "Current Users" screen contains a Username, Process ID, and a timestamp. This information is presented in a table in three columns, which are described as follows:

Column Name	Contents
Username	Login name of currently logged-in user.
Conan PID	Process ID of user's session.
Time of Log-in	Timestamp of user's login.

Table 7.10 Summary of Values

There is one button on this page: "Update", which allows the administrator to display the latest information about the currently logged-in users. Since the table represents a snapshot in time and does not automatically update itself, it is necessary to initiate the update by clicking the "Update" button.

7.6 Database Thresholds

The Broadword system uses a Sybase dataserer to maintain application audit events (see the ISSO section for more detailed information). If the partition on which the dataserer resides is full, then the Gatekeeper will cease to function until space on the system has been freed. In order to mitigate this risk, the Broadword system provides two thresholds at which the administrator is informed of the problem. At any time the system administrator may check the status of the dataserer's disk space by executing the following at the command line:

```
Check the status of Broadword processes (Requires the Database sa password)
% /opt/bswd3.0/scripts/whoserver
```

7.6.1 Level-One Threshold

The Level-One threshold warns the administrator that the dataserer is past a certain point, and that the ISSO should archive the audit logs. Once this threshold is surpassed, each time a user logs into the system the system administrator receives an e-mail warning that the system is nearly out of room to store its audits. The default setting for this threshold is 90%. In order to change this value, the administrator may execute the following at the command line:

```
Shutdown Broadword
% su - root
```

```
# /opt/bswd3.0/scripts/stopsserver  
  (Answer N, N, Y, Y to the stopsserver prompts)
```

Set the new threshold value

```
# source /opt/bswd3.0/etc/server_env_vars  
# setenv SYBASE $BSWD_HOME/odbc  
# setenv BSWD_DB_THRESHOLD <N>
```

Restart Broadsword

```
# /opt/bswd3.0/scripts/startserver  
  (Answer Y, Y to the startserver prompts)
```

Where <N> is an integer from 0 to 99. Setting this threshold to 0 disables notification at this level.

7.6.2 Level-Two Threshold

The Level-Two threshold is the limit after which no users may login to the system until the audits have been archived. If any users were logged into the system at the time that this threshold was reached, then they will be automatically logged out. At this point, the administrator is sent another e-mail. The administrator must now 1) stop the Broadsword system, 2) set this threshold to a higher value, 3) restart the system, and then allow the ISSO to archive the audit records. To reset the system with a new threshold, the system administrator may execute the following at the command line:

Shutdown Broadsword

```
% su - root  
# /opt/bswd3.0/scripts/stopsserver  
  (Answer N, N, Y, Y to the stopsserver prompts)
```

Get the old threshold value

```
# source /opt/bswd3.0/etc/server_env_vars  
# setenv SYBASE $BSWD_HOME/odbc  
# getenv BSWD_DB_FULL_THRESHOLD
```

Set the new value higher than the old one

```
# setenv BSWD_DB_FULL_THRESHOLD <N>
```

Restart Broadsword

```
# /opt/bswd3.0/scripts/startserver  
  (Answer Y, Y to the startserver prompts)
```

After the ISSO has archived the audit logs, the system administrator should execute these steps again, resetting **BSWD_DB_FULL_THRESHOLD** to 98%.

This page left intentionally blank

Chapter 8

System Statistics

System Statistics provides the administrator and site management a view into how their system is being used and how often it is being accessed. The information provided is grouped into three: (1) Batch Jobs, (2) Top Data Sources, and (3) Top Requests. By selecting on the System Statistics item (under the Administration popdown menu), the Administrator is presented with a set of options as shown in Figure 8.1.

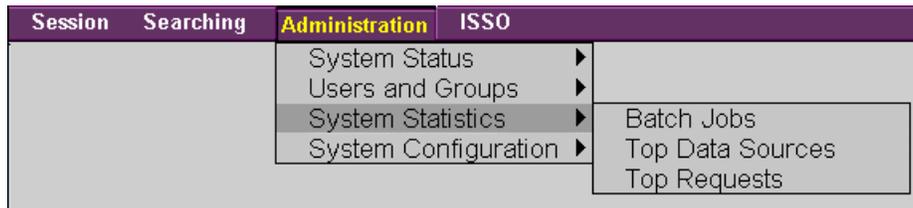


Figure 8.1 - Systems Statistic Tabs

8.1 Batch Jobs

The Batch Jobs screen provides the administrator a log of batch requests. Figure 8.2 provides a sample of this screen.

Batch Jobs						
Line	User	DATE	Status	Job ID	Query Name	Query
1	reganm	1720 May 09 2000	Pending	957892800.a	bahrain	TGT.CTRYCD = "BA"
2	nickl	1713 May 20 2000	Pending	958842780.a	tank_query	KEY.KEYWORD = "tank"
3	reganm	0410 May 10 2000	Pending	957931800.a	eqpctrydsn=US	EQP.CTRYDSN = "US"
4	reganm	1718 May 09 2000	Pending	957892680.a	armyOBT	EQP.OBTTYPE = "G"

Figure 8.2 - Sample "Batch Jobs" Screen

The "Batch Jobs" screen contains a table that shows the Line, User, Date, Status, Job ID, and Query or each Batch Job queued. A description of each column follows:

Column Name	Contents
Line	Line Number
User	Used ID
Date	Scheduled date of execution for the batch job.
Status	Batch job status.
Job ID	Job ID used by cron to identify the batch execution request.
Query	Query to run as a batch job.

Table 8.1 - Summary of Value

8.2 Top Data Sources

The Gatekeeper itself maintains information as to the number of requests that are processed against each of its sources and the number of times a specific product has been ordered. This information can be used by a site to determine which sources are being used the most and in those cases where the site is paying for a service, they can determine if they are getting their money's worth. Figure 8.3 provides a sample screen.

Top Data Sources			
Top 10 Sources	Data Source	Number of Queries	Date of Last Query
1	IPL 1.0 at Sun	7682	2000 May 09, 17:00:07
2	IPL 2.1 at Orion via Saturn	5634	2000 May 09, 17:00:07
3	Source Unk	5065	2000 May 03, 13:00:07
4	Source Unk	4755	2000 May 09, 16:57:49
5	5D at Saturn via Saturn	2351	2000 May 09, 16:50:39
6	5D at 480ig Via Saturn	1935	2000 Mar 01, 21:33:32
7	Source Unk	1582	2000 Feb 25, 21:04:52
8	Source Unk	653	2000 Apr 25, 20:58:18
9	MIDB at Hoth via Saturn	636	2000 May 09, 16:50:39
10	Source Unk	531	2000 May 09, 13:34:12

Figure 8.3 - Sample "Top Data Sources" Statistics Screen

The "Top Data Sources" screen contains a table that shows the top ten Sources, Data Source, Number of Queries, and Date of Last Query for each of the top ten sources accessed by the Gatekeeper. A description of each column follows:

Column Name	Contents
Top Ten Sources	Top Data Sources ordered according to decreasing numbers of references
Data Source	Name of Data Source
Number of Queries	Number of queries made against the Data Source.
Date of Last Query	Date that Data Source was last queried.

Table 8.2 - Summary of Values

8.3 Top Requests

This screen provides the "Top Requests". This portion contains a table that shows the Top 10 Requests, Product Accessid, Product Source, Number of Requests, and Date of Last Request for the Gatekeeper. Figure 8.3 provides a sample of this screen:

Top Requests				
Top 10 requests	Product Accessid	Product Source	Number of requests	Date of Last Request
1	10000000001444	Source Unk	375	2000 May 03, 17:25:59
2	10000000001444	Source Unk	287	2000 May 08, 14:08:02
3	FIVED0800201c10c519961118144341846	Source Unk	34	2000 Jan 25, 22:27:51
4	1000001	Source Unk	16	2000 Jan 11, 22:02:50
5	AFMSS_REPORT	MIDB at Hoth via Saturn	14	2000 Apr 27, 19:22:17
6	1000015	Source Unk	11	2000 Feb 23, 00:17:08
7	8832000	IPL 2.1 at Orion via Saturn	11	2000 Apr 28, 19:42:21
8	10001001027873	MIDB at Hoth via Saturn	10	2000 Apr 20, 13:31:27
9	IPA_sun_24164418ZNov98_757107	IPL 1.0 at Sun	10	2000 Apr 27, 13:17:48
10	1000003	Source Unk	9	2000 Jan 06, 12:53:17

Figure 8.3 - Sample "Top Requests" Statistics Screen

A Description of each column follows:

Column Name	Contents
Top 10 Requests	Line Number
Product Accessid	Unique ID for requested product.
Product Source	Source description from which product was requested.
Number of Requests	Number of requests for the product.
Date of Last Request	Date of last request.

Table 8.3 - Summary of Values

8.4 Web Server Statistics

The Web Server Statistics page capitalizes on W_Usage. W_Usage uses the HTTPD logs, analyzes the data and presents a number of reports. Figure 8.3 provides a sample page.

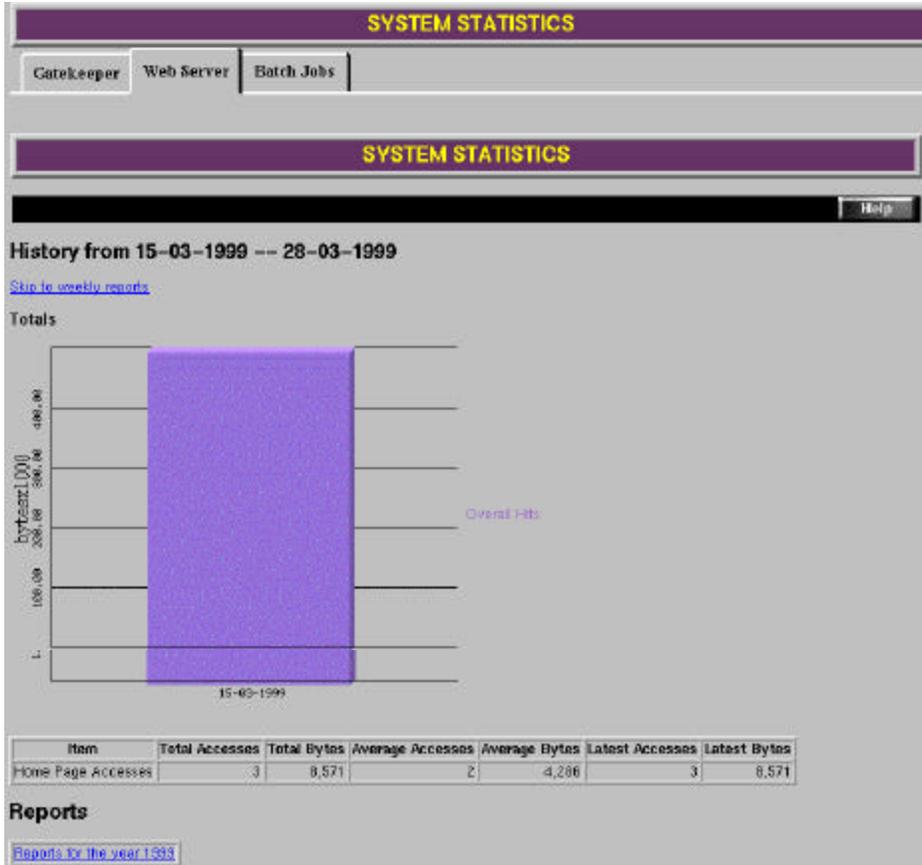


Figure 8.3 - Sample “Web Server” Screen

Totals	The totals from the beginning of the log files to the last time the usage statistics were regenerated for both the total number of bytes transferred and the number of homepage accesses made.
Reports	Links to more detailed weekly reports.

Table 8.4 Main Page

Type of Report	Report Description
Totals	The page begins with a table displaying total accesses and bytes transmitted per hour (average over the week) and per day.
Popular Documents Report	Next in the report is a pie chart and a table featuring the most frequently accessed documents on your site. The pie chart displays only the documents which were "popular" enough to occupy a visible pie slice, and combines the rest in the Other category. The table is ranked by total accesses.
The Frequent Sites Report	Beneath the documents table is a table of the sites that accessed your server most often. The table is ranked by total accesses.
The Result Codes Report	Next to last in the report is a summary of the number of accesses to your server which resulted in each HTTP result code. The result code 200 ("Ok") is usually the most common. Result codes such as 301 ("Moved Permanently") are not uncommon especially if your site uses imagemaps and other forms of redirection. The result code 404 ("Not Found") sometimes means that users are still trying to access a document that has been removed, and solving such problems is the purpose of the last section of the report.
The Documents Not Found Report	This is a list of the URLs that users unsuccessfully tried to retrieve from your server. Sometimes this is due to simple keyboarding error, or to outdated links from other sites. At other times, you may realize that you have accidentally removed or renamed a file, which is a good reason to turn on this option.

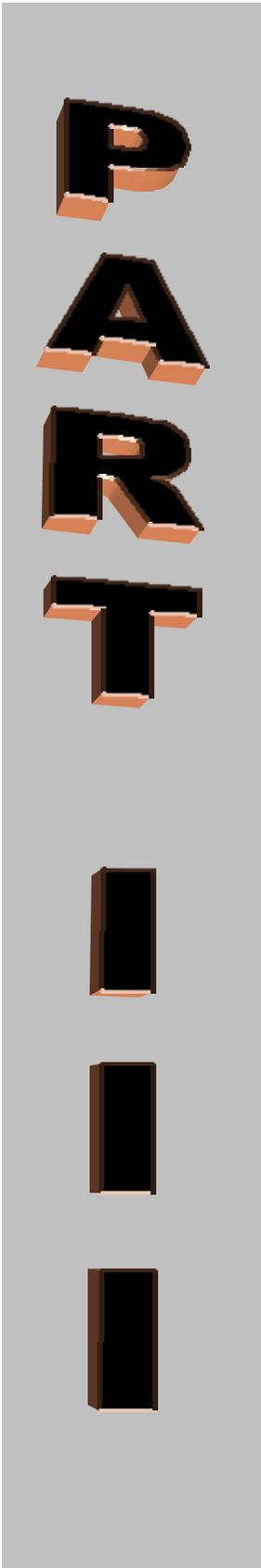
Table 8.5 Weekly Reports

This page left intentionally blank

ISSO

The purpose of this part is to provide security-auditing capability to the ISSO. Sections covered in this part are:

- Audit Log Maintenance
- Archived Logs
- Understanding the Audits



Chapter 9

ISSO

9.1 Audit Log Maintenance and Archiving Logs

The ISSO Interface provides the ability to view, archive, or remove audit information from the Broadsword Sybase Database based on users(s), date/time and audit event. It also allows the ISSO to retrieve previously archived audits. This access is limited to authorized users only. Figure 9.1 shows the **Audit Log Maintenance** page.

The screenshot shows a web interface titled "Audit Log Maintenance". It contains several input fields with labels on the left: "User" (text input with "bswduser"), "Start Date" (text input with "YYYYMMDDhhmmss" and "20000510121845"), "End Date" (text input with "YYYYMMDDhhmmss" and "20000510121845"), "Event" (dropdown menu with "User Logged In"), and "Archive File Name" (empty text input). Below these fields is a blue underlined link labeled "View Audit Report".

Figure 9.1 - Audit Log Maintenance Page

From this screen the ISSO may query the system for audit information based upon the criteria provided in the table. A description of each of these criteria follows:

Parameter	Description
User:	The user account being queried for audit information. DEFAULT: Blank; indicates all user accounts are being queried for audit information.
Start Date:	The start date/time of the audit information being queried. DEFAULT: Current date/time; if Start Date
End Date:	The end date/time of the audit information being

	<p>queried.</p> <p>DEFAULT: Current date/time; if Start Date</p>
Event:	<p>The audit event being queried.</p> <p>POSSIBLE ENTRIES: All Events, Added DAC, Added Group, Added Group Member, Removed Group, Removed Group Member, Added New Source, Get Column Attributes,</p> <p>Added User Privileges, Audit Dump, Get Audit Archive List, Delete Audit, Gatekeeper Started, Gatekeeper Stopped, Got Audit Report</p> <p>Modified Element, Query, Remove DAC, Remove Source, Remove Remote Gatekeeper, Remove User Privileges, Set Source Parameter</p> <p>Set User DAC, Transfer Request, Catalog Request, User Logged In, User Logged Out, Clear Statistics, Accept Registration From Remote Gatekeepers</p> <p>Register Our Gatekeeper With Keymaster, Update Daemon Status, New or Updated Gatekeeper Info, Set User Information, User Changed Password</p> <p>Initiate Stream Request, Terminate Stream Request, Client Profile Management, Client Profile Queue Management</p>
Archive File Name:	<p>Name of file to contain audit records being archived. (The directory path is not included in the filename.)</p> <p>PURPOSE: Needed only when using the "Archive Records" feature.</p>

Table 9.1 - Query Parameters

The function of the buttons in the bottom bar are described as follows:

Button Name	Function
Audit Report	Request an audit report for viewing based on the query parameters selected in the parameter table. If the query is successful, the audit report can be viewed by clicking the " View Audit Report " link located below the parameter table.
Archive Records	Archive the records returned from the query based on the parameters selected in the parameter table. The returned records are stored in the file indicated in the " Archive File Name " field of the parameter table. (This field contains only the filename and should not contain the directory path. The directory where the archive file goes is "/opt/bswd<version_number>/audits".)
Remove Records	Remove the records from the Broadsword Sybase Database that are returned from the query based on the parameters selected in the parameter table. Upon clicking this button, a verification warning message appears below the parameter table, requesting the administrator to click the " Remove Records " button a second time to complete the " Remove Records " request.

Table 9.2 - Button Functions

9.2 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
 - Changing Passwords (LDAP Gatekeepers Only)
 - 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
 - Performing Regional User Maintenance
- (3) ISSO Audits

9.2.1 User and Producer Audits

To begin, user launches a web browser on their local workstation and types in the URL of the assigned Gatekeeper (a Gatekeeper 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.

Table 9.3 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
User Changed Password	CHANGEPWD	LDAP Only
Client Profile Management		NOT USED BY CLIENT
Client Profile Queue Management		NOT USED BY CLIENT
Get Column Attributes		NOT USED BY CLIENT
User Logged Out	LOGOUT	All

Table 9.3 – List of User Audits

9.2.1.1 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 **Example 9.1a** 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 9.1a – Sample Login Record (Successful Login)

Example 9.1b, second line 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 9.1b – Sample Login Record (Invalid Login)

The user has a number of times in which they must correctly enter the login and password. If they don't, the account will be automatically disabled. The number of times, and the mechanism used, depends upon the flavor of Broadsword and the value set. **Example 9.1c** 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 **Example 9.1b**).

```
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 9.1c – Sample Login Record (Login Disabled)

9.2.1.2 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 hence auditing is not required. From a security viewpoint the majority of auditable requirements 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 plug-in(s). For each source that the user has queried an audit record is written verifying that the request was sent to the plug-in and is being processed. The plug-in then processes the request and sends the translated request to the source itself. When the source responds, the plug-in 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. **Example 9.2** 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 9.2 – Sample Query/Response Record

9.2.1.3 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 Plug-in. The Plug-in, 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. **Example 9.3** below 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/bswd3.0/client/PROTECTED/docs/session/4906/ FILENAME:
bswdreg.FIVED08002021976808002021976819980897081558206.NITF02.00
STATUS: Transfer successful. from 5D at Titan via Daleth
```

Example 9.3 – 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), identifies 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.

9.2.1.4 Cataloging a Product

The Broadsword Interface also allows users to produce imagery into IPL 1.0 and IPL 2.x. Every time a user/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. **Example 9.4** shows a product being sent to the IPL 2.1 at Saturn with the title of "BSWD PEND TEST LPA0".

```
CATALOG @ 20001005151630 : Catalog New Product Accepted, PRODUCT  
TITLE: BSWD PEND TEST LPA0 from IPL 2.1 at Saturn  
  
CATALOG @ 20001005151630 : Catalog New Product Ftp to IPA/IPL  
Successful. PRODUCT TITLE: BSWD PEND TEST LPA0 from IPL 2.1 at  
Saturn
```

Example 9.4 – Catalog a new product into IPL 2.1

The first record identifies that the IPL 2.1 plug-in has accepted the product. The second record indicates that the plug-in initiated an FTP session with the appropriate IPL 2.1 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.

9.2.1.5 Changing Passwords (LDAP Gatekeepers Only)

For Gatekeepers that have been configured using LDAP, the user will have the option to change their password through the client. Whenever the user changes their password an audit record is cut. To generate a report of password changes the ISSO can either request **All Events** or select only **Change Password** under the Event popup list. **Example 9.5a** shows that the user has successfully change their password.

```
CHANGEPWD @ 20000926110202 : Password Successfully Changed from  
daleth Gatekeeper
```

Example 9.5a – Changing Passwords

A valid password must meet a number of conditions. **Examples 9.5b – e** provide other possible audits that can be written. The first condition is that the password must be entered correctly and the same twice. If not the user will have a dialog box appearing with the description stating that the two passwords entered did not match and to reenter the passwords. **Example 9.5b** shows the specific audit record that is cut.

```
CHANGEPWD @ 20000926110202 : Passwords did not match from daleth  
Gatekeeper
```

Example 9.5b – Changing Passwords (Invalid Password, Passwords did not match)

The minimum password size is defaulted to 8 characters. When a user enters a new password that is less than 8, a dialog box will appear notifying the user that it must be 8 characters in length. An audit record as shown in **Example 9.5c** is also written.

```
CHANGEPWD @ 20000926110202 : Password is too short, min is 8 from  
daleth Gatekeeper
```

Example 9.5c – Changing Passwords (Invalid Password, Password to short)

Not only does the password have to be a minimum length, but it also must contain a minimum number of special characters. This minimum number is defaulted to 2 and is site configurable. If the user does not supply a password that meets this requirement a dialog box will appear indicating that the password must contain a minimum number of special characters (and what they are). An audit record will also be cut as shown in **Example 9.5d**.

```
CHANGEPWD @ 20000926110202 : Password doesn't have required  
number of special characters (2). Valid special characters are:  
, < . > / ? ; : ' " [ { ] } \ | ! @ # $ ^ & * ( ) - _ = and +.  
from daleth Gatekeeper
```

Example 9.5d – Changing Passwords (Invalid Password, Password must contain Special Character(s))

Other conditions that are enforced as to a valid password are: (1) the password cannot be the same as the user name nor can it be a circular shift of it, (2) it cannot exist in a dictionary and (3) it cannot be a previously used one. The number of previous passwords and their values are stored as part of a history file. The number of entries is site configurable. **Examples 7e – g** provide audits for these events.

```
CHANGEPWD @ 20000926110202 : Password cannot equal your user ID  
from daleth Gatekeeper
```

Example 9.5e – Changing Passwords (Invalid Password, Password cannot be the same as the userid)

A password cannot be a circular shift of the user's name or id. For example, if the user's name or ID were tester01 then the following passwords would not be valid:

```
ester01t      ster01te      ter01tes      er01test  
r01teste      01tester      1tester0
```

```
CHANGEPWD @ 20000926110202 : Password is a circular shift of  
username from daleth Gatekeeper
```

Example 9.5f – Changing Passwords (Invalid Password, Password cannot be a circular shift of your user ID)

A dictionary is provided. A password cannot be contained within the dictionary. If so a dialog box will appear indicating that the password supplied is contained in the dictionary and is not allowed.

```
CHANGEPWD @ 20000926110202 : Password invalid, it is in the  
password dictionary from daleth Gatekeeper
```

Example 9.5g – Changing Passwords (Invalid Password, Password cannot be a valid dictionary entry)

Previous passwords are stored by the system to ensure that the user does not use a previous password. The number of previous passwords is site configurable. If the new password that the user has entered is within the history, a dialog box will appear indicating that the user must enter a different password. An audit record will also be written.

```
CHANGEPWD @ 20000926110202 : Password is in the password history,  
history count is 3 from daleth Gatekeeper
```

Example 9.5h – Changing Passwords (Invalid Password, Password is in the history file)

9.2.1.6 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. **Example 9.6a** provides a sample of this audit.

```
LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper
```

Example 9.6a – 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 (refer to **Example 9.6b**).

```
LOGOUT @ 20000926110202 : Gatekeeper timed out from daleth  
Gatekeeper
```

Example 9.6b – Logout Record (user timed out)

9.2.2 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.

9.2.2.1 An Example with Only Local Requests

Our first example, as pictured in **Figure 9.2**, includes only one Gatekeeper. A Gatekeeper (Daleth, IP Address 123.45.678.89) is connected to three local sources: IPL 1.0, 5D and MIBD.

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".

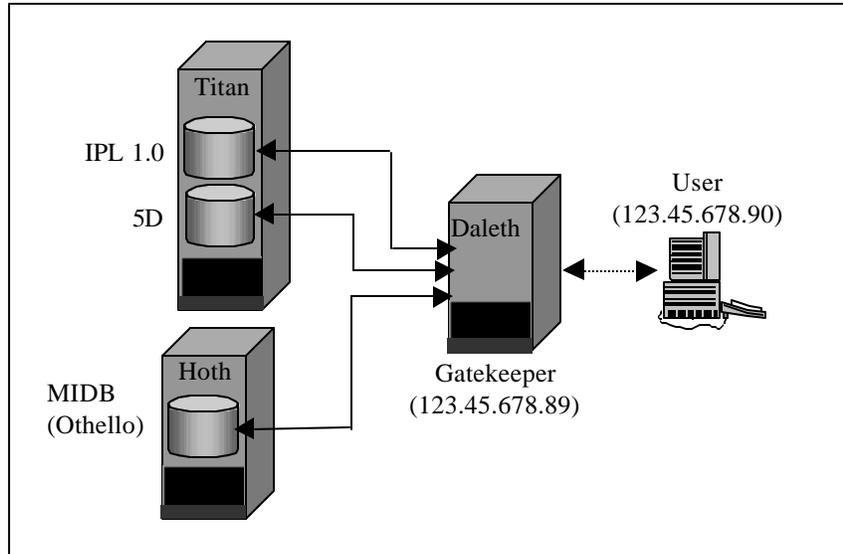


Figure 9.2 – Performing a Local Request

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. **Figure 9.3** 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 **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 Titan via Daleth
QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAILS=Y,
MAX_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from IPL 1.0 at Titan via Daleth
QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS, THUMBNAILS=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 1.0 at Titan via Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID: FIVED80201de96719970826204522533
from IPL 1.0 at Titan via Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID: FIVED80201de96719970826204301083
from IPL 1.0 at Titan via Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID: FIVED80201de96719970826204109470
from IPL 1.0 at Titan via Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID: FIVED80201de96719970826203915123
from IPL 1.0 at Titan via Daleth
QUERY @ 20000926105619 : titan IPA: 00060 Hits from IPL 1.0 at Titan via Daleth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

Figure 9.3 – Sample Audit Report (Request) for User “gen_user”

9.2.2.2 What do the Audits Say?

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 1.0 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 IPL 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 60 hits. Since the user/client requested a maximum of 5 hits, only 5 are sent back. (IPL 1.0 does not have the ability to limit the number of hits on its own – thus the plugin will receive all the hits from the given request and limit the hits based on the maximum hit size.)

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.

9.2.2.3 An Example with Local and Remote Requests

Our next example, as pictured in **Figure 9.4**, 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 2.1.

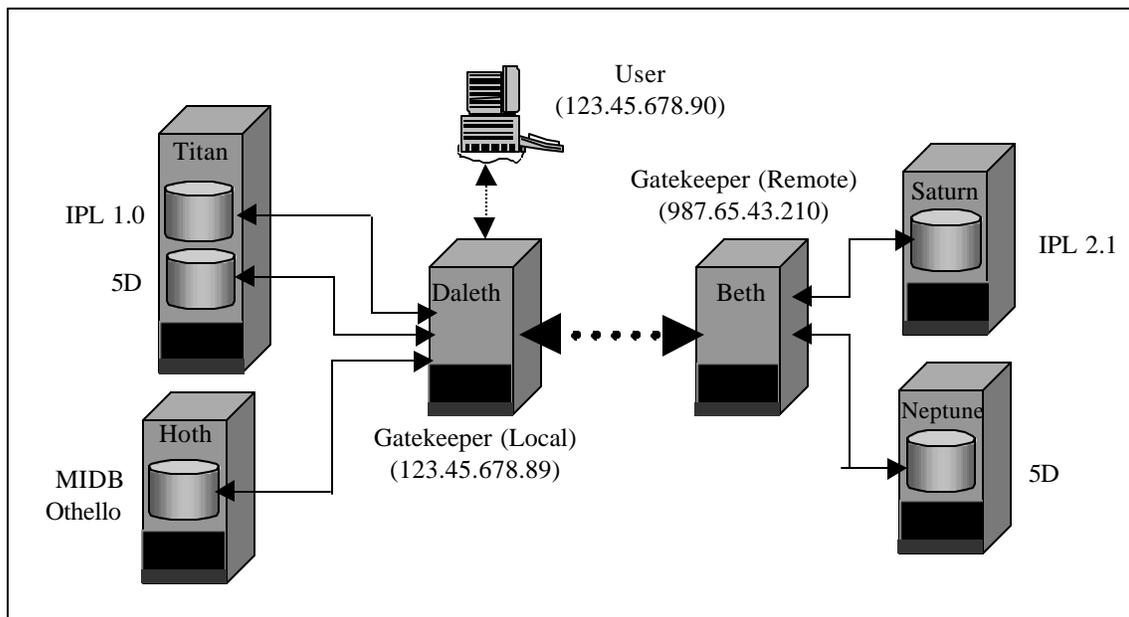


Figure 9.4 – Performing a Local & Remote Request

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. **Figure 9.5** 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 2.1. 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 Gtckpr:
123.45.678.89 Session Key: 4907
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULT ANEOUS,
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 5D at Saturn
via Beth

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

Q: How do I know this is a remote query?

A: This is not the name of the local Gatekeeper.

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED8002021976808002021976819970327205627650 from 5D at Titan via
Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED8002021976808002021976819970327211927560 from 5D at Titan via
Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED8002021976808002021976819970827081558206 from 5D at Titan via
Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED8002021976808002021976819970827082616003 from 5D at Titan via
Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED8002021976808002021976819970827083055386 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:
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

Local Gatekeeper Audits (Daleth)

Audit Report

User: gen_user For All Dates For All Events.

Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user Gtckpr:
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 Saturn
via Beth

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULTANEOUS,
THUMBNAIIS=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

Remote Gatekeeper Audits (Beth)

Figure 9.5 – Sample Audit Session with Local & Remote Queries

9.2.3 Administrative Audits - Configuring and Maintaining the System

The Broadword client provides the Administrator the ability to (1) configure/tailor the Broadword 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 get 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. **Table 9.4** provides a summary of the audits generated by the administrator.

Administrative 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		
Set User Information	SETUSERINFO	LDAP Only
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 9.4 – List of Administrator Audits

As described in Chapter 7, the administrator has the ability to configure and tailor the Broadword system to meet the site's specific requirements. Audit events are described below along with an example of a typical audit record. The specific auditable events include adding backside sources, configuring attributes, adding/modifying users, registering the gatekeeper with the keymaster.

9.2.3.1 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 (to be discussed later). Sources set to allow **Local Access Only** only allow access 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.

Example 9.9a shows the creation of a new backside source. The source that was added was an IPL 2.1 to the Gatekeeper whose name is 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 9.9a – 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**.

Example 9.9b 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

ADDAC @ 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 9.9b – Add an IPL 2.1 source and allow access to only local users

In this example, the **ADDAC** 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.

Example 9.9c 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 9.9c – 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. **Example 9.10** shows the audit record that is written when a source attribute has been modified while **Example 9.11** is an 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 9.10 - 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 9.11 - 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. **Example 9.12** 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 9.12 – Modifying the Gatekeeper's Point of Contact

9.2.3.2 INK Maintenance

Using the DE Configuration capability, the administrator can modify an existing attribute's name, help and pop-down values. **Example 9.13** and **Example 9.14** The 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 **Example 9.13** the administrator has removed an entry from the pop-down list. In **Example 9.14**, the administrator has added a new entry to the pop-down 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 9.13 – 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 9.14 - Adding a new pop-down

9.2.3.3 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 9.4 and 9.5**). The Keymaster maintains a global list of each Gatekeeper’s **local map** (referred to as the **global map**). **Table 9.5** provides a list of Keymaster audit events.

Administrative Security Audits (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 9.5 – Keymaster Audit Events

Figure 9.6 shows the example environment that we will consider for the following examples.

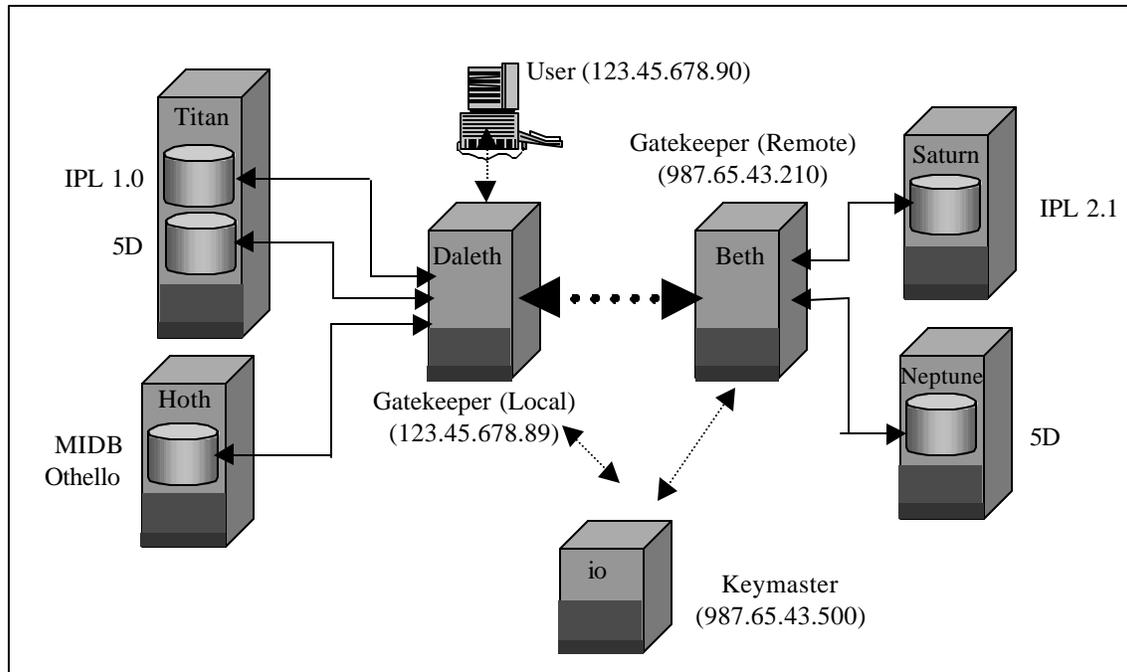


Figure 9.6 – Keymaster/Gatekeeper Environment

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.

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.

Figures 9.7a and **9.7b** provide example audit records from a successfully completed Gatekeeper registration, a map update, and the unregistration of a Gatekeeper.

09 January 2001

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 : Connection closed from io
Keymaster
CONFIGUPDATE @ 20001204185137 : Configuration Update From
io Keymaster, IP Addr: 123.45.678.90 Was Successful from
io Keymaster

```

Register New Gatekeeper

```

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 @ 20001204184638 : Gatekeeper Registration Started
from io Keymaster
INITREG @ 20001204184958 : Gatekeeper Registration
Completed For daleth Gatekeeper from io Keymaster
LOGOUT @ 20001204190507 : Connection closed from io
Keymaster

```

Map Updates

```

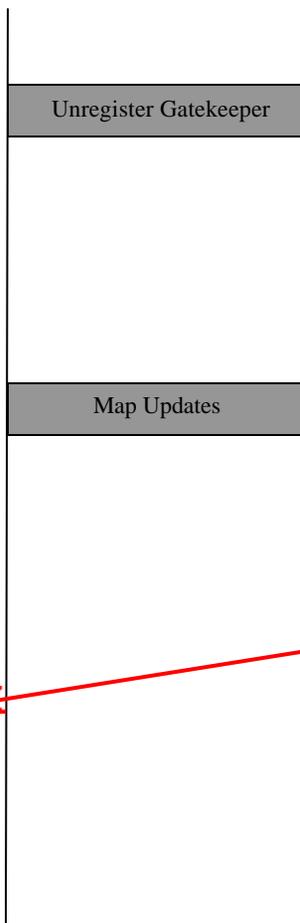
Login: root IP: 987.65.43.500 Orig. Login: root Gtkpr:
987.65.43.500 Session Key: 813
UPDATE_DAEMON @ 20001204184957 : Update Daemon Started
from io Keymaster
UPDATE_DAEMON @ 20001204185013 : Successfully sent
Configuration To (beth Gatekeeper), with Ref
(80aae5f1:987654123) from io Keymaster
UPDATE_DAEMON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

```

Figure 9.7a – 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
```



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  
UPDATE_DAEMON @ 20001204185138 : Update_daemon Exiting from io Keymaster
```

Figure 9.7b – Unregister a Gatekeeper

9.2.3.4 User Maintenance

Broadsword version 3.0 supports two methods for performing local user maintenance. The first method supports the way in which user access and authentication was performed in version 2.0. If the site chooses not to use the LDAP capability, they will continue to create user accounts through CSE-SS or Sun Tools and add privileges/accesses through the Broadsword administration interface.

If the site chooses to use the LDAP option, user maintenance is supported through a single administrator's interface. From this interface, the administrator creates user accounts and assigns groups and accesses. The information entered is stored in two different areas. General user information is stored in the Gatekeeper's LDAP while password management information is stored in a database (For more on this, see Section 1.2.3 of this document). **Examples 9.15a** and **9.15b** provide audit records for adding, and subsequently modifying a user account.

```
SETUSERINFO @ 20001005150223 : Following parameters Changed For daleth  
Gatekeeper, User gen_user: User Password, Given Name, Middle Initial,  
Surname, Language Proficiency (Reading Comprehension), Language Proficiency  
(Listening Comprehension), Citizenship, Home Organization, Account Locked?,  
Employee Type, Grade, Physical Country Name, Expert Country from daleth  
Gatekeeper
```

Example 9.15a – Adding a New User (LDAP Only)

```
SETUSERINFO @ 20001005150223 : Following parameters Changed For daleth  
Gatekeeper, User gen_user: Account Locked? from daleth Gatekeeper
```

Example 9.15b – Modifying an Existing User (LDAP Only)

The SETUSERINFO record is generated whenever an account is added or modified. The fields listed in **Example 9.15a** (e.g. - Given Name, User Password, etc.) are the mandatory fields required for creating an account.

Regardless of the gatekeeper configuration, an existing user can be deleted. In an LDAP configured system, the user's files along with all account information is deleted. In a CSE-SS or UNIX only system, 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, their accounts 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. **Example 9.16** displays the audit record that is written when a user account has been removed.

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

Example 9.16 – Removing an Existing User

Once the user has created the account using the LDAP version or are using CSE-SS/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 **Example 9.17**) is written.

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

Example 9.17 – Adding Source Access for a User

Likewise, when the administrator removes access to a given source an audit record (as shown in Example 9.2) is written.

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

Example 9.18 – Adding Source Access for a User

The administrator can add additional privileges to a user account. These privileges include Administrator, ISSO or producer/catalog ability. Our example below shows that the user “gen_user” was given the ability to catalog to an IPL2.1 system.

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

Example 9.19 – Adding Role Privilege

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

Example 9.20 – 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 examples show a user being added (**Example 9.21**) and removed (**Example 9.22**) from a group.

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

Example 9.21 – Adding a User to the Group ‘Test’

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

Example 9.22 – Removing a User from the Group ‘Test’

9.2.3.5 Group Maintenance

Users can belong to one or more groups. Groups allow the administrator to group a set of common accesses and privileges together and to simply add the user to the group. By doing this, the administrator does not have to go and individually add roles and sources to each user. 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, (e.g., - 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. **Example 9.23** shows the audit record written when the group is created.

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

Example 9.23 – 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. **Example 9.24** 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 9.24 – Modified Description for Group Named ‘DBM’

Example 9.25 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 9.25 – Added User Named ‘testact1’ to Group Named ‘DBM’

Example 9.26 provides 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 9.26 – Deleted User Named ‘testact1’ to Group Named ‘DBM’

Example 9.27 provides an example of an audit record when the group is deleted.

```
DELGROUP @ 20001006120814 : Deleted Group DBM from Daleth Gatekeeper
```

Example 9.27 – Deleted Group Named ‘DBM’

9.2.3.6 Operations Maintenance

Upon startup, the Gatekeeper cuts an audit record.

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

Example 9.28 – Gatekeeper Startup

9.2.3.7 Performing Regional User Maintenance

If a Gatekeeper is registered with a Keymaster, and configured to use the LDAP Gatekeeper, user accounts can be created by authorized Keymaster administrators. To add a user through the Keymaster, the administrator (assuming the administrator has been given the authority by the appropriate Gatekeeper Administrator) first chooses which Gatekeeper they would like to add a user account. An authentication process, similar to that used between Gatekeepers performing remote queries, is performed before the Keymaster is allowed in. From this point on, the Keymaster interface is identical to that of the local Gatekeeper. All information is entered directly into the Gatekeeper just as if a local administrator is performing the same operations. By accessing the Gatekeeper's information directly, the configuration data is always current.

9.2.4 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. **Table 9.6** 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 9.6 – ISSO Audits

Examples 9.29 – 9.32 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 9.29 – Query Audit Records

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

Example 9.30 – Generate an Audit Archive

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

Example 9.31 – Query an Archive Record

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

Example 9.32 – Delete an Audit Record

Example 9.29 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 **Example 9.30** the ISSO generated an audit archive for the previous audit record. **Example 9.31** 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 **Example 9.32**. 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 9.32 – 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.

This page left intentionally blank