



SYSTEM INSTALLATION & MAINTENANCE
GUIDE
FOR
BROADSWORD KEYMASTER
VERSION 3.0.1



Prepared for:

AFC2ISRC/A26
LANGLEY AIR FORCE BASE, VA 23665

Prepared by:

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

June 2002

Points of Contact

Broadsword Program Office: Captain Gretchen Anderson

Commercial Phone: (315) 330-7966

DSN: 587-7966

Unclassified email: andersog@rl.af.mil

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

Air Force POC: Major Hans. F. Von Milla, AFC2ISRC/A-264

Commercial Phone: (757) 225-1137

DSN: 575-1137

Unclassified email: hans.vonmilla@langley.af.mil

Configuration Management:

Commercial Phone: (315) 330-2723/4209

DSN: 587-2723/4209

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

Technical Assistance (IDHS Help Desk):

Commercial Phone: (315) 330-IDHS (4347)

DSN: 587-IDHS (4347)

Unclassified email: idhs.help@rl.af.mil

Mailing Address and Fax Number:

AFRL/IFEB

32 Brooks Road

Rome, New York 13441

(315) 330-3913



This page intentionally left blank

CHAPTER 1 INTRODUCTION	1
1.1 INSTALLATION OVERVIEW.....	1
1.2 SYSTEM DESCRIPTION.....	3
1.2.1 <i>Gatekeeper</i>	5
1.2.1.1 User Services.....	6
1.2.1.2 Administration Services.....	7
1.2.1.3 Security Audit Review.....	8
1.2.1.4 Plugins.....	9
1.2.2 <i>Keymaster</i>	9
1.2.3 <i>Trusted Transfer Agent (TTA)</i>	10
1.2.3.1 Overall Architecture of TTA.....	10
1.2.3.2 MD 5 Integrity Seals.....	11
1.2.3.3 Secure Socket Layer (SSL).....	12
1.2.3.4 Message level and field level filtering.....	12
1.2.3.5 Masking of Sensitive Fields for Information Passed from High to Low.....	13
1.2.4 <i>The Broadsword Client</i>	13
1.2.4.1 General.....	15
1.2.4.2 Searching.....	15
1.2.4.3 Administration.....	16
1.2.4.4 ISSO.....	17
1.2.4.5 Certification Boundary.....	17
CHAPTER 2 GETTING STARTED	21
2.1 SERVER REQUIREMENTS.....	21
2.2 PREPARING YOUR SYSTEM.....	22
2.3 SITE CONFIGURATION WORKSHEET.....	31
CHAPTER 3 INSTALLATION	37
3.1 LOADING THE SOFTWARE AND STARTING THE SETUP SCRIPT.....	38
3.2 PROVIDING INSTALLATION CHOICES.....	41
3.2.1 <i>Providing CD-ROM Registration Information</i>	42
3.2.2 <i>Determining the Import Preference</i>	43
3.2.2.1 Dataserver/Database Configuration.....	43
3.2.2.2 Creating a New Dataserver.....	44
3.2.2.3 Sharing an Existing Dataserver.....	48
3.2.3 <i>Keymaster Configuration</i>	51
3.2.4 <i>Client Configuration</i>	52
3.2.5 <i>POC Configuration</i>	53
3.3 CONFIRMING INSTALLATION CHOICES.....	54
3.4 INSTALLATION PROGRESS.....	55
3.5 INSTALLATION VERIFICATION.....	61
CHAPTER 4 SYSTEM ADMINISTRATION	66
4.1 GATEKEEPER/TTA REGISTRATION.....	66
4.2 VIEWING AND UNREGISTERING GATEKEEPERS OR TTA GATEKEEPERS.....	67
4.2.1 <i>How to Unregister a Gatekeeper or TTA Gatekeeper</i>	67
4.3 KEYMASTER CONFIGURATION.....	68
CHAPTER 5 USER MAINTENANCE	70
5.1 USER MAINTENANCE.....	70
5.2 ADDING/REMOVING ROLES.....	72
CHAPTER 6 CLIENT REQUIREMENTS	75
6.1 HTML BROWSERS.....	75

CHAPTER 7 SYSTEM STATUS	79
7.1 DAEMON STATUS	79
7.1.1 Possible Problems/Solutions.....	81
7.2 QUEUE MAINTENANCE.....	82
7.2.1 Possible Problems/Solutions.....	83
7.2.2 Pop Message Info	84
7.3 SET DEBUG FLAGS	84
7.4 SYSTEM AND LOG INFORMATION.....	85
7.5 CURRENT USERS.....	87
7.6 DATABASE THRESHOLDS	87
7.6.1 Level-One Threshold.....	88
7.6.2 Level-Two Threshold	88
CHAPTER 8 ISSO.....	92
8.1 AUDIT LOG MAINTENANCE AND ARCHIVING LOGS.....	92
8.2 UNDERSTANDING THE AUDITS.....	93
8.2.1 Global Registration/Maintenance.....	94
APPENDIX A - TEST CASES	A-1
APPENDIX B - CHANGING DATASERVER PASSWORD.....	B-1
APPENDIX C - UNINSTALLING KEYMASTER	C-1
APPENDIX D- COTS/GOTS SAMPLE INSTALLATION INSTRUCTIONS	D-1
APPENDIX E- KEYMASTER DIRECTORY LISTING.....	E-1

This page intentionally left blank

Chapter 1

Introduction

The purpose of the System Installation & Maintenance Guide is to provide detailed procedures to install a new copy of Broadsword Keymaster Version 3.0.1 or to upgrade an existing Version 3.0 to Version 3.0.1. It also provides configuration information and discussion on tools provided to maintain the system.

This document is divided into four parts: (I) Installation, (II) Configuration, (III) Maintenance, and (IV) ISSO. The remainder of this chapter provides an overview of the Broadsword system, its architecture and functionality, and an overview of the installation process.

1.1 Installation Overview

A Broadsword Keymaster may be installed either on a dedicated server or it can be installed on an existing server that supports other applications. It is only feasible to co-host Broadsword with another application if that host meets the server requirements described in Table 2.1.

In order to implement trusted transfer agent functionality across disparate security domains (e.g. reach down from high to low side) it is also necessary to install the TTA Version 1.0.2 software on a Broadsword Gatekeeper in each domain. Installation of TTA Version 1.0.2 requires three dedicated hosts: (1) TTA Gatekeeper (high side), (2) ISSE Guard, and (3) TTA Gatekeeper (low side). These three hosts are in addition to any Broadsword Gatekeepers that the site may wish to install in order to access local and remote backside sources on the high and low side.

Regardless of the configuration implemented, a Broadsword Keymaster Version 3.0.1 must be available within the respective security domain before attempting to register a Broadsword Gatekeeper Version 3.1 within that domain.

The remainder of this chapter provides an overview of Broadsword and TTA, architecture and functionality. Table 1.1 provides an outline of the steps necessary to install a dedicated Broadsword Keymaster or a Broadsword Keymaster co-hosted on another application server. Using Table 1.1, select the column with the “Existing Configuration” (at the top of the table) and “Target Configuration” (at the bottom of the table) that best matches your site’s current and desired Broadsword configuration. Be sure to complete all prerequisite steps listed in Table 1.1 (for your configuration) before proceeding with the installation of the Broadsword software. Samples for many of the prerequisite steps are provided in Appendix D of this document. For detailed instructions regarding Broadsword Keymaster installation, refer to Chapters 2-4.

Step	Description	Existing Configuration			
		BSWD 3.0 KM Solaris 2.6 CSE-SS 1.4.2.1 Sybase 11.5.1	BSWD 3.0 KM Solaris 7 CSE-SS 1.4.2.1 Sybase 11.5.1		
1	Full Backup (BSWD SIG App D)	✓	✓	✓	✓
2	Repartition disk drives (BSWD SIG App D)	✓	✓		
3	Restore Backup (BSWD SIG App D)	✓	✓		
4	Install Solaris 2.6 (BSWD SIG App D)				
5	Upgrade to Solaris 7 (+ patches) (BSWD SIG App D)	✓	✓		
6	Install Solaris 7 (+ patches) (BSWD SIG App D)				
7	CSE-SS 1.4.2.1 upgrade to Solaris 7 (BSWD SIG App D)	✓			
8	Install Sybase 11.9.2 (BSWD SIG App D)	✓	✓	✓	✓
9	Install CSE-SS 1.4.2.1 (BSWD SIG App D)				
10	Install CSE-SS Patches (BSWD SIG App D)	✓			
11	Install AFDI 1.1.0.1 (BSWD SIG App D)		✓		✓
12	BSWD Full Install (BSWD SYIMGK Chap 2-3)	✓	✓	✓	✓
13	BSWD GKPR Configuration & Registration (BSWD SYIMGK Chap 4)	✓	✓	✓	✓
14	Install, Configure, Register & Enable TTA 1.0.2 (BSWD SIG Chap 5-7)				
15	BSWD Client Configuration (BSWD TFM)	✓	✓	✓	✓
Step	Description	BSWD 3.0.1 KM Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.0.1 KM Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2	BSWD 3.0.1 KM Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.0.1 KM Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2
Target Configuration					

Table 1.1 Installation Sequence

8	Install Sybase 11.9.2 (BSWD SIG App D)	✓	✓	✓	
9	Install CSE-SS 1.4.2.1 (BSWD SIG App D)		✓		
10	Install CSE-SS Patches (BSWD SIG App D)		✓		
11	Install AFDI 1.1.0.1 (BSWD SIG App D)			✓	
12	Keymaster Full Install (SYIMGK Chap 2-3)	✓	✓	✓	
13	Keymaster Configuration & Registration (SYIMGK Chap 4)	✓	✓	✓	
14	Install, Configure, Register & Enable TTA 1.0.2 (BSWD SIG Chap 5-7)				
15	Keymaster Client Configuration (BSWD TFM)	✓	✓	✓	
Step	Description	BSWD 3.0.1 KM BSWD 3.1 GKPR Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2 Sybase 12	BSWD 3.0.1 KM Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.0.1 KM Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2	
Target Configuration					

Table 1.1 – Installation Sequence (continued)

1.2 System Description

Broadsword implements a multi-tier architecture supporting a single, seamless interface that is secure and administratively manageable. The Broadsword architecture contains four functional components. These components collectively act on behalf of all parties (the Information System Security Officer

(ISSO), System Administrator and User) and are tailored to meet the connectivity requirements of the site. Table 1.2 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	Maintains and distributes a global map of published data sources to permit remote Gatekeepers' users access, assuming both the data source's local Gatekeeper and the remote Gatekeepers are registered with the same Keymaster. In the existing environment, there is only one Keymaster for each Security Domain.
Trusted Transfer Agent (TTA)	TTA allows the user to query a lower security domain and retrieve products without human intervention while crossing between security domains. It is a separate package of code that also relies on the installation of an ISSEGUARD server.
Broadsword Client	Web Based graphical user interface which implements the Client/Gatekeeper API and provides ISSO, System Administrator and General Searching/Product Producer capabilities.

Table 1.2 – Summary of Broadsword Functional Components

1.2.1 Gatekeeper

The Gatekeeper 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. A third section is the various plugins which connect to the datasources. Figure 1.1 shows the architecture of the Gatekeeper.

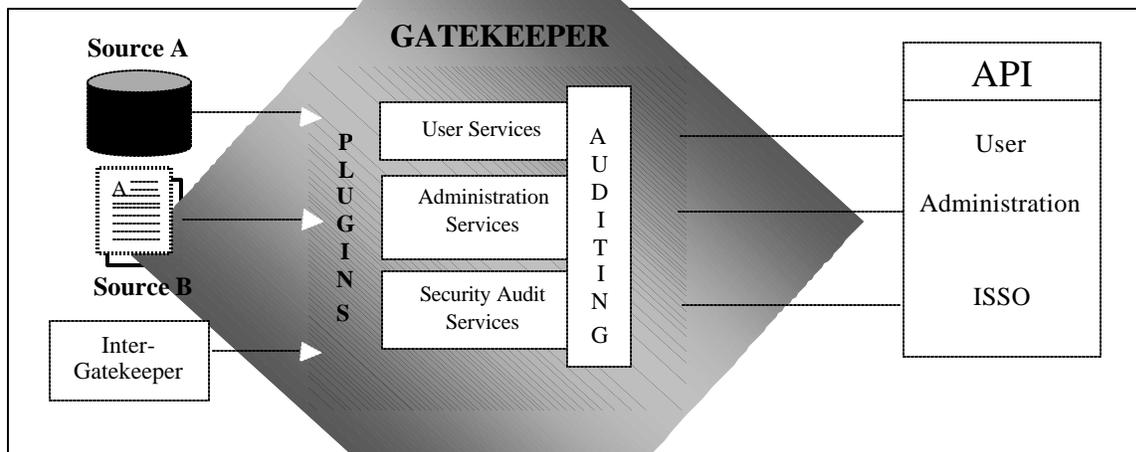
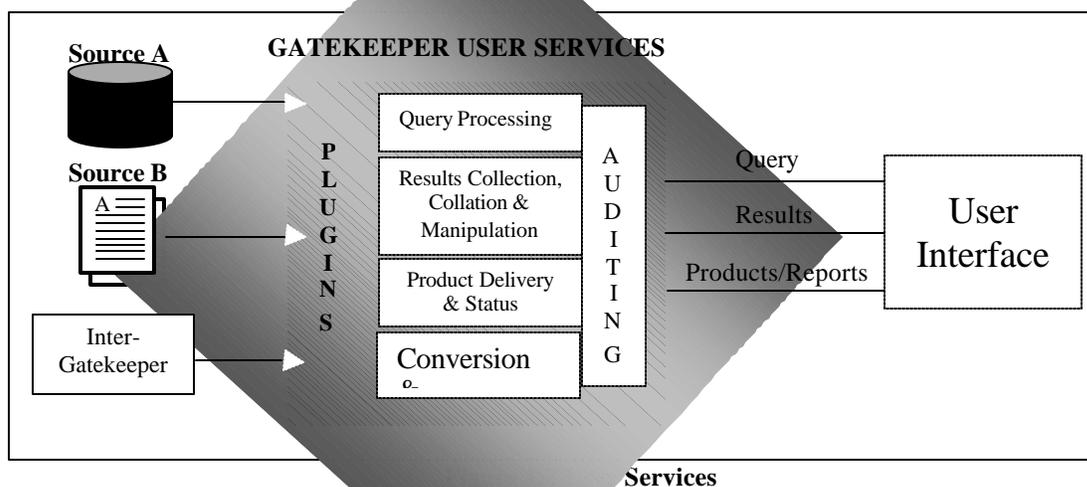


Figure 1.1 Gatekeeper Architecture

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 spatial or SQL based. The availability of request options (such as queryable data elements, returnable data elements, or applicable search utilities) is dependent upon the sources connected and what each source supports. Once a request is submitted, the Gatekeeper audits the request, forwards it to all appropriate sources via plugins, 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 the requester. Figure 1.2 summarizes the major functionality provided by the Gatekeeper through the User Service portion of the interface.



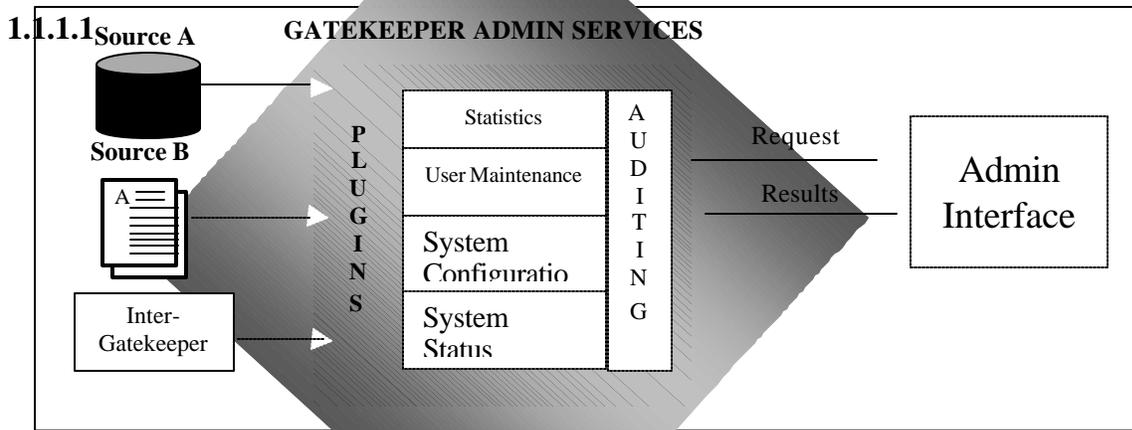
Some of the sources that are connected to the Gatekeeper may support the ordering and delivery of products. Products include reports from database sources, messages, documents, video clips, maps, and images. Delivery mechanisms from the individual sources include non-real-time mail order delivery, FTP delivery, or 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 do not have nor wish to pay for a special application), the Gatekeeper provides conversion support to TIFF 6.0 and JPEG formats.

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. The mode is a combination of Sun Tools/CSE-SS/AFDI and the Broadsword Administrative Interface. User account creation and password maintenance is managed through CSE or AFDI, while Broadsword roles and source accesses are maintained through the Broadsword Administration Interface. 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 1.3 summarizes the major functionality provided by the Administration Services.



Admin 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. Broadsword currently requires Sybase SQL Server or Adaptive Server 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 Out
Query	User Logged In	Delete a Managed Queue Entry
Update Managed Product Meta-data	Update Site Specific Catalog Info	
Administration Events:		
Added Discretionary Access Control (DAC)	Gatekeeper Stopped	Removed Group
Added Group	Get Column Attributes	Removed Group Member
Added Group Member	Initiate Stream Request	Remove Source
Added New Source	Modified Element	Set Source Parameter
Added User Privileges	New or Updated Gatekeeper Info	Set User Discretionary Access Control (DAC)
Clear Statistics	Register Our Gatekeeper With Keymaster	Terminate Stream Request
Gatekeeper Started	Remove Discretionary Access Control (DAC)	Update Daemon Status
Remove User Privileges	Removed Remote Gatekeeper	Modified Group
Client Management	Client Profile Queue Maintenance	
ISSO Events:		
Audit Dump	Got Audit Report	Delete Audit

Table 1.3 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 Broadsword.

1.2.1.4 Plugins

Plugins are the segments of code which sit between the Gatekeeper and a specific datasource. Examples include the IPL25 Plugin, which interfaces with IPL 2.5 and 2.5.1, or MIDB Plugin, which interfaces with MIDB. The Gatekeeper installs with a full set of plugins for all datasources that it currently exist supports. These plugins are not run until the Broadsword Administrator configures a backside source of the appropriate type through the Administrative services. One copy of each configured plugin is run, regardless of how many instances of that type of datasource is configured. Each of the above figures (Figures 1.2 and 1.3) demonstrate the logical placement of the plugins.

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 published sources. Queries and product requests performed between the available Gatekeepers do not involve the Keymaster. The Gatekeepers monitor themselves automatically for changes, and push any changes which affect the global map up to the Keymaster every four hours. In turn, the Keymaster consolidates this information and broadcasts either a 'No Change' message or a message detailing the change(s) to all the Gatekeepers registered to it every four hours. Changes in a specific Gatekeeper's configuration are propagated up to the registered Keymaster and are then propagated back down to all other Gatekeepers. Figure 1.4 shows the Broadsword architecture with two Gatekeepers and a Keymaster. 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.

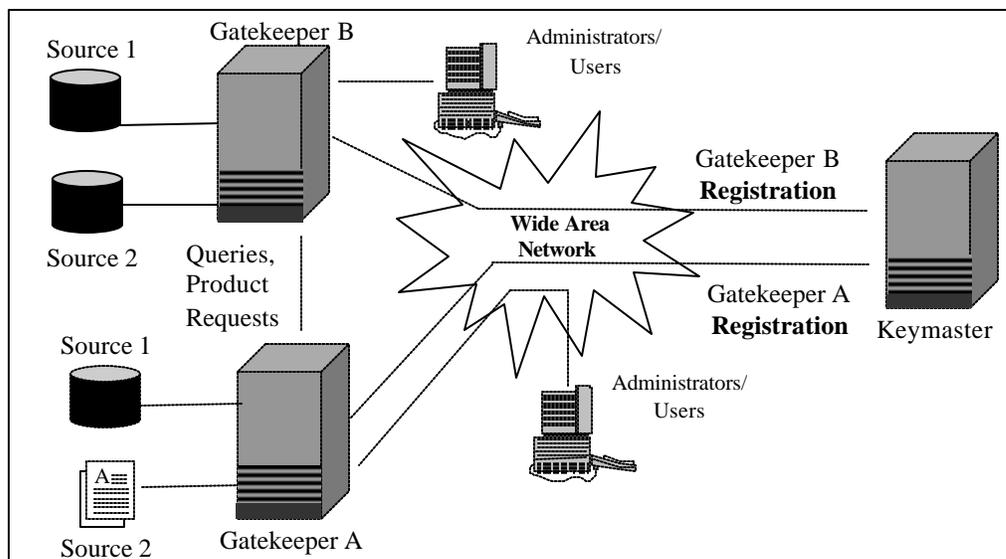


Figure 1.4 Gatekeeper/Keymaster Architecture

Keymaster Security Audits		
User Events:		
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
Register Our Gatekeeper With Keymaster	Set User Discretionary Access Control (DAC)	Removed Discretionary Access Control (DAC)
Added User Privileges	Update Daemon Status	Keymaster Started
ISSO Events:		
Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 1.4 Summary of Security Audits

1.2.3 Trusted Transfer Agent (TTA)

The Gatekeeper and Keymaster described above provide a powerful infrastructure for the interconnection of information sources within a single Community of Interest (COI) and a single security domain. The Trusted Transfer Agent (TTA) brings together this powerful infrastructure and the multiple security level (MSL) capability provided under the Information Support Server Environment (ISSE) Guard. TTA provides any authorized user within the Gatekeeper COI operating at the high-side security level the ability to access, query, and pull information from a low-side COI. Figure 1.5 displays the overall Gatekeeper/TTA Architecture.

1.2.3.1 Overall Architecture of TTA

The TTA High Gatekeeper and TTA Low Gatekeeper configurations include a number of processes that must work continuously and cooperatively in order to ensure proper operation of the TTA system. If a serious error is detected in any TTA process on either the high side or the low side platform action is taken automatically to shutdown either the high side or low side TTA processes, quickly, completely, and correctly. This ensures that no information will inadvertently pass through the TTA because processes are not working correctly, and protects against the UNIX file system directories, used in various locations within the TTA system, from becoming overloaded. Once TTA is started, high side and low side process controller components of TTA continuously monitor the status of all TTA high side and low side processes respectively. If one of those processes exits for any reason, the process control recognizes that fact and signals all other TTA processes to gracefully exit thus bringing down the high side or low side of the TTA completely. When this event occurs, messages are

written to the system log allowing the TTA administrator to determine when and why the event occurred.

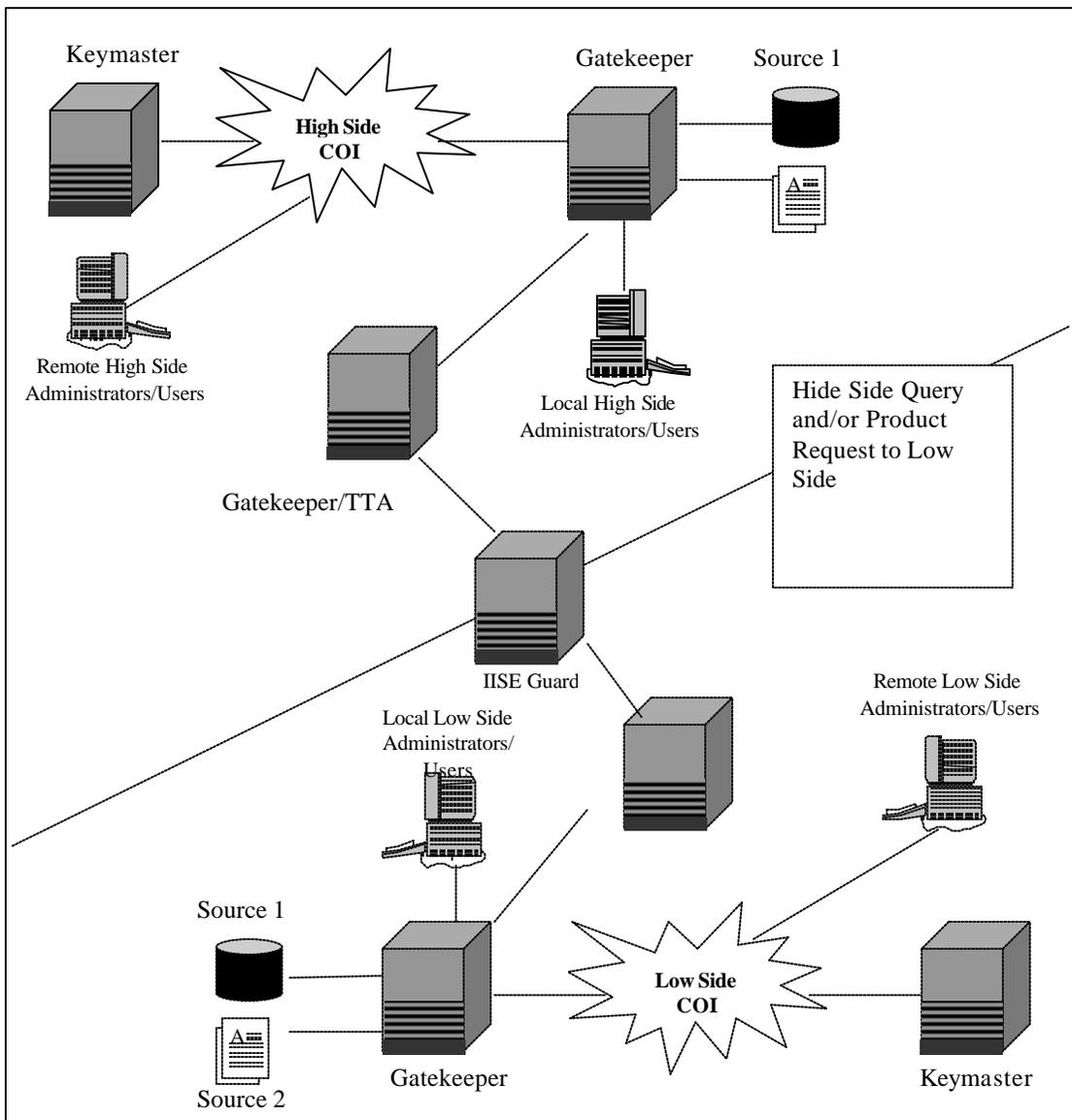


Figure 1.5 Overall TTA/Gatekeeper Architecture

1.2.3.2 MD 5 Integrity Seals

To ensure that information is not added (inadvertently or maliciously) to a TTA message once it enters the TTA processing stream, Message Digest 5 (MD5) integrity sealing is performed. Immediately after receiving a message from either the high side or low side, TTA assigns the Message Digest 5 (MD5) integrity seal, which passes between TTA or through the ISSE Guard. The attached MD5 is the integrity seal in the TTA package generated. Subsequently, whenever that package is recalculated, it is compared with the original integrity seal to verify the seal matches. This indicates that the package has not been modified in any way (either accidentally or maliciously) since it arrived at the TTA

interface. If the MD5 seal does not match at any point in the process, an error message is generated, processing of the message in question is terminated, and a system log is written indicating where the problem was detected within them TTA process flow.

1.2.3.3 Secure Socket Layer (SSL)

To provide additional layers of security, Broadsword v3.0.1 has implemented SSL. Broadsword provides SSL at three different points: (1) between a user's web browser and the Broadsword server, (2) between the Gatekeeper and the Keymaster, and (3) between the local and remote Gatekeepers. Adding SSL at these three points provides greater protection against both external and internal threats.

1.2.3.4 Message level and field level filtering

In order to ensure that high side information is not inadvertently passed through the TTA and ISSE Guard to the low side, extensive security filtering capabilities are included in the TTA Security Filtering Application (SFA) resident on the TTA High Gatekeeper platform. Since security policies change from time to time the security filters applied by the SFA are configurable by the ISSO working in concert with the TTA Administrator to enforce the appropriate security protection mechanisms. Two levels of security filtering capabilities are provided, message level filters and field level filters.

1.2.3.4.1 Message Level Filters

Message Level Filters reuse the software that performs "dirty word" filtering already accredited within ISSE Guard applications approved for the passage of formatted message traffic containing limited free text areas. Messages level filters use a "dirty word" list containing a list of words and/or phrases that are either not passable to the low side (i.e. classified code words, etc.) or strong indicators that the associated information in the message is not passable to the low side (i.e. security labels). By applying the message level filters, it is determined if a message passed through the TTA (and subsequently the ISSE Guard) from high to low contains any "dirty words." If a message is found to contain one or more words/phrases in the dirty word list, the processing of the message is terminated. Following this, an error message describing the filter violation is generated and sent through established Broadsword mechanism back to the originating user, and a error message is generated that is written to the system/Broadsword error log.

1.2.3.4.2 Field Level Filters

Field Level Filters are an additional capability added to TTA and are akin to NITF header filters already accredited within ISSE Guard applications and approved for the passage of the header portion of NITF imagery. Since the messages passing from high to low through the TTA contain formatted field-value pairs, additional filtering can be provided on a field-by-field basis. For each field within each message type, over which field level filter is needed, an entry in a file is generated describing how the information in the field is to be filtered. A variety of filter types have been created which test for a variety of conditions such as Value in Field, Value Not in Field, Value In Range etc.

1.2.3.5 Masking of Sensitive Fields for Information Passed from High to Low

The Broadsword Inter-Gatekeeper messages passed between Gatekeepers of the same security level contain sensitive information describing the high side security environment. Examples include Internet Protocol (IP) addresses, user logins and passwords, platform names, etc. When passed between platforms of different security levels, as is provided by TTA, this information cannot be passed, since it would disclose potentially sensitive information about the high side to the low side domains. For this reason, the TTA plugin and Keymap Receive applications manipulate the message to ensure the proper information, necessary for TTA operation, is inserted, and that no potential sensitive information is disclosed through the ISSE Guard to the low side security domain. The components maintain local aliasing tables that replace potentially sensitive information with masked out values prior to them being passed from high to low, and replace those masked out values with the original value in the response messages when they arrive back to the high side components.

1.2.4 The Broadsword Client

Broadsword 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 or group basis. These roles automatically include the General User role (i.e. 'Searching' role), and can may include one or more of the following functions: searching, Producer, Managed Producer, Catalog Manager, Administrator and/or 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 the 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 1.6 shows the overall User Interface Architecture.

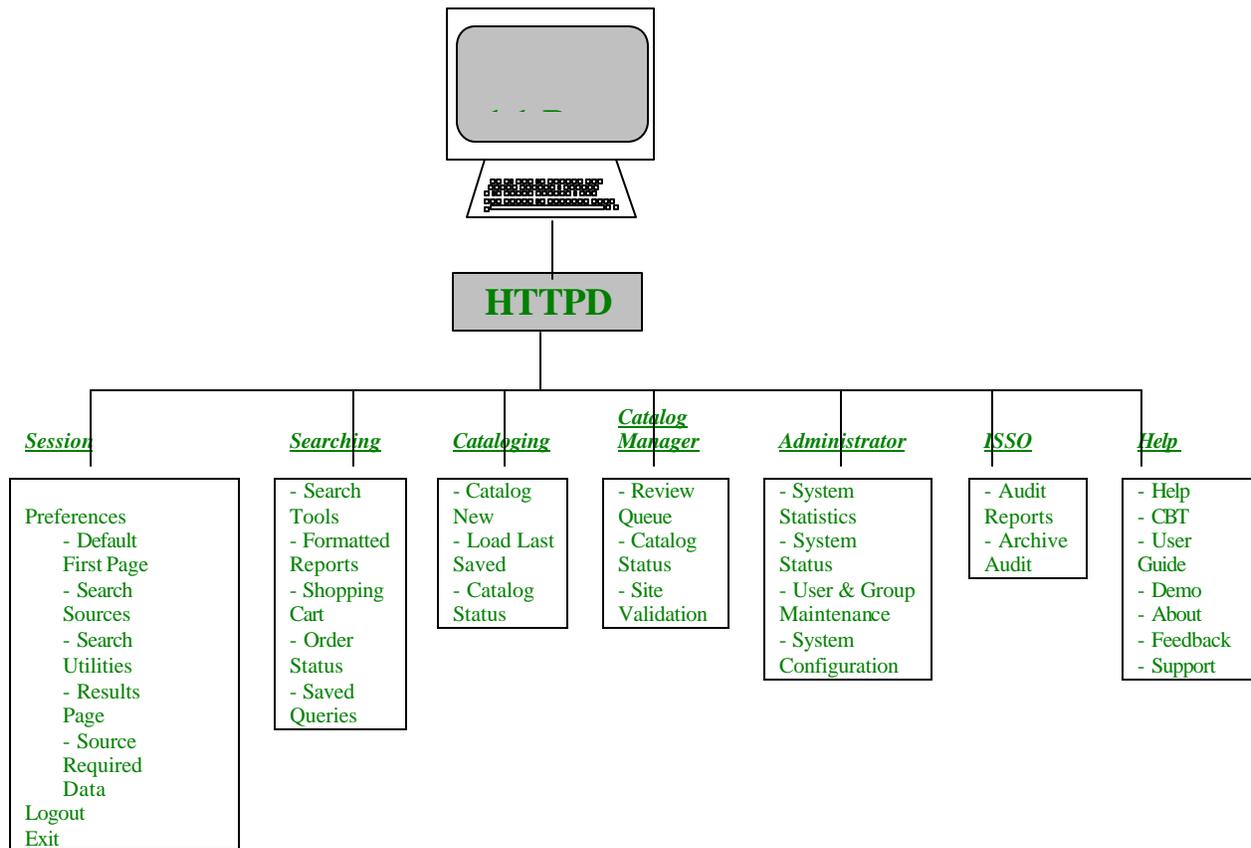


Figure 1.6 User Interface Architecture

1.2.4.1 General

These Session and Help functions are available to all authenticated users.

1.2.4.1.1 The Session Menu

The Session menu allows the user to log off or exit Broadsword safely. Additionally, the Preferences section allows the user to set up their default values and is split into five separate pages: (1) Default First Page; (2) Search Sources; (3) Search Utilities; (4) Results Page and (5) Source Required Data. Users are able to define what their Search Tools page looks like, which data sources to search, and their preferred search mechanism.

1.2.4.1.2 The Help Menu

The Help menu offers much assistance to the user. The Help page offers context-sensitive assistance with Broadsword functionality. The Demo page takes the user through an animated and narrated example of how to use the specific functionality they have loaded. The CBT is a full Computer Based Training capability. The User Guide provides detail on all of Broadsword's General and Catalog functionality. The Feedback page allows the user to provide on-line suggestions and comments about the interface to the local Broadsword administrator. 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.

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 all authenticated users.

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 Session -> Preferences -> Search Utility page Define Search Page preference. This preference selects 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 Tools 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 and/or MTI). 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 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 on the Search Tools Form page. Each source dictates the display and/or retrieval of its products.

Currently Broadsword 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 selecting 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 that the user saved on the Search Tools 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 Update and Batched Query Profiles. Update Profiles 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 these background processing utilities are viewed through the Profile Notification Page. Profile Notification capability not only allows viewing of Update 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 Broadsword system, the ability to turn on debug flags, and maintenance for Broadsword log files.

Under User & Group Maintenance, the system administrator grants additional privileges (i.e., Producer, Managed Producer, Catalog Manager, Administrator, and/or 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 popdowns 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.

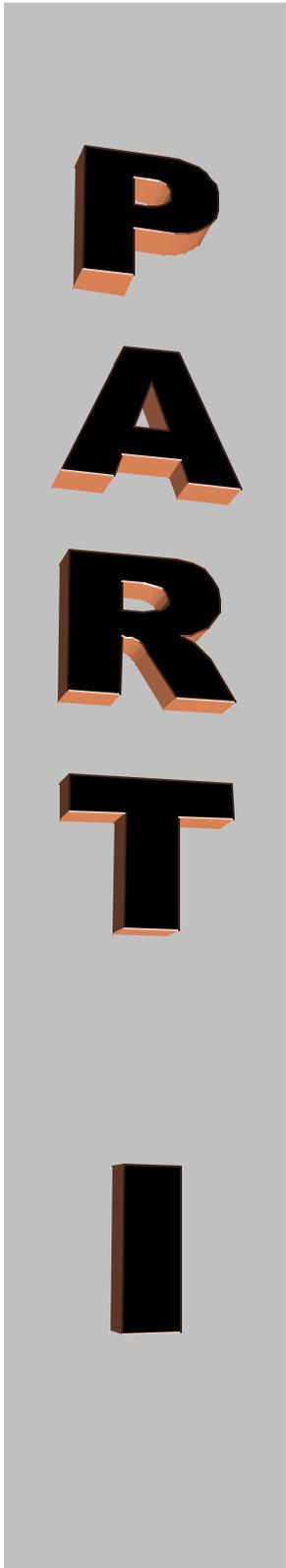
1.2.4.5 Certification Boundary

The Gatekeeper and Keymaster form the basis of the System High infrastructure. Part of the overall Broadsword version 3.1 architecture is the ability for high side users to be able to see low side sources, query the sources and pull products from the low side up to the high. To accomplish this, the TTA provides the gatekeeper with a controlled interface to the ISSE Guard. The ISSE Guard has been accredited at Protection Level 4.

The security boundary mechanism for TTA is the ISSE Guard version 3.2. The ISSE Guard is accredited for operation as this security boundary mechanism and has been successfully installed and configured in over 80 sites worldwide. It is constructed using protected executable code running on a Sun platform with Trusted Solaris 2.5.1. It includes extensive capabilities to ensure the integrity of information passing across security domains, performs verification of sender and destination information, and uses the capabilities provided by Trusted Solaris to maintain separation of the two security domains within a single platform. The ISSE Guard has undergone extensive testing and analysis to ensure malicious users and processes cannot penetrate from the low side into the high side security domain. Associated with each ISSE Guard executable process is a Cyclical Redundancy Check (CRC) value that is stored and re-verified each time the process is started. If the CRC does not match the expected value, the executable is not started and an error message notification is sent to the ISSE Guard Administrator. This CRC provides added protection to ensure that a malicious user cannot replace an ISSE Guard executable with a malicious application of the same name.

The TTA High Gatekeeper and TTA Low Gatekeeper configurations include a number of processes that must work continuously and cooperatively in order to ensure proper operation of the TTA system. If a serious error is detected in any TTA process on either the high side or the low side platform, action is taken automatically to shutdown either the high side or low side TTA processes, quickly, completely, and correctly. This ensures that no information will inadvertently pass through the TTA because processes are not working correctly, and protects against the Unix file system directories, used in various locations within the TTA system, from becoming overloaded. Once TTA is started, high side and low side process controller components of TTA continuously monitor the status of all TTA high side and low side processes respectively. If one of those processes exits for any reason the process control recognizes that fact and signals all other TTA processes to gracefully exit, thus bringing down the high side or low side of the TTA completely. When this event occurs, messages are written to the system log allowing the TTA administrator to determine when and why the event occurred.

This page intentionally left 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
 - Keymaster Configuration
 - Client Configuration
- Confirming Installation Choices
- Installation Progress
- Installation Verification

This page intentionally left blank.

Chapter 2

Getting Started

The purpose of this chapter is to prepare your system for installation/upgrade and to gather all the required information you will need beforehand. At the end of this chapter is a “Site Configuration Worksheet.” You should complete this worksheet 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 system or it can share a system with another Sybase application. Your system must be operating with at least the hardware/software specified in Table 2.1 in order to successfully install and use Broadsword.

Software	Hardware
<ul style="list-style-type: none"> • Sybase SQL OR Sybase Adaptive Server 11.5.1 or 11.9.2 (recommended) • Solaris 2.6 for TTA Gatekeepers • Solaris 2.6 or 7 for Broadsword Gatekeepers and Keymasters • Solaris 7 for Broadsword Gatekeepers that are required to interface to IPL 3.0. • GZIP 1.3 or higher (Required only if loading Netscape on Server) • 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 1.4.2.1 or AFDI 1.1 (not for TTA Gatekeepers) • X-Window Environment • Flash Shockwave Player 5 to use the Computer Based Training. 	<ul style="list-style-type: none"> • CD-ROM Drive • At least 2 processors • 1 GB/2 GB recommended memory (imagery products) • At least 1.5 GB free disk space for Solaris Operating System, Patches and Utilities • At least 5.7 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 GB for Audit Logs

Table 2.1 Server Requirements

Note: Installation of third party COTS and GOTS software is not the responsibility of the Broadsword PMO. However, sample installation instructions are provided in Appendix D for many of these products to assist with their configuration in support of Broadsword. These instructions are intended to supplement, not replace the OEM documentation. In all cases, these instructions are superseded by OEM documentation.

Note: As per instruction of the AFDI Program Office – a CSE-SS client can be administered by an AFDI administrative workstation, but an AFDI client can not be administered by a CSE-SS administrative workstation. If the Gatekeeper will be configured as an AFDI client there must be an AFDI administrative workstation available within that domain.

Note: All operating system patches required by AFCERT or the local DAA authorities should be applied to the applicable operating systems. Broadsword does not require any patches other than those required by AFCERT.

For CSE-SS Option:

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

For AFDI Option:

1. No special AFDI audit flags are required for Broadsword; the AFDI minimum audits will suffice, as Broadsword uses its own auditing scheme.
2. No additional operating system packages and subsets are required for Broadsword, except those required to support AFDI version 1.1.
3. No special steps are required to install Broadsword in an AFDI environment.

2.2 Preparing your System

This section provides a list of tasks to do **before** installing the Broadsword software. For sites with existing Broadsword systems, many of these tasks will already have been completed from the previous install. However, it is still imperative to review these steps and verify that the configuration associated with each task has been accomplished.

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

1 Allocate Broadword database devices

You must allocate disk space for use by the Sybase master device, sysprocs device, temp device, data device, data segment device and transaction log device. In general, try to locate the master and database devices on a different disk drive from the transaction log, temp, and sysprocs devices in order to maximize performance.

You can use raw partitions or UNIX file systems for these Sybase devices; however, Sybase Inc. recommends use of UNIX file systems with Sybase Version 11.9.2 and the Broadword PMO concurs with this recommendation. Initial install or upgrade of the operating system is the ideal time to configure UNIX filesystems for use with Sybase.

In either case, verify that there is enough space available on each partition or filesystem. You will be prompted during the Broadword installation for the location of these free space partitions. Sample partition tables are provided in Appendix D.

- For new systems not co-hosted on another application server, use the format utility appropriate to your system to partition the disk drives. Some of the utilities available include `format`, 'Veritas Volume Manager' or 'SparcStorage Array Volume Manager', if using a Sun Sparc Disk Storage Array. The following sizes are provided as guidelines, but can be made larger (2-GB limit):

▪ master device:	64 MB	
	128 MB	(for Sybase Adaptive Server)
• master mirror device:	64 MB	
	128 MB	(for Sybase Adaptive Server)
• sysprocs device:	64 MB	
	128 MB	(for Sybase Adaptive Server)
• temp device:	256 MB	{Worksheet Field #15}
• database device:	2047 MB	{Worksheet Field #18}
• database segment device:	2047 MB	{Same size as database device}
• transaction log:	512 MB	{Worksheet Field #20}

- For existing systems, disk space for these devices should already be allocated. However, you should still verify that these devices have been sized appropriately by examining the `/opt/keymaster3.0/etc/bswd_settings` file to determine the devices currently in use. This file contains configuration information from the previous installation of Broadword. Using this information, you can then verify that these devices are sized appropriately.
- For new systems that are co-hosted with another application and share a dataserver, it is not necessary to allocate space for a master device, sysprocs device, or temp device. These devices already exist as a result of the creation of the existing dataserver.
- For new systems that are co-hosted with another application and do NOT share a dataserver, it is necessary to allocate space for a master device, sysprocs device, or temp device.

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 Field #8) with your existing dataserver name. This will allow Broadsword 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 doubt, contact your local Sybase Administrator or Sybase, Inc. at 1-800-8-SYBASE.

Note: If you decide to share with an existing dataserver, 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 dataserver is case sensitive. To verify this, execute the "sp_helpsort" system stored procedure inside the dataserver in question to confirm the sort order is set as described above.

After partitioning has been completed, verify that each UNIX filesystem used by Sybase is owned by the appropriate Sybase user (e.g. *sybase* for a dedicated Keymaster) with group set to group *sys*. Also, verify that each UNIX filesystem used by Sybase has read/write permission for Sybase user (e.g. *sybase*) and read permission for group *sys*. For Keymasters that are co-hosted with an IPL and share a dataserver the UNIX filesystem used by Sybase should be owned by user *sybip1* with group set to group *sys*.

Note: For existing Broadsword Keymasters, the user *sybase* should already exist from the previous install. For new installs, the Sybase user should be created while installing Sybase Adaptive Server (see Appendix D).

The commands below are an example of how to change permissions and ownership of those UNIX filesystems that will be used exclusively by Sybase. This example assumes you have used the sample disk partitions provided in Appendix D. This example may not be applicable if you have used an alternate partition/filesystem scheme.

```
chown -R sybase:sys /syb_devices_0
chown -R sybase:sys /syb_devices_1
chmod -R 750 /syb_devices_0
chmod -R 750 /syb_devices_1
```

If you are using a four hard drive configuration based on the suggested partitioning tables listed in Appendix D you will also need to use the following commands:

```
chown -R sybase:sys /syb_devices_2
chown -R sybase:sys /syb_devices_3
chmod -R 750 /syb_devices_2
chmod -R 750 /syb_devices_3
```

2 Verify directories and determine available disk space

The standard location for Broadsword is in either the `/opt/keymaster3.0` or the `/h/keymaster3.0` directory. The location will be determined by the site based on their security infrastructure (CSE-SS or AFDI).

There should be at least 2 GB available on this filesystem (1 GB for Software, 1 GB for Map Data). The distribution media accounts for only a fraction of the 1 GB allocated for software; the rest is to allow for product and thumbnail caching.

Enter the following to determine if the applicable filesystem has adequate free space:

```
df -k /'applicable_filesystem'
```

Where `'applicable_filesystem'` is either `/opt` or `/h`

Then create the Broadsword install directory:

```
mkdir /'applicable_filesystem'/keymaster3.0
```

Where `'applicable_filesystem'` is either `/opt` or `/h`.

Note: The sample disk partitions provided in Appendix D swap the location (between drives 0 and 1) of the `/h` and `/opt` partition based on whether the Broadsword Keymaster will be installed with CSE-SS or AFDI. This is done to spread disk activity across as many drives as possible to improve system performance.

If the filesystem does not contain at least 2 GB of free space, then select a filesystem that is large enough and create a symbolic link. The following example assumes the `/opt` filesystem is not large enough and will use the `/big_opt` filesystem instead.

```
mkdir /big_opt/keymaster3.0
chmod 755 /big_opt/keymaster3.0
ln -s /big_opt/keymaster3.0 /opt/keymaster3.0
```

For AFDI only: If Broadsword is installed on a host that is running AFDI you must also create the following symbolic link:

```
mkdir /h/keymaster3.0/
chmod 755 /h/keymaster3.0
ln -s /h/keymaster3.0 /opt/keymaster3.0
```

3 Verify *sendmail* is running on your system

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

```
ps -ef|grep sendmail|grep -v grep
```

You will receive output from the system if the **sendmail** daemon is already running. Otherwise, start the **sendmail** daemon with the following command:

```
/etc/init.d/sendmail start
```

Be sure to check with the site ISSO for site security policy regarding sendmail.

4 Verify system kernel configuration

Several parameters must be configured into the kernel for the Sybase dataserer. Examine the **/etc/system** file and verify the following lines are present at the end of the file. If these lines are not already present then append them to the file.

```
*For Broadsword:
set shmsys:shminfo_shmmax=1310720000
set shmsys:shminfo_shmseg=32
set maxusers=512
```

Issue the following command after making the appropriate modifications to the **/etc/system** file:

```
touch /reconfigure
```

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

The system must now be rebooted for the new values to take effect:

```
init 6
```

5 Identify/create Keymaster group

Broadsword requires the designation of a Keymaster group (typically named *bswd* on a dedicated system) and all users connecting to the Keymaster interface must belong to this group. It is not necessary for the Keymaster group to be the primary group for Keymaster users. Keymaster users may also belong to other groups.

Check both the local and NIS/NIS+ (if applicable) group files to determine whether this group already exists.

```
cat /etc/group|grep bswd
ypcat group|grep bswd
niscat group.org_dir|grep bswd
```

If this group does not exist, you can either create it or designate an existing UNIX group on the system as the Keymaster group.

- If creating a new network wide group, coordinate the group name and group id (gid) with the site NIS administrator to avoid conflict.
- If creating this group locally on the Broadsword system, then use the appropriate group maintenance tool for the environment in which Broadsword is installed (i.e. CSE-SS Group Maintenance Tool, AFDI Group Maintenance Tool or Sun admintool).
- If designating an existing group, be aware that all users that are currently members of that group will also have access to Broadsword Keymaster. For example, the *ipa* group typically exists on an IPL server. If Broadsword is co-hosted on the IPL server and the *ipa* group is designated as the Broadsword group, then users that are members of the *ipa* group will be allowed to connect to Broadsword Keymaster.

Although Broadsword does not require a particular group id (gid), if available, the standard gid used by the Broadsword PMO is 600. Be sure to write the group chosen in Field #32 in the Site Configuration Worksheet

6 Identify/create Keymaster system administration user (*bswduser*)

Broadsword requires the creation/existence of a system administration account, named *bswduser*, with its primary group set to the Keymaster group (e.g. *bswd*). Check both the local and NIS (if applicable) passwd files to determine whether this user account already exists and has primary group set to the Broadsword group (e.g. *bswd*).

```
cat /etc/passwd|grep bswduser
ypcat passwd|grep bswduser
niscat passwd.org_dir|grep bswduser
```

If *bswduser* account does not exist, then it must be created with primary group set to the Broadsword group.

- If creating as a network account, coordinate the user name and user id (uid) with the site NIS administrator to avoid conflict.
- If creating this account locally on the Broadsword system, then use the appropriate user maintenance tool for the environment in which Broadsword is installed (i.e. CSE-SS User Maintenance Tool, AFDI User Maintenance Tool or Sun admintool).

The following parameters are provided as samples. Actual values should be consistent with site configuration and security policy.

- User Name: **bswduser**
- User ID: **1000 (or as designated by the site system administrator)**
- Primary Group/Group ID: **600 (must be gid of Keymaster group)**
- Comment/Full Name: **Broadsword Administrator Account.**
- Login Shell: **csch**
- Password: **Normal Password (Used with Admintool only)**
(Do not forget to assign a password consistent with site policy)
- Account Security / Password Aging Options: (Set options as per local site policy)
 - Min Change/Disallow password change for: **0**
 - Max Change/Force password change every: **90**
 - Warning/Warn before forced change for: **14**
- Create Directory: Select check mark **(Used with Admintool only)**
- Home Directory/LoginDirectory/Path:
 - /export/home/`hostname`/bswduser**
(Not for use with AFDI)
 - /h/USERS/`hostname`/bswduser**
(Used with AFDI only)

Note: Use the actual hostname of the server and be sure not to include the tick marks. If installing on system named *bswdserv* running AFDI the home directory path would be */h/USERS/bswdserv/bswduser*.

7 Assign Passwords and Sessions

Assign passwords to the *bswduser* and *cdimuser* accounts using the appropriate password tool for the environment in which Broadsword is installed (i.e. CSE-SS Assign Password Tool, AFDI Assign Password Tool or Sun Solaris `passwd` command).

If you used either the CSE-SS or AFDI User Maintenance Tool to create the *bswduser* and *cdimuser* accounts you must also assign a session to these accounts. To assign a session, use the CSE-SS or AFDI User Session Maintenance Tool and assign USER CDE Session from the Available Session list.

8 Allow X Server connections

Broadsword requires X server access to be enabled at all times to support Gazeteer functions. There are two methods you can use to open a new **xterm/terminal** window on the **console**.

- For a Keymaster without CSE-SS/AFDI loaded. Right click anywhere on the desktop. This will bring up the **Desktop Menu**. Go down to **Tools** and select **Terminal**.
- For a Keymaster configured with CSE-SS/AFDI. Right click anywhere on the desktop. This will bring up the **Workstation Main Menu**. Click on **ISSO Access** to open the **ISSO palette**. In the ISSO palette click on the **Shell** icon. In the new **xterm/terminal** window issue the following command:

```
/usr/openwin/bin/xhost `hostname`
```

Where ``hostname`` is the actual hostname of the system where you are installing from.

X server access must be enabled every time the Broadsword server is rebooted to maintain Gazeteer functionality.

9 Synchronize Clock with Time Server

Time synchronization among all Broadsword gatekeeper servers is crucial to generating audits that have correct timestamps. Therefore, if you are concerned about audits, you must install and configure the time synchronization software on your system.

Begin by determining an appropriate time server for the WAN where your Gatekeeper is located.

For Internet:

Refer to <http://tycho.usno.navy.mil/frtime.html>. Select the link entitled “Setting your computer to USNO time”. Then pick the “Network Time Protocol (NTP)” link to find an appropriate time server.

For SIPRNET:

Refer to <http://www.ismc.sgov.gov>. On the main page, there is a Support section. Under this section, there is a link to “Time Servers/Time Software.” Follow this link, then follow the link on the next page to find the location of the time servers on SIPRNET.

For JWICS:

Refer to <http://www.ic.gov>. On the main page, there is a Support section. Under this section, there is a link to “Time Servers/Time Software.” Follow this link, then follow the link on the next page to find the location of the time servers on JWICS.

Now that you have picked an appropriate time server, you can determine how to configure the software:

For CSE-SS Option:

The system should be configured appropriately at CSE-SS installation time. The xntpd software is included with CSE-SS and is configured by the CSE-SS installation program. Refer to the Installation and Configuration Guide for the CSE-SS software to configure the time synchronization software appropriately. This document is available on JWICS at <http://web1.rome.ic.gov/cse> and on SIPRNET at <http://www2.rl.af.smil.mil/cse>. It is also available on the Internet if you have a Cmdb account. On Internet, please refer to <http://extranet.if.af.mil/cse-ss/download.html>. Once you have obtained this document, please refer to the section regarding CSE-SS Setup, specifically the “Network Services” section contained therein.

For AFDI Option:

The system should be configured appropriately at AFDI installation time. The xntpd software is included with AFDI and is configured by the AFDI installation program. Refer to the Installation and Configuration Guide for the AFDI software segment to configure the time synchronization software appropriately. Reference to this document is available at <http://extranet.if.af.mil/infrastructure>. Once you have obtained this document, please refer to the section regarding AFDI Segment Setup, specifically the “Network Services” section contained therein.

For non-DODIIS sites that do not require AFDI or CSE:

With Solaris 2.6 and higher, xntpd is included and must simply be configured. Depending on the WAN where your system is located, refer to the following for installation instructions and software if necessary. The xntpd system manual page is also useful:

To the system manual page for xntpd
`% man xntpd`

For Internet:

Refer to <http://tycho.usno.navy.mil/frtime.html>, select the link for “Setting your computer to USNO time”, then pick the “Time Synchronization Software” link to find the appropriate xntpd time synchronization software and installation instructions.

For SIPRNET:

Refer to <http://www.ismc.sgov.gov>. On the main page, there is a Support section. Under this section, there is a link to “Time Servers/Time Software.” Follow this link, then follow the link on the next page to find the appropriate xntpd time synchronization software and installation instructions.

For JWICS:

Refer to <http://www.ic.gov>. On the main page, there is a Support section. Under this section, there is a link to “Time Servers/Time Software.” Follow this link, then follow the link on the next page to find the appropriate xntpd time synchronization software and installation instructions.

10 Complete the Site Configuration Worksheet

After successfully completing the above steps, fill out the **ENTIRE** worksheet in the next section, 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 within Table 2.2 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 Broadsword distribution CD-ROM.
2	CD Serial Number		Serial number as shown on the Broadsword distribution CD-ROM.
3	Import Selection		Answer “Yes” to import various items from a previous Broadsword version (Default: No).
4	Broadsword Previous Version Path		Path to previous version of Broadsword. 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 Broadsword (Default: sybase).
7	Sybase Home Directory Path		Home directory path of Sybase SQL Server or Sybase Adaptive server.
8	Sybase Dataserver Name		The dataserver name to create or share for Broadsword Sybase server (Default: BSWD_<hostname>_KM_SVR).

Field Number	Field Name	Your Answer	Description
9	Sybase Dataserver Port Number		UNIX port to be used by the Broadsword Sybase server. Asked only if creating a new dataserver (Default: 2703).
10	Sybase Dataserver Master Device Path		System location to place Broadsword dataserver master device. Can either be a raw device (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /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 master device. Can either be a raw device (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /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. systemprocs.dev) at the end of the path. The filename will be added automatically.
12	Sybase Backup Server Create?		Asked only if creating a new dataserver. If a Sybase Backup Server already exists on this system, you may click No.
13	Sybase Backup Server Port #		UNIX port to be used by the Sybase Backup Server. Asked only if creating a new dataserver and creating a Sybase Backup Server (Default: 2753).
14	Broadsword TempDevice Path		System location to place Broadsword TempDevice. Can either be a raw device (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /opt/bswd_syb_devices). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. tempdb.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 DatabaseDevice. Can either be a raw device (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /opt/bswd_syb_devices). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. Bswddata.dev) at the end of the path. The filename will be added automatically.

Field Number	Field Name	Your Answer	Description
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 (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /opt/bswd_syb_devices). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. Bswdlog.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	Keymaster Segment Device Path.		System location to place Keymaster Segment device path. Can either be a raw device (e.g. /dev/rdisk/c0t1d0s2) or a standard UNIX file path (e.g. /opt/bswd_syb_devices). Asked only if creating a new dataserver. Note: Do not include the device filename (e.g. Bswdseg.dev) at the end of the path. The filename will be added automatically.
22	Sybase Database Account Password to Set (user bswd3kmuser)	(don't write here)	Sybase Password to use for the new audit database (user bswd3kmuser). Must be at least 6 characters in length and cannot begin with a special character such as \$.
23	bswduser Account Password	(don't write here)	UNIX password for 'bswduser' account created in Chapter 2.
24	cdimuser Account Password	(don't write here)	UNIX password for 'cdimuser' account created in Chapter 2.
25	Existing IPA/IPL on this machine?		Click "Yes" if there is a co-located IPA or IPL 1.0 on THIS server.
26	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).
27	Installation Type		Type of install (Choices: Standard Broadsword, TTA Low, or TTA High).
28	Implement Interface using SSL?		Whether to use Secure Socket Layer (SSL) encryption protocol between web daemon (HTTPD) and web browser (Default: Yes).
29	Protected HTTP port #		UNIX port to be used by the Protected HTTP daemon (Default: 80).
30	Protected HTTP port # (SSL)		UNIX SSL port to be used by the Protected HTTP daemon. Asked only if SSL is used (Default: 443).
31	Network host machine is on		Network type host machine is connected to (Choices: SIPRNET, JWICS, or Internet) (Default: SIPRNET).
32	Additional network classification label (optional)		Any additional caveats or compartments that should be added to the security banner (i.e. SI/TK). Default: Blank
33	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

Field Number	Field Name	Your Answer	Description
			is unknown, contact the Centralized Help Desk at (315) 330-4347.
34	Group Name		UNIX group to use for Broadsword.
35	System Admin Name		System Administrator name (MANDATORY).
36	System Admin Branch		System Administrator branch (MANDATORY).
37	System Admin Organization		System Administrator organization (MANDATORY).
38	System Admin Organization Unit		System Administrator organization unit (MANDATORY).
39	System Admin Address1		System Administrator address (MANDATORY).
40	System Admin Address2		System Administrator address (MANDATORY).
41	System Admin Phone		System Administrator UNCLASSIFIED phone number (MANDATORY).
42	System Admin FAX		System Administrator FAX (MANDATORY).
43	System Admin E-mail		System Administrator E-mail (MANDATORY).
44	System Admin City		System Administrator City (MANDATORY).
45	System Admin State/Locality		System Administrator State/Locality (MANDATORY).
46	System Admin Country Code		System Administrator Country Code (MANDATORY).
47	ISSO Name		ISSO name.
48	ISSO Branch		ISSO branch.
49	ISSO Organization		ISSO organization.
50	ISSO Address1		ISSO address.
51	ISSO Address2		ISSO address.
52	ISSO Phone		ISSO UNCLASSIFIED phone number.
53	ISSO Fax		ISSO fax number.
54	ISSO Email		ISSO email address.
55	Intelink Site Info Manager Name		Intelink Site Information Manager name.
56	Intelink Site Info Manager Branch		Intelink Site Information Manager branch.
57	Intelink Site Info Manager Organization		Intelink Site Information Manager organization.
58	Intelink Site Info Manager Address1		Intelink Site Information Manager address.
59	Intelink Site Info Manager Address2		Intelink Site Information Manager address.

Field Number	Field Name	Your Answer	Description
60	Intelink Site Info Manager Phone		Intelink Site Information Manager UNCLASSIFIED phone number.
61	Intelink Site Info Manager Fax		Intelink Site Information Manager fax number.
62	Intelink Site Info Manager Email		Intelink Site Information Manager email address.
63	Keymaster POC & contact Phone Number		Information obtained from Section 4.4 and/or Section 8.1 of this document

Table 2.2 Site Configuration Worksheet

This page intentionally left blank.

Chapter 3

Installation

The purpose of this chapter is to provide detailed procedures to install the Keymaster software. Do not proceed unless you have completed Chapter 2 first. This chapter covers a full install for a new Keymaster and a full install for co-hosting on another application server. 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

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

Note: Upgrades cannot be performed between major releases (i.e. 3.0-->3.0.1). The full installation option must be selected even for an existing Broadsword Keymaster.

3.1 Loading the Software and Starting the Setup Script

- 1 Start a terminal window (xterm shell) and enable X server access from the command line.

```
/usr/openwin/bin/xterm
/usr/openwin/bin/xhost `hostname`
```

Where ``hostname`` is the actual hostname of the system where you are installing from.

Alternatively, a Terminal window may be launched from the desktop. You may want to launch additional windows in order to perform data gathering activities in parallel with the install.

- 2 Insert the installation CD into the CD-ROM drive.

```
cd /cdrom/cdrom0
```

- 3 Execute the setup script.

```
./setup.sh
```

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

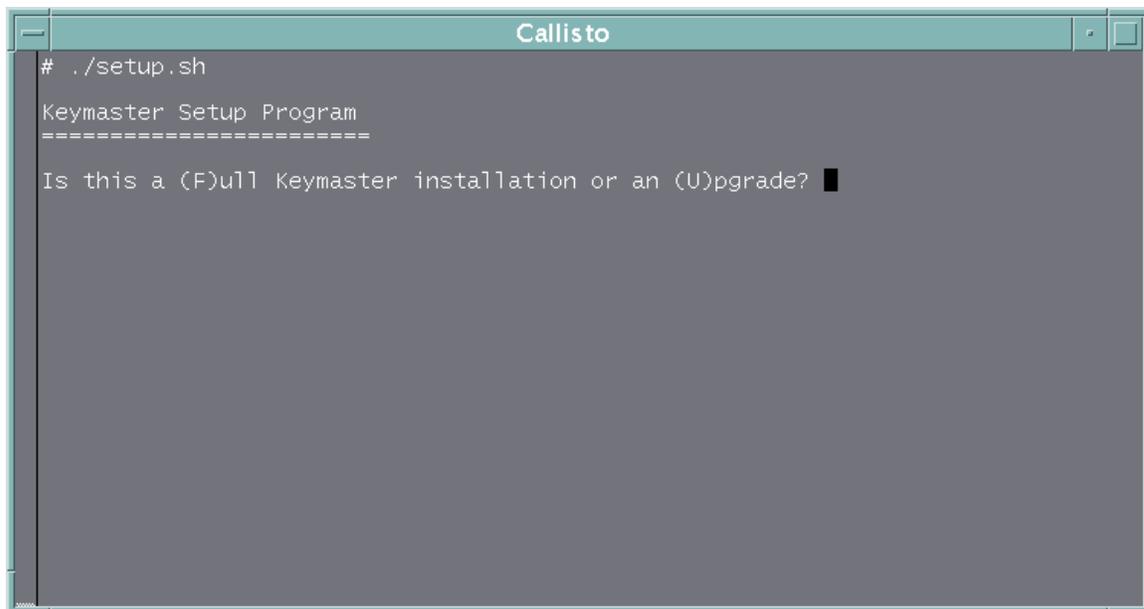


Figure 3.1 - Setup Script (Installation Type)

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

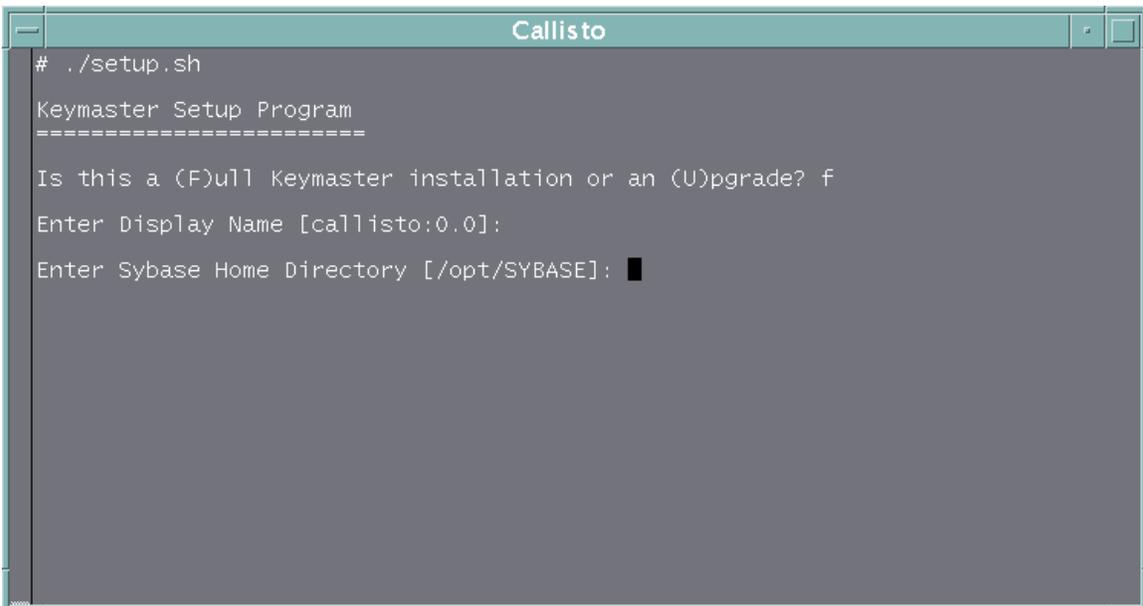
Select the “Full” option to install Broadsword 3.0.1. In the case of a full installation, the user will be prompted for the X display name on which to launch the installer interface. The X display name will default to the local hostname (e.g. bswdserv:0.0). If performing the installation locally from the Broadsword server then accept the default X display name. For remote installations, be sure to specify the hostname of the remote workstation where the installation is being performed. Figure 3.2 shows this screen.



```
Callisto
# ./setup.sh
Keymaster Setup Program
=====
Is this a (F)ull Keymaster installation or an (U)pgrade? f
Enter Display Name [callisto:0.0]: █
```

Figure 3.2 - Setup Script (X display Setup)

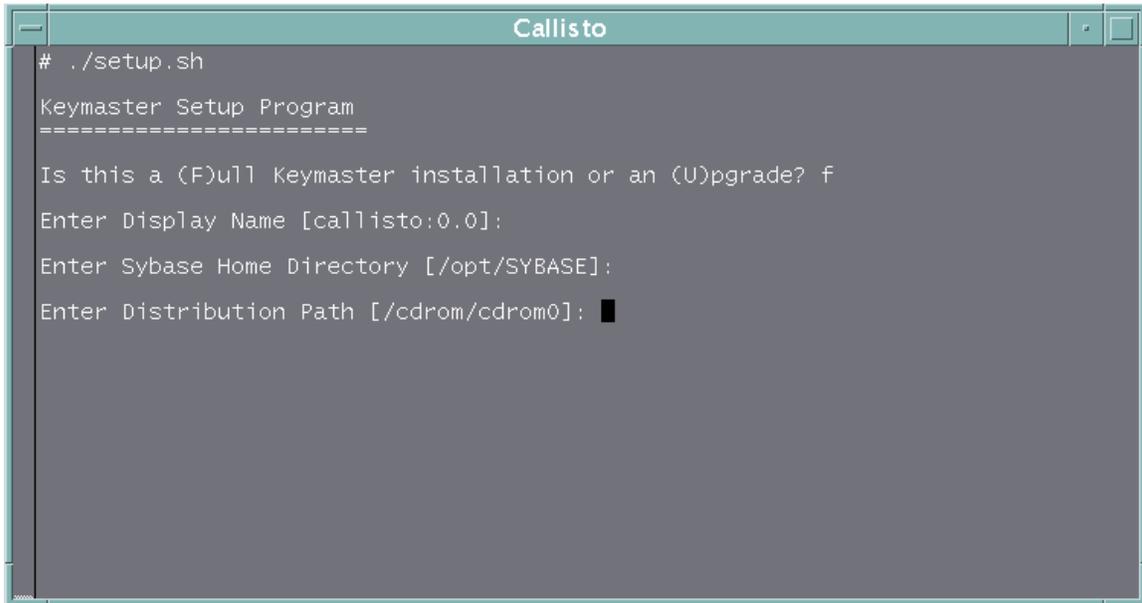
Next, the user is prompted to specify the directory on the server where the Sybase product is located (refer to Worksheet item #7 in the previous chapter). Figure 3.3 shows this screen.



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

Figure 3.3 – Setup Script (Sybase directory)

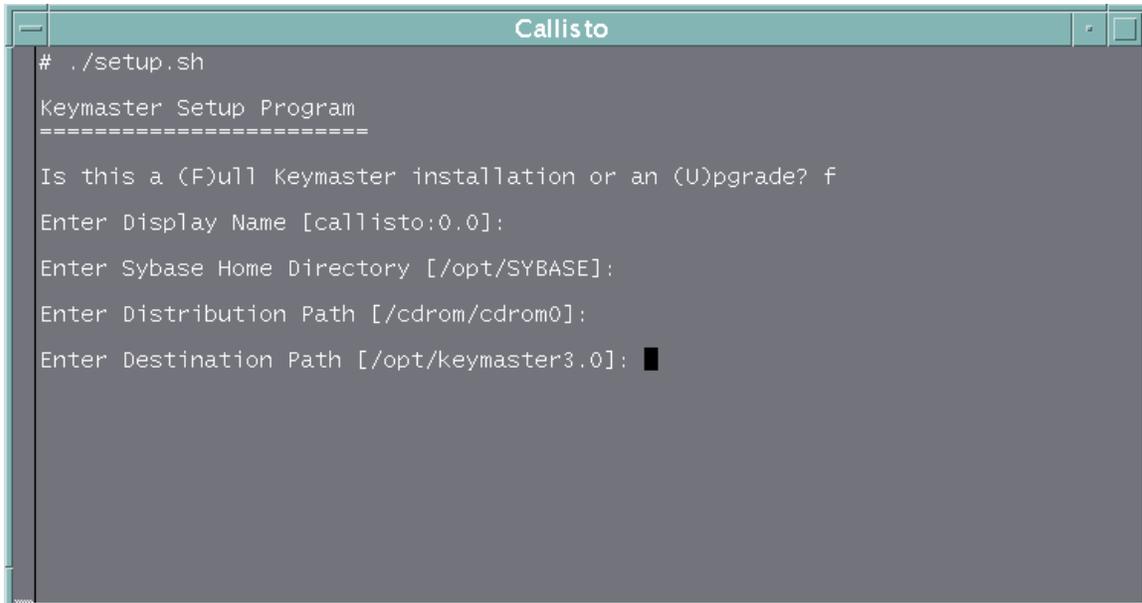
Next, the user is prompted to specify the directory where the Broadsword distribution tar files are stored. In general, this will be the distribution CD-ROM. Figure 3.4 shows this screen.



```
Callisto
# ./setup.sh
Keymaster Setup Program
=====
Is this a (F)ull Keymaster installation or an (U)pgrade? f
Enter Display Name [callisto: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 to specify the directory where the Broadsword software should be installed. Figure 3.5 shows this screen.



```
Callisto
# ./setup.sh
Keymaster Setup Program
=====
Is this a (F)ull Keymaster installation or an (U)pgrade? f
Enter Display Name [callisto:0.0]:
Enter Sybase Home Directory [/opt/SYBASE]:
Enter Distribution Path [/cdrom/cdrom0]:
Enter Destination Path [/opt/keymaster3.0]: █
```

Figure 3.5 – Setup Script (Destination Path)

Finally, the user will be asked to confirm extraction of the Broadsword software. This should always be answered ‘Y’, unless the software has already been extracted fully. The setup script will determine whether the destination path already exists and request confirmation from the user to create the directory if it does not exist. Figure 3.6 shows this screen.

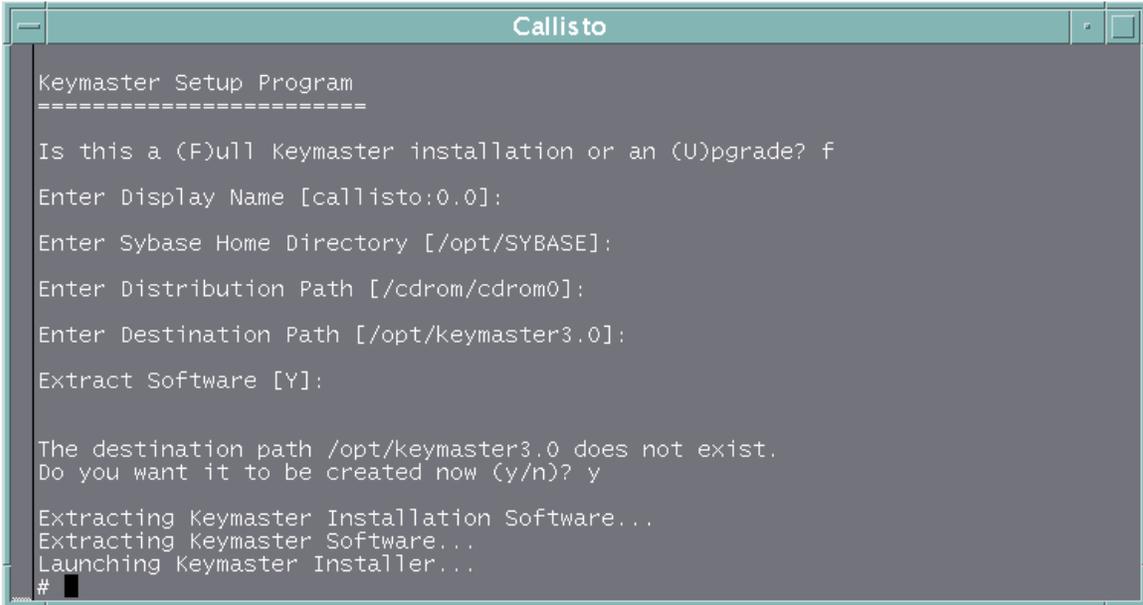


Figure 3.6 – Setup Script Extraction

The setup script will now launch either the Installation or Upgrade script, whichever is appropriate. The remainder of this chapter explains the details of the Installation process.

3.2 Providing Installation Choices

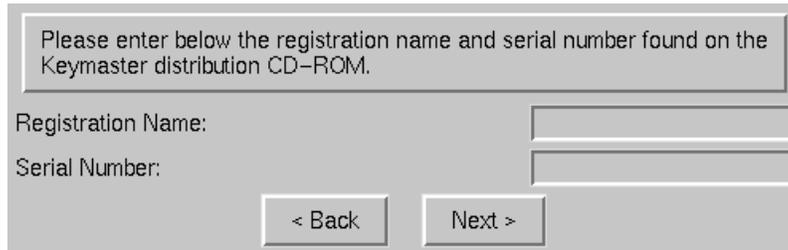
After the setup script has successfully extracted the distribution media, it will launch the graphical portion of the install process. This portion will take the installer step by step through the remainder of the installation process. Figure 3.7 shows the initial screen.



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 was noted in Worksheet Fields #1 and #2 in the previous chapter. A valid combination must be entered or the installation will not continue. After the installation is completed, this information is placed on the Broadsword "About" page for future reference. Figure 3.8 shows this screen



Please enter below the registration name and serial number found on the Keymaster distribution CD-ROM.

Registration Name:

Serial Number:

< Back Next >

Figure 3.8 - Registration Screen

Note: The Broadsword installation interface verifies the data entered on each screen before allowing the installer to proceed to the next screen. Tables are provided (where appropriate) for each screen showing the fields validated on that screen and legal values associated with those fields.

3.2.2 Determining the Import Preference

Note: This option is currently not applicable to a Keymaster installation.
Proceed to the next section

After clicking the “Next” button the installer is asked whether they would like to import various items from a previous version of Broadsword. Figure 3.9 shows this screen. Sites with existing Broadsword systems that wish to import information from the current version should select the “Yes” option. If "No" is selected the import path will be ignored.

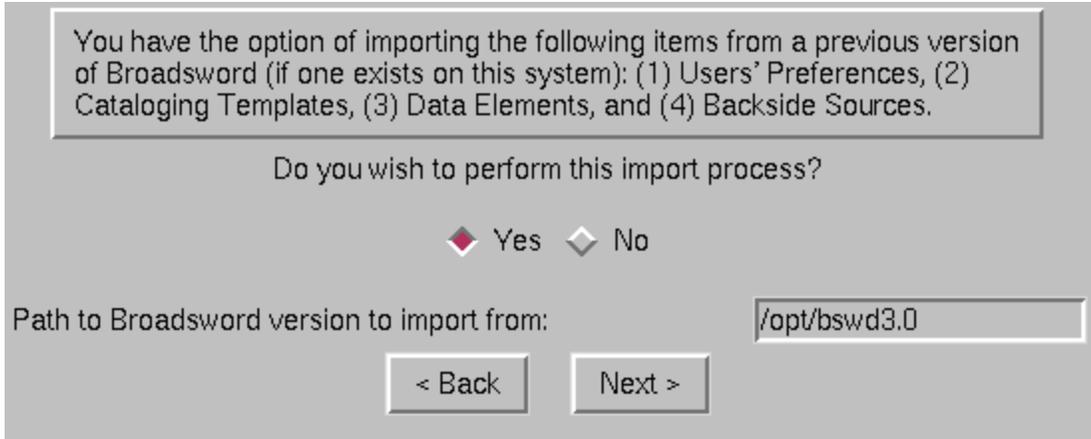


Figure 3.9 - Import Screen

Fields in this screen are validated according to the values specified in Table 3.1.

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

Table 3.1 - Fields Validated

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

```
# cd /etc/rc3.d
# mv SS99zstart_bswd3 old.SS99zstart_bswd3
```

3.2.2.1 Dataserver/Database Configuration

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

Note: The installation script doe NOT check for valid Sybase license(s). Site personnel must confirm the existence of valid Sybase licenses. If the site has only a single server license, the only option available to the site is to install the Database under the existing dataserver. The disadvantage of using a shared dataserver is that if it unavailable for any reason, all the Databases running under the dataserver will be unavailable. However, when sharing an existing dataserver for more than one database, less system resources are used.

Note: During this installation, there are several points at which device names and sizes are requested (i.e. Temp Device, Data Device, 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 GB, 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 GB. For example, if the partition in question had 4,299,162 Kbytes (about 4.1 GB) free, then filling up an additional 104,900 Kbytes (just over .1 GB) will fix the problem.

3.2.2.2 Creating a New Dataserver

The default option is to create a new Dataserver. Figure 3.10 provides a sample of this screen. The “Create new” option should be selected unless the Keymaster will co-hosted with another application server and will share an existing Dataserver. Skip to Section 3.2.3.2 if the “Share existing” option is selected.

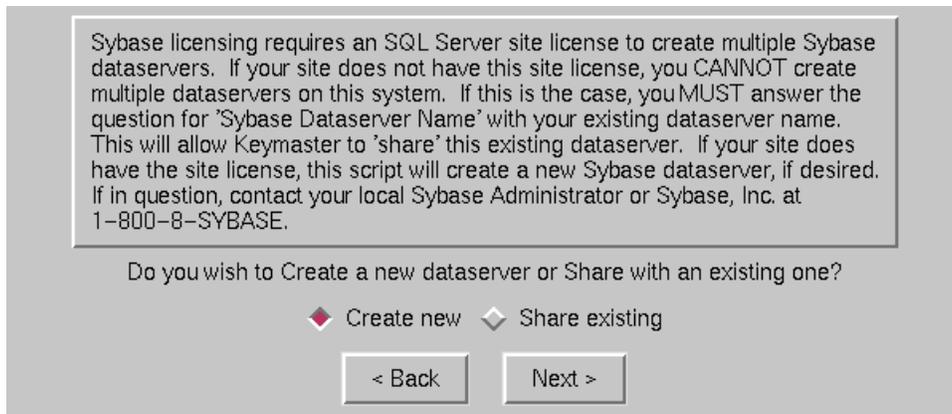


Figure 3.10 - Dataserver Creation Method Screen

If the “Create new” option was chosen (as shown in Figure 3.10), the installation script will next ask for information required to configure the Dataserver (as shown in Figure 3.11).

Figure 3.11 - Initial Dataserver Configuration Screen

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

Several fields will already be populated with default values. The installer must verify these values along with entering the additional requested information. Values for these fields should already have been identified in the Worksheet (Fields #10 and #11). The Master Device path and Sysprocs Device path identify where Sybase will physically write its data. A full path to a UNIX filesystem is recommended although the device path can also be the full path to a raw partition. Figure 3.12 shows a sample screen with the device paths filled in using UNIX filesystems 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 Dataserver Configuration Screen

Fields in this screen are validated according to the values specified in Table 3.2.

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.
Sysprocs Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device.
Backup Server Port #	Port number is not already in use.

Table 3.2 - Fields Validated for Broadword Dataserver Configuration Screen

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. Figure 3.14 provides an example of this screen.

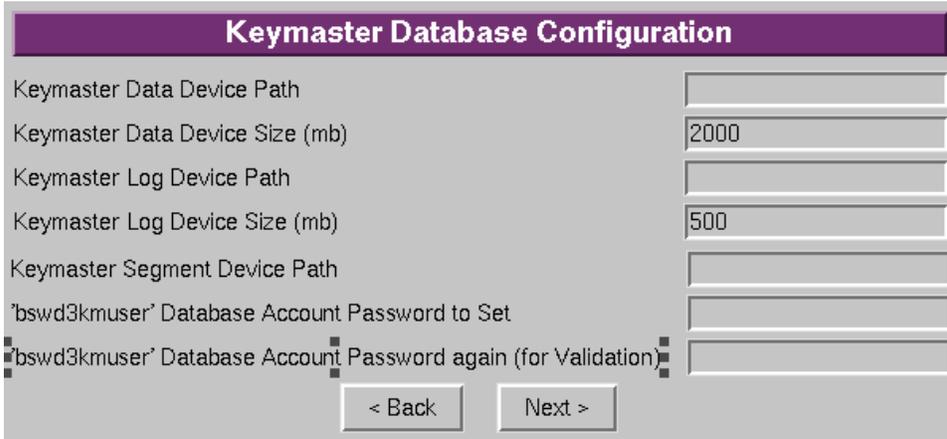


Figure 3.14 - Sample Database Configuration Screen

Note: 'bswd3kmuser' is a database account, not a UNIX account. Password must be at least 6 characters in length and cannot begin with a special character such as \$.

Fields in this screen are validated according to the values specified in Table 3.3.

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.
Keymaster Segment Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device. Must be at least as big as the Data Device Path.
Sybase Database Account Password to set (user bswd3kmuser)	Installer enters it twice AND length is at least 6 characters.

Table 3.3 Fields Validated for Database Configuration Screen

At this point all the necessary information to configure the Dataserver and Database is complete. The installation process will now request information needed to configure the Keymaster.

Skip to section 3.2.3 to proceed with the installation.

3.2.2.3 Sharing an Existing Dataserver

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 those specified for the original dataserver.

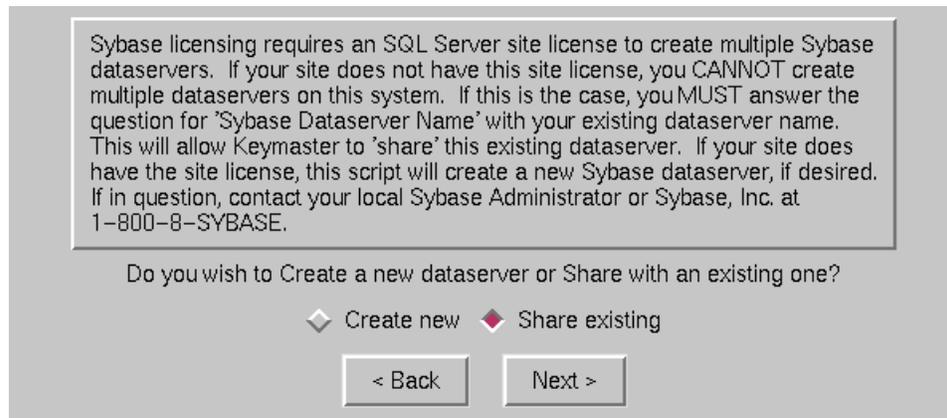


Figure 3.15 - Sharing an Existing Dataserver Screen

Several fields will already be populated with default values. 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 shows the initial, default screen. Figure 3.17 shows a sample screen with the device paths filled in.

Keymaster Database Configuration	
SYBASE Username	<input type="text" value="sybase"/>
SYBASE Home Directory Path	<input type="text" value="/opt/SYBASE"/>
SYBASE Dataserver Name to SHARE for Keymaster	<input type="text" value="BSWD_SATURN_KM_SV"/>
SYBASE Administrator Password for dataserver	<input type="text"/>
Administrator Password again (for Validation)	<input type="text"/>
Keymaster Data Device Path	<input type="text"/>
Keymaster Data Device Size (mb)	<input type="text" value="2000"/>
Keymaster Log Device Path	<input type="text"/>
Keymaster Log Device Size (mb)	<input type="text" value="500"/>
Keymaster Segment Device Path	<input type="text"/>
'bswd3kmuser' Database Account Password to Set	<input type="text"/>
'bswd3kmuser' Database Account Password again (for Validation)	<input type="text"/>
<input type="button" value=" < Back"/> <input type="button" value=" Next >"/>	

Figure 3.16 - Initial Default 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 the dataserver (i.e. SYBASE) is verified to be 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 in this screen are validated according to the values specified in Table 3.4.

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

3.2.3 Keymaster Configuration

The next part of the installation process is to provide information necessary to configure the Keymaster. 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. Finally, the installer can specify the Installation Type, choosing from Standard Broadsword or a TTA Low or High configuration. Figure 3.18 provides a sample of the Broadsword Keymaster Configuration Screen.

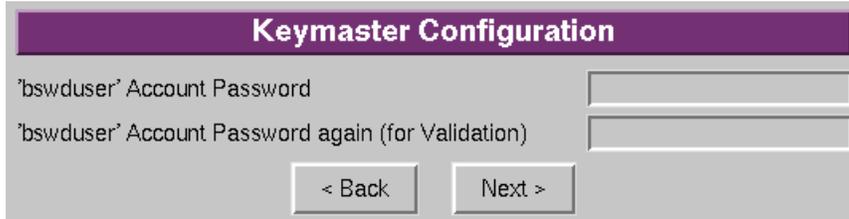


Figure 3.18 - Broadsword Keymaster Configuration Screen

Fields in this screen are validated according to the values specified in Table 3.5.

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. Only required if "currently running IPA or IPL on this machine" is selected (Y).

Table 3.5 - Fields Validated

3.2.4 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 several items for the Broadsword Client. For more detailed descriptions of these items, please see the Site Configuration Worksheet completed in Section 2.3. Figure 3.19 depicts the initial Broadsword Client Configuration Screen.

Figure 3.19 - Broadsword Client Configuration Screen

Fields in this screen are validated according to the values specified in Table 3.6.

FIELDS VALIDATED	
Client Protected HTTP Port #	Port number is not already in use.
Client Protected HTTP Port # (SSL)	Port number is not already in use.
System Group Name	Group name EXISTS on system.

Table 3.6 Fields Validated

3.2.5 POC Configuration

The final portion of the installation process is to configure the Support Page. This page provides the site's Points of Contact (POCs) for System Administration, ISSO, and Intelink Site Information Manager. The System Administration fields are mandatory. Figure 3.20 provides the initial point of contact information screen.

Point of Contact Information

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"/>
Organization Unit	<input type="text"/>	Address2	<input type="text"/>
Address1	<input type="text"/>	Phone	<input type="text"/>
Address2	<input type="text"/>	FAX	<input type="text"/>
Phone	<input type="text"/>	Email	<input type="text"/>
FAX	<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 3.20 - 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.

Note: The “Install” button may not be visible on systems with small monitors. In this case the <tab> <tab> <spacebar> keystroke sequence will also kick-off the install. Alternatively, the installer may click any portion of the window and drag it until the “Install” button become visible by holding down the <Alt> key.

Figure 3.21 is a sample confirmation page for a new dataserer. Figure 3.22 is a sample confirmation page for a shared dataserer confirmation. Both examples are using UNIX filesystems.

Keymaster will be configured with these settings:	
SYBASE User Name:	sybase
SYBASE Home Directory:	/opt/SYBASE
SYBASE Dataserver Name:	BSWD_EUROPA_KM_SVR
SYBASE Dataserver Port:	2703
SYBASE Dataserver Master Path:	/opt1/bswd3_km_syb_devices
SYBASE Dataserver Sysprocs Path:	/opt1/bswd3_km_syb_devices
SYBASE Backup Server Port:	2753
Keymaster TempDevice Path	/opt1/bswd3_km_syb_devices
Keymaster TempDevice Size:	100
Keymaster Data Device Path:	/opt1/bswd3_km_syb_devices
Keymaster Data Device Size:	100
Keymaster Log Device Path:	/opt1/bswd3_km_syb_devices
Keymaster Log Device Size:	25
Client Protected HTTP Port #:	84
Network:	S
Group Name:	bswd
Install Mode:	New

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

Figure 3.21 Sample Based on New Dataserver Confirmation Screen

Keymaster will be configured with these settings:	
SYBASE User Name:	sybase
SYBASE Home Directory:	/opt/SYBASE
SYBASE Dataserver Name:	SYBASE
Keymaster Data Device Path:	/opt1/bswd3_km_syb_devices
Keymaster Data Device Size:	100
Keymaster Log Device Path:	/opt1/bswd3_km_syb_devices
Keymaster Log Device Size:	25
Client Protected HTTP Port #:	84
Network:	S
Group Name:	bswd
Install Mode:	New

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 Shared Dataserver 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 3.23 provides an example of this screen.

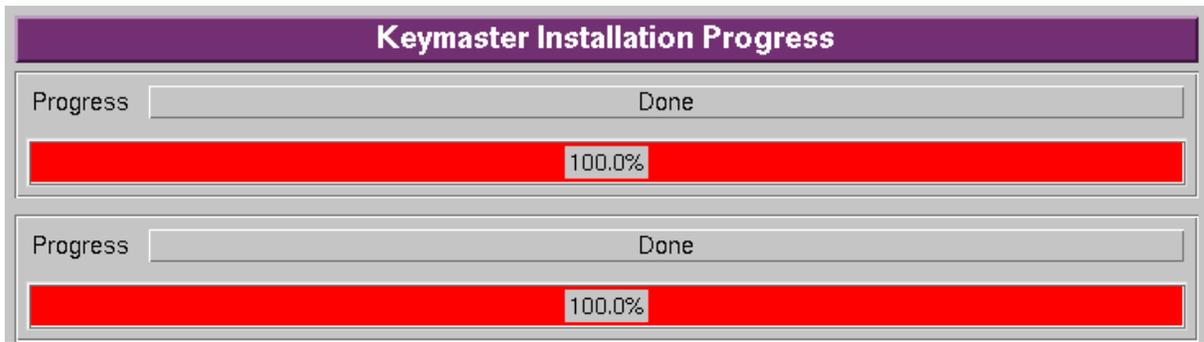


Figure 3.23 - Example of the Progress Gauge

The second screen provides a log of the process. Figure 3.24 provides an excerpt from a sample log screen. The information contained on the screen is also saved into a log file (`/opt/bswd3.1/logs/install.log`) for later reference. Also the configuration information is saved and if the installation process is restarted, it will read the saved file. Do not place another window over the "Broadsword Installation Progress" or it will not be updated dynamically and you will be unable to observe the progress of the install.

```

Keymaster Install (Install Log)
-->Initialize Install
-->Keymaster Dataserver Configuration
--->Create Dataserver
tcsh: getwd: Cannot stat ".": (Permission denied)
tcsh: Trying to start from "/"
The log file for this session is /opt/SYBASE/init/logs/log0511.004*.
WARNING: /opt1/bswd3_km_syb_devices/Bswd3KmMaster.dev is a regular file which is not recommended for a Server device.
Because this sybinit session was invoked with the '-T IGNORE_WARNINGS' flag, the above warning(s) will be ignored and the configuration will proceed.
Running task: update SQL Server entry in interfaces file.
Task succeeded: update SQL Server entry in interfaces file.
Running task: create the master device.
Building the master device
...Done
Task succeeded: create the master device.
Running task: update the SQL Server runserver file.
Task succeeded: update the SQL Server runserver file.
Running task: boot the SQL Server.
Task succeeded: boot the SQL Server.
Running task: create the sybserverprocs database.
sybserverprocs database created.
Task succeeded: create the sybserverprocs database.
Running task: install system stored procedures.
.....Done
Task succeeded: install system stored procedures.
Running task: set permissions for the 'model' database.
Done
Task succeeded: set permissions for the 'model' database.
Running task: set the default character set and/or default sort order for the SQL Server.
Setting the default character set to iso_1
Installing character set 'iso_1'
..Done
Sort order 'nocase' has been successfully installed.
Character set 'iso_1' is already the default.
Sort order 'nocase' has been successfully set to the default.
Task succeeded: set the default character set and/or default sort order for the SQL Server.
Running task: set the default language.
Setting the default language to us_english
Language 'us_english' is already the default.
Task succeeded: set the default language.
Configuration completed successfully.
Exiting.
The log file for this session is /opt/SYBASE/init/logs/log0511.004*.

--->Create Backup Server
tcsh: getwd: Cannot stat ".": (Permission denied)
tcsh: Trying to start from "/"
The log file for this session is /opt/SYBASE/init/logs/log0511.005*.
Running task: update Backup Server entry in interfaces file.
Task succeeded: update Backup Server entry in interfaces file.
Running task: update the Backup Server runserver file.
Task succeeded: update the Backup Server runserver file.
Running task: boot the Backup Server.
Task succeeded: boot the Backup Server.
Configuration completed successfully.
Exiting.
The log file for this session is /opt/SYBASE/init/logs/log0511.005*.

-->Keymaster Database Configuration
--->Acquiring next Sybase Device Number
Next VDEVNO = 2
--->Creating Transaction Log Device
--->Creating Data Device
--->Creating Database & Transaction Log
(return status = 0)
(return status = 0)
CREATE DATABASE: allocating 51200 pages on disk 'Bswd3KmData'
CREATE DATABASE: allocating 12800 pages on disk 'Bswd3KmLog'

```

```

--->Reconfiguring Dataserver
Parameter Name      Default  Memory Used Config Value Run Value
-----
total memory        7500    15000    12288    7500
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Parameter Name      Default  Memory Used Config Value Run Value
-----
number of user connections  25      1871     50       25
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Parameter Name      Default  Memory Used Config Value Run Value
-----
number of devices      10      #4       20       10
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Parameter Name      Default  Memory Used Config Value Run Value
-----
number of locks         5000    469     15000    5000
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Parameter Name      Default  Memory Used Config Value Run Value
-----
procedure cache percent  20      960     25       20
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Password correctly set.
Account unlocked.
New login created.
(return status = 0)
Database option 'trunc log on chkpt' turned ON for database 'bswd3_kmdb'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
Database owner changed.
(return status = 0)
Adding server 'BSWD_EUROPA_KM_SVR', physical name 'BSWD_EUROPA_KM_SVR'
Server added.
(return status = 0)
--->Creating Temp Device
Extending database by 51200 pages on disk BswdTemp
Database option 'select into/bulkcopy' turned ON for database 'tempdb'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
Database option 'trunc log on chkpt' turned ON for database 'tempdb'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
--->Loading Schema
--->Loading Indexes
--->Loading Stored Procedures
->Configuring Keymaster Server
--->Updating Configuration Files
HUPping syslogd PID 158
--->Encrypting Configuration Files
->Configuring Keymaster Client
--->Updating Configuration Files
--->Configuring Homepages
--->Configuring POC Page
--->Installing Initial Statistics Page
->Starting Keymaster 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/keymaster3.0/bin
Start these portions of BSWD? (Y/N/Q) [Y]: Starting Sybase...
SYBASE SQL Server is already running
SYBASE Backup Server is already running
Starting Background APs...
  Starting /opt/keymaster3.0/client/bin/conan
  Starting /opt/keymaster3.0/bin/keymaster.SVR4
  Starting /opt/keymaster3.0/bin/jivacron
  Starting /opt/keymaster3.0/bin/remote_plugin.SVR4

Keymaster 3.0 Process Status (Thu May 11 14:55:56 EDT 2000):

running /opt/keymaster3.0/bin/keymaster.SVR4
running /opt/keymaster3.0/bin/jivacron
running /opt/keymaster3.0/bin/remote_plugin.SVR4
running /opt/keymaster3.0/client/bin/conan

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

Figure 3.24 - Sample Log Screen

When the installation is complete, the last screen displayed will be the “Installation Complete” screen (as shown in Figure 3.25).

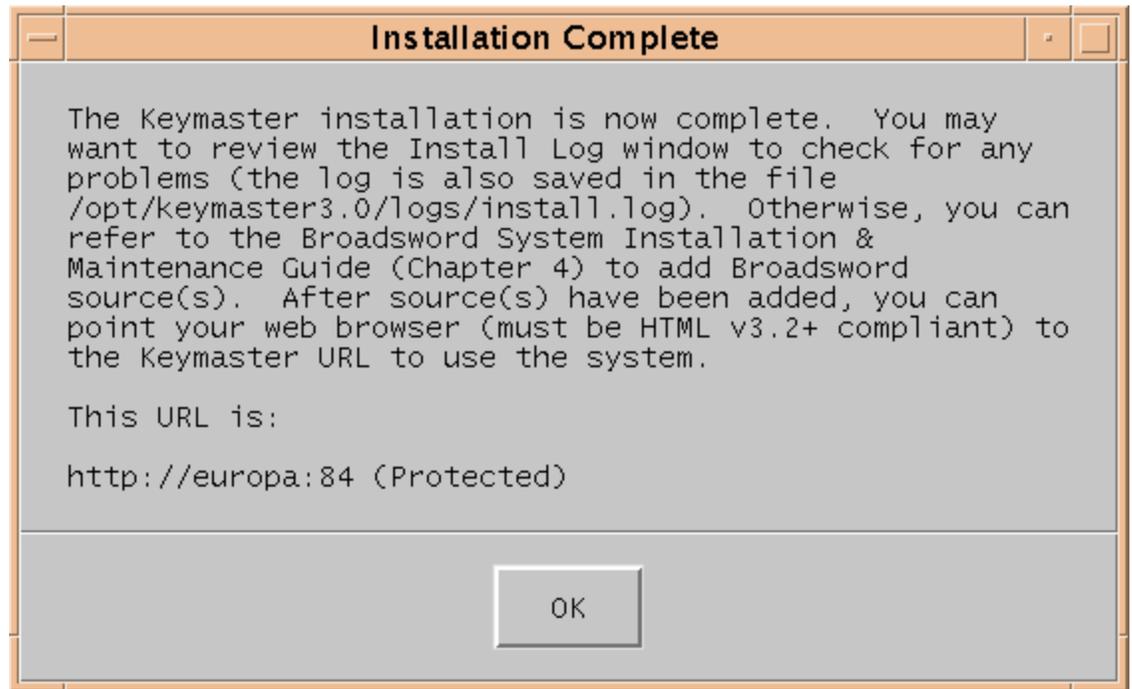


Figure 3.25- Installation Complete

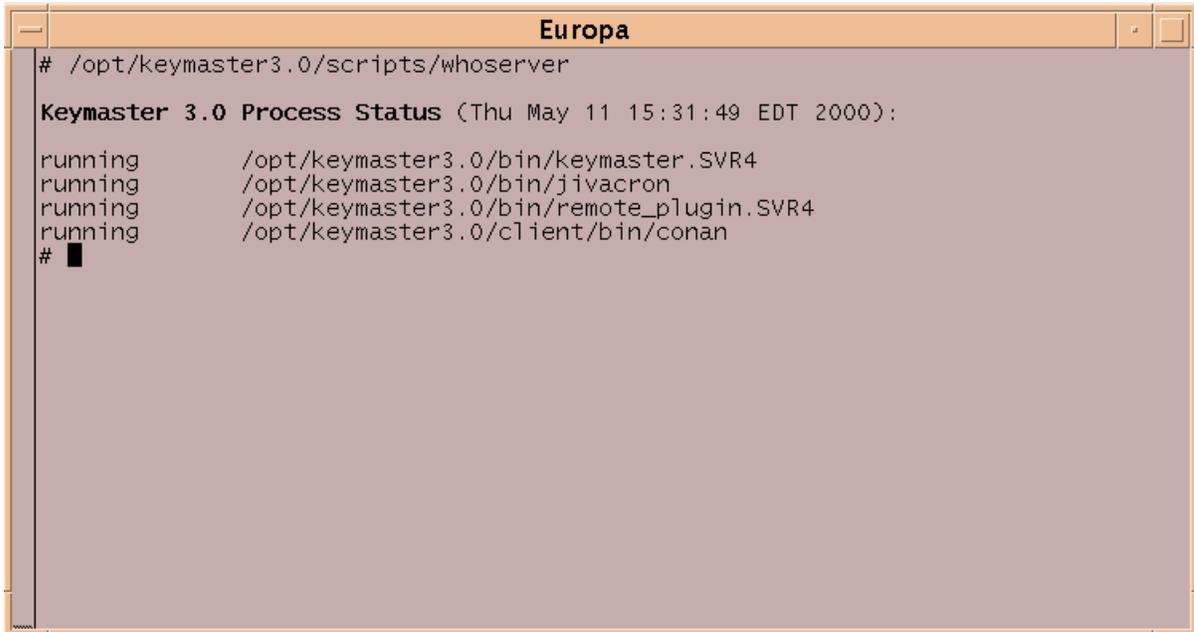
3.5 Installation Verification

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

```
/opt/keymaster3.0./scripts/whoserver<cr>
```

If all processes are running, the installation has most likely succeeded. Figure 3.26 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 `/opt/keymaster3.0./logs/install.log`) for any obvious problems during the installation. This script also displays the percentage of Broadsword audit database space free. The user must enter the correct Sybase 'sa' password to check this. If any problems cannot be fixed at this point contact the IDHS help desk (see page i), otherwise continue to TFM-Attachment I-Chapter1.

Note: Sybase and Broadsword are running from the `/cdrom/cdrom0` directory, effectively locking that device. To install other software from the CDROM it will be necessary to shutdown Broadsword in order to unmount the CDROM.



```

# /opt/keymaster3.0/scripts/whoserver

Keymaster 3.0 Process Status (Thu May 11 15:31:49 EDT 2000):

running      /opt/keymaster3.0/bin/keymaster.SVR4
running      /opt/keymaster3.0/bin/jivacron
running      /opt/keymaster3.0/bin/remote_plugin.SVR4
running      /opt/keymaster3.0/client/bin/conan
# █

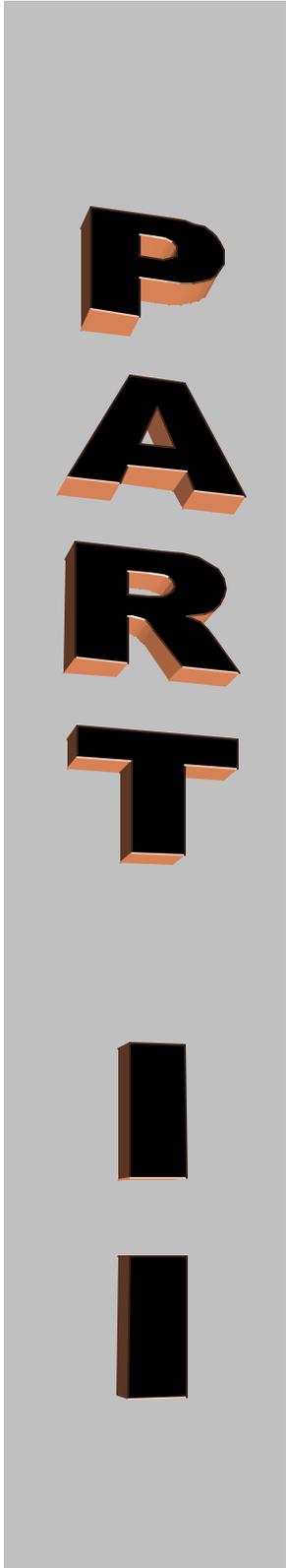
```

Figure 3.26- Sample Listing of Processes Running

3.6 Routine Log Maintenance

Please refer to the Broadsword Trusted Facility Manual (Administrator's User Guide Attachment) for instructions to maintain Broadsword log files.

This page intentionally left blank



CONFIGURATION

The purpose of this part is to provide detailed information to configure the system and register community Gatekeepers.

Topics covered in this part:

- System Administration
 - Gatekeeper Registration
 - Viewing/UnRegistering Gatekeepers
 - Keymaster Configuration

- User Maintenance
 - Editing/Modifying User Privileges

- Client Requirements
 - HTML Browsers

This page intentionally left blank

Chapter 4

System Administration

Once the installation of the basic system is complete, site specific configuration can be performed. This chapter provides details on how to register community Gatekeepers, view and unregister Gatekeepers, and modify system parameters. To begin, start your web browser and type the URL of the newly installed Keymaster system (i.e. <http://charon:80> or <https://charon> (for SSL)) 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 3.2.3), and click the “Accept” button. By selecting the System Configuration item (under the Administration popdown menu), the administrator is presented with the set of options shown in figure 4.1.



Figure 4.1 - System Configuration Tools

4.1 Gatekeeper/TTA Registration

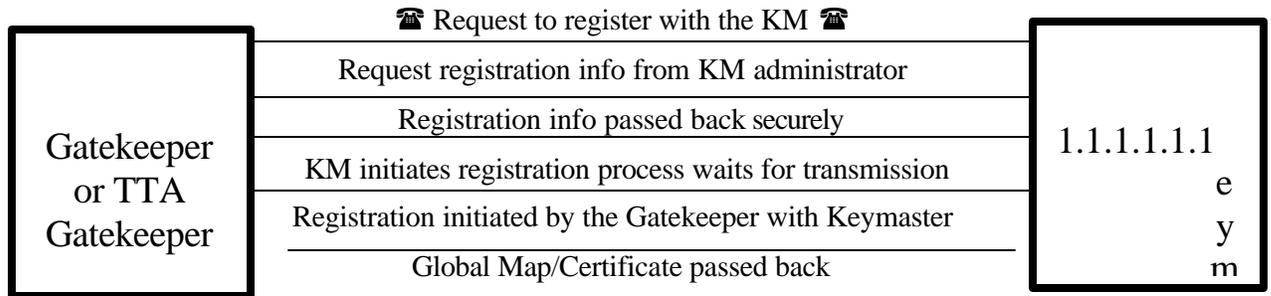
The purpose of this section is to allow the Keymaster to register new Gatekeepers & TTA Gatekeepers through the use of digital certificates. The procedure to accomplish this follows:

1. The *POC for the new Gatekeeper* (or new TTA Gatekeeper) will contact the Keymaster via telephone and request to register their Gatekeeper.
2. The *Keymaster* will select the **Start Registration** option to generate the Registration ID used for the registration process.
3. The *Keymaster* will then transmit (via secure means), the Keymaster’s IP address, port number, and Registration ID to the POC of the Gatekeeper (or TTA Gatekeeper).
4. The *POC of the new Gatekeeper* will then use the **Administration -> System Configuration -> Register Gatekeeper (or Register TTA)** option to enter the required data on their Broadsword page to complete the registration process at their site.
5. After the registration process has been initiated by the Keymaster, that status of the registration process will be updated and displayed every minute on the Keymaster Browser until the registration process is completed or terminated.

- The Keymaster may click on the **Abort** button to abort the current registration process anytime during the registration process.

Note: Only one registration process may be initiated and active at any given time. Clicking on any options on any popdown menu during the registration process will terminate the registration process.

The following diagram illustrates the process flow between the registering Gatekeeper (or TTA Gatekeeper) and the Keymaster:



4.2 Viewing and Unregistering Gatekeepers or TTA Gatekeepers

The purpose of this section is to allow the Keymaster to view all registered Gatekeepers and to unregister any or all Gatekeepers. Each registered Gatekeeper has the POC information and all of its backside sources listed.

4.2.1 How to Unregister a Gatekeeper or TTA Gatekeeper

- Click on the box next to the desired Gatekeeper in the UnRegister column.
- Click on the "UnRegister" button at the bottom of the page to perform the unregistration.

Note: Under each Gatekeeper in the right column are the sources that are available to that particular Gatekeeper. Keymaster users can only UnRegister the Gatekeeper as a whole and not the individual sources.

Figure 4.2 is a sample screen of the viewing/unregistering of Gatekeepers.

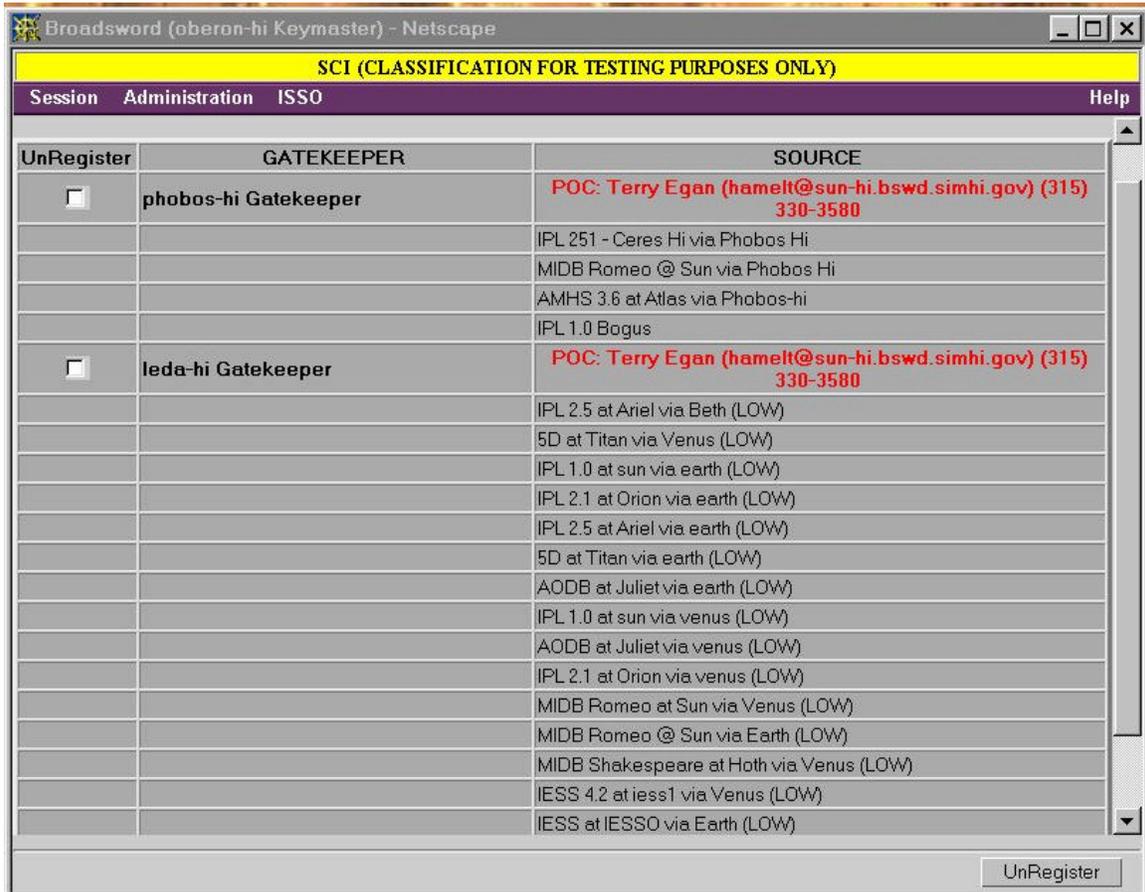


Figure 4.2 View/Remove Gatekeepers via High Side Keymaster

4.3 Keymaster Configuration

The “Edit Keymaster” screen allows the administrator to modify various parameters of the Keymaster. Figure 4.3 presents a sample screen.

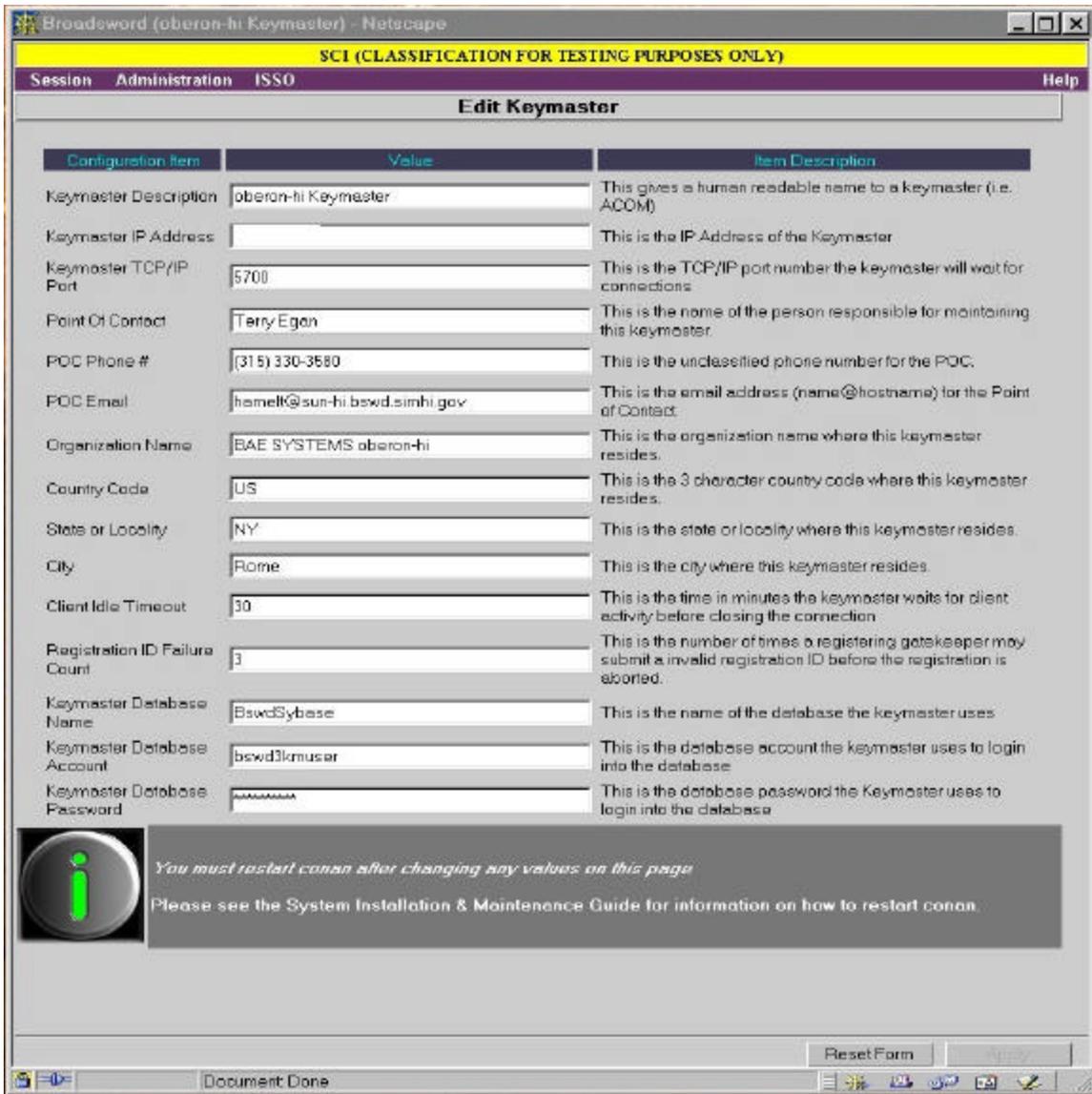


Figure 4.3 Sample "Edit Keymaster" Screen

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.

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

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

Chapter 5

User Maintenance

5.1 User Maintenance

If the administrator logs into a Broadsword Keymaster server, they will be unable to create user accounts through the Keymaster interface. 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. However, the Broadsword Keymaster interface will allow the administrator to grant roles. 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 → Local User. The following image (Figure 5.1) shows the initial page directly after an installation.

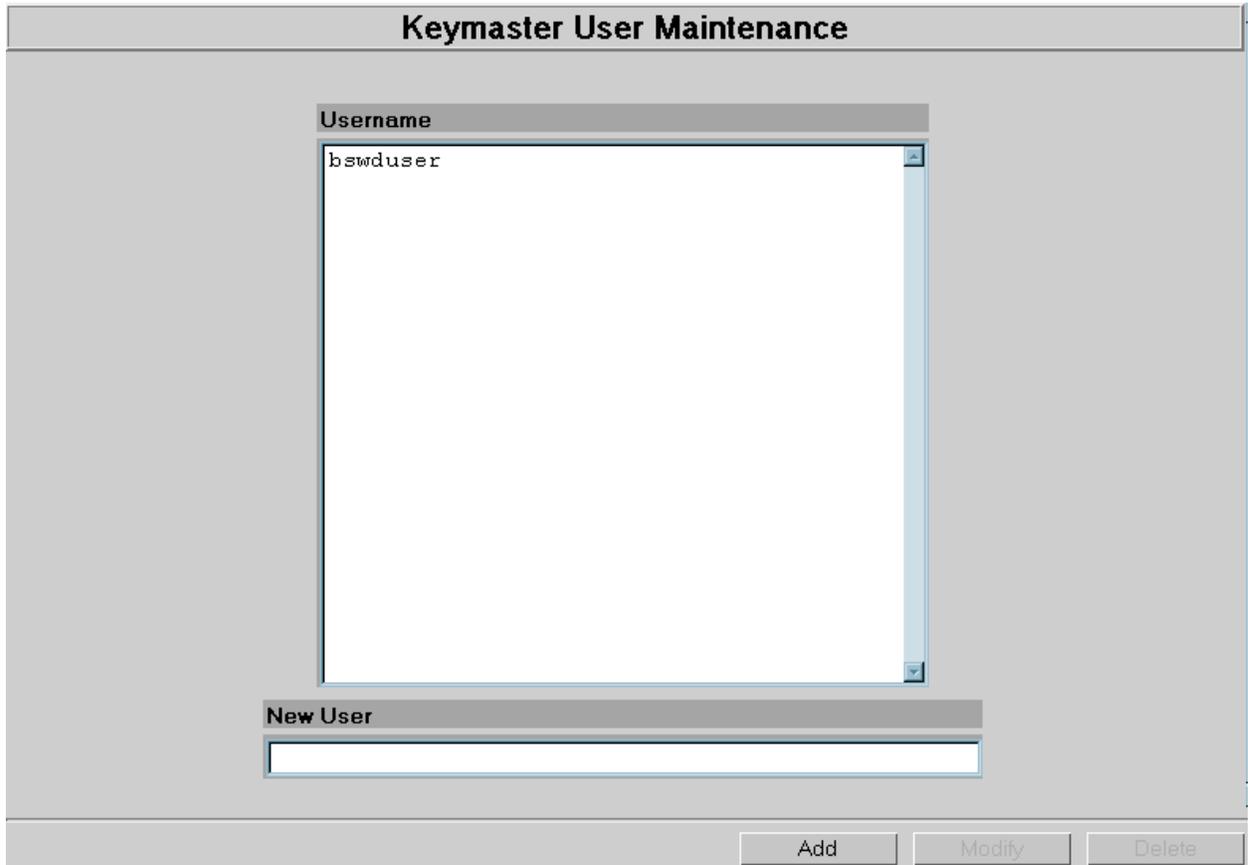


Figure 5.1 – Keymaster User Maintenance

This page contains a list of users who are able to log into the Keymaster.

Note: The username list is created by reading a directory in which Keymaster profiles are kept. Thus, if a user has *not* logged into Keymaster 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 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 5.2 shows a Username selected with the buttons activated.

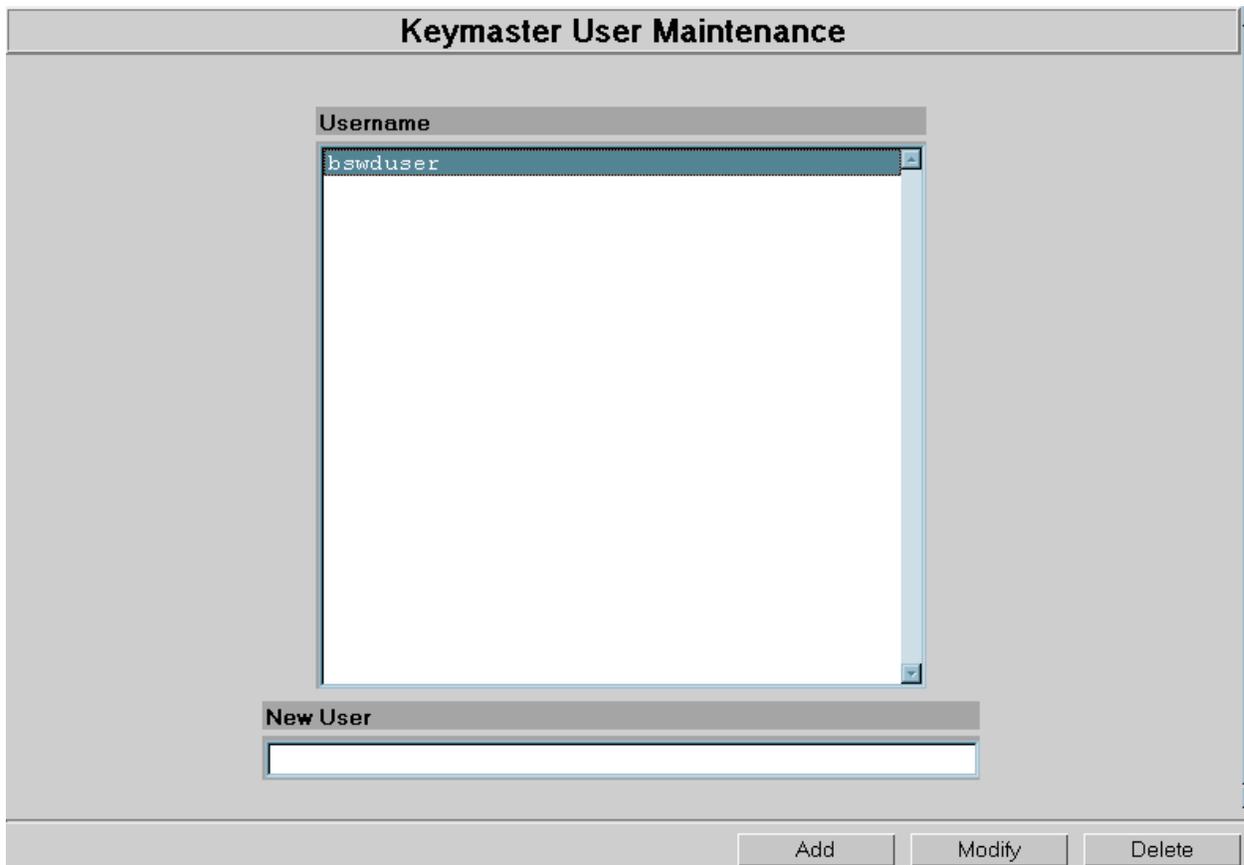


Figure 5.2 – Keymaster User Maintenance (username selected)

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

Note: Deleting a user does *not* actually delete the user from the entire system. Rather, it deletes the user's relevant Keymaster files only.

If the administrator clicks on the Delete button, a dialog box will appear that will allow the user to confirm the action.

The administrator may 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 5.2). If a user selects a Username and clicks on the Modify button, the following page will appear (Figure 5.3):

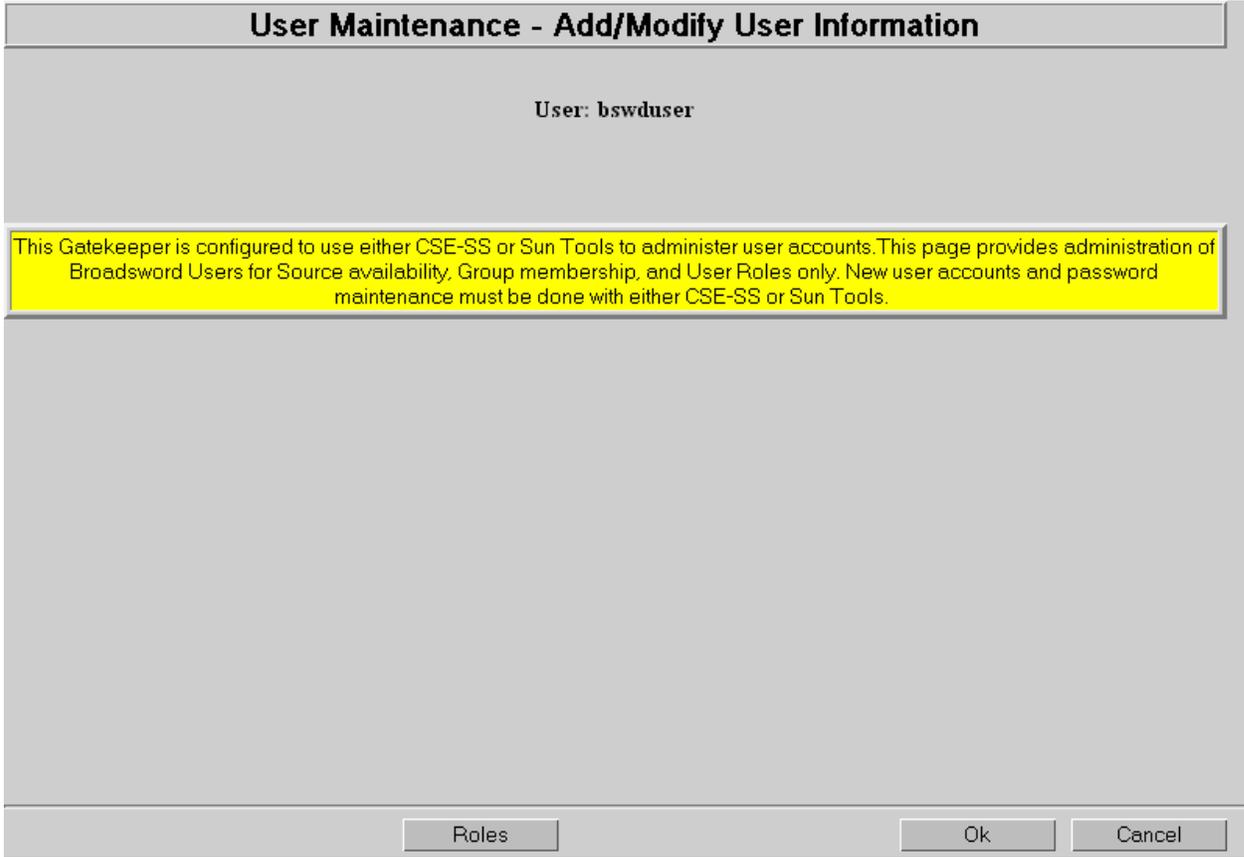


Figure 5.3 – Keymaster User Maintenance (Modifying a user)

The Modify user page (Figure 5.3) contains a yellow banner in the middle of the page. Similar to adding a user, Keymaster is unable to modify user information. 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 5.2). If the administrator selects the Roles button, they will be brought to the relevant page. For information pertaining to this button, reference section 5.2 of this manual.

5.2 Adding/Removing Roles

If the administrator would like to change a particular user’s Role(s), the administrator can click on the Roles button on the Modify User page (Figure 5.3). A sample page follows (Figure 5.4):

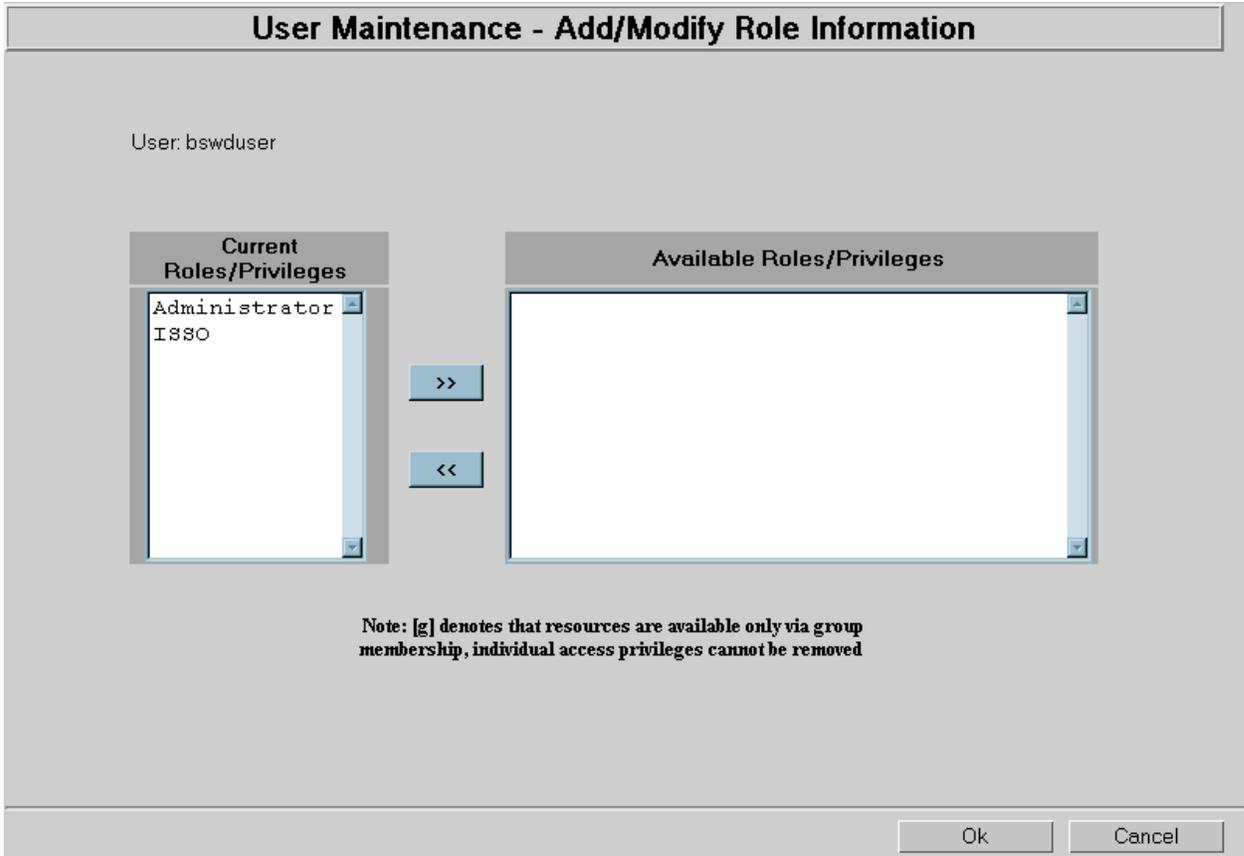


Figure 5.4 – Adding/Removing Roles

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.

This page intentionally left blank.

Chapter 6

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. There is NO specific client software required to be loaded. Specific topics to be covered include:

- HTML Browsers

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.

6.1 HTML Browsers

Keymaster 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 4.7+ or Internet Explorer 4.0+.

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 Keymaster 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).

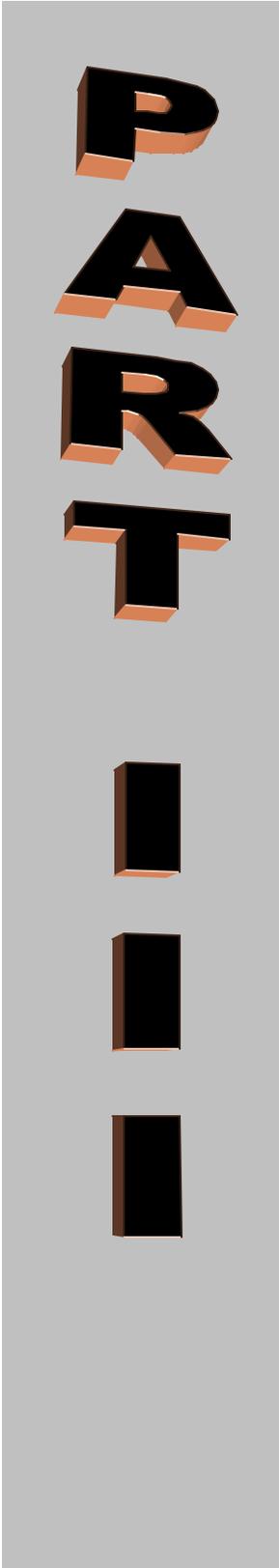
When using Netscape, resizing the browser window may cause the current page's data to be lost. The server will respond with a missing form data error. Reloading the form data will not return you to the expected page, since all of Keymaster's pages are created dynamically. In order to solve this problem, 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 in cache is compared to document on network* heading. For Internet Explorer, select **View ? Internet Options** and click on the **Settings** button under the **Temporary Internet files** heading. Ensure that the **Every visit to the page** radio button is selected.

Operating System	Browser
Solaris 2.5.1/2.6	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

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

This page intentionally left blank.



MAINTENANCE

The purpose of this part is to provide detailed information to maintain the system.

Topics covered in this part:

- System Status
- Daemon Status
- Set Debug Flags
- Queue Maintenance
- System and Log Info
- Current Users

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 popdown menu), the Administrator is presented with a set of options as shown in Figure 7.1.

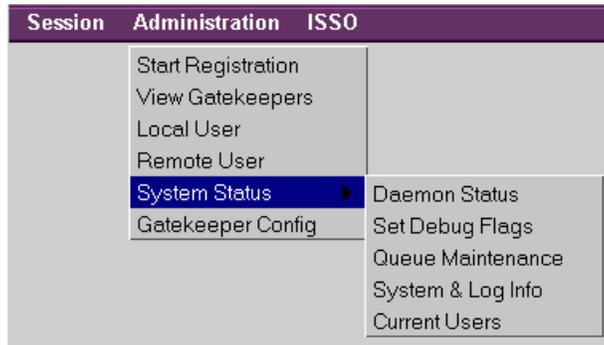


Figure 7.1 System Status Tools

7.1 Daemon Status

The “Daemon Status” screen provides the administrator with the status of the required system processes, 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	1794	running
keymaster	998	running
jivacron	1003	running

Figure 7.2 Sample “Daemon Status” Screen

Note: This page will automatically refresh every 30 seconds.

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, keymaster, jivacron, remote_plugin ADDITIONAL PROCESSES: none
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, keymaster, jivacron, remote_plugin) will appear in the process table. Each process will have a process ID and a status of **running**.

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 four 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.

To Start/Stop the System

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

```
/opt/keymaster3.0/scripts/startserver <cr>
```

and press *<cr>* to accept the defaults.

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

```
/opt/keymaster3.0/scripts/stopservice <cr>
```

and follow the prompts.

To Check the System

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

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

/opt/keymaster3.0/scripts/whoserver <cr>

Figure 7.3 illustrates an example of completely restarting Keymaster:

```

Saturn
# /opt/keymaster3.0/scripts/stopserver

Default KEYM shutdown? (Y/N/Q) [Y]: n
Stop Sybase? (Y/N) [Y]: n
Stop KEYM background APs? (Y/N) [Y]: y
You have chosen the following KEYM shutdown options:
  Stop Sybase ..... No
  Stop KEYM background APs..... Yes
  KEYM executables..... /opt/keymaster3.0/bin
Stop these portions of KEYM? (Y/N/Q) [Y]: y
Stopping /opt/keymaster3.0/bin/keymaster.SVR4$
Stopping /opt/keymaster3.0/bin/jivacron$
Stopping /opt/keymaster3.0/bin/remote_plugin.SVR4$
Stopping /opt/keymaster3.0/client/bin/conan$
Shutting down PROTECTED HTTP Daemon(PID=14143) ... Complete!
#
# /opt/keymaster3.0/scripts/startserver

Default KEYM startup? (Y/N/Q) [Y]: y
You have chosen the following KEYM startup options:
  Start Sybase ..... Yes
  Start KEYM background APs..... Yes
  KEYM executables..... /opt/keymaster3.0/bin
Start these portions of KEYM? (Y/N/Q) [Y]: y
Starting Sybase...
SYBASE SQL Server is already running
SYBASE Backup Server is already running
Starting Background APs...
  Starting /opt/keymaster3.0/client/bin/conan
  Starting /opt/keymaster3.0/bin/keymaster.SVR4
  Starting /opt/keymaster3.0/bin/jivacron
  Starting /opt/keymaster3.0/bin/remote_plugin.SVR4

Keymaster 3.0 Process Status (Mon May 15 10:56:03 EDT 2000):
running      /opt/keymaster3.0/bin/keymaster.SVR4
running      /opt/keymaster3.0/bin/jivacron
running      /opt/keymaster3.0/bin/remote_plugin.SVR4
running      /opt/keymaster3.0/client/bin/conan
#

```

Figure 7.3 Sample Keymaster Restart

7.1.1 Possible Problems/Solutions

The process table should contain information on each of the mandatory processes. In addition, 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 7.4 provides a sample of the Queue Maintenance screen.

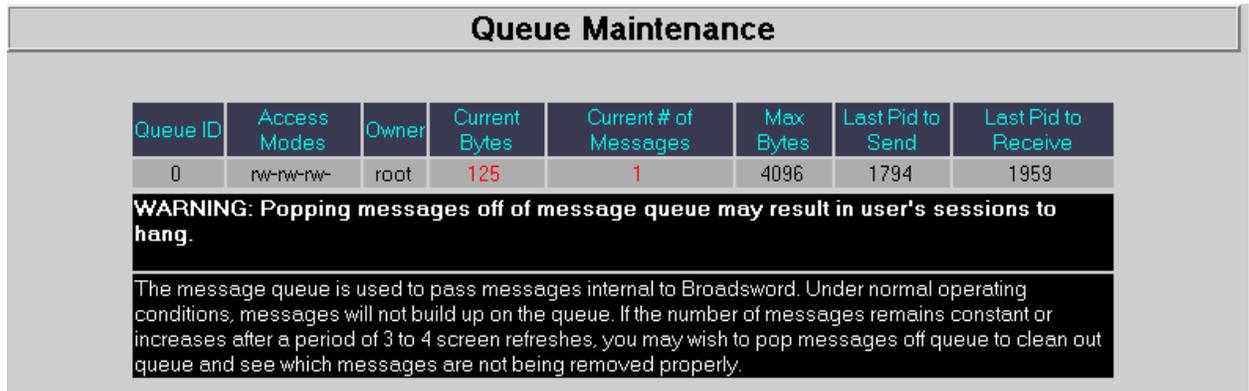


Figure 7.4 Sample Queue Maintenance Screen

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.

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 Keymaster or logins are taking an unusually long time	If the administrator cannot log into Keymaster 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/keymaster<version_number>/bin/startconan. If conan is running, follow the instructions in the next problem solution.
Response time is unusually long after clicking any action button - OR - Get no response after clicking any action button	Messages may be stuck on the message queue or the Current Bytes on the queue may have exceeded the Max Bytes . Check for this by clicking the "Update Display" button. 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 Notification Profiles, Remove Data Set, Update Data Set, Batch Profile 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 7.5 provides a sample of the Set Debug Flags screen.

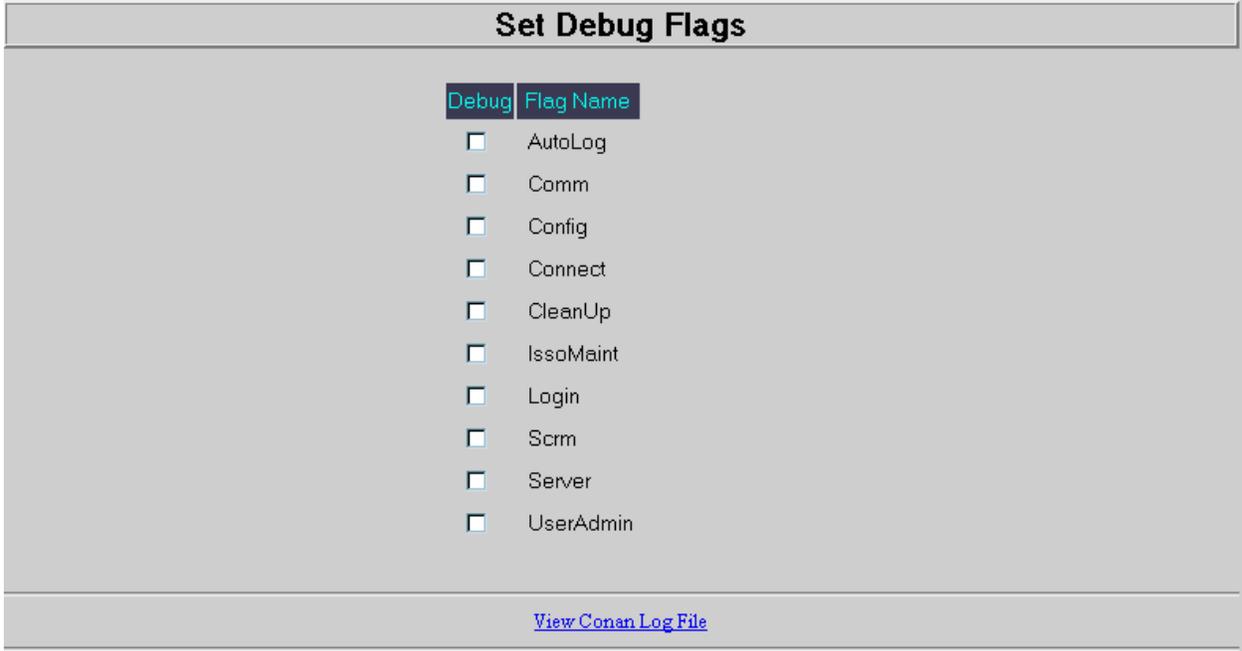


Figure 7.5 Sample Set Debug Flags Screen

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. AVAILABLE FLAGS: Autolog, Comm, Config, Connect, CleanUp, IssoMaint, Login, Scrm, Server, UserAdmin.

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 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 7.6 provides a sample of the “System and Log Info” screen.

System and Log Info

To purge one or more log files, select the log files to be purged and press the "Purge Marked" button located below. Refer to the table immediately above the button bar for information on disk usage for the file system on which the client resides.

Select	Log File	Size in Bytes
<input type="checkbox"/>	error_P.log	810
<input type="checkbox"/>	access_P.log	236,159
<input type="checkbox"/>	jivacronlog	2,805
<input type="checkbox"/>	conan.log	5,873

File System	Total Kilobytes	Used	Available	Capacity
/opt/keymaster3.0/client	1,255,424	360,448	894,976	29%

Figure 7.6 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 7.6
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.
jivacronlog	Logs Keymaster CRON activity 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 on this screen.

There are three 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 7.7 provides a sample of the "Current Users" screen.

Current Users as of 2001 May 09, 18:56:16		
Username	Conan PID	Time of Log-in
bswduser	1794	2001 May 09, 18:19:30

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 Keymaster system uses a Sybase database to maintain application audit events (see the ISSO section for more detailed information). If the partition on which the database 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 Keymaster 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 database's disk space by executing the following at the command line:

```
% /opt/keymaster3.0/scripts/whoserver
Check the status of Keymaster processes (Requires the Database sa password to check
database free space)
```

7.6.1 Level-One Threshold

The Level-One threshold warns the administrator that the database disk usage 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 Keymaster
% su - root
# /bin/csh
# /opt/keymaster3.0/scripts/stopsserver
  (Answer N, N, Y, Y to the stopsserver prompts)

Set the new threshold value
# source /opt/keymaster3.0/etc/server_env_vars
# setenv SYBASE $BSWD_HOME/odbc
# setenv BSWD_DB_THRESHOLD <N>
```

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

```
Restart Keymaster
# /opt/keymaster3.0/scripts/startserver
  (Answer Y, Y to the startserver prompts)
```

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 Keymaster 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 Keymaster
% su - root
# /bin/csh
# /opt/keymaster3.0/scripts/stopsserver
  (Answer N, N, Y, Y to the stopsserver prompts)

Get the old threshold value
# source /opt/keymaster3.0/etc/server_env_vars
# setenv SYBASE $BSWD_HOME/odbc
# echo $BSWD_DB_FULL_THRESHOLD
```

Set the new value higher than the old one (The default setting for this threshold is 90% if one isn't set)

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

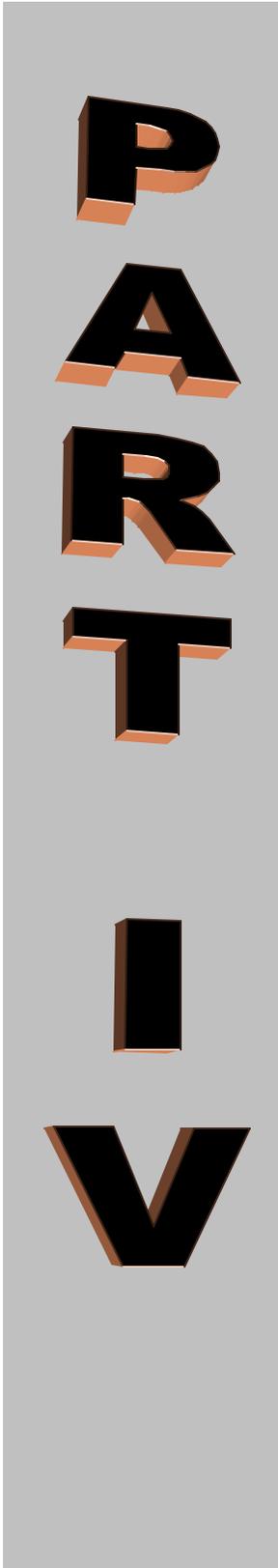
Restart Keymaster

```
# /opt/keymaster3.0/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 intentionally left 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 8

ISSO

8.1 Audit Log Maintenance and Archiving Logs

The ISSO Interface provides the ability to view, archive, or remove audit information from the Keymaster 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 8.1 shows the **Audit Log Maintenance** page.

Figure 8.1 - 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 queried. DEFAULT: Current date/time; if Start Date
Event:	The audit event being queried. POSSIBLE ENTRIES: All Events, Added DAC, Added Group,

	Added Group Member, Removed Group, Removed Group Member, Added User Privileges, Audit Dump, Get Audit Archive List, Delete Audit, Keymaster Started, Keymaster Stopped, Got Audit Report, Remove DAC, Set User DAC, Remove User Privileges, Remove Remote Gatekeeper, User Logged In, User Logged Out, Accept Registration From Remote Gatekeepers, Register Our Gatekeeper With Keymaster, Update Daemon Status, New or Updated Gatekeeper Info, Set User Information, User Changed Password
Archive File Name:	Name of file to contain audit records being archived. (The directory path is not included in the filename.) PURPOSE: Needed only when using the " Archive Records " feature.

Table 8.1 - Query Parameters

The function of the buttons in the bottom button 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/keymaster<version_number>/audits.")
Remove Records	Remove the records from the Keymaster 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.
Reset	Returns the selections to their previously applied values.

Table 8.2 - Button Functions

8.2 Understanding the Audits

The Keymaster 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. Most of the Keymaster audits are the same as the corresponding Gatekeeper audits. This section concentrates on those audits that are unique to the Keymaster.

8.2.1 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. The Keymaster maintains a global list of each Gatekeeper's **local map** (referred to as the **global map**). **Table 8.3** provides a list of Keymaster-specific 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 8.3 – Keymaster Audit Events

Figure 8.2 shows the example environment that we will consider for the following examples.

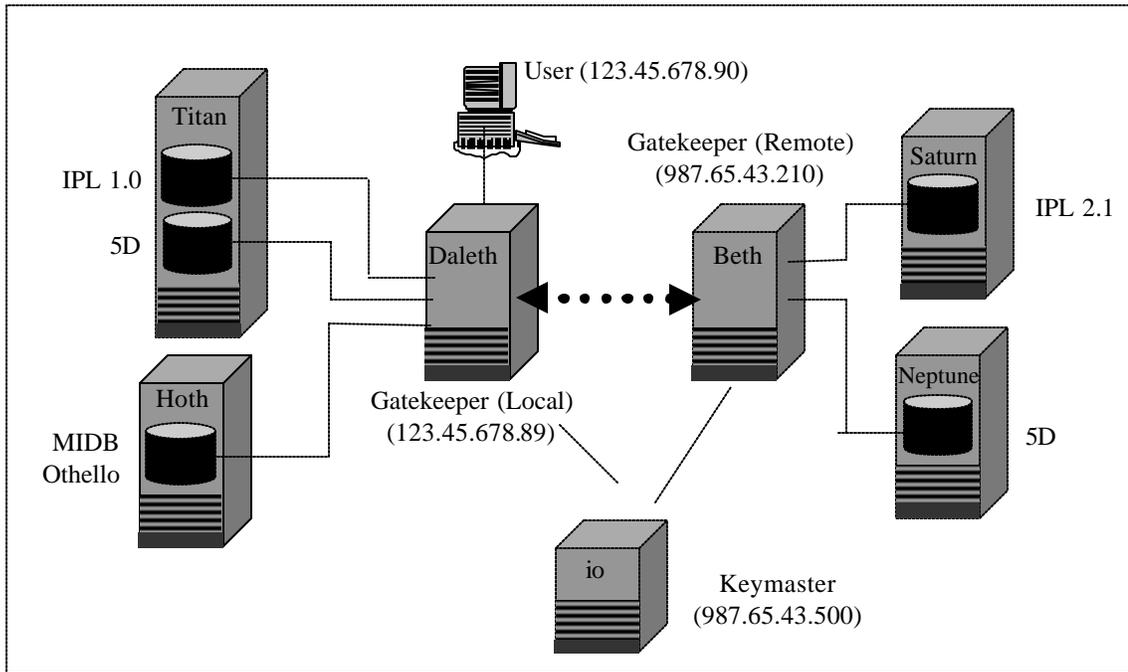


Figure 8.2 – Keymaster/Gatekeeper Environment

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.

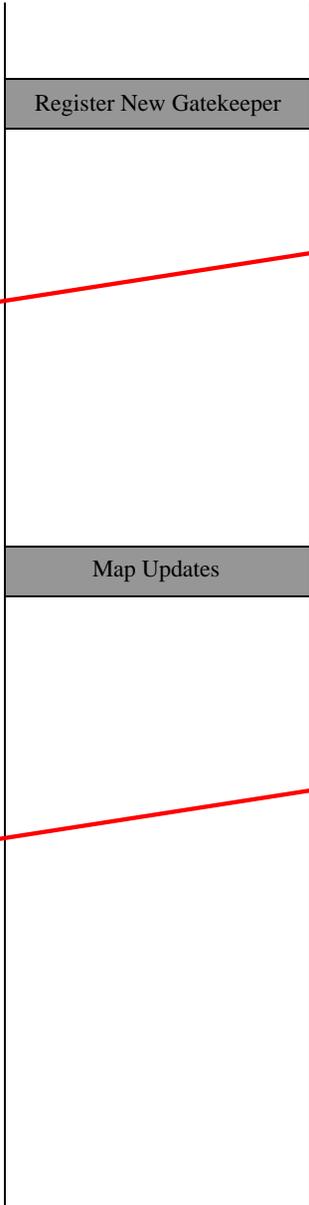
In some circumstances it becomes necessary to remove a Gatekeeper from a Keymaster's community. The Keymaster administrator has the ability to remove a Gatekeeper from the community. This removes all global map and certificates from the removed Gatekeeper, and removes all references to that Gatekeeper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

Figures 8.3a and **8.3b** provide example audit records from a successfully completed Gatekeeper registration, a map update, and the unregistration of a Gatekeeper.

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
```



Keymaster Logs (io)

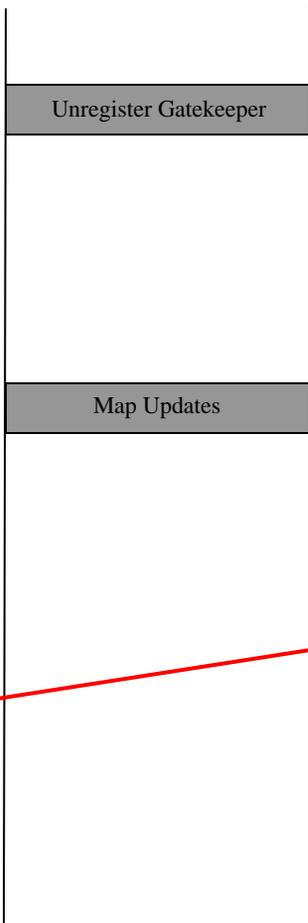
```
Login: keyadmin IP: 987.65.43.500 Orig. Login: keyadmin
Gtkpr: 987.65.43.500 Session Key: 672
LOGIN @ 20001204184358 : Successful Login from io
Keymaster
INITREG @ 20001204184638 : Gatekeeper Registration Started
from io Keymaster
INITREG @ 20001204184958 : Gatekeeper Registration
Completed For daleth Gatekeeper from io Keymaster
LOGOUT @ 20001204190507 : Connection closed from io
Keymaster
```

```
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 8.3a – 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 8.3b – Unregister a Gatekeeper

