



SYSTEM INSTALLATION GUIDE
FOR
BROADSWORD GATEKEEPER
VERSION 3.1 (Including TTA Functionality)



Prepared for:

**AFC2ISRC/A26
LANGLEY AIR FORCE BASE, VA 23665**

Prepared by:

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

September 2002

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 Von Milla, AC2ISRC/A-2X

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

Version Note

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

CHAPTER 1 INTRODUCTION.....	1
1.1 INSTALLATION OVERVIEW	1
1.2 SYSTEM DESCRIPTION	4
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	32
CHAPTER 3 INSTALLATION.....	38
3.1 LOADING THE SOFTWARE AND STARTING THE SETUP SCRIPT	38
3.2 PROVIDING INSTALLATION CHOICES	43
3.3 CONFIRMING INSTALLATION CHOICES	56
3.4 INSTALLATION PROGRESS	58
3.5 INSTALLATION VERIFICATION	61
3.6 RESTORE SYBASE INTERFACES FILE.....	62
CHAPTER 4 CLIENT REQUIREMENTS.....	64
4.1 HTML BROWSERS	64
4.2 IMAGE VIEWERS	65
4.3 SHOCKWAVE-FLASH PLAYERS	66
4.4 FTP SERVERS	66
4.5 MAP DATA	66
CHAPTER 5 TTA INSTALLATION.....	67
5.1 INSTALLING AND CONFIGURING THE ISSE GUARD SYSTEM.....	68
5.2 INSTALLING SOLARIS VERSION 2.6.....	68
5.3 CONFIGURING SOLARIS VERSION 2.6	69
5.4 INSTALLING AND CONFIGURING SYBASE DBMS SOFTWARE	77
5.5 INSTALLING AND CONFIGURING BROADSWORD GATEKEEPER SOFTWARE	77
5.6 INSTALLING AND CONFIGURING TTA HIGH GATEKEEPER SOFTWARE	77
5.6.1 <i>Installing TTA High Gatekeeper Software</i>	78
5.6.2 <i>Configuring TTA High Side Gatekeeper Software</i>	82
5.6.3 <i>Configuring TCP Wrappers on TTA High Side Gatekeeper</i>	87
5.7 INSTALLING AND CONFIGURING TTA LOW GATEKEEPER SOFTWARE	88
5.7.1 <i>Installing TTA Low Gatekeeper Software</i>	88
5.7.2 <i>Configuring TTA Low Side Gatekeeper Software</i>	92
5.7.3 <i>Configuring TCP Wrappers on the TTA Low Side Gatekeeper</i>	97

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

5.8 MODIFYING THE ISSE GUARD CONFIGURATION TO ACCESS TTA	98
5.9 UNINSTALLING TTA.....	102
5.9.1 Uninstalling TTA High Software	102
5.9.2 Uninstalling TTA Low Software	103
CHAPTER 6 TTA REGISTRATION	105
6.1 TTA HIGH SIDE GATEKEEPER REGISTRATION.....	105
6.2 TTA LOW SIDE GATEKEEPER REGISTRATION	106
CHAPTER 7 STARTING AND STOPPING TTA.....	108
7.1 STARTING TTA HIGH	108
7.2 STARTING TTA LOW	110
7.3 STOPPING TTA HIGH.....	112
7.4 STOPPING TTA LOW	113
APPENDIX A - PLUGIN WORKSHEETS.....	A-1
AIR FORCE WEATHER (WX)	
AIR ORDER OF BATTLE DATABASE (AODB)	
AUTOMATED MESSAGE HANDLING SYSTEM (AMHS)	
AUTOMATED MESSAGE HANDLING SYSTEM v3.6 (AMHS36)	
COMMERCIAL SATELLITE IMAGERY LIBRARY (CSIL)	
DEMAND DRIVEN DIRECT DIGITAL DISSEMINATION (5D)	
ELECTRONIC INTELLIGENCE (ELINT)	
FACILITIES INFRASTRUCTURE ENGINEERING SYSTEM (FIRES)	
IMAGE PRODUCT LIBRARY v1.0 (IPL)	
IMAGE PRODUCT LIBRARY v2.1 (IPL21)	
IMAGE PRODUCT LIBRARY v2.5 (IPL25)	
IMAGERY EXPLOITATION SUPPORT SYSTEM (IESS)	
INFORMATION EXTRACTION TOOL (IET)	
INFOSPHERE MANAGEMENT SYSTEM (ISM)	
INTELINK-HYDRA (INT)	
INTELINK-META SEARCH (META)	
MILITARY EQUIPMENT PARAMETRIC AND ENGINEERING DATABASE (MEPED)	
MILITARY INTEGRATED DATA BASE (MIDB)	
SPACE DATA BASE (SDB)	
APPENDIX B – TEST CASES.....	B-1
GENERAL FUNCTIONS TESTING	
QUERY-LOCAL & REMOTE SOURCES	
SHOPPING CART & ORDER STATUS TESTING	
SAVED & BATCH QUERIES TEST	
LOCAL USER MAINTENANCE USING CSE-SS/AFDI	
SECURITY AUDIT REVIEW TOOLS	
APPENDIX C - CHANGING DATASERVER PASSWORD.....	C-1
APPENDIX D –COTS/GOTS SAMPLE INSTALLATION INSTRUCTIONS.....	D-1
APPENDIX E - UNINSTALLING BROADSWORD.....	E-1
APPENDIX F - BROADSWORD FILE LISTING.....	F-1
APPENDIX G – TTA FILE LISTING.....	G-1
APPENDIX H – PATCH INSTALLATION.....	H-1

This page intentionally left blank

Chapter 1

Introduction

The purpose of the System Installation Guide is to provide detailed procedures to install a new copy of Broadsword Version 3.1 or to upgrade from an existing Version 3.0 system. This document contains two parts: (I) Broadsword Gatekeeper (BSWD GKPR) Installation and (II) Trusted Transfer Agent Gatekeeper (TTA GKPR) Installation.

1.1 Installation Overview

A Broadsword Gatekeeper 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 3.1 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 TTA Gatekeeper, a dedicated Broadsword Gatekeeper or a Broadsword Gatekeeper co-hosted on another application server (e.g. IPL 3.0). 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 Gatekeeper installation, refer to Chapters 2-4.
- TTA Gatekeeper installations (i.e. Broadsword Gatekeeper with TTA) refer to Chapters 5-7. The recommended installation sequence is as follows: (1) Broadsword Gatekeepers (high and low side) per instructions in this document, (2) ISSE Guard per ISSE Guard Installation Guide, (3) TTA Gatekeepers (high and low side) per instructions in this document.

Refer to the Broadsword Trusted Facility Manual for additional configuration information and discussion on administrator and ISSO tools provided to maintain the system.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Step	Description	Existing Configuration			
		BSWD 3.0 GKPR Solaris 2.6 CSE-SS 1.4.2.1 Sybase 11.5.1	BSWD 3.0 GKPR 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 SIG Chap 2-4)				
13	BSWD Full Install with import option (BSWD SIG Chap 2-4)	✓	✓	✓	✓
14	BSWD GKPR Configuration & Registration (BSWD TFM)	✓	✓	✓	✓
15	Install, Configure, Register & Enable TTA 1.0.2 (BSWD SIG Chap 5-7)				
16	BSWD Client Configuration (BSWD TFM)	✓	✓	✓	✓
Step	Description	BSWD 3.1 GKPR Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.1 GKPR Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2	BSWD 3.1 GKPR Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.1 GKPR Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2
Target Configuration					

Table 1.1 Installation Sequence

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Step	Description	Existing Configuration			
		IPL 3.0 Solaris 7 CSE-SS 1.4.2.1 Sybase 12	None (new install)		
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 SIG Chap 2-4)	✓	✓	✓	
13	BSWD Full Install with import option (BSWD SIG Chap 2-4)				
14	BSWD GKPR Configuration & Registration (BSWD TFM)	✓	✓	✓	
15	Install, Configure, Register & Enable TTA 1.0.2 (BSWD SIG Chap 5-7)				✓
16	BSWD Client Configuration (BSWD TFM)	✓	✓	✓	
Step	Description	BSWD 3.1 GKPR IPL 3.0 Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2 Sybase 12	BSWD 3.1 GKPR Solaris 7 CSE-SS 1.4.2.1 Sybase 11.9.2	BSWD 3.1 GKPR Solaris 7 AFDI 1.1.0.1 Sybase 11.9.2	TTA 3.1 GKPR Solaris 2.6 Sybase 11.9.2
Target Configuration					

Table 1.1 – Installation Sequence (continued)

1.2 System Description

Broadsword implements 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 product without human intervention while crossing between security domains. It is a separate package of code that also relies on the installation of an ISSE Guard 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 component is the heart of the overall architecture. It is a robust, thin layer of software which performs a variety of internal functions, including processing users' queries, auditing, communicating with various sources, interconnecting with other Gatekeepers, maintaining system status, and collection/compilation of results. The Gatekeeper supports a single Application's Programmer's Interface (API) for developers to access the functionality provided and to create applications. The API is based on a simple message passing mechanism and is divided into three sections: (1) User, (2) Administration, and (3) ISSO. A fourth section is the various plugins which connect to the datasources. Figure 1.1 shows the overall architecture of the Gatekeeper.

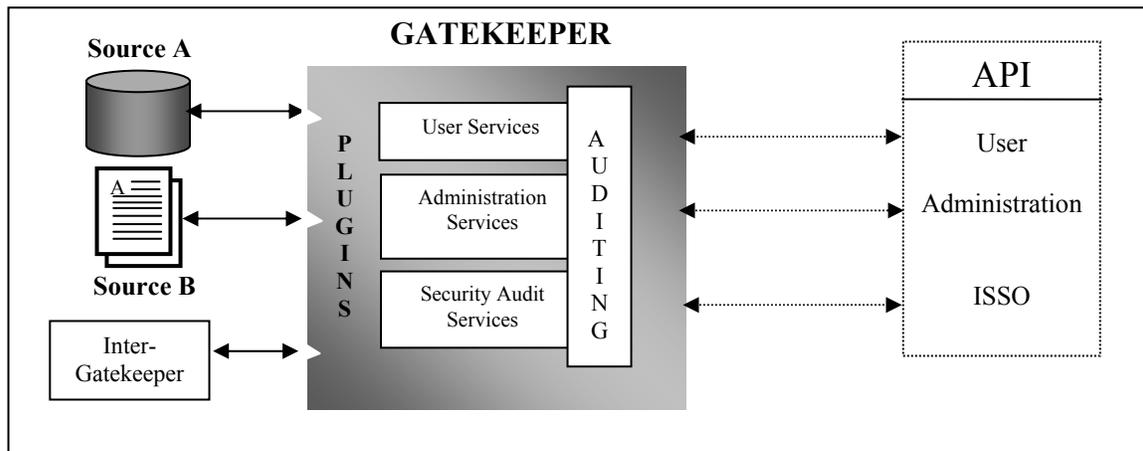


Figure 1.1 The Overall Gatekeeper Architecture

1.2.1.1 User Services

The Gatekeeper provides support for the processing of user requests, collating the results, delivering products and converting/compressing supported imagery. User requests can be 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 Services portion of the interface.

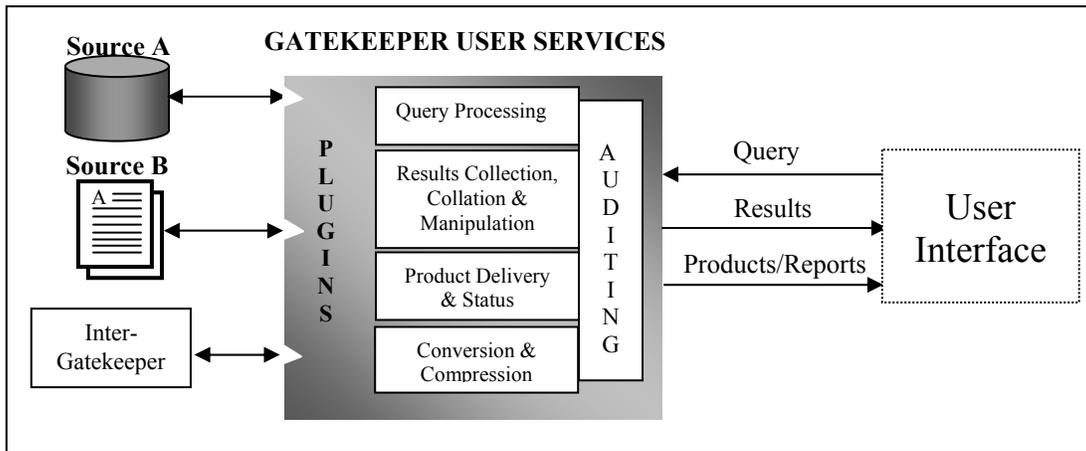


Figure 1.2 User Services

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.

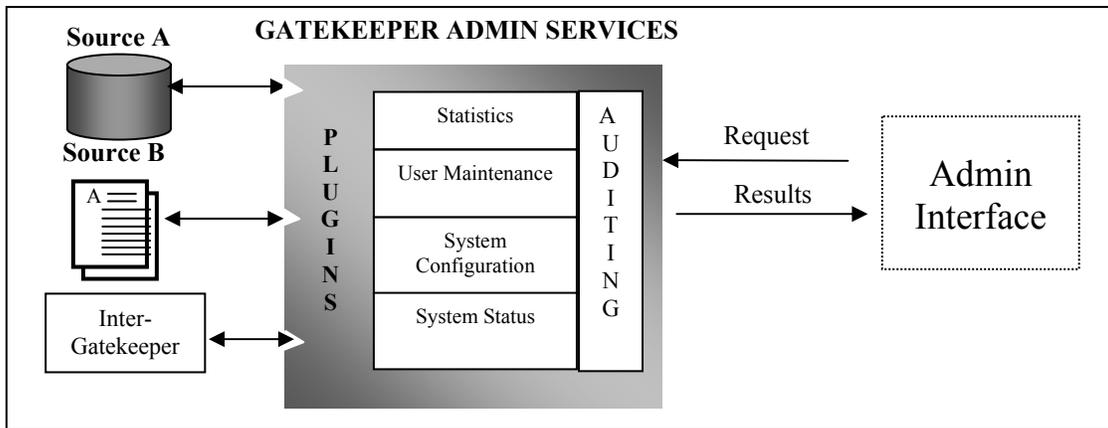


Figure 1.3 Admin Services

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.

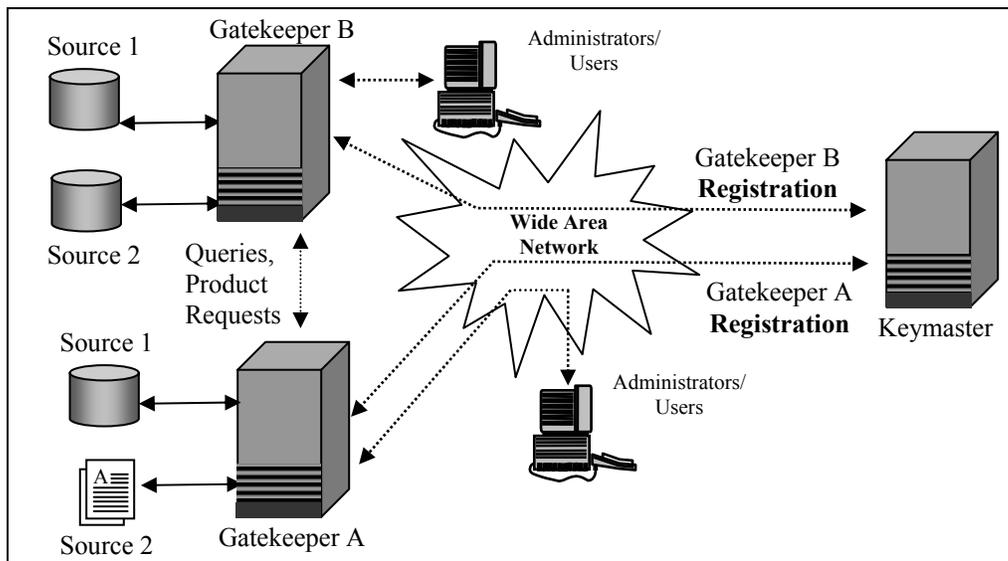


Figure 1.4 Gatekeeper/Keymaster Architecture

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.

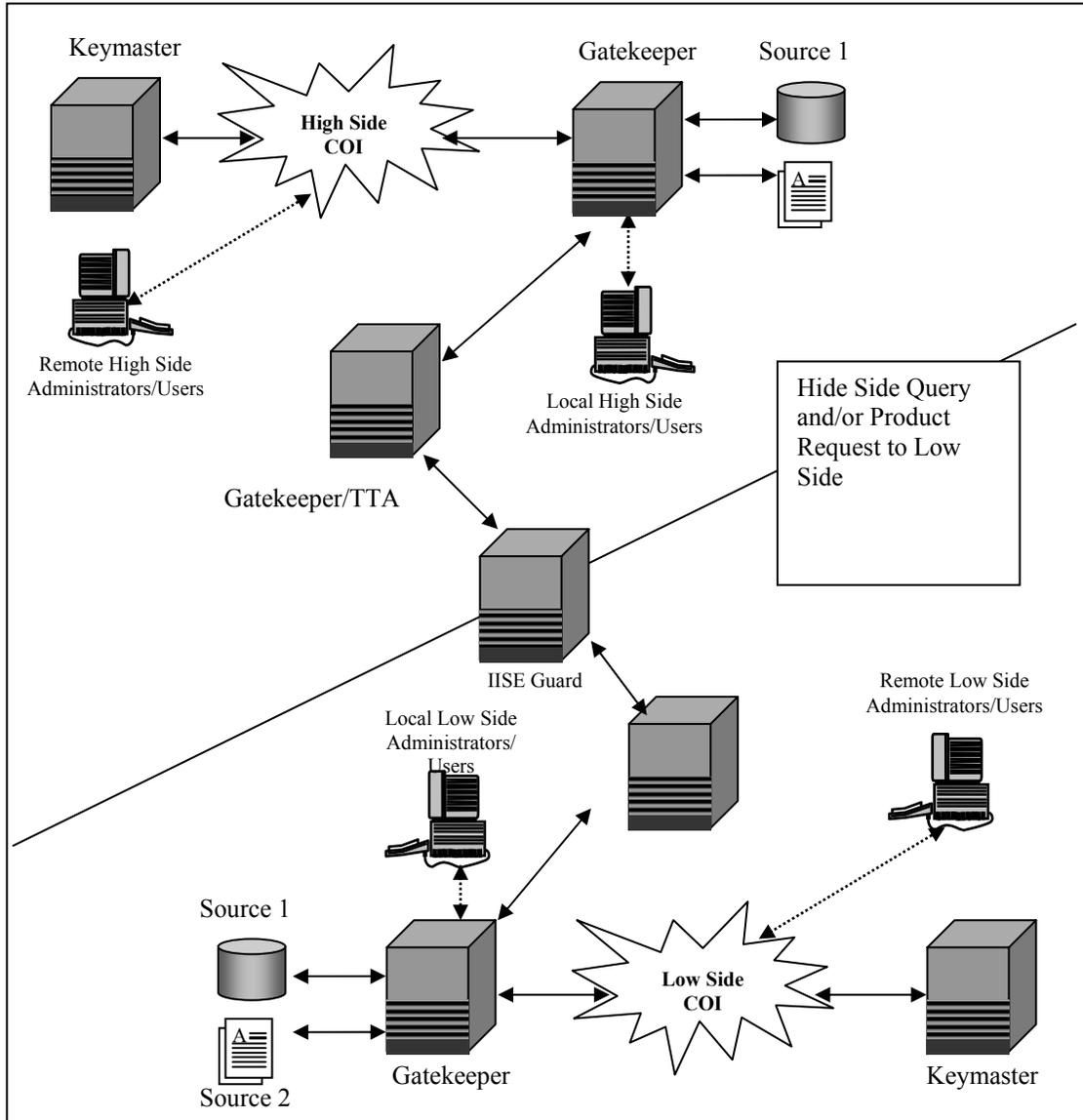


Figure 1.5 Overall TTA/Gatekeeper Architecture

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 on all information passing from high to low and low to high through the TTA. Immediately after receiving a message from either the high side or low side Broadsword interfaces TTA assigns a Message Digest 5 (MD5) integrity seal and passed between TTA processes or passed through the ISSE Guard the MD5 integrity on attaches that 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 v3.1 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.

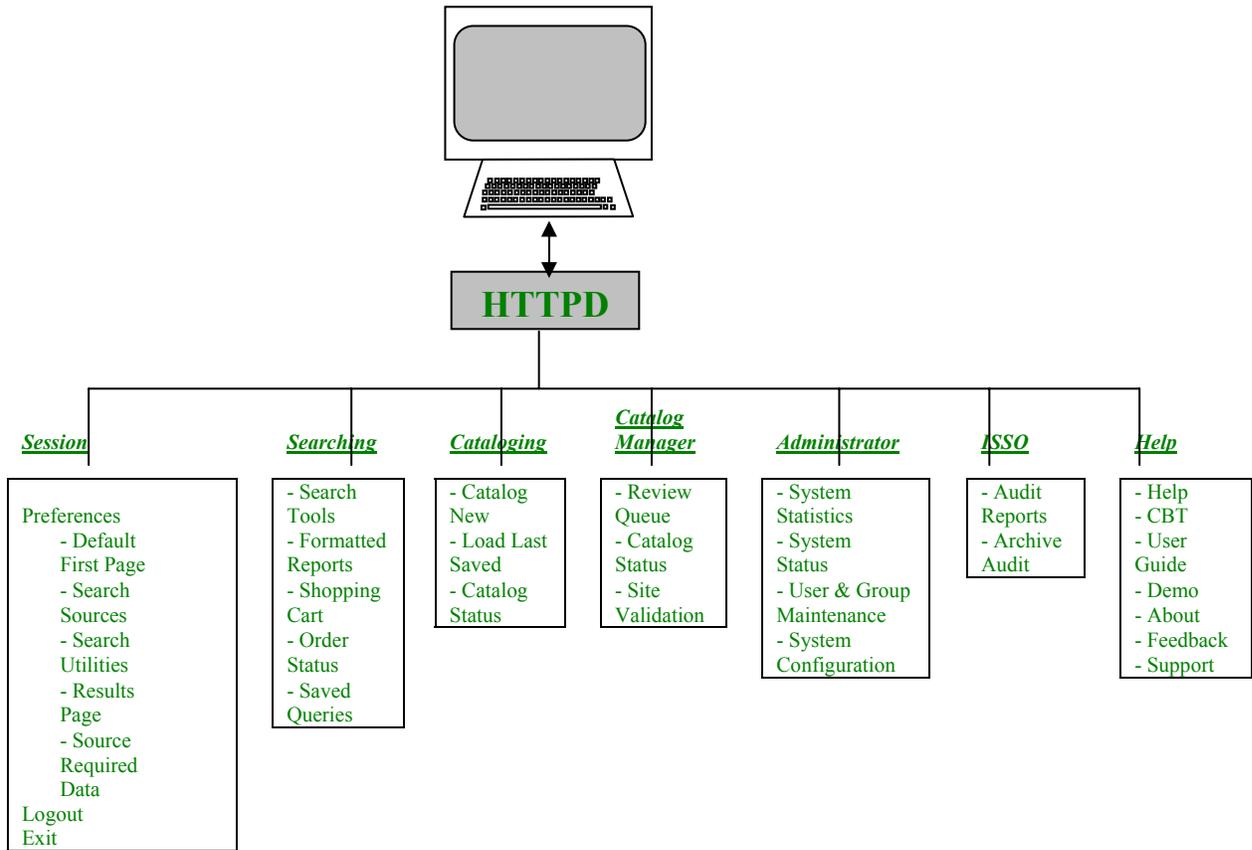


Figure 1.6 User Interface Architecture

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.

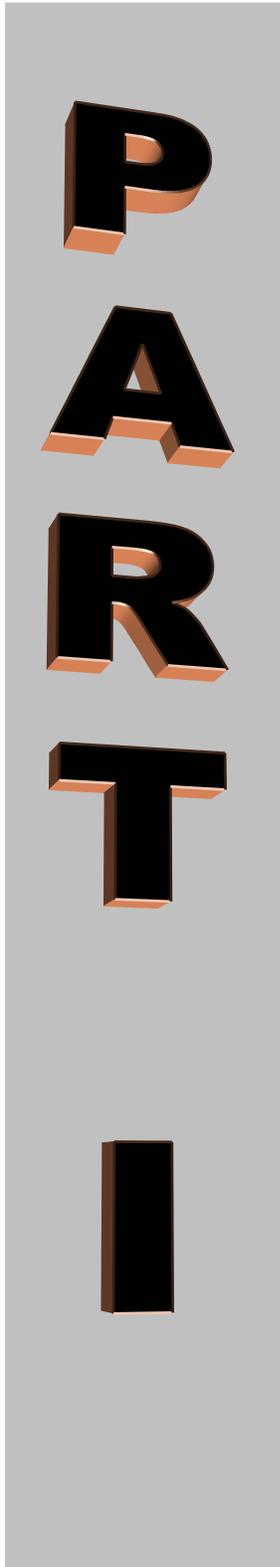
1.2.4.5 Certification Boundary

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
 - Gatekeeper Configuration
 - Client Configuration
- Confirming Installation Choices
- Installation Progress
- Installation Verification

Client Requirements

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 11.9.2• Solaris 2.6 for TTA Gatekeepers (only)• Solaris 7 for Broadsword Gatekeepers (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 (for BSWD Gatekeepers only)• X-Window Environment• Flash Shockwave Player 5 to use the Computer Based Training.• IONA Orbix 3.3.2 (only necessary if system will interface with IPL 3.0)	<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 superceded 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.

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 Broadsword 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 Broadsword 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 Broadsword 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/bswd3.0/etc/bswd_settings` file to determine the devices currently in use. This file contains configuration information from the previous installation of Broadsword. Using this information, you can then verify that these devices are sized appropriately.

➤ For new systems that are co-hosted with another application (e.g. IPL) 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 (e.g. IPL) and do NOT share a dataserver, it is necessary to allocate space for a master device, sysprocs device, or temp device.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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 Gatekeeper) 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 Gatekeepers that are co-hosted with an IPL and share a dataserver the UNIX filesystem used by Sybase should be owned by user *sybipl* with group set to group *sys*.

Note: For existing Broadsword Gatekeepers, 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 755 /syb_devices_0
chmod -R 755 /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 755 /syb_devices_2
chmod -R 755 /syb_devices_3
```

2 Verify directories and determine available disk space

The standard location for Broadsword is in either the `/opt/bswd3.1` or the `/h/bswd3.1` 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'/bswd3.1
```

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 Gatekeeper 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/bswd3.1  
chmod 755 /big_opt/bswd3.1  
ln -s /big_opt/bswd3.1 /opt/bswd3.1
```

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

```
ln -s /h/bswd3.1 /opt/bswd3.1
```

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 Broadsword group

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

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 Broadsword system administration user (*bswduser*)

Broadsword requires the creation/existence of a system administration account, named *bswduser*, with its primary group set to the Broadsword 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 Broadsword group)**
- Comment/Full Name: **Broadsword Administrator Account.**
- Login Shell: **csh**
- 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

Identify/create Broadsword CDIM User (*cdimuser*)

The Cognitive Desktop Information Manager account, *cdimuser*, is used primarily for profile notification operations and batch jobs.). 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 cdimuser<cr>
ypcat passwd|grep cdimuser<cr>
niscat passwd.org_dir|grep cdimuser<cr>
```

If *cdimuser* 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 provides as samples. Actual values should be consistent with site configuration and security policy.

- User Name: **cdimuser**
- User ID: **1001 (or as designated by the site system administrator)**
- Primary Group/Group ID: **600 (must be gid of Broadsword group)**
- Comment/Full Name: **Broadsword Profile Manager**
- 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`/cdimuser**
(Not for use with AFDI)
 - /h/USERS/`hostname`/cdimuser**
(Used with AFDI only)

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

8 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.

9 Allow X Server connections

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

- For a Gatekeeper 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 Gatekeeper 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 Gatekeeper functionality.

10 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.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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 timeserver, 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.

11 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.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Field Number	Field Name	Your Answer	Description
8	Sybase Dataserver Name		The dataserver name to create or share for Broadsword Sybase server (Default: BSWD31 <hostname> SVR).
9	Sybase Dataserver Port Number		UNIX port to be used by the Broadsword Sybase server. Asked only if creating a new dataserver (Default: 2504).
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: 2654).
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.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Field Number	Field Name	Your Answer	Description
			Note: Do not include the device filename (e.g. Bswddata.dev) at the end of the path. The filename will be added automatically.
18	Broadsword Data Device Size		Size to make the Broadsword database (Default: 2000 MB).
19	Broadsword Log Device Path		System location to place Broadsword database transaction log. Can either be a raw device (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	Broadsword Segment Device Path.		System location to place Broadsword Segment device. 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 bswd31user)	(don't write here)	Sybase Password to use for the new audit database (user bswd31user). Must be at least 6 characters in length.
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	Interface with IPL 3.0?		Answer "Yes" to configure IPL 3.0 as a local backside source to THIS Broadsword.
26	Path to IONA Orbix software on THIS machine		Only applicable if interfacing to a local IPL 3.0 (Default: /opt/iona).
27	Existing IPA/IPL on this machine?		Click "Yes" if there is a co-located IPA or IPL 1.0 on THIS server.
28	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).
29	Installation Type		Type of install (Choices: Standard Broadsword, TTA Low, or TTA High).
30	Implement Interface using SSL?		Whether to use Secure Socket Layer (SSL) encryption protocol between web daemon (HTTPD) and web browser (Default: Yes).
31	Protected HTTP port #		UNIX port to be used by the Protected HTTP daemon (Default: 80).
32	Protected HTTP port # (SSL)		UNIX SSL port to be used by the Protected HTTP daemon. Asked only if SSL is used (Default: 443).
33	Network host machine is on		Network type host machine is connected to (Choices: SIPRNET, JWICS, or Internet) (Default:

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Field Number	Field Name	Your Answer	Description
			SIPRNET).
34	Additional network classification label (optional)		Any additional caveats or compartments that should be added to the security banner (i.e. SI/TK). Default: Blank
35	Classification of TTA Low Side System		Please consult the site ISSO for the value to use for this parameter. This parameter specifies the security classification level at which the TTA Low Side system is operating.
36	Group Name		UNIX group to use for Broadsword. Default: bswd.
37	Broadsword Homepage Logo Image File		Site chosen image to be displayed in upper left corner of Broadsword homepage. Must be path to a GIF or JPEG image; recommended size 159x150 pixels. For no logo (default), just leave blank.
38	Log Rolling Count		Number of previous Broadsword log files to keep and archive (as compressed tar files), for example, if set to 10 (default), only 10 will be kept and the oldest will be overwritten.
39	Activate Cataloging Capability?		Click Yes if this server will be used for imagery production purposes (cataloging to an IPL 1.x/2.x) (Default: No).
40	System Admin Name		System Administrator name (MANDATORY).
41	System Admin Branch		System Administrator branch (MANDATORY).
42	System Admin Organization		System Administrator organization (MANDATORY).
43	System Admin Organization Unit		System Administrator organization unit (MANDATORY).
44	System Admin Address1		System Administrator address (MANDATORY).
45	System Admin Address2		System Administrator address (MANDATORY).
46	System Admin Phone		System Administrator UNCLASSIFIED phone number (MANDATORY).
47	System Admin FAX		System Administrator FAX (MANDATORY).
48	System Admin E-mail		System Administrator E-mail (MANDATORY).
49	System Admin City		System Administrator City (MANDATORY).
50	System Admin State/Locality		System Administrator State/Locality (MANDATORY).
51	System Admin Country Code		System Administrator Country Code (MANDATORY).
52	ISSO Name		ISSO name.
53	ISSO Branch		ISSO branch.
54	ISSO Organization		ISSO organization.
55	ISSO Address1		ISSO address.
56	ISSO Address2		ISSO address.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Field Number	Field Name	Your Answer	Description
57	ISSO Phone		ISSO UNCLASSIFIED phone number.
58	ISSO Fax		ISSO fax number.
59	ISSO Email		ISSO email address.
60	Intelink Site Info Manager Name		Intelink Site Information Manager name.
61	Intelink Site Info Manager Branch		Intelink Site Information Manager branch.
62	Intelink Site Info Manager Organization		Intelink Site Information Manager organization.
63	Intelink Site Info Manager Address1		Intelink Site Information Manager address.
64	Intelink Site Info Manager Address2		Intelink Site Information Manager address.
65	Intelink Site Info Manager Phone		Intelink Site Information Manager UNCLASSIFIED phone number.
66	Intelink Site Info Manager Fax		Intelink Site Information Manager fax number.
67	Intelink Site Info Manager Email		Intelink Site Information Manager email address.
68	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 basic server software. Do not proceed unless you have completed Chapter 2 first. This chapter covers a full install for a new Broadsword or TTA Gatekeeper, a full install **with** import for an existing Broadsword Gatekeeper, and a full install **without** import for co-hosting Broadsword 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
- Uninstalling the System (Current or Previous Version)

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-->3.1). The full installation option must be selected even for an existing Broadsword Gatekeeper. However, the installer can still import various items from the previous Broadsword version (i.e. Users' preferences, Cataloging Templates, Profiles, Data Elements, and Backside sources) by selecting the "import" option. If unsure whether an upgrade is possible, select the Upgrade option and the setup script will automatically determine whether an upgrade is possible.

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

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.

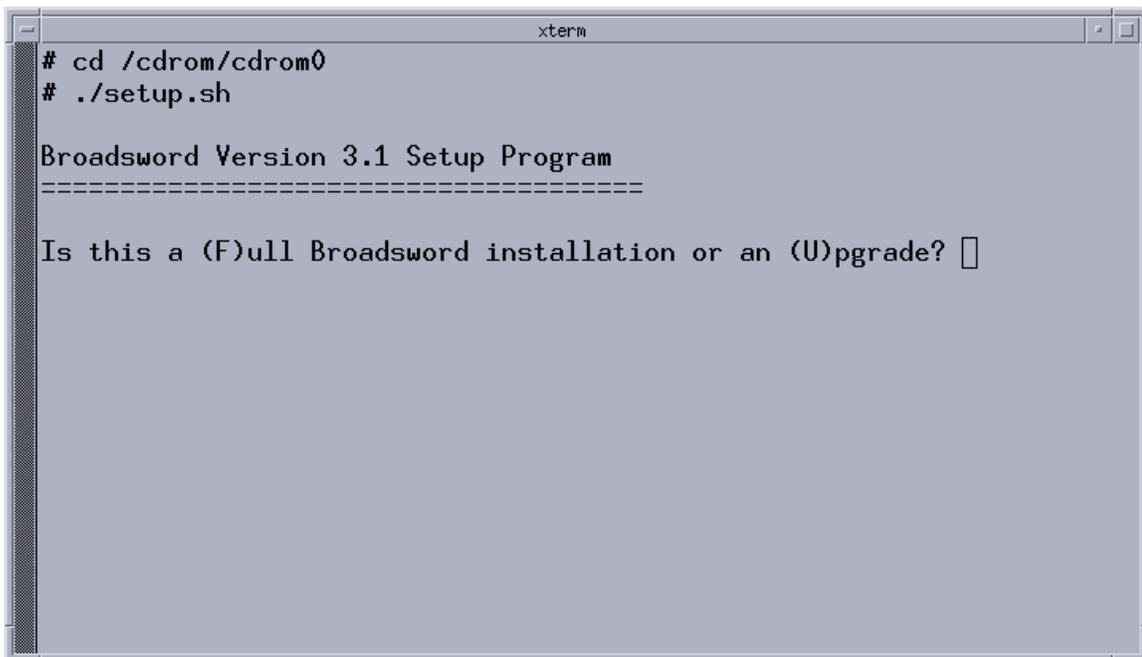
2 Insert the Broadsword installation CD into the CD-ROM drive.

```
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.



```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

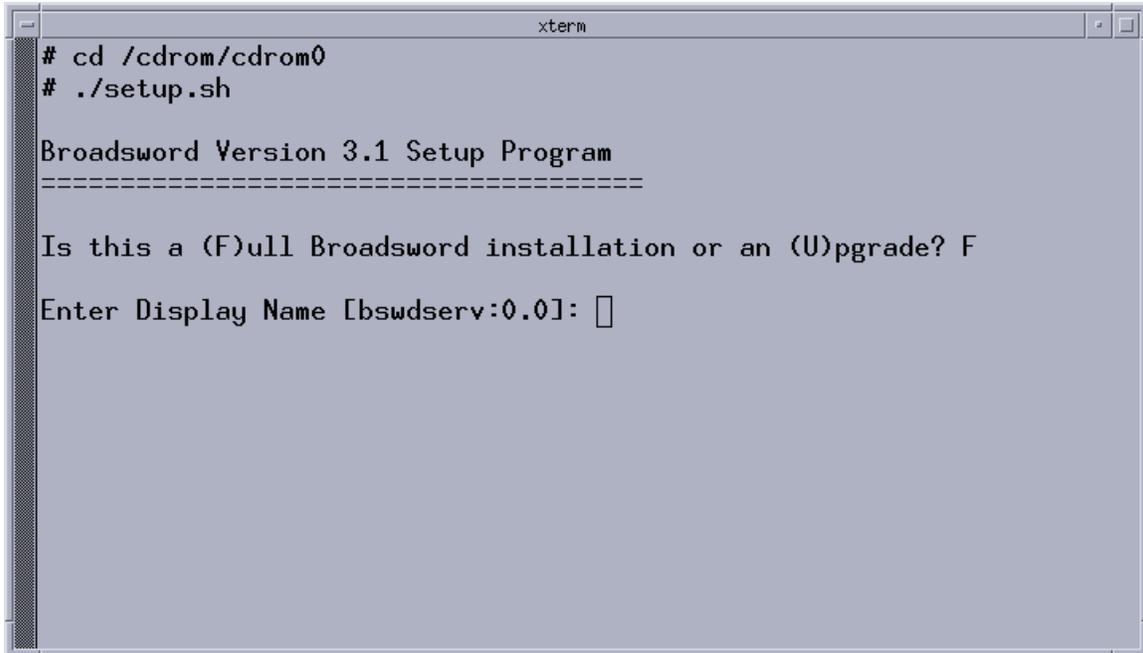
Broadsword Version 3.1 Setup Program
=====
Is this a (F)ull Broadsword installation or an (U)pgrade? [ ]
```

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 3.1. 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.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL



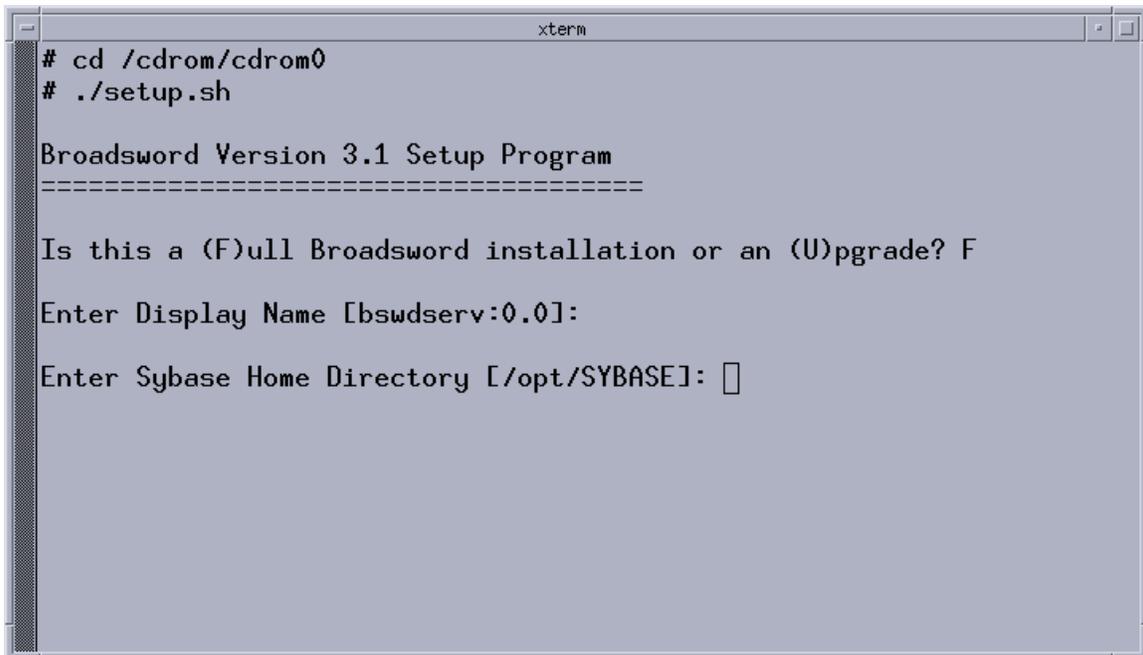
```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

Broadsword Version 3.1 Setup Program
=====

Is this a (F)ull Broadsword installation or an (U)pgrade? F
Enter Display Name [bswdserv: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.



```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

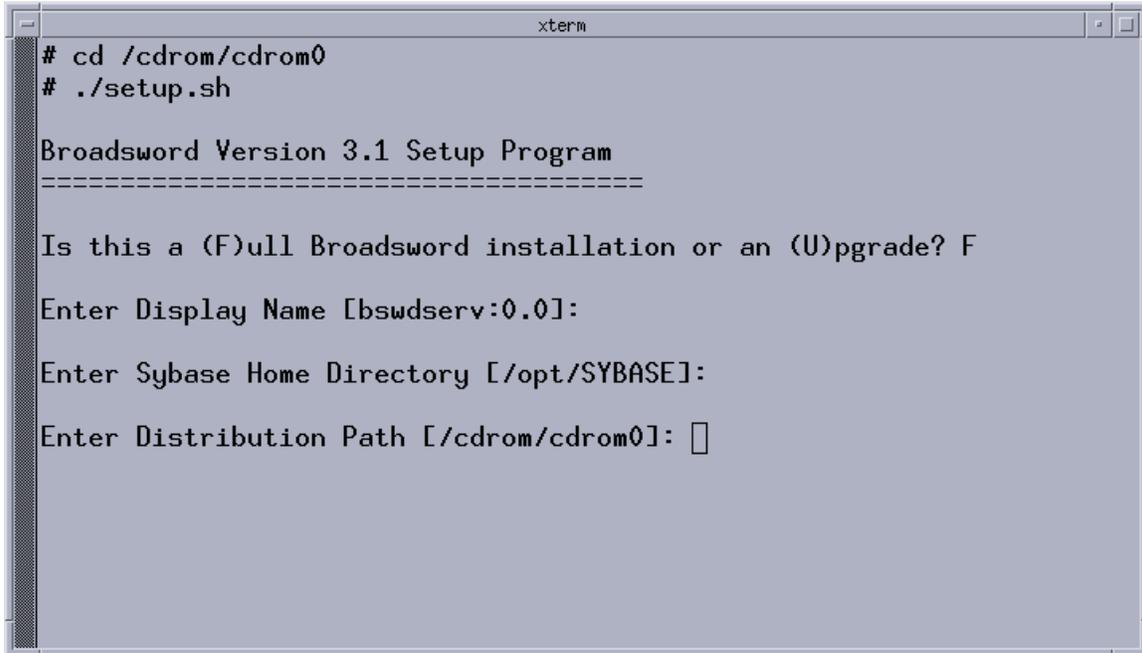
Broadsword Version 3.1 Setup Program
=====

Is this a (F)ull Broadsword installation or an (U)pgrade? F
Enter Display Name [bswdserv:0.0]:
Enter Sybase Home Directory [/opt/SYBASE]:
```

Figure 3.3 – Setup Script (Sybase directory)

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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.



```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

Broadsword Version 3.1 Setup Program
=====

Is this a (F)ull Broadsword installation or an (U)pgrade? F

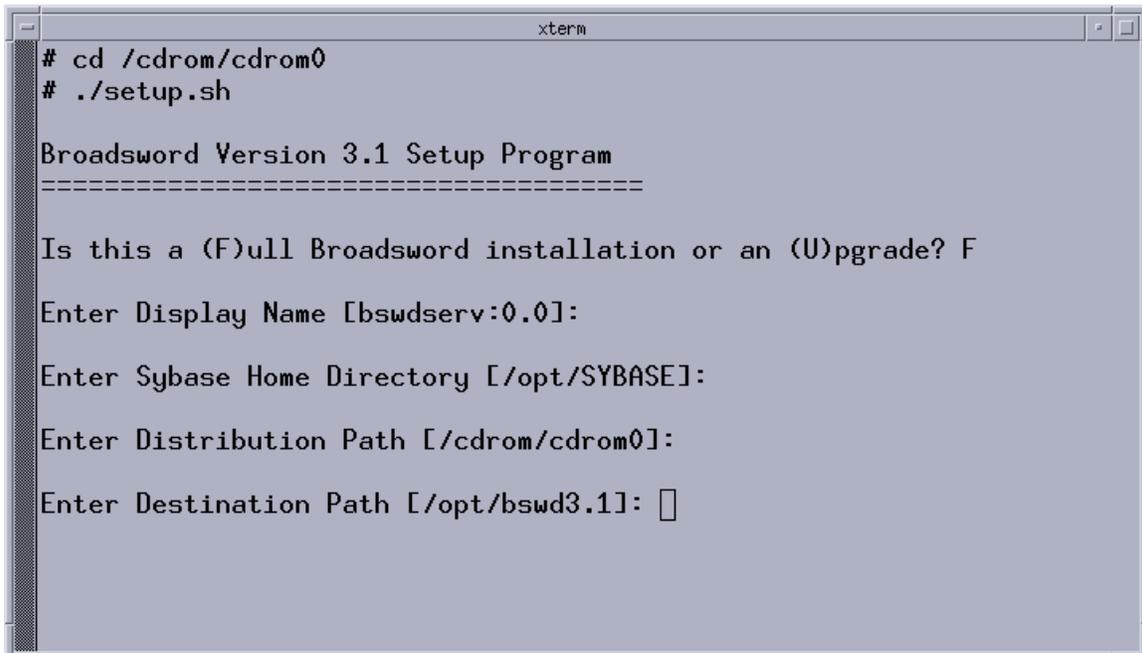
Enter Display Name [bswdserv:0.0]:

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.



```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

Broadsword Version 3.1 Setup Program
=====

Is this a (F)ull Broadsword installation or an (U)pgrade? F

Enter Display Name [bswdserv:0.0]:

Enter Sybase Home Directory [/opt/SYBASE]:

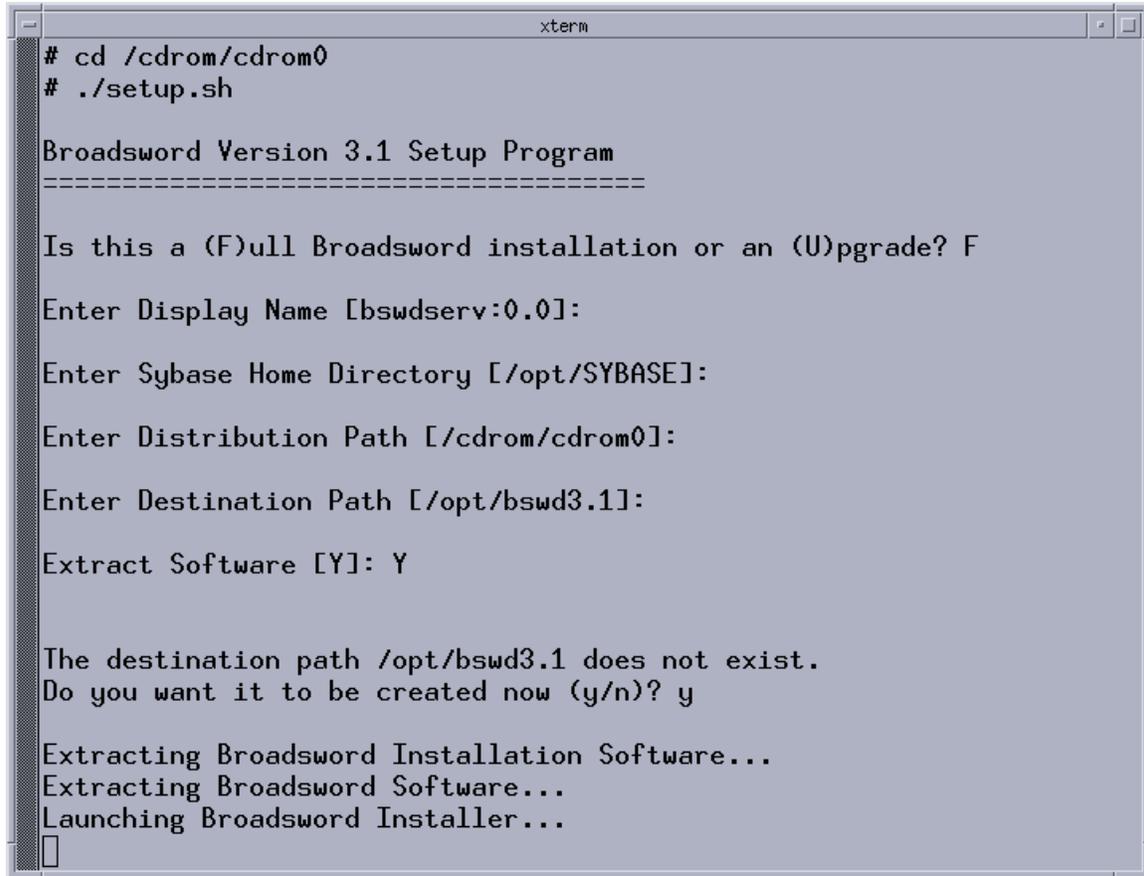
Enter Distribution Path [/cdrom/cdrom0]:

Enter Destination Path [/opt/bswd3.1]:
```

Figure 3.5 – Setup Script (Destination Path)

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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.



```
xterm
# cd /cdrom/cdrom0
# ./setup.sh

Broadsword Version 3.1 Setup Program
=====

Is this a (F)ull Broadsword installation or an (U)pgrade? F
Enter Display Name [bswdserv:0.0]:
Enter Sybase Home Directory [/opt/SYBASE]:
Enter Distribution Path [/cdrom/cdrom0]:
Enter Destination Path [/opt/bswd3.1]:
Extract Software [Y]: Y

The destination path /opt/bswd3.1 does not exist.
Do you want it to be created now (y/n)? y

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

Figure 3.6 – Setup Script 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

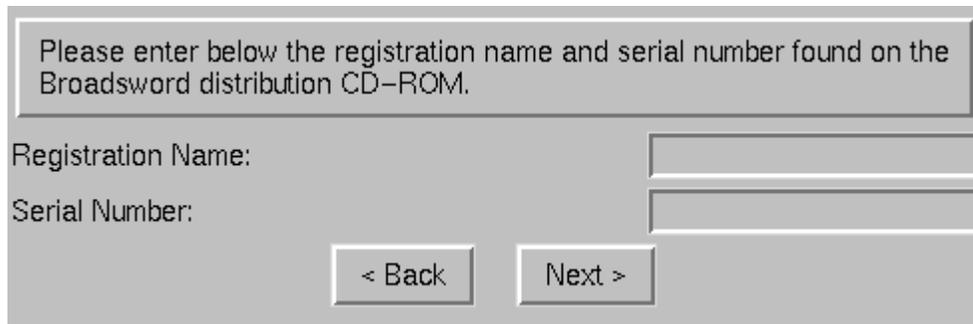


Figure 3.8 - Registration Screen

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

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 the default screen. Sites with existing Broadsword Gatekeepers that wish to import information from the current version should select the “Yes” option. If “No” is selected the import path will be ignored.

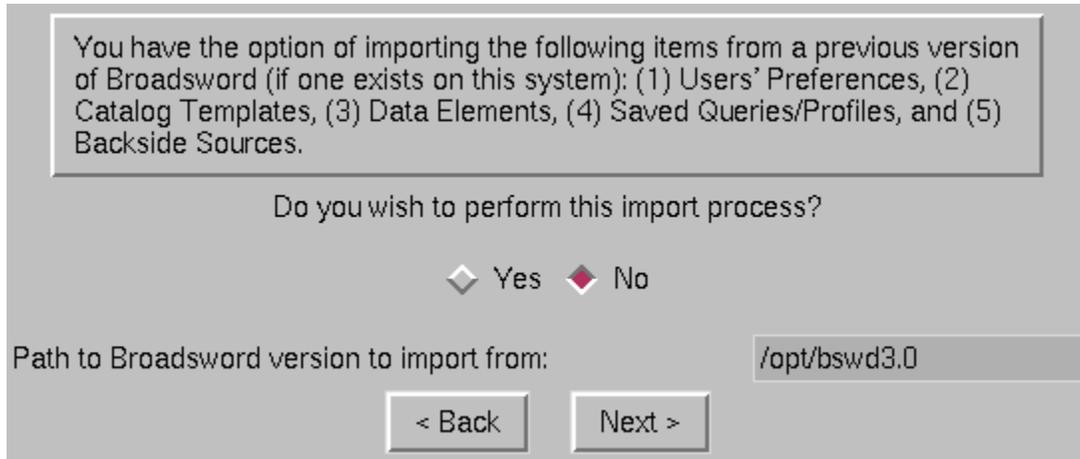


Figure 3.9 - Import Screen

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
```

3.2.3 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 does 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.

3.2.3.1 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 Gatekeeper 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.

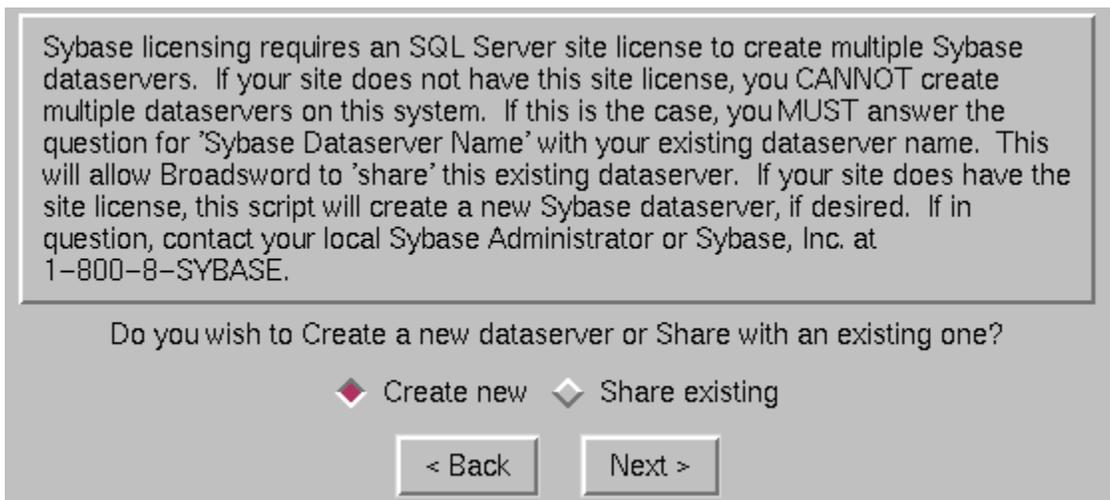


Figure 3.10 - Dataserver Creation Method Screen

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).

Broadsword Dataserver Configuration	
SYBASE Username	sybase
SYBASE Home Directory Path	/opt/SYBASE
SYBASE Dataserver Name to CREATE for Broadsword	BSWD31_BSWDSERV_S
SYBASE Dataserver Port Number to use for Broadsword	2504
SYBASE Dataserver Master Device path	
SYBASE Dataserver Sysprocs Device path	
Create a new SYBASE Backup Server?	<input checked="" type="radio"/> Yes <input type="radio"/> No
SYBASE Backup Server Port #	2654

< Back Next >

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 depicts the initial screen.

Figure 3.13 - Initial 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 the initial screen.

Figure 3.14 - Sample Database Configuration Screen

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.
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 bwd31user)	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 Gatekeeper.

Skip to section 3.2.4 to proceed with the installation.

3.2.3.2 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.

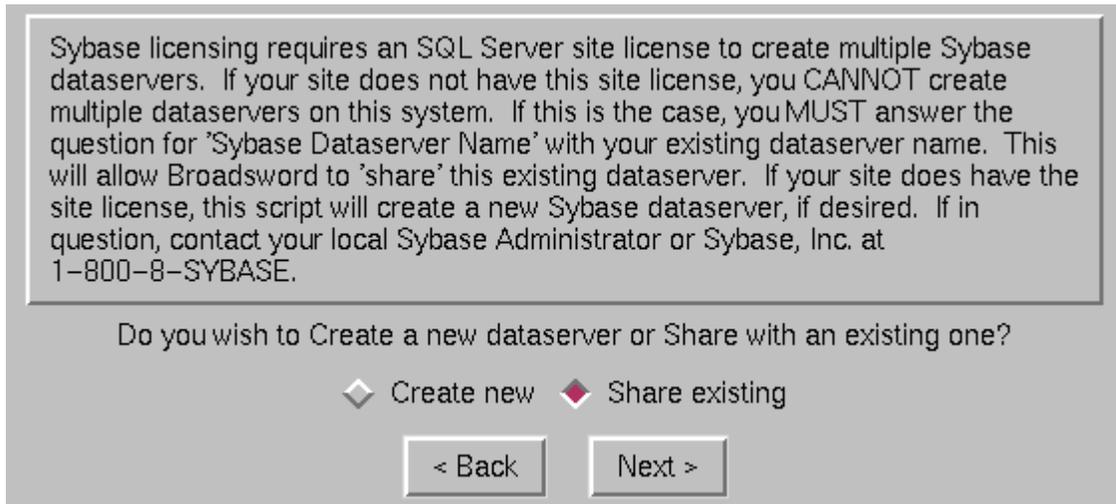


Figure 3.15 - Sharing an Existing Dataserver Screen

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.

Broadsword Database Configuration	
SYBASE Username	sybase
SYBASE Home Directory Path	/opt/SYBASE
SYBASE Dataserver Name to SHARE for Broadsword	BSWD31_BSWDSERV_S
SYBASE Administrator Password for dataserver	
Administrator Password again (for Validation)	
Broadsword Data Device Path	
Broadsword Data Device Size (mb)	2000
Broadsword Log Device Path	
Broadsword Log Device Size (mb)	500
Broadsword Segment Device Path	
'bswd31user' Database Account Password to Set	
'bswd31user' Database Account Password again (for Validation)	

< Back 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 files 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).
Segment Device Path	Path EXISTS AND is writable by the Sybase User entered earlier.
Sybase Database Account Password to set (user bswd31user)	Installer enters it twice AND length is at least 6 characters.

Table 3.4 - Fields Validated

3.2.4 Gatekeeper Configuration

The next part of the installation process is to provide information necessary to configure the Gatekeeper. This section provides the initial login (always 'bswduser') and password for the administrator to log into the interface and further configure the system. It also identifies whether the system will interface with an IPL 3.0 or 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 initial Broadsword Gatekeeper Configuration Screen.

Figure 3.18 - Broadsword Gatekeeper 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.
IONA Orbix S/W Path	File <Path Entered> EXISTS. Only required if "interface with an IPL 3.0 with this machine" is selected (Y).
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

3.2.5 Client Configuration

After clicking on the “Next” button the configuration information is processed and validated. If successful, the installation process will continue with the configuration of 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.

Broadsword Client Configuration

Implement Interface using SSL? Yes No

Note: SSL mandatory for interaction with TTA

Broadsword Client HTTP Port #

Broadsword Client HTTP Port # (SSL)

Network this machine is on SIPRNET JWICS Internet

Additional network classification label or caveat (optional)

Security Classification of TTA Low Side system

Note: Low Side Class mandatory for interaction with TTA

System Group Name to use

Homepage Logo file to use (optional)

Log Rolling Count (0 to disable log rolling)

Activate Cataloging capability? Yes No

Figure 3.19 - Broadsword Client Configuration Screen

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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.
SIPRNET Broadsword Program Office IP Address	If Network Type selected is SIPRNET, this field cannot be empty.
Security Classification of TTA Low Side System	Please consult the site ISSO for the value to use for this parameter. This parameter specifies the security classification level at which the TTA Low Side system is operating. High side Broadsword users are able to generate requests containing query statements. When low side sources are specified, these requests must be transferred electronically from the high side security domain, across the security boundary, to the low side security domain. Immediately prior to this occurring, the user is presented with the TTA Query Verification window in which they are asked to confirm that they have reviewed the contents of the query and that the contents are, in fact, releasable to the security classification of the low side domain. The value entered for this parameter appears in the message displayed in TTA Query Verification window.
System Group Name	Group name EXISTS on system.
Homepage Logo File	File entered EXISTS AND has gif, jpg, or jpeg extension.
Log Rolling Count	Must be greater than or equal to zero.

Table 3.6 Fields Validated

3.2.6 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 3.21 provides the initial point of contact information screen.

The screenshot displays a web form titled "Point of Contact Information" with a purple header. It is divided into three main sections:

- System Administrator:** A section with a note "Note: These fields are mandatory:" and ten input fields: Name, Branch, Organization, Organization Unit, Address1, Address2, Phone, FAX, Email, and City. The State/Locality field is empty, and the Country Code field contains "US".
- ISSO:** A section with seven input fields: Name, Branch, Organization, Address1, Address2, Phone, and FAX. The Email field is empty.
- Intelink Site Info Manager:** A section with seven input fields: Name, Branch, Organization, Address1, Address2, Phone, and FAX. The Email field is empty.

At the bottom of the form are two buttons: "< Back" and "Next >".

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.

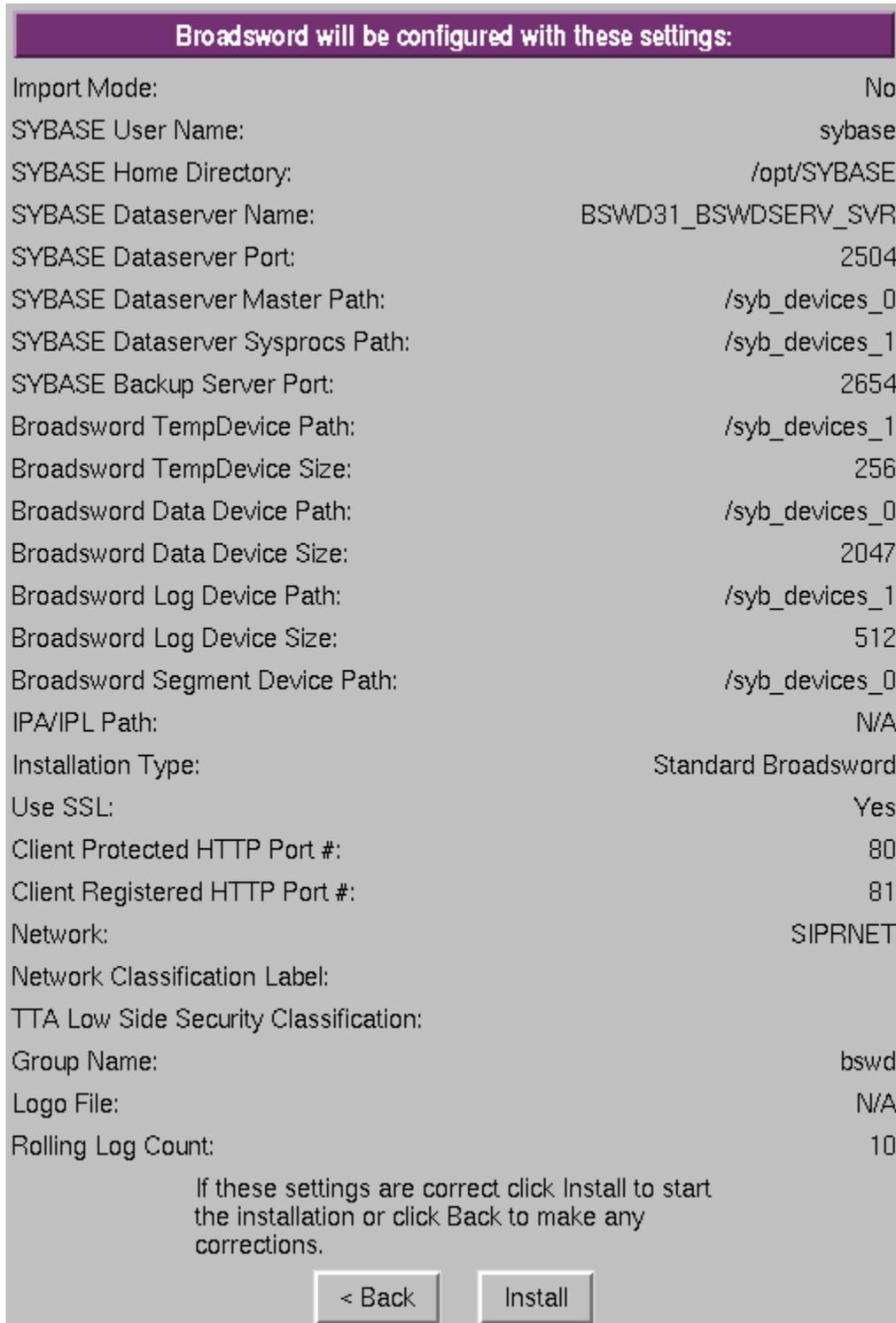


Figure 3.21 Sample Based on New Dataserver Confirmation Screen

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Broadsword will be configured with these settings:

Import Mode:	No
SYBASE User Name:	sybase
SYBASE Home Directory:	/opt/SYBASE
SYBASE Dataserver Name:	SYBASE
Broadsword Data Device Path:	/opt/bswd_test_syb_devices
Broadsword Data Device Size:	100
Broadsword Log Device Path:	/opt/bswd_test_syb_devices
Broadsword Log Device Size:	25
Broadsword Segment Device Path:	/opt/bswd_test_syb_devices
IPA/IPL Path:	N/A
Installation Type:	Standard Broadsword
Use SSL:	Yes
Client Protected HTTP Port #:	80
Client Registered HTTP Port #:	81
Network:	SIPRNET
Network Classification Label:	
TTA Low Side Security Classification:	Secret
Group Name:	bswd
Logo File:	N/A
Rolling Log Count:	10

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.

Broadsword Installation Progress

Progress	Done
<div style="background-color: red; width: 100%; text-align: center; color: white;">100.0%</div>	
Progress	Done
<div style="background-color: red; width: 100%; text-align: center; color: white;">100.0%</div>	

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

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.

```
xterm
->Initialize Install
->Broadsword Dataserver Configuration
->Broadsword Database Configuration
--->Loading Schema
--->Loading Indexes
--->Loading Stored Procedures
->Configuring Broadsword Server
--->Updating Configuration Files
--->Encrypting Configuration Files
->Configuring Broadsword Client
--->Updating Configuration Files
--->Creating SSL Certificates
--->Configuring Homepages
--->Configuring POC Page
--->Installing Logo File
--->Installing Initial Statistics Page
--->Establishing Data Element Configuration
Gkpr Config Files Updated Successfully!
Gkpr Config Files Updated Successfully!
->Starting Broadsword Processes
--->

Default BSWD startup? (Y/N/Q) [Y]: You have chosen the following BSWD startup options:
  Start Sybase ..... Yes
  Start BSWD background APs..... Yes
  BSWD executables..... /opt/bswd3.1/bin
Start these portions of BSWD? (Y/N/Q) [Y]: Starting Sybase...
SYBASE SQL Server is already running

Starting Background APs...
  Starting /opt/bswd3.1/bin/gatekeeper.SVR4
  Starting /opt/bswd3.1/bin/gatekeeperftp.SVR4
  Starting /opt/bswd3.1/bin/gatekeepermrs.SVR4
  Starting /opt/bswd3.1/bin/gatekeepermrs1.SVR4
  Starting /opt/bswd3.1/bin/gatekeepermmsi.SVR4
  Starting /opt/bswd3.1/bin/jivacron
  Starting /opt/bswd3.1/client/bin/conan
Waiting 5 seconds, then tickling MSL...

Broadsword 3.1 Process Status (Tue Jan 22 14:56:40 GMT 2002):

running      /opt/bswd3.1/bin/gatekeeper.SVR4
running      /opt/bswd3.1/bin/gatekeeperftp.SVR4
running      /opt/bswd3.1/bin/gatekeepermrs.SVR4
running      /opt/bswd3.1/bin/gatekeepermrs1.SVR4
running      /opt/bswd3.1/bin/gatekeepermmsi.SVR4
running      /opt/bswd3.1/bin/jivacron
running      /opt/bswd3.1/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

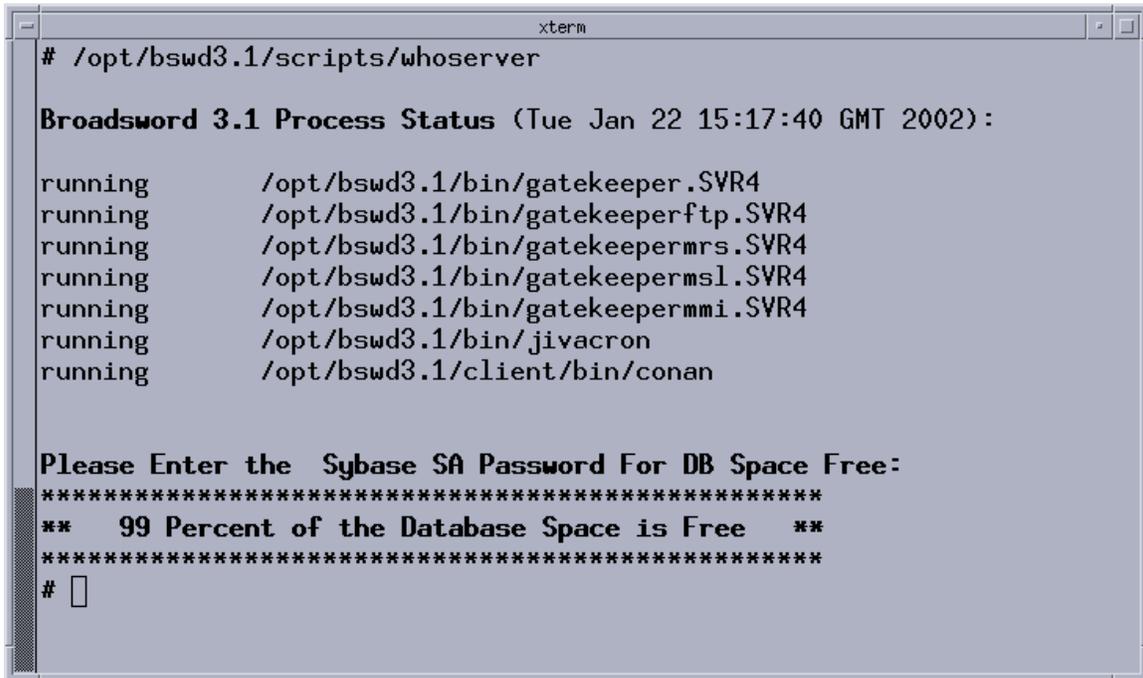
3.5 Installation Verification

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

```
/opt/bswd3.1/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/bswd3.1/logs/install1.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.



```
xterm
# /opt/bswd3.1/scripts/whoserver

Broadsword 3.1 Process Status (Tue Jan 22 15:17:40 GMT 2002):

running      /opt/bswd3.1/bin/gatekeeper.SVR4
running      /opt/bswd3.1/bin/gatekeeperftp.SVR4
running      /opt/bswd3.1/bin/gatekeepermrs.SVR4
running      /opt/bswd3.1/bin/gatekeepermsl.SVR4
running      /opt/bswd3.1/bin/gatekeepermmi.SVR4
running      /opt/bswd3.1/bin/jivacron
running      /opt/bswd3.1/client/bin/conan

Please Enter the Sybase SA Password For DB Space Free:
*****
** 99 Percent of the Database Space is Free **
*****
# 
```

Figure 3.26- Sample Listing of Processes Running

3.6 Restore Sybase Interfaces File

This section is only applicable to Broadsword 3.1 Gatekeepers that were built from existing Broadsword 3.0 Gatekeepers **AND** upgraded from Sybase 11.5.1 to Sybase 11.9.2.

The Sybase interfaces file is built dynamically during the Broadsword installation process. The new `/opt/SYBASE/interfaces` file (for Sybase 11.9.2) does not contain any of the backside source information that was present in the old `/opt/SYBASE_11.5.1/interfaces` file.

Stop the Broadsword server processes:

```
/opt/bswd31/scripts/stopserver
```

Make a copy of the new interfaces file:

```
cp /opt/ SYBASE /interfaces>>/opt/SYBASE/interfaces.ORIG
```

Append the old interfaces file to the new interfaces file:

```
cat /opt/SYBASE_11.5.1/interfaces>>/opt/SYBASE/interfaces
```

Edit the new interfaces file and remove the two entries for the old Sybase data server (e.g. BSWD_hostname_SVR) and backup server (e.g. SYB_BACKUP). Be careful that you do not remove the entries for the new Sybase data server and backup server at the top of the file.

Restart the Broadsword server processes:

```
/opt/bswd31/scripts/startserver
```

3.7 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

Chapter 4

Client Requirements

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

- HTML Browsers
- Image Viewers
- Shockwave-Flash Players
- Document Viewers
- FTP Servers
- Map Data

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.**

4.1 HTML Browsers

Broadsword requires a web browser that supports the HTML 4.0 standard. The system uses JavaScript and hence the JavaScript and cascading style-sheet options need to be on. The interface is best viewed using Netscape 4.7+ 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 Broadsword session, and then return to the login page and connect without retyping one's password. This problem may be circumvented by making sure to exit the browser after logging out, or by clearing the cache after a session. Another option is disabling the cache (see Note below).

When using Netscape, resizing the browser window may cause the current page's data to be lost. The server will respond with a missing form data error. Reloading the form data will not return you to the expected page, since all of Broadsword's pages are created dynamically. In order to solve this problem, the user must enable the memory or disk cache under advanced preferences. This value should be suitably large (1000 K should work). For Netscape, user should, under **Edit -> Preferences -> Advanced -> Cache** select the **Every Time** radio button under the *Document 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 under the **Check for newer versions of stored pages**. A summary of supported HTML browsers is available in Table 4.1.

Operating System	Browser
Solaris 2.6, 7	Netscape v4.7x
Windows 95/98/NT v4.0	Netscape v4.7x, Internet Explorer 4.01 SP2

Table 4.1 - Summary of Supported HTML Browsers

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

The majority of these helper applications have setup utilities that automatically make the browser aware of their existence on PC and Macintosh platforms. However, in some cases, the user can configure the browser manually to make it aware of helper applications.

IMPORTANT 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.

4.2 Image Viewers

To view NITF 1.1, NITF 2.0, TIFF 6.0 and Sun Raster image files an external viewer will be necessary. Listed below are some Image Applications or viewers that can be launched from a browser, their platform, and what formats they handle. A summary of Supported Imagery Viewers is available in Table 4.2.

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

Table 4.2 - Summary of Supported Imagery Viewers

4.3 Shockwave-Flash Players

The Video Clips provided as part of the Online Demonstrations are in Shockwave-Flash format and have both video and audio (with Closed Captioning). To play these video clips you must have a Shockwave-Flash plugin configured with any web browsers on the client machine. A summary of Supported Shockwave Flash Players is available in Table 4.3.

Platform	Application	Notes
UNIX	Shockwave-Flash plugin	Packaged with Netscape Communicator 4.7x or can be downloaded from the CBT CD-ROM by selecting <CDROM>/Plugins/Solaris/Plugin.tgz
Windows	Shockwave-Flash plugin	Packaged with Netscape Communicator 4.7x and Internet Explorer 4.0 SP2 or can be downloaded from the CBT CD-ROM by selecting <CDROM>/Plugins/Windows/Flashiei.exe – for Internet Explorer <CDROM>/Plugins/Windows/Flashnet.exe – for Netscape or <CDROM>/Plugins/Mac/Flash4pl.aye – for Macintosh

Table 4.3 - Summary of Supported Shockwave-Flash Players

4.4 FTP Servers

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

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

4.5 Map Data

Certain CADRG (Compressed ARC Digital Raster Graphics) map data must be loaded in order for Broadsword geographic queries to function properly. Specifically, GNC and JNC (Global Navigation Chart and Jet Navigation Chart) map data for the Northern and Southern hemispheres must be loaded. The Broadsword PMO has received permission from NIMA to distribute GNC/JNC Northern and Southern hemisphere map data and this data is included (on two CD-ROMs) with the Broadsword release set. Refer to the Broadsword 3.1 Trusted Facility Manual (Administrator's Users Guide Attachment) for instructions to load this map data. Additional map data (e.g. ONC, TPC, JOG, TLM) may be loaded at the site's discretion but is not provided with the Broadsword release set.

Chapter 5

TTA Installation

Installation of the Trusted Transfer Agent (TTA) version 1.0.2 requires three dedicated hosts, 1) ISSE Guard, 2) TTA High Side Gatekeeper, and 3) TTA Low Side Gatekeeper. The TTA high side and low side software is installed on top of Broadsword Gatekeeper systems thus the recommended hardware configuration is the same as that required for a typical Broadsword Gatekeeper configuration as described in Chapters 2 through 4.

Installing and configuring the TTA consists of performing the following eight steps:

- 1) Installing and configuring the ISSE Guard System.
- 2) Installing Solaris versions 2.6 on the High and Low Side TTA Gatekeeper platforms.
- 3) Configuring Solaris versions 2.6 on the High and Low Side TTA Gatekeeper platforms.
- 4) Installing and configuring the Sybase DBMS software on the High and Low Side TTA Gatekeeper platforms.
- 5) Installing and configuring the Broadsword Gatekeeper software on the High and Low Side TTA Gatekeeper platforms.
- 6) Installing and configuring the TTA v1.0.2 Software on the TTA High Side Gatekeeper platform.
- 7) Installing and configuring the TTA v1.0.2 Software on the TTA Low Side Gatekeeper platform.
- 8) Modifying the ISSE Guard configuration to allow it to access the High Side TTA Gatekeeper and the Low and High Side TTA Gatekeeper directories.

The following Sections 5.1 through 5.8 provide instructions for accomplishing these eight steps. Additionally, Section 5.9 contains instructions for uninstalling TTA should problems occur during installation that necessitate uninstalling the partially installed TTA software.

Note: Unless otherwise stated, executing the steps in the following sections will require root privileges. The System Administrator responsible for the system should either be present during the installation process, or should provide the installer with the necessary login and password information required to access the root account.

Note: Unless otherwise stated, the steps in the following sections are performed from within the C Shell.

Note: Note that in the following sections specific configuration files are changed and **no** backups of the original file are maintained. Though it is normal recommended practice for system administrator to maintain original copies of all modified configuration files, for security reasons, administrators should not maintain backups of original files on the TTA platforms. This is to ensure that, at some point in the future, an administrator does not inadvertently replace a modified, securely configured version of the file with the original, less secure version, thereby compromising the secure configuration of the TTA platform.

5.1 Installing and Configuring the ISSE Guard System

Due to the secure nature of the ISSE Guard system, installation and configuration of the ISSE Guard platform, operating system, and software is to be performed only by personnel approved by the Designated Accreditation Authority (DAA) for the respective secure computing environment.

Instructions for installing the ISSE Guard are provided in the following document: *Information Support Server Environment (ISSE) Guard Software Installation Guide V3.3*, November 2001, Control No. ISSE-3.3-GSIG-1101-E0. Installation and configuration time for the ISSE Guard when performed by an experienced ISSE Guard installer is approximately three hours.

Note: The installation of the ISSE Guard should be coordinated with the person responsible for installation of the TTA software. The name of the ISSE Guard platform should be noted for future reference. The host names of the High Side TTA Gatekeeper system and the Low Side TTA Gatekeeper system need to be known. Lastly, the directories on the High side and Low side TTA Gatekeeper systems to which the ISSE Guard is to deliver packages need to be collectively agreed upon.

5.2 Installing Solaris Version 2.6

Initial installation of the Solaris 2.6 operating system on the TTA High and TTA Low Gatekeeper platforms consists of the following steps:

- 1) Installation of the Solaris 2.6 operating system
- 2) Installation of all recommended and Y2K patches

The time required to perform these steps is approximately 2 hours.

Solaris 2.6 operating system installation should be performed in accordance with the instructions provided in Appendix D of this report, section *Solaris 2.6 Installation Instructions (excluding Sun Ultra 80)* for non-Ultra 80 platforms, or section *Solaris 2.6 Installation Instructions on Sun*

Ultra 80 for Ultra 80 platforms. TTA exceptions to the standard Solaris installation steps are noted in these sections. Disk partitioning recommendations for TTA Gatekeeper installations are provided in the section *Sample TTA Gatekeeper Disk Partitions*. The time required to perform this step is approximately 1 hour.

Installation of all recommended and Year 2000 (Y2K) Compliancy patches for Solaris 2.6 patches should be performed in accordance with the instructions provided in Appendix D of this report, section *Installing Solaris Patches*. As Sun Microsystems becomes aware of the security related weaknesses and vulnerabilities in their operating systems they make available operating system patches that address those weaknesses and reduce or eliminate the system vulnerability. For this reason, *the single most important step in securing a new or existing installation of the Solaris operating system required for TTA is to install all recommended patches for Solaris 2.6*, as well as any Y2K patches.

If the site uses a default router, instructions for configuring the default router provided in Appendix D of this report, section *Default Router Configuration*, should be followed.

Though Broadsword Gatekeepers can be installed and configured to use AFDI or CSE-SS as described in Chapter 2 and Appendix D, the Defense Intelligence Agency has mandated that CSE-SS and AFDI **not** be installed, configured, or used on the TTA High and TTA Low Gatekeeper platforms.

It has been mandated that the TTA platforms not include extraneous applications or utility software. For this reason the Appendix D instructions for *Installing Solaris Utilities, Automount Configuration, and DNS Configuration* should **not** be executed.

Note: The Solaris 2.6 Operating system is required for operation of TTA 1.0.2 on the TTA High and TTA Low Gatekeeper platforms.

Note: All recommended and Y2K Solaris patches should be installed.

Note: If the site uses a default router, it should be configured.

Note: CSE-SS and/or AFDI are **not** to be installed on the TTA High and TTA Low Gatekeeper platforms.

Note: The *Solaris Utility* package (including GZIP, LSOF, MPEG, TCSH, etc.) *Automount Configuration*, and *DNS Configuration* are **not** to be installed on the TTA High and TTA Low Gatekeeper platforms.

5.3 Configuring Solaris Version 2.6

Since the TTA system works in concert with the ISSE Guard to form a bridge capable of automatically moving information across security domains, it is especially important that the standard Solaris Operating system configurations on which TTA operates be modified to reduce and/or eliminate a variety of known security related system vulnerabilities. This section provides instructions for modifying the Solaris 2.6 operating system prior to TTA installation and

operation. These instructions should be executed, in their entirety, on both the TTA High Gatekeeper and TTA Low Gatekeeper platforms. These recommendations are based on the recommendations provided by the Defense Intelligence Agency and documented in the *Defense Intelligence Agency C2 Security Configuration and C2 Setup Checklist*¹

Note: Due to the extensive modifications made to limit the security related vulnerabilities of the Solaris operating system, reuse of the TTA configured operating system for non-TTA use is not recommended. If the platform is being retired from TTA use, the system administrator should re-install the operating system from Solaris distribution media provided by Sun Microsystems.

The remainder of this section provides a summary description of the security-related Solaris modifications that are performed on the TTA system, followed by the specific instructions for enacting these changes. The following items describe the security-related Solaris modifications:

- Limit the use of the **su** command by creating the group **wheel** and changing ownership to **wheel**.
- Install the Basic Security Module (BSM).
- Remove the **uucp** and **nuucp** users and all files and directories owned by these user ids.
- Force the system to clean up files in **/var/tmp**.
- Remove unnecessary start up scripts in **/etc/rc2.d** and **/etc/rc3.d** including: **S76snmpdx**, **S72autoinstall**, **S30sysid.net**, **S80PRESERVE**, **S73nfs.client** and **S74autofs**.
- Modify the **/etc/init.d/inetinit** file to turn off IP forwarding.
- Modify the **/etc/default/inetinit** file to generate unique-per-connection-id sequence numbers.
- Enforce the "no" router policy.
- Turn off the multicast interface in **/etc/init.d/inetsvc**.
- Remove crontabs for **adm**, **sys**, **lp**, **uucp**.
- Change ownership and permissions on the following control directories to 0755 and owned by root: **/dev**, **/etc**, **/usr/bin**, **/usr/sbin**, **/usr/lib**, **/usr/ucb**, **/usr/dt**, **/usr/openwin**, **/usr/include**.
- Change all files with the ownership of **bin:bin** to **root:root**.

¹ *Defense Intelligence Agency C2 Security Configuration and C2 Setup Checklist*, DRAFT, For Solaris 2.5.1 through Solaris 2.8 Systems, DIA, 2001.

- Add the trace route option to **inetd** so that all incoming connections for the TCP services are logged.
- Add the **-t** option to the audit daemon to close the audit files.
- Disallow the **root** user from ftp'ing by creating the **/etc/ftpusers** file and placing the **root** user id in the file.
- Create a standard DOD access identification file to be printed as a login prompt.
- Reconfigure the **inetd.conf** file so that all unnecessary services are turned off.
- Remove and create **/dev/null** links to obsolete daemon processes including: **in.fingerd**, **in.named**, **in.rexecd**, **in.rlogind**, **in.routed**, **in.rshd**, **in.rwhod**, **in.talkd**, **in.telnetd**, **in.tftpd**, **in.tnamed**, **nscd**, **rpc.bootparamd**, **rpc.nisd**, **rpc.nispasswd**, **rpc.rexd**.
- Create **/dev/null** links for **-- /rhosts**, **/etc/hosts.equiv** and **/.netrc** to protect against trust relationships.
- Provide buffer overflow protection.
- Change ownership to **root:sys** and permissions to **644** on the **/etc/passwd** file.
- Change ownership to **root:sys** and permissions to **400** on the **/etc/shadow** file.
- Add additional logging to the system, routerlog, daemonlog, loginlog, and maillog.
- Reconfigure system auditing to log the following: **lo** (login / logout events), **ad** (administrative actions), **ex** (system calls), **fm** (file modifications), **na** (non-attribute events), **-fr** (unsuccessful file reads), **-fw** (unsuccessful file writes), **-fa** (unsuccessful access of file attributes), **-fc** (unsuccessful file creation), **-fd** (unsuccessful file deletion), **+ot** (everything else).
- Modify security of login sessions to enforce lock out on failed attempts.
- Install TCP Wrappers.
- Install a TCP Wrapped version of Sendmail.
- Install and Configure IP Filtering.
- Modify the **etc/password** file to ensure that all non-login accounts default to **bin/false** for their login shell.
- Set the maximum login attempts allowed to 3.
- Set the **password** on the **root** account.
- Modify **/etc/default/login** to not allow the **root** account to login from the console.
- Set the **eeprom security password**.

The following provides the specific instructions for implementing the above modifications:

1. Login to the Workstation as the “root” user.

Insert the **TTA V1.0.2 Installation CD** into the CD-ROM drive.

2. Open a terminal window and execute the following commands to install the software to be used in subsequent steps. Change the current working directory to the *security_config* directory beneath the directory at which the CD-ROM has been mounted:

```
# cd /cdrom/<CD ROM mount point>/security_config
```

Execute the script to install the files required for security lockdown:

```
# ./install.csh
```

3. Install the GNU GZIP compression utility by executing the following commands:

```
# cd /tmp/c2/GNUzip
```

```
# pkgadd -d gzip-1.3-sol26-sparc-local
```

When prompted to select packages, press the **Enter** key to have “all” packages installed.

If prompted to create “/usr/local” enter **y**, then press the **Enter** key. The GNU GZIP compression utility is now installed.

Note: Though the GNU ZIP utility may already exist at a site, the version distributed on the TTA installation media should be used since it is known to function properly with the TTA installation software.

Install the IP Filter utility by executing the following commands:

```
# cd /tmp/c2/IPFilter/sparc-5.6
```

```
# pkgadd -d ipf-3.4.22-Sol6-sparc-32bit.pkg
```

When prompted to select packages, press the **Enter** key to have “all” packages installed.

The following prompts may be presented during installation of this package:

“Do you want to install these conflicting files [y,n,?,q]”, or

“... Do you want to continue with the installation of <ipf> [y,n,?]”

In either case, an acknowledgement of **y** should be entered and then press the **Enter** key. Any warranty related legal notices or warnings regarding running scripts as super user are normal and should be ignored.

4. In the terminal window, execute the following commands:

```
# cp /tmp/c2/checkbin /usr/local/bin/checkbin
```

```
# chmod 755 /usr/local/bin/checkbin
```

5. In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the **Browse** menu, select the **Groups** option. Under the **Edit** menu, select the **Add...** option to display the Add Group dialog. Add a group with the following attributes.

```
Group Name: wheel
Group ID: 13
Member List: root
```

When the parameters have been entered, select **Ok**, then Under the **Edit** menu, select the **Exit** option to close the admintool.

6. In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the Edit menu, select the **Add...** option to display the Add User dialog. Add users who will serve as System Administrators (not TTA Administrators since they will be created during subsequent steps). For each administrator to be added, set the following attributes.

```
User Name: <User Login Name>
User ID: <Any available UID>
Primary Group ID: staff
Secondary Group Ids: wheel
Comment: SYSTEM ADMINISTRATOR
Login Shell: Bourne
Password: "Normal Password"
Min Change: 1
Max Change: 180
Max Inactive: 60
Expiration Date: <no change>
Warning: 5
Create Home Dir: <Ensure box is checked>
Home Directory: /home/<User Login Name>
```

Note: If users cannot be added due to an error with the `/home/<User Login Name>` directory, select the `/export/home<User Login Name>` directory and retry.

When all System Administrator users have been added, close the **admintool: Add User dialog**, and choose **Exit** under the **File** menu to exit the **admintool**.

Note: Due to limitations in Solaris 2.6, it is necessary to instruct each user to reset their password after they log in successfully the first time. After 180 days each user's password will expire and have to be reset. Each user will be notified 5 days in advance of the password expiration.

Note: You **must** create at least one system administrator account. If there are no accounts with wheel group membership, root access will be unavailable on the system following the next reboot.

7. In the terminal, execute the following command to display the passwd file for editing:

```
# vi /etc/passwd
```

On every line that ends with a ':', add "/bin/false" at the end of the line after the ':

Save the file and exit vi. All system no-login accounts now have /bin/false for a login shell.

8. In the terminal window, execute the following commands to initiate the C2 lockdown script:

```
# cd /tmp/c2
# script c2.log
```

The message "Script started, file is c2.log" is displayed in the terminal window.

9. Perform the following command to execute the C2 script for a TTA installation:

```
# ./c2 TTA
```

Enter 'y' when prompted with "Shall we continue with the conversion now?" Note whether the script runs or doesn't run to completion. The script has run to completion if the following message is displayed:

```
"Successfully completed automated C2 settings. Proceed with the
manual steps."
"Exiting...Done"
```

Note: Warnings regarding /etc/hosts.allow and /etc/defaultrouter are normal and will be resolved during subsequent TTA installation and configuration steps

Press **Control-D** to stop the script session. The message "Script done, file is c2.log" is displayed in the terminal window.

If the "Successfully completed" message mentioned above was displayed, continue with step **Error! Reference source not found.** If the message was **not** displayed, a serious problem was encountered. The installer should note the messages that were displayed by the script, and report the problem to the Broadsword Help Desk awaiting further guidance.

10. The following IP Filter configuration steps will require detailed knowledge of the network onto which the system is being installed. The installer should review the steps below with a qualified System's Administrator to obtain the network parameters required, then perform the following steps to configure IP Filters.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

- a. In the terminal, execute the following command to display the IP filter configuration file:

```
# vi /etc/opt/ipf/ipf.conf
```

- b. At the bottom of the file, locate the group of lines shown below.

```
# block ftp from unwanted hosts
block in proto tcp from !<IPaddr>/<netmask> to any port = 21

# block smtp from unwanted hosts
block in proto tcp from !<IPaddr>/<netmask> to any port = 25

# block smtp submission from unwanted hosts
block in proto tcp from !<IPaddr>/<netmask> to any port = 587
```

- c. If configuring the TTA High Side System, the ISSE Guard needs to be added to the FTP, SMTP, and SMTP sections by substituting the IP address of the High Side of the ISSE Guard for the <IPaddr> parameter and the netmask of the ISSE Guard for the <netmask> parameter in the lines containing “port = 21”, “port = 25”, and “port = 587”.

Thus, to allow FTP, SMTP, and SMTP submission from ISSE Guard host (i.e. IP Address 9.8.7.1, netmask 255.255.255.0) the entries would be updated to resemble that shown below.

```
# block ftp from unwanted hosts
block in proto tcp from !9.8.7.1/255.255.255.0 to any port = 21

# block smtp from unwanted hosts
block in proto tcp from !9.8.7.1/255.255.255.0 to any port = 25

# block smtp submission from unwanted hosts
block in proto tcp from !9.8.7.1/255.255.255.0 to any port = 587
```

If configuring the TTA Low Side System, various sources accessible through Broadsword need to be allowed to send products via FTP to the TTA system. This is done by substituting the IP address of the Low Side network for the <IPaddr> parameter and the netmask of the network for the <netmask> parameter in line containing “port = 21”. Additionally, ISSE Guard needs to be added to the SMTP, and SMTP submission blocks by substituting the IP address of the Low Side of the ISSE Guard for the <IPaddr> parameter the netmask of the ISSE Guard <netmask> parameter in the lines containing “port = 25” and “port = 587”.

For example, to allow FTP from an entire class C network (i.e. IP Address 9.8.7.0, netmask 255.255.255.0), and SMTP, and SMTP submission from ISSE Guard host (i.e. IP Address 9.8.7.1, netmask 255.255.255.0) the entries would be updated to resemble that shown below.

```
# block ftp from unwanted hosts
block in proto tcp from !9.8.7.0/255.255.255.0 to any port = 21
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

```
# block smtp from unwanted hosts
block in proto tcp from !9.8.7.1/255.255.255.0 to any port = 25

# block smtp submission from unwanted hosts
block in proto tcp from !9.8.7.1/255.255.255.0 to any port = 587
```

d. Save and exit the `/etc/opt/ipf/ipf.conf` file.

11. The following configuration steps will need to be performed in order to establish a default domain name for both the TTA Low and TTA High Side systems.

a. Create the `/etc/defaultdomain` file by executing the following command:

```
# vi /etc/defaultdomain
```

Add the default domain name to this file. If you are unsure of the default domain name please consult the System Administrator for this information.

b. Save and exit the `/etc/defaultdomain` file by executing the following command:

```
:wq!
```

12. In the terminal window, execute the following command to edit the login file:

```
# vi /etc/default/login
```

Find the entry in the file matching that shown below:

```
CONSOLE=/dev/console
```

Modify the “CONSOLE” line to match the following:

```
CONSOLE=/dev/null
```

Save the file and exit vi.

13. In the terminal, execute the following command to set an eeprom password:

```
# eeprom security-mode=command
```

If an eeprom password was not already set on the system, you will receive prompts to enter and verify a new password.

If an eeprom password was already set, you will receive no output and will need to execute the following command to change the password:

```
# eeprom security-password=
Changing PROM password:
New password: <password>
Retype new password: <password>
```

14. In the terminal window, execute the following command to reboot the system:

```
# init 6
```

The system is rebooted.

Note: TTA Administrators, ISSOs and ISSMs should be familiar with these operating system modifications so that they can be aware of any possible subsequent modifications that may compromise the various protections afforded by the changes.

Note: The approval to operate TTA is contingent upon it running on this locked-down version of the Solaris operating system. These capabilities and services should not be changed by the TTA system administrator without prior coordination and approval of the Broadsword DODIIS Executive Agent (DExA): AFC2ISRC/A-264, 130 Andrews St., Suite 205, Langley AFB, VA 23665 Comm.(757) 225-1137 or DSN 575-1137 and the Broadsword/TTA/ISSE Guard Program Management Office, AFRL/IFEB, 32 Brooks Road, Rome, New York, Phone (315) 330-3638 or DSN 587-3638.

5.4 Installing and Configuring Sybase DBMS Software

In preparation for installing and configuring the Broadsword Gatekeeper Software on the TTA platforms, the Sybase DBMS software needs to be installed and configured. This installation should be performed in accordance with established Broadsword instructions as described in Appendix D of this report, section *Installing Sybase Adaptive Server 11.5.1 or 11.9.2*. The time required to perform this step is approximately 1 hour.

5.5 Installing and Configuring Broadsword Gatekeeper Software

Prior to installing TTA software on the TTA platforms, standard Gatekeeper processes need to be installed and configured on both the High and Low sides. This installation should be performed in accordance with established Broadsword instructions as described in Chapters 2 through 4 of this report. The time required to perform this step is approximately 1 hour.

Additionally, since Gatekeeper is configured and tested via a web interface, installation of the Netscape Communicator application should be performed in accordance with the instructions provided in Appendix D of this report, section *Installing Netscape Communicator 4.76*. The time required to perform this step is approximately 15 minutes.

5.6 Installing and Configuring TTA High Gatekeeper Software

The following describes the steps required to install and configure the TTA software on the High Side TTA Gatekeeper system. These steps are to be executed in their entirety by the TTA installer. The time required to perform this step is approximately 1 hour.

Additionally, since the Field Level Filter Administration Tool (FLFAT) is dependent upon the Java Runtime Environment (JRE) v 1.3.1, installation of the JRE v1.3.1 should be performed in accordance with the instructions provided in Section D of this report, section *Installing the Java Runtime Environment (JRE) v 1.3.1*. The time required to perform this step is approximately 15 minutes.

5.6.1 Installing TTA High Gatekeeper Software

Approximately 280 MB of free disk space is required for the installation of TTA High Gatekeeper software. If at any time during this sequence the installation process is aborted the partially installed TTA high software should be uninstalled following the steps described in section 5.9.1 of this report before attempting a reinstall.

Note: The System Administrator should confirm that both High and Low side TTA workstations are configured as mail servers, not clients.

Note: The TTA High side workstation must have the Java Runtime Environment (JRE) version 1.3 installed prior to the installation of TTA.

1. If not already booted, boot the High Side TTA System.
2. **If re-installing TTA, proceed to step 5 of this section.** Otherwise, log on as a user with system administration privileges, and then bring up an xterm and su to root.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the **Browse** menu, select the **Groups** option. Under the **Edit** menu, select the **Add...** option to display the Add Group dialog. Add the following three groups with the following attributes.

```
Group Name: tta  
Group ID: <any number greater than 100>  
Member List: <blank>
```

```
Group Name: cgiadmin  
Group ID: <any number greater than 100>  
Member List: <blank>
```

```
Group Name: cgiuser  
Group ID: <any number greater than 100>  
Member List: <blank>
```

When the parameters have been entered, select **Ok**, then under the **File** menu, select the **Exit** option to close the admintool.

Note: All local groups created need to have ids > 100. Consult with the System Administrator for direction with creating these groups and conflicts that might exist.

Note: It is assumed that the *bswd* group already exists as a result of the installing and configuring the Broadsword Gatekeeper software

3. Execute the following steps to create a *ttaadmin* non-login local user account with password. This account provides ownership of the directories and files that are placed on the system during an install.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the Edit menu, select the **Add...** option to display the Add User dialog. Add users who will serve as. For each administrator to be added, set the following attributes.

```
User Name: ttaadmin
User ID: <Any available UID greater than 1000>
Primary Group ID: tta
Secondary Group Ids: cgiadmin,cgiuser,bswd
Comment: TTA NON-LOGIN FTP ACCOUNT
Login Shell: /bin/false
Password: "Normal Password"
Min Change: <no change>
Max Change: <no change>
Max Inactive: <no change>
Expiration Date: <no change>
Warning: <no change>
Create Home Dir: <Ensure box is not checked>
Home Directory: <TTA Install Directory>
```

When the parameters have been entered, select **OK**, then under the **File** menu, select the Exit option to close the admintool.

4. Enable ftp ability for this local account by adding *"/bin/false"* to the */etc/shells* file. Perform the following steps to make the necessary changes to the */etc/shells* file:

```
# cd /etc
```

Edit/Create the *shells* file by performing the following command:

```
# vi shells
```

Add the following lines to the end of the file if they do not already exist:

```
/bin/false
/bin/csh
```

```
/bin/sh
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

5. Execute the following commands to create additional local user accounts that will serve as TTA administrators.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the Edit menu, select the **Add...** option to display the Add User dialog. Add users who will serve as TTA Administrators For each administrator being added, set the following attributes.

```
User Name: <User Login Name>
User ID: <Any available UID>
Primary Group ID: tta
Secondary Group Ids: wheel,cgiadmin,cgiuser,bswd
Comment: TTA ADMINISTRATOR
Login Shell: C Shell
Password: "Normal Password"
Min Change: 1
Max Change: 180
Max Inactive: 60
Expiration Date: <no change>
Warning: 5
Create Home Dir: <Ensure box is checked>
Home Directory: /home/<User Login Name>
```

When the parameters have been entered, select **OK**, then under the **File** menu, select the **Exit** option to close the admintool.

Note: Due to limitations in Solaris 2.6, it is necessary to instruct each user to reset their password after they log in successfully the first time. After 180 days each user's password will expire and have to be reset. Each user will be notified 5 days in advance of the password expiration.

6. Approximately 280 MB of free disk space is required for the installation of the TTA software. Select a location for the TTA software that provides this amount of free space, and as **root** user, create a directory where the High Side TTA v1.0.2 software will be installed. Record the full path to this directory for future reference. Though the installer determines the directory name, in the remaining steps this directory will be referred to as *tta_v1.0.2_high*, and the full path will be referred to as *<full path to tta_v1.0.2_high>*.

7. Enter the following command to change directory to the location where the High Side TTA v1.0.2 software was installed:

```
#cd <full path to tta_v1.0.2_high>
```

Verify the ownership of the **tta_v1.0.2_high** directory as user **ttaadm**n group **tta** and, if necessary, execute the following command to change the ownership of the newly created install directory to **ttaadm**n and the group to **tta**:

```
# chown ttaadm:tta <full path to tta_v1.0.2_high>
```

Verify the permission of the **tta_v1.0.2_high** directory as **777**, and, if necessary, execute the following command to change the permissions of the newly created install directory:

```
# chmod 777 <full path to tta_v1.0.2_high>
```

8. Place the **TTA v1.0.2 Installation CD-ROM** in the system's CD-ROM drive.
9. Change the current working directory to the **tta** directory beneath the directory at which the CD-ROM has been mounted:

```
# cd /cdrom/<CD-ROM mount point>/tta
```

Execute the High Side TTA install script by entering the following command:

```
# ./install.csh HIGH <full path to tta_v1.0.2_high>
```

View the script execution process and provide answers for the following questions listed in table 5.1:

PROMPTS	DESCRIPTION
TTA Gatekeeper Host Name	Host name of the system on which the BSWD/TTA system is being currently installed.
TTA Gatekeeper IP Address	IP address of the system on which the BSWD/TTA system is being currently installed.
TTA Gatekeeper Port	This value is listed in the <i>local.gkpr.conf</i> file located in the <i>\$BSWD_HOME/etc</i> directory. The entry is associated with the <i>GkprIpcPort</i> parameter beneath the <i>RcdName = GkprRcd</i> entry. If unsure of this value, the installer should consult with the Broadsword Administrator to obtain the value.
BSWD User Name	A valid UNIX user that has BSWD administration privileges. Consult the BSWD Administrator for this information.
BSWD User Password	Current password for the valid UNIX user that has BSWD administration privileges identified above. Consult the BSWD Administrator for this information.
BSWD DB User Name	BSWD Database login name. Consult the BSWD

	Administrator for this information.
BSWD DB User Password	Password for the BSWD Database login account described above. Consult the BSWD Administrator for this information.
TTA Non-Login FTP User Name	Enter “ <i>ttadm</i> n” as the “TTA Non-Login FTP User Name”.
TTA Non-Login FTP User Password	Password for the “ <i>ttadm</i> n” account. Consult the acting TTA Administrator for this information.
Explicit path where BSWD was installed	Identifies the explicit path to where the BSWD system has been installed. Consult the BSWD Administrator for this information.
Explicit path where the Java Runtime Environment (JRE) was installed	Identifies the explicit path to where the JRE package has been installed. Consult the System Administrator for this information.

Table 5.1: High Side TTA Configuration Parameters

10. Logout of the root session. Installation of the High Side TTA v1.0.2 software is complete.

5.6.2 Configuring TTA High Side Gatekeeper Software

The following describes the steps required to configure the TTA software on the High Side TTA Gatekeeper system. These steps are to be executed in their entirety by the TTA installer. In these steps, the full path to the TTA Low software, determined in section 5.6.1 step 5 should be substituted wherever the parameter *<full path to tta_v1.0.2_low>* appears.

1. Login to the system as a valid TTA Administrator.
2. Change the current working directory to the *tt*a directory by executing the following command:

```
% cd < full path to tta_v1.0.2_high >/tta
```

3. Set up the appropriate runtime environment by executing the following command:

```
% source ./TTAvars.csh
```

4. Change the current working directory to the binary directory where the TTA applications have been placed by executing the following command:

```
% cd < full path to tta_v1.0.2_high >/tta/bin/<platform>
```

where platform identifies the current version of the operating system (i.e., solaris25, solaris26, solaris27)

5. Execute the TTA Security Monitor to setup and initialize the runtime directories for the TTA System by executing the following command:

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

```
% ./TtaSecMon
```

6. Change the current working directory to the binary directory where the TTA CGI applications have been placed by executing the following command:

```
% cd < full path to tta_v1.0.2_high >/ttaCGI/bin/tta/<platform>
```

where platform identifies the current version of the operating system (i.e., solaris25, solaris26, solaris27)

7. As the “*root*” user, execute the CGI application to setup and initialize the runtime directories for the TTA CGI applications by executing the following commands:

```
# csh
# source < full path to tta_v1.0.2_high >/tta/TTAvars.csh
# ./cgiFixDirs
```

Exit out of the root session.

8. As the TTA Administrator, configure the TTA CGI applications so that they interface to the proper host during the transfer of the TTA packages and that the packages are delivered properly to the systems on the opposite side of the security boundary by executing the following command:

```
% ./cgiAdmin
```

This will present a Graphical User Interface (GUI) to the user for checking and modifying the appropriate values needed for the delivery of TTA packages.

- a. Select the *Workstation Config* button located on the main window.
 - i. The user will be presented with an additional window in which the targeted host will be identified for the transfer of the TTA packages. This host should identify the host name of the Guard platform.
 - ii. If the current host name does not reflect the Guard host, modify the entry in the text field by highlighting the entire contents of the text field and typing in the actual name of the Guard platform.
 - iii. Select the *Access* button next to the host name. The user will be presented with an additional window containing the ftp settings for the TTA Package Send process. Verify that the list contains the following:

```
CGI_FTP_USER=hiftpin
CGI_FTP_PASS=(appropriate passwd)
CGI_FTP_DIR=hiimage
```

- iv. If the ftp settings were changed in step iii, select the ‘Save’ button located at the bottom of the current screen. Select the ‘Exit’ button to exit the ftp settings window.
 - v. If the host name was changed in the step ii, select the ‘Apply’ button located at the bottom of the current screen.
 - vi. Select the ‘Exit’ button to exit the workstation configuration function.
- b. Select the *Environment Config* button located on the main window.
- i. The user will be presented with an additional scrollable window that will contain the current runtime environment for the TTA CGI applications. Of primary focus in this list of environment variables are the *CGI_AUTO_TO* and *CGI_AUTO_REV_MODE* entries.
 - ii. Scroll down through the list of variables until the above variable(s) are shown.
 - iii. Verify, and, if needed, set the value of the *CGI_AUTO_TO* variable to be of the form *ttadmin@<hostname>* where hostname is a valid low side delivery name configured on the Guard system where packages will be delivered containing high to low inter-Gatekeeper messages
 - iv. Verify, and, if needed, set the value of the *CGI_AUTO_REV_MODE* variable to *HIGH* to represent the side on which this TTA system is running.
 - v. If any values were changed in steps iii and iv, select the ‘Save’ button located at the bottom of the current screen.
 - vi. Select the ‘EXIT’ button to exit the environment configuration function.
- c. Select the Exit button to exit the *cgiAdmin* application.
9. Verify that the IP address for the High side of the Guard has been placed in the */etc/hosts* file. As the “*root*” user, view and, if necessary, modify the */etc/hosts* file by executing the following commands:

```
# cd /etc
```

Edit the *hosts* file by performing the following command:

```
# vi hosts
```

If the IP address does not exist in the file, add a line to the file using the following format:

```
<IP address>          <GUARD Hostname> <Aliases>
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

where **<IP address>** is the IP address of the high side of the Guard (e.g. 111.222.3.4), **<GUARD Hostname>** is the fully qualified domain name of the Guard (e.g. host1.domain1.mil), and **<Aliases>** is a list of any Guard hostname aliases (e.g. host1).

Save the file and exit the editor by performing the following command:

```
:wq!
```

10. As the “**root**” user, modify the **ipc_services.dat** file by performing the following steps:

```
# cd <BSWD install directory>/etc
```

Edit the **ipc_services.dat** file by performing the following command:

```
# vi ipc_services.dat
```

Add the following line to the end of the file:

```
tta_plugin      6666 localhost      #TTA PLUGIN
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

11. As the “**root**” user, modify the **/var/spool/cron/crontabs/root** file so that the **syslogd** process can be monitored by the TTA system. Perform the following steps to allow the TTA system to monitor syslogd:

```
# cd /var/spool/cron/crontabs
```

Edit the **root** file by performing the following command:

```
# vi root
```

Add the following as two new lines to the end of the file, substituting the TAB character for the word **<TAB>**, and the actual full path to the TTA High software for the parameter **< full path to tta_v1.0.2_High >**:

```
# restart syslog upon its death for TTA
0,5,10,15,20,25,30,35,40,45,50,55<TAB>*<TAB>*<TAB>*<TAB>* <TAB>< full path to
tta_v1.0.2_high >/tta/scripts/TtaAuditCheck.csh
```

Save the file and exit the editor by performing the following command:

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

```
:wq!
```

After the changes have been made, stop and restart the cron process by executing the following commands:

```
% /etc/rc2.d/S75cron stop
% /etc/rc2.d/S75cron start
```

12. As the “*root*” user, execute the following steps to edit the */etc/mail/aliases* file and add the necessary aliases for the TTA System:

```
# cd /etc/mail
```

Edit the *aliases* file by performing the following command:

```
# vi aliases
```

Immediately below the following comment block:

```
#####
#Local aliases below#
#####
```

Add the following 2 lines to the end of the file, substituting the actual full path to the TTA High software for the parameter <full path to tta_v1.0.2_High>:

```
ttaMailMon:|/<full path to tta_v1.0.2_high>/tta/bin/<platform>/cgiMailMon
ttaAdmins: (comma separated list of TTA administrators excluding "ttaadmn")
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

After the file has been saved, execute the following command to rebuild the database for the mail aliases:

```
# newaliases
```

13. To configure and start the Field Level Filter Administration Tool (FLFAT) use the following steps:

Login to the system as a valid TTA administrator

```
% cd <full path to tta_v1.0.2_high>/tta
% source TTAvvars.csh
% cd scripts
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

```
% ./RUN_FLFAT (this brings up the FLFAT screen)
```

Select **"connect"** (this brings up the connect to Broadsword screen)

Fill out the screen with the following:

Host: *<the IP address of a Broadsword Gatekeeper with a valid backside source, preferably the Broadsword Gatekeeper that has direct access to the TTA Gatekeeper; if this Gatekeeper has no backside sources then consult with the local Broadsword administrator to identify a suitable Gatekeeper>*

Port: *<the port number from the GkprIpcPort line in the /opt/bswd3.1/etc/local.gkpr.conf file from the host computer listed above>*

Username: bswduser

Password: *<appropriate bswduser password>*

Select **"OK"** after the Gatekeeper information has been entered.

After the FLFAT Application has successfully connected to the Gatekeeper the following message will be presented to the user in a dialog box:

**The FLFAT Configuration Has Been Configured to Use a
Default Set of Values.
This Configuration Needs to be Modified to Reflect the
Targeted Classification Level.
Do You Wish to Continue?**

Select **"Yes"** when prompted by a dialog box asking to save the configuration file.

Select **"Save"**

Select **"OK"**

Select **"Exit"**

Execute the following command to verify that the file was created:

```
% ls -l ../config/<high side machine name>/IFLF.cfg.ecr
```

14. Configuration of the High Side TTA v1.0.2 software is complete.

5.6.3 Configuring TCP Wrappers on TTA High Side Gatekeeper

TCP Wrappers provides a security layer around network services that are readily accessible on a UNIX platform. *TCP Wrappers* enforces access and control of the network services based upon IP address and network port numbers, protecting the system from unwanted intrusions while effectively monitoring and logging access from outside sources. *TCP Wrappers* allow or deny incoming service requests depending on the contents of a set of the */etc/hosts.allow* and */etc/hosts.deny* access control files.

For the TTA High Side Gatekeeper there are no modifications required to the *hosts.deny* file.

The *hosts.allow* file needs to be modified to identify the list of hosts that are allowed to send files via FTP or SMTP to the TTA workstation by executing the following steps:

1. In the terminal window, execute the following command:

```
# vi /etc/hosts.allow
```

2. In the *hosts.allow* file, locate the entries shown below.

```
in.ftpd:          <hostname>
sendmail:         <hostname>
```

3. Modify the entries found in the previous step to match those shown below, where <guardhost> is the IP address of the ISSE Guard.

```
in.ftpd:          <guardhost>
sendmail:         <guardhost>
```

4. Save and close the *hosts.allow* file by executing the following command:

```
:wq!
```

5.7 Installing and Configuring TTA Low Gatekeeper Software

The following describes the steps required to install and configure the TTA software on the Low Side TTA Gatekeeper system. These steps are to be executed in their entirety by the TTA installer. The time required to perform this step is approximately 1 hour.

5.7.1 Installing TTA Low Gatekeeper Software

Approximately 280 MB of free disk space is required for the installation of TTA Low Gatekeeper software. If at any time during this sequence the installation process is aborted the partially installed TTA low software should be uninstalled following the steps described in section 5.9.2 of this report before attempting a reinstall.

Note: The System Administrator should confirm that both High and Low side TTA workstations are configured as mail servers, not clients.

- 1) If not already booted, boot the Low Side TTA System.

- 2) **If re-installing TTA, proceed to step 5 of this section.** Otherwise, log on as a user with system administration privileges, and then bring up an xterm and su to root.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the **Browse** menu, select the **Groups** option. Under the **Edit** menu, select the **Add...** option to display the Add Group dialog. Add the following three groups with the following attributes.

```
Group Name: tta
Group ID: <any number greater than 100>
Member List: <blank>
```

```
Group Name: cgiadmin
Group ID: <any number greater than 100>
Member List: <blank>
```

```
Group Name: cgiuser
Group ID: <any number greater than 100>
Member List: <blank>
```

When the parameters have been entered, select **Ok**, then Under the **Edit** menu, select the **Exit** option to close the admintool.

Note: All local groups created need to have ids > 100. Consult with the System Administrator for direction with creating these groups and conflicts that might exist.

Note: It is assumed that the *bswd* group already exists as a result of the installing and configuring the Broadsword Gatekeeper software.

- 3) Execute the following steps to create a *ttadmin* non-login local user account with password. This account provides ownership of the directories and files that are placed on the system during an install.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the Edit menu, select the **Add...** option to display the Add User dialog. For the *ttadmin* non-login account, set the following attributes.

```
User Name: ttadmin
User ID: <Any available UID greater than 1000>
Primary Group ID: tta
Secondary Group Ids: cgiadmin,cgiuser,bswd
```

Comment: **TTA NON-LOGIN FTP ACCOUNT**
Login Shell: **/bin/false**
Password: **“Normal Password”**
Min Change: **<no change>**
Max Change: **<no change>**
Max Inactive: **<no change>**
Expiration Date: **<no change>**
Warning: **<no change>**
Create Home Dir: **<Ensure box is not checked>**
Home Directory: **<TTA Install Directory>**

When the parameters have been entered, select **OK**, then under the **File** menu, select the **Exit** option to close the admintool.

4.) Enable ftp ability for this local account by adding **"/bin/false"** to the **/etc/shells** file. Perform the following steps to make the necessary changes to the **/etc/shells** file:

```
# cd /etc
```

Edit/Create the **shells** file by performing the following command:

```
# vi shells
```

Add the following lines to the end of the file if they do not already exist:

```
/bin/false  
/bin/csh  
/bin/sh
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

5.) Execute the following commands to create additional local user accounts that will serve as TTA administrators.

In the terminal, execute the following command to open the admintool:

```
# admintool
```

Under the Edit menu, select the **Add...** option to display the Add User dialog. Add users who will serve as TTA Administrators For each administrator being added, set the following attributes.

User Name: **<User Login Name>**
User ID: **<Any available UID>**
Primary Group ID: **tta**

Secondary Group Ids: **wheel,cgiadmin,cgiuser,bswd**
Comment: **TTA ADMINISTRATOR**
Login Shell: **C Shell**
Password: **“Normal Password”**
Min Change: **1**
Max Change: **180**
Max Inactive: **60**
Expiration Date: **<no change>**
Warning: **5**
Create Home Dir: **<Ensure box is checked>**
Home Directory: **/home/<User Login Name>**

When the parameters have been entered, select **OK**, then under the **File** menu, select the **Exit** option to close the admintool.

Note: Due to limitations in Solaris 2.6, it is necessary to instruct each user to reset their password after they log in successfully the first time. After 180 days each user’s password will expire and have to be reset. Each user will be notified 5 days in advance of the password expiration.

6.) Approximately 280 MB of free disk space is required for the installation of the TTA software. Select a location for the TTA software that provides this amount of free space, and create a directory where the Low Side TTA software will be installed. Record the full path to this directory for future reference. Though the installer determines the directory name, in the remaining steps this directory will be referred to as ***tta_v1.0.2_low***, and the full path will be referred to as ***<full path to tta_v1.0.2_low>***.

7.) Enter the following command to change directory to the location where the Low Side TTA v1.0.2 software was installed:

```
# cd <full path to tta_v1.0.2_low>
```

Verify the ownership of the **tta_v1.0.2_low** directory as user **ttaadm** group **tta**, and, if necessary, execute the following command to change the ownership of the newly created install directory to **ttaadm** and the group to **tta**:

```
# chown ttaadm:tta tta_v1.0.2_low
```

8.) Verify the permission of the **tta_v1.0.2_low** directory as **777**, and, if necessary, execute the following command to change the permissions of the newly created install directory:

```
# chmod 777 tta_v1.0.2_low
```

9.) Place the **TTA v1.0.2 Installation CD-ROM** in the system’s CD-ROM drive.

10.) Change the current working directory to the **tta** directory beneath the directory at which the CD-ROM has been mounted:

```
# cd /cdrom/<CD-ROM mount point>/tta
```

Execute the Low Side TTA install script by entering the following command:

```
# ./install.csh LOW <full path to tta_v1.0.2_low>
```

View the script execution process and provide answers for the following questions listed in Table 5.2:

PROMPTS	DESCRIPTION
TTA Gatekeeper Host Name	Host name of the system on which the BSWD/TTA system is being currently installed.
TTA Gatekeeper IP Address	IP address of the system on which the BSWD/TTA system is being currently installed.
TTA Gatekeeper Port	This value is listed in the <i>local.gkpr.conf</i> file located in the <i>\$BSWD_HOME/etc</i> directory. The entry is associated with the <i>GkprIpcPort</i> parameter beneath the <i>RcdName = GkprRcd</i> entry. If unsure of this value, the installer should consult with the Broadsword Administrator to obtain the value.
BSWD User Name	A valid UNIX user that has BSWD administration privileges. Consult the acting BSWD Administrator for this information.
BSWD User Password	Current password for the valid UNIX user that has BSWD administration privileges identified above. Consult the acting BSWD Administrator for this information.
BSWD DB User	BSWD Database login name. Consult the acting BSWD Administrator for this information.
BSWD DB User Password	Password for the BSWD Database login account described above. Consult the acting BSWD Administrator for this information.
TTA Admin User Name	By default, “ <i>ttaadm</i> ” is the “TTA Admin User Name”.
TTA Admin User Password	Password for the “ <i>ttaadm</i> ” account. Consult the acting TTA Administrator for this information.
Explicit path where BSWD was installed	Identifies the explicit path to where the BSWD system has been installed. Consult the acting BSWD Administrator for this information.

Table 5.2: Low Side TTA Configuration Parameters

11.) Logout of the root session. Installation of the Low Side TTA software is complete.

5.7.2 Configuring TTA Low Side Gatekeeper Software

The following describes the steps required to configure the TTA software on the Low Side TTA Gatekeeper system. These steps are to be executed in their entirety by the TTA installer. In these steps, the full path to the TTA Low software, determined in section 5.7.1 step 5, should be substituted wherever the parameter *<full path to tta_v1.0.2_low>* appears.

1. Login to the system as a valid TTA Administrator.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

2. Change the current working directory to the *tta* directory by executing the following command:

```
% cd < full path to tta_v1.0.2_low >/tta
```

3. Set up the appropriate runtime environment by executing the following command:

```
% source ./TTAvars.csh
```

4. Change the current working directory to the binary directory where the TTA applications have been placed by executing the following command:

```
% cd < full path to tta_v1.0.2_low >/tta/bin/<platform>
```

where platform identifies the current version of the operating system (i.e., solaris25, solaris26, solaris27).

5. Execute the TTA Security Monitor to setup and initialize the runtime directories for the TTA System by executing the following command:

```
% ./TtaSecMon
```

6. Change the current working directory to the binary directory where the TTA CGI applications have been placed by executing the following command:

```
% cd < full path to tta_v1.0.2_low >/ttaCGI/bin/tta/<platform>
```

where platform identifies the current version of the operating system (i.e., solaris25, solaris26, solaris27)

7. Change user to *root*, and execute the CGI application to setup and initialize the runtime directories for the TTA CGI applications by executing the following commands:

```
# csh
# source < full path to tta_v1.0.2_low >/tta/TTAvars.csh
# ./cgiFixDirs
```

Exit from the root session.

8. As the TTA Administrator, configure the TTA CGI applications so that they interface to the proper host during the transfer of the TTA packages and that the packages are delivered properly to the systems on the opposite side of the security boundary by executing the following command:

```
% ./cgiAdmin
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

This will present a Graphical User Interface (GUI) to the user for checking and modifying the appropriate values needed for the delivery of TTA packages.

- a) Select the **Workstation Config** button located on the main window.
 - i. The user will be presented with an additional window in which the targeted host will be identified for the transfer of the TTA packages. This host should identify the host name of the Guard platform.
 - ii. If the current host name does not reflect the Guard host, modify the entry in the text field by highlighting the entire contents of the text field and typing in the actual name of the Guard platform.
 - iii. Select the **Access** button next to the host name. The user will be presented with an additional window in which the ftp settings for the TTA Package Send process. Verify that the list contains the following:

```
CGI_FTP_USER=loftpin
CGI_FTP_PASS=(appropriate passwd)
CGI_FTP_DIR=loimage
```

- iv. If the ftp settings were changed in step iii, select the 'Save' button located at the bottom of the current screen. Select the 'Exit' button to exit the ftp setting window.
 - v. If the host name was changed in the step ii, select the 'Apply' button located at the bottom of the current screen.
 - vi. Select the 'Exit' button to exit the workstation configuration function.
- b. Select the **Environment Config** button located on the main window.
 - i. The user will be presented with an additional scrollable window that will contain the current runtime environment for the TTA CGI applications. Of primary focus in this list of environment variables are the **CGI_AUTO_TO**, **CGI_AUTO_REV_MODE**, and **CGI_AUTO_TO_2** entries.

- ii. Scroll down through the list of variables until the above variable(s) are shown.
 - iii. Verify, and, if needed, set the value of the **CGI_AUTO_TO** variable to be of the form **ttadm@<hostname>** where hostname is a valid high side delivery name configured on the Guard system where packages will be delivered containing low to high inter-Gatekeeper messages.
 - iv. Verify, and, if needed, set the value of the **CGI_AUTO_TO_2** variable to be of the form **ttadm@<hostname>_2** where hostname is a valid high side delivery name configured on the Guard system where packages will be delivered containing low to high Keymap messages.

- v. Verify, and, if needed, set the value of the *CGI_AUTO_REV_MODE* variable to **LOW** to represents the side, low or high, on which this TTA system is running.
 - vi. If any values were changed in the steps iii through v, select the ‘Save’ button located at the bottom of the current screen.
 - vii. Select the ‘EXIT’ button to exit the environment configuration function.
- c. Select the Exit button to exit the *cgiAdmin* application.
9. Verify that the IP address for the Low side of the Guard has been placed in the */etc/hosts* file. As the “*root*” user, view and, if necessary, modify the */etc/hosts* file by executing the following commands:

```
# cd /etc
```

Edit the *hosts* file by performing the following command:

```
# vi hosts
```

If the IP address does not exist in the file, add a line to the file using the following format:

```
<IP address>          <GUARD Hostname> <Aliases>
```

where <IP address> is the IP address of the low side of the Guard (e.g. 111.222.3.4), <GUARD Hostname> is the fully qualified domain name of the Guard (e.g. host1.domain1.mil), and <Aliases> is a list of any Guard hostname aliases (e.g. host1) including the hostname of the High Side of the Guard.

Save the file and exit the editor by performing the following command:

```
:wq!
```

10. As the **root** user, modify the */var/spool/cron/crontabs/root* file so that the *syslogd* process can be monitored by the TTA system. Perform the following steps to allow the TTA system to monitor syslogd:

```
# cd /var/spool/cron/crontabs
```

Edit the *root* file by performing the following command:

```
# vi root
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Add the following as two new lines to the end of the file, substituting the TAB character for the word <TAB>, and the actual full path to the TTA Low software for the parameter <full path to tta_v1.0.2_low>:

```
# restart syslog upon its death for TTA
0,5,10,15,20,25,30,35,40,45,50,55<TAB>*<TAB>*<TAB>*<TAB>*<TAB><full path
to tta_v1.0.2_low>/tta/scripts/TtaAuditCheck.csh
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

After the changes have been made, stop and restart the cron process by executing the following commands:

```
# /etc/rc2.d/S75cron stop
# /etc/rc2.d/S75cron start
```

11. As the “*root*” user, execute the following steps to edit the */etc/mail/aliases* file and add the necessary aliases for the TTA System:

```
# cd /etc/mail
```

Edit the *aliases* file by performing the following command:

```
# vi aliases
```

Immediately below the following comment block:

```
#####
# Local aliases below #
#####
```

Add the following 2 lines to the end of the file, substituting the actual full path to the TTA Low software for the parameter <full path to tta_v1.0.2_low>:

```
ttaMailMon: |/<full path to tta_v1.0.2_low>/tta/bin/<platform>/cgiMailMon
ttaAdmins: (comma separated list of TTA administrators excluding "ttaadm")
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

After the file has been saved, execute the following command to rebuild the database for the mail aliases:

```
# newaliases
```

12. As the “*root*” user, execute the following steps to edit the *jivacrontab* file and add the necessary entry for the TTA keymap update daemon.

```
# cd <BSWD install directory>/client/etc
```

Edit the *jivacrontab* file by performing the following command:

```
# vi jivacrontab
```

Add the following as two new lines to the end of the file, substituting the TAB character for the word <TAB>, and the actual full path to the TTA Low software for the parameter <full path to tta_v1.0.2_low>:

```
# Runs the tta update_daemon every 10 minutes
```

```
*/10<TAB>*<TAB>*<TAB>*<TAB>*<TAB>root<TAB><full path to  
tta_v1.0.2_low>/tta /scripts/update_daemon.csh >/dev/null 2>&1
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

13. Configuration of the Low Side TTA software is complete.

5.7.3 Configuring TCP Wrappers on the TTA Low Side Gatekeeper

TCP Wrappers provides a security layer around network services that are readily accessible on a UNIX platform. *TCP Wrappers* enforces access and control of the network services based upon IP address and network port numbers, protecting the system from unwanted intrusions while effectively monitoring and logging access from outside sources. *TCP Wrappers* allow or deny incoming service requests depending on the contents of the */etc/hosts.allow* and */etc/hosts.deny* access control files.

For the TTA Low Side Gatekeeper there are no modifications required to the *hosts.deny* file.

The *hosts.allow* file needs to be modified to identify the list of hosts that are allowed to send files via FTP or SMTP to the TTA workstation by executing the following steps:

1. In the terminal window, execute the following command:

```
# vi /etc/hosts.allow
```

2. In the *hosts.allow* file, locate the entry shown below.

```
in.ftpd: <hostname>
```

```
sendmail: <hostname>
```

- The <hostname> parameter on the **in.ftpd** line needs to be replaced with a comma-delimited list of IP addresses of hostnames that are able to ftp to the TTA Low Side system. This list of IP addresses should include the ISSE Guard, any Broadsword Gatekeepers that could potentially ftp products to the TTA Low Side system and any hosts that have sources that are accessible to the TTA Gatekeeper that want to send products via FTP to the TTA system. The TTA installer should consult with the Broadsword Administrator to obtain this list. Once this list is obtained, modify the entry to match that shown below.

```
in.ftpd: <guardhost IP address>,<host1 IP address>,<host2 IP  
address>,...,<hostn IP address>  
>
```

Note: All host IP address entries made in the **hosts.allow** file must appear in the **/etc/hosts** file.

- In the **hosts.allow** file, locate the entry shown below.

```
sendmail: <guardhost>
```

Replace the <guardhost> parameter with the IP address of the Low Side of the ISSE Guard.

- Save and close the **hosts.allow** file by executing the following command:

```
:wq!
```

5.8 Modifying the ISSE Guard Configuration to Access TTA

In order to allow the ISSE Guard System to communicate with the newly added TTA functionality the TTA high side and low side hosts and file delivery points need to be defined to the ISSE Guard system. To accomplish this, the ISSE Guard installer working with the TTA installer will use the capabilities in the Guard Admin Application to add the host entries for the high side plug-in input directory (pi_results), the high side Keymaster input directory (kr_input), the low side Gatekeeper input directory (gkpr_input).

5.8.1 Configuring the HIGH Side Delivery Points

To configure the host parameters for the high side plug-in directory (pi_results), provide the following information via the ISSE Guard Admin Application:

PRIMARY HOSTNAME – <The hostname as it was set in Section 5.7.2, Step 8, substp b/iii for the environment variable CGI_AUTO_TO>

NETWORK – HIGH.

HOST IP ADDRESS – <The IP address for the PRIMARY HOSTNAME>

HOSTMODE – Host status (Do Not Modify)

VIRUS DETECTION – Virus Detection Status (Do Not Modify)

FTP ACCOUNT – The TTA ftp non-login user account, **ttaadm**n

FTP PASSWORD – <The password provided for the TTA ftp non-login user id as specified in Section 5.7.1, Step 3>

FTP DIRECTORY – /<full path to tta_v1.0.2_high>/tta/hisys/pi_results

SMTP OUTPUT STATE – Hostname (Do Not Modify)

SMTP OUTPUT FLAG – MIME Status (Do Not Modify)

FTP OUTPUT STATE – Hostname (Do Not Modify)

FTP OUTPUT FLAG – Ftp Status (Do Not Modify)

To configure the host parameters for the high side Keymaster input directory (kr_input), provide the following information via the ISSE Guard Admin Application:

PRIMARY HOSTNAME – <The hostname as it was set in Section 5.7.2, Step 8, substep b/iii for the environment variable CGI_AUTO_TO_2>

NETWORK – HIGH.

HOST IP ADDRESS – <The IP address for the PRIMARY HOSTNAME>

HOSTMODE – Hostmode status (Do Not Modify)

VIRUS DETECTION – Virus Detection Status (Do Not Modify)

FTP ACCOUNT – The TTA ftp non-login user account, **ttaadm**n

FTP PASSWORD – <The password provided for the TTA ftp non-login user id as specified in Section 5.7.1, Step 3>

FTP DIRECTORY – /<full path to tta_v1.0.2_high>/tta/hisys/kr_input

SMTP OUTPUT STATE – Hostname (Do Not Modify)

SMTP OUTPUT FLAG – MIME Status (Do Not Modify)

FTP OUTPUT STATE – Hostname (Do Not Modify)

FTP OUTPUT FLAG - Ftp Status (Do Not Modify)

5.8.2 Configuring the LOW Side Delivery Points

To configure the host parameters for the low side Gatekeeper input directory (gkpr_input), provide the following information via the ISSE Guard Admin Application:

PRIMARY HOSTNAME – <The hostname as it was set in Section 5.6.2, Step 8, substep b/iii for the environment variable CGI_AUTO_TO>

NETWORK – LOW.

HOST IP ADDRESS – <The IP address for the PRIMARY HOSTNAME>

HOSTMODE – Hostmode status (Do Not Modify)

VIRUS DETECTION – Virus Detection Status (Do Not Modify)

FTP ACCOUNT – The TTA ftp non-login user account, **ttaadm**

FTP PASSWORD – <The password provided for the TTA ftp non-login user id as specified in Section 5.6.1, Step 3>

FTP DIRECTORY – </full path to tta_v1.0.2_low>/tta/hisys/gkpr_input

SMTP OUTPUT STATE – Hostname (Do Not Modify)

SMTP OUTPUT FLAG – MIME Status (Do Not Modify)

FTP OUTPUT STATE – Hostname (Do Not Modify)

FTP OUTPUT FLAG - Ftp Status (Do Not Modify)

5.8.3 Configuring the Virus Detection and File Type Checking for TTA

Additionally, the following changes need to be made on the ISSE Guard platform to allow TTA packages to pass through Guard Virus Detection and File Type Checking.

Access the *Guard Apps* window by clicking on the file cabinet icon on the Guard desktop, selecting the *Application Manager*, the double clicking on the *Guard Apps* icon. In the *Guard Apps* window double click on the *Configure Guard* icon. This opens the *Configure Guard* file in a vi editor. Within the editor verify, and, if necessary, set the following configuration variables:

```
HL_FILE_TYPE_CHECK = "ON"
LH_FILE_TYPE_CHECK = "ON"
VIRUS_DETECTION = "ENABLED"
LOW_SCREENING = "ON"
VIRUS_ADMIN_HIGH = ttaMailMon@<highsidehost>
VIRUS_ADMIN_LOW = ttaMailMon@<lowsidehost>
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

```
ISSE_ADMIN_HIGH = ttaMailMon@<highsidehost>  
ISSE_ADMIN_LOW = ttaMailMon@<lowsidehost>  
USER_SUCCESS_REPLY_HIGH = "ON"  
USER_SUCCESS_REPLY_LOW = "ON"  
ADMN_SUCCESS_REPLY_HIGH = "ON"  
ADMN_SUCCESS_REPLY_LOW = "ON"
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

1. In the *Guard Apps* window double click on the *Define File Types* icon. This opens the *Define File Types* file in a vi editor. Within the editor add the following lines to the end of the file:

```
# TTA  
#  
| 0 | string | NOTUSED | TTA CONTROL FILE | .cntl |  
| 0 | string | NOTUSED | TTA MAP FILE | .kmap.0 |  
| 0 | string | NOTUSED | TTA DATA FILE | .0 |  
| 0 | string | NOTUSED | TTA PRODUCT FILE | .0 .1 |  
#
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

2. In the *Guard Apps* window double click on the *Edit Valid High Files*. This opens the *Edit Valid High Files* file in a vi editor. Within the editor add the following entries:

```
TTA CONTROL FILE  
TTA MAP FILE  
TTA DATA FILE  
TTA PRODUCT FILE
```

Save the file and exit the editor by performing the following command:

```
:wq!
```

3. In the *Guard Apps* window double click on the *Edit Valid Low Files*. This opens the *Edit Valid Low Files* file in a vi editor. Within the editor add the following entries:

TTA CONTROL FILE

TTA MAP FILE

TTA DATA FILE

TTA PRODUCT FILE

Save the file and exit the editor by performing the following command:

wq!

Configuration of the ISSE Guard for TTA operations is complete. You should now proceed to Chapter 6 of this report to perform TTA Registration.

5.9 Uninstalling TTA

If at any time during the TTA High or TTA Low software installation processes described in section 5.6 and 5.7 of this report, the installation process is aborted the partially installed TTA software should be uninstalled before attempting a re-install. The steps required to uninstall the TTA software are the same regardless of whether a full installation has taken place or a partial install has been aborted or has failed. The following sections describe the steps required to uninstall the TTA software on either the TTA High or TTA Low platforms.

Note: Unless otherwise stated, executing the steps in the following sections will require root privileges.

Note: Unless otherwise stated, the steps in the following sections are performed from within the C Shell.

5.9.1 Uninstalling TTA High Software

Uninstalling the TTA software on the TTA High platform consists of the following steps, stopping all TTA high processes including the TTA log daemon, changing directories to the uppermost TTA directory, and performing a recursive remove of the directory including all subordinate files, directories, and soft links. Specific instructions for performing this are as follows:

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_high> will denote the high side installation directory.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

1. Login to the TTA platform as a valid administrator and change user to root. Open a terminal window. Perform steps as directed in Section 7.3 for Stopping TTA High including killing the ttalogd.
2. Change directories to the top level TTA directory if it exists. If the top-level TTA directory was never created, proceed to step 5.

```
# cd <full path to tta_v1.0.2_high>
```

3. Change directories to the level above the top level TTA directory.

```
# cd ..
```

4. Remove all installed TTA software.

```
# rm -rf tta_v1.0.2_high
```

5. Change directories to /usr/lib

```
# cd /usr/lib
```

6. Remove the eight softlinks used by TTA:

```
# rm libSYbas12.so libSYmfront.so libSYutl12.so libcomm_r.so  
libcs_r.so libct_r.so libintl_r.so libtcl_r.so
```

After removal is complete, the system administrator may proceed with re-installing the TTA High system in accordance with the instructions provided in Section 5.6 of this report.

If the platform is being retired from use as a Broadsword/TTA platform, the system administrator should follow instructions for uninstalling the Broadsword Gatekeeper software. Due to the extensive modifications made to limit the security related vulnerabilities of the Solaris operating system as described in section 5.3 of this report, reuse of the TTA configured operating system for non-TTA use is not recommended. If the platform is being retired from TTA use the system administrator should re-install the operating system from Solaris distribution media provided by Sun Microsystems.

5.9.2 Uninstalling TTA Low Software

Uninstalling the TTA software on the TTA Low platform consists of the same three basic steps that are performed to uninstall the TTA software on the TTA High platform. Specific instructions for performing this on the TTA Low platform are as follows:

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_low> will denote the low side installation directory.

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

1. Login to the TTA platform as a valid administrator and change user to root. Open a terminal window. Perform steps as directed in Section 7.4 for Stopping TTA Low including killing the ttalogd.
2. Change directories to the top level TTA directory if it exists. If the top-level TTA directory was never created, proceed to step 5.

```
# cd <full path to tta_v1.0.2_low>
```

3. Change directories to the level above the top level TTA directory.

```
# cd ..
```

4. Remove all installed TTA software

```
# rm -rf tta_v1.0.2_low
```

5. Change directories to /usr/lib

```
# cd /usr/lib
```

6. Remove the eight softlinks used by TTA:

```
# rm libSYbas12.so libSYmfront.so libSYutl12.so libcomn_r.so  
libcs_r.so libct_r.so libintl_r.so libtcl_r.so
```

After removal is complete, the system administrator may proceed with re-installing the TTA Low system in accordance with the instructions provided in Section 5.7 of this report.

If the platform is being retired from use as a Broadsword/TTA platform, the system administrator should follow instructions for uninstalling the Broadsword Gatekeeper software. Due to the extensive modifications made to limit the security related vulnerabilities of the Solaris operating system as described in section 5.3 of this report, reuse of the TTA configured operating system for non-TTA use is not recommended. If the platform is being retired from TTA use the system administrator should re-install the operating system from Solaris distribution media provided by Sun Microsystems.

Chapter 6

TTA Registration

In order to make the Broadsword COI aware of the newly added TTA functionality the TTA Gatekeepers have to be registered with the Keymaster process. To accomplish this, the TTA installer should follow the instructions for TTA below.

This section details the process of modifying the Broadsword configuration to register the High Side TTA Gatekeeper with the High Side Keymaster, **which needs to be completed first**, and then register Low Side TTA Gatekeeper with the Low Side Keymaster.

6.1 TTA High Side Gatekeeper Registration

To begin this process, the administrator must contact the appropriate High Side Keymaster administrator for a one-time registration identifier.

Note: Keymaster POC information for the required security domain can be obtained by contacting the Centralized Help Desk (CHD) for Intelligence Data Handling Systems (IDHS) at DSN: 587-4347 or Commercial (315) 330-4347. The information obtained can be added to the install worksheet in Table 2.1 #68.

After receiving this information, logon to the High Side TTA platform as a valid TTA administrator. Open a browser window, and enter the URL of TTA High in the Location area. In the Username box, enter a user name and password for bswdadm, and click on “**Accept**”. Select the “**Register TTA**” option under the **Administration** → **System Configuration** popdown menu. The “**Register TTA**” screen allows the administrator to register a TTA with a Keymaster. Figure 6.1 is the initial “**Register TTA**” screen.

Register TTA	
Keymaster IP Address	<input type="text"/>
Keymaster Port	<input type="text"/>
Registration ID	<input type="text"/>

Figure 6.1 Initial “Register TTA” Screen

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

their sources) and a certificate used to authenticate itself with the other participating Gatekeepers. Successful registration is indicated with a response back from the Keymaster that the registration process was successful. Figure 6.2 illustrates a successful registration.

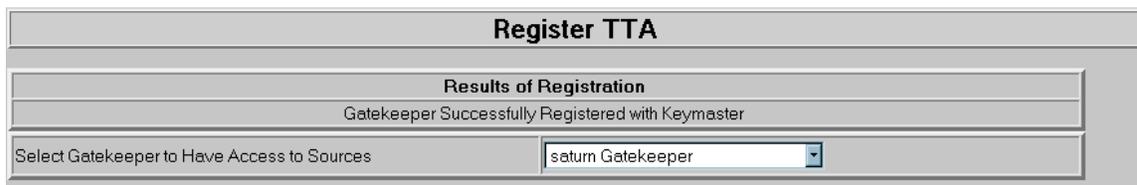


Figure 6.2 Sample Successful Registration Screen

After a successful registration with the Keymaster, the TTA administrator must select exactly one Gatekeeper to communicate with from the pop down list and click “**Set Gatekeeper**”. The Gatekeeper selected is the one on the low side network that this TTA Gatekeeper needs to access. If this is successful, the following screen will appear:



Figure 6.3 Successful “Set Gatekeeper” Screen

6.2 TTA Low Side Gatekeeper Registration

Registering the Low Side TTA Gatekeeper **after** the High Side has been registered. Registering the Low Side Gatekeeper takes place through the normal “**Register Gatekeeper**” process described in previous sections and repeated below.

To begin this process, the administrator must contact the appropriate Low Side Keymaster administrator for a one-time registration identifier.

Note: Keymaster POC information for the required security domain can be obtained by contacting the Centralized Help Desk (CHD) for Intelligence Data Handling Systems (IDHS) at DSN: 587-4347 or Commercial (315) 330-4347. The information obtained can be added to the install worksheet in Table 2.1 #68.

After receiving this information, logon to the Low Side TTA platform as a valid TTA administrator. Open a browser window, and enter the URL of TTA Low in the Location area. In the Username box, enter a user name and password for bswdadm and click on “**Accept**”. Select the “**Register Gatekeeper**” option under the Administration → System Configuration popdown menu. The “**Register Gatekeeper**” screen allows the administrator to register a Gatekeeper with a Keymaster.

After entering the information requested and clicking on the “**Register Gatekeeper**” button, all the necessary information is passed up to the Keymaster. Upon successful registration, the

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Keymaster will in turn pass back a Global Map (identifying other participating Gatekeepers and their sources) and a certificate used to authenticate itself with the other participating Gatekeepers. Successful registration is indicated with a response back from the Keymaster that the registration process was successful.

Chapter 7

Starting and Stopping TTA

Starting and stopping the Trusted Transfer Agent (TTA) consists of starting (or stopping) both the TTA High and TTA Low system applications. The following sections define the steps necessary to:

1. Start the TTA High Side Applications
2. Start the TTA Low Side Applications
3. Stop the TTA High Side Applications
4. Stop the TTA Low Side Applications

Note: Unless otherwise stated, executing the steps in the following sections will require TTA Administrator privileges.

Note: Unless otherwise stated, the steps in the following sections are performed from within the C Shell. In these steps, the command line system prompt is shown as a “%” symbol.

7.1 Starting TTA High

To start TTA High, execute the following steps on the TTA High system as a valid TTA Administrator:

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_high> will denote the high side installation directory.

1. Prior to starting the TTA High system, the TTA Administrator needs to verify that the Inclusive Field Level Filter file, *IFLF.cfg.ecr*, exists in the <full path to tta_v1.0.2_high>/tta/config/<hostname> directory. Perform the following steps to verify that this file exists:

```
% cd <full path to tta_v1.0.2_high>/tta/config/<hostname>
```

Check the contents of the directory by executing the following command:

```
% ls -al
```

If the encrypted version, *IFLF.cfg.ecr*, of the file does not exist in the directory, create it by configuring the field level filters using the Field Level Filter Administration Tool (FLFAT). Once you have saved the filters and exited FLFAT, this file should exist. For details on how to use FLFAT to create this file, refer to Section 5.6.2, Step 14 in this document.

2. Perform the following commands to initialize and start the TTA High system:

Change the current working directory to the installed TTA v1.0.2 directory.

```
% cd <full path to tta_v1.0.2_high>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA v1.0.2 *scripts* directory.

```
% cd <full path to tta_v1.0.2_high>/tta/scripts
```

Initialize the TTA System by performing the following:

```
% ./TtaInitSys.csh HIGH
```

A message similar to the following will be displayed in the terminal window to indicate the status of the TTA processes:

```
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/ttalogd
not running/opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgCre
not running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgSend
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/KeymapRcvProc
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/tta_plugin.SVR4
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/SFA
```

At times, given the current status of the TTA system, the **ttalogd** may or may not be running.

Following this, the installer will be prompted to continue with the TTA initialization process. Respond to each prompt by pressing the **Enter** key to continue the TTA Initialization process or the **Esc** key, if canceling the TTA Initialization process.

During the TTA initialization process the messages “No Match” or “Permission Denied” may be displayed. These messages are normal and do not indicate errors or problems. The initialization process is simply attempting to clean up files within the TTA environment where they may or may not have existed, depending on the TTA state if the

TTA processes were running prior to issuing the `TtaInitSys.csh` command. The following message will be displayed in the terminal window when the TTA initialization process is complete:

Exiting Done

Start up the TTA System by executing the following command:

```
% ./TtaSysStartup
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul  9 09:28:12 EDT 2001):  
running /opt/tta_v1.0.2_high/tta/bin/solaris26/ttalogd  
running/opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgCre  
running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgSend  
running /opt/tta_v1.0.2_high/tta/bin/solaris26/KeymapRcvProc  
running /opt/tta_v1.0.2_high/tta/bin/solaris26/tta_plugin.SVR4  
running /opt/tta_v1.0.2_high/tta/bin/solaris26/SFA
```

If the `TtaSysStartup` process was not successful, any or all of the servers will indicate this by displaying a “not running” status message in the terminal window. In the case that the `TtaSysStartup` was not successful, email messages will be sent to the TTA Administrator indicating the startup problems and error messages will be logged in the syslog as well.

A safety mechanism is in place which will terminate all TTA processes after a specified time interval has passed if any of the TTA processes have failed to execute properly. TTA High System status can be checked at any time by executing the following commands as a valid TTA administrator:

```
% cd <full path to tta_v1.0.2_high>/tta/scripts  
% ./TtaHighSysCheck
```

If successful, a message similar to that resulting from the `TtaSysStartup` command described previously in this section should be displayed.

7.2 Starting TTA Low

To start TTA Low, perform the following commands to initialize and start the TTA Low system as a valid TTA Administrator:

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_low> will denote the low side installation directory.

Change the current working directory to the installed TTA v1.0.2 directory.

```
% cd <full path to tta_v1.0.2_low>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA v1.0.2 *scripts* directory.

```
% cd <full path to tta_v1.0.2_low>/tta/scripts
```

Initialize the TTA System by performing the following command and responding to each prompt:

```
% ./TtaInitSys.csh LOW
```

A message similar to the following will be displayed in the terminal window to indicate the status of the TTA processes:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):  
not running /opt/tta_v1.0.2_low/tta/bin/solaris26/ttalogd  
not running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgCreate  
not running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgSend  
not running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaPrdStatDmn  
not running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaGkprIntrfc
```

At times, given the current status of the TTA system, the **ttalogd** may or may not be running.

Following this, the installer will be prompted to continue with the TTA initialization process. Respond to each prompt by pressing the **Enter** key to continue the TTA Initialization process or the **Esc** key, if canceling the TTA Initialization process.

During the TTA initialization process the messages “No Match” or “Permission Denied” may be displayed. These messages are normal and do not indicate errors or problems. The initialization process is simply attempting to clean up files within the TTA environment where they may or may not have existed, depending on the TTA state if the TTA processes were running prior to issuing the TtaInitSys.csh command. The following message will be displayed in the terminal window when the TTA initialization process is complete:

Exiting Done

Start up the TTA System by executing the following command:

```
% ./TtaSysStartup
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):  
running /opt/tta_v1.0.2_low/tta/bin/solaris26/ttalogd  
running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgCreate  
running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgSend  
running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaPrdStatDmn  
running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaGkprIntrfc
```

If the TtaSysStartup process was not successful, any or all of the servers will indicate this by displaying a “not running” status message in the terminal window. In the case that the TtaSysStartup was not successful, email messages will be sent to the TTA Administrator indicating the startup problems and error messages will be logged in the syslog as well.

A safety mechanism is in place which will terminate all TTA processes after a specified time interval has passed if any of the TTA processes have failed to execute properly. TTA Low system status can be checked at any time by executing the following commands as a valid TTA administrator:

```
% cd <full path to tta_v1.0.2_low>/tta/scripts  
% ./TtaLowSysCheck
```

If successful, a message similar to that resulting from the **TtaSysStartup** command described previously in this section should be displayed.

7.3 Stopping TTA High

To stop TTA High, execute the following commands on the TTA High system as a valid TTA Administrator:

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_high> will denote the high side installation directory.

Change the current working directory to the installed TTA v1.0.2 directory.

```
% cd <full path to tta_v1.0.2_high>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Broadsword-3.1-SYSIMG - 20 Sept 02 FINAL

Change the current working directory to the TTA v1.0.2 *scripts* directory.

```
% cd <full path to tta_v1.0.2_high>/tta/scripts
```

Halt the TTA System by performing the following command:

```
% ./TtaSysShutdown
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul  9 09:28:12 EDT 2001):  
running /opt/tta_v1.0.2_high/tta/bin/solaris26/ttalogd  
not running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgCreate  
not running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgSend  
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/KeymapRcvProc  
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/tta_plugin.SVR4  
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/SFA
```

These steps will shutdown all TTA process except for the *ttalogd* process. In general this process can remain active. If for some reason, the entire system needs to be halted, perform the above steps and, in addition, execute the following command to terminate the *ttalogd* process:

```
% kill `ps -e | grep ttalogd | awk '{print $1}'`
```

7.4 Stopping TTA Low

To stop TTA Low, execute the following commands on the TTA Low system as a valid TTA Administrator:

Note: The steps described below refer to the directories in which the TTA applications have been installed. In the following steps <full path to tta_v1.0.2_low> will denote the low side installation directory.

Change the current working directory to the installed TTA v1.0.2 directory.

```
% cd <full path to tta_v1.0.2_low>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA v1.0.2 *scripts* directory.

```
% cd <full path to tta_v1.0.2_low>/tta/scripts
```

Broadsword-3.1-SYSIMG - 20 Sept 02
FINAL

Halt the TTA System by performing the following command:

```
% ./TtaSysShutdown
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):  
running      /opt/tta_v1.0.2_low/tta/bin/solaris26/ttalogd  
not running  /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgCreate  
not running  /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgSend  
not running  /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaPrdStatDmn  
not running  /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaGkprIntrfc
```

These steps will shutdown all TTA process except for the *ttalogd* process. In general, this process can remain active. If for some reason, the entire system needs to be halted, perform the above steps and, in addition, execute the following command to terminate the *ttalogd* process:

```
% kill `ps -e | grep ttalogd | awk '{print $1}'`
```