

Release

4.1

Luna Imaging Inc.

insight[®]

Insight Installation and Configuration Manual

Luna Imaging Inc.

insight®

This document contains information proprietary to Luna Imaging, Incorporated (Luna). You may reproduce this proprietary information for use within your organization. You may not disclose or distribute this documentation to third parties.

Even though Luna has tested the hardware and software and reviewed the documentation, Luna makes no warranty or representation, either express or implied, with respect to the hardware, software, or documentation, their quality, performance, merchantability, or fitness for a particular purpose. Luna has made every effort to keep the information in this manual current and accurate as of the date of publication or revision. However, Luna does not guarantee or imply that this document is error free or accurate with regard to any particular specification.

In no event will Luna be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect in the hardware, software, or documentation, even if advised of the possibility of such damages. In particular, Luna shall have no liability for any programs or data stored in or used with Luna products, including the costs of recovering such programs or data.

No Luna agent, dealer, or employee is authorized to make any modification, extension, or addition to the above statements.

©2003 luna imaging, inc.
3542 hayden avenue
building one
culver city, california 90232-2413
phone 310.452.8370 • fax 310.452.8389

Table of Contents

INTRODUCTION	4
OVERVIEW OF THE COMPONENTS.....	4
OVERVIEW OF THE CDS.....	6
INSIGHT SYSTEM DIAGRAM.....	7
TECHNICAL SUPPORT.....	8
UPGRADING AN EXISTING INSIGHT INSTALLATION TO INSIGHT TO V4.19	
OVERVIEW OF INSIGHT 4.1 UPGRADE.....	9
WHAT'S NEW IN 4.1.....	9
UPGRADE FROM 4.0 TO 4.1.....	12
<i>Replace file method</i>	12
Backup all Insight components.....	12
User Manager Upgrade.....	12
Collection Manager Upgrade.....	13
Insight Browser Upgrade.....	14
Insight Administrator tools.....	17
<i>Full Install method</i>	17
<i>Insight Client Upgrades</i>	18
<i>Customize insight.dat file for use within Deploy Director</i>	19
<i>Verify your Install</i>	20
UPGRADE FROM 3.1 TO 4.1 OR FROM 3.5 TO 4.1.....	20
UPGRADE DATABASES.....	21
<i>Backup Databases</i>	21
<i>Upgrade Databases</i>	21
UPGRADE COLLECTION MANAGER AND USER MANAGER.....	23
<i>Install Upgrade</i>	23
<i>Make Changes to the Collection Manger Configuration Files</i>	24
<i>Make Changes to the User Manager Configuration Files</i>	24
<i>Copy Image-Group-Files, Link and Presentation folders from v3.1/v3.5/v4.0 Install</i>	24
<i>Reset Browser Thumbnail fields in Collection Configuration</i>	25
UPGRADE INSIGHT CLIENT.....	25
UPGRADE INSIGHT ADMINISTRATOR TOOLS.....	25
INSIGHT BROWSER UPGRADE.....	26
HELP FILE LINKS FOR INSIGHT APPLICATIONS.....	26

INSTALLATION AND CONFIGURATION FOR INSIGHT STANDARD.....27

<i>Installation Concepts</i>	27
INSTALLATION AND CONFIGURATION CHECK LIST.....	28
INSTALL INSIGHT STANDARD SERVERS.....	28
<i>Pre-Configuration</i>	28
PREPARE DATABASE.....	29
<i>Run the Installer</i>	29
<i>Register Your License</i>	31
<i>Activate AAT Vocabulary</i>	31
<i>Connect and Configure the Database for Insight Servers</i>	31
<i>Start the Servers</i>	33
<i>Users Created</i>	37
INSTALL THE MEDIA SERVER.....	39
<i>Copy the Media Files for the Sample Collection</i>	39
<i>Install and configure the MrSID Image Server</i>	39
PACKAGE AND DISTRIBUTE INSIGHT JAVA CLIENT.....	42
<i>Prepare Insight client configuration file</i>	42
<i>Package Insight client</i>	44
<i>Distribute Insight clients</i>	47
INSTALL AND CONFIGURE INSCRIBE.....	48
INSTALL AND CONFIGURE ADMINISTRATOR TOOLS.....	48
<i>Install Administrator Tools</i>	48
<i>Configure Administrator Tools</i>	48
VERIFY THE INSTALLATIONS.....	49
<i>Verifications</i>	49
<i>Update URLs</i>	49
BUILD YOUR OWN COLLECTION.....	50

INSTALLATION AND CONFIGURATION FOR INSIGHT BROWSER SERVER.....51

<i>Prerequisites</i>	51
Getting the Apache Tomcat JSP Server.....	51
Getting the Resin JSP Server.....	51
<i>Install Insight Browser Server</i>	51
Run the Insight Browser Server Installer.....	52
Configure Your JSP Server to run the Insight Browser Server.....	52
Testing your Browser Insight Installation.....	53
CONFIGURING INSIGHT BROWSER SERVER BY EDITING BROWSERINSIGHT.CONF.....	54
<i>Configure User Manager Connection</i>	54
<i>Bypass Login Page</i>	55

Configure Collection Manager Server Database Settings.....	55	Installing the Insight XML Gateway:	76
Create Insight Browser Background Image Slices.....	56	Run the Insight XML Gateway Installer	77
PC.....	56	Configure Your JSP Server to run the Insight XML Gateway.....	77
MAC.....	58	Defining a User for the XML Gateway	78
BROWSER INSIGHT REMOTE LAUNCH STRINGS.....	60	Configuring the XML Gateway to access Specific Insight Collection.....	79
Anatomy of a Remote Launch String:	60	Testing the Configuration of the XML Gateway.....	80
Required Parameters:.....	60	Next Steps – Getting started once the Gateway is installed.....	83
Making a Request Based on a Search:.....	60		
Making a Request for Specific Images:.....	62	INSTALLATION AND CONFIGURATION FOR INSIGHT SECURE MEDIA SERVER.....	84
Open in the Group Window.....	62	INTRODUCTION.....	84
Open in the Image Workspace.....	62	PREREQUISITES.....	85
Additional Insight JVA Launch String Parameters.....	63	Getting the Apache Tomcat JSP Server.....	85
Configure Browser Insight to use SSL (suggested when implementing Insight in a single sign-on environment).....	64	Getting the Resin JSP Server.....	85
Additional Installation Instructions for Resin:.....	64	INSTALL SECURE MEDIA SERVER:.....	85
Additional Installation Instructions for TomCat:.....	65	Run the Secure Media Server Installer.....	86
INSTALLATION FOR DEPLOY DIRECTOR.....	66	Configure Your JSP Server to run the Secure Media Server.....	86
OVERVIEW.....	66	CONFIGURING AN INSTANCE OF THE SECURE MEDIA SERVER TO SERVE IMAGES FROM A COLLECTION.....	88
Installation of Deploy Director.....	66	Configure an Insight Collection Manager to use the Secure Media Server.....	91
Setting up Deploy Director for Insight	69	Changing a Collection's URLs to point to the Secure Media Server.....	92
Customize insight.dat file for use within Deploy Director.....	70	Configuring Browser Insight to use the Secure Media Server.....	93
Verify your Install.....	71	Update your BrowserInsight Configuration File.....	94
Post Install.....	71	Enable the Browser Security Property	95
INSIGHT LAUNCH MANAGER.....	72	Edit your Secure Media Server Settings.....	95
OVERVIEW.....	72	Enabling Secure Media Access for the XML Gateway.....	96
Working With Remote Launch Strings (interoperability between the Insight JVA, Insight JSP Browser, and other Applications).....	72	CONFIGURING INSIGHT'S ADVANCED AUTHENTICATION AND AUTHORIZATION FEATURES.....	97
Configuring Remote Launch to work within your Local Environment:.....	73	ENABLING SIMPLE LDAP AUTHENTICATION FOR THE INSIGHT USER MANAGER.....	98
Understanding the Insight Launch Manager.....	74	Associating LDAP Users with Insight Users.....	100
INSTALLATION AND CONFIGURATION FOR INSIGHT XML GATEWAY.....	76	Using LDAP SSL Certificates with Insight.....	101
Prerequisites.....	76		
Getting the Apache Tomcat JSP Server.....	76		
Getting the Resin JSP Server.....	76		

KERBEROS & LDAP AUTHENTICATION AND AUTHORIZATION	101
<i>Kerberos Authentication - Overview</i>	101
<i>Specifying the Kerberos Settings</i>	102
<i>Enabling Kerberos Authentication for</i> <i>the Insight User Manager</i>	103
<i>LDAP Authorization - Overview ...</i>	103
<i>Specifying the LDAP Settings</i>	104
<i>Enabling LDAP Authorization for the</i> <i>Insight User Manager</i>	106
<i>Interaction of Kerberos & LDAP</i> <i>Users and Users in the Insight User</i> <i>Table</i>	107
<i>Using the Insight Administrator Tool</i> <i>to identify Insight Access Profiles</i>	107
<i>Windows® Active Directory & Insight</i> <i>User Account Information</i>	108
RESTORING THE DEFAULT SECURITY CONFIGURATION FOR INSIGHT	110
RESOURCES	112
Insight Security Release – Implementation Worksheet	113

Introduction

This document is intended to enhance your knowledge of Insight by providing you with the instructions necessary to install and configure Insight 4.1.

It is assumed that the reader of this document should be computer literate, familiar with databases, and has a general understanding of the Windows and/or Solaris environment. This manual also assumes you (the reader) are the Administrator with knowledge of your organization's hardware and software environment.

This document is organized into two basic sections: Upgrading Existing Insight installations to v4.1 and performing a new installation.

Overview of the Components

This document covers the installation and configuration of all Insight's components. Depending on your current license agreement, not all components may have been shipped to you. Please contact your Luna Account Manger if you have any questions.

Insight's Components include:

User Manager -- The User Manager handles all authentication and authorization for Insight, it is a required component for all implementations

Collection Manager – The Collection Manager provides search, image management, and backend functionality to the Insight Architecture. One collection manager is required for each unique data structure within Insight.

Insight Standard – Insight Standard is an out-of-the-box solution. It consists of a User Manager and a Collection Manager pre-configured with an implementation of the Visual Resources Association Core 3.0 Data Structure (see <http://www.vraweb.org> for more information), and a set of sample data records.

Insight Client – The Insight JVA Client is a rich java, client which provides access to Insight Content.

Inscribe Client – Inscribe is Insight's cataloging tool.

Administrator Tools – The Administrator tools provide backend access to configure User and Collection Managers, as well as perform media processing.

Browser Insight – Browser Insight provides a "lite" browser-only interface to Insight's content

Deploy Director – Deploy Director is an add-on for the Insight JVA Client allowing for auto-updating of the client, and enabling the end user to execute remote launch strings.

Media Server – The Media Server includes the Mr.Sid image extraction server with plugins for IIS on Windows and Apache on Linux and Solaris. The Media server is a required component and enhances the user experience in the Insight Image Workspace.

Secure Media Server – The Secure Media Server adds a layer of protection around images in Insight by requiring that all applications that request images from the server have a valid ticket.

XML Gateway – The XML Gateway is an optional component that provides an XML API for Insight's search and data functions. The gateway enables application developers to build their own applications around Insight's functionality.

Other Utilities:

Launch Manager – The Launch Manager provides an administrator with the tools to allow end-users to choose whether remote launch strings should be opened in either BrowserInsight or the JVA Client regardless of where they were created.

VRA Import Script – The VRA Import Script is a perl script that manages the import of data from various sources into Luna's VRA Structure.

Log Analyzer – the Log Analyzer is a tool which allows an administrator to produce usage reports from the Insight Server logs.

Command-Line Indexer – The command-line indexer allows Administrators to add or update content in Insight without running the Administrator tools – ideal for setting up indexing an automated or scheduled process.

SQL Upgrade Scripts – The SQL Upgrade Scripts are intended to upgrade current customers 3.1 of 3.5 database installations to 4.1.

Background Templates for Browser and JVA – The background templates provide a simple method to create backgrounds for the Insight JVA and BrowserInsight.

Other Documentation

Admin Tools Guide – The Insight Administrator Tools Guide provides help for building and managing collections.

Install and Config Guide (this document) – The Install and Configuration guide includes instructions for installing and configuring all of Insight's components.

Getting Started with the XML Gateway – The Getting Started Guide for the XML Gateway includes DTDs, sample XML, and other information necessary for building tools with the XML Gateway.

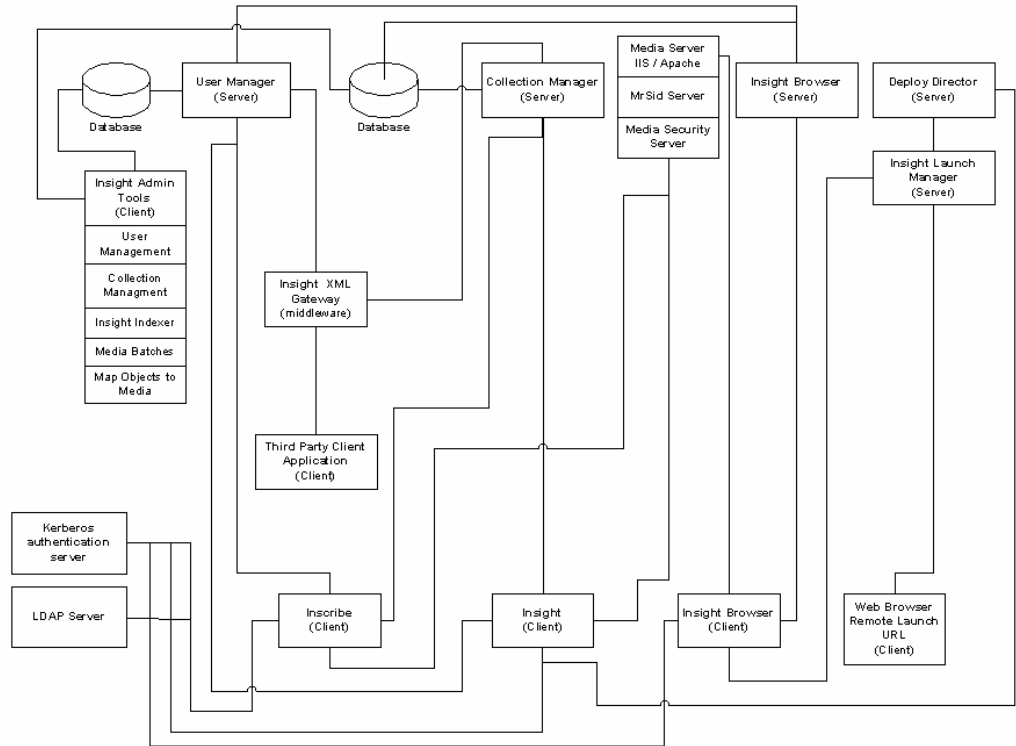
Inscribe Configuration Guide – The Inscribe Configuration Guide includes information on configuring inscribe on-top of an Insight collection.

Overview of the CDs

	CD 1 – Insight Standard	CD 2 – Inscribe	CD 3 – Insight Web Components	CD 4 – Insight Upgrade	CD 5 – Insight Upgrade (with support for Kerberos & LDAP) <i>(Available by special request)</i>	CD 6 Insight XML Gateway
Insight Standard	X					
Sample Media for Insight Standard	X					
Insight User Manager (upgrade)				X	X	
Insight Collection Manager Upgrade				X	X	
SQL Upgrade Scripts				X		
Insight Client	X			X	X	
Inscribe Client		X			X	
Mr.Sid Media Server	X					
Secure Media Server	X			X	X	
VRA Import Script	X					
Administrator Tools	X			X		
Browser Insight			X		X	
Log Analyzer	X			X		
Insight Launch Manager			X			
Command-Line Indexer	X			X		
Insight Background Tools	X		X	X		
Deploy Director			X			
All Insight Components with special support for Kerberos & LDAP Authorization and Authentication (available by special request)					X	
Insight Client (Upgrade for Deploy Director)			X	X		
XML Gateway						X
Install and Configuration Guide	X	X	X	X	X	X
Admin Tools Guide	X	X	X	X	X	X
Getting Started with the XML Gateway						X
Inscribe Configuration Guide		X				

Insight System Diagram

The following diagram shows the relationship between the Insight components and the database. The servers can be installed on a single machine, or separate machines.



Technical Support

For Technical Assistance:

Luna Help Desk 1-800-452-LUNA (5862) – ext. 268
Email: support@luna-img.com

Phone Support Hours: Monday – Friday
 9am – 5:30pm Pacific Standard Time

Upgrading an existing Insight Installation to InSight to V4.1

Overview of Insight 4.1 upgrade

The upgrade process for the version 4.1 has been enhanced to encourage consistency and structure. This is to help ease of the upgrade process.

What's new in 4.1

Security - Authentication / Authorization using existing Kerberos & LDAP Servers

Insight now supports the use of Kerberos and LDAP for authentication and authorization. Administrators may use a Kerberos server to authenticate the user, and then use a secured LDAP directory to provide authorization information.

Security – Authentication / Authorization using existing LDAP Servers

Insight 4.1 now supports the use of an LDAP directory as a password authority for the Insight User Database. These enhancements allow Insight to integrate into the conventional infrastructures currently used within our client base.

Security - Protect your Digital Assets: Insight Secure Media Server

Insight 4.1 has enhanced security with a new Secure Media Server to protect all Insight assets from unauthorized use. All Insight products have integrated support for the Insight Secure Media Server.

Inter-operability - Insight XML Gateway

Insight 4.1 includes an optional component: the Insight XML Gateway. The Insight XML Gateway allows third-party developers to search and retrieve Insight content using the Insight framework. The gateway may be used as an external Insight search engine, or can be used as an API on which a new client interface may be created. Contact a Luna Account Manager for more information.

Insight JVA - Create & Use Dynamic Presentations for Apple's Keynote Software

Insight 4.1 now has the ability to export presentations either to a web page (HTML), to MS Powerpoint (Windows only), or to Apple's Keynote (Mac OS-X only). Exported presentations maintain the same detail, position, and complexity of presentations within insight, including multiple composite images.

Insight 4.1 also has support for playing Keynote presentations from the open group menu, allowing one-click access to your presentation.

Insight JVA - Enhanced Variant Resolution Support: Annotations, Media Links, Web Links

Insight 4.1 now uses relative percents to ensure annotations appear on the region of the image the author originally intended.

Insight JVA - Enhanced Variant Resolution Support: Presentation Playback

Insight 4.1 now uses relative percents to ensure presentation slide elements appear as the author originally intended.

Insight JVA - Improved performance of select list presentation

Insight 4.1 uses a cache mechanism to improve the performance of select list values during data field searching.

Insight JVA / Browser Insight - Keyword Searching has been incorporated into Data Field Searching.

Insight 4.1 provides the use of keywords during data field searching to narrow a result set based on a defined keyword(s).

Browser Insight - Improved performance of Browser Group Window Paging

With the release of v4.1, the browser paging operations are up to 80% faster. Users may now explore the collection page-by-page with no performance penalty.

Browser Insight - Dialog appears to indicate the presence of pop-up blocker software.

If the user has pop-up block software enabled, Browser Insight will display an instructional dialog indicating the presence of the software.

Browser Insight - Improved performance of Image Workspace Initialization

Insight 4.1 has reduced the time necessary to initialize the Image Workspace. Initialization of the IW is up to 60% faster.

Inscribe - Fuzzy date indexing integrated into the "save record" process.

Fuzzy date indexing has been integrated into the "save record" process. This allows for the immediate use of fuzzy date searching within Insight, provided the user has permissions to commit to the indexed data.

Administration - Define the number of DB connections to be used by the Insight Collection Manager

Each connection made to the DB consumes resources, this property allow administrators to define the number of DB connections to be created by the Insight Collection Manager.

Resolved Issues:

Issue: Insight JVA - Save Group Panel - Complete list of available user group folders is not displayed when list exceeds vertical screen size

Resolution: A scroll bar now appears when the list of group files exceeds the visible area.

Issue: Insight JVA - DeployDirector - GW Paging - Paging forward before images have loaded completely may occasionally cause red Xs to appear throughout session.

Resolution: Removed the use of a deprecated method, images now display properly.

Issue: Insight JVA - Open Groups - Only folders containing groups should be displayed.

Resolution: Only group folders containing image groups will be displayed by the Open Group function. This preserves the hidden state of authentication user groups.

Issue: Browser Insight - Collection Level Groups - Users shouldn't be able to create groups if they do not have permissions to save/delete.

Resolution: Browser now properly applies the permissions as defined in the collection level profiles.

Issue: Browser Insight - Collection Selection: Remove virtual collections from the list of available collections.

Resolution: Virtual collections using the VCID method will no longer appear in the list of available collections. Virtual collections using the VCID method are not supported in Browser Insight, use the alternate VC method for Browser access.

Issue: Browser Indexer - If the first thumbnail field is null, records will not be added to DTFlatObjectData.

Resolution: The Browser Indexer now generates a list of valid objects, then searches for the thumbnail field values associated with the object. This ensure that each object containing a cataloged field will appear in Browser Insight.

Upgrade from 4.0 to 4.1

For the upgrade from version 4.0 to 4.1 there are two options “Replace file method” and the “Full install method”. The Replace file method is faster but will not keep in tact your current version 4.0 servers. The Full install method will enable you to run either 4.0 or 4.1 servers but requires you to reconfigure your collection managers and Insight Browser servers

Note: The Upgrade process for the Insight client software is the same for both methods. Instructions are located after the Full install method.

Replace file method

- This method will guide you through replacing only the components that have changed between 4.0 and 4.1
- **Note:** No database schema changes have been made in version 4.1

Backup all Insight components

- Backup Insight databases
- Backup Insight Collection Manager and User Manager directories
- Backup Browser Insight directories
- Backup Insight Administrator folder
- **Note:** To ensure proper file replacement, it is recommended to the administrator to delete the destination files or folders before adding the 4.1 replacement components

User Manager Upgrade

NOTE: if you are planning on using the new Authentication features in Insight v4.1 we recommended you use the full install method, as new properties have been added to the configuration files.

- 1) Stop the User Manager
- 2) Backup your User Manager database
- 3) Backup the directory the User Manager is installed in
- 4) Replace the following files in the directory the User Manager is installed into with the files from the “user_and_collection_managers\manual” directory of the **Insight Upgrade 4.1 CD**

Source	Destination
InsightUpgrade 4.1 CD \user_and_collection_managers\manual InsightLocale_en_US.conf InsightLocale_zh_CN.conf InsightLocale_zh_TW.conf	<Insight v4.0 Install Directory> \user_manager InsightLocale_en_US.conf InsightLocale_zh_CN.conf InsightLocale_zh_TW.conf
InsightUpgrade 4.1 CD \user_and_collection_managers\manual insightserver.jar bcprov-jdk14-115.jar	<Insight v4.0 Install Directory> \user_manager\lib insightserver.jar bcprov-jdk14-115.jar

- 5) Add the following line to the end of the InsightUserServer.dat

```
DefaultFuzzyDateHelpFile = fuzzydatehelptext.txt
```

- 6) Restart the User Manager manually
7) If the upgrade is successful, then at the top console it will say:

```
Insight User Server  
Build v4.1.26
```

- 8) If you were running the User Manager as a service, stop the user manager, and restart it as a service

Collection Manager Upgrade

- 1) Stop the Collection Manager
- 2) Backup your Collection Manager's database
- 3) Backup the directory the Collection Manager is installed in
- 4) Replace the following files in the directory the Collection Manager is installed into with the files from the "user_and_collection_managers\manual" directory of the **Insight Upgrade 4.1 CD**

Source	Destination
InsightUpgrade 4.1 CD \user_and_collection_managers\manual InsightLocale_en_US.conf InsightLocale_zh_CN.conf InsightLocale_zh_TW.conf	<Insight v4.0 Install Directory> \collection_manager InsightLocale_en_US.conf InsightLocale_zh_CN.conf InsightLocale_zh_TW.conf
InsightUpgrade 4.1 CD \user_and_collection_managers\manual insightserver.jar bcprov-jdk14-115.jar	<Insight v4.0 Install Directory> \collection_manager\lib insightserver.jar bcprov-jdk14-115.jar

Note: If you are running on a windows platform and used the “Install As Windows Service.exe” to add your collection as a service, you will need to add bcprov-jdk14-115.jar to the “MdSvc.inf” file. To do this:

- a. open the MdSvc.inf file located in the Collection Manager directory in a text editor
- b. change the following line from:

```
lib\insightserver.jar;lib\Sprinta2000.jar;lib\classes12.jar;  
lib\nls_charset12.jar
```

- c. to this: (note the addition of ;lib\bcprov-jdk14-115.jar at the end)

```
lib\insightserver.jar;lib\Sprinta2000.jar;lib\classes12.jar;  
lib\nls_charset12.jar;lib\bcprov-jdk14-115.jar
```

- 5) Restart the Collection Manager manually
- 6) If the upgrade is successful, then the at the top console it will say:

```
Insight Smart Server  
Build v4.1.26
```

- 7) If you were running the Collection Manager as a service, stop the collection manager, and restart it as a service

Insight Browser Upgrade

- 1) Stop the Tomcat or Resin server.
- 2) Backup the directory the Insight Browser Server is installed into
- 3) Replace the following files and directories in the directory Browser Insight is installed into with the files from the “browser\manual” directory of the **Insight Upgrade 4.1 CD**

Source	Destination
InsightUpgrade 4.1 CD \browser\WEB-INF\lib techempower.jar activation.jar bcprov-jdk14-115.jar jce-jdk13-115.jar mail.jar browserinsight.jar insightserver.jar	<Browser Insight v4.0 Install Directory> \WEB-INF\lib techempower.jar activation.jar bcprov-jdk14-115.jar jce-jdk13-115.jar mail.jar browserinsight.jar insightserver.jar
InsightUpgrade 4.1 CD \browser\ index.jsp css images jsp	<Browser Insight v4.0 Install Directory> \ index.jsp css images jsp

4) Delete version 4.0 compiled JSP

Resin Instructions

- Delete the **_jsp** directory located in the following directory

```
<Browser Insight v4.0 Install Directory>\WEB-INF\work
```

Apache Tomcat Instructions

- Delete the **jsp** directory located in the following directory

```
<Apache Tomcat home directory>\  
work\Standalone\localhost\BrowserInsight
```

5) Add new properties to the BrowserInsight.conf

Two new properties have been added to the BrowserInsight configuration:

SpeedSearchMaxValues: A speed search provides a value list containing possible matching values of a search. This property specifies the maximum number of values that can be displayed in the results of a speed search. If the property is not specified, the default is 250.

CollectionSelectionWindowMode: This property specifies what BrowserInsight does with the Collection Selection window at login. If set to 1, when a remote launch string is invoked the collection selection window will close after login, and browser insight will launch the selected collection. If set to 0, the default, browser insight will keep the collection selection window open in the background.

If you would like to maintain the defaults, there is no need to edit the BrowserInsight.conf. Otherwise, to add the properties:

1. Locate your BrowserInsight.conf, this is either in the root of your installation directory, or if you are using Resin, this may be at root of your resin directory. Open it with your preferred text editor.
2. Add the properties:

```
# CollectionSelectionWindowMode -  
  
# if set to 1, when a remote launch string is invoked the  
# collection selection window will close after login, and  
# browser insight will launch the selected collection  
  
# if set to 0, the default, browser insight will keep the  
# collection selection window open in the background  
  
CollectionSelectionWindowMode = 1  
  
#  
# Limiter for speed search, default value is '250'
```

```
# Range: integer  
# Default: 250  
#  
SpeedSearchMaxValues = 500
```

3. Save browserinsight.conf

Note to Administrator – Security: Applies to customers using 3.5 or 4.0 and Tomcat (this is not an issue currently with Resin). To prevent the disclosure of database names, userids, and passwords, Luna strongly recommends that the BrowserInsight.conf file not be located in the BrowserInsight installation directory, as it is web accessible. To prevent access/disclosure, perform the following steps:

- a) Create a new directory **BrowserInsight_Config** alongside (NOT UNDER) your Insight Browser installation directory.
- b) Move browserinsight.conf into this new folder.
- c) Edit web.xml (in the WEB-INF directory under the Insight Browser installation directory, and make the following change

1. Find the parameter called **ConfigurationFile**

```
<Param-name>ConfigurationFile</param-name>
```

2. Change the text inside the <param-value> tags.

For example:

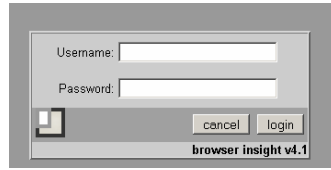
If **C:\Program Files\InsightBrowser4_0** was your installation directory, you would create the folder **C:\Program Files\InsightBrowser_Config**, place **browserinsight.conf** in it and change the **ConfigurationFile** parameter in **web.xml** to:

```
<param-value>  
C:\Program Files\InsightBrowser_Config\BrowserInsight.conf  
</param-value>
```

- 6) Restart Resin or Tomcat

Note: The Initial load of the Browser Insight client will be slow. This is due to the jsp compilation that takes place.

- 7) Launch Browser Insight in your browser, if the upgrade is successful, you should see the following screen



Insight Administrator tools

- 1) Quit the Insight Administrator Tools
- 2) Locate and backup the installation directory for the Insight Administrator Tools
- 3) Replace the following files in the directory the Insight Administrator Tools installed into are with the files from the “admin_tools\manual” directory of the **Insight Upgrade 4.1 CD**

Source	Destination
InsightUpgrade 4.1 CD \admin_tools\manual insightadministrator.jar jai_codec.jar jai_core.jar mlibwrapper_jai.jar	<InsightAdministrator v4.0 Install Directory> \lib insightadministrator.jar jai_codec.jar jai_core.jar mlibwrapper_jai.jar

- 4) Launch the Insight Administrator Tools

Full Install method

This method will produce a complete install of the Insight Server environment.

1. Back up the User Manager and Collection Manager databases.

Note: *You may want to make a copy of these databases for testing before going into a production environment. Apex customer can run a 4.1 collection manager on the same server as their 4.0 version without an Insight Development License. If you would like to run a test environment on a different server, please contact sales@luna-img.com to obtain a development license.*

2. Run the Insight Upgrade installer.

Follow the instructions in the section entitled **Upgrade Collection Manager and User Manager** below. This installer will create and partially configure the necessary Insight components. (i.e. InsightServer.dat, InsightBackend.dat, Insight.dat, Inscribe.dat and the InsightAdminStore.dat)

3. Update Collection Manager and User Manager “.dat” files with collection specific information.

Follow the instructions in following sections:

- **Make Changes to the Collection Manger Configuration Files**
 - **Make Changes to the User Manager Configuration Files**
4. Copy working files from the v4.0 User Manager and Collection Manager folders to their corresponding v4.1 folders.
- Look in the v4.0 User Manager folder for an Image-Group-Files folder. If present (it will only exist if you have defined folders for your users to save groups to, and if they have saved groups to them), copy the folder (and all child folders) to the v4.1 User Manager folder.
 - In all v4.0 Collection Manager folders (one will exist for each Collection Manager), look for any folders with names ending with:
 - Presentation-Files
 - Multi-View-Image-Files
 - Link-Files

If any of them are present (they will only exist if users have created presentations, multi-views or links in that particular collection), copy those folders (and any child folders) to their corresponding v4.1 Collection Manager folders.

Note: *Copying these folders will make all groups, links and presentations created by users in the previous version available to them in v4.1.*

Insight Client Upgrades

Insight Client Upgrade (InstallAnywhere)

- You will need to follow the instructions contained in chapter 2 of this document in a section titled “Package and Distribute Insight JVA Client”
- The source Insight clients for this can be found in the following location

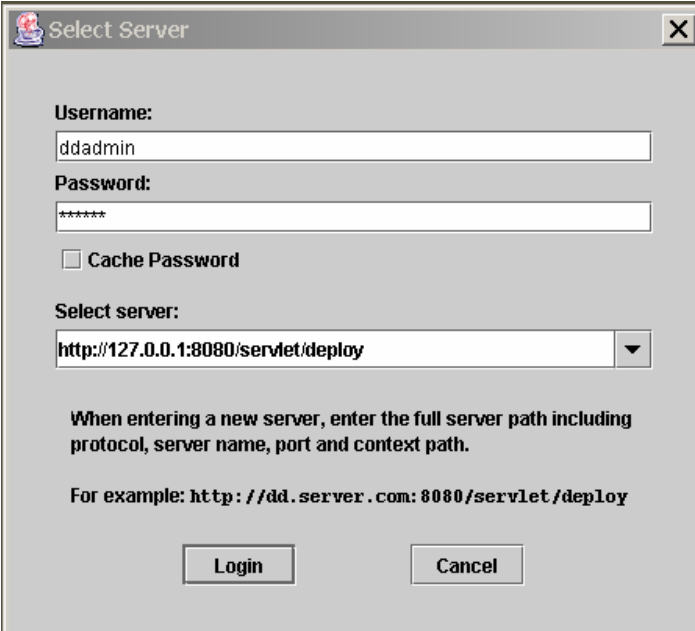
```
<InsightUpgrade 4.1 CD>\insight_client
```

Insight Client Upgrade (DeployDirector)

- Launch Deploy Director Admin

```
(DD_HOME)/DDAdmin/DeployDirectorAdmin.
```

Once you Launch the you will be presented with a Login screen



Select Server

Username:
ddadmin

Password:

Cache Password

Select server:
http://127.0.0.1:8080/servlet/deploy

When entering a new server, enter the full server path including protocol, server name, port and context path.
For example: http://dd.server.com:8080/servlet/deploy

Login Cancel

Enter username: ddadmin Password: f3nd3r or your password

Enter the Selected server. This is the server you installed Deploy Director on. An example is given in the panel.

Click Login

Under the File menu, click Import DAR. Navigate to the bundles directory on the Browser Components CD.

```
<InsightUpgrade 4.1 CD>\insight_client\DeployDirector
```

Select the insight.dar file. You will then be presented with Bundle Version window. The Bundle Name and version Name values should be pre-populated. Click 'OK' to import insight as a bundle. This will import the Insight Application.

Customize insight.dat file for use within Deploy Director

Refer to the [Prepare Insight client configuration file](#) in chapter 2 of this document

Once the bundle has been successfully imported to the server, click the Insight bundle node under the Bundles tab. Expand the node and select the 4.1.0.0 bundle. Now drill down on the tree 4.1.0.0 -> Platform All -> Files. In the right frame, delete the insight.dat file from the files list. Next, go to edit -> add files and navigate to the location to which you saved your customized insight.dat file. . Double click to insight.dat file to add it to the bundle.

Your insight installation is now complete.

Once the DAR has uploaded successfully, go to file -> update server. This will publish the new bundles and the installation and configuration process for deploydirector will be complete.

Verify your Install

To verify that the installation process was successful, open your web browser and enter `http://<installedhost>:8080/servlet/deploy/insight/launch` into the address bar.

When you initially log-in to the page, you will be presented with a Digital Certificate signed by Luna Imaging. After accepting the certificate, DeployDirector will install the necessary files and then launch Insight. When the Insight splash screen appears after the installation process, you know you are ready to deploy Insight.

Upgrade from 3.1 to 4.1 or from 3.5 to 4.1

The order of the process will be as follows:

5. Backup the User Manager and Collection Manager databases.

Note: You may want to make a copy of these databases for testing before going into Production environment. Apex customer can run a 4.1 collection manager on the same server as their 3.1 or 3.5 version without a Insight Development License. If you would like to run a test environment on a different server, Contact sales@luna-img.com to obtain a development license.

6. Run the database upgrade scripts on you User Manager and Collection Manager databases.
7. Run Standards Mapping scripts to implement the Crosswalk standards based on the Getty Metadata Crosswalk. (This is Optional and will require you to re-map your collection standard against the CDWA fields)
8. Run the Insight Upgrade installer. This installer will create and partially configure the necessary Insight components. (i.e. InsightServer.dat, InsightBackend.dat, Insight.dat, Inscribe.dat and the InsightAdminStore.dat)
9. Update Collection Manager and User Manager “.dat” files with collection specific information.
10. Copy Image-Group-Files folder from v3.1/v3.5 User Manager folder and Link and Presentation folders from v3.1/v3.5 Collection Manager Folders.

Upgrade Databases

Backup Databases

Note: It is strongly recommended that you have to backup the current Collection Manager database and User Manager database before upgrading the databases. In case that the upgrade failed, you should contact Luna Tech Support.

Upgrade Databases

You need to upgrade you database to Insight 4.1 level by running the SQL scripts provided on the CD of Insight Upgrade V4.1.

Note: With the addition of export presentation feature in Insight we are setting the default for the upgrade to the highest resolution for all profiles. If you would like to disable this feature for a particular profile or lower the resolution, edit the profile in the insight administrator tools.

Note2: After running the Crosswalk upgrade scripts you will need to remap your collection fields to CDWA fields to enable cross collection searching. You can perform this mapping in the Insight Administrator Tools.

For Microsoft SQL server:

Run the following scripts using Query Analyzer or ISQL provided by Microsoft SQL Server

1. Upgrade Collection Manager database

a. 31 to 41

```
\MSSQL\31 to 41\31 to 41 mssql.sql
```

b. 35 to 41

```
\MSSQL\35 to 41\35 to 41 mssql.sql
```

2. Upgrade User Manager database

a. 31 to 41

```
\MSSQL\31 to 41\IUM 31 to 41 MSSQL.sql
```

b. 35 to 41

```
\MSSQL\35 to 41\IUM 35 to 41 MSSQL.sql
```

3. Remove old standard mappings from your Collection Manager database

Note: This step must take place before the next step

```
\MSSQL\Crosswalk_Standards\removeOldSLStandardData.sql
```

4. Add Getty Crosswalk Metadata Standard Mappings to your Collection Manager database

```
\MSSQL\Crosswalk_Standards\InstallCrosswalk.sql
```

For Oracle:

Run the following SQL script using SQLPLUS or other utilities provided by Oracle

1. Upgrade Collection Manager database
 - a. 31 to 41

```
\Oracle\31 to 41\31 to 41 Oracle.sql
```

- b. 35 to 41

```
\Oracle\35 to 41\35 to 41 Oracle.sql
```

2. Upgrade User Manager database
 - a. 31 to 41

```
\Oracle\31 to 41\IUM 31 to 41 Oracle.sql
```

- b. 35 to 41

```
\Oracle\35 to 41\IUM 35 to 41 Oracle.sql
```

3. Remove old standard mappings from your Collection Manager database

Note: This step must take place before the next step

```
\Oracle\Crosswalk_Standards\removeOldSLStandardData.sql
```

4. Add Getty Crosswalk Metadata Standard Mappings to your Collection Manager database

```
\Oracle\Crosswalk_Standards\InstallCrosswalk.sql
```


Upgrade Collection Manager and User Manager

Install Upgrade

To upgrade your Insight Collection Manager and User manager, you need to run the installer on the CD for Insight Upgrade 4.1 at the system where your current Collection Manager and User manager are installed respectively:

Windows: \user_and_collection_managers\windows\installUpgrades.exe

Solaris: \user_and_collection_maangers\solaris\installUpgrades.bin

Please follow the instructions in the installer to place the Insight Collection Manager and User Manager file structures for you. The Insight Upgrade Installer offers two options:

- Typical

This option will upgrade both the Collection Manager and User Manager at a single machine.

- Custom

This option will install the component(s) you select to a machine

- Collection Manager, or
- User Manager

Note: During the installation, a script is automatically invoked, and you must respond to its prompts with the correct information about the hostname of the machine your Collection Manager .

If for any reason the install script does not run, you can run it manually after the installer completed.

On Windows in a dos prompt:

```
cd <install directory> -- change directories to the install  
directory
```

Run the following command:

```
support\bin\perl.exe support\install.pl "<install  
directory>" <user or collection>  
Note: the install directory should be in quotes
```

On Solaris, in a terminal:

```
cd <install directory> -- change directories to the install  
directory
```

Run the following command:

```
perl support/install.pl "<install directory>" <user or  
collection>
```

Make Changes to the Collection Manger Configuration Files

After the successful completion of upgrade installation, please Go to the <installation directory>/collection_manager/<collection_name>/ and make the following changes

1. Edit InsightBackend.dat
Note: this step is only required for Oracle database

Change the DefaultUsername and DefaultPassword to the proper oracle user for this collection.

2. Edit InsightServer.dat
 - Change port number if you would like the collection manager to listen to a different port
 - Note: this step is only required for Microsoft SQL Server.

Adjust the "DatabaseConnect =" string to point to the correct database where it says "database=" and change the "user=" and the "password=" portion for database authentication.

Make Changes to the User Manager Configuration Files

Go to the <installation directory>/user_manager/ and make the following changes:

1. Edit InsightBackend.dat
Note: this step is only required for Oracle database
Change the DefaultUsername and DefaultPassword to the proper oracle user for this collection.
2. Edit InsightUserServer.dat
 - Note: This step is only required for Microsoft SQL Server
Modify the "DatabaseConnect =" string to point to the correct database where it says "database=" and change the "user=" and the "password=" portion for database authentication.
 - Change the "MultipleCollectionImage =" to point to the correct cross collection background
 - Change the RGB setting for the MultipleCollectionColor settings

Copy Image-Group-Files, Link and Presentation folders from v3.1/v3.5/v4.0 Install

Locate the Image-Group-Files folder in you v3.1/v3.5/v4.0 User Manager folder and copy it to the Install location of your new User Manager.

Locate the Links and Presentation folders in you v3.1/v3.5/v4.0 Collection Manager folder and copy it to the Install location of your new Collection Manager.

Note: This makes the groups, links and presentations that were available in you previous version available in v4.1

Reset Browser Thumbnail fields in Collection Configuration

Using the Insight Administrator Tools set the browser thumbnail fields for your collection. Refer to the Edit Browser Attributes section in the Insight Administrator Tools Documentation to make these adjustments.

Upgrade Insight Client

Please follow the instructions in Chapter 2 in the section of “Package and Distribute Insight Client.” The Insight 4.1 client is located on the CD of Insight Upgrade 4.1 under the directory of insight_client. Use your existing configuration Insight.dat as a part of the client package to be distributed if you maintain the same User manager and other parameters.

Upgrade Insight Administrator Tools

Note: Insight Administrator Tools V4.1 will only work with the collections at Insight V4.0 or 4.1 level. If you would have collections in Insight 4.0/4.1 as well in Insight 3.1.1 concurrently for a period, you must continue to use Administrator Tools V3.1.1 to manager the collections at V3.1.1 release level. Therefore it is recommended that you install the Insight Administrator Tools V4.1 at a directory different from the directory where the Insight Administrator Tools V3.1.1 is installed.

Follow the steps below to upgrade Insight Admin Tools:

1. Back up the existing Admin Tools configuration files. If you already have Insight Admin Tools installed, locate the configuration file **InsightAdminStore.dat** , **compro.exe**, and **Iservrc** in the system, and save a copy of the files by renaming the copies to **InsightAdminStore.bak**, **compro.bak**, and **Isevrc.bak**.

Note: This step is only applicable if you have a previous release of Admin Tools installed on your system.

2. Start - Insert the CD for **Insight Upgrade V4.1** into your workstation where Admin Tools will be installed.
3. Install:

Windows Locate and execute the file **installAdministrator.exe** under the **admin_tools\windows** directory on the CD. Follow the directions in the installation package to install the system.

Solaris Locate and execute the file **installAdministrator.bin** under the **admin_tools\solaris** directory on the CD. Follow the directions in the installation package to install the system.

Insight Browser Upgrade

Please refer to the chapter for the installation and configuration for Insight Browser Server. You will need to perform a full install for this upgrade.

Help file links for Insight Applications

Below are links to the help files for the Insight client, Inscribe client and Insight Browser client. If your institution requires these help links to reside on a local server please contact Luna Imaging support department.

Email: support@luna-img.com

Phone: (800) 452-LUNA

Insight client http://www.lunaimaging.com/v4_0help/insight/insight4.htm

Inscribe client http://www.lunaimaging.com/v4_0help/inscribe/inscribhelp.htm

Insight Browser client http://www.lunaimaging.com/v4_0help/browser/insightbrowser.htm

Installation and Configuration for InSight Standard

Installation Concepts:

The Insight Standard package contains three unique server components:

- The User Manager
- The Collection Manager
- the Media Server (Either IIS or Apache)

The installation package will also install the following:

- Java Runtime Environment
- Sprinta JDBC Driver for Microsoft SQL Server
- Oracle Thin JDBC Driver for Oracle
- VRA Model contents
- Sample Rumsey Collection contents
- AAT vocabulary contents

These components, along with either Microsoft's SQL Server 7, SQL Server 2000 or an Oracle 8i or 9i database can be distributed across multiple machines, or be situated on specifically one. The basic concept is that depending on your hardware, you may want to separate components to complement your current hardware. You may have one dedicated machine which hosts all of your Insight components, or multiple machines that host specific components.

Installation and Configuration Check List

The following is a checklist to help you to install and configure Insight components and to also provide other system related information that you may need. Also, you can use the checklist for configuring the related components.

Insight Component	Required	Host Name of System	Database Port Number	Database User Name	Database User Password
User Manager	Yes				
Collection Manager	Yes				
Media Server	Yes				
Browser Server	Optional				
Insight JVA client	Yes				
Insight Administrator Tools	Yes				
Inscribe Data Editor	Optional				

Install Insight Standard servers

Pre-Configuration:

You will need the following information before you Install Insight Standard on your machine:

- 1) the hostname or IP address of the machine your are running the Collection Manager and/or User Manager
- 2) The name of your database
- 3) An administrative username / password for the database you are installing the insight standard databases to. Note: the user must have the permissions to create new users, create new databases and or tablespaces.
- 4) The TCP/IP port your database is running on (usually 1433 for MS SQL and 1521 for Oracle)
- 5) For Oracle specifically, you will need the SID name

NOTE: For MS SQL users: Insight requires the use of SQL Authentication, to turn on SQL authentication if you are using trusted authentication, contact your Database Administrator

NOTE: for Solaris users: The installation requires perl to be in the path + openwin to be installed (for xTerm access). If you do not have openwin installed, you can run the installation script manually after you have run the installer, information on running the script manually is located further on in this chapter.

Prepare Database

A relational database is an important part of the Insight system. The installation and configuration steps below assume that you have already installed and configured your relational database. If you have not, then you need to do the following:

- Install and configure either Microsoft SQL Server or Oracle if you have not already (see the documentation included with your database for more information).
- Create a database user that has the permissions to create new users, new databases and/or table spaces. The user ID and password of the user will be used by Insight servers to interact with the database.

Insight needs a set of tables and contents established in the database for its operations. The following preparations will create the necessary tables, and populate them with contents.

Run the Installer:

The installer is located on the CD for Insight Standard:

Windows: \user_and_collection_manager\windows\InstallStandard.exe

Solaris : \user_and_collection_manager\solaris\InstallStandard.bin

When running the installer, it allows you to install any / all of the insight components on a machine. Here are the options:

- Typical

This option will install both the Collection Manager VRA and User Manager at a single machine, and populate contents to a single database located on the same machine.

- Custom

This option will install the component(s) you select to a machine

- Collection Manager VRA or Base Collection Manager (choose one only), and/or
- User Manager

It's highly recommended to select the Typical installation, which will install both the User Manger and the VRA Collections Manager at the same time. The Typical installation will

- Set up the directory structure for your 4.1 installation

- Install the following components
 - o User Manager server code
 - o Collection Manager server code
 - o Java Runtime Environment 1.4
 - o Sprinta JDBC Driver for Microsoft SQL Server
 - o Oracle Thin JDBC Driver for Oracle
- Run a perl script to walk you through the configuration of the servers, the script will
 - o Create schema for User Manager and add contents to the database
 - o Create schema for Collection Manager to the database
 - o Create VRA model schema and add contents to the database
 - o Create AAT vocabulary schema and add contents to the database
 - o Add contents of the sample collection to the database
 - o Create configuration files for Insight client, Administrator Tools, and Inscribe Data Editor.

Note: The script is automatically invoked when running the installer, and is intended to help you configure your installation. Please respond to the prompts in the text window.

Instructions to run the perl script manually:

If for any reason the install script does not run, you can run it manually after the installer completed.

On Windows in a DOS prompt:

```
cd <install directory> -- change directories to the install  
directory
```

Run the following command:

```
support\bin\perl.exe support\install.pl "<install  
directory>" <user or collection>
```

Note: the install directory should be contained in quotes

As the install script runs, it will ask a series of questions in order to properly install insight, you must respond to the questions with correct information. While running, the install script will create a series of SQL scripts which will be placed in the <Install directory> for later use.

Note: you can install both the user and collection manager by entering the following:

```
support\bin\perl.exe support\install.pl "<install  
directory>" "user,collection"
```

(there's no space between user and collection)

On Solaris, in a terminal:

```
cd <install directory> -- change directories to the install  
directory
```

Run the following command:

```
perl support/install.pl "<install directory>" <user or  
collection>
```

Note: the install directory should be in quotes

As the install script runs, it will ask a series of questions in order to properly install insight, you must respond to the questions with correct information. While running, the install script will create a series of SQL scripts which will be placed in the <Install directory> for later use.

Note: you can install both the user and collection manager by entering the following:

```
support\bin\perl.exe support\install.pl "<install  
directory>" "user,collection"
```

(there's no space between user and collection)

Register Your License

In the end of the installation, it will bring up a web based form for registering your license. Please fill out the information, which will be sent and stored in Luna Imaging's system. Click "Done" to complete the installation.

Activate AAT Vocabulary

To activate the AAT Vocabulary, please contact **Luna Help Desk** at 1-800-452-LUNA (1-800-452-5862) – ext. 268, or email to support@luna-img.com

Connect and Configure the Database for Insight Servers

Microsoft SQL Server installation:

Once you complete the installation script, it will attempt to connect to your database (if it is local) and attach the User and Collection managers. If it encounters any errors, these will be displayed on the screen and written to the install log (found in the <install directory>). The script will also output the SQL to properly mount the databases later if there are problems, these too are placed in the <install directory>.

NOTE: if you have errors, or, are mounting the database on a different machine than the machine you are running the server on, the installer creates SQL scripts that can be used to manually mount the database. These are located in the install directory. You will need to edit the first line to tell the SQL server where it should find the database file, and then run it in ISQL or Query Analyzer on the database server. The SQL files are:

- <Installation Dir>\insight_attach_user.sql
- <Installation Dir>\insight_attach_vra.sql

Oracle Installation:

In order to configure Insight to use Oracle, you will need to create the following:

- tablespace for the InsightUser database
- tablespace for the InsightVRA database

- An INSIGHTUSER userid
- An INSIGHTVRA userid

To help you through the process, we have provided sample SQL scripts in the installation directory. These have been set up based on the answers to the installer questions. The files are:

- insight_attach_oracle_user.sql
- insight_attach_oracle_vra.sql

Once you have run these (or modified them and run them). You must import the database by running the Oracle Import command. See the following files in the installation directory:

- oracle_imp_user.command
- oracle_imp_vra.command

Finally, update the statistics by running these SQL scripts:

- insight_stat_oracle_user.sql
- insight_stat_oracle_vra.sql

Start the Servers

After the installation of the Collection Manager and User Manager, they are started as non-service applications.

Manually Start Collection Manager and User Manager on Windows

You can manually start the Collection Manager by double-clicking on the following executable:

```
<Installation  
Dir>\collection_manager\vra\InsightCollectionManager.exe
```

You can manually start the User Manager by double-clicking on the following executable:

```
<Installation Dir>\user_manager\InsightUserManager.exe
```

Manually Start Collection Manager and User Manager on Solaris

You can manually start the Collection Manager by running the executable from the command-line:

```
<Installation  
Dir>/collection_manager/vra/InsightCollectionManager
```

You can manually start the User Manager by running the executable from the command-line:

```
<Installation Dir>/user_manager/InsightUserManager
```

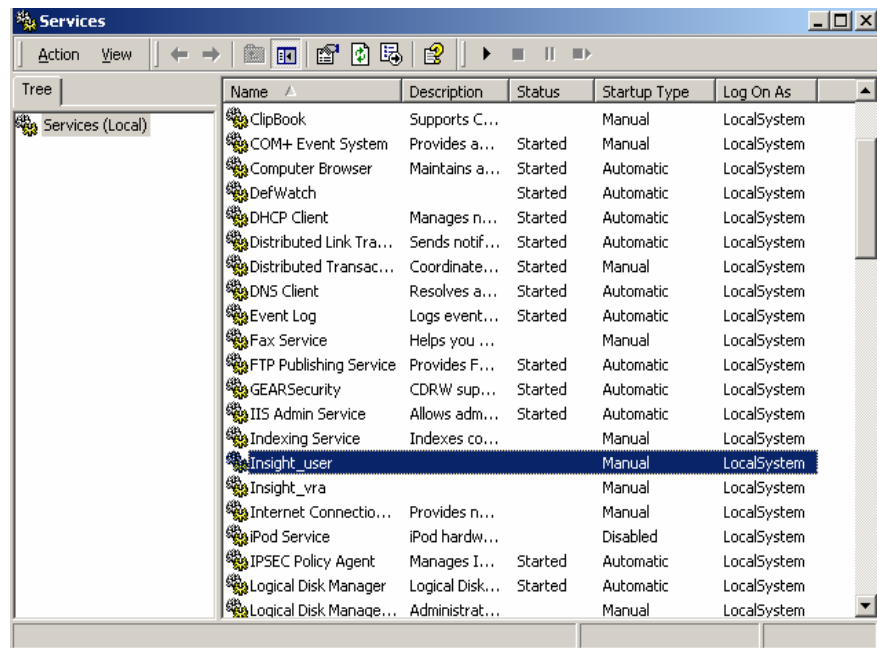
Run Collection Manager and User Manager as service on Windows (Optional)

To install your user manager or collection manager as a service on a WindowsNT/2000 platform follow the instructions below.

Note: We also recommend a product called Service Mill from <http://www.activeplus.com/>. This tool allows you to create a windows service for any application. It has many helpful features and is all GUI based, No registry edits.

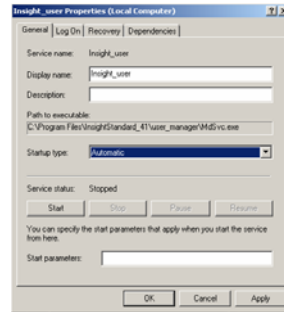
- Locate your Insight Standard directory (the default is "C:\Program Files\InsightStandard") and go into the collection_manager\vra folder.
- Run the "Install As Windows Service.exe" file, and you will see an application come up called "JMidoriService Configure Utility"
- Go to the install tab and press the "Install NT service"
- Test that the service is working.
 - Delete the file called "DatabaseConnector.txt"

- Go to your service control panel and look for the appropriate service i.e. Insight_vra (for running the Collection Manager as service), or Insight_user (for running the User Manager as service). Start the service.
 - Go back the folder that you deleted the “DatabaseConnector.txt” file from and verify that it has been recreated.
 - Launch the Insight JVA Client and try logging into the collection
- **Note:** If you are not able to connect to the collection using the Insight JVA client while the collection manager is running as a service, but are able to run the collection manager when it has been started manually, follow the instructions below:
- locate the installation directory for the user or collection manager, for Insight Standard, this is “c:\program files\InsightStandard”
 - copy the “jre” folder inside the installation directory into the “collection manager” folder
 - restart the service, and try connecting
- To set the service to run automatically:
- Launch the “services” control panel, located in the “administrative tools folder”



- Locate the service you would like to set to launch automatically and double-click it to get properties

- change the startup type from manual to automatic and click ok



Make the service dependent on MSSQL Server Agent.

Note: This step will instruct you to use Registry Editor. Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows. Microsoft does not guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

You should make a backup copy of the registry files before you edit the registry.

Note: The Insight collection manager requires immediate connectivity to the database or the collection manager will not function. For this reason you will need to make sure your database is running before you bring the collection manager up. For this reason you need to make the collection manager and user manager dependent on SQL Server Agent by doing the following:

- Go to start menu and select run.
- Run regedt32 (Note: please type exactly as spelled here)
- Go to the panel that says "HKEY_LOCAL_MACHINE"
- Go down the tree and select SYSTEM/CurrentControlSet/Services/Insight_vra for specify Microsoft SQL server as dependent service for the Collection Manager and select SYSTEM/CurrentControlSet/Services/Insight_user for specifying Microsoft SQL Server as dependent service.
- Under the Edit menu choose Add Value. In the Value Name enter "DependOnService", in the Data Type select "REG_MULTI_SZ", and click OK
- A data window will be displayed, and enter your dependency application
- Now in the right panel you will see your new value. Double click on it.
- Enter "SQLSERVERAGENT" in the box provided, and click OK
- Verify that the service now has a dependency. Go to your services control panel and double click on the service you just changed in the registry and click on Dependencies. You should see the dependency you added

Determine Whether the Collection Manager Is Running Properly:

If the Collections Manager starts properly, it will run for a while (sending text to the console). When the text stops, it should display the following message indicating success:

```
vra: Accepting connection.
```

If the user server starts properly, it will display a short amount of text concluding with the following message, indicating success:

```
IUS: Accepting connection.
```

If you have problems installing (general):

- check that the admin user has the permission to create users and mount databases
- check that the database attached properly (if it didn't, attach it using the SQL script) for more information see the previous section regarding manual installation
- then try running the server

Note: If the installation is verified to be successful, it is strongly recommended that you turn off the debug messages to improve server performance. The debug messages are turned on by setting `DebugLevel = 3`, and turned off by setting `DebugLevel = 0`. The parameters can be changed by editing and saving the following files:

User Manager: <Installation Dir> \user_manager\InsightUserServer.dat

Collection Manager: <Installation Dir> \collection_manager\InsightServer.dat

Users Created

A successful installation for Insight Standard will create five users – Student, Faculty, Cataloger, Editor and Admin with different privileges:

INSIGHT® INSTALLATION AND
CONFIGURATION MANUAL

Permission	Username				
	Student	Faculty	Cataloger	Editor	Admin
User Manager Specific Permissions (general)					
username	Student	Faculty	Cataloger	Editor	Admin
password	*****	*****	*****	*****	*****
User Manager Specific Permissions (access to coll.)					
Access to VRA Collection	Y	Y	Y	Y	Y
Collection Name	Demo Collection - VRA				
Collection ID	100				
IP of Collection Server	localhost				
Port for the Collection Server	300				
Virtual Collection?	No				
User Group Name	STUDENT	FAC	CAT	EDITOR	ADMIN
User Group Code-Key	STUDENT	FAC	CAT	EDITOR	ADMIN
User has access to collection	Y	Y	Y	Y	Y
User can save a group from collection level folder*	No	Y	Y	Y	Y
User can delete a group from collection level folder*	No	Y	Y	Y	Y
Access to Faculty Folder	N	Y	N	N	Y
User can save a group from faculty folder	N	Y	N	N	Y
User can delete a group from faculty folder					
Access to Student Folder	Y	Y	Y	Y	Y
User can save a group from student folder	Y	Y	Y	Y	Y
User can delete a group from student folder	Y	Y	Y	Y	Y
Collection Specific Permissions (general)					
Specify an image set (SPS) for user	1	1	1	1	1
Restricted by IP	No	No	No	No	No
Collection Specific Permissions (viewing)					
Allow User to Save a group	N	Y	Y	Y	Y
Allow user to delete a group	N	Y	Y	Y	Y
Max Export Resolution (0-8)	<384px	ALL	ALL	ALL	ALL
Max Print Resolution (0-8)	<384px	ALL	ALL	ALL	ALL
Max Viewable Resolution (0-8)	<6114px	ALL	ALL	ALL	ALL
Allow Exporting of HTML	N	Y	Y	Y	Y
Allow export of Presentation (0-8)	NO	<1600x1024px	<800x600px	<1280x960px	ALL
Collection Specific Permissions (editing)					
Allow editing of image links	N	N	N	Y	Y
Allow editing of multi-views	N	N	N	N	Y
Allow editing of multi-page-documents	N	N	N	N	Y
Inscribe Permissions					
Allow editing of data	N	N	Y	Y	Y
Allow vocabulary editing	N	N	N	N	Y
Allow user to view data	N	N	Y	Y	Y
Allow user to edit data	N	N	N	Y	Y
Allow user to add data	N	N	Y	Y	Y
Allow user to delete data	N	N	N	N	Y
Allow user to modify links between entities	N	N	Y	Y	Y
Allow user to modify links between records and images	N	N	N	Y	Y
Allow user to write to Source tables	N	N	N	N	Y
Allow user to write to insight tables	N	N	N	Y	Y
User permission level (lower number supervised by higher number 1-6)	NA	NA	1	3	6
Allow user to add entries to controlled vocabularies	N	N	N	Y	Y

* provided for reference but user does not have rights to actually control

Install the Media Server

Copy the Media Files for the Sample Collection

Copy the directory Demo and all the directories and files below from the CD for Insight Standard under the directory of

\Demo_Collection_Media

to your desired directory.

Note: The directory structure from Demo below (including Demo) must be preserved when copying the media files.

Set up access to media files from Browser Servers

For IIS

- Make a virtual directory called "Demo" that points to the Demo directory you just copied all the directories and files to. For instance, if you have copied all the media files to

C:\MyMediaFiles\Demo\...

Your virtual directory Demo will point to the physical directory of
C:\MyMediaFiles\Demo

- Make a virtual directory by invoking the Internet Service Manager, select Default Website/New/Virtual Directory, and "Demo" as the virtual directory and point to the physical directory of "C:\MyMediaFiles\Demo."

For Apache

- Make a symbolic link to the Docroot of Apache called "Demo" that points to the Demo Folder you just copied all the media files into.
- Make a symbolic link to Docroot/mrsid/mrsid_images/demo

Install and configure the MrSID Image Server

The MrSID media server serves high resolution SID files to Insight clients. You need to install the MrSID server on a system where either IIS or Apache is installed and configured. Following are the steps:

For Windows NT and 2000 with IIS:

1. Install Active Perl, by running the Active Perl installer on the CD of Insight Standard, under the directory:

\media_server\IIS

2. Install LizardTech NT MrSID Server by invoking the installer on the CD for Insight Standard and follow the installation instruction:

\\media_server\IIS\MrSIDImageServer.exe

3. Configure MrSID Server:

Configurations take place in the Internet Service Manager. You can find Internet Service Manager from

Start Menu/ Programs/Administrative Tools/

Or

Start Menu/Settings/Control Panel/Administrative Tool/

Warning: Do not use the HTML-base Internet Service Manager.

Add index.plx to the list of default documents:

- Select the default web site
- Right-click on the icon and choose Properties
- Select the Documents tab
- Click Add
- Type "index.plx" (it is a low case L)
- Click Apply
- Click OK to exit Properties

Set sid/bin directory executable.

- Right-click on the sid/bin directory
- Select Properties
- Select the Directory tab
- Locate the Permissions radio buttons or drop down list
- Select the Execute (including script) option
- Click Apply
- Click OK

Make the sid/bin/tmp directory writable:

- Right-click on the sid/bin/tmp directory
- Select Properties
- Using the check boxes or drop down list, set the Permissions to "Script Source Access"
- In Access Permissions, enable Write access
- Click Apply

- Click OK

Create an alias for SID collection images:

- Right-click on the sid directory
- Select New / Virtual Directory
- In the “New Virtual Directory Wizard” provide an alias for your SID directory, e.g. test_sid.
- Next, enter the physical path of your SID Image Directory.
- Using the check boxes or drop down list, set the Permissions to “Allow Read and Script Access”, and click Next.
- Select Finish.

4. Test the installation and configuration:

To verify that the installation and configuration is successful, invoke browser to display the following URL:

<http://localhost/sid>

The MrSID user interfaces will be displayed, and you can test its functions.

For Solaris and Linux with Apache:

1. Install perl v. 5.6.1+ on your web server
2. Enable your web server to process .pl files

Make sure that your httpd.conf allows .pl using the handler by adding the following section to the file

```
# To use CGI scripts:  
#  
AddHandler cgi-script .cgi .pl
```

3. Install the MrSID Server by installing the appropriate packages that can be found on the CD for Insight Standard:

Solaris: \media_server\apache\mrsidserver_sun.2.2.tar.gz

Linux: \media_server\apache\mrsidserver_linux.2.2.tar.gz
4. After the package is installed, please follow the instructions under the directory of /mrsid/help to configure it.
5. Configure the appropriate directories to run scripts:

Make sure that the following directory and below have the ExecCGI permission enabled.

- /mrsid/

NOTE: The ExecCgi option can be turned on in two different places (depending on your configuration)

You can turn it on with the following line:

```
Options ExecCGI
```

Depending on your configuration (mainly whether your administrator allows you to change your apache settings for running cgi scripts via the .htaccess file) you may need to adjust the settings in either the httpd.conf or in an htaccess file. If you're not sure, check the httpd.conf, if the default directory has the line "AllowOverride None", you probably need to edit it and create specific directory listings:

- a) it can be turned on in your .htaccess file
- b) it can be turned on using a <DIRECTORY></DIRECTORY> setting in your httpd.conf

6. Test the installation and configuration:

To verify that the installation and configuration is successful, invoke browser to display the following URL:

<http://localhost/mrsid>

If you run into problems, see the MrSID Doc.

Package and Distribute Insight JVA Client

Insight JVA is a Java client with rich functions. It runs on end-users' PCs or Macs to access Insight collections. The client needs to be customized so it can access the Insight User Manager in your installation.

Note: For the Insight client to run properly on a locked down system, the Insight-Cache folder in the install location needs write privileges. This is only a problem on locked down computer systems. If you need more information about distribution of the Insight client in a controlled or locked down environment, please contact our support department at support@lunaimaging.com.

The installer for Insight JVA client is located on the CD for Insight Standard:

Windows: \insight_client\windows\installInsight.exe

Mac OSX: \insight_client\macosx\InstallInsight.zip

Prepare Insight client configuration file

The Insight client package includes a configuration file (Insight.dat), which specifies the address of the User Manager that the client should be connected to, as well as other configuration parameters.

Note: When the User Manager and Collection Manager were installed, a configuration file called `Insight.dat` was automatically created in an adjacent directory called `dat_files`. It was configured to use the address of the system where the User Manager was installed as the user manager address. If you choose to use the created file as the configuration file, please review it, skip the step below, and go directly to “Package Insight Client” step.

If you would like to customize the `Insight.dat` file, here are the steps:

- Customize the file `Insight.dat` under the directory of `insight_client`. The `Insight.dat` file looks like the following before customization:

```
# Insight.dat
# Insight configuration file
#
# Lines starting with # signs are comments.
#
# UserServerAddress1 - the address of the user server.

# This address provides access to all collections

UserServerAddress1 = InsightUser.lunaimaging.com
# DefaultCollectionToOpen - If specified, this
# collection will be opened
# automatically at startup time. The user
# may still change the open a collection later by
# using the File menu's "Open Collection" option.
# If this value is not specified, the user will
# see a list of collections at startup time.

#DefaultCollectionToOpen =
#DebugLevel = 3

#DefaultUserName = user
#DefaultUserPassword = user
```

Change the User Manager server name to the hostname of the system where Insight User Manager is installed. For instance, if the hostname of the server is www.insightusermaneger.mycollege.edu, please change the line in `Insight.dat` to the following:

```
UserServerAddress1 = insightusermanager.mycollege.edu
```

Note: Versions 4+ of insight allow for multiple user managers to be defined. The syntax is as follows

```
UserServerAddress1 = insightusermanager.mycollege.edu
UserServerAddress2 = insightuser.lunaimaging.com
```

You can also set the `DebugLevel` and enter your `DefaultUserName` and `DefaultUserPassword`. If the **DefaultUserName** and **DefaultUserPassword** properties are set to a valid user name and password, the Insight client user

will not be asked to enter user name and password when accessing the collection.

Note: Any line beginning with # is a comment, and is ignored by the system. Comments exist only to assist you in preparing the file. They provide explanations and present alternatives. Be sure that the *UserServerAddress1* line is turned on (does not have a leading #).

Package Insight client

For Windows systems:

To distribute Insight JVA client to your end users, you need to repackage *installInsight.exe* with your customized configuration file *insight.dat* (see step above). The Insight JVA installation files for Windows are located on the CD for Insight 4.1 under the directory: *insight_client\windows*. Here are the steps to make the package for the end-users using Windows:

- 1) If you do not already have the WinZip archive utility and WinZip Self-Extractor, download and install them. (It is recommended that you order the software instead of merely downloading the trial copies. Though trial copies generate the package correctly, they produce a message indicating that unlicensed copies were used when end users unzip and install the package.)
 - For the trial copy of WinZip Archive Utility:
<http://www.winzip.com/downau81.cgi?winzip81.exe>
 - For the trial copy of WinZip Self-Extractor
<http://www.winzip.com/downauto.cgi?wzipse22.exe>
- 2) Start WinZip Self Extractor, select “**Self-extracting zip file for Software Installation,**” and press **Next**.
- 3) At the next panel, leave “**Span multiple removable disks**” unchecked, and press **Next**.
- 4) Next, press “**Run WinZip**”.
- 5) After passing the first two panels of WinZip by pressing **Next**, select “**Create a new Zip file**”.
- 6) Follow the instructions and create a Zip file (for example, *insight_and_dat.zip*) containing *installInsight.exe* from the the directory of *insight_client\windows* on the CD of Insight Standard, and your customized configuration file *insight.dat*.
- 7) After the Zip file is created, close the WinZip panel.
- 8) Return to WinZip Self Extractor (or you can restart it, and select “**Self-extracting file for software installation**”), select the Zip file you just created (for example, *insight_and_dat.zip*), and press **Next**.
- 9) In the next panel, enter the message you would like your end user to see when the files are self-extracted, and press **Next**.

- 10) Leave “**Unzip automatically**” unchecked, select English or German as the preferred language, and press **Next**.
- 11) ***Important:*** Enter `.installInsight.exe` under “**Command to issue when unzip operation completes.**” Leave “**Wait for**” blank, and press **Next**.
- 12) Enter your message, (which will be displayed when the package is unzipped and installed), and press **Next**.
- 13) Enter the information to be displayed in the “**About**” box (if desired), and press **Next**.
- 14) In the next panel, select your own icon (if desired), and press **Next**.
- 15) In the last panel, review all of your selections and all messages you have prepared. After verifying them, press **Finish**, to create the self-extracting executable file.
- 16) Test the self-extracting package to verify that it works correctly.

Place the self-extracting package in a location from where your end-users can download.

End-users will download the self extracting package, launch it, and follow the instructions to install the JVA. For users who have previous releases of Insight JVA installed, installing the new release of Insight JVA in the same location will cause their old **Insight.dat** file to be overwritten by the new one you packaged with *installJVA.exe*.

For MacOSX systems:

Note: you must do the following steps on a Mac OSX machine.

You need to take the following steps:

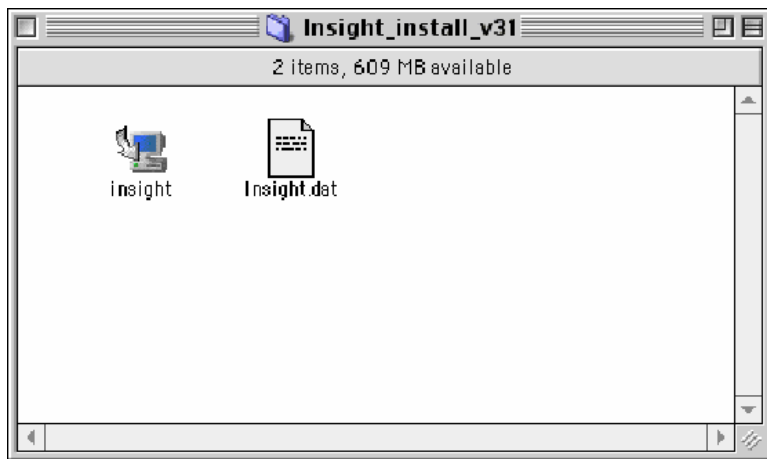
1. From the CD for Insight Standard, locate the file `installInsight.zip` under the directory of `\insight_client\macosx` unzip it to a directory on the Mac OSX machine, e.g. `<unzip directory>`.
2. Copy the `insight.dat` file that was created under the `<Installation Directory>\dat_files` on the system where User Manager and Collection Manager were installed to the same directory `<unzip directory>`, where you unzipped files, including the installer of `installInsight`, are located.
3. Make a new zip file (or other compressed package that can be processed and accepted under Mac OSX) containing both `InstallInsight` installer and `insight.dat`

For MacOS 9 systems:

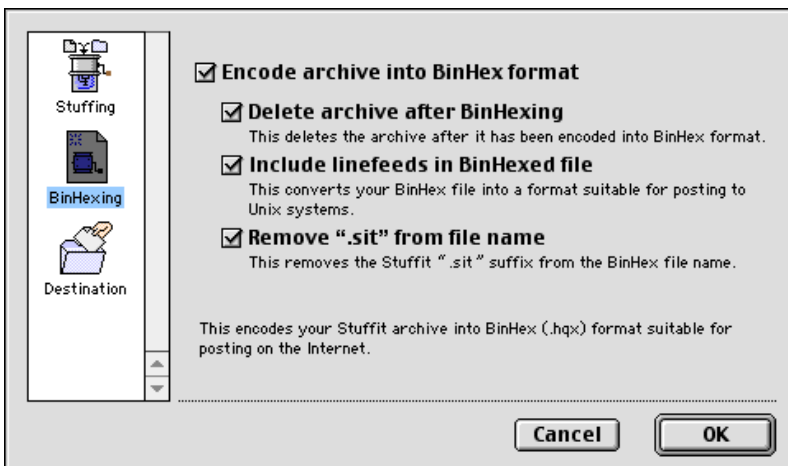
Note: Insight 4.1 JVA client requires JRE 1.3, which is not supported by Mac OS 9 and below. If you need to distribute Insight client for such systems, please go to the web site of www.lunaimaging.com, download Insight client 3.1.1 for Mac OS, and package it following the steps below. However, you need to be aware that Insight 3.1.1 will just run a compatible mode to Insight 4.1 servers, and will not have the new features provided in Insight 4.1

The Insight JVA 3.1.1 installation files can be downloaded from www.lunaimaging.com. And are also contained on the Insight Upgrade CD and the Insight Standard CD. In the subdirectory \insight_client\MacOS9

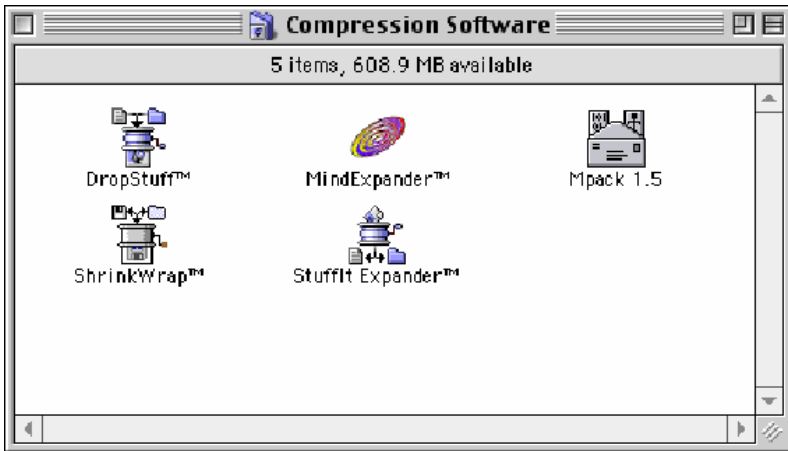
- Logon to a **MacOS** machine
 - Access **installJVA.bin** from and the customized **Insight.dat** from the steps above
 - Copy the installer **installJVA.bin** and the customized **Insight.dat** file into a new folder on your desktop.
1. Here is what your folder (from the created and pasted installer and adapted **Insight.dat** file) will look like:



2. Next, search for **DropStuff** and Set the **DropStuff** preferences. Make sure you select **BinHexing** and check all the boxes listed above.



3. Once the preferences are set, drag the folder containing the installer and the updated **Insight.dat** file onto the **Dropstuff** icon. Make sure the **Insight.dat** is renamed to a **.dat** and not a **.txt** file.



4. Once the stuffing process is completed, you will see an icon on your desktop called **#####.hqx**, which is the file you will distribute to your MacOS users. Open this file. You will see the stuffed version of the installer and a reconfigured **Insight.dat** file in a folder on your desktop. You should rename the file to **Insight400.hqx** or some other desired name before distribution. **DO NOT** change the file type of **hqx**.
5. After receiving the package, the MacOS user opens the folder and installs Insight using the installer in this folder. When you install from this installer, the properties from your updated **Insight.dat** file should hold.

Distribute Insight clients

Once the Insight client has been packaged, you can distribute it to end users by sending them the installable package, or by staging it on a website for them to download.

For Windows: The user receiving the client package will invoke the self extracting package, and follow instructions to install the client.

For Mac OSX and Mac OS 9: The user receiving the client package will unzip the package, and invoke the installer.

Install and Configure Inscribe

Inscribe is a data editor to be used to enter, edit, update, delete and maintain the data in a collection. You need to install Inscribe on the machine where the Inscribe user will work on.

Note: The number of Inscribe users is limited by the type of Insight License Agreement you have with Luna.

Please follow the steps to install Inscribe:

- Install Inscribe on the user machine using the following installer located on the CD for Inscribe 4.1

For Windows: \windows\InstallInscribe.exe

For Mac OSX: \macosx\InstallInscribe.zip

At the end of installation, you need to fill out the registration form. It is mandatory.

- Copy the file Inscribe.dat generated by the installer for Insight Standard in the directory of \dat_files under the install directory of Insight Standard, to replace the Inscribe.dat in the install directory of Inscribe.

Install and Configure Administrator Tools

Administration Tools is an important component of Insight, it is used to configure, build, update and maintain your collections, as well to manage your user community. You can install the Administrator Tools on a system that is connected to the system where the Collection Manager and User Manager and database is installed.

Install Administrator Tools

The installer for Insight Administrator Tools is located on the CD for Insight Standard:

For Windows: \admin_tools\windows\installAdministrator.exe

For Solaris: \admin_tools\solaris\installAdministrator.bin

For OSX: \admin_tools\macosx\installAdministrator.zip

Install the Administrator Tools by starting the appropriate installation package, and Follow the instructions issued by the installer.

Configure Administrator Tools

The Administrator Tools need to be configured to connect to the User Manager, Collection Manager, and the database. In the installation of Collection Manager and User manager, the configuration file AdminStore.dat has been created under the directory of \dat_files\. Please copy the file AdminStore.dat to the root directory where the Administrator Tools is installed and replacing the same file there.

Verify the Installations

Verifications

Now you have completed the installation of Insight servers, Inscribe Data Editor, Insight client, and Administrator Tools, you can verify whether the system works correctly:

- Make sure the database used by the Collection Manager and User Manager has started. If not, start the database
- Start the Collection Manager and User Manager
- Start the Insight client at the machine where the User Manager and VRA Collection Manager are installed, and enter one pair of the user name and password listed in the above section of Users Created (e.g. student/student, faculty/faculty, admin/admin). If the installation is successful, you should be able to access two collections:
 - Sample Collection VRA
This collection totally resides on your system.
 - David Rumsey Collection
This collection is hosted at Luna Imaging, and demonstrates the capability of Insight to access various shared collections in Insight collection community, whether it resides on your system or not..
- Start the Insight Administrator Tools, and do the following to verify it works correctly:
 - Go to the file tree, and click on User Managers.
 - Move cursor to the hostname of the machine where the User Manager is installed, and right click
 - Click the option of Connect, a dialog will be displayed
 - Enter admin for user name, and admin for password
 - You should be able to access and work on the User Manager
 - Do the same to access the Collection Manager by selecting Insight VRA 4.1 under Collection Manager

Update URLs

After successful verification of the installation, you need to update the URL information for VRA Collection Manager by running the following SQL scripts in your database system:

<install directory>\URL_Update.sql

For Microsoft SQL Server: Use Query Analyzer or ISQL to run the SQL scripts

For Oracle: Use SQLPLUS or other tools to run the SQL script

Once the URLs are updated, client Insight and Inscribe can run on other machines on the network to access the servers.

Build Your Own Collection

To build your collection, please follow the information in Administrator Tools User Guide, Chapter 2 – Building a Collection Using the VRA Model.

Installation and Configuration for Insight Browser Server

Installation and configuration of the Insight Browser Server is optional. If you would like to offer access to your collections through Browser interfaces, you need to install the Browser Server. Insight Browser Server can run using either the Tomcat or Resin JSP servers.

Prerequisites

The Insight Browser Server requires a working JSP Server. Luna currently supports either Apache's Tomcat Server or Caucho's Resin Server.

Getting the Apache Tomcat JSP Server

Before you install, you will need a working version of Apache's Tomcat Servlet / JSP Server (version 4x). You can download Tomcat from <http://www.apache.org/>. Tomcat requires the Java SDK 1.3 or above, though Luna suggests the Java SDK 1.4.1, which can be downloaded for free from <http://java.sun.com>

Please follow the installation and configuration instructions bundled with Tomcat, or if Tomcat has already been installed on your system, please proceed with the following steps below, see "Install Insight Browser Client".

Getting the Resin JSP Server

Before you install, you will need a working version of Caucho's Resin Servlet / JSP Serve (version 2.x). You can acquire Resin from **Caucho Technology** at <http://www.caucho.com>.

Please follow the installation and configuration instructions bundled with Resin, or if Resin has already been installed on your system, please proceed with the following steps immediately below.

Install Insight Browser Server:

The installer for Insight Browser Server is located on the CD for Insight Browser Server:

For Windows: \windows\installBrowser.exe

For Solaris: \solaris\installBrowser.bin

When running the installer, it will

- Set up the directory structure for Insight Browser Server
- Install the following components
 - o Insight Browser Server & associated files
 - o Sprinta JDBC Driver for Microsoft SQL Server
 - o JDBC Driver for Oracle 8i and 9i
 - o Servlet Configuration files (web.xml)
 - o a text file with additions for Tomcat's server.xml file
 - o a text file with additions for Resin's resin.conf file
 - o Insight Browser Server Configuration file (BrowserInsight.conf)

Run the Insight Browser Server Installer

Based on your installation location, the installer will place the Insight Browser Server components into a folder on your system and write the appropriate configuration files for the Browser Server. The configuration files will be written with the appropriate file locations based on where you installed the Browser Server. During installation, you will be presented with the option to specify the installation folder of your choice.

Note: It is important that you do not move the installation folder after you install the Insight Browser Server. If you must move the Insight Browser Server, you should re-run the installer to ensure that your configuration files are written correctly.

Configure Your JSP Server to run the Insight Browser Server

Configuring Tomcat

The following instructions assume a new installation of Tomcat. If you have modified the default Tomcat configuration, the steps required to configure Tomcat to run the Insight Browser Server may be different.

- 1) Locate your Tomcat Installation Directory
- 2) Locate the server.xml file located in the conf/ directory inside the Tomcat Installation Directory
- 3) Open the server.xml file in your preferred text editor locate the following

```
'<Context path="" docBase="ROOT" debug="0"/>'
```

- 4) Copy the contents of the file "Tomcat_conf_addition.txt" (located in the Insight Browser Server installation folder) and paste them under the above location. The result should look like this:

```
<Context path="" docBase="ROOT" debug="0"/>
<Context
className="org.apache.catalina.core.StandardContext"
crossContext="false" path="/BrowserInsight" debug="0"
reloadable="true" docBase="C:/Program
Files/InsightBrowser4 1/" defaultSessionTimeout="30">

<Logger className="org.apache.catalina.logger.FileLogger"
debug="0" verbosity="1" prefix="localhost browser log."
directory="logs" timestamp="true" suffix=".txt"/>
</Context>
```

- 5) Restart Tomcat

Configuring Resin

The following instructions assume a new installation of Resin. If you have modified the default Resin configuration, the steps required to configure Resin to run the Insight Browser Server may be different.

- 1) Locate your Resin Installation Directory
- 2) Locate the resin.conf file located in the conf/ directory inside the Resin Installation Directory
- 3) Open the resin.conf file in your preferred text editor locate the following

```
<host id=''>
```

- 4) Copy the contents of the file "Resin_conf_addition.txt" (located in the Insight Browser Server installation folder) and paste them under the above location. The result should look like this:

```
<host id=''>
<web-app id='/BrowserInsight' app-dir=' C:/Program
Files/InsightBrowser4 1/' class-update-interval='2'>
</web-app>
```

- 5) Restart Resin

Testing your Browser Insight Installation

Once you have modified the configuration files for Tomcat or Resin by adding the context for BrowserInsight, start Tomcat or Resin. By default, Tomcat and Resin are configured to run on Port 8080, to test that Resin or Tomcat is running properly:

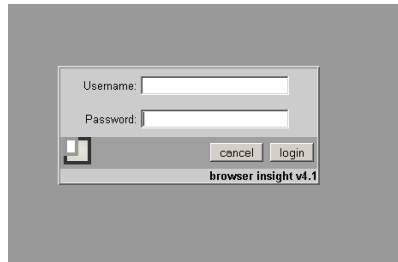
- 1) Open a web Browser on the Server running tomcat or resin and load the following page:

```
http://localhost:8080
```

- 2) Both Resin and Tomcat will display a default page stating that they are configured properly. If you are not seeing a page like this, please check your configuration files for errors, there may be a missing “<” or “>”. For other common configuration problems, review the Resin or Tomcat Manual.
- 3) If the default page loaded properly, please load the following page:

```
http://localhost:8080/BrowserInsight/BrowserInsight
```

- 4) If Insight is configured properly, you should see a login page (below):



Configuring Insight Browser Server by Editing BrowserInsight.conf

After installing Insight Browser Server, a default configuration file `InsightBrowser.conf` will be generated for you. You need to edit the file to fit your environment.

Configure User Manager Connection

The Insight Browser communicates directly with the User Manager, creating one point of authentication and access to the User Group Folders that are stored on the User Manager. If you have not already upgraded to the 4.0 version of the Browser, you will need to add the “*Browser Unique CID*” to the Collection in your User Manager. Refer to the “*Add a Collection to an Existing User Manager and Provide Access to Existing Users*” section of the Insight Administrator Tool guide to setup your collection.

In order to perform user authentication, the Insight Browser must connect to a User Manager. By default this is set to Luna’s main User Manager. Find the line

```
InsightUserAddress = insightuser.lunaimaging.com
```

in `BrowserInsight.conf`, and change `insightuser.lunaimaging.com` to the hostname or IP address of the User Manager you would like to use for user authentication.

Bypass Login Page

Insight Browser Server is initially configured to require users to enter a username and password to view collections. If you would like to allow users of Insight Browser direct access to collections without being asked to enter a username and password, you can provide default values in the configuration file. Find the lines

```
#DefaultBrowserInsightUsername =  
#DefaultBrowserInsightPassword =
```

in BrowserInsight.conf. Remove the comment character (#) from the beginning of both lines, and add the default username and password of your choice.

Configure Collection Manager Server Database Settings

Insight Browser can connect to multiple collection databases. For each database, you must configure the following parameters to specify the database connection for the collection. The example below uses two collections:

```
Collection.1.InsightDBDriver = sprinta  
Collection.1.connectString =  
www.dalton.org:1433?database=insightVRA&sql7=true&user=insig  
ht&password=admin  
Collection.1.username =  
Collection.1.password =  
Collection.2.InsightDBDriver = oracle  
Collection.2.connectString = @www.dalton.org:1521:insight  
Collection.2.username = a_user_name  
Collection.2.password = a_user_password
```

The properties Collection.1.xxx specify the database settings for the first collection, and the Collection.2.xxx properties specify the database settings for the second collection.

“sprinta” is the name of the JDBC driver for the database of the first collection, and “oracle” is the name of the JDBC driver for the database of the second collection. “sprinta” (a JDBC driver for Microsoft SQL Server) and “oracle” (the Oracle JDBC driver) are preconfigured in this file, and may therefore be used as values for the InsightDBDriver property of any additional collections you configure. If the database connect string includes the user name and password, you do not need to specify them for Collection.x.username and Collection.x.password.

You may configure up to five collections in BrowserInsight.conf. The number identifying each collection (Collection.n) is that collection's 'Collection Unique ID', and must match the Collection Unique ID of a collection known to the User Manager used for authentication.

Create Insight Browser Background Image Slices

To create background image slices using the "Insight Browser Background" action in Photoshop, follow the instructions below:

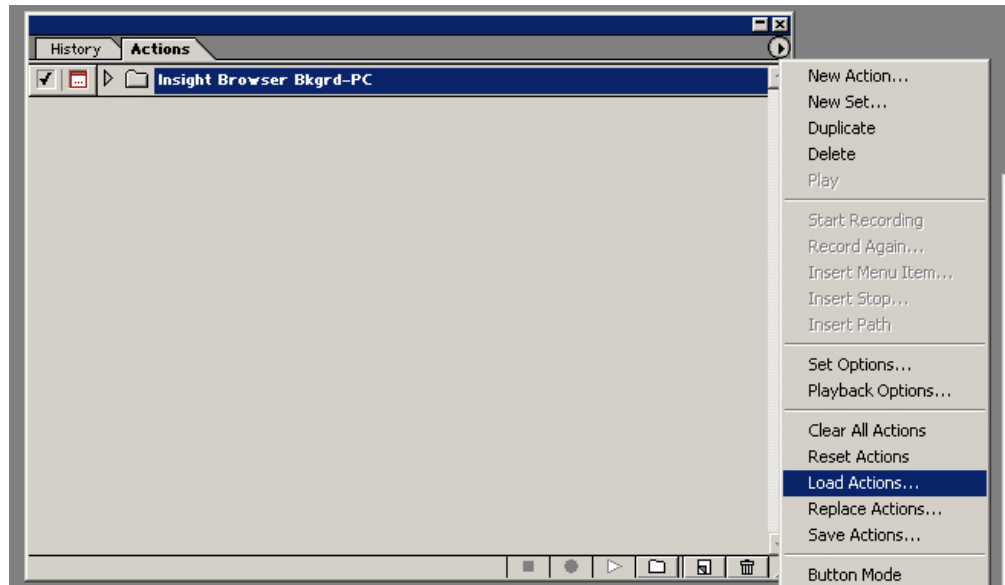
Once you have a background for Insight JVA you can use the "Insight Browser Background Maker_PC" or Insight Browser Background Maker_MAC to make the browser slices for you.

You can find the files on the Insight Browser CD under the utilities folder.

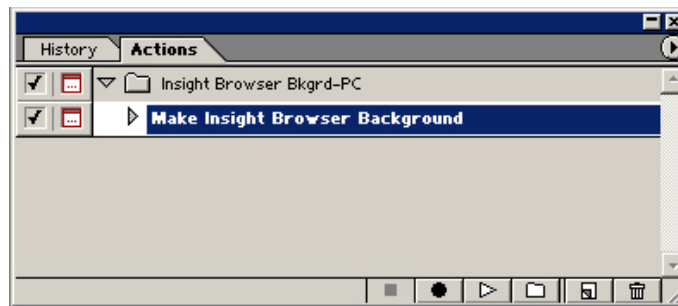
PC

- 1) Copy the Insight_Browser_Bkgrd_PC.zip file from CD.
- 2) Unzip the contents. The contents are named Insight Browser Bkgrd-PC. Once it is unzipped place the Inf folder at the root of your c:\ drive. The Inf folder is in the Insight Browser Bkgrd-PC folder.
- 4) Open Photoshop 6. Find the Action window by going to Window – Show Actions if the Action Window is not already open.
- 5) Load the action, which is in the Insight_Browser_Bkgrd_PC.zip, by clicking on the arrow in the circle in the upper right hand corner of the Action window in Photoshop and select Load Actions.

You will be prompted to browse to the action, which may be located in C:\unzipped\Insight_Browser_Bkgrd_PC\Insight Browser Bkgrd-PC depending where it was saved to in step 2.

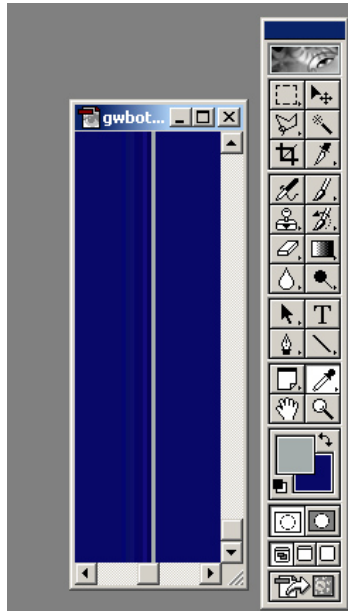


6) Run the action and follow the instructions. You can run the action by clicking the “play” button which is the arrow in the bottom of the action window.

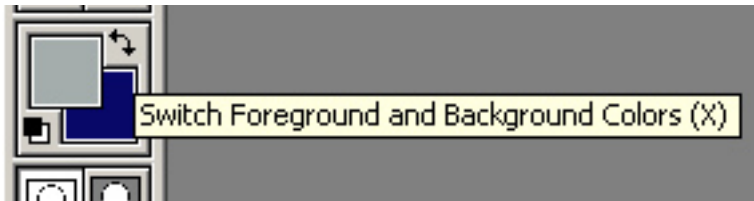


7) As you run through the action you will be prompted to perform various tasks. One task is to set the background and foreground colors in Photoshop. The foreground color will be used for the crosshairs in Insight and the background will be used as the surrounding, background color.

To set the foreground color you want to zoom in on the background until you see the cross hairs. Then use the eyedropper and click on the crosshair line. You will see the Photoshop tool bar foreground and background color change to match your selection.



To set the background colors you want to switch the foreground and background colors by using the arrows on the toolbar foreground and background colors option. Now set the background color using the eyedropper like you did for the foreground.



8) Continue with the script. Once the script completes you will be prompted to the location of the background pieces, which will be in the Inf folder.

9) Copy the c:\Inf ("Inf" refers to look and feel) folder to the web server that will be serving the sliced images. It does not matter where on the server you place this folder just so you can access the pieces as instructed in the Admin tools as described below the MAC instructions.

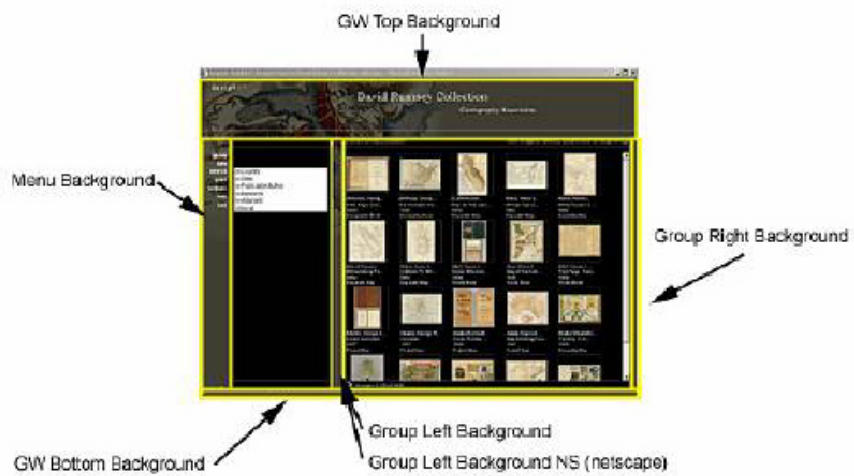
MAC

- 1) Copy the Insight_Browser_Bkgrd_MAC.hqx file from CD.
- 2) Unstuff the contents and place the Inf folder on your desktop.
- 3) Load the "Insight Browser Bkgrd-MAC.atn" action file into Photoshop. (This action was created in PhotoShop 6 on a MAC)
- 4) Run the action and follow the instructions.
- 5) Copy the Inf folder ("Inf" refers to look and feel) to the web server that will be serving the sliced images.

Add URLs to the “Edit Browser Attributes” section of the Collection Configuration node, using the insight Administrator tools

Refer to the “Edit Browser Attributes” section of the Insight Administrator tool documentation the files you will be referring to are as follows:

- gwtop_bg.jpg (GW Top Background)
- menu_bg.jpg (Menu Background)
- groupleft_bg.jpg (Group Left Background)
- groupleft_bg_ns.jpg (Group Left Background NS (Netscape))
- gwbottom_bg.jpg (GW Bottom Background)
- groupright_bg.jpg (Group Right Background)



Browser Insight Remote Launch Strings

Remote Launches are HTTP URL requests made to the Insight Browser server or the Insight Deploy Director server. In the following section we will provide several examples of remote launch strings and break them down to identify the individual components. These strings can be static or dynamically generated depending on your needs.

Anatomy of a Remote Launch String:

The first section is the “Base Request URL”

Browser Insight:

<http://library.Dalton.edu:8080/BrowserInsight/BrowserInsight?cmd=start>

Insight JVA via Deploy Director:

<http://library.Dalton.edu:8080/servlet/deploy/insight/launch?cmd=start>

This is the base of all requests made to the Insight Browser server. It is composed of the following.

1. Domain name “library.Dalton.edu”
2. Port of the application server “:8080”
 - a. Note: If you are running your application server on port 80 you will not need to specify a port
3. The “/BrowserInsight/BrowserInsight” is a call to the Browser Insight application or /servlet/deploy/insight/launch is for Deploy Director
4. Followed by “?cmd=start” specifying the function that will execute the request.

The section following “?cmd=start” are parameters separated by the “&”, these parameter will vary depending on the type of request being made. The following section will help clarify how these requests can be made.

Required Parameters:

The “cid” referred to as the “collection unique id”. This number is used to specify a unique instance of the Insight Browser. This is set in the BrowserInsight.conf file.

The “iia” “insight initial activity”

0= Open Group Window

1= Open Image Workspace

2= Open Both Group Window and Image Workspace

Making a Request Based on a Search:

<http://library.Dalton.edu:8080/BrowserInsight/BrowserInsight/?cmd=start&cid=5&iia=0&ig=The%20Dalton%20Library&isl=0&gwisp=0|Period|Period|1|Ming|1&gwia=3&gc=0>

cid=5&iia=0

This example would use the cid (collection unique id) information contained in the BrowserInsight.conf file for instance 5 and open the Group window (iia=0).

ig=The%20Dalton%20Library

The next parameter is "ig" identifies which media group to open. The %20 values are the hex value for a space character. If the ig parameter is not included the default group contained in the collection configuration will be used.

isl=0

The isl parameter indicates if the user of the remote launch has the right to create remote launch strings in Browser Insight. 0=NO 1=YES

gwis=0|Period|Period|1| Neolithic|1

This is where the search request is contained. They are formed as follows:
Bool|FieldName|FieldDisplayName|FieldType|FieldValue|Relation"

0|Period|Period|1| Neolithic|1

A Boolean operator of 0 refers to an OR
A Boolean operator of 1 refers to an AND

FieldName is the database column name that is searched.
FieldDisplayName is the name that will be displayed in the data window.
FieldType 1 is for text
FieldType 2 is for number
FieldValue is the value you are searching for.

Relation refers to how the value will be searched.

- 1= EQUALS
- 2= CONTAINS
- 3= BEGINS
- 4= ENDS
- 5= GREATER
- 6= LESS
- 9= DOES NOT CONTAIN

To do a complex Boolean search you concatenate the requests into one string.
In the example below you are searching the SubjectType field for Painting AND the EarlyDate (numeric) Field where the value is GREATER than 1900

gwis=0|SubjectType|Category|1|Painting|1|1|EarlyDate|Early%20Date|2|1900|5

gwia=3

Group Window Initial Activity (gwia) has three options

- 0 = Do nothing
- 1 = Show search menu
- 3 = Custom search

For your search to be preformed you must have this parameter and it needs to be set to 3.

&gc=0

This parameter controls paging. 0 represents the first image on the page if you enter 20 this will set you on the 2nd page of your search result. Each number represent an image starting at 0.

Making a Request for Specific Images:

The two requests detailed below are based on ImageID and ObjectID. These are internal numbers that identify a specific Image and the relating descriptive information for that image. Together they form a unique call for a referenced record.

The first portion of these strings are consistent with what has been described earlier in this section so we will just focus on the portions that are different.

Open in the Group Window

```
http://library.Dalton.edu:8080/BrowserInsight/BrowserInsight/?cmd=start&cid=5&iia=0
&ig=The%20Dalton%20Library&isl=0&gwis=0|ImageID|ImageID|2|101854:3013|1|0|
ImageID|ImageID|2|101842:301|1|0|ImageID|ImageID|2|101843:302|1&gwia=3&gc=-1
```

The main difference in this string has to do with the `gwis` parameter. Notice that there is a special keyword *ImageID* used for the `Fieldname` and `FieldDisplayName` sections. It is also identified as a numeric field. The `FieldValue` section there is `101854:3013` this is the `ObjectID:ImageID` reference for the record

Open in the Image Workspace

```
http://library.Dalton.edu:8080/BrowserInsight/BrowserInsight/?cmd=start&cid=5&iia=1
&ig=The%20Dalton%20Library&isl=0&ir=3013+301+302&id=101854+101842+101843
&iwas=2
```

When requesting images to open in the Image Workspace there are a couple of different parameter.

ir=3013+301+302

The `ir` refers to the ImageIDs being referenced separated by a plus sign.

id=101854+101842+101843

The `id` refers to the ObjectIDs being referenced separated by a plus sign.

These two references need to be in the correct relation to each other to get the correct result.

iwas=2

The `iwas` is the requested image size from Size 1 – max size in collection Size 8

Size 0 . up to 96 pixels on the long side
Size 1 . up to 192 pixels on the long side
Size 2 . up to 384 pixels on the long side
Size 3 . up to 768 pixels on the long side
Size 4 . up to 1536 pixels on the long side
Size 5 . up to 3072 pixels on the long side
Size 6 . up to 6144 pixels on the long side
Size 7 . up to 12288 pixels on the long side
Size 8 . up to 24576 pixels on the long side

NOTE: Two new parameters have been added to version 4 of Insight browser. “un” and “pw” this will allow an auto login into the Browser Insight collection. You may combine this with the “cid” to directly open a specific collection.

un=MyUsername

pw=MyPassword

Additional Insight JVA Launch String Parameters

With the addition of the Deploy Director server and the Insight Launch Manager you are now able to launch the Insight JVA client using the same launch strings used for Insight Browser. There are however a couple additional parameter that are allowed when making a request to the Insight JVA client.

Use the “c=” parameter to specify the collection you would like to open.

Use the “u=” to specify the User Manager that will authenticate your access.

c=The+Dalton+Collection

u=insightusermanager.dalton.org

Configure Browser Insight to use SSL (suggested when implementing Insight in a single sign-on environment)

To enable SSL during login:

- 1) Configure your servlet container (Resin or Tomcat) to use SSL. See your Resin or Tomcat documentation for directions on configuring and testing SSL. Note the port number on which SSL is configured.
- 2) Once the servlet container is properly listening for SSL connections on the specified port, open the BrowserInsight.conf, located in the root of the Browser Insight installation directory
- 3) Locate the following lines:

```
#-----  
# SSL Security Settings  
#-----  
  
# to enable secure login uncomment and update the  
# following lines  
  
#LoginSSL = yes  
#SecureDomain = https://browserinsight.lunaimaging.com:8085  
#StandardDomain = http://browserinsight.lunaimaging.com:8080
```

- 4) Uncomment the **LoginSSL** property and set it to 'yes' in your BrowserInsight.conf.
- 5) Uncomment the **SecureDomain** property and set it to match the domain on which the Secure version of Browser Insight is running. Commonly, the secure domain is composed of the protocol (https) + the host running BrowserInsight + the servlet container's SSL port number. For example, if your domain name is host.mydomain.com and your servlet container's SSL port is 8085, specify SecureDomain as: https://host.mydomain.com:8085

Note: If you are using the standard HTTPS port, 443, you may omit the port definition for the SecureDomain property, as seen in the example above.
- 6) Uncomment the **StandardDomain** property and set it to match the domain on which the unsecured version of Browser Insight is Running, commonly
- 7) Save the BrowserInsight.conf file and continue with the steps below specific to your servlet container.

Additional Installation Instructions for Resin:

- 1) Open the resin.conf file located in the <resin_install>/conf directory.

- 2) Search for the line beginning with <session-config in the resin.conf file, it should look something like the following:

```
<session-config enable-cookies='true' enable-url-rewriting='false' session-timeout='30' />
```

- 3) If **LoginSSL** is set to “yes” in BrowserInsight.conf, then the above line must be changed to the following:

```
<session-config enable-cookies='true' enable-url-rewriting='true' session-timeout='30' cookie-domain='.mydomain.com' />
```

- 4) The dot (.) character preceding ‘mydomain’ is required. Be sure to change ‘mydomain’ to the domain under which Browser Insight is running.

Note: setting ‘enable-url-rewriting’ to true, as shown above, has the effect that users who have disabled cookies in their web browser will still be able to use BrowserInsight.

- 5) Restart Resin after modifying resin.conf.

Additional Installation Instructions for TomCat:

- 1) Open the server.xml file located in the <tomcat_install>/conf directory.
- 2) Search for “BrowserInsight” in the server.xml file, it should look like the following:

```
<Context  
className="org.apache.catalina.core.StandardContext"  
crossContext="false" path="/BrowserInsight" debug="3"  
reloadable="true" docBase="<browser install dir>"  
defaultSessionTimeOut="30">
```

- 3) When using Tomcat with SSL, cookies may not be used to track user sessions. Disable cookies by changing the above line to the following:

```
<Context  
className="org.apache.catalina.core.StandardContext"  
crossContext="false" path="/BrowserInsight" debug="3"  
reloadable="true" docBase="<browser install dir>"  
defaultSessionTimeOut="30" cookies="false">
```

- 4) Restart Tomcat after modifying server.xml.

Chapter
4

Installation for Deploy Director

Overview

Deploy Director has been added to the Insight Suite of software to address two needs; Web Initiation of Insight JVA and centralized management control of the Insight JVA Client.

Web Initiated Insight enables centralized, automated, and incremental deployment and updating of Insight. Also, create links to Insight on the web using remote launch strings which can invoke specific collections, searches, groups, and images in either the Group Window or Image Workspace.

This section will show you how to Install Deploy Director on your server and customize the installation for your institution.

Note: Deploy Director is not required for Insight to function. This is an add-on and will add functionality to the Insight software.

Installation of Deploy Director

Deploy Director Works with Apache Tomcat and the Installation will install and configure it for you. It Also requires Java JDK 1.3 or above for Tomcat. This is also installed during your setup into the Deploy Director home directory/JDK

You will also need to obtain a license for Deploy Director. Please fill out the Deploy Director Product Registration form at <http://www.lunaimaging.com/support/register/deploydirector.html>

Once you receive your license you can continue with the installation process.

Deploy Director is a third party application that has it's own set of documentation that describes the install and configuration process. This can be found on the Insight Browser Components CD located in the DeployDirector folder (ddadminguide.pdf).

However You Must Follow the Instructions that follow to setup Deploy Director to work with Insight. Do not customize the Deploy Director Install of insight unless directed to do so.

To start the installation go to the Browser Components CD in the DeployDirector folder execute one of the following.

Windows: windows_dd_260.exe

Solaris: solaris_dd_260.bin

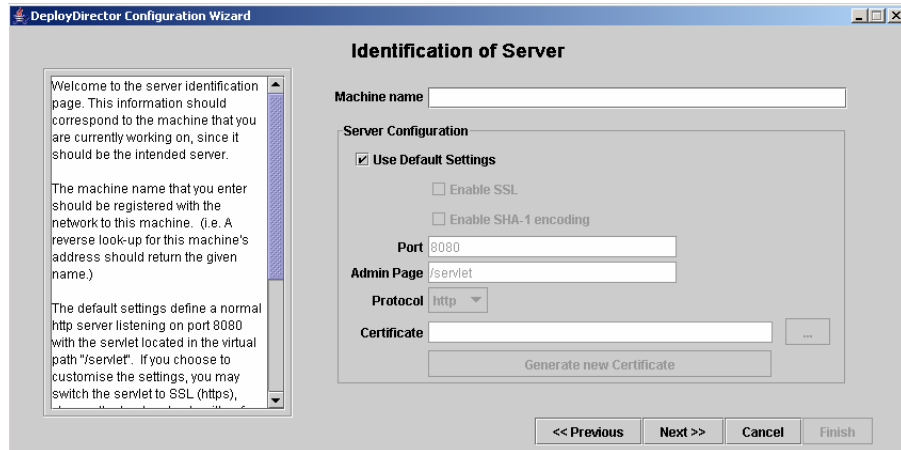
- Launch Installer
- Click Next at the Introduction panel
- Agree to License
- Click Next
- Choose **ALL** from the "Chose Product Feature" panel
- Click Next
- Specify the Installation path
- Click Next
- Specify the installation properties
- Click Next
- Click Install
- Wait for the installation process to complete

Immediately after the installation process, the Deploy Director Configuration Wizard will launch. If it dose not you can launch it manually from the following location.

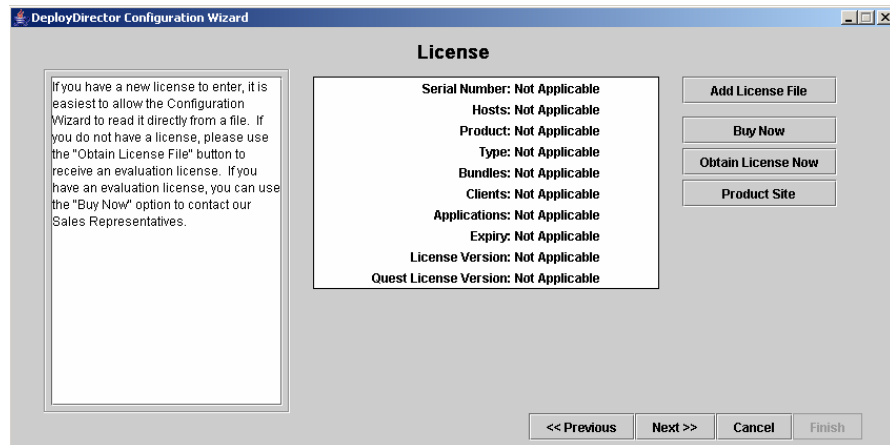
(DD_HOME)/standalone/bin/wizard.[bat|sh]

using the ".bat" file on windows and the ".sh" file on Unix

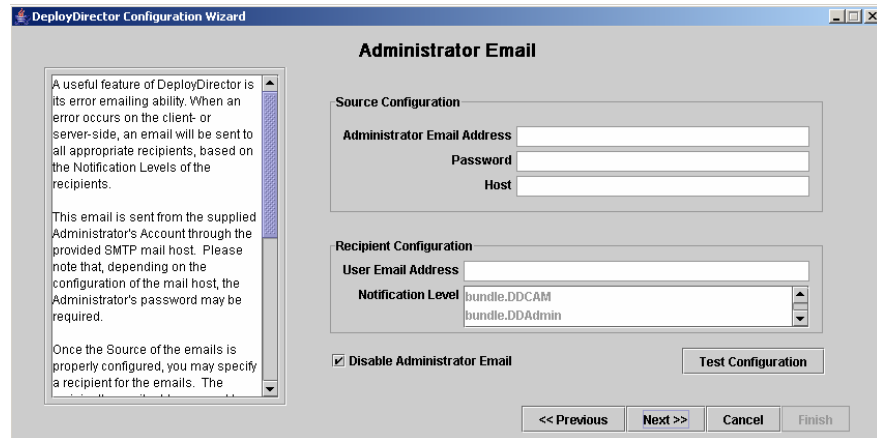
- Click Next at the Introduction panel
- At the JDK Selection panel, click the Update button to locate your installed JDK. Click the most recently installed JDK, then click Next. You will notice a funny path to a jdk located in a sub-directory of the DD installation directory, This is not correct you will find the correct jdk in (DD_HOME)/jdk.
- At the "Identification of Server" panel (seen below), define the machine name for the server you have installed DeployDirector on. The machine name that you enter should be registered with the network. The reverse lookup for the machine's address should return the given name. (i.e. deploy.lunaimaging.com is used as Luna's machine where DeployDirector is installed. This domain name resolves to 63.236.2.206, which is the primary IP of the machine.) Once you have specified the Machine Name, click Next.



- At the "License" panel (seen below), click the add license file and navigate the directory containing the license file you requested from Luna. Once you select the license file, the contents of the license should appear in the dialog window. Once the license has been loaded, click Next.



- At the "Administrator E-mail" panel (seen below), click Next, unless you wish to modify this setting now. This function is not necessary for Insight deployment.



- Click Next at the Configuration Summary.
- Click Finish to save your configurations.

Note: If you already have a application running on port 8080, you will need to modify the port number on which deploy director is running. The port definition can be found in \$INSTALLDIR/standalone/conf/server.xml. Open the file in a text editor, then modify the <Connector> port parameter from 8080 to 8082, or any other open port you may wish. Save the file. If you should need to modify the port, you will need to run through the DeployDirector Configuration Wizard and define the correct port at the "Identification of Server" panel.

Note2: If you have installed or planned to install Insight Browser you may be using port 8080 already. The Installation of these applications are separate processes and should remain separate.

DeployDirector\updates

Setting up Deploy Director for Insight

On the Browser Components CD in the DeployDirector/updates directory. Copy & paste the three directories into the root of the Deploy Director installation directory. You will be asked if you would like to overwrite the existing files, click "Yes to All". Once the file copy process has completed, launch Deploy Director.

Windows:

Launch Deploy Director from

Start -> DeployDirector -> Start DeployDirector.

Launch Deploy Director Admin

Start -> DeployDirector -> DeployDirector Admin.

Solaris:

Launch Deploy Director

(DD_HOME)/standalone/bin/startup.sh

Note: you may need to set execute privileges for this file.

Launch Deploy Director Admin

(DD_HOME)/DDAdmin/DeployDirectorAdmin.

Once you Launch the you will be presented with a Login screen

Select Server

Username:
ddadmin

Password:

Cache Password

Select server:
http://127.0.0.1:8080/servlet/deploy

When entering a new server, enter the full server path including protocol, server name, port and context path.
For example: http://dd.server.com:8080/servlet/deploy

Login Cancel

Enter username: ddadmin Password: f3nd3r

These are the defaults and you should change them later.

Enter the Selected server. This is the server you installed Deploy Director on and identified in the "Identification of Server" panel of the configuration wizard. An example is given in the panel.

Click Login

Under the File menu, click Import DAR. Navigate to the bundles directory on the Browser Components CD. DeployDirector\bundles\insight\ select the insight.dar file. You will then be presented with Bundle Version window. The Bundle Name and version Name values should be pre-populated. Click 'OK' to import insight as a bundle. This will import the Insight Application.

Customize insight.dat file for use within Deploy Director

Refer to the [Prepare Insight client configuration file](#) in chapter 2 of this document

Once the bundle has been successfully imported to the server, click the Insight bundle node under the Bundles tab. Expand the node and select the 4.0.0.0 bundle. Now drill down on the tree 4.0.0.0 -> Platform All -> Files. In the right frame, delete the insight.dat file from the files list. Next, go to edit -> add files and navigate to the location to which you saved your customized insight.dat file. . Double click to insight.dat file to add it to the bundle.

Your insight installation is now complete.

Next we need to Import the new version of the DDCAM.

To update the DDCAM, go to file -> Import DAR. The file is located on Browser Components CD. DeployDirector\bundles\ddcam and select the ddcam.dar file. This will import the updated version of the DDCAM.

Once the DAR has uploaded successfully, go to file -> update server. This will publish the new bundles and the installation and configuration process for deploydirector will be complete.

Verify your Install

To verify that the installation process was successful, open your web browser and enter `http://<installedhost>:8080/servlet/deploy/insight/launch` into the address bar.

When you initially log-in to the page, you will be presented with a Digital Certificate signed by Luna Imaging. After accepting the certificate, DeployDirector will install the necessary files and then launch Insight. When the Insight splash screen appears after the installation process, you know you are ready to deploy Insight.

Post Install

Changing Administrator Password

Refer to the Deploy Director Installation and configuration PDF on how to change your admin password. This can be found on the Insight Browser Components CD located in the DeployDirector folder (ddadminguide.pdf).

Online Administration Page

`http://<installedhost>:8080/servlet/admin/index.jsp`

Next; Install and configure the Insight Launch Manager

Chapter
5

Insight Launch Manager

Overview

As the use of remote launch strings for both the JVA client and the Browser become more prominent within our user community, administrators may want to provide end users with the choice of which application should respond to a remote launch string.

The Insight Launch Manager was introduced with version 4.0 of Insight in conjunction with Deploy Director to address these needs. The Launch Manager allows the end user to choose which Insight application (Insight JVA or Insight Browser) should be invoked when making a request. The user is also presented with an option to remember the decision. The following documentation describes the use and setup of the Insight Launch Manager.

Working With Remote Launch Strings (interoperability between the Insight JVA, Insight JSP Browser, and other Applications)

Both the insight Browser and the Java client support Remote Launch Strings, URLs, which when invoked launch Insight and perform a given action. Actions may include:

- Loading a collection
- performing a search
- opening up to 10 images in the Group Workspace
- opening up to 10 images in the Image Workspace
- opening up to 10 images in the Group and Image Workspaces simultaneously

These launch strings can then be embedded into documents, for example:

- Word Processing Documents
- Web pages
- Courseware Applications like WebCT or Blackboard
- PDFs
- Flash Movies

- Other Databases

An example of a movie with embedded Remote Launch Strings is available at:

<http://www.davidrumsey.com/quicktimevr.html>

Configuring Remote Launch to work within your Local Environment:

- 1) Determine which Insight tools you will be using:
 - Insight JVA Client with Deploy Director(TM)
 - Insight JSP Browser
 - Insight Launch Manager
- 2) Identify what the end user experience should be. Both the Insight JVA and the Browser respond to the same remote launch strings, the only thing that's different is the prefix of the URL.

- a. **If you just use the Java Client:** Set the remote launch URL to the URL for the Deploy Director version of Insight

<http://www.your-server.com:port/servlet/deploy/Insight/launch>

NOTE: as some users may have other versions of insight, it is best to include the user server parameter in the URL, by adding the

u=your.user-server-url.com

to the url, so it looks like this:

<http://www.your.server.com:port/servlet/deploy/Insight/launch?u=your.user-server-url.com>

- b. **If you are just using the Insight Browser:** Set the remote Launch user for the Browser to the browser start page:

http://your-server.com:8080/BrowserInsight/BrowserInsight?cmd=start&

- c. **If you are using both the Browser and the Java client:** there are a few options:
 - i. Set both the Browser and the Java client to point to the Browser
 - ii. Set both the Browser and the Java client to point to the Java Client
 - iii. Let the user decide by setting the Browser and the Java client to point both the Browser and the Java client to point to the **Insight Launch Manager**
- d. Finally, the Remote Launch feature may be disabled by the client

Understanding the Insight Launch Manager

The Insight launch manager (seen below) allows the end user to decide which version of insight they would like to use to view the remote launch string. The Launch Manager is a HTML page and an image (insight-icon.gif), which can be placed on any web or application server where it is accessible by all users. **The launch manager can be found on the Insight Browser Components CD in the Launch Manager folder (insightlaunchmanager.html).**



To configure the clients to use the Insight Launch Manager:

- 1) Place the Insight Launch Manager on your website
 - a. **Specify the Browser Server URL:**

Update this line: `var browserInsightURL = "...";` to point to your Browser server

- i. <http://deploy.lunaimaging.com:8082/browserinsight/browserinsight?cmd=start&>

NOTE: make sure the url ends in "?cmd=start&", as this tells the browser server what to do.

- b. **Specify the Deploy Director URL:**

Update this line: `var deployDirectorURL = "...";` to point to your deploy director instance.

- i. <http://deploy.lunaimaging.com:8080/servlet/deploy/Insight/launch?>

NOTE: make sure the URL ends in "/launch" as this tells deploy director what to do. (you may optionally also include the user server at the end

- c. **Specify the user server:**

Update this line: `var userServer = "...";` to point to your user server

- d. **Turn the Launch Manager clients into AutoLogin Clients:**

Optionally, you can pass a username and password via the Launch Manager to make all clients visiting the Launch Manager auto-login with a specific username and password this can be done by setting the following two variables:

Update this line: `var defaultUserName = "insight";` to specify the username

Update this line: `var defaultPassword = "insight";` to specify the password

- 2) Update the Java Client Launch URL to point to the Launch Manager URL
- 3) Update the Insight Browser Launch URL to point to the Launch Manager URL

Note: To allow users to create remote launch strings in Insight JVA and Insight Browser you will need to edit the Collection configuration. You will find instructions on how to do this in Insight Administrators User Guide under Chapter 4 subsection "Configure a Collection"

look for

Web Initiated JVA URL

Web Initiated JVA HTML Template

and Remote Launch URL for Browser Insight

Installation and Configuration for Insight XML Gateway

The XML Gateway is an optional middleware component allowing third party applications to access the search functionality and content of collection managers. The Insight XML Gateway is a separate add-on component. Check with your System Administrator or Luna Account Representative if you are unsure whether you purchased the XML Gateway.

Prerequisites

The Insight XML Gateway can run using either the Tomcat or Resin JSP servers.

Getting the Apache Tomcat JSP Server

Before you install, you will need a working version of Apache's Tomcat Servlet / JSP Server (version 4.x). You can download Tomcat from <http://www.apache.org/>. Tomcat requires the Java SDK 1.3 or above, though Luna suggests the Java SDK 1.4.1, which can be downloaded for free from <http://java.sun.com>

Please follow the installation and configuration instructions bundled with Tomcat, or if Tomcat has already been installed on your system, please proceed with the following steps below.

Getting the Resin JSP Server

Before you install, you will need a working version of Caucho's Resin Servlet / JSP Serve (version 2.x). You can acquire Resin from **Caucho Technology** at <http://www.caucho.com>.

Please follow the installation and configuration instructions bundled with Resin, or if Resin has already been installed on your system, please proceed with the following steps below.

Installing the Insight XML Gateway:

The installer for the Gateway is located on the XML Gateway CD:

For Windows: XMLGateway\windows\installGateway.exe

For Solaris: XMLGateway\solaris\installGateway.bin

When running the installer, it will

- Set up the directory structure for Insight XML Gateway
- Install the following components
 - o Insight XML Gateway Servlet
 - o Servlet Configuration File (web.xml)
 - o a text file with additions for Tomcat's server.xml file
 - o a text file with additions for Resin's resin.conf file

Run the Insight XML Gateway Installer

During installation, you are presented the option to specify the installation folder of your choice.

Based on your installation location, the installer will place the Insight XML Gateway components into a folder on your system and write the appropriate configuration files for the XML Gateway. The configuration files will be written with the appropriate file locations based on the installation path.

Note: Should you need to move the XML Gateway Components, backup your configuration files and re-run the installer to ensure all files are properly configured and moved into the appropriate places.

Configure Your JSP Server to run the Insight XML Gateway

Configuring Tomcat

The following instructions assume a new installation of Tomcat. If you have modified the default Tomcat configuration, the steps required to configure Tomcat to run the Insight XML Gateway may be different.

- 1) Locate your Tomcat Installation Directory
- 2) Locate the server.xml file located in the conf/ directory inside the Tomcat Installation Directory
- 3) Open the server.xml file in your preferred text editor locate the following

```
'<Context path="" docBase="ROOT" debug="0"/>'.
```

- 4) Copy the contents of the file "Tomcat_conf_addition.txt" (located in the Insight XML Gateway installation folder) and paste them under the above location. The result should look like this:

```
<Context path="" docBase="ROOT" debug="0"/>
<Context
className="org.apache.catalina.core.StandardContext"
crossContext="false" path="/insight/servlet" debug="0"
reloadable="true" docBase="C:/Program
Files/InsightXMLGateway/" defaultSessionTimeout="30">

<Logger className="org.apache.catalina.logger.FileLogger"
debug="0" verbosity="1" prefix="localhost gateway log."
directory="logs" timestamp="true" suffix=".txt"/>
</Context>
```

5) Restart Tomcat

Configuring Resin

The following instructions assume a new installation of Resin. If you have modified the default Resin configuration, the steps required to configure Resin to run the Insight XML Gateway may be different.

- 1) Locate your Resin Installation Directory
- 2) Locate the resin.conf file located in the conf/ directory inside the Resin Installation Directory
- 3) Open the resin.conf file in your preferred text editor locate the following

```
<host id=''>
```

- 4) Copy the contents of the file "Resin_conf_addition.txt" (located in the Insight XML Gateway installation folder) and paste them under the above location. The result should look like this:

```
<host id=''>
<web-app id='/insight/servlet/XMLGateway' app-
dir='C:/Program Files/InsightXMLGateway' class-update-
interval='2'>
</web-app>
```

5) Restart Resin

Defining a User for the XML Gateway

Like the JVA client, the username and password control the collections available to the XML Gateway. The collections to which the XML Gateway has access can be controlled by the defined username and password. As the XML Gateway functions on a system level, it is suggested that you create a specific username and password for the Gateway separate from the standard users on your user manager. Ultimately, this will reduce the likelihood for errors in the future.

Configuring the XML Gateway to access Specific Insight Collection

The Insight XML Gateway acts like an Insight JVA Client. It is configured with a user manager address, a Username, and a Password. By default, these are the only required configuration properties.

NOTE: The installer should automatically prompt you for a user manager, username, and password, and configure these files for you. If it does not, or if you would like to change your settings, please follow these steps.

- 1) Locate the XML Gateway configuration file (web.xml)

The web.xml file is located in the WEB-INF folder of the XML Gateway Installation Directory.

- 2) Open the web.xml file in your preferred text editor
- 3) Change the User Manager Address
 - a. Locate the following lines in the web.xml file

```
<param-name>UserServerAddress</param-name>  
<param-value>localhost</param-value>
```

- b. Change "localhost" to match the address of your Insight User Manager

- 4) Change the Username and Password
 - a. Locate the following lines in the web.xml file

```
<init-param>  
    <param-name>username</param-name>  
    <param-value>test</param-value>  
    <description>Username for User Manager  
    authentication.</description>  
</init-param>  
<init-param>  
    <param-name>password</param-name>  
    <param-value>test</param-value>  
    <description>Password for User Manager  
    authentication.</description>  
</init-param>
```

- b. Change the Username of “test” to match a valid username on your User Manager
- c. Change the Password of “test” to match the valid password for the username used above.

5) Restart Tomcat or Resin

Testing the Configuration of the XML Gateway

Testing the proper installation and configuration of the Insight XML Gateway is a two step process. Before testing the XML Gateway installation, please ensure that Tomcat or Resin is properly installed and is able to serve its standard web pages and servlets.

These instructions assume a default installation of Tomcat/Resin is being used as the servlet container, though Tomcat is shown. The testing process using Resin is similar, but exact steps and screenshots will differ.

The first step in testing is verifying that the servlet container is properly configured to recognize the access URL for the XML Gateway.

1) After installation and configuration is complete, navigate to the XML Gateway’s URL using a web browser. This URL will be of the form:

```
http://<ipaddress>:<port>/insight/servlet/XMLGateway
```

where <ipaddress> and <port> are those of the running Tomcat/Resin server.

When Tomcat/Resin and the XML Gateway are properly configured, you should receive no response in a web browser when navigating to the above URL. This is because the Gateway will not respond unless valid data in the form of an XML request is sent to it. After a short period of time, the connection to the XML Gateway will timeout, and your browser should display a blank page or if you browser supports XML then you will see a page as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE insightResponse (View Source for full doctype...)>  
- <insightResponse>  
  <status code="1">Improper request: Premature end of  
file.</status>  
</insightResponse>
```

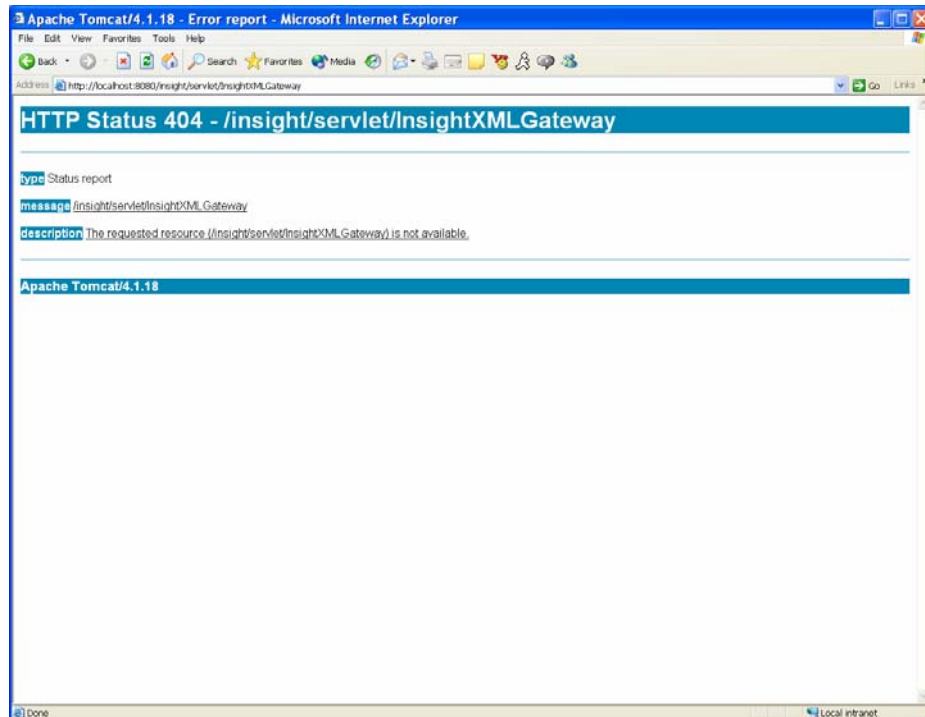
If you have access to Tomcat/Resin’s standard output, you will see information similar to the following, as the XML Gateway prints its current configuration:

```
InsightXMLGateway: Initializing  
InsightXMLGateway.InsightXMLGateway: requestHandlerPoolSize:  
10  
InsightXMLGateway: maxClientProxies: 25  
InsightXMLGateway: username: test  
InsightXMLGateway: parserClassName:  
org.apache.xerces.parsers.SAXParser  
InsightXMLGateway: userServerAddress: localhost
```

```
InsightXMLGateway: responseSystemID:  
http://www.lunaimaging.com/support/dtd/insightXMLGateway/v4.1/insightresponse.  
dtd  
InsightRequestHandler: Default maxClientProxies: 10
```

Troubleshooting a 404 error

If the XML Gateway's <context> definition in Tomcat's server.xml or Resin's resin.conf file is incorrect, or if the <servlet-mapping> definition in the XML Gateway's web.xml file is incorrect, then Tomcat/Resin will respond with the HTTP error code 404, 'Resource not found.' A typical example of this error in a web browser is provided in this screenshot.



This error condition will also be reported in Tomcat/Resin's server access log, similarly to the following:

```
127.0.0.1 - - [11/Nov/2003:16:09:16 -0800] "GET  
insight/servlet/XMLGateway HTTP/1.1" 404 767
```

The '404' in this log entry indicates that the servlet was not found. To fix this error condition, verify that the values of the 'path' and 'docBase' attributes in the <context> definition (found in server.xml or resin.conf) are correct, and that the values in the <servlet-mapping> for 'XMLGateway' (found in web.xml) are all correct. The Tomcat or Resin documentation may be useful in helping to diagnose and correct this problem.

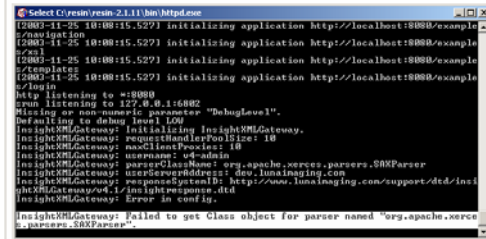
Ensure that Tomcat/Resin responds with something other than error status 404 before proceeding to the next step.

Troubleshooting a 503 error

If you are getting a 503, as seen below, then check the error log for Tomcat or Resin.

503 Unavailable

```
java.lang.UnavailableException: Error in config.  
at com.lunaxml.insight.xmlgateway.servlet.InsightXMLGateway.init(InsightXMLGateway.java:202)  
at com.caucho.server.http.Application.createServlet(Application.java:3111)  
at com.caucho.server.http.Application.loadServlet(Application.java:3062)  
at com.caucho.server.http.QServletConfig.loadServlet(QServletConfig.java:435)  
at com.caucho.server.http.Application.getFilterChainServlet(Application.java:2806)  
at com.caucho.server.http.Application.buildFilterChain(Application.java:2762)  
at com.caucho.server.http.Invocation.service(Invocation.java:313)  
at com.caucho.server.http.CacheInvocation.service(CacheInvocation.java:135)  
at com.caucho.server.http.HttpRequest.handleRequest(HttpRequest.java:246)  
at com.caucho.server.http.HttpRequest.handleConnection(HttpRequest.java:163)  
at com.caucho.server.TopConnection.run(TopConnection.java:139)  
at java.lang.Thread.run(Thread.java:534)
```



```
Select C:\resin\resin-2.1.1\bin\http.exe  
[2002-11-25 10:08:15.527] initializing application http://localhost:8080/example  
/admin  
[2002-11-25 10:08:15.527] initializing application http://localhost:8080/example  
/xml  
[2002-11-25 10:08:15.527] initializing application http://localhost:8080/example  
/servlets  
[2002-11-25 10:08:15.527] initializing application http://localhost:8080/example  
/login  
http listening to *:8080  
sun listening to 127.0.0.1:8082  
Missing or non-numeric parameter "debugLevel".  
Defaulting to debug level LOW  
InsightXMLGateway: initializing InsightXMLGateway.  
InsightXMLGateway: requestHandlerPoolSize: 10  
InsightXMLGateway: maxInflightSize: 10  
InsightXMLGateway: username: wf-admin  
InsightXMLGateway: parserClassName: org.apache.xerces.parsers.SAXParser  
InsightXMLGateway: userResponseDir: dev.lunaxml.com  
InsightXMLGateway: responseSystemId: http://www.lunaxml.com/support/dtd/ins  
ightXMLGateway4_1.xml  
InsightXMLGateway: Error in config.  
InsightXMLGateway: Failed to get Class object for parser named "org.apache.xerces.parsers.SAXParser"
```

If you see the line:

InsightXMLGateway: Failed to get Class object for parser named
"org.apache.xerces.parsers.SAXParser"

Then you need to add the XML Parser to you classpath, to do this:

- e. Locate the lib folder inside the support directory of your XML Gateway installation
- f. Copy the three jar files (xml-apis.jar, xalan.jar, xercesImpl.jar) into the lib directory, located in the servlet/WEB-INF directory

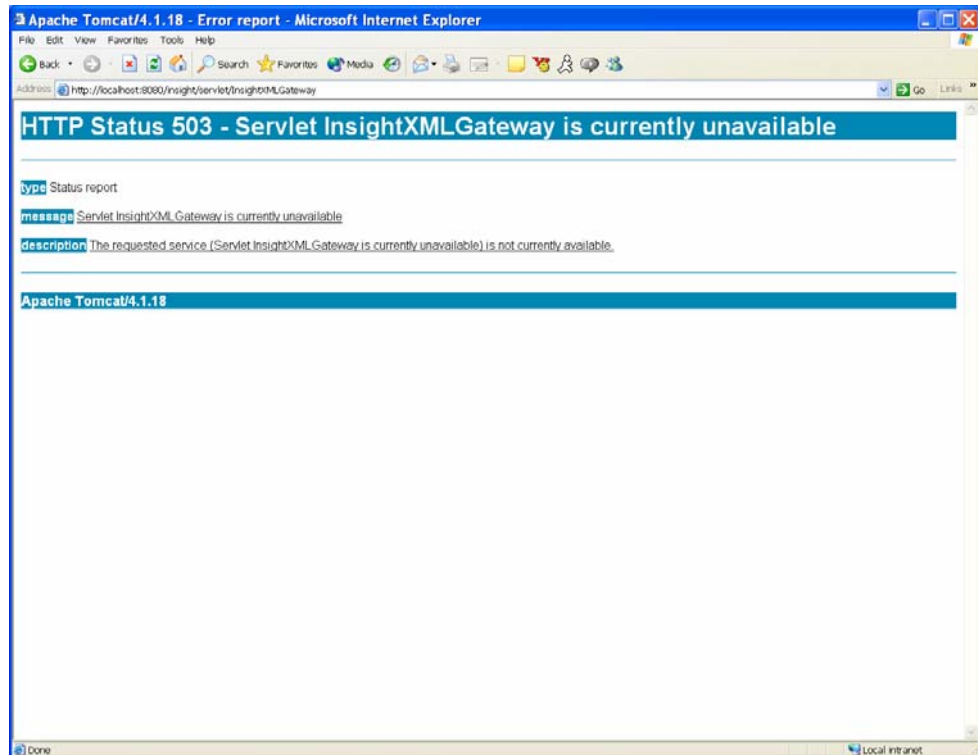
```
<installation_dir>/support/lib/xercesImpl.jar  
/xalan.jar  
/xml-apis.jar
```

go to:

```
<installation_dir>/servlet/lib/
```

- g. Restart tomcat/resin

If any configurable value in web.xml is incorrect, the XML Gateway servlet will be marked as unavailable, and Tomcat/Resin will respond with HTTP error status code 503, 'Unavailable'. A default Tomcat installation will display a web page similar to the following:



Note that the first time this URL is accessed, Tomcat/Resin may instead respond with error status 500 ('Internal Error'). In this case, reloading the web page in the browser should generate error 503.

Useful diagnostics for fixing configuration errors may be found in Tomcat/Resin's standard output. For example, if the XML Gateway is not able to establish a connection with the Insight User Server identified in web.xml, the following error message will be printed to Tomcat or Resin's standard output:

```
InsightXMLGateway: Failed connection to user manager at  
address "localhost".
```

Fix any error conditions identified, restart Tomcat/Resin, and navigate to the XML Gateway's URL again.

Next Steps – Getting started once the Gateway is installed

Once the gateway is installed and configured properly, please see the "Getting Started Guide" for the XML Gateway, located on the XML Gateway CD. The guide includes annotated DTDs, sample XML files, use cases, and sample code for building applications with the Gateway.

Installation and Configuration for Insight Secure Media Server

The Secure Media Server is an optional component adding a ticket-based security model to further protect access to Insight Media Servers. The Secure Media Server adds a layer of protection around images in Insight by requiring that all applications that request images from the server have a valid ticket. These tickets can only be created by Insight, and by default last 30 minutes. The Secure Media Server is compatible with all v4.1 Insight components including the Collection Servers, Insight & Inscribe Clients, the Browser Server, and XML Gateway.

Introduction

When an Insight client contacts a collection server, if that server has media security enabled, the collection server will create an encrypted "media ticket" and send it to the Secure Media Server (where the ticket is decrypted). The media ticket contains a random 20-letter ticket number, how long the ticket is good for, the maximum media resolution that the ticket authorizes, and the Insight client's IP address. If the ticket is successfully registered by the Secure Media Server, the collection server then sends the registered ticket back to the client.

When the client makes a media request the media ticket number is appended to the end of the media URL. If the URL request is directed to the Secure Media Server, thereby making the media secure, the server will extract the ticket number. If the ticket number is valid and has not expired, the Secure Media Server will identify the media resolution by examining the request URL string. If the resolution is less than or equal to the maximum authorized resolution for the ticket, then the Secure Media Server will locate and transmit the requested media back to the client. If the request is for a SID image, the Secure Media Server will proxy the request to the SID server and send the image back to the client.

Now going back a bit, if the Secure Media Server determines that the client's ticket has expired, an appropriate error code is sent back to the client. The client will then make one attempt to get a new media ticket number from the collection server and try again.

Information contained in the session ticket includes:

- 1) **Media Ticket** – A random 20-letter ticket number. The ticket number is used to generate a new service ticket once the ticket has expired.
- 2) **Client IP** – IP address of the authenticated client

3) **Session Duration** – Duration (in minutes) before the ticket expires, time is relative to the media server

4) **Max Resolution** – The max resolution to be provided to the client, dictated by access profile.

Prerequisites

The Insight Secure Media Server can run using either the Tomcat or Resin JSP servers.

Getting the Apache Tomcat JSP Server

Before you install, you will need a working version of Apache's Tomcat Servlet / JSP Server (version 4.x). You can download Tomcat from <http://www.apache.org/>. Tomcat requires the Java SDK 1.3 or above, though Luna suggests the Java SDK 1.4.1, which can be downloaded for free from <http://java.sun.com>

Please follow the installation and configuration instructions bundled with Tomcat, or if Tomcat has already been installed on your system, please proceed with the following steps below.

Getting the Resin JSP Server

Before you install, you will need a working version of Caucho's Resin Servlet / JSP Serve (version 2.x). You can acquire Resin from **Caucho Technology** at <http://www.caucho.com>.

Please follow the installation and configuration instructions bundled with Resin, or if Resin has already been installed on your system, please proceed with the following steps below.

Install Secure Media Server:

The installer for Secure Media Server is located on the Web Components CD:

For Windows: secure_media_server\windows\installMediaServer.exe

For Solaris: secure_media_server\solaris\installMediaServer.bin

When running the installer, it will

- Set up the directory structure for Secure Media Server
- Install the following components
 - o Secure Media Server
 - o Servlet Configuration File (web.xml)

- Secure Media Server Configuration File (mediaSecurity.dat)
- a text file with additions for Tomcat's server.xml file
- a text file with additions for Resin's resin.conf file

Run the Secure Media Server Installer

During installation, you are presented the option to specify the installation folder of your choice.

Based on your installation location, the installer will place the Secure Media Server components into a folder on your system and write the appropriate configuration files for the Secure Media Server. The configuration files will be written with the appropriate file locations based on where you installed the Secure Media Server.

Note: It is important that you do not move the installation folder after you install the Secure Media Server. If you must move the Secure Media Server, you should re-run the installer to ensure that your configuration files are written correctly.

Configure Your JSP Server to run the Secure Media Server

Configuring Tomcat

The following instructions assume a new installation of Tomcat. If you have modified the default Tomcat configuration, the steps required to configure Tomcat to run the Secure Media Server may be different.

- 1) Locate your Tomcat Installation Directory
- 2) Locate the server.xml file located in the conf/ directory inside the Tomcat Installation Directory
- 3) Open the server.xml file in your preferred text editor locate the following

```
'<Context path="" docBase="ROOT" debug="0"/>'.
```

- 4) Copy the contents of the file "Tomcat_conf_addition.txt" (located in the Secure Media Server installation folder) and paste them under the above location. The result should look like this:

```
<Context path="" docBase="ROOT" debug="0"/>
<Context
className="org.apache.catalina.core.StandardContext"
crossContext="false" path="/MediaSecurityServer" debug="0"
reloadable="true" docBase="C:/Program
Files/InsightMediaSecurityServer/"
defaultSessionTimeout="30">

<Logger className="org.apache.catalina.logger.FileLogger"
debug="0" verbosity="1" prefix="localhost mediaSec log."
directory="logs" timestamp="true" suffix=".txt"/>
</Context>
```


5) Restart Tomcat

Configuring Resin

The following instructions assume a new installation of Resin. If you have modified the default Resin configuration, the steps required to configure Resin to run the Secure Media Server may be different.

- 1) Locate your Resin Installation Directory
- 2) Locate the resin.conf file located in the conf/ directory inside the Resin Installation Directory
- 3) Open the resin.conf file in your preferred text editor locate the following

```
<host id=''>
```

- 4) Copy the contents of the file "Resin_conf_addition.txt" (located in the Secure Media Server installation folder) and paste them under the above location. The result should look like this:

```
<host id=''>  
<web-app id='/MediaSecurityServer' app-dir=' C:/Program  
Files/InsightMediaSecurityServer/' class-update-  
interval='2'>  
</web-app>
```

- 5) Note: Resin does not always properly load the security library properly, to ensure it is loaded:
 - a. Locate the lib directory inside the installation directory of resin
 - b. Copy the bcprov-jdk14-115.jar from the servlet\WEB-INF\lib directory inside the installation directory for the Secure Media Server into the lib directory for resin.

```
<secure media server install dir>\servlet\WEB-  
INF\lib\bcprov-jdk14-115.jar
```

copy to

```
<resin_installation_directory>\lib\ bcprov-jdk14-115.jar
```

- 6) Restart Resin

Configuring an instance of the Secure Media Server to serve images from a collection

To configure the Secure Media Server:

- 1) Locate the MediaSecurity.dat file, located in the root of the installation directory for the Secure Media Server
- 2) Open the MediaSecurity.dat file in your preferred Text Editor
- 3) Define the Root directory for the collection's media files. The root directory is pre-pended to media file path that the server extracts from the request URL. For easier migration from an unsecured media server to the secure media server, the root directory should reflect the same structure used by the web server.

a. Locate the following line:

```
# MediaFileRootDir - The root directory where the
# servlet can access the media.

MediaFileRootDir = c:\\mediasamples\\Demo
#MediaFileRootDir = /opt/mediafiles
```

b. Change the MediaFileRootDir property to match the root directory where the server can access the media.

NOTE: Directory paths on Windows must have their back-slashes (\) escaped as \\. (e.g. MediaFileRootDir = c:\\mycollection\\media).

- 4) Define the Maximum Resolution available for the Collection's Media files. The Max Resolution is the last resolution that the Secure Media Server is enforcing security for. This value is used to determine the last resolution marker that should be present in this configuration file.

a. Locate the following line:

```
# MaxResolution - The last resolution that the security
# servlet is enforcing security for.

MaxResolution = 5
```

b. Define the MaxResolution property. This value corresponds with the number of resolutions defined in the Collections SPS Data. For more information on SPS definitions, refer to the SPS Data section of the Administrator Tools User Guide.

- 5) Define a Marker to identify the Sid Server. This is the sub-string that the Secure Media Server can use to identify a SID URL.

NOTE: The installer for the Secure Media Server pre-configures many properties with commonly used values, please check your installation before making changes

- a. Locate the following lines:

```
# SidUrlMarker - The sub-string that the servlet can use to
# identify a SID URL.

SidUrlMarker = iisid.dll

#SidUrlMarker = image_jpeg.pl
```

- b. Define the SidUrlMarker property. For Sid media file access (Resolutions 5- 8), the SidUrlMarker defines the API call to the Sid Image Server. For Microsoft Internet Information Server (IIS), set this property to iisid.dll. For Apache Web Server, set this property to "image_jpeg.pl".

- 6) Define a range of IP Address that can create tickets (ideally this should only include the IP addresses of the Collection Servers, Browser Servers, and XML Gateways that access this Image Server

- a. Locate the following lines:

```
# MediaSecurityAdminIPs - The IP addresses for computers
# that are allowed to register security tickets to the
# servlet.

MediaSecurityAdminIPs = 192.168.1.51
```

- b. Define the MediaSecurityAdminIPs property. The IP addresses for computers that are allowed to register security tickets to the servlet. The IP of the collection managers that contact this servlet must be included in the range of IPs defined for this property.

Note: Do not define the client IPs here, only define the IPs of the collection managers to which the Secure Media Server's content belongs.

- 7) Define the Secret Key that the Collection Server, Browser Server must pass to request a ticket:

- a. Locate the following lines:

```
# MediaSecuritySecretKey - The secret key to use
# for encrypting and decrypting ticket numbers. This
# password must be the same in both the collection
# server and servlet environments.

MediaSecuritySecretKey = insight
```

- b. Define the `MediaSecuritySecretKey` property. The secret key to use for encrypting and decrypting ticket numbers. This key **MUST** be the **SAME** in both the collection manager and servlet environments. Once you have defined the secret key, take of the value; you will need it when specifying the collection manager properties for Secure Media Server support.
- 8) Define Resolution Markers for each Resolution. These values correspond with the SPS size suffix for a particular resolution and tell the Secure Media Server which size image to send to the client.

NOTE: The installer for the Secure Media Server pre-configures many properties with commonly used values, please check your installation before making changes

- a. Locate the following line(s):

```
# ResolutionMarker - The sub-string that the servlet
# can use to identify each resolution.

ResolutionMarker0 = /Size0/,/Base64/

ResolutionMarker1 = /Size1/,/Base16/

ResolutionMarker2 =
/Size2/,/Base4/,cvid,mp3,mpg1,qtvr,svq1,ulaw,mov

ResolutionMarker3 = /Size3/,/Base/

ResolutionMarker4 = /Size4/,/4Base/

ResolutionMarker5 = level=0

ResolutionMarker6 = level=1

ResolutionMarker7 = level=2

ResolutionMarker8 = level=3
```

- b. Each Resolution marker represents the sub-string that the servlet can use to identify each resolution. This tells the servlet that a URL requests containing “Base64” or “Size0” in the query string reference the size 0 resolution. These values correspond with the SPS size suffix for a particular resolution. You can specify multiple markers for each resolution by comma-separating them. Note that resolution 5 is a SID resolution and therefore ResolutionMarker5 uses the SID server syntax for the level. For example, for Resolution 0, the ResolutionMarker property would be `ResolutionMarker0 = /Base64/,/Size0/`.

Configure an Insight Collection Manager to use the Secure Media Server

- 1) To enable media security support on your Insight Collection Manager:
- 2) Open the InsightServer.dat file located in the root of collection manager instance.
- 3) To enable media security:
 - a. Locate the following lines:

```
# MediaSecurityEnabled - Turns media security on or off.  
  
# Note: Enabling media security will have no effect  
# unless the media SPS entries are directed to a correctly  
# configured media security server. (1= ON; 0=OFF)  
  
MediaSecurityEnabled = 0
```

- b. Set the property to 1. To disable media security, set the property to 0.

Note: Enabling media security will have no effect unless the media SPS entries are directed to a properly configured media security servlet. These configurations will be covered later in the document.

- 4) Define the Location of the Secure Media Server:
 - a. Locate the following lines:

```
# MediaSecurityServletUrl - The base URL for the  
# media security servlet.  
  
# i.e. MediaSecurityServletUrl =  
http://insight.lunaimaging.com:8080/SecureMediaServer/srvr  
  
MediaSecurityServletUrl =
```

NOTE: If you are upgrading from 4.0 and are using your 4.0 configuration files, the example URL may be different, the correct URL should follow the pattern above.

- b. Set the **MediaSecurityServletUrl** property to the base URL for the media security server. This servlet URL is used to establish the initial session ticket.
- 5) Define the Secret Key used by the Media Security Server:
 - a. Locate the following lines:

```
# MediaSecuritySecretKey - The secret key to use  
# for encrypting and decrypting ticket numbers. This
```

```
# password must be the same in both the collection server  
# and media security servlet environments.  
  
MediaSecuritySecretKey = insight
```

- b. Define the **MediaSecuritySecretKey** property. The secret key password to use for encrypting and decrypting ticket numbers. This password must be the same in both the collection manager and servlet environments. Enter the value you had previously defined in the MediaSecurity.dat file.
- 6) Define the duration of a Media Security Ticket:
 - a. Locate the following lines:

```
# MediaTicketDuration - How long a media ticket lasts  
# (in minutes).  
  
MediaTicketDuration = 30
```

- b. Define the **MediaTicketDuration** property. The length of time (in minutes) each media ticket is valid for. After a media ticket has expired, Insight will generate a new media ticket. Media URLs accessed outside of Insight will return a expired ticket response once the specified duration has been exceeded.

Changing a Collection's URLs to point to the Secure Media Server

If you are unfamiliar with how Insight segments a media URL into three separate parts, you may wish to review the Managing Media section of the Admin Tool User Guide prior to continuing.

Each time a media file is requested, three location segments are joined together to form a URL to the requested media. The segments are referred to as SPS (Storage Path Segment), LPS (Logical Path Segment), and Filename.

The SPS refers to the machine on which the media resides. In the case of the media security server SPS, it refers to the media security server instance and provides a resolution marker. The LPS refers to the subdirectory structure between the SPS and the filename. The following is an example of how a URL is formed.

URL = Storage Path Segment + / + Logical Path Segment + / + File Name

An unsecured SPS simply refers to the web server and the sub-directory under which the media can be found (e.g. <http://Insight.lunaimaging.com/dalton/size4>). Media Server SPS references provide the same information, but use the media security servlet as a proxy to the media.

(e.g.
<http://insight.lunaimaging.com:8080/SecureMediaServer/srvr?mediafile=/dalton/Size4>).

When defining a media security SPS, each path should start with the media security servlet's base URL followed by the URL parameter prefix "mediafile=" followed by the start of the actual media file path.

Media Security SPS for Media Resolutions 0-4

Base URL: <http://insight.lunaimaging.com:8080/SecureMediaServer/srvr?>

Parameter Prefix: mediafile=

Media File Path: /dalton/Size4

Media Security SPS for Media Resolutions 5-8 (MrSid Resolutions)

For SID resolutions, the media file path references the MrSid Server prefix instead of a local directory path.

Base URL: <http://insight.lunaimaging.com:8080/SecureMediaServer/srvr?>

Parameter Prefix: mediafile=

Media File Path:
<http://sid.lunaimaging.com/sid/bin/iisid.dll?Extract?client=Dalton&image=SID>

Using the Insight Administrator Tool to define Media Security SPS References:

- 1) Launch the Insight Administrator Tools
- 2) Expand the Collection Manager node and connect to your collection
- 3) Select the SPS Data node.
- 4) Double-click an unsecured SPS reference. In the URL text box, replace the base web server path with the base media server path. For example, if the resolution 4 SPS was <http://Insight.lunaimaging.com/dalton/size4>, the media security path would be

<http://insight.lunaimaging.com:8080/SecureMediaServer/srvr?mediafile=/dalton/Size4>.

- 5) Repeat step four for each resolution and media type.

Defining the Media Security SPS references is what will actually call the Secure Media Server for the media and therefore make the media secure. Without modifying the SPS entries to call the Secure Media Server, the media will not be secure.

Configuring Browser Insight to use the Secure Media Server

Before configuring the Browser to use the Secure Media Server, ensure that your collection contains SPS references to the Secure Media Server. For more information on this, please review the preceding section.

Update your BrowserInsight Configuration File

To update a collection to use the Secure Media Server, locate your browserinsight.conf and open it in your preferred text editor.

- 1) Locate the connection properties for the collection you are enabling secure media access for. For example, if my collection is #1:

```
Collection.2.insightDBDriver = sprinta
Collection.2.connectString =
www.lunaimaging.com:1433?database=Dalton&sql7=true&user=luna
&password=insight
#Collection.2.username      =
#Collection.2.password     =
```

- 2) Set the **mediaSecurityEnabled** property to yes

```
Collection.2.mediaSecurityEnabled = yes
```

- 3) Set the **mediaSecurityServletUrl** property to the URL for your Secure Media Server

```
Collection.2.mediaSecurityServletUrl =
http://localhost:8080/SecureMediaServer/srvr
```

- 4) Set the **mediaTicketDuration** property. We suggest 30 minutes.

```
Collection.2.mediaTicketDuration = 30
```

- 5) Set the **mediaSecuritySecretKey** property to the key you defined earlier (check your mediasecurity.dat file on your secure media server if you are unsure of this property).

```
Collection.2.mediaSecuritySecretKey = insight
```

Note: Resin does not always properly load the security library properly, to ensure it is loaded:

- a. Locate the lib directory inside the installation directory of resin
- b. Copy the bcprov-jdk14-115.jar from the servlet\WEB-INF\lib directory inside the installation directory for the Secure Media Server into the lib directory for resin.

```
<secure media server install dir>\servlet\WEB-
INF\lib\bcprov-jdk14-115.jar
```

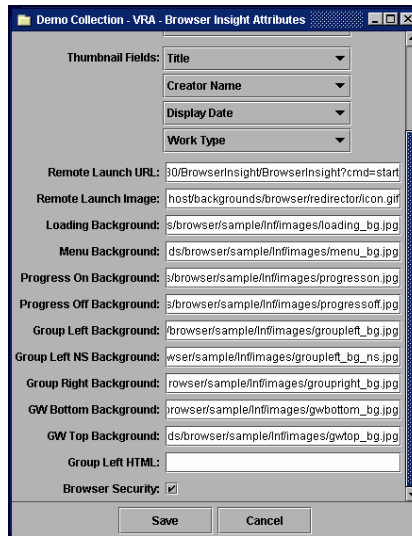
copy to

```
<resin_installation_directory>\lib\ bcprov-jdk14-115.jar
```


- 6) Restart Tomcat/Resin

Enable the Browser Security Property

- 1) Open the Insight Administrator Tools
- 2) Locate the Collection Configuration Properties tab of the Collection Manager you wish to enable Secure Media access for
- 3) Edit the Collection Configuration Properties
- 4) Open the “Edit Browser Properties” Subsection
- 5) Check the “Browser Security” button is checked (seen below)



- 6) Restart Tomcat/Resin

Edit your Secure Media Server Settings

The last step in enabling Secure Media access for BrowserInsight is to ensure that the Secure Media Server is setup with the Browser’s IP Address in the AdminIPs. To do this:

- 1) Locate your mediasecurity.dat file within your SecureMediaServer installation Directory. Open the file in your preferred text editor.
- 2) Locate the IP Address(es) for the Server BrowserInsight is running on.
- 3) Update the MediaSecurityAdminIP property to include the IP Addresses identified in step #2

```
MediaSecurityAdminIPs = 192.168.1.50,192.168.1.127
```

NOTE: you can separate multiple IP addresses / ranges with a comma as above

- 4) Restart the instance of Tomcat / Resin that the Secure Media Server is running on

Enabling Secure Media Access for the XML Gateway

To enable secure media access for the XML Gateway, simply add the IP address of the server running the XML Gateway to the list of Admin IPs for the Secure Media Server. To do this:

- 1) Locate your mediasecurity.dat file within your SecureMediaServer installation Directory. Open the file in your preferred text editor.
- 2) Locate the IP Address(es) for the Server the XML Gateway is running on.
- 3) Update the MediaSecurityAdminIP property to include the IP Addresses identified in step #2

```
MediaSecurityAdminIPs = 192.168.1.50,192.168.1.127
```

NOTE: you can separate multiple IP addresses / ranges with a comma as above

- 4) Restart the instance of Tomcat / Resin that the XML Gateway is running on.

Configuring Insight's Advanced Authentication and Authorization Features

The Insight User manager currently supports three Security Models. By default, Insight is configured with the standard security model, which simply uses the usernames and passwords in the user manager. With Insight 4.1, Luna has modularized the methods that Insight uses to manage Authentication and Authorization. Luna has also released two new security modules for those institutions that are interested in configuring Insight to work with an existing security provider:

Pure LDAP

The first security module out-sources the process of Authentication to an LDAP Server. To use this module, you must first have an LDAP Directory Server that supports LDAP v3. The following are LDAP Servers that Luna has tested against:

- Windows 2000's Active Directory server
- OpenLDAP
- SunONE Directory Server v5.2

NOTE: Insight optionally supports SSL connections for LDAP Queries

Kerberos & LDAP

The second security module out-sources Authentication to a Kerberos 5 Server and Authorization to an LDAP Server. To use this module you must have a working Kerberos 5 implementation and an LDAP Server that supports GSS-API SASL. The following implementations have been tested

- Windows 2000's Active Directory server (provides both Kerberos & LDAP)
- MIT Kerberos 5 KDC with one of the following:
 - OpenLDAP
 - SunONE Directory Server v5.2

NOTE: Insight optionally supports SSL connections for LDAP Queries

Enabling Simple LDAP Authentication for the Insight User Manager

NOTE: Changing Insight's Security model can have major repercussions. Please consult with your Network and Security Administrators before implementing **any** changes regarding your local security environment.

NOTE: Please read and complete the Insight Security Worksheet at the end of this chapter before going any further.

NOTE: Finally, please test all configurations on a **test server** before implementing in a production environment.

1. In a text editor, open the InsightUserServer.dat file located in the "<insight_install>\user_manager" directory.
2. Change the Insight Authentication Handler to use LDAP:

- a. Locate the following lines:

```
##  
# AuthenticationHandler - the full class name of the  
# authentication handler to use for authentication.  
  
AuthenticationHandler =  
com.luna.insight.client.security.DefaultAuthenticationHandle  
r
```

- b. Change the `AuthenticationHandler` property to:
`com.luna.insight.client.security.SimpleLDAPAuthenti
cationHandler`. This will tell the User Manager to use LDAP when
authenticating users.

3. Change the Authorization Handler to use LDAP:

- a. Locate the following lines:

```
##  
# AuthorizationHandler - the full class name of the  
# authorization handler to use for authorization.  
AuthorizationHandler =  
com.luna.insight.client.security.DefaultAuthorizationHandler
```

- b. Change the `AuthorizationHandler` property to:
`com.luna.insight.client.security.SimpleLDAPAuthoriz
ationHandler`. This will tell the User Manager to use LDAP when

authorizing users.

4. Define the URL for the LDAP v3 Server:

a. Locate the following lines:

```
##  
# LdapURL - The URL of the LDAP server.  
# (note: under Windows 2000/Active Directory, this is the  
# address # of the Active Directory machine pre-pended with  
# ldap:// )  
  
#LdapURL = ldap://ldap.lunaimaging.com
```

b. Uncomment the LdapURL property and change it to match the URL for your LDAP Server, when done, it should look like this:

```
##  
# LdapURL - The URL of the LDAP server.  
# (note: under Windows 2000/Active Directory, this is the  
# address # of the Active Directory machine pre-pended with  
# ldap:// )  
  
LdapURL = ldap://your.ldap.server.edu
```

5. Define whether insight should use SSL to communicate with the LDAP Server:

a. Locate the following lines:

```
# LoginSSL - A value of 1, yes, or true, will cause LDAP  
# communication to use SSL. The LDAP server must be  
# configured to use SSL. Any other value (with 0 being the  
# correct one), or not specified, and LDAP communication  
# will not be secured.  
  
# LoginSSL = 0
```

b. Uncomment and change the LoginSSL property to 1, when done, it should look like this:

```
# LoginSSL - A value of 1, yes, or true, will cause LDAP  
# communication to use SSL. The LDAP server must be  
# configured to use SSL. Any other value (with 0 being the  
# correct one), or not specified, and LDAP communication  
# will not be secured.  
  
LoginSSL = 1
```

6. Define the LDAP User Path, this is the directory path in the LDAP Server identifying where to find valid users

- a. Locate the following lines:

```
##  
# LdapUserPath: Directory path in the LDAP server  
# identifying object containing authenticatable users.  
  
LdapUserPath = ou=people,dc=lunaimaging,dc=com
```

- b. Uncomment the LdapUserPath property and set it to the path in the LDAP database that Insight should use to find valid users, when complete, it should look like this:

```
##  
# LdapUserPath: Directory path in the LDAP server  
# identifying object containing authenticatable users.  
  
LdapUserPath = ou=people,dc=lunaimaging,dc=com
```

7. Define the LDAP User Attribute – this is the field that usernames are authenticated against

- a. Locate the following Lines:

```
##  
# LdapUserAttribute - LDAP Attribute to match usernames  
# against.  
  
# Examples:  
# LdapUserAttribute = cn // Active Directory  
# LdapUserAttribute = uid // LDAP using EduPerson schema  
  
#LdapUserAttribute = uid
```

- b. Uncomment the LdapUserAttribute and set it to the field in your LDAP Database that contains usernames, when complete, it should look like this:

```
##  
# LdapUserAttribute - LDAP Attribute to match usernames  
# against.  
  
# Examples:  
# LdapUserAttribute = cn // Active Directory  
# LdapUserAttribute = uid // LDAP using EduPerson schema  
  
LdapUserAttribute = uid
```

Associating LDAP Users with Insight Users

Each User in the Insight User manager will be matched with an LDAP user by comparing the username properties. Usernames must be unique for this authentication model to work properly. Please also ensure that passwords are blank in the Insight User Server (as the passwords will be provided via the LDAP Query).

Using LDAP SSL Certificates with Insight

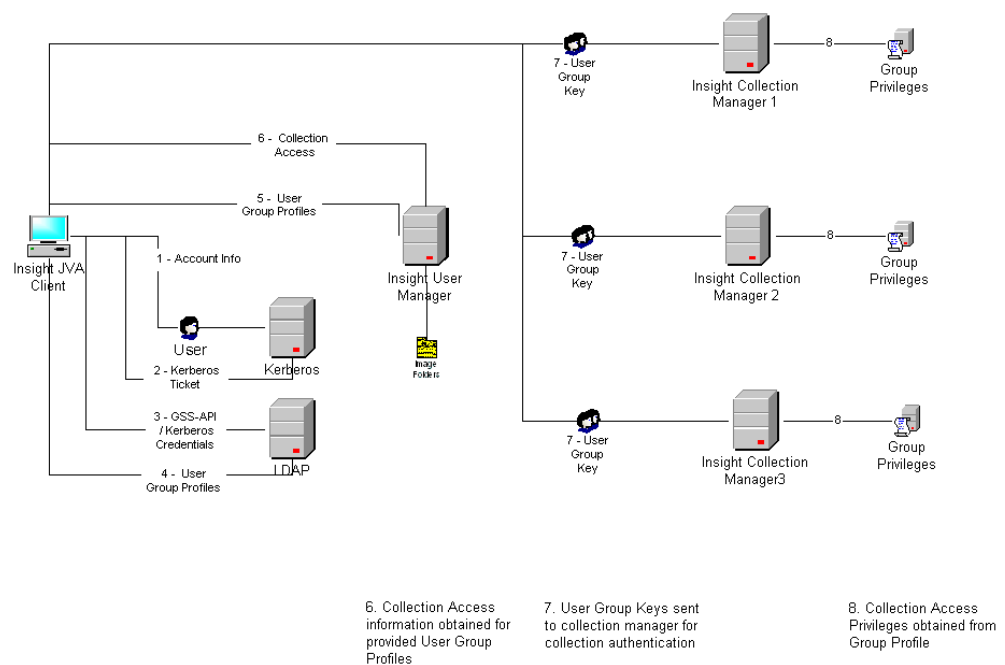
Secure Socket Layer (SSL) Communications require a certificate to encrypt data during transit, as well as to prove the identity of each party involved. For public use, trusted certificate authorities (i.e. Verisign, Thwate) provide trusted ssl certificates. Insight's LDAP Authentication method will automatically recognize and support Versign & Thwate SSL Certificates. If you are using another certificate authority, or wish to generate a self-signed certificate, please contact Luna Support at support@luna-img.com and we will provide the necessary information.

Kerberos & LDAP Authentication and Authorization

NOTE: Changing Insight's Security model can have major repercussions. Please consult with your Network and Security Administrators before implementing **any** changes regarding your local security environment.

NOTE: Please read and complete the Insight Security Worksheet at the end of this chapter before going any further.

NOTE: Finally, please test all configurations on a **test server** before implementing in a production environment.



Kerberos Authentication - Overview

Kerberos Version 5 is used for both the authentication and secure communication aspects of the Luna client and server applications. In order to use the Kerberos authentication method, you will need access to a Kerberos installation. To configure the Insight User Manager, you will need the default realm and the default KDC of your

Kerberos installation. Contact your network administrator responsible for the Kerberos server for these configurations.

As with all Kerberos installations, a Kerberos Key Distribution Center (KDC) is required. It needs to contain the user name and password you will use to be authenticated to Kerberos. Note: A KDC implementation is part of a Kerberos installation, not a part of the Insight installation.

The essential Kerberos configuration information is the default realm and the default KDC. Typically, the default realm and the KDC for that realm are indicated in the Kerberos krb5.conf/krb5.ini configuration file. On Windows, the krb5.ini file can be located in c:\winnt\. On unix, the file is located in the \etc\ directory. If this file does not exist or you are unsure of the configurations, contact your network administrator responsible for the Kerberos server for these settings.

To minimize client configuration requirements, Insight provides a version of the kerberos configuration file to each Insight client when Kerberos authentication is used. This file is written to the application's installation directory and has no impact upon the krb5.conf/krb5.conf file that may or may not reside on your system. Insight uses this file for the default realm and default KDC information. These values are defined in the InsightUserManager.dat file located in the Insight User Manager sub-directory.

Specifying the Kerberos Settings

8. In a text editor, open the InsightUserServer.dat file located in the "<insight_install>\user_manager" directory.
9. Define the **KerberosRealm** property. This is the default Kerberos realm to which the user will be authenticated. This Kerberos Realm will be attached to the user's id for authentication. The Kerberos Realm must be defined in a ALL CAPS. The Kerberos Realm must be defined in a ALL CAPS. (e.g. KerberosRealm = LUNAIMAGING.COM)
10. Define the **KerberosServer** property. This is the default Kerberos Key Distribution Center (e.g. KerberosServer = kerberos1.lunaimaging.com).

If you are unsure of these values, you may wish to submit the Implementation Worksheet to your system administrator responsible for Kerberos and Directory Services.

For example, say I was unsure of the default realm and default KDC used at my institution. After contacting my network administrator, he/she provides the following information:

```
Default Realm = LUNAIMAGING.COM  
Default KDC = kerberos1.lunaimaging.com
```

With this information I open the InsightUserServer.dat file located in the Insight User Manager installation directory. In this example, I define the KerberosRealm as

LUNAIMAGING.COM. I also define the KerberosServer as kerberos1.lunaimaging.com. It is important to note that the Kerberos Realm is defined in ALL CAPS. Under Windows 2000/Active Directory the Kerberos Realm is usually the same as the Active Directory domain name. On Solaris, the Kerberos Realm may or may not be the same as your domain, but conventions encourage using the domain name, in upper-case letters. In this example, members of lunaimaging.com are in the Kerberos realm LUNAIMAGING.COM.

```
KerberosRealm = LUNAIMAGING.COM
KerberosServer = kerberos1.lunaimaging.com
```

Based on the example above, the krb_config.conf file created on the client's application installation directory would contain the following information:

```
### insight krb_config.conf file ###

[realms]
LUNAIMAGING.COM = {
  kdc = kerberos1.lunaimaging.com
}

[domain realm]
.lunaimaging.com = LUNAIMAGING.COM

### end insight krb_config.conf file ###
```

Enabling Kerberos Authentication for the Insight User Manager

In order to enable the Kerberos Authentication Handler, in the InsightUserServer.dat file, modify the AuthenticationHandler property to reference the KerberosAuthenticationHandler instead of the standard Insight DefaultAuthenticationHandler. Save changes and restart the Insight User Manager.

For example, the AuthenticationHandler property should appear as below.

```
AuthenticationHandler =
com.luna.insight.client.security.KerberosAuthenticationHandl
er
```

If you wish to later re-enable the standard Insight User Database authentication method, simply replace the line above with "AuthenticationHandler = com.luna.insight.client.security.DefaultAuthenticationHandler". Save changes and restart the Insight User Manager.

LDAP Authorization - Overview

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling individuals and applications to locate information about organizations, individuals, and other resources. In the case of Insight, the LDAP Directory is used to store Insight authorization information. Insight uses the Kerberos credentials obtained during the Kerberos authentication process to gain access to the LDAP Directory Service. The

use of Kerberos authentication by the LDAP server unites the LDAP services with the Kerberos credentials and Kerberos based services. This also removes the need for Insight to ever store administrative passwords to the LDAP Directory service.

The use of Kerberos credentials for LDAP Directory access requires an LDAP server supporting the GSS-API SASL mechanism. The Generic Security Service API (GSS-API) provides a common interface for accessing different security services, such as Kerberos V5. Simple Authentication and Security Layer (SASL) is the mechanism used to authenticate against another service using existing Kerberos credentials. The GSS-API SASL mechanism is only supported by LDAP v3 servers. The LDAP servers that support the GSS-API SASL mechanism include Windows 2000's Active Directory server, OpenLDAP, and the SunONE Directory Server v5.2.

The use of a LDAP server for Insight Authorization requires the ability to assume the identity of the authenticated Kerberos principal. In other words, the Kerberos Principal Name provided during authentication must also be present in the LDAP Directory. For example, if your Kerberos principal name is `jsmith@foobar.com`, an attribute containing the value `"jsmith@foobar.com"` must exist in the directory.

Specifying the LDAP Settings

1. In a text editor, open the `InsightUserServer.dat` file located in the `"<insight_install>\user_manager"` directory.
2. Define the URL for the LDAP v3 Server:
 - a. Locate the following lines:

```
##  
# LdapURL - The URL of the LDAP server.  
# (note: under Windows 2000/Active Directory, this is the  
# address # of the Active Directory machine pre-pended with  
# ldap:// )  
  
#LdapURL = ldap://ldap.lunaimaging.com
```

- b. Uncomment the `LdapURL` property and change it to match the URL for your LDAP Server, when done, it should look like this:

```
##  
# LdapURL - The URL of the LDAP server.  
# (note: under Windows 2000/Active Directory, this is the  
# address # of the Active Directory machine pre-pended with  
# ldap:// )  
  
LdapURL = ldap://your.ldap.server.edu
```

3. Define the LDAP User Path, this is the directory path in the LDAP Server identifying where to find valid users
 - a. Locate the following lines:

```
##  
# LdapUserPath: Directory path in the LDAP server  
# identifying object containing authenticatable users.  
  
LdapUserPath = ou=people,dc=lunaimaging,dc=com
```

- b. Uncomment the `LdapUserPath` property and set it to the path in the LDAP database that Insight should use to find valid users, when complete, it should look like this:

```
##  
# LdapUserPath: Directory path in the LDAP server  
# identifying object containing authenticatable users.  
  
LdapUserPath = ou=people,dc=lunaimaging,dc=com
```

4. Define the field in the LDAP database that contains the Insight User Profile:

- a. Locate the following lines:

```
##  
#TargetAttributeName - The LDAP attribute name which stores  
# the collection data/profile ID's needed by the  
# application.  
  
#(note: in the case of Active Directory, "info" is the  
#"notes" field under the "telephones" tab in a user's  
properties.)  
  
#TargetAttributeName = info
```

- b. Uncomment and define the **TargetAttributeName** property. This is the LDAP attribute in which the Insight Access Profile may be found. This is the LDAP attribute name containing the Insight Access Profile needed for authorization. Insight requires the use of an LDAP attribute name, which stores the collection access information. For Windows 2000 Active Directory, by default, the "info" attribute is used. See the Windows® Active Directory & Insight User Account Information section of the documentation for additional details. For other LDAP servers, you will need to determine which attribute is currently unused, or create a new attribute to store the Insight Access Profile.

5. Define User metadata fields in the LDAP Directory

- a. Locate the following lines:

```
##  
#UserAttributeName - The LDAP directory attribute name under  
# which the user's unique login name can be found.  
  
#UserAttributeName = userprincipalname  
  
# User Info Attributes - Added 2003-07-24
```

```
#OrganizationAttributeName      = company
#EmailAttributeName             = mail
#PhoneAttributeName             = homePhone
```

- b. Uncomment and define the **UserAttributeName**, **OrganizationAttributeName**, **EmailAttributeName**, and **PhoneAttributeName** properties. The User Attribute name is the LDAP attribute in which the full Kerberos name may be found. This attribute is used to uniquely identify the user when searching the LDAP directory. The values stored in this field MUST be of the form, <YOUR USERNAME>@<YOUR KERBEROS REALM>. For Windows 2000 Active Directory, this attribute will always be “userprincipalname”. For OpenLDAP using the kb5-kdc.schema, this attribute will be the “krb5PrincipalName”. (e.g. UserAttributeName = userprincipalname)

The **OrganizationAttributeName** property is the LDAP attribute in which the user's organizational membership information is stored. Obtained values are used for administrative purposes within Inscribe. For Windows 2000 Active Directory, the “company” attribute is used to store this information. For OpenLDAP using the EduPerson schema, the “organizationName” attribute will typically be used.

The **EmailAttributeName** property is the LDAP attribute in which the user's e-mail address information is stored. Obtained values are used for administrative purposes within Inscribe. For Windows 2000 Active Directory, the “mail” attribute is used to store this information. For OpenLDAP using the EduPerson schema, the “mail” attribute will typically be used.

The **PhoneAttributeName** property is the LDAP attribute in which the user's telephone contact information is stored. Obtained values are used for administrative purposes within Inscribe. For Windows 2000 Active Directory, the “homePhone” attribute is used to store this information. For OpenLDAP using the EduPerson schema, the “telephonePhone” attribute will typically be used.

Enabling LDAP Authorization for the Insight User Manager

In order to enable the LDAP Authorization Handler, in the InsightUserServer.dat file, modify the AuthorizationHandler property to reference the LDAPAuthorizationHandler instead of the standard Insight DefaultAuthorizationHandler. Save changes and restart the Insight User Manager.

For example, the AuthorizationHandler property should appear as below.

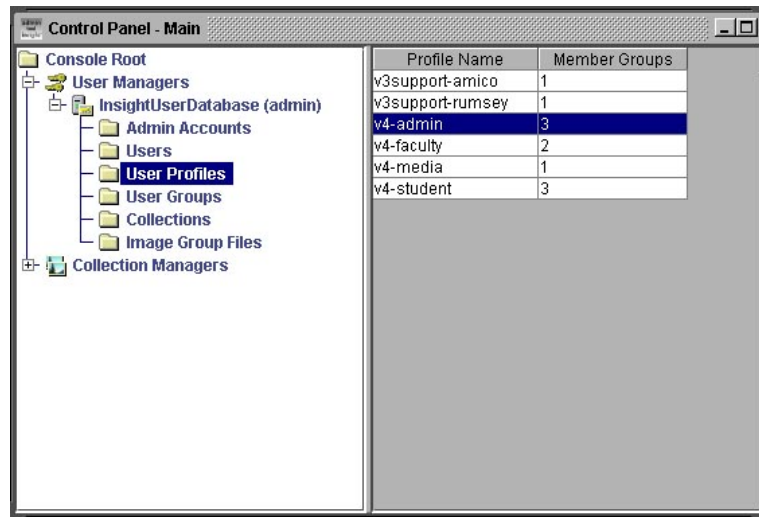
```
AuthorizationHandler =
com.luna.insight.client.security.LDAPAuthorizationHandler
```

Interaction of Kerberos & LDAP Users and Users in the Insight User Table

NOTE: Before enabling Kerberos & LDAP, please ensure that you delete all users from the Users tab in the Admin Tools. Maintaining existing users in the Insight User Manager introduces a potential security hole as clients that are not enabled for Kerberos & LDAP security will continue to try and authenticate using the Standard Authentication method.

Using the Insight Administrator Tool to identify Insight Access Profiles

1. Launch the Insight Administrator Tools
2. Expand the User Manager node and connect to your default Insight User Manager
3. Click on the User Profiles node. User Profiles determine how users access collections and whether the user has read, write, and delete privileges within User Groups. The User Groups Profiles are used as Insight Access Profiles when using LDAP authorization. For more information on User Profiles, review the Create a User Profile section in the Insight Administrator Tools User Guide.



Profile Name	Member Groups
v3support-amico	1
v3support-rumsey	1
v4-admin	3
v4-faculty	2
v4-media	1
v4-student	3

4. Identify the User Group Profile to be associated with a LDAP user account. For example, from the illustration above v4-admin and v4-media will be used to associate with the user's LDAP directory entry.
5. Note the User Group Profile Names and continue to the
6. Populate the LDAP Insight Profile Attribute with the Insight Access Profile. For Active Directory, follow the Windows® Active Directory & Insight User Account Information section of this document. If you are using OpenLDAP, you will

need to update the directory records through the OpenLDAP command-line interface. Consult your user documentation for details.

Windows® Active Directory & Insight User Account Information

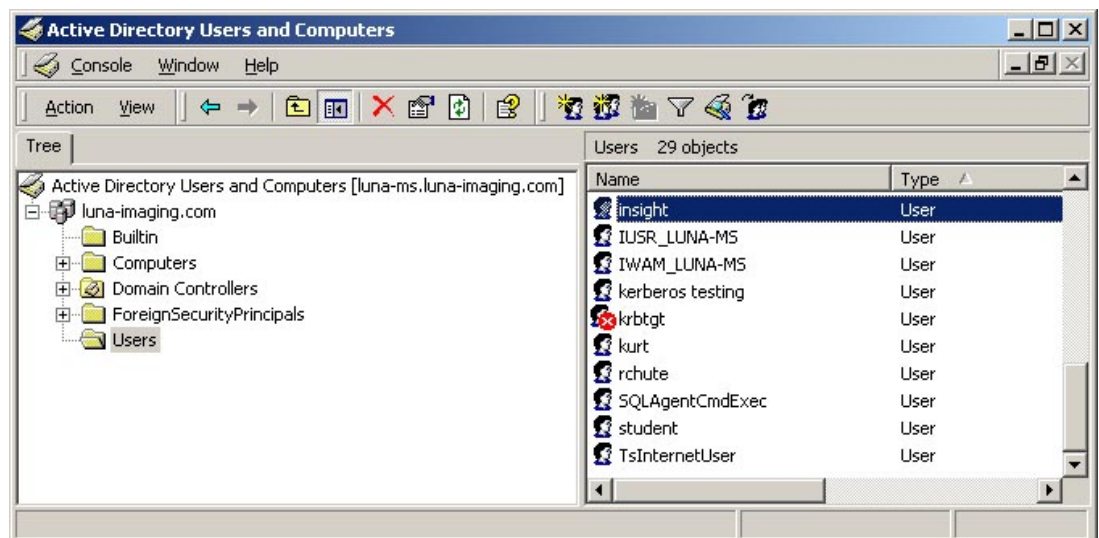
The Windows® 2000 operating system implements the Kerberos network authentication protocol as its default authentication method. On a Windows 2000 Domain Controller, both Kerberos and LDAP account information are managed using the Active Directory management consoles. Each Windows 2000 Domain Controller, also represent a Kerberos Key Distribution Center.

Users belonging to a Windows 2000 domain are managed through the Active Directory Users and Computers management console. To access the Active Directory Users and Computers console you will need administrative privileges on the domain controller you are using as your primary KDC for Insight. You may need to provide the following information to your Network Administrator responsible for Active Directory Administration.

Prior to managing user accounts using Active Directory, ensure that you have defined the User Group Profiles within the Insight Administrator tool. Refer to Section X.X of the Insight Administrator Tool documentation for details.

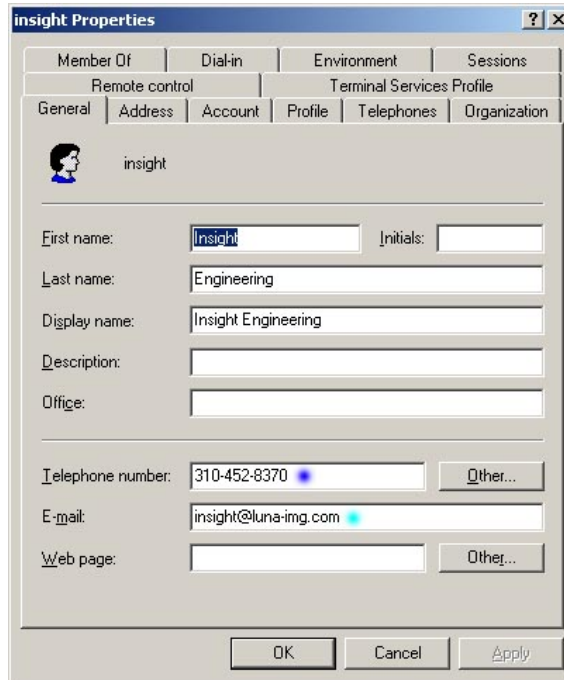
To manage Insight user account information using Active Directory:

- 1) Log-on to the Windows 2000 Domain Controller with administrative privileges.
- 2) Click Start -> Program Files -> Administrative Tools -> Active Directory Users and Computers
- 3) In the Active Directory Users and Computers, click the Users directory under the appropriate domain.



- 4) Double-click on a user account you wish to grant Insight Access to.

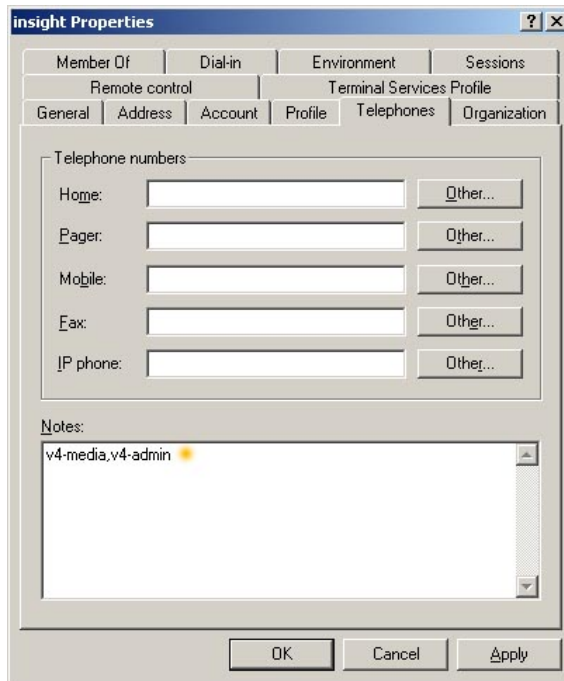
- 5) Once the properties window appears, a series of tabs will appear along the top. The General Properties tab is contain the basic information about the user.



The screenshot shows the 'insight Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: Member Of, Dial-in, Environment, Sessions, Remote control, Terminal Services Profile, General, Address, Account, Profile, Telephones, and Organization. The 'General' tab is active, showing a user profile for 'insight' with a small icon. The fields are as follows: First name: 'Insight', Initials: (empty), Last name: 'Engineering', Display name: 'Insight Engineering', Description: (empty), Office: (empty), Telephone number: '310-452-8370' with an 'Other...' button, E-mail: 'insight@luna-img.com' with a 'Other...' button, and Web page: (empty) with an 'Other...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The Telephone Number and E-mail address entries are used by Inscribe during authorization to update editorial contact information. No modifications are necessary in the General Properties tab.

- 6) Click the Telephones tab to the right of General Properties. Insight requires the use of an LDAP attribute name, which stores the collection access information (e.g. Notes).



In this example, the Notes text box is used to store the Insight Access Profile information, but any unused attribute name may be configured to store this property. User accounts may be associated with a single profile, or multiple profiles by separating each profile name with a comma. See the illustration above for an example.

- 7) Apply Changes to save the defined Insight Access Profile.

Restoring the Default Security Configuration for Insight

1. In a text editor, open the InsightUserServer.dat file located in the "<insight_install>\user_manager" directory.
2. Change the Insight Authentication Handler to the default Handler:
 - c. Locate the following lines:

```
##  
# AuthenticationHandler - the full class name of the  
# authentication handler to use for authentication.  
  
AuthenticationHandler =  
com.luna.insight.client.security.DefaultAuthenticationHandle  
r
```

- d. Change the `AuthenticationHandler` property to:
`com.luna.insight.client.
security.DefaultAuthenticationHandler`. This will tell the

User Manager not to use Kerberos or LDAP when authenticating users.

3. Change the Authorization Handler to the Default Handler:

e. Locate the following lines:

```
##  
# AuthorizationHandler - the full class name of the  
# authorization handler to use for authorization.  
AuthorizationHandler =  
com.luna.insight.client.security.DefaultAuthorizationHandler
```

Change the AuthorizationHandler property to:

```
com.luna.insight.client.security.DefaultAuthorizationHandler.
```

This will tell the User Manager not to use Kerberos or LDAP when authorizing users.

Resources

Windows 2000 Kerberos Interoperability, Microsoft Whitepaper

<<http://www.microsoft.com/WINDOWS2000/library/howitworks/security/kerbint.asp>>

Kerberos 5 (krb5 1.0) Interoperability, Technical Walkthrough, Microsoft whitepaper

<<http://www.microsoft.com/technet/win2000/kerbstep.asp> >

Kerberos interoperability issues - Paul B. Hill - MIT

<http://www.usenix.org/events/lisa-nt2000/hill/hill_html/>

Kerberos Infrastructure HOWTO

<<http://www.cryptnet.net/fdp/crypto/kerby-infra.html>>

GSS-API/Kerberos v5 Authentication

<<http://java.sun.com/products/jndi/tutorial/ldap/security/gssapi.html>>

Generic Security Service API Version 2 : Java Bindings

<<http://www.faqs.org/rfcs/rfc2853.html>>

A Recipe for Configuring and Operating LDAP Directories

<<http://www.georgetown.edu/gjia/internet2/ldap-recipe/>>

Using LDIFDE to Import and Export Directory Objects to Active Directory

<<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q237/6/77.ASP&NoWebContent=1>>

