

# AccessData AD eDiscovery<sup>®</sup>

## Administration Guide



# AccessData Legal and Contact Information

Document date: May 17, 2016

## Legal Information

©2016 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.  
588 West 400 South Suite 350  
Lindon, UT 84042  
USA

## AccessData Trademarks and Copyright Information

The following are either registered trademarks or trademarks of AccessData Group, Inc. All other trademarks are the property of their respective owners.

AccessData®	DNA®	PRTK®
AccessData Certified Examiner® (ACE®)	Forensic Toolkit® (FTK®)	Registry Viewer®
AD Summation®	Mobile Phone Examiner Plus®	Summation®
Discovery Cracker®	MPE+ Velocitor™	SilentRunner®
Distributed Network Attack®	Password Recovery Toolkit®	

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.
- AFF® and AFFLIB® Copyright© 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

BSD License: Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WordNet License

This license is available as the file LICENSE in any downloaded version of WordNet.

WordNet 3.0 license: ([Download](#))

WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or

Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database. Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

## Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using *[variable\_data]* format. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

## Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

## Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, [www.accessdata.com](http://www.accessdata.com) anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

## AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments

## Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

### AccessData Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, Inc. 588 West 400 South Suite 350 Lindon, UT 84042 USA  <i>Voice: 801.377.5410; Fax: 801.377.5426</i>
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	<i>Voice: 800.574.5199, option 1; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Federal Sales:	<i>Voice: 800.574.5199, option 2; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Corporate Sales:	<i>Voice: 801.377.5410, option 3; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Training:	<i>Voice: 801.377.5410, option 6; Fax: 801.765.4370</i> <i>Email: Training@AccessData.com</i>
Accounting:	<i>Voice: 801.377.5410, option 4</i>

## Technical Support

Technical support is available on all currently licensed AccessData solutions.

You can contact AccessData Customer and Technical Support in the following ways:

### AccessData Support Portal

You can access the Chat, Knowledge Base, Discussion Boards, White Papers and more through the AccessData Support Portal:

<https://support.accessdata.com>

### E-Mail Support:

[support@accessdata.com](mailto:support@accessdata.com)

### Telephone:

Americas/Asia-Pacific:

800-658-5199 (North America)

Support Hours: Mon-Fri, 7:00 AM – 6:00 PM (MST), except corporate holidays.

NOTE: Emergency support is available on weekends:

Saturday and Sunday 8:00am – 6:00pm MST via [support@accessdata.com](mailto:support@accessdata.com)

## Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation:  
[documentation@accessdata.com](mailto:documentation@accessdata.com)

## Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of Summation, FTK, FTK Pro, Enterprise, eDiscovery, Lab and the entire Resolution One platform. They can help you resolve any questions or problems you may have regarding these solutions.

## Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

### AccessData Professional Services Contact Information

Contact Method	Number or Address
<i>Phone</i>	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410, option 7
<i>Email</i>	<a href="mailto:services@accessdata.com">services@accessdata.com</a>

# Contents

- AccessData Legal and Contact Information** . . . . . 2
- Contents** . . . . . 7
- Part 1: Introducing eDiscovery** . . . . .17
- Chapter 1: Introducing eDiscovery** . . . . . 18
  - About eDiscovery . . . . .18
  - About the Audience for this Admin Guide . . . . .18
  - What You Can Do with eDiscovery. . . . .19
  - Basic Workflow of eDiscovery. . . . .20
  - About This Admin Guide . . . . .21
- Chapter 2: Getting Started** . . . . . 22
  - Terminology . . . . .22
  - About the AccessData Web Console . . . . .23
  - About User Accounts . . . . .24
  - Opening the AccessData Web Console . . . . .24
  - Installing the Browser Components . . . . .26
  - Introducing the Web Console . . . . .29
  - The Project List Panel . . . . .31
  - User Actions . . . . .34
  - Using Elements of the Web Console . . . . .36
- Part 2: Administrating and Configuring** . . . . .42
- Chapter 3: Introduction to Application Management**. . . . . 43
  - Workflows for Administrators . . . . .43
- Chapter 4: Using the Management Page** . . . . . 44
  - About the Management Page . . . . .44
  - Opening the Management Page . . . . .44
  - Management Page . . . . .45
- Chapter 5: Configuring and Managing System Users,**

<b>User Groups, and Roles</b> .....	46
About Users .....	46
About User Roles and Permissions .....	46
About Admin Roles and Permissions .....	48
About the Users Tab .....	51
About the Admin Roles Tab .....	53
Managing Admin Roles .....	54
Managing Users .....	56
Configuring and Managing User Groups .....	63
<b>Chapter 6: Using System Jobs</b> .....	67
About System Jobs .....	67
Adding a System Job .....	69
Agent Operations .....	73
Executing a System Job .....	74
<b>Chapter 7: Configuring the System</b> .....	76
About System Configuration .....	76
System Configuration Tab - Standard Settings .....	76
<b>Chapter 8: Configuring Advanced System Settings</b> .....	86
System Configuration Tab - Advanced Settings .....	86
<b>Chapter 9: Using the Work Manager Console and Logs</b> .....	95
Using the Work Manager Console .....	95
Work Manager Console Tab .....	95
Validating Activate Work Orders .....	97
Configuring a Work Manager .....	98
Using the System Log and Activity Log .....	99
<b>Chapter 10: Using the Site Server Console</b> .....	102
Monitoring Site Servers .....	102
Restarting the Site Server Service .....	103
Setting Network Traffic Control .....	104
Managing Jobs on the Site Server .....	105
Configuring Phone Home Settings .....	107
Replacing Windows Agent Installers .....	107
Viewing Site Server Health Metrics .....	108



<b>Part 3: Configuring Data Sources</b> .....	109
<b>Chapter 11: About Data Sources</b> .....	110
<b>Chapter 12: Managing People, Groups, Computers and Network Shares</b> .....	112
Managing People (Custodians) as Data Sources .....	112
Managing Computers for Collecting Data .....	124
Managing Network Shares for Collecting Data .....	129
Configuring Data Source Credential Options .....	132
Managing Groups for Collecting Data .....	133
Configuring Network Collectors .....	142
Managing Evidence for Collecting Data .....	143
<b>Chapter 13: Configuring Third-Party Data Repositories as Data Sources</b> .....	145
Configuring for a Domino Server .....	146
Configuring for an Exchange Online/365 Server .....	147
Configuring for Exchange 2003, 2007, and 2010 Servers .....	148
Configuring for Exchange 2010 SP1 and 2013 Servers .....	150
Configuring for an Enterprise Vault Server .....	152
Configuring for a Documentum Server .....	158
Configuring for a SharePoint Server .....	160
Configuring for Web Sites .....	163
Configuring for a DocuShare Server .....	165
Configuring for Cloud Mail .....	167
Configuring for an OpenText ECM Server .....	169
Configuring for Gmail .....	170
Configuring for Google Drive .....	171
Configuring for Druva .....	172
Configuring for a CMIS Repository .....	174
Configuring for Box .....	177
<b>Chapter 14: Getting Started with KFF (Known File Filter)</b> .....	179
About KFF .....	179
About the KFF Server and Geolocation .....	184
Installing the KFF Server .....	185
Configuring the Location of the KFF Server .....	187
Migrating Legacy KFF Data .....	188

Importing KFF Data . . . . .	189
About CSV and Binary Formats . . . . .	196
Uninstalling KFF . . . . .	199
Installing KFF Updates . . . . .	200
KFF Library Reference Information . . . . .	201
What has Changed in Version 5.6 . . . . .	206
<b>Chapter 15: Using KFF (Known File Filter)</b> . . . . .	<b>207</b>
About KFF and De-NIST Terminology . . . . .	207
Process for Using KFF . . . . .	208
Configuring KFF Permissions . . . . .	208
Adding Hashes to the KFF Server . . . . .	209
Using KFF Groups to Organize Hash Sets . . . . .	215
Enabling a Project to Use KFF . . . . .	219
Reviewing KFF Results. . . . .	221
Re-Processing KFF . . . . .	225
Exporting KFF Data . . . . .	226
<b>Part 4: Managing Projects</b> . . . . .	<b>228</b>
<b>Chapter 16: Introduction to Project Management</b> . . . . .	<b>229</b>
About Projects . . . . .	229
Workflow for Project/Case Managers . . . . .	229
<b>Chapter 17: Using the Project Management Home Page</b> . . . . .	<b>231</b>
Viewing the Home Page . . . . .	231
Introducing the Home Page . . . . .	232
Evidence Tab . . . . .	236
Adding Custom Properties . . . . .	238
Managing People for a Project . . . . .	240
<b>Chapter 18: Creating a Project</b> . . . . .	<b>245</b>
Creating Projects . . . . .	245
Using Project Properties Cloning . . . . .	258
Viewing and Editing Project Details . . . . .	259
<b>Chapter 19: Managing Custodians for a Project</b> . . . . .	<b>261</b>
About Managing Custodians for a Project . . . . .	261

Using the Home Custodians Tab . . . . .	262
Using the Data Sources People Tab . . . . .	266
<b>Chapter 20: Managing Tags</b> . . . . .	267
Managing Labels . . . . .	269
Managing Issues . . . . .	272
<b>Chapter 21: Setting Project Permissions</b> . . . . .	275
About Project Permissions . . . . .	275
Permissions Tab . . . . .	279
Associating Users and Groups to a Project . . . . .	281
Associating Project Roles to Users and Groups . . . . .	282
Creating a Project Role . . . . .	283
<b>Chapter 22: Running Reports</b> . . . . .	285
Accessing the Reports Tab . . . . .	285
<b>Chapter 23: Configuring Review Tools</b> . . . . .	290
Configuring Markup Sets . . . . .	290
Configuring Custom Fields . . . . .	294
Configuring Tagging Layouts . . . . .	297
Configuring Highlight Profiles . . . . .	302
Configuring Redaction Text . . . . .	306
<b>Chapter 24: Monitoring the Work List</b> . . . . .	308
Accessing the Work List . . . . .	308
<b>Chapter 25: Managing Document Groups</b> . . . . .	310
About Managing Document Groups . . . . .	310
Creating a Document Group During Import . . . . .	313
Creating a Document Group in Project Review . . . . .	313
Renumbering a Document Group in Project Review . . . . .	314
Deleting a Document Group in Project Review . . . . .	314
Managing Rights for Document Groups in Project Review . . . . .	315
<b>Chapter 26: Managing Transcripts and Exhibits</b> . . . . .	316
Creating a Transcript Group . . . . .	316

Capturing Realtime Transcripts . . . . .	320
Using Transcript Vocabulary. . . . .	325
Uploading Exhibits. . . . .	327
<b>Chapter 27: Managing Review Sets</b> . . . . .	328
Creating a Review Set . . . . .	328
Deleting Review Sets . . . . .	330
Renaming a Review Set . . . . .	331
Manage Permissions for Review Sets. . . . .	332
<b>Chapter 28: Project Folder Structure</b> . . . . .	333
Project Folder Path . . . . .	333
Project Folder Subfolders . . . . .	334
<b>Chapter 29: Using Language Identification</b> . . . . .	336
Language Identification . . . . .	336
<b>Part 5: Using Lit Holds</b> . . . . .	338
<b>Chapter 30: Using Litigation Holds</b> . . . . .	339
About Litigation Holds . . . . .	339
Basic Workflow of Litigation Holds . . . . .	341
Process for Using Litigation Holds . . . . .	342
Configuring the System for Litigation Holds . . . . .	342
Configuring Litigation Hold Settings . . . . .	346
Creating a Litigation Hold . . . . .	357
Managing Litigation Holds . . . . .	365
Using Lit Hold Dashboard Widgets . . . . .	373
<b>Part 6: Loading Data</b> . . . . .	374
<b>Chapter 31: Introduction to Loading Data</b> . . . . .	375
Importing Data . . . . .	375
<b>Chapter 32: Using the Evidence Wizard</b> . . . . .	376
Using the Evidence Wizard . . . . .	376
Adding Evidence to a Project Using the Evidence Wizard . . . . .	382
<b>Chapter 33: Importing Evidence</b> . . . . .	385
About Importing Evidence Using Import . . . . .	385

Importing Evidence into a Project . . . . .	386
<b>Chapter 34: Data Loading Requirements</b> . . . . .	388
Document Groups . . . . .	388
Email & eDocs . . . . .	391
Coding . . . . .	393
Related Documents . . . . .	396
Transcripts and Exhibits . . . . .	397
Work Product . . . . .	399
Sample DII Files . . . . .	400
DII Tokens . . . . .	404
<b>Chapter 35: Analyzing Document Content</b> . . . . .	408
Using Cluster Analysis . . . . .	408
Using Entity Extraction . . . . .	411
<b>Chapter 36: Editing Evidence</b> . . . . .	414
Editing Evidence Items in the Evidence Tab . . . . .	414
Evidence Tab . . . . .	415
<b>Part 7: Using Jobs</b> . . . . .	417
<b>Chapter 37: Introduction to Jobs</b> . . . . .	418
About Jobs . . . . .	418
<b>Chapter 38: Introduction to the eDiscovery Collection Job</b> . . . . .	423
About Collection Jobs . . . . .	423
<b>Chapter 39: Creating and Managing Jobs</b> . . . . .	425
Adding a Job . . . . .	426
General Job Wizard Tabs . . . . .	428
Approving a Job . . . . .	452
Executing a Job . . . . .	452

Processing a Job . . . . .	453
Using Job Reports . . . . .	454
Using Job Notifications . . . . .	456
Using Job Templates and Filter Templates . . . . .	458
Additional Job Tasks . . . . .	462
<b>Chapter 40: Configuring Jobs for Third-Party Data Sources . . . . .</b>	<b>468</b>
Other Data Sources Filter Options . . . . .	470
Box Collections Options . . . . .	471
Cloud Mail Collection Options for People . . . . .	473
Domino Collection Options . . . . .	474
Documentum Collections Options . . . . .	475
DocuShare Collection Options . . . . .	477
Enterprise Vault Server Collection Options . . . . .	479
Collecting Exchange Emails for Custodians . . . . .	482
Exchange Public Folder Collection Options . . . . .	484
Google Drive Collection Options . . . . .	485
OpenText ECM Collection Options . . . . .	486
SharePoint Collection Options . . . . .	487
Website Collection Options . . . . .	490
Druva Collection Options . . . . .	491
CMIS Collection Options . . . . .	493
<b>Part 8: Using the Dashboard . . . . .</b>	<b>496</b>
<b>Chapter 41: Using the Dashboard . . . . .</b>	<b>497</b>
About the Dashboard . . . . .	497
Configuring Dashboard Widgets . . . . .	499
<b>Part 9: Configuring and Using LawDrop . . . . .</b>	<b>500</b>
<b>Chapter 42: Understanding LawDrop™ . . . . .</b>	<b>501</b>
About LawDrop . . . . .	501
<b>Chapter 43: Administrating LawDrop™ . . . . .</b>	<b>503</b>
About Administrating LawDrop . . . . .	503
Configuring the System for Using LawDrop . . . . .	504
<b>Chapter 44: Using LawDrop™ . . . . .</b>	<b>508</b>
Getting Started with LawDrop . . . . .	508

Creating and Deleting Sub-Folders in LawDrop . . . . .	511
Dropping and Uploading Files to LawDrop . . . . .	512
Viewing and Managing Uploaded Files . . . . .	514
Sharing Files and Folders . . . . .	518
Adding Evidence to Projects Using LawDrop . . . . .	521
Exporting Files to LawDrop . . . . .	523
<b>Part 10: Reference</b> . . . . .	<b>524</b>
<b>Chapter 45: Installing the AccessData Elasticsearch Windows Service</b> . . . . .	<b>525</b>
About the Elasticsearch Service . . . . .	525
Installing the Elasticsearch Service . . . . .	526
<b>Chapter 46: Using the Site Server</b> . . . . .	<b>528</b>
About Site Servers . . . . .	528
Before Installing a Site Server. . . . .	530
Installing a Site Server . . . . .	530
Site Server Configuration . . . . .	531
<b>Chapter 47: Agent Certs</b> . . . . .	<b>534</b>
About Certs . . . . .	534
Creating Certs . . . . .	537
<b>Chapter 48: Installing the Windows Agent</b> . . . . .	<b>542</b>
Supported Hashing Algorithms . . . . .	542
Manually Installing the Windows Agent . . . . .	542
Using Your Own Certificates. . . . .	548
Controlling Consumption of the CPU . . . . .	549
Important Information . . . . .	549
<b>Chapter 49: Installing the Unix / Linux Agent</b> . . . . .	<b>550</b>
Installing The Enterprise Agent on Unix/Linux . . . . .	550
<b>Chapter 50: Installing the Mac Agent</b> . . . . .	<b>552</b>
Configuring the AccessData Agent installer . . . . .	552
Installing the Agent . . . . .	554
Uninstalling the Agent . . . . .	554
<b>Chapter 51: Integrating with AccessData Forensics Products</b> . . . . .	<b>555</b>
Installation . . . . .	556

Managing User Accounts and Permissions Between	
FTK and Summation/eDiscovery . . . . .	556
Creating and Viewing Projects . . . . .	556
Known Issues with FTK Compatibility . . . . .	559



# Part 1

# Introducing eDiscovery

This part introduces eDiscovery and includes the following chapters:

- [Introducing eDiscovery](#) (page 18)
- [Getting Started](#) (page 22)

# Chapter 1

## Introducing eDiscovery

---

### About eDiscovery

eDiscovery helps you to identify and collect relevant data in-house to address electronic discovery from beginning to end. You can run collections across the entire enterprise Network of a company. The collected evidence can then be processed, reviewed, and exported.

The reports are enhanced by the use of keyword searches and filters to gather only relevant data that pertains to a case. The resulting production set can then be exported into an AD1 format, or into a variety of load file formats such as Concordance, Summation, EDRM, Introspect, and iConect.

### About the Audience for this Admin Guide

This product is intended for use in gathering and processing electronically stored evidence for criminal, civil, and internal corporate cases.

The audience for this forensic investigation software tool includes law enforcement officials as well as corporate security and IT professionals who need to access and evaluate the evidentiary value of files, folders, computers, and other electronic data sources. They should be well-versed in the eDiscovery process. They should also have a good understanding of Chain of Custody and the implications of running the eDiscovery process within an organization. They should also have the following competencies when using this software:

- Basic knowledge of and training in forensic policies and procedures
- Familiarity with the fundamentals of collecting digital evidence and ensuring the legal validity of the evidence
- Understanding of forensic images and how to acquire forensically sound images
- Experience with case studies and reports

# What You Can Do with eDiscovery

eDiscovery addresses the entire eDiscovery model in a repeatable, defensible, and automated manner, using a single solution.

See [Getting Started](#) on page 22.

## What you can do with eDiscovery

Phase in the eDiscovery Model	What you can do
Information Management	<ul style="list-style-type: none"> <li>• Thoroughly audit for and identify electronically stored information (ESI) that falls outside your records retention policies.</li> <li>• Flag non-compliant files and log their locations.</li> </ul>
Preserve and Collect	<ul style="list-style-type: none"> <li>• Forensically collect ESI from workstations, laptops, network servers, email servers, and structured data repositories.</li> <li>• Collect only relevant data from shared resources or all people-created data, as you choose, using advanced searching and filtering options.</li> <li>• Create native PSTs and NSFs from email servers.</li> <li>• Perform incremental collections to only collect data that has changed from a previous collection.</li> <li>• Reuse previously executed collections and associate them with multiple projects.</li> </ul>
Processing and deduplication	<ul style="list-style-type: none"> <li>• Process data as you collect, while maintaining complete chain of custody.</li> <li>• Use distributed processing that greatly reduces processing time.</li> <li>• Automatically identify and categorize data, including encrypted files.</li> <li>• Deduplicate email and documents across the case or for a specific people.</li> <li>• Scale processes to handle massive data sets.</li> </ul>
Analysis and Review	<ul style="list-style-type: none"> <li>• Use a friendly web-based interface with native file review that allows for collaborative, full review prior to creating a production set and exporting to a load file format.</li> <li>• Perform advanced searches with hit highlighting in files, emails, and attachments that lets you quickly find responsive evidence without having to read every single word.</li> <li>• Cull data by leveraging sophisticated searching and rich filtering.</li> <li>• View documents by families or similarity.</li> <li>• View email grouped by conversations.</li> </ul>
Production	<ul style="list-style-type: none"> <li>• Produce responsive-only documents and email in native format or an AD1 forensic archive, organized by people or as a single instance, with options to preserve the original folder structure.</li> <li>• Generate load files for export to popular third-party review tools, including Concordance, EDRM XML, iConect, Introspect, Relativity, Ringtail (MDB), or Summation eDII.</li> <li>• Produce detailed reports, such as search reports, processing exception reports, production, and exclusion reports.</li> <li>• Utilize rolling production support that enables batch production.</li> </ul>

# Basic Workflow of eDiscovery

Although there is no formal order in which you collect, process, and export evidence using eDiscovery, you can use the following basic workflow as a guide.

## Basic Workflow of eDiscovery

Step	Task	Link to the tasks
1	Configure and setup eDiscovery and eDiscovery users before you begin collecting evidence.	<ul style="list-style-type: none"><li>• See <a href="#">Configuring the System</a> on page 76.</li></ul>
2	Add people, Network shares, computers, and groups whose data you want to collect.	<ul style="list-style-type: none"><li>• See <a href="#">About Data Sources</a> on page 110.</li></ul>
3	Create a project.	<ul style="list-style-type: none"><li>• See <a href="#">Creating a Project</a> on page 245.</li></ul>
4	(Optional) Create a litigation hold.	<ul style="list-style-type: none"><li>• See <a href="#">Using Litigation Holds</a> on page 339.</li></ul>
5	Collect evidence from the people, network shares, computers, and groups that you added.	<ul style="list-style-type: none"><li>• See <a href="#">Introduction to Jobs</a> on page 418.</li></ul>
6	Approve, execute, and then process a collection.	<ul style="list-style-type: none"><li>• See <a href="#">Approving a Job</a> on page 452.</li><li>• See <a href="#">Executing a Job</a> on page 452.</li><li>• See <a href="#">Processing a Job</a> on page 453.</li></ul>
7	Review data.  After you process a collection, you open the resulting case from the Project List into Project Review. From Project Review, you filter, search, and apply labels on the processed data until you have a production set that contains only relevant files for the case. At that point, you can export the production set to a load file as described in the next step.	<ul style="list-style-type: none"><li>• See the <i>Reviewer Guide</i>.</li></ul>
8	Export the production set to a load file.	<ul style="list-style-type: none"><li>• See the <i>Reviewer Guide</i>.</li></ul>

# About This Admin Guide

This Admin Guide explains how administrators do the following:

- Configure system settings
- Create and manage projects
- Configure data sources
- Configure and use e-discovery features
- Use the Dashboard
- Use platform components such as the Site Server and agents

This guide includes the following parts:

- [Getting Started](#) (page 22)
- [Administrating and Configuring](#) (page 42)
- [Configuring Data Sources](#) (page 109)
- [Managing Projects](#) (page 228)
- [Loading Data](#) (page 374)
- [Introduction to Jobs](#) (page 418)
- [Using the Dashboard](#) (page 496)
- [Using Lit Holds](#) (page 338)
- [Configuring and Using LawDrop](#) (page 500)
- [Reference](#) (page 524)

For information about reviewing project data using Project Review, see the *eDiscovery Reviewer Guide*.

For information about new features, fixed issues, and known issues, see the *eDiscovery Release Notes*.

You can download the *Reviewer Guide* and *Release Notes* from the *Help/Documentation* link. See [User Actions](#) on page 34.

# Chapter 2

## Getting Started

---

### Terminology

Features and technology are shared across the multiple applications. To provide greater compatibility between products, some terminology in the user interface and documentation has been consolidated. The following table lists the common terminology:

#### Terminology Changes

Previous Term	New Term
Case	Project
Custodian	Person
Custodians	People
System Console	Work Manager Console
Security Log	Activity Log
Audit Log	User Review Activity

# About the AccessData Web Console

The application displays the AccessData web-based console that you can open from any computer connected to the network.

All users are required to enter a username and password to open the console.

What you can see and do in the application depends on your product license and the rights and permissions granted to you by the administrator. You may have limited privileges based on the work you do.

See [About User Accounts](#) on page 24.

---

**Note:** Like many applications that you run in a browser, do not click the browser's Back button. Use the menus and buttons to navigate in the console.

---

## Web Console Requirements

### Software Requirements

The following are required for using the features in the web console:

- Windows-based PC running the Internet Explorer web browser:
  - Internet Explorer 9 or higher is required for full functionality of most features.
  - Internet Explorer 10 or higher is required for full functionality of all features. (Some new features use HTML5 which requires version 10 or higher.)

---

**Note:** If you have issues with the interface displaying correctly, view the application in compatibility view for Internet Explorer.

---

- The console may be opened using other browsers but will not be fully functional.
- Internet Explorer Browser Add-on Components
  - Microsoft Silverlight--Required for the console.
  - Adobe Flash Player--Required for imaging documents in Project Review.
- AccessData console components
  - AD NativeViewer--Required for viewing documents in the Alternate File Viewer in Project Review. Includes Oracle OutsideX32.
  - AD Bulk Print Local--Required for printing multiple records using Bulk Printing in Project Review. To use these features, install the associated applications on each users' computer. See [Installing the Browser Components](#) on page 26.

### Hardware Recommendations

- Use a display resolution of 1280 x 1024 or higher.  
Press **F11** to display the console in full-screen mode and maximize the viewing area.

# About User Accounts

Each user that uses the web console must log in with a user account. Each account has a username and password. Administrators configure the user accounts.

User accounts are granted permissions based on the tasks those users perform. For example, one account may have permissions to create and manage projects while another account has permissions only to review files in a project.

Your permissions determine which items you see and the actions you can perform in the web console.

There is a default Administrator account.

## *User Account Types*

Depending on how the application is configured, your account may be either an Integrated Windows Authentication account or a local application account.

The type of account that you have will affect a few elements in the web interface. For example, if you use an Integrated Windows Authentication account, you cannot change your password within the console. However, you can change your password within the console if you are using an application user account.

# Opening the AccessData Web Console

You use the AccessData web console to perform application tasks.

See [About the AccessData Web Console](#) on page 23.

You can launch the console from an approved web browser on any computer that is connected to the application server on the network.

See [Web Console Requirements](#) on page 23.

To start the console, you need to know the IP address or the host name of the computer on which the application server is installed.

When you first access the console, you are prompted to log in. Your administrator will provide you with your username and password.

### **To open the web console**

1. Open Internet Explorer.

---

**Note:** Internet Explorer 7 or higher is required to use the web console for full functionality. Internet Explorer 10 or 11 is recommended.

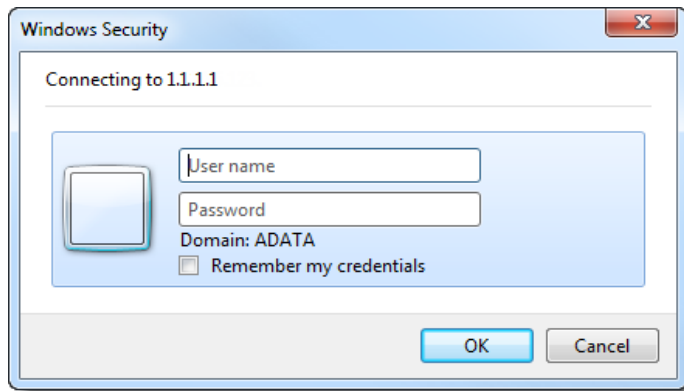
---

2. Enter the following URL in the browser's address field:  
`https://<host_name>/ADG.map.Web/`  
where `<host_name>` is the host name or the IP address of the application server.  
This opens the login page.  
You can save this web page as a favorite.



3. One of two login pages displays:  
If you are using Integrated Windows Authentication, the following login page displays.

### Integrated Windows Authentication Page



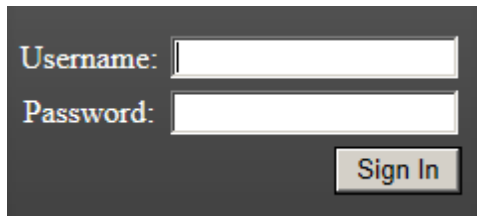
---

**Note:** If you are using Integrated Windows Authentication and are not on the domain, you will see a Windows login prompt.

---

If you are *not* using Integrated Windows Authentication, the login page displays the product name and version for the product license that your organization is using and provides fields for your username and password.

### Non-Integrated Windows Authentication Login



4. On the login page, enter the username and password for your account.  
If you are logging in as the administrator for the very first time and have not enabled Integrated Window Authentication, enter the pre-set default user name and password. Contact your technical support or sales representative for login information.
5. Click **Sign In**.  
If you are authenticated, the application console displays.  
If you cannot log in, contact your administrator.
6. The first time the web console is opened on a computer, you may be prompted to install the following plug-ins:
  - Microsoft Silverlight
  - Adobe Flash Player
  - AD Alternate File Viewer (Native Viewer)
  - AD Bulk Print LocalDownload the plug-ins. When a pop-up from Internet Explorer displays asking to run or download the executable, click **Run**. Complete the install wizard to finish installing the plug-in.  
See [Web Console Requirements](#) on page 23.  
See [Installing Browser Components Manually](#) on page 28.

# Installing the Browser Components

To use all of the features of the web console, each computer that runs the web console must have Internet Explorer and the following add-ons:

- [Microsoft Silverlight](#)--Required for the console.
- [Adobe Flash Player](#)--Required for imaging documents in Project Review.
- [AccessData Alternate File Viewer \(Native Viewer\)](#)--Required for imaging documents in Project Review. This includes the Oracle OutsideX32 plug-in.
- [AccessData Local Bulk Print](#)--Required for printing multiple records using Bulk Printing in Project Review

**Important:** Each computer that runs the console must install the required browser components. The installations require Windows administrator rights on the computer.

Upon first login, the web console will detect if the workstation's browser does not have the required versions of the add-ons and will prompt you to download and install the add-ons.



See [Installing Components through the Browser](#) on page 26.

See [Installing Browser Components Manually](#) on page 28.

## *Installing Components through the Browser*

### Microsoft Silverlight

#### To install Silverlight

1. If you need to install Silverlight, click **Click now to install** in the Silverlight plug-in window.
2. Click **Run** in the accompanying security prompts.
3. On the *Install Silverlight* dialog, **Install Now**.  
When the Silverlight installer completes, on the Installation successful dialog, click **Close**.

If the web browser does not display the AD logo and then the console, refresh the browser window.



The application Main Window displays and you can install Flash Player from the plug-in installation bar.

## Adobe Flash Player

### To install Flash Player

1. If you need to install Flash Player, click the **Flash Player** icon.
2. Click **Download now**.
3. Click **Run** in the accompanying security prompts.
4. Complete the installation.
5. Refresh the browser.

Once the application is installed, you need to install the Alternate File Viewer and Local Bulk Print software. You can find the links to download the add-ons in the dropdown in the upper right corner of the application.

## AccessData Alternate File Viewer (Native Viewer)

### To install the AD Alternate File Viewer (Native Viewer)

1. From the *User Actions* dropdown, select **AD Alternate File Viewer**.
2. Click **RUN** on the *NearNativeSetup.exe* prompt.
3. Click **Next** on the *InstallShield Wizard* dialog.
4. Click **Next** on the *Custom Setup* dialog.
5. Click **Install** on the *Ready to Install the Program* dialog.
6. Allow the installation to proceed and then click **Finish**.
7. Close the browser and re-log in.
8. Click **Allow** on the *ADG.UI.Common.Document.Views.NearNativeControl* prompt.
9. Refresh the browser.

## AccessData Local Bulk Print

### To install the Local Bulk Print add-on

1. From the *User Actions* dropdown, select **AD Local Bulk Print**.
2. Click **Run** at the AccessData Local Bulk Print.exe prompt in Internet Explorer.
3. In the *InstallShield Wizard* dialog, click **Next**.
4. Accept the license terms and click **Next**.
5. Accept the default location in the *Choose Destination Location* dialog and click **Next**.
6. Click **Install** on the *Ready to Install the Program* dialog.
7. Click **Finish**.

## Installing Browser Components Manually

You can use EXE files to install the components outside of the browser. You can run these locally or use software management tools to install them remotely.

### Installing AD Alternate File Viewer

To install the Alternate File Viewer add-on, navigate to the following path on the server:

C:\Program Files (x86)\AccessData\MAP\NearNativeSetup.exe

### To install the AD Alternate File Viewer add-on

1. Run the *NearNativeSetup.MSI* file.
2. Click **Next** on the *InstallShield Wizard* dialog.
3. Click **Next** on the *Custom Setup* dialog.
4. Click **Install** on the *Ready to Install the Program* dialog.
5. Allow the installation to proceed and then click **Finish**.

### Installing the Local Bulk Print Tool

To install the Local Bulk Print tool, navigate to the following path on the server:

C:\Program Files (x86) \AccessData\MAP\AccessDataBulkPrintLocal.exe

### To install the Local Bulk Print add-on

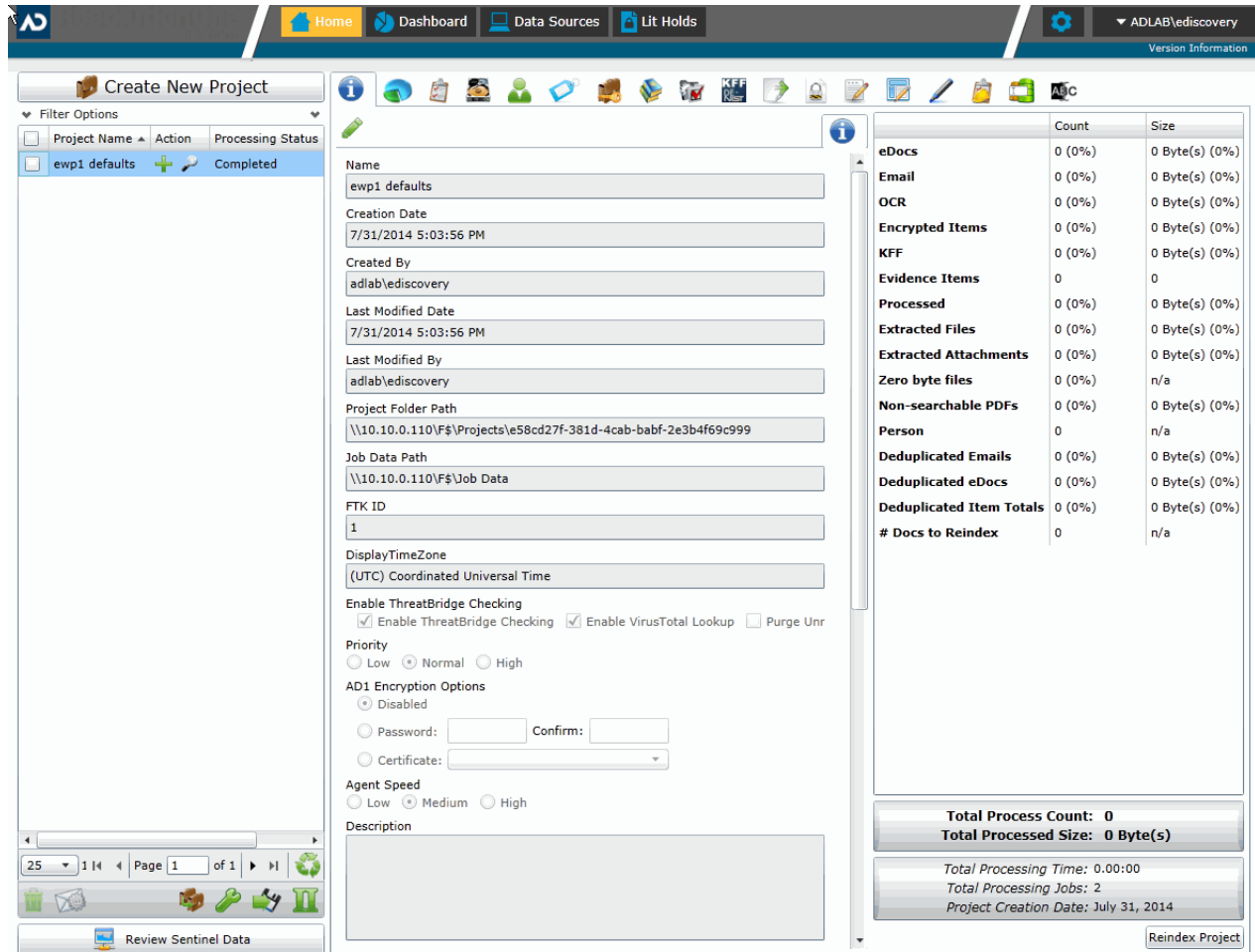
1. Run the *AccessDataBulkPrintLocal.exe*. The wizard should appear.
2. Click **Next** to begin.
3. Click **Next** on the *Select Installation Folder* dialog.
4. Click **Next**. After the installation is complete, click **Close**.

### Installing Adobe Flash Player

Visit <http://get.adobe.com/flashplayer/> and follow the prompts to install the flash player.

# Introducing the Web Console

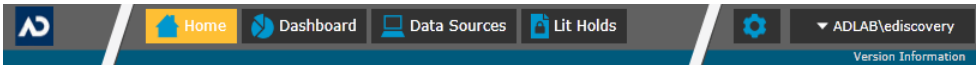
The user interface for the application is the AccessData web console. The console includes different tabs and elements.





The items that display in the console are determined by the following:

- Your application's license
- Your user permissions

The main elements of the application are listed in the following table. Depending on the license that you own and the permissions that you have, you will see some or all of the following:

Component	Description
Navigation bar	This lets you open multiple pages in the console. 
Home page	The <i>Home</i> page lets you create, view, manage, and review projects based on the permissions that you have. This is the default page when you open the console. See <a href="#">Using the Project Management Home Page</a> on page 231.

Component	Description
Dashboard	(Available in eDiscovery or with a special Litigation Hold license.) The <i>Dashboard</i> allows you to view important event information in an easy-to-read visual interface. See <a href="#">Using the Dashboard</a> on page 497.
Data Sources	The <i>Data Sources</i> tab lets you manage people, computers, network shares, evidence, as well as several different connectors. This tab allows you to manage these data sources throughout the system, not just by project. See <a href="#">About Data Sources</a> on page 110.
Lit Hold	(Available in eDiscovery or with a special Litigation Hold license.) The <i>Lit Hold</i> tab lets you create and manage litigation holds. See <a href="#">Using Litigation Holds</a> on page 339.
Management (gear icon)	The <i>Management</i> page lets administrators perform global management tasks. See <a href="#">Opening the Management Page</a> on page 44.
	
User Actions	Actions specific to the logged-in user that affects the user's account. See <a href="#">User Actions</a> on page 34.
 Project Review	The <i>Project Review</i> page lets you analyze, filter, code and label documents for a selected project. You access <i>Project Review</i> from the <i>Home</i> page. See the <i>Reviewer Guide</i> for more information on Project Review. You can download the <i>Reviewer Guide</i> from the <i>Help/Documentation link</i> . See <a href="#">User Actions</a> on page 34.

# The Project List Panel

The *Home* page includes the *Project List* panel. The *Project List* panel is the default view after logging in. Users can only view the projects for which they have created or been given permissions.

<input type="checkbox"/>	Project Name ▲	Action	Processing Status	Size
<input checked="" type="checkbox"/>	001ProductionSe5.2.2.63		Completed	28 MB
<input type="checkbox"/>	001ProductionSet5.2.2.64		Completed	29 MB
<input type="checkbox"/>	001ProductionSet5.2.2.65		Completed	31 MB
<input type="checkbox"/>	001ProductionSet5.2.2.66		Completed	4.1 MB
<input type="checkbox"/>	001ProductionSet5.2.2.67		Completed	13 MB
<input type="checkbox"/>	001ProductionSet5.2.2.68		Completed	26 GB
<input type="checkbox"/>	001ProductionSet-5.2.2Pa		Processing	8.6 GB
<input type="checkbox"/>	01ProductionSet		Completed	131 MB
<input type="checkbox"/>	01ProductionSet-PSR		Completed	33 MB
<input type="checkbox"/>	02ProductionSet		Completed	1.2 GB
<input type="checkbox"/>	02ProductionSet-PSR		Completed	4.0 MB
<input type="checkbox"/>	03ProductionSet		Completed	55 MB
<input type="checkbox"/>	04ProductionSet		Completed	216 KB

Page Size: 25 Total: 13 (0) Page 1 of 1






Administrators and users, given the correct permissions, can use the project list to do the following:

- Create projects.
- View a list of existing projects.
- Add evidence to a project.
- Launch Project Review.




If you are not an administrator, you will only see either the projects that you created or projects to which you were granted permissions.

The following table lists the elements of the project list. Some items may not be visible depending on your permissions.

## Elements of the Project List

Element	Description
Create New Project	Click to create a new project. See <a href="#">Creating a Project</a> on page 245.
Filter Options	Allows you to search and filter all of the projects in the project list. You can filter the list based on any number of fields associated with the project, including, but not limited to the project name. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Filter Enabled	Displayed if you have enabled a filter.
Project Name Column	Lists the names of all the projects to which the logged-in user has permissions.
Action Column	Allows you to add evidence to a project or enter Project Review.
	 Add Data Allows you to add data to the selected project.
	 Project Review Allows you to review the project using Project Review. See the Reviewer Guide for more information on using Product Review. You can download the Reviewer Guide from the Help/Documentation link. See <a href="#">Changing Your Password</a> on page 35.
Processing Status Column	Lists the status of the projects: Not Started - The project has been created but no evidence has been added. Processing - Evidence has been added and is still being processed. Completed - Evidence has been added and processed. <b>Note:</b> When processing a small set of evidence, the Processing Status may show a delay of two minutes behind the actual processing of the evidence. You may need to refresh the list to see the current status. See <a href="#">Refresh</a> below.
Size Column	Lists the size of the data within the project.
Page Size drop-down	Allows you to select how many projects to display in the list. The total number of projects that you have permissions to see is displayed.
Total	Lists the total number of projects displayed in the Project List.
Page	Allows you to view another page of projects.
 Refresh	If you create a new project, or make changes to the list, you may need to refresh the project list
 Delete	Select one or more projects and click <b>Delete Project</b> to delete them from the <i>Project List</i> .
 Project Property Cloning	Clone the properties of an existing project to another project. You can apply a single project's properties to another project, or you can pick and choose properties from multiple individual projects to apply to a single project. See <a href="#">Using Project Properties Cloning</a> on page 258.

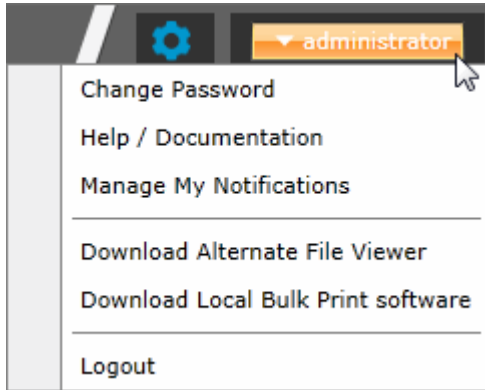


Element	Description
 Custom Properties	Add, edit, and delete custom columns that will be listed in the Project list panel. When you create a project, this additional column will be listed in the project creation dialog. See <a href="#">Adding Custom Properties</a> on page 238.
 Export to CSV	Export the Project list to a .CSV file. You can save the file and open it in a spreadsheet program.
 Columns	Add or remove viewable columns in the <i>Project List</i> .

# User Actions

Once in the web console, you can preform user actions that are specific to you as the logged-in user. You access the options by clicking on the logged-in user name in the top right corner of the console.

## User Actions



## User Actions

Link	Description
Logged-on user	The username of the logged-on user is displayed; for example, administrator.
Change password	Lets the logged-on user change their password. See <a href="#">Changing Your Password</a> on page 35. <b>Note: This function is hidden if you are using Integrated Windows Authentication.</b>
Help/ Documentation	Lets you to access the latest version of the Release Notes and User Guide. The files are in PDF format and are contained in a ZIP file that you can download.
Manage My Notifications	Lets you to manage the notifications that you have created and that you belong to. See <a href="#">About Managing Notifications for a Job</a> on page 456. You can delete notifications, export the notifications list to a CSV file, and filter the notifications with the Filter Options. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Download Alternate File Viewer	Lets you to download the Alternate File Viewer application. See <a href="#">AccessData Alternate File Viewer (Native Viewer)</a> on page 27.
Download Local Bulk Print software	Lets you to access the latest version of the Local Bulk Print software. See <a href="#">AccessData Local Bulk Print</a> on page 28.
Logout	Logs you off and returns you to the login page. <b>Note: This function is hidden if you are using Integrated Windows Authentication.</b>

## Changing Your Password

---

**Note:** This function is hidden if you are using Integrated Windows Authentication. You must change your password using Windows.

---

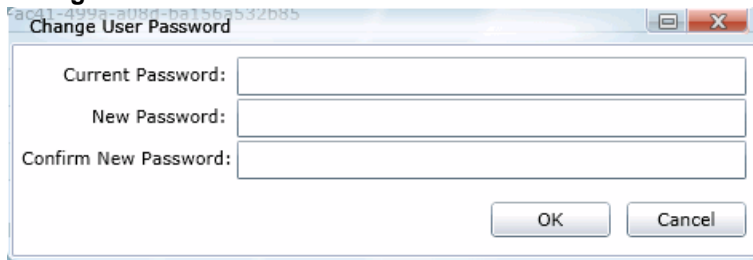
Any logged-in user can change their password. You may want to change your password for one of the following reasons:

- You are changing a default password after you log in for the first time.
- You are changing your password on a schedule, such as quarterly.
- You are changing your password after having a password reset.

### To change your own password

1. Log in using your username and current password.  
See [To open the web console](#) on page 24.
2. In the upper right corner of the console, click your logged-in username.
3. Click **Change Password**.

### Change User Password



4. In the **Change User Password** dialog, enter the current password and then enter and confirm the new password in the respective fields. The following are password requirements:
  - The password must be between 7 - 50 characters.
  - At least one Alpha character.
  - At least one non-alphanumeric character.
5. Click **OK**.

# Using Elements of the Web Console

## *Maximizing the Web Console Viewing Area*

You can press **F11** to enable or disable the console in full-screen mode.


## *About Content in Lists and Grids*

Many objects within the console are made up of lists and grids. Many elements in the lists and grids recur in the panels, tabs, and panes within the interface. The following sections describe these recurring elements.

You can manage how the content is displayed in the grids.

- See [Refreshing the Contents in List and Grids](#) on page 36.
- See [Managing Columns in Lists and Grids](#) on page 37.
- See [Sorting by Columns](#) on page 36.
- See [Filtering Content in Lists and Grids](#) on page 39.
- See [Changing Your Password](#) on page 35.

## Refreshing the Contents in List and Grids

There may be times when the list you are looking at is not dynamically updated. You can refresh the contents by clicking  .

## Sorting by Columns

You can sort grids by most columns.

---

**Note:** You can set a default column to sort by when you create a project or in the *Project Details* pane. The default is ObjectID.

---

### **To sort a grid by columns**

1. Click the column head to sort by that column in an ascending order.  
A sort indicator (an up or down arrow) is displayed.
2. Click it a second time to sort by descending order.
3. Click **Search Options > Clear Search** to return to the default column.

## Sorting By Multiple Columns

In the *Item List* in *Project Review*, you can also sort by multiple columns. For example, you can do a primary sort by file type, and then do a second sort by file size, then a third sort by accessed date.

### To sort a grid by columns

1. Click the column head to sort by that column in an ascending order.  
A sort indicator (an up or down arrow) is displayed.
2. Click it a second time to sort by descending order.
3. In the *Item List* in *Project Review*, to perform a secondary search on another column, hold Shift+Alt keys and click another column.  
A sort indicator is displayed for that column as well.
4. You can repeat this for multiple columns.

## Moving Columns in a Grid View

You can rearrange columns in a Grid view in any order you want. Some columns have pre-set default positions. Column widths are also sizable.

### To move columns

- ❖ In the Grid view, click and drag columns to the position you want them.





## Managing Columns in Lists and Grids

You can select the columns that you want visible in the Grid view. Project managers can create custom columns in the Custom Fields tab on the *Home* page.

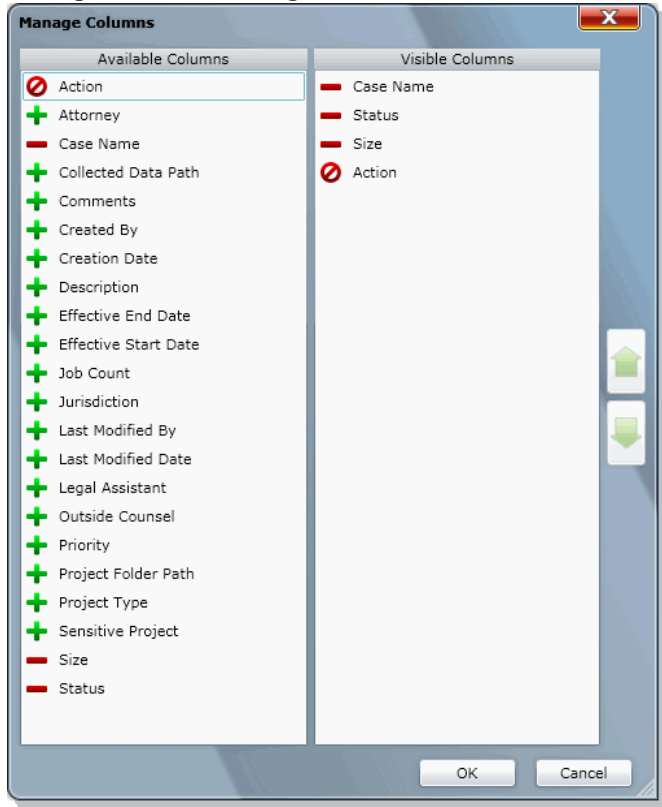
See [Configuring Custom Fields](#) on page 294.

For additional information on using columns, see *Using Columns in the Item List Panel* in the *Reviewer Guide*.

### To manage columns

1. In the grid, click  **Columns**.
2. In the *Manage Columns* dialog, there are two lists:
  - *Available Columns*  
Lists all of the Columns that are available to display. They are listed in alphabetical order.  
If the column is configured to be in the Visible Columns, it has a  .  
If the column is not configured to be in the Visible Columns, it has a  .  
If the column is a non-changeable column (for example, the Action column in the Project List), it has a  .
  - *Visible Columns*  
Lists all of the Columns that are displayed. They are listed in the order in which they appear.

## Manage Columns Dialog



3. To configure columns to be visible, in the *Available Columns* list, click the **+** for the column you want visible.
4. To configure columns to not be visible, in the *Visible Columns* list, click the **-** for the column you want not visible.
5. To change the display order of the columns, in the *Visible Columns* list, select a column name and click **↑** or **↓** to change the position.
6. Click **OK**.

## Managing the Grid's Pages

When a list or grid has many items, you can configure how many items are displayed at one time on a page. This is helpful for customizing your view based on your display size and resolution and whether or not you want to scroll in a list.

### To configure page size

1. Below a list, click the **Page Size** drop-down menu.
2. Select the number of items to display in one page.
3. Use the arrows by **Page *n* of *n*** to view the different pages.

## Filtering Content in Lists and Grids

When a list or grid has many items, you can use a filter to display a portion of the list. Depending on the data you are viewing, you have different properties that you can filter for.

For example, when looking at the Activity Log, there could be hundreds of items. You may want to view only the items that pertain to a certain user. You can create a filter that will only display items that include references to the user.

For example, you could create the following filter:

**Activity contains BSmith**

This would include activities that pertain to the BSmith user account, such as when the account was created and permissions for that user were configured.

You could add a second filter:

**Activity contains BSmith**

**OR Username = BSmith**

This would include the activities performed by BSmith, such as each time she logged in or created a project.

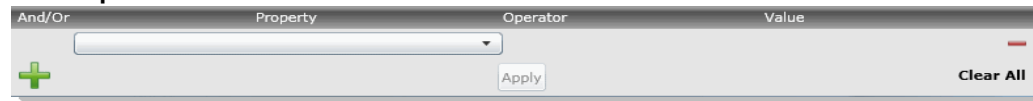
In this example, because an OR was used instead of an AND, both sets of results are displayed.

You can add as many filters as needed to see the results that you need.

### To use filters


1. Above the list, click **Filter Options**.  
This opens the filter tool.

#### Filter Options



The screenshot shows the 'Filter Options' tool interface. It features a header with four columns: 'And/Or', 'Property', 'Operator', and 'Value'. Below the header, there is a green plus sign on the left, a text input field under 'Property', a dropdown menu under 'Operator', and a text input field under 'Value'. At the bottom of the tool, there is an 'Apply' button and a 'Clear All' button.

2. Use the *Property* drop-down to select a property on which to filter.  
This list will depend on the page that you are on and the data that you are viewing.
3. Use the *Operator* drop-down to select an operator to use.  
See [Filter Operators](#) on page 40.
4. Use the *Value* field to enter the value on which you want to filter.  
See [Filter Value Options](#) on page 41.
5. Click **Apply**.  
The results of the filter are displayed.  
Once a filter had been applied, the text *Filter Enabled* is displayed in the upper-right corner of the panel. This is to remind you that a filter is applied and is affecting the list of items.
6. To further refine the results, you can add additional filters by clicking **+ Add**.
7. When adding additional filters, be careful to properly select *And/Or*.  
If you select **And**, all filters must be true to display a result. If you select **OR**, all of the results for each filter will be displayed.

8. After configuring your filters, click **Apply**.
9. To remove a single filter, click  **Delete**.
10. To remove all filters, click **Disable** or **Clear All**.
11. To hide the filter tool, click **Filter Options**.

## Filter Operators

The following table lists the possible operators that can be found in the filter options. The operators available depend upon what property is selected.

### Filter Operators

Operator	Description
=	Searches for a value that equals the property selected. This operator is available for almost all value filtering and is the default value.
!=	Searches for a value that does not equal the property selected. This operator is available for almost all value filtering.
>	Searches for a value that is greater than the property selected. This operator is available for numerical value filtering.
<	Searches for a value that is less than the property selected. This operator is available for numerical value filtering.
>=	Searches for a value that is greater than and/or equal to the property selected. This operator is available for numerical value filtering.
<=	Searches for a value that is less than and/or equal to the property selected. This operator is available for numerical value filtering.
Contains	Searches for a text string that contains the value that you have entered in the value field. This operator is available for text string filtering.
StartsWith	Searches for a text string that starts with the value that you have entered in the value field. This operator is available for text string filtering.
EndsWith	Searches for a text string that ends with a value that you have entered in the value field. This operator is available for text string filtering.



## Filter Value Options

The following table lists the possible value options that can be found in the filter options. The value options available depend upon what property is selected.

### Filter Value Options

Value Option	Description
Blank field	This value allows you to enter a specific item that you can search for. The <i>Description</i> property is an example of a property where the value is a blank field.
Date value	This value allows you to enter a specific date that you can search for. You can enter the date in a m/d/yy format or you can pick a date from a calendar. The <i>Creation Date</i> property is an example of a property where the value is entered as a date value.
Pulldown	This value allows you to select from a pulldown list of specific values. The pulldown choices are dependent upon the property selected. The <i>Priority</i> property with the choices <i>High, Low, Normal, Urgent</i> is an example of a property where the value is chosen from a pulldown.

## Part 2

# Administering and Configuring

This part describes how to administrate the application and includes the following chapters:

- [Introduction to Application Management](#) (page 43)
- [Using the Management Page](#) (page 44)
- [Configuring and Managing System Users, User Groups, and Roles](#) (page 46)
- [Configuring the System](#) (page 76)
- [Using the Work Manager Console and Logs](#) (page 95)
- [Using the Site Server Console](#) (page 102)
- [Using Language Identification](#) (page 336)
- [Getting Started with KFF \(Known File Filter\)](#) (page 179)
- [Using KFF \(Known File Filter\)](#) (page 207)

## Chapter 3

# Introduction to Application Management

---

This chapter is designed to help application administrators perform management tasks. Application administration tasks are performed on the Management page. Administrators can perform their tasks as long as they have been granted the correct permissions.

See [About User Roles and Permissions](#) on page 46.

## Workflows for Administrators

Administrators and managers configure and manage the global application environment.

Before creating and reviewing projects, you should review and perform the following tasks for configuring the application.

### Workflow for Configuring the Application

Step	Task	Link to the Tasks
1	Decide which authentication mode to use	See <a href="#">Opening the AccessData Web Console</a> on page 24.
2	Manage users, groups, and roles	See <a href="#">Planning User Roles</a> on page 47. See <a href="#">Managing Users</a> on page 56. See <a href="#">Configuring and Managing User Groups</a> on page 63.
3	Configure default project settings	See <a href="#">Configuring Default Project Settings</a> on page 83.

At regular intervals, administrators should perform the following tasks to manage the overall system health and performance of the application.

### Workflow for Managing the Application

Step	Task	Link to the tasks
1	Monitor system activity using logs	See <a href="#">Viewing the System Log or Activity Log</a> on page 101.
2	Monitor the performance of the Distribution Server and the Work Managers	See on page 95.

Most of these administrative tasks are performed in the web console in the *Management* page.

## Chapter 4

# Using the Management Page

---

## About the Management Page

Administrators manage the application through the Management page. You can manage users and users permissions, configure aspects of the application on a global basis, and monitor activity on the system.

See [Management Page](#) on page 45.

## Opening the Management Page

Administrators, and users with management permissions, use the *Management* page to configure and manage the application.

### To access the Management page

1. Log in to the web console as administrator or as a user with management permissions.  
See [Opening the AccessData Web Console](#) on page 24.  
See [Managing Users](#) on page 56.
2. In the web console, click **Management**.

# Management Page

You can use the *Management* page to maintain the list of people who use the application, including their specific usage rights and roles. From *Management*, you can view system and security logs.

You can also configure Active Directory, agent credentials, a notification email server. The system administration console area of the *Management* page lets you view Work Manager status.

Depending on the license that you own and the permissions that you have, you will see some or all of the following:

## Management Page Features and Options

Management Feature	Available Options
Users 	See <a href="#">About the Users Tab</a> on page 51. See <a href="#">Managing Users</a> on page 56.
User Groups 	See <a href="#">Configuring and Managing User Groups</a> on page 63. See <a href="#">User Groups Tab</a> on page 64.
Admin Roles 	See <a href="#">About Admin Roles and Permissions</a> on page 48. See <a href="#">Managing Admin Roles</a> on page 54.
System Jobs 	See <a href="#">Adding a System Job</a> on page 69. See <a href="#">System Job Options</a> on page 70.
System Configuration 	See <a href="#">Configuring Active Directory Synchronization</a> on page 77. See <a href="#">Configuring Export Options</a> on page 85. See <a href="#">Configuring Default Project Settings</a> on page 83.
Work Manager Console 	See <a href="#">Using the Work Manager Console and Logs</a> on page 95.
Site Server Console 	See <a href="#">Using the Site Server Console</a> on page 102.
System Log 	See <a href="#">Using the System Log and Activity Log</a> on page 99. See <a href="#">System Log Tab</a> on page 99.
KFF Library 	See <a href="#">Using KFF (Known File Filter)</a> on page 207.
KFF Group Templates 	See <a href="#">Using KFF (Known File Filter)</a> on page 207.
Activity Log 	See <a href="#">Using the System Log and Activity Log</a> on page 99. See <a href="#">Activity Log Tab</a> on page 100.

## Chapter 5

# Configuring and Managing System Users, User Groups, and Roles

---

This chapter will help administrators to configure users, user groups, and roles.

## About Users

A user is any person who logs in and performs tasks in the web console. Each person should have their own user account. You can configure accounts to have specific permissions to perform specific tasks. When users open the console, what they see and do is based on their assigned permissions.

There are two users in the database that do not appear in the user interface. The passwords for these accounts are unique per system/strong passwords:

- Administrator - This is a different user than the Application Administrator role
- eDiscoveryProcessingUser

Permissions are managed by user roles.

See [Adding Users](#) on page 57.

## About User Roles and Permissions

You can assign users different permissions based on the tasks that you want them to perform. The permissions that a user has affects the items that they see and the tasks that they can perform in the web console.

For example, you can have one group of users that can manage the whole application and another group can create projects and another group can only reviews files in a project.

Changes to permissions for a currently logged-in user take effect when they log out and log back in.

You assign permissions to a user by configuring roles and then associating users, or groups of users, to those roles.

You can configure roles at the following levels:

- Admin roles
- Project roles

*Admin roles* provide global permissions to a user for the whole application. The following are examples of admin permissions that you can use:

- Application Administrator
- Manage Users
- Create/Edit Projects
- Manage Admin Roles
- View the System Console

See [About Admin Roles and Permissions](#) on page 48.

*Project roles* only apply to a specific project. The following are examples of global permissions that you can use:

- Project Administrator (for that project only)
- Project Reviewer
- Manage Evidence
- View Project Reports
- Manage Project People

For more information, see [Introduction to Project Management](#) on page 229.

## *Planning User Roles*

Before creating users, plan the types of roles your users will be performing. This facilitates the process of assigning roles and permissions to users.

See [Workflows for Administrators](#) on page 43.

Possible things to consider when planning user roles:

- How many and which users should have Administrator permissions for the entire application?
- How many and which users should have application management permissions to perform tasks such as creating and managing other users, roles, and projects?
- How do you want to distinguish between users who can create and manage projects versus those who can only review them?
- How many and which users should have project-level permissions to perform tasks such as adding and managing evidence and creating production sets?

# About Admin Roles and Permissions

An admin role is a set of permissions that you assign to users or groups. Each admin role has specific permissions that allows users to manage the application, such as managing users, managing roles and permissions, and creating and managing projects.

See [Admin Permissions](#) on page 48.

You can create admin roles or assign one of the default admin roles already created in the system. There are three default admin roles:

## Admin Roles Default Roles

Role	Description
Application Administrator	This role grants all permissions to manage the application.
Power User	This role grants the user permissions for create/edit project, manager user groups, and manage users.
Users	This role grants the user permissions for create/edit project.

## Creating Admin Roles

When you create an admin role, you can grant users Administrator permissions (all permissions) or grant a combination of individual permissions.

If you want to grant permissions to a user that only allows them to review a project, then use project roles instead of admin roles.

---

**Note:** The admin permissions available depend upon the license that you have.

---

## Admin Permissions

You can configure admin roles with the following admin permissions

### Admin Permissions

Permissions	Description
<b>Administrator</b>	Grants all rights to the user/group for all projects.
<b>SubAdmin</b>	Grants rights as a SubAdmin in a multi-tenant environment. (Summation only) See <a href="#">Understanding the Multi-Tenant Environment</a> on page 338.
<b>Custom Selection</b>	You can select the following individual administrator roles:



## Admin Permissions

Permissions	Description
<b>Create/Edit Projects</b>	<p>Grants the right to create projects.</p> <p>Users with this permission are automatic administrators of any projects that they create.</p> <p>They can also view properties for all other projects on the <i>Home</i> page.</p> <p>See <a href="#">Creating a Project</a> on page 245.</p>
<b>Create/Edit Projects - Restricted</b>	<p>Grants the rights to create projects.</p> <p>However, users with this permission do not have administrator status for the projects that they create.</p> <p>Users with this permission can do the following for the projects they create:</p> <ul style="list-style-type: none"> <li>• Associate users to the projects they create</li> <li>• Assign permissions for the projects they create</li> <li>• View people and data sources for the projects they create</li> </ul> <p>They can also view properties for all other projects on the <i>Home</i> page.</p> <p>See <a href="#">Creating a Project</a> on page 245.</p>
<b>Delete Project</b>	<p>Grants the right to delete projects on the <i>Home</i> page</p> <p>See <a href="#">Creating a Project</a> on page 245.</p>
<b>Manage User Groups</b>	<p>Grants the right to add, edit, delete, and assign roles to groups.</p> <p>See <a href="#">Planning User Roles</a> on page 47.</p>
<b>Manage Users</b>	<p>Grants the rights to add, edit, delete, activate, deactivate, reset passwords, and assign admin roles to users.</p> <p>See <a href="#">About Users</a> on page 46.</p> <p>See <a href="#">Adding Users</a> on page 57.</p> <p>See <a href="#">Editing the Email Address of a User</a> on page 59.</p> <p>See <a href="#">Deleting Users</a> on page 61.</p> <p>See <a href="#">Deactivating a User</a> on page 62.</p> <p>See <a href="#">Activating a User</a> on page 62.</p> <p>See <a href="#">Resetting a User's Password</a> on page 60.</p> <p>See <a href="#">Associating User Groups and Admin Roles to a User</a> on page 58.</p>
<b>Create People</b>	<p>Grants the right to create and manage People.</p> <p>See <a href="#">Configuring and Managing System Users, User Groups, and Roles</a> on page 46.</p>
<b>Delete People</b>	<p>Grants the right to delete People.</p> <p>See <a href="#">Deleting Users</a> on page 61.</p>
<b>Create Nodes</b>	<p>Grants the right to create job targets.</p> <p>See <a href="#">Managing People, Groups, Computers and Network Shares</a> on page 112.</p>
<b>Delete Nodes</b>	<p>Grants the right to delete job targets.</p> <p>See <a href="#">Managing People, Groups, Computers and Network Shares</a> on page 112.</p>

## Admin Permissions

Permissions	Description
<b>Global ID Admin</b>	Grants the right to access and change the permissions of any user in any project. See <a href="#">Associating User Groups and Admin Roles to a User</a> on page 58.
<b>Manage Project Permissions</b>	Grants the right to manage project permissions. See <a href="#">Setting Project Permissions</a> on page 275.
<b>System Console</b>	Grants the right to view and use the <i>Work Manager Console</i> and <i>Site Server Console</i> on the <i>Management</i> page. See on page 95 and <a href="#">Using the Site Server Console</a> on page 102.
<b>LitHold Manager</b>	Grants the right to manage Litholds.
<b>Evidence Admin</b>	Grants the right to add, delete, and associate the evidence. See <a href="#">Using the Evidence Wizard</a> on page 376.
<b>Manage Admin Roles</b>	Grants the right to add, edit, delete and assign admin roles. See <a href="#">About Admin Roles and Permissions</a> on page 48. See <a href="#">Creating an Admin Role</a> on page 54. See <a href="#">Managing Admin Roles</a> on page 54. See <a href="#">Adding Permissions to an Admin Role</a> on page 54.
<b>Manage KFF</b>	Grants the right to create and manage KFF libraries, sets, templates, and groups. See <a href="#">Using KFF (Known File Filter)</a> on page 207.
<b>System Jobs</b>	Grants the right to view and use the System Jobs tab on the Management page. See <a href="#">Using System Jobs</a> on page 67.
<b>View Activity Log</b>	Grants the right to view the <i>Activity Log</i> on the <i>Management</i> page. See <a href="#">Viewing the System Log or Activity Log</a> on page 101.
<b>Purge Activity Log</b>	Grants the right to purge the <i>Activity Log</i> . See <a href="#">Activity Log Tab</a> on page 100.
<b>Manage Job Templates</b>	Grants the right to manage the following: <ul style="list-style-type: none"> <li>• Job Templates</li> <li>• Filter Templates</li> <li>• System Job Templates</li> </ul> See <a href="#">Managing Templates</a> on page 91.

# About the Users Tab







The *Users* tab on the *Management* page can be used by administrators to add, edit, delete, and associate users on a global scale. Users are people who are logging in and working in the application.

From the *Users* list, you can also add, edit, or delete the application’s users. You can set users as active or inactive, reset user passwords, and set global and group permissions.




The *Users* tab is the default page when you click **Management** on the menu bar. The *User Groups* tab below the *Users* list pane allows you to associate and remove associations to users. The *Admin Roles* tab below the *Users* list pane identifies the admin roles that are associated with a highlighted user.

Changes to permissions for a currently logged-in user take effect after they log out of the system and log back in.

## Elements of the Users Tab

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Users List	Displays all users. Click the column headers to sort by the column.
Refresh 	Refreshes the Users list. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the Users list. See <a href="#">Sorting by Columns</a> on page 36.
Delete 	Deletes the selected user. Only active when a user is selected. See <a href="#">Deleting Users</a> on page 61.
Add Users 	Adds a user. See <a href="#">About Users</a> on page 46.
Edit User 	Edits the selected user. You can add or change a selected user’s email address that is used for notifications of the application’s events. See <a href="#">Editing the Email Address of a User</a> on page 59.
Delete User 	Deletes the selected user(s). See <a href="#">Deleting Users</a> on page 61.
Reset a User’s Password 	Assigns a new password for the selected user. See <a href="#">Resetting a User’s Password</a> on page 60.
Deactivate Users 	Makes selected user(s) inactive in the application. See <a href="#">Deactivating a User</a> on page 62.
Activate Users 	Reactivates selected user. See <a href="#">Activating a User</a> on page 62.
User Groups Tab 	Allows you to associate or disassociate groups to users. See <a href="#">Associating Users/Admin Roles to a Group</a> on page 65.










## Elements of the Users Tab (Continued)

Element	Description
Admin Roles Tab 	Allows you to associate or disassociate admin roles to users. See <a href="#">Associating User Groups and Admin Roles to a User</a> on page 58.
Add Association 	Associates a user to a group or admin role.
Remove Association 	Disassociates a user from a group or admin role.

# About the Admin Roles Tab

The *Admin Roles* tab on the *Management* page can be used to add, edit, delete, and associate admin roles. Admin roles are a set of global permissions that you can associate with a user or a group.

## Elements of the Admin Roles Tab


Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Admin Roles List	Displays all admin roles. Click the column headers to sort by the column.
Refresh 	Refreshes the Admin Roles List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the Admin Roles List. See <a href="#">Sorting by Columns</a> on page 36.
Delete 	Deletes the selected admin roles. Only active when an admin roles is selected. See <a href="#">About Admin Roles and Permissions</a> on page 48.
Add Admin Roles 	Adds an admin role. See <a href="#">Creating an Admin Role</a> on page 54.
Edit Admin Roles 	Edits the selected admin roles.
Delete Admin Roles 	Deletes the selected admin roles.
Users Tab 	Allows you to associate or disassociate users to an admin role.
Groups Tab 	Allows you to associate or disassociate groups to an admin role.
Features Tab 	Allows you to add administrator permissions to an admin role. See <a href="#">Adding Permissions to an Admin Role</a> on page 54.

# Managing Admin Roles

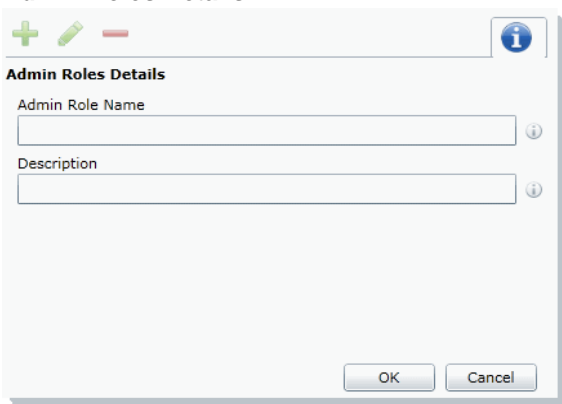
## Creating an Admin Role

Before you can assign permissions to an admin role, you have to create the role.

### To create an admin role

1. Log in to the web console using administrator rights.
2. Click the **Management** tab.
3. Click the **Admin Roles** tab.  
See [About Admin Roles and Permissions](#) on page 48.
4. Click the **Add** button  .

### Admin Roles Details



Admin Roles Details

Admin Role Name

Description


OK Cancel

5. Enter a name for the admin role and a description.
6. Click **OK**.  
The role is added to the Admin Role list.

## Adding Permissions to an Admin Role

After you have created an admin role, you need to add permissions to it before you assign it to a user or a group.

### To add permissions to an admin role

1. Log in to the web console using administrator rights.
2. Click the **Management** tab.
3. Click the **Admin Roles** tab.
4. Select the role from the *Admin Roles List*.
5. Click the **Features** tab  .
6. Select the permissions.  
See [About Admin Roles and Permissions](#) on page 48.

---

**Note:** Users with the Manage Admin Roles, Manage Users, or Manage User Groups permission have the ability to upgrade themselves or other users to system administrators.

---

7. Click **Save**.

# Managing Users

Administrators, and users assigned the Manage Users permission, manage users by doing the following:

- [Managing the List of Users](#) on page 56
- [Adding Users](#) on page 57
- [Editing the Email Address of a User](#) on page 59
- [Resetting a User's Password](#) on page 60
- [Deleting Users](#) on page 61
- [Deactivating a User](#) on page 62
- [Activating a User](#) on page 62
- [Associating User Groups and Admin Roles to a User](#) on page 58

## About User Account Types

You can configure the application to use one of two user types:


- Integrated Windows Authentication (IWA) account (uses synced Active Directory user accounts)
- Local application account (forms authentication - you create all application users)

The type of user that you use changes some elements of creating and managing users. For example, if you use an Integrated Windows Authentication account, you can either manually create application users based on AD users or import them directly from AD. Also, you cannot manage a user's password.

## Managing the List of Users

You create and manage users from the *Users* tab on the *Management* page.

### To open the Users tab

1. Log in as an administrator or a user that has the Manage Users permission.  
See [Opening the AccessData Web Console](#) on page 24.
2. Click **Management**.
3. Click **Users**  .

The users list lets you view all the users, including the following columns of information about them:

- Username
- Email Address of the user
- Date that the user was created
- Date of last login for the user
- Active status of a user
- First and Last name of the user
- Description



From the users list, you can also do the following:

- Add users
- Edit users
- Delete users
- Set users as active or inactive
- Reset user passwords (forms authentication only)
- Associate users to User Groups and Admin roles

When you create and view the list of users, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display the items that you want.  
See [Filtering Content in Lists and Grids](#) on page 39.

## Adding Users

Each person that uses the console must log in with a username and password. Each person should have their own user account.

Administrators, and users assigned the Manage Users permission, can add new user accounts.

When a user is created, an entry for that user is created in the system databases.

How you add users differs depending on whether you use Integrated Windows Authentication or Forms Authentication.

See [About User Account Types](#) on page 56.

If you are using Forms Authentication, you need to configure both the username and password. In this mode, a password is required, and the *Password* field is bolded.

If you *are* using Integrated Windows Authentication, you can do one of the following:

- Manually add a domain user - enter the domain username but *do not* enter a password. In this mode, the Password field is hidden.
- Import users from Active Directory

### To manually add a user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the *User Details* pane, click **+ Add**.
3. In the **Username** field, enter a unique username.  
If you are using forms authentication, the name must be between 7 - 32 characters and must contain only alphanumeric characters.  
If you are using Integrated Windows Authentication, enter the user's domain and username. For example, <domain>\<username>.
4. Enter the First and Last name of the user.
5. (Optional) In the **Email Address** field, enter the email address of the user.

6. If you are using forms authentication, enter a password in the **Password** and the **Reenter Password** fields.  
The password must be between 7 - 20 characters.
7. Click **OK**.

### To import users from Active Directory (IWA mode only)

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the *User Details* pane, **Import From AD**.
3. Search for users that you want to add.  
For example, usernames that start with A.  
You can search using the following:
  - Starts With
  - Match Exact
  - Ends With
  - Contains
  - 3a. Select a search operator.
  - 3a. Enter a value to search on.
  - 3b. Click **Search**.
  - 3c. Check the names that you want to import.
  - 3d. Click **Add to Import List**.
  - 3e. (Optional) Perform another search.
4. In the *Import List*, review the list of users.
5. (Optional) Select and delete any users you do not want to import.
6. Click **Continue**.
7. Check for any conflicts and verify the list that you want to import.
8. Click **Import**.
9. View the list of users that were imported.
10. (Optional) Click **Add more** to add import more users.
11. Click **Close**.
12. Verify the user list.

## Associating User Groups and Admin Roles to a User


Administrators, and users assigned the Manage Users permission, can associate User Groups and Admin Roles to users.

See [About User Roles and Permissions](#) on page 46.

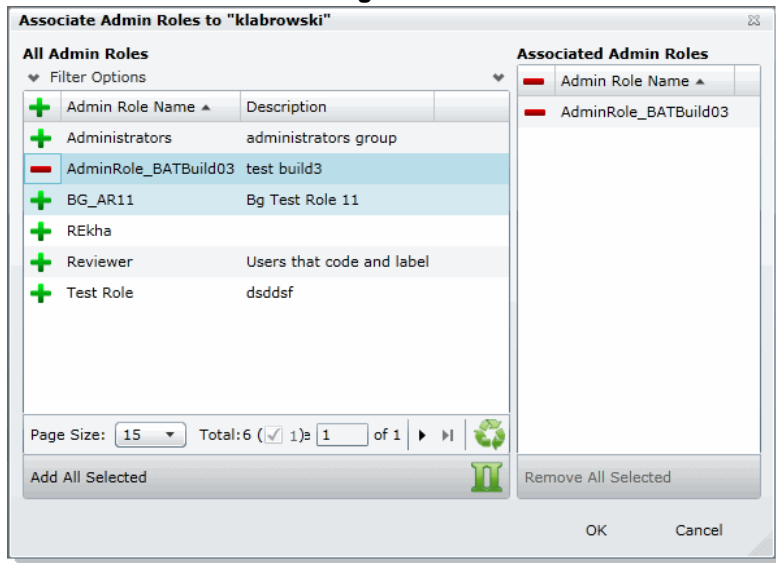
See [Configuring and Managing User Groups](#) on page 63.


### To associate Users Groups or Admin Roles to user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, select a user to associate to an admin role.

3. In the bottom pane, select the *User Groups* or *Admin Roles* tab.
4. Click the **Add Association** button .

### Associate Admin Roles Dialog




5. Click  to add the group or role to the user.
6. Click **OK**.

## Disassociating a User Group or Admin Role from a User

Administrators, and users assigned the Manage Users permission, can disassociate User Groups and Admin Roles from users.

See [About User Roles and Permissions](#) on page 46.


### To disassociate User Groups or Admin Roles from a user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, select a user who you want to disassociate from an admin role.
3. In the bottom pane, click the *User Groups* or *Admin Roles* tab.
4. Check the group or role that you want to remove.
5. Click the **Remove Association** button .

## Editing the Email Address of a User

If you are using Forms Authentication, administrators, and users assigned the Manage Users permission, can change the email address of an existing user. If you need to make more than an email change (such as changing the username), you must delete the user and then recreate the user with the correct information.

### To edit the email address of a user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, select the user whose email address you want to edit.
3. In the *User Details* pane, click  **Edit**.
4. In the *Email Address* field, enter the email address of the user.
5. Click **OK**.

## Resetting a User's Password

If you are using Forms Authentication, and of a user has forgotten their password, administrators and users assigned the Manage Users permission can reset passwords for users.

---

**Note:** This function is hidden if you are using Integrated Windows Authentication. Reset a password using Windows methods.

---

You cannot reset the password of the Service Account.


See [Changing the Password of the Service Account](#) on page 60.

When you reset a user's password, a new password is automatically created. You can then give the new password to the user. After they log in with the new password, they can change the password themselves.

You cannot reset your own password. To change your own login password, use the *Change Password* dialog, not the *User* page.

See [Changing Your Password](#) on page 35.

### To reset the password of an administrator or user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, select a user.
3. Click .
4. Copy the password and email it to the user, informing them that they can change the password after logging in.

## Changing the Password of the Service Account

This only applies if you are using Forms Authentication. The service account password can only be changed by the user who is logged in as the master administrator. This person is typically the one who initially performed the installation. The username cannot be changed.

See [Changing Your Password](#) on page 35.

You can use the same process as you do for a user.

See [Resetting a User's Password](#) on page 60.

## Managing Locked User Accounts

If you are using Forms Authentication, if a user logs into the application with an invalid password, after six incorrect attempts, the user will be locked out of the account.

---

**Note:** If you are using Integrated Windows Authentication, domain user accounts are not locked out.

---

On the *Users* tab, you can add the *Is Locked* column to see which user accounts are locked. The value will display either *True* or *False*.

A locked user account be unlocked in the following ways:

- An administrator can unlock the account
- The account will be unlocked after a configured period of time (see below).

## Changing the Lockout setting

When a user's account is locked, there is a time period where the user is locked out. After the time period, the user can attempt to log into the account again. You can change the Lockout timeout setting and specify how long the timeout session is. You change the Lockout timeout setting by editing a value in the C:\Program Files\AccessData\Common\FTK Business Services\AdgWindowsServiceHost.exe.config file.


### To change the lockout setting

1. Navigate to C:\Program Files\AccessData\Common\FTK Business Services\AdgWindowsServiceHost.exe.config file.
2. Locate the key `<add key="FailedAuthenticationLockoutPeriodInMinutes" value=" " />` .
3. The value is the number of minutes that you want the timeout period to be.
4. Save the file and close.

## Unlocking a User Account

When a user's account is locked, an administrator can unlock the account.

### To unlock a locked account



1. As a User administrator, click Management > Users.
2. Select the user account that is locked.
3. Click the  (unlock) icon.

## Deleting Users

Users can be deleted by an administrator or a user with the right to delete users.

If you try to recreate a deleted user, you receive a warning that the user already exists in the application and was marked as deleted. You can continue to create the user and assign user rights as a new user.

### To delete users


1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. Do one of the following:
  - In the users list, select the user that you want to delete. In the *User Details* pane, click  **Delete**.
  - In the users list, select one or more users that you want to delete. Click  **Delete**.
3. In the **Confirm Deletion** dialog box, click **OK**.

## Deactivating a User

You can deactivate users as needed to make the console unavailable to them. When you deactivate a user, that user remains in the users list of the *Users* tab, and has the status of *False* in the *Active* column. The user's data remains in the database; however, the user cannot log in, and they are not available for any other assignments or work. The user remains inactive until an administrator reactivates them. You can activate or deactivate users individually or collectively.

See [Activating a User](#) on page 62.

### To deactivate a user


1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, check one or more users whose **Active** status is **True**.
3. Click  **Deactivate**.
4. In the *Deactivate user* message box, click **Yes**.

## Activating a User

You can activate users as needed. When a user is activated, they can log in and be available for work. An activated user remains active until an administrator deactivates them. You can activate or deactivate users individually or collectively.

See [Deactivating a User](#) on page 62.

### To activate a user

1. Open the *Users* tab.  
See [Managing the List of Users](#) on page 56.
2. In the user list pane, check one or more users whose *Active* status is *False*.
3. In the bottom of the middle pane, click  .
4. In the *Activate user* frame, click **Yes**.

# Configuring and Managing User Groups


Groups are a set of users grouped together. Groups allow you to put sets of users together who perform the same tasks. Putting users into groups makes it easier to assign and manage project permissions for users.

The project permissions that you assign to users define the tasks that they can perform. Therefore, if you have a group of users who all are going to review documents, you can put them in a group and grant them permissions to review, code, and label documents.

Administrators, and users assigned the Manage Groups permission, can manage groups.

## *Opening the User Groups Tab*

### **To open the User Groups tab**

1. Log in as an administrator or a user with the Manage Groups admin role.  
See [Opening the AccessData Web Console](#) on page 24.
2. Click **Management**.
3. Click **User Groups** .

The users list lets you view all the groups, including the following columns of information about them:

- User Group Name
- Description

From the group list, you can also add, edit, or delete groups. You can associate groups to users and admin roles.

When you create and view the list of groups, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display the items that you want.

## User Groups Tab

The *User Groups* tab on the *Management* page can be used to add, edit, delete, and associate user groups on a global scale. Groups are collections of users who perform the same tasks in the application.


### Elements of the User Groups Tab

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Groups List	Displays all groups. Click the column headers to sort by the column.
Refresh 	Refreshes the Groups List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the Groups List. See <a href="#">Sorting by Columns</a> on page 36.
Export to CSV 	Exports the user group list to a CSV file.
Delete 	Deletes the selected group. Only active when a group is selected. See <a href="#">Deleting Groups</a> on page 65.
Add Groups 	Adds a group. See <a href="#">Adding Groups</a> on page 65.
Edit Groups 	Edits the selected group. See <a href="#">Editing Groups</a> on page 65.
Delete Groups 	Deletes the selected group. See <a href="#">Deleting Groups</a> on page 65.
Users Tab 	Allows you to associate or disassociate users to groups. See <a href="#">Associating Users/Admin Roles to a Group</a> on page 65.
Admin Roles Tab 	Allows you to associate or disassociate admin roles to groups. See <a href="#">Associating Users/Admin Roles to a Group</a> on page 65.
Add Association 	Associates a group to a user or admin role.
Remove Association 	Disassociates a group from a user or admin role.





## Adding Groups

### To add a group

1. Open the *User Groups* tab.  
See [Opening the User Groups Tab](#) on page 63.
2. In the *Groups Details* pane, click  **Add**.
3. In the **User Group Name** field, enter a unique username.  
The name must be between 7 - 32 characters and must contain only alphanumeric characters.
4. Enter a **Description**.
5. Click **OK**.


## Deleting Groups

### To delete a group

1. Open the *User Groups* tab.  
See [Opening the User Groups Tab](#) on page 63.
2. Do one of the following:
  - In the groups list, highlight the group that you want to delete. In the *Groups Details* pane, click  (delete).
  - In the users list, check one or more users that you want to delete. Click  **Delete**.
3. In the *Confirm Deletion* dialog box, click **OK**.

## Editing Groups

### To edit a group


1. Open the *User Groups* tab.  
See [Opening the User Groups Tab](#) on page 63.
2. In the *Groups Details* pane, click  (edit).
3. In the **User Group Name** field, enter a unique username.  
The name must be between 7 - 32 characters and must contain only alphanumeric characters.
4. Enter a **Description**.
5. Click **OK**.

## Associating Users/Admin Roles to a Group

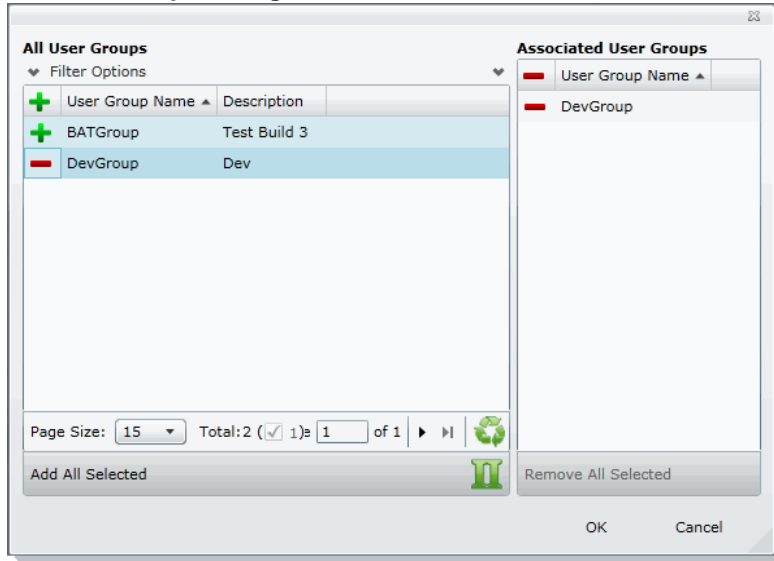
From the *User Groups* tab, you can associate users and admin roles to the selected group.

### To associate users/admin roles to a group

1. Open the *User Groups* tab.  
See [Opening the User Groups Tab](#) on page 63.
2. In the user list pane, select a group to which you want to add an association.

3. In the bottom pane, do one of the following:
  - Select the **Users** tab to associate users to the group.
  - Select the **Admin Roles** tab to associate roles to the group.
4. Click **Add Association** .
5. Click **+** to add users/roles.
6. Click **OK**.

### All User Groups Dialog



7. Click **+** to associate the user to the group.
8. Click **OK**.

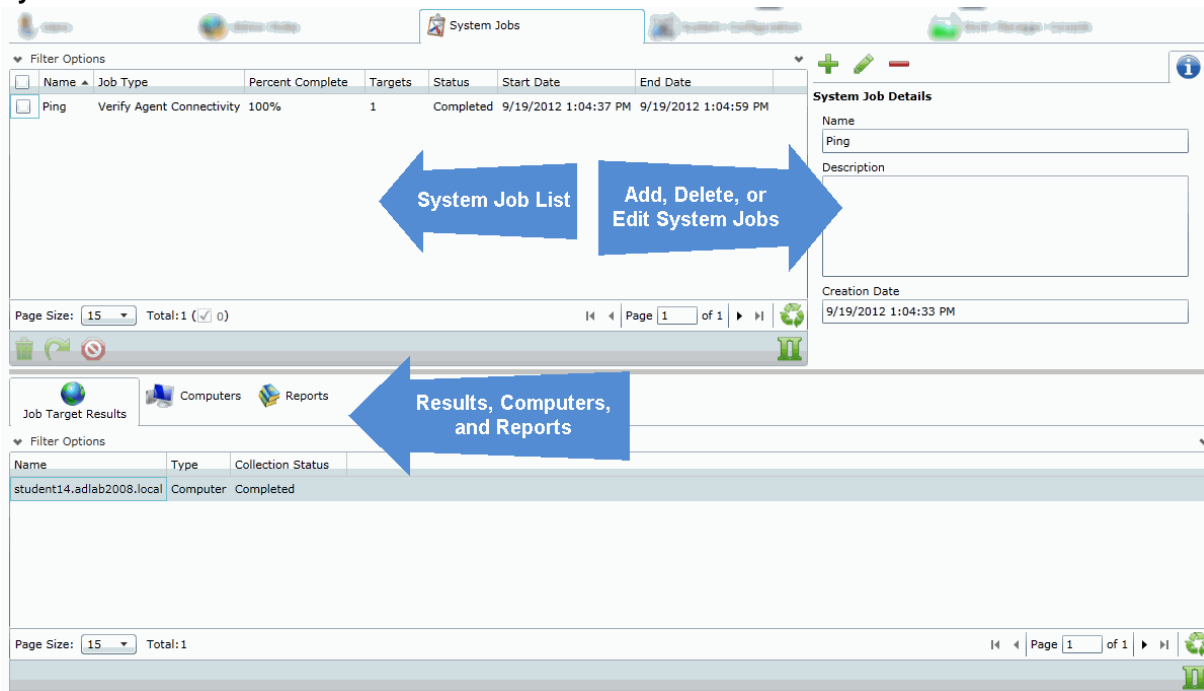
# Chapter 6

## Using System Jobs

### About System Jobs

The System Jobs Tab on the Management page is dedicated to managing System Jobs. System Jobs are primarily used for inventorying agents. As an administrator, you can add system jobs to push the agent to multiple data sources, ping multiple agents to test connectivity, or map nodes to people.









#### System Jobs Tab



#### Elements of the System Jobs Tab

Element	Description
Filter Options	Allows you to filter system jobs in the list. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
System Jobs List	Displays all system jobs. Click the column headers to sort by the column.

## Elements of the System Jobs Tab (Continued)

Element	Description
Refresh 	Refreshes System Jobs List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the System Jobs List. See <a href="#">Sorting by Columns</a> on page 36.
Delete 	Deletes the selected system job. Only active when a system job is selected.
Resubmit Job 	Reruns a job under a new name.
Stop Job 	Stops a current job.
Add System Job 	Adds a system job.
Edit System Job 	Edits the selected system job.
Delete System Job 	Deletes the selected system job(s).
Job Target Results	Lists all of the results for the selected job. You can resubmit a job, stop a job, or cancel ETM policies on a computer(s) in the job.
Status	Lists the failure status of a job in detail.
Associated Computers	Lists the computers associated with the selected job.
Reports	Reports are only available for agent operations. The following report is available: Agent Op Report.

# Adding a System Job



As an administrator, you can add system jobs to push the agent to multiple data sources, ping multiple agents to test connectivity, or map nodes to people.

See [Executing a System Job](#) on page 74.

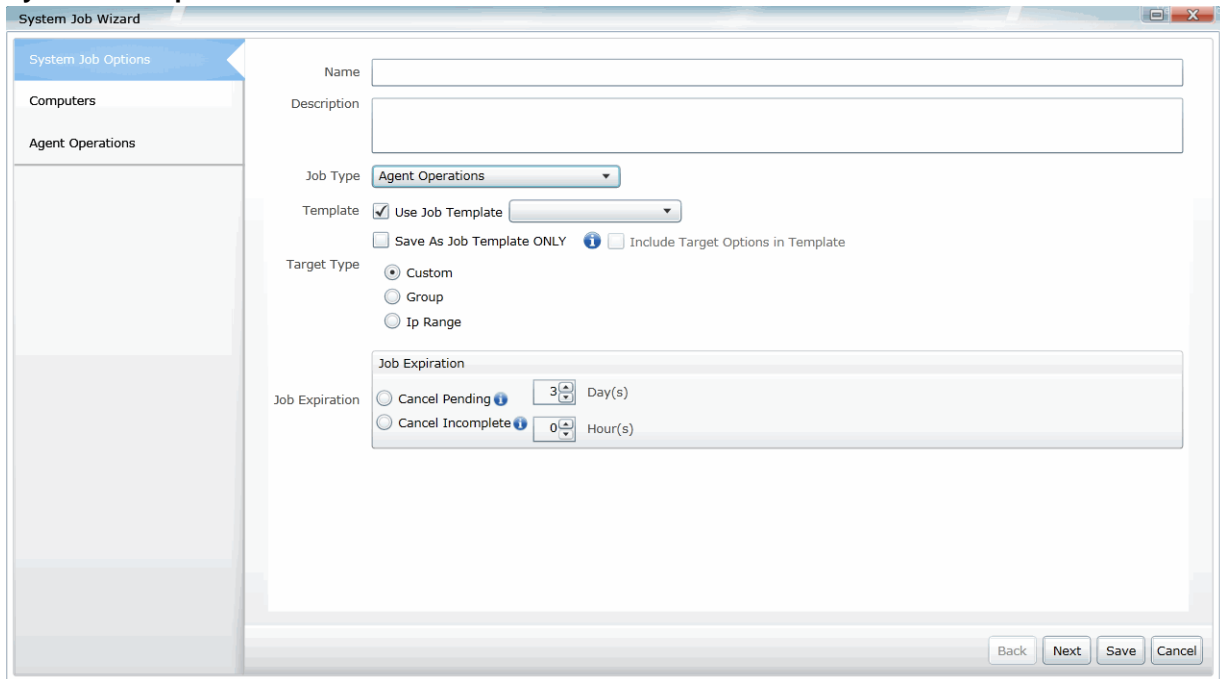
See [Deleting System Jobs](#) on page 75.

See [Configuring Agent Credentials](#) on page 87.

## To add a system job

1. On the menu bar, click **Management**.
2. Click **System Jobs** .
3. In the *System Jobs Details* pane, click .

## System Job Options



4. In the *System Job Options*, set the options that you want.  
See [System Job Options](#) on page 70.
5. Do one or more of the following:

---

**Note:** Depending on the *Target Type* that you set in the *System Job Options*, some of the following panels may not be available.

---

- **Groups** screen, check the groups who will receive the system job.
- **Group Computers** screen, check the computers for the groups who will receive the system job.
- **Computers** screen, check the computers who will receive the system job.
- **IP Range** screen, specify a valid starting IP address and an ending IP address.

6. Click **Save** to submit the job for execution.

## Installing the Agent from a Command Prompt

There are times you will install an agent from a Command Prompt. The following syntax also configures the heartbeat settings. To install from a Command Prompt:

1. Open the Command Prompt.
2. Enter the following syntax, replacing the <> text with the correct paths and IP address:  
`msiexec /i <path to agent msi> cer=<path to public certificate> mama=<IPaddress:site server port>`

Example:

```
msiexec /i c:\agentinstall\agent.msi cer=c:\agentinstall\accessdata_E1.crt
mama=10.10.32.17:54545
```

## System Job Options

The following table describes the options that are found in the *System Job Options* when you add a system job.

See [Configuring Agent Credentials](#) on page 87.

See [Editing a System Job](#) on page 74.

### System Job Options Dialog

### System Job Options

Option	Description
Name	Sets the name of the system job.
Description	Lets you add a description of the system job.

## System Job Options (Continued)

Option	Description
Job Type – Map Node To People	Associates a computer that has the Agent installed on it to people. When you edit a system job, you cannot change the job type.
Job Type – Verify Agent Connectivity	Tests the reachability of the agents in an Active Directory group, an IP range, or on selected computers. Pinging the agent also updates the agent version number in the database. When you edit a system job, you cannot change the job type.
Job Type – Agent Operations	Pushes the agent to Active Directory groups, an IP range, or to selected computers. When you edit a system job, you cannot change the job type.
Template	Allows you to: <ul style="list-style-type: none"> <li>• Create a job from an existing job template. See <a href="#">Default System Job Templates</a> on page 72.</li> <li>• Save the created job as a template to use later. You can choose to save target options in the template.</li> </ul>
Target Type – Custom	Targets the system job to selected computers.
Target Type – Group	Targets the system job to selected Active Directory groups.
Target Type – IpRange	Targets the system job to a specified IPv4 address range.
Job Expiration	Select the days and hours for when unfinished jobs will expire.
Agent Operations dialog	Displays if you select Agent Operations as your job type. See <a href="#">Agent Operations</a> on page 73.
Uninstall	Select to remove the agent from the machine.
Install	Select to push the agent to the machine. Remember that the agent install may cause the machine to restart without a warning. <b>Note:</b> You may need to restart Windows 7 machines before you can perform jobs on that machine.
Make Public Instance	Configure the agent to check a public instance after the agent is installed.
Configure Periodic Check-In	Configure the agent to communicate back to the server.
Dynamic Agent Options	Dynamic Agents use an encrypted file-based storage. Other agents use a traditional protected storage.
Dynamic Agent Option – One Time	Creates the agent as a service that functions until the target machine(s) restarts.
Dynamic Agent Option – Run Time	Hides the One Time agent on the target machine(s).
Dynamic Agent Option – Persistent	Creates the agent as a service that remains on the target machine(s), even after a reboot.
Agent expires after	Configures the time an agent will be active. When the time expires on an agent, the agent removes itself. You can set the time using days, hours, or minutes. <b>Note:</b> If the agent is executing a job during the expiration date/time, the agent will complete the job before removing itself.

## System Job Options (Continued)

Option	Description
Size of Data Store	Set the size of the data on the machine that you can store
Size of Store	The amount of storage allocated to the agents self administration. It is not recommended that you change this setting.
Port Number	Enter the port designated to communicate with the agent.
Service Name	Enter the name that you want the agent to be displayed as.
Executable Name	Enter the name of the file that is being run.

## Default System Job Templates

The following table lists the default System Job templates available.

### Default System Job Templates

Template	Description
Agent Verification	System job that verifies if an agent is on a targeted machine.
Internal Agent with Local Folder Storage	System job targets machines that do not communicate outside of the network.
Internal Agent with Protected Store	System job that installs non-public agent with a hidden data store on selected machines.
Internal Agent with Periodic Check in and Local Storage	System job that installs a non-public agent on selected machines. This agent will also check in periodically via heartbeat.
Internal Agent with Periodic Check in and Protected Store	System job that installs a non-public agent with a hidden store on selected machines. This agent will also check in periodically via heartbeat.
Map Nodes to People	System job identifies the person that has last logged in and associate the node to that person.
Public Agent Install with Local Storage	System job that installs an agent on target machines that may communicate outside of the network.
Public Agent Install with Protected Store	System job that installs an agent on target machines that may communicate outside of the network and has a hidden data store.
Install Temporary Agent	This agent is installed on a temporary basis and will uninstall itself after one day.



# Agent Operations

The *Agent Operations* dialog allows you to configure what the System Agent will do. You can choose to install or uninstall the agent, configure dynamic agent options, and/or configure additional options.



# Executing a System Job

You can execute a system job and view the percent complete in the System Job list pane.

See [Configuring Agent Credentials](#) on page 87.

See [Deleting System Jobs](#) on page 75.

## To execute a system job

1. On the *Management* tab, click **System Jobs** .
2. In the *System Job* list pane, highlight a system job that has not yet started.
3. In the *System Job Details* pane, click **Execute**  to run the job.

## Editing a System Job



You can edit an existing system job only if it has not yet executed. If the job has already executed, you can only view the job's settings, or you can create a new system job with the settings that you want.

When you edit a system job, you can change everything in the job except the job type.

See "About system jobs" on page 113.

See [Configuring Agent Credentials](#) on page 87.

## To edit a system job

1. On the *Management* tab, click **System Jobs** .
2. In the *System Job* list pane, select the system job that you want to edit.
3. In the right side of the upper pane, click .
4. Edit the system job options that you want.  
See [System Job Options](#) on page 70.
5. Do one or more of the following:

---

**Note:** Depending on the *Target Type* that you set in the *System Job Options* panel, some of the following panels may not be available.

---

6. Do one or more of the following:

---

**Note:** Depending on the *Target Type* that you set in the *System Job Options*, some of the following panels may not be available.

---

- **Groups** screen, check the groups who will receive the system job.
  - **Group Computers** screen, check the computers for the groups who will receive the system job.
  - **Computers** screen, check the computers who will receive the system job.
  - **IP Range** screen, specify a valid starting IP address and an ending IP address.
7. Click **Save** to submit the job for execution.




## Deleting System Jobs

You can delete one or more jobs from the **System Jobs** list pane.

See [Configuring Agent Credentials](#) on page 87.

See [Executing a System Job](#) on page 74.

### To delete a system job

1. On the *Management* tab, click **System Jobs** .
2. Do one of the following:
  - In the *System Job* list pane, highlight a system job that you want to delete. In the *System Job Details* pane, click .
  - In the *System Job* list pane, check one or more system jobs that you want to delete. In the lower left corner of the *System Job* list pane, click .
3. Click **OK** to confirm the deletion.

## Viewing and Managing System Job Templates

An application administrator or as a user with the *Manage Job Templates* permission can use a central location on the *Management* page to view, add, edit, and delete system job templates.

See [Managing Templates](#) on page 91.

### To access the Manage System Jobs Templates page

1. Login in as an admin or as a user with the Manage Job Templates permission.
2. Open the *Management* page.
3. Click **System Configuration**.
4. Click **Manage Templates**.
5. Click **System Job Templates**.

# Chapter 7

## Configuring the System

---

This chapter will help administrators configure the system to their preferences.

### About System Configuration





You can configure many settings for the application system. These are global settings that affect the entire system.

### System Configuration Tab - Standard Settings






The *System Configuration* tab on the *Management* page allows you to configure multiple items. This section describes each item.

Depending on the license that you own and the permissions that you have, you will see some or all of the following:

#### Elements of the System Configuration Tab

Element	Description
 <b>Active Directory</b>	Allows you to configure Active Directory to synchronize and import Active Directory users. Synchronization is from Active Directory to the application only. See <a href="#">Configuring Active Directory Synchronization</a> on page 77.
 <b>Email Server</b>	Allows you to configure the Email Notification Server so that you can send notification emails to specified users for certain events. This configuration is also necessary for sending Litigation Hold emails to appropriate recipients. See <a href="#">Configuring the Email Notification Server</a> on page 81.
 <b>Create Notifications</b>	Allows you to configure email notifications for the project and user related events. See <a href="#">Creating Notifications</a> on page 81.
 <b>Manage Certificates</b>	Allows you to manage certificates used for encrypting AD1 files.

## Elements of the System Configuration Tab

Element	Description
 <b>Project Defaults</b>	Allows you to configure the following settings that will be used every time you create a project: <ul style="list-style-type: none"><li>• Default paths for project data</li><li>• Default options for processing evidence in projects</li></ul> See <a href="#">Default Evidence Processing Options</a> on page 84.
 <b>Export Options</b>	Allows you to set the application to include Australian numbering.
 <b>Processing Priority Options</b>	Allows you to configure how much of the available CPU will be used for processing. If not configured, the evidence processing engine will use all available CPUs.
 <b>Notes Certificates</b>	Allows you to manage certificates used for encrypting Lotus Notes files.
 <b>KFF</b>	Allows you to configure KFF. See <a href="#">Using KFF (Known File Filter)</a> on page 207.
<b>Other Advanced Options</b>	Depending on the license that you own and the permissions that you have, you may see other advanced options. See <a href="#">Configuring Advanced System Settings</a> on page 86.

## Configuring Active Directory Synchronization

Depending on your product license, you can sync with Active Directory in order to import some AD objects into your environment.

You can import the following AD objects:

- Summation (Using forms authentication mode):
  - Domain users as People (This is Data Sources *People*, not as application users.)
- eDiscovery (Using forms authentication mode):
  - Domain users as People (This is Data Sources *People*, not as application users.)
  - Computers as Data Sources
  - Groups as Data Sources
  - Shares as Data Sources
- Summation or eDiscovery (IWA mode only):
  - Domain users as application users on the *Users* tab.

When configuring AD sync, you must provide the address of the AD server and credentials for that server.

After performing an initial sync, you can sync on a recurring schedule.

You can also select to import one or more types of objects. For example, you can select to only sync Users on a recurring schedule. This can be helpful to easily add new users only.

When you sync with Active Directory, all objects of that type are imported. Synchronization only occurs from Active Directory to the application. Changes made to the application do not sync back to Active Directory.


You can also configure the system to send an email notification when a value in Active Directory is changed and synced with Summation or eDiscovery. This can be helpful when you have a custodian in a Litigation Hold and the status of that user changes. For example, they may move locations or may no longer be employed. You configure the email notifications as part of the Active Directory sync setting. You can select which Active Directory fields you want to be notified about when changes occur and which application users to send an email to. The notification email contains a time stamp, the name of the user that the change occurred for, the properties that changed, and the old and new values of the changed properties.

---

**Note:** After migrating from an earlier version of the application, you must re-enter the Active Directory password. If not, the Active Directory data does not appear in the application. See [Active Directory Configuration Options](#) on page 80.

---

### To configure Active Directory synchronization

1. Log in as an administrator.  
See [Opening the AccessData Web Console](#) (page 24).
2. Click **Management**.
3. Click  **System Configuration**.
4. If you want to use email notifications, configure the email server.  
See [Configuring the Email Notification Server](#) on page 81.
5. Click **Active Directory**.
6. In the *Active Directory Configuration* dialog, set all options and click **Next**.  
See [Active Directory Configuration Options](#) on page 80.
7. Click **Next**.
8. Select which Active Directory fields to import into User information.  
In the *Active Directory Fields* dialog box, in the *Active Directory Fields* list box, select an alias attribute and click the green arrow next to the user field that you want associated with the attribute.

Bold user field names are required fields.

The following are examples of fields that you can use:

#### Active Directory Fields

Active Directory Field	Person Field
givenname	<i>First Name</i> (Required)
sn	<i>Last Name</i> (Required)
samaccountname	<i>Username</i> (Required)
displayname	Notes Username
mail	Email

9. Click **Next**.
10. To configure Active Directory object change notification, do the following:
  - 10a. In the *Active Directory Fields* list, select a field that you want to be notified about if they change and click the right arrows.
  - 10b. Repeat for all desired fields.
  - 10c. Select the application users that you want to be notified. (Each will receive an email.)  
You can filter on the list of application users.
11. Click **Next**.
12. Do one of the following:
  - To save the settings, but not perform a sync, click **Save**.
  - If you have completed all the settings and are ready to sync, click **Save and Sync**.
13. View the imported user in the *Users* tab.

## Active Directory Configuration Options

### Elements of the Active Directory Configuration Dialog

Element	Description
Server	Enter the server name of a domain controller in the enterprise.
Use Global Catalog	Select to use the global catalog.
Port	Enter the connection port number used by Active Directory. The default port number is 389. If you want to support synch with an entire Active Directory forest, set the port as 3268. Otherwise, the synch only collects information from one domain instead of the entire forest. The default ports for communicating with Active Directory are: LDAP: 389 Secure LDAP(SSL): 636 Global Catalog: 3268 Secure Global Catalog(SSL): 3269
Base DN	Enter the starting point in the Active Directory hierarchy at which the search for users and groups begins. The Base DN (Distinguished Name) describes where to load users and groups. For example, in the following base DN <code>dc=domain,dc=com</code> you would replace <b>domain</b> and <b>com</b> with the appropriate domain name to search for objects such as users, computers, contacts, groups, and file volumes.
User DN	Enter the distinguished name of the user that connects to the directory server. For example <ul style="list-style-type: none"><li>• tjones or &lt;domain&gt;tjones</li></ul>
Password	Enter the password that corresponds to the User DN account. This is the same password used when connecting to the directory server.
Active Directory Authentication	Select to enable authentication against Active Directory on login.
AD Sync Objects	You can select which types of objects to include or not include: Users, Groups, Computers, or Shares. All objects are selected by default. If you want to exclude objects from being synced, de-select those objects. This can be helpful to easily add new users only.
AD Sync Recurrence	Configure a daily recurrence by selecting or entering the time of day to start the sync. If a sync is in progress when the interval occurs, the interval is skipped to allow the current sync to complete.
Test Configuration	Click to test the current configuration to ensure proper communication exists with the Active Directory server.
AD Synchronization	Set to inactive by default.



## Configuring the Email Notification Server

You can configure the Email Notification Server so that when you create a litigation hold, your notification emails are sent successfully.

### To configure an email notification server

1. Click **Management**.
2. Click **System Configuration**.
3. Click **Email Server**.
4. In the *Email Server Configuration* dialog box, set the email options that you want. See [Email Server Configuration Options](#) on page 81.
5. Click **Save**.

## Email Server Configuration Options

### Email Server Configuration Options

Option	Description
SMTP Server Address	Specifies the address of the SMTP mail server (for example, smtpserver.domain.com or server1) on which you have a valid account. You must have an SMTP-compliant email system, such as a POP3 mail server, to receive notification messages from the application.
SMTP Port	Specifies the SMTP port to use. Port 25 is the standard non-SSL SMTP port. However, if a connection is not established with default port 25, contact the email server administrator to get the correct port number.
SMTP SSL?	Allows you configure the use of SSL by the SMTP server. The default SSL port is 465.
Default from Address	Specifies the name of the default email account from which alerts and notifications are sent.
Domain	Specifies the sender's domain.
Username	Specifies the sender's name. The default credentials (Username, Password, Domain) are optional.
Password	Specifies the sender's password.
Confirm Password	Confirms the sender's password that had been entered in the <b>Password</b> field.

## Creating Notifications

### About Event Notifications

You can configure event notifications for when certain system events occur. You select which type of event for which you want a notification and the users to whom the notification is sent.

You can create notifications for the following events:

- Project Created
- Project Deleted

- User Created
- User Deleted

---

**Note:** For eDiscovery, you can also create notifications for job events.

---

## Creating Event Notifications

### To create an email event notification

1. Click **Management**.
2. Click **System Configuration**.
3. Click **Create Notifications**.
4. Click **Select Event Type** and select the event type for which you want a notification.
5. Select the user or users that you want to receive the notification.
6. Click **Create Event Notification**.
7. Click **Close**.

## Viewing and Deleting Job Notifications

You can view and delete either the job notifications that you created or the job notifications to which you are subscribed.

### To view and delete event notifications

1. In the console, click your logged-in name (top-right corner) to open the user actions menu.
2. Click **Manage My Notifications**.  
For information on managing list columns or filtering items in the list, see [Managing Columns in Lists and Grids](#) (page 37).
3. Do one or more of the following:
  - In the *Notifications I Created* group box, under the *Notification Type* column header, select the job notifications that you want to delete.
  - In the *Notification I Belong To* group box, under the *Notification Type* column header, select the job notifications that you want to delete.
4. Click **Delete**.
5. In the *Confirm Deletion* dialog box, click **OK**.

# Configuring Default Project Settings

## About Default Project Settings

You can configure the following settings to use every time you create a project:

- Default paths for project data
- Default options for processing evidence in projects

In most cases, you are not required to configure defaults.

---

**Note:** The exception is if you use LawDrop™, then you must set a default LawDrop folder path.

---

See [Configuring the System for Using LawDrop on page 504](#).

For processing options, there are defaults that are pre-configured.

If no default project paths are configured, the person creating the project provides this information.

If you configure default settings, you can have the application display those settings when a project is created. If you allow the values to display, the user creating the project can view and/or change the values.

You can also hide the default values. If hidden, the person creating the project cannot view the options and/or change them.

See [Setting Default Project Settings on page 83](#).

See [Default Evidence Folder Options on page 84](#).


See [Default Evidence Processing Options on page 84](#).

## Setting Default Project Settings

You can configure default project evidence settings.

See [About Default Project Settings on page 83](#).

### To set default project options

1. Log in as an administrator.  
See [Opening the AccessData Web Console \(page 24\)](#).
2. Click **Management**.
3. Click  **System Configuration**.
4. Click **Project Defaults**.
5. On the *Info* tab, set the default path settings.  
See [Default Evidence Folder Options on page 84](#).
6. On the *Processing Options* tab, set the default evidence processing options.  
See [Default Evidence Processing Options on page 84](#).
7. Click **Save**.

## Default Evidence Folder Options

When you create a project, you must configure the following:

(see [General Project Properties](#) (page 246))


- Project Folder Path
- Job Data Path

On this page, you can define default locations so that you do not have to set them manually each time you create a project. If you configure paths here, when you create a project these default paths are populated. However, they are only defaults and can be changed.

On this page, you can also set the location for the LawDrop DropSpace path.

When setting these paths, be aware of the following:

- Local paths only work on single box installations.
- If a network UNC path is specified, you can validate the path to ensure that the application can access the location. If the path is not validated, you may need to re-enter the path correctly or specify a new path.

To verify the path, click .

### Paths

Project Folder Path	Allows you to specify a local path or a UNC network path to the project folder. This path is the location where most project data is stored.
Job Data Path	Allows you to specify a default job data path. <ul style="list-style-type: none"><li>• When used with Summation, this sets the path used to store some reports.</li><li>• When used with eDiscovery, this sets the responsive folder path for data from jobs. Under this path, a folder is created for each job. The job sub-folders contain job reports and ad1 files for collected files.</li></ul> See <a href="#">Job Options Tab</a> on page 428.
LawDrop DropSpace Path	If you use LawDrop, you must set a default folder path for the DropSpace. This is an application- level setting separate from project settings. See <a href="#">Configuring the System for Using LawDrop</a> on page 504.

## Default Evidence Processing Options

The processing options configured here are the default options used by a project when it is created.

See [About Default Project Settings](#) on page 83.

See [Evidence Processing and Deduplication Options](#) on page 248.

If you configure default settings, you can have the application display those settings when a project is created. If you allow the values to display, the user creating the project can view and/or change the values.

---

**Note:** After upgrading the application, [Enable Standard Viewer Processing Option](#) is turned off by default because it is a slower performing processing option. If you want this functionality, you need to enable it manually in [System Configuration > Project Defaults > Processing Options](#).

---

You can also hide the default values. If hidden, the person creating the project cannot view the options and/or change them.

Hover the mouse over the information icon to get information about each item.

### Default Evidence Processing Options


Option	Description
Hide Processing Options	Allows you to hide the processing options dialog when a user creates a project. This forces the project to use the default values set here. The default is off.
Individual Processing Options.	See <a href="#">Evidence Processing and Deduplication Options</a> on page 248.
Show All Time zones	When selected, allows you to select any time zone recognized by the operating system when adding evidence.

## Configuring Export Options

You can configure *Export Options* to specify the document ID numbering when exporting an export set to a load file.

For more information on production sets, see the *Exporting* documentation.

### To configure export settings

1. Log in as an administrator.  
See [Opening the AccessData Web Console](#) (page 24).
2. Click **Management**.
3. Click  **System Configuration**.
4. Click **Export Options**. The option available is described in the following table.

### Alternative Numbering

Option	Description
Use Australian Numbering Scheme	<p>This option is specific to what options are available when exporting to a load file format.</p> <p>The same underlying technology performs both U.S. and Australian numbering. For example, the Box level in the Australian scheme corresponds to the Volume level in the U.S. scheme, and the Folder level is the same in both schemes.</p> <p>Changes the <b>Volume/Document Options</b> page in Export to include the numbering elements that are needed for Australian document IDs. For example, the U.S. numbering scheme uses volumes and folders in the load file.</p> <p>The Australian numbering scheme uses a party code, boxes, and folders for their volume structure in the load file.</p> <p>See the <i>Exporting</i> documentation for more information on Australian numbering.</p>

5. If you want to change from the default U.S. numbering scheme, select a different option.
6. Click **Save**.

## Chapter 8

# Configuring Advanced System Settings

---

This chapter will help administrators configure the advanced system settings for the application.

These are global settings that affect the entire system.

See [Configuring the System](#) on page 76.





## System Configuration Tab - Advanced Settings

The *System Configuration* tab on the *Management* page allows you to configure multiple items. This section describes the advanced items.




For other options, see [System Configuration Tab - Standard Settings](#) on page 76.

The following options display depending on your license and permissions:

### Elements of the System Configuration Tab

Element	Description
<b>Agent Credentials</b> 	You can define the credentials used by the system to install the Agent on a target computer. See <a href="#">Configuring Agent Credentials</a> on page 87.
<b>Atlas Configuration</b> 	You can configure PSS Atlas to enable the integration of its database with AccessData's collection features. See <a href="#">Configuring PSS Atlas</a> on page 88.
<b>Credant Configuration</b> 	You can configure a Credant site server so that it automatically finds and uses Credant Shield files for Credant encrypted Network shares and computers in an organization. See <a href="#">Configuring Credant Settings</a> on page 90.
<b>EFS Certificates</b> 	You can configure EFS Certificates for decrypting file-system level encryption. See <a href="#">Configuring EFS Certificates</a> on page 88.

## Elements of the System Configuration Tab

Element	Description
 <b>Geolocation</b>	<p>Configures Geolocation location data.</p> <p>See <i>Configuring the Geolocation Requirements</i> in the <i>Reviewer Guide</i>.</p> <p><b>Note:</b> Custom Geolocation IP data that you have previously entered from the Geolocation Configuration block is not retained when upgrading the application from 5.5 to 5.6. You must re-add the custom Geolocation IP data after upgrading the application.ou can download the Reviewer Guide from the Help/Documentation link.</p> <p>See <a href="#">User Actions</a> on page 34.</p> <p><b>Important:</b> You can download the Reviewer Guide from the Help/Documentation link. See <a href="#">User Actions</a> on page 34. Any time you save new data, the KFF Service is automatically restarted. This can affect running KFF jobs.</p>
 <b>Manage Templates</b>	<p>You can manage the following:</p> <ul style="list-style-type: none"><li>• Job Templates</li><li>• Filter Templates</li><li>• System Job Templates</li></ul> <p>See <a href="#">Managing Templates</a> on page 91.</p>
 <b>Person 3rd Party Database Sync</b>	<p>Allows you to connect to an outside database and import business-only fields to be imported to people instead of adding them by hand.</p> <p>See <a href="#">Configuring the Person 3rd Party Database Sync</a> on page 92.</p>
 <b>Redirected Acquisition</b>	<p>You can use <b>Redirected Acquisition</b> to direct the results of a full disk (logical or physical) collection from the subject agent to the configured collection data path, and by-pass the local Work Manager.</p> <p>See <a href="#">Configuring Redirected Acquisition</a> on page 90.</p>
 <b>Share Credentials</b>	<p>You can define the credentials used by the system to access Network shares.</p> <p>See <a href="#">Configuring Share Credentials</a> on page 87.</p>
<b>Other Standard Options</b>	<p>Depending on the license that you own and the permissions that you have, you may see other standard configuration options.</p> <p>See <a href="#">System Configuration Tab - Standard Settings</a> on page 76.</p>

## Configuring Agent Credentials

You can define the credentials used by the system to install the Agent on a target computer.

Enter a **Domain**, **Username**, and **Password** in the provided fields.

## Configuring Share Credentials

You can define the credentials used by the system to access network shares.


Enter a **Domain**, **Username**, and **Password** in the fields provided.

## Configuring EFS Certificates

EFS is a file system driver that provides file system-level encryption in most Microsoft Windows operating systems. Files are transparently encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer. To decrypt the EFS files so that the system can process them, you will need to configure an EFS certificate. You can configure an EFS certificate under the *Management* tab.

### To configure EFS certificates

1. Log in as an administrator.
2. Click **Management**.
3. Click **System Configuration**.
4. Click **EFS Certificates**.
5. On the **EFS Certificates** page, do one of the following:
  - In the **Certificate** field, type the path to a .pfx certificate file.
  - Click **Browse** to locate a .pfx certificate file.
6. In the **Password** field, enter the password that is necessary to access the .pfx file.
7. Click **Save Certificate** to add the certificate to the *Certificate* list box.
8. (Optional) Repeat steps 3-5 to add additional certificates.

In the *Certificates* list box, select a certificate and then click  to delete the certificate.

## Configuring PSS Atlas

PSS Atlas enables global companies to minimize legal risk, comply with diverse legal duties for information, and proactively manage information based on its business value.

You can configure PSS Atlas to enable the integration of its database with AccessData's collection features.

---

**Note:** If you installed the PSS Atlas Integration component during the application's installation, you also need to either install an instance of Oracle ODAC (available for download from Oracle) or, install the PSS Atlas Integration component on the same computer where FTK Business Services is installed (an Oracle client exists in that location).

---

Litigation Holds are created in the company's PSS Atlas database, with people existing in this database. To use the application to do collections on these people, the PSS Atlas configuration must be configured as **Enabled**.

---

**Note:** The PSS Atlas Sync service must already be installed before you can configure PSS Atlas. Typically, the PSS Atlas Sync service is installed during the installation of the application.

---

If you choose to integrate using a manual sync of PSS Atlas, the service will only sync once every 60 minutes, by default. You can reconfigure the sync time in the following configuration file:

`PssAtlas.WindowsService.exe.config`

By default, the configuration file is located in `C:\Program Files\AccessData\eDiscovery\PSS Atlas`. The time configuration is found on the following line:

`synchronizationWaitIntervalInMinutes`



When a PSS Atlas sync takes place, it pulls all people associated with the given project. It also pulls the following person data:

- Name
- Description
- Attorney
- Comments
- Creation Date
- Effective Start date
- Effective End date
- Jurisdiction
- Outside Counsel

The PSS Atlas database tables that the application uses during synchronization are the following:

- REP\_RT\_MATTER\_VW
- rep\_rt\_request\_vw
- rep\_rt\_people\_inscope\_vw
- rep\_rt\_person\_vw
- legalmatterhistory
- rep\_rt\_ach\_execution\_vw
- rep\_rt\_ach\_plan\_vw
- person

#### To configure PSS Atlas

1. Log in as an administrator.
2. Click **Management**.
3. Click **System Configuration**.
4. Click **Atlas Configuration**.
5. In the **PSS Atlas Configuration** dialog, click **Enabled**.
6. In the **Oracle Connection String** field, specify the connection string ID. If the connection string is valid, you should see a list of projects in PSS Atlas.

The connection string contains the information that the provider needs to know to be able to establish a connection to the database or the data file. The connection is done locally on your computer, or on your local Network.

You can use the following format as an example of an Oracle connection string:

```
Data Source=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=MyHost)(PORT=MyPort)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=MyOracleSID)));User Id=myUsername;Password=myPassword;
```

The username and the password must have full read permissions to PSS Atlas.

7. Click **Sync Now**.  
You should see a list of all the projects currently available to the account that was used to log in to the Oracle schema for PSS Atlas.
8. In the Import PSS Matter field, select either List or Manual Entry. If you select Manual Entry, enter the Matter ID in the field.
9. Click **Import PSS Matter**.
10. Click **OK**.

## Configuring Redirected Acquisition

You can use **Redirected Acquisition** to direct the results of a full disk (logical or physical) collection from the subject agent to the configured collection data path, and bypass the local Work Manager. This method prevents using all or too much of the Work Manager disk space and also saves time.

If you intend to use this feature for a full disk collection, you must first complete the redirect acquisition configuration.

### To configure Redirected Acquisition

1. Log in as an administrator.
2. Click **Management**.
3. Click **System Configuration**.
4. Click **Redirected Acquisition**.
5. On the **Redirected Acquisition** page, enter the username, domain, and password.
6. Click **Save**.

## Configuring Credant Settings

You can configure a Credant site server so that it automatically finds and uses Credant Shield files for Credant encrypted network shares and computers in an organization. Credant encrypts user data throughout an organization similar to how EFS functions.

Instead of configuring a Credant site server, you can choose to configure specific Credant-encrypted network shares or computers with Credant Shield files. When you use this method, select **Explicit Asset Configuration** to enable it, and to also view the number of configured shares and computers.

When you select **Disabled**, data is collected from the Credant-encrypted network share or computer, but does not decrypt the data using the associated Shield file

See [Credant Site Server Configuration Options](#) on page 90.

### To configure Credant

1. Log in as an administrator.
2. Click **Management**.
3. Click **System Configuration**.
4. Click **Credant Encryption**.
5. On the **Credant Configuration** page, click the configuration option that you want, and set any associated options.  
See [Credant Site Server Configuration Options](#) on page 90.
6. Click **Save**.

## Credant Site Server Configuration Options

The following table describes the options that are available on the **Credant Configuration** page.

See [Configuring Data Source Credant Options](#) on page 132.

### Credant Site Server Configuration Options

Option	Description
Address	Specifies the IP address of the Credant servers.
Port	Provides the port number that is used for communication to the Credant server. The default is 8081.
Domain	Specifies the domain address of the Credant server.
Username	Specifies the Credant management console user name. This name is often "Superadmin" but may have been changed to something else.
Password	Specifies the user's password for access to the Credant server.
Confirm Password	Specifies the user's password for confirmed password access to the Credant server.
Remove Server	Removes the configuration of the Credant site server in the application.

## Managing Templates

An application administrator or as a user with the *Manage Job Templates* permission can do the following:

- [Managing Job Templates](#) (page 91)
- [Managing Filter Templates](#) (page 92)
- [Managing System Job Templates](#) (page 92)




See [Admin Permissions](#) on page 48.

## Managing Job Templates

You can use the *Job Wizard* to create job templates.

[Using Job Templates and Filter Templates](#) (page 458)

You can do the following to manage job templates:

	View all existing job templates and their descriptions. You can use the filter to restrict the list of jobs. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
	Create a job template using the Job Wizard. See <a href="#">Managing Job Templates and Filter Templates</a> on page 458.
	Edit a job template using the Job Wizard. See <a href="#">Managing Job Templates and Filter Templates</a> on page 458. An updated template will not affect any workflows in place.



Delete a single job template.  
See [Deleting Job Templates](#) on page 459.



Select and then delete a multiple job templates.  
See [Deleting Job Templates](#) on page 459.

## Managing Filter Templates

You can manage filter templates.

See [Managing Job Templates and Filter Templates](#) on page 458.

## Managing System Job Templates

You can manage system job templates.

See [About System Jobs](#) on page 67.

You can do the following to manage system templates:



View all existing system job templates and their descriptions.  
You can use the filter to restrict the list of jobs.  
See [Filtering Content in Lists and Grids](#) on page 39.



Create a job template using the Job Wizard.  
See [Adding a System Job](#) on page 69.



Edit a system job template.  
See [Editing a System Job](#) on page 74.



Delete a single system job templates.  
See [Deleting System Jobs](#) on page 75.



Select and then delete a multiple system job templates.

## Configuring the Person 3rd Party Database Sync



The Person 3rd Party Database Sync allows you to connect to any third-party database that is compatible with ODBC (Open Database Connectivity) and import fields from that database into a custom property that has been added to a person. This allows you to import business-only fields to people instead of adding them by hand. You can use these fields to filter people and viewed wherever custom columns can be viewed (such as the Home page and Project wizard).

Before using this feature, you should consult with AccessData's support and the database administrator or manager for your organization. You will need the following:

- Configuration string to attach to the third-party database. This configuration string to the database must either contain a trusted connection for the eDiscovery servers or credentials stored in the string as plain text. This configuration string must also be a ODBC connection string and not a connection string for a specific database, such as SAP or PeopleSoft. Please see AccessData's support and your database administrator for more information.

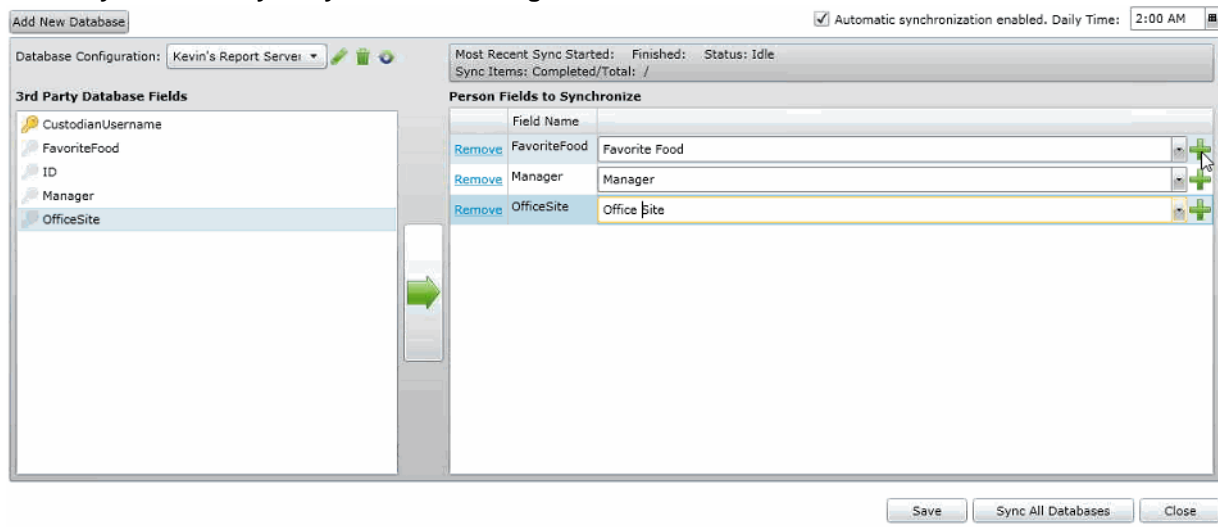
- View Name for the view that you want to attach to. You can attach to either a table or a view in the database. Obtain the name for the view from your database administrator.
- List of people that you want to import from. People need to be created in the system under the *Data Sources* tab that have the same usernames as the usernames of the people in the third-party database. This allows the system to properly sync with the third-party database. See [Adding People](#) on page 116.
- List of custom fields that you want to import from. These custom fields should be created in the *Custom Fields* tab before configuring the 3rd Party database sync. See [Configuring Custom Fields](#) on page 294.

### To add a database to the 3rd party database sync

1. Under the *Management* tab, click **Person 3rd Party Database Sync**.
2. Click **Add New Database**.
3. In the *Sync People with 3rd Party Database* dialog, enter the following information:
  - In the **Config Name** field, enter the name that you want to give the database. This does not have to match the third-party database.
  - In the **Connection String** field, enter the string that you obtained. The string must match exactly, or the databases will not sync.
  - In the **View Name** field, enter the name that you obtained. The view name must match exactly, or the databases will not sync.
4. Click **Connect and Get Fields**.
5. (optional) You can add additional databases as needed.
6. (optional) Click  **Edit** to edit any of the fields in the *Sync People with 3rd Party Database* dialog.
7. (optional) Click  **Delete** to delete the database configuration.






Once the database(s) have been created, you can sync the databases, so that the custom field data from the database that you are connecting to populate custom fields in the system.

### 3rd Party Database Sync Synchronize Dialog



### To synchronize the fields between the two databases

1. If there are multiple databases added to the system, select the database that you want to sync with from the dropdown menu.

2. Click on  key next to the username in the **3rd Party Database Fields** pane in order to select the username. This must be done before proceeding, and a warning appears until you select the username.
3. Select a field that you want to sync with. Click on  to add the field to the **Person Fields to Synchronize** pane. You can add additional fields by selecting the field and clicking .
4. A  next to the field indicates that the custom field was not created in the system. However, if you click **Save**, the custom field will be created in the system. If custom fields were created previously in the system, you can view, select, and edit the custom field options from a dropdown next to the *Custom Field* name.
5. (optional) Remove custom fields from the **Person Fields to Synchronize** pane by clicking **Remove**.
6. (optional) Check **Automatic synchronization enabled** to allow the system to automatically sync with the third-party database. Select the time to sync from the calendar dropdown.
7. If syncing one database, click . To sync all the databases, click **Sync All Databases**. All changes made to the fields will be saved and each database configuration queued up for synchronization.

---

**Note:** Once the sync has been committed, you cannot cancel the process. You can close the window and complete other actions while the synchronization occurs.

---

The status of the synchronization appears in the upper right of the **3rd Party Database Sync Synchronization** dialog. This status does not refresh automatically. However, you can check on the progress of the synchronization after the dialog has been closed by selecting **Management > Person 3rd Party Database Sync**.

After the database(s) have been synchronized, you can view the data from the third-party database under the *Data Source* tab. You must first refresh the information in the tab before the data appears.

## Chapter 9

# Using the Work Manager Console and Logs

---


## Using the Work Manager Console

From **Work Manager Console**, the Administrator can monitor the performance of the **Distribution Server** and the **Work Managers**. Click any work manager node by name to view specific server details.

As an administrator, you can use the *Work Manager Console* to view pending, active, or completed work orders. You can also view the performance of the entire system or specific Work Managers.

### *Opening the Work Manager Console*

#### To open the Work Manager Console page

1. Log in as an administrator.  
See [Opening the AccessData Web Console](#) (page 24).
2. Click **Management**.
3. Click  **Work Manager Console**.

## Work Manager Console Tab

The *Work Manager Console* tab, on the *Management* page, allows administrators to monitor the performance of the *Distribution Server* and the *Work Managers*. Click on any work manager node by name to view specific server details.

As an administrator, you can use the *System Administration Console* to view pending, active, or completed work orders. You can also view the performance of the entire system or specific Work Managers.

#### Elements of the Work Manager Console Tab

Element	Description
Overall System Status Pane	Allows you to view the performance of the entire system or specific Work Managers.
Queued Work Orders	Displays work orders waiting to execute.

## Elements of the Work Manager Console Tab

Element	Description
Active Work Orders	Displays active work orders.
Completed Work Orders	Displays completed work orders.
Overall System Performance	Displays overall system performance. You can access the <i>Overall System Performance</i> panel by expanding the <i>Performance</i> pane on the right side of the page. On the <i>Overall System Performance</i> panel, the displayed time range indicates the time frame in which the status information was collected.

See [Validating Activate Work Orders](#) on page 97.

See [Viewing the System Log or Activity Log](#) on page 101.

See [Configuring a Work Manager](#) on page 98.



# Validating Activate Work Orders

**Validate Active Work Orders** allows you to remove orphaned work orders from the Active Work Orders table. Work orders can become orphaned when the work manager handling the work order shuts down his/her computer or in some other way loses contact with the Distribution server. When this happens, however, it does not change the status of the associated job in the Jobs list.


## To validate active work orders

1. In the *Work Manager Console*, click a work manager name to view active work orders.
2. At the bottom of the left pane, click **Validate Active Work Orders** to confirm and update current work orders and their status.

# Configuring a Work Manager

You can configure a selected Work Manager by setting various property values.

## To configure a Work Manager

1. Open the *Work Manager Console*.  
See [Opening the Work Manager Console](#) (page 95).
2. In the left pane of the *Work Manager Console*, under *Overall System Status*, click a work manager name.
3. In the right pane, click the **Configuration** tab.
4. In the *Configuration* pane, click  **Edit**.
5. When completed, click **OK**.

# Using the System Log and Activity Log

## About the System Log

When certain internal events occur in the system, it is recorded in the System Log. This can be used in conjunction with the activity log to monitor the work and status of your system.

The following are examples of the types of events that are recorded:

- Completion of evidence processing for an individual project
- Exports started and finished
- Starting of internal services
- Job failures
- System errors
- Errors accessing computers and shares



You can filter the log information that is displayed based on the following different types of criteria:

- Date and time of the log message
- Log type such as an error, information, or warning
- Log message contents
- Which component caused the log entry
- Which method caused the log entry
- Username
- Computer name

## System Log Tab

The *System Log* tab on the *Management* page is only accessible to the administrator. This log maintains an historical record of the events that take place in the application. The administrator can view, clear, and export the log file.

### Elements of the System Log Tab

Element	Description
Filter Options	Allows you to filter the items in the System Log. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
System Log	Displays all the events. Click the column headers to sort by the column.
Clear Log 	Deletes all the events in the log. See <a href="#">Clearing the Log</a> on page 101.
Export Log 	Exports the log. It is recommended that you export and save logs before you clear them. See <a href="#">Exporting the Log</a> on page 101.

## About the Activity Log

When certain internal activities occur in the system, it is recorded in the Activity log. This can be used in conjunction with the System Log to monitor the work and status of your system.

See [About the System Log](#) on page 99.

The following are examples of the types of activities that are recorded:

- A user logged out
- A user is forced to log out due to inactivity
- Processing started on the project
- A project is opened

You can filter the log information that is displayed based on the following different types of criteria:

- Category
- Activity Date
- Activity
- Username





## Activity Log Tab

The *Activity Log* tab on the *Management* page can only be accessed by the administrator. The *Activity Log* can help you detect and investigate attempted and successful unauthorized activity in the application and to troubleshoot problems.

The *Activity Log* event columns include the activity date, username, activity, and category.

Only an administrator can view, clear, and export the *Activity Log* file.

### Elements of the Activity Log Tab

Element	Description
Filter Options	Allows you to filter the items in the activity log. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Activity Log	Displays all the events. Click the column headers to sort by the column.
Clear Log 	Deletes all the events in the log.
Export Log 	Exports the log. It is recommended that you export and save logs before you clear them.
Refresh 	Refreshes activity log. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the activity log. See <a href="#">Sorting by Columns</a> on page 36.




## Viewing the System Log or Activity Log

An administrator can view, clear, and export the log file.

Event lists are displayed in a grid. You can modify the contents of the grid as follows:

- You can control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.

### To open the Log page

1. Log in as an administrator.
2. Click **Management**.
3. Click  **System Log** or  **Activity Log**.
4. To refresh the log view, click  (refresh).

## Clearing the Log

As an Administrator, you can clear the log. When you clear the log, you delete all log entries across all pages. A new entry is created stating that the log was cleared and who cleared it. Before clearing the log, consider exporting the log file to keep a historical record.

### To clear the log

1. Open the *Logs* page.
2. In the bottom left corner, click **Clear Log**.
3. Click **Yes** to confirm the deletion.

## Exporting the Log

Exporting the log lets you maintain a historical record of events in the software and saves a copy of the log for future use, even after the log is cleared. Only an administrator can view, clear, and export the log file. You can export the log to a CSV file to allow others, who may not have view log access, the ability to query and access the saved events.

### To export the log

1. Open the *Logs* page.  
See [Activity Log Tab](#) (page 100).
2. In the bottom left corner of the **View Log** pane, click **Export Log**.
3. In the **Save As** dialog box, specify a file name and file location.
4. Click **Save**.

## Chapter 10

# Using the Site Server Console

---

Using the Site Server Console, you can monitor your Site Servers, monitor jobs on the Site Servers, get statuses of various Site Servers, set the bandwidth throttling on Agent or Site Server from Network Traffic Controls and set Phone Home Setting for your Site Servers.

## Monitoring Site Servers

You can view statistics about your Site Servers using the Status tab of the Site Server Console.

### To view the status of a Site Server

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.

## Site Server Status Tab

The screenshot displays the Site Server Console interface. At the top, there are navigation tabs: Users, System Jobs, System Configuration, Work Manager Console, Site Server Console (selected), System Log, Security Log, Library, and Group Templates. Below the navigation is a 'Site Servers' section with a filter input field containing 'Enter site server'. A list of site servers is shown, with 'QA-CIRT-VM5' selected. To the right of the list, the 'Status' tab is active, displaying detailed statistics for the selected server. A blue arrow labeled 'List of Site Servers' points to the list, and another blue arrow labeled 'Statistics for the Selected Site Server' points to the status details.

**Site Servers**

Filter: Enter site server

QA-CIRT-VM5

**Status** | Network Traffic Control | Jobs | Phone Home Settings | Agent Installers

**Name:** QA-CIRT-VM5  
**Site Server Type:** Root  
**Site Server Status:** Online  
**Domain:** 0.0.0.0/1  
**Machine CPU Usage:** 0 B  
**Process CPU Usage:** 0 B  
**Version:** 1, 2, 0, 18  
**Page Memory:** 31.4818 GB  
**Page Memory Available:** 25.7047 GB  
**Physical Memory:** 15.7418 GB  
**Physical Memory Available:** 11.6054 GB  
**Virtual Memory:** 8 TB  
**Virtual Memory Available:** 7.9994 TB  
**Agent Throttle Inbound:** 0 KB  
**Agent Throttle Outbound:** 0 KB  
**Site Server Throttle Inbound:** 0 KB  
**Site Server Throttle Outbound:** 0 KB

**Drives:**

Drive Letter: C:\Total Size: 931.5107 GBFreeSpace: 864.1703 GB  
Drive Letter: D:\Total Size: 566.873 GBFreeSpace: 440.7107 GB  
Drive Letter: E:\Total Size: 1.1642 TBFreeSpace: 511.7367 GB  
Drive Letter: F:\Total Size: 29.2959 GBFreeSpace: 16.3633 GB  
Drive Letter: G:\Total Size: 3.6334 GBFreeSpace: 0 B

**Thread Pool Stat:**

Name: Outgoing ThreadsMax Threads: 50 BQueued: 0 BRunning: 1 B  
Name: Incoming ThreadsMax Threads: 50 BQueued: 0 BRunning: 1 B  
Name: Command ThreadsMax Threads: 50 BQueued: 0 BRunning: 1 B

**Interfaces:**

Host: QA-CIRT-VM5.adlab.local( 10.10.32.25 )Port: 54545

**Replication Stat:**

**Has Parent:** False

Refresh

4. Select a Site Server from the list.
5. To refresh the list, click Refresh.
6. Click the **Status** tab.  
Statistics for the selected Site Server are displayed.

## Restarting the Site Server Service

You can now restart the site server service from the *Site Server Console* page.

### To restart the service

- ❖ On the *Site Server Console* tab, click **Restart Service**.

# Setting Network Traffic Control

You can set the inbound and outbound data maximums for information passed between the Site Server and the agent.

## To set network traffic control maximums

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.
4. Click the **Network Traffic Control** tab.

## Site Server Console Network Traffic Control Tab

The screenshot shows the 'Network Traffic Control' tab in the Site Server Console. It features a navigation bar with tabs for 'Status', 'Network Traffic Control', 'Jobs', 'Phone Home Settings', and 'Agent Installers'. Below the navigation bar, there are six configuration items, each with a slider and a numeric input field:

- Site Server to Agent Inbound Max: Slider at 0, input field 0 KB
- Site Server to Agent Outbound Max: Slider at 0, input field 0 KB
- Site Server to Site Server Inbound Max: Slider at 0, input field 0 KB
- Site Server to Site Server Outbound Max: Slider at 0, input field 0 KB
- Maximum Incoming Threads: Slider at 50, input field 50
- Maximum Outgoing Threads: Slider at 50, input field 50

At the bottom center of the configuration area is a 'Save' button.

5. Move the slider bars to set the maximums of inbound and outbound data.



# Managing Jobs on the Site Server

## Monitoring Jobs on the Site Server

You can monitor the status of jobs and tasks on the Site Server using the *Jobs* tab in the Site Server console. From the *Jobs* tab, you can cancel jobs or tasks, and delete jobs.

### To view the jobs on the Site Server

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.

### Site Server Console Jobs Tab

The screenshot shows the Site Server Console interface with the **Jobs** tab selected. The interface includes a navigation bar at the top with tabs for Status, Network Traffic Control, Jobs, Phone Home Settings, and Agent Installers. Below the navigation bar, there are three main sections:

- Jobs:** A table with columns: Description, Operation, State, StartDate, SubmittedDate, Expires. A blue arrow points to this table with the text "List of Jobs on the Site Server". Below the table are "Delete" and "Cancel" buttons.
- Tasks:** A table with columns: Connection, State, Submitted Date, StartDate, EndDate, Target ID, Task ID. A blue arrow points to this table with the text "List of Tasks in the Job". Below the table is a "Cancel" button.
- Task Details:** A table with columns: Hash, Filename, Path. A blue arrow points to this table with the text "List of Files Received in each Task".

4. Select a Site Server from the list.
5. Click the **Jobs** tab.

## Deleting Jobs on Site Server

You can delete jobs on the Site Server from the Site Server Console. Deleted jobs will be reflected on the *Home* page in the application.

### To delete jobs on the Site Server

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.
4. Select a Site Server from the list.
5. Click the **Jobs** tab.
6. Select the job that you want to delete in the Jobs pane.
7. Click the **Delete** button.

## Canceling Jobs on Site Server

You can cancel jobs on the Site Server from the Site Server Console. Canceled jobs will be reflected on the *Home* page in the application.

### To cancel jobs on the Site Server

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.
4. Select a Site Server from the list.
5. Click the **Jobs** tab.
6. Select the job that you want to cancel in the Jobs pane.
7. Click the **Cancel** button.

## Canceling Job Tasks on Site Server

You can cancel single tasks within jobs on the Site Server from the Site Server Console.

To cancel tasks within jobs on the Site Server

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.
4. Select a Site Server from the list.
5. Click the **Jobs** tab.
6. Select the job that contains the task in the Jobs pane.
7. Select the task that you want to cancel.
8. Click the **Cancel** button.

## Viewing the Site Server that is Performing Tasks

You can see the specific site server that is performing tasks.

On the *Jobs* tab, in the *Tasks* list, there is a column named *Site Server*. View this column to see the name of the Site Server that is performing the task.

## Configuring Phone Home Settings

You can configure the phone home settings of the Site Server to have agents check in at specified intervals.

### To configure the phone home settings

1. Log in to the application as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.
4. Select a Site Server from the list.
5. Click the **Phone Home Settings** tab.

### Site Server Console Phone Home Settings Tab

The screenshot shows the 'Phone Home Settings' tab in the Site Server Console. It features a navigation bar with tabs for 'Status', 'Network Traffic Control', 'Jobs', 'Phone Home Settings', and 'Agent Installers'. The 'Phone Home Settings' tab is active. Below the navigation bar, there are three settings: 'Connect Every' with a slider and a dropdown menu set to '30 Minute(s)'; 'Retry' with a slider and a dropdown menu set to '3 Time(s)'; and 'Wait' with a slider and a dropdown menu set to '30 Second(s) between retries'. There is also a checked checkbox for 'Refresh Metrics on Startup' and two buttons: 'Save' and 'Discard Changes'.

6. Set how often you want the agent to connect by setting the *Connect Every Minute(s)*.
7. Set how many times you want the agent to try to connect, if it is unable to connect, by setting the *Retry Time(s)*.
8. Set how many seconds between retries that you want the agent to wait before trying to connect again by setting the *Wait Second(s) between retries*.
9. Check **Refresh Metrics on Startup** to have the Phone Home Settings refresh on the agent when it starts up.
10. Click **Save**.

## Replacing Windows Agent Installers

### To replace the agent installers

1. Log in as a user with Administrative permissions.
2. Click the **Management** tab.
3. Click the **Site Server Console** tab.

4. Click the **Agent Installers** tab.

### Site Server Console Agent Installers Tab

Status Network Traffic Control Jobs Phone Home Settings Agent Installers

Agent Installer Location:  Browse

Agent Path:  ⓘ

Replicate Agent File

5. In the *Agent Installer Location*, browse to the new MSI you wish to upload.
6. In the *Agent Field* path, enter the location and name where you'd like to put the new installer, within the "Agent" folder in the Site Server Results Directory:  
To replace the 32-bit installer, enter \x32\AccessData Agent.msi  
To replace the 64-bit installer, enter \x64\AccessData Agent (64-bit).msi  
Note: You may want to backup any existing Agent installers before replacing them.
7. Click **Replicate Agent File**.

## Viewing Site Server Health Metrics

You can use the *Health Metrics* tab to view the following site server values:

- CPU %
- Memory Usage
- Memory Available
- Page Memory
- Page Memory Available
- Total Disk Space Usage
- Total Disk Space Usage Availability
- Status (such as online)
- Type of Site Server (such as Root)
- Domain
- Locality
- Version
- Virtual Memory
- Virtual Memory Available

## Part 3

# Configuring Data Sources

This part describes how to configure data sources and includes the following chapters:

- [About Data Sources](#) (page 110)
- [Managing People, Groups, Computers and Network Shares](#) (page 112)
- [Configuring Third-Party Data Repositories as Data Sources](#) (page 145)

# Chapter 11

## About Data Sources

---

Data Sources are sources of data relevant to a project during electronic discovery or security investigation. The data can include electronically stored information on employees, system management computers, and can refer to people, Network shares, Domino or Exchange email accounts, or other public repositories associated with the person.

Once the application has been configured to collect from a data source, you can execute a job to gather the data. After the job has executed, you can examine the data in Project Review and filter the evidence. You can define the scope of the data by data sources in the Navigation panel in Project Review.

You can add, define, delete, and edit data sources from the Data Sources page. You can also manage Network shares, jobs, groups, and computers and their association with a data source.

### To manage Data Sources



You can manage the following types of data sources:

Data Source Type	Link for more information
Groups	See <a href="#">Managing Groups for Collecting Data</a> on page 133.
People	See <a href="#">Managing People (Custodians) as Data Sources</a> on page 112.
Evidence	See <a href="#">Managing Evidence for Collecting Data</a> on page 143.
Computers	See <a href="#">Managing Computers for Collecting Data</a> on page 124.
Network Shares	See <a href="#">Managing Network Shares for Collecting Data</a> on page 129.
Network Collectors	See <a href="#">Configuring Network Collectors</a> on page 142.

3rd Party Data Source Type	Link for more information
Domino	See <a href="#">Configuring for a Domino Server</a> on page 146.
Exchange	See <a href="#">Configuring for an Exchange Online/365 Server</a> on page 147. See <a href="#">Configuring for Exchange 2003, 2007, and 2010 Servers</a> on page 148. See <a href="#">Configuring for Exchange 2010 SP1 and 2013 Servers</a> on page 150.
Enterprise Vault	See <a href="#">Configuring for an Enterprise Vault Server</a> on page 152.
Oracle URM	See <a href="#">Configuring for a Documentum Server</a> on page 158.
Documentum	See <a href="#">Configuring for a Documentum Server</a> on page 158.
SharePoint	See <a href="#">Configuring for a SharePoint Server</a> on page 160.
Websites	See <a href="#">Configuring for Web Sites</a> on page 163.
DocuShare	See <a href="#">Configuring for a DocuShare Server</a> on page 165.
Cloud Mail	See <a href="#">Configuring for Cloud Mail</a> on page 167.
OpenText ECM	See <a href="#">Configuring for a OpenText ECM Server</a> on page 169.
Gmail	See <a href="#">Configuring for Gmail</a> on page 170.
Google Drive	See <a href="#">Configuring for Google Drive</a> on page 171.
Druva	See <a href="#">Configuring for Druva</a> on page 172.
CMIS Repository	See <a href="#">Configuring for a CMIS Repository</a> on page 174.

## Chapter 12

# Managing People, Groups, Computers and Network Shares

---

This chapter describes how to configure settings for collecting data from people (custodians), computers, and Network shares and include the following topics:

- [Managing People \(Custodians\) as Data Sources](#) (page 112)
- [Managing Computers for Collecting Data](#) (page 124)
- [Managing Network Shares for Collecting Data](#) (page 129)
- [Configuring Data Source Credant Options](#) (page 132)
- [Managing Groups for Collecting Data](#) (page 133)
- [Configuring Network Collectors](#) (page 142)
- [Managing Evidence for Collecting Data](#) (page 143)

## Managing People (Custodians) as Data Sources

### *About People (Custodians)*

The term “person” or “custodian” references any identified user who may have data relevant to a project under consideration during electronic discovery. This can include electronically stored information (ESI) on employee or management computers, and can refer to computers, shares, email, or other public repositories associated with the user.

In Review, you can do the following:

- Use the *DataSource* column to see the person that is associated with each item. You can sort, filter, and search using the *DataSource* column.
- Use the General > *Custodians* facet to filter on the person that is associated with evidence items.

### *About the People Page*

You manage people from the *People* tab on the *Data Sources* page. The people are listed in the *People* List. The main view of the *People* List includes the following sortable columns:



## People Information Options

Option	Description
First Name	The first name of the person. This field is required.
Middle Initial	The middle initial of the person.
Last Name	The last name of the person. This field is required.
Username	The computer username of the person. This field is required.
Domain	The network domain to which the person belongs.
Notes Username	The username of the person as it appears in their Lotus Notes Directory. A Lotus Notes username is typically formatted as Firstname Lastname/Organization as in the following example: Pat Ng/ICM

When you create and view the list of people, this list is displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- Sort the columns
- Define a column on which you can sort.
- If you have a large list, you can apply a filter to display only the items you want.

See [Managing Columns in Lists and Grids](#) on page 37.

Highlighting a person in the list populates the *Custodian (Person) Details* info pane on the right side. The info pane has information relative to the currently selected person, beginning with the first name.











At the bottom of the page, you can use the following tabs to view and manage the items that the highlighted person is associated with:

- Computers
- Network shares
- Evidence
- Vault Archives
- Lit Holds
- Jobs
- Job results
- Groups
- Projects
- Cloud Mail







## People Tab Options

The following table lists the various options that are available under the *People* tab.




### Person Tab Options

Element	Description
Filter Options	Allows you to filter the person list. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Add 	Click to add a person. See <a href="#">Adding People</a> on page 116.
Edit 	Click to edit a person. See <a href="#">Editing a Person</a> on page 117.
Delete 	Click to remove a person. See <a href="#">Removing a Person</a> on page 117.
Refresh 	Click to refresh the person list.
Delete 	Click to remove multiple people. See <a href="#">Removing a Person</a> on page 117.
Import People 	Click to import people from a CSV file. See <a href="#">Importing Custodians From a CSV File</a> on page 117.
Custom Properties 	Click to add custom properties. Custom properties must be defined before importing CSV files with custom fields in the headers. See <a href="#">Adding Custom Properties</a> on page 238.
Export to CSV 	Export the current set of data to a CSV file.
Columns 	Click to adjust what columns display in the Person List. See <a href="#">Managing Columns in Lists and Grids</a> on page 37.
Computers 	<p>Allows you to view computers that have been associated to a person. In the <i>Computer</i> pane, you can do the following:</p> <ul style="list-style-type: none"><li>• Filter the <i>Computers</i> list.</li><li>• Add a computer. See <a href="#">Adding a Computer</a> on page 125.</li><li>• Edit a computer. See <a href="#">Editing a Computer</a> on page 126.</li><li>• Associate and disassociate a computer to a person. See <a href="#">Associating Computers to a Person</a> on page 120.</li><li>• Export the <i>Computer</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Computers</i> list.</li></ul> <p><b>Note:</b> You cannot delete a computer that has been added in this pane. To delete a computer, see the <i>Computers</i> tab under <i>Data Sources</i>. See <a href="#">Deleting a Computer</a> on page 126.</p>

## Person Tab Options

Element	Description
Network Shares 	<p>Allows you to view network shares that have been associated to a person. In the <i>Network Shares</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the <i>Network Shares</i> list.</li> <li>● Add a network share. See <a href="#">Adding a Network Share</a> on page 130.</li> <li>● Edit a network share. See <a href="#">Editing a Network Share Path</a> on page 131.</li> <li>● Associate and disassociate a network share to a person. See <a href="#">Associating Network Shares to a Person</a> on page 120.</li> <li>● Export the <i>Network Share</i> list to a CSV file.</li> <li>● Adjust the columns' display in the <i>Network Share</i> list.</li> </ul>
Evidence 	<p>Allows you to view evidence that has been associated to a person. In the <i>Evidence</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the Evidence list.</li> <li>● Add Custom Properties. See <a href="#">Adding Custom Properties</a> on page 238.</li> <li>● Export the <i>Evidence</i> list to a CSV file.</li> <li>● Adjust the columns' display in the <i>Evidence</i> list.</li> <li>● See <a href="#">Managing Evidence for Collecting Data</a> on page 143.</li> </ul>
Vault Archives 	<p>Allows you to view the Enterprise Vault archives that has been associated to a person. In the <i>Vault Archives</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the <i>Vault Archives</i> list.</li> <li>● Add a Vault archive. See <a href="#">Adding an Enterprise Vault Archive to a Person</a> on page 120.</li> <li>● Edit a Vault archive. See <a href="#">Editing an Enterprise Vault Archive Added to a Person</a> on page 121.</li> <li>● Delete a Vault archive. See <a href="#">Removing an Enterprise Vault Archive Added to a Person</a> on page 121.</li> <li>● Add Custom Properties. See <a href="#">Adding Custom Properties</a> on page 238.</li> <li>● Export the <i>Vault Archives</i> list to a CSV file.</li> </ul> <p>Adjust the columns' display in the <i>Vault Archives</i> list.</p>
Lit Holds 	<p>Allows you to view Lit Holds that have been associated to a person. In the <i>Lit Hold</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the <i>Lit Holds</i> list.</li> <li>● Export the <i>Lit Holds</i> list to a CSV file.</li> <li>● Adjust the columns' display in the <i>Lit Hold</i> list.</li> </ul>
Jobs 	<p>Allows you to view jobs that has been assigned to a person. In the <i>Jobs</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the <i>Jobs</i> list.</li> <li>● Export the <i>Jobs</i> list to a CSV file.</li> <li>● Adjust the columns' display in the <i>Jobs</i> list.</li> </ul>
Job Results 	<p>Allows you to view job results from a job that has been assigned to a person. In the <i>Job Results</i> pane, you can do the following:</p> <ul style="list-style-type: none"> <li>● Filter the <i>Job Results</i> list.</li> <li>● Export the <i>Job Results</i> list to a CSV file.</li> <li>● Adjust the columns' display in the <i>Job Results</i> list.</li> </ul>

## Person Tab Options

Element	Description
Groups 	Allows you to view groups that a person belongs to. In the <i>Groups</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Groups</i> list.</li><li>• Export the <i>Groups</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Groups</i> list.</li></ul>
Projects 	Allows you to view a project that a person belongs to. In the <i>Projects</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Projects</i> list.</li><li>• Associate and disassociate a project to a person. See <a href="#">Associating a Project to a Person</a> on page 121.</li><li>• Export the <i>Groups</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Groups</i> list.</li></ul>
Cloud Mail 	Allows you to add people to a cloud mail server. In the <i>Cloud Mail</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Cloud Mail</i> list.</li><li>• Add a person to a cloud mail server. See <a href="#">Adding a Cloud Mail Server to a Person</a> on page 122.</li><li>• Edit the person added to a cloud mail server. See <a href="#">Editing a Cloud Mail Server</a> on page 122.</li><li>• Delete the person added to a cloud mail server. See <a href="#">Removing a Cloud Mail Server</a> on page 122.</li><li>• Export the <i>Cloud Mail</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Cloud Mail</i> list.</li></ul>

## Adding People


Administrators, and users with permissions, can add people.

You can add people in the following ways:

- Manually adding people
- Importing people from a file  
See [Importing Custodians From a CSV File](#) on page 117.
- Creating or importing people while importing evidence  
See [Managing Evidence for Collecting Data](#) on page 143.
- Importing people from Active Directory.  
See [Adding People Using Active Directory](#) on page 118.

## Manually Creating People


### To manually create a person

1. On the **Home > Data Sources > People** tab, click  **Add**.
2. In *Person Details*, enter the person details.
3. Click **OK**.

## Editing a Person

You can edit any person that you have added to the project.



### To edit a project-level person

1. On the **Home > Data Sources > People** tab, select a person that you want to edit.
2. Click  **Edit**
3. In *Person Details*, edit person details.
4. Click **OK**.

## Removing a Person

You can remove one or more people from a project.

### To remove one or more people from a project


1. On the **Home > Data Sources > People** tab, select the check box for the people that you want to remove.
2. If you want to remove one person, check the person that you want to remove, and select  **Delete**.
3. If you want to remove more than one person, check the people that you want to remove, and select  **Delete**.
4. To confirm the deletion, click **OK**.

## Importing Custodians From a CSV File

From the *People* tab, you can import a list of people into the system from a CSV file. Before importing people from a CSV file, you need to be aware of the following items:

- You must define any custom columns before importing the CSV file. See [Adding Custom Properties](#) on page 238.
- Make sure that your columns have headers.
- Multiple items in columns must be separated by semicolons.

## To import people from a CSV file

1. On the **Home > People** tab, click  **Import Custodians**.
2. From the *Import Custodians from CSV* dialog, choose from the following options:
  - **Import custom columns**. This option is not available if custom columns have not been previously defined.
  - **Merge into existing people**. This option will overwrite fields, such as first name, last name, and email address. It also adds new computers, network shares, etc. to existing associations.

---

**Note:** For an entry to be considered a duplicate in the External Evidence column, the network path, assigned person, and type (such as image or native file) must be the same. If there are any differences between these three fields, the entry is brought in as a new External Evidence item.

---

- **Download Sample CSV**. This allows you to download a sample CSV file illustrating how your CSV file should be created. This example is dynamic; if you have created custom columns for people, those custom columns appear in the sample CSV file.

---

**Note:** If your license does not support certain features (such as network shares or computers), the columns for those items appear in the CSV without any data populated in the columns.

---

3. Once options have been selected, click **OK**.
4. Browse to the CSV file that you want to upload.
5. After file has been uploaded, a *People Import Summary* dialog appears. This displays the number of people added, merged, and/or failed, with details if an import failed. Click **OK**.

## Adding People Using Active Directory

You can add people by importing from Active Directory.

If you have not already done so, be sure that you have configured Active Directory in the application. When Active Directory is properly configured, the Active Directory filter list opens in the wizard.

See [Configuring Active Directory Synchronization](#) on page 77.

The person information automatically populates the **Person List** when you create people using Active Directory. You can edit person information.

In order to add users with the correct domain name, the system parses the user's domain name from the user principal name provided by Active Directory (For example: `accessdata.com\hhadley`). This allows the system to use the full domain name instead of truncating the name (For example, `development.accessdata.com` will be used instead of `development`).

If you find that there are errors in the system's automatic retrieval of the domain name, you can override the domain name and enter a value manually. See [To add people using Active Directory](#) on page 119. for more information.

---

**Note:** If you want to have the system truncate the domain name, update your Infrastructure service configuration file. Edit The AppSetting key `ReturnDomainAsFullyQualifiedDomainName` and change the value from `UserPrincipalName` to `CanonicalName`.

---

## To add people using Active Directory

1. In the *Data Sources > People* page, click  **Import from AD**.
2. Set the search/Browse depth to **All Children** or **Immediate Children**.
3. (optional) Check **Domain Name Override** if you want to specify the domain or domain portion for the users created. If you leave this unchecked, the application ignores any text in the **Domain Name Override** field.

---

**Note:** The domain for the users created is drawn and parsed from the userPrincipalName in Active Directory. Because all Active Directories are configured according to the needs of the directories' organization, what populates automatically based on the userPrincipalName may not suit your organization's needs. In this case, use Domain Name Override to specify the domain.


---

4. (optional) In the **Domain Name Override** field, add the domain for users created. For example, if you type `accessdata.com`, the user name will appear as `accessdata.com\<user name>`

---

**Note:** The domain name is applied once you advance to the second screen of the wizard. Navigating back to the first page and changing the domain name will not affect any users added to the import list and queued for creation. To change the domain name, remove all users from the **To Be Added** list and add them again from the search results.





---

5. Select where you want to perform the search.
6. Set the search options to one of the following:
  - Match Exact
  - Starts With
  - Ends With
  - Contains
7. Enter your search text.
8. Check the usernames that you want to add as people.
9. Click  **Add to Import List**.
10. Click **Continue**.
11. Review the members selected, members to add as people, and conflicted members. If you need to make changes, click **Back**.
12. Click **Import**.

## Associating Computers to a Person

From the *Computers* pane under the *Person* tab, you can associate and disassociate computers to a selected person.





### To associate a computer to a person

1. In the *Computers* list pane, click  to add computers.
2. In the *Associate Computers to <Person>* dialog, do one of the following:
  - In the *All Computers* pane, click  to add computers to the *Associated Computers* pane.
  - In the *All Computers* pane, click  to remove computers from the *Associated Computers* pane.
3. Click **OK**.
4. (optional) Click  to remove a computer from an associated person.

## Associating Network Shares to a Person

From the *Network Shares* pane under the *Person* tab, you can associate and disassociate network shares to a selected person.

### To associate a network share to a person

1. In the *Network Shares* list pane, click  to add network shares.
2. In the *Associate Network Shares to <Person>* dialog, do one of the following:
  - In the *All Network Shares* pane, click  to add network shares to the *Associated Network Shares* pane.
  - In the *All Network Shares* pane, click  to remove network shares from the *Associated Network Shares* pane.
3. Click **OK**.
4. (optional) Click  to remove network shares from an associated person.


## Adding an Enterprise Vault Archive to a Person

From the *Vault Archive* pane under the *Person* tab, you can add an Enterprise Vault archive to a selected person. Before adding an Enterprise Vault archive to a person, you must first configure the system to collect from an Enterprise Vault archive.

See [Configuring for Enterprise Vault](#) on page 154.




### To add an Enterprise Vault archive to a person

1. In the Person list, select the person that you want to add a cloud mail server to.
2. Under the *Vault Archives* tab, click  **Add**.
3. In the **Archive Name** field, enter the name of the Vault archive.
4. Enter the archive ID in the **Archive ID** field.
5. Select the Enterprise Vault server from the **Enterprise Vault** pull-down.
6. Select the archive type from the **Archive Type** pull-down. You can choose either Exchange, Notes, or File Store.
7. Click **Ok**.

## Editing an Enterprise Vault Archive Added to a Person

You can edit any Enterprise Vault archive server that you have added to a person.



### To edit an Enterprise Vault archive server

1. On the **Vault Archives** tab, select the name and username of the Enterprise Vault archive server that you want to edit.
2. Click  **Edit**
3. In *Vault Archives*, edit the Enterprise Vault details.
4. Click **OK**.

## Removing an Enterprise Vault Archive Added to a Person

You can remove one or more Enterprise Vault servers that you have added to a person.

### To remove one or more Enterprise Vault archive servers





1. On the **Vault Archives** tab, select the name of the Enterprise Vault archive server that you want to edit.
2. If you want to remove one server, check the name that you want to remove, and select  **Delete**.
3. If you want to remove more than one server, check the names that you want to remove, and select  **Delete**.
4. To confirm the deletion, click **OK**.

## Associating a Project to a Person

From the *Projects* pane under the *Person* tab, you can associate and disassociate projects to a selected person.

### To associate a project to a person

1. Click  **Projects** .


2. In the *Project* list pane, click  to add projects.
3. In the *Associate Projects to <Person>* dialog, do one of the following:
  - In the *All Projects* pane, click  to add projects to the *Associated Projects* pane.
  - In the *All Projects* pane, click  to projects from the *Associated Projects* pane.
4. Click **OK**.
5. (optional) Click  to remove projects from an associated person.

## Adding a Cloud Mail Server to a Person

From the *Cloud Mail* pane under the *Person* tab, you can add a cloud mail server to a selected person. Before adding a cloud mail server to a person, you must first configure the system to collect from a cloud mail server.

See [Configuring for Cloud Mail](#) on page 167.


### To add a cloud mail server to a person

1. In the *Person* list, select the person that you want to add a cloud mail server to.
2. Under the *Cloud Mail* tab, click  **Add**.
3. In the **Name** field, enter the name of the person.
4. Select the cloud mail server from the **Cloud Mail Server** pull-down.
5. In the **Username** field, enter the name of the user that you will be collecting from on the cloud server.
6. In the **Password** field, enter the password of the username on the cloud server.
7. Re-enter the password in the **Confirm Password** field.
8. Click **Ok**.

## Editing a Cloud Mail Server

You can edit any cloud mail server that you have added to a person.



### To edit a cloud mail server

1. On the **Cloud Mail** tab, select the name and username of the cloud mail server that you want to edit.
2. Click  **Edit**
3. In *Cloud Mail Details*, edit the cloud mail details.
4. Click **OK**.

## Removing a Cloud Mail Server

You can remove one or more cloud mail servers that you have added to a person.

### To remove one or more cloud mail servers

1. On the **Cloud Mail** tab, select the name and username of the cloud mail server that you want to edit.
2. If you want to remove one name, check the name that you want to remove, and select  **Delete**.
3. If you want to remove more than one name, check the names that you want to remove, and select  **Delete**.
4. To confirm the deletion, click **OK**.

# Managing Computers for Collecting Data

## About Computer Management

One of the primary sources of evidence used in a project originates on workstations (or nodes) managed by a person. To acquire that data, the application installs an agent on any node that could potentially host evidence. A Work Manager contacts the agent and requests that files, or an entire drive, be transmitted to the Work Manager. The Work Manager then runs the Evidence Processing sub-system for processing, placing the evidence into the data store.

On the network, you can add any number of computers as possible evidence sources for a collection. These may or may not be associated with the people included in the **Person List** view. These computers are managed by way of the **Computer Management** page.

---

**Note:** In order for processing to start, the application must mark a node as cancelled in order for a collection to complete. Because of this, nodes that have been cancelled before processing will display a completed processing status, even though processing does not occur on the cancelled node. See [Processing a Job](#) on page 453.

---

When you create and view the list of computers, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.

See [Managing Columns in Lists and Grids](#) on page 37.

On the bottom of the page, you can associate People, Jobs, and Groups to computers.




See [Adding People](#) on page 116.

See [Managing Groups for Collecting Data](#) on page 133.









## Computer Tab Options

The following table lists the various options that are available under the *Computer* tab.

### Computer Tab Options


Element	Description
Filter Options	Allows you to filter the Computer list.
Add 	Click to add a computer. See <a href="#">Adding a Computer</a> on page 125.
Edit 	Click to edit a computer. See <a href="#">Editing a Computer</a> on page 126.
Delete 	Click to remove a computer. See <a href="#">Deleting a Computer</a> on page 126.

## Computer Tab Options

Element	Description
Refresh 	Click to refresh the computer list.
Delete 	Click to remove multiple computers. See <a href="#">Deleting a Computer</a> on page 126.
Import Computers from CSV 	Import a list of computers from a CSV file. See <a href="#">Importing Computers from a CSV file</a> on page 127.
Export to CSV 	Export the current set of data to a CSV file.
Columns 	Click to adjust what columns display in the <i>Computer</i> List.
People 	Allows you to view people that been associated to a computer. In the <i>People</i> pane, you can do the following: <ul style="list-style-type: none"><li>● Filter the <i>People</i> list.</li><li>● Associate and disassociate people to a computer. See <a href="#">Associating People to a Computer</a> on page 126.</li><li>● Export the <i>Computers</i> list to a CSV file.</li><li>● Adjust the columns' display in the <i>Computers</i> list.</li></ul>
Jobs 	Allows you to view jobs that have run on a computer. In the <i>Jobs</i> pane, you can do the following: <ul style="list-style-type: none"><li>● Filter the <i>Jobs</i> list.</li><li>● Export the <i>Jobs</i> list to a CSV file.</li><li>● Adjust the columns' display in the <i>Jobs</i> list.</li></ul>
Groups 	Allows you to view groups that a computer belongs to. In the <i>Groups</i> pane, you can do the following: <ul style="list-style-type: none"><li>● Filter the <i>Groups</i> list.</li><li>● Export the <i>Groups</i> list to a CSV file.</li><li>● Adjust the columns' display in the <i>Groups</i> list.</li></ul>

## Adding a Computer


### To add a computer

1. Click  **Add**.
2. Enter the computer name and description.
3. (Optional) Enter Credant Options.  
See [Configuring Data Source Credant Options](#) on page 132.
4. Click **Save**.

## Editing a Computer

You can edit the properties of a computer.

### To edit a computer

1. Click  **Edit**.
2. Make any desired changes.
3. (Optional) Enter Credant Options.  
See [Configuring Data Source Credant Options](#) on page 132.
4. Click **Save**.

## Deleting a Computer

You can delete one or more computers from the system. You should avoid removing or deleting a computer if it is already used in a collection.


---

**Note:** If you delete a computer it may cause the Work Manager to stop functioning.

---

See [About Network Shares](#) on page 129.





### To delete a computer

1. Select one or more computers that you want to delete.
2. Click  **Delete**.
3. Verify the deletion by clicking **OK**.

## Associating People to a Computer

From the *People* pane under the *Computers* tab, you can associate and disassociate people to a selected computer.

### To associate a person to a computer


1. In the *People* list pane, click  to add people.
2. In the *Associate People to <Computer>* dialog, do one of the following:
  - In the *All People* pane, click  to add people to the *Associated People* pane.
  - In the *All People* pane, click  to remove people to the *Associated People* pane.
3. Click **OK**.
4. (optional) Click  to remove a person from an associated computer.

## Importing Computers from a CSV file

From the *Computers* tab, you can import a list of computers into the system from a CSV file. Before importing computers from a CSV file, you need to be aware of the following items:

- Make sure that the Computer column has a header. Also if you import computers with associations to groups, make sure that the Groups column has a header.
- If you want more than one group associated to a computer, separate the groups by semicolon in the Groups column.
- In the computer column, you can designate computers by host name or IP address.

### To import computers from a CSV file

1. Click  to import a list of computers from a CSV file.
2. From the *Import Computers from CSV* dialog, choose from the following options:
  - **Associate to Groups**
  - **Merge new groups with existing computers.** This allows you to associate new groups to computers that were previously added by CSV import. For example, if Group C is added to the system after computers have been added, you can re import your list with this option selected. This adds Group C to the list of computers added, in addition to groups in the CSV list that are associated to computers.

---

**Note:** Associations can be added by CSV import, but cannot be deleted by CSV import.


---

- **Download Sample CSV.** This allows you to download a sample CSV file illustrating how your CSV file should be created. This example is dynamic; if you select Associate to Groups, the sample CSV file includes a column for groups as well as for computers.
3. Once options have been selected, click **OK**.
4. Browse to the CSV file that you want to upload.

After file has been uploaded, a *Computer Import Summary* dialog appears. This displays the number of computers added, merged, and/or failed, with details if an import failed. Click **OK**. From the *Computers* tab, you can import a list of computers into the system from a CSV file. Before importing computers from a CSV file, you need to be aware of the following items:

- Make sure that the Computer column has a header. Also if you import computers with associations to groups, make sure that the Groups column has a header.
- If you want more than one group associated to a computer, separate the groups by semicolon in the Groups column.
- In the computer column, you can designate computers by host name or IP address.

### To import computers from a CSV file

1. Click  to import a list of computers from a CSV file.
2. From the *Import Computers from CSV* dialog, choose from the following options:
  - **Associate to Groups**
  - **Merge new groups with existing computers.** This allows you to associate new groups to computers that were previously added by CSV import. For example, if Group C is added to the system after computers have been added, you can re import your list with this option selected. This

adds Group C to the list of computers added, in addition to groups in the CSV list that are associated to computers.

---

**Note:** Associations can be added by CSV import, but cannot be deleted by CSV import.

---

- **Download Sample CSV.** This allows you to download a sample CSV file illustrating how your CSV file should be created. This example is dynamic; if you select Associate to Groups, the sample CSV file includes a column for groups as well as for computers.
3. Once options have been selected, click **OK**.
  4. Browse to the CSV file that you want to upload.
  5. After file has been uploaded, a *Computer Import Summary* dialog appears. This displays the number of computers added, merged, and/or failed, with details if an import failed. Click **OK**.



# Managing Network Shares for Collecting Data

## About Network Shares

Shares are network folders on which the person may possess read and write access permissions. You can add or remove shares from this page, edit a share path, or add and edit a share's locality and description.

When you create and view the list of shares, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.









See [Managing Columns in Lists and Grids](#) on page 37.

**Important:** When a job targets a network share, if a file on the share is locked from reading, the job will skip that file and enter an entry in the log.




## Network Shares Tab Options

The following table identifies the tasks that you can perform from the **Network Shares** page.

### Network Shares Tasks

Task	Description
Filter Options	Allows you to filter the <i>Network Shares</i> list.
Add 	Adds a network share. See <a href="#">Adding a Network Share</a> on page 130.
Edit 	Lets you edit the network path where the share is located. See <a href="#">Editing a Network Share Path</a> on page 131.
Delete 	Deletes the selected share from the list of shares associated with the person. See <a href="#">Deleting Network Shares</a> on page 131.
Refresh 	Refreshes the <i>Network Shares</i> list.
Delete 	Deletes multiple selected shares from the list of shares associated with the person. See <a href="#">Deleting Network Shares</a> on page 131.
Import Network Shares from CSV 	Import a list of network shares from a CSV file. See <a href="#">Importing Network Shares from CSV</a> on page 132.
Export to CSV 	Export the current set of data to a CSV file.
Columns 	Click to adjust what columns display in the <i>Computer List</i> .

## Network Shares Tasks (Continued)

Task	Description
People 	Allows you to view people that been associated to a network share. In the <i>People</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Network Shares</i> list.</li><li>• Add a person to the network share.</li><li>• Edit a person that has been added to the network share.</li><li>• Associate and disassociate people to a network share.</li><li>• Export the <i>Network Shares</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Network Shares</i> list.</li></ul>
Jobs 	Allows you to view jobs that have run on a network share. In the <i>Jobs</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Jobs</i> list.</li><li>• Export the <i>Jobs</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Jobs</i> list.</li></ul>
Groups 	Allows you to view groups that a computer belongs to. In the <i>Groups</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>Groups</i> list.</li><li>• Export the <i>Groups</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Groups</i> list.</li></ul>

## Adding a Network Share

The network identity used to install the application on the server must have Network administrator privileges to be able to access all shares.



---

**Note:** In order to collect from network shares, configuration changes should be made to the application during the installation process. Please consult with AccessData's support during installation if you plan on collecting from network shares as a data source.

---

See [About Network Shares](#) on page 129.

### To add a network share

1. Click  **Add**.
2. Enter the name.
3. Specify the path to a network share.
4. Click  **Validate** to verify the network path that you entered.
5. (Optional) In the **Description** field, enter a description that can help you identify the network path.
6. (Optional) In the **Username** and **Password** fields, specify a username and password to the Network share.

---

**Note:** Make sure that when you are setting up your network share, you fill the username and password fields correctly to avoid errors. If you try to collect a network share with an invalid username/password, the job will go to pending and never finish. When you run a job with network shares, make sure to specify a job

expiration date in the job wizard. This will allow the job to expire within a specified time, even if there was an invalid user or password. See [Job Expiration Options](#) on page 431.

---



7. (Optional) Under *User Credentials*, select either the **No Credentials** or **New Credentials** radio button
8. Click **OK**.

## Editing a Network Share Path

You can edit a network share path if it is not already included in a collection.

See [About Network Shares](#) on page 129.

### To edit a network share path

1. On the *Data Sources* page, click **Network Shares**.
2. Click  **Edit**.
3. In the **Path** field, update the Network Share path.
4. Click  **Validate** to verify the Network Path that you entered.
5. (Optional) In the **Username** and **Password** fields, specify a username and password to the network share.
6. (Optional) Enter Credant options.  
See [Configuring Data Source Credant Options](#) on page 132.
7. Click **Save**.

## Deleting Network Shares

You should avoid removing or deleting a network share if it is already used in a collection.



---

**Note:** If you delete a network share it may cause the *Work Manager* to **stop functioning**.

---

See [About Network Shares](#) on page 129.


### To delete network shares

1. On the *Data Sources* page, click **Network Shares**
2. Select one or more shares that you want to delete.
3. If you want to remove one network share, check the network share that you want to remove, and select  **Delete**.
4. If you want to remove more than one network share, check the network shares that you want to remove, and select  **Delete**.
5. Verify the deletion by clicking **OK**.

## Importing Network Shares from CSV

From the *Network Shares* tab, you can import a list of network shares into the system from a CSV file.

### To import network shares from a CSV file

1. Click  to import a list of network shares from a CSV file.
2. From the *Import Network Shares from CSV* dialog, click **OK**.
3. Browse to the CSV file that you want to upload.
4. After file has been uploaded, a *Network Shares Import Summary* dialog appears. This displays the number of network shares added, merged, and/or failed, with details if an import failed. Click **OK**.

## Configuring Data Source Credant Options

The following table describes the options that are available when you add or remove Credant on network shares or computers as data sources.

See [Credant Site Server Configuration Options](#) on page 90.

See [Managing Computers for Collecting Data](#) on page 124.

See [Managing Network Shares for Collecting Data](#) on page 129.

### Manage Credant Options

Option	Description
No Shield (no device encryption)	No encryption is enabled on the network share or computer.
Current Shield File	Uses the currently associated Credant Shield file on the Network share or the computer.
Upload New Shield File	Upload a new Credant Shield file that you want to associated with the Credant-encrypted Network share or computer. You need to provide the file path and password to the new file.

# Managing Groups for Collecting Data

## Accessing the Groups Tab

### To access the Groups tab

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.



## Groups Tab Options

The following table identifies the tasks that you can perform from the **Groups** page.

### Groups Tasks

Task	Description
Search	Allows you to search the <i>Groups</i> list.
Add 	Adds a group. See <a href="#">Adding a Group Manually</a> on page 135.
Edit 	Edits a group. See <a href="#">Editing a Manually Added Group</a> on page 135.
Delete 	Deletes a group. See <a href="#">Deleting a Manually Added Group</a> on page 135.
Refresh 	Refreshes the <i>Groups</i> list.
People 	Allows you to view people that been associated to a group. In the <i>People</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the <i>People</i> list.</li><li>• Add a person manually. See <a href="#">Adding a Person to a Group Manually</a> on page 136.</li><li>• Add people to a group using Active Directory. See <a href="#">Adding People to Groups Using Active Directory</a> on page 136.</li><li>• Export the <i>People</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>People</i> list.</li></ul>

## Groups Tasks (Continued)

Task	Description
Computers 	<p>Allows you to view computers that have been associated to a group. In the <i>Computers</i> pane, you can do the following:</p> <ul style="list-style-type: none"><li>• Filter the <i>Computers</i> list.</li><li>• Add a computer to a group. See <a href="#">Adding Computers to a Group Manually</a> on page 138.</li><li>• Edit a computer that has been added to a group. See <a href="#">Editing a Computer Added to a Group Manually</a> on page 139.</li><li>• Remove a computer from a group. See <a href="#">Removing Computers from a Group</a> on page 139.</li><li>• Adding computers to a group using Active Directory. See <a href="#">Adding Computers to a Group Using Active Directory</a> on page 137.</li><li>• Export the <i>Computers</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Computers</i> list.</li></ul> <p><b>Note:</b> You cannot delete a computer that has been added in this pane. To delete a computer, see the <i>Computers</i> tab under <i>Data Sources</i>. See <a href="#">Deleting a Computer</a> on page 126.</p>
Network Shares 	<p>Allows you to view network shares that are associated with a group. In the <i>Network Shares</i> pane, you can do the following:</p> <ul style="list-style-type: none"><li>• Filter the <i>Network Shares</i> list.</li><li>• Add a network share to a group. See <a href="#">Adding Network Shares to a Group Manually</a> on page 140.</li><li>• Editing a network share that has been added to a group. See <a href="#">Editing Manually Added Network Shares to a Group</a> on page 141.</li><li>• Add a network share using Active Directory. See <a href="#">Adding Network Shares to a Group using Active Directory</a> on page 139.</li><li>• Export the <i>Network Shares</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Network Shares</i> list.</li></ul>

## Syncing to Active Directory from Groups

Active Directory is the paramount platform operator. Therefore, you need to make sure that your Active Directory listing is kept current. When you synch to Active Directory, it loads any changes that were made to people in an organization unit into your Active Directory listing since the last synchronization.

The Person unique identifier (UID) is used to filter duplicate names.

Synchronization is from Active Directory to the application only.

Groups, people, computers, and network shares that you have added manually in *Groups*, are different record types, and are not synchronized with Active Directory. Instead, you must update such records manually.

---

**Note:** Before you attempt to sync Active Directory from *Groups*, you must first make sure that you have configured Active Directory synchronization in the application.

---

See [Configuring Active Directory Synchronization](#) on page 77.

### To synchronize to Active Directory from Groups

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.

3. On the *Groups* list pane, in the bottom right corner, click  **Synchronize**.

## Adding a Group Manually

You can add groups manually instead of using Active Directory. Added groups can contain people, computers, and network shares that you have also added manually.


When you add a group manually, it is added to the left-most list box in the *Groups* list pane area.

See [Adding a Person to a Group Manually](#) on page 136.

See [Adding Computers to a Group Manually](#) on page 138.

See [Adding Network Shares to a Group Manually](#) on page 140.


### To add a group manually

1. Click **Data Sources**.
2. Click the **Groups** tab.
3. In the right side of the *Groups* list pane, click  **Add**.
4. On the *Group Details* list pane, enter a name and description.
5. Click **OK**.

## Editing a Manually Added Group

You can edit any group that you have added manually to the *Groups* page.



### To edit a manually added group

1. In the *Data Sources* page, click **Groups**.
2. In the right side of the *Groups* list pane, click  **Edit**.
3. In the *Group Details* list pane, edit the options you want.
4. Click **OK**.

## Deleting a Manually Added Group

You can delete any group that you have added manually to the *Groups* page. When you delete a group, all associated people, computers, and network shares are removed as well.

### To delete a manually added group

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. In the left-most search list of the upper pane, select a group that has  next to its name.
4. In the right side of the *Groups* list pane, click  **Delete**.
5. Click **OK**.

## Adding People to Groups Using Active Directory

You can add people to groups using Active Directory.

The *Filter Options* feature is available throughout the user interface in *Groups*. You can filter on people, computers, and network shares to refine the list that is displayed.

Before you add people, be sure that you have configured Active Directory synchronization in *Management* and recently synched to Active Directory in *Groups*.

See [Configuring Active Directory Synchronization](#) on page 77.

See [Syncing to Active Directory from Groups](#) on page 134.





See [Adding a Person to a Group Manually](#) on page 136.

See [Removing People from a Group](#) on page 137.

After you create the groups that you want, you can add jobs and select the groups whose data you want to collect.

See [Adding a Job](#) on page 426.

### To add people to a group using Active Directory

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add people.
4. In the *Associated* tab, click  **People**.
5. In the *People* list pane, click  to add people.
6. In the *Associate People to <group\_name>* dialog, do one of the following:
  - In the *All People* pane, click  to add people to the *Associated People* pane.
  - In the *All People* pane, click  to remove people from the *Associated People* pane.
7. Click **OK**.

## Adding a Person to a Group Manually

You can add people to groups manually, instead of using Active Directory.

---

**Note:** Groups, people, computers, and Network shares that you have added manually in *Groups*, are a different record type and are not synchronized with Active Directory. Instead, you must update such records manually.



---

See [Adding People to Groups Using Active Directory](#) on page 136.

### To add people to a group manually

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.



3. On the *Groups* list pane, use the search panes to select a group whom you would like to add people manually.
4. In the Associated tabs, click  **People**.
5. In the right side of the *People* list pane, click  **Add**.
6. In the *Person Details*, enter information about the person.

---

**Note:** The Domain is the network domain that the person belongs to. For Active Directory, the domain would have the following syntax: `dc=<my_domain>,dc=com`.

---

7. Click **OK**.



## Removing People from a Group

You can remove one or more people from an associated group.

See [Adding People to Groups Using Active Directory](#) on page 136.

See [Adding a Person to a Group Manually](#) on page 136.

### To remove people from a group

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group that contains people that you want to disassociate from the group.
4. In the Associated tabs, click  **People**.
5. In the *Person* list pane, check the people that you want to delete.
6. In the lower left corner of the pane, click  to remove the people from the associated group.

## Adding Computers to a Group Using Active Directory

You can add computers to groups using Active Directory.

The *Filter Options* feature is available throughout the user interface in *Groups*. You can filter by people, computers, and network shares to refine the list that is displayed.

Before you add computers, be sure that you have configured Active Directory synchronization in *Management* and recently synced to Active Directory in *Groups*.

See [Configuring Active Directory Synchronization](#) on page 77.

See [Syncing to Active Directory from Groups](#) on page 134.





See [Adding Computers to a Group Manually](#) on page 138.

See [Removing Computers from a Group](#) on page 139.

After you create the groups that you want, you can add jobs and select the groups whose data you want to collect.

See [Adding a Job](#) on page 426.

### To add computers to a group using Active Directory

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add computers.
4. In the Associated tabs, click  **Computers**.
5. In the *Computers* list pane, click  to add computers.
6. In the *Associate Computers to <group\_name>*, do one of the following:
  - In the *All Computers* pane, click  to add computers to the *Associated Computers* pane.
  - In the *All Computers* pane, click  to remove computers from the *Associated Computers* pane.
7. Click **OK**.

## Adding Computers to a Group Manually

You can add computers to groups manually, instead of using Active Directory.



---

**Note:** Groups, people, computers, and Network shares that you have added manually in *Groups*, are a different record type and are not synchronized with Active Directory. Instead, you must update such records manually.

---

See [Adding Computers to a Group Using Active Directory](#) on page 137.



### To add computers to a group manually

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add people manually.
4. In the Associated tabs, click  **Computers**.
5. In the right side of the *Computers* list pane, click  **Add**.
6. On the *Computer Details* tab, enter a *Computer Name* and *Description*.
7. Click **OK**.

## Editing a Computer Added to a Group Manually

You can edit any computer that you have added manually to the *Groups* page.

### To edit a computer

1. In the *Data Sources* page, click **Groups**.
2. In the Associated tabs, click  **Computers**.
3. In the right side of the *Computers* list pane, click  **Edit**.
4. In the *Group Details* list pane, edit the options you want.
5. Click **OK**.



## Removing Computers from a Group

You can remove one or more computers from an associated group.

See [Adding Computers to a Group Using Active Directory](#) on page 137.

See [Adding Computers to a Group Manually](#) on page 138.

### To remove computers from a group

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group that contains computers that you want to disassociate from the group.
4. In the Associated tabs, click  **Computers**.
5. In the *Computers* list pane, check the computers that you want to remove from the associated group.
6. In the lower left corner of the pane, click .

## Adding Network Shares to a Group using Active Directory

You can add network shares to groups using Active Directory.

The *Filter Options* feature is available throughout the user interface in *Groups*. You can filter by people, computers, and Network shares to refine the list that is displayed.

Before you add network shares, be sure that you have configured Active Directory synchronization in *Management* and recently synched to Active Directory in *Groups*.

See [Configuring Active Directory Synchronization](#) on page 77.

See [Syncing to Active Directory from Groups](#) on page 134.





See [Adding Network Shares to a Group Manually](#) on page 140.

See [Removing Network Shares from a Group](#) on page 141.

After you create the groups that you want, you can add jobs and select the groups whose data you want to collect.

See [Adding a Job](#) on page 426.

### To add network shares to a group using Active Directory

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add computers.
4. In the Associated tabs, click  **Network Shares**.
5. In the *Network Shares* list pane, click  to add network shares.
6. In the *Associate Network Shares to <group\_name>*, do one of the following:
  - In the *All Network Shares* pane, click  to add computers to the *Associated Network Shares* pane.
  - In the *All Network Shares* pane, click  to remove computers from the *Associated Network Shares* pane.
7. Click **OK**.

## Adding Network Shares to a Group Manually

You can add network shares to groups manually, instead of using Active Directory.



---

**Note:** Groups, people, computers, and Network shares that you have added manually in Groups, are a different record type and are not synchronized with Active Directory. Instead, you must update such records manually.

---

See [Adding Network Shares to a Group using Active Directory](#) on page 139.

### To add network shares to a group manually

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add network shares manually.
4. In the Associated tabs, click  **Network Shares**.
5. In the right side of the *Network Shares* list pane, click  **Add**.
6. On the *Network Details* tab, enter a *Path* and *Description*.

---

**Note:** The local folder path or the UNC path to a Network share is where the data resides. Make sure double backslash characters (\\) precede the UNC path. Or, enter the IP address path to a Network share. Make sure double backslash characters (\\) precede the IP address path.



---

7. (Optional) Select **User Credentials**
8. Click **OK**.

## Editing Manually Added Network Shares to a Group

You can edit network shares that have been added to groups manually.

### To edit network shares that have been added to a group manually

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group whom you would like to add network shares manually.
4. In the Associated tabs, click  **Network Shares**.
5. In the right side of the *Network Shares* list pane, click  **Edit**.
6. Click **OK**.



## Removing Network Shares from a Group

You can remove one or more network shares from an associated group.

See [Adding Network Shares to a Group using Active Directory](#) on page 139.

See [Adding Network Shares to a Group Manually](#) on page 140.

### To remove Network shares from a group

1. Click the **Data Sources** tab.
2. Click the **Groups** tab.
3. On the *Groups* list pane, use the search panes to select a group that contains computers that you want to disassociate from the group.
4. In the Associated tabs, click  **Network Shares**.
5. In the *Network Shares* list pane, check the network shares that you want to remove from the associated group.
6. In the lower left corner of the pane, click .

# Configuring Network Collectors

The Network Collectors tab on the Data Sources page is where you can add your network collectors for collection jobs.

---

**Note:** If you enter incorrect information in a required field, the system displays a Submit operation failed error when attempting to save the network collector. This alerts you immediately to any problems with the data entered. You can then edit the field(s) and provide correct data.

---

See [Using Sentinel](#) on page 616.

## Network Collector Detail Options

Option	Description
DB Provider	Displays a choice between MSSQL and Oracle for the database. These are the only supported databases
Server	Specifies the address of the server. This field is required. For example: 10.10.32.15
Port	The port that accepts traffic. This field is required.
Database Name/SID	The name of the database. This field is required.
Description	Describes the network collector.
Username	The Username of user who has access to the server and the database. This field is required.
Password	Password associated with the User. This field is required.

# Managing Evidence for Collecting Data

## About the Evidence Tracker

The *Evidence* tab under *Data Sources* is referred to as the Evidence Tracker. It allows you to add and manage evidence globally throughout the system. In the Evidence Tracker, you can reuse evidence, much like you can reuse an existing person or computer. You can track evidence activity and view the:

- Time evidence was collected and sent
- Location of evidence
- Person that the evidence was sent to and how the evidence was sent.

In addition to viewing the evidence, you can add additional evidence to specific projects or add evidence to the system that is available to all people. Evidence can be added without processing or can be processed immediately after adding. When you add evidence, the Evidence Wizard appears.


See [Using the Evidence Wizard](#) on page 376.

In the Evidence Tracker, you can edit evidence fields, allowing users to update information associated with a given piece of evidence. You can edit description, unprocessed paths, associated people, and custom fields.

Users who have system administration permissions or Evidence administration permissions may view all the evidence in the system. Users who do not have those permissions can only view the evidence that they are given permission to see.

## Accessing the Evidence Tracker

### To access the Evidence Tracker

1. Click the **Data Sources** tab.
2. Click the **Evidence**  tab.

## About the Evidence Tracker Page












You can manage evidence from the *Evidence Tracker* tab on the *Data Sources* page.

The following table identifies the tasks that you can perform from the **Evidence Tracker** page.

### Evidence Tracker Options

Element	Description
Filter Options	Allows the user to filter the list.
Evidence Path List	Displays the paths of evidence in the project. Click the column headers to sort by the column.

## Evidence Tracker Options

Element	Description
Add 	Click to add evidence with the <b>Evidence Wizard</b> . Evidence is added through the evidence wizard and may be added without processing. Evidence added through the Evidence Tracker is not associated with any project, but is available in the Global Evidence list. See <a href="#">Using the Evidence Wizard</a> on page 376.
Edit 	Click to edit the evidence selected. See <a href="#">Using the Evidence Wizard</a> on page 376.
Delete 	Click to delete evidence selected. See <a href="#">Using the Evidence Wizard</a> on page 376.
Refresh 	Click to refresh the evidence list.
Columns 	Click to adjust what columns display in the Evidence Path List.
Export to CSV 	Export the current set of data to a CSV file.
Custom Properties 	Click to add custom properties. Custom properties must be defined before importing CSV files with custom fields in the headers. See <a href="#">Configuring Custom Fields</a> on page 294.
Delete 	Click to delete selected evidence.
Projects 	Lists the Projects that are associated with selected evidence. Projects are shown by name, person, the processing state, description, and last modified date. You can export the list to a CSV file.
Change History 	Track the changes that have been made to the evidence. You can view the changes by action type, date, who performed the changes, the field name, the project that the evidence is associated with, the target user, the new value added, and the old value that was changed. You can export the list to a CSV file.
Access Permissions 	View who has access permissions to the evidence. You can view by username, first name, last name and last modified date. You can associate and unassociate evidence to the users listed. You can export the list to a CSV file.



## Chapter 13

# Configuring Third-Party Data Repositories as Data Sources

---

In order to collect data from a third-party data repository, you need to perform the following actions:

### Public Data Repository Workflow

Step	Task
1	Configure the application to collect from a public data repository.
2	Run a collection job. See <a href="#">About Collection Jobs</a> on page 423.

This chapter describes how to configure settings for collecting data from public data repositories and include the following topics:

- [Configuring for a Domino Server](#) (page 146)
- [Configuring for an Exchange Online/365 Server](#) (page 147)
- [Configuring for Exchange 2003, 2007, and 2010 Servers](#) (page 148)
- [Configuring for Exchange 2010 SP1 and 2013 Servers](#) (page 150)
- [Configuring for Enterprise Vault](#) (page 154)
- [Configuring for a Documentum Server](#) (page 158)
- [Configuring for a SharePoint Server](#) (page 160)
- [Configuring for Web Sites](#) (page 163)
- [Configuring for a DocuShare Server](#) (page 165)
- [Configuring for Cloud Mail](#) (page 167)
- [Configuring for an OpenText ECM Server](#) (page 169)
- [Configuring for Gmail](#) (page 170)
- [Configuring for Google Drive](#) (page 171)
- [Configuring for Druva](#) (page 172)
- [Configuring for a CMIS Repository](#) (page 174)
- [Configuring for Box](#) (page 177)

For information on using jobs to collect data from public data repositories, see [About Jobs](#) (page 418).

# Configuring for a Domino Server

You can configure the application to collect the data from your IBM Lotus Domino server. Such data might be emails, instant messages, calendars, forum messages, and blogs. You can also collect documents associated with Lotus Symphony, such as word processor documents, spreadsheets, and presentations.

Once you have configured the application to collect from your Domino server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Person's Domino** as an option under **People** in the **Custom Selection** pane. At that point, a *People* page appears in the left pane. You can then specify what to collect from the Domino server.




---

**Note:** The Lotus Notes Client must be run at least once to configure it before it can be collected.

---

See [About Collection Jobs](#) on page 423.

## To configure the application for collecting from a Domino Server

1. On the *Data Sources* page, click **Domino**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Domino Server Configuration Fields](#) on page 146.
4. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.
5. Click **OK**.

## Domino Server Configuration Fields

The following table describes the fields that are available in the Domino Server configuration dialog box.

See [Configuring for a Domino Server](#) on page 146.

### Notes Server Configuration Fields

Field	Description
Name	Specifies the name that you want to have appear in the <b>Jobs Wizard</b> for the Domino Server.
Locality	Specifies the location of the server.
Address	Specifies the path to the Domino server.
AdminID File	Specifies the path to the administrator's ID file on the Domino server.
Password	Specifies the password to the administrator's ID file.

# Configuring for an Exchange Online/365 Server




You can configure the application to collect data from your Microsoft Online/365 Exchange server. This data might include email, calendars, contacts, faxes, and voice mail.

Once you have configured the application to collect from your Exchange Online/365 server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Person's Exchange** as an option under **People** in the **Custom Selection** pane. At that point, a *People* page appears in the left pane. You can then specify what to collect from the Exchange server.

Before configuring the application for an Exchange Online/365 server, you need to do the following:

- Outlook must be run at least once with the application service account (Exchange Administrator) logged in to create the administrative profile.
- You need to configure Outlook to correctly send and receive against the Exchange Server.
- Make sure that the server's password is current. Passwords for Microsoft Exchange Online/365 servers have an expiration date, and the application cannot collect from the server with an expired password.
- In order to collect from the server, you need to download Microsoft extensions to run Microsoft Powershell commands on the local system against the server. Consult with AccessData's support for more information.

## To configure the application for collecting from an Exchange Online/365 Server

1. On the *Data Sources* page, click **Exchange**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Exchange Server Online/365 Configuration Fields](#) on page 148.
4. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.
5. Click **OK**.

## Associating People to an Exchange Online/365 Server


For the application to collect from an Exchange server, people must be assigned to the server in the *Exchange* tab. You can associate people to more than one server. Assign people in one of two ways:

- Click **Associate To All people** in the *Exchange Mail Server Details* panel to associate people to the server.

---

**Note:** If you have previously associated a list of people to the server, **Associate To All People** will overwrite the previous associations.

---

- Add individual people from the *People* tab in the *Exchange* panel. To add people, click on the Associate link .

## Exchange Server Online/365 Configuration Fields

The following table describes the fields that are available in the Exchange Server Online/365 configuration dialog box.

See [Configuring for an Exchange Online/365 Server](#) on page 147.

### Exchange Server Online/365 Configuration Fields

Field	Description
Name	Specifies the friendly name of the Exchange Server. This name appears in the <b>Job Wizard</b> for the Exchange Server.
Locality	Specifies the location of the server. This field is not required.
Address	Specifies the path to the Exchange Server. The server name is in the form of 'exchange.mycompany.com' where 'exchange' is determined by your IT staff and 'mycompany' is the name of your company. Alternatively, an IP address can be used. The IP address must point to the front-end Exchange Server.
Username	Specifies the username of the Exchange Online/365 Server.
Password	Specifies the password for the Exchange Online/365 Server. <b>Note:</b> Exchange server passwords have an expiration date. You cannot collect from Exchange if the password is expired. Make sure that the password is current before setting up the server in the application.
Use Custom AD Settings	By default, the application uses the local Active Directory server. If you have an advanced scenario, such as a cross-domain scenario, you can select to this option and specify the AD Server, AD Port, AD BaseDN settings.
Associate To All People	Check to associate all of your people to the server. If you have previously associated individual people to a server, this action will overwrite the associations of the individual people.

## Configuring for Exchange 2003, 2007, and 2010 Servers

You can configure the application to collect data from your Microsoft Exchange server. This data might include email, calendars, contacts, faxes, and voice mail.

Outlook must be run at least once with the application service account (Exchange Administrator) logged in to create the administrative profile.

You need to configure Outlook to correctly send and receive against the Exchange Server.

---




**Note:** The application does not support EWS (Exchange Web Service integration) for Exchange 2010. EWS is only supported for 2010 SP1 and 2013 versions.

---

**Note:** Proxy support has been added to the Exchange EWS.

---

### To configure the application for collecting from an Exchange 2003, 2007, or 2010 Server

1. On the *Data Sources* page, click **Exchange**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Server Configuration Fields for Exchange 2003, 2007, and 2010](#) on page 149.
4. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.
5. Click **OK**.

## Associating People to Exchange 2003, 2007, or 2010 Server


For the application to collect from an Exchange server, people must be assigned to the server in the *Exchange* tab. You can associate people to more than one server. Assign people in one of two ways:

- Click **Associate To All People** in the *Exchange Mail Server Details* panel to associate people to the server.

---

**Note:** If you have previously associated a list of people to the server, **Associate To All People** will overwrite the previous associations.

---

- Add individual people from the *People* tab in the *Exchange* panel. To add people, click on the Associate link .

## Server Configuration Fields for Exchange 2003, 2007, and 2010

The following table describes the fields that are available in the server configuration dialog for Exchange 2003, 2007, and 2010. See [Configuring for Exchange 2003, 2007, and 2010 Servers](#) on page 148.

### Server Configuration Fields for Exchange 2003, 2007, and 2010

Field	Description
Name	Specifies the friendly name of the Exchange Server. This name appears in the <b>Job Wizard</b> for the Exchange Server.
Locality	Specifies the location of the server. This field is not required.

## Server Configuration Fields for Exchange 2003, 2007, and 2010

Field	Description
Address	Specifies the path to the Exchange Server. The server name is in the form of 'exchange.mycompany.com' where 'exchange' is determined by your IT staff and 'mycompany' is the name of your company. Alternatively, an IP address can be used. The IP address must point to the front-end Exchange Server.
Use Custom AD Settings	By default, the application uses the local Active Directory server. If you have an advanced scenario, such as a cross-domain scenario, you can select to this option and specify the AD Server, AD Port, AD BaseDN settings.
Associate To All People	Check to associate all of your people to the server. If you have previously associated individual people to a server, this action will overwrite the associations of the individual people.

## Configuring for Exchange 2010 SP1 and 2013 Servers

You can configure the application to collect data from your Microsoft Exchange server.

Outlook must be run at least once with the eDiscovery service account (Exchange Administrator) logged in to create the administrative profile.




You need to configure Outlook to correctly send and receive against the Exchange Server.

---

**Note:** When configuring the application for either a 2010 SP1 or 2013 server, make sure to properly specify the correct version. Specifying the wrong version of Exchange will cause the connector to fail.

---

### To configure the application for collecting from an Exchange 2010 SP1 or 2013 Server

1. On the *Data Sources* page, click **Exchange**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Server Configuration Fields for Exchange 2010 SP1 and 2013](#) on page 151.
4. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.
5. Click **OK**.

## Associating People to an Exchange 2010 SP1/2013 Server


For the application to collect from an Exchange server, people must be assigned to the server in the *Exchange* tab. You can associate people to more than one server. Assign people in one of two ways:

- Click **Associate To All People** in the *Exchange Mail Server Details* panel to associate people to the server.

---

**Note:** If you have previously associated a list of people to the server, **Associate To All People** will overwrite the previous associations.

---

- Add individual people from the *People* tab in the *Exchange* panel. To add people, click on the **Associate** link  .

## Server Configuration Fields for Exchange 2010 SP1 and 2013

The following table describes the fields that are available in the server configuration dialog box for Exchange 2010 SP1 and 2013.

See [Configuring for Exchange 2010 SP1 and 2013 Servers](#) on page 150.

### Server Configuration Fields for Exchange 2010 SP1 and 2013

Field	Description
Name	Specifies the friendly name of the Exchange Server. This name appears in the <b>Job Wizard</b> for the Exchange Server.
Locality	Specifies the location of the server. This field is not required.
Address	Specifies the path to the Exchange Server. The server name is in the form of 'exchange.mycompany.com' where 'exchange' is determined by your IT staff and 'mycompany' is the name of your company. Alternatively, an IP address can be used. The IP address must point to the front-end Exchange Server.
Exchange Web Services Enabled?	This must be checked if you want to use EWS (Exchange Web Service). When collecting from a 2010 SP1 server, you must have this checked in order to use specific 2010 SP1 features, such as recoverable items, archive mail, and filters.
Username	Specifies the username for the server.
Password	Specifies the password for the server. <b>Note:</b> Exchange server passwords have an expiration date. You cannot collect from Exchange if the password is expired. Make sure that the password is current before setting up the server in the application.
Exchange Server-side Mailbox Indexing Enabled?	If you have indexing enabled on the server, check this action. If you want to use filters on the data collected, you must have this action checked.
Use Custom AD Settings	By default, the application uses the local Active Directory server. If you have an advanced scenario, such as a cross-domain scenario, you can select to this option and specify the AD Server, AD Port, AD BaseDN settings.
Associate To All People	Check to associate all of your people to the server. If you have previously associated individual people to a server, this action will overwrite the associations of the individual people.

# Configuring for an Enterprise Vault Server

## *About Configuring for an Enterprise Vault Server*

You can configure the application so that you can collect data from Symantec Enterprise Vault using the **Job Wizard**. This data might include email, files, social media communications, SharePoint content, instant messages, and other electronically stored information.

Once you have configured the application to collect from your Enterprise server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, you can select **Enterprise Vaults** as an option under **People** in the **Custom Selection** pane. At that point, a Enterprise Vault Server page appears in the left hand pane. You can then select the Enterprise Vault servers from which you want to collect.

See [About the Jobs Tab](#) on page 419.

See [Enterprise Vault Server Collection Options](#) on page 479.

Before you can configure Enterprise Vault to collect data, each Enterprise Vault server must be running the AccessData Enterprise Vault Connector. To install the connector you need the application's Installation media.

See [Installing the AccessData Enterprise Vault Connector](#) on page 153.

See [Configuring for Enterprise Vault](#) on page 154.

The **Enterprise Vault Configuration** page has three panels that you can configure:

- **Enterprise Vault Servers**
- **Enterprise Vault Stores**
- **Unassociated Archives**

The **Enterprise Vault Stores** tab and the **Unassociated Archives** tab both reference servers on the **Enterprise Vault Servers** tab.

---

**Note:** Symantec fixed an issue with Enterprise Vault that has existed in versions prior to 8.0, service pack 4. The issue, as stated by Symantec, is that "retrieving large items (that is, files larger than 50 MB) resulted in corrupt data being returned." This issue adversely impacts the retrieval process for the application because the application often retrieves attachments and items from various File System Archives that are larger than 50 MB. As such, it is highly recommended that you upgrade and install the latest version of Enterprise Vault, along with the most recent service pack.

---

---

**Note:** When collecting email from an Enterprise Vault Server, make sure that the Task Controller Service and Enterprise Vault Storage Service is running on the Enterprise Vault Server. Otherwise, the collection will run without errors, but the files are not collected. An error stating that Enterprise Vault is unavailable is

---



recorded in the Integration Service logs. If you get this error, start the services and re-submit the collection.

---

## *Installing the AccessData Enterprise Vault Connector*

Before you can configure Enterprise Vault to collect data, the Enterprise Vault server at your site must have the AccessData Enterprise Vault Connector service installed on it. This integration service allows remote the application Work Managers to issue requests against the local Enterprise Vault program.

The service issues the following limited set of requests against Enterprise Vault:

- Lookup archive types (Directory Service)
- Apply collection filter criteria against the archives (index service)
- Retrieve matching documents (storage service)

You can install the connector service on one Enterprise Vault Server at a site, or you can install the connector service on multiple servers across different sites to assist with workload balancing.

The following components are necessary to run the Enterprise Vault Connector service on the Enterprise Vault Server:

- Microsoft .NET Framework 3.5 (SP1 or greater) Client Profile
- Microsoft .NET Framework 3.5 (SP1 or greater) Extended

If you do not have these components installed, the AccessData Enterprise Vault Connector installation prompts you to install them before you continue.

The connector service needs read access to all of the Enterprise Vault archives. To accomplish this, do one of the following:

- Run the service with the same credentials as the service account under which Enterprise Vault runs (the installation steps below use this scenario).
- Create a new domain account and grant it read access to each archive.

Following the installation, you can check that the AccessData Enterprise Vault Integration service has started using Windows **Computer Management**.

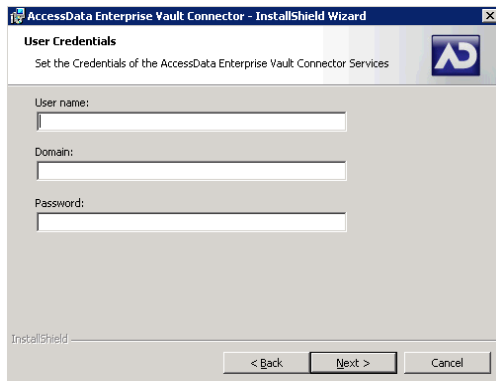
Use Windows **Control Panel** to uninstall **AccessData Enterprise Vault Connector** from the Enterprise Vault Server.

See [Configuring for Enterprise Vault](#) on page 154.

### **To install the AccessData Enterprise Vault Connector**

1. Log on to the Enterprise Vault Server computer by using either the Administrator account or an account that has administrator privileges.
2. Insert the application installation media into the media drive of the server.
3. From the root of the installation media, in the **application \EnterpriseVaultConnector** folder, double-click **AccessData Enterprise Vault Connector.exe** to start the installation.
4. On the **Welcome** window, click **Next**.
5. In the **License Agreement** window, read the license, and then click **I accept the terms in the license agreement**.

6. Click **Next**.
7. In the **Destination Folder** window, do one of the following:
  - Click **Next** to accept the default install path of the connector service.
  - Click **Change** to select a new install path, and then click **Next**.
8. In the **User Credentials** window, specify the credentials of the Enterprise Vault service account, and the domain where the server resides.






9. Click **Next**.
10. In the **Ready to Install the Program** window, click **Install**.  
You can now configure Enterprise Vault in the application.





## Configuring for Enterprise Vault

Before you can configure the application to collect from Enterprise Vault, make sure that each Enterprise Vault server at your site has an installation of the AccessData Enterprise Vault Connector.

See [Installing the AccessData Enterprise Vault Connector](#) on page 153.

### To configure the application to collect from Enterprise Vault

1. On the *Data Sources* page, click **Enterprise Vault**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Enterprise Vault Servers Tab Fields](#) on page 155.
4. Click **OK** to add the configuration to the **Enterprise Vault Servers** table.
5. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional Enterprise Vault Servers.
  - Continue with the next step.

7. On the **Enterprise Vault Stores** tab, click  **Add**.
8. Set the Enterprise Vault Store fields.  
See [Enterprise Vault Stores Tab Fields](#) on page 156.
9. Click **OK** to add the configuration to the **Enterprise Vault Stores** table.
10. Do one of the following:
  - Repeat steps 6-8 to configure additional Enterprise Vault Stores.
  - Continue with the next step.
11. On the **Unassociated Archives** tab, click  **Add**.
12. Set the **Unassociated Archive** fields.  
See [Unassociated Archives Tab Fields](#) on page 156.
13. Click **OK** to add the configuration to the **Unassociated Archives** table.
14. Do one of the following:
  - Repeat steps 10-12 to configure additional Enterprise Vault Stores.
  - Continue with the next step.
15. (Optional) On a tab, do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Enterprise Vault Servers Tab Fields

Servers must be entered on this tab before you can configure the **Enterprise Vault Stores** tab or the **Unassociated Archives** tabs.

The following table identifies the available fields in the **Enterprise Vault Servers** tab, on the **Enterprise Vault Configuration** page.

See [Configuring for Enterprise Vault](#) on page 154.

### Enterprise Vault Servers Tab Fields

Field	Description
Name	Specifies the friendly name of the server as chosen by the administrator.
Address	Specifies the IP address or host name of the Enterprise Vault Server.
Port	The port number that is used for communication from the Enterprise Vault server to the application Web application server. The default is 9132.

## Enterprise Vault Servers Tab Fields

Field	Description
Locality	(Optional) Lets you choose from a list of existing localities. The server is associated to the location or IP range of nodes. <b>Note:</b> If you want to assign the Enterprise Vault Server or the Enterprise Vault Store a locality, only the Work Managers with that locality are able to collect from the specified archive. Otherwise, leave this field blank so that they can be collected by Work Managers that also have a blank locality.

## Enterprise Vault Stores Tab Fields

The Enterprise Vault Store holds logical containers that are configured on an Enterprise Vault server against which you would like to perform collections. For each record that you configure and add, you must specify the **Vault Store ID**. You can get the Vault Store ID from the **General** tab on the **Vault Store Properties** dialog box within the Enterprise Vault Administration Console.

The following table identifies the available fields in the **Enterprise Vault Stores** tab, on the **Enterprise Vault Configuration** page.

See [Configuring for Enterprise Vault](#) on page 154.

### Enterprise Vault Stores Tab Fields

Field	Description
Name	Specifies the friendly name of the server as chosen by the administrator.
VaultStore ID	You can find the <b>Vault Store ID</b> on the <b>General</b> tab of the Vault Store properties found within the Enterprise Vault Administration Console.
Archive Type	Lets you choose from the following archive types: Exchange Notes (Domino) FileStore
Server	Specifies the Enterprise Vault Server against which you would like to perform collections. The servers in the dropdown list come from the Enterprise Vault Servers tab. See <a href="#">Enterprise Vault Servers Tab Fields</a> on page 155.

## Unassociated Archives Tab Fields

You can individually add the archives stored on an Enterprise Vault server against which you would like to perform collections.

For each record that you configure and add, you must specify the Archive ID. You can get the Archive ID from the **Advanced** tab of the **Archive Properties** dialog box within the Enterprise Vault Administration Console.

The following table identifies the available fields in the **Unassociated Archives** tab, on the **Enterprise Vault Configuration** page.

See [Configuring for Enterprise Vault](#) on page 154.

### Unassociated Archives Tab Fields

Field	Description
Name	Specifies the friendly name of the server as chosen by the administrator.
Archive ID	Specifies the necessary Archive ID.
Archive Type	Lets you choose from the following archive types: Exchange Notes (Domino) FileStore
Server	Specifies the Enterprise Vault Server against which you would like to perform collections. The servers in the drop-down list come from the Enterprise Vault Servers tab. See <a href="#">Enterprise Vault Servers Tab Fields</a> on page 155.
Internal Location	This field only applies to FileStore archives. It enables the collection of a specific sub-directory found within a FileStore when it is not prudent to collect the entire archive. The values you specify should be formatted as folder paths relative to the parent archive file. For example, if you wanted to only collect Brad Jones's documents out of the specified archive, you would enter the directory path to the files such as the following: /bjones/docs/ As long as the path exists within the archive, the files within that folder are correctly configured for future collections.

# Configuring for a Documentum Server




You can configure the application for EMC Documentum, a solution for capturing, organizing, storing, and delivering unstructured content within an enterprise.

Once you have configured the application to collect from your Documentum server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, you can select **Documentum** as an option in the **Other Data Sources** pane. At that point, a Documentum page appears in the left pane. You can then select the Documentum servers from which you want to collect.

See [Adding a Job](#) on page 426.

See [Documentum Collections Options](#) on page 475.

## To configure the application to collect from Documentum

1. On the *Data Sources* page, click **Documentum**.
2. Click  **Add**.
3. In the **Details** pane, set each field.  
See [Documentum Configuration Fields](#) on page 158.
4. Click **OK** to add the configuration to the table.
5. Do one of the following:
  - Repeat steps 2-4 to configure additional Documentum repositories.
  - Continue with the next step.
6. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Documentum Configuration Fields

The following table describes the parameters that you can set when you are configuring the application to collect from a Documentum repository.

See [Documentum Collections Options](#) on page 475.

### Documentum Configuration Fields

Parameter	Description
Repository Name	Name of the Documentum repository from which the application can collect. (case-sensitive)
Locality	Specifies the location of the Documentum repository.
Server	Sets the URL for the instance of the Documentum Web service. The URL is required to communicate with the Documentum server.

## Documentum Configuration Fields

Parameter	Description
Port	Provides the port number that is used for communication.
Domain	This field is not mandatory.
Username	Specifies the user name to access the Documentum repository. (case-sensitive)
Password	Specifies the user's password for access to the Documentum repository. (case-sensitive)

# Configuring for a SharePoint Server

You can configure the application to perform collections on Microsoft SharePoint 2013, 2010 and 2007 servers by using the **Job Wizard**. The SharePoint connector can collect from document libraries, wikis, blogs, calendars, contacts, announcements, surveys, and discussion boards on team and individual sites.

Once you have configured the application to collect from your SharePoint server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, you can select **SharePoint** as an option in the **Other Data Sources** pane. At that point, a SharePoint page appears in the left pane. You can then select the SharePoint servers from which you want to collect.




See [Adding a Job](#) on page 426.

Considerations when configuring the application for a SharePoint Server:

- If you want to specify the locality of a SharePoint server, only the Work Managers with that locality can collect from the specified SharePoint server. You may want to leave the Locality field empty so that it can be collected by Work Managers that also have a blank locality.
- For the application to collect data from a given SharePoint server, you must make sure that you give the AccessData Service Account full read-only permissions to specific SharePoint servers.
- If you want to perform keyword searching on data collected from a SharePoint Server, you must configure an index server. The index server must have FrontPage server extensions. The Search Service also needs to be running in order to perform the searches.
- You must ensure that the username/password combination for the SharePoint site that you add has credentials to access all sub-sites of the SharePoint site added. Specifically, you need to at least have Read Access in the Web App Policy for the user given. Otherwise the Collection Service will not be able to collect from these sub-sites and will sit in *Waiting For Retry* status waiting to connect and collect from these sub-sites.

See [Setting Service Account Permissions for a SharePoint Server](#) on page 161.

## To configure the application to collect from SharePoint

1. On the *Data Sources* page, click **SharePoint**.
2. Click  **Add**.
3. In the **SharePoint Details** pane, set each field.
4. See [SharePoint Details Fields](#) on page 161.
5. Click **OK** to add the configuration to the **SharePoint Web Applications** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional SharePoint Web Applications.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.



## SharePoint Details Fields

The following table describes the fields that are available in the **SharePoint Details** dialog box.

See [Configuring for a SharePoint Server](#) on page 160.

### SharePoint Details Fields

Field	Description
Web Application URL	<p>Lets you specify the URL of the Web application.</p> <p>The value of this field is typically be formatted as the following: <b>http://&lt;address&gt;:&lt;port&gt;</b> where &lt;address&gt; is the host name or IP address of the system hosting the SharePoint Web Application. You can optionally use the &lt;port&gt; address if you are connecting to a specific SharePoint web application. If you provide a URL that does not specify the port, port 80 is used.</p> <p>If you specify a root path, such as <b>http://server_name/</b>, when you run the <b>Collection Wizard</b>, you can select SharePoint site URLs that may exist within sub sites off of the root path. For example, you could include URLs of any blogs, discussion boards, document libraries, or wikis within the specified root path.</p> <p>If you specify a SharePoint path to a particular organization's department, you can include the blogs, discussion boards, document libraries, or wikis just within that department site. For example, the path may look like <b>http://server_name/sites/marketing</b>.</p>
Locality	(Optional). Lets you type the name of the desired locality to associate this server to a specific location or IP range of nodes.
Domain	(Optional) If the user account entered in the Username field is a domain user account, the domain must be specified; otherwise leave this field blank.
Username	<p>Lets you specify the username of an account that is granted Full Read access to SharePoint.</p> <p>See <a href="#">Setting Service Account Permissions for a SharePoint Server</a> on page 161.</p>
Password	Lets you set the current password of the provided user account.

## Setting Service Account Permissions for a SharePoint Server

For the application to collect data from a given SharePoint server, you must make sure that you give the AccessData Service Account full read-only permissions to specific SharePoint servers.

See [Configuring for a SharePoint Server](#) on page 160.

### To set AccessData Service Account permissions for a SharePoint server

1. On the Windows **Start** menu, click **Administrative Tools > SharePoint 3.0 Central Administration**.
2. On the **Central Administration** page, click the **Application Management** tab.
3. On the **Application Management** page, under **Application Security**, click **Policy for Web Application**.
4. On the toolbar of the **Policy for Web Application** page, in the **Web Application** field, make sure that the correct Web application path and port number is shown.  
If the Web application for which you want to set policy for users is not shown, click **Change Web Application** and select the Web application that you want.
5. On the toolbar, click **Add Users**.

6. On the **Add Users** page, click **Next**.
7. In the **Choose Users** section, in the **Users** box, add the domain\username path.  
Optionally, you can click the check mark icon below the **Users** box to validate the path.
8. In the **Choose Permissions** section, check **Full Read - Has full read-only access**.
9. Click **Finish**. The AccessData Service Account now has the correct permissions set so that you can perform a collection on the specified SharePoint server.
10. Repeat the steps for each Web application whose data you want to collect.

# Configuring for Web Sites

## About Collecting Files from Websites

You can configure the application to collect files from websites.

Once you have configured the application to collect from websites, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, you can select **Website** as an option in the **Other Data Sources** pane. At that point, a Website page appears in the left pane. You can then select which website from which you want to collect.

See [Adding a Job](#) on page 426.

See [Website Collection Options](#) on page 490.

---

**Note:** In order to collect from websites, you need to install the Microsoft SQL Server Compact 3.5 Service Pack 2 for Windows. You can find this service pack at <http://www.microsoft.com/en-us/download/details.aspx?id=5783>. Make sure that BOTH 32-bit and 64-bit versions of the SQLCE are installed on a 64-bit systems. Only the 32-bit version needs to be installed on a 32-bit system. This needs to be done for every work manager you have, in addition to your desktop install.

---

You can use one of the following options:




### Websites that you can collect from

Type	Description
General	<p>You can use this option to collect files from your website. It will collect the following files:</p> <ul style="list-style-type: none"><li>• html</li><li>• cs</li><li>• icon</li><li>• gif</li><li>• png</li><li>• jpeg</li><li>• jpg</li><li>• css</li></ul> <p>You can configure how many files you collect based on the following settings:</p> <ul style="list-style-type: none"><li>• Maximum file size</li><li>• How deep you go from the main index.html based on the number of links. For example, some pages may be viewable only after clicking six different links starting from the home page. You can specify how many links you want to “crawl”.</li></ul> <p><b>Note:</b> You can customize settings to collect additional file types, such as PDF, ISO, and ZIP files. Contact AccessData’s support for more information.</p>

## Collecting from Websites

### To Configure the application to Collect From Websites

1. On the *Data Sources* page, click **Websites**.

2. Click  **Add**.
3. In the **Details** pane, set each field.
4. See [Website Details Fields](#) on page 164.
5. Click **OK** to add the configuration to the **Websites** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional websites.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Website Details Fields

The following table describes the fields that are available in the **Websites Details** dialog box.

See [Configuring for Web Sites](#) on page 163.

### Website Details Fields

Field	Description
Name	Name of the website that will appear in the Job Wizard.
Locality	(Optional). Lets you type the name of the desired locality to associate this server to a specific location or IP range of nodes.
Address	Specify the URL of the website that you are collecting from. For example: <code>http://wikipedia.org</code>
Throttling Delay (MS)	(Optional) Lets you specify a throttling delay when collecting files from general websites. Some Web servers may limit access when many files are being copied from it. You can use the setting to put a delay between copying each file. The setting is in milliseconds.
Depth	This specifies how deep in the Web files the collection will go. You specify the number of links from the home page that you want to "crawl".
Max File Size (MB)	The specified the maximum size of a file that is collected. You specify the size in MB.
User Credentials	When collecting public files from a public website, no credential are required. If you are collecting files from a Web server that has credentials, only Windows credentials are supported, not forms authentication.
Password	Lets you set the current password of the provider user account.

# Configuring for a DocuShare Server

You can configure the application to collect data from Xerox DocuShare.




Once you have configured the application to collect from your DocuShare server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **DocuShare** as an option in the **Other Data Sources** pane. At that point, a *Docushare* page appears in the left pane. You can then specify what to collect from the DocuShare server.

See [DocuShare Collection Options](#) on page 477.

You can collect the following entity types:

- File
- Bulletin
- Email
- Mail Messages
- Blog
- Wiki

## To configure settings for collecting DocuShare data

1. On the *Data Sources* page, click **DocuShare**.
2. Click  **Add**.
3. In the **Details** pane, set each field.
4. See [DocuShare Repository Details Fields](#) on page 165.
5. Click **OK** to add the configuration to the **DocuShare Repository Details** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional DocuShare Repository server.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## *DocuShare Repository Details Fields*

The following table describes the fields that are available in the **DocuShare Repository Details** dialog box.

See [Configuring for a DocuShare Server](#) on page 165.

### DocuShare Repository Fields

Field	Description
Name	Name of the website from which AD the application can collect.
Locality	(Optional). Lets you type the name of the desired locality to associate this server to a specific location or IP range of nodes.
Address	The URL of the server. You can specify an IP address or computer name. For example, http://10.10.4.49
Port	Provides the port number that is used for communication. Typically the port is 8080.
DocuShare Root	Provides the root folder. Typically, this is /docushare.
Domain	This field is not mandatory.
Username	Specifies the user name to access the DocuShare repository.
Password	Specifies the user's password for access to the DocuShare repository.

# Configuring for Cloud Mail

You can configure the application to collect data from a cloud mail server, such as Yahoo! Mail. For collecting Gmail, use the Gmail connector.

Once you have configured the application to collect from your cloud mail server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Person's Cloud Mail** as an option under **People** in the **Custom Selection** pane. At that point, a *People* page appears in the left pane. You can then specify what to collect from the Cloud Mail server.




See [Cloud Mail Server Details Fields](#) on page 167.

---

**Note:** Make sure to configure your firewall to allow traffic to and from your cloud server. Failure to do so will generate errors.

---

## To configure settings for collecting data from a cloud server

1. On the *Data Sources* page, click **Cloud Mail**.
2. Click  **Add**.
3. In the **Details** pane, set each field.
4. See [Cloud Mail Server Details Fields](#) on page 167.
5. Click **OK** to add the configuration to the **Cloud Mail** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional cloud servers.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Cloud Mail Server Details Fields

The following table describes the fields that are available in the Cloud Mail Server Details dialog box. Information to complete these fields can be provided by the cloud mail server host.

### Cloud Mail Server Details Fields

Field	Description
Name	Name of the cloud mail server from which the application can collect.
Connection Type	Specify whether the connection to the cloud mail server is either POP or IMAP.
Address	The URL of the cloud server. You can specify an IP address or computer name. For example, <code>http://imap-ssl.mail.yahoo.com</code>

### Cloud Mail Server Details Fields

Field	Description
Port	Provides the port number that is used for communication.
Encryption Type	Your cloud mail server may require a secure connection (SSL) or other encryption. Choose between None, SSL, TLS, or Auto.
Locality	(Optional). Lets you type the name of the desired locality to associate this server to a specific location or IP range of nodes.
Password	Lets you set the current password of the provided user account.



# Configuring for a OpenText ECM Server




You can configure the application to collect data from OpenText ECM.

Once you have configured the application to collect from your OpenText ECM server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, you can select **OpenText ECM** as an option in the **Other Data Sources** pane. At that point, a OpenText ECM page appears in the left pane. You can then select which OpenText ECM repository from which you want to collect.

See [Adding a Job](#) on page 426.

See [OpenText ECM Collection Options](#) on page 486.

## To configure settings for collecting OpenText ECM data

1. On the *Data Sources* page, click **OpenText ECM**.
2. Click  **Add**.
3. In the **Details** pane, set each field.
4. See [OpenText ECM Repository Details Fields](#) on page 169.
5. Click **OK** to add the configuration to the **OpenText ECM Repository** Details table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional OpenText ECM Repository servers.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## OpenText ECM Repository Details Fields

The following table describes the fields that are available in the **OpenText ECM Repository Details** dialog box.

### OpenText ECM Repository Details Fields

Field	Description
Url	Specifies the URL for the OpenText ECM Content Server.
Username	Specifies the username for the OpenText ECM Content Server.
Password	Specifies the password for the OpenText ECM Content Server.

# Configuring for Gmail

You can configure the application to collect data from Gmail. If you want to collect from a cloud mail server other than Gmail, you can use the Cloud Mail connector.

Once you have configured the application to collect from your Gmail, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **People > Select Person's Gmail** as an option in the **Custom Selection** pane.

See [Configuring for Cloud Mail](#) on page 167.

---


**Note:** Make sure to configure your firewall to allow traffic to and from your Gmail server. Failure to do so will generate errors.

---

Before the application can be configured to collect data from Gmail, important information from Google must be obtained. This information is obtained by the following steps:

- 8.
9. create an api project and client id

## To configure settings for collecting Gmail

1. On the *Data Sources* page, click **Gmail**.
2. Click  **Add**.
3. In the **Details** pane, set the following fields:
  - **Domain**
  - **Google API Client ID** - this is the Client ID obtained when creating the API project. See above for more information.
  - **Google API Client Secret** - this is the Client Secret obtained when creating the API project. See above for more information.
4. Click **OK** to add the configuration to the **Gmail Details** table.
5. Click the **Google** button to authorize Gmail access.
6. Google's dialog will appear, asking permission to access the domain's collector. Click **Allow access**.
7. Copy the key provided by Google, and paste it into the Authorization Code field.
8. Click **Ok**.

# Configuring for Google Drive

You can configure the application to collect all of the Google docs from a Google drive.




**Important:** Google Drive 2 is currently supported. Google Drive 1 is no longer supported

Once you have configured the application to collect from your Google Drive, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Google Drive** as an option in the **Other Data Sources** pane. At that point, a *Google Drive* page appears in the left pane. You can then select from which Google Drive to collect.

See [Adding a Job](#) on page 426.

## Configuring for Google Drive

### To configure the application for Google Drive

1. On the *Data Sources* page, click **Google Drive**.
2. Click  **Add**.
3. In the **Details** pane, set the fields.
4. See [Google Drive Details Fields](#) on page 171.
5. Click **OK** to add the configuration to the **Google Drive** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional Google Drive sites.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Google Drive Details Fields

The following table describes the fields that are available in the **Google Drive Details** dialog box.

See [Configuring for Google Drive](#) on page 171.

### Google Drive Details Fields

Field	Description
Name	Specifies the name which will appear in the Job Wizard.
Username	Specifies the username of the Google drive.
Password	Specifies the password of the Google drive.

# Configuring for Druva

You can configure the application to collect data from your Druva endpoint backup solution.

You need to be aware of the following considerations when configuring the application to attach to a Druva server:

- In 6.0.1 and higher, files greater than 4GB are now supported.
- In 6.0.1 and higher, the connector path no longer requires an SSL UNC path but now uses an HTTP address.
- In 6.0.1 and higher, Site Server is no longer a required component for using the Druva connector.
- The application uses the WebDAV protocol and is case-sensitive.
- Microsoft limits WebDAV to a maximum file size of 50 MB that can be downloaded. This limit is imposed to protect the system from a Denial of Service (DOS) attack. In order to change the file size, follow the instructions found at <http://support.microsoft.com/kb/900900>.

---

**Note:** Files that exceeded the WebDAV limit are not collected. If attempting to collect a file larger than the limit, an error from Site Server occurs, stating “Unable to access.”

---




Once you have configured the application to collect from your Druva server, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Druva** as an option in the **Other Data Sources** pane. At that point, a *Druva* page appears in the left pane. You can then select from which Druva server to collect.

See [Adding a Job](#) on page 426.

See [Druva Collection Options](#) on page 491.

## Configuring for Druva

### To configure the application for Druva

1. On the *Data Sources* page, click **Druva**.
2. Click  **Add**.
3. In the **Details** pane, set the fields.
4. See [Druva Details Fields](#) on page 173.
5. Click **OK** to add the configuration to the **Druva** table.
6. Do one of the following:
  - Repeat steps 2-4 to configure additional Druva servers.
  - Continue with the next step.
7. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Druva Details Fields

The following table describes the fields that are available in the **Druva Details** dialog box.

### Druva Details Fields

Field	Description
Name	Specifies the name of the Druva server to which you are connecting. This name must be exact because the connector is case-sensitive.
Path	Specifies the path to the Druva server. This path must be a SSL UNC path. For example, \\Druva-InSync.lab.local@SSL\webdav\TestLegalHold.
Locality	Specifies the location of the Druva server.
Username	Specifies the name of the user from the Druva server.
Password	Specifies the password needed to collect from the repository.

# Configuring for a CMIS Repository

You can configure the application to collect data from your content management systems through CMIS (Content Management Interoperability Services). You connect to the various content management systems by connecting to a CMIS server. Once you connect to the CMIS server, you can select the specific repository or repositories (For example a Documentum or FileNet data source) from which to collect.

You can upload a custom filter for the CMIS repository. See [Custom Filters for CMIS](#) on page 175.




When you have configured the application to collect from your CMIS repository, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **CMIS Repository** as an option in the **Other Data Sources** pane. At that point, a *CMIS Repository* page appears in the left pane. You can then select from which CMIS repository to collect.

See [Adding a Job](#) on page 426.

See [CMIS Repository Details Fields](#) on page 174.

## Configuring for a CMIS Repository

### To configure the application for a CMIS repository

1. On the *Data Sources* page, click **CMIS Repository**.
2. Click  **Add**.
3. In the **Details** pane, set the fields.
4. See [CMIS Repository Details Fields](#) on page 174.
5. Click **Connect** to retrieve repositories for the newly created CMIS configuration. You must have the **URL**, **Username**, and **Password** fields populated in order to retrieve repositories.
6. Select a repository from the dropdown list. These repositories are the individual data sources, such as a Documentum or FileNet data source.
7. Click **OK** to add the configuration to the **CMIS Repository** table.
8. Do one of the following:
  - Repeat steps 2-4 to configure additional CMIS servers.
  - Continue with the next step.
9. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## CMIS Repository Details Fields

The following table describes the fields that are available in the **CMIS Repository Details** dialog box.

## CMIS Repository Details

Field	Description
Url	Specifies the URL of the CMIS repository.
Username	Specifies the username for the CMIS repository drive.
Password	Specifies the password for the CMIS repository drive.
Protocol Binding	Specifies whether the repository deploys either Atom Publishing or Web Services.
Connect	Allows you to connect to the CMIS repository. If the connection is unsuccessful, a dialog appears warning you of the error. <b>Note: You must populate the URL, Username, and Password in order to connect to the CMIS repository.</b>
Select Repository	Allows you to select which specific repository from which to collect data. This dropdown does not populate until you have connected to the CMIS repository.

## Custom Filters for CMIS

You can upload a custom filter that applies to the data gathered from CMIS. The filter should be written in XML, and a sample XML filter is available for download from the *Upload Custom Filter* dialog found on the configuration page.

Any custom filters uploaded will be applied to all configured CMIS repositories. The custom filter can be combined with the Job Wizard filters. The custom filter in combination with the *Job Wizard* filters acts as an OR operator, not an AND. This means that a piece of collected data will match either the *Job Wizard* Filters or the Custom filters, but the data does not have to match both filters concurrently.

A sample of the correct syntax and how to write a custom CMIS filter can be found below.


## Example of Custom Filter for CMIS

```

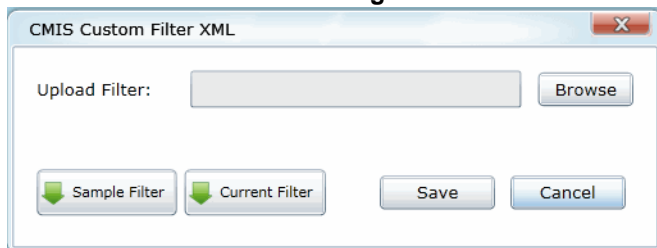
<?xml version="1.0"?>
<!-- General Structure -->
<!--
*****
SourceField - Field/Attribute to be searched on Values - Value to searched Criterion | Operator
_____ | _____ StringCriterion | Contains, DoesNotContain ValueCriterionOfInt64 |
Equals, NotEquals, LessThan, GreaterThan, (Value2 ignored for operators Equals, NotEquals, LessThan, GreaterThan)
ValueRangeCriterionOfInt64 | Between, OutsideOf ValueCriterionOfDateTime | Equals, NotEquals, LessThan, GreaterThan,
(Value2 ignored for operators Equals, NotEquals, LessThan, GreaterThan) Format: ISO8601 ValueRangeCriterionOfDateTime |
Between, OutsideOf Format: ISO8601 Note: Criterion within a filter are ANDed. The results of multiple filters are ORed.
*****
-->
<!-- A CMIS Job Filter Example -->
<CMISJobFilter xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  - <InclusionCriteria>
    - <CMISCriteria>
      <FilterName>Example XML Filter</FilterName>
      - <UserDefinedCriteria>
        <!-- Example filtering on String value in the 'Color' Column -->
        - <Udc>
          - <Criterion xsi:type="StringCriterion">
            - <Values>
              <string>Red</string>
            </Values>
            <Operator>DoesNotContain</Operator>
            <!-- Contains, DoesNotContain -->
          </Criterion>
          <SourceField>Color</SourceField>
        </Udc>
        <!-- Example filtering on Integer value in the 'Box Number' Column. -->
        <!-- ValueCriterionOfInt64 and ValueRangeCriterionOfInt64 should not be used together -->
        - <Udc>
          - <Criterion xsi:type="ValueCriterionOfInt64">
            <Value>10</Value>
            <Operator>NotEquals</Operator>
            <!-- Equals, NotEquals, LessThan, GreaterThan -->
          </Criterion>
          <SourceField>Box_x0020_Number</SourceField>
        </Udc>
        <!-- Example filtering on Integer Range in the 'Box Number' Column. -->
        <!-- ValueCriterionOfInt64 and ValueRangeCriterionOfInt64 should not be used together -->

```

### To upload a custom filter

1. Go to **Data Sources > CMIS Repository**.
2. Click  **Upload Custom Filter**.

### CMIS Custom Filter XML Dialog



3. Browse to the location where you have saved the custom XML filter.
4. (optional) Click **Sample Filter** to download a copy of a custom XML filter.
5. (optional) Click **Current Filter** to view the current filter uploaded to the system.
6. Click **Save**.



# Configuring for Box

You can configure the application to collect the data from your Box cloud storage system.

Once you have configured the application to collect from your Box cloud storage system, you can choose to collect from this source with a collection job. In the **Job Wizard > Job Options**, select **Box** as an option in the **Other Data Sources** pane. At that point, a *Box* page appears in the left pane. You can then select from which Box system to collect.

See [Adding a Job](#) on page 426.

## Creating a Box Application

Before the application can be configured to collect data from Box, you must create a Box application on the Box website:

### To create a Box application

1. Log in to <https://developers.box.com> with appropriate administrator permissions.
2. Select **My Apps**.
3. Under *Applications*, select **Create a Box Application**.
4. In the field provided, name the Box application.
5. Click the **Box Content** radio button and click **Create Application**.
6. At the *Success!* window, click **Configure your application**.
7. Scroll down to the *OAuth2 Parameters* pane. Record the `client_id`, `client_secret`, and `redirect_uri`. You need this information in order to configure the application.

---

**Note:** The `redirect_uri` must be <https> and include the IP address or server name (if DNS is enabled) as the application's server. It is recommended that the path component (For example, `/BoxRedirect` in `https://10.10.200.27/BoxRedirect`) be a unique name, such as company name, pet name, etc. If the additional path component is not provided, when the eDiscovery application posts a listen on that uri, it may conflict with another application listening on port 443 on the server.


---

8. Note the information in the API Key and Redirect url fields under *Backend Parameters*. Make sure that Redirect url matches the `redirect_uri`.
9. Select **Save Application**. The newly created Box application should appear in the *My Applications* page.

## Configuring for Box Application

After a Box application has been created on the Box website, you need to configure the application to connect to the Box application.

### To configure the application for Box Application



1. On the *Data Sources* page, click **Box**.
2. Click  **Add**.

3. In the **Details** pane, set the fields.  
See [Box Details Fields](#) on page 178.
4. Click **Authorize**.
5. In the pop-up window, enter the administrator's credentials that you used to login to developers.box.com.
6. Click **Authorize**.
7. In the following window, click **Grant access to Box**.
8. A *There is a problem with this website's security certificate* page may appear. If so, click **Continue to this website (not recommended)**.
9. Close the **You have successfully connected to the Box!** window.
10. Click the **OK** button on the *Box Details* pane.

---

**Note:** You must click the OK button within 30 seconds of closing the You have successfully connected to the Box! window. If not, the window will time out and you will get an http error 400 Bad Request. For more information, see <https://developers.box.com/oauth/>.

---

11. (Optional) Do any of the following:
  - Click  **Edit** to edit the parameters of a given configuration.
  - Click  **Delete** to delete a configuration.

## Box Details Fields

The following table describes the fields that are available in the **Box Details** dialog box.

See [Configuring for Box Application](#) on page 177.

### Box Details Fields

Field	Description
Box Name	Specifies the name which will appear in the Job Wizard.
Box Client ID	Specifies the client ID of the Box application. Enter the data you recorded from creating the Box application. See <a href="#">Creating a Box Application</a> on page 177.
Box Client Secret	Specifies the client secret of the Box application. Enter the data you recorded from creating the Box application. See <a href="#">Creating a Box Application</a> on page 177.
Box Redirect Url	Specifies the redirect Url of the Box application. Enter the data you recorded from creating the Box application. See <a href="#">Creating a Box Application</a> on page 177.

## Chapter 14

# Getting Started with KFF (Known File Filter)

---

This document contains the following information about understanding and getting started using KFF (Known File Filter).

- [About KFF](#) (page 179)
- [About the KFF Server and Geolocation](#) (page 184)
- [Installing the KFF Server](#) (page 185)
- [Configuring the Location of the KFF Server](#) (page 187)
- [Migrating Legacy KFF Data](#) (page 188)
- [Importing KFF Data](#) (page 189)
- [About CSV and Binary Formats](#) (page 196)
- [Installing KFF Updates](#) (page 200)
- [Uninstalling KFF](#) (page 199)
- [KFF Library Reference Information](#) (page 201)
- [What has Changed in Version 5.6](#) (page 206)

**Important:** AccessData applications versions 5.6, 6.0, and later use a new KFF architecture. If you are using one of the following applications version 5.6 or later, you must install and implement the new KFF architecture:

- FTK-based products (FTK, FTK Pro, AD Lab, AD Enterprise)
- Summation
- eDiscovery

See [What has Changed in Version 5.6](#) on page 206.

## About KFF

KFF (Known File Filter) is a utility that compares the file hash values of known files against the files in your project. The known files that you compare against may be the following:

- Files that you want to ignore, such as operating system files
- Files that you want to be alerted about, such as malware or other contraband files

The hash values of files, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension. This helps you identify files even if they are renamed.

Using KFF during your analysis can provide the following benefits:

- Immediately identify and ignore 40-70% of files irrelevant to the project.
- Immediately identify known contraband files.

## Introduction to the KFF Architecture

There are two distinct components of the KFF architecture:

- **KFF Data** - The KFF data are the hashes of the known files that are compared against the files in your project. The KFF data is organized in KFF Hash Sets and KFF Groups. The KFF data can be comprised of hashes obtained from pre-configured libraries (such as NSRL) or custom hashes that you configure yourself.  
See [Components of KFF Data](#) on page 180.
- **KFF Server** - The KFF Server is the component that is used to store and process the KFF data against your evidence. The KFF Server uses the AccessData Elasticsearch Windows Service. After you install the KFF Server, you import your KFF data into it.

---

**Note:** The KFF database is no longer stored in the shared evidence database or on the file system in EDB format.

---

## Components of KFF Data

Item	Description
<b>Hash</b>	The unique MD5 or SHA-1 hash value of a file. This is the value that is compared between known files and the files in your project.
<b>Hash Set</b>	A collection of hashes that are related somehow. The hash set has an ID, status, name, vendor, package, and version. In most cases, a set corresponds to a collection of hashes from a single source that have the same status.
<b>Group</b>	KFF Groups are containers that are used for managing the Hash Sets that are used in a project.  KFF Groups can contains Hash Sets as well as other groups.  Projects can only use a single KFF Group. However, when configuring your project you can select a single KFF Group which can contains nested groups.
<b>Status</b>	The specified status of a hash set of the known files which can be either Ignore or Alert. When a file in a project matches a known file, this is the reported status of the file in the project.
<b>Library</b>	A pre-defined collection of hashes that you can import into the KFF Serve. There are three pre-defined libraries: <ul style="list-style-type: none"><li>• NSRL</li><li>• NDIC HashKeeper</li><li>• DHS</li></ul> See <a href="#">About Pre-defined KFF Hash Libraries</a> on page 182.

Item	Description
<b>Index/Indices</b>	<p>When data is stored internally in the KFF Library, it is stored in multiple indexes or indices.</p> <p>The following indices can exist:</p> <ul style="list-style-type: none"> <li>● NSRL index A dedicated index for the hashes imported from the NSRL library.</li> <li>● NDIC index A dedicated index for the hashes imported from the NDIC library.</li> <li>● DHC index A dedicated index for the hashes imported from the DHC library.</li> <li>● KFF index A dedicated index for the hashes that you manually create or import from other sources, such as CSV.</li> </ul> <p>These indices are internal and you do not see them in the main application. The only place that you see some of them are in the KFF Import Tool.</p> <p>See <a href="#">Using the KFF Import Utility</a> on page 190.</p> <p>The only time you need to be mindful of the indices is when you use the KFF binary format when you either export or import data.</p> <p>See <a href="#">About CSV and Binary Formats</a> on page 196.</p>

## About the Organization of Hashes, Hash Sets, and KFF Groups

Hashes, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension.

You can also import hashes into the KFF Server in **.CSV** format.

For FTK-based products, you can also import hashes into the KFF Server that are contained in **.TSV**, **.HKE**, **.HKE.TXT**, **.HDI**, **.HDB**, **.hash**, **.NSRL**, or **.KFF** file formats.

You can also manually add hashes.

Hashes are organized into Hash Sets. Hash Sets usually include hashes that have a common status, such as Alert or Ignore.

Hash Sets must be organized into to KFF Groups before they can be utilized in a project.

## About Pre-defined KFF Hash Libraries

All of the pre-configured hash sets currently available for KFF come from three federal government agencies and are available in KFF libraries.

See [About KFF Pre-Defined Hash Libraries](#) on page 201.

You can use the following KFF libraries:

- NIST NSRL  
See [About Importing the NIST NSRL Library](#) on page 193.
- NDIC HashKeeper (Sept 2008)  
See [Importing the NDIC Hashkeeper Library](#) on page 194.
- DHS (Jan 2008)  
See [Importing the DHS Library](#) on page 195.

It is not required to use a pre-configured KFF library in order to use KFF. You can configure or import custom hash sets. See your application's *Admin Guide* for more information.

## How KFF Works

The Known File Filter (KFF) is a body of MD5 and SHA1 hash values computed from electronic files. Some pre-defined data is gathered and cataloged by several US federal government agencies or you can configure your own. KFF is used to locate files residing within project evidence that have been previously encountered by other investigators or archivists. Identifying previously cataloged (known) files within a project can expedite its investigation.

When evidence is processed with the MD5 Hash (and/or SHA-1 Hash) and KFF options, a hash value for each file item within the evidence is computed, and that newly computed hash value is searched for within the KFF data. Every file item whose hash value is found in the KFF is considered to be a known file.

---

**Note:** If two hash sets in the same group have the same MD5 hash value, they must have the same metadata. If you change the metadata of one hash set, all hash sets in the group with the same MD5 hash file will be updated to the same metadata.

---

The KFF data is organized into Groups and stored in the KFF Server. The KFF Server service performs lookup functions.

## Status Values

In order to accelerate an investigation, each known file can be labeled as either Alert or Ignore, meaning that the file is likely to be forensically interesting (Alert) or uninteresting (Ignore). Other files have a status of Unknown.

The Alert/Ignore designation can assist the investigator to hone in on files that are relevant, and avoid spending inordinate time on files that are not relevant. Known files are presented in the Overview Tab's File Status Container, under "KFF Alert files" and "KFF Ignorable."

## Hash Sets

The hash values comprising the KFF are organized into hash sets. Each hash set has a name, a status, and a listing of hash values. Consider two examples. The hash set “ZZ00001 Suspected child porn” has a status of Alert and contains 12 hash values. The hash set “BitDefender Total Security 2008 9843” has a status of Ignore and contains 69 hash values. If, during the course of evidence processing, a file item’s hash value were found to belong to the “ZZ00001 Suspected child porn” set, then that file item would be presented in the KFF Alert files list. Likewise, if another file item’s hash value were found to belong to the “BitDefender Total Security 2008 9843” set, then that file would be presented in the KFF Ignorable list.

In order to determine whether any Alert file is truly relevant to a given project, and whether any Ignore file is truly irrelevant to a project, the investigator must understand the origins of the KFF’s hash sets, and the methods used to determine their Alert and Ignore status assignments.

You can install libraries of pre-defined hash sets or you can import custom hash sets. The pre-defined hash sets contain a body of MD5 and SHA1 hash values computed from electronic files that are gathered and cataloged by several US federal government agencies.

See [About KFF Pre-Defined Hash Libraries](#) on page 201.

## Higher Level Structure and Usage

Because hash set groups have the properties just described, and because custom hash sets and groups can be defined by the investigator, the KFF mechanism can be leveraged in creative ways. For example, the investigator may define a group of hash sets created from encryption software and another group of hash sets created from child pornography files and then apply only those groups while processing.

# About the KFF Server and Geolocation

In order to use the Geolocation Visualization feature in various AccessData products, you must use the KFF architecture and do the following:

- Install the KFF Server.  
See [Installing the KFF Server](#) on page 185.
- Install the Geolocation (GeoIP) Data (this data provide location data for evidence)  
See [Installing the Geolocation \(GeoIP\) Data](#) on page 195.  
From time to time, there will be updates available for the GeoIP data.  
See [Installing KFF Updates](#) on page 200.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.



# Installing the KFF Server

## About Installing the KFF Server

In order to use KFF, you must first install and configure a KFF Server.

For product versions 5.6.x and 6.0.x and later, you install a KFF Server by installing the AccessData Elasticsearch Windows Service.

Where you install the KFF Server depends on the product you are using with KFF:

- For FTK and FTK Pro applications, the KFF Server must be installed on the same computer that runs the FTK Examiner application.
- For all other applications, such as AD Lab, Summation, or eDiscovery, the KFF Server can be installed on either the same computer as the application or on a remote computer. For large environments, it is recommended that the KFF Server be installed on a dedicated computer.

Once the KFF components are installed, they will be accessible via the *Windows Start Menu*, as well as through FTK in the *Manage* menu.

---

**Note:** KFF components will only be available in the *Windows Start Menu* on the computer where they are physically installed.

---

After installing the KFF Server, you configure the application with the location of the KFF Server.

See [Configuring the Location of the KFF Server](#) on page 187.

## About KFF Server Versions

The KFF Server (AccessData Elasticsearch Windows Service) may be updated from time to time. It is best to use the latest version.

AccessData Elasticsearch Windows Service	Released	Installation Instructions
Version 1.3.2.x	<ul style="list-style-type: none"><li>• November 2014 with 5.6 versions of<ul style="list-style-type: none"><li>■ FTK-based products</li><li>■ Summation</li><li>■ eDiscovery</li></ul></li><li>• November 2015 with 6.0 versions of<ul style="list-style-type: none"><li>■ FTK-based products</li><li>■ Summation</li><li>■ eDiscovery</li></ul></li></ul>	See <a href="#">Installing the KFF Server Service</a> on page 186.

For applications 5.5 and earlier, the KFF Server component was version 1.2.7 and earlier.

## About Upgrading from Earlier Versions

If you have used KFF with applications versions 5.5 and earlier, you can migrate your legacy KFF data to the new architecture.

See [Migrating Legacy KFF Data](#) on page 188.

## Process for Installing KFF

The process for installing KFF is as follows:

1. [Downloading the Latest KFF Installation Files](#) (page 186)
2. [Installing the KFF Server Service](#) (page 186)
3. Configuring the KFF Server location:
  - [Configuring the KFF Server Location on FTK-based Computers](#) (page 187)
  - [Configuring the KFF Server Location on Summation and eDiscovery Applications](#) (page 187)
4. (Optional) Upgrading or importing KFF data.
  - See [Migrating Legacy KFF Data](#) on page 188.
  - [About Importing KFF Data](#) (page 189)
  - [Importing Pre-defined KFF Data Libraries](#) (page 192)
  - [Installing the Geolocation \(GeoIP\) Data](#) (page 195)

## Downloading the Latest KFF Installation Files

You can download ISO files which has the latest KFF files. Files may be updated from time to time.

### To download the latest KFF Installation Files

1. Go to the AccessData [Current Releases - Digital Forensics](#) product download page. You can also download the file from the FTK or AD Lab product download pages.
2. Click **Known File Filter (KFF) Compatible with 5.6 and above**.
3. Do one of the following:
  - To download the KFF Server files, utilities, and NSRL data, click **KFF for all 6.0 products**.
  - To download the DHS library, click **KFF DHS**.
  - To download the NDIC library, click **KFF NDIC**.
4. Click **Download Now**.

## Installing the KFF Server Service

The KFF Server Service is install by installing the AccessData Elasticsearch Windows Service

For instructions on installing the AccessData Elasticsearch Windows Service, see [Installing the Elasticsearch Service](#) (page 526).

# Configuring the Location of the KFF Server

After installing the KFF Server, on the computer running the application, such as FTK, AD Lab, Summation, or eDiscovery, you configure the location of the KFF Server.

Do one of the following:

- [Configuring the KFF Server Location on FTK-based Computers](#) (page 187)
- [Configuring the KFF Server Location on Summation and eDiscovery Applications](#) (page 187)

## Configuring the KFF Server Location on FTK-based Computers

Before using KFF with FTK, FTK Pro, Lab, or Enterprise, with KFF, you must configure the location of the KFF Server.

**Important:** To configure KFF, you must be logged in with Admin privileges.

### To view or edit KFF configuration settings

1. In the *Case Manager*, click **Tools > Preferences > Configure KFF**.
2. You can set or view the address of the KFF Server.
  - If you installed the KFF Server on the same computer as the application, this value will be localhost.
  - If you installed the KFF Server on a different computer, identify the KFF server.
3. Click **Test** to validate communication with the KFF Server.
4. Click **Save**.
5. Click **OK**.

## Configuring the KFF Server Location on Summation and eDiscovery Applications

When using the KFF Server with Summation or eDiscovery applications, two configuration files must point to the KFF Server location.

These settings are configured automatically during the KFF Server installation. If needed, you can verify the settings.

However, if you change the location of the KFF Server, do the following to specify the location of the KFF Server.

1. Configure `AdgWindowsServiceHost.exe.config`:
  - 1a. On the computer running the application (for example, the server running Summation), go to `C:\Program Files\AccessData\Common\FTK Business Services`.
  - 1b. Open `AdgWindowsServiceHost.exe.config`.
  - 1c. Modify the line `<add key="KffElasticSearchUrl" value="http://localhost:9200" />`.
  - 1d. Change *localhost* to be the location of your KFF server (you can use hostname or IP).
  - 1e. Save and close file.
  - 1f. Restart the business services common service.
2. Configure `AsyncProcessingServices.web.config`:

- 2a. On the computer running the application (for example, the server running Summation), go to `C:\Program Files\AccessData\AsyncProcessingServices`.
- 2b. Open `web.config`.
- 2c. Modify the line `<add key="KffElasticSearchUrl" value="http://localhost:9200" />`.
- 2d. Change `localhost` to be the location of your KFF server (you can use hostname or IP).
- 2e. Save and close file.
- 2f. Restart the AsyncProcessing service.

## Migrating Legacy KFF Data

If you have used KFF with applications versions 5.5 and earlier, you can migrate that data from the legacy KFF Server to the new KFF Server architecture.

**Important:** Applications version 5.6 and later can only use the new KFF architecture that was introduced in 5.6. If you want to use KFF data from previous versions, you must migrate the data.

**Important:** If you have NSRL, NDIC, or DHS data in your legacy data, those sets will not be migrated. You must re-import them using the 5.6 versions or later of those libraries. Only legacy custom KFF data will be migrated.

Legacy KFF data is migrated to KFF Groups and Hash Sets on the new KFF Server.

Because KFF Templates are no longer used, they will be migrated as KFF Groups, and the groups that were under the template will be added as sub-groups.

You migrate data using the KFF Migration Tool. To use the KFF Migration Tool, you identify the following:

- The Storage Directory folder where the legacy KFF data is located.  
This was folder was configured using the KFF Server Configuration utility when you installed the legacy KFF Server. If needed, you can use this utility to view the KFF Storage Directory. The default location of the `KFF_Config.exe` file is `Program Files\AccessData\KFF`.
- The URL of the new KFF Server (the computer running the AccessData Elastic Search Windows Service)  
This is populated automatically if the new KFF Server has been installed.

### To install the KFF Migration Tool

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the `autorun.exe`.
2. Click the *64 bit* or *32 bit* **Install KFF Migration Utility**.
3. Complete the installation wizard.

### To migrate legacy KFF data

1. On the legacy KFF Server, you must stop the KFF Service.  
You can stop the service manually or use the legacy KFF Config.exe utility.
2. On the new KFF Server, launch the KFF Migration Tool.
3. Enter the directory of the legacy KFF data.
4. The URL of Elasticsearch should be listed.
5. Click **Start**.
6. When completed, review the summary data.

# Importing KFF Data

## About Importing KFF Data

You can import hashes and KFF Groups that have been previously configured.

You can import KFF data in one of the following formats:

### KFF Data sources that you can import

Source	Description
Pre-configured KFF libraries	<p>You can import KFF data from the following pre-configured libraries</p> <ul style="list-style-type: none"><li>• NIST NSRL</li><li>• NDIC HashKeeper</li><li>• DHS</li></ul> <p>To import KFF libraries, it is recommended that you use the KFF Import Utility.</p> <p>See <a href="#">Using the KFF Import Utility</a> on page 190.</p> <p>See <a href="#">Importing Pre-defined KFF Data Libraries</a> on page 192.</p> <p>See <a href="#">KFF Library Reference Information</a> on page 201.</p>
Custom Hash Sets and KFF Groups	<p>You can import custom hashes from CSV files.</p> <p>See <a href="#">About the CSV Format</a> on page 196.</p> <p>For FTK-based products, you can also import custom hashes from the following file types:</p> <ul style="list-style-type: none"><li>• Delimited files (CSV or TSV)</li><li>• Hash Database files (HDB)</li><li>• Hashkeeper files (HKE)</li><li>• FTK Exported KFF files (KFF)</li><li>• FTK Supported XML files (XML)</li><li>• FTK Exported Hash files (HASH)</li></ul> <p>To import these kinds of files, use the KFF Import feature in your application.</p> <p>See <a href="#">Using the Known File Feature</a> chapter.</p>
KFF binary files	<p>You can import KFF data that was exported in a KFF binary format, such as an archive of a KFF Server.</p> <p>See <a href="#">About CSV and Binary Formats</a> on page 196.</p> <p>When you import a KFF binary snapshot, you must be running the same version of the KFF Server as was used to create the binary export.</p> <p>To import KFF binary files, it is recommended that you use the KFF Import Utility.</p> <p>See <a href="#">Using the KFF Import Utility</a> on page 190.</p>

## About KFF Data Import Tools

When you import KFF data, you can use one of two tools:

### KFF Data Import Tools

The application's Import feature	The KFF management feature in the application lets you import both .CSV and KFF Binary formats. Use the application to import .CSV files. See <i>Using the Known File Feature</i> chapter. Even though you can import KFF binary files using the application, it is recommend that you use the KFF Import Utility.
KFF Import Utility	It is recommended that you use the KFF Import Utility to import KFF binary files. See <a href="#">Using the KFF Import Utility</a> on page 190.

## About Default Status Values

When you import KFF data, you configure a default status value of Alert or Ignore. When adding Hash Sets to KFF Groups, you can configure the KFF Groups to use the default status values of the Hash Set or you can configure the KFF Group with a status that will override the default Hash Set values.

See [Components of KFF Data](#) on page 180.

## About Duplicate Hashes

If multiple Hash Set files containing the same Hash identifier are imported into a single KFF Group, the group keeps the last Hash Set's metadata information, overwriting the previous Hash Sets' metadata. This only happens within an individual group and not across multiple groups.

## Using the KFF Import Utility

### About the KFF Import Utility

Due to the large size of some KFF data, a stand-alone KFF Import utility is available to use to import the data. This KFF Import utility can import large amounts of data faster than using the import feature in the application.

It is recommend that you install and use the KFF Import utility to import the following:

- NSRL, DHC, and NIST libraries
- An archive of a KFF Server that was exported in the binary format

After importing NSRL, NDIC, or DHS libraries, these indexes are displayed in the *Currently Installed Sets* list.

See [Components of KFF Data](#) on page 180.

You can also use the KFF Import Utility to remove the NSRL, NDIC, or DHS indexes that you have imported.

An archive of a KFF Server, which is the exported *KFF Index*, is not shown in the list.

## Installing the KFF Import Utility

You should use the KFF Import Utility to import some kinds of KFF data.

### To install the KFF Import Utility

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the `autorun.exe`.
2. Click the *64 bit* or *32 bit* **Install KFF Import Utility**.
3. Complete the installation wizard.

## Importing a KFF Server Archive Using the KFF Import Utility

You can import an archive of a KFF Server that you have exported using the binary format.

If you are importing a pre-defined KFF Library, see [Importing Pre-defined KFF Data Libraries](#) (page 192).

### To import using the KFF Import Utility

1. On the KFF Server, open the KFF Import Utility.
2. To test the connection to the KFF Server's Elasticsearch service at the displayed URL, click **Connect**.  
If it connects correctly, no error is shown.  
If it is not able to connect, you will get the following error: Failed after retrying 10 times: 'HEAD accessdata\_threat\_indicies'.
3. To import, click **Import**.
4. Click **Browse**.
5. Browse to the folder that contains the KFF binary files.  
Specifically, select the folder that contains the `Export.xml` file.
6. Click **Start**.
7. Close the dialog.

## Removing Pre-defined KFF Libraries Using the KFF Import Utility

You can remove a pre-defined KFF Library that you have previously imported.

You cannot see or remove existing custom KFF data (the *KFF Index*).

### To remove pre-defined KFF Libraries

1. On the KFF Server, open the KFF Import Utility.
2. Select the library that you want to remove.
3. Click **Remove**.

## *Importing Pre-defined KFF Data Libraries*

### About Importing Pre-defined KFF Data Libraries

After you install the KFF Server, you can import pre-defined NIST NSRL, NDIC HashKeeper, and DHS data libraries.

See [About Pre-defined KFF Hash Libraries](#) on page 182.

In versions 5.5 and earlier, you installed these using an executable file. In versions 5.6 and later, you must import them. It is recommend that you use the KFF Import Utility.

After importing pre-defined KFF Libraries, you can remove them from the KFF Server.

See [Removing Pre-defined KFF Libraries Using the KFF Import Utility](#) on page 191.

See the following sections:

- [About Importing the NIST NSRL Library](#) (page 193)
- [Importing the NDIC Hashkeeper Library](#) (page 194)
- [Importing the DHS Library](#) (page 195)



## About Importing the NIST NSRL Library

You can import the NSRL library into your KFF Server. During the import, two KFF Groups are created: NSRL\_Alert and NSRL\_Ignore. In FTK-based products, these two groups are automatically added to the Default KFF Group.

The NSRL libraries are updated from time to time. To import and maintain the NSRL data, you do the following:

### Process for Importing and Maintaining the NIST NSRL Library

1. Import the complete NSRL library.	You must first install the most current complete NSRL library. You can later add updates to it. To access and import the complete NSRL library, see <a href="#">Importing the Complete NSRL Library</a> (page 194)
2. Import updates to the library	When updates are made available, import the updates to bring the data up-to-date. See <a href="#">Installing KFF Updates</a> on page 200. <b>Important:</b> In order to use the NSRL updates, you must first import the complete library. When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data.

### Available NRSL library files (new format)

NSRL Library Release	Released	Information
Complete library version 2.45 (source .ZIP file)	Nov 2014	For use only with applications version 5.6 and later. Contains the full NSRL library up through update 2.45. See <a href="#">Importing the Complete NSRL Library</a> on page 194.

### Available Legacy NRSL library files

Legacy NSRL Library Release	Released	Information
version 2.44 (.EXE file)	Nov 2013	For use with the legacy KFF Server that was used with applications versions 5.5 and earlier. Contains the full NSRL library up through update 2.44. Install this library first. <b>Note:</b> NSRL updates for the legacy KFF format will end in the 2nd quarter of 2015. From that time, NSRL updates will only be provided in the new format.

## Importing the Complete NSRL Library

To add the NSRL library to your KFF Library, you import the data. You start by importing the full NSRL library. You can then import any updates as they are available.

See [About Importing the NIST NSRL Library](#) on page 193.

See [Installing KFF Updates](#) on page 200.

**Important:** The complete NSRL library data is contained in a large (3.4 GB) .ZIP file. When expanded, the data is about 18 GB. Make sure that your file system can support files of this size.

**Important:** Due to the large amount of NSRL data, it will take 3-4 hours to import the NSRL data using the KFF Import Utility. If you import from within an application, it will take even longer.

### To install the NSRL complete library

1. Extract the NSRLSOURCE\_2.45.ZIP file from the KFF Installation disc.  
See [Downloading the Latest KFF Installation Files](#) on page 186.
2. On the KFF Server, launch the *KFF Import Utility*.  
See [Installing the KFF Import Utility](#) on page 191.
3. Click **Import**.
4. Click **Browse**.
5. Browse to and select the NSRLSource\_2.45 folder that contains the **NSRLFile.txt** file.  
(Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
6. Click **Select Folder**.
7. Click **Start**.
8. When the import is complete, click **OK**.
9. Close the *Import Utility* dialog and the NSRL library will be listed in the *Currently Installed Sets*.

## Importing the NDIC Hashkeeper Library

You can import the Hashkeeper 9.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

### To import the Hashkeeper library

1. Have access the NDIC source files by download the ZIP file from the web:  
See [Downloading the Latest KFF Installation Files](#) on page 186.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.  
See [Installing the KFF Import Utility](#) on page 191.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the NDIC source folder that contains the **Export.xml** file.  
(Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
7. Click **Select Folder**.

8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the NDIC library will be listed in the *Currently Installed Sets*.

## Importing the DHS Library

You can import the DHS 1.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

### To import the DHS library

1. Have access the NDIC source files by download the ZIP file from the web:  
See [Downloading the Latest KFF Installation Files](#) on page 186.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.  
See [Installing the KFF Import Utility](#) on page 191.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the DHS source folder that contains the **Export.xml** file.  
(Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
7. Click **Select Folder**.
8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the DHS library will be listed in the *Currently Installed Sets*.

## Installing the Geolocation (GeoIP) Data

Geolocation (GeoIP) data is used for the Geolocation Visualization feature of several AccessData products.

See [About the KFF Server and Geolocation](#) on page 184.

You can also check for and install GeoIP data updates.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.

The Geolocation data that was used with versions 5.5 and earlier is version 1.0.1 or earlier.

The Geolocation data that is used with versions 5.6 and later is version 2014.10 or later.

### To install the Geolocation IP Data

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the *autorun.exe*.  
See [Downloading the Latest KFF Installation Files](#) on page 186.
2. Click the *64 bit* or *32 bit* **Install Geolocation Data**.
3. Complete the installation wizard.

# About CSV and Binary Formats

When you export and import KFF data, you can use one of two formats:

- CSV
- KFF Binary

## About the CSV Format

When you use the .CSV format, you use a single .CSV file. The .CSV file contains the hashes that you import or export.

When you export to a CSV file, it contains the hashes as well as all of the information about any associated Hash Sets and KFF Groups. You can only use the CSV format when exporting individual Hash Sets and KFF Groups.

When you import using a CSV file, it can be a simple file containing only the hashes of files, or it can contain additional information about Hash Sets and KFF Groups.

However, CSV files will usually take a little longer to export and import.

To view the sample of a .CSV file that contains binaries and Hash Sets and KFF Groups, perform a CSV export and view the file in Excel.

You can also use the format of CSV files that were exported in previous versions.

To import .CSV files, use the application's KFF Import feature.

## About the KFF Binary Format

When you use the KFF binary format, you use a set of files that are in an internal KFF Server (Elasticsearch) format that is referred to as a Snapshot. The binary format is essentially a snapshot of one of the indices contained in the KFF Server. You can only have one binary format snapshot for each index.

See [Components of KFF Data](#) on page 180.

The benefit of the binary format is that it is able to support larger amounts of data than the CSV format. For large data sets, the binary format will export and import faster than the CSV format.

For example, when you import the DHC or NDIC Hashkeeper libraries, they are imported from a KFF binary format.

If you export your custom Hash Sets or KFF Groups using the KFF binary format, everything in the *KFF Index* is included.

See [About Choosing to Export in CSV or KFF Binary Format](#) on page 197.

When exporting in a Binary format, you specify an existing parent folder and then the name of a new sub-folder for the binary data. The new sub-folder must not previously exist and will be created by the export process.

After export, the binary export folder contains the following:

- **Indices** sub-folder - The folder contains the exported KFF data
- **Export.xml** - This file is the only file that is not an Elasticsearch file and is created by the export feature and contains the KFF Group and Hash Set definitions for the index.

- **Index** - an index file generated by Elasticsearch
- **metadata-snapshot** file with the data and time it was created
- **snapshot-snapshot** file with the data and time it was created

---

**Note:** The binary format is dependent on the version of the KFF Server. When exporting and importing the binary format, the systems must be using the same version of the KFF Server. When new versions of the KFF Server are released in the future, an upgrade process will also be provided.

---

## About Choosing to Export in CSV or KFF Binary Format

When you export your own KFF data, you have the option of using either the CSV or the binary format. The results are different based on the format that you use:

CSV format	
Exporting in CSV format	<p>When you export KFF data using the CSV format, you can export specific pieces of KFF data, such as one or more Hash Sets or one or more KFF Groups. The exported data is contained in one .CSV file.</p> <p>The benefits of the CSV format are that CSV files can be easily viewed and can be manually edited. They are also less dependent on the version of the KFF Server.</p>
Importing from CSV format	<p>When you import a CSV file, the data in the file is data is added to your existing KFF data that is in the <i>KFF Index</i>.</p> <p>See <a href="#">Components of KFF Data</a> on page 180.</p> <p>For example, suppose you started by manually created four Hash Sets and one KFF Group. That would be the only contents in your <i>KFF Index</i>. Suppose you import a .CSV file that contains five hash sets and two KFF Groups. They will be added together for a total of nine Hash Sets and three KFF Groups.</p> <p>To import .CSV files, use the KFF Import feature in your application. See <i>Using the Known File Feature</i> chapter.</p>
KFF binary format	
Exporting in KFF binary format	<p>If you export your KFF data using the KFF binary format, all of the data that you have in the <i>KFF Index</i> will be exported together. You cannot use this format to export individual Hash Sets or KFF Groups.</p> <p>See <a href="#">Components of KFF Data</a> on page 180.</p> <p>You will only want to use this format if you intend to export all of the data in the <i>KFF Index</i> and import it as a whole. This can be useful in making an archive of your KFF data or copying KFF data from one KFF Server to another.</p> <p>Because NSRL, NIST, and DHC data is contained in their own indexes, when you do an export using this format, those sets are not included. Only the data in the <i>KFF Index</i> is exported.</p>

Importing KFF  
binary format

**IMPORTANT:** When you import a KFF binary format, it will import the complete index and will *replace* any data that is currently in that index on the KFF Server.

For example, if you import the DHC library, and then later you import the DHC library again, the DHC index will be replaced with the new import.

If you have a KFF binary format snapshot of custom KFF data (which would have come from a binary format export) it will replace all KFF data that already exists in your *KFF Index*.

For example, suppose you manually created four Hash Sets and one KFF Group. Suppose you then import a binary format that has five hash sets and two KFF Groups. The binary format will be imported as a complete index and will replace the existing data. The result will be only be the imported five Hash Sets and two KFF libraries.

When importing KFF binary files, it is recommend that you use the KFF Import Utility.

See [Installing the KFF Import Utility](#) on page 191.

# Uninstalling KFF

You can uninstall KFF application components independently of the KFF Data.

Main version	Description
Applications 5.6 and later	<p>For applications version 5.6 and later, you uninstall the following components:</p> <ul style="list-style-type: none"><li>• <i>AccessData Elasticsearch Windows Service</i> (KFF Server) v1.2.7 and later Note: Elasticsearch is used by multiple features in various applications, use caution when uninstalling this service or the related data.</li><li>• <i>AccessData KFF Import Utility</i> (v5.6 and later)</li><li>• <i>AccessData KFF Migration Tool</i> (v1.0 and later)</li><li>• <i>AccessData Geo Location Data</i> (v2014.10 and later) Note: This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature.</li></ul> <p>The location of the KFF data is configured when the <i>AccessData Elasticsearch Windows Service</i> was installed. By default, it is located at C:\Program Files\AccessData\Elasticsearch\Data.</p>
Applications 5.5 and earlier	<p>For applications version 5.5 and earlier, you can uninstall the following components:</p> <ul style="list-style-type: none"><li>• KFF Server (v1.2.7 and earlier) Note: The KFF Server is also used by the geolocation visualization feature.</li><li>• <i>AccessData Geo Location Data</i> (1.0.1 and earlier) This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature.</li></ul> <p>The location of the KFF data was configured when the <i>KFF Server</i> was installed. You can view the location of the data by running the <i>KFF.Config.exe</i> on the KFF Server.</p> <p>If you are upgrading from 5.5 to 5.6, you can migrate your KFF data before uninstalling the KFF Server.</p>

# Installing KFF Updates

From time to time, AccessData will release updates to the KFF Server and the KFF data libraries.

Some of the KFF data updates may require you to update the version of the KFF Server.

To check for updates, do the following:

1. Go to the KFF product download page.  
See [Downloading the Latest KFF Installation Files](#) on page 186.
2. Check for updates.
  - See [About KFF Server Versions](#) on page 185.
  - See [About Importing the NIST NSRL Library](#) on page 193.
3. If there are updates, download them.
4. Install or import the updates.



# KFF Library Reference Information

## *About KFF Pre-Defined Hash Libraries*

This section includes a description of pre-defined hash collections that can be added as AccessData KFF data.

The following pre-defined libraries are currently available for KFF and come from one of three federal government agencies:

- NIST NSRL (The default library installed with KFF)
- NDIC HashKeeper (An optional library that can be downloaded from the AccessData Downloads page)
- DHS (An optional library that can be downloaded from the AccessData Downloads page)

---

**Note:** Because KFF is now multi-sourced, it is no longer maintained in HashKeeper format. Therefore, you cannot modify KFF data in the HashKeeper program. However, the HashKeeper format continues to be compatible with the AccessData KFF data.

---

### **Use the following information to help identify the origin of any hash set within the KFF**

- The NSRL hash sets do not begin with “ZZN” or “ZN”. In addition, in the AD Lab KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. For example: “Password Manager & Form Filler 9722.”
- All HashKeeper Alert sets begin with “ZZ”, and all HashKeeper Ignore sets begin with “Z”. (There are a few exceptions. See below.) These prefixes are often followed by numeric characters (“ZZN” or “ZN” where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Two examples of HashKeeper Alert sets are:
  - “ZZ00001 Suspected child porn”
  - “ZZ14W”An example of a HashKeeper Ignore set is:
  - “Z00048 Corel Draw 6”
- The DHS collection is broken down as follows:
  - In 1.81.4 and later there are two sets named “DHS-ICE Child Exploitation JAN-1-08 CSV” and “DHS-ICE Child Exploitation JAN-1-08 HASH”.
  - In AD Lab there is just one such set, and it is named “DHS-ICE Child Exploitation JAN-1-08”.

Once an investigator has identified the vendor from which a hash set has come, he/she may need to consider the vendor’s philosophy on collecting and categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her project. The following descriptions may be useful in assessing hits.

## NIST NSRL

The NIST NSRL collection is described at: <http://www.nsrl.nist.gov/index.html>. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by AccessData staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are “empty”, that is, they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, allows AccessData to modify (or selectively alter) NSRL’s own set names to remove ambiguity and redundancy.

Find contact info at <http://www.nsrl.nist.gov/Contacts.htm>.

## NDIC HashKeeper

NDIC’s HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be connected to child pornography. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of KFF, AccessData staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. AccessData labels the following sets Alert even though HashKeeper had assigned them as Ignore: “Z00045 PGP files”, “Z00046 Steganos”, “Z00065 Cyber Lock”, “Z00136 PGP Shareware”, “Z00186 Misc Steganography Programs”, “Z00188 Wiping Programs”. The names of these sets may suggest the intent to conceal data on the part of the suspect, and AccessData marks them Alert with the assumption that investigators would want to be “alerted” to the presence of data obfuscation or elimination software that had been installed by the suspect.

The following table lists actual HashKeeper Alert Set origins:

### A Sample of HashKeeper KFF Contributions

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00001 Suspected child porn	Det. Mike McNown & Randy Stone	Wichita PD		
ZZ00002 Identified Child Porn	Det. Banks	Union County (NJ) Prosecutor's Office	(908) 527-4508	case 2000S-0102
ZZ00003 Suspected child porn	Illinois State Police			
ZZ00004 Identified Child Porn	SA Brad Kropp, AFOSI, Det 307		(609) 754-3354	Case # 00307D7- S934831

### A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00000, suspected child porn	NDIC			
ZZ00005 Suspected Child Porn	Rene Moes, Luxembourg Police		rene.moes@police.eta t.lu	
ZZ00006 Suspected Child Porn	Illinois State Police			
ZZ00007b Suspected KP (US Federal)				
ZZ00007a Suspected KP Movies				
ZZ00007c Suspected KP (Alabama 13A-12- 192)				
ZZ00008 Suspected Child Pornography or Erotica	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminoleshe riff.org	suspected child pornogrphay from 20010000850
ZZ00009 Known Child Pornography	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminoleshe riff.org	200100004750
ZZ10 Known Child Porn	Detective Richard Voce CFCE	Tacoma Police Department	(253)594-7906, rvoce@ci.tacoma.wa.u s	
ZZ00011 Identified CP images	Detective Michael Forsyth	Baltimore County Police Department	(410)887-1866, mick410@hotmail.com	
ZZ00012 Suspected CP images	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminoleshe riff.org	
ZZ0013 Identified CP images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD02-70707

### A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ14W	Sgt Stephen May		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 41929134
ZZ14U	Sgt Chris Walling		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 41919887
ZZ14X	Sgt Jeff Eckert		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG Internal
ZZ14I	Sgt Stephen May		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 041908476
ZZ14B	Robert Britt, SA, FBI		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 031870678
ZZ14S	Sgt Stephen May		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 041962689
ZZ14Q	Sgt Cody Smirl		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 041952839
ZZ14V	Sgt Karen McKay		Tamara.Chandler@oa g.state.tx.us, (512)936-2898	TXOAG 41924143
ZZ00015 Known CP Images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD04-38144
ZZ00016	Marion County Sheriff's Department		(317) 231-8506	MP04-0216808

The basic rule is to always consider the source when using KFF in your investigations. You should consider the origin of the hash set to which the hit belongs. In addition, you should consider the underlying nature of hash values in order to evaluate a hit's authenticity.

## Higher Level KFF Structure and Usage

Since hash set groups have the properties just described (and because custom hash sets and groups can be defined by the investigator) the KFF mechanism can be leveraged in creative ways. For example:

- You could define a group of hash sets created from encryption software and another group of hash sets created from child pornography files. Then, you would apply only those groups while processing.
- You could also use the Ignore status. You are about to process a hard drive image, but your search warrant does not allow inspection of certain files within the image that have been previously identified. You could do the following and still observe the warrant:
  - 4a. Open the image in Imager, navigate to each of the prohibited files, and cause an MD5 hash value to be computed for each.
  - 4b. Import these hash values into custom hash sets (one or more), add those sets to a custom group, and give the group Ignore status.
  - 4c. Process the image with the MD5 and KFF options, and with AD\_Alert, AD\_Ignore, and the new, custom group selected.
  - 4d. During post-processing analysis, filter file lists to eliminate rows representing files with Ignore status.

## Hash Set Categories

The highest level of the KFF's logical structure is the categorizing of hash sets by owner and scope. The categories are AccessData, Project Specific, and Shared.

### Hash Set Categories

Category	Description
AccessData	The sets shipped with as the Library. Custom groups can be created from these sets, but the sets and their status values are read only.
Project Specific	Sets and groups created by the investigator to be applied only within an individual project.
Shared	Sets and groups created by the investigator for use within multiple projects all stored in the same database, and within the same application schema.

**Important:** Coordination among other investigators is essential when altering Shared groups in a lab deployment. Each investigator must consider how other investigators will be affected when Shared groups are modified.

# What has Changed in Version 5.6

With the 5.6 release of eDiscovery, Summation, and FTK-based products, the KFF feature has been updated.

If you used KFF with applications version 5.5 or earlier, you will want to be aware of the following changes in the KFF functionality.

## Changes from version 5.5 to 5.6

Item	Description
KFF Server	<p>KFF Server now runs a different service.</p> <ul style="list-style-type: none"><li>• In 5.5 and earlier, the KFF Server ran as the <i>KFF Server</i> service.</li><li>• In 5.6 and later, the KFF Server uses the <i>AccessData Elasticsearch Windows Service</i>.</li></ul> <p>For applications version 5.6 and later, all KFF data must be created in or imported into the new KFF Server.</p>
KFF Migration Tool	<p>This is a new tool that lets you migrate custom KFF data from 5.5 and earlier to the new KFF Server.</p> <p>NIST NSRL, NDIC HashKeeper, or DHS library data from 5.5 will not be migrated. You must re-import it.</p> <p>See <a href="#">Migrating Legacy KFF Data</a> on page 188.</p>
KFF Import Utility	<p>This is a new utility that lets you import large amounts of KFF data quicker than using the import feature in the application.</p> <p>See <a href="#">Using the KFF Import Utility</a> on page 190.</p>
KFF Libraries, Templates, and Groups	<p>In 5.5, all Hash Sets were configured within KFF Libraries. KFF Libraries could then contain KFF Groups and KFF Templates.</p> <p>KFF Libraries and Templates have been eliminated. You now simply create or import KFF Groups and add Hash Sets to the groups.</p> <p>You can now nest KFF Groups.</p>
NIST NSRL, NDIC HashKeeper, or DHS libraries	<p>In 5.5 and earlier, to use these libraries, you ran an installation wizard for each library. You now import these libraries using the KFF Import Utility.</p> <p>See <a href="#">About Importing Pre-defined KFF Data Libraries</a> on page 192.</p>
Import Log	<p>FTK-based products no longer include the Import Log.</p> <p>eDiscovery and Summation products did not have it previously.</p>
Export	<p>When you export KFF data you can now choose two formats:</p> <ul style="list-style-type: none"><li>• CSV format which replaced XML format</li><li>• A new binary format</li></ul> <p>See <a href="#">About CSV and Binary Formats</a> on page 196.</p>

# Chapter 15

## Using KFF (Known File Filter)

---

This chapter explains how to configure and use KFF and has the following sections:

- See [About KFF and De-NIST Terminology](#) on page 207.
- See [Process for Using KFF](#) on page 208.
- See [Configuring KFF Permissions](#) on page 208.
- See [Adding Hashes to the KFF Server](#) on page 209.
- See [Using KFF Groups to Organize Hash Sets](#) on page 215.
- See [Exporting KFF Data](#) on page 226.
- See [Enabling a Project to Use KFF](#) on page 219.
- See [Reviewing KFF Results](#) on page 221.
- See [Re-Processing KFF](#) on page 225.

## About KFF and De-NIST Terminology

You can configure the interface to display either the term “KFF” (Known File Filter) or “De-NIST”. For example, this can change references of a “KFF Group” to a “De-NIST Group.”

This does not affect the functionality of KFF, but only the term that is displayed. This allows users in forensic environments to see the term “KFF” while users in legal environments can see the term “De-NIST.”

By default, the KFF term is used in the interface.

This setting only affects text in the interface. The following new icon is used with either setting:



In this manual, the KFF term is used.

### To change the KFF and De-NIST terminology

1. In the `web.config` file, in the `<ReviewOptions>` section, add or modify the following entry:  
`<add key="KFFAlternateName" value="KFF" />`
2. To change the setting to use De-NIST terminology, change the `value=` from “KFF” to “De-NIST”.

# Process for Using KFF

To use the KFF feature, you perform the following steps:

## Process for using KFF

Step 1.	Install and configure the KFF Server. See <a href="#">Installing the KFF Server</a> on page 185.
Step 2.	Configure KFF permissions. <a href="#">Configuring KFF Permissions</a> (page 208)
Step 3.	Add and manage KFF hashes on the KFF Server. See <a href="#">Adding Hashes to the KFF Server</a> on page 209.
Step 4.	Add and manage KFF Groups to organize KFF Hash Sets. <a href="#">Using KFF Groups to Organize Hash Sets</a> (page 215)
Step 5.	Configure a project to use KFF. See <a href="#">Enabling a Project to Use KFF</a> on page 219.
Step 6.	Review KFF results in Project Review. See <a href="#">Reviewing KFF Results</a> on page 221.
Step 7.	(Optional) Re-process the KFF data using different hashes. See <a href="#">Re-Processing KFF</a> on page 225.
Step 8.	(Optional) Archive or export KFF data to share with other KFF Servers. See <a href="#">Exporting KFF Data</a> on page 226.

## Configuring KFF Permissions

In order to create and manage KFF libraries, sets, templates, and groups, you must have one of the following permissions:

- Administrator
- Manage KFF

You assign the *Manage KFF* permission to an Admin Role and then associate that role with users.

See [Configuring and Managing System Users, User Groups, and Roles](#) on page 46.

A user with project management permissions does not require the *Manage KFF* permission in order to enable KFF for a new project.



# Adding Hashes to the KFF Server

You must add the hashes of the files that you want to compare against your evidence data. When adding hashes to the KFF Serer, you add them in KFF Hash Sets.

See [Components of KFF Data](#) on page 180.

You can use the following methods to add hashes to the KFF Library:

Migrate legacy KFF Server data	You can migrate legacy KFF data that is in a KFF Server in applications versions 5.5 and earlier. See <a href="#">Migrating Legacy KFF Data</a> on page 188.
Import hashes	You can import previously configured KFF hashes from .CSV files. See <a href="#">Importing KFF Data</a> on page 210.
Manually create and manage Hash Sets	You can manually add hashes to a Hash Set. See <a href="#">Manually Creating and Managing KFF Hash Sets</a> on page 212.
Create hashes from evidence files in <i>Review</i>	You can add hashes from the files in your evidence using <i>Review</i> . See <a href="#">Adding Hashes to Hash Sets Using Project Review</a> on page 213.

## About the Manage KFF Hash Sets Page

To configure KFF data, you use the *KFF Hash Sets* and *KFF Groups* pages.

### To open the KFF Hash Sets page


1. Log in as an Administrator or user with Manage KFF permissions.

2. Click **Management >**  **Hash Sets**


If the feature does not function properly, check the following:

- The KFF Server is installed.  
See [Installing the KFF Server](#) on page 185.
- The application has been configured for the KFF Server.  
See [Configuring the Location of the KFF Server](#) on page 187.
- The KFF Service is running.  
In the Windows Services manager, make sure that the AccessData Elasticsearch service is started.

### Elements of the KFF Hash Sets page

Element	Description
<i>Hash Sets</i>	Displays all of the Hash Sets that have been imported or created in the KFF Server.
	Lets you create a Hash Set. See <a href="#">Manually Creating and Managing KFF Hash Sets</a> on page 212.

## Elements of the KFF Hash Sets page

Element	Description
	Lets you edit the active Hash Set. See <a href="#">Manually Creating and Managing KFF Hash Sets</a> on page 212.
	Lets you delete the active Hash Set. Warning: You are not prompted to confirm the deletion. See <a href="#">Manually Creating and Managing KFF Hash Sets</a> on page 212.
 <i>Delete</i>	Lets you delete one or more checked Hash Sets.
 <i>View Hashes</i>	Lets you view and manage the hashes in the Hash Set. See <a href="#">Searching For, Viewing, and Managing Hashes in a Hash Set</a> on page 213.
 <i>Import File</i>	Lets you import KFF data. See <a href="#">Importing KFF Data</a> on page 210.
<i>Export</i>	Lets you export KFF data. See <a href="#">Exporting KFF Data</a> on page 226.
	Refreshes the Hash Sets list.

## Importing KFF Data

### About Importing KFF Data

To understand the methods and formats for importing KFF data, first see [About Importing KFF Data](#) (page 189).

This chapter explains how to import KFF data using the application's management console.

### Importing KFF Hashes

You can import KFF data from the following:

- KFF export CSV files
- KFF binary files
  - Warning:* Importing KFF binary files will replace your existing KFF data.  
See [About CSV and Binary Formats](#) on page 196.
  - It is recommended that you use the external *KFF Import Utility* to import KFF binary files.  
See [Using the KFF Import Utility](#) on page 190.

When importing KFF data, you can enter default values for the following fields:

- Default Status
- Default Vendor
- Default Version

- Default Package

These are default values that will be used if they import file does not contain the information.

When importing hash lists using the CSV import, each hash within the CSV can have the same, different or no status. During the import process you must choose a default status of Alert or Ignore. This default status will have no affect on any hash in your CSV that already contains a status, however, any hash that does not have a pre-assigned status will have this default status assigned to them.

The override status for the hash sets that you import will be automatically set to No Override. This is to ensure that if your hash set contains both Alert and Ignore hashes, the program will not override the original status. You can, however, choose to override the individual hash status within a set by choosing to set the whole set to Alert or Ignore.


You can use these value to organize your hashes. For example, you can filter or sort data based on these values.

### To import KFF hashes from files

1. Log in as an Administrator or user with Manage KFF permissions.

2. Click **Management** >  **Hash Sets**.

3. Click  **Import File**.

4. On the KFF Import File dialog, click  **Add File**.

5. Browse to and select the file.

6. Click **Select**.

7. Specify a *Default Status*.

This sets a default status only for the hashes that do not have a status specified in the file.

8. (Optional) Specify a default Vendor, Version, and Package.

This sets values only for the hashes that do not have a value specified in the file.

9. (Optional) Add other files.

10. Click **Import**.

11. View the *Import Summary* to see the results of the Import.

12. Click **Close**.

### To import KFF data from a binary format

*Warning:* This process may replace your existing KFF data.

See [About the KFF Binary Format](#) on page 196.

1. Log in as an Administrator or user with Manage KFF permissions.

2. Click **Management** >  **Hash Sets**.

3. Click  **Import File**.

4. On the KFF Import File dialog, click **Binary Import**.

5. Browse to the folder that contains the binary files (specifically the `Export.xml` file) and click **Select**.

6. Click **Import**.

## Manually Creating and Managing KFF Hash Sets

You can manually create Hash Sets and then add hashes to them. You can also edit and delete Hash Sets.



You can also add, edit, or delete the hashes in Hash Sets.

---




**Note:** You cannot manually add, edit, and delete hash values that were imported from NSRL, NDIC HashKeeper, and DHS libraries.

---

### To manually create a Hash Set

1. Log in as an Administrator or user with Manage KFF permissions.
2. Click **Management** >  **Hash Sets**.
3. On the *KFF Hash Sets* page, in the right pane, click *Add* .
4. Enter a name for the Hash Set.
5. Select the status for the Hash Set: *Alert*, *Ignore*, or *No Override*.
6. (Optional) Enter a package, vendor, or version.  
These are not required, but you can use these values for sorting and filtering results.
7. Click **Save**.


### To manually manage Hash Sets

1. Click **Management** >  **Hash Sets**.
2. Do one of the following:
  - To edit a Hash Set, select a set a set, and click *Edit* .
  - To delete a single Hash Set, select a set, and click *Delete* .
  - To delete a multiple Hash Sets, select the sets, and click *Delete* .

### To manage hashes in a hash set

1. On the *KFF Hash Sets* page, select a Hash Set.
2. Click **View Hashes**.

### To add hashes to a hash set

1. On the *KFF Hash Sets* page, select a Hash Set.
2. Click **View Hashes**.
3. In the *KFF Hash Finder* dialog, click *Add* .
4. Enter the KFF hash value.
5. Enter the filename for the hash.
6. (Optional) Enter other reference information about the hash.
7. Click **Save**.  
The new hash is displayed.

## Searching For, Viewing, and Managing Hashes in a Hash Set

Due to the large number of hashes that may be in a Hash Set, a list of hashes is not displayed. (However, you can export a KFF Group that contains the Hash Set and view the hashes in the export file.)


You can use the *KFF Hash Finder* dialog to search for hash values within a hash set. You search by entering a complete hash value. You can only search within one hash set at a time.

While the *KFF Hash Finder* does not display a list of hashes, it does display the number of hashes in the set.


### To search for hashes in a hash set

1. On the *KFF Hash Sets* page, select a Hash Set.
2. Click **View Hashes**.
3. In the *KFF Hash Finder dialog*, enter the complete hash value that you want to search for.
4. Click **Search**.  
If the hash is found, it is displayed in the hash list.  
If the hash is not found a message is displayed.

### To edit hashes in a hash set

1. In the *KFF Hash Finder* dialog, search for the hash that you want to edit.
2. Click *Edit* .
3. Enter the hash information.
4. Click **Save**.  
The edited hash is displayed.

### To delete hashes from a hash set

1. In the *KFF Hash Finder* dialog, search for the hash that you want to delete.
2. Click *Delete* .

## Adding Hashes to Hash Sets Using Project Review

You may identify files that exist in a project as files that you want to add to your KFF hashes. For example, you may find a graphics file that you want to either alert for or ignore in this or other projects. Using *Project Review*, you can select files and then add them to existing or new KFF Hash Sets.





When you add hashes using *Project Review*, it starts a job that adds the hashes to the KFF Library.

### To use Project Review to add hashes to Hash Sets

1. Log in as an Administrator or user with Manage KFF permissions.
2. Select a project and enter *Project Review*.
3. Select the files that you want to add to a hash set.
4. In the *Actions* drop-down, select **Add to KFF**.
5. Click **Go**.
6. In the *Add Hash to Set* dialog, select a status for the hash.

7. Specify a Hash Set.  
You can select an existing set or create a new set.
  - To create a new set, do the following:
    - 7a. Select [Add New].
    - 7b. Enter the name of the new set.
    - 7c. Enter a name for the hash set.
    - 7d. (Optional) Add other information.
    - 7e. Click **Save**.
  - To use an existing set, do the following:
    - 7a. Select an existing set.  
By default, you will only see the sets that match the status that you select.  
To see Hash Sets that have a *No Override* status as well, enable the *Display hash sets with no override status* option.
    - 7b. You can filter and sort the list with the following filters:
      - Name
      - Override
      - Package
      - Vendor
      - Version
    - 7c. Click **Save**.

### To verify that hashes were added to the KFF Server

1. Click  to exit *Review*.
2. On the *Home* page, select the project that you are using.
3. Click *Work List*  .  
See [Monitoring the Work List](#) on page 308.  
Click *Refresh*  to see the current status.
4. View the *Add Hash to KFF* job types.
5. Click *Refresh*  to see the current status.
6. When the jobs are completed, at the bottom of the page, you can view the results.  
It will show the number of files that were added or any errors generated.
7. From the *KFF Hash Sets* tab on the *Management* page, you can view the Hash Sets.  
See [Searching For, Viewing, and Managing Hashes in a Hash Set](#) on page 213.

# Using KFF Groups to Organize Hash Sets

## About KFF Groups

KFF groups are containers for one or more Hash Sets. When you create a group, you then add Hash Sets to the group. KFF Groups can also contain other KFF Groups.

When you enable KFF for a project, you select which KFF Group to use during processing.

Within a KFF group, you can manually edit custom Hash Sets.

## About KFF Groups Status Override Settings

When you create a KFF Group, you can choose to use the default status of the Hash Set (*Alert* or *Ignore*) or override it. You do this by setting one of the following Status Override settings:

- *Alert* - All Hash Sets within the KFF Group will be set to *Alert* regardless of the status of the individual Hash Sets.
- *Ignore* - All Hash Sets within the KFF Group will be set to *Ignore* regardless of the status of the individual Hash Sets.
- No Override - All Hash Sets will maintain their default status.

For example, if you have a Hash Set with a status of *Alert*, if you set the KFF Group to No Override, then the default status of *Alert* is used. If you set the KFF Group with a status of *Ignore*, the Hash Set *Alert* status is overridden and *Ignore* is used.

As a result, use caution when setting the Status Override for a KFF Group.

## About Nesting KFF Groups

KFF Groups can contain Hash Sets or they can contain other KFF Groups. When one KFF Group includes another KFF Group, it is called nesting.

The reason that you may want to nest KFF Groups is that you can use multiple KFF Groups when processing your data. When you enable KFF for a case, you can only select one KFF Group. By nesting, you can use multiple KFF Groups.



For example, you may have one KFF Group that contains Hash Sets with an *Alert* status. You may have a second KFF Group that contains Hash Sets with an *Ignore* status. When processing a case, you may want to use both of those KFF Groups. To accomplish this, you can create another KFF Group as a parent and then add the other two KFF Groups to it. When processing, you would select the parent KFF Group.

When nesting KFF Groups you must be mindful of the Status Override of the parent KFF Group. The Status Override for the highest KFF Group in the hierarchy is used when nesting KFF Groups. In most cases, you will want to set the parent KFF Group with a status of *None*. That way, the status of each child KFF Group (or their Hash Sets) is used. If you select an *Alert* or *Ignore* status for the parent KFF Group, then all child KFF Groups and their Hash Sets will use that status.



## Creating a KFF Group

You create KFF groups to organize your Hash Sets. When you create a KFF Group, you add one or more Hash Sets to it. You can later edit the KFF Group to add or remove Hash Sets.

### To create a KFF Group

1. Log in as an Administrator or user with Manage KFF permissions.
2. Click **Management** >  **Groups**.
3. Click **Add** .
4. Enter a *Name*.
5. Set the *Status Override*.
6. See [About KFF Groups Status Override Settings](#) on page 215.
7. (Optional) Enter a Package, Vendor, and Version.
8. Click **Save**.

### To add a Hash Sets to a KFF Group

1. Click **Management** >  **Groups**.
2. In the *Groups* list, select the group that you want to add Hash Sets to.
3. In the *Groups and Hash Sets* pane, click  **Add**.
4. Select the Hash Sets that you want to add to the group.
5. You can filter the list of Hash Sets to help you find the hash sets that you want.
6. After selecting the sets, click **OK**.

## Viewing the Contents of a KFF Group

On the *KFF Groups* page, you can select a KFF Group and in the *Groups and Hash Sets* pane, view the Hash Sets and child KFF Groups that are contained in that KFF Group.

## Managing KFF Groups

You can edit KFF Groups and do the following:


- Rename the group
- Change the Override Status
- Add or remove Hash Sets and KFF Groups

You can also do the following:

- Delete the group
  - Export the group
- See [Exporting KFF Data](#) on page 226.



## To manage a KFF Group

1. Click **Management** >  **Groups**.
2. In the *Groups* list, select a KFF Group that you want to manage.
3. Do one of the following:
  - Click  *Edit*.
  - Click  *Delete*.
  - Click **Export**.  
See [Exporting KFF Data](#) on page 226.

## About the Manage KFF Groups Page

To configure KFF Groups, you use the *KFF Groups* page.





### To open the KFF Groups page

1. Log in as an Administrator or user with Manage KFF permissions.
2. Click **Management** >  **Groups**




If the feature does not function properly, check the following:

- The KFF Server is installed.  
See [Installing the KFF Server](#) on page 185.
- The application has been configured for the KFF Server.  
See [Configuring the Location of the KFF Server](#) on page 187.
- The KFF Service is running.  
In the Windows Services manager, make sure that the AccessData Elasticsearch service is started.

### Elements of the KFF Groups page

Tab	Element	Description
<i>KFF Groups pane</i>	<i>KFF Groups</i>	Displays all of the KFF Groups that have been imported or created in the KFF Server.
		Lets you create a KFF Group. See <a href="#">Creating a KFF Group</a> on page 216.
		Lets you edit the active KFF Group. See <a href="#">Managing KFF Groups</a> on page 216.
		Lets you delete the active KFF Group. See <a href="#">Managing KFF Groups</a> on page 216.
	 <i>Delete</i>	Lets you delete one or more checked KFF Groups.

## Elements of the KFF Groups page

Tab	Element	Description
	<i>Export</i>	Lets you export KFF data. See <a href="#">Exporting KFF Data</a> on page 226.
		Refreshes the KFF Groups list.
<i>Groups and Hash Sets Pane</i>	Lets you add and remote Hash Sets from KFF Groups. See <a href="#">Managing KFF Groups</a> on page 216.	
	 <b>Add</b>	Displays the list of Hash Sets that you can add to a KFF Group. See <a href="#">Managing KFF Groups</a> on page 216.
	 <b>Remove</b>	Lets you remove Hash Sets from a KFF Group. See <a href="#">Managing KFF Groups</a> on page 216.
	<i>View Hashes</i>	Lets you view and manage the hashes in the Hash Set. See <a href="#">Searching For, Viewing, and Managing Hashes in a Hash Set</a> on page 213.

# Enabling a Project to Use KFF

When you create a project, you can enable KFF and configure the KFF settings for the project.

## About Enabling and Configuring KFF

To use KFF in a project you do the following:


### Process for enabling and configuring KFF

1. Create a new Project	If you want to use KFF you must enable it when you create the project. You cannot enable KFF for a project after it has been created.
2. Enable KFF	Enable the KFF processing option. See <a href="#">Enabling and Configuring KFF</a> on page 219.
2. Configure how to process ignorable files	You can choose how to process ignorable files: <ul style="list-style-type: none"><li>• <i>Skip Ignorable Files</i> - This option will not process any files determined to be Ignorable. Any files that are ignorable will not be included or visible in the project. This is the default option.</li><li>• <i>Process and Flag Ignorable Files</i> - This option will process ignorable files, but flag them as Ignorable. Any files that are Ignorable will be included and visible in the project, but can be filtered. See <a href="#">Using Quick Filters</a> on page 222.</li></ul>
4. Select a KFF Group	When enabling KFF for a project, you select one KFF Group that you want to use. You do not create KFF Group at that time. You can only select an existing group. Because of this, you must have at least one KFF Group created before creating a project. See <a href="#">Using KFF Groups to Organize Hash Sets</a> on page 215. However, after processing, you can re-process the data using a different KFF template. This lets you create and use different templates after you initially process the project. See <a href="#">Re-Processing KFF</a> on page 225.

## Enabling and Configuring KFF

### To enable and configure KFF for a project

1. Log in as an Administrator or user with Create/Edit Projects permissions.
2. Create a new project.
3. In *Processing Options*, select **Enable KFF**.

A  *Options* tab option displays.

4. In *Processing Options*, select how to handle ignorable files.

5. Click  **Options**.

The KFF Options window displays.

6. In the drop-down menu, select the KFF Group that you want to use.  
See [Using KFF Groups to Organize Hash Sets](#) on page 215.
7. In the *Hash Sets* pane, verify that this template has the hash sets that you want. Otherwise select a different template.
8. Click **Create Project and Import Evidence** or click **Create Project** and add evidence later.

# Reviewing KFF Results

KFF results are displayed in Project Review.

You can use the following tools to see KFF results:



- Project Details page
- Project Review
  - KFF Information Quick Columns
  - KFF Quick Filters
  - KFF facets
  - KFF Details

You can also create and modify KFF libraries and hash sets using files in Review.

See [Adding Hashes to Hash Sets Using Project Review](#) on page 213.

## Viewing KFF Data Shown on the Project Details Page

### To View KFF Data on the Project Details page

1. Click the **Home** tab.
2. Click the  *Evidence* tab.
3. Verify that the project has completed processing.
4. Click the  *Project Details* tab.
5. In the right column, you can view the number of KFF known files.

## About KFF Data Shown in the Review Item List

You can identify and view files that are either Known or Unknown based on KFF results.

Depending on the KFF configuration options, there are two or three possible KFF statuses in Project Review:

- *Alert (2)* - Files that matched hashes in the template with an Alert status
- *Ignore (1)* - Files that matched hashes in the template with an Ignore status (not shown in the Item List by default)
- *Unknown (0)* - Files that did not match hashes in the template

If you configured the project to skip ignorable files, files configured to be ignored (Ignore status) are not included in the data and are not viewable in the Project Review.

See [Enabling and Configuring KFF](#) on page 219.

## Using the KFF Information Quick Columns

You can use the *KFF Information Quick Columns* to view and sort and filter on KFF values. For example, you can sort on the KFF Status column to quickly see all the files with the Alert status.

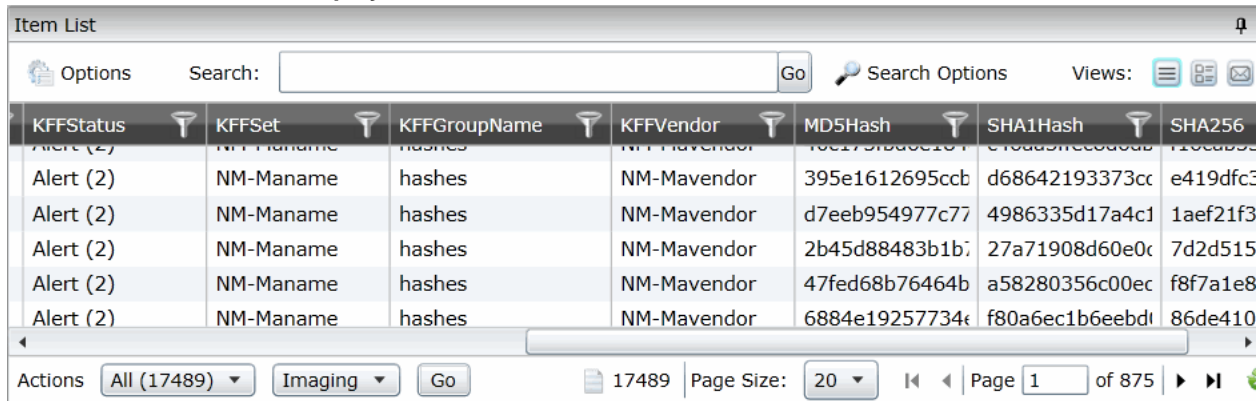
See [Using Document Viewing Panels](#) on page 76.

To see the KFF columns, activate the *KFF Information* Quick Columns.

### To activate the KFF Information Quick Columns

1. From the *Item List* in the *Review* window, click **Options**.
2. Click **Quick Columns > KFF > KFF Information**.  
The KFF Columns display.

### Item List with KFF Tabs displayed



The screenshot shows the 'Item List' window with a search bar and 'Options' button. Below is a table with columns: KFFStatus, KFFSet, KFFGroupName, KFFVendor, MD5Hash, SHA1Hash, and SHA256. The table contains six rows of data, each starting with 'Alert (2)'. At the bottom, there are 'Actions' buttons, a dropdown for 'All (17489)', 'Imaging', and 'Go', along with page navigation controls showing 'Page 1 of 875'.

KFFStatus	KFFSet	KFFGroupName	KFFVendor	MD5Hash	SHA1Hash	SHA256
Alert (2)	NM-Maname	hashes	NM-Mavendor	395e1612695ccb	d68642193373cc	e419dfc3
Alert (2)	NM-Maname	hashes	NM-Mavendor	d7eeb954977c77	4986335d17a4c1	1aef21f3
Alert (2)	NM-Maname	hashes	NM-Mavendor	2b45d88483b1b7	27a71908d60e0c	7d2d515
Alert (2)	NM-Maname	hashes	NM-Mavendor	47fed68b76464b	a58280356c00ec	f8f7a1e8
Alert (2)	NM-Maname	hashes	NM-Mavendor	6884e19257734e	f80a6ec1b6eebd	86de410

### KFF Columns

Column	Description
KFF Status	Displays the status of the file as it pertains to KFF. The three options are <i>Unknown (0)</i> , <i>Ignore (1)</i> , and <i>Alert (2)</i> . <ul style="list-style-type: none"><li>• If you configured the project to skip Ignorable files, these files are not included in the data.</li><li>• If you configured the project to flag Ignorable files, and the <i>Hide Ignorables</i> Quick Filter is set, these files are in the data, but are not displayed. See <a href="#">Using Quick Filters</a> on page 222.</li></ul>
KFF Set	Displays the KFF Hash Set to which the file belongs.
KFF Group Name	Displays the name created for the KFF Group in the project.
KFF Vendor	Displays the KFF vendor.

See [Filtering by Column in the Item List Panel](#) on page 143.

## Using Quick Filters

You can use Quick Filters to quickly show or hide KFF Ignorable files.

You can toggle the quick filter to do the following:

- *Hide Ignorables* - enabled by default
- *Show Ignorables*

The *Hide Ignorables* Quick Filter is set by default. As a result, even if you selected to process and flag Ignorable files for the project, they are not included in the Item List by default.

To show ignorable files in the Item list, change the Quick Filter to Show Ignorables.

---

**Note:** If you configured the project to skip ignorable files, files configured to be ignored (Ignore status) will not be shown, even if you select to *Show Ignorables*.

---

### To change the KFF Quick Filters

1. From the *Item List* in the *Review* window, click **Options**.
2. Click **Quick Filters > Show Ignorables**.

## Using the KFF Facets

You can use the KFF facets to filter data based on KFF values. For example, you can apply a facet to only display items with an Alert status or with a certain KFF set.

See [About Filtering Data with Facets](#) on page 128.

---

**Note:** If you configured the project to skip Ignorable files, these files are not included in the data and the *Ignore* facet is not available. If you configured the project to flag Ignorable files, and the *Hide Ignorables* Quick Filter is set, the *Ignore* facet is available, but the files will not be displayed.

---

See [Using Quick Filters](#) on page 222.

You can use the following KFF facets:

- KFF Vendors
- KFFGroups
- KFF Statuses
- KFF Sets

Within a facet, only the filters that are available in the project are available. For example, if no files with the Alert status are in the project, the Alter filter will not be available in the KFF Statuses facet.

### To apply KFF facets

1. From the *Item List* in the *Review* window, open the facets pane.
2. Expand **KFF**.
3. Select the facets that you want to apply.

## Viewing Detailed KFF Data

You can view KFF results details for an individual file.

The screenshot shows a web interface for viewing file details. At the top, there is a 'Detail Information' header with four tabs: 'Archived Details', 'Cerberus', 'KFF Details' (which is highlighted in red), and 'Evidence Source'. Below the tabs, there are three main sections:

- File Details:** Contains fields for 'Filename' (Southern Pinwheel - Alert KFF.jpg), 'File size (bytes)' (10753), 'SHA1' (99b9f4f78aab28f5157d0f9b38d86be8d68cf039), 'MD5' (2cf62ee23f20b99a6c970608386d2381), and 'Fuzzy Hash' (SHA2, etc).
- KFF Details:** Contains fields for 'Category', 'Sub-Category', 'Reference 1', 'Reference 2', 'Reference 3', 'Description', 'Created Date' (1/15/2014 12:05:52 PM), and 'User Created' (with a checked checkbox).
- Recent Changes:** Contains fields for 'Last Modified' (1/15/2014 12:05:52 PM) and 'Modified By'.

At the bottom of the panel, there is a row of view tabs: 'Natural', 'Image', 'Text', and 'Detail Information' (which is highlighted in yellow).

### To view the KFF Details

1. For a project that you have run KFF, open Project Review.
2. Under *Layouts*, select the **CIRT Layout**.  
See [Managing Saved Custom Layouts](#) on page 54.
3. In *Project Review*, select a file in the *Item List* panel.
4. In the view panel, click the **Detail Information** view tab.
5. Click the **KFF Details** tab.



# Re-Processing KFF

After you have processed a project with KFF enabled, you can re-process your data using an updated or different KFF Group. This is useful in re-examining a project after adding or editing hash sets.

See [Adding Hashes to Hash Sets Using Project Review](#) on page 213.

If you want to re-process KFF with updated hash sets, be sure that the selected KFF Group has the desired sets.

You can only select from existing KFF Groups.


## To re-process KFF

1. From the *Home* page, select a project that you want to re-process.

2. Click the  tab.

The currently selected group is displayed along with its corresponding hash sets.

3. (Optional) If you want to change the KFF Group, in the drop-down menu, select a different KFF Group and click **Save**.
4. In the Hash Sets pane, verify that the desired sets are included.
5. Click **Process KFF**.

6. (Optional) On the *Home* page, for the project, click *Work Lists*  , and verify that the KFF job starts and completes.  
See [Monitoring the Work List](#) on page 308.

7. Click *Refresh*  to see the current status.
8. Review the KFF results.  
See [Reviewing KFF Results](#) on page 221.

# Exporting KFF Data

## *About Exporting KFF Data*

You can share KFF Hash Sets and KFF Groups with other KFF Servers by exporting KFF data on one KFF Server and importing it on another. You can also use export as a way of archiving your KFF data.

You can export data in one of the following ways:

- Exporting Hash Sets - This exports the selected Hash Sets with any included hashes. (CSV format only)
- Exporting KFF Groups - This exports the selected KFF Groups with any included sub-groups and any included hashes. (CSV format only)
- Exporting an archive of all custom KFF data - This exports all the KFF data except NSRL, NIST, and DHC data (in a binary format).

When exporting KFF Groups or Hash Sets, you can export in the following formats:

- CSV file
- Binary format

**Important:** Even though it appears that you can select and export one Hash Set or one KFF Group, if you export using the KFF binary format, all of the data that you have in the *KFF Index* will be exported together. You cannot use this format to export individual Hash Sets or KFF Groups. Use the CSV format instead.

See [About CSV and Binary Formats](#) on page 196.

## *Exporting KFF Groups and Hash Sets*

You can share KFF hashes by exporting KFF Hash Sets or KFF Groups. Exports are saved in a CSV file that can be imported.

### **To export a one or more KFF Groups or Hash Sets**

1. Do one of the following:

- Click **Management** >  **Hash Sets**.

- Click **Management** >  **Groups**.

2. Select one or more KFF Groups or Hash Sets that you want to export.

3. Click **Export**.

4. Select **CSV** (do not select **Export Binary**).

5. Browse to and select the location to which you want to save the exported file.

6. Click **Select**.



7. Enter a name for the exported file.

8. Click **OK**.

9. In the *Export Summaries* dialog, view the status of the export.

10. Click **Close**.

## To create an archive of all your custom Hash Sets and Groups

1. Do one of the following:
  - Click **Management** >  **Hash Sets**.
  - Click **Management** >  **Groups**.
2. Select a KFF Group or Hash Set.
3. Click **Export**.
4. Select **Export Binary**.
5. Browse to and select the location to which you want to save the exported files.
6. Click **Select**.
7. Enter a name for the folder to contain the binary files (This is a new folder created by the export).
8. Click **OK**.
9. In the *Export Summaries* dialog, view the status of the export.
10. Click **Close**.

## To view the Export History

1. Do one of the following:
  - Click **Management** >  **Hash Sets**.
  - Click **Management** >  **Groups**.
2. Click **Export**.
3. Select **View Export History**.
4. In the *Export Summaries* dialog, view the status of the export.
5. Click **Close**.

## Part 4

# Managing Projects

This part describes how to manage projects and includes the following chapters:

- [Introduction to Project Management](#) (page 229)
- [Using the Project Management Home Page](#) (page 231)
- [Creating a Project](#) (page 245)
- [Managing Custodians for a Project](#) (page 261)
- [Managing Tags](#) (page 267)
- [Setting Project Permissions](#) (page 275)
- [Running Reports](#) (page 285)
- [Configuring Review Tools](#) (page 290)
- [Monitoring the Work List](#) (page 308)
- [Managing Document Groups](#) (page 310)
- [Managing Transcripts and Exhibits](#) (page 316)
- [Managing Review Sets](#) (page 328)
- [Project Folder Structure](#) (page 333)
- [Using Language Identification](#) (page 336)
- [Using KFF \(Known File Filter\)](#) (page 207)

## Chapter 16

# Introduction to Project Management

---

This guide is designed to help project/case managers perform common tasks. Project/case manager tasks are performed on the Home page and in Project Review. Project/case managers can perform their tasks as long as the administrator has granted the project manager the correct permission. See the Administrators guide for more information on how administrators can grant global permissions.

## About Projects

When you want to assess a set of evidence, you create a project and then add evidence to the project. When evidence is added to the project, the data is processed so that it can be later reviewed, coded, and labeled by a team of reviewers using the Project Review interface.

## Workflow for Project/Case Managers

Administrators, or users that have been given rights to manage projects, use the *Home* page of the console to create and manage projects by doing the following tasks.

### Basic Workflow for Project Managers

Task	Link to the tasks
Create a project	See <a href="#">Creating a Project</a> on page 245.
Configure the user/group permissions for a project	See <a href="#">Setting Project Permissions</a> on page 275.
Loading Data	You can load data using import or by processing the evidence into the system. See the Loading Data documentation for more information.
Manage evidence and people	See the Loading Data documentation.
Configure the review tools to be used in project review	See <a href="#">Configuring Markup Sets</a> on page 290. See <a href="#">Creating Category Values</a> on page 296. See <a href="#">Configuring Custom Fields</a> on page 294. See <a href="#">Configuring Highlight Profiles</a> on page 302.
View details about the project	See <a href="#">Viewing and Editing Project Details</a> on page 259.

## Basic Workflow for Project Managers (Continued)

Task	Link to the tasks
Monitor the Work List	See <a href="#">Work List Tab</a> on page 308. See <a href="#">Monitoring the Work List</a> on page 308.
Manage Document Groups	See <a href="#">Managing Document Groups</a> on page 310.
Upload Transcripts/Exhibits	See <a href="#">Updating Transcripts</a> on page 317.
Create Production Sets	See the Exporting documentation.
Export the selected evidence	See the Exporting documentation.
Run reports	See <a href="#">Running Reports</a> on page 285.

## Chapter 17

# Using the Project Management Home Page

---

## Viewing the Home Page

Administrators, and users given permissions, use the *Home* page to do the following:

- Create projects
- View a list of existing projects
- Add evidence to a project
- Launch Project Review

If you are not an administrator, you will only see either the projects that you created or projects to which you were granted permissions.

### To view the home page

1. Log in to the console.
2. In the application console, click **Home**.  
The Project List Panel is on the left-side of the page.

See [The Project List Panel](#) on page 233.

Administrators, and users with the Create/Edit Projects permission, create projects to add and process evidence.

See [About Projects](#) on page 229.

# Introducing the Home Page

The project management Home page is where you see the Project list and details about the project.

## Home Page

**Project List Panel**

Project Name	Action	Processing Status	Size
01Case	+	Completed	6.5 MB
01FamilyData	+	Completed	3.7 MB
02Case	+	Completed	4.7 MB
02FamilyData	+	Completed	2.8 MB
03FamilyData	+	Completed	2.8 MB
AgiCase1	+	Completed	1.9 MB
AgiCase2	+	Completed	5.6 MB
BG1	+	Completed	420 MB
BG2	+	Completed	508 MB
DJ-30207	+	Completed	3.6 MB
EP Case1	+	Completed	23 MB
Search	+	Completed	1.3 MB
TopTenWorkflows	+	Completed	9.5 MB

**Project Details for BG2**






Name: BG2  
 Creation Date: 9/17/2013 12:22:06 PM  
 Created By: bguptha1  
 Last Modified By: bguptha1  
 Project Folder Path: \\10.10.4.126\Summation\Cases\c69dec55-19d7-4  
 Job Data Path: \\10.10.4.126\Summation\JobData  
 FTK ID: 3  
 Priority:  Low  Normal  High

**Project Manager Task Tabs**

	Count	Size
eDocs	252 (8%)	43 MB (8%)
Email	3,072 (92%)	464 MB (92%)
OCR	0 (0%)	0 Byte(s) (0%)
Encrypted Items	0 (0%)	0 Byte(s) (0%)
KFF	0 (0%)	0 Byte(s) (0%)
Evidence Items	0	0
Processed	3,077 (93%)	507 MB (100%)
Extracted Files	126 (4%)	309 MB (61%)
Extracted Attachments	565 (17%)	182 MB (36%)
Zero byte files	25 (1%)	n/a
Non-searchable PDFs	0 (0%)	0 Byte(s) (0%)
Person	1	n/a


**Summary:**  
 Total Process Count: 3,324  
 Total Processed Size: 507 MB  
 Total Processing Time: 0.00:02  
 Total Processing Jobs: 2  
 Project Creation Date: September 17, 2013

## Elements of the Home Page

Elements	Description
Project List Panel	See <a href="#">The Project List Panel</a> on page 233.
Project Details 	See <a href="#">Viewing and Editing Project Details</a> on page 259.
Jobs 	See <a href="#">Introduction to Jobs</a> on page 418.
Evidence 	The evidence in the project. See <a href="#">Evidence Tab</a> on page 236.
People 	People that are associated to the project. You can add people and associate and disassociate people to the project. See <a href="#">Managing People for a Project</a> on page 240. In the <i>Evidence</i> tab at the bottom, you can also see any people that have been associated to specific evidence within the project.
Tags 	See <a href="#">Managing Tags</a> on page 267.



## Elements of the Home Page (Continued)

Elements	Description
Permissions 	See <a href="#">Setting Project Permissions</a> on page 275.
Reports 	See <a href="#">Running Reports</a> on page 285.
Processing Options 	The processing options used for the project. See <a href="#">Evidence Processing and Deduplication Options</a> on page 248.
KFF 	See <a href="#">Using KFF (Known File Filter)</a> on page 207..
Printing/Export 	See <a href="#">Introduction to Exporting Data</a> on page 257.
Lit Hold 	You can use Lit Hold if you have an AccessData eDiscovery license or if you have purchased a special licence for Summation. See <a href="#">Using Litigation Holds</a> on page 339.
Markup Sets 	See <a href="#">Configuring Markup Sets</a> on page 290.
Tagging Layout 	See <a href="#">Configuring Tagging Layouts</a> on page 297.
Highlight Profiles 	See <a href="#">Configuring Highlight Profiles</a> on page 302.
Work List 	See <a href="#">Monitoring the Work List</a> on page 308.
Custom Fields 	See <a href="#">Configuring Custom Fields</a> on page 294.
Redaction Text 	See <a href="#">Configuring Redaction Text</a> on page 306.

## The Project List Panel

The *Home* page includes the *Project List* panel. The *Project List* panel is the default view after logging in. Users can only view the projects for which they have been given permissions.

Administrators and users, given the correct permissions, can use the project list to do the following:





- Create projects.
- View a list of existing projects.

- Add evidence to a project. See [Importing Data](#) on page 375.
- Launch Project Review.





If you are not an administrator, you will only see either the projects that you created or projects to which you were granted permissions.

The following table lists the elements of the project list. Some items may not be visible depending on your permissions.

### Elements of the Project List

Element	Description
Create New Project	Click to create a new project.
Filter Options	Allows you to search and filter all of the projects in the project list. You can filter the list based on any number of fields associated with the project, including, but not limited to the project name. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Project Name Column	Lists the names of all the projects to which the logged-in user has permissions.
Status Column	Lists the status of the projects: Not Started - The project has been created but no evidence has been imported. Processing - Evidence has been imported and is still being processed. Completed - Evidence has been imported and processed. <b>Note:</b> The Processing Status may show a delay of two minutes behind the actual processing of the evidence. This is only noticeable when processing a small set of evidence. See Refresh below.
Size Column	Lists the size of the data within the project.
Action Column	Allows you to add evidence to a project or enter Project Review.
 Add Data	Allows you to add data to the selected project.
 Project Review	Allows you to review the project using Project Review. See the Reviewers Guide for more information.
Page Size Drop-down	Allows you to select how many projects to display in the list. The total number of projects that you have permissions to see is displayed.
Total	Lists the total number of projects displayed in the Project List.
Page	Allows you to view another page of projects.
 Refresh	If you create a new project, or make changes to the list, you may need to refresh the project list
 Custom Properties	Add, edit, and delete custom columns with the default value that will be listed in the Project list panel. When you create a project, this additional column will be listed in the project creation dialog. See <a href="#">Adding Custom Properties</a> on page 238.

## Elements of the Project List (Continued)

Element	Description
 Project Property Cloning	Clone the properties of an existing project to another project. You can apply a single project's properties to another project, or you can pick and choose properties from multiple individual projects to apply to a single project. See <a href="#">Using Project Properties Cloning</a> on page 258.
 Export to CSV	Export the Project list to a .CSV file. You can save the file and open it in a spreadsheet program.
 Columns	Add or remove viewable columns in the <i>Project List</i> .
 Delete	Highlight project and click <b>Delete Project</b> to delete it from the <i>Project List</i> .

# Evidence Tab

Users with permissions can view information about the evidence that has been added to a project. To view the *Evidence* tab, users need one of the following permissions: administrator, create/edit project, or manage evidence.

## Evidence Tab

The screenshot displays the Evidence Tab interface. At the top, there is a toolbar with various icons. Below it is a 'Filter Options' section. The main area contains a table with columns for Path, Description, and Evidence Type. The table lists four evidence items, with the third item selected. To the right of the table is the 'External Evidence Details' panel, which shows fields for Path, Description, Evidence Type, Associated Person Name, Created By, and Created Date. Below the table is a pagination control showing 'Page Size: 15' and 'Total: 4'. At the bottom of the interface is a 'Processing Status' section with tabs for 'General' and 'Progress', and fields for 'Error Messages' and 'Messages'.

Path	Description	Evidence Type
\\cvg-dcstorage\cases\Agi\doc		Native
\\cvg-dcstorage\cases\Agi\doc		Native
\\cvg-dcstorage\cases\TestData_Load\DII\CVG7_002\CVG7_002_img01.tif		Native
\\cvg-dcstorage\cases\TestData_Load\Sally\Small Control Set\gmail.pst		Native

**External Evidence Details**

Path: \\cvg-dcstorage\cases\TestData\_Load\DII\CVG7\_002\CVG7\_002\_img01.tif

Description: [Empty field]

Evidence Type: Native

Associated Person Name: [Empty field]

Created By: Administrator

Created Date: 12/8/2011 9:01:42 PM


Page Size: 15 Total: 4 Page 1 of 1

Processing Status: [General] [Progress]


Error Messages: [Empty field]

Messages: [Empty field]

## Elements of the Evidence Tab

Element	Description
Filter Options	Allows the user to filter the list.
Evidence Path List	Displays the paths of evidence in the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Groups List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.

## Elements of the Evidence Tab (Continued)



Element	Description
Columns 	Adjusts what columns display in the Groups List. See <a href="#">Sorting by Columns</a> on page 36.
External Evidence Details	Includes editable information about imported evidence. Information includes: <ul style="list-style-type: none"><li>• That path from which the evidence was imported</li><li>• A description of the project, if you entered one</li><li>• The evidence file type</li><li>• What people were associated with the evidence</li><li>• Who added the evidence</li><li>• When the evidence was added</li></ul>
Processing Status	Lists any messages that occurred during processing.

# Adding Custom Properties

With Custom Properties, you can add, edit, and delete custom columns with the default value that will be listed in the Project list panel. When you create a project, these additional columns will be listed in the project creation dialog and will be available to populate when editing projects that have already been created.

When you create a new project, any custom properties marked as required will be available at the top of the Create New Project dialog, while non-required custom properties will be at the bottom of the dialog. When you edit an existing project, all custom properties will be at the bottom of the pane, whether they are required or not. However, the required custom properties will be bolded to differentiate from non-required custom property fields.




## To add a custom Properties

1. In the console, in the Project List, click  **Custom Properties**.
2. Click  **Add**.
3. Configure the custom property details and click **OK**.



## Custom Properties

The following table lists the options available to you in the Custom Properties dialog:

### Custom Properties Dialog

Element	Description
	Allows you to add a custom property.
	Allows you to edit a custom property.
	Allows you to delete a custom property.
Name	This is a required field for a new custom property.
Description	This field is optional.
Required Field	Mark to make the custom property a required column. If the custom property column is a required field, any previously created project must have this field populated when you edit the project.
Type	Choose whether the column is a text field or a choice field
Text	Choose to make the custom property field a text field.
Default Value	When this field is populated for text custom properties, the Default Value will display on all existing projects.
Choice	Choose to make the custom property field a choice field. Enter one choice per line, separated by the Enter key. The first choice listed in the choice field will be the default for all projects. If you do not want the first choice to be the default choice, leave the first line blank.

### Custom Properties Dialog (Continued)

Element	Description
	Allows you to refresh the Custom Properties list.
	Allows you to delete a custom property.

# Managing People for a Project

## About People

The term “person” references any identified person or custodian who may have data relevant to evidence in a project. You can associate people to a specific project and to specific evidence items within that project.

In Review, you can use the *Person* column to see the person that is associated with each item. You can sort, filter, and search using the *Person* column.

---

**Note:** A person references people that are associated with evidence, they are not the users of the Summation product.

---

## About Managing People

When you manage people, you do the following:

- Create a person
- Edit the properties of a person
- Delete a person
- Associate a person with or dis-associate a person from a project
- Associate a person to a specific evidence item.

You can create a person in the following ways:

- Using the *People* tab on the *Data Sources* page. This creates people at a global level which can be associated with any project.  
See the *Data Sources* chapter.
- Using the *People* tab on the *Home* page. This creates people for a specific project.  
See [Adding People](#) on page 242.
- Using the *Add Evidence Wizard*.  
See [About Associating People with Evidence](#) on page 378.

For the most functionality of managing people, there are more options on the *Data Sources* page than on the *Home* page. For example, on the *Data Sources* page, you can delete People and add them using

You associate people to projects in the following ways:

- Associate a person to a whole project when you create a project.  
See [Creating Projects](#) on page 245.
- Associate a person to a whole project after you create a project.  
See [Associating a Project to a Person](#) on page 244.
- Associate a person to specific evidence that you add to a project.  
See [About Associating People with Evidence](#) on page 378.



## About the Project's Person Tab



You can manage people for a project from the **People** tab on the *Home* page. The people are listed in the *Person List*. The main view of the *Person List* includes the following sortable columns:

### People Information Options

Option	Description
First Name	The first name of the person.
Last Name	The last name of the person.
Username	The computer username of the person.
Email Address	The email address of the person.
Creation Date	The date that the person resource was created.
Domain	The network domain to which the person belongs.

When you create and view the list of people, this list is displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- Sort the columns
- Define a column on which you can sort.
- If you have a large list, you can apply a filter to display only the items you want.

See [Managing Columns in Lists and Grids](#) on page 37.

Highlighting a person in the list populates the **Person Details** info pane on the right side. The **Person Details** info pane has information relative to the currently selected person, beginning with the first name.








At the bottom of the page, you can use the *Evidence* tab to view the evidence that person is associated with.

## Project's Person Tab Options

The following table lists the various options that are available under the *Person* tab.

**Note:** To import people from Active Directory or to delete a person, use the *Data Sources* page.

### Person Tab Options

Element	Description
Filter Options	Allows you to filter the person list. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Add 	Click to add a person. See <a href="#">Adding People</a> on page 242.
Edit 	Click to edit a person. See <a href="#">Editing a Person</a> on page 243.
Refresh 	Click to refresh the person list.
Import People 	Click to import people from a CSV file. See <a href="#">Importing People From a CSV File</a> on page 244.
Export to CSV 	Export the current set of data to a CSV file.
Columns 	Click to adjust what columns display in the Person List. See <a href="#">Managing Columns in Lists and Grids</a> on page 37.
Evidence 	Allows you to view evidence that has been associated to a person. In the <i>Evidence</i> pane, you can do the following: <ul style="list-style-type: none"><li>• Filter the Evidence list.</li><li>• Add Custom Properties. See <a href="#">Adding Custom Properties</a> on page 238.</li><li>• Export the <i>Evidence</i> list to a CSV file.</li><li>• Adjust the columns' display in the <i>Evidence</i> list.</li><li>• See <a href="#">Managing Evidence for Collecting Data</a> on page 143.</li></ul>

## Adding People

Administrators, and users with permissions, can add people.

You can add people in the following ways:

- Manually adding people
- Importing people from a file  
See [Importing People From a CSV File](#) on page 244.
- Creating or importing people while importing evidence  
See [Managing Evidence for Collecting Data](#) on page 143.


- Importing people from Active Directory.  
See [Adding People Using Active Directory](#) on page 143.

### People Information Options

Option	Description
First Name	The first name of the person. This field is required.
Middle Initial	The middle initial of the person.
Last Name	The last name of the person. This field is required.
Username	The computer username of the person. This field is required.
Domain	The network domain to which the person belongs.
Notes Username	The username of the person as it appears in their Lotus Notes Directory. A Lotus Notes username is typically formatted as Firstname Lastname/Organization as in the following example: Pat Ng/ICM
Email Address	The email address of the person.

## Manually Creating People for a Specific Project


### To manually create a person

4. On the **Home > Data Sources > People** tab, click  **Add**.
5. In *Person Details*, enter the person details.
6. Click **OK**.

## Editing a Person

You can edit any person that you have added to the project.

### To edit a project-level person


1. On the **Home > Data Sources > People** tab, select a person that you want to edit.
2. Click  **Edit**
3. In *Person Details*, edit person details.
4. Click **OK**.

## Importing People From a CSV File

From the *People* tab, you can import a list of people into the system from a CSV file. Before importing people from a CSV file, you need to be aware of the following items:

- You must define any custom columns before importing the CSV file. See [Adding Custom Properties](#) on page 238.
- Make sure that your columns have headers.
- Multiple items in columns must be separated by semicolons.

### To import people from a CSV file

1. On the **Home > People** tab, click  **Import People**.
2. From the *Import People from CSV* dialog, choose from the following options:
  - **Import custom columns.** This option is not available if custom columns have not been previously defined.
  - **Merge into existing people.** This option will overwrite fields, such as first name, last name, and email address. It also adds new computers, network shares, etc. to existing associations.

---

**Note:** For an entry to be considered a duplicate in the External Evidence column, the network path, assigned person, and type (such as image or native file) must be the same. If there are any differences between these three fields, the entry is brought in as a new External Evidence item.

---

- **Download Sample CSV.** This allows you to download a sample CSV file illustrating how your CSV file should be created. This example is dynamic; if you have created custom columns for people, those custom columns appear in the sample CSV file.

---

**Note:** If your license does not support certain features (such as network shares or computers), the columns for those items appear in the CSV without any data populated in the columns.





---

3. Once options have been selected, click **OK**.
4. Browse to the CSV file that you want to upload.
5. After file has been uploaded, a *People Import Summary* dialog appears. This displays the number of people added, merged, and/or failed, with details if an import failed. Click **OK**.

## Associating a Project to a Person

From the *Projects* pane under the *Person* tab, you can associate and disassociate projects to a selected person.

### To associate a project to a person

1. In the *Person* list pane, click  to add people.
2. In the *Associate People to <Project>* dialog, do one of the following:
  - In the *All People* pane, click  to add projects to the *Associated People* pane.
  - In the *All People* pane, click  to projects from the *Associated People* pane.
3. Click **OK**.
4. (optional) Click  to remove people from an associated project.

# Chapter 18

## Creating a Project

---

### Creating Projects

Administrators and project managers with the *Create Project* admin role can create projects from the Project List panel.

#### To create a new project

1. Log in as an administrator or as a user that has permissions to create projects.
2. Click **Create New Project**.
3. In the *Create New Project* page, on the *Info* tab, configure the general project properties.  
See [General Project Properties](#) on page 246.
4. (Optional) Click the **People** tab to add people to the project.  
This is where you configure the people who are the custodians of the evidence in this project. You can associate existing people or, if you have proper permissions, create new people. People for the project can be configured later, but should be done before processing evidence. See [Managing People \(Custodians\) as Data Sources](#) on page 137.
5. Click the **Processing Options** tab to set the processing options for the project.  
This is where you set the options for how the evidence is processed when it is added to the project. This setting may have a default value that you can use or change, or this setting may be configured and hidden by the administrator.  
See [Evidence Processing and Deduplication Options](#) on page 248.

---

**Note:** You cannot change the processing options after you have created the project.

---

6. Select one of the following options:
  - **Create Project:** Click to create the project without importing evidence. This option will create the project and return you to the Project Management page. You can then configure the project by adding evidence, assigning permissions, and so on.
  - **Create Project and Import Evidence:** Click to create the project and begin importing evidence. See the Loading Data documentation for information on how to import evidence.

## General Project Properties

You can set the properties of the specific project.

Many of the fields may be populated by values set in the **Project Defaults** configuration block under the *Management* tab. See [Configuring Default Project Settings](#) on page 83. The following table describes the general Project Properties.

### General Project Info Properties Options

Option	Description
Project Name	Project Names must be only alphanumeric characters. Special characters will cause the project creation to fail.
Description	(Optional) This option allows you to enter the description of the project.
Project Folder Path	Allows you to specify a local path or a UNC network path to the project folder. This path is the location where all project data is stored. <b>Note:</b> This setting may have a default value that you can use or change, or this setting may be configured and hidden by the administrator. For example, a folder with the Project name can be created in the actual directory to be identified and managed easily. You then change the path to reflect and include the new directory. See the Admin Guide for information on configuring <i>Default Evidence Folder Options</i> .
Job Data Path	<ul style="list-style-type: none"><li>• When used with Summation, this sets the path used to store some reports.</li><li>• When used with eDiscovery, this sets the responsive folder path for data from jobs. Under this path, a folder is created for each job. The job sub-folders contain job reports and ad1 files for collected files.</li></ul> See <a href="#">Job Options Tab</a> on page 428.
Display Time Zone	This option allows you to display the dates and times of files and emails based on this specified time zone. For example, if data was collected in the Eastern Time zone, you can select to display times in the Pacific Time zone and all dates will be offset by four hours to display in PST. The default is set for (UTC) Coordinated Universal Time. See <a href="#">Normalized Time Zones</a> on page 247.
Sort Evidence Items By	You can set the default column that you want to sort by when opening <i>Project Review</i> . You select the default column and then select the default sorting order: ascending or descending. The setting is project-specific and not user specific. In <i>Review</i> , you can still click any column to sort on. See <a href="#">Sorting by Columns</a> on page 36.
Sub Administrator	(Summation only) If you are using the multi-tenant environment, you can assign this project to a Sub Admin environment. See <a href="#">Understanding the Multi-Tenant Environment</a> on page 338.
Copy Properties from Existing Project	(Optional) This allows you to apply properties of an existing project to the newly created project. You can also apply properties to an existing project once it has been created. See <a href="#">Using Project Properties Cloning</a> on page 258.

## Normalized Time Zones

All data brought into a project using evidence processing or a collection job is stored in UTC time zone. You can configure a *Display Time Zone* for the project that will offset the times and display them in the specified time zone.

See [Display Time Zone](#) on page 246.

However, all data brought into a project using import load files is stored in the time setting that the data was created which causes an issue when trying to set the correct display time zone. The following features help you normalize time zone data.

- When adding data to the case through evidence processing or collection from a FAT storage device, you need to select the proper time zone for the device so that the data can be normalized to UTC.
- No adjustment is needed for data added to the case from NTFS storage devices.
- The columns in the *Item List* grid will display the UTC time zone.
- During load file import, you must choose the time zone that the load file was created with so the date and time values can be converted to a normalized UTC value in the database.

See [Importing Evidence into a Project](#) on page 386.

When you set a time zone display value for each project, you will be able to see the date and times when certain events occurred. The following types of dates are displayed in the configured time zone rather than in UTC:

- Natural View for email - Email To and From dates
- Images for email
- File creation, modified and accessed dates
- Items in the Item List grid including filtered columns
- Items in Panels
- Search

When creating a project, and specifying a Display Time Zone, that time zone is used when performing searches on metadata. For example, when searching for an email receive date, it will offset all of the UTC dates to the specified time zone for the search.

- Facets
- Conversation Panel and Conversation View x
- Time Zone adjustments for emails that have been converted to SWF or TIFF

When the case is set with a specific time zone setting, documents that are converted to SWF or TIFF display the selected time zone in the display-able date fields.

This will primarily affect email sent and received dates as most other document types do not have dynamic date values displayed in the body of the document.

- Regional Formatting for DocDate and NoteDate Fields  
You can now see the DocDate and NoteDate field values in a dd/mm/yyyy format.
- Date and Time offset in Search

When creating a project, and specifying a Display Time Zone, that time zone is used when performing searches on metadata. For example, when searching for an email receive date, it will offset all of the UTC dates to the specified time zone for the search.

- Load files with date and time fields

## Evidence Processing and Deduplication Options

The options you select determine the data that is contained in projects, reports, and consequently, production sets. When you create a project, you can specify unique options or use the default options. Options that increase processing time when selected are marked by a turtle icon.

See the *Configuring the System* chapter in the *User Guide*.

---

**Note:** You cannot edit any settings on the **Processing Options** section after you have added evidence to a project

---

The following table describes the **Processing Options**. Depending on the license that you own, you may some or all of the following options.

See [About Deduplication](#) on page 253.

### Processing Options

Option	Description
<b>Processing Mode</b>	
<i>Standard Mode</i>	<p>Enabled by default. Enables the default processing options. <b>Note: These defaults are not editable.</b> Will include:</p> <ul style="list-style-type: none"><li>• Hashing</li><li>• Deduplication - Project level for both Documents and Email</li><li>• File Signature Analysis</li><li>• Expand Compound Files (archive expansion) of the following file types: 7-ZIP, IPD, BZIP2, DBX, PDF, GZIP, NSF, MBOX, MS Exchange and Office documents, MSG, PST, RAR, RFC822 Internet email, TAR, ZIP</li></ul> <p><b>Note: You cannot expand system image files, such as AD1 and E01, if they are located inside of another archive. You must first export the files and add the files as evidence to be properly processed.</b></p> <p>Will index:</p> <ul style="list-style-type: none"><li>• Text data</li></ul> <p>Will not index:</p> <ul style="list-style-type: none"><li>• Graphic files and executable files</li></ul> <p>Will refine out:</p> <ul style="list-style-type: none"><li>• Microsoft OLE Streams</li><li>• Office 2010 package contents</li><li>• File slack</li><li>• Free space</li><li>• Deleted items</li><li>• Zero length files</li><li>• OS/File System Files</li></ul>



## Processing Options (Continued)

Option	Description
<i>Standard No Search</i>	<p>Uses the default processing options but does not include the indexing of text data.</p> <p>See <a href="#">About Indexing for Text Searches of Content of Files</a> on page 255.</p>
<i>Forensic</i>	<p>Will include:</p> <ul style="list-style-type: none"> <li>• Hashing (MD-5, SHA-1, SHA-256)</li> <li>• Flag bad extensions</li> <li>• Thumbnails for graphics</li> <li>• Deleted files</li> <li>• Microsoft OLE Streams</li> <li>• Microsoft OPC documents</li> <li>• Refinement options: <ul style="list-style-type: none"> <li>■ File slack</li> <li>■ Free space</li> </ul> </li> </ul> <p>Will index:</p> <ul style="list-style-type: none"> <li>• all file types</li> </ul> <p>Will not include:</p> <ul style="list-style-type: none"> <li>• KFF (for faster processing)</li> <li>• Expand Compound Files (archive expansion)</li> <li>• HTML file listing</li> <li>• eDiscovery Deduplication</li> </ul>
<i>Quick</i>	<p>Increases the speed of the processing of evidence by using minimal options to expedite the processing.</p> <p>Indexing, hashing, archive file drill down, and file identification are disabled. (Files are identified by header analysis instead of file extension.)</p> <p>If you select this option, the <i>KFF Lookup</i> option is disabled. Disabling <i>KFF Lookup</i> occurs because <i>Field Mode</i> is a processing option that is intended to speed up the process. It turns off indexing, hashing, and other options that tend to slow down data processing. The <i>KFF Lookup</i> option takes time to process and slows down data processing. Therefore, if both <i>Field Mode</i> and <i>KFF Lookup</i> were both enabled, it would defeat the purpose of the Quick option.</p>

## Processing Options (Continued)

Option	Description
<p><i>Security</i></p>	<p>Enables the default security processing options. Will include:</p> <ul style="list-style-type: none"> <li>• Hashing</li> <li>• Indexing</li> <li>• eDiscovery Deduplication - Project level for both Documents and Email</li> <li>• File signature analysis</li> <li>• Expand Compound Files (archive expansion) of the following file types: 7-ZIP, IPD, BZIP2, DBX, PDF, GZIP, NSF, MBOX, Microsoft Exchange, MS Office documents, MSG, PST, RAR, RFC822 Internet email, TAR, ZIP, EMFSPool, EXIF, ThumbsDB, TMbLIST, ThumbCacheDB, NTDS, SQLITE, and PKCs7</li> </ul> <p>Will refine out:</p> <ul style="list-style-type: none"> <li>• File slack</li> <li>• Free space</li> <li>• Deleted items</li> <li>• Microsoft OLE Streams</li> <li>• Office 2010 package contents</li> <li>• Zero length files</li> <li>• OS/File System Files</li> </ul> <p>Will not index:</p> <ul style="list-style-type: none"> <li>• Graphic files</li> </ul> <p><b>Note:</b> In the Job Wizard, collection jobs executed in projects with standard processing selected have Auto Processing selected by default. See <a href="#">Job Options Tab</a> on page 428.</p>
<p><b>Optical Character Recognition</b></p>	
<p><i>Enable OCR</i></p>	<p>Generates text from graphics files and indexes the resulting content. You can then use <i>Project Review</i> to search and label the content and treat that content the same as any other text in the project.</p> <p>AccessData uses the GlyphReader engine for optical character recognition. Selecting this option can increase processing time up to 50%. It also may give you results that differ between processing jobs on the same computer, with the same piece of evidence.</p> <p>Pre-set default is off.</p> <p>See <a href="#">About Optical Character Recognition (OCR)</a> on page 255.</p> <p>Enabling this option may increase processing times.</p>
<p><b>General Email Options</b></p>	
<p><i>Expand Embedded Graphics</i></p>	<p>Pre-set default is off. Enabling this option may increase processing times.</p>
<p><b>KFF (Known File Filter)</b></p>	
<p><i>Enable KFF</i></p>	<p>Enables the Known File Filter (KFF). See <a href="#">Using KFF (Known File Filter)</a> on page 207. Pre-set default is on.</p>

## Processing Options (Continued)

Option	Description
<b>Email Body Caching</b>	
<i>Enable Email Body Caching</i>	This option will speed up load file generation. Pre-set default is off. Enabling this option may increase processing times.
<b>Advanced Options</b>	Enabled by default. <i>Keep the database indexes while processing.</i> Database indexes improve performance, but slow processing when inserting data. If this option is checked, all of the data reindexes every time more data is loaded. Only select this option if you want to load a large amount of data quickly before data is reviewed.
<b>Standard Viewer</b>	
<i>Enable Standard Viewer</i>	The option does the following: <ul style="list-style-type: none"> <li>Generates files that can be annotated and redacted (SWF format). SWF files are generated for most all user-created processed documents such as .DOC, .PPT, .MSG, and so forth (not .XLS). This enables you to work on a file in <i>Review</i> without waiting for a SWF file to be created. SWF files are generated for documents with a size of 1 MB and larger.</li> <li>Makes the <i>Standard Viewer</i> the default viewer in <i>Review</i>.</li> </ul> For more information, see <i>Using the Standard Viewer and the Alternate File Viewer</i> in the <i>Viewing Data</i> chapter. This option is checked as the default for the Summation license, but can be enabled in other products. <b>Note: This option slows processing speeds.</b>
<b>Video Files</b>	
<i>Enable Video Conversion</i>	Enabled by default. When you process the evidence in your case, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be viewed in the Natural Panel. All converted videos are stored in the case folder. You can define the following: <ul style="list-style-type: none"> <li>Bit rate</li> <li>Video resolution</li> </ul>
<b>Generate Thumbnails</b>	Enabled by default. Creates thumbnail images for each video file in a project. These thumbnails can be seen in the <i>Thumbnails View</i> in <i>Review</i> . The thumbnails let you quickly examine a portion of the contents within video files without having to watch the full content of each media file. You can define the thumbnail generation interval based on one of the following: <ul style="list-style-type: none"> <li>Percent (1 thumbnail every “n” % of the video)</li> <li>Interval (1 thumbnail every “n” minutes of the video)</li> </ul> This feature can be used when you choose the <i>Standard</i> , <i>Standard No Search</i> , or <i>Forensic</i> processing modes. This is not available when using the <i>Security</i> or <i>Quick</i> processing mode. This is also not available for import loaded files.
<b>Miscellaneous Options</b>	

## Processing Options (Continued)

Option	Description
<i>Geolocation</i>	Allows you to view processed evidence in the Geolocation Visualization filter. <b>Note:</b> Geolocation IP address data may take up to eight minutes to generate, depending upon other jobs currently running in the application.
<i>Generate Image Thumbnails</i>	Generates thumbnails for all image files in the project. These thumbnails can be viewed in the <i>Thumbnail View</i> in <i>Review</i> . This option is enabled by default with the <i>Standard</i> , <i>Standard No Search</i> , and <i>Forensic</i> Processing Modes.
<b>Timeline Options</b>	
<i>Expand Additional Timeline Events</i>	Lets you expand Log2Timeline, Event Logs, Registry, and Browser History. For example, this will recognize CSV files that are in the Log2Timeline format and parses the data within the single CSV into individual records within the case. The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data.  In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis. When you expand CSV files into separate records, you can use several new columns in the Item List to view each CSV Log2Timeline field.
<b>Indexing Options</b>	
<i>Disable Tag Indexing</i>	Summation license only. This option is enabled by default. This option disables the reindexing of labels, categories, and issues for projects. This allows the project to process more quickly. This option only applies to new projects. If enabled, after processing, the following text is displayed in <i>Review</i> : <i>Tag indexing is disabled.</i>
<b>Document Deduplication</b>	See <a href="#">About Deduplication</a> on page 253.
<b>Email Deduplication</b>	See <a href="#">About Deduplication</a> on page 253.
<b>Document Analysis Options</b>	You can perform an automatic cluster analysis of documents and emails which provides grouping of email and documents by similar content. See <a href="#">Using Cluster Analysis</a> on page 408. You can configure the number of paired keywords that are stored for the comparison of documents during cluster analysis and predictive coding. For performance reasons, the default number of keyword storage is 30 keywords. This can limit the effectiveness of cluster analysis or predictive coding. You can increase the number of pairs, but this will impact the time needed for processing.
<i>Max Keyword Pairs</i>	You can change the number of allowable pairs by a set number or select <i>Unlimited</i> .
<i>Cluster Analysis</i>	Enabled by default. <i>Perform Cluster Analysis:</i> Enables the extended analysis of documents to determine related, near duplicates, and email threads. See <a href="#">Using Cluster Analysis</a> on page 408. You can view the similarity results in the <i>Similar Panel</i> in <i>Review</i> .

## Processing Options (Continued)

Option	Description
<i>Entity Extraction</i>	Enabled by default. Identifies and extracts specific types of data in your evidence. You can process and view each of the following types of entity data: <ul style="list-style-type: none"><li>• Credit Card Numbers</li><li>• Email addresses</li><li>• People</li><li>• Phone Numbers</li><li>• Social Security Numbers</li></ul> See <a href="#">Using Entity Extraction</a> on page 411. In <i>Review</i> , under the <i>Document Content</i> facet category, there is a facet for each data type that you extracted.
<b>Language Identification</b>	See <a href="#">Using Language Identification</a> on page 336.
<i>None</i>	Enabled by default. Performs no language identification, all documents are assumed to be written in English. This is the faster processing option.
<i>Basic</i>	Performs language identification for English, Chinese, Spanish, Japanese, Portuguese, German, Arabic, French, Russian, and Korean.
<i>Extended</i>	Performs language identification for 67 different languages. This is the slowest processing option.

## About Deduplication

Deduplication helps a project investigation by flagging duplicate electronic document (e-document) files and emails within the data of a project or person. The duplicates filter, when applied during project analysis, removes all files flagged “True” (duplicate) from the display, significantly reducing the number of documents an investigator needs to review and analyze to complete the project investigation.

If you set document deduplication at the project level, and two people have the same file, one file is flagged as primary and the other file or files are flagged as duplicates. The file resides in the project and the file paths are tracked to both people. To limit the production set, the file is only created one time during the load file/native file production. You can also deduplicate email, marking the email, email contents, or email attachments as duplicates of others.

---

**Note:** In *Project Review*, if the duplicate filter is on, and if you perform a search for a file using a word that is part of the file path, and that path and file name is a duplicate, the search will not find that file. For example, there is a spreadsheet that is located in one folder called Sales and a duplicate of the file exists in a folder called Marketing. The file in Sales is flagged as the primary and the file in Marketing is flagged as a duplicate. If you do a search for spreadsheets in the folder named Sales, it is found. However, if you do a search for spreadsheets in the folder named Marketing, it is not found. To locate the file in the Marketing folder, turn off the duplication filter and then perform the search.

---

See [Evidence Processing and Deduplication Options](#) on page 248.

Deduplication options are integrated on the *Processing Options* page.

The following tables describe the deduplication options that are available in the *Processing Options*.

### Document Deduplication Options

Option	Description
No Deduplication	Processes the project without document deduplication. This feature allows the case to process more quickly. This option is the default for Security processing.
Project Level	Deduplication compares each of the e-documents processed within a project against the others as they receive their hash during processing. If the hash remains singular throughout processing, it receives no duplicate flag. In the project of duplicate files, the first hash instance receives a “primary” flag and each reoccurrence of the hash thereafter receives a “secondary” flag.
Person Level	Deduplication compares the e-documents found in each custodial storage location against the other files from that same custodial location (people, or in the project of no person, the storage location). If the hash remains singular throughout processing, it receives no duplicate flag. In the project of duplicate files the first hash instance receives a “primary” or “master” flag and each reoccurrence of the hash thereafter receives a “duplicate” flag.
Actual Files Only	Deduplicates actual files instead of all files. Checking this option excludes OLE files and Alternate Data Stream files.

You can also deduplicate email, marking the email, email contents, or email attachments as a duplicate of others.

### Email Deduplication Options

Option	Description
No Deduplication	Processes the project without email deduplication. This feature allows the case to process more quickly. This option is the default for Security processing.
Project Level	The scope of the email deduplication. Deduplication compares each of the emails processed within a project against the others as they are processed. If the deduplication value remains singular throughout processing, it receives no duplicate flag. In the project of duplicate email, the first value instance receives a “primary” flag and each reoccurrence of the value thereafter receives a “duplicate” flag. If two people have the same email, it is marked as a duplicate.
Person Level	The scope of the email deduplication. Deduplication compares the email found in each custodial storage location against the other emails from that same custodial location (people, or in the project of no person, the storage location). If the value remains singular throughout processing it receives no duplicate flag. In the project of duplicate emails, the first email instance receives a “primary” or “master” flag and each reoccurrence of the email thereafter receives a “duplicate” flag. In the project of duplicate files, the first value instance receives a “primary” flag and each reoccurrence of the value thereafter receives a “duplicate” flag.
Email To	Deduplicates email based on the recipients in the “To” field.
Email From	Deduplicates email based on the senders in the “From” field.

## Email Deduplication Options (Continued)

Option	Description
Email CC	Deduplicates email based on the recipients in the “Carbon Copy” field.
Email Bcc	Deduplicates email based on the recipients in the “Blind Carbon Copy” field.
Email Subject	Deduplicates email based on the contents in the “Subject” field.
Email Submit Time	Deduplicates email based on the date and time the email was initially sent.
Email Delivery Time	Deduplicates email based on the date and time the email was delivered to the recipients.
Email Attachment Count	Deduplicates email based on the number of attached files.
Email Hash	Deduplicates email based on the hash value.
Body and Attachments	Includes email body, recipients (the “To” field), sender (the “From” field), CC, BCC, Subject field contents, body, the number of attachments, and the attachments for deduplication.
Body Only	Includes only the email body and the list of attachment names for deduplication.

## About Indexing for Text Searches of Content of Files

By default, when you add evidence to a project, the files are indexed so that the content of the files can be searched. You can select a *No Search* processing mode, which is faster, but does not index the evidence.

## About Optical Character Recognition (OCR)

Optical Character Recognition (OCR) is a feature that generates text from graphic files and then indexes the content so the text can be searched, labeled, and so forth.

OCR is currently supported in English only.

Some limitations and variables of the OCR process include:

- OCR can have inconsistent results. OCR engines have error rates which means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.
- OCR may incur longer processing times with some large images and, under some circumstances, not generate any output for a given file.
- Graphical images that have no text or pictures with unaligned text can generate illegible output.
- OCR functions best on typewritten text that is cleanly scanned or similarly generated. All other picture files can generate unreliable output.
- OCR is only a helpful tool for you to locate images with index searches, and you should not consider OCR results as evidence without further review.

The following table describes the OCR options that are available in *Processing Options*:

## OCR Options

Option	Description
Enable OCR	Enables OCR and expands the OCR pane to select options for OCR processing.
File Types	Specifies any or all of the following file types to process for OCR: <ul style="list-style-type: none"> <li>• PDF. This file type is checked by default when enabling OCR.</li> <li>• JPEG</li> <li>• PNG</li> <li>• TIFF. This file type is checked by default when enabling OCR.</li> <li>• BMP</li> <li>• GIF</li> <li>• Uncommon (PCX, TGA, PSD, PCD. . .)</li> </ul> See <a href="#">Supported File Types for OCR</a> on page 256.
Do Not OCR. . .	<ul style="list-style-type: none"> <li>• Defines the minimum and maximum file size in bytes of documents to be processed by OCR. You can either enter a value in the spin box, or use arrows to select the value. If you clear the box without entering a value, the values return to the default setting.</li> </ul> <p><b>Note: The maximum size that can be specified in the Do not OCR documents over _____ bytes field is 9,223,372,036,854,775,807 bytes</b></p> <ul style="list-style-type: none"> <li>• Excludes full color documents to be processed by OCR.</li> </ul>
PDF Existing Filtered Text Size	Excludes documents that have text exceeding the limit specified. Documents over the specified limit will not be OCRed. This option is only available when PDF is selected as a file type.

## Supported File Types for OCR

The following file types are supported for OCR:

ABC	ABIC	AFP	ANI	ANZt	ARW	AWD	BMP	CAL
CGM	CIN	CLP	CMP	CMW	CMX	CR2	CRW	CUR
CUT	DGN	DOC	DOCX	DCR	DCS	DCM	DCX	DNG
DOC	DOCX	DRW	DWF	DWG	DXF	ECW	EMF	EPS
EXIF	FAX	FIT	FLC	FPX	GBR	GIF	HDP	HTML
ICO	IFF	IOCA	IMG	ITG	JBG	JB2	JPG	JPEG-XR
JPEG-LS	J2K	JP2	JPM	JPX	KDC	MAC	MIF	MNG
MO:DCA	MSP	MRC	MRC	NAP	NEF	NITF	NRW	ORF
PBM	PCD	PCL	PCL6	PCT	PCX	PDF	PGM	PLT
PNG	PNM	PPM	PPT	PPTX	PS	PSD	PSPo	PTK
RAS	RAF	RAW	RTF	RW2	SCT	SFF	SGI	SHP
SMP	SNP	SR2	SRF	SVG	TDB	TFX	TGA	TIFF



---

TIFX	TXT	VFF	WBMP	WFX	WMF	WMZ	WPG	XBM
XLS	XLSX	XPM	XPS	XWD				

---

## Viewing OCR Confidence Scores

When you OCR a document, a confidence score is now calculated that indicates how successful the OCR was. There is a new *OcrScore* column that displays the OCR confidence % score for each file that has been processed with OCR. This column is sortable and searchable which helps you determine which files may need to be manually reviewed for keywords.

The OcrScore value may be one of the following:

- 1-100 — The OCR confidence % score for a document that had a successful OCR process--the higher the score, the higher the confidence
- 0 (None) — The OCR process did not identify any text to extract
- -1 (Skipped) — The OCR process was skipped due to some condition
- -2 (Failed) — The OCR process failed for that file
- blank — The file does not need the OCR process, for example, a .DOC file or email

---

**Note:** For data that is upgraded from a previous version, if a file has been previously processed with OCR, it will show a value of 2. You can use the *OCR Documents* action in *Review* to re-OCR the document and you will get the new OCR confidence score.

---

## Interruption of Evidence Processing

On occasion, processing might be interrupted by a catastrophic failure. Examples of catastrophic events include the network going down or power outages. In these situations, the application performs a roll back of the processing job. A roll back is when records added during the interrupted job are not available in the database and does not appear in *Review*. This action of rolling back of a job insures that you do not receive incomplete records in *Review*. *Processing Status* tab of the *Work List* alerts you to the error and shows that the system is attempting a roll back.

When a catastrophic event occurs, the *Processing Status* tab of the *Work List* alerts you to the error and shows that the system is attempting a roll back. See [Monitoring the Work List](#) on page 308.

You need to be aware of the following considerations with the roll back option:

- For multiple adding evidence jobs, only the job that fails will roll back. Jobs that complete successfully have data appear in the system.
- If records are locked by another process, the roll back may fail to delete physical files from the case folder. You can view what files did not get removed by viewing the log found in \\<server or IP address>\Users\Public\Documents\AccessData\Resolution1\Logs\Summation.
- For Evidence Processing jobs where some records are added, only newly added records roll back.
- Roll back only occurs with failure during Evidence Processing jobs, not Import jobs.
- Incidences, such as if an Evidence Processing job fails to advance (for example, the interface displays that the job is processing for a long time), do not trigger the roll back action.

# Using Project Properties Cloning

As an administrator or a project manager with the *Create/Edit Project* administrator role, you can clone the properties of an existing project to another project. You can also apply a single project's properties to another project. You can also pick and choose properties from multiple individual projects to apply to a single project.

---

**Note:** The project data is not copied from one project to another. Only the project properties are copied.

---

You can apply Project Properties Cloning to a project as it is being created or it can be applied to projects that have already been created.

You can clone properties from a project *only* if you have permission that allows you to view or create that type of object. This is a security measure that prevents users from cloning properties from projects to which they should not be accessing.

- If you do not have any View permissions for a project, that project is not displayed as a Source project
- If you do not have any Create permissions for a project, that project is not displayed as a Target project
- Within the project wizard, the ability to clone from an existing project is hidden from users with Create/Edit Case Restricted, since those users do not have administration rights in the project that they are creating

You can apply the following properties:

- Custom Fields
- Category and Issue Values
- Tagging Layouts
- Labels
- Users and Groups
- Markup Sets
- People
- Highlight Profiles

## To use Project Properties Cloning

1. From the *Source Project* menu, select the source project from which you want to copy.
2. If you are applying the properties to a previously created project, select the target project to which you want to copy from the pull-down menu.
3. Under *Elements to Copy*, select the properties that you want to apply to the project. You can select **All** or choose specific properties to apply.

---

**Note:** If you select only **Category Values**, Project Properties Cloning will copy over all of the custom fields. If you select only **Tagging Layouts**, Project Properties Cloning will only copy over the tagging layouts. You must also select Custom Fields and Category Values if you want those values copied over.

---

4. If you are applying *Project Properties Cloning* to a project as it is being created, finish the *Project Wizard*.

If you are applying *Project Properties Cloning* to a project that has already been created, click **Merge**.

# Viewing and Editing Project Details

You can view the configured properties of the project on the *Project Details* tab.

You can also edit some of the project properties, for example:

- Name
- Job Data Path

- Sort Evidence Items By

You can set the column that you want to sort by default when opening *Project Review*.



You select the default column and then select the default sorting order: ascending or descending.

The setting is project-specific and not user specific.

In *Review*, you can still click any column to sort on.

See [Sorting by Columns](#) on page 36.


## To access the Project Details tab

1. From the *Home* page, select a project, and click the  **Project Details** tab.  
See [Project Details Tab](#) on page 259.
2. To edit properties, click  *Edit*.

## Project Details Tab

The *Project Details* tab displays data for the selected project. You can also edit some of the project data from this tab.

### Elements of the Project Information Tab

Element	Description
Edit Button 	Allows you to edit information about the selected project. Only the <i>Name</i> , <i>Job Data Path</i> , and the <i>Description</i> can be edited.
General Project Properties	See <a href="#">General Project Properties</a> on page 246.
Creation Date	Displays the date that the project was created.
Created By	Displays the user who created the project.
Last Modified Date	Displays the date when the project was last modified.
Last Modified By	Displays the user who last modified the project.
FTK Case ID	Displays the case ID for the associated FTK case if applicable.
Associated FTK Case Pane	Displays any associated FTK cases.

## Elements of the Project Information Tab (Continued)

Element	Description
Display Time Zone	This option allows you to display the dates and times of files and emails based on this specified time zone. For example, if data was collected in the Eastern Time zone, you can select to display times in the Pacific Time zone and all dates will be offset by four hours to display in PST. The default is set for (UTC) Coordinated Universal Time. See <a href="#">Normalized Time Zones</a> on page 247.
Sort Evidence Items By	You can set the default column that you want to sort by when opening <i>Project Review</i> . You select the default column and then select the default sorting order: ascending or descending. The setting is project-specific and not user specific. In <i>Review</i> , you can still click any column to sort on. See <a href="#">Sorting by Columns</a> on page 36.

## Chapter 19

# Managing Custodians for a Project

---

## About Managing Custodians for a Project

You can associate custodians to a project. A custodian is a person who has ownership of information that you want to review.

You may configure and use custodians for one or more of the following reasons:

- Associate certain evidence items to a certain custodian.  
When reviewing evidence in a project you can quickly identify the custodian of any evidence item or cull data by custodian.  
See [About Associating a Person to an Evidence Item](#) on page 265.
- Manage custodians in a project for a litigation hold.  
See [Using Litigation Holds](#) on page 339.

You can manage custodians in the following ways:

Manage custodians at the application level	<p>You can manage custodians at the application level and then associate them to projects.</p> <p>You can configure custodians at the application level in the following ways:</p> <ul style="list-style-type: none"><li>● Adding and managing custodians from the <i>Data Sources / People</i> tab. If using eDiscovery, see <a href="#">Managing People (Custodians) as Data Sources</a> (page 112) If using Summation, see <a href="#">Managing People (Custodians) as Data Sources</a> (page 137)</li><li>● Automatically syncing from Active Directory. See <a href="#">Configuring Active Directory Synchronization</a> on page 77.</li><li>● Adding and managing custodians from the Project's <i>Custodian</i> tab. See <a href="#">Managing Custodians for a Project</a> on page 261.</li></ul>
Manage custodians for use in a project	<p>Users with proper permissions can manage custodians for a project in two ways:</p> <ul style="list-style-type: none"><li>● <a href="#">Using the Home Custodians Tab</a> (page 262)</li><li>● <a href="#">Using the Data Sources People Tab</a> (page 266)</li></ul> <p>For information on user permissions, see <a href="#">Setting Project Permissions</a> (page 275).</p> <p><b>Note:</b> In order for people to be used in Project Review, people must be created and selected before you process the evidence. See <a href="#">About Associating a Person to an Evidence Item</a> on page 265.</p>

# Using the Home Custodians Tab

User with proper permissions can associate and manage the custodians for a project using the *Custodians* tab on the *Home* page.

You can associate existing custodians to the project or you can create new custodians. If you create new custodians, they will also be visible in the *Data Sources > People* tab.

In order to manage custodians in a project, you must have one of the following permissions:

- Global Admin Role permissions
  - Application Administrator
  - Create/Edit Projects (for the projects that they create)
- Project-level permissions
  - Project Administrator
  - Manage Project People (cannot import from CSV file)






## To manage custodians for a project

- ❖ From the *Home* page, select a project, and click the  *Custodians* tab.





When you create and view the list of people, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.  
See [About Content in Lists and Grids](#) on page 36.

## Elements of the People Tab

Element	Description
Filter Options	Allows you to search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
People List	Displays the people for the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Evidence Path list.
Export to CSV 	Export the list to a .csv file.
Refresh 	Refreshes the Groups List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the Groups List. See <a href="#">Sorting by Columns</a> on page 36.
Add Association 	Associates existing people to the project.

## Elements of the People Tab (Continued)

Element	Description
Remove Association 	Disassociates an existing person from the project.
Import People 	Imports people from a csv file.
Add Person 	Adds a person.
Edit Person 	Edits the selected person.
Evidence Tab	Lists the evidence associated with the selected person.




## Associating an Existing Custodian to a Project

You can associate a a custodian to a project in the following ways:

- Associating an existing custodian
- Manually adding people
- Importing people from a file  
See [Importing Project Custodians From a File](#) on page 264.
- Creating or importing people while importing evidence  
See the Loading Data documentation for more information on creating people during import.

If you manually add or import people, they are added to the shared list of people.


### To add an existing custodian

1. On the **Home > project > Custodian** tab, click  **Add**.  
The *Associate Custodian to project* page displays.
2. Select the custodian that you want associated with the project.  
You can click a single person or use Shift-click or Ctrl-click to select multiple people.
3. Click  or **Add all Selected**.  
This moves the people to the *Associate Custodian* list.  
You can also check the selection box next to *First Name* to add all of the people.
4. You can remove people from the *Associate Custodian* list by selecting people and clicking  or **Remove All Selected**.  
You can also clear the selection box next to *First Name* to remove all of the people.
5. Click **OK**.

You can also add custodians using the *People* tab when creating a project.

## Manually Creating Custodians for a Project

### To manually create a project-level custodian


1. On the **Home > project > Custodian** tab, click  **Add**.
2. In *Custodian Details*, enter the person details.
3. Click **OK**.

You can also manually create custodians from the *Custodians* tab when creating a project.

## Editing a Custodian

You can edit any custodian that you have added to the project.


### To edit a custodian

1. On the **Home > project > Custodian** tab, select a person that you want to edit.
2. Click  **Edit**.
3. In *Person Details*, edit person details.
4. Click **OK**.

## Removing a Custodian

You can remove one or more custodians from a project. This does not delete the custodian from the global list of people, it just disassociates it from the project.

### To remove one or more custodians from a project

1. On the **Home > project > Custodian** tab, select the check box for the people that you want to remove.
2. Below the person list, click  **Remove**.

To confirm the deletion, click **OK**.

## Importing Project Custodians From a File

You can import a list of people into the system from a CSV file. For more information see the following:

- If using eDiscovery, see [Importing Custodians From a CSV File](#) (page 117)
- If using Summation, see [Importing People From a CSV File](#) (page 143)



## About Associating a Person to an Evidence Item

You can use people to associate data to its owner.

You can associate a person to an evidence item in one of two ways; however, the results are different.

- Specify a person when importing an evidence item.  
This associates the person when the evidence is processed. You can then use person data when in Project Review and in exports.  
See the Loading Data documentation for more information on creating people on import.  
When you associate a person to an evidence item, the person will be associated to all evidence in that item, whether the evidence item contains a single file or a folder of many files, messages, and so on.
- Edit an evidence item that has already been imported and associate a person.  
Using this method, the person association will not be visible or usable in Project Review nor in exports. You can only view this association in the *Evidence* and *People* tabs of the *Home* page.

# Using the Data Sources People Tab

Generally, you use the *Data Sources > People* tab to maintain the global list of all people (custodians) available for all projects in the application. You can add, edit and delete people, as well as import lists of people.

For general information on using the *Data Sources > People* tab see the following:

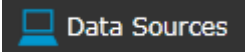





- If using eDiscovery, see [Managing People \(Custodians\) as Data Sources](#) (page 112)
- If using Summation, see [Managing People \(Custodians\) as Data Sources](#) (page 137)

Also, from the *Data Sources > People* tab, you can associate a person to projects.

In order to use the *Data Sources > People* tab to associate a person to a project, you must have one of the following permissions:

- Application Administrator
- Combination of
  - Create People admin permission
  - Permissions for the project that you want to associate the person to

## To associate a person to a project

1. Click  **Data Sources** .
2. Click  **Projects** .
3. In the *Project* list pane, click  to add projects.
4. In the *Associate Projects to <Person>* dialog, do one of the following:
  - In the *All Projects* pane, click  to add projects to the *Associated Projects* pane.
  - In the *All Projects* pane, click  to projects from the *Associated Projects* pane.
5. Click **OK**.
6. (optional) Click  to remove projects from an associated person.

# Chapter 20

## Managing Tags

---

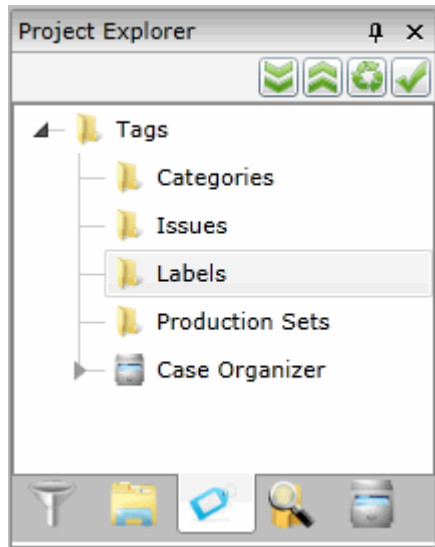
The *Tags* tab on the *Home* page and in the *Project Explorer* can be used to do the following:

- Create and manage Labels
- Create and manage Issues
- View categories
- Create category values
- Create Production Sets
- View Case Organizer objects.

Project managers can create labels and issues for the reviewer to use.

You can also view documents assigned to tags using the *Tags* tab in the *Project Explorer*.

### Tags Tab in Project Explorer



## Elements of the Tags Tab

Elements	Description
Categories	Displays all the existing categories for the project. Right-click to create category values. See <a href="#">Creating Category Values</a> on page 296. See <a href="#">Viewing Documents with a Category Coded</a> on page 202.
Issues	Displays all the existing issues. Right-click to create a new issue for the project. See <a href="#">Managing Issues</a> on page 272. See <a href="#">Viewing Documents with an Issue Coded</a> on page 202.
Labels	Contains all the existing labels. Right-click to create a new label for the project. See <a href="#">Managing Labels</a> on page 269. See <a href="#">Viewing Documents with a Label Applied</a> on page 202.
Production Sets	Check to include Production Sets in your search. Right-click to create Production Sets. See <a href="#">Creating Production Sets</a> on page 269.
Case Organizer	Displays all the existing case organizer objects for the project. Right-click to create new objects. See <a href="#">Using the Case Organizer</a> on page 204.

# Managing Labels

Labels are a tool that reviewers can use to group documents together. Reviewers apply labels to documents, then project/case managers can use the Labels filter to view all the documents under the selected label. Before reviewers can use a label, the project/case manager must create it.




Project Managers can do the following:

- Create labels
- Rename labels
- Edit labels
- Delete labels
- Manage labels permissions

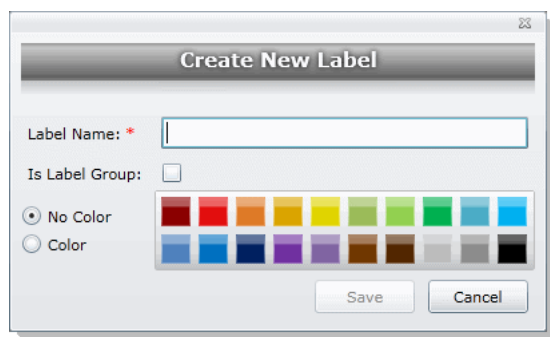
## Creating Labels

Project/case managers can create labels for reviewers to use when reviewing documents.

### To create a label

1. Log in as a user with Project Administrator rights.
2. Open the *Tags* page by doing one of the following:
  - On the *Home* page:
    - 2a. On the *Home* page, click  *Tags*.
  - In *Review*:
    - 2a. Click the  *Project Review* next to the project in the *Project List*.
    - 2b. Click the  *Tags* in the *Project Explorer*.
3. Right-click the *Labels* folder and click **Create Label**.

### Create Label Dialog



4. Enter a *Label Name*.
5. (Optional) Select **Is Label Group** to create a Label Group to contain other labels and then skip to the last step.

6. Do one of the following:
  - **No Color:** Select this to have no color associated with the label.
  - **Color:** Select this and then select a color to associate a color with the label.

---

**Note:** The default color is black if you select the Color option. The color selected appears next to the label in the labels folder.

---

7. Click **Save**.

## *Deleting Labels*

Project/case managers can delete existing labels.

### **To delete a label**

1. Log in as a user with Project Administrator rights.
2. Expand the *Labels* folder.
3. Right-click the label that you want to delete and click **Delete**.
4. Click **OK**.

## *Renaming a Label*

Project/case managers can rename labels in the Project Review.

### **To rename a label**

1. Log in as a user with Project Administrator rights.
2. Expand the *Labels* folder.
3. Right-click the label that you want to rename and click **Rename**.
4. Enter the new name for the label.

## *Managing Label Permissions*

Project/case managers can grant permissions of labels to groups for use. Groups of users can only use the labels for which they have permissions.

In order for groups to be assigned, they must first be associated to the project.

### **To manage permissions for labels**

1. Log in as a user with Project Administrator rights.
2. Expand the *Labels* folder.
3. Right-click the label for which you want to grant permissions and click **Manage Permissions**.

## Assign Security Permissions



4. Select the groups that you want to grant permissions for the selected label.

---

**Note:** By default, all groups that the logged-in user belongs to will be selected. To make it a personal label, all groups should be un-selected.

---

5. Click **Save**.

## Applying Labels to Documents

After an label has been created and associated with a user group, you can apply labels to documents.

### To apply a label to a document

1. Create an label.  
See [Creating Labels](#) on page 269.
2. Grant permissions for the label.  
See [Managing Label Permissions](#) on page 270.
3. Apply labels to documents.  
For instructions, see *Using Labels* in the *Reviewer Guide* or go to [Using Labels](#) (page 198).




# Managing Issues

Project/case managers with *View Issues and Assign Issues* permissions can create, delete, rename, and assign permissions for issues. Issues work like labels. Reviewers can apply issues to documents to group similar documents.

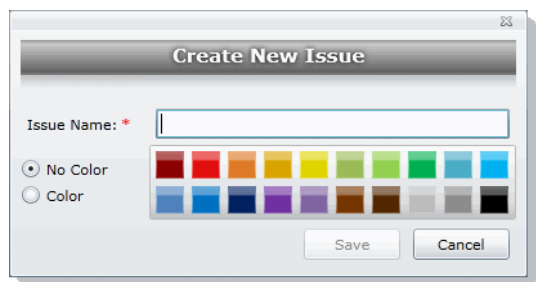
## Creating Issues

Project/case managers with *View Issues and Assign Issues* permissions can create issues for other users to code.

### To create an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Open the *Tags* page by doing one of the following:
  - On the *Home* page:
    - 2a. On the *Home* page, click  *Tags*.
  - In *Review*:
    - 2a. Click the  *Project Review* next to the project in the *Project List*.
    - 2b. Click the  *Tags* in the *Project Explorer*.
3. Right-click the *Issues* folder and click **Create Issue**.

### Create New Issue Dialog



4. Enter an *Issue Name*.
5. Do one of the following:
  - **No Color**: Select this to have no color associated with the issue.
  - **Color**: Select this and then select a color to associate a color with the issue.
6. Click **Save**.



## Deleting Issues

Project/case managers with *View Issues and Assign Issues* permissions can delete issues.

### To delete an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Expand the *Issues* folder.
3. Right-click the issue that you want to delete and click **Delete**.
4. Click **OK**.

## Renaming Issues

Project/case managers with *View Issues and Assign Issues* permissions can rename issues.

### To rename an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Expand the *Issues* folder.
3. Right-click the issue that you want to rename and click **Rename**.
4. Enter the new name for the issue.

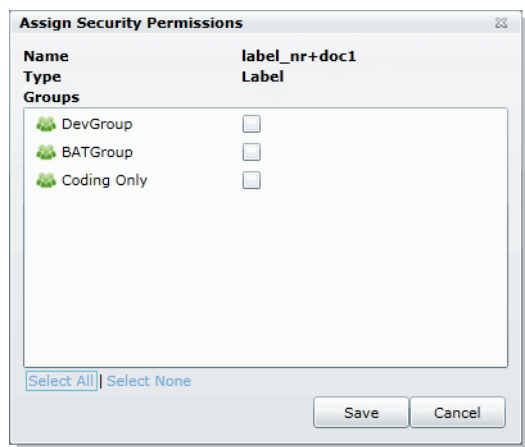
## Managing Issue Permissions

Project/case managers can grant permissions of issues to groups for use. Groups of users can only use the labels for which they have permissions.

### To manage permissions for labels

1. Log in as a user with View Issues and Assign Issues rights.
2. Expand the *Issues* folder.
3. Right-click the issue for which you want to grant permissions and click **Manage Permissions**.

#### Assign Security Permissions



4. Check the groups that you want to grant permissions for the selected issue.

5. Click **Save**.

## *Applying Issues to Documents*

After an issue has been created and associated with a user group, it can then be added to a tagging layout for coding.

### **To apply an issue to a document**

1. Create an issue.  
See [Creating Issues](#) on page 272.
2. Grant permissions for the issue.  
See [Managing Issue Permissions](#) on page 273.
3. Add Issues to the Tagging Layout.  
See [Associating Fields to a Tagging Layout](#) on page 299.
4. Check out a review set of documents. (optional)  
See the Reviewer Guide for more information on checking out review sets.
5. Code the documents in the review set with the issues you created.  
See the Reviewer Guide for more information on coding.

# Chapter 21

## Setting Project Permissions

---

### About Project Permissions

The user who creates a project automatically has administrator permissions for that project. User with the Application Administrator role also have administrator permissions for all projects.

For all other users, you must assign permissions to a specific project. You can assign project permissions to individual users or user groups.

In the project list of the *Home* page, users will only see projects to which they have permissions. You can give a user permissions to review a project but not see any project properties on the *Home* page.

Project permissions are project specific, not global. For information on how to manage global permissions, see the *Admin Guide*.

In order to configure project permissions, you must have either *Administrator* or *Create/Edit Projects* permissions.

You assign project permissions to users or user groups by using Project Roles.

### About Project Roles

Before you can apply permissions to a user or group, you must set up project roles. A project role is a set of permissions that you can associate to multiple users or groups. Creating a project role simplifies the process of assigning permissions to users who perform the same tasks. To use project roles, you do the following:

1. Associate users or user groups to a project.
2. Create a project role.
3. Assign permissions to the project role.
4. Associate users or user groups to the project role.  
You can do the following:
  - Select an existing project role
  - Create or edit a role and assign permissions to that role

You can create and use multiple project roles.

## Project-level Permissions

By default, when you associate a user (without global permissions) to a project, they can see the project in the *Project List*, and they can enter Project Review, but they do not have permissions to see any of the data in the project. In order to see data and perform any review tasks, they must be given explicit permissions to the project.

You can only assign permissions to a project role, which you then associate with users or user groups.

The following table describes the available project permissions that you can assign to a project role.

### Project-level Permissions in the Project Role Details pane

Permission	Description
Project Administrator	This grants all permissions to the project, for example: <ul style="list-style-type: none"><li>• Can Manage Project Roles.</li><li>• Can assign access permissions to users &amp; groups.</li><li>• Has all project level functional permissions listed below.</li><li>• Can import/export.</li><li>• Can see job list for jobs created for his project.</li></ul>
<b>Individual Permissions:</b>	<b>These are individual permissions that you can assign to one or more roles.</b>
Admin Reviewer	Can view all objects in the Item List that are in the project. However, they must have other permissions to view contents in the viewers (Native and Text), run searches, view and use labels, view document groups, and so on. You can also use Document Groups to let users see items in the Item List.
Manage Project Roles	Can manage Project Roles.
Manage Project People	Provides access to the People tab where you can create and edit People (custodians) associated with the project.
Run Search	Can run searches in the Project Review. <b>Note:</b> User must have this permission to perform other search functions as well.
Save Search	Can save searches that the user performs themselves.
Manage Saved Search Permissions	Can share your saved searches with other groups.
View Labels	Can view the labels everywhere that labels appear.
Assign to Labels	Can assign labels to objects.
Manage Labels Permissions	Can grant permissions to labels.
Create Labels	Can create and edit labels in the Project Explorer in Project Review. <b>Note:</b> Must have View Labels permission as well to create and delete labels.
Delete Labels	Can delete labels in Project Review.
Create Review Sets	Can create review sets.
Delete Review Sets	Can delete review sets in Project Review.
View Review Sets	Can view the review sets in the Project Explorer and Review Batches panel in the Project Review.

## Project-level Permissions in the Project Role Details pane (Continued)

Permission	Description
Manage Review Set Permissions	Can assign review sets to users/groups.
View Native	Can view the Native panel in Project Review.
View Text	Can view the Text panel in Project Review.
View Coding Layout	Can view the Coding panel in Project Review.
Edit Document	Can change data for document fields using tagging layouts.
Create Categories	Can create or edit categories in Project Review.
Delete Categories	Can delete categories in Project Review.
View Categories	Can view categories in Project Review.
Assign Categories	Can assign a document to a category.
Manage Category Permissions	Can assign permissions for categories and category values.
View Issues	Can view issues in Project Review.
Assign Issues	Can assign issues to a document.
Create Issues	Can create and edit issues in Project Review.
Delete Issues	Can delete issues in Project Review.
Manage Issue Permissions	Can assign permissions for issue values.
View Notes	Can view notes everywhere that they appear in Project Review.
Add Notes	Can add notes in Project Review.
Delete Notes	Can delete notes in Project Review.
View Annotations	Can view annotations in Image, Natural, and Transcript panels in Project Review.
Add Annotations	Can add annotations in Project Review (but no view them unless the View Annotation permission is granted).
Delete Annotations	Can delete annotations in Project Review.
View Activity History	Can view Activity panel in Project Review.
Create Production Set	Can create production sets in Project Review.
Delete Production Set	Can delete production sets in Project Review.
Manage Production Set Permissions	Can edit and assign permissions for production sets.
Delete Evidence	Can delete evidence items from the Item List grid.
Imaging	Can perform the imaging mass action in the Item List panel and can create an image using the Annotate option in the Natural panel.
Upload Transcripts	Can upload transcripts in Project Review.

## Project-level Permissions in the Project Role Details pane (Continued)

Permission	Description
Upload Transcript Exhibits	Can upload exhibits in Project Review.
Manage Transcript Permissions	Can assign permissions to Transcript Groups.
Create Transcript Group	Can create a transcript group in Project Review.
Predictive Coding	Can apply predictive coding to documents in Project Review.
Global Replace	Can search and replace words throughout a project in Project Review.
View Data Reports	Can view the <i>Data Volume Reports</i> on the <i>Reports</i> tab for projects which they have the rights to access.
<p><b>The following are available if you have an eDiscovery or Litigation Hold license:</b>            For more information, see the following in the <i>Using Lit Holds</i> chapter:  <a href="#">Project-level Lit Hold Permissions</a> (page 344)</p>	
Approve Litholds	Can approve configured Litigation Holds.
Create Litholds	Can create Litigation Holds.
Delete Litholds	Can delete Litigation Holds.
View Litholds	Can view Litigation Holds.
Hold Manager	Can manage Lit Holds, including creating, viewing, and deleting Lit Holds.
<p><b>The following are available if you have an eDiscovery license:</b></p>	
View Project Jobs	Can view all jobs. See <a href="#">Introduction to Jobs</a> on page 418.
Approve Jobs	Can approve jobs.
Create Collection	Can create Collection jobs. Also enables the View Project Jobs permission.
Create Report Only	Can create Report Only jobs.
Delete Jobs	Can delete jobs.
Execute Jobs	Can execute jobs.
Express Export	
Initiate Processing	Can process the files from a collection job. Also enables the View Project Jobs permission.
View Status Reports	Can view the project's Reports page and can view reports such as the Completion Status Report.
View Audit Log Report	Can view the Audit Log report for a project.

# Permissions Tab

The *Permissions* tab on the *Home* page is used to assign users or groups permissions within the project.

The *Permissions* tab is project specific, not global. For information on how to manage global permissions, see the *Admin Guide*.

## Permissions Tab

The screenshot displays two sections of the Permissions Tab interface. The top section is for 'User/Group Details' and the bottom section is for 'Project Role Details'. Both sections include a table of items, a details panel on the right, and a pagination bar at the bottom.

**User/Group Details**

<input type="checkbox"/>	User/UserGroup Name	Type	Description
<input type="checkbox"/>	jseymour	User	
<input type="checkbox"/>	jwayne	User	
<input type="checkbox"/>	mjackson	User	
<input type="checkbox"/>	Power Users	Group	Power Users
<input type="checkbox"/>	Reviewers	Group	Case Reviewers
<input type="checkbox"/>	Users	Group	Users

Page Size: 15 Total: 6 (0) Page 1 of 1

**User/Group Details**

User/UserGroup Name: jseymour

Type: User

**Project Role Details**

<input type="checkbox"/>	Project Role Name	Is Project Administrator	Permission Count
<input type="checkbox"/>	Reviewer	False	1

Page Size: 15 Total: 1 (0) Page 1 of 1

**Project Role Details**

Project Role Name: Reviewer

Project Administrator

**Permissions**

Project Reviewer








Manage Project Roles

Run Search


Save Search

Manage Saved Search Permissi

## Elements of the Permissions Tab

Element	Permission
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Users/User Group List	Displays the users and groups associated with the project. Click the column headers to sort by the column.
Refresh 	Refreshes the User/Group List.
Export to CSV 	Exports the Permissions List to a CSV file.
Columns 	Adjusts what columns display in the User/Group List.
Add Association 	Adds either a group/user to a role or a role to a group/user.
Remove Association 	Disassociates a group/user from a role or disassociate a role from a group/user.
<i>User/Group Details</i> pane	Displays the details for the selected user or group.
Project Roles Tab	Displays the available roles for the project.
Add Role 	Adds a role. Specify the permissions of the role in this data form.
Edit Role 	Edits the selected role.
<i>Project Role Details</i> pane	Displays the details for the selected project role name.

### To access the Permissions tab

1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.

To apply permissions to a user or group, you must create a project role. You can then associate that project role to a user or group on the *Permissions* tab.

See [Creating a Project Role](#) on page 283.

See [Associating Users and Groups to a Project](#) on page 281.



See [Project-level Permissions](#) on page 276.



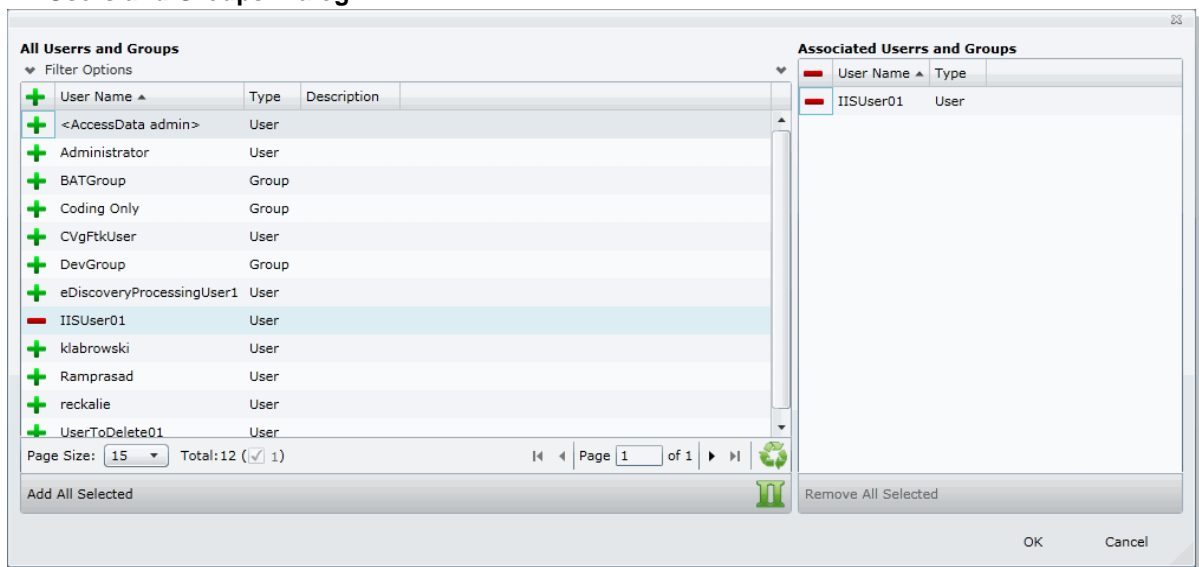
# Associating Users and Groups to a Project


Before you can apply a project role to a user or group, you must first associate the user or group to the project. Administrators and project managers with the correct permissions can associate users and groups to a project in the *Permissions* tab. Once a user or group is added to a project, the user can see the project in the *Project List* panel.

## To associate a user or group to a project

1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.
3. In the User/Group list pane, click **Add Association** .

## All Users and Groups Dialog




4. Click  to add the user or group to the project.
5. Click **OK**.
6. To grant specific permissions to a user or group, associate them to a project role. See [Associating Project Roles to Users and Groups](#) on page 282.

## Disassociate Users and Groups from a Project

Administrators and project/case managers with the correct permissions can remove users from a project by disassociating them from the project in the *Permissions* tab.

## To disassociate a user or group to a project

1. On the *Home* page, select a project, and click the **Permissions** tab.
2. Check the user or group you want to remove from the project in the User/Group list pane.
3. In the User/Group list pane, click the **Remove Association** button .

# Associating Project Roles to Users and Groups




After you have associated a user or user group to a project, you can associate them to a project role.

See [Associating Users and Groups to a Project](#) on page 281.

You can select an existing project role or create a new one.

For information on creating new project roles, see [Creating a Project Role](#) (page 283).

## To associate a project role to a user or group



1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.
3. In the *User/UserGroup* pane, select a user or group that has been associated to the project.
4. Do one of the following:
  - Associate the user or group to an existing project role.
    - 4a. In the *Project Role* pane (bottom of the page), click the  *Add Association* button.
    - 4b. In the All Project Role dialog, click the  *Add* button for the desired project roles to associate with the user or group.
    - 4c. Click **OK**.
  - Create a new project role.

See [Creating a Project Role](#) on page 283.

## Disassociating Project Roles from Users or Groups

Administrators and users with the *Manage Project* permissions can disassociate project roles from users and groups for a specific project.

## To disassociate a project role to a user or group





1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.
3. In the *User/UserGroup* pane, select a user or group that has been associated to the project.
4. In the *Project Roles* pane, click the **Remove Association** button .

# Creating a Project Role

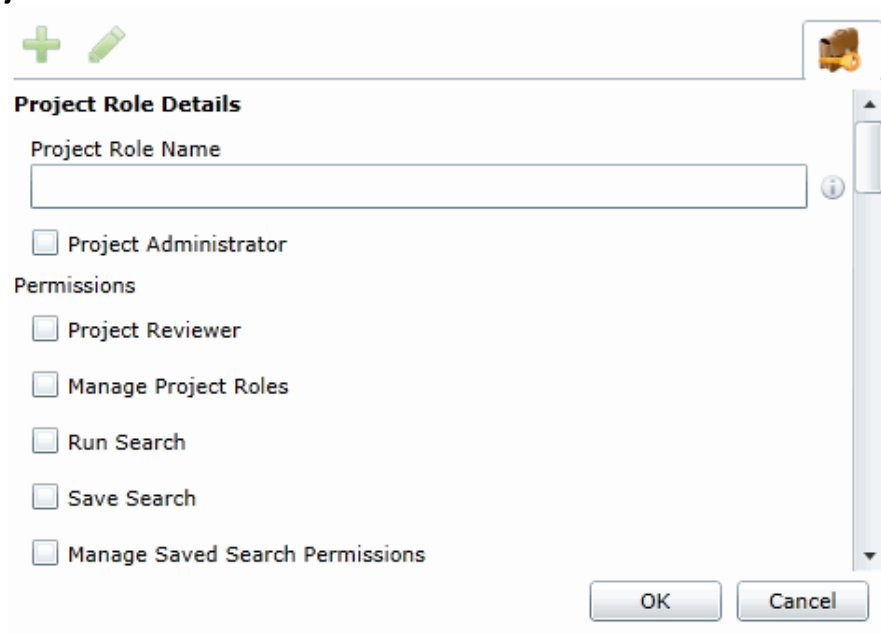
After you have associated a user or user group to a project, you can associate them to a project role. You can use an existing role or create a new role.

See [About Project Roles](#) on page 275.

## To create a project role

1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.
3. If no user is associated with the project, associate a user by doing the following:
  - 3a. In the *Users/UserGroup* pane, click the  *Add Associations* button.
  - 3b. Add a user or group by clicking the  *Add* button for a user or group.
  - 3c. Click **OK**.
4. In the *Project Roles* pane at the bottom of the screen, click the  *Add* button.

## Add Project Roles Data Form



**Project Role Details**

Project Role Name

Project Administrator

**Permissions**

Project Reviewer

Manage Project Roles

Run Search

Save Search

Manage Saved Search Permissions

OK Cancel



5. Enter a *Project Role Name*.
6. Check the permissions that you want to include in the role. See [Project-level Permissions](#) on page 276.
7. Click **OK**.

## Editing and Managing a Project Role

You can edit project roles if you want to alter the permissions in the role.

Because project roles can be used across multiple projects, you cannot delete a project role as it may affect other projects.

### To edit a project role

1. On the *Home* page, select a project.
2. Click the  *Permissions* tab.
3. Select a user that has the project role associated with it.
4. In the *Project Roles* pane at the bottom of the screen, select a role and click the edit button .
5. Edit the role and click **OK**.

# Chapter 22

## Running Reports

---

This chapter is designed to help you execute and understand reports. Reports allow you to view data about your project.

Users with the necessary project-level permissions can run reports for a project using the *Reports* tab and the *Exports* tab on the *Home* page. Permissions for the *Reports* and *Exports* tabs are project specific, not global.


See [Setting Project Permissions](#) on page 275.

The following reports are available:

- [Basic Reports](#) (page 286)
  - [Audit Log Report](#) (page 286)
  - [Deduplication Report](#) (page 287)
  - [Data Volume Report](#) (page 287)
  - [Search Reports](#) (page 287)
  - [Export Set Reports](#) (page 288) (Only appears after generated)
  - [Export Set Reports](#) (page 288) (Only appears after generated)
  - [Case Organizer Reports](#) (page 289)
  - [Case Organizer Reports](#) (page 289)
- [Search Reports](#) (page 287)
  - [Project Result Report](#) (page 289)
  - [Completion Status Report](#) (page 289)
  - [Custodian Datamap Report](#) (page 289)

## Accessing the Reports Tab

### To access the Reports tab

- ❖ From the Home page, select a project, and click the  **Reports** tab.

### To run a report

1. Select a project in the Project List Panel.
2. Click the **Reports** tab on the *Home* page.
3. Click **Generate Report** for the report that you want to run.
4. Wait for the report to generate.

5. After the report is generated, click **Download**.

## *Basic Reports*

The following reports are available with all product licenses.

### Audit Log Report

This log records the user activities at the Project Review and evidence object level. The log records the following actions in the report:

- Project Review Activities:
  - Entered Review
  - Exited Review
  - Perform Search
  - Save Search
  - Apply Filter
  - Create Label
  - Create Document Group
  - Create Issue
  - Create Category
  - Create Review Set
  - Check Out Review Set
  - Check In Review Set
  - Create Production Set
  - Export Data
- Evidence Object Activities
  - Label Document
  - Annotate Document
    - Create Redaction
    - Delete Redaction
    - Remove Redaction
    - Create Highlight
  - Edit Document (via Editable Grid)
  - Image Document
  - Code Document (via Tagging)
  - Delete Document
  - View Document (Includes Duration)
  - Link Document
  - Compare Document
  - Print Document

## Deduplication Report

You can open the Deduplication Summary report to view duplicate files and emails that were filtered in the project. Also included in the report are the deduplication options that were set for documents and email.

You can generate the report, print it, and save it in a variety of formats, and download it to a spreadsheet.

## Data Volume Report

You can generate the Data Volume Report to view the size of processed data, evidence file counts by file category, and a breakout of files by extension.

You can view the report, print it, and save it in a variety of formats.

## Search Reports

You can generate and download a report that shows you the overall results of your search.

---

**Note:** When generating a search report that includes a large number of items, such as over 100,000, the report generation can take a long time, possibly two hours or more. You should not perform other tasks using the console during this time. Even if the console closes due to inactivity, the report will still generate.

---

The following details are included in the Search report:

- **Total Unique Files:** This count is the total items that had at least one keyword hit. If a document has several keywords that were found within its contents, a count of 1 is added to this total for that document.

---

**Note:** If a search term contains a keyword hit, due to a variation search (stemming, phonic, or fuzzy), the character “&” is added to the end of each search term in the File details to indicate the variation search. However, a search term found with the synonym or related search will not show the “&.” at the end of the term.

---

- **Total Unique Family Items:** This count is the number of files where any single family member had a keyword hit. If any one file within a document family had a keyword hit, the individual files that make up this family are counted and added to this total. For example, one email had 3 attachments and the email hit on a keyword, a count of 4 files would be added to this count as a result.
- **Total Family Emails:** This count is the number of emails that have attachments where either the email itself or any of the attachments had a search hit. This count is for top level emails only. Emails as attachments are counted as attachments.
- **Total Family Attachments:** This count is the number of the attachments where either the top level email or any of the attachments had a search hit. For example, if you have an email with an email attached and the attached email has 4 documents attached to it, this count would include the 5 attachments.
- **Total Unique Emails with no Attachments:** This count is the number of the emails that have no attachments where a search hit was found.
- **Total Unique Loose eDocs:** This count is the number of loose eDocuments where a search hit was found. This does not include attachments to emails, but does count the individual documents where a hit was found from within a zip file.
- **Total Hit Count:** This count is the total number of hits that were found within all of the documents.

---

**Note:** For some queries, the total hit count may be incorrect.

---

### To generate and download a search report

1. Perform a search.

In *Project Review*, click **Search Options > Generate Report**.

## Export Set Reports

The Export Set report supplies information about exported production sets. You can also generate and download a report either before or after you export the set to a load file. Each time you generate the report, it overwrites any previously generated report for that export set.

After an export set report has been generated, you can download it in Microsoft Office Excel Worksheet format (XLSX) and save it to a new location. You can also view a list of the Export Set Reports under the *Reports* tab.

### To run an export set report

1. Select a project in the *Project List* panel.
2. Click the **Printing/Export** tab on the *Home* page.
3. Under the *Export Set History* tab, select an export and click **Show Reports**.
4. Under *Summary*, click **Generate**. Once an export report has been generated, click **Download**.

## Export Set Info

- **Name:** The name of the Export Set as defined by the user when the set was created.
- **Labels:** Lists which labels are included in the document set.
- **Comments:** Lists any comments that added when the export set was created.
- **File Count:** Displays a total of the number of documents contained within the exported set of data.
- **File Size:** Displays the total size of the documents being exported.

## File Breakout

- **Type:** Lists the document type by file extension of the files contained within the exported set of documents.
- **Count:** Displays a count of how many documents are contained within each group.
- **Size:** Displays the total size of the files within each of the groupings.

## File List

- **Object Name:** Displays the name of the file being exported.
- **Person:** Displays the name of the associated person.
- **Extension:** Displays the file extension of the exported item.
- **Path:** Displays the original filepath of the exported item.
- **Create Date:** Displays the metadata property for the created date of the exported item.
- **Last Access Date:** Displays the metadata property for the last access date of the exported item.



- **Modify Date:** Displays the metadata property for the modification date of the exported item.
- **Logical Size:** Displays the metadata property for the logical size of the exported item.
- **File Type (Generic):** Displays the file type of the exported item.

## Case Organizer Reports

The Case Organizer report supplies information about case organizer objects in your project.

You can must generate the report from the *Tags* tab in *Review*.

After an report has been generated, you can download it in Microsoft Word format (DOCX) and save it to a new location. You can also view exported files.

For details, see the *Using Case Organizer* information in the *Review Guide*.

## Image Conversion Exception Report

The Image Conversion Exception (ICE) report displays documents that were not imaged due to limitations of the image conversion tools or system failures.

### To run an image conversion exception report

1. Select a project in the *Project List* panel.
2. Click the **Export** tab on the *Home* page.
3. Expand the **Download Reports** button of a production set.
4. Select **Download ICE Report**.

## eDiscovery Reports

If you have an eDiscovery license, you can also use the following reports.

## Project Result Report

You can generate the Project Result Report to shows a summary and detailed information about collected and external evidence.

## Completion Status Report

The Completion Status report shows the status of a job. You can generate the report after the job starts running and at least one job target status is collecting.

## Custodian Datamap Report

You can generate the Custodian Datamap Report to show all the custodians and their associated data sources for a given legal matter. For example, the report can display the custodian name, the data source type and name, whether or not the data source was collected, and the date of the last collection that was made.

# Chapter 23

## Configuring Review Tools

---

Project/case managers with the correct permissions can configure many of the review tools that admin reviewers use in Project Review. See [Setting Project Permissions](#) (page 275) for information on the permissions needed to set up review tools. The following review tools can be set up from the *Home* page:

- Markup Sets: [Configuring Markup Sets](#) (page 290)
- Custom Fields: [Configuring Custom Fields](#) (page 294)
- Tagging Layouts: [Configuring Tagging Layouts](#) (page 297)
- Highlight Profiles: [Configuring Highlight Profiles](#) (page 302)
- Redaction Text: [Configuring Redaction Text](#) (page 306)

### Configuring Markup Sets

Markup sets are a set of redactions and annotations performed by a specified group of users. For example, you can create a markup set for paralegals, then when paralegal reviewers perform annotations on documents in the Project Review, all of their markups will only appear when the Paralegal option is selected as the markup for the document in the Natural or Image panel of Project Review.

---



**Note:** Only redactions and annotations are included in markup sets.

---

## Markup Sets Tab

The *Markup Sets* tab on the *Home* page can be used to create markup sets for reviewers to use. Markup sets are a set of redactions and highlights performed by a specified group of users.


### Markup Sets Elements

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Markup Sets List	Displays the markup sets already created for the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Markup Sets List.
Columns 	Adjusts what columns display in the Markup Sets List.
Delete 	Deletes selected markup set. Only active when a markup set is selected.
Add Markup Set 	Adds a markup set.
Edit Markup Set 	Edits the selected markup set.
Delete Markup Set 	Deletes the selected markup set.
Users Tab 	Allows you to associate users to a markup set.
Groups Tab 	Allows you to associate groups to a markup set.
Add Association 	Associates a group/user to a markup set.
Remove Association 	Disassociates a markup set from a user/group.

## Adding a Markup Set


Before you can assign a markup set to a user or group, you must first create the markup set on the *Home* page. Project/case managers with the Project Administrator permission can create, edit, and delete markup sets.

### To add a markup set

1. Log in as a user with Project Administrator rights.
2. Click the **Markup Sets** tab.  
See [Markup Sets Tab](#) on page 291.
3. Click the **Add** button .
4. In the *Markup Set Detail* form, enter the name of the *Annotation Set*.
5. Click **OK**.

## Deleting a Markup Set


### To delete a markup set

1. Log in as a user with Project Administrator rights.
2. Click the **Markup Sets** tab.  
See [Markup Sets Tab](#) on page 291.
3. Select the markup set that you want to delete.
4. Click the **Delete** button .
5. In the confirm deletion dialog, click **OK**.

## Editing the Name of a Markup Set

You can edit the name of an existing markup set if you have Project Administrator rights.


### To edit a markup set

1. Log in as a user with Project Administrator rights.
2. Click the **Markup Sets** tab.  
See [Markup Sets Tab](#) on page 291.
3. Select the markup set that you want to edit.
4. Click the **Edit** button .
5. Change the name of the *Annotation Set*.
6. Click **OK**.

## Associating a User or Group to a Markup Set

If you are a user with Project Administrator rights, you can associate users or groups to markup sets. Once associated, annotations that the user performs in the Project Review will appear on the document in Native or Image view when the markup set is selected.


### To associate a user or group to a markup set

1. Log in as a user with Project Administrator rights.
2. Click the **Markup Sets** tab.  
See [Markup Sets Tab](#) on page 291.
3. Select the markup set that you want to associate to a user or group.
4. Click the *User* or *Group* tab at the bottom of the page.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click the plus sign to add the user or group to the markup set.
7. Click **OK**.

## Disassociating a User or Group from a Markup Set

If you are a user with Project Administrator rights, you can disassociate users or groups to markup sets.

### To disassociate a user or group from a markup set

1. Log in as a user with Project Administrator rights.
2. Click the **Markup Sets** tab.  
See [Markup Sets Tab](#) on page 291.
3. Check the markup set that you want to disassociate to a user or group.
4. Click the *User* or *Group* tab at the bottom of the page.
5. Click the **Remove Association** button .

# Configuring Custom Fields







Custom fields include the columns that appear in the Project Review and categories that can be coded in Project Review. You can create custom fields that will allow you to display the data that you want for each document in Project Review, in production sets, and in exports. Custom fields allow you to:

- Map fields from documents upon import to the custom fields you create. See the Loading Data documentation for more information on mapping fields.
- Code documents for the custom fields in Project Review, using tagging layouts. See the Reviewer Guide for more information on coding data.
  - See [Adding Custom Fields](#) on page 295.
  - See [Creating Category Values](#) on page 296.
  - See [Adding a Tagging Layout](#) on page 298.

## Custom Fields Tab

The *Custom Fields* tab on the *Home* page can be used to add and edit custom fields for Project Review and coding.

### Elements of the Custom Fields Tab


Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Highlight Custom Fields	Displays the custom fields already created for the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Custom Fields List.
Columns 	Adjusts what columns display in the Custom Fields List.
Delete 	Deletes selected custom fields. Only active when one or more custom fields are selected. <b>IMPORTANT:</b> See <a href="#">About Deleting Custom Fields</a> on page 296.
Add Custom Fields 	Adds a custom field.
Edit Custom Fields 	Edits the selected custom field.
Delete Custom Fields 	Deletes the selected custom field. <b>IMPORTANT:</b> See <a href="#">About Deleting Custom Fields</a> on page 296.

## Adding Custom Fields

Project/case managers with the Project Administrator permission can create and edit custom fields. You can use the custom fields to add categories, text, number, and date fields.

When creating a custom field, the application will prevent you from using the name of an existing field.

### To add a custom field

1. Log in as a user with Project Administrator rights.
2. Click the **Custom Fields** tab.  
See [Custom Fields Tab](#) on page 294.
3. Click the **Add** button .
4. In the *Custom Field Detail* form, enter the name of the custom field.
5. Select a Display Type:
  - Check box: Create a column that contains a check box. This is for coding categories only.
  - Date: Create a column that contains a date.
  - Number: Create a column that contains a number.
  - Radio: Create a column that contains a radio button. This is for coding categories only.
  - Text: Create a column that contains text.
6. Enter a *Description* for the custom field.
7. Select **ReadOnly** to make the column un-editable.
8. Click **OK**.

## Editing Custom Fields

Project/case managers with the Project Administrator permission can create and edit custom fields. You cannot edit the Display Type of the custom field.


### To edit a custom field

1. Log in as a user with Project Administrator rights.
2. Click the **Custom Fields** tab.  
See [Custom Fields Tab](#) on page 294.
3. Select the custom field you want to edit.
4. Click the **Edit** button.
5. Make your edits.
6. Click **OK**.

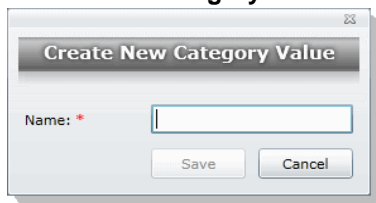
## Creating Category Values

After you have created a Custom Field for check boxes or radio buttons, you can add values to the check boxes and radio buttons in *Project Review*. You can create multiple values for each category.

### To add values to categories

1. Log in as a user with Assign Categories permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, click the **Tags** tab.
4. Expand the *Categories*.
5. Right-click on the category and select **Create Category Value**.

### Create New Category Value Dialog



6. Enter a *Name* for the value.
7. Click **Save**.

## About Deleting Custom Fields

The intent of this feature is that you can quickly delete a custom field that you created with properties that you did not intend. For example, you may realize after saving a custom field that you selected the wrong display type.

If you have been using a custom field, and there is associated data with it, in most cases you will not want to delete it.

**IMPORTANT:** Be aware of the following:

- If you delete a custom field that has been previously used, it will also delete the data contained within the field.
- If you delete a custom field that is used in a Tagging Layout, it will be removed from the layout, but the layout will remain.
- If you delete a custom field that is in use as a column in the *Item List* by another user, the column will stay in their grid until they manually remove it as a selected column. In *Review*, in the *Select Columns* dialog, the deleted column will no longer be displayed in the *Available* columns list, but users will still have to manually remove it from their *Selected* column list.
- It may cause similar problems for any other panel where this field is used.
- It may also cause problems if the field is used in a global replace job that involves the field that hasn't run yet.
- Any user with the appropriate permissions can delete a custom field. For example one user with Admin rights can delete a custom field that was created by a different user.



# Configuring Tagging Layouts

Tagging Layouts are layouts used for coding in the *Project Review* that the project manager creates. Users must have Project Administration permissions to create, edit, delete, and associate tagging layouts. First, you must create the layout, then associate fields to the layout for the reviewer to code, and finally, associate users or groups to the layout so that they can code with it in *Project Review*.









Custom fields must be created by the project manager before they can be added to a tagging layout. See [Configuring Custom Fields](#) (page 294) for information on how to create custom fields.

Tagging Layouts can be used to code fields in the *Project Review* for documents in the project. Coding is editing the data that appears in the fields for each document.




## Tagging Layout Tab

The *Tagging Layout* tab on the *Home* page can be used to create layouts for coding in the *Project Review*.

### Elements of the Tagging Layout Tab

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Tagging Layout List	Displays the tagging layouts already created for the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Tagging Layout List.
Columns 	Adjusts what columns display in the Tagging Layout List.
Delete 	Deletes selected tagging layout. Only active when a tagging layout is selected.
Add Tagging Layout 	Adds a tagging layout.
Edit Tagging Layout 	Edits the selected tagging layout.
Delete Tagging Layout 	Deletes the selected tagging layout.
Tagging Layout Fields Tab 	Allows you to associate/disassociate fields to a tagging layout.
Users Tab 	Allows you to associate users to a tagging layout.


## Elements of the Tagging Layout Tab (Continued)

Element	Description
 Groups Tab	Allows you to associate groups to a tagging layout.
 Add Association	Associates a group, user, or field to a tagging layout.
 Remove Association	Disassociates a tagging layout from a user, group, or field.

## Adding a Tagging Layout

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate tagging layouts.


### To add a tagging layout

1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Click the **Add** button .
4. In the *Tagging Layout Detail* form, enter the name of the *Tagging Layout*.
5. Enter the number of the order that you want the layout to appear to the user in the Project Review. Repeated numbers appear in alphabetical order.
6. Click **OK**.

## Deleting a Tagging Layout

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate tagging layouts.

### To delete a tagging layout

1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Check the layout that you want to delete.
4. Click the **Delete** button .

---

**Note:** You can also delete multiple layouts by clicking the trash can delete button.


---

5. In the confirmation dialog, click **OK**.

## Editing a Tagging Layout

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate tagging layouts.

### To edit a tagging layout



1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Click the **Edit** button .
4. In the *Tagging Layout Detail* form, enter the name of the *Tagging Layout*.
5. Enter the number of the order that you want the layout to appear to the user in the Project Review. Repeated numbers appear in alphabetical order.
6. Click **OK**.

## Associating Fields to a Tagging Layout

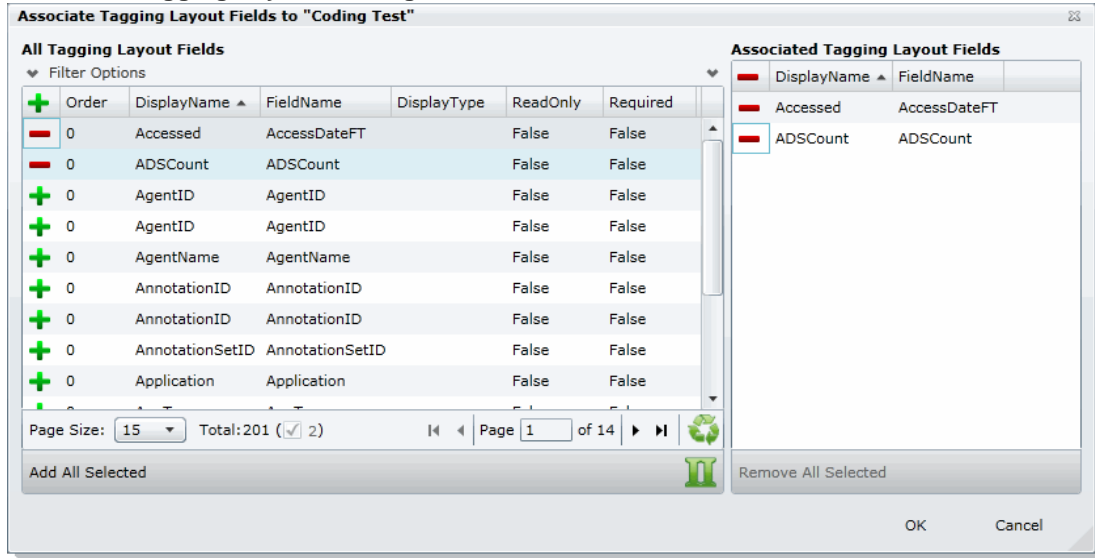
Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate tagging layouts. Custom fields must be created before you can associate them with a tagging layout.

See [Configuring Custom Fields](#) on page 294.

### To associate fields to a tagging layout

1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Select the layout that you want from the Tagging Layout list pane.
4. Select the fields tab in the lower pane .
5. Click the **Add Association** button .

## Associate Tagging Layouts Dialog



- Click to add the field to the layout.
- Click **OK**.
- Enter a number for the Order that you would like the fields to appear in the coding layout.
- Select the fields that you just added (individually) and click the **Edit** button in the Tagging Layout Field Details. Select one of the following:
  - **Read Only**: Select to make the field read only and disallow edits. Any standard or custom field that is defined to be 'Read Only' cannot be redefined as a "Required" or "None."
  - **Required**: Select to make the field required to code before the reviewer can save the coding.
  - **None**: Select to have no definition on the field.
  - **Is Carryable**: Check to allow the field data to carry over to the next record when the user selects the *Apply Previous* button during coding.
- Click **OK**.

---

**Note:** Some fields are populated by processing evidence or are system fields and cannot be changed. These fields, when added to the layout, will have a `ReadOnly` value of `True`.



---

## Disassociating Fields from a Tagging Layout

Project/case managers with the *Project Administrator* permission can disassociate tagging layouts.

### To disassociate fields from a tagging layout



- Log in as a user with Project Administrator rights.
- Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.

3. Select the layout that you want from the Tagging Layout list pane.
4. Click the fields tab in the lower pane .
5. Click the **Remove Association** button .

## Associate User or Group to Tagging Layout

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate tagging layouts.


### To associate users or groups to a tagging layout

1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Select the layout that you want from the Tagging Layout list pane.
4. Open either the *User* or *Groups* tab.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click  to add the user or group to the tagging layout.
7. Click **OK**.

## Disassociate User or Group to Tagging Layout

Project/case managers with the *Project Administrator* permission can disassociate tagging layouts.

### To disassociate users or groups from a tagging layout

1. Log in as a user with Project Administrator rights.
2. Click the **Tagging Layout** tab.  
See [Tagging Layout Tab](#) on page 297.
3. Check the layout that you want from the Tagging Layout list pane.
4. Open either the *User* or *Groups* tab.
5. Check the user or group that you want to disassociate.
6. Click the **Remove Association** button .

# Configuring Highlight Profiles








You can set up persistent highlighting profiles that will highlight predetermined keywords in the *Natural* panel of Project Review. Persistent highlighting profiles are defined by the administrator or project/case manager and can be toggled on and off using the *Select Profile* drop-down in the *Project Review*.

See [Highlight Profiles Tab](#) on page 302.




## Highlight Profiles Tab

The *Highlight Profiles* tab on the *Home* page can be used to set up persistent highlighting profiles that will highlight predetermined keywords in the *Natural* panel in Project Review. Persistent highlighting profiles are defined by the administrator or project manager and can be toggled on and off using the *Select Profile* drop-down in the *Project Review*.

### Elements of the Highlight Profiles Tab

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Highlight Profiles List	Displays the highlight profiles already created for the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Highlight Profiles List.
Columns 	Adjusts what columns display in the Highlight Profiles List.
Delete 	Click to delete selected highlight profiles. Only active when a highlight profile is selected.
Add Highlight Profiles 	Adds a highlight profile.
Edit Highlight Profiles 	Edits the selected highlight profile.
Delete Highlight Profiles 	Deletes the selected highlight profile.
Highlight Profile Keywords 	Allows you to add keywords and highlights to the highlight profile.
Users Tab 	Allows you to associate users to a highlight profile.


## Elements of the Highlight Profiles Tab (Continued)

Element	Description
Groups Tab 	Allows you to associate groups to a highlight profile.
Add Association 	Associates a user or group to a highlight profile.
Remove Association 	Disassociates a highlight profile from a user or group.

## Adding Highlight Profiles

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate highlight profiles.


### To add a highlight profile

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Click the **Add** button .
4. In the *Highlight Profile Detail* form, enter a *Profile Name*.
5. Enter a *Description* for the profile.
6. Click **OK**.

## Editing Highlight Profiles

Project/case managers with the *Project Administrator* permission can create, edit, delete, and associate highlight profiles.


### To edit a highlight profile

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Select the profile that you want to edit.
4. Click the **Edit** button  .
5. In the *Highlight Profile Detail* form, enter a *Profile Name*.
6. Enter a *Description* for the profile.
7. Click **OK**.

## Deleting Highlight Profiles

Project/case managers with the Project Administrator permission can create, edit, delete, and associate highlight profiles.

### To delete a highlight profile

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Select the profile that you want to delete.
4. Click the **Delete** button  .

---


**Note:** You can also delete multiple profiles by clicking the trash can delete button.

---


## Add Keywords to a Highlight Profile

After you have created a highlight profile, you can add keywords to the profile that will appear highlighted in the *Natural* panel of the *Project Review* when the profile is selected.

### To add keywords to a highlight profile

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Select a profile.
4. Select the **Keywords** tab  .



5. Click the **Add Keywords**  button.
6. In the *Keyword Details* form, enter the keywords (separated by a comma) that you want highlighted.
7. Expand the color drop-down and select a color you want to use as a highlight.
8. Click **OK**.
9. You can add multiple keyword highlights, in different colors, to one profile.

---


**Note:** You can edit and delete keyword details by clicking the pencil or minus buttons in the **Keywords** tab.

---

## Associating a Highlight Profile

Project/case managers with the Project Administrator permission can create, edit, delete, and associate highlight profiles. You can associate highlight profiles to users and groups.


### To associate a highlight profile to a user or group

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Select the profile that you want to associate to a user or group.
4. Open either the *User* or *Groups* tab.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click the plus sign to associate the user or group with the profile.
7. Click **OK**.

## Disassociating a Highlight Profile

Project/case managers with the Project Administrator permission can disassociate highlight profiles from users or groups.

### To disassociate a highlight profile from a user or group

1. Log in as a user with Project Administrator rights.
2. Click the **Highlight Profiles** tab.  
See [Highlight Profiles Tab](#) on page 302.
3. Select the profile that you want to disassociate from a user or group.
4. Open either the *User* or *Groups* tab.
5. Select the user or group that you want to disassociate.
6. Click the **Remove Association** button .







# Configuring Redaction Text

Project/case managers with the Project Administration permission can create redaction text profiles with text that appears on redactions on documents. Redactions can be made in the *Image* or *Natural* panel of the *Project Review*.

## Redaction Text Tab

The *Redaction Text* tab on the *Home* page can be used to add, edit, and delete redaction text profiles. Redactions can be made in the *Image* view of the *Project Review*.

### Elements of the Redaction Text Tab


Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Redaction Text Profile List	Displays the available redaction text profiles. Click the column headers to sort by the column.
Refresh 	Refreshes the Redaction Text Profile list.
Columns 	Adjusts what columns display in the Redaction Text Profile list.
Delete 	Deletes selected redaction text profile. Only active when a redaction text is selected.
Create Redaction Text Profile 	Creates a redaction text profile. See <a href="#">Creating a Redaction Text Profile</a> on page 306.
Edit Redaction Text 	Edits the selected redaction text profile.
Delete Redaction Text 	Deletes the selected redaction text profile.

## Creating a Redaction Text Profile

Project/case managers with the *Project Administration* permission can create the text that appears on redactions by adding redaction text profiles.

### To create redaction text profiles


1. Log in as a user with Project Administrator rights.
2. Click the **Redaction Text** tab.  
See [Redaction Text Tab](#) on page 306.

3. Click the **Add** button  .
4. In the *Redaction Text Detail* form, enter the text that you want to appear on the redaction.
5. Click **OK**.

## Editing Redaction Text Profiles

Project/case managers with the *Project Administration* permission can edit the text that appears on redactions by editing the redaction text profiles.


### To edit redaction text profiles

1. Log in as a user with Project Administrator rights.
2. Click the **Redaction Text** tab.  
See [Redaction Text Tab](#) on page 306.
3. Click the **Edit** button  .
4. In the *Redaction Text Detail* form, enter the text that you want to appear on the redaction.
5. Click **OK**.

## Deleting Redaction Text Profiles

Project/case managers with the *Project Administration* permission can delete redaction text profiles.

### To delete redaction text profiles

1. Log in as a user with Project Administrator rights.
2. Click the **Redaction Text** tab.  
See [Redaction Text Tab](#) on page 306.
3. Select the redaction text that you want to delete.
4. Click the **Delete** button  .

# Chapter 24

## Monitoring the Work List


---

The project/case manager can use the *Work List* tab on the *Home* page to monitor certain activities in the project. The following items are recorded in the Work List: searches, review sets, imaging, label assignments, imports, bulk coding, cluster analysis, bulk labeling, transcript/exhibit uploading, and delete summaries.

The Job IDs are unique to every job. Jobs cannot be deleted or edited, only monitored. Project managers can be informed as to the actions performed in the project and errors that users have encountered in the project from the *Work List* tab.

## Accessing the Work List



### To access the Work List

- ❖ From the Home page, select a project, and click the  **Work List** tab.


### *Work List Tab*

The *Work List* tab on the *Home* page can be used to view data for the selected project. The bottom panel displays the number of documents processed and number of errors. This will be updated periodically to reflect current status.

### Elements of the Work List Tab

Element	Description
Filter Options	Allows you search and filter all of the items in the list. You can filter the list based on any number of fields. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Work List	Displays the jobs associated with the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Work List. <b>Note: The Work List will automatically refresh every three minutes.</b>
Columns 	Adjusts what columns display in the Work List.

## Elements of the Work List Tab (Continued)

Element	Description
Overview Tab 	Displays the statistics on the data found in the Work List.


## Cancelling Review Jobs

You can cancel certain jobs that you may have started while in Review. This allows you to resubmit work or cancel a process that you may not want to complete. Cancelling these jobs will cancel any work that has not yet been completed. Any work that has already completed will be retained.

You can cancel the following jobs from the work list:

- Imaging
- Bulk Coding
- Network Bulk Printing
- OCR Documents

### To cancel a review job from the Work List

1. From the Work List, select the review job that you want to cancel.
2. Click  to cancel the review job.

# Chapter 25

## Managing Document Groups

---

### About Managing Document Groups

Project/case managers with *Folders and Project Administration* permissions can manage document groups. Document groups are folders where imported evidence is stored. You use document groups to organize your evidence by culling the data via permissions.

Document groups can contain numerous documents. However, any given document can be in only one document group. You cannot assign permissions for documents unless the documents are in a document group. All documents in a group will be assigned DocIDs. Documents not within a document group, will NOT have DocIDs.

You can name your document group to reflect where the files were located. The name can be a job number, a business name, or anything that will allow you to recognize what files are contained in the group.

Document groups can be created in two ways: by importing evidence, or by selecting Document Groups in *Project Review*.

See [Creating a Document Group During Import](#) on page 313.

See [Creating a Document Group in Project Review](#) on page 313.

---

**Note:** To make sure that the DocID, ParentDocID, and AttachDocIDs fields populate in the Family records, include at least one parent document and one child document when creating the document group.

---

### About DocIDs and Object IDs

DocIDs are assigned to document groups by sorting into the object ID order and then putting the objects into the family order. The family order takes top priority.

Suppose you ignore all objects that are in a family except for the heads of family. The remaining objects (all objects that are not in a family and all heads of family) appear in object ID order. Objects that are in a family appear immediately after the head of family.

### How DocIDs are Created

Doc IDs can either be imported or generated. When an import occurs, in the load file there is generally a doc ID associated with each object. The doc ID for each imported object can be seen in the *DocID* column in Review. This doc ID is also known as the *original* doc ID.

Doc IDs are also generated during the creation of a production set or export set. These doc IDs do not appear in the *DocID* column in review – they are only associated with the object in the context of the production set or export set.

Note that there is also a *Page ID* generated for each page of a document. The *Page ID* can be branded on each page. In most cases, the *Page ID* is related to the *Doc ID*.

## Production Sets and Load File and Native Export Sets

There are two numbering styles for production/export sets: *Australian*, and *US and all others*. This topic only describes US-style numbering.

When creating a production set, on the *Volume Document Options* tab, there are four *Naming Options*:

- New Production Doc ID
- Original Doc ID
- Original File Name
- Original File Name with Original Path

### New Production Doc ID

This is the default. The doc ID is generated based on the selections in the Document section on the right-hand side of the *Volume Document Options* tab. There are three different options, but with any option, the doc ID consists of an optional prefix, a number that is padded with zeroes on the left, and an optional suffix. The numeric portion begins with the starting number, which defaults to 1. The *Padding* is the minimum width of the numeric portion. For example, if *Prefix* is *ABC*, *Suffix* is empty, *Starting Number* is 1, and *Padding* is 4, then the first doc ID will be *ABC0001*.

How the doc IDs are incremented and how the page IDs are generated differ based on the option:

- Independent Document and Page Numbering. There are separate sections for documents and pages for the prefix, suffix, starting number, and padding. The document settings control the doc ID, the name of the exported native file, and the name of the exported text file. The documents are numbered sequentially. The page settings control the page ID and the names of the images files. Each page is numbered sequentially. For images files with one file for the entire document, e.g., PDF, the name of the image file is the same as the page ID of the first page. The doc IDs and the page IDs are not correlated – the doc ID is incremented once for each document, while the page ID is incremented once for each page of each document. For example, the doc IDs might be D000001, D000002, D000003, etc. The page IDs might be:
  - For D000001, page IDs P000001, P000002, P000003, P000004.
  - For D000002, page IDs P000005
  - For D000003, page IDs P000006, P000007, P000008.
  - Etc.
- Number by Document with Page Counter Suffix. Documents are numbered sequentially. The page ID of each page is the doc ID followed by a period (.) and the page number padded with zeroes to a width of four digits. For example, the documents might be ABC000001, ABC000002, etc. The pages of ABC000002 would be numbered ABC000002.0001, ABC000002.0002, ABC000002.0003, etc.
- Number by Page. The page IDs of each page of each document are numbered sequentially, continuing across documents. For example, if the page ID of the first page of the first document is D000001, and the document contains two pages, then the page ID of page 2 of the first document is D000002, and the page

ID of the first page of the second document is D000003. The doc ID of each document is the page ID of the first page of the document.

## Original Doc ID

The doc ID of each document is the doc ID imported with the document or assigned to it when it is added to a document group. The prefix, suffix, starting number, and padding that are selected in the document naming parameters are only used for documents that do not have an original doc ID.

- **Independent Document and Page Numbering.** There are separate sections for documents and pages for the prefix, suffix, starting number, and padding. The doc ID is taken from the original doc ID, if the document has one; otherwise, the doc ID is generated from the document settings. The doc ID is used as the file name for the exported native file and the exported text file. The page settings control the page ID and the names of the images files. Each page is numbered sequentially. For images files with one file for the entire document, e.g., PDF, the name of the image file is the same as the page ID of the first page.
- **Number by Document with Page Counter Suffix.** The doc ID is the original doc ID. The page ID of each page is the doc ID followed by a period (.) and the page number padded with zeroes to a width of four digits.
- **Number by Page.** The doc ID is the original doc ID. The page ID of the first page is the doc ID. The page ID of each subsequent page is one higher than that of the previous page. This option assumes that there is a sufficient gap between successive doc IDs to provide a unique number for each page. If this is not the case, then the same page ID may be assigned to pages in different documents. This is especially the case when the original doc IDs are sequential. For example, let's say that ten documents of ten pages each are imported, and that the doc IDs of these documents are ABC000001, ABC000011, ABC000021, ..., ABC000091. The page IDs of ABC000001 will be ABC000001, ABC000002, ABC000003, ..., ABC000010. The page IDs of ABC000011 will be ABC000011, ABC000012, ABC000013, ..., ABC000020. The page IDs of ABC000091 will be ABC000091, ABC000092, ABC000093, ..., ABC000100. On the other hand, if these same documents were imported with doc IDs of ABC000001, ABC000002, ABC000003, ..., ABC000010, then the page IDs of ABC000001 will be ABC000001, ABC000002, ABC000003, ..., ABC000010, while the page IDs of ABC000002 will be ABC000002, ABC000003, ABC000004, ..., ABC000011. Thus most of the page IDs of the imported files overlap. The second example demonstrates that with imported files with sequential doc IDs, if using original doc ID naming, the documents should generally be numbered with the Number by Document with Page Counter Suffix option and not the Number by Page option.

## Original File Name and Original File Name with Original Path

The doc ID is the original file name (not including the rest of the file path) without the file extension.



# Creating a Document Group During Import


While importing evidence, you can create a document group. You can also place the documents into an existing document group.

See the *Loading Data* documentation for information on how to create new document groups while importing evidence and putting evidence into existing document groups.

## Creating a Document Group in Project Review

Project/case managers with *Folders* permissions can create Document Groups in the Project Review.


### To create document groups in Project Review

1. Prepare documents to be added to a Document Group by applying labels. See [Managing Labels](#) on page 269.
2. Log in as a user with Project Administrator rights.
3. Click the **Project Review**  button next to the project in the *Project List*.
4. In the *Project Explorer*, click the *Explore* tab.
5. Right-click **Document Groups** and select **Create Document Group**.
6. Enter a *Name* for the document group.
7. Enter a *Description* for the document group.
8. Click **Next**.
9. Check the labels that you want to include in the document group.
10. Click **Next**.
11. Select one of the following:
  - **Continue from Last**: Select to continue the numbering from the last document.
  - **Assign DocIDs**: Select to assign DocID numbers to the records.
12. Enter a *Prefix* for the new numbering.
13. Enter a *Suffix* for the new numbering.
14. Select a *Starting Number* for the documents.
15. Select the *Padding* for the documents.
16. Click **Next**.
17. Review the *Summary* and click **Create**.
18. Click **OK**.
19. When the job is successfully created, click **Close**.

# Renumbering a Document Group in Project Review

Project/case managers with *Folders* permissions can renumber Document Groups in the Project Review. This lets you eliminate gaps and correct incorrect numbering. Upon the case of a deleted and recreated sub set of documents within a document group, you can provide different numbering.

## To renumber document groups in Project Review


1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, expand the **Document Groups** folder.
4. Right-click an existing *Document Group* folder and select **Renumber Document Group**.
5. Enter a *Prefix* for the new numbering.
6. Enter a *Suffix* for the new numbering.
7. Select a *Starting Number* for the documents.
8. Select the *Padding* for the documents.
9. Click **Next**.
10. Review the *Summary* and click **Renumber**.
11. Click **OK**.

# Deleting a Document Group in Project Review

Project/case managers with *Folders* permissions can delete Document Groups in the Project Review. Deleting a document group allows you to move a document from one document group to another group, create sub document groups and create master document groups. When deleting a document group, the application deletes any associations to the deleted group that a particular document has.

The application also deletes any DocIDs of documents that were in the deleted group. This allows you to assign a document to a new document group, or alter an existing document group. You will need to assign new DocIDs to documents that were in a deleted document group.

## To delete document groups in Project Review


1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, expand the **Document Groups** folder.
4. Right-click a *Document Group* and select **Delete Document Group**.
5. Click **OK**.

# Managing Rights for Document Groups in Project Review

You can designate an existing User Group to have security permissions to manage Document Groups.

For information on creating User Groups, see and *Admin Guide*.

## To assign security permissions to a User Group for a Document Group

1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, expand the **Document Groups** folder.
4. Right-click a *Document Group* and select **Manage Permissions**.
5. Check the User Groups that you want to assign.
6. Click **Save**.

## Chapter 26

# Managing Transcripts and Exhibits



---

Project/case managers with *Upload Exhibits*, *Upload Transcripts*, and *Manage Transcripts* permissions can upload transcripts, create transcript groups, grant transcript permissions to users, and upload exhibits. Transcripts are uploaded from Project Review and can be viewed and annotated in the Transcripts panel.

## Creating a Transcript Group

Project/case managers with the *Create Transcript Group* permission can create transcript groups to hold multiple transcripts.


### To create a transcript group

1. Log in as a user with *Create Transcript Group* permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, right-click the *Transcripts* folder and click **Create Transcript Group**.
4. Enter a *Transcript Group Name*.
5. Click **Save**.
6. After creating the group, refresh the panel by clicking  (*Refresh*) at the top of the Project Explorer panel.

## Uploading Transcripts

Project/case managers with the *Upload Transcripts* permission can upload either .PTX or .TXT transcript files and put them in transcript groups. You can only add transcripts one at a time. When you upload a transcript, they are automatically indexed.

### To upload transcripts

1. Log in as a user with *Upload Transcripts* permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, right-click the *Transcripts* folder and click **Upload Transcript**.

## Upload Transcript Dialog

Upload Transcript

Transcript File: \*  Browse...

Transcript Groups: \* Group1


Deponent: \*

Deposition Date: \* 11/30/2011 15

Deposition Volume: 0  
(Deposition Volume cannot be greater than 200.)

This transcript contains unnumbered preamble pages.


Upload Transcript Cancel

4. Click **Browse** to find the transcript file, highlight the file, and click **Open**.
5. Select a *Transcript Group* from the menu.  
See [Creating a Transcript Group](#) on page 316.
6. Enter the name of the *Deponent*.
7. Select the *Deposition Date*.
8. If you are uploading more than one transcript from the same day, specify the volume number to differentiate between transcripts uploaded on the same date.
9. Select **This transcript contains unnumbered preamble pages** to indicate that there are pages prior to the testimony. If you check this box, enter the number of preamble pages prior that occur before the testimony. These pages will be numbered as "Preamble 0000#." The numbering continues as normal after the preamble pages.
10. If the transcript is password protected, enter the password in the **Password** field.
11. Click **Upload Transcript**.
12. After the upload is complete, refresh the *Item List*.
13. To view the transcripts that have been uploaded, select the Transcript Groups that you want to view and click  (*Apply*) on the *Project Explorer* panel.  
See the *Reviewer Guide* for more information on viewing and working with transcripts.

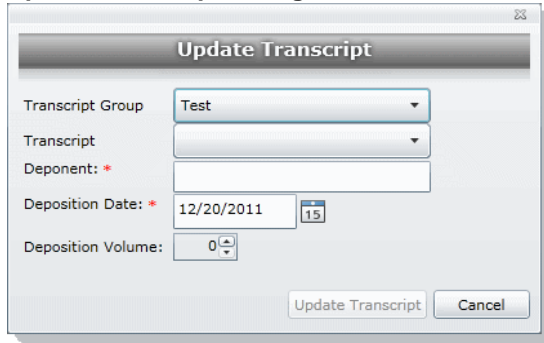
## Updating Transcripts

Project managers with the Upload Transcripts permission can update transcripts in transcript groups. You can only update transcripts one at a time.

### To update transcripts

1. Log in as a user with Upload Transcripts permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, right-click the *Transcripts* folder and click **Update Transcript**.

## Update Transcript Dialog



4. Select a *Transcript Group*.
5. Select a *Transcript*.
6. Enter the *Deponent* name.
7. Enter the *Deposition Date*.
8. If you are uploading more than one transcript on the same day, specify the volume number to differentiate between transcripts uploaded on the same date.
9. Click **Update Transcript**.

## Creating a Transcript Report


Project/case managers with the *Create Transcript Report* permission can create a report of the notes and highlights on a transcript. If there are no notes or highlights on a report, a report will not be generated.

---

**Note:** You can create a report containing issues with notes or a report containing issues without notes, but you cannot create a report that contains both issues with notes and issues without notes. If you create a report with notes without issues but the selected notes have been previously assigned to an issue, those notes will not appear in the report.

---

### To create a transcript report

1. Log in as a user with *Create a Transcript Report* permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. From the **Explore** tab in the *Project Explorer*, right-click the *Transcripts* folder and click **Transcript Report**.

## Transcript Report Dialog

Transcript Report View

Notes

Include Notes

My notes  All Users notes

- Fraud
- Insurance
- Tax

[Select All](#) | [Select None](#)

Highlights

Include Highlights


My highlights  All Users highlights

4. Select **Include Notes**. You can mark whether to generate a report of all the users' notes or just your own notes.
5. Check any issues that you want included in the report. Click **Select All** to select all of the issues to include or click **Select None** to deselect all of the issues.
6. Select **Include Highlights**. You can mark whether to generate a report of all the users' highlights or just your own highlights.
7. Click **Generate Report**.

# Capturing Realtime Transcripts

You have the ability to run a Realtime transcript session and capture the stream from a court reporter's stenographer machine. You can either connect to a court reporter's machine or run a demonstration of the Realtime transcript with a simulated transcription.

## To capture a Realtime transcript

1. Log in as a user with *Realtime Transcripts* permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. From the *Explore* tab in the *Project Explorer*, right-click the *Transcripts* folder and select **Start Realtime Transcripts**.
4. A dialog displays asking to start a new Realtime session or resume a previous session. Click **Start New Realtime Session**.
5. Click **Next**.
6. Enter the options that you want associated with this transcript:
  - **Transcript Group:** You must select a group for the realtime transcript. If no groups are defined, exit the wizard and create a group. See [Creating a Transcript Group](#) on page 316.
  - **Deponent**
  - **Deposition Date**
  - **Volume:** If you are capturing more than one transcript on the same day, specify the volume number to differentiate between the transcripts captured on the same date.
7. Click **Next**.
8. Select the serial port that will contain the feed from the court reporter's machine. The default port is COM1. Once selected, ask the Court Reporter to type a few lines to test the port. If you do not see any lines behind the wizard window, select another port and retry. If none of the ports work, check your connections.
9. Click **Next**.

## Set up Realtime Transcript Properties Dialog

Set up Realtime Transcript

**Properties**

Source | Steno Feed | Serial Port Settings

Source Type:  
Serial

Lines Per Page: 25

Time Codes

Time of Day  
 Time From Court Reporter  
 Start Time 10:07:14  
 No Time Codes

Time Codes every: 5 lines

Click Next to continue

Back Next Cancel



10. In the **Set up Realtime Transcript Properties** dialog, you have several options in setting up your transcript.
11. Click **Test** to test the connection. Once the connection test is successful, click **Finish**.

### Elements of the Set up Realtime Transcript Properties Dialog

Element	Description
<b>Source</b>	
Source Type	Allows you to select from which port you are receiving the stenographer's feed. The default is the serial port.
Lines Per Page	Allows you to enter how many lines you want to appear for each page of the transcript.
Time Codes	Allows you to stamp a time code on the transcript. You can choose to display the time based on the following options: <ul style="list-style-type: none"> <li>• Time of Day - Marks the transcript with the time of day as indicated by your system.</li> <li>• Time From Court Reporter - Marks the transcript with the same time as indicated by the court reporter's stenographer machine.</li> <li>• Start Time - Specifies the time stamped on the transcript.</li> <li>• No Time Codes - Specifies that no time code is stamped on the transcript.</li> <li>• Time Codes every x lines - Specifies how frequent the time code appears on the transcript.</li> </ul>
<b>Steno Feed</b>	
	Allows you to set the options for the court reporter's stenographer feed. Before connecting and receiving the stenographer feed, make sure that you have the correct serial settings for the stenographer feed.
Steno Feed Format	Allows you to choose to receive the court reporter's feed in either CaseView or ASCII format.
Line Terminator	<b>Available only for ASCII format.</b> Allows you to indicate line termination by CRLF (carriage return line feed), CR only (Carriage return), or LF only (line feed).
<b>Serial Port Settings</b>	
	Allows you to configure the serial port settings for the stenographer feed. You can set the following options: <ul style="list-style-type: none"> <li>• Port - The interface where the feed is transmitted. This will usually be COM1.</li> <li>• Baud Rate - The speed in which the data is sent. You can select a rate between 110 baud and 56000 baud.</li> <li>• Data Bits - The number of data bits sent with each character. Most characters will have eight bits (ddb8).</li> <li>• Parity - Parity detects errors in the feed. You can set the parity to either None, Even, Odd, Mark, and Space. The default setting is None.</li> <li>• Stop Bits - Stop bits allow the system to resynchronize with the feed. The default setting is one bit.</li> </ul>

## Marking Realtime Transcripts

Once you have a successful connection and start receiving the transcript, you can mark it and link it to other documents in the project. The Transcript window displays after connecting to the stenographer's machine. The Transcript window displays two panes: the *Notes/ Linked* pane and the *Transcript* pane. The following tables describe the functions of the elements of the two panes.


## Realtime Notes/Linked Panels

Page	Line	Note	Issues	Date	Owner
3		6the		04/13/2013	
9		10VI		04/13/2013	

Actions:   
Page 2 | Page Size: 25 | Page 1 of 1

Tabs:

## Realtime Notes/Linked Panel Elements

Element	Description
<b>Notes</b>	This tab manages the Quick Mark notes that are produced in the Realtime transcript.
<b>Actions</b>	Provides the ability to perform a selected task on the items within the panel.
<b>Delete</b>	Provides the ability to delete any Quick Mark notes or links.
<b>Filters</b>	Provides the ability to filter notes and linked documents. You can filter notes by page, line, note, issues, date or owner. You can filter linked documents by DocID, LinkObjectID, or file path.
<b>Linked</b>	This tab manages links from the transcript to other documents in the project.
	Provides the ability to link to other documents in the project.

## Realtime Transcript Panel

Transcript


13 to  
 14 DRA~  
 02:22:50 15  
 16 it?  
 17 whatever  
 18 A.  
 19 A.  
 02:22:59 20  
 21 utilized  
 22  
 23 BY  
 24 the  
 02:23:04 25

---

Page Number 00004

1 you  
 2 remember  
 3 mark  
 4 A.  
 02:23:10 5  
 6 A.  
 7 Q.


## Realtime Transcript Panel Elements

Element	Description
Disconnect	This option allows you to disconnect from the court reporter's feed.
Line/Word	This option controls how the data is entered into the transcript. You can have the data entered word by word, or allow a line to be completed and populated before the data is transmitted.
No Scroll/Auto Scroll	This option displays whether the feed scrolls or not. If No Scroll is selected, the scroll bar will continue to move, but the feed will not move until you pull down the scroll bar. Exercise this option by toggling.
Suspend/Continue	This option allows you to either suspend or continue the feed. Exercise this option by toggling.
Quick Mark	This option allows you to quick mark the transcript. A quick mark is a note that you can enter and add additional information to the transcript. The quick mark will occur at the last known word/line. You can also quick mark the transcript by clicking the space bar.
	The search bar allows you to search for words or phrases within the transcript.
Save	Allows you to save the transcript draft.

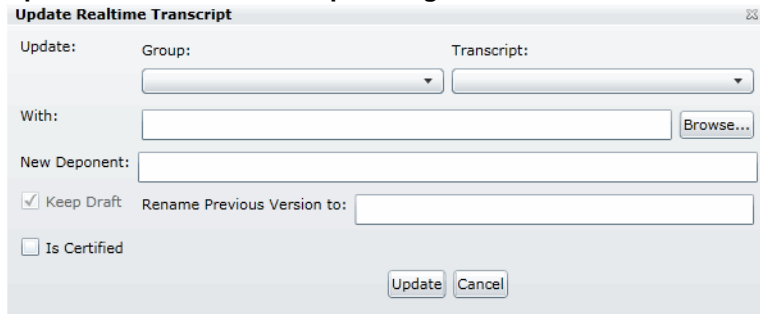
## Updating a Realtime Transcript

Project managers with the Update Realtime Transcript permission can replace an earlier saved version of a Realtime transcript with a new version.

### To update a Realtime transcript

1. Click the **Project Review**  button next to the project in the *Project List*.
2. From the **Explore** tab in the *Project Explorer*, right-click the *Transcripts* folder and click **Update Realtime Transcript**.
3. Enter the information in the dialog.
4. Click **Update**.

### Update a Realtime Transcript Dialog



## Elements of the Realtime Transcript Dialog


Element	Description
Update	Allows you to enter the transcript that you want to replace. Select the transcript name and group name from the pull-down menu.
With	Allows you to enter the new transcript. You can enter the filename in the field or browse to the location on the system.
New Deponent	Allows you to add a new deponent to the transcript if you want.
Keep Draft	Allows you to select to keep the original version that you are replacing.
Rename Previous Version to:	Allows you to rename the original version to avoid confusion between versions.
Is Certified	Allows you to select whether the new version of the transcript is certified or not.

# Using Transcript Vocabulary

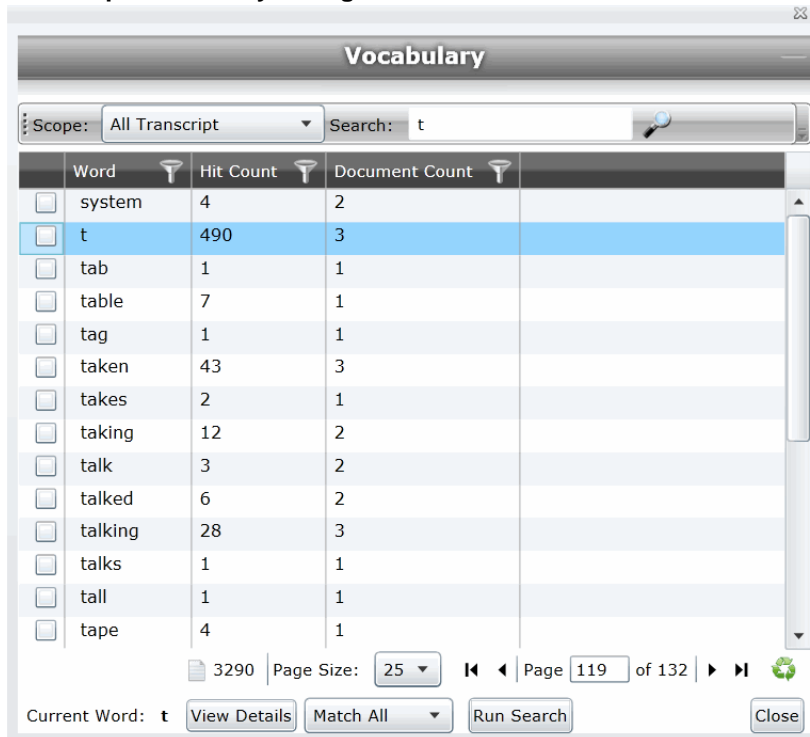
The Transcript Vocabulary feature uses dtSearch to create an index of all of the unique words in a transcript. The index lists all of the unique words contained in the specific transcript or all transcripts. (Noise words, such as **an** and **the**, are not included in the index.) You can use the Transcript Vocabulary feature to isolate transcripts that include specific words, and search for those words in the transcript. Navigate between highlighted terms and view the highlighted terms in context of the transcript.

**Note:** The content of headers, preambles, and margins of the transcripts are included in the Vocabulary index.

## To use Transcript Vocabulary

1. Click the **Project Review**  button next to the project in the *Project List*.
2. Select **Vocabulary** from the **Search Options** menu.  
The *Vocabulary* dialog appears.



## Transcript Vocabulary Dialog



## Elements of the Vocabulary Dialog

Element	Description
Scope	Narrows the scope of the vocabulary index as follows: <ul style="list-style-type: none"><li>• All Transcript - Builds an index from all of the transcripts in the project.</li><li>• Transcript in List - Builds an index from the transcripts in the <i>Item List</i>.</li></ul>

## Elements of the Vocabulary Dialog

Element	Description
Search	Allows you to search for a word or a group of words in the vocabulary list. Entering a letter in the search field retrieves a list of words that begins with the letter entered.
	Displays the word count of the vocabulary index. This count changes depending upon the scope of the transcript vocabulary.
Page Size	Changes the number of word rows displayed in the pane.
Page ___ of	Navigates between pages of words listed.
	Refreshes the word list.
View Details	Displays more details on documents that contain the word in the highlighted row. This word appears in the <i>Current Word</i> field. <b>Note:</b> Only details of the highlighted word appear in the <i>Current Word</i> field, even when other words are selected in the Vocabulary list. When selected, a dialog appears. See <a href="#">Viewing Details of Words in the Vocabulary Dialog</a> on page 326.
Run Search	Searches for documents containing certain words selected in the Vocabulary list. <b>Note:</b> This search searches the entire project, not just transcript documents. Any documents found post back to the <i>Item List</i> . You can check any number of words to include in the search. Select <i>Match All</i> from the menu to return documents that contain all of the words selected or <i>Match Any</i> to return documents that contain any of the words selected.

## Viewing Details of Words in the Vocabulary Dialog

In the Vocabulary dialog, you can view details of the documents that contain the word that you are examining. Within the *Documents Containing* dialog, you can view a list of documents and filter by TranscriptName, ObjectID, or Hit Count.

---

**Note:** The TranscriptName contains the deponent name, deposition date, and volume (if specified).


---

Select a document in the document list and click **View Selected Document** to open the document to view the selected word. The document opens in the *Natural Viewer* and the selected word highlights in the *Natural Viewer*. Click Close to exit the *Documents Containing* dialog.

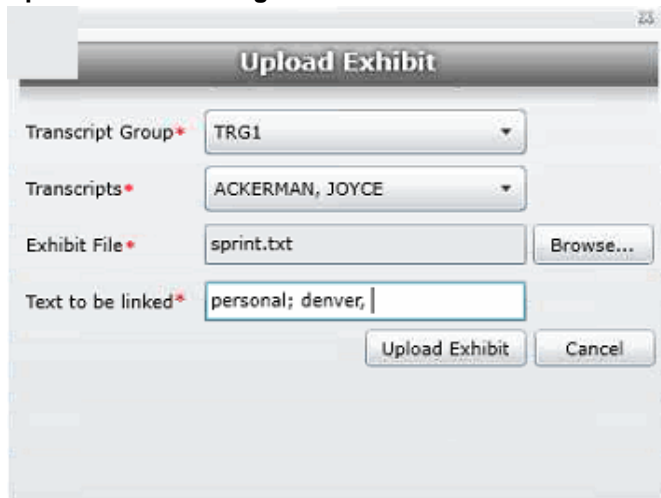
# Uploading Exhibits

Project/case managers with the *Upload Exhibits* permission can upload exhibits in Project Review. You can view exhibits in the exhibits panel.

## To upload an exhibit

1. Log in as a user with *Upload Exhibits* permissions.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. In the *Project Explorer*, right-click the *Transcripts* folder and click **Upload Exhibits**.

## Upload Exhibit Dialog



4. Select the *Transcript Group* that contains the transcript to which you want to link the exhibit.
5. From the *Transcripts* menu, select the transcript to which you want to link the exhibit.
6. Click **Browse**, highlight the exhibit file, and click **Open**.
7. In the *Text to be linked* field, enter the text (from the transcript) that will become a link to the exhibit. You can enter multiple text or aliases to be linked. Separate the terms by either a comma and/or a semi-colon. Every occurrence of the text in the transcript becomes a hyperlink to the exhibit.
8. Click **Upload Exhibit**.

# Chapter 27

## Managing Review Sets


---

Review sets are batches of documents that you can check out for coding and then check back in. Review sets aid in the work flow of the reviewer. It allows the reviewer to track the documents that have been coded and still need to be coded. Project/case managers with Create/Delete Review Set permissions can create and delete review sets.

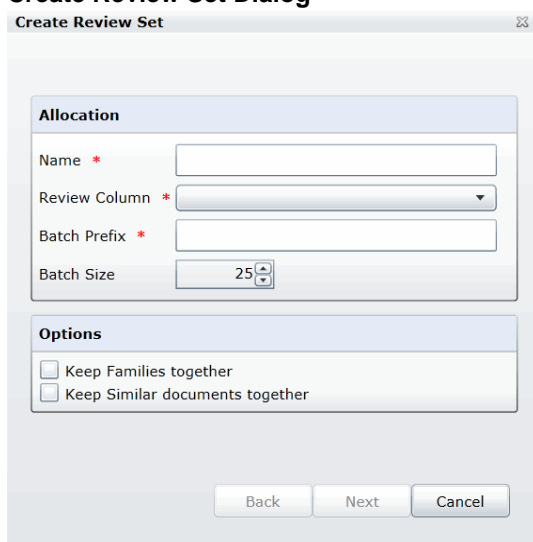
### Creating a Review Set

Project/case managers with *Create/Delete Review Set* permissions can create and delete review sets.

#### To create a review set

1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. Click the **Review Sets** button in the *Project Explorer*.  
See the Reviewer Guide for more information on the Review Sets tab.
4. Right-click the **Review Sets** folder and click **Create Review Set**.

#### Create Review Set Dialog



**Allocation**

Name \*

Review Column \*

Batch Prefix \*

Batch Size

**Options**

Keep Families together

Keep Similar documents together

5. Enter a *Name* for the review set.



6. Select a **Review Column** that indicates the status of the review. New columns can be created in the *Custom Fields* tab of the *Home* page.  
See [Custom Fields Tab](#) on page 294.
7. Enter a prefix for the batch that will appear before the page numbers of the docs.
8. Increase or decrease the *Batch Size* to match the number of documents that you want to appear in the review set.
9. Check the following options if desired:
  - **Keep Families together**: Check this to include documents within the same family as the selected documents in the batch.
  - **Keep Similar document sets together**: Check this to include documents related to the selected documents in the batch.

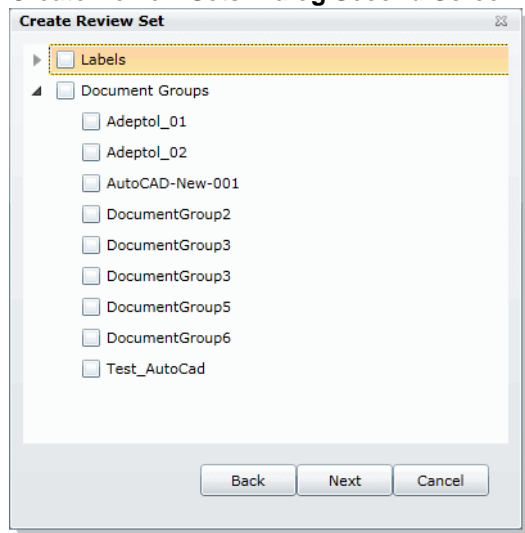
---

**Note:** Any “Keep” check box selected will override the restricted Batch Size.

---

10. Click **Next**.

### Create Review Sets Dialog Second Screen




11. Expand *Labels* and check the labels that you want to include in the review set. All documents with that label applied will be included in the review set. This is only relevant if the documents have already been labeled by reviewers.
12. Expand the *Document Groups* and check the document groups that you want to include in the review set.
13. Click **Next**.
14. Review the summary of the review set to ensure everything is accurate and click **Create**.
15. Click **Close**.

# Deleting Review Sets

Project/case managers with *Create/Delete Review Set* permissions can create and delete review sets.


## To create a review set

1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. Click the **Review Sets** button in the *Project Explorer*.  
See the Reviewer Guide for more information on the Review Sets tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to delete and click **Delete**.
6. Click **OK**.

# Renaming a Review Set

Project/case managers with *Manage Review Set* permissions can rename review sets.


## To rename a review set

1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. Click the **Review Sets** button in the *Project Explorer*.  
See the Reviewer Guide for more information on the *Review Sets* tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to rename and click **Rename**.
6. Enter a name for the review set.

# Manage Permissions for Review Sets

Project/case managers with *Manage Review Set* permissions can manage the permissions for review sets.

## To rename a review set

1. Log in as a user with Project Administrator rights.
2. Click the **Project Review**  button next to the project in the *Project List*.
3. Click the **Review Sets** button in the *Project Explorer*.  
See the Reviewer Guide for more information on the Review Sets tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to manage permissions for and click **Manage Permissions**.

## Assign Security Permissions Dialog



6. Check the groups that you want to grant permissions to the review set. Groups granted the Check In/Check Out Review Batches permission will be able to check out the review sets to which they are granted permission.
7. Click **Save**.

# Chapter 28

## Project Folder Structure

---

This document describes the folder structure of the projects in your database. The location of the project folders will differ depending on the project folder path where you saved the data.

### Project Folder Path

When a project is created, a Project Folder is created in the Project Folder Path provided by the user that creates the project. The Project Folder consists of alphanumeric characters auto generated by the application.

Project Folder example: 3fc04d13-1b48-40a5-80d3-0e410e8e9619.

### *Finding the Project Folder Path*

You can find your project folder path by looking at the Project Details tab.

#### **To find the project folder path**

1. Log in to the application.
2. Select the project in the *Project List* panel.
3. Click on the **Project Detail** tab on the Home page.
4. Under *Project Folder Path*, the path is listed.

# Project Folder Subfolders

Within the Project Folder, there are multiple subfolders. What subfolders that are available to view will depend upon the project and the evidence loaded within the project. This section describes those subfolders.

Please note most of the files within the subfolders are in the DAT extension. This is the extension that the application requires in order to read the contents of these files. The filename (<number>.dat) represents the ObjectID of that document. It should match the ObjectID column displayed in the Project Review.

- **CoolHTML:** This folder contains the CoolHTML files. The application converts all email files into CoolHTML files in order for the native viewer to display them.
- **Native:** This folder contains all the native files. This only pertains to Imported DII Documents and Production Set Documents.
- **Tiff:** This folder contains the Image Documents. This only pertains to Imported DII Image Documents, Production Set Image Documents, and Documents imaged using the “Imaging” option in the Item List panel of the Project Review.
- **PDF:** This folder contains the Image Documents. These are imaged using the “Imaging” option in the Item List panel of Project Review and selecting the pdf option.
- **Graphic\_Swf:** This folder contains flash files created when imaging documents. There are two ways to create these flash files:
  - Click on the **Annotate** button from the *Image* tab of the Document Viewer.
  - Select **Imaging** in the mass operations of the *Item List* panel and then select the **Process for Image Annotation** option.
- **Native\_Swf:** This folder contains flash files created when imaging documents. There are two way to create these flash files:
  - Click on the **Annotate** button from the *Natural* tab of Document Viewer.
  - Select **Imaging** in the mass operations of the *Item List* panel and then select the **Process for Native Annotation** option.
- **Reports:** This folder contains any report that is downloadable from within the program’s interface, including project level reports such as Deduplication, Data Volume, Search, and Audit Log Reports.
- **Slipsheets:** This folder is a temporary location to place slipsheets during an imaging, production set, or export job where images are requested. During the job if a particular document cannot be imaged, the program will create a slipsheet for the document, which is stored in this file. As the job gets to completion, the program will move that slipsheet into the appropriate folder (with the appropriate number in the project of export and production sets.)
- **Dts\_idx:** This folder contains the DT Search Index Files. These are needed to be able to search for full text data.
- **Email\_body:** This folder contains files that are the text of an email body.
- **Filtered:** This folder contains the files that are the text of the Native file extracted by the application at the time of Add Evidence.
- **OCR:** This folder contains the files that are the text of the Native/Image files loaded via Import DII.
- **JT:** This folder contains files that are used for communication between processing host and processing engine. This is internal EP communication.
- **Jobs:** This folder contains the jobs sent via the application (i.e. Import, Add Evidence, Cluster Analysis, etc.) There are multiple Job folders:

- **AA:** This folder contains the Additional Analysis Jobs which consist of Jobs from Import, Imaging, Transcript Uploads, Clustering, etc.  
This folder also contains subfolders for the respective jobs performed by the Additional Analysis jobs. These folders contain compressed job information log files that are used for troubleshooting. The user should not need to access these log files.
- **AE:** This folder contains the jobs processed through Add Evidence.  
This folder also contains subfolders for the respective Add Evidence jobs. These folders contain compressed job information log files that are used for troubleshooting. The user should not need to access these log files.
- **MI:** This folder contains files for Index Manager jobs. These are run anytime you run another job to help update the database.  
This folder also contains subfolders for the respective jobs performed by the Index Manager jobs. These folders contain compressed job information log files that are used for troubleshooting. The user should not need to access these log files.
- **EvidenceHistory.log:** This folder contains a log file of Add Evidence, Additional Analysis, and Indexing Jobs. A user should not need to access these log files.

## *Opening Project Files*

To open any of the DAT files, you'll need to know the original extension of the files. For example, if the file is in the Tiff Folder, you know that it was originally a TIFF file. So if you change the extension from DAT to TIFF, you can open the file and it'll open as a TIFF File.

The files in the Native Folder are a little more complicated. You will need to match up the ObjectID to the one shown in the Project Review and determine what kind of native file it is and then change it to that extension accordingly. So that you do not alter the original file, it is best that you make a copy of the data files and then change the extension accordingly.

## *Files in the Project Folder*

In the main Project Folder, there are many files that are not in folders. Some of the loose files that you may encounter include:

- **EvidenceHistory.log:** This is a log file of Add Evidence Jobs, Imaging Jobs, Production Sets, and Clustering Jobs.

## Chapter 29

# Using Language Identification

---

## Language Identification

When selecting Evidence Processing, you can identify documents based on the language they were created in.

See [Default Evidence Processing Options](#) on page 84.

With Language Identification, you can identify and isolate documents that have been created in a specific language. Because Language Identification extends the processing time, only select the Language Identification needed for your documents. There are three levels of language identification to choose from:

### None

The system will perform no language identification. All documents are assumed to be written in English. This is the faster processing option.

### Basic

The system will perform language identification for the following languages:

- Arabic
- Chinese
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

If the language to identify is one of the ten basic languages (except for English), select Basic when choosing Language Identification. The Extended option also identifies the basic ten languages, but the processing time is significantly greater.



## Extended

The system will perform language identification for 67 different languages. This is the slowest processing option. The following languages can be identified:

- 
- |              |              |              |                   |
|--------------|--------------|--------------|-------------------|
| • Afrikaans  | • Esperanto  | • Latin      | • Scottish Gaelic |
| • Albanian   | • Estonian   | • Latvian    | • Serbian         |
| • Amharic    | • Finnish    | • Lithuanian | • Slovak          |
| • Arabic     | • French     | • Malay      | • Slovenian       |
| • Armenian   | • Georgian   | • Manx       | • Spanish         |
| • Basque     | • German     | • Marathi    | • Swahili         |
| • Belarusian | • Greek      | • Nepali     | • Swedish         |
| • Bosnian    | • Hawaiian   | • Norwegian  | • Tagalong        |
| • Breton     | • Hebrew     | • Persian    | • Tamil           |
| • Bulgarian  | • Hindi      | • Polish     | • Thai            |
| • Catalan    | • Hungarian  | • Portuguese | • Turkish         |
| • Chinese    | • Icelandic  | • Quechua    | • Ukrainian       |
| • Croatian   | • Indonesian | • Romanian   | • Vietnamese      |
| • Czech      | • Irish      | • Rumantsch  | • Welsh           |
| • Danish     | • Italian    | • Russian    | • Yiddish         |
| • Dutch      | • Japanese   | • Sanskrit   | • West Frisian    |
| • English    | • Korean     | • Scots      |                   |
-

## Part 5

# Using Lit Holds

This part describes how to use Litigation Holds and includes the following:

- [Using Litigation Holds](#) (page 339)

# Chapter 30

## Using Litigation Holds

---

### About Litigation Holds

AccessData's Litigation Hold (lit hold) feature is a notification management system that efficiently handles all aspects and stages of the litigation hold process within your enterprise. The lit hold features offers email notification templates and interview question templates, reports, histories, reminders, acceptance records, interview response records, and centralizes the relevant data in one location.

You can use lit hold if you have an eDiscovery license or if you have purchased a special Lit Hold licence for Summation.

There are three locations in the application where you can create, approve, and manage lit holds:

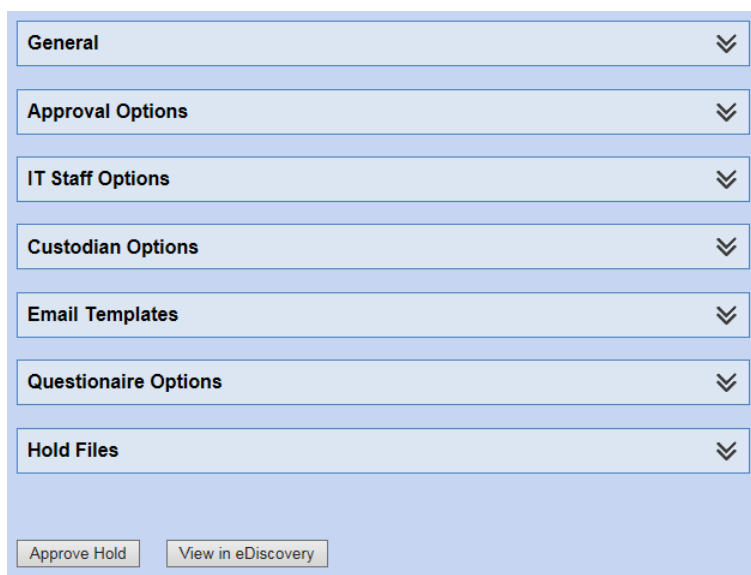
- The application *Lit Holds* tab



- The *Lit Hold* tab on the *Home* project page



- Dedicated HTML pages for different lit hold roles to view and approve holds



## About Lit Hold Roles

Several people can be involved in a lit hold. The following table describes the roles of people that can be involved.

### Lit Hold Roles

Role	Description
Lit hold manager / creator	A person with designated permissions that can create and manage lit holds.
Lit hold approver	One or more people with designated permissions that can approve a lit hold.
IT Staff	One or more people can be designated as IT Staff. These are individuals that you want to inform that data, for example emails and files stored on the network, must be preserved during the hold. These individuals are notified when a lit hold is created and must acknowledge that they have a role in the lit hold. They are also notified with reminders and when the lit hold is terminated.
Custodians	One or more people can be designated as a Custodian. These are people that are designated as owners of information that must be preserved during a lit hold. These people are notified when a lit hold is created and must acknowledge that they have a role in the lit hold. They may also be required to provide information about data that they may be aware of. They are also notified with reminders and when the lit hold is terminated.
Stage One Escalation Manager	A person who is notified if a custodian does not acknowledge a lit hold within a configured number of days. This can be the custodians manager as designated in Active Directory or another individual.
Stage Two Escalation Manager	A person who is notified when a custodian does not acknowledge a lit hold within a configured number of days. This may be the lit hold manager or another individual.

# Basic Workflow of Litigation Holds

This following is a basic workflow that illustrates how lit holds work.

---

**Note:** Many properties of a lit hold can be customized. The following represent a sample basic workflow.

---

1. A system administrator configures the application for lit holds.
2. A lit hold manager configures general lit hold settings.
3. A manager with permissions create a project and associates relevant custodians to the project.
4. A lit hold manager uses the Lit Hold wizard to create a lit hold.  
Many lit hold configuration options are available, but key options include the following:
  - The project to be associated with the lit hold
  - One or more people designated as a lit hold approver
  - One or more people designated as IT staff
  - One or more people designated as custodians
  - Email reminder schedules
  - Text of email notifications
  - Custodian interview questions
5. The designated lit hold approvers approve the lit hold. (They may receive email notifications if configured to do so.)
6. The designated IT staff receive notification emails with a link to a web page where they can review and acknowledge the lit hold.
7. The designated custodians receive notification emails with a link to a web page where they can review and acknowledge the lit hold. They also answer any specified interview questions.
8. If configured, and if a custodian does not acknowledge a lit hold, they can receive a stage one or stage two reminder to acknowledge the lit hold.
9. The lit hold manager can track the status of the hold.
10. During the lit hold, collection jobs can be run to collect relevant data.
11. If configured, IT staff and custodians receive reminder notification emails.
12. When appropriate, the lit hold manager can terminate the lit hold and IT staff and custodians receive termination emails.

# Process for Using Litigation Holds

You must perform the following steps to use lit holds:

## Process for using litigation holds

Step	Description
1.	<a href="#">Configuring the System for Litigation Holds</a> (page 342)
a.	<a href="#">Configuring IIS for Lit Holds</a> (page 342)
b.	<a href="#">Configuring Application Email Settings</a> (page 343)
c.	<a href="#">Configuring User Roles and Permissions for Lit Holds</a> (page 343)
d.	<a href="#">Configuring Projects and Custodians</a> (page 345)
2.	<a href="#">Configuring Litigation Hold Settings</a> (page 346)
a.	<a href="#">Configuring Lit Hold General Settings</a> (page 346)
b.	<a href="#">Configuring IT Staff</a> (page 347)
c.	(Optional) <a href="#">Configuring Application Email Settings</a> (page 343)
d.	(Optional) <a href="#">Configuring Lit Hold Interview Templates</a> (page 351)
3.	<a href="#">Creating a Litigation Hold</a> (page 357)
4.	<a href="#">Managing Litigation Holds</a> (page 365)

## Configuring the System for Litigation Holds

There are several elements of the application that must be configured in order to use lit holds.

### *Configuring IIS for Lit Holds*

Users with the proper roles can open links from notification emails to perform tasks, such as approve a hold. In order to open the link correctly, the LitHoldNotification authentication settings must be configured.

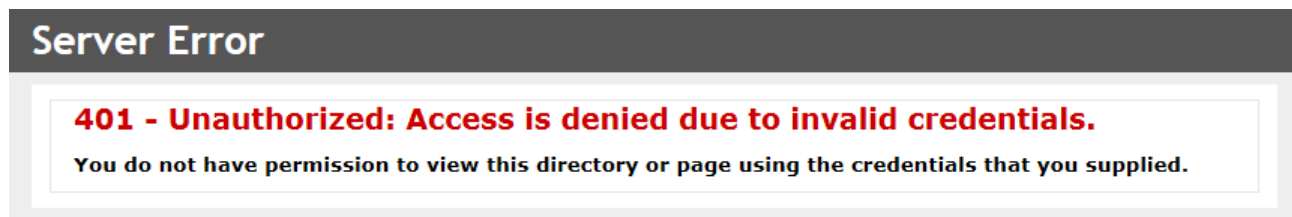
By default, the configuration is set to use Active Directory for the IT and Person acceptance landing pages when clicking links. However, you must change the setting from Active Directory and use Anonymous. This does not affect the general use of Active Directory and IWA in the rest of the application.

#### To configure anonymous authentication

1. On the Windows **Start** menu, in the **Search programs and files** field, enter `INetMgr`.
2. In the **Internet Information Services (IIS) Manager** application, in the left pane, expand the top-most server option.
3. Expand **Sites > Default Web Site**.
4. Click **LitHoldNotification**.

5. In the middle pane, in the **IIS** section, double-click **Authentication**.
6. In the **Authentication** pane, under the **Name** column, right-click **Windows Authentication**, and then click **Disable**.  
At this point, all options are disabled.
7. In the **Authentication** pane, under the **Name** column, right-click **Anonymous Authentication**, and then click **Enable**.
8. In the left pane, right-click **LitHoldNotification**, and then click **Explore**.  
Notice the Web.config file.
9. Open Web.config in Notepad.
10. Locate the following line in the file:  
`<authentication mode="Windows"></authentication>`
11. Change "Windows" to "None". The text is case-sensitive.
12. Locate the following line in the file:  
`<deny users="?"></deny>`
13. Change "?" to "0".
14. Save Web.config, and then exit Notepad.
15. Close the Explore window where Web.config is displayed.
16. Exit the Internet Information Services (IIS) Manager window.
17. Restart IIS.

If this is not configured, when an approver or custodian gets an email and tries to open the link, they will see the following:



## *Configuring Application Email Settings*

The main purpose of a lit hold is sending notification emails to related individuals. Before you can send any litigation hold notification emails, you must first make sure that you have configured **Email Notification Server**.

See [Configuring the Email Notification Server](#) on page 81.

## *Configuring User Roles and Permissions for Lit Holds*

You must have system users that have permissions to create and manage lit holds.

For example, you must first have a user that has the permission to create lit holds. Secondly you must have a user that has the permission to approve lit holds. These two roles may be performed by the same user or different users.

During the litigation hold creation process approvers are selected from the **User List** page. Only the users with Administrators, Project Manager, Project Administrator, LitHold Managers, Approve Lit Holds rights in your program database are loaded into the **Approval** page of the **Hold Creation Wizard**.

See [Configuring and Managing System Users, User Groups, and Roles](#) on page 46.

When configuring users to create and manage lit holds, you can configure two types of lit hold permissions:

- Global
- Project-specific

## Global Lit Hold Roles and Permissions

You can use admin roles and global permissions. User with these permissions have global rights that are not project-specific.

See [About Admin Roles and Permissions](#) on page 48.

You can use the following global roles and permissions

- *Application administrator* - A user with the application administrator role can configure lit hold and perform all lit hold tasks for all projects.
- *LitHold Manager* - You can create a custom admin role and assign the Lit Hold Manager permission. A user with the LitHold Manager permission can configure lit hold and perform all lit hold tasks for all projects.

However, by itself, this permission neither lets the user see projects on the Home page nor access the Lit Hold tab for a project. If you associate the user with this permission to a project, or give other project admin permissions, the user can then see the project and the Lit Hold tab for the project.

## Project-level Lit Hold Permissions

You can use project-specific permissions to grant lit hold permissions for specific projects. When you assign lit hold project-specific permissions, the user can only perform lit hold tasks for those projects.

See [Setting Project Permissions](#) on page 275.

Users project-specific permissions can view the lit hold features in the following ways:

- They can access the main *Lit Holds* tab, but will only see the lit holds that are associated with the projects they have permissions for.
- On the *Home* page, they can see the projects that they have permissions for and can access the project *Lit Hold* tab.



The following table displays the project level permissions and the tasks that they allow:

### Project-level permissions

Permissions:	Create holds	Approve holds	View holds	Edit holds	Delete holds	Activate/Deactivate	View hold data	Send notices	Hold reports	Custom Properties
<i>Project Admin</i>	x	x	x	x	x	x	x	x	x	x
<i>Create Litholds</i>	x		x	x			x		x	
<i>Approve Litholds</i>		x	x	x			x		x	
<i>View Litholds</i>			x	x			x		x	
<i>Delete Litholds</i>			x	x	x		x		x	
<i>Hold Manager (general tab)</i>	x		x	x			x	x	x	x
<i>Hold Manager (project-level tab)</i>	x		x	x	x	x	x	x	x	x

**Note:** When selecting a permission, the View Litholds permissions is also selected.

## Configuring Projects and Custodians

When you create a lit hold, you specify the projects and custodians that already exist in the application's database. If you have not already created these, you must do so before you create a lit hold.

- **Projects**  
 During the creation of a litigation hold, it is required that you associate it with an existing project. Before you create a lit hold, you must first create a project to associate it with.  
 See [Creating a Project](#) on page 245.  
 You must also associate custodians to the project.
- **Custodians**  
 During the creation of a litigation hold, you select custodians to be associated to the lit hold. However, you can only select from a list of custodians that have already been associated to the selected project. Before you create a lit hold, you must first configure custodians and associate them to the project.  
 See [Managing Custodians for a Project](#) on page 261.

# Configuring Litigation Hold Settings

## Configuring Lit Hold General Settings

Before you create litigation holds, you configure your Litigation Hold general settings. Prior to this, make sure you have configured your Email notification server.

See [Configuring the Email Notification Server](#) on page 81.

### To configure Litigation Hold general settings

1. In the application console, click **Lit Holds**.
2. On the **Lit Holds** page, click **LitHold Configuration**.
3. On the **LitHold Configuration** page, set the options that you want.  
See [Lit Hold Configuration Options](#) on page 346.
4. Click **Save**.
5. (Optional) In the *Send Test Email to:* field, enter a single email address of a recipient, and then click **Send Test Email**.

## Lit Hold Configuration Options

The following table describes the options that are available on the Lit Hold Configuration page.

See [Configuring Lit Hold General Settings](#) on page 346.

### Lit Hold Configuration Options

Option	Description
Email Sent From Address	Specifies the sender's email address. If desired, the IT department or a Network administrator can set up a default "From" address that people cannot reply to. See <a href="#">Configuring the Email Notification Server</a> on page 81.
Website Base Address	This is the base address of the server running Lit Hold. When approvers, custodians, and IT Staff get notification emails, it includes a link to an HTML page when they accept the Lit Hold. This base address is used for that HTML page. If this is not set correctly, the link to the HTML page will not work correctly. The base address includes the protocol and server name, but not the application or the page that is currently displayed. For example, <code>http://&lt;server_name_or_IP_address&gt;/</code>

## Lit Hold Configuration Options

Option	Description
Default Escalation Stage Two Email Address	<p>You can set two levels of escalation policies for person hold acceptance.</p> <p>Stage One: If a person doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.</p> <p><b>Note: Stage One escalation requires one of the following:</b></p> <ul style="list-style-type: none"><li>- Active Directory to be configured previously. In the <i>Manager</i> field of the Active Directory Account Screen, enter the manager that you want to be notified for the first escalation email.</li><li>- In the litigation hold wizard, you can manually specify a stage one address. See <a href="#">People Options</a> (page 359).</li></ul> <p>Stage Two: After a specified number of days, the next escalation is sent to the specified email address.</p> <p>This field is where you configure the default email address for Stage Two Escalations.</p> <p>See <a href="#">People Options</a> on page 359.</p> <p>See <a href="#">Email Notifications Options</a> on page 360.</p>
Hold Report temporary storage path	You can specify a dedicated path for reports data.
Person/IT Acceptance Message	Lets you enter any message or instruction that you want the person or IT staff to receive for their acceptance. The acceptance message displays at the bottom of the Person and IT Staff Hold Notification pages, just above the Accept button. This is the "By clicking accept you agree to the terms set forth." message.
Save	Saves the settings.
Send Test Email To	Specifies a single recipient email address that receives the test email.
Send Test Email	Sends a test email to the recipient specified above.

## Configuring IT Staff

### About Managing the IT Staff in a Litigation Hold

The IT Staff are those individuals in an organization that work with the organization's file aging. During a lit hold, they can receive notifications about lit holds.

IT Staff are first configured as a lit hold configuration option by the Lit Hold Manager or an administrator. Unlike people and approvers, there is no default database list that populates the IT Staff list. Instead, individuals must be entered manually.

IT staff are then associated to a Lit Hold in the creation wizard.

See [Configuring an IT Staff Member for Use in a Litigation Hold](#) on page 348.

See [Editing an IT Staff Member](#) on page 348.

See [Deleting an IT Staff Member](#) on page 349.

Individuals that you add to IT Staff become available for you to select from in the **Hold Creation Wizard**.


See [Creating a Litigation Hold](#) on page 357.

## Configuring an IT Staff Member for Use in a Litigation Hold

You must add individuals to IT Staff manually. Individuals that you add here become available for you to select from in the **Hold Creation Wizard**.

See [About Managing the IT Staff in a Litigation Hold](#) on page 347.

To add an IT staff member for use in a litigation hold

1. On the *Lit Holds* page, click **LitHold IT Staff**.
2. On the **Manage IT Staff** page, click .
3. In the **Add New IT Staff** dialog box, set the options that you want.  
See [IT Staff Options](#) on page 348.
4. Click **OK** to add the individual to the table on the **Manage IT Staff** page.

### IT Staff Options

The following table identifies the options that are available in the **Add New IT Staff** dialog box and the **Edit IT Staff** dialog box.

See [Configuring an IT Staff Member for Use in a Litigation Hold](#) on page 348.

See [Editing an IT Staff Member](#) on page 348.

#### IT Staff Options


Option	Description
First Name	First name of the individual.
Middle Initial	Middle initial of the individual.
Last Name	Last name of the individual.
Email	Email address of the individual. The address is where notifications are sent.
Title	Given job title of the individual.
Username	Computer username of the individual.
Domain	Network domain where the individual's computer resides.
Cancel	Cancels the addition of the individual.
OK	Adds the individual to the Manage IT Staff page.

### Editing an IT Staff Member

Any edits or changes that you make here are propagated to existing litigation holds of which the individual may be a part.

See [About Managing the IT Staff in a Litigation Hold](#) on page 347.

To edit an IT staff member


1. On the *Lit Holds* page, click **LitHold IT Staff**.
2. On the **Manage IT Staff** page, in the table, select a name whose information you want to edit.
3. Click .
4. In the **Edit IT Staff** dialog box, set the options that you want.  
See [IT Staff Options](#) on page 348.
5. Click **OK**.

## Deleting an IT Staff Member

Individuals that you delete are removed from the list of IT Staff that you can select from in the **Hold Creation Wizard** and they are removed from all existing litigation holds.

See [About Managing the IT Staff in a Litigation Hold](#) on page 347.

To delete an IT staff member

1. On the *Lit Holds* page, click **LitHold IT Staff**.
2. On the **Manage IT Staff** page, in the table, select a name that you want to delete.
3. Click .
4. Click **OK** to confirm the deletion.

## Configuring LitHold Email Templates

### About Managing Email Templates for Use in Litigation Holds

Lit holds send email notifications to people, IT Staff, and the Hold Approver informing them of the status and events of the lit hold. When creating a lit hold, you must specify the text of these email notifications.

To expedite this process, you can store and use text in email templates. When you create a lit hold, you can choose the template that you want to use.

You can use predefined email templates, or create your own custom email templates. You can edit or delete predefined email templates.

Templates are created and managed in the **LitHold Email Templates** section of the lit hold configuration options.

Before creating a lit hold you should prepare the email templates that you want to use.

---

**Note:** It is possible that messages sent by the litigation hold notification system are flagged as junk email by clients such as Microsoft Outlook. You may need to ensure that these messages are considered “trusted” and not automatically filtered to a junk email folder.

---

See [Template Type Options](#) on page 350.

See [Creating an Email Template for Use in Litigation Holds](#) on page 350.

## Template Type Options

The following table describes the types of email templates that are available for a litigation hold.

See [Creating an Email Template for Use in Litigation Holds](#) on page 350.

### Template Types

Template Type	Description
Approval	Sent to the litigation hold manager for their approval.
Stop Aging Acceptance	Sent to the IT Staff describing the parameters of the hold, and linking them to the Landing Page where they can view the Stop aging Letters and acknowledge receipt of the litigation hold.
Stop Aging Reminder	Reminds the IT Staff that they are still involved a litigation hold order.
Stop Aging Termination	Notifies the IT Staff that their participation in the litigation hold order is no longer necessary.
Hold Acceptance	Notifies the people of the hold, and links them to the Landing page where they can acknowledge receipt of the hold.
Hold Reminder	Reminds the people of the litigation hold.
Hold Termination	Notifies the people that the litigation hold has ended.
Hold Escalation Stage One	<p>There are two levels of escalation policies for person hold acceptance.</p> <p>Stage One: If a person doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.</p> <p><b>Note: Stage One escalation requires one of the following:</b></p> <ul style="list-style-type: none"><li>- Active Directory to be configured previously. In the <i>Manager</i> field of the Active Directory Account Screen, enter the manager that you want to be notified for the first escalation email.</li><li>- In the litigation hold wizard, you can manually specify a stage one address. See <a href="#">People Options</a> (page 359).</li></ul> <p>Stage Two: After a specified number of days, the next escalation is sent to the specified email address.</p> <p>This is the email template for a Stage One Escalation.</p>
Hold Escalation Stage Two	This is the email template for a Stage Two Escalation.
Person Questions Changed Reminder	<p>You may change the interview questions of a hold.</p> <p>This is the email template that will remind people of the change in interview questions and that they need to re-answer them.</p>

## Creating an Email Template for Use in Litigation Holds

You can create your own email templates from scratch, or you can use an existing email template as the basis for a new template.

You can add basic HTML formatting to the message body of an email.

See [About Managing Email Templates for Use in Litigation Holds](#) on page 349.

To create an email template for use in litigation holds

1. On the *Lit Holds* page, click **Configuration**.
2. Click **LitHold Email Templates**.
3. On the **Email Templates** page, in the **Template Type** drop-down list, select the type of template that you want to create.  
See [Template Type Options](#) on page 350.
4. In the **Templates** drop-down list, do one of the following:
  - Click the name of an existing template.
  - Click **Create New Template**.
5. In the **Subject** and **Message Body** fields, add or delete the text that you want to appear in the email for the given template type.  
When you save the template, the text that you entered in the **Subject** field is also used for the template name that appears in the **Templates** drop-down list.  
You can use the HTML text editor to format the text as you would like to have it displayed. You can also copy HTML text from another source.
6. (Optional) Click **Macros**. In the **Name** column, click a macro name to insert it into the message body where your cursor was last located.  
Based on the macro that you added to the message body, its associated information is inserted into the email at the time it is sent. The associated information comes from the various fields that were filled at the time you went through the **Hold Creation Wizard** to create the litigation hold.  
You can enter macros manually if the “code” is already known.

---

**Note:** The Lit Hold email notification email template allows you to manually enter in the [CompanyImage] macro. When the macro is not present in the template, the company image's placement defaults to the top center of the email.

---

7. (Optional) In the *Send Test Email to:* field, enter an email address of a single recipient, and then click **Send Test Email**.
8. Click **Save**.

## Configuring Lit Hold Interview Templates

### About Managing Interview Templates for Use in Litigation Holds

When you create a lit hold, you have the option of specifying interview questions. These interview questions are given to custodians when they accept a lit hold.

Interview questions are optional.

You can create interview templates with standard questions that you can re-use when you create a lit hold.

See [Creating an Interview Template for Use in Litigation Holds](#) on page 353.

See [Editing an Interview Template](#) on page 354.

See [Deleting an Interview Template](#) on page 355.

See [Creating a Litigation Hold](#) on page 357.

## About Interview Question and Answer Types

When you create an interview question template, you have flexibility in the kinds of questions, and potential answers, that are used.

You can also specify that certain interview questions are required to answer.

In an interview question template, you can configure the following different types of interview questions:

### LitHold Interview Template Questions Types

Questions Type	Description
Text Input Question	When you use this question type, a user answers the question by typing text.
Selection Question (Check Boxes)	When you use this question type, you also create a set of answers that the user can select from. The answers are provided as check boxes. The user can answer the question by selecting any of the check boxes that apply. You also have flexibility in the type of answers that you provide. <a href="#">LitHold Interview Template Answer Types</a> (page 352) Depending on the type of question that you ask, you may want to provide a selection for None.
Selection Question (Radio Buttons)	When you use this question type, you also create a set of answers that the user can choose from. The answers are provided as radio buttons. The user can answer the question by selecting only one radio button. Depending on the type of question that you ask, you may want to provide a selection for None.

You also have flexibility in the types of answers that accompany the check box and radio button questions. You can configure the following answer types.

### LitHold Interview Template Answer Types

Questions Type	Description
Add Answer	The administrator specifies the text that accompanies the check box or radio button and the user simply chooses which selection to make.
Add Input Answer	The check box or radio button does not contain any accompanying text and the user must input text after selecting it.
Add Input Answer with Text	The administrator specifies the text that accompanies the check box or radio button and the user can also input text after selecting it.

The following graphic is a sample of a template which has each of the three question types, and each of the three answer types.



## Sample of interview questions with the different types of questions and answers

The screenshot shows a window titled "Interview Questions" with three question types listed:

- This is a "Text Input Question" type of question** (checked "Is Required"): A single "User Input" text box.
- This is a "Selection Question (Check Boxes)" type of question** (unchecked "Is Required"): Three options, each with a checkbox and a "User Input" field:
  - Unchecked checkbox: "This is an 'Add Answer' (plain check box) type of answer"
  - Checked checkbox: "This is an 'Add Input Answer with Text' (check box with user input) type of answer"
- This is a "Selection Question (Radio Buttons)" type of question** (checked "Is Required"): Three options, each with a radio button and a "User Input" field:
  - Selected radio button: "This is an 'Add Answer' (plain radio button) type of answer"
  - Unselected radio button: "This is an 'Add Input Answer with Text' (radio button with user input) kind of answer"

On the right side of the window, there are green up and down arrows for reordering questions.

The first question simply provides a box for the user to input the answer.

The second question provides check boxes for answers. The first answer is a simple check box with text provided in the template. The second answer is a check box where the user inputs text after selecting it. The third answer is a check box with text, but also includes a box for a user to input text.

The third question provides radio buttons with the three possible answer types.

The difference between questions with check boxes and questions with radio buttons is that with check boxes, a user can select any and all check boxes. With radio buttons, the user can choose only one.


When creating a template, you can use the green up and down arrows on the right side to change the order the questions.

## Creating an Interview Template for Use in Litigation Holds

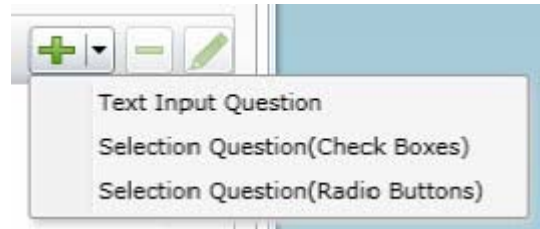
You can create any number of interview templates that contain the questions you want to ask people and others. You specify which templates you want to use when you go through the **Hold Creation Wizard**.

See [About Managing Interview Templates for Use in Litigation Holds](#) on page 351.

### To create an interview template for use in litigation holds

1. On the *Lit Holds* page, click on the **Configuration** tab
2. Click **LitHold Interview Templates**.
3. On the **Manage Interview Templates** page, click .
4. Enter a template name.  
The name of the template appears in the **Templates** drop-down list in the LitHold Wizard.
5. Enter a template description.

6. Add interview questions.

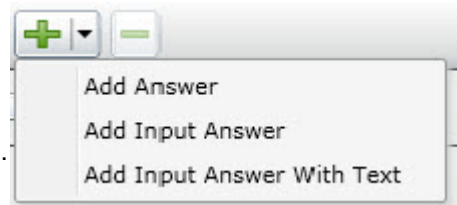


With the add button is a drop-down menu.

Select the type of question that you want to add.


See [About Interview Question and Answer Types](#) on page 352.

7. In the *Question* field, enter the text of the question.
8. (Optional) Select the *Answer Required* check box if you want to require an answer.
9. If you selected a Text Input Question (text input only), click **Add**.
10. If you selected a *Select Question* type with either check boxes or radio buttons, do the following:
  - 10a. click the add button with the drop-down button in the lower left corner of the dialog.



- 10b. Select an answer type.

See [About Interview Question and Answer Types](#) on page 352.

- 10c. Enter as many answers as desired.
- 10d. Click **Add**.
11. Add all of the questions that you want to be in this template.
12. (Optional) To edit a question or an answer, highlight a question and click  **Edit**.
13. (Optional) Highlight a question and use the green up and down arrows on the right side to change the order of the question.
14. Click **Save**.
15. (Optional) Create additional templates with other questions.


## Editing an Interview Template

You can edit an existing interview template to add or delete questions and answers to the template. You can also check or uncheck questions as required or not.

See [Creating an Interview Template for Use in Litigation Holds](#) on page 353.

See [About Managing Interview Templates for Use in Litigation Holds](#) on page 351.

### To edit an interview template

1. On the *Lit Holds* page, click on the **Configuration** tab
2. Click **LitHold Interview Templates**.
3. On the **Manage Interview Templates** page, highlight a template and click  **Edit**.

4. Make any desired changes.
5. Click **Save**.


## Deleting an Interview Template

You can delete an existing interview template so it is no longer available to choose in the **Hold Creation Wizard**.

See [Creating an Interview Template for Use in Litigation Holds](#) on page 353.

See [About Managing Interview Templates for Use in Litigation Holds](#) on page 351.

### To delete an interview template

1. On the *Lit Holds* page, click on the **Configuration** tab.
2. Click **LitHold Interview Templates**.
3. On the **Manage Interview Templates** page, highlight a template and click  **Delete**.
4. Click **OK** to confirm.

## Configuring Lit Hold Custom Properties

You can define and populate custom properties for lit holds. This can be useful in providing specific information about a given lit hold. For example, you may want to have information about a custodian, such as their date of hire, manager name, or employment status.

You can use the following types of property data:

- Text (For example, a manager's name)
- Date (For example, a hire date)
- Choices (A list of options to select, for example Full-time and Part-Time)



You can also specify the following:

- If a property is required
- Default values

When you create a new lit hold, the custom fields that you have defined are displayed in the Wizard. You can use default values or enter new values.

The custom properties and their values are displayed as columns in the lit hold list and in the Lit Hold Details report.

### To configure custom lit hold properties


1. On the Lit Hold page, click .
2. To add a new property, click .
3. Enter a name and description.
4. Specify whether or not this field is required.
5. Select the type of property.
6. For *Choices*, enter the optional choices separated by a Return.

7. (Optional) For text, enter default text.
8. (Optional) Edit a property
9. (Optional) Delete a property.

# Creating a Litigation Hold


You use the Litigation Hold Wizard to create and configure litigation holds.

## To create a litigation hold

1. On the *Lit Holds* page, click  **New Hold**.
2. For each page of the wizard, set the options that you want.

## Lit Holds Options

General page	See <a href="#">General Info Options</a> on page 357.
Approval page	See <a href="#">Approval Options</a> on page 358.
IT Staff page	See <a href="#">IT Staff Options</a> on page 359.
People page	See <a href="#">People Options</a> on page 359.
Email Notifications page	See <a href="#">Email Notifications Options</a> on page 360.
Documents page	See <a href="#">Documents Options</a> on page 362.
Interview Questions page	See <a href="#">Interview Questions Options</a> on page 363.
Summary page	See <a href="#">Summary</a> on page 364.

3. Click **Next**.
4. On the **Summary** page, Click **Save** to save the hold.
5. In the Success dialog box, click **Hold List**.
6. In the Hold List view, select the litigation hold that you just created.
7. If you are the designated approver, click  to approve the hold.

## General Info Options

The following table describes the options that you can set on the **General Info** page of the *Litigation Hold Wizard*.

See [Creating a Litigation Hold](#) on page 357.

### General Info Page Options

Option	Description
Name	(Required) Sets the name of the litigation hold.
Description	Describes the litigation hold.
Requested By	Sets the name of the person who requested the litigation hold. This name is included, by default, in the email notifications by using a macro.
Force Time Constraints	(Optional) Defines the time period associated with the hold. When the time period expires, the system sends hold termination emails, and the hold is closed.

## General Info Page Options

Option	Description
Start Date	(Required) Specifies the start date of the litigation hold. <b>Note:</b> You cannot edit field after a hold has been approved.
End Date	Specifies the end date of the litigation hold.
Custom Properties	If you configured <i>Custom Properties</i> , enter in the data. Fields highlighted in blue are required. See <a href="#">Configuring Lit Hold Custom Properties</a> on page 355.
Project	(Required) Specifies the project that is associated with the litigation hold.

## Approval Options

The following describes the options that you can set on the **Approval** page of the *Litigation Hold Wizard*.

No email notices to people (custodians) or IT Staff are sent until a hold is approved. When creating a hold, you select those who can approve a lit hold.

Approvers are selected from the user list on the *Approval* page. Only the users who have rights to approve holds are displayed on this page. To approve a hold, a user must have one of the following permissions:

- Global permissions using an *Admin Role*:
  - *Application Administrator*
  - *Create/Edit Project*
  - *LitHold Manager*
- Project-level permissions:
  - *Approve Litholds*

[Configuring User Roles and Permissions for Lit Holds](#) (page 343)

You can configure the following options:

### Approval Page Options

Option	Description
Any Approver	(Default) Any valid user that is listed in the table can approve the litigation hold. <b>IMPORTANT:</b> If you select this option, no Approval Notifications are sent, if you select to send them.
All Selected	You can select one or more Approvers and all of those users must approve the litigation hold.
Send Acceptance Emails to People and IT Staff on hold approval.	After the hold is approved, acceptance notification e-mails are sent to the IT staff and the people that are associated with the hold. The emails that are sent are configured in the Lit Hold email templates. See <a href="#">Configuring LitHold Email Templates</a> on page 349.

## Approval Page Options

Option	Description
Send Approval Notifications	Approval notification e-mails are sent to the approvers that are selected in the Approval table list. The emails that are sent are configured in the Lit Hold email templates. See <a href="#">Configuring LitHold Email Templates</a> on page 349. IMPORTANT: This option does not work if you selected <i>Any Approver</i> .
Send Approval Reminder every x days	After a specified number of days, the approval notification e-mail is resent to the approvers that are selected in the Approval table list.

## IT Staff Options

The following describes the options that you can set on the **IT Staff** page of the *Litigation Hold Wizard*.

You specify which IT Staff to send notification emails to.

See [Configuring IT Staff](#) on page 347.


The emails that are sent are configured in the Lit Hold email templates.

See [Configuring LitHold Email Templates](#) on page 349.

The litigation hold does not go into effect until all selected IT Staff have accepted it. When acceptance is complete, aging notifications continue.

You can configure the following options:

### IT Staff Page Options

Option	Description
 (Add New Staff Member)	Add IT Staff members to the litigation hold.
<enter filter text here>	If you have a large list of IT Staff, you can filter the list. See <a href="#">Configuring IT Staff</a> on page 347. Enter some text related to any property and click the search icon. To clear the filter, click the X icon.
Send Aging Acknowledgement every x Days	Re-sends the litigation hold Aging Acknowledgment email to the selected IT Staff members who have not acknowledged every number of specified days. This email continues to be sent until it is acknowledged.
Send Aging Reminder every x Days	Resends the litigation hold Aging Reminder email to the selected IT Staff members every number of specified days.
Disable Termination emails	When this option is selected, when a hold is terminated, IT Staff will not receive the termination notices.

## People Options

The following describes the options that you can set on the **People** page of the *Litigation Hold Wizard*.

You specify which people to send notification emails to.

See [Configuring Projects and Custodians](#) on page 345.

The emails that are sent are configured in the Lit Hold email templates.

See [Configuring LitHold Email Templates](#) on page 349.

Multiple people can be involved in a litigation hold. However, only people that are already associated with the selected project are displayed in the list.

You can also specify people within a hold to be excluded from the interview or escalation policies.

You can configure the following options:

### People Page Options

Option	Description
Display Person data sources on acceptance page.	Shows the sources of the person's data on the Acceptance page.
Send Hold Acknowledgement every x Days	Sends the litigation hold Acknowledgment email to all selected people that have not acknowledged, every number of specified days. This email continues to be sent until it is acknowledged.
Send Hold Reminder every x Days	Re-sends the litigation hold Reminder email to all selected people every number of specified days.
Escalations	<p>These settings allows you to set two levels of escalation policies for person hold acceptance.</p> <p>The emails that are sent are configured in the Lit Hold email templates. See <a href="#">Configuring LitHold Email Templates</a> on page 349.</p> <p>Stage One: If a person doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.</p> <p>Stage One escalations are sent to one of two possible email addresses:</p> <ul style="list-style-type: none"><li>• Their manager's email. This requires Active Directory to be configured previously. In the <i>Manager</i> field of the Active Directory Account Screen, enter the manager that you want to be notified for the first escalation email.</li><li>• <i>Override Escalation stage one email address</i>: When specified, this email address will be used instead of the manager's email address as specified in Active Directory.</li></ul> <p>Stage Two: After a specified number of days, the next escalation is sent to the specified email address.</p> <p>Repeat: Both of these escalations can be set to repeat if necessary. People within a hold can be excluded from the escalation policy if needed.</p>

## Email Notifications Options

The following table describes the options that you can set on the **Email Notifications** page of the *Litigation Hold Wizard*.

You configure the email notifications that will be sent from the lit hold.

You can do either of the following:

- Use content from a pre-configured template  
See [Configuring LitHold Email Templates](#) on page 349.
- Modify content from a pre-configured template
- Create new content



Some email notifications are required based on the options that you have chosen so far in the wizard.

The **Required** section of the **Email Notifications** page records the notifications that you have completed. The **Not Required** section lists the notifications that are not necessary to complete.

You can configure the following options:

### General Email Notification Page Options

Option	Description
Load from Template	Lets you select an email template for the associated tab. See <a href="#">About Managing Email Templates for Use in Litigation Holds</a> on page 349.
Load	Loads the selected email template into the <b>Edit</b> tab.
Preview	Opens the subject and message body of the email in a preview frame.
Edit	Lets you edit the subject and message body of the email. You can use the HTML text editor to format the text as you would like to have it displayed. You can also copy HTML text from another source.
View	Lets you view the email message with any macro fields populated with data. The macro field data comes from the information that you entered on the wizard pages prior to the <b>Email Notifications</b> page. For example, the macro field <code>[Hold Name]</code> retrieves the name that was entered on the <b>General</b> page of the <b>Hold Creation Wizard</b> . In the predefined email templates that come with the system, some emails have “XXXX” or “YYYY” in the message body. When a recipient receives the email, these fields appear as requested data that a recipient must fill in with the appropriate information.
Macros	Lets you add, edit, or delete macro fields in the message body of the email. You can edit the macro fields inserted into the message body by highlighting the text between the brackets and changing the text. The following macros are available for the email
	<b>Hold Name</b> - Lets you insert the name of the hold.
	<b>Hold Requestor</b> - Lets you insert the name of the person who requested the hold.
	<b>Time Frame Start</b> - Lets you insert the date when the hold starts.
	<b>Time Frame End</b> - Lets you insert the date when the hold ends.
	<b>Hold Person List</b> - Lets you insert a list of people for the hold. This list must be separated with commas.
	<b>Hold Description</b> - Lets you insert the description of the hold.
	<b>Project Name</b> - Lets you insert the name of the associated project.
	<b>View Hold Link</b> - Lets you insert a Hold Link hyperlink into the email. The Hold Link allows recipients of the email to view a list of active holds.
Send Test Email to	You can send a test email so that you can verify the email notification. Enter a single email address of a recipient, and then click <b>Send Test Email</b> .
Add CC:	You can add additional email address of people other than the specified people and IT staff that you would like to receive the email.

## Email Notification Page Options

Option	Description
Approval tab	Lets you edit the Approval email notification that is sent to users who are identified on the Approval list.
Person Acceptance tab	Lets you edit the Person Acceptance email that is sent to inform associated people of the litigation hold and have them accept the hold.
Person Reminder tab	Lets you edit the Person Reminder email that is sent to remind people of their involvement with the hold.
Person Termination tab	Lets you edit the Person Termination email that is sent to inform people that the hold is complete and closed.
IT Acceptance tab	Lets you edit the IT Staff Acceptance email that is sent to inform associated IT Staff members of the litigation hold and have them accept the hold.
IT Reminder tab	Lets you edit the IT Staff Reminder email that is sent to remind IT Staff members of their involvement with the hold.
IT Termination tab	Lets you edit the Person Termination email that is sent to inform people that the hold is complete and closed.
Escalation Stage One Escalation Stage Two	<p>You can set two levels of escalation policies for person hold acceptance.</p> <p>Stage One: If a person doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.</p> <p>There are two levels of escalation policies for person hold acceptance.</p> <p>Stage One: If a person doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.</p> <p><b>Note: Stage One escalation requires one of the following:</b></p> <ul style="list-style-type: none"> <li>- Active Directory to be configured previously. In the <i>Manager</i> field of the Active Directory Account Screen, enter the manager that you want to be notified for the first escalation email.</li> <li>- In the litigation hold wizard, you can manually specify a stage one address. See <a href="#">People Options</a> (page 359).</li> </ul> <p>Stage Two: After a specified number of days, the next escalation is sent to the specified email address.</p> <p>These tabs let you configure the Escalation email that is sent to inform managers of the escalation.</p>


## Documents Options

The following table describes the options that you can set on the **Documents** page of the *Litigation Hold Wizard*.

Documents are any supporting documents that you want to attach to the litigation hold notification emails. The document files are stored on the hard drive of the Hold Manager who creates the hold. Attached documents have read-only permissions.

See [Creating a Litigation Hold](#) on page 357.

### Documents Page Options

Option	Description
 (Add supporting files button)	Lets you add files in support of the litigation hold and have them categorized and distributed by <b>Notice - Person</b> or <b>Aging - IT Staff</b> . Documents that you add to a litigation hold are visible to the email recipient by way of a link back to the landing page.
Description field	Lets you double-click the description field of an added file and enter information you want about the file.
Delete button	Removes the file from the Supporting Documents table list.

### Interview Questions Options

The following table describes the options that you can set on the **Interview Questions** page of the *Litigation Hold Wizard*.


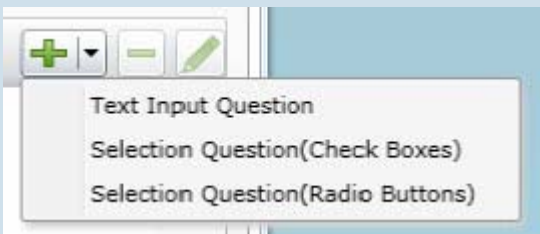

See [Creating a Litigation Hold](#) on page 357.

You can create interview questions here or you can load questions from your templates.



When you create interview questions, you have a variety of options on how to configure the questions and answers.

See [About Interview Question and Answer Types](#) on page 352.



### Interview Questions Page Options

Option	Description
 (Load question from template)	Lets you select a previously defined interview question template that has the question set you want. See <a href="#">About Managing Interview Templates for Use in Litigation Holds</a> on page 351.
Add a interview question	 <p>Specifies a question you want to ask recipients. You should enter and add one question at a time. For information on how to create and format questions and answers, see the following: <a href="#">About Interview Question and Answer Types</a> (page 352) <a href="#">Creating an Interview Template for Use in Litigation Holds</a> (page 353)</p>
 Delete button	Removes the highlighted question from the list.

## Interview Questions Page Options

Option	Description
 Edit button	Edits the highlighted question in the list.
	You can select a question and change its order in the list.
Allow Interview Review	Allows recipients to see the interview questions and their answers after they accept the litigation hold notification.
Allow Modification	If you select this option, people can change their answers after the initial interview.

## Summary

1. On the **Summary** page, do one of the following:
  - Click  in a upper-right corner of General or Approval sections to edit the information you want.
  - In the left pane of the wizard, click a wizard page name to navigate the wizard pages and edit any information you want. Click **Summary** in the left pane again to return to the **Summary** page and activate the **Save** button.
2. Click **Save** to save the hold.
3. In the Success dialog box, click **Hold List**.
4. In the Hold List view, select the litigation hold that you just created.
5. Click  (Approve Hold).

# Managing Litigation Holds

## Using the Lit Hold Page




The *Lit Hold* page is the default view when you click **Lit Holds** in the application console. You can use the *Lit Hold* page view to display all the litigation holds in the application and information about the hold.

There are two main elements of the Lit Hold page:





Lit Hold list	<p>You can view a list of lit holds in a grid. You can do the following to modify the contents of the grid:</p> <ul style="list-style-type: none"><li>• Control which columns of data are displayed in the grid.</li><li>• Sort on the columns</li><li>• If you have a large list, you can apply a filter to display only the items you want. See <a href="#">Managing Columns in Lists and Grids</a> on page 37.</li></ul> <p>You can also perform the following lit hold actions:</p> <ul style="list-style-type: none"><li>• Create a hold</li><li>• Delete a hold</li><li>• Activate a hold</li><li>• Deactivate a hold</li><li>• Resubmit a hold</li></ul>
Lit Hold information tabs	<p>Below the list of holds, you can use tabs to see the following information about the highlighted hold:</p> <ul style="list-style-type: none"><li>• Overall status</li><li>• Approvals</li><li>• List of Associated People</li><li>• List of the associate IT Staff</li><li>• Logs</li><li>• Email History</li><li>• Hold reports</li></ul>

The following table describes each item in the **Hold List** page.

### Hold List Elements

Links	Description
<b>Action</b>	Depending on the permissions of the logged-in-user and the status of the hold, you can do one of the following:
 <i>Approve</i>	If the logged-in-user is configured as an approver, and if a hold is waiting to be approved, you can click this to approve the hold.
 <i>Edit</i>	Lets you view and edit the selected hold
 <i>Delete</i>	Deletes the selected hold.
<b>Name</b>	The name of the lit hold.

## Hold List Elements

Links	Description
<b>Status</b>	<p>Displays the status of each hold in the list:</p> <ul style="list-style-type: none"> <li>• <i>Awaiting Approval</i> - The hold has been created but had not yet been approved.</li> <li>• <i>Waiting for Acknowledgements</i> - The hold has been approved, but has not yet been acknowledged by all IT Staff and Custodians.</li> <li>• <i>All Acknowledged</i> - The hold has been approved and acknowledged by all IT Staff and Custodians.</li> <li>• <i>Not Active</i> - On of the following three conditions exists: <ul style="list-style-type: none"> <li>■ The hold has reached its forced end date.</li> <li>■ The hold was Deactivated.</li> <li>■ The hold was terminated by sending Stop Notices.</li> </ul> </li> </ul> <p>You can sort on the status or use the filter to display holds by a certain status.</p>
<b>Creation Date</b>	The creation date of each lit hold
<b># IT</b>	The number of IT Staff associated to each lit hold.
<b>#People</b>	The number of People associated to each lit hold.
<b>Active</b>	Whether or not the list hold is active. (Information only)
 <b>New Hold</b>	Lets you create a lit hold using Opens the <b>Hold Creation Wizard</b> . See <a href="#">Creating a Litigation Hold</a> on page 357.
 <i>Delete Hold</i>	Lets you delete the selected holds. See <a href="#">Deleting a Litigation Hold</a> on page 368.
 <i>Activate or Deactivate hold</i>	Lets you activate or deactivate the selected hold. See <a href="#">Deactivating and Activating a Litigation Hold</a> on page 367.
 <b>Resubmit Hold</b>	Lets you resubmit a hold. This sets it back to its original state so that all actions must be performed again. See <a href="#">Resubmitting a Litigation Hold</a> on page 368.
<b>Overall Status</b>	Provides general status information about the highlighted hold. See <a href="#">Viewing the Overall Status of a Litigation Hold</a> on page 370.
<b>Approvals</b>	Displays the approval status and type.
<b>People</b>	Displays the names of the people that are associated with the selected hold. You can click <b>Preview Acceptance Page</b> at the bottom of the tab to open the <b>Person Hold Notification</b> page.
<b>IT Staff</b>	Displays the IT Staff members that are associated with the selected hold. You can click <b>Preview Acceptance Page</b> at the bottom of the tab to open the <b>IT Staff Hold Notification</b> page. See <a href="#">Configuring an IT Staff Member for Use in a Litigation Hold</a> on page 348.
<b>Log</b>	Displays filter options, a list of event types and related information, messages and date stamp for the selected Hold. See <a href="#">About the Hold Event Log for a Litigation Hold</a> on page 371.

## Hold List Elements

Links	Description
<b>Email Distribution History</b>	Displays filter options, a list of emails, and date stamp for the selected hold. See <a href="#">About the Email Distribution History of a Litigation Hold</a> on page 371.
<b>Hold Reports</b>	Details the people involved in the hold, and the approval/acceptance status of the approvers, people, and IT Staff. See <a href="#">You can view the history of emails that were sent, their type, date sent, by whom, recipient count, and subject. You can also use filtering to select a hold and type of email.</a> on page 371.

## Editing a Litigation Hold

You can open an existing litigation hold to either edit the settings, or to just view the settings.


See [Creating a Litigation Hold](#) on page 357.

What you can change in a litigation hold depends on when you edit it. If the hold has not been approved, then you can edit all properties.

After a hold has been approved, you cannot change general elements of hold such as the name, description, start date, project, the approver, the IT staff, the approval and acceptance emails. However, you can add people.

When you save the hold, it performs necessary actions. For example, suppose that you have a hold that has already been approved and acceptance emails have already been sent and all people have acknowledged the hold. Before editing the hold, the hold status is *All Acknowledged*. When you edit the hold and add a new person, the status is changed to *Waiting for Acknowledgements* and the acknowledgement email is sent to the new person.

### To edit a litigation hold

1. On the *Lit Holds* page, highlight a template and click  (edit).
2. Click **Next** to navigate the pages of the hold so you can review the settings, or make any necessary changes to existing settings.
3. When you have advanced to the **Summary** page, do one of the following:
  - Click **Cancel** if you did not make any changes to the litigation hold settings, or you want to cancel any changes you made to the hold.
  - Click **Save** to save the litigation hold settings that you changed.

## Deactivating and Activating a Litigation Hold

You can deactivate and then re-activate a litigation hold.

Deactivating a hold does not terminate or delete the hold; instead, the hold is “paused” or made not active, regardless of any pending actions. While an hold is deactivated, scheduled email notifications, such as reminders, are no longer sent. If you make the litigation hold inactive, its status is displayed as **Not Active** in the **Lit Hold** view. Also, deactivated holds do not appear in the list on the HTML pages for IT Staff and people.

It is important to note that when you deactivate a hold, it is not terminated and people and IT staff do not receive termination notices. The purpose of the deactivation is that you may want to temporarily deactivate a hold for administrative reasons without sending out termination notices.

You can re-activate any hold that is not active. A hold may have been made not active by the following actions:

- The termination date has occurred - See [General Info Options](#) on page 357.
- A hold was deactivated - See [Deactivating and Activating a Litigation Hold](#) on page 367.
- A hold was manually stopped (terminated) - See [Viewing the Overall Status of a Litigation Hold](#) on page 370.



When you activate a hold, it returns to the status it was in before it was made not active.

For example, if a hold had an *Awaiting Approval* status when it was deactivated, when re-activated, it will have an *Awaiting Approval* status again. However, notifications are not sent out automatically. For example, if a hold had an *Waiting for Acknowledgments* status when it was deactivated, when re-activated, it will not automatically send out Acknowledgment Notices. You must do so manually on the *Overall Status* tab > *Options*. See [Viewing the Overall Status of a Litigation Hold](#) on page 370.

If you make a litigation hold active, the hold's last known status is displayed in the **Lit Hold** view.

**Important:** When you deactivate or activate a hold, no email notification is sent notifying people of the change in status.

### To activate or deactivate a litigation hold


1. On the *Lit Holds* page, under the *Lit Hold* tab, select a litigation hold.
2. Click  **Activate** or  **Deactivate** either to activate or deactivate the litigation hold.
3. At the *Confirms Holds* dialog, click **Ok**.

## Deleting a Litigation Hold

You can delete an existing litigation hold, even if the hold is not active.

Notification emails are not sent out if a litigation hold is deleted.

### To delete a litigation hold

1. On the *Lit Holds* page, under the *Lit Hold* tab, select a litigation hold.
2. Click  **Delete**. You can find this icon by the litigation hold and also at the bottom of the task pane.
3. (Optional) Check **Keep Archive** to remove the holds from the user interface but keep an archive record of the litigation hold, such as IT staff, people, approver, histories, email templates, interview questions and answers. These are stored in database tables.
4. Click **Yes** in the *Confirm Deletion dialog* to confirm the deletion.

## Resubmitting a Litigation Hold


You can resubmit a hold. This creates a new copy of the hold and sets it back to its original state so that all actions must be performed again. You can use this to replace a hold that is already in place or clone an existing hold and leave the first one in tact.



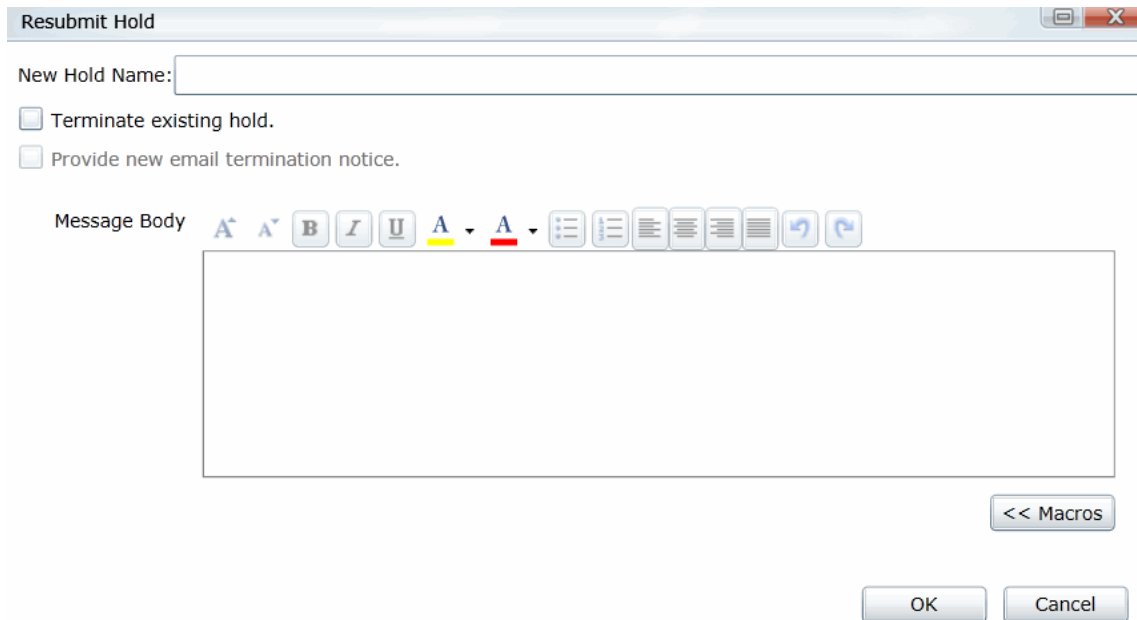
If you replace the hold, you are given the opportunity to send out an email explain that the previous hold has been replaced. A link is provided to acknowledge the new hold. This email functions as both a Termination Notice and an Acknowledgment Notice.

See [Creating a Litigation Hold](#) on page 357.

### To resubmit a litigation hold

1. On the *Lit Holds* page, under the *Lit Hold* tab, select a litigation hold.
2. Click  **Resubmit Hold** at the bottom of the task pane.
3. The *Resubmit Hold* dialog appears.

### Resubmit Hold Dialog



4. Enter the **New Hold Name** in the field provided.
5. You can check **Terminate existing hold** and/or **Provide new email termination notice**.
6. Add your information in the message body. You can format your text with basic word processing commands.
7. Under **Macros**, find macros to add to the body of your message. These macros include:
  - Hold Name
  - Hold Requestor
  - Time Frame Start
  - Time Frame End
  - Hold Person List
  - Project Name
  - View Hold Link
8. Click **Ok**.

## Viewing Information About Holds

You can view the overall status, approvals, IT Staff, and people of a selected litigation hold.

See [Using the Lit Hold Page](#) on page 365.

See [Viewing the Overall Status of a Litigation Hold](#) on page 370.

## Viewing the Overall Status of a Litigation Hold

You can view the overall status of a highlighted hold, including the following:

- Whether or not it is active
- The number of IT Staff and People
- The configured time frame
- Which actions have been completed and by how many  
For example, the hold may have four people associated with it. This will show how many of the people have acknowledged the hold.
- Links to action options.
  - **Send/Resend Notification** - If the hold has not been approved, you can send a reminder notice to the approver.
  - **Send Acknowledgment Notices** - This will send an acceptance reminder notice to any IT Staff or custodians who have not acknowledged the hold. For example, suppose only some of the people have acknowledged the hold. You can click the Send Acknowledgment Notices link. This will send another email to only those people who have not acknowledged the hold.
  - **Send Reminders Now** - This will send the following notices: *Hold Reminder* to custodians and *Stop Aging Reminder* to IT staff.
  - **Sent Stop Notices** - This will end (Deactivate) the hold and send the following notices: *Hold Termination* to custodians and *Stop Aging Termination* to IT staff. You cannot perform this action until the hold has been approved. You can Activate the hold at a later time. See [Deactivating and Activating a Litigation Hold](#) on page 367.

You can refresh the information shown on the tab to check the current status.

## About the Approvals Tab

The **Approvals** tab displays the hold's approval status and approval type. The option **Send/Resend All Approval Notices** becomes inactive after the hold is approved.

## About the People Tab

The **People** tab displays the list of people that are involved in the litigation hold; the Total, Accepted, and Pending counts of all the people. The sent, visited, and accepted status of each person is displayed in a grid. When you highlight a person in the grid, the associated **Detail View** shows the custodial options and responses to interview questions.

## About the IT Staff Tab

The **IT Staff** tab displays the total, accepted, and pending count of the IT Staff that are listed. The status of **Sent, Visited, Accepted, and End Notice** is also displayed. When you select an IT staff name, the associated **Detail View** area is displayed.

## About the Hold Event Log for a Litigation Hold

You can use **Hold Event Log** to review the events and messages of a selected litigation hold. You can also apply filter options to select the Hold and Event Type. The Log pane displays the type, date and time, initiator, and the message of each log item. Select a type item from the list to view the associated Message.

## About the Email Distribution History of a Litigation Hold

You can view the history of emails that were sent, their type, date sent, by whom, recipient count, and subject. You can also use filtering to select a hold and type of email.

## About Lit Hold Reports

You can use **Reports** in the **Holds** to generate various predefined reports with summary or detailed information about a particular litigation hold. Reports are generated in CSV format.

You can view the following types of reports for a given litigation hold.

### Available Litigation Hold Reports

Report	More information
Holds Summary	You can generate the <b>Holds Summary</b> report to display an overview of all litigation holds, all active holds, and all Inactive holds. These reports list their approval and acceptance status, associated project, and when it was created. Also included are number of people and IT Staff associated with a litigation hold, and the current stage of approval.
Hold Details	You can generate the <b>Hold Details</b> report to display a detailed overview of a litigation hold's approvers, people, IT Staff, any associated document files, and interview questions. Also included are the start and end dates of the hold, the priority of the hold, and a description, if one was entered in the <b>Hold Creation Wizard</b> .
Interview Responses	You can generate the <b>Interview Responses</b> report to display the answers to interview questions that are associated with a litigation hold.
Person Details	You can generate a detail report of the people's hold information.
Selected Project's Holds	You can generate a summary of all holds in the selected project.

## Searching Litigation Holds

You can perform a search for litigation holds using text that is in the following:

- Hold data
  - Text in the litigation hold name
  - Text in the litigation hold description
- Notification data
  - Text in the email notifications

After performing a search, any holds with the search results are displayed in a list.

If a search resulted in hits, the search is saved for re-use.

You can export your searches and search results.

### To perform a litigation hold search

1. On the *Lit Holds* page, click the **Search Lit Holds** tab.
2. Click **Search All Holds**.
3. Enter a Search Title for the saved search.
4. In the search terms field, enter the terms that you want to search for.  
You can enter multiple terms separated by a space. It will perform an OR search function.  
For example, the search terms *security approval* will return holds that contain either term.  
It will also search for words that contain your term.  
For example, a search term of *prov* will return prove, proved, approve, approved, approval, and so on.
5. You can choose the search to include *Active Holds*, *Inactive Holds*, or *Both*.
6. You can choose to search in *Hold Data*, *Notification Data*, or *Both*.
  - Hold data
    - Text in the litigation hold name
    - Text in the litigation hold description
  - Notification data
    - Text in the email notifications
7. Click **OK**.
8. A message is displayed showing the number of hits found.
9. If the search resulted in a hit, the search will be saved and displayed in the upper panel searches list.  
If the search resulted with 0 hits, the search will not be saved.
10. The litigation holds that are hits for the search are displayed in the lower panel results list.

### To view litigation hold search results

1. After a successful search, click a litigation hold in the search results panel.
2. On the right side, is an information panel. It may show a *Hold Info* tab, *Notifications* tab, or both depending on where the search terms were found.
3. You can click either tab and the search term is highlighted in red.
4. You can also view details about the hold.

### To delete a litigation hold search

1. Check the selection box for the hold or holds that you want to delete.
2. Click the *Delete* icon.

### To export searches or search results

1. For either list, click **Export**.
2. Click **OK**.

### To remove litigation holds from the search results list

1. In the lower pane, select the holds that you want to remove from the list.
2. Click **Mark as Non-Responsive**.

## Using Lit Hold Dashboard Widgets

You can use the Dashboard to view Lit Hold data.

See [Using the Dashboard](#) on page 497.

## Part 6

# Loading Data

This part describes how to load data and includes the following sections:

- [Importing Data](#) (page 375)
- [Using the Evidence Wizard](#) (page 376)
- [Importing Evidence](#) (page 385)
- [Using Cluster Analysis](#) (page 408)
- [Editing Evidence](#) (page 414)

# Chapter 31

## Introduction to Loading Data

---

### Importing Data

This document will help you import data into your project. You create projects in order to organize data. Data can be added to projects in the forms of native files, such as DOC, PDF, XLS, PPT, and PST files, or as evidence images, such as AD1, E01, and OFF files.

To manage evidence, administrators, and users with the Create/Edit Projects permission, can do the following:

- Add evidence items to a project
- View properties about evidence items in a project
- Edit properties about evidence items in a project
- Associate people to evidence items in a project

---

**Note:** You will normally want to have people created and selected before you process evidence.

---

See [About Associating People with Evidence](#) on page 378.

See the following chapters for more information:

#### To import data

1. Log in as a project manager.
2. Click the **Add Data** button next to the project in the *Project List* panel.
3. In the *Add Data* dialog, select one of the methods by which you want to import data. The following methods are available:
  - Evidence (wizard): See [Using the Evidence Wizard](#) on page 376.
  - Job (eDiscovery applications): See [About Jobs](#) on page 418.
  - Import: See [Importing Evidence](#) on page 385.
  - Cluster Analysis: See [Using Cluster Analysis](#) on page 408.

# Chapter 32

## Using the Evidence Wizard

---

### Using the Evidence Wizard

When you add evidence to a project, you can use the *Add Evidence Wizard* to specify the data that you want to add. You specify to add either parent folders or individual files.

---

**Note:** If you activated Cluster Analysis as a processing option when you created the project, cluster analysis will automatically run after processing data.

---

You select sets of data that are called “evidence items.” It is useful to organize data into evidence items because each evidence item can be associated with a unique person.

For example, you could have a parent folder with a set of subfolders.

```
\\10.10.3.39\EvidenceSource\  
\\10.10.3.39\EvidenceSource\John Smith  
\\10.10.3.39\EvidenceSource\Bobby Jones  
\\10.10.3.39\EvidenceSource\Samuel Johnson  
\\10.10.3.39\EvidenceSource\Edward Peterson  
\\10.10.3.39\EvidenceSource\Jeremy Lane
```

You could import the parent `\\10.10.3.39\EvidenceSource\` as one evidence item. If you associated a person to it, all files under the parent would have the same person.

On the other hand, you could have each subfolder be its own evidence item, and then you could associate a unique person to each item.

An evidence item can either be a folder or a single file. If the item is a folder, it can have other subfolders, but they would be included in the item.

When you use the Evidence Wizard to import evidence, you have options that will determine how the evidence is organized in evidence items.



When you add evidence, you select from the following types of files.

### Evidence File Types

File Type	Description
Evidence Images	You can add AD1, E01, or AFF evidence image files.
Native Files	You can add native files, such as PDF, JPG, DOC PPT, PST, XLSX, and so on.

When you add evidence, you also select one of the following import methods.

### Import Methods

Method	Description
CSV Import	<p>This method lets you create and import a CSV file that lists multiple paths of evidence and optionally automatically creates people and associates each evidence item with a person.</p> <p>Like the other methods, you specify whether the parent folder contains native files or image files.</p> <p>See <a href="#">Using the CSV Import Method for Importing Evidence</a> on page 378.</p> <p>This is similar to adding people by importing a file.</p> <p>See the Project Manager Guide for more information on adding people by importing a file.</p>
Immediate Children	<p>This method takes the immediate subfolders of the specified path and imports each of those subfolders' content as a unique evidence item. You can automatically create a person based on the child folder's name (if the child folder has a first and last name separated by a space) and have it associated with the data in the subfolder.</p> <p>See <a href="#">Using the Immediate Children Method for Importing</a> on page 380.</p> <p>Like the other methods, you specify if the parent folder contains native files or image files.</p>
Folder Import	<p>This method lets you select a parent folder and all data in that folder will be imported. You specify that the folder contains either native files (JPG, PPT) or image files (AD1, E01, AFF).</p> <p>A parent folder can have both subfolders and files.</p> <p>Using this method, each parent folder that you import is its own evidence item and can be associated with one person.</p> <p>For example, if a parent folder had several AD1 files, all data from each AD1 file can have one associated person. Likewise, if a parent folder has several native files, all of the contents of that parent folder can have one associated person.</p>
Individual File(s)	<p>This method lets you select individual files to import. You specify that these individual files are either native files (JPG, PPT) or image files (AD1, E01, AFF).</p> <p>Using this method, each individual file that you import is its own evidence item and can be associated with a person.</p> <p>For example, all data from an AD1 file can have an associated person. Likewise, each PDF, or JPG can have its own associated person.</p>

---

**Note:** The source network share permissions are defined by the administrator credentials.

---

## About Associating People with Evidence

When you add evidence items to a project, you can specify people, or custodians, that are associated with the evidence. These custodians are listed as People on the *Data Sources* tab.

In the *Add Evidence Wizard*, after specifying the evidence that you want to add, you can then associate that evidence to a person. You can select an existing person or create a new person.

**Important:** If you want to select an existing Person, that person must already be associated to the project. You can either do that for the project on the *Home* page > *People* tab, or you can do it on the *Data Sources* page > *People* tab.

You can create people in the following ways:

- On the *Data Sources* tab before creating a project.  
See the *Data Sources* chapter.
- When adding evidence to a project within the *Add Evidence Wizard*.  
See [Adding Evidence to a Project Using the Evidence Wizard](#) on page 382.
- On the *People* tab on the *Home* page for a project that has already been created.

## About Creating People when Adding Evidence Items

In the *Add Evidence Wizard*, you can create people as you add evidence. There are three ways you can create people while adding evidence to a project:

- Using a CSV Evidence Import.  
See [Using the CSV Import Method for Importing Evidence](#) on page 378.
- Importing immediate children.  
See [Using the Immediate Children Method for Importing](#) on page 380.
- Adding a person in the *Add Evidence Wizard*.  
You can select a person from the drop-down in the wizard or enter a new person name.  
See the Project Manager Guide for more information on creating people.

## Using the CSV Import Method for Importing Evidence

When specifying evidence to import in the *Add Evidence Wizard*, you can use one of two general options:

- Manually browse to all evidence folders and files.
- Specify folders, files, and people in a CSV file.  
There are several benefits of using a CSV file:
  - You can more easily and accurately plan for all of the evidence items to be included in a project by including all sources of evidence in a single file.
  - You can more easily and accurately make sure that you add all of the evidence items to be included in a project.
  - If you have multiple folders or files, it is quicker to enter all of the paths in the CSV file than to browse to each one in the wizard.
  - If you are going to specify people, you can specify the person for each evidence item. This will automatically add those people to the system rather than having to manually add each person.

When using a CSV, each path or file that you specify will be its own evidence item. The benefit of having multiple items is that each item can have its own associated person. This is in contrast with the Folder Import method, where only one person can be associated with all data under that folder.

Specifying people is not required. However, if you do not specify people, when the data is imported, no people are created or associated with evidence items. Person data will not be usable in Project Review.

See the Project Manager Guide for information on associating a person to an evidence item.

If you do specify people in the CSV file, you use the first column to specify the person's name and the second column for the path.

If you do not specify people, you will only use one column for paths. When you load the CSV file in the *Add Evidence Wizard*, you will specify that the first column does not contain people's names. That way, the wizard imports the first column as paths and not people.

If you do specify people, they can be in one of two formats:

- A single name or text string with no spaces  
For example, JSmith or John\_Smith
- First and last name separated by a space  
For example, John Smith or Bill Jones

In the CSV file, you can optionally have column headers. You will specify in the wizard whether it should use the first row as data or ignore the first row as headers.

## CSV Example 1

This example includes headers and people.

In the wizard, you select both **First row contains headers** and **First column contains people names** check boxes.

When the data is imported, the people are created and associated to the project and the appropriate evidence item.

### People, Paths

JSmith,\\10.10.3.39\EvidenceSource\JSmith

JSmith,\\10.10.3.39\EvidenceSource\Sales\Projections.xlsx

Bill Jones,\\10.10.3.39\EvidenceSource\BJones

Sarah Johnson,\\10.10.3.39\EvidenceSource\SJohnson

Evan\_Peterson,\\10.10.3.39\EvidenceSource\EPeterson

Evan\_Peterson,\\10.10.3.39\EvidenceSource\HR

Jill Lane,\\10.10.3.39\EvidenceSource\JLane

Jill Lane,\\10.10.3.39\EvidenceSource\Marketing

This will import any individual files that are specified as well as all of the files (and additional subfolders) under a listed subfolder.

You may normally use the same naming convention for people. This example shows different conventions simply as examples.

## CSV Example 2

This example does not include headers or people.

In the wizard, you clear both **First row contains headers** and **First column contains people names** check boxes.

When the data is imported, no people are created or associated with evidence items.

```
\\10.10.3.39\EvidenceSource\JSmith
\\10.10.3.39\EvidenceSource\Sales\Projections.xlsx
\\10.10.3.39\EvidenceSource\BJones
\\10.10.3.39\EvidenceSource\SJohnson
\\10.10.3.39\EvidenceSource\EPeterson
\\10.10.3.39\EvidenceSource\HR
\\10.10.3.39\EvidenceSource\JLane
\\10.10.3.39\EvidenceSource\Marketing
```

## *Using the Immediate Children Method for Importing*

If you have a parent folder that has children subfolders, when importing it through the *Add Evidence Wizard*, you can use one of three methods:

- Folder Import
- Immediate Children
- CSV Import

See [Using the CSV Import Method for Importing Evidence](#) on page 378.

When using the Immediate Children method, each child subfolder of the parent folder will be its own evidence item. The benefit of having multiple evidence items is that each item can have its own associated person. This is in contrast with the Folder Import method, where all data under that folder is a single evidence item with only one possible person associated with it.

Specifying people is not required. However, if you do not specify people, when the data is imported, no people are created or associated with evidence items. Person data will not be usable in Project Review.

See the Project Manager Guide for more information on associating a person to evidence.

When you select a parent folder in the *Add Evidence Wizard*, you select whether or not to specify people.

If you do specify people, the names of people are based on the name of the child folders.

Imported names of people can be imported in one of two formats:

- A single name or text string with no spaces  
For example, JSmith or John\_Smith

- First and last name separated by a space

For example, John Smith or Bill Jones

For example, suppose a parent folder had four subfolders, each containing data from a different user. Using the Immediate Children method, each subfolder would be imported as a unique evidence item and the subfolder name could be the associated person.

\Userdata\ (parent folder that is selected)

\Userdata\INewstead (unique evidence item with INewstead as a person)

\Userdata\KHetfield (unique evidence item with KHetfield as a person)

\Userdata\James Ulrich (unique evidence item with James Ulrich as a person)

\Userdata\Jill\_Hammett (unique evidence item with Jill\_Hammett as a person)

---

**Note:** In the Add Evidence Wizard, you can manually rename the people if needed.

---

The child folder may be a parent folder itself, but anything under it would be one evidence item.

This method is similar to the CSV Import method in that it automatically creates people and associates them to evidence items. The difference is that when using this method, everything is configured in the wizard and not in an external CSV file.

# Adding Evidence to a Project Using the Evidence Wizard

You can import evidence for projects for which you have permissions.

When you add evidence, it is processed so that it can be reviewed in Project Review.

Some data cannot be changed after it has been processed. Before adding and processing evidence, do the following:



- Configure the Processing Options the way you want them.  
See the Admin Guide for more information on default processing options.
- Plan whether or not you want to specify people.  
See the Project Manager Guide for more information on associating a person to evidence.
- Unless you are importing people as part of the evidence, you must have people already associated with the project.  
See the Project Manager Guide for more information on creating people.

---

**Note:** Deduplication can only occur with evidence brought into the application using evidence processing. Deduplication cannot be used on data that is imported.

---

## To import evidence for a project

1. In the project list, click  (add evidence) in the project that you want to add evidence to.
2. Select **Evidence**.
3. In the *Add Evidence Wizard*, select the *Evidence Data Type* and the *Import Method*.  
See [Using the Evidence Wizard](#) on page 376.
4. Click **Next**.
5. Select the evidence folder or files that you want to import.  
This screen will differ depending on the *Import Method* that you selected.
  - 5a. If you are using the *CSV Import* method, do the following:
    - If the CSV file uses the first row as headers rather than folder paths, select the **First row contains headers** check box, otherwise, clear it.
    - If the CSV file uses the first column to specify people, select the **First column contains people's names** check box, otherwise, clear it.
      - See [Using the CSV Import Method for Importing Evidence](#) on page 378.
      - Click **Browse**.
      - Browse to the CSV file and click **OK**.  
The CSV data is imported based on the check box settings.  
Confirm that the people and evidence paths are correct.  
You can edit any information in the list.  
If the wizard can't validate something in the CSV, it will highlight the item in red and place a red box around the problem value.  
If a new person will be created, it will be designated by .
  - 5b. If you are using the *Immediate Children* method, do the following:
    - If you want to automatically create people, select **Sub folders are people's names**, otherwise, clear it.
      - See [Using the Immediate Children Method for Importing](#) on page 380.
    - Click **Browse**.
    - Enter the IP address of the server where the evidence files are located and click **Go**.

For example, 10.10.2.29

- Browse to the parent folder and click **Select**.


Each child folder is listed as a unique evidence item.

If you selected to create people, they are listed as well.

Confirm that the people and evidence paths are correct.

You can edit any information in the list.

If the wizard can't validate something, it will highlight the item in red and place a red box around the problem value.

If a new person will be created, it will be designated by .

5c. If you are using the Folder Input or Individual Files method, do the following:

- Click **Browse**.
- Enter the IP address of the server where the evidence files are located and click **Go**.

For example, 10.10.2.29


- Expand the folders in the left pane to browse the server.
- In the right pane highlight the parent folder or file and click **Select**.

If you are selecting files, you can use Ctrl-click or Shift-click to select multiple files in one folder.

The folder or file is listed as a unique evidence item.

6. If you want to specify a person to be associated with this evidence, select one from the *Person Name* drop-down list or type in a new person name to be added.

See [About Associating People with Evidence](#) on page 378.

If you enter a new person that will be created, it will be designated by .

You can also edit a person's name if it was imported.

7. Specify a Timezone.

From the Timezone drop-down list, select a time zone.


See [Evidence Time Zone Setting](#) on page 384.

8. (Optional) Enter a *Description*.

This is used as a short description that is displayed with each item in the *Evidence* tab.

For example, "Imported from Filename.csv" or "Children of *path*".

This can be added or edited later in the *Evidence* tab.


9. (Optional) If you need to delete an evidence item, click the  for the item.

10. Click **Next**.

11. In the *Evidence to be Added and Processed* screen, you can view the evidence that you selected so far. From this screen, you can perform one of the following actions:

- *Add More*: Click this button to return to the *Add Evidence* screen.
- *Add Evidence and Process*: Click this button to add and process the evidence listed.

When you are done, you are returned to the project list. After a few moments, the job will start and the project status should change to *Processing*.

12. If you need to manually update the list or status, click  **Refresh**.

13. When the evidence import is completed, you can view the evidence items in the *Evidence* and *People* tabs.

See [Evidence Tab](#) on page 236.

## *Evidence Time Zone Setting*

Because of worldwide differences in the time zone implementation and Daylight Savings Time, you select a time zone when you add an evidence item to a project.

In a FAT volume, times are stored in a localized format according to the time zone information the operating system has at the time the entry is stored. For example, if the actual date is Jan 1, 2005, and the time is 1:00 p.m. on the East Coast, the time would be stored as 1:00 p.m. with no adjustment made for relevance to Greenwich Mean Time (GMT). Anytime this file time is displayed, it is not adjusted for time zone offset prior to being displayed.

If the same file is then stored on an NTFS volume, an adjustment is made to GMT according to the settings of the computer storing the file. For example, if the computer has a time zone setting of -5:00 from GMT, this file time is advanced 5 hours to 6:00 p.m. GMT and stored in this format. Anytime this file time is displayed, it is adjusted for time zone offset prior to being displayed.

For proper time analysis to occur, it is necessary to bring all times and their corresponding dates into a single format for comparison. When processing a FAT volume, you select a time zone and indicate whether or not Daylight Savings Time was being used. If the volume (such as removable media) does not contain time zone information, select a time zone based on other associated computers. If they do not exist, then select your local time zone settings.

With this information, the system creates the project database and converts all FAT times to GMT and stores them as such. Adjustments are made for each entry depending on historical use data and Daylight Savings Time. Every NTFS volume will have the times stored with no adjustment made.

With all times stored in a comparable manner, you need only set your local machine to the same time and date settings as the project evidence to correctly display all dates and times.



# Chapter 33

## Importing Evidence

---

### About Importing Evidence Using Import

As an Administrator or Project Manager with the Create/Edit Projects permissions, you can import evidence for a project.

You import evidence by using a load file, which allows you to import metadata and physical files, such as native, image, and/or text files that were obtained from another source, such as a scanning program or another processing program. You can import the following types of load files:

- Summation DII - A proprietary file type from Summation. See [Data Loading Requirements](#) on page 388.
- Generic - A delimited file type, such as a CSV file.
- Concordance/Relativity - A delimited DAT file type that has established guidelines as to what delimiter should be used in the fields. This file should have a corresponding LFP or OPT image file to import.

Transcripts and exhibits are uploaded from *Project Review* and not from the *Import* dialog. See the Project Manager Guide for more information on how to upload transcripts and exhibits.

### *About Mapping Field Values*

When importing you must specify which import file fields should be mapped to database fields. Mapping the fields will put the correct information about the document in the correct columns in the *Project Review*.

After clicking **Map Fields**, a process runs that checks the imported load file against existing project fields. Most of the import file fields will automatically be mapped for you. Any fields that could not be automatically mapped are flagged as needing to be mapped.

---

**Note:** If you need custom fields, you must create them in the *Custom Fields* tab on the *Home* page before you can map to those fields during the import. If the custom names are the same, they will be automatically mapped as well.

---

Any errors that have to be corrected before the file can be imported are reported at this time.

When importing a CSV or DAT load file that is missing the unique identifier used to map to the DocID file, an error message will be displayed.


Notes:

- If a record contains the same values for the DocID as the ParentID, an error is logged in the log file and the record is not imported. This allows you to correct the problem record and make sure all records in the family are included in the loadfile correctly.

- In review, the AttachmentCount value is displayed under the EmailDirectAttachCount column.
- The Importance value is not imported as a text string but is converted and stored in the database as an integer representing a value of either *Low*, *Normal*, *High*, or blank. These values are case sensitive and in the import file must be an exact match.
- The Sensitivity value is not imported as a text string but is converted and stored in the database as an integer representing a value of either *Confidential*, *Private*, *Personal*, or *Normal*. These values are case sensitive and in the import file must be an exact match.
- The Language value is not imported as a text string but is converted and stored in the database as an integer representing one of 67 languages.
- Body text that is mapped to the *Body* database field is imported as an email body stream and is viewable in the Natural viewer. When importing all file types, the import *Body* field is now automatically mapped to the *Body* database field.

## Importing Evidence into a Project

### To import evidence into a project

1. Log into the application as an Administrator or a user with Create/Edit Project rights.
2. In the *Project List* panel, click **Add Evidence**  next to the project.
3. Click **Import**.
4. In the *Import* dialog, select the file type (EDII, Concordance/Relativity, or Generic).
  - 4a. Enter the location of the file or **Browse** to the file's location.
  - 4b. (optional - Available only for Concordance/Relativity) Select the *Image Type* and enter the location of the file, or **Browse** to the file's location. You can choose from the following file options:
    - OPT - Concordance file type that contains preferences and option settings associated with the files.
    - LFP - Ipro file type that contains load images and related information.
5. Perform field mapping.
 

Most fields will be automatically mapped. If some fields need to be manually mapped, you will see an orange triangle.

  - 5a. Click **Map Fields** to map the fields from the load file to the appropriate fields.  
See [About Mapping Field Values](#) on page 385.
  - 5b. To skip any items that do not map, select **Skip Unmapped**.
  - 5c. To return the fields back to their original state, click **Reset**.

---

**Note:** Every time you click the *Map Fields* button, the fields are reset to their original state.

---

6. Select the *Import Destination*.
  - 6a. Choose from one of the following:
    - **Existing Document Group:** This option adds the documents to an existing document group. Select the group from the drop-down menu.  
See the Project Manager Guide (or section) for more information on managing document groups.
    - **Create New Document Group:** This option adds the documents to a new document group. Enter the name of the group in the field next to this radio button.

7. Select the *Import Options* for the file. These options will differ depending on whether you select DII, Concordance/Relativity, or Generic.
  - General Options:
    - **Enable Fast Import:** This will exclude database indexes while importing.
  - DII Options:
    - **Page Count Follows Doc ID:** Select this option if your DII file has an @T value that contains both a Doc ID and a page count.
    - **Import OCR/Full Text:** Select this option to import OCR or Full Text documents for each record.
    - **Import Native Documents/Images:** Select this option to import Native Documents and Images for each record.
    - **Process files to extract metadata:** Selecting this option will import only the metadata that exists on the load file and not process native files as you import them with a load file.
  - Concordance/Relativity, or Generic Options:
    - **First Row Contains Field Names:** Select this option if the file being imported contains a row header.
    - **Field, Quote, and Multi-Entry Separators:** From the pull-down menu, select the symbols for the different separators that the file being imported contains. Each separator value must match the imported file separators exactly or the field being imported for each record is not populated correctly.
    - **Return Placeholder:** From the pull-down menu, select the same value contained in the file being imported as a replacement value for carriage return and line feed characters. Each return placeholder value must match the imported file separators.
8. Configure the **Date Options**.
  - Select the date format from the **Date Format** drop-down menu.

This option allows you to configure what date format appears in the load file system, allowing the system to properly parse the date to store in the database. All dates are stored in the database in a yy-mm-dd hh:mm:ss format.
  - Select the *Load File Time Zone*.

Choose the time zone that the load file was created in so the date and time values can be converted to a normalized UTC value in the database.

See [Normalized Time Zones](#) on page 247.
9. Select the Record Handling Options.
  - **New Record:**
    - **Add:** Select to add new records.
    - **Skip:** Select to ignore new records.
  - **Existing Record:**
    - **Update:** Select to update duplicate records with the record being imported.
    - **Overwrite:** Select to overwrite any duplicate records with the record being imported.
    - **Skip:** Select to skip any duplicate records.
10. **Validation:** This option verifies that:
  - The path information within the load file is correct
  - The records contain the correct fields. For example, the system verifies that the delimiters and fields in a Generic or Concordance/Relativity file are correct.
  - You have all of the physical files (that is, Native, Image, and Text) that are listed in the load file.
11. (optional) **Drop DB Indexes.** Database indexes improve performance, but slow processing when inserting data. If this option is checked, all of the data reindexes every time more data is loaded. Only select this option if you want to load a large amount of data quickly before data is reviewed.
12. Click **Start**.

# Chapter 34

## Data Loading Requirements

---

This chapter describes the data loading requirements of eDiscovery and Summation and contains the following sections:

- [Document Groups](#) (page 388)
- [Email & eDocs](#) (page 391)
- [Coding](#) (page 393)
- [Related Documents](#) (page 396)
- [Transcripts and Exhibits](#) (page 397)
- [Work Product](#) (page 399)
- [Sample DII Files](#) (page 400)
- [DII Tokens](#) (page 404)

## Document Groups

---

**Note:** You can import and display Latin and non-Latin Unicode characters. While the application supports the display of fielded data in either Latin or non-Latin Unicode characters, the modification of fielded data is supported only in Latin Unicode characters.

---

---

**Note:** The display of non-Latin Unicode characters does not apply to transcript filenames, since transcript deponents are defined by project users, or work product filenames, which are not displayed in the application.

---

## *Images*

The following describes the required and recommended formats for images.

### Required

- A DII load file is required to load image documents. 0
- Group IV TIFFS: single or multi-page, black and white (or color), compressed images, no DPI minimum.
- Single page JPEGs for color images.

## Full-Text or OCR

The following describes the required and recommended formats for full-text or OCR.

### Required

- If submitting document level OCR, page breaks should be included between each page of text in the document text file.  
Failure to insert page breaks will result in a one page text file for a multi-page document. The ASCII character 12 (decimal) is used for the “Page Break” character. All instances of the character 12 as page breaks will be interpreted.
- Document level OCR or page level OCR.
- All OCR files should be in ANSI or Unicode text file format, with a \*.txt extension.
- A DII load file. Loading Control List (.LST) files are not supported.

### Recommended

- OCR text files should be stored in the same directories as image files.
- Page level OCR is recommended to ensure proper page breaks.

## DII Load File Format for Image/OCR

---

**Note:** When selecting the **Copy ESI** option, the DII and source files *must* reside in a location accessible by the IEP server; otherwise, import jobs will fail during the **Check File** process.

---

The following describes the required format for a DII load file to load images and OCR.

### Required

- A blank line after each document summary.
- **@T** to identify each document summary.
- **@T** should equal the beginning Bates number.
- If OCR is included, then use **@FULLTEXT** at the beginning of the DII file (**@FULLTEXT DOC** or **@FULLTEXT PAGE**).
- If **@FULLTEXT DOC** is included, OCR text files are assumed to be in the **Image** folder location with the same name as the first image (TIFF or JPG) file.
- If **@FULLTEXT PAGE** is included, OCR text files are assumed to be in the **Image** folder location with the same name as the image files (each page should have its own txt file).
- If **@O** token is used, **@FULLTEXT** token is not required.
- If Fulltext is located in another directory other than images, use **@FULLTEXTDIR** followed by the directory path.

- The page count identifier on the @T line can be interpreted ONLY if it is denoted with a space character.

For example:

```
@FULLTEXT PAGE
@T AAA0000001 2
@D @\IMAGES\01\
AAA0000001.TIF
AAA0000002.TIF
@T AAA0000003 1
@D @\IMAGES\02\
AAA0000003.TIF
```

Import controls the **Page Count Follows DocID** option. If this option is deselected, the page count identifier on the @T line would not be recognized.

## Recommended

- DII load file names should mirror that of the respective volume (for easy association and identification).
- @T values (that is, the BegBates) and EndBates should include no more than 50 characters. Non-alphabetical and non-numerical characters should be avoided.

# Email & eDocs

You can host email, email attachments, and eDocs (electronic documents in native format) for review and attorney coding, as well as associated full-text and metadata. It is also possible to include an imaged version (in TIFF format) of the file at loading. A DII load file is required in order to load e-mail and electronic documents.

---

**Note:** You can import and display of Latin and non-Latin Unicode characters. While the application supports the display of fielded data in either Latin or non-Latin Unicode characters, the modification of fielded data is supported only in Latin Unicode characters.

---

---

**Note:** The display of non-Latin Unicode characters does not apply to transcript filenames, since transcript deponents are defined by users, or work product filenames, which are not displayed.

---

## General Requirements

The following describes the required and recommended formats for DII files that are used to load email, email attachments, and eDocs.

A DII load file with a \*.dii file extension, using only the tokens, is listed in [DII Tokens](#) (page 404).

- **@T** to identify each email, email attachment, or eDoc record.
- **@T** is the first line for each summary.
- **@T** equals the unique **DocID** for each email, email attachment, or eDoc record. There should be only one **@T** per record.
- A blank line between document records.
- **@EATTACH** token is required for email attachments and **@EDOC** for eDocs. These tokens contain a relative path to the native file.
- **@MEDIA** is required for email data with a value of **eMail** or **Attachment**. For eDocs, the **@MEDIA** value must be **eDoc**.
- **@EATTACH** is required when **@MEDIA** has a value of **Attachment** and is not required when **@MEDIA** has a value of **eMail**.
- To maintain the parent/child relationship between an e-mail and its attachments (family relationships for eDocs), the **@PARENTID** and **@ATTACH** tokens are used.
- To include images along with the native file delivery, use the **@D @I** tokens at the end of the record.
- **@O** token is extended to support loading FullText into eDoc and eMails also.  
If record has both **@O** and **@EDOC/@EATTACH** tokens, FullText is loaded from the file specified by the **@O** token. If **@O** token does NOT exist for the record, FullText is extracted from the file specified by the **@EDOC/@EATTACH** token.
- **@AUTHOR** and **@ITEMTYPE** tokens are NOT supported.

## Recommended

- **@T** values (Begbates/DocID) should include no more than 50 characters. Non-alphabetical and non-numerical characters should be avoided.
- Specify parent-child relationship in the DII file based on the following rule:

- In the DII file, email attachments should immediately follow the parent record, that is:

@T ABC000123

@MEDIA eMail

@EMAIL-BODY

Please reply with a copy of the completed report.

Thanks for your input.

Beth

@EMAIL-END

@ATTACH ABC000124; ABC000125

@T ABC000124

@MEDIA Attachment

@EATTACH \Native\ABC000124.doc

@PARENTID ABC000123

@T ABC000125

@MEDIA Attachment

@EATTACH \Native\ABC000125.doc

@PARENTID ABC000123



# Coding

The following describes the required and recommended formats for coded data.

## Recommended

- Coded data should be submitted in a delimited text file, with a \*.txt extension.
- Use the following default delimiter characters:

Field Separator	
Multi-entry Separator	;
Return Placeholder	~
Quote Separator	^

Users can, however, specify any custom character in the Import user interface for any of the separators above.

- The standard comma and quote characters (',' ""') are accepted. When these characters are present within coded data, different characters must be used as separators.

For instance,

DOCID|SUMMARY|AUTHOR

^DOJ000001^|^Test "Summary1"^^Smith, John^

In the above file,

Field Separator |

Quote Separator ^

- Date field values should have any of the following formats. The date 16<sup>th</sup> August 2009 can be represented in the load file as:
  - 08/16/2009
  - 16/08/2009
  - 20090816

In addition, fuzzy dates are also supported. Currently only **DOCDATE** field supports fuzzy dates.

- If a day is fuzzy, then replace dd with 00.
- If a month is fuzzy, then replace mm with 00.
- If a year is fuzzy, replace yyyy with 0000.

<b>Format</b>	<b>Example</b>
mm/dd/yyyy	00/16/2009 (month fuzzy)
	08/00/2009 (day fuzzy)
	08/16/0000 (year fuzzy)
	00/16/0000 (month and year fuzzy)
	08/00/0000 (day and year fuzzy)
	00/00/2009 (month and day fuzzy)
	00/00/0000 (all fuzzy)
	08/16/2009 (no fuzzy)
yyyymmdd	00000816 (year fuzzy)
	20090016 (month fuzzy)
	20090800 (day fuzzy)
	00000016 (year and month fuzzy)
	00000800 (year and day fuzzy)
	20090000 (month and day fuzzy)
	00000000 (all fuzzy)
	20090816 (no fuzzy)
dd/mm/yyyy	00/08/2009 (day fuzzy)
	16/00/2009 (month fuzzy)
	16/08/0000 (year fuzzy)
	16/00/0000 (month and year fuzzy)
	00/08/0000 (day and year fuzzy)
	00/00/2009 (day and month fuzzy)
	00/00/0000 (all fuzzy)
	16/08/2009 – no fuzzy

- Time values should have any of the following formats. The time 1:27 PM can be represented in the load file as:
  - 1:27 PM
  - 01:27 PM
  - 1:27:00 PM
  - 01:27:00 PM
  - 13:27
  - 13:27:00

Time values for standard tokens @TIMESENT/@TIMERCVD/@TIMESAVED/TIMECREATED will not be loaded for a document unless accompanied by a corresponding DATE token DATESENT/ @DATERCVD/ @DATESAVED/@DATECREATED.

## Recommended

- You can use Field Mapping where the user can select different fields to be populated from the DII/CSV files. Fields would be automatically mapped during Import if the name of the database field matches the name of the field within the DII/CSV file.
- Field names within the header row will appear exactly as they appear within the delimited text file. Use consistent field naming for subsequent data deliveries.
- DocID/BegBates/EndBates values should include no more than 50 characters. Non-alphabetical and non-numerical characters should be avoided.
- Coding file names should mirror that of the respective volume (for easy association and identification). For example:

DOCID|TITLE|AUTHOR

```
^AAA-000001|^Report to XYZ Corp|^Jillson, Deborah;Ward, Simon;LaBelle, Paige^  
^AAA-000005|^Financial Statement|^Mubark, Byju;Aminov, Marina^  
^AAA-000008|^Memo|^McMahon, Brian^
```

## Related Documents

You can review related documents the **@ATTACHRANGE** token or the **@PARENTID** and **@ATTACH** tokens.

The related documents must be coded in sequential order by their DOCID. The sequence determines the first document and the last document in the related document set.

---

**Note:** Bates number of the first document in **@ATTACHRANGE** populates the ParentDoc column.

---

---

**Note:** **@ParentID** populates the ParentDoc field and **@ATTACH** populates the AttachIDs.

---

Either **@Attachrange** or **@ParentID** can be used at a time.

For example:

**@ATTACHRANGE** ABC001-ABC005

OR

**@PARENTID** ABC001

OR

**@ATTACH** ABC001;ABC002;ABC003;ABC004;ABC005

# Transcripts and Exhibits

---

**Note:** You can import and display of Latin and non-Latin Unicode characters. While the application supports the display of fielded data in either Latin or non-Latin Unicode characters, the modification of fielded data is supported only in Latin Unicode characters.

---

**Note:** The display of non-Latin Unicode characters does not apply to transcript filenames, since transcript deponents are defined by users, or work product filenames, which are not displayed.

---

From **Menu > Transcript > Manage**, you can upload new transcripts to any transcript collection to which they have access. All transcripts are displayed individually, and each has its own menu that controls various transcript management functions.

## *Transcripts*

The following describes the required and recommended formats for transcripts.

### Required

- ASCII or Unicode files (\*.txt) in AMICUS format.

### Recommended

- Transcript size is less than one megabyte.
- Page number specifications:
  - All transcript pages are numbered.
  - Page numbers are up against the left margin. The first digit of the page number should appear in Column 1. See the figure below.
  - Page numbers appear at the top of each page.
  - Page numbers contain no more than six digits, including zeros, if necessary. For example, Page 34 would be shown as **0034**, **00034**, or **000034**.
  - The first line of the transcript (Line 1 of the title page) contains the starting page number of that volume. For example, if the volume starts on Page 1, either **0001** or **00001** are correct. If the volume starts on Page 123, either **0123** or **00123** are correct.
  - Line numbers appear in Columns 2 and 3.
  - Text starts at least one space after the line number. It is recommended to start text in Column 7.
  - No lines are longer than 78 characters (including letters and spaces).
  - No page breaks, if possible. If page breaks are necessary, they should be on the line preceding the page number.
  - Consistent numbers of lines per page, if neither page breaks nor page number formats are used.
  - No headers or footers.
  - All transcript lines are numbered.

Column numbers:		1234567	
No page breaks,	22	Q	Okay. Will you produce that in 14 days,
headers or footers	23		please?
	24	A	Okay.
Zero-filled →	00028		
page numbers	1	Q	Off the top of your head, how many appraisals
start in Column 1	2		do you have pending?
	3	A	Nine, I believe.
Line numbers →	4	Q	Okay. How many properties do you have listed
start in Column 2	5		for sale?
	6	A	I think there's only one that's currently
Text starts	7		listed.
in Column 7	8	Q	Okay. Are you sharing any listings or
	9		appraisals with any other brokers or appraisers?

**Preferred Transcript Format**

*Exhibits*

The following describes the required format for Exhibits.

**Required**

- Exhibits that will be loaded must be in PDF format.
- If an Exhibit has multiple pages, all pages must be contained in one file instead of a file per page.

# Work Product

---

**Note:** You can import and display of Latin and non-Latin Unicode characters. While the application supports the display of fielded data in either Latin or non-Latin Unicode characters, the modification of fielded data is supported only in Latin Unicode characters.

---

**Note:** The display of non-Latin Unicode characters does not apply to transcript filenames, since transcript deponents are defined by users, or work product filenames, which are not displayed.

---

From **Menu > Work Product > Manage** you can upload, view, and review Work Product files. Work Product can be any type of file: text, word processing, PDF, or even MP3. (MP3 files are useful when you wish to send an audio transcript or message to the members of the group who have access to Work Product). The application does not maintain edits or keep version control information for the documents stored. Users working with Work Product documents must have the appropriate native application, such as Microsoft Word or Adobe Acrobat, to open them.

# Sample DII Files

---

**Note:** You can import and display of Latin and non-Latin Unicode characters. While the application supports the display of fielded data in either Latin or non-Latin Unicode characters, the modification of fielded data is supported only in Latin Unicode characters.

---

**Note:** The display of non-Latin Unicode characters does not apply to transcript filenames, since transcript deponents are defined by users, or work product filenames, which are not displayed.

---

**Note:** When selecting the **Copy ESI** option, the DII source files *must* reside in a location accessible by the IEP server; otherwise, import jobs will fail during the **Check File** process.

---

## *eDoc DII Load Files*

### Required DII Format (eDocs)

@T SSS00000007  
@MEDIA eDoc  
@EDOC \folder\SSS00000007.xls

@T SSS00000008  
@MEDIA eDoc  
@EDOC \Native\SSS00000008.doc

### Recommended DII format (eDocs)

@T ABC00000123  
@MEDIA eDoc  
@EDOC \Natives\ABC00000123.xls  
@APPLICATION Microsoft Excel  
@DATECREATED 05/25/2002  
@DATESAVED 06/05/2002  
@SOURCE Dee Vader



## *eMail DII Load Files*

### Required DII File Format for Parent Email (Emails)

@T ABC000123

@MEDIA eMail

@EMAIL-BODY

Please reply with a copy of the completed report.

Thanks for your input.

Beth

@EMAIL-END

@ATTACH ABC000124;ABC000125

### Required DII File Format for Related Email Attachment (Emails)

@T ABC000124

@MEDIA Attachment

@EATTACH \Native\ABC000124.doc

@PARENTID ABC000123

## Recommended DII Format for Parent Email (Emails)

@T ABC000123  
@MEDIA eMail  
@ATTACH ABC000124; ABC000125  
@EMAIL-BODY  
Please reply with a copy of the completed report.

Thanks for your input.

Beth

@EMAIL-END  
@FROM Abe Normal (anormal@ctsummation.com)  
@TO abcody@ctsummation.com; rob.hood@wolterskluwer.com  
@CC Willie Jo  
@BCC Jopp@ctsummation.com  
@SUBJECT Please reply  
@APPLICATION Microsoft Outlook  
@DATECREATED 06/16/2006  
@DATERCVD 06/16/2006  
@DATESENT 06/16/2006  
@FOLDERNAME \Normal\Sent Items  
@READ Y  
@SOURCE Abe Normal  
@TIMERCVD 1:36 PM  
@TIMESENT 1:35 PM

## Recommended DII Format for Related Email Attachments (Emails)

@T ABC000124  
@MEDIA Attachment  
@EATTACH \Native\ABC000124.doc  
@PARENTID ABC000123  
@APPLICATION Microsoft Word  
@DATECREATED 05/25/2005  
@DATESAVED 06/05/2005  
@SOURCE Abe Normal  
@AUTHOR Abe Normal  
@DOCTITLE Sales Report June 2005

## Recommended DII Format for Native Plus Images Deliveries (Email and eDocs)

(Append to the previous recommended DII formats for eDocs or email.)

@D @|\Images\  
ABC000124-001.tif

ABC000124-002.tif

# DII Tokens

Data for all tokens must be in a single line except the @OCR...@OCR-END, @EMAIL-BODY ... @EMAIL-END and @HEADER ... @HEADER-END.

TOKEN	FIELD POPULATED	DESCRIPTION OF USAGE
@T	DOCID & BEGBATES	This token is required for each DII record. This must be the first token listed for the document. This must be unique in the case. The @BEGBATES or @DOCID should not be used. @T ABC000123
@APPLICATION	Application	The application used to view the electronic document. For example: @APPLICATION Microsoft Word
@ATTACH	AttachDocs	IDs of attached documents. For example: @ATTACH ABC000124;ABC000125
@ATTACHRANGE	ParentDoc	The document number range of all attachments if more than one attachment exists. The beginning number in the range populates the PARENTDOC. For example: @ATTACHRANGE WGH000008 – WGH0000010
@ATTMSG	Media & Native file is copied into the file system using the path provided	The file name of the e-mail attachment (that is an e-mail message itself) including the relative or absolute path to the document. The relative path is evaluated using the path to the DII file as the root path. The native file is then loaded. The Media field is populated with the value eMail.
@BATESBEG	Begbates	Beginning Bates number, used with @BATESEND. For example: @BATESBEG SGD00001
@BATESEND	EndBates	Ending Bates number. For example: @BATESEND SGD00055
@BCC	EmailBCC	Anyone sent a blind copy on an e-mail message. For example: @BCC Nick Thomas
@C	Custom Field	Code used to load a custom field in the database. The syntax for the @C token is: @C <FIELDNAME> <DATA> The FIELDNAME value cannot contain spaces. For example, to fill in the DEPARTMENT field of the database with the value Accounting, the line would read: @C DEPARTMENT Accounting
@CC	EmailCC	Anyone copied on an e-mail message. For example: @CC John Ace

@D @I	Link to images	<p>Required token for each DII record that has an image associated with it. This designates the directory location of the image file(s). Note that only the “@D @I” sequence is allowed. The “@D @V” sequence is not recognized.</p> <p>The following 2 examples are equivalent:</p> <p>--Example 1  @D @I\Images\001\  ABC00123.tif  ABC00124.tif</p> <p>--Example 2  @D @I\Images\  001\ABC00123.tif  001\ABC00124.tif. Note the directory should be relative to the load file. If this token is in the record, it must be the last token in the record.</p> <p>Also UNC paths in the Image Directory field  (For example @D <a href="#">\\Server\PFranc\Images</a>) are recognized but no hard coded drive letters.</p>
@DATECREATED	CreationDateFT	The date that the file was created. For example: @DATECREATED 01/04/2003
@DATERCVD	DeliveryTimeFT	Date that the e-mail message was received.
@DATESAVED	ModificationDateFT	Date that the file was saved.
@DATESENT	SubmitTimeFT	Date that the e-mail message was sent.
@EATTACH	Native file is copied into the file system using the path provided	Relative path (from the load file location) of the native file to be loaded. Valid for Attachments.
@EDOC	Native file is copied into the file system using the path provided	Same as @EATTACH except for eDocs. For example @EDOC \Attachments\ABC000123.xls Valid for edocs only.
@EMAIL-BODY @EMAIL-END	Email body is copied into a file in the file system.	Body of an e-mail message. Must be a string of text contained between @EMAIL-BODY and @EMAIL-END. The @EMAIL-END token must be on its own line. For example: @EMAIL-BODY Bill, This looks excellent. Ted @EMAIL-END
@FILENAME	Filename of the native	Original Filename of the native file (Edoc/Email/Attachment) For example @FILENAME AnnualReport.xls
@FOLDERNAME	FolderNameID	The name of the folder that the e-mail message came from. For example: @FOLDERNAME \Inbox\Projects\ARProject
@FROM	EmailFrom	From field in an e-mail message. For example: @FROM Kelly Morris

@FULLTEXT	N/A (text processing directive)	Determines how OCR is associated with the document. This token should be placed at the top of the file, before any @T tokens. The OCR files must have the same names as the images (not including the extension), and they must be located in the same directory. Variations: @FULLTEXT DOC - One text file exists for each database record. The name of the file must be the same name as the first image file. @FULLTEXT PAGE - One text file exists for each page.
@FULLTEXTDIR	Link to Full text Directory	The @FULLTEXTDIR token is a partner to the @FULLTEXT token. @FULLTEXTDIR allows specifying a directory from which the full-text will be copied during the import. Therefore, the full-text files do not have to be located in the same directory as the images at the time of import. The @FULLTEXTDIR token gives you the flexibility to import the DII file and full-text files without requiring you to copy the full-text files to the network first. For example: @FULLTEXTDIR Vol001\Box001\ocrFiles The above example shows a relative path. The application searches for the full-text files in the same location as the DII file that is imported and follows any subdirectories listed after the @FULLTEXTDIR token. The @FULLTEXTDIR token applies to all subsequent records in the DII file until it is changed or turned off.
@HEADER @HEADER-END	EmailHeader	E-mail header content. The @HEADER-END token must be on its own line. For example: @HEADER <Header Text> @HEADER-END
@INTMSGID	InternetMessageID	Internet message ID. For example: @INTMSGID <00180c34fe5\$bf2d5\$050@SKEETER>
@MEDIA	Media	Indicates the type of document. This must be populated with one of the following values: {email, attachment, and eDoc} This value is REQUIRED. This value is used by the application to determine how to display the document. For example: @MEDIA eDoc
@MSGID	EntryID	E-mail message ID generated by Microsoft Outlook or Lotus Notes. For example: @MSGID 00E8324B3A0A800F4E954B8AB427196A1304012000
@MULTILINE	Any custom field with multiple lines	Allows carriage returns and multiple lines of text to populate a specified text field. Text must be between @MULTILINE and @MULTILINE-END. The @MULTILINE-END token must be on its own line. For example: @MULTILINE FIELDNAME Here is the first line. Here is the second line. Here is the third line. Here is the last line. @MULTILINE-END
@O	OCRTEXT / FULLTEXT is copied into a file in the file system	This token is used to load full-text documents. The text files can be located someplace other than the image location as specified by the @D line of the DII file. There can only be one text file for the record. The value following the @O should contain the relative path (from the load file location) of the .txt file. @O \Text\ABC000123.txt

@OCR @OCR-END	OCRTEXT is copied into a file in the file system	The @OCR and @OCR-END tokens offer the flexibility to include the full-text (including carriage returns) in the DII file. The @OCR-END token must appear on a separate line. For example: @OCR <full-text extracted from the electronic document, which can span multiple lines> @OCR-END
@PARENTID	ParentDoc	Parent document ID of an attachment. For example: @PARENTID ABC000123
@PSTFILE0	PSTFilePath and PSTStoreNameID	<p>The original PST File name and ID</p> <ol style="list-style-type: none"> <li>1) The name and/or location of the .PST file.</li> <li>2) The unique ID of the .PST file.</li> </ol> <p>The two values are separated by a comma. The unique ID can be any unique value that identifies the .PST file. For example: @PSTFILE EMAIL001\PFranc.pst, PFranc_14April_07</p> <p>The .PST file's unique ID (the second value) is populated into the PST ID field designated in eMail Defaults.</p> <p>The PST ID value specified by the @PSTFILE token is assigned to the record it appears in and will apply to all subsequent e-mail records. The value is applied until either the @PSTFILE token is turned off by setting the token to a blank value or the value changes. The @PSTFILE token can occur multiple times in a single DII file and assign a different value each time. This allows processing multiple .PST files and presenting the data for all .PST files in a single DII file.</p> <p>As a best practice, the @PSTFILE token should be placed above the @T token.</p>
@READ	IsUnread (stores 0 if Y and 1 if N)	Notes whether the e-mail message was read. For example: @READ Y
@RELATED	LinkedDocs	The document IDs of related documents. For example: @RELATED WGH000006
@SOURCE	Source	Custodian of the data. You can quickly filter documents by this field. @SOURCE Joe Custodian
@SUBJECT	Subject	The subject of an e-mail message. For example: @SUBJECT RE: Town Issues
@TIMECREATED	CreationDateFT	Time the file/e-mail/edoc was created
@TIMERCVD	DeliveryTimeFT	Time that the e-mail message was received.
@TIMESAVED	ModificationDateFT	Time that the file/e-mail/edoc was last saved
@TIMESENT	SubmitTimeFT	Time that the e-mail message was sent.
@TO	EmailTo	To field in an e-mail message. For example: @TO Conner Stevens
@UUID	UUID	Customer-specific and unique identifier for a record (not used internally by the application) For example: @UUID AE01R95

# Chapter 35

## Analyzing Document Content

---

### Using Cluster Analysis

#### *About Cluster Analysis*

You can use Cluster Analysis to group Email Threaded data and Near Duplicate data together for quicker review.

---

**Note:** If you activated Cluster Analysis as a processing option when you created the project, cluster analysis will automatically run after processing data and will not need to be run manually.


---

Cluster Analysis is performed on the following file types:

- Documents (including PDFs)
- Spreadsheets
- Presentations
- Emails

Cluster Analysis is also performed on text extracted from OCR if the OCR text comes from a PDF. Cluster Analysis cannot be performed on OCR text extracted from a graphic.

#### **To perform cluster analysis**

1. Load the email thread or near duplicate data using Evidence Processing or Import.
2. On the *Home* page, in the *Project List* panel, click the  *Add Evidence* button next to the project.
3. In the *Add Data* dialog, click **Cluster Analysis**.
4. Click **Start**.

You can view the similarity results in the *Similar Panel* in *Review*.

The data for the email thread appears in the *Conversation* tab in *Project Review*. The data for Near Duplicate appears in the *Related* tab in *Project Review*.

An entry for cluster analysis will appear in the *Work List*.

#### Words Excluded from Cluster Analysis Processing

Noise words, such as “if,” “and,” “or,” are excluded from Cluster Analysis processing. The following words are excluded in the processing:

a, able, about, across, after, ain't, all, almost, also, am, among, an, and, any, are, aren't, as, at, be, because, been, but, by, can, can't, cannot, could, could've, couldn't, dear, did, didn't, do, does, doesn't, don't, either, else,



ever, every, for, from, get, got, had, hadn't, has, hasn't, have, haven't, he, her, hers, him, his, how, however, i, if, in, into, is, isn't, it, it's, its, just, least, let, like, likely, may, me, might, most, must, my, neither, no, nor, not, of, off, often, on, only, or, other, our, own, rather, said, say, says, she, should, shouldn't, since, so, some, than, that, the, their, them, then, there, these, they, they're, this, tis, to, too, twas, us, wants, was, wasn't, we, we're, we've, were, weren't, what, when, where, which, while, who, whom, why, will, with, would, would've, wouldn't, yet, you, you'd, you'll, you're, you've, your

## *Filtering Documents by Cluster Topic*

Documents processed with Cluster Analysis can be filtered by the content of the documents in the evidence. The Cluster Topic filter is created in Review under the Document Contents filter from data processed with Cluster Analysis. Data included in the Cluster Topic is taken from the following types of documents: Word documents and other text documents, spreadsheets, emails, and presentations.

In order for the application to filter the data with the Cluster Topic filter, the following must occur:

- [Prerequisites for Cluster Topic](#) (page 409)
- [How Cluster Topic Works](#) (page 409)
- [Filtering with Cluster Topic](#) (page 410)
- [Considerations of Cluster Topic](#) (page 410)

## Prerequisites for Cluster Topic

Before Cluster Topic filter facets can be created, the data in the project must be processed by Cluster Analysis. The data can be processed automatically when Cluster Analysis is selected in the Processing options or you can process the data manually by performing **Cluster Analysis** in the *Add Evidence* dialog.

[Evidence Processing and Deduplication Options](#) (page 248)

## How Cluster Topic Works

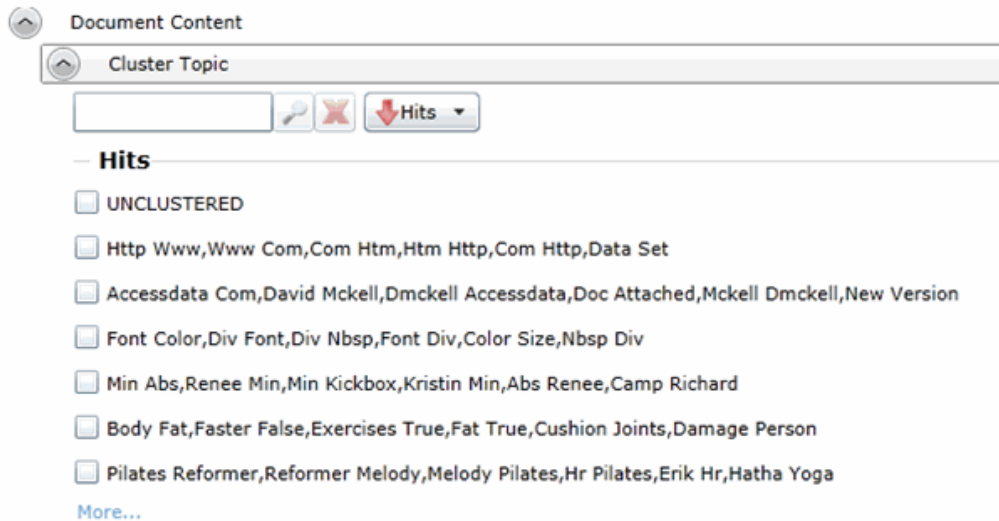
The application uses an algorithm to cluster the data. The algorithm accomplishes this by creating an initial set of cluster centers called pivots. The pivots are created by sampling documents that are dissimilar in content. For example, a pivot may be created by sampling one document that may contain information about children's books and sampling another document that may contain information about an oil drilling operation in the Arctic. Once this initial set of pivots is created, the algorithm examines the entire data set to locate documents that contain content that might match the pivot's perimeters. The algorithm continues to create pivots and clusters documents around the pivots. As more data is added to the project and processed, the algorithm uses the additional data to create more clusters.

Word frequency or occurrence count is used by the algorithm to determine the importance of content within the data set. Noise words that are excluded from Cluster Analysis processing are also not included in the Cluster Topic pivots or clusters.

## Filtering with Cluster Topic

Once data has been processed by Cluster Analysis and facets created under the Cluster Topic filter, you can filter the data by these facets.

### Cluster Topic Filters



The topics of the facets available are cluster terms created. Documents containing these terms are included in the cluster and are displayed when the filter is applied. Topics are comprised of two word phrases that occur in the documents. This is to make the topic more legible.

The UNCLUSTERED facet contains any documents that are not included under a Cluster Topic filter.

For more information, see *Filtering Data in Case Review* in the *Reviewer Guide*.

## Considerations of Cluster Topic

You need to aware the following considerations when examining the Cluster Topic filters:

- Not all data will be grouped into clusters at once. The application creates clusters in an incremental fashion in order to return results as quickly as possible. Since the application is continually creating clusters, the Cluster Topic facets are continually updated.
- Duplicate documents are clustered together as they match a specific cluster. However, if a project is particularly large, duplicate documents may not be included as part of any cluster. This is to avoid performance issues. You can examine any duplicate documents or any documents not included in a cluster by applying the UNCLUSTERED facet of the Cluster Topic filter.

# Using Entity Extraction

## About Entity Extraction

You can extract entity data from the content of files in your evidence and then view those entities.

You can extract the following types of entity data:

- Credit Card Numbers
- Email Addresses
- People
- Phone Numbers
- Social Security Numbers

The data that is extracted is from the body of documents, not the meta data.

For example, email addresses that are in the *To:* or *From:* fields in emails are already extracted as meta data and available for filtering. This option will extract email addresses that are contained in the body text of an email.

Using entity extraction is a two-step process:

1. Process the data with the *Entity Extraction* processing options enabled.  
You can select which types of data to extract.
2. View the extracted entities in *Review*.

The following tables provides details about the type of data that is identified and extracted:

Type	Examples
<b>Credit Card Numbers</b>	Numbers in the following formats will be extracted as credit card numbers:
16-digit numbers used by VISA, MasterCard, and Discover in the following formats.	For example, <ul style="list-style-type: none"><li>• 1234-5678-9012-3456 (segmented by dashes)</li><li>• 1234 5678 9012 3456 (segmented by spaces)</li></ul> Not: <ul style="list-style-type: none"><li>• 1234567890123456 (no segments)</li><li>• 12345678-90123456 (other segments)</li></ul>
15-digit numbers used by American Express in the following formats.	For example, <ul style="list-style-type: none"><li>• 1234-5678-9012-345 (segmented by dashes)</li><li>• 1234 5678 9012 345 (segmented by spaces)</li></ul>
	Notes: Other formats, such as 14-digit Diners Club numbers, will not be extracted as credit card numbers

Type	Examples
<b>Email Addresses</b>	Text in standard email format, such as jsmith@yahoo.com will be extracted.
	Note: Email addresses that are in the <i>To:</i> or <i>From:</i> fields in emails are already extracted as meta data and available for filtering. This option will extract email addresses that are contained in the body text of an email.
<b>People</b>	Text that is in the form of proper names will be extracted as people.
	Proper names in the content are compared against personal names from 1880 - 2013 U.S. census data in order to validate names.

Type	Examples
<b>Phone Numbers</b>	Numbers in the following formats will be extracted as phone numbers:
Standard 7-digit	For example: <ul style="list-style-type: none"> <li>• 123-4567</li> <li>• 123.4567</li> <li>• 123 4567</li> </ul> Not: 1234567 (not segmented)
Standard 10-digit	For example: <ul style="list-style-type: none"> <li>• (123)456-7890</li> <li>• (123)456 7890</li> <li>• (123) 456-7809</li> <li>• (123) 456.7809</li> <li>• +1 (123) 456.7809</li> <li>• 123 456 7809</li> </ul> Not 1234567890 (not segmented) <p>Note: A leading 1, for long-distance or 001 for international, is not included in the extraction, however, a +1 is.</p>

Type	Examples
International	<p>Some international formats are extracted, for example,</p> <ul style="list-style-type: none"> <li>• +12-34-567-8901</li> <li>• +12 34 567 8901</li> <li>• +12-34-5678-9012</li> <li>• +12 34 5678 9012</li> </ul> <p>Not 12345678901 (not segmented)</p> <p>Other international formats are not extracted, for example,</p> <ul style="list-style-type: none"> <li>• 123-45678</li> <li>• (10) 69445464</li> <li>• 07700 954 321</li> <li>• (0295) 416,72,16</li> </ul> <p>Notes: Be aware that you may get some false positives. For example, a credit number 5105-1051-051-5100 may also be extracted as the phone number 510-5100.</p>

Type	Examples
<b>Social Security Numbers</b>	<p>Numbers in the following formats will be extracted as Social Security Numbers:</p> <ul style="list-style-type: none"> <li>• 123-45-6789 (segmented by dashes)</li> <li>• 123 45 6789 (segmented by spaces)</li> </ul> <p>The following will not be extracted as Social Security Numbers:</p> <ul style="list-style-type: none"> <li>• 123456789 (not segmented)</li> <li>• 12345-6789 (other segments)</li> </ul>

## Enabling Entity Extraction

### To enable entity extracting processing options:

1. You enable *Entity Extraction* when creating a project and configuring processing options. See [Evidence Processing and Deduplication Options](#) on page 248.

## Viewing Entity Extraction Data

### To view extracted entity data

1. For the project, open *Review*.
2. In the *Facet* pane, expand the *Document Content* node.
3. Expand the *Document Content* category.
4. Expand a sub-category, such as *Credit Card Numbers* or *Phone Numbers*.
5. Apply one or more facets to show the files in the *Item List* that contain the extracted data.

# Chapter 36

## Editing Evidence

---

### Editing Evidence Items in the Evidence Tab

Users with Create/Edit project admin permissions can view and edit evidence for a project using the Evidence tab on the Home page.

#### To edit evidence in the Evidence tab

1. Log in as a user with *Create/Edit* project admin permissions.
2. Select a project from the *Project List* panel.
3. Click on the **Evidence** tab.
4. Select the evidence item you want to edit and click the **Edit** button.
5. In the *External Evidence Details* form, edit the desired information.

# Evidence Tab

Users with permissions can view information about the evidence that has been added to a project. To view the *Evidence* tab, users need one of the following permissions: Administrator, Create/Edit Project, or Manage Evidence.

## Evidence Tab


The screenshot displays the Evidence Tab interface. At the top, there is a toolbar with various icons. Below it is a 'Filter Options' section. The main area contains a table with the following data:

Path	Description	Evidence Type
\\cvg-dcstorage\cases\Agi\doc		Native
\\cvg-dcstorage\cases\Agi\doc		Native
\\cvg-dcstorage\cases\TestData_Load\DII\CVG7_002\CVG7_002_img01.tif		Native
\\cvg-dcstorage\cases\TestData_Load\Sally\Small Control Set\gmail.pst		Native


Below the table, there is a 'Page Size' dropdown set to 15, a 'Total: 4' indicator, and navigation buttons. A 'Refresh' icon is also present. To the right of the table is the 'External Evidence Details' panel, which includes fields for Path, Description, Evidence Type (Native), Associated Person Name, Created By (Administrator), and Created Date (12/8/2011 9:01:42 PM).

At the bottom of the interface is a 'Processing Status' section with 'General' and 'Progress' tabs, and fields for 'Error Messages' and 'Messages'.

## Elements of the Evidence Tab

Element	Description
Filter Options	Allows the user to filter the list.
Evidence Path List	Displays the paths of evidence in the project. Click the column headers to sort by the column.
Refresh 	Refreshes the Evidence Path List.

## Elements of the Evidence Tab (Continued)

Element	Description
Columns 	Click to adjust what columns display in the Evidence Path List.
External Evidence Details	Includes editable information about imported evidence. Information includes: <ul style="list-style-type: none"><li>• That path from which the evidence was imported</li><li>• A description of the project, if you entered one</li><li>• The evidence file type</li><li>• What people were associated with the evidence</li><li>• Who added the evidence</li><li>• When the evidence was added</li></ul>
Processing Status	Lists any messages that occurred during processing.



## Part 7

# Using Jobs

This part describes how to create and manage jobs.

Depending on the license that you own and the permissions that you have, you will see some or all of the following and includes the following sections:

- [About Jobs](#) (page 418)
- [Introduction to the eDiscovery Collection Job](#) (page 423)
- [Creating and Managing Jobs](#) (page 425)
- [Configuring Jobs for Third-Party Data Sources](#) (page 468)

# Chapter 37

## Introduction to Jobs

---


### About Jobs

You can create jobs to perform collections on a computer, network share, public data repository, email account, or all of the above within the enterprise. The collection can be set up with filters to find only the files that are needed for the project.

Jobs are responsible for the gathered, filtered, and archived information that comes from a variety of sources within an organization such as computers, laptops, personal digital assistants, and so forth.

Once you collect the data from the job, you can view the data in Project Review. You can filter the data and view the data by job or data source.

You use the Job Wizard to create Jobs. You can access the Job Wizard from one of two places in the application:

- From **Home > Project > Jobs** tab, click the  **Add** button on the *Info* pane. See [About the Jobs Tab](#) on page 419.
- From the *Project List* on the *Home* page, click the  **Add** button next to a particular case.

**Important:** When a job targets a network share, if a file on the share is locked from reading, the job will skip that file and enter an entry in the log.

See [Adding a Job](#) on page 426.

### About Job Categories

Depending on the license that you own, you can use the following categories of jobs:

#### Job Categories

Option	Description
Collection Job	You can use a collection job to collect data to process and review. You specify targets and can configure filters to collect specific files. See <a href="#">Introduction to the eDiscovery Collection Job</a> on page 423. chapter.
Report Only	Identifies files that can be collected. This lets you specify the same targets and filters as a collection job. This job type is used primarily to provide information about what you would collect if performing a collection.

## About Approving Jobs

After you configure a job, it must first be approved before it is executed. Job approval allows administrative oversight of the job by either supervisors or legal professionals prior to executing the job.

You can designate that a job be approved by one or more approvers.

You designate who has permissions to approve a job by using roles and permissions. In order to approve a job, a user must have one of the following:

- Application Administrator role
- Case Administrator role
- Project Manager Role
- Approve LitHold Rights
- LitHold Manager
- Custom role with the Approve Jobs permission

You can designate that a job be approved by any user with the approve role permission, or you can designate specific users with the approver permission. If you designate multiple specific users, all of them may approve the job.

See [Approving a Job](#) on page 452.

## About the Jobs Tab


Administrators, and users given permissions, use the *Jobs* tab to do the following:

- Create jobs
- View a list of existing jobs and their associations to people, computers, network shares, and groups.
- Manage jobs

If you are not an administrator, you will only see either the jobs that you created or projects to which you were granted permissions.

The *Jobs* tab refreshes every three minutes.

### To view the Jobs tab

1. Log in to the console.
2. In the application console, click **Home**.
3. Select a project.
4. Click the **Jobs** tab. 

## Jobs tab

The screenshot shows the Jobs tab interface. At the top, there is a toolbar with various icons. Below it is a 'Filter Options' section. The main area contains a table with columns: Name, Job Type, Targeted, Completed, Failed, Hits, Errors, Status, Start Date, End Date, and Proc. The table lists four jobs: ThreatScan, Collection, Volatile 2, and Volatile. The ThreatScan job is selected. To the right of the table is a 'Job Details' panel with fields for Name, Description, Responsive File Path, and Creation Date.

Name	Job Type	Targeted	Completed	Failed	Hits	Errors	Status	Start Date	End Date	Proc
ThreatScan	Threat Scan	1	1	0	1	0	Completed	9/2/2014 3:08:11 PM	9/2/2014 3:11:15 PM	Not
Collection	Collection	100	100	0	88799	0	Completed	9/2/2014 2:21:22 PM	9/2/2014 2:43:33 PM	Proc
Volatile 2	Volatile	100	100	0	NA	NA	Completed	9/2/2014 2:17:58 PM	9/2/2014 2:20:03 PM	Not
Volatile	Volatile	100	0	100	NA	NA	Failed	9/2/2014 2:00:33 PM	9/2/2014 2:04:21 PM	Not

Page Size: 15 Total: 4 (0)

Page 1 of 1

Job Details

Name: ThreatScan

Description:

Responsive File Path: \\10.10.0.81\JobData\ThreatScan

Creation Date: 9/2/2014 3:07:59 PM

## Elements of the Jobs Tab

Element	Description
Filter Options	Allows the user to filter jobs in the list. See <a href="#">Filtering Content in Lists and Grids</a> on page 39.
Jobs List	Displays the jobs associated with the project. Click the column headers to sort by the column. <b>Note: If a job doesn't collect and report on certain types of data, NA displays in the column. For example, for volatile jobs, the Hits and Errors columns display NA.</b>
Refresh 	Refreshes Jobs List. See <a href="#">Refreshing the Contents in List and Grids</a> on page 36.
Columns 	Adjusts what columns display in the Jobs List. See <a href="#">Sorting by Columns</a> on page 36.
Delete 	Deletes the selected job. The button is only active when a job is selected.
Resubmit 	Resubmits a job under a new name.
Cancel 	Stop the current job.
Manage Notifications 	Creates notifications for the checked job(s). See <a href="#">About Managing Notifications for a Job</a> on page 456.
Manage Templates 	Manages the templates for jobs. See <a href="#">Managing Job Templates and Filter Templates</a> on page 458.
Test Work Flow 	Tests the work flow of the job. <b>Note: This may take up to 30 seconds</b>
Export to CSV 	Imports the job list to a CSV file.

## Elements of the Jobs Tab (Continued)

Element	Description
Job Details Pane	Includes the ability to add jobs (plus sign button), edit jobs (pencil button), and delete jobs (minus sign button).
Job Target Results Tab	Displays all the targets for the selected job.
Status Tab	Displays the failure status of a job in detail. See <a href="#">Status Tab</a> on page 421.
People Target Tab	Displays the People targeted for the selected job.
Computers Target Tab	Displays the Computers targeted for the selected job.
Network Shares Target Tab	Displays the Network Shares targeted for the selected job.
Groups Target Tab	Displays the Groups targeted for the selected job.
Reports Tab	Displays statistics about jobs run. See <a href="#">Reports Tab</a> on page 422.

## Status Tab

The *Status* tab allows you to view the failure status of a job in detail. The errors that cause a failure status to display are invalid network shares for collection jobs against a network share and any errors reported to the application by Site Server.

See [Network Shares Tab](#) on page 440.

The *Status* tab can be viewed by any user, even a user without admin permissions. You can view if a job has failed on an individual target and why the job fails for a particular target. If the entire job fails, a red bar error displays the reason why the job has failed.

---

**Note:** For combination jobs, the *Status* tab displays the status of each job being processed.

---

### Job Status Tab



**Job Failure Reasons:**

Share requires authentication, no share credentials were provided :

Collection-Failed				No of Targets	Error Message
	<i>In-Progress</i>	<i>Completed</i>	<i>Failed</i>		
<b>Targets:</b>	0	0	1	1	Job Submission Error
<b>Start Date:</b>	6/4/2014 2:34:58 PM				
<b>End Date:</b>	6/4/2014 2:35:28 PM				

## Reports Tab

The *Reports* tab allows you to generate and download reports on a selected job. You can download the following reports:

- Full Error Report - This report shows a breakdown of failed targets and the errors associated to them.
- Job Report - This report displays details pertinent to the specific job. The report can be created on a completed job or a job that is in the middle of executing.

See [Using Job Reports](#) on page 454.

## Chapter 38

# Introduction to the eDiscovery Collection Job

---

## About Collection Jobs

You can use the *Jobs* tab to perform Collection Jobs on a computer, network share, public data repository, email account, or all of the above within the enterprise. Collection Jobs let you capture data for processing and review.

Jobs are the gathered, filtered, and archived information that comes from a variety of sources within an organization such as computers, lap tops, personal digital assistants, and so forth.

You use the Job Wizard to create Collection Jobs.

See [Adding a Job](#) on page 426.

## About Collections

Collections are the gathered, filtered, and archived information from a wide variety of sources. This allows a transfer of data from an organization to legal counsel. After collection, data is processed and reviewed for relevance. This collection process and the review of collected files is the essence of eDiscovery.

In the **Custom Selection** and **Other Data Sources** panes under the **Job Options** tab, you can select the data sources that you want to collect from.

## About Collection Job Sources

The following are the types of data sources that you can collect from:

- People. When you select a person to collect from, you can also choose to collect from the following data sources that a person is associated to:
  - Computers
  - Network Shares
  - Enterprise Vaults
  - Microsoft Exchange server
  - Cloud Mail server, such as Yahoo
  - Domino Server
  - GmailSee [Custodian Tab](#) on page 435.
- Computers. See [Computers Tab](#) on page 437.

- Network Shares. See [Network Shares Tab](#) on page 440.
- Documentum. See [Documentum Collections Options](#) on page 475.
- DocuShare. See [DocuShare Collection Options](#) on page 477.
- Enterprise Vault Server. See [Enterprise Vault Server Collection Options](#) on page 479.
- Exchange Public Folder. See [Exchange Public Folder Collection Options](#) on page 484.
- FileNet. See [Google Drive Collection Options](#) on page 485.
- Google Drive. See [Enterprise Vault Server Collection Options](#) on page 479.
- OpenText ECM. See [OpenText ECM Collection Options](#) on page 486.
- Sharepoint. See [SharePoint Collection Options](#) on page 487.
- Website. See [Website Collection Options](#) on page 490.
- Druva. See [Druva Collection Options](#) on page 491.
- Box. See [Box Collections Options](#) on page 471.

---

**Note:** If you collect from the data sources under the People option, data will only be collected from data sources that are associated to a person. If you want to collect data from a particular data source, both associated and unassociated to a person, select the data source by name and not by the People option.

---



# Chapter 39

## Creating and Managing Jobs

---

This chapter explains how to create, run, and manage jobs and includes the following topics:

- [Adding a Job](#) (page 426)
- [General Job Wizard Tabs](#) (page 428)
- [Approving a Job](#) (page 452)
- [Processing a Job](#) (page 453)
- [Using Job Reports](#) (page 454)
- [Using Job Notifications](#) (page 456)
- [Using Job Templates and Filter Templates](#) (page 458)
- [Additional Job Tasks](#) (page 462)
  - [Testing the Collection Workflow](#) (page 462)
  - [Stopping a Job](#) (page 462)
  - [Resubmitting a Job](#) (page 462)
  - [Editing a Job](#) (page 463)
  - [Deleting Jobs](#) (page 464)

For information about third-party data sources, see [Configuring Third-Party Data Repositories as Data Sources](#) (page 145).

# Adding a Job

You use the *Job Wizard* to create jobs for a project.




See [About Jobs](#) on page 418.

You can set up the job with filters to find only the files that are needed for the project in the Project Review.

See [Using Job Filters](#) on page 445.

## To add a job

1. Do one of the following:

- In the *Project List* panel, click the  next to the project and then click **Job**.
- On the *Home* tab, select a project, click  **Jobs**, then in the right side of the upper pane, click .

The Job Wizard opens.

2. In the *Job Wizard* dialog, in the *Job Options* screen, set the options that you want and click **Next**.  
Bold names in the user interface indicate required fields.

See [Job Options Tab](#) on page 428.

3. Click **Next**.

4. The next screens you see will depend on the Job Target Options that you selected on the first page. The following Job Types result in a screen specific to that type:

- Custodians: See [Custodian Tab](#) on page 435.
- Computers: See [Computers Tab](#) on page 437.
- Network Shares: See [Network Shares Tab](#) on page 440.
- Third-party Connectors. See [Configuring Jobs for Third-Party Data Sources](#) on page 468.
- Groups: See [Group Selection Tab](#) on page 433.
- IP Range See [IP Range Tab](#) on page 434.

5. Click **Next**.

6. In the Scheduling screen, set how you would like the job to be executed. You can execute the job manually, or schedule a time for the job to be executed.

See [Scheduling Tab](#) on page 441.

7. Click **Next**.

8. In the *Approvers* screen, set the options that you want and click **Next**.

See [Approvers Tab](#) on page 444.

## Job Wizard Summary

**Job Options**

<b>Name</b>	fdsads
<b>Description</b>	adfa
<b>Type</b>	Volatile
<b>Project</b>	jk-kff-testing
<b>Job Data Path</b>	\\10.10.32.20\Jobs\jk-kff-testing\fdsads
<b>Job Expiration</b>	Unfinished jobs expire after 30 day(s) 0 Hour(s)

**Group Selection**

<b>Groups Count</b>	0
<b>Computers Count</b>	0
<b>Network Shares Count</b>	0
<b>Persons Count</b>	0

**Volatile Options**

<b>Include Processes</b>	No
<b>Include Services</b>	No
<b>Include Drivers</b>	No
<b>Include Users</b>	No
<b>Include NICs</b>	No
<b>Include Network Sessions</b>	No
<b>Include Registry</b>	No
<b>Cerberus Stage One</b>	No
<b>Cerberus Stage Two</b>	No

**Scheduling**

<b>Job Execution</b>	Manual Job Execution
----------------------	----------------------

Back Next Save Cancel

9. On the *Job Summary* page, carefully review the settings that you have made to ensure that it includes and excludes the proper terms and documents.
10. Click **Save** to submit the job for approval.

# General Job Wizard Tabs

You can use the following general tabs to configure Jobs:

- [Job Options Tab](#) (page 428)
- [Group Selection Tab](#) (page 433)
- [IP Range Tab](#) (page 434)
- [Custodian Tab](#) (page 435)
- [Computers Tab](#) (page 437)
- [Network Shares Tab](#) (page 440)
- [Scheduling Tab](#) (page 441)
- [Approvers Tab](#) (page 444)

You can also specify filters to narrow down the files on targets.

See [Using Job Filters](#) on page 445.

## Job Options Tab

The following describes the options that are available in the *Job Options* tab of the *Job Wizard*.

### General Job Options

Option	Description
Job Type	Select the type of job: <ul style="list-style-type: none"><li>• Collection</li><li>• Report</li></ul> See <a href="#">About Job Categories</a> on page 418.
Name	Enter the name of the job. The job name should not be longer than 255 characters.
Description	(Optional) Enter a description to help you further identify what you are collecting in the job.
Template	<ul style="list-style-type: none"><li>• <b>Use Job Template</b> Lets you choose a job template that you have previously saved. There is also a list of pre-defined job templates that come with the application from which you can select. See <a href="#">Default Job Templates</a> on page 459.</li><li>• <b>Save As Job Template</b> Lets you save the configuration of the job as a template for use in future jobs that you add. If a job is saved as a job template, the name of the job should be no longer than 64 characters. See <a href="#">Deleting Job Templates</a> on page 459.</li></ul>

## General Job Options (Continued)

Option	Description
Job Data Path	<p>This sets the responsive folder path for data from eDiscovery jobs. Under this path, a folder is created for each job. The job sub-folders contain job reports and ad1 files for collected files.</p> <p>You can select to inherit the path that was configured for the project or configure a different path. See <a href="#">General Project Properties</a> on page 246.</p> <p>For a multiple server installation, this path is the UNC path or IP address path to a network share that serves as the output location for all the items that are copied during the job collection.</p> <p>Make sure double backslash characters (\\) precede the UNC path or the IP address path.</p> <p>If a network UNC path is specified, the path can be validated to ensure that the program can access the location. The validation also ensures that your job output is available for viewing.</p> <p>Local paths only work on single box installations.</p>
Inherit from Project	Inherits the job data path from the associated project.
Job Data Browse Button	<p>Lets you browse to the job data path root field to expedite finding the job by this name.</p> <p><b>Note:</b> The folder does not have to exist. If a new folder is specified, the system will create it for the user upon execution of the specified job.</p>

## Job Target Options

Option	Description
Job Target Options - Custom	Lets you manually select sources such as custodians (people), computers, network shares, and email servers, whose data you want to collect.
Job Target Options - Group	<p>Lets you select data sources that you want to collect from based on Active Directory organizational units and logical administrative units for people, groups, and resource objects such as computers and file shares.</p> <p>When you create a job that includes <i>Group</i> as a target, a snapshot of all of the data sources in the group is made and used for the life of the job. If the group changes after the job is created and executed (not just approved), those changes do not affect the targets of the group that were used in an executing job.</p>
Job Target Options - IP Range	<p>Select this to enter a range of IP addresses from which you want to collect data. This is an easy way to collect from a group of computers that are in an IP range.</p> <p><b>Note:</b> If you select this option, configure a short Cancel Pending date or the job will never complete, because there is no guarantee of an agent being in the IP range.</p> <p>See <a href="#">IP Range Tab</a> on page 434.</p>
Job Target Options - Custodians	<p>A network user who can be responsible for or have access to computers, network shares, email, or public data repositories that contain files of interest for the current job. The user's non-email and email are also included in a CIRT job when selected.</p> <p>See <a href="#">Custodian Tab</a> on page 435.</p>

## Job Target Options (Continued)

Option	Description
Job Target Options - Computers	A computer in the network that can contain files of interest. In order to collect from a computer, the computer must have the appropriate agent installed on it. See <a href="#">Computers Tab</a> on page 437.
Job Target Options - Network Shares	A network repository for stored files that can contain files of interest. See <a href="#">Network Shares Tab</a> on page 440.

## Job Other Data Sources Options

Option	Description
<b>Other Data Sources</b>	See <a href="#">Configuring Third-Party Data Repositories as Data Sources</a> on page 145.
Box	See <a href="#">Configuring for a Documentum Server</a> on page 158. See <a href="#">Box Collections Options</a> on page 471.
CMIS	See <a href="#">Configuring for a Documentum Server</a> on page 158. See <a href="#">CMIS Collection Options</a> on page 493.
Documentum	See <a href="#">Configuring for a Documentum Server</a> on page 158. See <a href="#">Documentum Collections Options</a> on page 475.
DocuShare	See <a href="#">Configuring for a DocuShare Server</a> on page 165. See <a href="#">DocuShare Collection Options</a> on page 477.
Druva	See <a href="#">Configuring for Druva</a> on page 172. See <a href="#">Druva Collection Options</a> on page 491.
Enterprise Vault Server	See <a href="#">Configuring for an Enterprise Vault Server</a> on page 152. See <a href="#">Enterprise Vault Server Collection Options</a> on page 479.
Exchange Public Folder	See <a href="#">Configuring for a Documentum Server</a> on page 158. See <a href="#">Collecting Exchange Emails for Custodians</a> on page 482.
Google Drive	See <a href="#">Configuring for Google Drive</a> on page 171. See <a href="#">Google Drive Collection Options</a> on page 485.
OpenText ECM	See <a href="#">Configuring for a OpenText ECM Server</a> on page 169. See <a href="#">OpenText ECM Collection Options</a> on page 486.
SharePoint	See <a href="#">Configuring for a SharePoint Server</a> on page 160. See <a href="#">SharePoint Collection Options</a> on page 487.
Website	See <a href="#">Configuring for Web Sites</a> on page 163. See <a href="#">Website Collection Options</a> on page 490.

### Job Priority and Agent Speed Options

Option	Description
Job Priority - Inherit from Project	Inherits the job priority from the associated project.
Job Priority - Low, Medium, High	Select a priority for the job.

### Processing And Remediation Options

Option	Description
Auto Process Options	Check to have the data auto processed. If this option is checked, the job and evidence is processed automatically. If you do not want to process the evidence at this time, leave this option unselected.

### Job AD1 Encryption Options

Option	Description
AD1 Encryption	The AD1 Encryption option set is only available if you choose the Collection Job Type.
Inherit from Project	Inherits the AD1 encryption setting from the associated project.
Disabled	Turns off encryption of an AD1 evidence image file.
Password	Encrypts an AD1 evidence image file with a password that you specify.
Certificate	Encrypts an AD1 evidence image file with a certificate. Certificates use public keys for encryption and corresponding private keys for decryption. You can configure the certificates that appear in the drop-down menu.
Agent Collection	Check to create AD1 image on the agent.

### Job Expiration Options

Option	Description
<b>Job Expiration</b>	Define the amount of time the system (Site Servers) will try and contact data sources within a job. After the time period, jobs meeting the conditions cancel. You have two condition options to specify for the job:
Single Attempt	Fails the job on Agent or Share after a first attempt.

## Job Expiration Options (Continued)

Option	Description
Cancel Pending	<p>Define the amount of time the system (Site Servers) will try and contact data sources within a job when the job is in a pending state. After the time period, any jobs still pending cancel. This stops the job from attempting to contact agents on which it has not yet started tasks (pending tasks). Agents that have already been contacted within the time defined with continue to run until the task is complete regardless of the expiration date.</p> <p>This only cancels the pending job(s), not other jobs in various states.</p> <p><b>Note:</b> When cancelling a recurring job, only the job that is currently running in Site Server will cancel. The next occurrence of the job will start at its appointed time. A recurring Volatile job is cancelled according to the Cancel Pending parameters.</p>
Cancel Incomplete	<p>Define the amount of time the system (Site Servers) will try and contact data sources within a job. After the time period, any incomplete jobs cancel. This is selected by default.</p> <p>This cancels all jobs that have not completed, even jobs that are in progress.</p>

## Job Auto Deploy Agents Options

Option	Description
Auto Deploy Agents	Turn on or Off. It is Off by default.

## Run Scripts

Option	Description
Run Scripts	Select to execute a script after a job completes. See <a href="#">Running Scripts</a> on page 444.

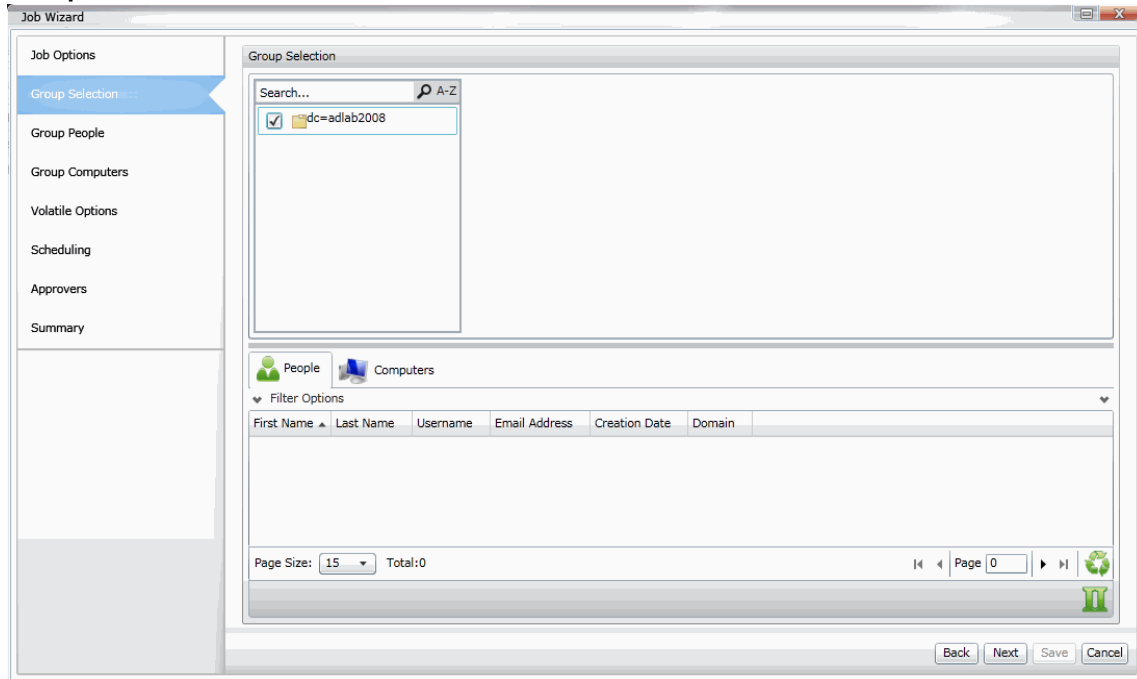


## Group Selection Tab

The *Group Selection* appears only if you select **Group** in the *Job Target Options* earlier in the wizard.




See [Adding a Job](#) on page 426.

### Group Selection Tab



The following table describes the options that are available in the *Select People* of the *Job Wizard*.

### Group Selection Options

Option	Description
Groups list (upper pane)	Displays the computers that you can select to add to the job. The list box identifies computers by their name and by their description and locality, if specified.
Filter Options (lower pane)	Allows you to filter the information in the associated list pane.
	Displays all people within the selected group.
	Displays all computers within the selected group.
	Displays all file shares within the selected group.

## IP Range Tab

The *IP Range* screen appears if you select **IP Range** as the *Job Target Option* in the *Job Options* screen of the *Job Wizard*.

See [Adding a Job](#) on page 426.

### IP Range Tab

The screenshot shows the 'Job Wizard' window with the 'IP Range' tab selected in the left sidebar. The main area is titled 'Computers' and contains a 'Start' field with IP address '10.1.2.3' and an 'End' field with IP address '10.1.2.10'. Below these fields is a 'Filters' section with two empty boxes labeled 'Include' and 'Exclude'. At the bottom of the 'Filters' section are four icons: a green plus sign, a red minus sign, a green pencil, and a green downward arrow. Below the icons is an 'Advanced Options' section with a downward arrow. At the bottom right of the window are four buttons: 'Back', 'Next', 'Save', and 'Cancel'.

### IP Range Options

Option	Description
Start	Allows you to enter the IP address for the starting point of the IP range.
End	Allows you to enter the IP address for the ending point of the IP range.
Include Filters	See <a href="#">Using Job Filters</a> on page 445.
Exclude Filters	See <a href="#">Using Job Filters</a> on page 445.
Advanced Options	See <a href="#">Computers Tab</a> on page 437.

## Custodian Tab



The *Custodian* options appear only if you selected **Custom > Custodian** in the *Job Target Options* group box in the Job Options.

See [Adding a Job](#) on page 426.




You can select the custodians (people) that you want to collect from. In addition to selecting custodians, you can select a person's:

- Computers
- Network Shares
- Enterprise Vault
- Exchange Server
- Domino Server
- Cloud Mail
- Gmail Mail

### Custodian Options

Option	Description
View by Project	Displays custodians associated with the selected project.
View All	Displays all custodians.
Filter Options	Allows you to filter the information in the associated list pane.
Custodian Details (upper pane, right side)	Specifies the full name and username of the custodian. You can set the highlighted custodian's default associations with computers, network shares, Exchange email, Lotus Notes email, or non-email data such as task items, calendar items, and so forth. For example, if you check <b>Computers</b> , all the computers that are listed in the <i>Computers</i> tab of the <i>Select People</i> frame, become associated with the custodian.
 Computers List tab	Displays the computers that you can associate or unassociate with the highlighted custodian.
Computer Details area	Identifies the name of the highlighted computer and, if available, its locality and description.
 Network Shares List tab	Displays the network shares that you can associate or unassociate with the highlighted custodian.
Network Share Details area	Identifies the network share path of the highlighted share and, if available, its locality and description.
<b>Enterprise Vault</b> wizard page	Lets you collect Enterprise data for the highlighted custodian.
<b>Exchange</b> wizard page	Lets you collect Exchange email for the highlighted custodian.
<b>Domino</b> wizard page	Lets you collect Notes email for the highlighted custodian.

## Custodian Options (Continued)

Option	Description
<b>Cloud Mail</b> wizard page	Lets you collect Cloud Mail email for the highlighted custodian.
<b>Gmail</b> wizard page	Lets you collect Cloud Mail email for the highlighted custodian.
	Adds a data source.
	Edits a data source.
	Depending on the selected tab above, opens the <i>Associate Computers to &lt;custodian_name&gt;</i> panel or the <i>Associate Network Shares to &lt;custodian_name&gt;</i> panel. This allows you to associate one or more computers or network shares to the custodian.

## Computers Tab

The *Computers* options appear only if you click **Custom**, and then check **Computers** in the *Job Target Options* group box earlier in the wizard.

See [Adding a Job](#) on page 426.

For agents that are configured to use a proxy server, the Work Manager initiates a secure connection with the first proxy server in the list. If the proxy is configured with two network interface cards, the internal IP address is used. If a secure connection cannot be established, the next proxy server in the list is attempted until the list is exhausted. Several attempts are made to contact a proxy server, after which an error is recorded for the job.



Upon successful connection, the connected proxy server is recorded for the collection.

The file request is transmitted to the proxy server. Every 20 minutes, the agent initiates a secure connection. The file request is transmitted to the agent, which reads the file request and transmits the file back to the proxy server. The Work Manager repeats these steps for each identified node (computer) that is configured to use a Proxy server.

The following table describes the options that are available on the *Computers* options of the *Job Wizard*.

See [Network Shares Tab](#) on page 440.

### Computers Options

Option	Description
<i>Filter Options</i>	Filters the computers in the associated list pane. See <a href="#">Filtering Content in Lists and Grids</a> on page 39. <b>Note: If your filter results in listing multiple computers, you can choose to either target all of the computers matching the filter you applied, or target only specific computers that you have checked in the list. If you choose to target all computers matching filter, the filter must be enabled.</b>
Computers list box	Displays all the computers that you can select to add to the job. This list comes from the computers that are defined in the Data Sources tab. See <a href="#">Managing Computers for Collecting Data</a> on page 124. The list box identifies computers by their name and by their description and locality, if specified.
<i>Computer Details</i> area (upper pane, right side)	Identifies the name of the highlighted computer and, if available, its locality and description.  You can click  to add a computer to the list.  You can click  to edit the details of a computer in the list.
<i>Filtered Collection</i>	Expand to either show or hide the Filters options. See <a href="#">Using Job Filters</a> on page 445.
<i>Full Disk Acquisition</i>	Allows you to collect an entire computer disk.
<i>Advanced Options</i>	
Logical Disk	Allows you to scan and collect only the target's logical drive space (Allocated space)

## Computers Options (Continued)

Option	Description
Physical Disk	Allows you to scan and collect the target's entire physical drive (Allocated and Unallocated space).
	<p><b>Collect Specific Sectors</b> - You can collect specific sectors of the physical disk instead of the full disk. If Collect Specific Sectors is selected, you can specify the beginning and ending sectors for collection. With collecting specific sectors:</p> <ul style="list-style-type: none"> <li>• Sector 0 can be collected</li> <li>• You can examine the RAW file collected in a hex editor or third party tools</li> <li>• There is no limit on the number of sectors you can collect</li> </ul>
Use Redirected Acquisition	Allows you to retrieve additional information about deleted files. <b>Note: If selecting this option, the Auto Process Feature will be disabled by default. If you want to auto process evidence, turn it on again.</b>
<i>Advanced Options</i>	Click the arrow to either show or hide the Advanced Options. Allows you to see advanced options for collection. Depending on the job type that you are creating, not all Advanced options are available.
Collect from Target options	<ul style="list-style-type: none"> <li>• File System: Select to collect the drives from the target's file system.</li> <li>• Logical Disk: Select to collect only the target's logical drive space.</li> <li>• Physical Disk: Select to collect the target's entire physical drive.</li> </ul>
'Search with' options	<ul style="list-style-type: none"> <li>• Search with Agent: Select to search files using the agent.</li> <li>• Search with Either Agent or Site Server: Select to search first with the agent and then with the Site Server.</li> <li>• Search with the Site Server: Select to search using the Site Server.</li> </ul>
System Files	Allows you to search system files that are normally hidden from view. Files with "\$" contain system metadata and in NTFS, the \$MFT contains the file system pointers to all files.
Scan Deleted Files	Scans free space of a partition for files matching the filter criteria. Select this option if you have parsed \$I30 INDX records.
Scan Unused Disk Area	Scans unallocated disk space for files matching filter criteria.
Archive Drill Down	<p>If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive files as part of the job and checks them against keywords supplied in the keyword filter.</p> <p><b>Note:</b> When selecting specific files for a Remediation job with Archive Drill Down selected, the Remediation job will delete the entire archive file if one or more of the specified files match the criteria of the job.</p>
Collect Response Archive	Collects any archive that contains files that match filter criteria.
Specify Extensions for Archive Drill Down	Allows you to specify the extension for the archive drill down. If you don't specify, the default will be used.
Collect Non-Extension Files	Collects all files that do not have an extension.

## Computers Options (Continued)

Option	Description
Use Internal File Identification	Recognizes internal file identification when checking file extensions.
Collect Unsearchable Encrypted Files	Collects files that cannot be accessed to search for keyword filter criteria.
Report on Non-Responsive Items	Generates a report detailing files that matched all filter criteria, but did not contain the specified keyword.
Parse \$I30 INDX Records	Parses \$I30 INDX records, so you can identify deleted files and display metadata contained in the file. This option is available for metadata, collection, and full disk acquisition jobs.
Exclude Removable Drives/Media	Excludes removable drives that are recognized by Site Server from the collection. This option is only available for collection jobs. Not all removable drives are recognized as such so this option may not exclude ALL removable drives.

## Network Shares Tab



The *Network Shares* options appear only if you click **Custom** and then check either **Network Shares** or in the *Job Target Options* panel earlier in the wizard.

See [Adding a Job](#) on page 426.

The following table describes the options that are available in the *Network Shares* options of the *Job Wizard*.

See [Computers Tab](#) on page 437.

### Network Shares Options

Option	Description
<i>Filter Options</i>	Filters the network shares in the associated list pane. See <a href="#">Filtering Content in Lists and Grids</a> on page 39. <b>Note:</b> If your filter results in listing multiple network shares, you can choose to either target all of the network shares matching the filter you applied, or target only specific network shares that you have checked in the list. If you choose to target all network shares matching filter, the filter must be enabled.
Network shares list box	Displays all the network shares that you can select to add to the job. This list comes from the network shares that are defined in the Data Sources tab. See <a href="#">Managing Network Shares for Collecting Data</a> on page 129. The list box identifies network shares by their name and by their description.
Network Share Details area (upper pane, right side)	Identifies the name of the highlighted share and description. You can click  to add a new network share to the list. You can click  to edit the details of network sharer in the list.
<i>Filters</i>	Click the arrow to either show or hide the Filters options. See <a href="#">Using Job Filters</a> on page 445.
<i>Advanced Options</i>	Click the arrow to either show or hide the Advanced Options.
Archive Drill Down	If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive files as part of the job and checks them against keywords supplied in the keyword filter. <b>Note:</b> When selecting specific files for a Remediation job with Archive Drill Down selected, the Remediation job will delete the entire archive file if one or more of the specified files match the criteria of the job.
Collect Responsive Archives	Collects any archive that contains any fields that match keyword filter criteria.
Specify extensions for archive drill down	Allows you to specify extensions for Archive Drill Down.
Collect Non-Extension Files	Collects all files that do not have an extension.
Use Internal File Identification	Recognizes internal file identification when checking file extensions.



## Network Shares Options (Continued)

Option	Description
Collect Encrypted Files	Collects files that cannot be accessed to search for keyword filter criteria.
Report on Non-Responsive Items	Generates a report detailing files that matched all filter criteria, but did not contain the specified keyword.
System Files	Allows you to search system files that are normally hidden from view. Files with "\$" contain system metadata and in NTFS, the \$MFT contains the file system pointers to all files.

## Scheduling Tab

You can schedule when you would like a job to execute using the Scheduling options screen in the Job Wizard. You can also set when and if you would like the job to reoccur.

See [Scheduling a Recurring Job](#) on page 442.

There are two different types of scheduling.

- **Server Scheduled:** Available for all jobs except RMM, Network Acquisition, and Volatile. Server scheduled starts a new instance of the job on the Server. The server job collects data from the agents as they report results.
- **Agent Scheduled:** Available for volatile jobs. Agent scheduled jobs are set to repeat on agents. Once an agent has been contacted and the job is received, it will repeat as specified in the scheduling options.

See [Adding a Job](#) on page 426.

## Scheduling Tab in the Job Wizard

The screenshot shows the 'Scheduling' tab in the Job Wizard. The interface is divided into a left sidebar and a main content area. The sidebar contains 'Job Options', 'Computers', 'Scheduling' (highlighted), 'Approvers', and 'Summary'. The main content area has two radio buttons: 'Manual Job Execution' and 'Scheduled Job Execution' (selected). Below this is a 'Start Date & Time' section with a 'Start job on' field set to '11/27/2012 1:46 PM'. The 'Recurrence' section is checked, showing a 'Recurrence Pattern' of 'Hourly' with 'Every 1 Hour(s)'. The 'End Recurrence' section has 'After 1 occurrence(s)' selected, with a 'by' field set to '11/28/2012 1:46 PM'. At the bottom right are 'Back', 'Next', 'Save', and 'Cancel' buttons.

## Options in the Scheduling Tab

Option	Description
Scheduled Job Execution	Select this to set a date and time when you want the job to execute. You can also set a reoccurrence on the job to execute on a regular basis.
Manual Job Execution	Select this to manually execute a job.

## Scheduling a Recurring Job

You can schedule a job to execute multiple times by enabling recurrence for that particular job. When recurrence is enabled for a job, the job executes the same requested actions during each recurrence. All the data and objects that meet the job criteria are collected again each time the job reoccurs.

The application allows you to configure your job(s) to execute by the minute, hourly, or daily. You can also configure the job to end at a given time.

---

**Note:** When scheduling Volatile jobs within a Combination Job, the recurrence schedule for the combination job overrides the recurrence schedule for the Volatile job itself.

---

### To schedule a recurring job

1. From the Scheduling tab, click **Scheduled Job Execution**.
2. Select **Enable Recurrence**. See [Recurrence Options](#) on page 442.
3. Under *Recurrence Pattern*, specify how often the job reoccurs. Specify when the recurring job will end. You can specify the recurrence of the job to end after so many occurrences or specify the recurrence of the job to end after a specific date and time.
4. Specify when the recurrence job ends.

### Recurrence Options

Option	Description
Use Relative Start Time	You may not know when a recurring job will get approved or started in relation to the scheduled time. With this option selected, if a job is approved after the scheduled start time, it will start at the next given iteration instead of having to be rescheduled.
Minute	Allows you to specify the number of minutes between job recurrences with the minimum option being 1 minute and the maximum being 30 minutes.
Hourly	Allows you to specify the number of hours between job recurrences with the minimum being 1 hour and the maximum being 12 hours.
Daily	Allows you to specify a specific time for the job recurrence to occur. The time specified must be an hourly instance, such as 4:00 AM or 7:00 PM.
Weekly	Allows you to specify a specific day for the weekly job recurrence to occur.
Monthly	Allows you to specify a specific day for a monthly job recurrence to occur. You can specify the day that the monthly job recurs by number or by day name.

## Recurrence Options

Option	Description
Yearly	Allows you to specify a specify day for a yearly job recurrence to occur. You can specify the month and day that the yearly job recurs.
End Recurrence	Allows you to specify when the recurrence job ends. You can specify that the job never ends, ends after so many occurrence, or ends by a specific date.

5. (optional) Select **Incremental Collection** to collect files that are new or have been changed since the last job execution. See [Incremental Collection](#) on page 443.
6. Click **Next** and follow the Job Wizard.

## Incremental Collection

You can use incremental collection as an option for collection jobs. Incremental collection allows the application to collect only new files that are new or have been changed since the last collection job. This option is turned on by default.

You can schedule the incremental collection job to recur automatically at a time increment that you specify (such as hourly, daily, or weekly) under Recurrence Pattern. You can specify a date or after so many recurrences for the incremental collection job to end.

- Incremental collection can be applied to the collection portion of a combination job, as well a full collection job.
- Targets available for incremental collection are computers, network shares, and Exchange mailboxes.

---

**Note:** Multiple files are collected from incremental jobs executed against Exchange mailboxes: PST file, sent file, receive file, and sometimes the Exchange top of the file. If multiple incremental jobs are executed against an Exchange mailbox, extra files with be generated.

---

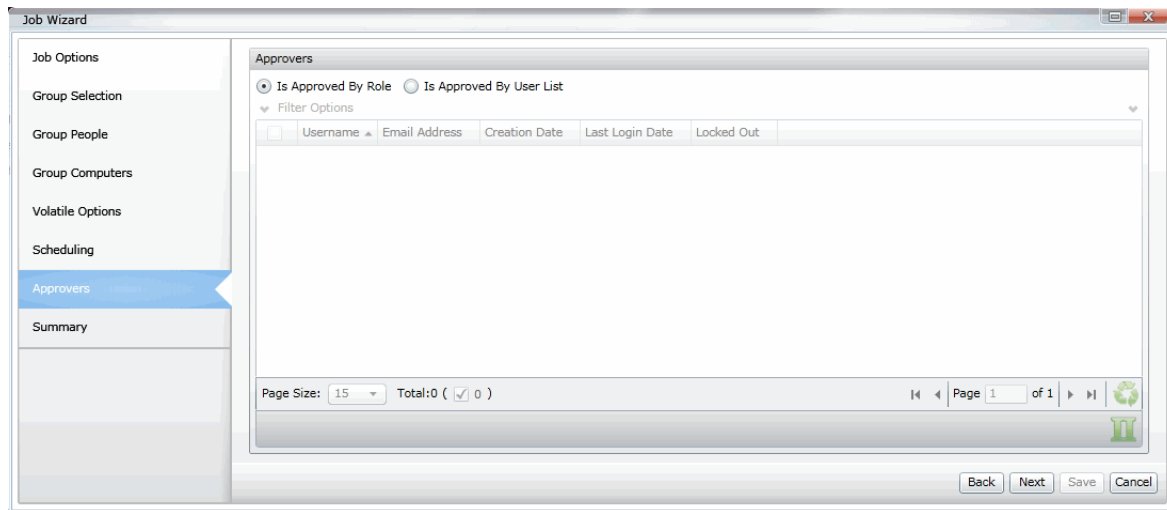
- Incremental collection only counts files as hits, not folders. However the folders appear in an AD1 file created from the data.
- Moving a file from one folder to another does not count as an incremental change and does not cause an update to occur. Moving files from one folder to another causes duplicates in the data to occur.

## Approvers Tab

The following describes the options that are available on the *Approvers* screen of the *Job Wizard*.

See [Adding a Job](#) on page 426.

### Job Approvers Tab



### Job Approvers Options

Option	Description
Is Approved By Role	Allows any user with job approval rights to approve the collection. After you complete the Job Wizard, the job must first be approved and then it must be executed.
Is Approved By User List	Allows you to select one or more users that are associated with the selected project, and that have approval rights, to approve the job. After you complete the Job Wizard, the job must first be approved. If you selected more than one user to approve the job, each user must log into CIRT and approve the collection. Once all approvals are complete, you can execute the job.

## Running Scripts

When creating a job, you can specify a script to execute after a job completes. This allows you greater control and customization of a job.

You can run the following files as scripts:

- executable (.EXE)
- batch files (.BAT)
- Powershell scripts (.PS1)

To execute the script, copy the script to the Work Manager Scripts folder, then select the option when creating the job.

### To execute a script

1. Navigate to **Program Files > AccessData > eDiscovery > Work Manager > Scripts**.
2. Copy the script that you want to execute to the **Scripts** folder.

---

**Note:** If you have multiple work managers, you must copy the script to each of the work managers.

---

3. Close the file.
4. Create a job. See [Adding a Job](#) on page 426.
5. At the Job Options tab, select Run Scripts On Job Completion under Run Scripts.
6. Populate the **Execute As** fields. These fields grant permissions for the script to execute on the agents that you send the job down to:
  - File Name
  - Domain
  - User Name
  - Password
  - Confirm Password
7. Complete configuring the job and execute.

## Script Execution Options

You can control the script execution after a job by editing a configuration file. You can:

- Change the location of the scripts folder. This allows you to save the script to a network share that communicates with multiple work managers
- Control how long a script runs. If this value is not changed, the script runs for 30 minutes.

### To edit the config file

1. Navigate to the Infrastructure.WorkExecutionServices.Host.exe.config file.
2. Add the following keys to the configuration file:
  - To change the location of the scripts folder: `<add key="ScriptFolder" value="" />` . Enter the value as the location of the new scripts folder.
  - To control how long a script runs: `<add key="ScriptMaxExecutionTime" value="" />` . Enter the value in milliseconds how long that you want the script to run.
3. Save and close the file.

## Using Job Filters

When configuring a job, you can use filters to target certain files by either including or excluding files.

The following are some examples of filters that you can use:

- Include or exclude only some files extensions. For example, include only DOC or XLSX files.
- Include or exclude a path. For example, exclude the WINDOWS folder and all sub-folders.
- Include or exclude files above or below a certain size.
- Include or exclude files based on file creation, modified, or last accessed date.
- Include or exclude files based on keywords in the documents.

- Include or exclude files based on file MD5 hashes.
- Combine filters: For example:
  - Include only the PDF files in a certain folder.
  - Exclude the EXE and DLL files in the WINDOWS folder.
  - Include only DOCX and XLSX files that were created after a specified date.

## Different Filter Types

The filters that you can use depends on the type of target that you are running jobs on. There are a set of filters available for Computers and Network Shares, and different filters available for third-party repositories like Exchange or SharePoint.

See [Computer and Network Share Filter Options](#) on page 447.

## Combining Filters

You can combine filters to get more specific results. There are different ways that you can combine filters and the method used will generate different results.

- You can use multiple properties within a single filter. This results in an AND function.
- You can use multiple filters. The results in an OR function

### Using multiple properties within a single filter - AND function

When you add a filter, you can configure one or more properties within the filter. If you specify multiple properties within a single filter, the properties are combined as an AND function.

For example, if you add an inclusion filter, and in that one filter specify an extension of PDF and also a file size of greater than 2MB, the logic is “PDF” AND “>2MB”. The results will include only PDF files that have a file size greater than 2 MB.

As another example, if you add an inclusion filter, and in that one filter specify the two extensions of DOCX and XLSX, and also a file creation date of after 1/1/2016, then the results will include only DOCX and XLSX files that have a file creation date of after 1/1/2016.

As another example, if you include a path as a property in a filter, any other properties specified in the *same* filter will only apply to the specified path. Suppose you target a network share `\\documents` and you create an inclusion filter and specify the folder `my_Work_files`. And suppose that in the same filter you specify a file extension, such as PDF. The results will be that it considers the path first and the extensions second. In this example, only the PDF files in the `my_Work_files` folder are included. No other PDF files will be included and no other files outside of `my_Work_files` will be included. Similarly, if you create one inclusion filter and you specify two paths and PDF and DOCX extensions, it will include all of the PDF and DOCX files from only the two folders.

Some filters include multiple tabs. For example, when using filters for computers and network shares, there are four tabs of filter properties. You can use properties from multiple tabs to perform an AND function. For example, when adding an include filter, on the *Meta Info* tab, you can specify an extension of PDF, and then on the *MD5* tab, you can add a list of MD5 hashes. The result will be only the PDF files that have the listed MD5 files. As another example, when adding an include filter, on the *Meta Info* tab, you can specify one or more folders and then on the *File Content* tab, you can add a list of keywords. The result will be only the files within the specified folders that contain the listed keywords.

### Using multiple filters - OR function

In contrast, you can use multiple filters and get the results of both. The functions as an OR function.

For example, if you add one inclusion filter, and in that filter specify an extension of PDF, and then add a second filter, and specify a file size of greater than 2MB, the logic is “PDF” OR “>2MB”. The results will include all PDF files *and* all files with a size greater than 2 MB.

As another example, suppose you target a network share \\documents and you create one filter to include the folder my\_Work\_files. You can create a second filter and specify an extension of PDF. The results will include all of the files in my\_Work\_files and all of the PDF files within the share regardless of paths.

### Using Inclusion and Exclusion filters - AND function

You can also use Include and Exclude filters together.

For example, you can add an Inclusion filter and specify an extension of PDF. You can also add an Exclusion filter and specify a file size greater than 3MB. The result is to include only PDF files that are less than 3MB.

As another example, you can add an Inclusion filter and specify an extension of PDF. You can also add an Exclusion filter and specify a path of one or more sub-folders. The result is to include only PDF files that are not in the excluded folders.

## Computer and Network Share Filter Options

When using a job to collect data from *Computers* and *Network Shares*, you can use Inclusion or Exclusion filters to either include or exclude specified data.





See [Computers Tab](#) on page 437.

See [Network Shares Tab](#) on page 440.





When you configure a filter for a job, you can save it as a template and load it in another occurrence.

The following table describes the filters elements:

### Filters Options

Option	Description
<i>Filters</i>	Click the arrow to either show or hide the Filters options.
<i>Include</i>	Lets you create or load an Include filter.
	Opens the <i>Include</i> panel where you can specify file inclusion filter information such as meta data information, file content, or MD5 hash sets.
	Deletes the selected filter template from the <i>Include</i> list box.
	Allows you to edit the settings of a selected filter in the <i>Include</i> list box.
	Lets you load a previously saved <i>Include</i> filter template.
<i>Exclude</i>	Displays the names of each file exclusion filter that you have created.

## Filters Options

Option	Description
	Opens the <i>Exclude</i> panel where you can specify file exclusion filter information such as meta data information, and file content.
	Deletes the selected filter template from the <i>Exclude</i> list box.
	Allows you to edit the settings of a selected filter in the <i>Exclude</i> list box.
	Lets you load a previously saved <i>Exclude</i> filter template.

The following tables describe the Inclusions and Exclusions filter options that are available:

- Meta Info
- File Content
- MD5
- Notes Archive Options

### Meta Info Tab

Option	Description
Filter Name	(Required) The name of the new file include filter.
Extension(s)	Includes or excludes files by extension. You can use an asterisk (*) as a wildcard. For example, <code>doc*</code> which will include <code>.DOC</code> and <code>.DOCX</code> .  You can specify multiple extensions by separating with a comma. For example, <b><code>bmp,jpg,png</code></b> <b>Note:</b> Do not include spaces before or after commas. If you do, the application will remove them.
Path Contains	Includes or excludes files by path sub-folders. <a href="#">Using "Path Contains" in a Filter</a> (page 449)
File Size	Includes files based on file size. You can designate file size ranges using <i>Is</i> , <i>Greater Than</i> , or <i>Less Than</i> and on an associated file size in bytes, kilobytes, or megabytes.
File Creation Date	Includes files based on any date, a specific creation date, or a data range.
File Modified Date	Includes files based on any edit date, a specific edit date, or an edit data range.
File Last Accessed Date	Includes files based on any last accessed date, a specific last accessed date, or a last accessed date range.
Save Filter As Template	Lets you save the configured filter as a template so that you can reuse it in other jobs.



## Using “Path Contains” in a Filter

You can include or exclude files based on folders/sub-folders in the share or on the computer.

You can specify folders by doing the following:

- Include or exclude a complete folder name  
For example, suppose you target a network share `\\documents`. Also, suppose that the share has a folder structure of  
`\\documents\my_Work_files\  
\\documents\my_Own_files\  
\\documents\shared files`

If you enter `my_Work_files` in this field, it will include that folder.

- Include or exclude a folder name using wildcards.  
For example, if you enter `*work*` in this field, it will include the `my_Work_files` folder.

---

**Note:** You do not need to include the full path, just the name of a folder that is within the target.

---

You can specify multiple folders by separating the folder names by a comma. For example,

`my_work_files,shared files,*own*`

**Note:** Do not include spaces before or after commas. If you do, the application will remove them.

Spaces within a folder name are allowed (for example, `shared files`).

You can also click **Browse** and import a list of paths from a TXT or CSV file. In the file, specify each path name either with commas (no spaces), or on its own line (commas will be inserted when imported). Do not include any headers or other text in the file. For example,

`my_work_files,shared files,*own*`

or

`my_work_files`

`shared files`

`*own*`

When the target is a computer, you can do the following:

- Collect a single file by specifying an absolute file path. This allows you to quickly gather items that you know are stored in a certain directory. For example, specifying the path `c:\program files\accessdata\agent\agentcore.exe` only collects that particular executable.
- Collect files by specifying a system environmental variable. This allows to locate objects at any location on the system. For example, when an agent is installed on a machine, a system variable is created: `%ADAgentDir%`. By specifying the `%ADAgentDir%` variable, you can locate all files in the agent folder. Be sure to define the variable in the Path Contains field as `%<variable>%`.
  - You can specify any system environmental variable that is on a system
  - You can also specify any custom system environmental variable that you may have defined on a system

---

**Note:** If you create a custom system variable on the agent, you must reboot the agent machine before the collection job can find the variable.

---

**Note:** Due to a known issue, if you use the *Path Contains* property in an exclusion filter, you MUST also include a value in the Extension(s) property. If you want to exclude all the files in the specified folders, put *.\** in Extension(s) field. As an alternative, you can specify an extension, such as pdf. In that scenario, only the PDF files in the paths will be excluded.

---

## File Content Tab

Option	Description
Keywords	You can use the <i>File Content</i> tab with either Inclusion or Exclusion filters.
Simple or Regext	Lets you select whether to use simple text or regular expression keywords.
Keyword text field	Lets you enter text, patterns of data (regular expressions), or hexadecimal values. You can include files that contain specific keywords. When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example: <ul style="list-style-type: none"><li>• <b>Apple AND orange</b> returns files with both terms <b>apple</b> and <b>orange</b>.</li><li>• <b>Apple OR orange</b> returns files with either the term <b>apple</b> or <b>orange</b>.</li><li>• <b>(Apple AND orange) OR (banana)</b> returns files with either the terms <b>apple</b> and <b>orange</b> or files with the term <b>banana</b>.</li><li>• <b>'Apple and orange' OR banana</b> returns files with either the term <b>apple and orange</b> or files with the term <b>banana</b>.</li></ul>
Search File name only	Lets you narrow the keyword filter to search only the file name.
<i>Luhn Options</i>	
Credit Card Numbers	Includes credit card numbers using Luhn testing. Luhn testing distinguishes valid credit card numbers from what could be a random selection of digits.
Custom	Includes a custom regex expression. To filter by regular expressions, check <b>Custom</b> , and then enter the regular expression delimiters. For example: <code>\d\d\d\d</code> . <b>Note: You are not able to use dashes when creating a custom regex expression. For example: <code>\d\d\d\d-\d\d\d\d-\d\d\d\d</code></b>
Save Filter As Template	Lets you save the configured filter as a template so that you can reuse it in other jobs.

---

**Note:** There is a current issue that if you create one filter and use a property on the Meta Info tab and then create a second filter and use a property from another tab, only the filter with the Meta Info tab property is used and any other filter is ignored. If you combine the tab's properties within one filter, it works correctly.

---

## MD5 Tab

Option	Description
MD5 hash list box	Lets you add MD5 hash values to the MD5 list box. The added values are included in the job.
Import Hash List	Lets you browse and open an MD5 hash value file into the MD5 hash list box.
Save Filter As Template	Lets you save the configured filter as a template so that you can reuse it in other jobs.


# Approving a Job

Each Job has to be approved before it can be executed. Select **By Role** to allow any user with specified roles to approve the job, or select specific users from the User List.

See [Adding a Job](#) on page 426.

See [Executing a Job](#) on page 452.

## To approve a job

1. Log in to CIRT if you are a user who has been grant permission to give approval to a specific job.
2. Click **Jobs**.
3. In the *Jobs* list pane, highlight a job that has not yet been approved.
4. In the right pane, click **Approve** .

# Executing a Job

You can execute a job after it is approved.

Executing a job begins the process of collecting the data that meets any filter or keyword criteria that you configured in the *Job Wizard*.

See [Adding a Job](#) on page 426.

See [Approving a Job](#) on page 452.

## To execute a job

1. Log in if you are a user who has been granted permission to execute a specific job.
2. Click **Jobs**.
3. In the *Jobs* list pane, highlight a job that has not yet executed.
4. In the right pane, click **Execute**.

# Processing a Job


When you add a job, you have the option of having the job automatically processed.

See [Job Options Tab](#) on page 428.

If you do not enable this options, you can process a job after it is executed.


See [Executing a Job](#) on page 452.

## To process a job

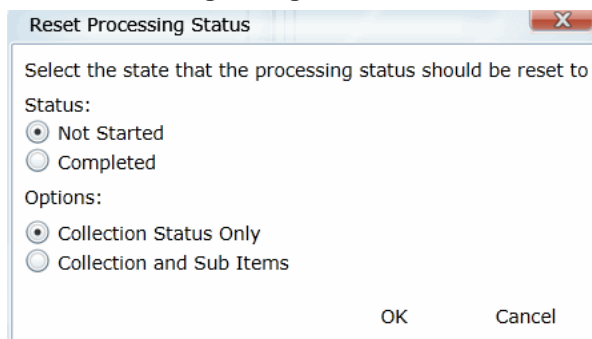
1. If not already, log in as a user who has been granted permission to approve a specific job.
2. Select the project that has the job that you want to process.
3. In the *Jobs* list pane, highlight a job that has not yet been processed.
4. In the right *Information* pane, click  **Process**.

If a job has already been processed, you can reset the processing status.

## To reset the processing status

1. If not already, log in as a user who has been granted permission to approve a specific job.
2. Select the project that has the job that you want to reset the process.
3. In the *Jobs* list pane, highlight the processed job that you want to reset.
4. Click  **Reset Processing Status** in the **Information** pane.

## Reset Processing Dialog



5. In the Reset Processing dialog, select whether you want the status to be reset to either **Not Started** or **Completed**.
6. Select between the **Collection Status Only** or **Collection** and **Sub Items** option.
7. Click **OK**.

# Using Job Reports

You can use *Job Reports* to generate various predefined reports with detailed information about collected files, emails, file statistics, remediated files, and so forth.

You can download a job report in the Excel spreadsheet format (.xls) format.


The following job reports are available:

- **Job Details Report:** Displays comprehensive information on the job options that were applied when the job was created.
- **Job Results:** Displays information on job results for the job.
- **Full Error Report:** Displays a breakdown of failed targets and the errors associated to them.

## *Running the Job Detail Report*

All jobs have the Job Detail report available.


### **To run the Job Detail report**

1. On the *Home* page, select a project and click the **Jobs** tab.
2. In the *Jobs* list pane, select a job.
3. In the lower pane, click **Reports** .
4. Click **Job Detail > Download** to view the report.

## *Running the Job Results Report*

The Job Results report is available for Search and Review and Volatile jobs. You can generate a job results report once a job begins collecting and at least one job target status is also collecting.

### **To run the Job Results report**


1. On the *Home* page, select a project and click the **Jobs** tab.
2. In the *Jobs* list pane, select a job.
3. In the lower pane, click **Reports** .
4. Click **Job Results > Download** to download the report.
5. Click **Job Results > View** to view the report.

## *Running the Full Error Report*

The Full Error Report shows a break down of failed targets and the errors associated to them. You can generate a full error report on a completed job where one or more targets have failed.

### **To run the Job Results report**

1. On the *Home* page, select a project and click the **Jobs** tab.
2. In the *Jobs* list pane, select a job.

3. In the lower pane, click **Reports** .
4. Click **Full Error Report > Download** to download the report.
5. Open the report.

## *Retrieving Reports for Deleted Jobs*

You can retrieve Job reports, System logs, and Activity logs for jobs that have been deleted. You can retrieve the logs by navigating to a folder that you have specified in the web.config file.

In order to enable this feature, you must edit the web.config file. You can find the web.config file at **C:\Program Files\AccessData\MAP\Web.config**. In the web.config file, locate the `<add key="PersistLogsToPath" value= ""/>`. For the `PersistLogsToPath` value, enter a path to where you would like to save the logs.

---

**Note:** Only previously generated reports for a job are available after a job has been deleted.

---

# Using Job Notifications

## About Managing Notifications for a Job

You can use *Manage Notifications* to set up a list of subscribers to email notifications for a given target job or target project, and an event type such as when job processing is completed.

Target types and their associated event types include the following:

### Notification Type

Target type	Associated event types
Projects	<ul style="list-style-type: none"><li>• Job Approved</li><li>• Job Completed</li><li>• Job Created</li><li>• Processing Completed</li></ul>
Jobs	<ul style="list-style-type: none"><li>• Job Approved</li><li>• Job Completed</li><li>• Processing Completed</li></ul> <p>See <a href="#">Creating Job Notifications</a> on page 456. See <a href="#">Deleting Job Notifications</a> on page 457.</p>
System	<ul style="list-style-type: none"><li>• User Created</li><li>• User Deleted</li><li>• Project Created</li><li>• Project Deleted</li></ul>

Before you can have email notifications sent for a job event, you must first make sure that you have configured the email notification server that you want to use.


See [Configuring the Email Notification Server](#) on page 81.

## Creating Job Notifications

After you create a job notification, you can view all the notifications that you have created by going to the *Manage Notification Subscriptions* view available from the Home page.

See [About Managing Notifications for a Job](#) on page 456.

### To create job notifications

1. On the menu bar, click **Jobs**.
2. In the *Jobs* list pane, check one or more jobs whose events you want to target for email notification.
3. In the lower left area of the project list pane, click .
4. In the *Create Event Notification* page, select a notification event type from the drop-down list.
5. In the *Select Users to Notify* group box, check the users who will receive the notification email message.
6. Click **Create Event Notification**.





## Deleting Job Notifications

You can delete job notifications that you created or job notifications that you are subscribed to.

See [About Managing Notifications for a Job](#) on page 456.

### To delete job notifications

1. On the **Home** page, in the Project List panel, click .
2. Do one or more of the following:
  - In the *Notifications I Created* group box, under the *Notification Type* column header, check the job notifications that you want to delete.
  - In the *Notification I Belong To* group box, under the *Notification Type* column header, check the job notifications that you want to delete.
3. Click .
4. In the *Confirm Deletion* dialog box, click **OK**.


# Using Job Templates and Filter Templates

## *Managing Job Templates and Filter Templates*

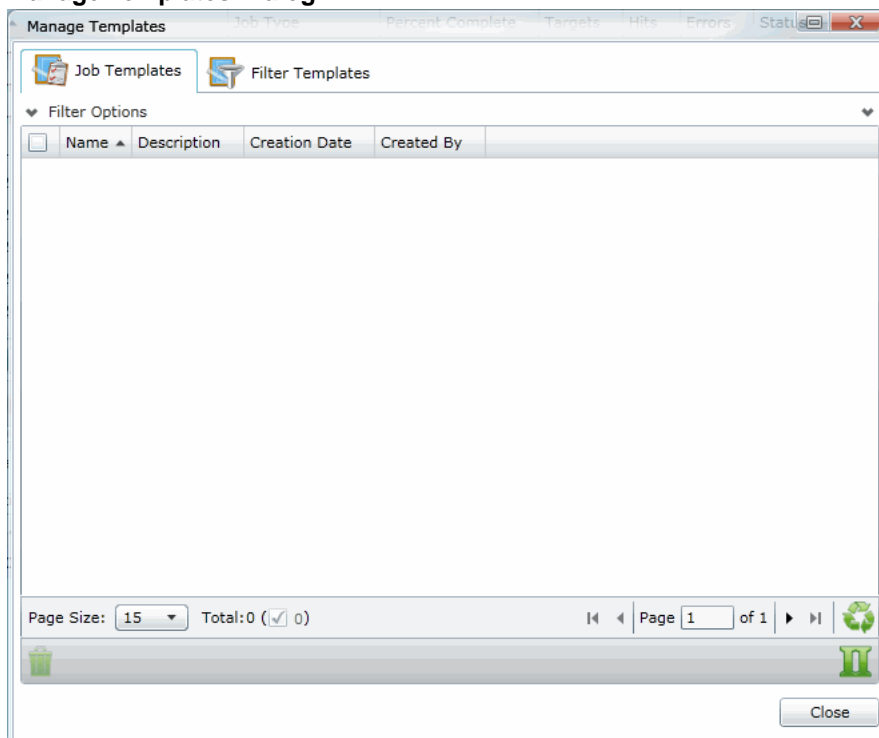
You can view and delete job templates and filter templates that you created for jobs.


See [Job Options Tab](#) on page 428.

### To view and delete templates

1. On the *Home* page, select the project that has the job that want to create a template for.
2. In the *Jobs* list pane, select a job.
3. Click  **Manage Templates** at the bottom of the upper right pane.

### Manage Templates Dialog




4. Click the **Job Templates** tab.
5. Select the template from the list and click  **Delete**.
6. Click **Close**.

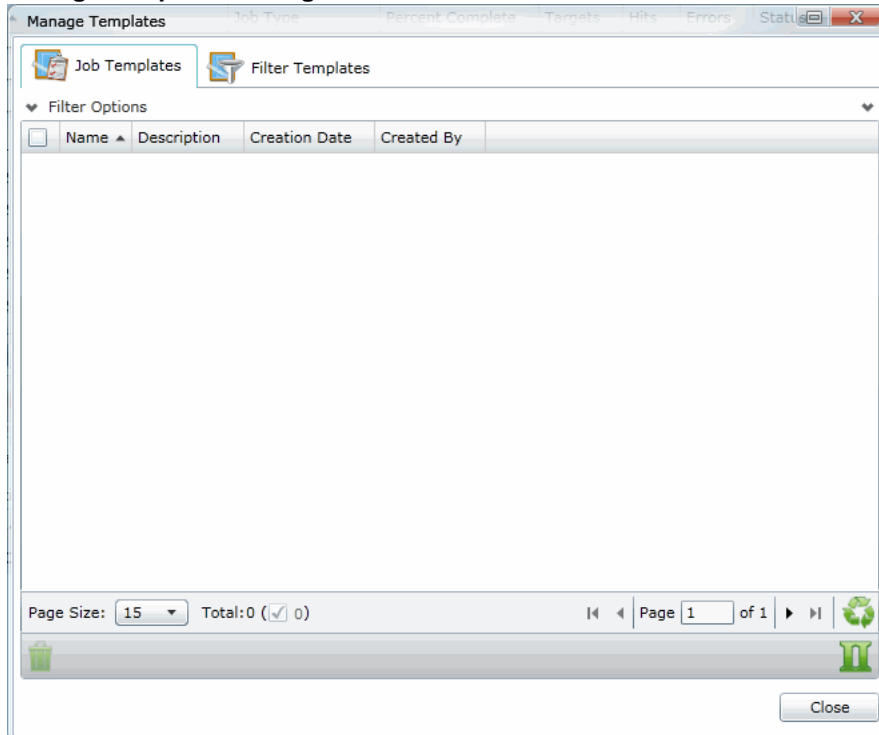
## Deleting Job Templates


You can delete job templates that you create for jobs from the Jobs tab on the Home page.

### To delete jobs

1. On the *Home* page, click **Jobs**.
2. Click the **Manage Job Templates** button .

### Manage Templates Dialog



3. Select the job template from the list and click the delete button .
4. Click **Close**.

## Default Job Templates

In addition to creating your own job templates, you can choose from a list of default job templates that is available in the application. The following table lists the job templates available.

### Default Job Templates

Template	Description
Coll-evtX	Executes a collection job that collects all the evtX (Windows Event log) files in the Windows/System32 folder.
Drop Process by PID	Executes a Process Dump/Memory Operations job for a PID specified by the user.

## Default Job Templates

Template	Description
EXE-Metadata-Cerb	Executes a metadata only job on all executables in the Windows\System32 folder and performs a Cerberus score.
File System Enumeration - Metadata	Executes a metadata only job that retrieves directory and file system information.
IR - Deep	Executes a volatile job that searches processes, sockets, DNS Cache, browser history, DLL, users, prefetch, filesystem, registry, and event logs.
IR Triage	Executes a volatile job that searches for DLLs and shared libraries, users, prefetch, sockets, and DNS.
Lockdown NIC	Executes an agent remediation that executes a script on the agent machine to disable its NIC card.
LockdownEnableNIC	Executes an agent remediation job that executes a script to disable the NIC card on the agent for four hours. After four hours, the NIC is enabled.
Memory Acquisition	Executes a memory acquisition job that includes a page file and creates an archive file.
Memory Analysis	Executes a memory analysis job collecting DLLs, Drivers, Handles, Registry, Sockets, and VAD information.
Registry On Disk	Executes a volatile job collecting all registry items. Because this job collects a lot of data, the job may take a long time.
Registry-Autostart	Executes a volatile job collecting only the Autostart information.
Registry-Full	Executes a volatile job collecting certain preset registry information. This job template differs from Registry On Disk because it does not collect all registry data.
Remediate-Name	Executes an agent remediation job to stop a process by a name specified by the user.
Remediate-PID	Executes an agent remediation job to stop a process by the PID specified by the user.
Small-exes-cerb	Executes a collection job that looks for any executable file that is under 250kb in size.
Software Inventory	Executes a software inventory job.
Vol-Deep	Executes a volatile job with all of the options selected except registry.
Vol-Deep-Cerb	Executes a volatile job with all of the options except registry. The job performs Cerberus scoring on running processes.
Vol-Hidden-Cerb	Executes a volatile job that searches for hidden processes and performs a Cerberus score.
Vol-Hidden-Injected	Executes a volatile job that searches for hidden processes and injected DLLs.
Vol-Quick-Cerb	Executes a volatile job that searches for just processes and DLLs and performs a Cerberus score.
Vol-Quick-Sched	Executes a volatile job that searches for just processes and DLLs running every five minutes for five times.

## *Viewing and Managing Job and Filter Templates*

An application administrator or as a user with the *Manage Job Templates* permission can use a central location on the *Management* page to view, add, edit, and delete job and filter templates.

See [Managing Templates](#) on page 91.

### **To access the Manage Job and Filters Templates page**


1. Login in as an admin or as a user with the Manage Job Templates permission.
2. Open the *Management* page.
3. Click **System Configuration**.
4. Click **Manage Templates**.

# Additional Job Tasks

## Testing the Collection Workflow

You can test the collections workflow to insure that everything is collecting properly.

### To test the collections workflow

1. On the *Home* page, select the project that has the job that you want to check the collection workflow.
2. In the *Jobs* list pane, select a job or jobs.
3. Click  **Test Collection Workflow** at the bottom of the *Jobs* list pane.

---

**Note:** This process could take up to 30 seconds to execute.

---

4. Click **OK**.


## Stopping a Job

You can stop active jobs after they have been approved and executed.

When you stop a job, the Job Status column in the Jobs list pane does not immediately show “Canceled.” Instead, the status shows “Canceling” until the task is complete.

See [Deleting Jobs](#) on page 464.

### To stop a job

1. On the menu bar, click **Jobs**.
2. In the *Jobs* list pane, check a job you want to cancel.
3. In the lower left corner of the Jobs list pane, click .
4. Click **Yes**.

---

**Note:** Stopping an already executed job (completed) results in a dialog box that says “There are no jobs to cancel. None of the selected jobs are executing.”

---

## Resubmitting a Job

You can resubmit a job if it has failed, the computer has restarted, some of the items in the job did not complete, or you want to add incremental data.


---

**Note:** Users without the Create Jobs Project permission cannot create jobs by resubmitting existing jobs.

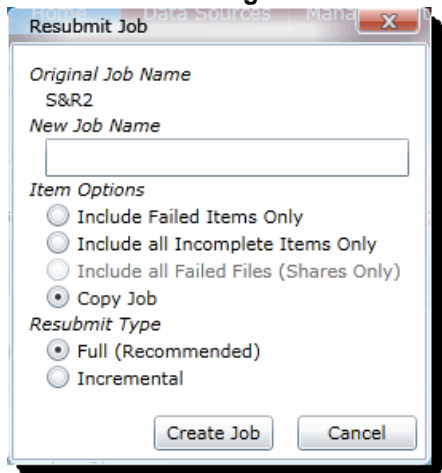
---

### To resubmit a job

1. On the menu bar, click **Jobs**.
2. In the *Jobs* list pane, check a job name.

- In the lower left corner of the Jobs list pane, click .
- In the *Resubmit Job* dialog, set the options that you want. The following table describes the available options.

### Resubmit Job Dialog



### Resubmit Collection Options

Option	Description
New Job Name	Specify a new name for the job.
<i>Item Options</i>	
Include Failed Items Only	Collects only targeted items that have failed for various reasons, such as no connection.
Include all Incompleted Items Only	Collects only targeted items that do not have a “Completed” status. The status may be Collecting, Queued, Waiting for Retry, Cancelled, Terminated, and so forth.
Include all Failed Files (Shares Only)	Tries to collect only failed files that reside on a network share.
Copy Job	Recollects all the originally targeted items.
<i>Resubmit Type</i>	
Full (Recommended)	Reruns the entire job again and gathers all hung, new, or modified data.
Incremental	Reruns the job, but only gathers new or modified data since the last collection.

- Click **Create Job**.


## Editing a Job

You can edit a job only if it has not yet been approved or executed. If a job is already approved or executed, you can only view the job’s settings.

See [Approving a Job](#) on page 452.

See [Executing a Job](#) on page 452.

### To edit a job

1. On the menu bar, click **Jobs**.
2. In the *Jobs* list pane, highlight a job name.
3. In the task pane, click .
4. In the *Edit Job* page, open the desired panel of the wizard, and then set the options that you want.
5. Click **Save** to return to the Jobs list pane where you can select the job, approve it, and then execute it.

## Deleting Jobs

You can delete one or more jobs from the Jobs list view. You should use caution when you use this feature because a selected job may be active. If a job is active and you delete it, the Work Manager may stop.



---

**Note:** There may be a delay between the time you delete the job and the time that the program updates the overall project size. You can still proceed with your work while the program is updating the project size.

---

See [Stopping a Job](#) on page 462.

### To delete jobs

1. On the menu bar, click **Jobs**.
2. Do one of the following:
  - In the *Jobs* list pane, highlight a job name you want to delete. In the right side of the upper pane, click .
  - In the *Jobs* list pane, check one or more jobs that you want to delete. In the lower left corner of the Jobs list pane, click .
3. (Optional) In the *Confirm Deletion* pane, check **Keep Archive** to keep an archive record of the jobs, and remove the jobs from the user interface.
4. Click **OK**.



## Chapter 40

# Configuring Jobs for Third-Party Data Sources

---

You can access third-party data sources for data. To access these sources, you need to configure job options in the *Job Wizard*. The following jobs access third-party data sources:

See [Introduction to the eDiscovery Collection Job](#) on page 423.

---

**Note:** Before you can access third-party data sources with a job, you need to configure the application to connect to the third-party data source in Data Sources.

See [Configuring Third-Party Data Repositories as Data Sources](#) on page 145.

---

When configuring job options, you may configure the following third-party Data Sources.

### Other Data Sources Job Options

Option	Description
Box	Lets you select data sources from your Box cloud storage system. See <a href="#">Box Collections Options</a> on page 471.
Cloud Mail	Lets you select data sources from a cloud mail server. See <a href="#">Cloud Mail Collection Options for People</a> on page 473.
CMIS	Lets you select data sources from a server connected by CMIS. See <a href="#">CMIS Collection Options</a> on page 493.
Documentum	Lets you select data sources from a Documentum server. See <a href="#">Documentum Collections Options</a> on page 475.
DocuShare	Lets you select data sources from a DocuShare server. See <a href="#">DocuShare Collection Options</a> on page 477.
Domino	Lets you select data sources from a Domino See <a href="#">Domino Collection Options</a> on page 474.
Druva	Lets you select data sources from a Druva server. See <a href="#">Druva Collection Options</a> on page 491.
Enterprise Vault Server	Lets you select data sources from an Enterprise Vault Server or select from a particular person on an Enterprise Vault Server. See <a href="#">Enterprise Vault Server Collection Options</a> on page 479.
Exchange	Lets you collect Exchange emails from a person. See <a href="#">Collecting Exchange Emails for Custodians</a> on page 482.



## Other Data Sources Job Options

Option	Description
Exchange Public Folder	Lets you collect data sources from an Exchange Public Folder. See <a href="#">Exchange Public Folder Collection Options</a> on page 484.
FileNet	Lets you select data sources from a FileNet server. See <a href="#">Google Drive Collection Options</a> on page 485.
Gmail	Lets you select data sources from a Gmail server.
Google Drive	Lets you select data sources from a Google Drive. See <a href="#">Enterprise Vault Server Collection Options</a> on page 479.
OpenText ECM	Lets you select data sources from an OpenText ECM server. See <a href="#">OpenText ECM Collection Options</a> on page 486.
SharePoint	Lets you select data sources from a SharePoint server. See <a href="#">SharePoint Collection Options</a> on page 487.
Website	Lets you select data sources from a Website through a Google account. See <a href="#">Website Collection Options</a> on page 490.

## Other Data Sources Filter Options

When using a job to collect data, you can use filters to either include or exclude specified data.

You are not required to configure filters to complete a job. If you do not configure any filters, the application collects all the files in the data storage locations.

You configure filters by expanding the Filters panel on the wizard page and then clicking  or  to add or edit an Include or Exclude filter.

# Box Collections Options

This option appears only if you select **Box** in the *Other Data Sources* pane in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured the application to collect from a Box data source.

See [Configuring for Box](#) on page 177.

In the *Box* panel, you can select a server that you want to collect from.

## Box Include and Exclude Filters

You also have the option to configure the Box filters. You can customize filters to include or exclude certain variables.

### Box Filters

The screenshot shows a dialog box titled "Include" with a green plus icon. It contains the following fields and controls:

- Filter Name: Test Filter
- Ancestor Folder Ids: Contains dropdown
- File Extension: Contains dropdown
- File Creation Date: Any dropdown
- File Modified Date: Any dropdown
- Owner: Contains dropdown
- Query: Contains dropdown, with "eBook," entered in the text box
- Scope: Contains dropdown
- File Size (bytes): Any dropdown

Buttons: OK, Cancel

### Box Filters

Option	Description
Filter Name	The name of the filter.
Ancestor Folder Ids	Allows you to select Box files based on the parent folder. You can select files that are within the ancestor folder or are not within the ancestor folder. Use commas to separate multiple folders.
File Extension	Allows you to select Box files based on file extension. You can select files that contain the file extension or do not contain the file extension. Use commas to separate multiple extensions.
File Creation Date	Allows you to select Box files based on file creation date. You can specify a single file creation date or a date range when the file was created. <b>Note: Do not select Range - Date Outside for this option. The filter will collect the Date Inside range instead of Date Outside range.</b>

## Box Filters

Option	Description
File Modified Date	<p>Allows you to select Box files based on file modified date. You can specify a single file modified date or a date range when the file was modified.</p> <p><b>Note: Do not select Range - Date Outside for this option. The filter will collect the Date Inside range instead of Date Outside range.</b></p>
Owner	<p>Allows you to select Box files based on the owner. You can select files that contain the owner or do not contain the owner. Use commas to separate multiple owners.</p>
Query	<p>This field is required. You must query on at least one keyword.</p>
Scope	<p>Allows you to select Box files based on the scope of the authentication token. You can select files that contain the scope of the authentication token or contain the scope of the authentication token. Use commas to separate multiple scopes.</p>
File Size	<p>Allows you to select Box files based on file size. You can specify a single file size or a file size range.</p> <p><b>Note: Do not select Range - Date Outside for this option. The filter will collect the Date Inside range instead of Date Outside range.</b></p>

## Cloud Mail Collection Options for People

You can collect cloud mail for Custodians. To collect, select **People** and **Select Person's Cloud Mail** in the *Job Target Options* group box in the Job Wizard.

When you collect the mail, you may notice a discrepancy in the email count between collecting from an POP server and collecting from an IMAP server. It might seem that there is more email collected from the IMAP server than the POP server.

The reason is because of the difference between the way IMAP handles email compared with the way POP handles email. If there is an email sent on an IMAP server that has the same **To:** address as the **Sent From:** address (For example, if you had sent an email to yourself), IMAP will store a copy of the email in two separate locations: one in the **To:** folder, and one in the **Sent From:** folder. POP will only store one copy of the email.

# Domino Collection Options

The Domino tab lets you collect Notes email for the highlighted custodian. In the Domino pane, you can do the following:

- **Include Notes** Collect Notes email for the highlighted custodian in the list box.
- **Collect Folders** Collect email folders on the highlighted custodian in the list box.

---

**Note:** You should not put spaces in a comma-delimited list of folders that you want to collect.

---

- **Collect Non-Email Data** Collect non-email data, such as task items or calendar items, on the highlighted custodian.
- **Domino Filters** Filter the collected emails by variables such as subject, creation date, or keywords. You can customize the filters, edit them, and delete them.

You must select a custodian from the *Custodians* pane before you can select any of the above options.

When dealing with a Domino Server, you should understand that Domino differentiates between internet email servers and other email servers. As an administrator, you need to make sure that you have the correct value listed in the Domino filter when setting up collecting with a Domino server.

## To obtain the values for the Domino filter

1. On your Domino server, select an email from the user you want to define as a Domino custodian in eDiscovery.
2. Right click the user.
3. The Domino server will display a fields tab and the values associated with those fields.
4. Highlight and copy the value string of the field that you want to edit.


---

**Note:** On the Domino server, the value string for a sender's email server is listed in *From* under the *Fields* tab, while the value string for a sender's internet email server is listed in *INetfromfield* under the *Fields* tab.

---

## Domino Email Values

### To set up email values in the Domino filter

1. In the *Custodians* option, under *Job Wizard*, select the custodian that you want.
2. Select the **Domino** tab.
3. Check **Include Notes**.
4. Select **Domino Filters**.
5. In the *Include* group box, click  **Add**. The **Include** dialog appears.
6. Enter the value string in the Senders' Internet Email and Senders' Email fields.
7. Click **OK**.

# Documentum Collections Options

This option appears only if you click **Custom**, and then check **Documentum** in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured the Documentum data source.

See [Configuring for a Documentum Server](#) on page 158.

In the *Documentum* panel, you can select a server that you want to collect from.

## Documentum Include and Exclude Filters

You also have the option to configure the Documentum filters. You can customize filters to include or exclude certain variables.

### Documentum Filters

**+ Include**

Filter Name:

Cabinet(s):

Author(s):

Owner:

Creator:

Keyword(s):

Modified By:

Name:

Extension(s):

File Size (bytes):

Subject:

Title:

File Creation Date:

File Modified Date:

OK Cancel

### Documentum Filters

Option	Description
Filter Name	(Required) The name of the new filter.



## Documentum Filters (Continued)

Option	Description
Cabinet(s)	The name of the cabinet that you are collecting from.
Author(s)	Filters files based on the author(s).
Owner	Filters files based on the owner.
Creator	Filters files based on the creator.
Keyword(s)	Filters files based on keywords.
Modified By:	Filters files based on the Modified By: field.
Name	Filters files based on the name.
Extension(s)	Filters files by extension. You can separate multiple extensions with a comma. For example, bmp,jpg,png. You can use an asterisk (*) as a wildcard.
File Size (bytes)	Filters files based on file size. You can designate file size ranges using <i>Equals</i> , <i>Not Equals</i> , <i>Greater Than</i> , or <i>Less Than</i> size in bytes.
Subject	Filters files based on the subject.
Title	Filters files based on the title.
File Creation Date	Filters files based on any date, a specific creation date, or a data range.
File Modified Date	Filters files based on any edit date, a specific edit date, or an edit data range.

# DocuShare Collection Options

This option appears only if you click **Custom**, and then check **DocuShare** in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured the DocuShare data source.

See [Configuring for a DocuShare Server](#) on page 165.

In the *DocuShare* panel, you can select a server from which you want to collect.

## DocuShare Include and Exclude Filters

You also have the option to configure the Docushare Filters. You can customize filters to include certain values or exclude certain values.

### DocuShare Filters

**+ Include**

**Filter Name:**

**Author(s):**

**Keyword(s):**

**Description:**

**File Type:**

**Handle:**

**Keyword Property:**

**Modified By:**

**Owner:**

**File Size (bytes):**

**Summary:**

**Title:**

**File Name:**

**File Creation Date:**

**File Modified Date:**

OK Cancel

## DocuShare Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Author(s)	Filters files based on the author(s).
Keyword(s)	Filters files based on keyword(s).
Description	Filters files based on content in the description
File Type	Filters files based on file type.
Handle	Filters files based on the handle.
Keyword Property	Filters files based on keyword property.
Modified By	Filters files based on the Modified By: field.
Owner	Filters files based on the owner.
File Size (bytes)	Filters files based on file size. You can designate file size ranges using <i>Equals</i> , <i>Not Equals</i> , <i>Greater Than</i> , or <i>Less Than</i> size in bytes.
Summary	Filters files based on the content in the summary.
Title	Filters files based on the title.
File Name	Filters files based on the file name.
File Creation Date	Filters files based on any date, a specific creation date, or a data range.
File Modified Date	Filters files based on any edit date, a specific edit date, or an edit data range.

# Enterprise Vault Server Collection Options

The *Enterprise Vault Server* options appear only if you click **Custom** and then check **Enterprise Vault Server** in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a Enterprise Vault Server data source.

[Configuring for an Enterprise Vault Server](#) (page 152)

In the *Enterprise Vault Server* panel, you can select an Enterprise Vault Server, Enterprise Vault Store, and Unassociated Archives.

## Enterprise Vault Include and Exclude Filters

You also have the option to configure the Email Archive Filters or the File Archive Filters. You can customize filters to include certain values or exclude certain values.

### Email Archive Filters for Enterprise Vault Server

**+ Include**

**Filter Name:**

**BCC's Email:**

**CC's Email:**

**Keyword(s):**

**Apply Keywords:**  Content  Attachments  Both

**Recipient's Email:**

**Sender's Email:**

**Senders Names:**

**Subject:**

**Mailbox Folder Name:**

**Created Date:**

OK Cancel

### Enterprise Vault Email Archive Filters

Option	Description
Filter Name	(Required) The name of the new filter.
BCC's Email	Filters files based on the BCC's email.
CC's Email	Filters files based on the CC's email.
Keyword(s)	Filters emails based on keyword(s).

## Enterprise Vault Email Archive Filters (Continued)

Option	Description
Apply Keywords	Applies keywords entered in the Keyword field by content, attachments, or both.
Recipient's Email	Filters files based on recipient's email.
Sender's Email	Filters files based on sender's email.
Senders Names	Filters files based on the senders names.
Subject	Filters files based on the subject.
Mailbox Folder Name	Filters files based on the mailbox folder name.
Created Date	Filters files based on the created date. You can filter by a single date, a range of dates, or any date.

## File Archive Filters for Enterprise Vault Server

## Enterprise Vault File Archive Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Extension(s)	Filters files by extension. You can separate multiple extensions with a comma. For example, bmp,jpg,png. You can use an asterisk (*) as a wildcard.
File Size (bytes)	Filters files based on file size. You can designate file size ranges using <i>Equals</i> , <i>Not Equals</i> , <i>Greater Than</i> , or <i>Less Than</i> size in bytes.
Keywords	Filters files based on keywords.

## Enterprise Vault File Archive Filters (Continued)

Option	Description
Apply Keywords	Applies keywords entered in the Keyword field by content, attachments, or both.
File Creation Date	Filters files based on any edit date, a specific edit date, or an edit data range.
File Modified Date	Filters files based on any edit date, a specific edit date, or an edit data range.

# Collecting Exchange Emails for Custodians

The Exchange tab lets you collect Exchange email for the highlighted custodian. The data that you can collect from a server depends upon the version of Exchange server that you are collecting from.

A custodian must be associated to an Exchange server before you can collect from that server.

See [Configuring for an Exchange Online/365 Server](#) on page 147.

See [Configuring for Exchange 2003, 2007, and 2010 Servers](#) on page 148.

See [Configuring for Exchange 2010 SP1 and 2013 Servers](#) on page 150.

## Collecting Data from an Exchange Server

### To collect Exchange email from a custodian

1. In *Job Wizard*, under *Custom Selection*, select **People** and **Select Person's Exchange**.
2. Click **Next**.
3. Select the person or people that you want to collect from using Exchange.
4. Under *Exchange* tab, click **Include Exchange**.
5. Populate the *Include Exchange* fields.
6. Select **Next**.

## Exchange Collection Options

The following table describes the fields that are available in the Include Exchange panel.

---

**Note:** When collecting from Exchange public folders, Include and Exclude filters will only work with Exchange 2013. Attempting to use a filter when collecting from public folders from earlier versions of Exchange will result in job target failure.

---

### Include Exchange Fields

Field	Description
Exchange MAPI	MAPI (Messaging Application Programming Interface) data is available from Exchange 2003, 2007, and 2010 servers. Depending upon which servers the custodians are associated with, both MAPI and EWS options may be available. If only a server is set up to collect MAPI data only, only MAPI data options will be available.
Complete Mailbox	Creates a local, unfiltered PST containing the full contents of the custodian's mailbox. With this option, you can collect additional data besides the custodian's mailbox.
Filtered Mailbox	Allows you to filter email by variables such as subject, creation date, or keywords. You can customize the filters, edit them, and delete them. If filters are not set, the complete mailbox will be collected. <b>Note:</b> Only custodians that have been indexed can successfully use this option. See <a href="#">Configuring for an Exchange Index Server</a> on page 146.

## Include Exchange Fields

Field	Description
Include Dumpster	Allows you to collect emails that are soft-deleted.
Collect Non-Email Data	Allows you to collect non-email data, such as task items or calendar items associated with that custodian.
<b>Exchange Web Services</b>	Exchange Web Services data is available from Exchange Online/365, Exchange 2010 SP1, and 2013 servers. Depending upon which servers the custodians are associated with, both MAPI and EWS options may be available. <b>Note: Discovery does not support EWS data for Exchange 2010. Only MAPI data can be collected from Exchange 2010.</b>
Apply Filter	Allows you to apply the Exchange filters to the EWS data.
Include Recoverable Deletes	Allows you to collect deletions. Deletions are enabled by default in Exchange. There's no need to specify a folder path because there is no folder structure retained for those items.
Include Recoverable Purges	Allows you to collect purges (hard deletes) of data. In order to collect purges from an Exchange server, enable purges in the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.
Include Recoverable Versions	Allows you to collect versions of data that have been saved. In order to collect versions from an Exchange server, enable versions in the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.
Include Archive MailBox	Allows you to collect from an archive mailbox.
Mailbox Folder Path(s)	Specifies the mailbox folder to collect from an archive mailbox. In the field, you can put in the exact path of the destination of the mailbox, a root path of the destination, or you can put in a keyword. If you use a keyword, the application will collect from every mailbox with the keyword. <b>Note: Each mailbox folder path, and its options, is assigned per custodian, so if you need to have multiple custodians with the same job target, you need to define the mailbox folder and options under each custodian.</b>



# Exchange Public Folder Collection Options

The *Exchange Public Folder* options appear only if you check **Exchange Public Folder** in the *Other Data Sources* group box in the *Job Options* screen of the wizard.

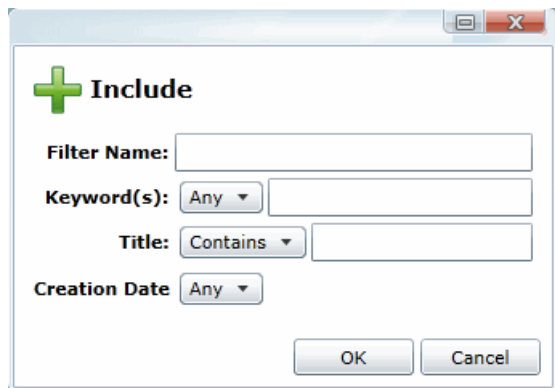
In order to make any selections, you must have already configured a Exchange Server data source.

In the *Exchange Public Folder* panel, you can select a server that you want to collect from.

## Exchange Include and Exclude Filters

You also have the option to configure the Exchange Public Folder filters. You can customize filters to include or exclude certain variables.

### Exchange Public Folder Include Filter



The screenshot shows a dialog box titled "Include" with a green plus sign icon. It contains the following fields and controls:

- Filter Name:** A text input field.
- Keyword(s):** A dropdown menu set to "Any" followed by a text input field.
- Title:** A dropdown menu set to "Contains" followed by a text input field.
- Creation Date:** A dropdown menu set to "Any".
- Buttons for "OK" and "Cancel" at the bottom right.

### Exchange Public Folder Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Keywords	Filters files based on keywords.
Title	Filters files based on the title.
Creation Date	Filters files based on any edit date, a specific edit date, or an edit data range.

# Google Drive Collection Options

The *Google Drive* option appears only if you click **Custom** and then check **Google Drive** in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a Google Drive data source.

---

**Note:** The Google Drive connector will only collect documents that have been created in Google Drive. It will not collect documents that have been uploaded to Google Drive from other sources, such as Microsoft Word or Excel files.

---

[Configuring for Google Drive](#) (page 171)

In the *Google Drive* panel, you can select a server from which you want to collect.

## Google Drive Include and Exclude Filters

You also have the option to configure the Google Drive Filters. You can customize filters to include or exclude certain keywords.

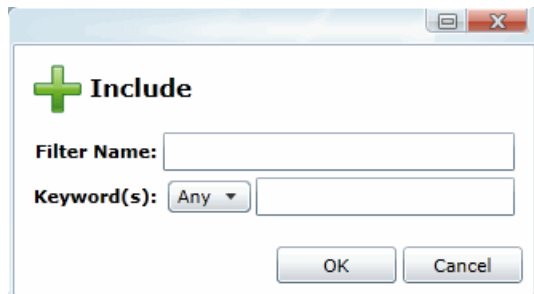
---

**Note:** For Google Drive, the exclude filters are ignored

---

Make sure to separate multiple keywords by commas.

### Google Drive Filters



### Google Drive Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Keyword(s)	Filters files based on keywords.

# OpenText ECM Collection Options

The *OpenText ECM* options appear only if you click **Custom** and then check **OpenText ECM** in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a OpenText ECM data source.

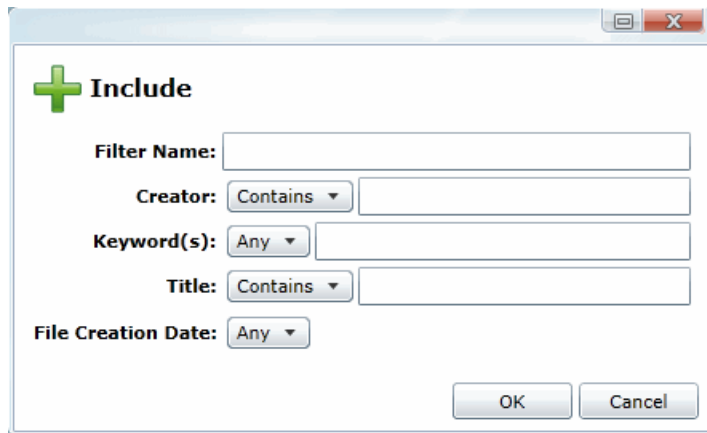
[Configuring for Cloud Mail](#) (page 167)

In the *OpenText ECM* panel, you can select a OpenText ECM repository.

## OpenText ECM Include and Exclude Filters

You also have the option to configure the OpenText ECM filters. You can customize filters to include certain values or exclude certain values.

### Include Filter for OpenText ECM



### FileNet Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Creator	Filters files based on the creator.
Keyword(s)	Filters files based on keywords.
Title	Filters files based on the title.
File Creation Date	Filters files based on any edit date, a specific edit date, or an edit data range.

# SharePoint Collection Options

The *SharePoint* options appear only if you click **Custom** and then check **SharePoint** in the *Job Target Options* panel earlier in the wizard.

In order to make any selections, you must have already configured a SharePoint data source.

See [Configuring for a SharePoint Server](#) on page 160.

You can select the Top-Level Site URL(S) and SubSites. For the SubSite, you can select to include the following:

## Select SharePoint Collection Type Options

Option	Description
Top-Level Site URL(S) list box	Lists all the Top-Level Site URL(S) that you can select to add to the job to collect from. This list is populated based on settings in the Data Sources tab. See <a href="#">Configuring for a SharePoint Server</a> on page 160.
Filter Options	Lets you filter the information in the associated list pane. See <a href="#">Managing Columns in Lists and Grids</a> on page 37.
SubSites list box	Lists all the SubSites that you can select to add to the job to collect from. This list is populated based on settings in the Data Sources tab. See <a href="#">Configuring for a SharePoint Server</a> on page 160.
<b>SubSite Options</b>	
Include Blog	Collects blog data within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list. You can choose to include the whole page in collecting or not.
Include Discussion Board	Collects discussion board data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list. You can choose to include the whole page in collecting or not.
Include Wiki	Collects wiki data within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Document Library	Collects document data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Calendar	Collects calendar data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Contacts	Collects contacts data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Tasks	Collects tasks data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Announcements	Collects announcements data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.
Include Survey	Collects survey data from within the specified root path of a highlighted individual site or a team site in the SharePoint Site URL list.

## Sharepoint Include and Exclude Filters

You also have the option to configure the File Filters. You can customize filters to include certain values or exclude certain values.

### Sharepoint Filters

Option	Description
Filter Name	(Required) The name of the new filter.
Extension(s)	Filters files by extension. You can separate multiple extensions with a comma. For example, bmp,jpg,png. You can use an asterisk (*) as a wildcard.
URL Contains	Filters any URL with the designated name in the path.
File Size (bytes)	Filters files based on file size. You can designate file size ranges using <i>Equals</i> , <i>Not Equals</i> , <i>Greater Than</i> , or <i>Less Than</i> size in bytes.
Title	Filters files based on the title.
Author(s)	Filters files based on the author(s).
Editor(s)	Filters files based on editor(s).
Content Type	Filters files based on the content type.

### Sharepoint Filters (Continued)

Option	Description
Keyword(s)	Filters files based on keywords.
Name	Filters files based on the name.
File Creation Date	Filters files based on any date, a specific creation date, or a data range.
File Modified Date	Filters files based on any edit date, a specific edit date, or an edit data range.

## Website Collection Options

The *Website* option appears only if you check **Website** in the **Other Data Sources** pane in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a website data source.

See [Configuring for Web Sites](#) on page 163.

In the *Website* panel, you can select a website from which you want to collect.

There are no filters available for websites.

# Druva Collection Options

The *Druva* option appears only if you check **Druva** in the **Other Data Sources** pane in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a Druva data source.

See [Configuring for Druva](#) on page 172.

In the *Druva panel*, you can select a Druva server.

## Druva Include and Exclude Filters

You also have the option to configure the File Filters. You can customize filters to include certain values or exclude certain values. You can add a filter, delete a filter, edit a filter, or load a saved filter.

### Druva Include Filter

**+ Include**

Meta Info | File Content | MD5

**Meta Info**

Filter Name:

Extension(s): Equals  ⓘ

Path Contains: Text  ⓘ

File Size (bytes): Greater Than  Bytes

File Creation Date: Any

File Modified Date: Any

File Last Accessed Date: Any

Save Filter as a Template

OK Cancel

### Druva Include Filter Options

Option	Description
Filter Name	(Required) The name of the new filter.
Extension(s)	Filter files by extensions. Specify whether the value(s) filtered equals or does not equal the data entered in the field. Separate multiple extensions by comma.



## Druva Include Filter Options

Option	Description
Path Contains	Filter files by what values are contained in the path. Specify whether the value filtered is text or a regular expression. Separate multiple extensions by comma.
File Size (bytes)	Filter files by file size. Specify whether the value filtered is greater than, is, less than, or any value entered in the file size field. You can specify the size by bytes, kilobytes, and kilobytes.
File Creation Date	Filter files by file creation. Specify the data by a range of dates, a single date, or any specific date.
File Modified Date	Filter files by the time the file was modified. Specify the data by a range of dates, a single date, or any specific date.
File Last Accessed Date	Filter files by the last time the file was accessed. Specify the data by a range of dates, a single date, or any specific date.
Save Filter as a Template	Save the filter created as a template that can be loaded by other users.

# CMIS Collection Options

The *CMIS Repository* option appears only if you check **CMIS** in the **Other Data Sources** pane in the *Job Target Options* group box in the *Job Options* screen of the wizard.

In order to make any selections, you must have already configured a CMIS Repository data source.

See [Configuring for a CMIS Repository](#) on page 174.

In the *CMIS panel*, you can select a CMIS Repository server. Checking **Use Global Custom Filters** allows the job to use a custom filter that you may have uploaded when configuring the application for CMIS collection.

---

**Note:** The custom filter can combine with the Include and Exclude filters. The custom filter in combination with the Include/Exclude filters acts as an OR not AND. That is, data matching either the specifications in the Include/Exclude or in the custom filter. The data does not need to match both filters.

---

## *CMIS Include and Exclude Filters*

You also have the option to configure the File Filters. You can customize filters to include certain values or exclude certain values. You can add a filter, delete a filter, edit a filter, or load a saved filter.

Although there are many fields available in the Include and Exclude filters, not all fields available can be filtered. The values that are available for you to filter depends upon how you have set up your CMIS repository.

**Note:** Please note that the user interface displays the application's default filters. Not all of the values that are available in the filter apply to every CMIS repository. If you filter on a value that is not available in the CMIS repository, the collection job will fail.

### CMIS Include Filters

### CMIS Include Filter Options

The following lists the options that are available to filter in the Include filter.

**Note:** In the following table, if there is no description listed, the field cannot be searched and the job will fail.

#### CMIS Include Filter Options

Option	Description
Filter Name	(Required) The name of the new filter.
Name	Filters files based on the name. Specify whether the data contains the value or not.
Description	
Path	

## CMIS Include Filter Options

The following lists the options that are available to filter in the Include filter.

---

**Note:** In the following table, if there is no description listed, the field cannot be searched and the job will fail.

---

### CMIS Include Filter Options

Option	Description
Keyword(s)	Filters files based on the keyword(s). Specify whether to filter on any of the keywords or all of the keywords.
Creator	Filters files based on the creator. Specify whether the data contains the value or not.
Modified By	Filters files based on the person who modified the file. Specify whether the data contains the value or not.
File Creation Date	Filters files based on the file creation date. Specify the data by a range of dates, a single date, or any specific date.
File Modified Date	Filters files based on the file modified date. Specify the data by a range of dates, a single date, or any specific date.
Object ID	
Object Type ID	
Parent ID	
Version Label	
Version Series ID	
Content Stream Length	
Content Stream Mime Type	
Content Stream File Name	Filters files based on the content stream file name. Specify whether the data contains the value or not.
Content Stream ID	

## Part 8

# Using the Dashboard

This part describes how to use the dashboard and includes the following section:

- [Using the Dashboard](#) (page 497)

# Chapter 41

## Using the Dashboard

### About the Dashboard

The Dashboard allows you to view important information in an easy-to-read visual interface. The Dashboard has different widgets that display the monitored data using a variety of charts.

You can customize most widgets in the following ways:

- The type of chart that is used, such as a pie chart, horizontal bar chart, or vertical bar chart.
- Whether to show information about all projects or selected projects.



Depending upon your product license, you can view widgets for the following features:

### Dashboard widgets

Feature	Description
Lit Hold	<p>(eDiscovery or Lit Hold license only)</p> <p>You can view the following widgets:</p> <ul style="list-style-type: none"><li>• Most Recent Holds with Approval/Acceptance Status</li><li>• Top Custodians and the number of holds assigned</li><li>• Top Custodians and the number of days pending approval</li><li>• All Hold broken out by status</li><li>• Top holds and the number of custodians assigned</li><li>• Top IT Staff and the number of holds assigned</li></ul> <p>See <a href="#">Using Litigation Holds</a> on page 339.</p>
Jobs	<p>(eDiscovery only)</p> <p>You can view the number of jobs broken out by their status: completed, completed with errors, cancelled, or failed.</p> <p>See <a href="#">About Jobs</a> on page 418.</p>





# Configuring Dashboard Widgets

The Dashboard tab has several widgets that display the monitored data. You can use the following elements to view and filter the data.

## To view Dashboard

1. Click the **Dashboard** tab at the top of the screen.

## Elements of Dashboard Widget

Element	Description
 Widget Options	Clear the gear icon to configure the following options:
	Changes the appearance of the chart. You can choose to display the data in either pie, vertical bar, or horizontal bar chart form.
	Filters the chart results by project. The button displays what projects are being filtered and displayed. See <a href="#">The Filter Case Chart Results Pane</a> on page 499.
	Refreshes the data in the widget. The button displays the last time that the data had been refreshed, either manually or automatically.

## The Filter Case Chart Results Pane

In the Filter Case Chart Results pane, you can filter the items displayed in the widget.

## Elements of the Filter Case Chart Results Pane

Element	Description
Filter by selected case(s)	Allows you to search for a specific case. Click Filter to filter by the search terms.
Selected cases only	Posts only the selected projects to the widget. You can scroll down the project list and check the projects that you want to display.
Unselect all	Deselects all of the projects in the project list.
Apply/Apply - all cases	Applies the selected projects to the Dashboard widget. This button displays the number of projects selected. For example, if you have selected four cases, the button displays <b>Apply - 4 cases</b> .
Cancel	Returns you to the main widget.



## Part 9

# Configuring and Using LawDrop

This part describes how to configure and use Law Drop and includes the following chapters:

- [Understanding LawDrop™](#) (page 501)
- [Administrating LawDrop™](#) (page 503)
- [Using LawDrop™](#) (page 508)

# Chapter 42

## Understanding LawDrop™

---

### About LawDrop

You can use LawDrop™ as an interface for application users to manage project evidence files without accessing the file system on the Summation or eDiscovery server. This is beneficial for letting users who don't have permissions to access the server's file system to add files to a project or access exported files. For example, LawDrop is the only method to perform several tasks when using Summation in a hosted, multi-tenant environment.

The screenshot displays the LawDrop interface. On the left is a navigation pane with a tree view containing 'Project-1', 'Exports', 'Intake', 'Project-2', 'Exports', 'Intake', 'My DropSpace', and 'Shared with me'. The main area shows a table with columns: Name, Owner, Last Modified, File Size, and Actions. Two items are listed: 'dii.zip' (959.03 KB) and 'User\_Guide.pdf' (6.09 MB), both owned by 'ADTester1' and last modified on 'Jan 13, 2016'. Below the table, it indicates '2 Total Items'. At the bottom, there are three buttons: 'Upload All' (green), 'Pause All' (orange), and 'Cancel All' (red). Below these buttons is a table showing upload progress for three files:

Name	Size	Progress	Actions
Computer1.ad1	536.87 MB	0.00%	[Upload] [Pause] [Cancel]
Federalist_Papers.pdf	1.33 MB	0.00%	[Upload] [Pause] [Cancel]
US_Constitution.docx	35.73 KB	0.00%	[Upload] [Pause] [Cancel]

This is a partial screenshot of the navigation pane from the LawDrop interface, showing the same tree view structure as the main screenshot above, with 'My DropSpace' highlighted in blue.

You can use LawDrop to do the following:

## Features of LawDrop

Feature	Description						
Upload files to the Summation or eDiscovery Server	You can use LawDrop to drag, drop, and upload files to the server. You can upload files to two different types of locations in LawDrop						
	<table border="1"> <tr> <td>My DropSpace</td> <td>You can upload files to a location called My DropSpace. This is a general area where you can upload, manage, and organize evidence files.</td> </tr> <tr> <td>Project Intake Folders</td> <td> <p>For every project in the system, LawDrop has a project <i>Intake</i> folder. This folder acts as a staging area for files that you want to add to a project.</p> <p>When you have identified files that you want to add to a project, you can copy them from the DropSpace to the Intake folder for that project. (You can also upload files directly to an Intake folder.)</p> <p>From the project Intake folder, users with permissions can add files as evidence to that project.</p> </td> </tr> </table>	My DropSpace	You can upload files to a location called My DropSpace. This is a general area where you can upload, manage, and organize evidence files.	Project Intake Folders	<p>For every project in the system, LawDrop has a project <i>Intake</i> folder. This folder acts as a staging area for files that you want to add to a project.</p> <p>When you have identified files that you want to add to a project, you can copy them from the DropSpace to the Intake folder for that project. (You can also upload files directly to an Intake folder.)</p> <p>From the project Intake folder, users with permissions can add files as evidence to that project.</p>		
	My DropSpace	You can upload files to a location called My DropSpace. This is a general area where you can upload, manage, and organize evidence files.					
Project Intake Folders	<p>For every project in the system, LawDrop has a project <i>Intake</i> folder. This folder acts as a staging area for files that you want to add to a project.</p> <p>When you have identified files that you want to add to a project, you can copy them from the DropSpace to the Intake folder for that project. (You can also upload files directly to an Intake folder.)</p> <p>From the project Intake folder, users with permissions can add files as evidence to that project.</p>						
Share your uploaded files with other users	The person who uploads files in LawDrop is considered the owner of those files. By default, when you use LawDrop, you can only see the files that you are the owner of. However, you can share your uploaded files so that other users can access them as well. Where users see files that have been shared with them depends on where the files were uploaded.						
	<table border="1"> <tr> <td>Sharing from My DropSpace</td> <td>Each user has their own <i>MyDropSpace</i> folder. When you share files from your <i>MyDropSpace</i> with another application user, they can see those files in a LawDrop folder called <i>Shared with me</i>.</td> </tr> <tr> <td>Sharing from a project Intake folder</td> <td>When you share files from a project <i>Intake</i> folder or sub-folder, other users with permissions to that project can then see them in the same <i>Intake</i> folder. For example, a user may have permissions to add a file to an Intake folder but not to add and process it in the project. Other users with enhanced permissions can add and process shared files in the project.</td> </tr> <tr> <td>Sharing files with external users</td> <td>You can also share files to people that are not application users by specifying their email address. These external users will receive an email with an HTML link to the shared files.</td> </tr> </table>	Sharing from My DropSpace	Each user has their own <i>MyDropSpace</i> folder. When you share files from your <i>MyDropSpace</i> with another application user, they can see those files in a LawDrop folder called <i>Shared with me</i> .	Sharing from a project Intake folder	When you share files from a project <i>Intake</i> folder or sub-folder, other users with permissions to that project can then see them in the same <i>Intake</i> folder. For example, a user may have permissions to add a file to an Intake folder but not to add and process it in the project. Other users with enhanced permissions can add and process shared files in the project.	Sharing files with external users	You can also share files to people that are not application users by specifying their email address. These external users will receive an email with an HTML link to the shared files.
	Sharing from My DropSpace	Each user has their own <i>MyDropSpace</i> folder. When you share files from your <i>MyDropSpace</i> with another application user, they can see those files in a LawDrop folder called <i>Shared with me</i> .					
	Sharing from a project Intake folder	When you share files from a project <i>Intake</i> folder or sub-folder, other users with permissions to that project can then see them in the same <i>Intake</i> folder. For example, a user may have permissions to add a file to an Intake folder but not to add and process it in the project. Other users with enhanced permissions can add and process shared files in the project.					
Sharing files with external users	You can also share files to people that are not application users by specifying their email address. These external users will receive an email with an HTML link to the shared files.						
	<b>Note:</b> Currently, you cannot share files from a project Intake folder with external users.						
Download files	You can download the files that you can access in LawDrop to your own computer.						
Use LawDrop as a destination when exporting files	When performing an export, you can select LawDrop as the destination. After the export, users with proper permissions can access the exported files within LawDrop without having access to the server's file system. Exported files are located in a project's <i>Exports</i> folder. Users can download the exported files to their own computers.						

# Chapter 43

## Administering LawDrop™

---

### About Administering LawDrop

#### *About the LawDrop File Storage Folder Structure*

There are two locations files to store files that are uploaded using LawDrop:

##### **LawDrop file storage folder structure**

Destination	Description
DropSpace	<p>When users use LawDrop to upload files, they may upload files to a DropSpace folder. An Administrator creates and specifies a share path to be used as the parent DropSpace folder.</p> <p>See <a href="#">Configuring the System for Using LawDrop</a> on page 504.</p> <p>When a user first accesses LawDrop, a sub-folder (with their user id) is created under the parent DropSpace folder.</p> <p>When a user uses LawDrop to upload files to the DropSpace, they are uploaded here. Using LawDrop, users may create sub-folders under here.</p> <p>For example:</p> <pre>\\Server\LawDrop_DropSpace_Share\dropspace\user ID\user-created subfolders</pre>
Project intake folder	<p>Whenever a project is created, a folder for that project is created (using a guid as the folder name) under the share path where you specified the project folder to be stored.</p> <p>See <a href="#">Project Folder Path</a> on page 246.</p> <p>See <a href="#">Default Evidence Folder Options</a> on page 84.</p> <p>Under that project guid folder, a <i>lawdrop</i> folder is created.</p> <p>For example:</p> <pre>\\Server\Projects_share\ project guid\lawdrop</pre> <p>Under the lawdrop folder are two sub-folders:</p> <ul style="list-style-type: none"><li>• <i>Intake</i> - When a user uses LawDrop to upload files to a project folder, they are uploaded here. Using LawDrop, users may create sub-folders under here. See <a href="#">Uploading and Managing Files in the File Upload Queue</a> on page 513.</li><li>• <i>Export</i> - When you perform an export and select LawDrop as the destination, the exported files are placed here. See <a href="#">Viewing Exported Files in LawDrop</a> on page 523.</li></ul> <p>For example:</p> <pre>\\Server\Projects_share\ project guid\lawdrop\export \\Server\Projects_share\ project guid\lawdrop\intake</pre>

If you are a system administrator, you can use the file system to view files that have been uploaded or exported using LawDrop.

**WARNING:** Do not attempt to move or delete uploaded files using the files system without contacting Technical Support. Use the LawDrop interface to copy, move, or delete uploaded files.

## Configuring the System for Using LawDrop

You must perform the following administrative tasks before using LawDrop:

- [Configuring the LawDrop DropSpace Folder](#) on page 504
- [Configuring the System To Share LawDrop Files with External Users](#) on page 505

### *Configuring the LawDrop DropSpace Folder*

Before using LawDrop, an administrator must configure the file location to be used by LawDrop for the DropSpace folder.


If the file location is not set, when any user clicks the LawDrop tab, they will see the following error:

*The default path for user's DropSpace folder is not set. Please the default path or contact your System Administrator.*

To configure the location of the DropSpace folder, you designate a folder just like you designate default project data folders for your projects and job data.

See [Default Evidence Folder Options](#) on page 84.

#### **To configure the LawDrop DropSpace path**

1. Identify a location where you have adequate space to store all files that may be uploaded to the DropSpace.  
This location may be on the same or different drive as the *Project Folder* or *Job Data* paths.
2. Create a share that you will point to in the interface.  
For example, if you use the following share path for your project folder:  
`\\Server\share\Projects`  
You may want to create the following share path:  
`\\Server\share\LawDrop_DropSpace`.
3. As an administrator, log into the console.
4. Open the *Management* page.
5. Click **System Configuration**.
6. Click **Project Defaults**.
7. Enter the path for the *LawDrop DropSpace Path*.
8. Click the check mark  to verify the path.
9. Click **Save**.

## Configuring the System To Share LawDrop Files with External Users

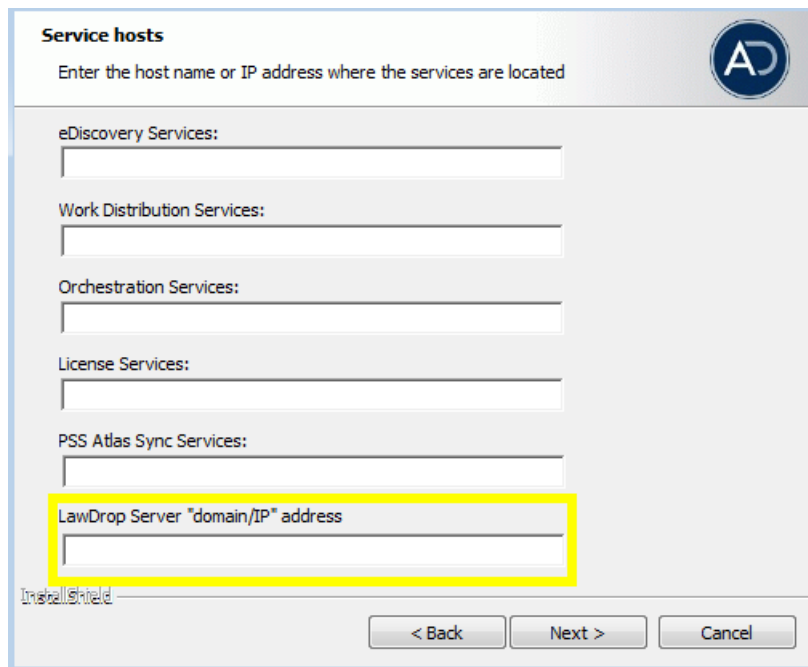
It is possible to share files and folders with users that are external to the application. This is done by providing the email address of the external user in the Share dialog. An email is then sent to the external user and there is an HTML link to the shared files.

In order for this to work properly, the following must be configured properly:

- The Email Server must be configured correctly. This allows the application to send emails. See [Configuring the Email Notification Server](#) on page 81.
- The location of the LawDrop server must be configured correctly in the AdgWindowsServiceHost.exe.config file. See [Configuring the AdgWindowsServiceHost.exe.config File](#) below.

## Configuring the AdgWindowsServiceHost.exe.config File

When you installed the application, you had the opportunity to configure the LawDrop Server domain/IP address.



By default, a value of “https://localhost/adg/map/web” is used.

In order for the external sharing to work, the “localhost” value must be changed to the actual server name or IP address of the server running MAP.

If you did not change the localhost setting to the actual server name or IP address, you may change the setting in a config file.

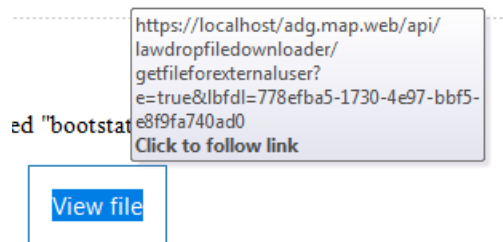
### To verify or change the setting

1. On the server running MAP, navigate to and open in a text editor the following file:  
Program Files\AccessData\Common\FTK\Business Services\AdgWindowsServiceHost.exe.config

2. In the config file, find "LawboxFileDownloadUrlBase".  
`<add key="LawboxFileDownloadUrlBase" value="https://localhost/ADG.MAP.Web..."`
3. Verify or change the value `localhost` to your server domain name or IP address of the server running MAP.  
 For example, `value="https://10.10.128.220/ADG.MAP.Web..."`
4. If you change the value, in the computer Services, you must restart the AccessData Business Services Common.

## Troubleshooting Sharing with External Users

- When you share a file or folder with an external user, the user should get an email from the application server entitled New LawDrop Share.
  - If the user never receives the email, verify that email notifications for the application server are working.  
 See [Configuring the Email Notification Server](#) on page 81.  
 You can try other email notifications, such as LitHolds or other email notification features.
- In the email, there is a link to **View file**.
  - If the link does not work, hover your mouse over the *View file* link and look at the URL.



If the link shows a URL with `localhost`, when you click the link, you will get the following:



## This page can't be displayed

- Make sure the web address `https://localhost` is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

[Fix connection problems](#)

**To fix this, you must do the following:**

1. Follow the steps listed in [Configuring the AdgWindowsServiceHost.exe.config File](#) on page 505
2. Re-send the email through the Share dialog.  
The link in the email must contain the updated path that is not localhost.



# Chapter 44

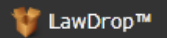
## Using LawDrop™

---

### Getting Started with LawDrop

All application users can access the LawDrop page.

#### To access LawDrop

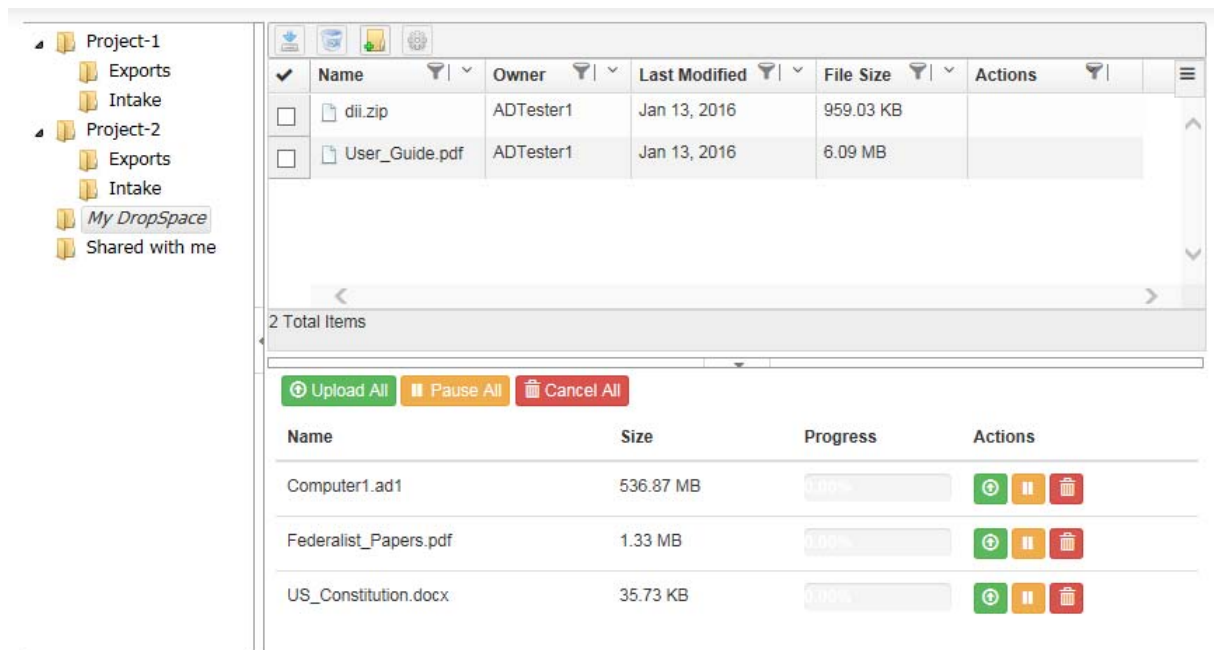
1. Log in to the application with your credentials.
2. Click the LawDrop™ tab .

If LawDrop is not configured properly, you will see the following error:

*The default path for user's DropSpace folder is not set. Please the default path or contact your System Administrator.*

See *Configuring the System for Using LawDrop*.

3. The LawDrop page is displayed.

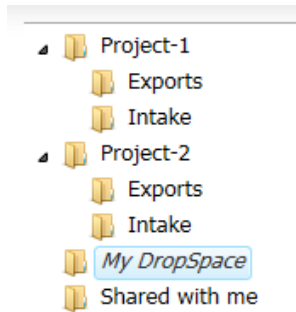


The screenshot displays the LawDrop interface. On the left, a navigation pane shows a tree structure with folders: Project-1 (Exports, Intake), Project-2 (Exports, Intake), My DropSpace, and Shared with me. The main area features a table with columns: Name, Owner, Last Modified, File Size, and Actions. Two items are listed: 'dii.zip' (959.03 KB) and 'User\_Guide.pdf' (6.09 MB), both owned by 'ADTester1' and last modified on 'Jan 13, 2016'. Below the table, a status bar indicates '2 Total Items'. At the bottom, there are three buttons: 'Upload All' (green), 'Pause All' (orange), and 'Cancel All' (red). Below these buttons is another table with columns: Name, Size, Progress, and Actions. Three items are listed, all with 0.00% progress: 'Computer1.ad1' (536.87 MB), 'Federalist\_Papers.pdf' (1.33 MB), and 'US\_Constitution.docx' (35.73 KB). Each item has a set of three action icons: a green play button, an orange pause button, and a red trash can icon.

## About the LawDrop Page

The LawDrop page has several elements.

### About the Folder List



On the left side of the LawDrop is the folder list. In the folder list, all users see the following folders:

- *My DropSpace* - This is where you can upload and organize files.  
You can create sub-folders under this folder. This is a private folder. You only see the files that you uploaded in the *My DropSpace* folder. You can share files that you have uploaded with other users.
- *Shared with me* - If other users share files from their *My DropSpace* folder with you, this is where you see those files.  
You cannot create sub-folders under this folder, but if other users have created sub-folders for their shared files, you will see them.  
You cannot upload or copy files to this folder.










In the folder list, you may also see the following:

- Project folders - If you have permissions to see any projects on the *Home* page, you will also see a folder for each of those projects in LawDrop.  
Under each project folder are two sub-folders:
  - *Intake* - You can upload and organize files for a project in the *Intake* folder.  
You can create sub-folders under this folder.  
Every file you upload to an *Intake* folder is private unless you share it.  
See [About Sharing Files and Folders](#) on page 518.  
If another user has shared a file from a project *Intake* folder with you, you will see it in the same folder.  
If you have project administrator permissions, you can add and process files from an *Intake* folder into a project. (You cannot add files to a project directly from the *My DropSpace* folder. You must first copy it to a project *Intake* folder.)  
See [Adding Evidence to Projects Using LawDrop](#) on page 521.
  - *Exports* - If an export is performed in a project and saved to LawDrop, they are saved here. You can see and download exported files.  
See [Exporting Files to LawDrop](#) on page 523.  
Important: Only those who have permissions to view export sets and production sets in Review can see the exported files in LawDrop. (For example, Admin and Admin Reviewer, or if you created the export set).  
You cannot upload files to the project *Exports* folder.

## About the File Queue

You can add files to LawDrop by dragging and dropping files onto the LawDrop page. When you drag a file to LawDrop, the file queue appears at the bottom of the LawDrop page. The file queue displays a list of files and their upload status. You can show or hide the file queue.

Upload All Pause All Cancel All

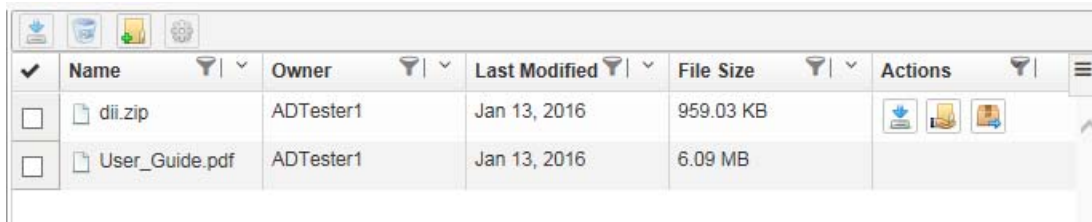
Name	Size	Progress	Actions
Computer1.ad1	536.87 MB	53.34%	  
Federalist_Papers.pdf	1.33 MB	0.00%	  
US_Constitution.docx	35.73 KB	0.00%	  




See [Dropping and Uploading Files to LawDrop](#) on page 512.

See [Viewing and Managing Uploaded Files](#) on page 514.

## About the Item List

After you have uploaded files to LawDrop, they are displayed in the Item List.



	Name	Owner	Last Modified	File Size	Actions
<input type="checkbox"/>	dii.zip	ADTester1	Jan 13, 2016	959.03 KB	  
<input type="checkbox"/>	User_Guide.pdf	ADTester1	Jan 13, 2016	6.09 MB	

The item list displays the items that are in the currently selected folder in the folder list. You can also perform actions on folders and files.

See [Using the Item List Grid](#) on page 514.

# Creating and Deleting Sub-Folders in LawDrop

When you add files to LawDrop, you can upload them to one of the following:

- The *My DropSpace* folder
- A project *Intake* folder (if you have permissions to the project)

To help organize files that you upload, you can create sub-folders in either location. You can create multiple levels of sub-folders.

You can upload files to the root of the folder or to a sub-folder. You can also copy and move files from one folder or sub-folder to another.



See [Moving and Copying Uploaded Items](#) on page 515.

You can also delete sub-folders that you create in the *My DropSpace* folder.

## To create a sub-folder

1. Open LawDrop.
2. In the folder list, click a folder, such as *My DropSpace* or a project *Intake* folder.
3. Do one of the following:
  - In the tool bar, click  *New Folder*.
  - Right-click and click  *New Folder*.
4. Enter a folder name.
5. Click Create.

## To delete a sub-folder

1. In the *My DropSpace* folder list, click the sub folder that you want to delete.
2. Do one of the following:
  - In the tool bar, click  *Delete*.
  - Right-click and click  *Delete* .
3. Confirm the deletion.

# Dropping and Uploading Files to LawDrop

## *About Dropping and Uploading Files*

You can add files to LawDrop by dragging and dropping files into a valid folder in LawDrop. When uploading files to LawDrop, files are uploaded using HTML. There are no set limits to the size of uploads, however, performance will be based on available bandwidth, network traffic, and the size of files.

You can upload files to the following LawDrop folders:

- *My DropSpace* and its sub-folders
- A project *Intake* folder that you have permissions for and its sub-folders

When you attempt to drop files to a LawDrop folder, if the folder is a valid folder, the color of the boundary turns green. If it is an invalid folder, it does not turn green. For example, invalid folders include the *Shared with me* folder, the root the project folder, and project *Exports* folder.

Uploading files is a two-step process:

1. You drop files onto a valid folder and the files are placed in the file upload queue.
2. You upload files from the queue into the folder.

During the upload, one file is uploaded at a time. File data is chunked into 1 MB chunks, and four chunks are uploaded at a time. The chunks are uploaded to the server, then when the chunks are complete, they are saved as the original file in the designated folder. If you lose your connection to the server during the upload, you simply drop the file again to the queue and upload it. However, it will resume from previous spot when connection was lost as it maintains the previous chunks that were uploaded.

## *About Dropping and Uploading Folders*

Internet Explorer does not support dropping and uploading folders, only files. However, you may want to add and process a complete folder using the *Add Evidence Wizard*. As a work-around, uploading a folder requires a four-step process:

1. Create a .ZIP file of the folder that you want to upload.
2. Drag the .ZIP file onto a valid folder.
3. Upload the .ZIP file.
4. Use a LawDrop action to extract the .ZIP into a folder.  
See [Action Icons](#) on page 517.

## *Dropping Files into the File Upload Queue*

**Important:** As a best practice, upload files to the *My DropSpace* folder and then copy files to a project *Intake* folder

### **To drop files into the File Upload Queue**

1. Open a File Explorer window with the files that you want to upload.
2. In the LawDrop folder list, click the folder that you want to upload files to.
3. Click and drag the files onto the LawDrop page.

4. If the destination is a valid folder, the border around the item list turns green.
5. Release the mouse button to drop the files.
6. The *file upload queue* is opened and the files are displayed in the queue.

## Uploading and Managing Files in the File Upload Queue

After you have dropped files in the *file upload queue*, you can do the following:

- Upload the files.
- Pause and resume the uploading of files
- Delete the files from the queue

You can perform actions on all files in the queue or on one individually.

While a file is uploading, an upload progress is displayed.

After a file has completed uploading, the file is removed from the queue.

If you upload the same file to a folder more than once, the later files will be appended with a (1), (2), and so on.

If files are currently uploading, and you click to go to a different a different place in the application, such as the **Home** page, you are warned that leaving LawDrop will cancel all the uploads.

⬆️ Upload All
⏸️ Pause All
🗑️ Cancel All

Name	Size	Progress	Actions
Computer1.ad1	536.87 MB	<div style="width: 53.34%; background-color: #28a745; height: 10px;"></div> 53.34%	<span style="border: 1px dashed green; padding: 2px;">⬆️</span> <span style="background-color: #ffc107; padding: 2px;">⏸️</span> <span style="background-color: #dc3545; padding: 2px;">🗑️</span>
Federalist_Papers.pdf	1.33 MB	<div style="width: 0%; background-color: #6c757d; height: 10px;"></div> 0.00%	<span style="background-color: #28a745; padding: 2px;">⬆️</span> <span style="background-color: #ffc107; padding: 2px;">⏸️</span> <span style="background-color: #dc3545; padding: 2px;">🗑️</span>
US_Constitution.docx	35.73 KB	<div style="width: 0%; background-color: #6c757d; height: 10px;"></div> 0.00%	<span style="background-color: #28a745; padding: 2px;">⬆️</span> <span style="background-color: #ffc107; padding: 2px;">⏸️</span> <span style="background-color: #dc3545; padding: 2px;">🗑️</span>

### To upload files in the queue

- ❖ Click either **Upload All** or the single *upload* icon.

---

**Note:** If you have more than one file in the queue and upload a single file, after that file is uploaded, all other files in the queue will then be automatically uploaded. If you want to upload only one file, do the following: click **Pause All**, then upload the single file.

---

### To pause the uploading of files in the queue

- ❖ Click either **Pause All** or the single *pause* icon.  
The upload status indicator turns orange.  
You can either resume the upload or cancel it.

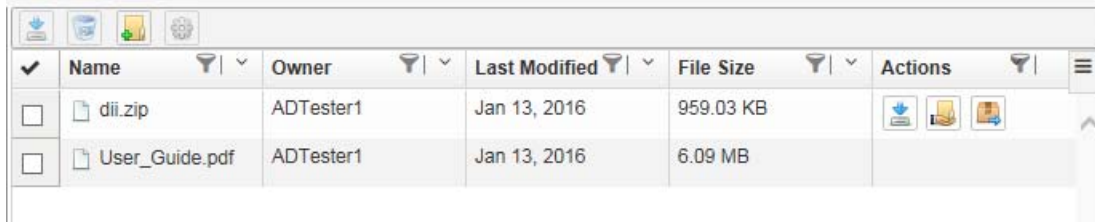
### To cancel or delete files in the queue




- ❖ Click either **Cancel All** or the single *delete* icon.

# Viewing and Managing Uploaded Files

## Using the Item List Grid

After you have uploaded files to LawDrop, they are displayed in the Item List.



	Name	Owner	Last Modified	File Size	Actions
<input type="checkbox"/>	dli.zip	ADTester1	Jan 13, 2016	959.03 KB	  
<input type="checkbox"/>	User_Guide.pdf	ADTester1	Jan 13, 2016	6.09 MB	

The item list displays the items that are in the currently selected folder in the folder list.


By default, the item list displays the following columns:

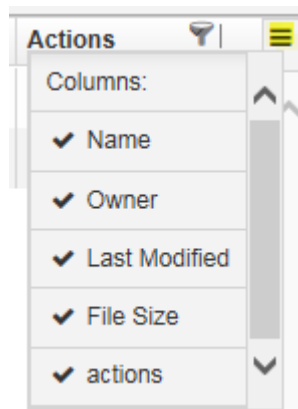
- *Name* - The name of the file or folder.
- *Owner* - The login name of the user who uploaded the file.
- *Last Modified* - The date that the file was last modified.
- *File Size* - The size of the file.
- *Actions* - Displays icons for actions that you can perform on that one item.

You can do the following with the item list grid:

- Select which columns to display.
- Sort the item list by a column.
- Filter the item list by one or more columns. (Not currently working)
- See available actions for individual items in the list.

### To select which columns to display

1. In the item list, click  .



2. Select the columns to display

### To sort or filter the list by a column

- ❖ Click the sort by or filter icon.

**Important:** The filter action is currently not working.

## Moving and Copying Uploaded Items

You can use folders to organize uploaded files. You can also use a project *Intake* folder to organize or stage files that you want to add to a project. See [Adding Evidence to Projects Using LawDrop](#) on page 521.

To help you organize files and folders, you can drag items from one folder to another. Depending on where you are dragging items, the item will either be copied or moved:

Note the following scenarios:

- **Within *My DropSpace*:** If both the source and the destination of the drag is within *My DropSpace*, the file or folder is moved.

Examples:

- Suppose under your *My DropSpace*, you have a sub-folder named *MDS1*. If you have a file in your *My DropSpace* and drag it to *MDS1*, it will move the file.
- Suppose under your *My DropSpace*, you have two sub-folders named *MDS1* and *MDS2*. If you have a file in *MDS1* and drag it to *MDS2*, it will move the file.

---

**Note:** If you move a file that has been shared, the sharing is removed.

---

- **Outside of *My DropSpace*:** If either the source or destination of the drag is outside of *My DropSpace*, the file or folder is copied.

Examples:

- If you drag a file in *My DropSpace* to a project *Intake* folder, the file will be copied.
- If you drag a folder in *Shared with me* to a project *Intake* folder, the folder will be copied.
- If you drag a folder in *Shared with me* to *My DropSpace*, the folder will be copied.
- If you drag a file in a project *Intake* folder to a different folder, the file will be copied.

---

**Note:** If you drag and copy a file or folder from *Shared with me*, the copy will list you as the owner.

---

If you copy a file to a folder more than once, the later files will be appended with a (1), (2), and so on.

Note the following limitations:

- When dragging items to a project folder, you must drag it to the *Intake* sub-folder. You cannot drag items to the root of a project folder or to a project's *Exports* sub-folder.
- You cannot drag items from a project's *Exports* sub-folder. (If needed you can download). See [Viewing Exported Files in LawDrop](#) on page 523.
- You cannot drag items to the *Shared with me* folder. Items will only appear there after they have been shared by another user. See [Sharing Files and Folders](#) on page 518.



# Performing Actions on LawDrop Items

## Using the Tool Bar and Action Icons





You can use the action bar or action icons to perform actions on items in the list.

### Tool Bar

Using the tool bar on the top of the action list, you can select one or more files or folders and then perform the following actions: (some actions are not always available)



#### Law Drop Tool Bar





Download 	<p>From within LawDrop, you cannot view the contents of files. For example, you cannot view the contents of an uploaded DOCX file. To view a file, you can download a file or folder then view it.</p> <p>When you download a file or folder, they are downloaded as .ZIP files.</p>
Delete 	<p>In <i>MyDropSpace</i>, you can delete files that you uploaded or sub-folders that you created.</p> <p>You cannot delete the following files or folders:</p> <ul style="list-style-type: none"><li>• Items shared with you in the <i>Shared with Me</i> folder.</li><li>• Items shared with you in project <i>Intake</i> folders.</li><li>• Items in project <i>Export</i> folders.</li></ul> <p>See <a href="#">Creating and Deleting Sub-Folders in LawDrop</a> on page 511.</p> <p><b>Note:</b> Files that have been processed or imported are no longer displayed in the LawDrop project Intake folder.</p>
New folder 	<p>You can add sub-folders. (<i>My DropSpace</i> and project <i>Intake</i> folders only. Not supported in <i>Shared with Me</i> or project <i>Export</i> folders.)</p> <p>See <a href="#">Creating and Deleting Sub-Folders in LawDrop</a> on page 511.</p>
Add Evidence 	<p>If you have project admin permissions you can select files or folders and add them as evidence to a project. (Project <i>Intake</i> folders only.)</p> <p>See <a href="#">Adding Evidence to Projects Using LawDrop</a> on page 521.</p>

## Action Icons

Using the action icons in the Actions column of the action list, you can perform the following actions on one single folder or file at a time: (some actions are not always available)



### Law Drop Action Icons

Download 	<p>From within LawDrop, you cannot view the contents of files. For example, you cannot view the contents of an uploaded DOCX file. To view a file, you can download a file or folder then view it.</p> <p>When you download a file or folder, they are downloaded as .ZIP files.</p>
Share 	<p>You can share a file or folder with another user.</p> <p>(<i>My DropSpace</i> and project <i>Intake</i> folders only. Not supported in <i>Shared with Me</i> or project <i>Export</i> folders.)</p> <p>See <a href="#">Sharing Files and Folders</a> on page 518.</p>
Extract 	<p>You can extract an uploaded zip file.</p> <p>(<i>My DropSpace</i> and project <i>Intake</i> folders only. Not supported in <i>Shared with Me</i> or project <i>Export</i> folders.)</p> <p>See <a href="#">About Dropping and Uploading Folders</a> on page 512.</p>
Import 	<p>You can import files as evidence. If you have project admin permissions you can select files and add them as evidence using import.</p> <p>(Project <i>Intake</i> folders only.)</p> <p>See <a href="#">Importing Data</a> on page 522.</p>

# Sharing Files and Folders

## About Sharing Files and Folders

Any files or folders that you upload are private. Even files that you upload to a project *Intake* folder are private to you even if additional people are working in the same project. To let other people see and access files that you upload, you can share them.

You can share individual files or folders. If you share folders, others will see all of the contents of that folder.

How and where others see items that you shared depend on multiple scenarios:

- Sharing with other Summation or eDiscovery application users:
  - Files and folders in *My DropSpace*
    - You can share items in your *My DropSpace* with any other application user.
    - When you share items in your *My DropSpace* folder, others see the items in their LawDrop *Shared with me* folder.
    - When someone else share items in their *My DropSpace* folder with you, you see the files in your *Shared with me* folder. If they have files under sub-folders, you will see them in the same hierarchy.
  - Files and folders in project folders
    - If you share items in an *Intake* folder, others will see them in the same folder.
    - For others to see shared items in an *Intake* folder, they must be associated to the project. (There are no specific project-level permissions required, just that they are associated to the project.)
    - You cannot share items in the *Exports* folder.  
Instead, you can download the exported files. You can then re-upload them to your *My DropSpace* and share them or you can make them available using a network share or email. See [Viewing Exported Files in LawDrop](#) on page 523.
- Sharing with external users
  - My DropSpace - If you share items in your *My DropSpace* folder with an external user, the user receives an email with a link to the files.
  - Project Folders - Not currently supported.

You can only share files that you uploaded (that you are the owner of). You cannot share files that were shared with you. However, you can copy the item and then share the copied items.


You cannot delete files that were shared with you.

If you share a file or folder that is nested under other sub-folders, the person will see the hierarchy of folders. However, they will only see files in the folder that was shared, not any folders higher.

## Sharing Files and Folders with other Application Users

You can share one file or one sub-folder at a time.

### To share files and folders with application users

1. Go to the LawDrop folder list and open the parent folder of the item that you want to share.
2. In the item list, for the sub-folder or file that you share, in the far right column, click the share  icon.

3. In the *Shared options* dialog, click in the *Invite more people* field.
4. Type the username of the person you want to share with.  
Note the following:
  - After typing the first three letters, any matches with application users will be displayed.
  - If you are using a multi-tenant environment, type the name of your environment first, and then select the username.
5. Click the name that you want to add.
6. Click **Add**.  
The name is added to a list in the dialog. The first letter of the username is shown in a circle.
7. If desired, add additional user names.
8. When completed, click **Done**.

## Sharing Files and Folders with External People

You can share files or folders with external people. To do this, you enter the person's email address and the person receives an email. The email includes a link to files on the server. When the person clicks the link, the ZIP file with the shared items is automatically download.

You can share one file or one sub-folder at a time.


---

**Note:** You can only share files externally from your *My DropSpace* folder. Sharing from an *InTake* folder to an external user is not supported.

---

There are settings that must be configured correctly in order for the email to work correctly. See [Configuring the System To Share LawDrop Files with External Users](#) on page 505.


### To share files and folders with external people

1. Go to your *My DropSpace* folder.
2. In the item list, for the sub-folder or file that you share, in the far right column, click the share  icon.
3. In the *Shared options* dialog, click in the *Invite more people* field.
4. Type the email address of the person you want to share with.  
Note that the name is notated with (external user).
5. Click the name that you want to add.
6. Click **Add**.  
The name is added to a list in the dialog. The first letter of the username is shown in a circle.
7. If desired, add additional user names.
8. When completed, click **Done**.
9. An email is sent to the user.
10. If needed, you can re-send the email.

## Unsharing Files and Folders

You can unshare files and folders from a specific user or from all users. This will cause the files or folders to no longer be visible to others.

### To unshare files and folders

1. Go to the LawDrop folder list and open the parent folder of the item that you want to unshare.
2. In the item list, for the sub-folder or file that you unshare, in the far right column, click the share icon. 
3. In the *Shared options* dialog, do one of the following:
  - To unshare a file or folder with a specific user, click the X on the far right of the user list.
  - To unshare a file or folder with all users, click **Unshare folder** or **Unshare file**.

# Adding Evidence to Projects Using LawDrop

## *About Adding Evidence to Projects Using LawDrop*

From LawDrop, you can add evidence in similar ways that you can use on the Home page:

- [Adding Evidence Using the Add Evidence Wizard](#) on page 521
- [Importing Data](#) on page 522

---

**Note:** If you are using Summation in a sub-admin environment, you cannot add evidence to a project from the Project List on the Home page. You can only add evidence to a project from LawDrop.

---

You can only add evidence to a project from the project *Intake* folder. If you want to add a file or folder that you have uploaded to your *My DropSpace*, you can drag and copy it to an *Intake* folder.

You can delete files from a project Intake folder that have not yet been processed or imported. Files that have been processed or imported are no longer displayed in the LawDrop project *Intake* folder.

See [Moving and Copying Uploaded Items](#) on page 515.

**Important:** Only those who have administrator permissions to the project can add files to a project.

## Adding Evidence Using the Add Evidence Wizard

Users with project administrator permissions can add files or folders to a project from LawDrop. When items are added, the *Add Evidence Wizard* is opened and you complete the wizard.

See [Using the Evidence Wizard](#) on page 376.


Depending on the items that you select to add, you will have different options available in the *Add Evidence Wizard*.

Note the following scenarios for adding evidence:

- The *CSV Import* method for adding shares is not supported from within LawDrop. Any CSV file will be imported as a native file.
- When selecting items to add to a project, you can add either files or folders at one time, not both. For example, you can add two or more files at one time, but not a file and a folder. This is because in the *Add Evidence Wizard*, you must specify if you are adding files or folder.
- If you are adding loose files in AD1 or E01 format, add them without other types of files. In the wizard, the *Individual Files* and *Native Files* options are selected by default. You must change the Data Type from *Native Files* to *Evidence Images*.
- If you add one or more loose files of other formats, in the wizard, the *Individual Files* and *Native Files* options are selected by default and all other options are disabled.
- If you add one or more folders, in the wizard, the *Folder Import* and *Native Files* options are selected by default. If the folder contains AD1 or E01 files, you must change the Data Type from *Native Files* to *Evidence Images*.

### Adding evidence to a project

1. Go to the LawDrop folder list and open the parent folder of the item that you want to add.
2. In the LawDrop item list, select one or more files or one or more folders.

3. Click the *Add Evidence*  icon.
4. The *Add Evidence Wizard* is opened.  
The available options are based on the types of items selected.
5. Complete the wizard.  
See [Using the Evidence Wizard](#) on page 376.
6. To view the status, go to the *Evidence* tab on the *Home* page.  
See [Evidence Tab](#) on page 236.

## Importing Data

Users with project administrator permissions can import files to a project from LawDrop. When items are added, the *Import* wizard is opened and you complete the wizard.

See [Importing Evidence](#) on page 385.


From an *Intake* folder, you can import a file that is one the following formats:

- CSV
- DAT
- TXT
- DII

You can import the following types of load files:

- Concordance
- Generic
- Summation dii

### Importing evidence into a project

1. Go to the LawDrop folder list and open the parent folder of the item that you want to add.
2. In the LawDrop item list, mouse over the file you want to import.
3. In the *Actions* column, click the *Import*  icon.
4. The *Import* dialog is opened.
5. Select the import file type.  
For the Concordance image type selection, you must know the name of the associated OPT or LFP file. You can copy and paste the image name.
6. You cannot change the path.
7. Complete the dialog.  
See [Importing Evidence into a Project](#) on page 386.

**Important:** If you perform an import validation and find errors, you cannot edit the import file within LawDrop. You must edit the original files and re-drop them into LawDrop.

## Exporting Files to LawDrop

When you create an export, instead of selecting a file path, you can select to *Send to LawDrop*.



The screenshot shows a dialog box titled "Load File Export Options". At the top, there is a checkbox labeled "Send to LawDrop™" which is checked and highlighted in yellow. Below this, there is a text input field labeled "Export Path" containing the text "\\localhost\path". The input field is disabled, indicated by a light gray background.

When you export to LawDrop, the *Export Path* is disabled.

---

**Note:** If you are in a Summation sub-admin environment, you cannot use an export path. You can only export to LawDrop.

---

All other aspects of the export are completed as usual.

See [About Exporting Data](#) on page 257.

### *Viewing Exported Files in LawDrop*

After an export is complete, exported files are viewable in the project's Exports folder.

In order to view exported files, you must meet one of the following conditions:

- Be an administrator of the project
- Have *Admin Reviewer* permissions for the project
- Be the user who created the export

You can download exported files. Files are zipped and then downloaded. Be aware the exports can be quite large and may take some time to download. As a result, download only one export at a time.

At this time, you cannot share items in the *Exports* folder. Instead, you can download the exported files. You can then re-upload them to your *My DropSpace* and share them or you can make them available using a network share or email.



# Part 10

# Reference

- [Installing the AccessData Elasticsearch Windows Service](#) (page 525)
- [Using the Site Server](#) (page 528)
- [Installing the Windows Agent](#) (page 542)
- [Installing the Unix / Linux Agent](#) (page 550)
- [Installing the Mac Agent](#) (page 552)
- [Integrating with AccessData Forensics Products](#) (page 555)

## Chapter 45

# Installing the AccessData Elasticsearch Windows Service

---

## About the Elasticsearch Service

The AccessData Elasticsearch Windows Service is used by multiple features in multiple applications, including the following:

- KFF (Known File Filter) in all applications
- Visualization Geolocation in all applications

The AccessData Elasticsearch Windows Service uses the Elasticsearch open source search engine.

### *Prerequisites*

- For best results with eDiscovery products and AD Lab and Enterprise, you should install the AccessData Elasticsearch Windows Service on a dedicated computer that is different from the computer running the application that uses it.

For single-computer installations such as FTK, you can install the AccessData Elasticsearch Windows Service on the same computer as the application.

A single instance of an AccessData Elasticsearch Windows Service is usually sufficient to support multiple features. However, if your network is extensive, you may want to install the service on multiple computers on the network. Consult with support for the best configuration for your organization's network.

- You can install the AccessData Elasticsearch Windows Service on 32-bit or 64-bit computers.
- 16 GB of RAM or higher
- Microsoft .NET Framework 4  
To install the AccessData Elasticsearch Windows Service, Microsoft .NET Framework 4 is required. If you do not have .NET installed, it will be installed automatically.
- If you install the AccessData Elasticsearch Windows Service on a system that has not previously had an AccessData product installed upon it, you must add a registry key to the system in order for the service to install correctly.

# Installing the Elasticsearch Service

## Installing the Service

### To install the AccessData Elasticsearch Windows Service

1. Click the AccessData Elasticsearch Windows Service installer.  
It is available on the KFF Installation disc by clicking *autorun.exe*.
2. On the welcome page, click **Next**.
3. Accept the License Agreement and click **Next**.
4. If you do not have Java installed, a message is displayed stating that you must install Java and the installation will end. See [Prerequisites](#) on page 525.
5. If you have upgraded your Java, you will get a Path Mismatch dialog. This asks you if you want to change the path of the JAVA\_HOME variable to your new Java version. Click **Yes**.
6. On the *Destination Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.  
This is where the Elasticsearch folder with the Elasticsearch service is installed.
7. On the *Data Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.  
This is where the Elasticsearch data is stored.

---

**Note:** This folder may contain up to 10GB of data.

---

8. (For use with KFF) In the *User Credentials* dialog, you can configure credentials to access KFF Data files that you want to import if they exist on a different computer.  
This provides the credentials for the Elasticsearch service to use in order to access a network share with a user account that has permissions to the share.  
Enter the user name, the domain name, and the password. If the user account is local, do not enter any domain value, such as localhost. Leave it blank instead.
9. In the *Allow Remote Communication* dialog, you can scale Elasticsearch by adding more machines.  
(Optional) *Select Enable Remote Communication*.

---

**Note:** If *Enable Remote Communication* is selected, a firewall rule will be created to allow communication to the AccessData Elasticsearch Windows Service service for every IP address added to the IP Address field. If no IP addresses are listed, then ANY IP address will be able to access the AccessData Elasticsearch Windows Service.

---

Either leave blank or add machines and click **Next**.

10. Configure ports for Elasticsearch to use and click **Next**.
  - HTTP Port
  - Transport Port

You can use the default ports or specify your own.

Using the defaults, whenever you click *Next*, the system will determine if the ports are available. If one is in use, a new value will automatically be entered. Click **Next** again to verify the ports and continue.

11. The *Configuration 1* dialog contains the following fields:

- **Cluster name** - This field automatically populates with the system's name.
- **Node name** - This field automatically populates with the system's name.

---

**Note:** If installing the AccessData Elasticsearch Windows Service on more than one system, allow the first system to install with the system's name in the cluster and the node fields. In the second and subsequent systems, enter the first system's name in the cluster field, and in the node field, enter the name of the system to which you are installing.

---

- **Heap size** - This is the memory allocated for the AccessData Elasticsearch Windows Service. Normally you can accept the default value. For improved performance of the AccessData Elasticsearch Windows Service, increase the heap size.

12. The *Configuration 2* dialog contains the following options:

- **Discovery** - Selecting the default of *Multicast* allows the AccessData Elasticsearch Windows Service search to communicate across the network to other Elasticsearch services. If the network does not give permissions for the service to communicate this way, select *Unicast* and enter the IP address(es) of the server(s) that the AccessData Elasticsearch Windows Service is installed on in the *Unicast* host names field. Separate multiple addresses with commas.
- **Node** - The Master node receives requests, and can pass requests to subsequent data nodes. Select both Master node and Data node if this is the primary system on which the AccessData Elasticsearch Windows Service is installed. Select only Data node if this is a secondary system on which the AccessData Elasticsearch Windows Service is installed. Click **Next**.

13. In the next dialog, click **Install**.

14. If the service installs properly, a command line window appears briefly, stating that the service has installed properly.

15. At the next dialog, click **Finish**.

## *Troubleshooting the AccessData Elasticsearch Windows Service*

Once installed, the AccessData Elasticsearch Windows Service service should run without further assistance. If there are issues, go to `C:\Program Files\Elasticsearch\logs` to examine the logs for errors.

# Chapter 46

## Using the Site Server

---

### About Site Servers

You can use Site Servers to collect data that you gather from agent sources and network shares. Jobs for data sources can be initiated from the interface and sent down through the site server path to a group of agent sources. After jobs are completed, the resulting data can be stored on the Site Server and then replicated up to either Parent Site Servers or to the Work Manager. Site Server can support over 50,000 nodes.

Site Servers can help you do reduce the quantity of traffic that must be sent through the network. For example, instead of sending the same job 100 times to 100 computers over a low bandwidth connection, you can send the job once to a site server, and then the site server can pass the job on to each the computers. Likewise, instead of multiple computers reporting the data back to work manager, they can report it to the Site Server. The Site Server can gather the data and report it back up to the system.

The following are the types of Site Servers.

#### Site Sever types

Type	Description
Root	<p>Root Site Servers are the main collection point. Root Site Servers store data to be collected and then pass it upstream to the Work Manager. Each Root Site Server must be bound to a locally installed Work Manager.</p> <p>You can have a hierarchy of Site Servers where the Root Site Server is the parent and hands off jobs to child Site Servers. Root Site Servers are the final destination of data from multiple Children Site Servers before data is handed off to the Work Manager.</p> <p>Root Site Servers can also directly serve agent sources.</p>
Private	<p>Private Site Servers are used to support agent sources that are connected through the local intranet.</p> <p>A private site server can function as both a child and a parent.</p> <p>For example, a Private Site Server may function at a regional level. It could receive jobs from a Parent Root Site Server, and then pass jobs to a child site servers at each specific site.</p>
Private (protected)	<p>Protected Private Site Servers are used only in environments when, due to security issues, you don't want the child Site Server calling to the parent Site Server.</p>

## Site Server types

Type	Description
Public	<p>Public Site Servers are used to support agent sources that are not currently connected to the local intranet.</p> <p>Public Site Servers may not support Children Site Servers. They are able to receive data and hold it, but they are not able to transmit it.</p> <p>For example, if an agent source has been given an acquisition job, and then is disconnected from the intranet before the results of the job are collected, if the agent source later connects through the internet, then it can pass the data to public site server. The data on the public site server can then be collected by a parent Private or Root Site Server.</p>

## *Supported Hashing Algorithms*

The certificates used by the agent and site server can use either the SHA-1 or SHA-256 hashing algorithm. They do not require any “Key Usage” or other special fields.

# Before Installing a Site Server

Before you install the Site Server software, do the following on the Site Server computer:

- Determine which type of Site Server you want the computer to function as.  
Root Site Servers must be installed on the same computer as the Work Manager.  
Public and Private Site Servers must report to either a Parent Site Server or a Root Site Server.
- Install the .Net 4.0 software locally.
- Install a PostgreSQL database locally.
- Record the database's system password.
- Record the names and ports to use of any Parent or Children Site server that the computer will work with.
- If the Site Server will directly support agents, record the IP ranges of the agent sources that you want the Site Server to support.
- Copy your Public and Private certificates to a local destination on the computer.

## Installing a Site Server

You manually install the software on each Site Server computer.

### To Install a Site Server

1. On the computer where you want to install a Site Server, run the Site Server installation file.
2. In the *Welcome to the AccessData Site Server Setup Wizard* window, click **Next**.
3. In the *End-User License Agreement* window select **I accept the terms in the License Agreement**, and click **Next**.
4. In the *Destination Folder* window, specify where you want to install the Site Server application files. To browse to a specific destination folder, click **Change**.
5. In the *User Credentials* window you can configure credentials.  
If you are installing this computer as a child site server, you can configure a service that automatically communicates to the eDiscovery Server's response path without having to communicate through the parent site server. In order to do this, you must specify the credentials of an account name that exists on both the site server and the eDiscovery server. Use the Specific User Account option to set the credentials.  
Otherwise you can use the default Local System Account setting.
6. In the *Ready to install AccessData Site Server* window, click **Install**.
7. In the *Completed the AccessData Site Server Setup Wizard* window, click **Finish**.  
The *Site Server Configuration Utility* automatically opens. See [Site Server Configuration](#) (page 531)

# Site Server Configuration

The Site Server Configuration utility automatically opens after you install the Site Server software on the computer. If you need to access the Site Server Configuration utility, on the Site Server computer, click **Start > Programs > AccessData > Site Server > Site Server Configuration**.

## Site Server Configuration General Options

Category	Option	Description
<b>Type</b>		See <a href="#">About Site Servers</a> on page 528.
	<i>Root, Private, Private protected, Public</i>	
	<i>Friendly Name</i>	(Optional) Lets you provide a name (identifier) for the Site Server.
<b>Secure Communications</b>		The certificates used for communication between multiple Site Servers and between Site Servers and agents.
	<i>Private Certificate</i>	This is used to communicate with agents. Supported certificate types include PFX/PKCS12, ADP12, and PEM. Any format other than ADP12 will be automatically converted to P12. Agents must be installed with corresponding public cert (same root CA). See <a href="#">Agent Certs</a> on page 534.
	<i>Public Certificate</i>	This is used to communicate with clients and other Site Servers. This is the location of the public key certificate. The public key must be available on the local computer. Supported certificate types include CER, CRT, and P7B. The public key must be the top-level (CA) certificate. (If the format is P7B, it can include both the CA certificate and the leaf certificate). Client programs must be configured with corresponding private cert (signed by same root CA). See <a href="#">Agent Certs</a> on page 534.
<b>Database</b>		
	<i>System Password</i>	This is the system password for the locally installed PostgreSQL database.
	<i>Database Port</i>	The port for the database listener service. The default is port 5432. This port is configured at the time when the PostgreSQL database is installed.
<b>IP Configuration</b>		
	<i>Internal/FQDN</i>	(Public type only) This lets you specify an internal name of the Site Server computer. The is used for communications between multiple Site Servers. For example, server.company.local.
	<i>External/FQDN</i>	(Public type only) This lets you specify public facing resolvable name. The is used for communications between the Site Server and agents. For example, server.company.com.
	<i>Internet Protocol Version</i>	Lets you specify the following: IPv4, IPv6, or both.
	<i>Port</i>	The port used for the Site Server to communicate with other Site Servers or agents.



## Site Server Configuration General Options

Category	Option	Description
	Heartbeat Port	This option allows you to specify a different port for the heartbeat protocol to traverse. This allows the heartbeat to be reliable and respond more quickly. By specifying a different port for the heartbeat, you can ensure that the heartbeat does not clutter the jobs running through the Site Server.
	Client Port	(Root type only) This is the outbound port from which a Root Site Server communicates through to the Work Manager. The default port is 54321.
	Use Secure Client	(Root type only) This option encrypts data communications between the Root Site Server and the Work Manager. (Enabled by default) If this is unchecked, clients can connect to the Site Server instance without a cert. See <a href="#">Agent Certs</a> on page 534.
<b>Results</b>		This location is where data is stored before it is replicated up through the Site Server system to the Work Manager. You can use a local folder or a domain share.
	<i>Results Directory</i>	Enter either the local directory or the UNC path.
	<i>Share domain</i>	Lets you specify a domain and the credentials to access that domain.
<b>Site Server System</b>		
	<i>Parent Instance</i>	This option is used for Public and Private (child) Site Servers only. This option lets you define a parent server to replicate data up-stream to. You must provide a definition of the parent server and the port to access. You can replace the string "parent" with the computer name, IP address, DNS Alias, or IPv6 address.
	<i>Children Instances</i>	This option is used for Root and Private (parent) Site Servers only. This option lets you define child Site Servers from which data can be gathered from. You must provide a definition of the child servers and the ports to access. You can replace the string "child" with the computer name, IP address, DNS alias, or IPv6 address. You can add multiple children instances in this field by separating each with a comma character.
<b>Locality</b>		
	<i>Managed Subnet (Address(es))</i>	Every task/target can have a locality. You can also set a locality for the Site Server as well. If they match, then the Site Server will execute that task that is valid in a multiple Site Server environment. This option lets you define the range of agent computers the Site Server can interact with. This option requires CIDR notation. You can add multiple ranges by separating each with a comma character. You can configure multiple site servers to support overlapping ranges.
	<i>Default Domain</i>	
	<i>Locality</i>	
<b>Configuration</b>		This lets you configure communication settings.
	<i>Max Client Connections</i>	

## Site Server Configuration General Options

Category	Option	Description
	<i>Max Incoming Threads</i>	
	<i>Max Outgoing Threads</i>	
	<i>Max Event Threads</i>	
	<i>Replication Threads</i>	
	<i>Retry Count</i>	
	<i>Retry Delay (ms)</i>	
<b>Bandwidth Control</b>		This lets you configure communication settings.
	<i>___ bits/second in from SiteServer</i>	
	<i>___ bits/second out from SiteServer</i>	
	<i>___ bits/second in from Agent</i>	
	<i>___ bits/second out from Agent</i>	
<b>Logging Level</b>		
	<i>NONE</i>	Disable all logging.
	<i>ERROR</i>	
	<i>WARNING</i>	
	<i>DEBUG</i>	
	<i>TRACE</i>	
	<i>INFO</i>	
	<i>USER</i>	
	<i>AUDIT</i>	
	<i>ALL</i>	Includes all logging.

# Chapter 47

## Agent Certs

---

### About Certs

#### *Definitions*

- Agent – A service running on a target machine that will allow for remote collection of volatile, drive, and other data.
- Client – The program that submits jobs to and collects results from the Site Server. An example is the eDiscovery work manager service.
- Site Server System – A system that will allow the collection of data from a set of Agents.
- Site Server Instance – A service within the Site Server System that communicates with Agents and performs the tasks requested by the Client.
- Public Cert – A file with an X.509 certificate or cert chain. Must include the root CA X.509.
- Private Cert – A file with a private key and X.509 certificate signed by root CA.

#### *Where Certs are Used*

Certs are used for secure communication in the following instances:

- Between the Client program and Site Server (Optional)
- Between Site Server and agents (Required)
- Between two Site Server instances (Required)

#### *Cert requirements*

- In supported format (see sections below)
- SHA-1 or SHA-256 hashing algorithm are both supported
- Public Certs must include the root CA cert
- Neither Key Usage nor Extended Key Usage cert extensions are required; ignored if present

#### *Supported formats for Public Certs*

- Base64 encoded CER/CRT
- Binary DER encoded P7B

## Supported formats for Private Certs

- Unencrypted PEM
- ADP12
- PFX\*

\*The PFX/PKCS#12 format is not supported directly by Site Server or Clients. It must be converted to ADP12 or PEM before it can be used. See instructions in the Cert Conversion sections for more details.

## About Using Certs

The following table lists which certs are used and when:

Agents:	<ul style="list-style-type: none"><li>• Agents only use a Public Cert. It must be provided at install time.</li></ul>
Site Server	<ul style="list-style-type: none"><li>• Site Server certs are configured using the Site Server Config tool (SS_Config.exe).</li><li>• Site Server uses its Private Cert to communicate with agents.</li><li>• Site Server uses its Public Cert to communicate with Clients (if Use Secure Client is selected) and to communicate with other Site Server instances.</li></ul>
Client:	<ul style="list-style-type: none"><li>• Client programs use a Private Cert to communicate with Site Server instance. For the eDiscovery Work Manager, the path to the Private Cert must be entered into its config file.</li></ul>

## Configuring Site Server for User with Certs

The following figure illustrates how to configure the certs used by Site Server

See [Using the Site Server](#) on page 528.

The screenshot shows the 'Site Server Configuration' dialog box with the 'General' tab selected. The configuration is as follows:

- General:** Type: Root; Friendly Name: Phil's awesome SS root.
- Secure Communications:** Private Certificate: C:\extras\agent\_certs\communication\test256.pem.adp12; Public Certificate: C:\extras\agent\_certs\communication\test256.p7b.
- Database:** System Password: (empty); Database Port: 5432.
- IP Configuration:** Internal Addresses/FQDN: (empty); External Addresses/FQDN: (empty); Internet Protocol Version: Both; Port: 54545; Heartbeat Port: 54555; Client Port: 54321;  Use Secure Client.
- Results:** Results Directory or unc path: c:\SiteServer\Results; Results share domain: (empty); Results share username: (empty); Results share password: (empty).
- Site Server System:** Parent Instance: parent.port; Children Instances: (empty).
- Locality:**  Default Domain; Managed Subnet Address(es): 192.168.8.0/24,10.10.0.0/16; Locality (optional): (empty).
- Configuration:** Max Client Connections: 10; Replication Threads: 5; Max Incoming Threads: 50; Retry Count: 5; Max Outgoing Threads: 50; Retry Delay (ms): 100; Max Event Threads: 50.
- Bandwidth Control:**  0 bits/second in from SiteServer;  0 bits/second out to SiteServer;  0 bits/second in from Agent;  0 bits/second out to Agent.
- Logging Level:** ALL.

Annotations in red text with arrows pointing to specific fields:

- Agents must be installed with corresponding public cert (same root CA). (Points to Public Certificate field)
- Client programs must be configured with corresponding private cert (signed by same root CA). (Points to Private Certificate field)
- If this is unchecked, Clients can connect to this SS instance without a cert. (Points to Use Secure Client checkbox)

Buttons: Apply, Close

# Creating Certs

Examples are given in following sections for how to create your own certs. These are just examples and your situation and needs may be different. The examples show how to create certs using OpenSSL. As a result, you must first obtain OpenSSL.

## *Install OpenSSL*

### **Installing OpenSSL on Windows**

The OpenSSL project does not distribute binaries for Windows, and does not officially recommend any specific binary distributions. Therefore, it is usually safer to use OpenSSL on Linux, obtaining it from your official distro repository. If you still would like to use Windows, an informal list of third party binary distributions can be found here: <https://wiki.openssl.org/index.php/Binaries>

- Download and extract files or run installer. (Use at your own risk.)
- After installing you should have a folder that contains at least openssl.exe, libeay32.dll, and ssleay32.dll.
- Follow steps below to configure OpenSSL (openssl.cnf)

### **Installing OpenSSL on Debian Linux**

- Run this command from a terminal window: `sudo apt-get install openssl`

### **Installing OpenSSL on RedHat Linux**

- Run this command from a terminal window: `sudo yum install openssl`

## Configure OpenSSL

This step is required if you wish to establish yourself as a Root CA, which you will want to do unless someone else is performing the role of CA.

Download the example openssl.cnf from here and modify as desired: <ftp://ftp.binarytool.com/pub/linux/ssl/openssl.cnf>

Alternatively, especially on Linux, you may have an existing openssl.cnf (e.g., at /etc/ssl/openssl.cnf) that already suits your needs. Take special note of the "dir" variable in your openssl.cnf. It may be something like "./demoCA". You may need to adjust your commands below slightly depending on this variable.

Change to a directory where you want to store files associated with your CA and run these commands:

```
mkdir CA
```

```
cd CA
```

```
mkdir newcerts
```

```
mkdir private
```

```
echo 01 > serial
```

```
touch index.txt (on Windows, create an empty file named index.txt)
```

A more comprehensive guide for establishing yourself as a Root CA can be found here:

<http://www.eclectica.ca/howto/ssl-cert-howto.php/>

A simpler approach that does not require a Root CA would be to create a single self-signed cert and use this same cert everywhere, but this is not recommended as it is obviously not as secure.

## Creating Certs Using OpenSSL

### Generating the Root CA Self-signed Public Cert and Private Key

To generate the Root CA Self-signed Public Cert and Private Key, run this command:

```
openssl req -x509 -sha256 -newkey rsa:2048 -out ca.crt -keyout ca.key -days 3650
```

- Leave off `-sha256` if you want to use SHA-1 hashing algorithm.
- The `-days 3650` will make the cert valid for 10 years; change to another value if desired.
- add `-nodes` if you don't want to encrypt the ca private key (bad idea)

When prompted, enter desired passphrase (twice). Then follow the prompts to enter the Country Name, State, Organization, etc. You will probably want to include "Root" or "CA" somewhere in the Common Name.

The resulting `ca.crt` is the Public Cert that needs to be provided to agents during install and can also be used as the Public Cert for Site Server instances. The resulting `ca.key` should be kept private and secure.

You may run this command to combine private key with X.509 to create a Private Cert for the CA:

```
cat ca.crt ca.key > ca.pem
```

However, this step is not necessary unless you are taking shortcuts and want to use the CA certs for everything (less secure). Also, this pem file cannot be used directly unless you added `-nodes` above so it won't be encrypted, or you convert this PEM to ADP12 format.

### Generating a Public/Private Cert Pair

You can generate a Public/Private Cert Pair for use by a Site Server instance or a Client

Every Site Server instance and Client can and should use its own unique keypair. But all certs need to be signed by the root CA, and public certs need to include the CA X.509.

1. Create a CSR (certificate signing request).

```
openssl req -new -nodes -out site_server_1.csr -keyout site_server_1.key
```

The `-nodes` makes the PEM unencrypted; you may leave it off, but encrypted PEMs are not supported directly by Site Server or Client programs, so you will need to convert it to ADP12 format after.

(Note: SS\_Config will convert it to ADP12 for you).

Follow the prompts to enter the Country Name, State, Organization, and so on.

Use a Common Name that uniquely describes the specific Client or Site Server instance

2. Sign the CSR to create X.509 CRT.

(Depending on your `openssl.cnf`, you may need to run this command from the CA directory, or `demoCA` directory, or a parent directory).

```
openssl ca -config ./openssl.cnf -md sha256 -days 3650 -policy policy_match -keyfile ca.key  
-cert ca.crt -out site_server_1.crt -infile site_server_1.csr
```

- Leave off `-sha256` if you want to use SHA-1 hashing algorithm.
- The `-days 3650` will make the cert valid for 10 years; change it to some other value if desired.

Answer `y` when prompted to sign `y/n`.

Edit the resulting `site_server_1.crt` and remove all the lines before the

```
-----BEGIN CERTIFICATE-----.
```



3. Combine CA's X.509 with newly signed X.509 CRT to create a usable Public Cert.  
`openssl crl2pkcs7 -nocrl -outform DER -certfile site_server_1.crt -certfile ca.crt -out site_server_1.p7b`  
The `-outform DER` is very important; only P7B files in binary DER format are supported.
4. Combine private key and X.509 to create Private Cert:
  - Linux: `cat site_server_1.crt site_server_1.key > site_server_1.pem`
  - Windows: `copy /b site_server_1.crt + site_server_1.key site_server_1.pem`
5. At this point you may want to delete the CRT file (`site_server_1.crt`)

**Important:** This file is not usable as a Public Cert because it does not contain the CA cert. Only the `site_server_1.p7b` or the `ca.crt` are usable because they contain the CA cert. There is still a copy of the X.509 inside the `site_server_1.p7b` and the `site_server_1.pem`, so it is not lost.

The resulting `site_server_1.p7b` and `site_server_1.pem` are the Public Cert and Private Cert to be entered into the Site Server Config tool for a Site Server instance.

Or, in the case of a Client, if the files are named `client_1.crt` and `client_1.pem`, then the `client_1.pem` must be entered into the config file for the Client program.

## *Converting Certs using OpenSSL*

### **Converting a Private Cert from PFX to PEM (unencrypted) using openssl**

```
openssl pkcs12 -in cert.pfx -out test.pem -nodes
```

When prompted, enter the password of the PFX file; you may have to enter it more than once.

Then, using a text editor, edit the file and remove all lines outside of

```
-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.
```

For example, remove all lines such as Bag Attributes, Key Attributes, `subject=`, `issuer=`, etc.

### **Converting a Private Cert from PEM to PFX using openssl**

```
openssl pkcs12 -export -out cert.pfx -in cert.pem
```

When prompted for an export password, enter a chosen password; you may need to enter it twice. Do not leave the password empty; although this may appear to work, PKCS#12 requires private keys in the PKCS#12 container to be encrypted, so a PFX that does not conform to this is invalid and may not be supported.

## *Examining Certs using OpenSSL*

### **Print human-readable contents of a CRT/CER file**

`openssl x509 -in cert.crt -noout -text` (to view X.509)

### **Print human-readable contents of a PEM file**

`openssl x509 -in cert.pem -noout -text` (to view X.509)

`openssl rsa -in cert.pem -noout -text` (to view private key)

### **Print human-readable contents of a PFX/PKCS12 file**

Follow steps in previous section to convert PFX to PEM format, then print out contents of PEM using commands above.

## *Cert Conversion to ADP12 using Site Server Config*

You can convert a Private Cert from PFX or PEM format to ADP12 using the Site Server Config tool (SS\_Config.exe).

1. Enter the path into the Private Certificate text box and hit the Apply button.
2. SS\_Config will prompt for the password and then convert the file to ADP12 format.
3. Find the resulting .adp12 file on your file system in the same folder as the PEM or PFX file.

# Chapter 48

## Installing the Windows Agent

---

This chapter covers the manual installation of the agent in a Windows environment.

This chapter includes the following topics:

- See [Supported Hashing Algorithms](#) on page 542.
- See [Manually Installing the Windows Agent](#) on page 542.
- See [Using Your Own Certificates](#) on page 548.

## Supported Hashing Algorithms

The certificates used by agent and site server can use either the SHA-1 or SHA-256 hashing algorithm. These do not require any “Key Usage” or other special fields.

## Manually Installing the Windows Agent

Perform the following steps to manually install the Enterprise Agent in Windows:

- [Specific Instructions for eDiscovery](#) (page 542)
- [Specific Instructions for AD Enterprise](#) (page 543)
- [Installing the Agent](#) (page 544)
- [Configuring Execname and Servicename Values](#) (page 546)

### *Specific Instructions for eDiscovery*

Follow these instructions if installing the Windows agent for use in eDiscovery.

A certificate (both a public certificate and a private certificate) is required for secure communication with agents.

#### **Configuring the Work Manager for the private certificate to use with Site Server**

- 1.
2. Navigate to %\Program Files\AccessData\eDiscovery\Work Manager
3. In Notepad or some other text editor, open `Infrastructure.WorkExecutionServices.Host.exe.config`.
4. Go to the line:  
`<add key="SSAgentCertFile" value="path" />`

5. Enter the path of your file.
6. Go to the line:  
`<add key="SSCommunicationCertPath" value="path" />`
7. Enter the path of your file.
8. Save the file.

## Specific Instructions for AD Enterprise

Follow these instructions if installing the Windows agent for use in AD Enterprise.

## Preparing the AD Enterprise Agent Certificate

### About Enterprise Security Certificates:

When installing AccessData Enterprise *Examiner*, you need a security certificate. Enterprise Management Server creates Enterprise security certificates, the CRT public key and the PEM public and private key pair files. However, the Enterprise Configuration Management Tool now also accepts PKCS#12 certificates.

If you have a third-party certificate chain in the PKCS#12 format, the Enterprise Configuration Management Tool reads the PKCS#12 certificate and asks for the user password. The certificate is decrypted only long enough to gather the information necessary for the Enterprise installation, then re-encrypts the private key. The public key, regardless of source, must be in standard binary or base-64 encoding.

If the Agent is installed, or pushed, to the workstations using Enterprise, the certificate information will automatically be read from the Enterprise Configuration Management Tool. If the Agent is pushed out, the certificate information (paths and filenames) must be re-entered. The public certificate itself must be in an area of the network where it can be accessed by the Agent machine during installation, but does not need to be stored on the Agent machine.

In addition, the Agent uses only a public key. As long as that public key is in binary or base-64 format, it will automatically be read by the Agent. For more information, see [Using Your Own Certificates](#) (page 548).

### To prepare the certificate

1. Prepare the Agent Certificate.
2. Copy the needed certificate from the Management Server to your deployment location.  
Management Server creates certificates during the setup in:  
`[Drive]:\Program Files\AccessData\AccessData Management Server\certificates.`  
The certificate name is the `ManagementServer.crt`.
3. Copy `ManagementServer.crt` to a folder of your choice where it can be accessed while installing the Agent.

## Installing the Agent

### To install the Agent

1. Run `AccessDataAgent.msi` or `AccessDataAgent(64bit)` using `msiexec`.

**Note:** These .msi files are located in the `Program Files\AccessData\Forensic Toolkit\5.1\Bin\Agent\<x32 or x64>` folder after installation.

There are several command line parameters available to use with this .msi as documented below. Here is an example command line that will install with the defaults:

If `AccessDataAgent.msi` resides in the folder `C:\enterprise` and `ManagementServer.crt` resides in `[Drive]:\certificates`, type the following command line to install the agent with defaults:

```
msiexec /i [Drive]:\enterprise\AccessDataAgent.msi  
CER=[Drive]:\certificates\ManagementServer.crt.
```

The following table lists the command line options available for use with this `AccessDataAgent.msi`:

#### Command Line Options

Option	Action
<code>/i</code> (i or x required)	Specifies install.
<code>/x</code> (i or x required)	Specifies un-install.
<code>/qn</code> (optional)	Allows you to install in quiet mode with no user interaction.
<code>&lt;path and msi file name&gt;</code> (required)	If running from the folder where the .msi is located you do not have to include path, only the filename.
<code>CER=&lt;path and certificate file name&gt;</code> (required)	Specifies the certificate the agent uses. <i>Always include the path, regardless of location.</i>
<code>ALLUSERS=&lt;n&gt;</code>	Configures the installer to be available to all users. The default option varies per operating system. The options are: <ul style="list-style-type: none"><li>• <code>allusers=1</code> configures the installer to be available to all users.</li><li>• <code>allusers=0</code> configures the installer to be available to only the user who is installing the agent.</li></ul>
<code>INSTALLDIR=&lt;custom install path&gt;</code> (optional)	Allows you to change the install location from the default folder: <code>(C:\Program Files\AccessData\Agent)</code> .
<code>PORT=&lt;xxxx&gt;</code> (optional)	Allows you to change the port from the default port (3999).
<code>LIFETIME=&lt;d&gt;</code> (optional)	Allows you to configure the life cycle of the agent. The “d” value equals the Time To Live (TTL) measured in days. Adding a number preceded by a dash measures the TTL in minutes. For example: <code>&lt;-d&gt;</code> .
<code>CONNECTIONS=&lt;n&gt;</code>	Allows you to configure the number of maximum connections for the agent.
<code>STORESIZE=&lt;n&gt;</code>	Allows you to configure the size of the data store.
<code>TRANSIENT=1</code>	Allows you to configure the agent as a <i>Transient Agent</i> . Transient Agents have no protected storage and remove themselves when the agent machine is restarted.

## Command Line Options (Continued)

Option	Action
FOLDER_STORAGE=1	<p>Allows you to configure the agent as a <i>Persistent Agent</i>. Persistent Agents use a “local” file system based storage and not protected storage. Persistent Agents also remain on the agent machine after the machine is restarted.</p> <p>This allows for local logical disc space to store the results of Public Site Server jobs operating while the Agent is not on the WAN or can get to the Public Site Server.</p>
SERVICELESS=1	<p>Allows you to configure the agent to install with no protected storage and no installed service. The agent removes itself when the agent machine restarts or when the lifetime option expires, whichever comes first.</p>
PCD=<x > (optional)	<p><b>Enterprise Only:</b> Allows you to configure the Proxy Cycle Delay (PCD). The PCD is the time interval at which the agent attempts to connect to proxy to check if any work has been assigned. The PCD “x” value is measured in seconds. The default is 1200 (20 minutes).</p>
PROXY= (see example below) (optional) <PrimaryIP>,<SecondaryIP>:<Port >><PrimaryIP2>,<SecondaryIP2>: <Port2>	<p><b>Enterprise Only:</b> Allows you to configure a proxy-able agent. PrimaryIP should refer to the IP address to which the agent should try to communicate. (Usually this will be the internal private network IP of the proxy server.)</p> <p>The “SecondaryIP” should refer to the IP address to which the agent should try to connect when the attempts to connect to the “PrimaryIP” have failed. (Often this IP will represent the public IP of the proxy server.)</p> <p>PrimaryIP2 and SecondaryIP2 should refer to an additional proxy server address and is delimited by a tilde (~). Additional proxy servers can be added by following this same pattern.</p>
MAMA=<Site Server IP address:port>	<p><b>eDiscovery Only:</b> Allows you to configure the IP Address of the Site Server to which the agent reports.</p> <p>For example, 10.32.41.113:54545</p> <p>This parameter is used so that the Agents know which Site Server to check into for the first time. Additionally, after that first check-in, the Agents will learn the Site Servers that has its CIDR and check there next time. It will update based on movement of the physical IP of the node.</p>

## Command Line Options (Continued)

Option	Action
PUBSS=<public instance IP>	<p><b>eDiscovery Only:</b> Allows you to configure the agent to connect to a Public Site Server (PUBSS). See <a href="#">About Site Servers</a> on page 528.</p> <p>For example, pubss=192.192.192.192:5432</p> <p>The Agent in Public Site Server (PUBSS) mode will check-in to the original PUBSS value that was part of the install. After that first check-in, it will receive a list of other Public Site Servers in the DMZ and then ping around to find the closest/fastest connection.</p> <p>For example, if the user is in New York and a job starts there, and then the user goes to Los Angeles, the user will go from the NYC PUBSS to the LA PUBSS and the collection should resume and support interruption. This is all completed based on the resolution of the IP address for the target and assignment in a proper CIDR range on Site Server config.</p> <p>See <a href="#">Site Server Configuration</a> on page 531.</p> <p>This list will also get updated whenever it might change. This list comes from the Site Server configuration parameters you setup on your internal servers and not specifically some additional data entry. It comes from the virtue of having any Public Site Servers deployed.</p> <p>See <a href="#">MAMA=&lt;Site Server IP address:port&gt;</a> on page 545.</p>
PUBSS_DELAY=<seconds>	<p><b>eDiscovery Only:</b></p> <p>This can be used to delay the default check-in interval (30 minutes). You may want to alter this value if you have a lot of Agents on the PUBSS system.</p>

### Example Command Line Install

```
msiexec /i "C:\AgentInstall\AccessData Agent (64-bit).msi" cer="C:\AgentInstall\AccessData E1.crt"  
mama=10.10.35.32:54545 TRANSIENT=1 Persistent=1 Serviceless=1 lifetime=1 or lifetime=-5  
pubss=192.192.192.192 5432
```

## Configuring Execname and Servicename Values

The Execname and Servicename values change the names of the agent executable and agent service respectively. These values are added to the MSI using an MSI editor (such as [ORCA.exe](#) — a free MSI editor).

### Changing the Execname Value

#### To make changes to the execname value

1. Run Orca.EXE.
2. Click **File > Open**.

3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file. The default path is:  
[Drive]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\
4. In the *Tables* list, select **File...**
5. In the *FileName* column, double-click “u4jwdc7h.exe | agentcore.exe”.
  - 5a. Enter the filename to use for the agent core executable.

---

**Note:** Replace the entire string with the filename.

---

6. Press **Enter**.
7. Click **File > Save**.

---

**Note:** Do not close Orca if you are also changing the service name.

---

## Changing the Servicename Value

### To make changes to the Servicename value

If you closed Orca, begin with Step 1. Otherwise, skip to Step 4.

1. Run Orca.EXE.
2. Click **File > Open**.
3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file. The default path is:  
[Drive]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\
4. In the *Tables* list, select “ServiceControl”.
5. In the *Name* column, double-click “AgentService”.
  - 5a. Enter the name to use for the *AgentService* and press **Enter**.

---

**Note:** Use the same value in steps 5a, 7a and 8a.

---

6. In the *Tables* list, select “ServiceInstall”.
7. In the *Name* column, double-click “AgentService”.
  - 7a. Enter the name to use for the *AgentService* (use the same value entered in step 5a) and press **Enter**.
8. In the *DisplayName* column, double-click “AgentService”.
  - 8a. Enter the name to use for the *AgentService* (use the same value entered in steps 5a and 7a) and press **Enter**.
9. Click **File > Save**.
10. Click **File > Close**.



# Using Your Own Certificates

Use this information if you are using your own of the following certificates:

- PKCS#12: Standard certificate packaging to securely transfer public/private key pairs
- PKCS#7: Standard certificate package to store certificates for S/MIME encryption--used for storing sets of public key chains.

*Important:*

- A CER/CRT public certificate must be in Base64 format (not binary DER).
- A P7B public certificate must be in binary DER (not Base64) format.
- If using a P7B, make sure it includes the top-level certificate. (It may be easiest to just make sure it includes the full certificate path.)

## To export the public certificate when using a PFX (PKCS#12) key

1. Using the PKCS#12 provided by the Certificate Administrator, double-click PKCS#12 to open it.
2. Install the certificate into a local Microsoft certificate store by following the wizard supplied when you double-click the certificate file.
3. View the public certificate of the installed certificate by opening the local machine's certificate store. (This can be done with *Microsoft Management Console* or in *Internet Explorer* under **Tools > Internet Options > Content > Certificates**)
4. Find the bottom level certificate and double-click the certificate to view it.
5. Click the **Certification Path** tab to verify that the certificate has a full verification path, meaning that nothing is missing from the top of the chain to the bottom.
6. Click the **Details** tab and click **Copy to File**.
7. Click **Next** and click **Cryptographic Message Syntax Standard - PKCS #7 Certificates**.
8. Select **Include all certificates in the certificate path if possible**.
9. Click **Next** and enter a file export path.
10. Click **Next**.
11. Click **Finish**.
12. Double-click the exported PKCS#7 and verify that all of the public certificates in the chain are in the PKCS#7.

The exported file you created will be used as the certificate for the agent installation.

# Controlling Consumption of the CPU

You can edit a registry key that allows you to control what percentage of the CPU is used for the agent. This gives you the ability to throttle the CPU and insure that the agent does not consume all of the CPU available.

## To add a throttling registry key

1. In the Registry Editor, expand the `HKEY_LOCAL_MACHINE` hive and locate the `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared` folder.
2. Add a new **DWORD (32-bit) value** to the **Shared** folder. (`HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared\throttling`)
3. The data value of the **DWORD** should be the maximum percentage of the CPU allowed to be used by the module. For example, if you want the maximum percentage of the CPU used to be 25 percent, modify the **DWORD** data value and enter 25 in the *Edit DWORD* dialog. The value should be from 0-100. If the data value is left at 0, the CPU will not be throttled when the agent is started.
4. In the *Edit DWORD* dialog, select the **Decimal** radio button and click **OK**.
5. After applying the registry key changes, restart the agent service.

For more information on adding and editing registry keys, see Microsoft's documentation.

## Important Information

The following information is important to know about installing and executing an agent:

- The **ADMON** module does not run on low resource priority. The **ADMON** module must run on Normal priority or higher in order to maintain connection to the system drivers.

# Chapter 49

## Installing the Unix / Linux Agent

---

This chapter discusses the Unix Agent Installer. It includes the following topics:

- See [Installing The Enterprise Agent on Unix/Linux](#) on page 550.

### Installing The Enterprise Agent on Unix/Linux

The AccessData Agent is available for Unix-, Linux-, and Mac-based operating systems as well as for Windows. This appendix discusses the specific installation files to use for supported Unix and Linux platforms.

#### *Supported Platforms*

The Unix Agent Installer supports the following platforms:

##### Unix Agent Supported Platforms

Installer	OS
agent-rh5.sh or agent-rh5x64.sh	RedHat 5 (32- & 64-bit) SLED 11 (Suse Linux Enterprise Desktop) (32- & 64-bit) CentOS Enterprise 5 (32- & 64-bit) Ubuntu 9 (and newer) (64-bit)
agent-rh3.sh or agent-rh3x64.sh	RedHat 3 (32- & 64-bit) Novell Linux Desktop (NLD) 9 (32-bit) SLED 10 (Suse Linux Enterprise Desktop) (32- & 64-bit)
Be sure to use the correct installer file for your 32- or 64-bit architecture/OS)	

To install the Unix Agent

Execute the following command as root, and provide the appropriate information:

```
agent-<os>.sh <certpath> [-installpath] -i <installpath>]
```

where <os> is the operating system agent that is being used, and where <certpath> is the location of the public certificate to be used for identification, and where [-i | -installpath] indicates the directory to install the agent in.

This defaults to:  
/usr/AccessData/agent

### Enterprise Unix/Linux Agent Install Parameters and Options

Option	Result
-installpath, -i <installpath>	The destination path for installing the agent. Default: /usr/AccessData/agent/.
-lifetime, -l <lifetime>	The lifetime of the agent. Default: 0. If <lifetime> ==0, it will never uninstall itself. If <lifetime> >0 it is days before uninstall. If <lifetime> <0 it is in minutes before uninstall.
-port, -p <port>	The port the agent listens on. Default: 3999.
-connections, -c <connections>	The maximum number of concurrent connections allowed by the agent. Default is 10.
-size, -s <storage size>	The protected storage area size. Default is 16777216 (16 MB)

## Uninstallation

To uninstall the Unix Agent, execute the following command as root:  
# ./agent.sh -rf

## Configuration

The configuration file is located in the install path and is named **ADAgent.conf**. It supports the following parameters:

- **Port:** Port on which to listen for activity.
- **MinThreadCount:** Minimum number of threads to have ready, waiting for connections.
- **MaxThreadCount:** Maximum number of threads servicing connections.
- **CertificatePath:** Fully qualified network path or local path to the certificate. The installer, by default, puts the certificate in the installation path.

## Starting the Service

To start the Unix Agent service, execute the following command as root:  
/etc/init.d/adagentd start

## Stopping the Service

To stop the Unix Agent service, execute the following command as root:  
/etc/init.d/adagentd stop

# Chapter 50

## Installing the Mac Agent

---

This chapter discusses the Agent Installer for Apple Macintosh. It includes the following topics:

- See [Configuring the AccessData Agent installer](#) on page 552.
- See [Installing the Agent](#) on page 554.
- See [Uninstalling the Agent](#) on page 554.

### Configuring the AccessData Agent installer

The AccessData Agent requires an X.509 certificate in order to establish a secure network connection to the server or for AD Enterprise, the computer running *Examiner*. The package installer has been provided to aid in the distribution efforts of these certificates by allowing an Administrator to modify the AccessDataAgent package installer prior to installation of AccessData Agent software for Apple Macintosh. In addition to certificate distribution, the port used by the Agent can be configured.

The following instructions allow an Administrator to configure the AccessData Agent package installer.

#### *Bundling a Certificate*

The AccessData Agent installer requires that a certificate (or certificate tree) is bundled with the installer. The following is the sequence of steps that must be followed to bundle a certificate file into the installer.

1. Create a folder named **Configure**.
2. Create a single file, named **adagent.cert** that contains one or more X.509 certificates to be distributed to each installation of the Agent, and place it in the Configure folder.
3. Right-click the **AccessDataAgent** package installer file on the install disc, (`[Drive]:\Enterprise\Agents\agent-Mac.dmg`).
4. Select **Show Package Contents** popup menu item.
5. Drag the **Configure** folder from the Package Contents into the folder opened in Step 4 (alongside the **Contents** folder).

#### *Configuring the Port*

The **AccessDataAgent** installer allows an Administrator to (optionally) configure the port the Agent will use to communicate with an *Examiner* when installed. This is done by adding a file containing the port number to the **AccessDataAgent** package installer. The following is a set of instructions an Administrator will use to configure

the AccessData Agent package installer. To do so, complete Steps 1-5 under Bundling a Certificate, then continue with Step 1 here. If you do not need to do a custom configuration of the port, skip to Step 6 below.

1. Create a text file named `adagent.port` that contains the port number the Agent is to use; this file is to be distributed to each installation of the Agent.
2. Place the `adagent.port` file into the **Configure** folder (previously created to contain the X.509 certificate).
3. Right-click the `AccessDataAgent` package installer file.
4. Select **Show Package Contents** popup menu item.
5. Ensure that the **Configure** folder is located in the same folder opened in Step 4 (alongside the **Contents** folder).
6. Close the window.

---

**Note:** The installer will not run successfully if all of the above steps are not already completed. The folder and file names must be exactly as documented

---

## Additional Configuration Options

The Mac installer now supports the same settings as the Unix installer. Each setting should be added to the `.mpkg` file in a directory called **Configure**.

### Enterprise Mac Agent Configuration Options

Option	Result
- <code>adagent.cert</code>	Specifies the certificate file used for communication
- <code>adagent.port</code>	Specifies the port the agent will listen on. The setting should contain nothing more than a number. The default port number is 3999
- <code>adagent.lifetime</code>	Specifies the amount of time before the agent dissolves. Again the file should contain nothing more than a number. Same rules as for the Linux agent about sign and value. The default is 0.
- <code>adagent.connections</code>	Sets the maximum number of concurrent connections allowed by the agent. The file should contain only a number. The default is 10.
- <code>adagent.size</code>	Sets the protected storage area size. The file should contain only the number. The default is 16777216. (16 MB).

## Installing the Agent

When the certificate is bundled and the port configuration file is complete and saved, distribute the **AccessDataAgent** package installer to each target computer and run it locally.

## Uninstalling the Agent

The AccessData Agent can be uninstalled by double-clicking the uninstall utility located in **/Library/Application Support/AccessData**. You will be required to enter your password; you must have administration rights for the uninstall to complete correctly.

---

**Note:** The account must have a password assigned to it.

---

# Chapter 51

## Integrating with AccessData Forensics Products

---

Web-based products (Summation and eDiscovery) can work collaboratively with FTK-based forensics products, (FTK, Lab, FTK Pro, and Enterprise).

---

**Note:** For brevity, in this chapter, all FTK-based products will be referenced as FTK and Summation and eDiscovery applications will be referenced as Summation.

---

You can access the same project data on the same database to perform legal review and forensic examination simultaneously. The benefit of this compatibility is that FTK provides some features that are not available in the web-based products. For example, you can create projects in Summation and then open, review, and perform additional tasks in FTK and then continue your work in Summation.

Using FTK, you can do the following with Summation projects:

- Open and review a project
- Backup and restore a project
- Add and remove evidence
- Perform Additional Analysis after the initial processing
- Search, index, and label data
- View graphics and videos
- Export data

**Important:** For compatibility, the version of the web-based product and the version for FTK must be the same-- both must be 5.0.x or be 5.1.x. For example:

Summation 5.2.x must be used with FTK 5.2.x

Summation 5.5 must be used with FTK 5.5



# Installation

You can install FTK and Summation on either the same computer or on different computers. The key is that they share a common database. The database that the data is stored in is unified so that the data can be shared between products.

It is recommended that you install the web-based product first, configure the database, and then install FTK and point FTK to that database. The administrator account for the web-based product is the administrative account for the database for FTK.

When launching FTK and logging into the database, you use the administrator credentials from the web-based product.

**Important:** For compatibility, the version for Summation and the version for FTK must be the same.

**Important:** Note that FTK and Summation may use different versions of the processing engine. If this is the case there will be information in the *Release Notes*.

## Managing User Accounts and Permissions Between FTK and Summation/eDiscovery

You can create a user account in either product and then use that user name in the other product.

### Permissions

When users are assigned permissions in one application, such as Summation, the permissions of the user in FTK are not affected.

## Creating and Viewing Projects

Using either product, you can create projects and add evidence to that project. You can then use either product to open the project and perform tasks on the project data.

You can have users in each program reviewing the data at the same time.

### *Managing Evidence in FTK*

#### Adding Evidence using FTK

You can use FTK to add evidence to a project that was created in Summation. Reviewers in Summation can then review the new evidence. Using FTK, you can add live evidence and static evidence. When you add evidence, you can add image files (such as AD1, E01), individual files, physical drives, and logical drives.

**Important:** When you collect volatile data in FTK, you cannot see it in Summation.

## Processing Evidence using FTK

FTK provides processing options that are not available in Summation. You can utilize the processing abilities of FTK and then review the data in Summation/eDiscovery. You can do all processing in FTK or you can perform an Additional Analysis in FTK after an initial processing.

The following are examples of additional processing options that are available in FTK:

- Processing Profiles
- Known File Filter (KFF)
- Automatic File Decryption
- Create Thumbnails for Video
- Generate Common Video File
- Explicit Image Detection
- PhotoDNA
- Cerberus Analysis

When you create a project with specific processing options, those options are maintained when the project is viewed in the other product. (15940)

**Important:** If you create a project in Summation, process the evidence, then add more evidence using FTK, if you compare the JobInformation.log files, the processing options applied by FTK are different from Summation.

## Managing Evidence Groups in FTK and People in Summation

It is important to note that FTK does not use people, but rather has evidence groups. Evidence groups let you create and modify groups of evidence. In FTK, you can share groups of evidence with other projects, or make them specific to a single project.

When you create people in a project in Summation, and then look at the project in FTK, the people will be listed as evidence groups. The opposite is also true. If you create an evidence group in FTK, it will be listed as a person in Summation.

**Important:** When you use FTK to add data to an evidence group that was an existing Summation person, two child entries of the same person are created for the data. When you look at the person data in Summation, there will be two child objects under the person with the same name, one with Summation data and the other with FTK data.

## *Reviewing Evidence in FTK*

## Searching Evidence using FTK

You can use FTK to search evidence in Summation projects. The search capabilities in FTK are more robust than Summation. In FTK, you can perform an index search as well as a live search. Live search includes options such as text searching, pattern searching, and hexadecimal searching.

**Important:** Note the following issue:

- Issue: The search results counts for the same project may be different when viewed in the different products due to the way search options are executed in the respective products. For example:
  - Summation only search columns that are visible to the user. FTK will search columns that are not visible to a eDiscovery user.
  - Re-indexing the data will change the search results.
- Because of FTK's Live Search feature, FTK will return more search results hits than in Summation.

## Labeling Evidence Using FTK

After searching and identifying data in FTK, you can label the data and then review the project in Summation and see the labeled data. You can then perform additional review, culling, and export tasks.

## Viewing Labeled Evidence in FTK

When reviewing data in Summation, you can label data, and then that labeled data is viewable in FTK. This can be useful in workflow management. For example, when reviewing the data, you can label data indicating that it needs additional analysis. When the project is opened in FTK, the labeled data is visible.

## Exporting Data using FTK

You can review and cull data in Summation and then export the data from FTK using its export capabilities.

The following are examples of what you can export using FTK:

- Export files to an AD1 Image file
- Save file list information
- Export the contents of the project list to a word list
- Export hashes from a project
- Export search hits
- Export emails to PST or MSG

## Viewing Documents Groups and Review Sets in FTK

Important: In Summation, there are separate views and permissions defined for Document Groups and Review Sets. In FTK, Document Groups and Review Sets that were created in Summation are displayed within the Manage Labels dialog.

## *Reviewing FTK Data in Summation*

You can use the following review features in Summation to help manage the workflow of working with data that was added and processed using FTK.

- Review the data by reviewers in the Web console.
- Cull the data and get the desired data set.
- Export the data using Summation using its export capabilities.

## Known Issues with FTK Compatibility

See the product's and FTK Release Notes for a list of known issues with FTK Compatibility.