Perceptive Content

Manage Content User Guide

Version: Foundation EP1

Written by: Documentation Team, R&D
Date: Friday, February 13, 2026

HYLAND™

Documentation Notice

The information and software described in this document are furnished only under a separate agreement and may only be used or copied according to the terms of such agreement. It is against the law to copy the software except as specifically allowed in such agreement. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright law, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Hyland Software, Inc. and/or one of its affiliates.

Hyland, OnBase, Alfresco, Nuxeo, Content Innovation Cloud, and other product or brand names are registered and/or unregistered trademarks of Hyland Software, Inc. and its affiliates in the United States and other countries. All other trademarks, service marks, trade names and products of other companies are the property of their respective owners.

© 2026 Hyland.

The information in this document may contain technology as defined by the Export Administration Regulations (EAR) and could be subject to the Export Control Laws of the U.S. Government including for the EAR and trade and economic sanctions maintained by the Office of Foreign Assets Control as well as the export controls laws of your entity's local jurisdiction. Transfer of such technology by any means to a foreign person, whether in the United States or abroad, could require export licensing or other approval from the U.S. Government and the export authority of your entity's jurisdiction. You are responsible for ensuring that you have any required approvals prior to export.

DISCLAIMER: This documentation contains available instructions for a specific Hyland product or module. This documentation is not specific to a particular customer or industry. All data, names, and formats used in this document's examples are fictitious unless noted otherwise. This document may reference websites operated by third parties. In such a case, Hyland has no control or liability for the content of such third-party websites. The inclusion of such a link shall not constitute an endorsement or affiliation with such a third-party website; the reference is provided for information purposes only. If you have questions about discrepancies in this document, please contact Hyland. Hyland customers are responsible for making their own independent assessment of the information in this documentation. This documentation: (a) is for informational purposes only, (b) is subject to change without notice, (c) is confidential information of Hyland Software, Inc. and its affiliates, and (d) does not create any commitments or assurances by Hyland. This documentation is provided "as is" without representation or warranty of any kind. Hyland expressly disclaims all implied, express, or statutory warranties. Hyland's responsibilities and liabilities to its customers are controlled by the applicable Hyland agreement. This documentation does not modify any agreement between Hyland and its customers.

Table of Contents

Documentation Notice ... **3**
Set up Content system ... **38**
Manage licenses ... 38
License groups ... *38*
What are License groups? ... 38
Create a license group ... 38
Rename a license group ... 38
Delete a license group ... 39
Add a user to a license group ... 39
Remove a user from a license group ... 39
Remove a user from a license group ... 40
Distribute licenses to a license group ... 40
Add a license group to a distribution list ... 41
Manage named license allocations ... 41
About licensing in Perceptive Content ... *41*
About licensing Citrix environments ... *43*
About licensing CaptureNow ... *43*
What is the licensing process? ... *44*
What is a system fingerprint? ... *44*
Generate a system fingerprint in a licensed system ... 44
Generate a system fingerprint using INTool ... 45
Install Perceptive Content licenses ... *45*
View ImageNow licenses ... *45*
What is demonstration mode? ... *46*
Supported licenses for demonstration mode ... 46
What is failover licensing? ... *47*
What is overdraft protection licensing? ... *48*
Generate overdraft licensing report ... 48
Manage the server ... 49
Change the inuser password ... *49*
Enable hidden search operators ... *49*

inserver directories *50*
audit 50
bin 50
bin64 50
db 50
etc 50
fax 50
help 50
install_temp 50
job 51
learnmode 51
log 51
osm_01.00001 51
osm_02.00001 51
osm_03.00001 51
script 51
temp 51
update 51
user 51
workflow 52
Troubleshoot connection issues *52*
Automatic logoff is not working 52
Users are not receiving workflow alarms 52
Remoted agents cannot communicate with ImageNow Server 53
Users are unable to send documents to other users 53
Users are unable to connect to ImageNow Server 53
Users are unable to log in with LDAP user authentication 54
Users are unable to log in to Interact Desktop with Windows domain authentication 54
Users are unable to log in with SQL user authentication 55
Object Storage Manager *55*
OSM definitions 55
Primary Set 55

Reference Set 55
Cache Set 56
Sub-Object Set 56
OSM features 56
OSM record fields 57
OSM set fields 57
OSM tree fields (FSS) 59
OSM set caching support information 61
Move the OSM 62
Set up OSM caching 63
Delete an OSM cache set 64
OSM Sets 64
About OSM sets 64
Primary sets 64
Reference sets 65
Cache sets 65
Subobject sets 65
Add an OSM set 66
Display all OSM sets 67
Update an OSM set 67
Delete an OSM set 68
OSM Filters 68
What are OSM filters? 68
Add an OSM filter 68
Display all OSM filters 69
Update an OSM filter 69
Delete an OSM filter 70
OSM Trees 70
About OSM trees 70
Add an OSM tree 71

Display all OSM trees ... 71
Update an OSM tree ... 72
Delete an OSM tree ... 72
Server information ... *73*
Export ImageNow Server technical information ... 73
Run diagnostic system information report ... 73
Use a terminal server ... *73*
About using ImageNow with a terminal server ... 73
Paths for a terminal server ... 74
Example assignments for [Paths] ... 74
Set up ImageNow Client on a terminal server ... 74
Troubleshoot terminal server issues ... 75
LearnMode issues ... 75
ImageNow Client issues ... 76
Interact Desktop Issues ... 77
Troubleshoot ImageNow Client issues on terminal servers ... 77
Troubleshoot Interact Desktop issues on terminal servers ... 78
Troubleshoot LearnMode issues on terminal servers ... 79
Configure your database ... 80
What is INEMUSER? ... *80*
Configure DataDirect DSN to enable SSL encryption ... *80*
Configure SQL Server to use a certificate for SSL ... *80*
Import a certificate for SQL Server on Windows ... *81*
What is automatic database reconnection? ... *81*
Manage user authentication ... 81
What is user authentication and authorization? ... *81*
What is token-based authentication? ... *82*
Set up token-based authentication ... 82
Generate an authentication token for an agent ... 82
What is Epic user authentication? ... *83*
Set up user authentication using Epic ... 83

What is LDAP user authentication? ... *84*
Set up user authentication using LDAP ... 84
Set up LDAP authentication with SSL overview ... 91
Configure the MMC snap-in ... 91
Use the MMC snap-in to install the certificate on the LDAP server ... 91
Export the certificate from your LDAP server ... 92
Import a certificate into Perceptive Content Server on Windows ... 94
Import a certificate into Perceptive Content Server on UNIX ... 95
Enable FIPS mode for LDAP on UNIX ... 96
Configure LDAP SSL/TLS cipher suites for UNIX ... 97
Configure an SSL trust store on Linux ... 97
What is multiple LDAP server authentication? ... *97*
What is SQL user authentication? ... *98*
Set up user authentication using SQL ... 98
What is System user authentication? ... *100*
Set up user authentication using System ... 101
Manage configuration files ... 101
inmc.ini [Remote] settings ... *101*
inmc.ini [Remote] setting ... 101
inow.ini ... *102*
inow.ini [Audit] settings ... 102
inow.ini [Auto Form] settings ... 103
inow.ini [Data Capture] settings ... 103
inow.ini [Digital Signature] settings ... 103
inow.ini [Directory Locations] settings ... 104
inow.ini [Doc] settings ... 105
inow.ini [DocLock] settings ... 105
inow.ini [Envoy] settings ... 106
inow.ini [ERM] settings ... 106
inow.ini [Experience] setting ... 106
inow.ini [Fax Out] settings ... 106
inow.ini [Folders] settings ... 107

inow.ini [Forms] settings 107
inow.ini [General] settings 107
inow.ini [iScript] settings 108
inow.ini [Licenses] settings 108
inow.ini [Locale] settings 109
inow.ini [Logging] settings 109
inow.ini [Logon Control] settings 109
inow.ini [Memory] settings 115
inow.ini [Message Queuing] settings 115
Server Settings 115
Client Settings 117
inow.ini [Migration] settings 119
inow.ini [Network] settings 119
inow.ini [OCR] settings 120
inow.ini [ODBC] settings 121
inow.ini optional settings 125
inow.ini [OSM] settings 125
inow.ini [Records] settings 127
inow.ini [Redaction] settings 127
inow.ini [Statistics] settings 127
inserver.ini *138*
inserver.ini [Anonymous Login] settings 138
inserver.ini [Business Insight] settings 138
inserver.ini [ClientINI] settings 139
inserver.ini [DepartmentsINI] settings 140
inserver.ini [Experience URL] settings 140
inserver.ini [Folders] settings 142
inserver.ini [General] settings 143
inserver.ini [LearnMode] settings 146
inserver.ini [Logging] settings 147
inserver.ini [Network] settings 148
inserver.ini [OpenID Connect Login Profiles] settings 149

inserver.ini [Remote] settings 153
inserver.ini [Timing] settings 154
inserver.ini [Views] settings 157
inserverAlarm.ini *158*
[General] 158
[Email] 158
inserverBatch.ini *159*
[General] 159
[Batch Logging] 160
[ReadSoft] 160
inserverEM.ini *162*
[General] 162
[Expire] 163
[Logging] 164
[Purge] 164
inserverFS.ini *165*
[General] 165
inserverImp.ini *166*
[DOD Record Metadata Mapping] 167
[Mode DOD_XML] 168
[File Concatenation] 168
[General] 168
[Key Mapping] 171
inserverImp.ini [Logging] settings *171*
[Mode COMBO] 172
[Mode DATA_CAPTURE] 172
[Mode DOD_RECORD] 174
[Mode FILENAME] 175
[Mode INDEX_FILE] 176
[Mode KEYMAPPING] 178
[Mode TIFF_TEXT_COMBO] 179
inserverINI.ini [OSM] settings *179*
inserverImp.ini [Remote] settings *180*

inserverImp.ini [Serial Number] settings *181*
inserverJob *182*
General 182
Timers 182
Logging 184
inserverMonitor.ini [Defaults] settings *184*
inserverMonitor.ini [Defines] settings *186*
inserverMonitor.ini [EventLog] settings *186*
inserverMonitor.ini [Logging] settings *187*
inserverMonitor.ini [Polling] settings *187*
inserverMonitor.ini [Processes] settings *188*
inserverMonitor.ini [Profiles] settings *189*
inserverNotification.ini *191*
[General] 191
[Email] 191
[Logging] 192
[Workers] 192
inserverOSM.ini *193*
[General] 193
[Logging] 194
[Verification] 195
inserverRetention.ini [Assign] settings *196*
inserverRetention.ini [Cutoff] settings *196*
inserverRetention.ini [Deletion] settings *196*
inserverRetention.ini [Event Hold] settings *197*
inserverRetention.ini [General] settings *198*
inserverRetention.ini [Logging] settings *199*
inserverRetention.ini [Notification] settings *199*
inserverRetention.ini [PolicyApplyScheduling] settings *201*
inserverRetention.ini [Remove] settings *202*
inserverTask.ini *202*
[General] 202
[Deletion] 203

[Logging] 205
[Workload] 205
inserverWorkflow.ini *206*
[General] 206
[Logging] 207
[Workload] 207
Use command line tools 211
INTool commands *211*
INTool Audit commands 211
import-all-audit-templates 211
import-audit-template 212
INTool Database Management commands 212
db-struct 212
db-rec-num 212
db-list-tables 213
db-show-execution-plan 213
get-db-version 213
db-schema-validation 213
General Commands 214
-name 214
-description 214
-company 214
-version 214
-service 214
-help and -? 214
--category 215
--find <keyword> 215
Installation Commands 215
build-osm 215
add-subob-templ 216

add-users ... 216
create-output-profiles ... 216
populate-calendar ... 217
populate-enumerations ... 217
create-bootstrap-user ... 217
iScript Commands ... 218
218
License commands ... 218
intool --cmd license-check (--type | --seats | --installed) <type> ... 218
intool --cmd license-tokens --report [--client-name <client name>][--lictype <license name>] ... 218
intool --cmd license-tokens --release [--client-name <client name>][--lictype <license name>] ... 219
intool --cmd license-sysfp --file <file name.sysfp> ... 219
intool --cmd license-validate-tokens [--lictype <license name>] ... 219
intool --cmd release-stale-tokens --lictype <license name> --days <number of days unused> ... 220
intool --cmd update-license-allocations ... 220
intool --cmd set-demo-mode ... 220
Logs commands ... 221
zip-logs ... 221
run-system-report ... 221
create-reflect-dataset ... 221
OSM Commands ... 222
build-osm ... 222
fix-next-slot ... 223
add-osm-set ... 223
add-osm-set --reference ... 224
add-osm-tree ... 224
add-osm-filter ... 225
add-osm-cache ... 225
update-osm-set ... 226

update-osm-set --reference 227
update-osm-tree 227
update-osm-filter 228
update-osm-cache 228
validate-osm-report 229
validate-document 231
delete-osm-set 232
delete-osm-tree 232
delete-osm-filter 232
delete-osm-cache 233
delete-cache-set 233
list-osm-sets 233
list-osm-sets --primary 233
list-osm-sets --reference 233
list-osm-trees 234
list-osm-filters 234
list-osm-caches 234
transfer-doc 234
cleanup-orphan-erm 235
add-osm-plugin 235
delete-osm-plugin 235
update-osm-plugin 236
list-osm-plugins 236
Reasons commands 236
add-digsig-reasons 236
add-task-reasons 237
add-ooo-reasons 237
Server commands 238
intool --cmd revoke-all-certs 238

intool --cmd revoke-cert 238
intool --cmd import-cert 238
intool --cmd control-logins 239
Uncategorized commands 241
export-all-record-objects 241
User Administration commands 241
add-users 241
logoff 242
logoff-expired-sessions 242
delete-users 243
promote-perceptive-manager 243
demote-perceptive-manager 244
send-message 244
expire-digital-ids 245
create-authentication-token 245
openidconnect-invalidate-discovery-configuration 245
Views Commands 246
create-default-view 246
explain-vsl 247
remove-default-user-views 247
Workflow commands 247
reset-item-count 247
unlock-process 248
reset-item-status 248
verify-subqueue-names 249
reset-workflow-views 249
validate-integration-asq 249
INUpgradeUtil commands *250*
convert-integration-queues 250
remove-fulltext-artifacts 250

upgrade-server-queries 250
upgrade-privs 251
upgrade-digsig-reasons 251
upgrade-digsig-version 251
upgrade-learn-mode 251
upgrade-composite-properties 252
update-rules 252
import-all-audit-templates 252
update-license 252
upgrade-views 252
upgrade-users 252
upgrade-timing 253
upgrade-outlook-source-profile 253
upgrade-remote-service-files 253
upgrade-audit-templates 253
upgrade-custom-properties 253
upgrade-policy-queues 253
Run INTool commands *254*
Run INUpgradeUtil commands *254*
Use VSL 254
What is VSL? *254*
VSL property constraints *255*
VSL statement syntax *267*
Manage users groups **273**
Manager roles 273
What is a Perceptive Manager? *273*
Promote a user to Perceptive Manager *273*
What is a Department Manager? *274*
Promote a user to Department Manager *274*
Demote a Department Manager *275*
Users 275
About copying security attributes of users and groups *275*
Import users from a local computer *276*

Remove a user from a group *276*
Security attribute duplication within a department *276*
Rename a user *277*
Import users from a domain *278*
Change a user's active status *278*
Import users from LDAP *278*
Delete a user *279*
Import users from a file *279*
Add a user to a group *279*
Security attribute duplication in a cross department setting *280*
Promote a user to Perceptive Manager *280*
Groups 281
Security attribute duplication in a cross department setting *281*
Create a group *281*
Delete a group *282*
Security attribute duplication within a department *282*
What is a group? *283*
About copying security attributes of users and groups *283*
Modify a group *284*
Out of Office 285
What is Out of Office? *285*
Create an Out of Office event *285*
Create a user's Out of Office event *285*
Disable a user's Out of Office event *286*
Disable an Out of Office event *286*
Modify a reason for Out of Office *286*
View a user's Out of Office event *287*
Assign privileges **287**
About assigning privileges 287
What is the privilege hierarchy? 288
Remove management privileges 288
Assign user access to ERM report documents 289
Restrict a user from a specific function 290

View privileges for a user 290
View privileges for a group 292
Create a department 293
Grant management privileges to users 294
Privilege definitions overview 294
Annotation Template Privileges *296*
Create 296
Delete 296
Hide 296
Modify 296
View 296
Application Plan Privileges *296*
Link Documents 296
Auto Create Folders 296
View 296
Manage 297
Declare Records 297
Auto Create Record Folders 297
Category Privileges *297*
View 297
Connection Type Privileges *297*
Apply 297
Remove 297
Department: Administer Group Privileges *297*
Drawer Privileges 297
Document Type Privileges 297
Folder Type Privileges 298
Workflow Process Privileges 298
File Plan Privileges 298
Record Type Privileges 298
Record Folder Type Privileges 298
Record Category Type Privileges 298
Access Control Marking Privileges 298

Record Container Privileges 298
Connection Type Privileges 298
Department: Administer User Privileges *298*
Drawer Privileges 298
Document Type Privileges 298
Folder Type Privileges 299
Workflow Process Privileges 299
File Plan Privileges 299
Record Type Privileges 299
Record Folder Type Privileges 299
Record Category Type Privileges 299
Access Control Marking Privileges 299
Record Container Privileges 299
Connection Type Privileges 299
Department: Manage *299*
Groups 299
Application Plans 300
Annotation Templates 300
Drawers 300
Document Types 300
Folder Types 300
Custom Properties 300
Task Templates 300
Workflow Processes 300
Forms 301
Capture Profiles 301
Source Profiles 301
Output Profiles 301
Document Views 301
Folder Views 301
Retention Policies 301
Retention Holds 301
Fax Recipients 302

Record Types 302
File Plans 302
Record Folder Types 302
Record Category Types 302
Connection Types 302
Access Control Markings 302
Record Views 302
Record Folder Views 302
Document Type: Document Management *303*
Use Version Control 303
Remove from Version Control 303
Undo 3rd Party Check Out 303
Delete Version History 303
Document Type: Documents *303*
Open 303
Sign 303
Void Signatures 304
Edit Drawer 304
Edit Type 304
Edit Keys 304
Edit Custom Properties 304
Edit Notes 304
Delete 304
Merge 304
Page Delete 305
Page Reorder 305
Move Page 305
Delete Signed Documents 305
Move Signature Representations 305
Delete Signature Representations 305
Copy to Clipboard 305
Document Type: Explorer/Folder Viewer *305*
Print Documents 305

Email ImageNow Link 305
Email Web Link 306
Mail as Attachment 306
Save Local Copies 306
Fax Document 306
Launch Associated Application 306
Send Documents to User 306
Send to ShareBase 306
Document Type: Viewer *306*
Print Document 306
Email ImageNow Link 307
Email Web Link 307
Mail as Attachment 307
Save Local Copies 307
Fax Document 307
Launch Associated Application 307
Send Document to User 307
Send to ShareBase 307
Drawer: Batch (Proposed Key) *307*
Process 307
Drawer: Content *308*
Open 308
Search 308
Create/Append 308
Move 308
Rename 308
Delete 309
Edit Custom Properties 309
Edit Drawer 309
Edit Type 309
Create Shortcuts 309
Remove Shortcuts 309
Drawer: Document Management *309*

Use Version Control ... 309
Remove from Version Control ... 310
Undo 3rd Party Check Out ... 310
Delete Version History ... 310
Drawer: Documents ... *310*
Sign ... 310
Void Signatures ... 310
Edit Keys ... 310
Edit Notes ... 310
Merge ... 310
Page Delete ... 311
Page Reorder ... 311
Move Page ... 311
Delete Signed Documents ... 311
Move Signature Representations ... 311
Delete Signature Representations ... 311
Copy to Clipboard ... 311
Drawer: Explorer/Folder Viewer ... *311*
Print Documents ... 311
Email ImageNow Link ... 311
Email Web Link ... 312
Mail as Attachment ... 312
Save Local Copies ... 312
Fax Document ... 312
Launch Associated Application ... 312
Send Documents to User ... 312
Send to ShareBase ... 312
Drawer: Folders ... *312*
Edit Status ... 312
Drawer: Viewer ... *313*
Print Document ... 313
Email ImageNow Link ... 313
Email Web Link ... 313

Mail as Attachment 313
Save Local Copies 313
Fax Document 313
Launch Associated Application 313
Send Document to User 313
Send to ShareBase 313
File Plan: Content *314*
Open 314
Search 314
Create/Append 314
Move 314
Rename 314
Delete 314
Edit Custom Properties 314
Edit File Plan 315
Edit Type 315
Reassign Retention Policy 315
Apply Cutoffs 315
Reverse Cutoffs 315
Override Closed State 315
Close 315
Reopen 316
Vital Status 316
File Plan: Explorer/Folder Viewer *316*
Print Record 316
Save Local Copies 316
Launch Associated Application 316
Email ImageNow Link 316
Email as Attachment 316
Fax Record 316
File Plan: Record Categories *317*
Modify Properties 317
Modify Notifications 317

File Plan: Record Folders *317*
Edit Status 317
File Plan: Records *317*
Edit Properties 317
Edit Notes 317
Merge 318
Page Delete 318
Page Reorder 318
Move Page 318
Modify Page Properties 318
Copy to Clipboard 318
File Plan: Viewer *318*
Print Record 318
Save Local Copies 319
Launch Associated Application 319
Email ImageNow Link 319
Email as Attachment 319
Fax Record 319
Folder Type Privileges *319*
Use 319
Manage 319
Form Privileges *320*
Create 320
Delete 320
Modify 320
View 320
Global: Administer Group Privileges *320*
ERM Privileges 320
Capture Privileges 320
Interact Search Privileges 320
Batch Users 320
Global: Administer User Privileges *321*
ERM Privileges 321

Capture Privileges 321
Interact Search Privileges 321
Batch Users 321
Global: Batch (General) *321*
QA 321
Link 321
Delete 321
Edit Batch Notes 322
Modify Batch Step or State 322
Resubmit Batch 322
Bypass QA 322
Global: Capture *322*
Batch Mode 322
Single Mode 322
Package Mode 322
Global: Manage *323*
LearnMode Options 323
Server Administrator 323
Basket Groups 323
Package Mode Document Rules 323
Batch Upload Settings 323
Capture Profiles 323
Scanner Profiles 324
Devices 324
Digital ID 324
Digital Signatures 324
Audit Template Management 324
Audit Template Assignment 324
Reports 324
Run iScript Remotely 324
Task Views 324
Modify User Profiles 325
View User Profiles 325

Global: Reports *325*
View 325
Global: Search *325*
ERM 325
ERM: Load Local Query 325
ERM: Load Server Query 325
ERM: Manage Local Queries 325
ERM: Manage Server Queries 326
Interact for Office Documents 326
Interact for Office Folders 326
Global: Viewer (Unlinked Documents) *326*
Print Document 326
Email as Attachment 326
Save Local Copies 326
Launch Associated Application 327
Hold Privileges *327*
Apply Document Hold 327
Remove Document Hold 327
Search for Documents on Hold 327
Workflow: Process *327*
Workflow: Queue *327*
Add 328
Anywhere 328
Archive 328
Delete 328
Process 328
Remove 328
Upstream 328
Record Category Privileges *328*
File Content 329
Search 329
Record Category Type Privileges *329*
Manage 329

Use 329
Record Folder Privileges *329*
File Content 330
Search 330
Record Folder Type Privileges *330*
Manage 330
Use 330
Record Type: Explorer/Folder Viewer *330*
Print Record 330
Save Local Copies 330
Launch Associated Application 331
Email ImageNow Link 331
Email as Attachment 331
Fax Record 331
Record Type: Records *331*
Open 331
Edit File Plan 331
Edit Type 331
Edit Properties 332
Edit Custom Properties 332
Edit Notes 332
Delete 332
Merge 332
Page Delete 333
Page Reorder 333
Move Page 333
Copy to Clipboard 333
Modify Page Properties 333
Record Type: Viewer *333*
Print Record 333
Save Local Copies 333
Launch Associated Application 333
Email ImageNow Link 334

Email as Attachment 334
Fax Record 334
Report Security Privileges *334*
Run 334
View 334
Workflow: Route Out Restrictions *334*
Restrict Route Out 334
Task Template Privileges *335*
Create 335
Delete 335
Manage 335
Modify 335
Review 335
View 335
Workflow: Application Plan *336*
Update Only Empty Key Values 336
Modifiable 336
Allow Blank 336
Host Entry Validation 336
Manage departments **337**
What is department administration? 337
What is a department label? 337
What are the cross department settings? 338
Create a department 338
Select a department 339
About implementing department privileges 339
Manage transfer 340
What is a department transfer profile? *340*
What is a department transfer package? *340*
Department transfer components *340*
About transferring components to another department *342*
Transfer components between departments *342*
Create and export a transfer package *342*

Create a transfer profile *343*
Import a transfer package *343*
Create a cross-department migration profile *343*
Preview a transfer package *344*
Modify a transfer profile *344*
Share items with departments 345
What is shared department content? *345*
Share an item with another department *345*
Share an application plan with another department 346
Share a capture profile with another department 346
Share a source profile with another department 347
Share a document type category with another department 347
Share a document type list with another department 347
Share a document type with another department 348
Share a document view with another department 348
Share a drawer with another department 348
Share a folder type list with another department 349
Share a folder type with another department 349
Share a group with another department 349
Share an item with another department 350
Share a data definition with another department 351
Share a form file with another department 351
Share a form with another department 351
Share a presentation with another department 352
Share a fax recipient with another department 352
Share a custom property with another department 352
Share a connection type with another department 353
Share a cutoff instruction with another department 353
Share a file plan with another department 353
Share a picklist with another department 354
Share a record category type with another department 354
Share a record folder type with another department 354
Share a record type with another department 355

Share a retention date period with another department 355
Share a retention hold reason with another department 355
Share a retention hold with another department 356
Share a retention physical file template with another department 356
Share a retention physical location with another department 356
Share a retention physical property with another department 357
Share a retention policy authority with another department 357
Share a retention policy with another department 357
Share a task reason list with another department 358
Share a task template with another department 358
Share a workflow alarm with another department 358
Share a workflow process with another department 359
Share a workflow reason list with another department 359
Share a workflow rule with another department 359
Delete a shared item *360*
Manage migration **360**
What is migration? 360
Migration components 361
Components and component references 361
Duplicate Components and Component References *361*
Missing Components and Component References *362*
About migrating views 362
About renaming queues 363
Manage migration profiles 363
What is a migration profile? *363*
Create or modify a migration profile *363*
Export a migration package *364*
Import a migration package *365*
Preview a migration package *365*
Run diagnostics **366**
Status Report 366
What is the ImageNow Server Resource Status report? *366*
View ImageNow Server Resource Status report *366*

Client Performance 366
What is ImageNow Client performance reporting? *366*
What is Job Manager? *366*
About rating your system performance *367*
ImageNow Client detailed performance report data *367*
Configure an ImageNow Client performance report *368*
Export a condensed performance report *369*
Export a detailed performance report *369*
Logging 370
What are ImageNow log files? *370*
Create a log file *370*
Configure logging *371*
Include socket communication in server log *371*
Delete a controller log file *372*
Enable rolling log files *372*
Change the Perceptive Content log file directory location *372*
Archive log reports *372*
Real Time Telemetry System *374*
What is performance monitoring logging? 374
Configure performance log files 374
View performance log files 374
Performance logging settings 375
Category descriptions 375
Category settings 376
Performance log file components 380
Time Travel Logging *383*
About time travel logging configuration 383
About reporting incident conditions 384
View time travel incident reports 384
Categories table 384
Condition use cases 386
Time travel logging on error 386

Time travel logging on a slow performing server call 386
Time travel logging on a slow performing SQL statement 386
Parameters table 386
Error opt in example 388
Application and OS exception opt out example 388
Controller Log Files *388*
View the Controller Log file 388
Create the Controller Log file 388
Delete a controller log file 388
Auditing 388
What is auditing? *388*
Create a new audit template overview *389*
Add an audit template 389
Add predefined conditions to an audit template 389
Add client audit conditions to a template 389
Add server audit conditions to the template 390
Assign an audit template to users or groups 390
Enable an audit template 391
Create an audit authentication template *391*
Copy an audit template *392*
Modify or rename an audit template *392*
Delete an audit template *393*
Set the audit log format *393*
Audit conditions *394*
Available predefined conditions 394
Available categories, actions, and objects for server-side conditions 395
Category 396
Action 397
Object 399
Available actions for client-side conditions 406
Sessions 406
About monitoring user and agent connection *406*

View agent sessions ... *407*
View user sessions ... *407*
ImageNow Client API ... **408**
Manage agents ... **408**
Fax Agent ... 408
Fax an item ... *408*
Add a fax number for fax recipients ... *408*
Retention Agent ... 408
What is retention? ... *408*
What is Retention Agent? ... *409*
About Retention Policies and File Plans ... *409*
Glossary of retention terms ... *409*
What is a retention policy? ... *412*
Create a retention policy ... *412*
View record categories assigned to a policy ... *412*
What is record offline transfer? ... *413*
What are record export sets? ... *413*
Physical Locations ... *414*
About administering physical locations ... 414
Create a physical location ... 414
Modify or rename a physical location ... 415
Delete a physical location ... 415
Physical Properties ... 415
Physical property data types ... 415
Create a physical property overview ... 417
Modify or rename a physical property ... 417
Copy a physical property ... 417
Delete a physical property ... 418
About administering physical file templates ... 418
About administering physical file templates ... 418
Create a physical file template ... 418
Copy a physical file template ... 419

Modify or rename a physical file template ... 419
Delete a physical file template ... 420
Holds ... *420*
What is a retention hold? ... 420
Export a hold set ... 420
Create a retention hold in Management Console ... 421
Rename a hold ... 422
Copy a hold ... 422
Modify a hold ... 422
Delete a hold ... 423
View hold history ... 423
Disable a hold ... 423
Reasons ... 424
Create a retention hold reason ... 424
Modify a hold reason ... 424
Delete a hold reason ... 424
Sets ... *425*
What are retention set notifications? ... 425
Retention set types ... 425
Retention set state definitions ... 428
Destruction ... *428*
What are destruction sets? ... 428
Confirm a destruction set ... 429
Generate a destruction report ... 429
View a destruction set ... 429
Export ... *430*
What are export sets? ... 430
Confirm an export set ... 430
Generate an export set report ... 431
Retry an export set request ... 431
View an export set ... 432
Move and Copy ... *432*

What are move and copy sets? 432
Confirm a move or copy set 433
Retry a move or copy set report 433
Recognition Agent 433
What is Recognition Agent? *433*
Licenses for Recognition Agent *433*
Guidelines for enhancing recognition rates *434*
Set Recognition Agent logging *434*
Forms Identification Module *435*
Enable automatic form identification 435
Set a document type to automatic form identification 435
Test automatic form identification 436
Troubleshoot automatic form identification 436
I am unable to match captured images to the correct master forms 436
I am unable to log information for automatic form identification 437
OCR *437*
What is OCR? 437
Create an OCR zone for a document property 438
OCR zone properties 439
OCR methods 440
Output Agent 441
What is Output Agent? *441*
Manually create a keyfile *441*
Output annotations on output files *442*
Common output file formats *442*
Specify a header for output pages *443*
Troubleshoot item output *443*
Output takes longer than expected 443
Microsoft Outlook settings are not available when outputting an item to email 443
Set Output Agent logging *444*
About logging for Output Agent *444*
Ooutput Variables *444*

What are output variables? 444
Output variable guidelines 445
Guidelines 445
Available output variables for file names 445
Exported Document 445
Exported Document Page 446
Exported Document File 446
Exported Sheet/Output Page 446
Available output variables for page headers 447
Variables 447
Example 447
Import Agent 448
What is Import Agent? *448*
Import Agent import modes *448*
INDEX_FILE 448
COMBO 448
KEYMAPPING 449
TIFF_TEXT_COMBO 449
FILENAME 449
DATA_CAPTURE 449
DOD_RECORD 449
DOD_XML 449
CAPTURE_PROFILE 449
Configure Import Agent capture profile mode overview *449*
Configure Import Agent for Capture Profile mode *450*
Create an Import Agent capture profile for a document *451*
Create an Import Agent capture profile for a record *452*
Import Agent key mapping options *453*
Import Agent serial number formats *455*
About running multiple instances of Import Agent *457*
Install another instance of Import Agent *457*
Set Import Agent logging *458*

Monitor Agent 458
What is Monitor Agent? *458*
What is a Monitor Agent process? *459*
What is a Monitor Agent profile? *459*
Monitor Agent process elements *459*
Elements 459
Create a Monitor Agent process *462*
Monitor Agent profile elements *463*
Elements 463
Create a Monitor Agent profile *466*
Restart non-responsive agents *467*
Restart agents on a defined schedule *468*
Restart agents based on a threshold *469*

Set up Content system

Manage licenses

License groups

What are License groups?

License groups allow you to allocate licenses from your total license pool to individual groups based on your business requirements. This distribution ensures that the appropriate number of licenses are allocated to groups who require them.

You create license groups, add users to license groups, and then determine the number of licenses to distribute from your unassigned licenses to the license groups. You can create as many license groups as your business needs require. A user can belong to only one license group.

In addition to assigning licenses to individual groups, you can leave some licenses unassigned. These unassigned licenses serve as an overflow. The system uses assigned licenses before consuming unassigned licenses. At any time, you can rename or remove license groups as well as remove users from a license group.

License groups can be implemented with named and concurrent licenses. License groups can also be used with combo licenses. You cannot distribute overdraft enabled licenses to individual groups.

Create a license group

To set up a license group and add users to it, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select **License Groups**.
3. On the **License Groups** tab, click **New**.
4. Enter a name for the license group and press `Enter`.

Rename a license group

To rename a license group, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select **License Groups**.
3. On the **License Groups** tab, select a license group from the list and click **Rename**.
4. Enter a new name for the license group and press `Enter`.

Delete a license group

To delete a license group, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select**License Groups**.
3. On the **License Groups** tab, select the license group that you want to delete, and then click **Delete**. In the confirmation dialog box, click **Yes**.

> **Note:** Deleting a license group does not delete the users assigned to it.

Add a user to a license group

To add a user to a license group, complete the following steps.

1. In the **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select **License Groups**.
3. On the **License Groups** tab, select the group to which you want to add the user, and then click **Modify**.
4. In the **License Group** dialog box, click **Add**.
5. In the **Select Users** dialog box, on the **Users** tab, in the **Search for users** box, type all or part of the user name you want to locate, and then click **Search**. In the **Search** results list, select one or more users, click **Add**, and then click **OK**.
6. If you are adding another user, in the **License Group** dialog box, click **Apply**, and then add another user. If you are done adding users, in the **License Group** dialog box, click **OK**. In the confirmation dialog box, click **Yes**.

> **Note:** When you add users to a license group, they are removed from their currently assigned license group. To reassign users, in the confirmation dialog box, click **OK**.

Remove a user from a license group

To remove a user from a license group, complete the following steps.

1. In the **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select**License Groups**.
3. On the **License Groups** tab, select the group that contains the user you want to remove, and then click **Modify**.
4. In the **License Group** dialog box, select the user you want to remove from the group, and then click **Remove**. In the confirmation dialog box, click **Yes**.

Remove a user from a license group

To remove a user from a license group, complete the following steps.

1. In the **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select**License Groups**.
3. On the **License Groups** tab, select the group that contains the user you want to remove, and then click **Modify**.
4. In the **License Group** dialog box, select the user you want to remove from the group, and then click **Remove**. In the confirmation dialog box, click **Yes**.

Distribute licenses to a license group

To manage the license distribution for a license group, complete the following steps.

1. In the **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select **License Distribution**.
3. On the **License Distribution** tab, select the license type that you want to distribute, and then click **Modify**.
4. In the **License Distribution** dialog box, select the license group for which you want to manage license distribution and complete one of the following steps.

Situation	Steps
Add an existing license group	1. Click **Add**. 2. In the **License Group Distribution** dialog box, select a license group and then click **OK**.
Modify the number of licenses distributed to a license group	1. Select a license group and then click **Modify**. 2. Enter the number of licenses to distribute. 3. Click **OK**.
Remove a license group from the distribution list	• Select a license group and then click **Remove**. **Note:** When you remove a license group from the distribution list, all licenses distributed to that group return to the **Licenses remaining** count.

5. In the **License Distribution** dialog box, click **Apply** and then click **OK**.

Add a license group to a distribution list

You can add existing license groups to the license distribution list for a specific application. To add a license group for license distribution, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, expand **Licenses** and select **License Distribution**.
3. On the **License Distribution** tab, select the license type that you want to distribute and click **Modify**.
4. In the **License Distribution** dialog box, click **Add**.
5. In the **License Group Distribution** dialog box, select a license group and click **OK**.
6. Modify the license distribution for this group.

   If no licenses are distributed to a group, the group is removed from the license type.

Manage named license allocations

Named licenses are allocated on behalf of a user when they first log in using a client compatible with the Perceptive Named User license. Due to performance considerations, these allocations are only updated when license distributions are changed. Other licensing events do not cause existing allocations to be automatically updated. For example, overflow allocations from the unassigned pool are not reassigned to a user s license group when allocations become available in their license group. When a user is removed from a license group, their allocations are moved to the unassigned pool. When the user is assigned to a new license group, their allocations are not automatically updated. As a result, license allocations can accumulate in the unassigned pool. To resolve this, you may force the system to update affected named license allocations.

1. On the **Perceptive Content Server** computer, perform one of the following actions:
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In Unix, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following command: `intool --cmd update-license-allocations`.

   A message displays to confirm that license allocations have been successfully updated.

About licensing in Perceptive Content

Computers and servers running Perceptive Content must contain a certain type and number of licenses in order to operate.

Depending on how you implement Perceptive Content, different types of licenses are required for such things as how users access Perceptive Content, the number of users logged in to Perceptive Content at any one time, or different types of document processing. However, every computer running the Perceptive Content Server must have a hardware node license. Additionally, a Perceptive Content Server license and a minimum number of client licenses are required.

All Perceptive Content licenses are bound together by a License Group ID (LGID) created with the Perceptive Content Server license. Perceptive Content licenses are available as Live, Demo, Test, Not-for-resale (NFR), and Failover licenses. When new licenses are added, the new licenses use the same LGID. If you use all of your Perceptive Content licenses, you can add more licenses by contacting your Lexmark Enterprise Software representative.

Perceptive Content uses the following licensing types to control access to its components.

- `Concurrent use`. This is a software license that is based on the number of simultaneous users accessing Perceptive Content. For example, in a five-user concurrent license, after five users log in to the program, the program prevents a sixth user from logging in. When any of the first five users log off, the next user can log in. Concurrent licensing limits the number of users running Perceptive Content from a centralized location, such as the Perceptive Content Server, based on the current license agreement. The licenses in concurrent licensing are a pool of available licenses that can be used from any client computer and are not node-locked to a specific client computer.
- `Per seat`. This is a node-locked license that is based on the number of computers on which you install the software. A node-locked license is locked to a computer by specific information about the computer. For example, an Perceptive Content Client per-seat license is node locked by placing a token on the client computer the first time that client runs. For per-seat clients and some Agents, this token is generated in the background and stored locally on the client computer. The token is a file that contains specific information about the license type. The token also contains the encoded hardware information consisting of 5-10 unique properties of the client computer, such as MAC address, disk drive serial number, disk drive size, and processor serial number. The license will work as long as 60 percent of the hardware comprising the original encoded hardware information remains the same.
- `Named`. This is a license based on Perceptive Content user names. Valid named licenses work regardless of hardware or device. Like per seat licenses, named licenses are token-based and are similarly managed. To access named licensing features, tokens are acquired and licenses are validated by the client on behalf of the user. For example, when a user attempts to access a named license feature, a token is acquired and validated for the user and access is then granted. This named license token is available for accessing the feature on any machine or device. If no named licenses are available, the user is not granted access to the feature.
- `Transaction package`. This licensing limits the number of transactions, or volume of work, for a specified period. Transaction package licensing is controlled from a centralized location. Transactions licenses are based on counting the number of transactions within Perceptive Content and decrementing this number over a period of time. The transactions are usually server calls or object retrievals. Once all of the transactions are used in a specified period, no more transactions can be done until the period expires.
- `Feature`. This licensing makes functionality available. Feature licenses are set at the server level and are either available or not available for all users.

About licensing Citrix environments

Citrix is a terminal server application that enables you to access ImageNow Client on a remote computer. Licensing your Citrix environment may vary based on your licensing scheme.

The ImageNow Server is licensed normally in a Citrix environment. However, the licensing of some client applications may be affected. Citrix environments do not affect concurrent or transaction licensing schemes. However, in per-seat licensing scheme, Perceptive Content counts each terminal services client as a separate machine and each client instance consumes its own license. Although an application may only be installed on one host computer, all clients that can access the application must be licensed. For instance, scanner stations require a license for each client machine that can access them.

About licensing CaptureNow

CaptureNow licensing is provided on a per-seat basis. CaptureNow licenses are provided per workstation running the ImageNow Client.

Perceptive Software offers the following types of CaptureNow to meet your unique capture requirements.

- `CaptureNow - File IP (Image Processing).` CaptureNow File with IP provides client-side image processing, barcode recognition, and patchcode detection on files imported in Single or Batch modes from ImageNow Client.
- `CaptureNow -ISIS Level 1`, CaptureNow - ISIS Level 2, and CaptureNow - ISIS Level 3. CaptureNow ISIS supports the ability to scan and import files using Single, Batch and Package modes, as well as image processing, barcode recognition, and patchcode detection using Pixel translation methods.
- `CaptureNow - Adrenaline`. CaptureNow Adrenaline is the interface that allows scanners driven by Kofax Adrenaline software to communicate with the scanning environment. CaptureNow Adrenaline supports all Kofax Adrenaline products, including VirtualReScan (VRS), and provides functionality for Single, Batch and Package modes. CaptureNow Adrenaline leverages Adrenaline Image Processing Engine (AIPE) for detection of barcodes and patchcodes.
- `CaptureNow - TWAIN`. CaptureNow TWAIN supports remote scanning, such as in a Citrix environment, through the TWAIN imaging protocol. As with CaptureNow ISIS, CaptureNow TWAIN supports scanning in Single, Batch and Package modes, as well as image processing, barcode recognition, and patchcode detection.

You can license one or more scanning devices from the ImageNow Client. To license a device, the user logged in to the local machine must have the Write permission to the [drive]:\Documents and Settings\All Users\Application Data\ImageNow\etc folder. When you attempt to add a new scanning device, enable file image processing, or import a Capture Profile, Perceptive Content checks for a current valid token on the computer. A token is an electronic representation of a real per-seat license. If a valid token is not found, Perceptive Content checks to see if there is an available, unused CaptureNow license and whether there are any unused tokens. If there are unused tokens available, you are prompted to use one of the tokens. If all of the tokens are taken, you are prompted to enter a new license.

What is the licensing process?

In order to license your Perceptive Content system, you need server hardware node licenses, an ImageNow Server license, and client licenses. The client licenses vary based on the applications incorporated into your Perceptive Content system.

In Perceptive Content, each server computer running ImageNow Server requires a hardware node license. The Perceptive Content hardware node license is node-locked to the specific server computer by specific information about the computer. Additionally, an ImageNow Server license is required to run concurrently with the server hardware node licenses. Only one ImageNow Server license is required, regardless of the number of server computers you are using.

A License Group ID (LGID) is created with the ImageNow Server license, and all other licenses that connect to the server must have the same LGID. The LGID is a unique, random number that has no dependencies on hardware or software keys. In Perceptive Content, the LGID replaces the MAC address to bind the different Perceptive Content licenses together. Your remaining licenses, such as client licenses, are created based on the LGID.

If you change your hardware, the ImageNow Server license becomes invalid and you must obtain a new ImageNow Server license. Also, if you move your ImageNow Server to a different server computer, you must obtain a new ImageNow Server license. Since the LGID remains the same for your new license, all of your other licenses are unaffected.

What is a system fingerprint?

The system fingerprint is an encrypted data file that contains information about every computer that is registered in your Perceptive Content installation, and it is the file that you send to your Perceptive Software representative when you request new or additional licenses.

A system fingerprint lists the computer name, hardware, license status, and registration time for each computer. The system fingerprint also contains the system LGID and a list of your product licenses.

Generate a system fingerprint in a licensed system

To generate a system fingerprint, complete the following steps.

Prerequisite to generate a system fingerprint, you must be the administrator user on Windows or the root user on UNIX platforms. You also must run the register command on each server computer.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the right pane, click **Licenses**.
3. In the right pane, click **Manage Licenses**.
4. Select **Save system fingerprint**.
5. Click **OK**.
6. In the **Save As** dialog box, enter a name for the file, and then navigate to the location where you want to save the report.
7. Click **Save**.

Next Contact your Perceptive Software representative for instructions on where to send the system fingerprint file. The file has a SYSFP extension.

Generate a system fingerprint using INTool

Your system fingerprint contains the hardware and system information required to obtain licenses in one file. To generate your system fingerprint using INTool, complete the following steps.

1. Click **Start > Run**.
2. In the **Run** dialog box, type `cmd` and then click **OK**.
3. In the **Command Prompt** window, perform one of the following actions.
   - In Windows, change to the *[drive:]\inserver\bin* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/etc* directory.
4. At the prompt enter `intool --cmdlicense-sysfp--file <file name>`.

Next Send the generated system fingerprint file to your Perceptive Software representative.

Install Perceptive Content licenses

To install Perceptive Content licenses, complete the following steps.

Prerequisite You must generate a system fingerprint and obtain license files from Lexmark Enterprise Software before starting this task.

1. When you receive the license files from your Enterprise Software representative, copy them to a temporary folder where you can access them with a **Perceptive Content** Client.
2. Click **Start** > **All Programs** > **Perceptive Content**.
3. On the login page, click **License Manager**.
4. In the **License Management** dialog box, select **Upload Licenses**, and then click **OK**.
5. Navigate to the temporary folder that contains the license files.
6. Select the LIC files to upload, and then click **Open**.
7. Enter the **User Name**, **Password**, and **Server Location**.
8. Click **OK**.
9. Restart all **Perceptive Content Server** instances.

View ImageNow licenses

License properties include the type of product that is licensed, the licensing schema, the number of licenses installed, and the number of licenses in use for each product. To view your Perceptive Content system's licenses, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the left pane, click **Licenses**.

   A list of Perceptive Content licenses appears in the right pane.
3. To sort the **Licenses** list in ascending or descending order, click the **Product**, **Scheme**, **Available**

Licenses, or **In Use Licenses** column headers.

4. To refresh the list of **Perceptive Content** licenses, click **Refresh**.

What is demonstration mode?

When you install Perceptive Content the first time, the product is in demonstration mode until you install a Perceptive Content Server license.

The first client that logs into the server and does not see any licenses in Perceptive Content is given a choice of two demonstration modes.

The first choice is 30 days with five concurrent users. A combined total of five users can log in an unlimited number of times for 30 days. These users have unlimited access to all core Perceptive Content functionality. After the 30 days expires, users cannot log into Perceptive Content until you purchase licenses. The second choice is 5,000 documents with five concurrent users. This allows a total of five users to log in and add up to 5,000 documents. After 5,000 documents are added, users cannot log in until you purchase licenses.

After a license is purchased and added to Perceptive Content Server, demonstration mode becomes inaccessible. For more information, refer to License commands.

Supported licenses for demonstration mode

The following licenses are supported in demonstration mode.

License	Limitations
CaptureNow - File IP	Limited to one user
CaptureNow -ISIS Level 1	Limited to one user
CaptureNow - ISIS Level 2	Limited to one user
CaptureNow - ISIS Level 3	Limited to one user
CaptureNow - Adrenaline	Limited to one user
Document Management	None
Fax Agent	Limited to one server
ImageNow Forms	None
ImageNow Client	Limited to five concurrent users, with no overdraft
ImageNow Database Connector	None

License	Limitations
ImageNow Interact for Microsoft Office	Limited to five users
ImageNow iScript	None
ImageNow Server	None
Mail Agent	Limited to one server
Message Agent Server	Limited to one server
Message Agent Transaction Pack	Limited to five packages per hour, with no overdraft
Output Agent	Limited to one server
Recognition Agent - OCR	Limited to one server
User Replication Agent	Limited to one server

What is failover licensing?

Failover licensing provides a way to purchase a separate license to help ensure availability of a particular service. A failover license will allow for an application to run with full functionality for a restricted amount of time (typically 90 days).

In a failover environment, the ImageNow Server license allows additional instances of the ImageNow Server to run on computers that are registered with a server hardware node license.

Perceptive Software provides a standard server licensing policy as part of the purchase and implementation. The licenses entitle you to run the ImageNow Server on any computer that you register with a server hardware node license. An ImageNow Server license also runs concurrently and controls the number of instances of the server that are running. ImageNow Server tracks the additional instances that run in a failover environment. For more information, contact your Perceptive Software representative.

Image processing or running scanning devices from Kofax or Pixel requires additional licenses for each scanner workstation configuration. Since Perceptive Content requires these separate licenses for specific features of CaptureNow, you can create a failover environment for each scanning workstation that has a CaptureNow license.

Failover licenses are available for the following per seat licensed products:

- ERM Server
- Fax Agent
- Forms Processing Agent
- Full Text Agent
- ImageNow Printer

- ISIR Agent
- Mail Agent
- Message Agent
- Output Agent
- Recognition Agent
- SAP ArchiveLink
- User Replication Agent

These licenses are not necessary with a Concurrent licensing scheme.

What is overdraft protection licensing?

Overdraft protection licensing allows you to continue using an application if you have exceeded the license count for that application.

The system tracks and reports any overuse for later billing. Overdraft protection is only available for the following concurrent and transaction licensed products:

- Integration Server Transaction Pack
- ImageNow Client
- Combo Client
- Message Agent Transaction Pack
- Interact Desktop

Generate overdraft licensing report

If you purchased overdraft licensing protection for Perceptive Content concurrent client licenses, you generate this report quarterly to send to Perceptive Software. An overdraft licensing report checks the usage status of your license overdrafts. To generate an overdraft licensing report, complete the following steps.

1. On the **ImageNow Server** computer, perform one of the following actions.
   - In Windows 32-bit, open a **Command Prompt**window and change to the *[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter `intool --cmdoverdraftintool --cmd overdraft --start-time"YYYY-MM-DD" --end-time "YYYY-MM-DD"` where start time is the beginning of the report period and end time is the end of the report period.

   Example By default, the start time is 12:00:00:00 MA GMT and the end time is 11:59:59: PM GMT.
3. When you receive a message similar to this one: `Report successfully written to overdraft_report_1173193645.txt"` , then the report has been successfully saved to the *[drive:]**inserver\bin*** folder. Close the command prompt.

Next E-mail the report to license@perceptivesoftware.com.

Manage the server

Change the inuser password

To change the inuser password in Perceptive Content, complete the following steps.

1. Stop the **Perceptive Content** services.
2. Change your password in your database application.
3. To change the **inuser** password for **Perceptive Content** Server running on Windows, complete the following substeps.
   1. Open the *inow.ini* file located at *[drive:]****inserver*****etc**.
   2. In the *inow.ini* file, under `[ODBC]`, for `odbc.user.password`, supply the new password.

      Example

      ```
      [ODBC]odbc.dsn=your_DBMS_type

      odbc.user.id=inuser

      odbc.user.password=your_password
      ```

   3. Save and close the *inow.ini* file.
4. To change the **inuser** password for **Perceptive Content** Server running on Linux, complete the following substeps.
   1. Open the *inow.ini* file located at *$(IMAGENOWDIR)/etc*.
   2. In the *inow.ini* file, under `[ODBC]`, for `odbc.user.password`, supply the new password.

      Example

      ```
      [ODBC]odbc.dbms=your_DBMS_type

      odbc.dsn=ImageNow 6

      odbc.user.id=inuser

      odbc.user.password=your_password
      ```

   3. Save and close the *inow.ini* file.
5. Start the **Perceptive Content** services.

Enable hidden search operators

By default, the Search and Quick Search tabs do not include contains, does not contain, ends with, and does not end with operators. To enable the hidden search operators, complete the following steps.

When you enable hidden search operators, any search that uses the *contains*, *does not contain*, *ends with*, or *does not end with* operator may slow ImageNow Server performance, depending on the volume of documents. For more information about VSL operators in Perceptive Content, refer to What is VSL?

1. On the **ImageNow Server** computer, navigate to the *[drive:]****inserver*****etc** directory and open the *inserver.ini* file in a text editor.

2. In the *inserver.ini* file, under `[Remote]`, set `vsl.extended.operators.enabled = true`.
3. Restart your **Perceptive Content** services.

inserver directories

The following section lists the default directories that are created after you install Perceptive Content Server and a description of the contents within these directories.

audit

This is the location for audit log files when the *audit.format* setting in the *inow.ini* file is set to 1 or 3, and auditing is enabled. Auditing logs are stored in an XML format and Perceptive Content exports a file for each 24-hour period during which a user member logged onto the system.

bin

This is the storage location for all Perceptive Content agent executable (EXE) files, DLLs, and the product readme PDF for 32-bit systems.

bin64

This is the storage location for all Perceptive Content agent executable (EXE) files, DLLs, and the product readme PDF for 64-bit systems.

db

This is the location for database tables for Perceptive Content Server using Embedded Perceptive Content SQL. If you install the Perceptive Content Server for an external DBMS, such as SQL Server or Oracle, this directory does not appear.

etc

This is the storage location for the configuration (INI) files for all locally installed agents. This directory also stores the hardware fingerprint license file, *in_hwfp*, required to license the Perceptive Content Server.

fax

This is the temporary storage location for image files received by the Fax Agent. By default, the system creates a subdirectory for each channel enabled on the fax board.

help

This is the location for Administrator Help (CHM) files.

install_temp

This is the storage location for files, such as default task and out of office reasons, used during the initial installation of Perceptive Content Server.

job

This is the location for pending jobs on the Perceptive Content Server for specific agents, such as Recognition Agent.

learnmode

This is the storage location for font files used for HyperLearn application plans. The Perceptive Content Server can store up to 50 font files in this directory.

log

This is the location for all upgrade, error, performance, and agent log files. To change the location of this directory, refer to Change the Perceptive Content log file directory location.

osm_01.00001

This is the storage location for all item objects. Each item page is stored as a separate Object Storage Manager (OSM) file.

osm_02.00001

This is the location for subobjects, such as annotations, applied to items.

osm_03.00001

This is the storage location for all items that currently appear in the All Batches view in Perceptive Content Explorer. After an item is indexed, the system removes that item from this directory and relocates the item, by default, to osm_01.00001.

script

This is the location that stores all scripts used in the Perceptive Content system.

temp

This is the temporary storage location used as a working directory by the Import Agent and Output Agent.

update

This is the location that stores the update packages used by the Automatic-Update service to deliver new updates to Perceptive Content.

user

This is the temporary storage location for all users when an operation, such as capture, requires that Perceptive Content send a file to Perceptive Content Server.

workflow

Files are not currently stored in this directory.

Troubleshoot connection issues

If you experience issues connecting in Perceptive Content or Interact Desktop, you can try one of the following possible resolutions.

Automatic logoff is not working

Cause	Resolution
TCP Port 7200 is not open on your network.	To enable communications between ImageNow Server and ImageNow Clients and agents, you must open a TCP port on your network. ImageNow Server requires this port to perform automatic logoff on ImageNow Client. Port 7200 is the default port for these communications, though you can modify the port by changing the `mq.agent.ip.port` setting in the *inow.ini* file after installation.

Users are not receiving workflow alarms

Cause	Resolution
The alarm rule is not configured correctly in Workflow Designer.	Test an alarm
TCP Port 7200 is not open on your network.	To enable communications between ImageNow Server and ImageNow Clients and agents, you must open a TCP port on your network. ImageNow Server requires this port to send workflow alarms. Port 7200 is the default port for these communications, though you can modify the port by changing the `mq.agent.ip.port` setting in the *inow.ini* file after installation.

Remoted agents cannot communicate with ImageNow Server

Cause	Resolution
TCP Port 7200 is not open on your network.	To enable communications between ImageNow Server and ImageNow Clients and agents, you must open a TCP port on your network. ImageNow Server requires this port to communicate with remote agents. Port 7200 is the default port for these communications, though you can modify the port by changing the `mq.agent.ip.port` setting in the *inow.ini* file after installation.

Users are unable to send documents to other users

Cause	Resolution
TCP Port 7200 is not open on your network.	To enable communications between ImageNow Server and ImageNow Clients and agents, you must open a TCP port on your network. ImageNow Server requires this port to send documents to users. Port 7200 is the default port for these communications, though you can modify the port by changing the `mq.agent.ip.port` setting in the *inow.ini* file after installation.
The user is no longer connected to ImageNow Client.	Verify the user is logged in.

Users are unable to connect to ImageNow Server

Cause	Resolution
A Windows NT user has not been granted the user rights to log on locally.	If the user was not allowed to log on to the server despite using the correct user name and password, and the user is configured in ImageNow Client, the administrator must give the user the right to log on locally to resolve this issue.
When you receive the "Host not found" message while attempting to connect to ImageNow Server, Perceptive Content is unable to locate the specified	Verify the following: • You have the correct IP address or host name in the Server ID box of the login profile.

Cause	Resolution
host or server.	• TCP/IP is installed and configured on the ImageNow Server host computer and the ImageNow Client local computer (workstation).

Users are unable to log in with LDAP user authentication

Cause	Resolution
The user account does not exist within the LDAP structure specified within the *inow.ini* file.	Verify that the user name and password are correct, and then verify that the LDAP settings under the `[Logon Control]` section in the *inow.ini* file are pointing to the correct LDAP structure and that the user account exists within that LDAP structure.
A `Confidentiality Required` message appears.	This message appears when you attempt to log in to ImageNow Client after you configure Perceptive Content for authentication against an LDAP server. Set the LDAP server to Allow Clear Text Passwords.
You are running Perceptive Content in an Oracle Solaris 8 environment, which causes case sensitivity in the *inow.ini* file.	Change the *inow.ini* LDAP settings to lowercase.
The number of users available for import in the following directories surpasses the maximum search results set by your LDAP server configuration.	Ask your LDAP administrator to increase the maximum search results setting on the LDAP server.

Users are unable to log in to Interact Desktop with Windows domain authentication

Cause	Resolution
When a user launches Interact Desktop, instead of bypassing the login screen, the login screen appears and in some instances, the user can log in to Interact Desktop without entering a password.	Verify domain authentication is enabled in the Interact Desktop profile and in the *inow.ini* file on the ImageNow Server computer.

Users are unable to log in with SQL user authentication

Cause	Resolution
An ODBC connection has not been set up.	Create an ODBC connection.
The user is inactive in the custom SQL database table or inactive in ImageNow Client.	Change the user s status to active or specify a different user.
A setting in the [ODBC] section of the *inow.ini* file is incorrect.	Check these settings for validity.
The logon.method in *inow.ini* is set to LDAP or SYSTEM.	Change this setting to SQL.
The auth.odbc.userid setting in the *inow.ini* lists a user name that does not have permission to access the database that contains the table specified in the select query.	Change this user setting.

Object Storage Manager

OSM definitions

OSMs are used to manage content. OSMs use either a primary set or a reference set to represent a logical collection of objects. Trees are used to define the physical storage of the sets. When a relationship is added to a set it becomes a cache set or a sub-object set. The following provides definitions for each set and the relationships allowed between them.

Primary Set

A primary set is a collection of documents controlled by Perceptive Content. In a primary set the user can create, retrieve, update and delete documents.

- Allows one related cache set
- Allows one related sub-object set, such as thumbnails
- Allows a filter to redirect documents back to the primary set

Reference Set

A reference set contains links to external documents that are separate from Perceptive Content. The user can add and delete the links to the external documents, however, external documents cannot be created, updated or deleted.

- Allows one related cache set, such as, local caching of documents stored on an external system
- Allows one related sub-object, such as, thumbnails of documents stored on external systems
- Cannot be used as a cache set
- Cannot be used as a sub-object set
- Cannot include a filter that redirects documents back to the reference set

Cache Set

A cache set has a relationship to another set and is used for local caching of documents.

- Includes one set that it is caching documents for
- Cannot contain a sub-object set
- Cannot be used as a sub-object set
- Cannot include another cache set of itself, such as, a cache of a cache
- Cannot include a filter that redirects documents back to the cache set

Sub-Object Set

A sub-object set has a relationship to another set and is used for storing objects, such as thumbnail images.

- Includes storage for one primary set
- Allows one related cache set
- Cannot be used as a cache set
- Cannot include another sub-object set related to itself, such as, a sub-object for a sub-object
- Cannot include a filter that redirects documents back to the sub-object set.

OSM features

The OSM provides the following features:

- Multiple OSMs - You can create separate object storage structures that can be subdivided by virtually any logical construct. This enables you to create a separate OSM structure for each drawer in your Perceptive Content system. This feature is useful when you want to separate information, such as Human Resource information, from other information.
- OSM spanning - You can represent several physical drives as one logical drive, which allows a single OSM to expand beyond the bounds of a single physical drive.
- OSM mirroring - You can enable mirroring to distribute duplicate object storage structures to multiple sites. This feature enables you to create a real-time duplicate OSM to support mission-critical functions, disaster recovery, and real-time backup.
- Data set management - You can easily move, copy, or delete OSM structures based on a wide variety of business rules.
- OSM caching - You can cache files that are read or written to the main OSM storage device on a faster device, such as a SAN, to improve performance and reduce bottlenecks. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

- OSM cache lifecycle management - You can adjust the cache lifecycle from the default of 1,440 minutes to a shorter or longer value.

OSM record fields

This topic outlines the record fields for OSM sets or trees. You can specify fields of this record in INTool commands.

OSM set fields

OSM set name

The name of the OSM set.

Values

This field represents a string, typically osm_ followed by a two-digit number. Use a leading zero if the value is less than 10.

Example

HR Files

OSM set location type

The ease of accessibility of the files in the OSM set.

Values

1 Online: The object files in the set are immediately accessible by Perceptive Content, typically on a local drive.

2 Near-line: The object files in the set are accessible by Perceptive Content, but storing and retrieving speeds are slower than for the online location type.

3 Offline: The object files in the set are not accessible. The user must restore the files to an online OSM to access them through Perceptive Content.

Example

1

Values

`0 Mixed`: The OSM can store any type of object.

`1 Document`: The OSM can store only document objects, which are pages.

`2 Cold (ERM)`: The OSM can store only ERM Serverobjects after conversion.

`3 Subob`: The OSM can store only subobjects, such as thumbnails and annotations.

`4 Batch`: The OSM can store only batch objects (pages).

OSM set type

The type of objects that can be stored in the set.

Example

1

OSM set description

Description of the OSM set.

Values

Any valid string.

Example

OSM set for HR files

Subobject OSM set name

The name of a subobject OSM set.

Values

This field represents a string, typically osm_ followed by a two-digit number. Use a leading zero if the value is less than 10.

Example

osm_02

Notes

Comments about the OSM set.

Values

Any valid string.

Example

Created especially for Human Resources

OSM Integration Type

The storage device type.

Values

0 FSS (File System Storage): Covers the file systems supported by all platforms.

2 EXT (External Storage): Is used with External plugins.

OSM tree fields (FSS)

OSM tree name

The unique ID of the OSM tree.

Values

This field represents a string, typically osm_ followed by a two-digit number. Use a leading zero if the value is less than 10.

Example

osm_01.0001

OSM set name

The unique ID of the OSM set.

Values

This field represents a string, typically osm_ followed by a two-digit number. Use a leading zero if the value is less than 10.

Example

osm_01

OSM Tree Description

A descriptive string that describes the OSM tree.

Example

Created for HR.

Retrieve Tree

When mirroring is enabled, the tree from which to retrieve data.

Values

0 (primary): Retrieves data from the primary tree.

1 (mirror): Retrieves data from the mirror tree.

Example

0

Mirroring

Enable the file to be stored in two places.

Values

0 (mirroring off): Stores the file in one location.

1 (mirroring on): Stores the file in two locations.

OSM tree path

The file directory that points to the OSM tree.

Values

The valid file directory for the OSM tree. The path syntax must conform to the file path conventions of the operating system.

Example

C:\inserver6\osm_01.00001

OSM tree next slot

The location where the next file is stored.

Values

Three black-slash separated eight-digit numeric strings.

Example

00000000/00000000/00000002

Subobject OSM set name

The unique ID of the OSM set.

Values

This field represents a string, typically osm_ followed by a two-digit number. Use a leading zero if the value is less than 10.

Example

osm_02

Media Type

Specifies the physical medium used to store data.

Values

0: Represents magnetic storage.

1: Represents optical storage.

Example

0

Mirror Media Type

Specifies the physical medium used to store mirrored data when mirroring is enabled.

Values

0: Represents magnetic storage.

1: Represents optical storage.

Example

0

Example

1

Files per directory in OSM tree

The maximum number of files or subfolders in each OSM directory.

Example

20

Retries

The number of times the server attempts to store a file it if fails on the first try.

Example

3

Delay

The wait time, in seconds, between retries of storing a file.

Example

15

OSM set caching support information

When you create a new OSM set, you can cache to another existing OSM set. In this case, you are prompted for the cache OSM set name. When you provide the name, Perceptive Content enables caching. The cached OSM set has read-only caching with a lifetime of 1440 minutes.

You can also cache to an OSM set when adding a new OSM set by providing the name in the record. You can specify the record as follows:

```
^<osm set name>^<osm set location type>^<osm set type>^<osm set
description>^<subob osm set name>^<notes>^<integration type>^[<cache osm
set name>]^
```

In this example, the final field `<cache osm set name>` is optional.

If you do not provide a record, prompts appear for each field. Whether you provide the record or not, a prompt appears for the OSM cache set name field.

Move the OSM

Due to drive space considerations, you may need to redirect or move the OSM structure. We recommend redirecting the OSM structure if possible. However, if you must move the OSM, complete the following steps as they apply to your environment.

Prerequisite Depending on the number of images you have on your Perceptive Content system, moving OSM_01 may take a long time. Performance during quality assurance, linking, or OCR may suffer if you place OSM_02 and OSM_03 and any additional OSM sets on separate drives or on slower network shared drives. Perceptive Content services also must have Read/Write/Delete access to the OSM structure.

1. Stop all **Perceptive Content** services and perform the following substeps:
   1. View the list of **OSM** sets you need to move using **INTool** commands.
   2. Run the `list-osm-trees` command to find all of the **OSM** trees that need to be moved.
   3. For each tree, run the `update-osm-tree` command and follow the prompts.

      The fields that are required to update an FSS tree can be found at the following location: `OSM Tree^OSM Set^^Description^Mirroring^^Tree Path^^Next Slot^^^^FilesPerDirectory^Retries^Delay` and `osm_07.00001^osm_07^0^centera cache tree^0^0^$(IMAGENOWDIR)/osm_07.00001^^00000000/00000000/00000027^0^0^0^50^3^60^`
   4. Log on to the new storage device as a user with **Read/Write/Delete** access.
   5. On the new storage device, create the new **OSM** path or paths. For example, `/opt/instore/osm_01.00001`.
   6. Move all the subdirectories and files from the **original osm_01** directory to the **new osm_01** directory that was previously created.

   Note: Depending on the number of images, this may take some time.
2. Repeat the substeps for **OSM_02** and **OSM_03**, making sure to modify the SQL update statement to reflect each **OSM**.
3. Start all **Perceptive Content** services and test them to determine if the move was successful by performing the following substeps:
   1. Log in to **Perceptive Content** and open an existing multi-page document.
   2. In **ImageNowViewer**, verify that the thumbnails appear.
   3. Scan or import a document in **Batch** mode without selecting **Bypass QA** or **Automatic Server Processing**.

4. Navigate to **ImageNowViewer** and verify that there are **OSM** files within the **OSM_03** structure with a timestamp close to the current time.
5. Test and link the batch, and then verify that the **OSM** files are not in the **OSM_03** structure.
6. Open a document page from the batch you scanned or imported three steps ago.
7. Click **View > Thumbnails** and verify that thumbnails appear normally.
8. Close the document.

Next Delete a document and verify that it was a normal deletion.

Set up OSM caching

You can cache files that are read or written to the main OSM storage device on a faster device, such as a SAN, to improve performance and reduce bottlenecks. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects. To set up OSM caching, complete the following high level steps.

Prerequisite You must have the default OSM sets that are created automatically during installation of Perceptive Content.

1. To create the cache **OSM** set and **OSM** tree, complete the following substeps.
   1. To create a new **OSM** set, run the `intool --cmd add-osm-set` command.
   2. To create the new **OSM** tree, run the `intool --cmd add-osm-tree` command.
   3. To point the **OSM** set to the **OSM** tree, run the `add-osm-set` command. Provide the same values for the options as you did in the command. You must set the writable tree name to the tree you created in `add-osm-tree`: `intool --cmd update-osm-set`.
2. To point the permanent **OSM** storage set to the cache **OSM** set, complete the following substeps.
   1. To set up an **OSM** cache so that items are added to the cache if a cache-miss occurs when getting an item, run the `intool --cmd add-osm-cache --permanent-osm-set osm_01 --cache-osm-set osm_04`command.
   2. Optional. To enable asynchronous write caching, run the `intool --cmd update-osm-cache --permanent-osm-set osm_01 --cache-level read-write` command.

      Note: When write caching is enabled, to observe the write job states from the ImageNow Client toolbar, click **Settings > Job Manager.** The File System Agent service is responsible for these job states.
3. Optional. To update the amount of time an item resides in the cache, run the `intool --cmd update-osm-set` command.
4. Optional. To update your **OSM** cache settings, navigate to the *inserverFT.ini* file and open. In the **[General]** section, adjust **OSM** cache settings.
   1. To change the number of retry attempts for an **OSM** write cache job, adjust the value for the **max.osm.replication.retries** setting. The default value is 3.

      Note: The time between retries for the job framework in general is managed by the **auto.resume.interval** setting in the *[drive:]\inserver\etcinserverJob.ini* file. The default value is

600 seconds.

2. To change the number of **OSM** cache replication threads (asynchronous), adjust the value for the **num.osm.replication.workers** setting. The default value is 2.
3. Save and close the file.

Delete an OSM cache set

You can use the `delete-cache-set` command to delete an OSM cache set from both the database and the file system. The command first disables the specified cache and then attempts to delete the cache set and any associated objects still in the cache. If the cache is configured as a write-cache and all objects have not been replicated to the permanent set, the command terminates and intentionally leaves the cache in a disabled state. Once the OSM Agent replicates all objects, you can rerun the command to complete the cache set deletion. The file system directories associated with the cache are then deleted. To delete an OSM cache set, complete the following steps.

1. On the Perceptive **Content Server** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the `intool --cmd delete-cache-set --cache-set <cache set name>` command.

The following example deletes the OSM cache set with the name `centera_cache`.

```
intool --cmd delete-cache-set --cache-set centera_cache
```

OSM Sets

About OSM sets

OSM sets are used to logically define collections of content and how those collections are related to one another. Primary, cache, and subobject sets are all primary sets. However, the relationship added to a primary set changes it to a cache or subobject set. A primary set is used for content storage and retrieval. A reference set is used when retrieving content from external systems. Cache sets are used to cache content from related sets. subobject sets are used to store annotations and thumbnails from content in related sets. Each set requires an associated OSM tree. The OSM tree is responsible for the physical interactions with the underlying file system (FSS tree) or external storage (EXT trees). Note that EXT sets cannot be cache sets. You would need an FSS cache set corresponding to an EXT primary set.

Primary sets

Primary sets are the main mechanism used to store and retrieve documents created by, or captured into Perceptive Content. In a primary set the user can create, retrieve, update, and delete documents.

- Includes an FSS or EXT OSM tree
- Allows one related cache set
- Allows one related subobject set, such as thumbnails
- Allows filters to redirect documents back to the primary set

Note: Several primary sets are created automatically to contain different categories of data used in different phases of capture and storage. For example, one OSM set contains temporary data for items in batch processing, and another contains supporting data for annotations. You can create additional sets for special purposes.

Reference sets

A reference set contains links to external documents that are separate from Perceptive Content s OSM. Reference sets allow access to an existing reference object but are read-only. When modifying a document containing reference objects, the modified object is transferred into a primary set based on the document s filtering rules. If the reference object is removed from Perceptive Content, the object continues to reside in the originating storage solution. Removing files from Perceptive Content does not delete them from the reference sets.

Note:

- Includes an EXT OSM tree
- Allows one related cache set, such as, local caching of documents stored on an external system
- Allows one related subobject, such as thumbnails of documents stored on external systems
- Cannot be used as a cache set
- Cannot be used as a subobject set
- Cannot be the destination set of a filter

Cache sets

A cache set has a relationship to a primary set or a reference set and provides local caching of content located in the related set.

- Includes an FSS tree
- Includes one set for which it is caching content
- Cannot contain or be used as a subobject set
- Cannot include another cache set of itself, such as a cache of a cache
- Cannot include a filter

Subobject sets

A subobject set has a relationship to a primary set or a reference set, and provides storage for content thumbnail images and annotations.

- Includes an FSS or EXT tree
- Includes storage for one primary set
- Allows one related cache set
- Cannot be used as a cache set
- Cannot include another subobject set related to itself, such as a subobject for a subobject
- Cannot include a filter

Add an OSM set

When you install Perceptive Content, several primary OSM sets are created automatically to contain different categories of data used in different phases of capture and storage for items. Primary sets are the main mechanism for storing and retrieving documents created by, or captured into Perceptive Content. You can also create additional primary or reference OSM sets. Reference sets allow you to retrieve a document with pages that refer to content previously created or captured into another system. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects. To create and implement a custom OSM set, complete the following steps.

1. On the **Perceptive Content** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. To add a primary or reference set, perform one of the following actions.
   - To add a primary set, type `intool --cmd add-osm-set`.
   - To add a reference set, type `intool --cmd add-osm-set --reference`.
3. The **INTool** command prompts you for the required properties. Alternatively, you can provide information using one of the following record formats [`--record <record>`], set off with quotation marks.
   - Record format for primary sets. `Set_Name^Location_Type^Set_Type^Set_Desc^Subob_OSM_Set_Name^Notes^Integration_Type^[Cache_OSM_Set_Name^]`
   - Record format for reference sets. `Set_Name^Location_Type^Set_Desc^Subob_OSM_Set_Name^Notes^[Cache_OSM_Set_Name^]`

The following example creates a primary OSM set called `osm_40`.

```
intool --cmd add-osm-set --record "osm_40^1^1^OSM set for HR
files^osm_41^Created for a filter^0^osm_40_cache"
```

The following example creates a reference OSM set called `osm_50`.

```
intool --cmd add-osm-set --reference --record "osm_50^1^OSM reference
set for legacy files^^Created to reference existing documents in the
legacy system^"
```

Next After creating the OSM set, you must create a corresponding OSM tree before you can use the OSM set.

Display all OSM sets

There are two types of OSM sets: primary sets and reference sets. You can view only primary sets, only reference sets, or all OSM sets. To view the properties of these sets, complete the following steps.

1. On the **Perceptive Content** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. To view the properties of one or both set types, perform one of the following actions.
   - To display all primary OSM sets, type `intool --cmd list-osm-sets --primary`
   - To display all reference OSM sets, type `intool --cmd list-osm-sets --reference`
   - To display all OSM sets, type `intool --cmd list-osm-sets`

Update an OSM set

To change certain properties of an existing OSM set, complete the following steps. If the OSM set already contains items, you should leave all fields in the OSM set record unchanged except for the Description and Notes fields. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or subobjects.

1. On the **Perceptive Content** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. To update a primary or reference set, perform one of the following actions.
   - To update a primary set, type `intool --cmd update-osm-set`.
   - To update a reference set, type `intool --cmd update-osm-set --reference`.
3. The **INTool** command prompts you for the required properties. Alternatively, you can update the description and notes using one of the following record formats [`--record <record>`], set off with quotation marks.
   - Record format for primary sets. `Set_Name^Location_Type^Set_Type^Set_Desc^Subob_OSM_Set_Name^Notes^Integration_Type^[Cache_OSM_Set_Name^`
   - Record format for reference sets. `Set_Name^Location_Type^Set_Desc^Subob_OSM_Set_Name^Notes^[Cache_OSM_Set_Name^]`

The following example updates a primary OSM set with new Description and Notes information.

```
intool --cmd update-osm-set --record "osm_40^1^1^Personnel Data^osm_
41^Was formerly HR Files^0^osm_40.00001^"
```

Delete an OSM set

OSM sets contain different categories of data used in different phases of capture and storage. To delete an OSM set, complete the following steps. This procedure does not remove the OSM directory.

Prerequisite The OSM set must be empty before you can delete it.

1. On the **ImageNow Server** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following `intool --cmd delete-osm-set --osm-set <OSM Set Name>` command. You must provide information for the following parameter.
   - <OSM Set Name> is the name of the OSM set you are removing.

The following example deletes the OSM set with the name osm_01.

```
intool --cmd delete-osm-set --osm-set osm_01
```

OSM Filters

What are OSM filters?

An OSM filter enables you to store newly captured items in separate OSM sets, which function as filter sets.

OSM filters contain a single filtering condition: either a drawer name and value or an item type and value. As a result, you create a drawer filter or a key filter for an item. To update an existing filter, change the OSM set in which filtered items are stored. Filters affect only items that are captured after the filter's creation.

For example, you create an OSM filter to store all items with a drawer value of AP in a separate OSM set. You also create an OSM filter to store all items with an Invoice item type value in a separate OSM set. In the situation where a newly captured item has a drawer value (for example, AP) that satisfies one filter's condition and also an item s key value (for example, Invoice) that satisfies another filter's condition, the drawer filter is used instead of the item s key filter.

Note:
You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or subobjects.

Add an OSM filter

An OSM filter enables you to store newly captured items in separate OSM sets, which function as filter sets. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects. To create and implement an OSM filter, complete the following steps.

1. On the **Perceptive Content** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64*

directory.
- In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.

2. Enter the following `intool --cmd add-osm-filter --osm-set <OSM Set Name> --type <type> --value <value>` command. Provide information for the following parameters.
   1. `<OSM Set Name>` is the name of the **OSM** set in which the filter items are stored.
   2. `<type>` is either `DRAWER`, `RECORD CATEGORY`, `FOLDER TYPE`, or `DOCTYPE`, depending on which item key you want to filter on. It is case sensitive.
   3. `<value>` is the name of the drawer, record category, folder type, or document type corresponding to the `DRAWER`, `RECORD CATEGORY`, `FOLDER TYPE`, or `DOCTYPE` selection.

The following example adds an OSM filter that stores all newly captured items with a drawer value of `DEFAULT` in the OSM set called `osm_08`.

```
intool --cmd add-osm-filter --osm-set osm_08 --type <value> --value
DEFAULT
```

Display all OSM filters

To show information about all active OSM filters, complete the following steps.

1. On the **OSM** computer, do one of the following actions.
   - In Windows, open a command prompt window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. To display all **OSM** filters, type `intool --cmd list-osm-filters`.

Update an OSM filter

To change the destination OSM set of an existing OSM filter, complete the following steps. Note that you cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

Prerequisite If the destination OSM set does not yet exist, you must create it and the corresponding OSM tree before you can update the OSM filter.

1. On the **Perceptive Content** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following command: `intool --cmdupdate-osm-filter--osm-set <OSM Set Name> --type <Type> --value <value>`. You must provide information for the following parameters.
   - <OSM Set Name> is the name of the OSM set where filtered documents are stored.
   - <Type> is DRAWER or DOCTYPE, whichever type applies to the filter you are updating. This value is case-sensitive.
   - <Value> is the drawer name or document type name used in the existing filter.

The following example updates an OSM filter of items with a DRAWER value of DEFAULT and changes the destination OSM set to osm_40.

```
intool --cmdupdate-osm-filter--osm-set osm_40 --type DRAWER --value
DEFAULT
```

Delete an OSM filter

Removing an OSM filter has no effect on any filtered items. They remain in the set designated by the filter. To delete an OSM filter from ImageNow Server, complete the following steps.

1. On the **ImageNow Server** computer, do one of the following actions.
   - In Windows 32-bit, open a command prompt window and change to the *[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a command prompt window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following `intool --cmd delete-osm-filter --type <filter type> --value <filter value>` command. You must provide information for the following parameters.
   - <filter type> depends on the key used to define the filter. It is case sensitive.
   - <filter value> is the name of the container or item type.

The following example deletes an OSM filter that filters all newly captured documents assigned to the DEFAULT container.

```
intool --cmd delete-osm-filter --type DRAWER --value DEFAULT
```

OSM Trees

About OSM trees

OSM trees help manage the content in an OSM set. A set represents the logical collection of objects, while a tree defines the physical storage of objects by defining the structure of directories and sub-directories where captured items are stored.

There are a limited number of slots in one OSM tree, so you may need to create additional OSM trees to continue storing to the same device, just within a different directory. When the original OSM tree uses up its available disk space, Perceptive Content Server automatically moves to the next OSM tree with no interruption in service.

OSM sets and OSM trees use two integration types.

File System Storage (FSS)

Designates storage to a file system available to the OSM.

Can associate with a primary set but not a reference set.

External Storage (EXT)

Designates storage to an external source and requires a specialized OSM plugin.

Can associate with a primary set and a reference set.

Add an OSM tree

To define an OSM set that you expect to become very large, you can create a separate OSM tree for each additional drive you may need. To create and implement an OSM tree, complete the following steps.

1. On the **Perceptive Content Server** computer, complete one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR/BIN* directory.
2. Enter the following `intool --cmd add-osm-tree --type <integration type> [--record <record> [--delim <delim>]]` command. You must provide information for the following parameters.
   1. *<integration type>* is the storage device type. Valid values are FSS (File System Storage) and EXT (External File Storage), which utilizes OSM plugins.
   2. *<record>* is the information that describes the **OSM** tree record.
   3. *<delim>* is the delimiter that separates the values between the record fields. The default delimiter is ^.

The following example creates an FSS OSM tree called osm_40.00001. The record definition must be off set with quotation marks.

```
intool --cmd add-osm-tree --type FSS --record "osm_40.00001^osm_
40^TreeDescription^0^0^/opt/inserver/osm_
40.00001^^00000000/00000000/00000000^0^0^0^512^5^1^ "
```

Display all OSM trees

OSM trees define the structure and database locations of documents in an OSM set. To display all OSM trees in an OSM set, complete the following steps.

1. On the **ImageNow Server** computer, perform one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. To view all **OSM** trees added to an **OSM** set, enter the following command: `intool --cmd list-osm-trees --osm-set <OSM Set Name>`. You must provide information for the following parameter.
   - <OSM Set Name> is the name of the OSM set that contains the OSM trees.

The following example displays information for all trees added to the OSM set called osm_40.

```
intool --cmd list-osm-trees --osm-set osm_40
```

Update an OSM tree

To change certain properties of an existing OSM tree, complete the following steps. If the OSM tree already contains documents, you should leave all fields in the OSM tree record unchanged except for the Description, Retries, and Delay fields.

1. On the **Perceptive Content Server** computer, complete one of the following actions.
   - In Windows, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following command: `intool --cmd update-osm-tree --type <integration type> [--record <record> [--delim <delim>]]` and provide information for the following parameters.
   - <integration type> is the storage device type. Valid values are FSS (File System Storage) and EXT (External File Storage). FSS is accepted by all platforms and EXT is used with OSM plugins.
   - <record> is the information that describes the OSM tree record.
   - <delim> is the delimiter that separates the values between the record fields. The default delimiter is ^.

The following example updates an FSS OSM tree with new Description, Retries, and Delay information.

```
intool --cmd update-osm-tree --type FSS --record "osm_23.00001^osm_
23^new
description^0^0^c:\inserver6\treefolder^^00000000/00000000/00000000^0
^0^0^5125^1"
```

Delete an OSM tree

OSM trees define the structure and database locations of items in an OSM set. To remove an OSM tree from an OSM set, complete the following steps.

Prerequisite The OSM tree must be empty before you can delete it.

1. On the **ImageNow Server** computer, complete one of the following actions.
   - In Windows, open a command prompt window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following `intool --cmd delete-osm-tree --osm-tree <OSM Tree Name>` command. You must provide information for the following parameter.
   - <OSM Tree Name> is the name of the OSM tree you are removing.

The following example deletes the OSM tree with the name osm_01.00001.

```
intool --cmd delete-osm-tree --osm-tree osm_01.00001
```

Server information

Export ImageNow Server technical information

To export ImageNow Server technical information to a text file, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the right pane, click **Server Information > Export**.
3. In the **Save As** dialog box, specify the file name and location, and then click **Save**.

Run diagnostic system information report

To run a diagnostic system information report using a command, complete the following steps.

1. Click **Start > Run**.
2. In the **Run** dialog box, type `cmd`, and then click **OK**.
3. On the **ImageNow Server** computer, do one of the following substeps:
   1. In **Windows 32-bit**, open a **Command Prompt** window and change to the ***[drive:]\inserver\bin*** directory.
   2. In **Windows 64-bit**, open a **Command Prompt** window and change to the ***[drive:]\inserver\bin64*** directory.
   3. In **UNIX**, change to the *$(IMAGENOWDIR)/bin* directory.
4. At the **Command Prompt** window, type the `intool --cmd run-system-report` command.

   The command returns a combination of system, hardware, and performance reports for diagnostic purposes.

Use a terminal server

About using ImageNow with a terminal server

Using Perceptive Content with a terminal server allows you to remotely access ImageNow Client using a computer acting as a thin client.

The benefits of using a terminal server as a thin client are to leverage older hardware, simplify software deployment, and use lower bandwidth connections.

Perceptive Content is compatible with terminal server applications such as Microsoft Terminal Services and Citrix Presentation Server (formerly Citrix Metaframe/Winframe) products.

Citrix Presentation Server is a presentation layer that relies upon the Microsoft Windows Terminal Services. It builds on the foundation of the Terminal Services application and enables the publishing of applications to Citrix applications, rather than publishing the entire Windows desktop. Citrix requires Microsoft Terminal Services. However, Terminal Services does not require Citrix. The benefits of using Citrix are increased efficiency over low bandwidths, improved manageability and security, and load balancing among many servers in a Citrix farm.

Paths for a terminal server

When you set up Perceptive Content on a terminal server, you can modify the inowsystem.ini file to provide paths to your working folder and the folder that contains your Perceptive Content executable file. You can type the actual path or you can also insert environment variables in the path to make the path dynamic.

This environment variable is determined by the user who is logged into Windows and is not the same as the Perceptive Content user name. For example, if you use an environment variable for the user called %USERNAME%, you can add the following path to the inowsystem.ini file: `WorkPath=Z:\%USERNAME%\imagenow\work`. When the currrent user is Jeff Smith, the resulting path is actually Z:\JeffSmith\imagenow\work.

The following list contains sample paths to help you determine the path to define.

Example assignments for [Paths]

```
[Paths]WorkPath=\\NetPath\user1\ImageNowWork

[Paths]WorkPath=C:\Program Files\ImageNowWork\%USERNAME%

[Paths]WorkPath=C:\Program Files\ImageNowWork"ExePath="C:\Program
Files\ImageNow

[Paths]WorkPath=C:\Program Files\ImageNow"ExePath="C:\Program
Files\ImageNow
```

Set up ImageNow Client on a terminal server

To set up ImageNow Client on a terminal server, complete the following steps.

Prerequisite Citrix XenApp 5 with hotfix rollup 6 is not compatible with Management Console. To enable XenApp 5 to run with Management Console, apply hotfix PSE450R06W2K3001 for 32-bit systems, or apply hotfix PSE450R06W2K3X64001 for 64-bit versions. Refer to the Citrix support website for information.

1. Install the same version of **ImageNow Client** on each terminal server.
2. Optional. By default, the first time you launch **ImageNow Client** on a terminal server, a user's application settings are installed and stored in configuration files in *[drive:]:\Documents and Settings\<%username%>\Application Data\ImageNow*. You can automate copying these files from one terminal server to the other terminal servers on a regular basis, or to redirect the terminal servers to use the same inowsystem.ini file from a shared network path, you can perform the following substeps on each terminal server.
    1. On the terminal server, if the *[drive:]\Program Files\ImageNow6\inowsystem.ini* file exists, open the file in a text editor. If the file does not exist, open a new document in a text editor, and save

the text document to this folder as **inowsystem.ini**.

2. In the **inowsystem.ini** file, add the following lines. Replace `<path to INI files>` with the path to your working files, which includes the INI, log, and temporary files; forms; and the batch, temp, and workflow folders. Replace `<path to EXE file>` with the path to your executable files, which includes the EXE, DLL, Help, and Readme files; demo apps and images; splash screen; and the INowSystem.ini file.

   An ideal work path is a network share that all terminal servers can access. For example, `WorkPath=\\<domain>.com\users\%username% [Paths] WorkPath=<path to INI files> ExePath=<path to EXEfiles>`.

3. Save and close the file.
4. Start **ImageNow Client**.

Troubleshoot terminal server issues

If you encounter issues using a terminal server, try any of the following possible resolutions.

LearnMode issues

Cause	Resolution
LearnMode does not work if ImageNow Client is local and the business application is installed on a terminal server.	Install both ImageNow Client and the business application on the terminal server. With a terminal server, application processing takes place on the terminal server, rather than on the local desktop. The user sees a mirror of the application session on the terminal server of the local desktop. Therefore, LearnMode does not work if the business application is on the terminal server and ImageNow Client is on the local desktop. This is also often true when you install the business application on the local desktop and ImageNow Client on the terminal server. Occasionally, HyperLearn does work if you install ImageNow Client on the desktop and the business application on the terminal server.
LearnMode works intermittently when ImageNow Client and the business application are both installed on a terminal server.	When publishing applications through terminal servers, configure the environment so that ImageNow Client and the business application launch simultaneously. To do this create a batch file that launches both the business application and ImageNow Client and that configure the business application shortcut to point to the batch file. This situation generally occurs if there is more than one server in the terminal server farm. For example, when a user launches the business application, the

Cause	Resolution
	business application may launch from terminal server A, and when the user launches ImageNow Client, the client may launch from terminal server B. Since the business application and ImageNow Client reside in sessions on two different servers, LearnMode cannot access the business application.

ImageNow Client issues

Cause	Resolution
ImageNow Client features work for the Windows Administrator user, but not for other users.	Switch to Install mode before installing ImageNow Client. 1. On the terminal server, open a window that accepts command prompts. 2. Enter `change user /install`. 3. Enter the command to launch the ImageNow Client installation. For example, *ClientSetup.exe*. By default, a Terminal Services session starts in Execute Mode. In this mode, any application you install places the necessary DLL files in the users Windows directory (*[drive]:\Documents and Settings\<username>\WINDOWS*), rather than the systems Windows directory (*[drive]:\WINDOWS*).
ImageNow Client issues that should be resolved by an upgrade are only resolved intermittently.	Verify that the correct version of ImageNow Client is running on all servers in the farm. If you upgraded the ImageNow Client to fix an issue and later discover that it is only resolved intermittently, most likely ImageNow Client was upgraded on some but not all of the servers in the terminal server farm.
ImageNow Client slows down performance for all applications on the same terminal server.	Turn off animations by changing the `scroll.login.image` setting to 0 (zero) in the *imagenow.ini* file. Animations in ImageNow Client can slow the performance of one or more of the CPUs on a terminal server.
I am unable to disable features on the ImageNow Client login screen.	Disable the ImageNow Client login options.

Interact Desktop Issues

Cause	Resolution
Interact Desktop features work for the Windows Administrator user, but not for other users.	Switch to Install mode before installing Interact Desktop. 1. Open a window that accepts command prompts on the Citrix server. 2. Enter `change user /install`. 3. Enter the command to launch the Interact Desktop installation. For example, *ClientSetup.exe*. By default, a Citrix server session starts in Execute Mode. In this mode, any application that you install places the necessary DLL files in the users Windows directory (*[drive]:\Documents and Settings\<username>\WINDOWS*), rather than the systems Windows directory (*[drive]:\WINDOWS*).
Interact Desktop issues that should be resolved by an upgrade are only resolved intermittently.	Verify that the correct version of Interact Desktop is running on all servers in the terminal server farm. If you upgraded Interact Desktop to correct an issue and later discover that it is only resolved intermittently, most likely Interact Desktop was upgraded on some but not all of the servers in the terminal server farm.
A maximized host application window in Citrix hides the Interact Desktop toolbar.	Run Interact Desktop in Citrix s published desktop mode or resize the host application window manually. Citrix does not support docking windows when you run a published application. Interact Desktop presents a minimized toolbar at the side of the window. When you maximize any host application window, that window overlaps the Interact Desktop toolbar.

Troubleshoot ImageNow Client issues on terminal servers

If you encounter any issues using ImageNow Client on terminal servers, try any of the following possible resolutions

ImageNow Client features work for the Windows Administrator user, but not for other users.

Switch to Install mode before installing ImageNow Client. On the terminal server, open a window that accepts command prompts. Enter `change user /install`. Enter the command to launch the ImageNow Client installation, such as `Client-Setup.exe`.

By default, a Terminal Services session starts in Execute Mode. In Execute Mode, any application you install places the necessary DLL files in the users Windows directory, *[drive]:\Documents and Settings\<username>\WINDOWS*, rather than the systems Windows directory, *[drive]:\WINDOWS*.

ImageNow Client issues that should be resolved by an upgrade are only resolved intermittently.

Verify that the correct version of ImageNow Client is running on all servers in the terminal server farm.

If you upgraded ImageNow Client to fix an issue and later discover that it is only resolved intermittently, most likely ImageNow Client was upgraded on some but not all of the servers in the terminal server farm.

ImageNow Client slows down performance for all applications on the same terminal server.

Turn off animations in ImageNow Client by changing the `scroll.login.image` setting in the imagenow.ini file to `0`.

Animations in ImageNow Client can slow the performance of one or more of the CPUs on a terminal server.

I cannot disable features on the ImageNow Client login screen.

Disable the ImageNow Client login options.

Troubleshoot Interact Desktop issues on terminal servers

If you encounter issues using Interact Desktop on terminal servers, try any of the following possible resolutions.

Interact Desktop features work for the Windows Administrator user, but not for other users.

Switch to Install mode before installing Interact Desktop. Open a window that accepts command prompts on the Citrix server. Enter `change user /install`. Enter the command to launch Interact Desktop installation, such as `Client-Setup.exe`.

By default, a Citrix server session starts in Execution Mode. In Execution Mode, any application you install places the necessary DLL files in the users Windows directory, *[drive]:\Documents and Settings\<username>\WINDOWS*, rather than the systems Windows directory, *[drive]:\WINDOWS*.

Interact Desktop issues that should be resolved by an upgrade are only resolved intermittently.

Verify that the correct version of Interact Desktop is running on all servers in the terminal server farm.

If you upgraded Interact Desktop to correct an issue and later discover that it is only resolved intermittently, Interact Desktop was upgraded on some but not all of the servers in the terminal server farm.

A maximized host application window in Citrix hides the Interact Desktop toolbar.

Run Interact Desktop in Citrix s published desktop mode or resize the host application window manually.

Citrix does not support docking windows when you run a published application. Interact Desktop presents a minimized toolbar at the side of the window. When you maximize any host application window, that window overlaps the Interact Desktop toolbar.

Troubleshoot LearnMode issues on terminal servers

If you encounter issues using LearnMode on a terminal server, try any of the following resolutions.

LearnMode does not work if ImageNow Client is local and the business application is installed on a terminal server.

Install both ImageNow Client and the business application on the terminal server.

With a terminal server, application processing takes place on the terminal server, rather than on the local desktop. The user sees a mirror of the application session on the terminal server of the local desktop. Therefore, LearnMode does not work if the business application is on the terminal server and ImageNow Client is on the local desktop. This is also often true when you install the business application on the local desktop and ImageNow Client on the terminal server. Occasionally, HyperLearn does work if you install ImageNow Client on the desktop and the business application on the terminal server

LearnMode works intermittently when ImageNow Client and the business application are both installed on a terminal server.

When publishing application through terminal servers, configure the environment so that ImageNow Client and the business application launch simultaneously. To do this, create a batch file that launches both the business application and ImageNow Client and then configure the business application shortcut to point to the batch file.

This situation generally occurs if there is more than on server in the terminal server farm. For example, when a user launches the business application, the business application may launch from terminal server A, and then the user launches ImageNow Client, the client may launch from terminal server B. Since the business application and ImageNow Client reside in sessions on two different servers, LearnMode cannot access the business application.

Configure your database

What is INEMUSER?

Perceptive Content includes a database user, called INEMUSER, which enables external applications to activate events through External Messaging Agent.

A user logged into the INOW6 database as the external messaging user has sufficient privileges to add, remove, and update data in the External Messaging Agentdatabase tables without risk of corrupting information stored in the Perceptive Contentdatabase. Additionally, external applications can only access the Perceptive Content database through the external messaging user. Refer to your ImageNow Server installation guide for instructions on creating the INEMUSER user account.

Configure DataDirect DSN to enable SSL encryption

The Secure Sockets Layer (SSL) is an encryption security protocol that helps protect your data during a transfer. To configure DataDirect DSN to enable SSL encryption, complete the following steps.

Prerequisite This process can differ for different versions of Microsoft SQL Server. Refer to Microsoft documentation before configuring SSL encryption.

1. In the **ODBC Data Source Administrator**, open the **System DSN** tab.
2. Select the system data source and click **Configure**.
3. On the **Security** tab, in the **Encryption Method** box, complete one of the following options:
   - For Perceptive Content**SQL Wire** protocol, select **1 - SSL**.
   - For Perceptive Content**Oracle Wire** protocol, select **1 SSL Auto**.
4. Optional. To test the connection, click **Test Connection**.
5. Click **OK**.

Configure SQL Server to use a certificate for SSL

To configure Microsoft SQL Server to use a certificate for SSL validation, complete the following steps.

Prerequisite This process can differ for different versions of Microsoft SQL Server. Refer to Microsoft documentation before configuring SSL encryption.

1. Open **SQL Server Configuration Manager**.
2. In the left pane, right-click the **SQL Server instance** you want to use, and then select **Properties**.
3. Complete one of the following options in the **Force Encryption** box:
   - If you require encryption, select **Yes**.
   - If you do not require encryption, select **No**.
4. In the **Hide Instance** field, select **No**.
5. Open the **Certificate** tab and, in the **Certificate** box, select the certificate you want to use, and then click **OK**.
6. Restart the **SQL Server** service.

Import a certificate for SQL Server on Windows

SQL Server uses a certificate imported from a Certificate Authority for encryption. To import a certificate from a Certificate Authority into the certification store on Windows, complete the following steps.

1. On the Microsoft SQL Server computer, open a **Command Prompt** window and change to the *[drive:]****inserver*****bin*** directory.
2. In the **Command Prompt** window, run *mmc.exe*.
3. To add the certificates snap-in for the local machine, click **File > Add/Remove snap-in > Certificates**.
4. Select **Computer account**, click **Finish** and click **OK**.
5. In the tree view, navigate to **Certificates > Personal** and right-click **Certificates**.
6. Select **All Tasks > Import**.
7. In the **Certificate Import Wizard** dialog, browse to the PFX file and click **Next**.
8. To import the key, enter the password, select the options you want, and then click **Next**.
9. To secure your PFX file somewhere other than on the production machines where it is used, deselect **Mark this key as exportable**. When you are prompted to specify where the certificates in the store should be placed, select **Personal**.
10. Click **Finish**.

What is automatic database reconnection?

The Perceptive Content database can automatically reconnect if it disconnects from ImageNow Server.

If the connection to the database stops unexpectedly, Perceptive Content automatically attempts to reestablish the connection once per minute for up to 60 minutes. If Perceptive Content is unable to complete the connection, ImageNow Server shuts down.

If the connection is not established, contact your system administrator.

Manage user authentication

What is user authentication and authorization?

User authentication and authorization is the process of validating the user name and password that a user provides when logging in, and then determining if the user is registered and what documents the user can access and what processes the user can perform.

For the authentication process, Perceptive Content relies on external sources to validate the password. ImageNow Server can run in one of three modes to accomplish the process of authenticating the user name and password: System, LDAP, or SQL. The same authentication process is conducted for all clients, including ImageNow Client and Integration Server.

For the authorization process, a registered user is a user created in Perceptive Content with the same user name that was supplied during the authentication process. For example, using the default authentication mode of SYSTEM, you add user names to Perceptive Content that match each user name on the domain.

When determining what items the user can access and what processes the user can perform, the authorization process uses the security information from Perceptive Content to determine the user s privileges.

What is token-based authentication?

Token-based authentication is a supported mechanism for authenticating agents when they connect to Perceptive Content.

Once token signing credentials are configured, authentication tokens can be generated for specific agents. An authentication token can then be used to connect to Perceptive Content by any instance of the agent for which the token was generated.

Set up token-based authentication

To set up token-based authentication, complete the following steps.

1. On the **Perceptive Content Server** computer, navigate to the *[drive:]\inserver\etc* folder and open the *inow.ini* file in a text editor.
2. In the **[Logon Control]** section, complete the following substeps.
   1. In the `token.signing.key.path` setting, enter the path to the token signing key.
   2. Optional. In the `token.signing.key.password` setting, enter the password for the token signing key.
   3. In the `token.signing.algorithm` setting, enter the algorithm for signing authentication tokens.

   Note: Perceptive Content requires either an elliptic curve or RSA key pair to be used as token signing credentials. Key pairs must be in **Base64 encoded DER (PEM)** format. For elliptic curve signing keys, valid signing algorithms are **ES256**, **ES384** or **ES512**. For RSA signing keys, valid signing algorithms are **RS256**, **RS384** or **RS512**.
3. Save the *inow.ini* file, and then close it.
4. Using a command line tool, import the token signing certificate by running the following command.

   ```
   intool --cmd import-cert --file <certificate file name> --type token-auth
   ```

   Example

   ```
   intool --cmd import-cert --file P256.crt --type token-auth
   ```

Generate an authentication token for an agent

Authentication tokens can be generated for Mail Agent, ImageNow Forms Server, and ImageNow Business Insight. To generate an authentication token, complete the following steps.

1. On the **Perceptive Content Server** machine, generate an authentication token for **Email Agent** by running the command.

   ```
   intool --cmd create-authentication-token --lictype <application name> --
   file <output file name>
   ```

Example

```
intool --cmd create-authentication-token --lictype Mail Agent --file
MailAgentToken.txt
```

2. Import the authentication token following the steps in the appropriate product or agent-specific installation guide.

What is Epic user authentication?

Epic user authentication provides single sign-on integration between Epic and the ImageNow Client.

When you configure this authentication method, users who are logged in to Epic can access and view content in ImageNow Client without having to enter user name and password information.

To use this method of authentication, you must have an ImageNow Interact for Epic license.

For example, Abby is a Release of Information (ROI) clerk and she receives an ROI request. She enters the request information in Epic's HIM ROI module and needs to verify the patient's date of birth. Because Epic user authentication is configured, Abby can immediately access the patient's birth date information in ImageNow Client, which reduces the amount of time it takes to complete the request.

Set up user authentication using Epic

User authentication is a security measure that allows you to identify and verify who is accessing an Perceptive Content system. To authenticate ImageNow Client users through the Epic single sign-on (SSO) system, complete the following steps.

Prerequisite To set up user authentication using Epic, you must have Server Administrator privileges.

1. To configure the *inow.ini* file on **ImageNow Server**, perform the following substeps:
   1. On the **ImageNow Server** computer, browse to the *[drive:]****inserver*****etc*** folder.
   2. Using a text editor, open the *inow.ini* file.
   3. Under **[Logon Control]**, create the setting **epic.sso** and set the value to TRUE.
   4. Under **[Logon Control]**, create the setting **epic.sso.key** and set the value to the token sent from **Perceptive Content**. This is the same value specified for the **SSO.key** setting in the **INEpicViewer.ini** file.
2. Save and close the *inow.ini* file.
3. To make your changes effective, restart the **ImageNow Server**.
4. To configure the **ImageNow Client** to allow a user to log in through the Epic SSO, perform the following substeps:
   1. On the **ImageNow Client** computer, browse to the *\Users\<user name>\AppData\Roaming\ImageNow* folder.
   2. Using a text editor, open the *ImageNow.ini* file.
   3. Under **[General]**, add the setting **epic.sso** and set the value to TRUE.
   4. Save and close the *ImageNow.ini* file.

What is LDAP user authentication?

LDAP authentication is one of three methods available in Perceptive Content for authenticating users. Using LDAP authentication, Perceptive Content authenticates to an LDAP server using the LDAP Simple Bind method. The ImageNow Server attempts a "bind" to the LDAP server using the credentials provided by the user. In addition to simple bind, Perceptive Content also supports LDAP authentication using simple bind over SSL (Secure Sockets Layer). You can also use multiple LDAP servers to authenticate against.

To demonstrate the advantages of LDAP user authentication with Perceptive Content, consider the following scenario: Perceptive Content is running on Oracle Solaris, and the LDAP server is using the Microsoft Active Directory for all its enterprise users. Using the default System authentication method, your system administrator must create and store user names and passwords on the Oracle Solaris server running ImageNow Server, as well as in the Active Directory. In this scenario, your system administrator must create and maintain two sets of user names and passwords. By using LDAP authentication, your system administrator only needs to create and maintain one set of user names and passwords. This is possible because the ImageNow Server does not store passwords, just user names. With LDAP authentication, users are authenticated in Perceptive Content using the user names and passwords from the LDAP directory. Microsoft Active Directory is only one example of a user directory that supports LDAP; you can use any LDAP-compliant directory. You can use the User Replication Agentto synchronize the user names between ImageNow Server and the LDAP server.

Most LDAP servers support authentication using a simple user name, such as jsmith, for the user distinguished name (DN); other LDAP servers require a fully-qualified DN for the user DN. At login, Perceptive Content provides the user DN and password as a string to the LDAP Server. The LDAP server responds to these credentials with a succeed or fail message. A fully-qualified DN is made up of the relative distinguished names (RDNs) of the entry and each of the entry's parent entries, up to the root of the directory tree. RDNs are usually separated by commas and optional spaces. Follow the naming convention as supported by the LDAP server and configured by your LDAP administrator.

Perceptive Content supports other formats for the user DN, depending on the LDAP server. As an example, Microsoft Active Directory supports bind requests with the format of an e-mail address such as jdoe@acme.com for the user DN. Active Directory also supports the format of the User Principal Name (UPN) such as jsmith@domain.com for the user DN. The UPN enables users to use their Windows domain name and password for login. These formats are often easier to configure and maintain because this format follows the same pattern for all users, regardless of their Organizational Unit (OU). Also, these formats are not affected if the user entry in the directory moves to another container.

Set up user authentication using LDAP

User authentication is a security measure that allows you to identify and verify who is accessing an Perceptive Content system. To set up user authentication using LDAP, complete the following steps.

1. On the **ImageNow Server** computer, navigate to the *[drive:]**inserver****etc*** folder, and then open the *inow.ini* file in a text editor.
2. In the **[Logon Control]** section, change the following settings:
    1. In the **logon.method** setting, replace the existing entry with LDAP.
    2. In the **LDAP.server** setting, enter the IP address or host name of the LDAP server.

3. In the **LDAP.server.port** setting, enter the port number of the LDAP server, which is typically 389.
4. In the **LDAP.anonymous.logon.enabled** setting, assign TRUE when you want the initial bind to the LDAP server to be anonymous during the search for user entries. When this setting is TRUE, the **LDAP.login** and **LDAP.password** settings are ignored. The default setting is FALSE.
5. In the **LDAP.login** setting, enter the LDAP user DN for binding to the LDAP server to begin the search for user entries.

   Example LDAP.login=jsmith@acme.com.
6. In the **LDAP.password** setting, enter the LDAP password for the user DN specified in the **LDAP.login** setting.
7. In the **LDAP.ImageNow.Groups** setting, enter the **Perceptive Content** groups you want to authenticate to **Perceptive Content** using this LDAP server configuration. Separate each name with a caret (^). If you do not enter any values in this setting and the **LDAP.ImageNow.Users** setting, then any **Perceptive Content** user can authenticate using this server configuration.

   Example LDAP.ImageNow.Groups=group1^group2.
8. In the **LDAP.ImageNow.Users** setting, enter the users you want to authenticate to **Perceptive Content** using this LDAP server configuration. Separate each name with a caret (^). If you do not enter any values in this setting and the **LDAP.ImageNow.Groups** setting, then any **Perceptive Content** user can authenticate using this server configuration.

   Example LDAP.ImageNow.Users=user1^user2.

   Note: When you enter users in this setting, any users that are owners or managers must be added to this list if you want those users to be able authenticate using this server configuration.
9. Optional. You can create the **logon.settings.delimiter** setting. This setting allows you to select a character to be the delimiter for the **LDAP.ImageNow.Groups** and **LDAP.ImageNow.Users** settings. You can use any symbol you want except for square brackets - '[' or ']'.
10. In the **LDAP.method** setting, use direct binding by entering DIRECT to use the prepend and append settings to create your user DN or use indirect binding by entering INDIRECT to search the base DN and its containers for the attribute that matches the user's login.

3. If you chose direct binding (Method 1 as shown in the *inow.ini* file), to add strings (such as an RDN) before and after the username, modify the following settings.
   1. Modify the **LDAP.name.prepend** setting.

      Example LDAP.name.prepend=CN=
   2. Modify up to 20 **LDAP.name.append**settings.

      Example LDAP.name.append1=,CN=Users,OU=Marketing,DC=AcmeInc,DC=com LDAP.name.append2=,CN=Users,OU=Sales,DC=AcmeInc,DC=com LDAP.name.append3= LDAP.name.append4= LDAP.name.append5=

   Note: This is typically not necessary, and it is recommended to attempt authentication using a simple

username or other user DN, such as e-mail address, before adding prepend and append settings. The format to use depends on the LDAP server and the way the LDAP administrator configured it. In either case, you follow the naming convention supported by the LDAP server.

4. If you chose indirect binding (Method 2 as shown in the *inow.ini* file), do the following substeps to use indirect binding without translation.
   1. In the LDAP.base.dn setting, enter the base or root DN of the LDAP server where you want the search to begin and search all its containers.

      Example LDAP.base.dn="OU=Research and Development, DC=acme, DC=com".

   2. In the**LDAP.login.attr** setting, enter the LDAP user attribute you want to search for in the LDAP server. The search looks for this attribute whose value is the value entered in the **Perceptive Content** login.

      Example LDAP.login.attr=sAMAccountName.

   3. In the **LDAP.login.translate.username** setting, enter FALSE. This setting is used only when you are doing translation for user names.

      Example LDAP.login.translate.username=FALSE.

   4. In the **LDAP.login.translated.attr** setting, leave the value blank. This setting is used only when you are doing translation for user names.
5. If you chose indirect binding (Method 2 as shown in the *inow.ini* file), do the following substeps to use indirect binding with translation
   1. In the **LDAP.base.dn** setting, enter the base or root DN of the LDAP server where you want the search to begin and search all its containers.

      Example LDAP.base.dn="OU=Research and Development, DC=acme, DC=com".

   2. In the **LDAP.login.attr** setting, enter the attribute for the user name you want to translate. The search looks for this attribute whose value is the value entered in the **Perceptive Content** login. A value for this setting is required when the LDAP.login.translate.username is set to TRUE for translation to work.

      Example LDAP.login.attr=sAMAccountName.

   3. In the **LDAP.login.translate.username** setting, enter TRUE.

      Example LDAP.login.translate.username=TRUE.

   4. In the **LDAP.login.translated.attr** setting, enter the name of the attribute to use for the translated user name. A value for this setting is required when the LDAP.login.translate.username is set to TRUE for translation to work.

      Example LDAP.login.translated.attr=userPrincipalName.

   Note: Use of this feature can cause a user s log and displayed user name to be different than the user name used to log in.
6. Optional. Set up secondary LDAP servers for authentication:

1. Optional. Underneath your primary LDAP server configuration settings, start a new line and add a comment for a heading for the server configuration.
2. Type each setting you need for this configuration.
3. Make the server configuration unique by adding a number to the LDAP key, as shown by the following Configuration 1 and Configuration 2 server setting example.

   Example

```
; Configuration 1 - Server 1, Method DIRECT (1), with SSL
LDAP.server=server1.acme.com
LDAP.server.port=636
LDAP.ImageNow.Groups=group1^group2^user1^user2
LDAP.use.ssl=TRUE
LDAP.method=DIRECT
LDAP.anonymous.logon.enabled=FALSE
LDAP.login=user1
LDAP.password=password
; LDAP method DIRECT (1) variables
LDAP.name.prepend=
LDAP.name.append1=@acme.com
LDAP.name.append2=
LDAP.name.append3=
LDAP.name.append4=
LDAP.name.append5=
; Configuration 2 - Server 2, Method INDIRECT (2), no SSL
LDAP2.server=server2.acme.com
LDAP2.server.port=389
LDAP2.ImageNowGroups=group3^test3
LDAP2.use.ssl=FALSE
LDAP2.method=INDIRECT
LDAP2.anonymous.logon.enabled=FALSE
```

```
LDAP2.login=user1
LDAP2.password=password
LDAP2.base.dn=0=acme,C=US
LDAP2.login.attr=cn
```

4. Repeat these sub-steps for each LDAP server configuration you want to set up.

Note: You can set up more than one LDAP server to authenticate against by adding an additional section to the inow.ini file for each LDAP server. You can use Method DIRECT (1) or Method INDIRECT (2) as well as SSL as needed in each section. Tip: You can also copy the settings from an existing server configuration and then modify them for each server configuration.

7. Save the *inow.ini* file, and then close it.
8. Restart the **ImageNow Server** to make the changes effective, and then verify that all your users can log in to the **ImageNow Client**.

Complete *inow.ini* file LDAP section example.

```
[Logon Control]
logon.method=LDAP
; The LDAP certificatedirectory remains a global setting that
applies to all
; LDAP server configurations
LDAP.ssl.cert.path=/opt/inserver/etc/certs
;Configuration 1 Server 1, Method DIRECT (1), with SSL
LDAP.server=server1.acme.com
LDAP.server.port=636
LDAP.ImageNow.Groups=group1^group2^user1^user2
LDAP.use.ssl=TRUE
LDAP.method=DIRECT
LDAP.anonymous.logon.enabled=FALSE
LDAP.login=test1
LDAP.password=password
; LDAPmethod 1 variables
```

```
LDAP.name.prepend=
LDAP.name.append1=@acme.com
LDAP.name.append2=
LDAP.name.append3=
LDAP.name.append4=
LDAP.name.append5=
; Configuration Server 2, Method INDIRECT(2), no SSL
LDAP2.server=server2.acme2.com
LDAP2.server.port=389
LDAP2.ImageNow.Groups=group3^test3
LDAP2.use.ssl=FALSE
LDAP2.method=INDIRECT
LDAP2.anonymous.logon.enabled=FALSE
LDAP2.login=test1
LDAP2.password=password
LDAP2.base.dn=O=othersite,C=US
LDAP2.login.attr=cn
;Configuration 3 - Server 3 (Active Directory), Method DIRECT
(1),no SSL
LDAP3.server=server3.acmeusers.net
LDAP3.server.port=389
LDAP3.ImageNow.Groups=
LDAP3.use.ssl=FALSE
LDAP3.method=DIRECT
LDAP3.anonymous.logon.enabled=FALSE
LDAP3.login=test1
LDAP3.password=password
LDAP3.name.prepend=
LDAP3.name.append1=@acmeusers.net
```

```
LDAP3.name.append2=

LDAP3.name.append3=

LDAP3.name.append4=

LDAP3.name.append5=

;Translation configuration example for Microsoft Active
Directory,no SSL

LDAP.server=acme.com

LDAP.server.port=389

LDAP.use.ssl=FALSE

LDAP.method=INDIRECT

LDAP.ImageNow.Groups=

LDAP.name.prepend=

LDAP.name.append1=

LDAP.name.append2=

LDAP.name.append3=

LDAP.name.append4=

LDAP.name.append5=

LDAP.anonymous.logon.enabled=FALSE

LDAP.login=

LDAP.password=

LDAP.base.dn=DC=acme,DC=com

LDAP.login.attr=sAMAccountName

LDAP.login.translate.username=TRUE

LDAP.login.translated.attr=userPrincipalName
```

Set up LDAP authentication with SSL overview

User authentication is a security measure that allows you to identify and verify who is accessing an Perceptive Content system. To set up LDAP authentication with SSL, complete the following sequence of procedures.

Prerequisite This task assumes you are already using LDAP user authentication, and that you have verified that LDAP authentication is working correctly. This allows you to verify that the LDAP directory is responding to LDAP requests before setting it up for SSL. Verifying first also permits you to ensure that you are correctly binding to the LDAP server. In order for Perceptive Content Server to communicate with the LDAP server using SSL 3.0, you must import a copy of the LDAP server certificate into the Perceptive Content Server certificate database. Importing the certificate requires a Windows computer. If you are running Perceptive Content on a UNIX server, you can copy the certificate database to the server after the import process is complete.

- Configure the MMC snap-in.
- Use the MMC snap-in to install the certificate on the LDAP server.
- Export the certificate from your LDAP server.
- Import the certificate into Perceptvie Content Server on Windows.
- Import the certificate into Perceptive Content Server on UNIX.
- Set up SSL on the Perceptive Content Client.
- Enable FIPS mode for LDAP on UNIX.
- Configure LDAP SSL/TLS cipher suites for UNIX.

Configure the MMC snap-in

The Microsoft Management Console (MMC) snap-in can add, install, and export certificates. To configure the MMC snap-in, complete the following steps.

1. To open the MMC console, click **Start > Run**.
2. In the **Run** dialog box, type `MMC`, and then click **OK**.
3. Click **File > Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates > Add**.
6. In the **Certificates Snap-in** dialog box, select **Computer Account**, and then click **Next**.
7. In the **Select Computer** dialog box, select **Local computer > Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.

Use the MMC snap-in to install the certificate on the LDAP server

To install the certificate on the server using the MMC snap-in, complete the following steps.

1. In the **Console Root tree**, click **Certificates (Local Computer) > Personal**.
2. Right-click anywhere in the right pane, click **All Tasks > Request New Certificate**.

3. In the **Certificate Request Wizard** dialog page, click **Next**.
4. In the **Certificate Type** page, under **Certificate types**, select **Computer > Next**.
5. In the **Friendly Name** text box you can type a friendly name for the certificate or leave the text box blank, and then complete the wizard.

   After the wizard finishes, you will see the certificate in the folder with the fully qualified computer domain name.

Result Your installed certificates are located in the Certificates folder in the Personal container.

Export the certificate from your LDAP server

There are several methods you can use to export your certificate. The method you choose depends on your platform, the LDAP directory you are using, and the LDAP server. Normally, documentation regarding implementation and maintenance of an LDAP server is provided by the vendor of that LDAP service software. Typically, the vendor documentation includes instructions for exporting an LDAP server certificate. The following methods provide some examples of exporting certificates. To export the certificate from your LDAP server, complete the following steps.

Prerequisite Perceptive Content does not require certificate-based authentication, so there is no need to export your private key along with your public key when you export your certificate. Use your LDAP directory utility, if provided. Many LDAP directories provide their own tools for managing certificates. For example, some versions of Microsoft Active Directory have the Certificate Authority software.

1. Choose the export method that best suits your environment.

Situation	Steps
MMC snap-in	1. Locate your certificate in the **Personal** folder. 2. Right-click the certificate name, click **All Tasks > Export**. 3. In the **Certificate Export Wizard** welcome page, click **Next**. 4. In the **Export Private Key** page, click **Next**. 5. In the **Export File Format** page, select **DER encoded binary X.509 (CER)**, and then click **Next**. Your certificate must be in DER encoded binary X.509 or Base-64 encoded DER X.509 (DER, CER) format to be successfully imported into the UNIX certificate database. 6. In the **File to Export** page, browse to the temporary directory you created for the downloaded certificate utility files. In the **File name** box, enter a name for the

Situation	Steps
	certificate. 7. Click **Next > Finish**.
Internet Explorer 6	1. On any Windows computer in your network domain, open Internet Explorer and navigate to the site of the secure LDAP server. For example, go to *https://myserver.edu:636*. 2. In the **Security Alert** dialog box, click **View Certificate**. 3. In the **Certificate** dialog box, on the **Details** tab, click **Copy to File**. 4. In the **Certificate Export Wizard** welcome page, click **Next**. 5. In the **Export File Format** page, select **DER encoded binary X.509 (CER)**, and then click **Next**. Your certificate must be in DER encoded binary X.509 or Base-64 encoded DER X.509 (DER, CER) format to be successfully imported into the UNIX certificate database. 6. In the **File to Export** page, browse to the temporary directory you created for the downloaded certificate utility files, and then name the certificate by typing a filename with a CER extension in the **File name** box. 7. Click **Next > Finish**.
Mozilla Firefox 2.0.0.3	1. On any Windows computer in your network domain, open Mozilla Firefox and navigate to the site of the secure LDAP server. For example, go to *https://myserver.edu:636* 2. On the **Website Certified <...>** dialog box, click **Examine Certificate**. 3. On the **Certificate Viewer** dialog box, click **Save to File**. 4. In the **Save Certificate to File** dialog box, in the **File name** box, type a name for your certificate using the CER file name extension.

Situation	Steps
	5. In the **Save as type** list, select **X.509 Certificate (DER)**. Your certificate must be in DER encoded binary X.509 or Base-64 encoded DER X.509 (DER, CER) format to be successfully imported into the UNIX certificate database. 6. Click **Save**. 7. On the **Alert** dialog box, click **OK**. Note the path where the file is saved as you will need to copy the file when importing the certificate.

Import a certificate into Perceptive Content Server on Windows

To import a certificate into Perceptive Content Server on a Windows operating system, complete the following steps.

Prerequisite Your LDAP server must support SSL 3.0 or TLS 1.0. SSL/TLS communication must take place on a separate TCP port.

1. Click **Start > Run**.
2. In the **Run** dialog box, type `MMC`, and then click **OK**.
3. In the left pane, in the **Console Root** tree, click **Certificates (Local Computer) > Trusted Root Certification Authorities**.
4. Right-click anywhere in the right pane, and click **All Tasks > Import**.
5. In the **Certificate Import Wizard** welcome page, click **Next**.
6. In the **File to Import** page, browse to the certificate you just created, and click **Next**.
7. In the **Certificate Store** page, verify **Place all certificates in the following store** is selected, and click **Next**.
8. In the **Completing the Certificate Import Wizard** page, click **Finish**.
9. Double-click the certificate and verify it imported successfully.
10. On the **Perceptive Content** Server computer, navigate to the *[drive:]**inserver****etc*** directory, open *inow.ini* in a text editor, and in the **[Logon Control]** section, make the following changes.
    - Verify the LDAP.server setting. If you are already using LDAP user authentication, you should not need to change this setting. Note that you must specify the fully qualified domain name (FQDN) for the LDAP.server setting.
    - In the LDAP.server.port setting, enter the port number of the LDAP server, which is typically 636 when using SSL.
    - Change the LDAP.use.ssl setting to `TRUE`.

    Example `LDAP.use.ssl=TRUE`

Example `LDAP.server=acme.com`

Example `LDAP.server.port=636`

11. Save the file, and then close it.
12. Restart the **Perceptive Content** Server to make the changes effective, and then verify that your users can log into the **Perceptive Content** client.

Note: After you restart the Perceptive Content Server, you cannot re-import the certificate while the certificate databases are in use. If the certificate is not working properly, stop the Perceptive Content Server services before you re-import the certificate and copy the new files.

Import a certificate into Perceptive Content Server on UNIX

To import a certificate into Perceptive Content Server on a UNIX operating system, complete the following steps.

Prerequisite Your LDAP server must support SSL 3.0 or TLS 1.0. SSL/TLS communication must take place on a separate TCP port.

Note: Both *cert7.db* and *cert8.db* database files are supported.

1. Import your LDAP server certificate into a Network Security Services Tools (NSS) certificate database using the following command.
   `certutil -A -n [certificate nickname] -t [trust attributes] -i [path to certificate file] -d [path to database directory].`

Certificate Type	Code Sample
Import and trust a peer SSL certificate	`certutil -A -n LDAPServer -t P,, -i /opt/inserver/etc/LDAPServer.cer -d /opt/inserver/etc`
Import and trust a Certificate Authority (CA) certificate	`certutil -A -n LDAPServer-CA -t C,, -i /opt/inserver/etc/LDAPServer-CA.cer -d /opt/inserver/etc`

2. On the **Perceptive Content Server** computer, navigate to the ***[drive:]\inserver\etc*** directory, open *inow.ini* in a text editor, and in the **[Logon Control]** section, make the following changes.
   - Verify the LDAP.server setting. If you are already using LDAP user authentication, you should not need to change this setting. Note that you must specify the fully qualified domain name (FQDN) for the LDAP.server setting.
   - In the LDAP.server.port setting, enter the port number of the LDAP server, which is typically 636 when using SSL.
   - Change the LDAP.use.ssl setting to `TRUE`.

- Change the path to the certificates database by modifying the LDAP.ssl.cert.path setting to use the actual path, as shown in the following example.

Example

```
   LDAP.use.ssl=TRUE LDAP.ssl.cert.path=/opt/inserver/etc
   LDAP.server=acme.com LDAP.server.port.port=636
LDAP.use.ssl=TRUE | FALSE If using LDAP over SSL, set value to TRUE.
Default is FALSE.
```

3. Save the file, and then close it.
4. Restart the **Perceptive Content** Server to make the changes effective, and then verify that your users can log into the **Perceptive Content** client.

Note: After you restart the Perceptive Content Server, you cannot re-import the certificate while the certificate databases are in use. If the certificate is not working properly, stop the Perceptive Content Server services before you re-import the certificate and copy the new files.

Enable FIPS mode for LDAP on UNIX

To enable FIPS mode for LDAP SSL/TLS on UNIX environments, complete the following steps.

1. In a command window, run the following commands.
   1. Create a certificate database:
      `modutil -create -dbdir [path to database directory]`
   2. Configure the certificate database to enable FIPS mode:
      `modutil -fips true -dbdir [path to database directory]`
   3. Verify FIPS mode is enabled:
      `modutil -chkfips true -dbdir [path to database directory]`
   4. Obtain the token name of the FIPS module:
      `modutil -list -dbdir [path to database directory]`
   5. Initialize a password for the FIPS token:
      `modutil -dbdir [path to database directory] -changepw [FIPS token name]`
   6. Import your LDAP server certificate into a Network Security Services (NSS) Tools certificate database:
      `certutil -A -n [certificate nickname] -t [trust attributes] -i [path to certificate file] -d [path to database directory]`
2. Navigate to your inow.ini file. In the [Logon Control] section, configure the following settings.
   - `ldap.ssl.cert.path`
   - `ldap.ssl.cert.fips.token`
   - `ldap.ssl.cert.fips.password`
3. To enable auditing, configure the following environment variable.
   - NSS_ENABLE_AUDIT=1

Configure LDAP SSL/TLS cipher suites for UNIX

The supported versions of LDAP SSL/TLS cipher suites are SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. To configure the SLL/TLS cipher suites, configure the following settings.

1. Navigate to your *inserver/etc* directory and open the *inow.ini* file in a text editor.
2. Assign values to the following settings. Valid values are `SSL3`, `TLS10`, `TLS11`, and `TLS12`.
   - `ldap.ssl.version.min=TLS11`
   - `ldap.ssl.version.max=TLS12`
3. Save and close the *inow.ini* file.
4. Restart **Perceptive Content Server** to make the changes effective, and verify that your users can log in to **Perceptive Content** Client.

Configure an SSL trust store on Linux

On Linux the SSL trusted certificate authority (CA) bundle is set using a global software setting. The trusted CA bundle can be used for HTTP calls from iScript, message queuing, and certain web-based OSM plugins. The trusted CA bundle should contain one or more concatenated certificates in PEM format. You may choose to use a system trust store that is in the same format. Based on the configuration and the Linux distribution, the actual location of the system trust stores may vary.

To configure the SSL trusted CA bundle on Linux, complete the following steps.

1. Stop all **Perceptive Content** services.
2. Set the **SSL_CERT_FILE** environment variable to the full path of the trusted CA bundle file.

   Example

   ```
   export SSL_CERT_FILE=/etc/pki/ca-trust/extracted/openssl/ca-
   bundle.trust.crt
   ```

3. Start all **Perceptive Content** services.

What is multiple LDAP server authentication?

Multiple LDAP server authentication allows you to use more than one LDAP server to authenticate users logging in to Perceptive Content.

To use this feature, you set up an additional server configuration for each LDAP server you want to use.

You can specify a list of groups and users in your configuration to limit which users and groups can use that LDAP server configuration. If you do not provide a value for this setting, then all users can use that configuration for Perceptive Content authentication. By providing users and groups for each configuration, you can prevent users from existing in more than one configuration.

When you use more than one LDAP server for user authentication, Perceptive Content responds according to certain rules:

- When one of your users attempts to log in to Perceptive Content, Perceptive Content looks through each LDAP server configuration until it locates a configuration the user can use. Perceptive Content then attempts to authenticate the user to that LDAP server.
- If the authentication fails because the LDAP server is down or unreachable, then Perceptive Content continues looking through the server configurations.
- If Perceptive Content finds another server configuration the user can use, it attempts to authenticate the user to that LDAP server. Perceptive Content continues through to the end of the available server configurations.
- When the LDAP authentication is successful, the user logs in. If the user is set up to use a configuration, but not in the LDAP server for that user, it is considered a login failure and the server will not attempt to authenticate against any additional configurations. If Perceptive Content does not locate any server configurations for the user, the user receives an error message stating that the LDAP connection failed.
- If Perceptive Content does locate a server configuration the user can use, but the authentication failure occurs because the user is not located in the LDAP server, the user receives an error message.

What is SQL user authentication?

SQL user authentication is one of three methods available for authenticating users when they log in to Perceptive Content.

The SQL user authentication method uses an Open Database Connectivity (ODBC) SELECT statement to validate the password the user provides. This method allows the system administrator to specify a unique, environment-specific SQL SELECT statement that validates the user name and password combination provided by the user through the ImageNow Client. The SQL table that contains the user names and passwords is external to Perceptive Content, and you can store the table in any database that is available through an ODBC connection.

Set up user authentication using SQL

User authentication is a security measure that allows you to identify and verify who is accessing Perceptive Content. To set up user authentication using SQL, complete the following steps.

Prerequisite Prior to performing this procedure, you must install Perceptive Content Server and Perceptive Content Client, and then set up users that match the users in your SQL database. You must have a custom SQL database with a table that contains the users and passwords that need access to Perceptive Content Client. Make sure that this table has no joins to other tables. To log in, the user must be active in the SQL database and active in Perceptive Content Client user security settings.

1. To change Logon Method to SQL in the *inow.ini* file, complete the following substeps.
    1. On the **Perceptive Content** Server computer, navigate to the ***[drive:]\inserver\etc*** folder and open the *inow.ini* file in a text editor.
    2. In the [`Logon Control`] section, change the `logon.method` setting to `SQL`.

        Example `[Logon Control]logon.method=SQL`
    3. In the same section, below the LDAP settings, change the `auth.sql.query` setting to the SQL query string for authentication.

Example `auth.sql.query=SELECT * FROM SQLAUTH WHERE LOGINNAME='[USERID]'AND PASSWORD='[PASSWORD]' AND USERSTATUS=1`

Example Additional Boolean conditions, using AND and OR operators, are allowed but not required. `SELECT * FROM SQL_AUTH WHERE USER_NAME = '[USERID]' AND PASSWORD = '[PASSWORD]' AND IS_ACTIVE = 1` works as long it returns one row if valid, and no rows if invalid.

Note: `'[USERID]'` and `'[PASSWORD]'` are replaced with the user supplied user name and password. Also, SQL query statements are case sensitive. In the `auth.sql.query` setting, do not use a "SELECT COUNT (*)...". This query must return one row if valid, and no rows if invalid.

2. Make the following changes in the `[ODBC]` section of the *inow.ini* file.
   1. Remove the semicolon in front of each `auth.obdc` setting.
   2. Change the `auth.odbc.dbms` setting to the name of your authentication database.

      Example `auth.odbc.dbms=SQLServer`

   3. In the `auth.odbc.dsn` setting, type the data source name used by an ODBC application when requesting a connection to the data source for your database. On Windows, the same data source name appears in the **ODBC Data Source Administrator** dialog box in the **Control Panel ODBC Data Source Administrator**.

      Example You could enter `auth.odbc.dsn=SQL_Auth`.

   4. In the `auth.odbc.user.id` setting, enter the user id of your ODBC connection.
   5. In the `auth.odbc.user.password` setting, enter the password of your ODBC connection. This value is encrypted and removed from the setting after restarting **Perceptive Content** Server.

      Example

      ```
      [ODBC]auth.odbc.dbms=SQLServer

      auth.odbc.dsn=SQL_Auth

      auth.odbc.user.id=inuser

      auth.odbc.user.password=defaultpassword
      ```

3. Save the file and close it.
4. To create an ODBC connection on Unix, complete the following substeps.
   1. On the **Perceptive Content** Server computer, navigate to the appropriate folder for your platform and open the *odbc.ini* file in a text editor.
   2. In the `[ODBC Data Sources]` section, add the following, where <*data source name*> is a unique name for your ODBC data source.

      Example You can set this to `SQL_Auth=Data Direct 6.0 SQL Server Wire Protocol.<data source name>=DataDirect 6.0 SQL Server Wire Protocol`

   3. Create a new section using the exact data source name. This name must match the name you just entered in the previous step.

Example [SQL_Auth]

4. Add your connection parameters to this section you just created. The highlighted settings in the example below are the relevant ones for this authentication method.

   Example `[SQL_Auth]Address],1433`

5. Save the file and close it.

5. To create an ODBC connection on Windows, complete the following substeps.
   1. In the **ODBC Data Source Administrator** dialog box, select the **System DSN** tab, click **Add**, select the driver for your authentication database, and click **Finish**.
   2. In the **Create New Data Source** dialog box, select the driver for your authentication database and click **Finish**.

      Example SQL Server

   3. In the **Create a New Data Source to** <*driver name*> wizard, in the **Name** box, type the name of the authentication database. This name must match the name used in the *inow.ini* file.

      Example SQL_Auth

   4. In the **Create a New Data Source to** <*driver name*> wizard, in the **Description** box, type a description to describe your data source. This description can be any text you want.
   5. In the **Create a New Data Source to** <*driver name*> wizard, in the **Server** list, select where your authentication database resides and click **Next**.
   6. On the next page, select the authentication method the ODBC driver should use to connect to your authentication database. If you select the second option, enter the login ID and password of the system account for your authentication database and click **Next**.
   7. On the next page, make sure that the **Change the default DB** check box is selected, select your authentication database, and click **Next**.

      Example Select **SQL_Auth**.

   8. On the next page, accept the defaults and click **Finish**.
   9. On the summary page, optionally click **Test** to test your connection, and then click **OK**.
6. Restart **Perceptive Content** Server to make the changes effective, and then make sure that all your users can log in to the client.

What is System user authentication?

By default, Perceptive Content is set to System user authentication, in which users are authenticated against the operating system on which the ImageNow Server is running.

The System authentication method is one of three methods available in Perceptive Content for authenticating users. When used in Windows, the ImageNow Server attempts to authenticate users against its local user list and the network domain or a directory service, such as Active Directory, depending on which is used by your server. You can also use domain authentication when users are logged into a valid Windows NT domain on their ImageNow Client computer with the NT domain account that is an exact match to the user ID. In this case, when a user launches Perceptive Content, the user is logged in automatically.

For Linux, the ImageNow Server attempts to authenticate users against the user database of the Linux server. In both cases, the user must have a user name and password on either the local server or the network.

Set up user authentication using System

User authentication is a security measure that allows you to identify and verify who is accessing Perceptive Content. Perceptive Content automatically uses System user authentication by default. You can use domain authentication with this method by configuring your connection profile. To set up System user authentication, complete the following steps.

1. On the **ImageNow Server** computer, navigate to *[drive:]**inserver****etc***, and then open the *inow.ini* file in a text editor.
2. Under the `[Logon Control]` section, change the `logon.method` to `logon.method=SYSTEM`
3. Optional. To enable domain authentication, do the following substeps:
    1. Also under the `[Logon Control]` section, set the `client.validation` setting to `TRUE`.
    2. Change the `nt.domain.list` setting to your Windows NT domain name.
4. Optional. To enable domain authentication on the client side, do the following substeps:
    1. Click **Start > Programs > Perceptive Content**.
    2. In the **Perceptive Content** login dialog box, click **Connection Profiles**.
    3. Click **Edit connection profiles**.
    4. In the **Connection Profiles** dialog box, select your user profile, and then click **Modify**.
    5. In the **Modify Connection Profile** dialog box, in **Username**, select the **Use domain authentication** check box, and then click **OK**.
5. Save the *inow.ini* file, and then close it.
6. Restart the **ImageNow Server** to make the changes effective, and then verify that your users can log in to the **ImageNow Client**.

Manage configuration files

inmc.ini [Remote] settings

inmc.ini [Remote] setting

This topic displays the inmc.ini setting under [Remote]. The setting in the inmc.ini file is specific to Management Console.

socket.default.timeout

Specifies how many seconds Management Console waits for APIs.

Do not change this setting without first consulting with Enterprise Software Product Support.

socket.default.timeout = any positive integer

The default is 60.

inow.ini

The following topics provide definitions and sample data for the settings in the inow.ini configuration file. Each topic displays the INI settings for the group that appears in its title, such as [Network].

Each setting offers two or more options, which are defined in the following topics along with a description. Use these topics as a guide when customizing the inow.ini file.

- Audit
- Auto Form
- Data Capture
- Digital Signature
- Directory Locations
- Doc
- DocLock
- Envoy
- ERM
- Fax Out
- Folders
- Forms
- General
- iScript
- Licenses
- Locale
- Logon Control
- Memory
- Message Queuing
- Migration
- Network
- OCR
- ODBC
- Optional
- OSM
- Records
- Redaction
- Statistics

inow.ini [Audit] settings

The following settings are available under the [Audit] group in the inow.ini configuration file.

audit.format = 1, 2, or 3

Specifies where audit details are stored.

- 1 = XML formatted file
- 2 = Database
- 3 = Both XML file and database

Default = 1

login.audit.level = 0 or 1

Specifies the verboseness level for user authentication auditing.

- 0 = No authentication auditing
- 1 = Audits only failed authentication attempts

Default = 0

inow.ini [Auto Form] settings

The following settings are available under the [Auto Form] group in the inow.ini configuration file.

auto.form.integration = TRUE or FALSE

Determines whether Auto Form integration is active.

- TRUE = Auto Form integration is activated.
- FALSE = Auto Form integration is deactivated.

Default = None

inow.ini [Data Capture] settings

The following setting is available under the [Data Capture] group in the inow.ini configuration file.

data.capture.integration = TRUE or FALSE

Specifies whether DataCapture is enabled.

- TRUE = Data Capture integration is activated.
- FALSE = Data Capture integration is deactivated.

Default = FALSE

inow.ini [Digital Signature] settings

The following settings are available under the [Digital Signature] group in the inow.ini configuration file.

These settings are only available if you have a Document Management license.

You must restart ImageNow Server if you change these settings in the inow.ini file. If you make changes from the Management Console, you do not need to restart the server.

digIDExpireInterval = any positive integer

Specifies the expiration period, in days, for digital IDs.

0 = Digital ID never expires.

Default = 365

digSigReportDisplay = 0, 1, or 2

Specifies the digital signature display option when printing a Digital Signature report.

- 0 = Disables the report.
- 1 = Prints only valid digital signatures on the report.
- 2 = Prints all digital signatures on the report.

Default = 1

digSigPwdOption = TRUE or FALSE

Specifies whether a user who digitally signed a document but who did not log out before the specified timeout value must re-enter his or her digital signature password.

- TRUE = Digital signature password option is activated.
- FALSE = Digital signature password option is deactivated.

Default = FALSE

dig.sig.pwd.imagenow.timeout = 1, 2, 3, 4, 5, 10, 15, 20, 25, 30. 40, 50, or 60

Specifies the amount of time, in minutes, before the user must re-enter his or her digital signature password when logged in to Perceptive Content.

The timeout applies globally to all digital signatures.

Adding any value other than those specified results in the value being ignored.

Default = 1

dig.sig.lock.addendum.only = TRUE or FALSE

Specifies whether an addendum is required to modify a signed document.

- TRUE = An addendum is required.
- FALSE = An addendum is not required.

Default = FALSE

inow.ini [Directory Locations] settings

The following settings are available under the [Directory Locations] group in the inow.ini configuration file.

form.dir = any valid directory

Specifies the forms directory.

You may set the directory to any location, including other drives, such as *Z:\forms*, and it can be named anything. You may also set it as a Windows UNC path name, such as *computername**form**path*. The original path may still be used under this new capacity.

Default = *$(IMAGENOWDIR)/form*.

form.shared.dir = any valid directory

Specifies the location of shared form files.

Can be its own full path. You may set the directory to any location, including other drives, such as *Z:\formsshare*, and it can be named anything. You may also set it as a Windows UNC path name, such as *computername**share**path*. The original path may still be used under this new capacity.

Default = shared

logging.dir = any valid directory

Specifies the directory in which ImageNow Server and Agents store log files.

Default = *$(IMAGENOWLOCALDIR)/log*.

inow.ini [Doc] settings

The following settings are available under the [Doc] group in the inow.ini configuration file.

scan.as.creation = TRUE or FALSE

Specifies whether the scanning user or current user is identified as the document creation user.

- TRUE = Scanning user is document creation user.
- FALSE = Current user is document creation user.

Default = TRUE

inow.ini [DocLock] settings

The following settings are available under the [DocLock] group in the inow.ini configuration file.

doclock.lock_retries = any positive integer

Specifies the number of attempts allowed to lock a document.

Default = 5

doclock.lock_timeout = any positive integer

Specifies the number of milliseconds ImageNow Server waits between lock retries.

Default = 1000

inow.ini [Envoy] settings

The following settings are available under the [Envoy] group in the inow.ini configuration file.

date.time.zone.enabled = TRUE or FALSE

- TRUE = Includes the time zone from the end of an XSD date type.
- FALSE = Removes the time zone from the end of an XSD date type. For example, if set to FALSE, YYYY-MM-DDZ will be displayed as YYYY-MM-DD, where Z is the time zone.

Default = FALSE

pcr.soap.bridge.url = http://<location of pcr instance>/rs/soapBridge

URL of the pcr instance with SOAPBridge Connector.

inow.ini [ERM] settings

The following setting is available under the [ERM] group in the inow.ini configuration file.

erm.enabled = TRUE or FALSE

Specifies whether you are using ERM.

- TRUE = ERM is enabled.
- FALSE = ERM is disabled.

Default = FALSE

inow.ini [Experience] setting

The following setting is available under the [Experience] group in the inow.ini configuration file.

experience.url

Specifies the URL for Perceptive Experience.

experience.url = any valid URL

The default is `http://host/experience/`.

inow.ini [Fax Out] settings

The following setting is available under the [Fax Out] group in the inow.ini configuration file.

fax.out.integration = TRUE or FALSE

Specifies whether outbound faxing is enabled.

- TRUE = Outbound faxing is enabled.
- FALSE = Outbound faxing is disabled.

Default = FALSE

inow.ini [Folders] settings

The following setting is available under the [Folders] group in the inow.ini configuration file.

search.in.subfolders.enable = TRUE or FALSE

Specifies whether to search within the subfolders of a folder hierarchy.

- TRUE = Searching within subfolders is activated.
- FALSE = Searching within subfolders is deactivated.

Default = FALSE

inow.ini [Forms] settings

The following setting is available under the [Forms] group in the inow.ini configuration file.

form.integration = TRUE or FALSE

Specifies whether forms are enabled.

- TRUE = Forms are enabled.
- FALSE = Forms are disabled.

Default = FALSE

inow.ini [General] settings

The following settings are available under the [General] group in the inow.ini configuration file.

workerthread.monitor.enabled = TRUE or FALSE

Specifies whether unresponsive workers should be detected throughout the server process.

- TRUE = Unresponsive workers are monitored.
- FALSE = Unresponsive workers are not monitored.

Default = TRUE

workerthread.monitor.hangthreshold = any positive integer

Marks a thread as unresponsive or hung, if it is inactive for <*value*> seconds.

Default = 300

workerthread.monitor.pollinginterval = any positive integer

Specifies the interval, in seconds, at which worker threads are checked for responsiveness.

Default = 180

resource.monitor.query.timeout = any positive integer

Specifies the timeout, in seconds, for querying the resource health monitor.

Default = 5

num.crossnode.cache.recovery.attempts = any positive integer

Specifies the number of times to requeue a cross-node cache work item after failing to publish. There is a one minute delay between publication attempts after each failure. Inserver and inserverWorkflow can use this setting for cross-node cache publication behavior.

Default = 1

num.async.retry.workers = any positive integer

Specifies the number of worker threads in the asynchronous retry pool.

Default = 1

async.retry.between.work.delay.milliseconds = any positive integer

Specifies the interval, in milliseconds, in which the asynchronous retry queue is checked for new work.

Default = 100

inow.ini [iScript] settings

The following setting is available under the [iScript] group in the inow.ini configuration file.

iscript.encoding = UTF-8 or ANSI

Unicode build default = UTF-8

Non-Unicode build default = ANSI

inow.ini [Licenses] settings

The following setting is available under the [Licenses] group in the inow.ini configuration file.

hardware.amazonec2.support = TRUE or FALSE

Set this setting to TRUE when you are acquiring an Amazon EC2 ImageNow Server node license and generate a hardware system fingerprint.

- TRUE = You are using an Amazon EC2 ImageNow Server node license.
- FALSE = You are not using an Amazon EC2 ImageNow Server node license.

Default = FALSE

inow.ini [Locale] settings

The following setting is available under the [Locale] group in the inow.ini configuration file.

supported.locale = EN, FR, DE, ES

Specifies the languages that are supported.

- EN = English
- FR = French
- DE = German
- ES = Spanish

Default = EN

inow.ini [Logging] settings

The following settings are available under the [Logging] group in the inow.ini configuration file.

rolling.log.files.enabled = TRUE or FALSE

Enables Perceptive Content to create multiple log files of a size you specify. This setting is useful in large scale environments where log files tend to be large.

rolling.log.files.enabled = TRUE or FALSE

The default is FALSE.

rolling.log.files.threshold = any positive integer

When rolling.log.files.enabled is set to TRUE, this setting specifies the size in MB of the log files.

rolling.log.files.threshold = any positive integer

The default is 100.

inow.ini [Logon Control] settings

The following settings are available under the [Logon Control] group in the inow.ini configuration file.

logon.method = SYSTEM, LDAP, or SQL

Specifies the value that determines what method to use when inserver authenticates user logons.

- SYSTEM = inserver uses OS authentication methods. For Windows, inserver authentication methods as defined by `nt.logontype`.
- LDAP = inserver uses LDAP authentication methods as defined by LDAP values.
- SQL = inserver users SQL authentication methods as defined by `auth.*`values.

Default = SYSTEM

nt.logontype = 1, 2, or 3

If logon.method is set to SYSTEM, and Windows NT is the operating system, this setting specifies the type of NT User verification logon Perceptive Content passes to the NT LogonUser API call.

Note: Do not change these settings without first consulting with Enterprise Software Support.

- 1 = Logon_Interactive
- 2 = Logon_Service
- 3 = Logon_Batch

Default = 1

client.validation = TRUE or FALSE

Specifies whether Perceptive Content allows the Perceptive Content Client to log on with the User ID provided in the Perceptive Content logon dialog box.

- TRUE = Perceptive Content Client logs on with the User ID provided in the Perceptive Content logon dialog box as long as the user is logged into a valid Windows NT domain on the client PC with a NT domain account that is equal to the Perceptive Content User ID. Otherwise, Perceptive Content validates user and password requests through the Perceptive Content Server.
- FALSE = Perceptive Content Client does not log on with the User ID provided.

Default = FALSE

nt.domain.list = domains separated by commas

Specifies the valid NT Domain list that Perceptive Content Client must already be logged into on the requesting PC.

Default = None

ldap<*n*>.server= any valid IP address or server name

If logon.method is set to LDAP, Perceptive Content uses the `ldap.*` settings for LDAP logon authentication.

This setting specifies the IP address or name of the server.

Note: You can define additional LDAP server configurations by creating additional LDAP settings that are sequentially numbered, such as ldap2.server, ldap2.server.port, and so on.

When using LDAP with SSL, you must specify the fully qualified domain name (FQDN) for this setting.

Default = 0.0.0.0

ldap<*n*>. server.port = any valid port number

Specifies the port number used by the LDAP server.

Default = 389

ldap<*n*>.login = any valid user DN

Specifies the LDAP user DN for binding to the LDAP server to begin the search for user entries.

Note: This setting is required for direct and indirect authentication.

Default = None

ldap<*n*>.password = any valid password

Specifies the LDAP password for the user DN specified in the `ldap.login` setting. It is required for direct and indirect authentication. This value is encrypted and removed from the setting after running the `inserver -encrypt-config` command.

Note: If the ldap.password or ldap.login property is left blank, Perceptive Content Server automatically attempts an anonymous login.

Default = None

ldap<*n*>.password.encrypted = encrypted password

Specifies the encrypted LDAP password for the user DN generated from the supplied password in the `ldap.password` setting.

ldap<*n*>use.ssl = TRUE or FALSE

Specifies whether to use LDAP over SSL.

- TRUE = LDAP over SSL is enabled.
- FALSE = LDAP over SSL is disabled.

Default = FALSE

ldap<*n*>.method

Specifies which LDAP method to use.

1 = Direct binding

2 = Indirect binding

The default is 1.

ldap<*n*>.ImageNow.Groups = any list of valid groups separated by carets (^)

Specifies lists of groups that use LDAP.

Default = None

ldap<*n*>.ImageNow.Users = any list of valid users separated by carets (^)

Specifies lists of users that use LDAP.

Default = None

ldap<*n*>.name.prepend = any string

If `ldap.method` is set to `1`, this setting specifies the string to add before the user name.

Default = None

ldap<*n*>.name.append<*n*> = any string

If `ldap.method` is set to `1`, this setting specifies the string to add after the user name.

Note: You can specify multiple appends by adding sequentially numbered ldap.name.append settings.

Default = None

ldap<*n*>.base.dn = any valid DN

Specifies the base or root DN of the LDAP server where you want the search to begin and search all its containers, such as `ldap.base.din = OU = Research and Development, DC = acme, DC = com .`

Default = None

ldap<*n*>.login.attr = any valid attribute

Specifies the LDAP user attribute you want to search for in the LDAP server. The search looks for the attribute whose value is the value entered in the Perceptive Content login, such as `ldap.login.attr = sAMAccountName`.

Default = None

ldap.ssl.cert.path = any valid directory

Specifies the location of the LDAP SSL certificate.

Default = *$(IMAGENOWDIR)/etc*

Example value = /opt/inserver/etc

ldap.ssl.version.min=SSL3, TLS10, TLS11, TLS12

Specifies the minimum version of SSL/TLS.

Default = TLS10

Note: This setting is for UNIX environments only.

ldap.ssl.version.max=SSL3, TLS10, TLS11, TLS12

Specifies the maximum version of SSL/TLS.

Default = TLS12

Note: This setting is for UNIX environments only.

ldap.ssl.cert.fips.token

Specifies the name of the FIPS token in the certificate database.

Default = None

Example value = NSS FIPS 140-2 Certificate DB

Note: This setting is for UNIX environments only.

ldap.ssl.cert.fips.password

Specifies the password for the FIPS token in the certificate database. This password can be encrypted for additional security by running the `inserver -encrypt-config` command.

The password must meet the following criteria.

- At least seven characters in length.
- Includes characters from three or more character classes. Character classes include digits, lowercase letters, uppercase letters, and ASCII non-alphanumeric characters.

Note: If the first character is an uppercase letter or the last character is a digit, these do not count toward the character class requirement.

Default = None

Note: This setting is for UNIX environments only.

auth.sql.query = any valid string

If logon.method is set to SQL, this setting defines the SQL query string for authentication.

Note: Do not use a SELECT COUNT (*) . This query must return one row if valid and no rows if invalid.

Default = None

logon.singlesignon.enable = TRUE or FALSE

Specifies whether users running multiple desktop clients can use the same workstation.

- TRUE = Perceptive Content Server allows users running multiple desktop clients on the same workstation to log on to both clients by logging into one client and sharing the connection between the two clients. The user is only prompted to log in once.
- FALSE = Perceptive Content Server does not allow single sign-on.

Default = TRUE

logon.minclientversion = any valid Perceptive Content Client version number that uses the general format, <major>.<minor>.<revision>.<build>

Specifies the Perceptive Content version number the Windows Client must meet or exceed to log on to Perceptive Content Server.

Default = 0.0.0.1

Note: This may be changed to force upgrades for revisions and builds within the same release version.

logon.minclientversion.msg = any text string

Specifies the message that appears when the user s Windows Client version does not meet or exceed the logon.minclientversion setting.

Default = Consult your system administrator for assistance in upgrading Perceptive Content Client.

token.signing.key.path = any valid path

Specifies the path to a PEM encoded RSA or ECC private key to be used for signing tokens.

Default = None

token.signing.key.password = any valid password

Specifies the password to use if the signing key is encrypted.

Default = None

token.signing.algorithm = any valid algorithm

Specifies the algorithm to use to sign tokens.

Depending on key size, valid values for RSA signing keys are RS256, RS384, and RS512.

Depending on the eliptic curve, valid values for ECC signing keys are ES256, ES384, and ES512.

Default = None

inow.ini [Memory] settings

This topic displays in a list the inow.ini settings under the [Memory] group.

receive.memory.threshold

Specifies whether a temp file or memory is used during transfers if more than <*value*> MB of data is received.

receive.memory.threshold = any positive integer

The default is 1.

inow.ini [Message Queuing] settings

This topic displays in a list the inow.ini settings under the [Message Queuing] group.

Server Settings

mq.reconnect.interval

Specifies how long, in seconds, Perceptive Content waits before reattempting to connect to the message queuing broker after a failed attempt.

mq.reconnect.interval = any positive integer

The default is 60.

mq.host

Specifies the hostname or IP address of the node running the message queuing broker.

mq.host = any valid hostname or IP address

mq.port

Specifies the port the message queuing broker uses.

mq.host = any valid port

Note: The commonly used message queuing port is 5672.

mq.vhost

Specifies the name of a virtual host.

mq.host = name of the virtual host

mq.username

The user name used when connecting to the message queuing broker.

mq.username = any valid user name

mq.password

Specifies the password consumed for encryption in the mq.password.encrypted setting. This value is encrypted and removed from the setting after running the `inserver -encrypt-config` command.

mq.password = password for the user name

Note: You can run the `inserver -encrypt-config` command after configuring local agents to obfuscate any stored passwords.

mq.password.encrypted

Indicates the encrypted password used by the message queuing broker.

The password is supplied in the mq.password setting and is encrypted after running the `inserver -encrypt-config` command.

Note: Do not manually update this setting value.

mq.secure.enable

Specifies whether SSL/TLS is used.

mq.secure.enabled = TRUE or FALSE

The default is FALSE.

Note: For Windows, the default verify locations for the TLS server certification validation are used. For Linux, the SSL_CERT_DIR environment variable must be set to the location of the CAP.pem file.

mq.validate.server.certificate.enable

Enables certification validation.

mq.validate.server.certificate.enable = TRUE or FALSE

The default is TRUE.

Note: You must set mq.secure.enable to TRUE and mq.validate.server.certification.enable to TRUE for the validation to be performed.

mq.connection.wait.milliseconds

Specifies how long, in milliseconds, Perceptive Content may wait to establish a connection to the message queuing broker. This setting is only used by INTool.

mq.connection.wait.milliseconds = any positive integer

The default is 0.

Note: A value of 0 means Perceptive Content will not wait to establish a connection to the message queuing broker.

mq.publication.retry.interval.seconds

Specifies how long, in seconds, Perceptive Content waits to republish a persistent message after the first publication attempt fails. This setting is used by all agents that publish persistent messages to the MQ broker.

mq.publication.retry.interval.seconds = any positive integer

The default is 300.

Client Settings

Note: If any of the following settings are incorrectly specified in the inow.ini file, Perceptive Content Client cannot connect to the message queuing broker. If this occurs, a message is logged in the Message Center.

mq.client.reconnect.interval

Specifies how long, in seconds, Perceptive Content waits before reattempting to connect to the message queuing broker after a failed attempt.

mq.client.reconnect.interval = any positive integer

The default is 60.

mq.client.host

Specifies the hostname or IP address of the node running the message queuing broker.

mq.client.host = any valid hostname or IP address

mq.client.port

Specifies the port used to connect to the message queuing broker from the Perceptive Content Client.

mq.client.port = any valid port

The default is the port specified for the mq.port setting.

mq.client.username

The user name used when connecting to the message queuing broker.

mq.client.username = any valid user name

mq.client.password

Specifies the password consumed for encryption in the mq.client.password.encrypted setting. This value is encrypted and removed from the setting after running the `inserver -encrypt-config` command.

mq.client.password = password for the user name

Note: You can run the `inserver -encrypt-config` command after configuring local agents to obfuscate any stored passwords.

mq.client.password.encrypted

Indicates the encrypted password used by the message queuing broker.

The password is supplied in the mq.client.password setting and is encrypted after running the `inserver -encrypt-config` command.

Note: Do not manually update this setting value.

mq.client.secure.enable

Specifies whether SSL/TLS is used.

mq.client.secure.enabled = TRUE or FALSE

The default is FALSE.

Note: For Windows, the default verify locations for the TLS server certification validation are used. For Linux, the SSL_CERT_DIR environment variable must be set to the location of the CAP.pem file.

mq.client.validate.server.certificate.enable

Enables certification validation.

mq.client.validate.server.certificate.enable = TRUE or FALSE

The default is TRUE.

Note: You must set mq.client.secure.enable to TRUE and mq.client.validate.server.certification.enable to TRUE for the validation to be performed. Also note that if this setting is enabled, all clients must have a signed trusted CA Root certificate installed and configured or the message queuing connection fails.

inow.ini [Migration] settings

This topic displays in a list the inow.ini settings under the [Migration] group.

migration.enabled

Specifies whether migration functionality is enabled for Perceptive manager users only.

migration.enabled = TRUE or FALSE

The default is TRUE.

inow.ini [Network] settings

The following setting is available under the [Network] group in the inow.ini configuration file.

encryption.enabled = FALSE

Specifies whether data encryption is enabled for the network.

Values = TRUE or FALSE

- TRUE = Encryption is enabled.
- FALSE= Encryption is not enabled.

ipv6.enabled = FALSE

Specifies whether Internal Protocol version 6 (IPv6) is enabled for the network. If it is disabled, the process supports IPv4.

Values = TRUE or FALSE

- TRUE = IPv6 is enabled.
- FALSE = IPv6 is disabled.

encryption.symmetric.min.key.strength = 128

Specifies the allowed minimum AES key strength to use when communicating with the server.

Note: Prior to altering the default value, review your Java encryption policies for any deployed Perceptive server applications to ensure they support the same encryption strengths.

Values = 128, 192, 256

encryption.symmetric.max.key.strength = 128

Specifies the allowed maximum AES key strength to use when communicating with the server.

Note: Prior to altering the default value, review your Java encryption policies for any deployed Perceptive server applications to ensure they support the same encryption strengths.

Values = 128, 192, 256

encryption.asymmetric.min.key.strength = 512

Specifies the allowed minimum RSA key strength to use when authenticating with the server.

Note: Prior to altering the default value, review your Java encryption policies for any deployed Perceptive server applications to ensure they support the same encryption strengths.

Values = 512, 1024, 2048, 4096

Note: Setting the value to 4096 may result in extended login times.

encryption.asymmetric.max.key.strength = 512

Specifies the allowed maximum RSA key strength to use when authenticating with the server.

Note: Prior to altering the default value, review your Java encryption policies for any deployed Perceptive server applications to ensure they support the same encryption strengths.

Values = 512, 1024, 2048, 4096

Note: Setting the value to 4096 may result in extended login times.

inow.ini [OCR] settings

This topic displays in a list the inow.ini settings under the [OCR] group.

ocr.integration

Specifies whether OCR is enabled.

ocr.integration = TRUE or FALSE

The default is FALSE.

inow.ini [ODBC] settings

The following information is available under the [ODBC] group in the inow.ini settings .

odbc.dbms

Specifies the DBMS that Perceptive Content uses.

odbc.dbms = Oracle or SQL Server

The default is *SQL Server*.

odbc.dsn

Specifies the name of your Perceptive Content database.

odbc.dsn = any valid database name

The default is Perceptive Content.

odbc.user.id

Specifies the user ID for the ODBC connection.

odbc.user.id = any valid user name

The default is *inuser*.

odbc.user.password

Specifies the password that is consumed by the application for encryption in the odbc.user.password.encrypted setting. This value is encrypted and removed from the setting after running the `inserver -encrypt-config` command.

odbc.user.password = any valid password

The default is *imagenow*.

odbc.user.password.encrypted

Specifies the encrypted password for the database that is maintained by the application.

The password is supplied in odbc.user.password.

odbc.use_dddriver

Specifies whether ODBC uses the DD driver.

odbc.use_dddriver = TRUE or FALSE

The default is TRUE.

odbc.grid.max.fetch.countodbc.dbms

Specifies the maximum number of records retrieved by ODBC at one time.

This setting applies to workflow, batch, related documents, document search, folder search, ERM, and folder viewer grids.

Note: For changes to this setting to take effect in Perceptive Content, you must also change the Maximum results setting in View Designer, or in the Appearance properties of the folder type, workflow queue, or workflow process.

odbc.grid.max.fetch.countodbc.dbms = any positive integer

The default is 2000.

auth.odbc.dbms

Perceptive Content Server uses auth.* settings to connect to the authorization database when logon.method is set to SQL.

This setting specifies the database management system (DBMS) Perceptive Content uses.

auth.odbc.dbms = Oracle or SQL Server

There is no default for this setting.

auth.odbc.dsn

Specifies the name of your Perceptive Content database.

auth.odbc.dsn = any valid database name

There is no default for this setting.

auth.odbc.user.id

Specifies the user ID for the ODBC connection.

auth.odbc.userid = any valid user name

The default is *inuser*.

auth.odbc.user.password

Specifies the password that is consumed by the application for encryption in the auth.odbc.user.password.encrypted setting. This value is encrypted and removed from the setting after running the `inserver -encrypt-config` command.

auth.odbc.user.password = any valid password

The default is *imagenow*.

auth.odbc.user.password.encrypted

Specifies the encrypted password for the ODBC connection that is maintained by the application.

The password is supplied in auth.odbc.user.password.

auth.odbc.unicode

Specifies whether the AUTH database is Unicode or ANSI.

TRUE = The AUTH database is Unicode.

FALSE = The AUTH database is ANSI.

The default for Unicode builds is TRUE.

The default for ANSI builds is FALSE.

odbc.oracle.optimizer_cost_based_transformation

Controls whether the optimizer tries different transformations against a query using cost with and without the transformations.

odbc.oracle.optimizer_cost_based_transformation = TRUE or FALSE

TRUE = Enables optimizer query transformations.

FALSE = Disables optimizer query transformations.

The default is FALSE.

odbc.oracle.optimizer_cost_based_transformation.override.enabled

Overrides odbc.oracle.optimizer_cost_based_transformation behavior when running on an Oracle database. We recommend enabling this setting when odbc.oracle.relace_virtual_ columns.override.enabled is set to true and you are running Perceptive Content agents on a Linux environment.

odbc.oracle.optimizer_cost_based_transformation.override.enabled = TRUE or FALSE

TRUE = Enables overriding odbc.oracle.optimizer_cost_based_transformation at the session level. The system uses the value for odbc.oracle.optimizer_cost_based_transformation.

FALSE = The system uses the default value for odbc.oracle.optimizer_cost_based_transformation.

The default is FALSE.

odbc.oracle.replace_virtual_columns

Changes the explain plan to either enable or disable the use of function based indexes.

odbc.oracle.replace_virtual_columns = TRUE or FALSE

TRUE = Explain plan does not use the function based index.

FALSE = Explain plan uses the function based index.

The default is FALSE.

odbc.oracle.replace_virtual_columns.override.enabled

Overrides odbc.oracle.replace_virtual_columns behavior when running on an Oracle database. We recommend enabling this setting. If necessary, consult with your system database administrator.

odbc.oracle.replace_virtual_columns.override.enabled = TRUE or FALSE

TRUE = Enables overriding odbc.oracle.replace_virtual_columns at the session level. The system uses the value for odbc.oracle.replace_virtual_columns.

FALSE = The system uses the default value for odbc.oracle.replace_virtual_columns parameter.

The default is FALSE.

odbc.oracle.views.dynamic.sampling.override.enabled

Specifies a dynamic sampling when you are running views on an Oracle database.

odbc.orcale.dynamic.views.sampling.override.enabled = TRUE or FALSE

TRUE = Dynamic sampling can be set to a value from 0 to 10.

FALSE = Oracle s dynamic sampling does not change from its default.

The default is FALSE.

odbc.oracle.views.dynamic.sampling

Specifies a dynamic sampling when you are running views on an Oracle database.

odbc.oracle.views.dynamic.sampling = any integer from 0 to 10

0 = Disables dynamic sampling.

Higher values increase the triggering criteria and sample size of dynamic sampling.

The default is 2.

recovery.reuse.db.conn

Specifies whether connections are reused in the respective DB connection pool after a database failure occurs.

recovery.reuse.db.conn = TRUE or FALSE

TRUE = Connections are reused in the respective DB connection.

FALSE = Connection pooling should be disabled on the ODBC datasource to ensure these settings work correctly.

The default is FALSE.

inow.ini optional settings

This topic displays in a list optional settings for the inow.ini file.

In addition to the standard settings, you can add the following settings to inow.ini as needed.

logon.settings.delimiter

Under {Logon Control}, add `logon.settings.delimiter`.

This setting allows you to select a character to be the delimiter for the LDAP.Perceptive Content.Groups and LDAP.Perceptive Content.Users settings. You can use any symbol you want except for the square brackets, [and].

temp.dir

Under [Directory Locations], add `temp.dir`.

This setting allows you to change the directory Perceptive Content uses for temporary files. The default location is $(IMAGENOWDIR)/temp.

inow.ini [OSM] settings

filesystem.minimum.required.space

Specifies, in bytes, the free disk space threshold for OSM storage. When the threshold is exceeded, Perceptive Content displays a warning message.
This value is a maximum of (2^31) bytes. If the device has fewer bytes available than the value specified in this setting, no document is stored. This statement applies to FSS trees. If an OSM tree does not have enough space, Perceptive Content checks other OSM trees in that OSM set. If there is no tree available that contains enough space, an error results.

filesystem.minimum.required.space = any integer from 0 to 2,147,483,648

The default is 2,000,000.

large.file.temp.dir

Specifies the location of the directory OSM plugins used for temporary storage of large files.

Note: This setting does not appear in the inow.ini file by default. You must create it.

large.file.temp,dir = any valid directory

The default is *$(IMAGENOWDIR)/temp/osmtmp*.

osm.secure.delete

Specifies whether OSM objects should be securely deleted when files are deleted from the system.

osm.secure.delete = TRUE or FALSE

TRUE = Wipes files with a single pass before deleting them to prevent data from being recovered with file recovery tools.

FALSE = Does not wipe files, and some data may be recoverable with file recovery tools.

The default is FALSE.

osm.allowed.file.extensions

Specifies the file extensions the system allows for importing.

Note: This setting takes precedence over the osm.disallowed.file.extensions setting. All values in osm.disallowed.file.extensions are ignored if this setting is populated. If this setting has been populated, all imported objects must have a file type.

osm.allowed.file.extensions = any valid file extension.

Note: You must separate multiple extensions with semicolons.

There is no default for this setting.

osm.disallowed.file.extensions

Specifies the file extensions the system does not allow for importing.

Note: The osm.allowed.file.extensions setting takes precedence over this setting. All values in this setting are ignored if the osm.allowed.file.extensions setting has been populated.

osm.disallowed.file.extensions = any valid file extension.

Note: You must separate multiple extensions with semicolons.

There is no default for this setting.

inow.ini [Records] settings

This topic displays in a list the inow.ini settings under the [Records] group.

records.retain.metadata

Specifies whether the system saves metadata for reporting purposes during a destruction action for records and record folders.

records.retain.metadata = TRUE or FALSE

The default is FALSE.

declare.record.default.organization

Specifies the default value of the organization for declaring a document as a record.

declare.record.default.organization = any valid organization name

By default, the value of this settings is left blank.

inow.ini [Redaction] settings

This topic displays in a list the inow.ini settings under the [Redaction] group.

redaction.service.uri=

Specifies the URI for the Redaction service.

inow.ini [Statistics] settings

This topic displays in a list the inow.ini settings under the [Statistics] group.

stats.ss.delimiter

Specifies the character used as a delimiter between column in statistics log files.

stats.ss.delimiter = any valid character

There is no default for this setting.

stats.all.log.type

Specifies the logging period for all types of statistics logs.

Note: If you set a subsequent status.<*category*>.log.type setting, that category s settings override these global statistic settings.

stats.all.timer.period = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.all.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 2.

stats.all.timer.period

If stats.all.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a statistics log.

stats.all.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.all.start.time

If stats.all.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.all.start.time = any positive integer from 0 to 23

The default is 0.

stats.all.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.all.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.servercall.log.type

Specifies the logging period for ImageNow Server logs.

stats.servercall.timer.period = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.servercall.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.servercall.timer.period

If stats.servercall.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a ImageNow Server log.

stats.servercall.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.servercall.start.time

If stats.servercall.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.servercall.start.time = any positive integer from 0 to 23

The default is 0.

stats.servercall.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.servercall.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.query.log.type

Specifies the logging period for SQL logs.

stats.query.log.type = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.query.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.query.timer.period

If stats.query.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a SQL log.

stats.query.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.query.start.time

If stats.query.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.servercall.start.time = any positive integer from 0 to 23

The default is 0.

stats.query.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.query.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.query.plan.threshold

Specifies, in seconds, the threshold for queries. And query that takes longer to run than the threshold is included in the log. The query is logged in a separate details log where the execution plan for that query is written.

stats.query.plan.threshold = any positive integer from 0 to 3599.999

The default is 1.0.

stats.query.plan.freq

Specifies how often query plans are included in the log.

stats.query.plan.freq = any positive integer from 0 to 100

0 = Query plans are not logged.

n = Query plans that exceed the threshold specified in stats.query.plan.threshold are included in every *n* log periods and are logged to a separate details log.

For example, stats.query.plan.freq = 2 means query plans are logged once every two log periods.

The default is 1.

stats.storage.log.type

Specifies the logging period for OSM storage operations logs.

stats.storage.log.type = 0, 1, 2, 3, 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.storage.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.storage.timer.period

If stats.storage.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates an OSM storage operations log.

stats.storage.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.storage.start.time

If stats.storage.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.servercall.start.time = any positive integer from 0to 23

The default is 0.

stats.storage.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.storage.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.mq.log.type

Specifies the logging period for message queue logs.

stats.mq.log.type = 0, 1, 2, 3, 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.mq.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.mq.timer.period

If stats.storage.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a message queue log.

stats.mq.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.mq.start.time

If stats.mq.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.mq.start.time = any positive integer from 0to 23

The default is 0.

stats.mq.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.mq.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.wfaction.log.type

Specifies the logging period for WFActions logs.

stats.wfaction.log.type = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

> **Note:** If you set this setting to 1, you must specify the number of seconds in the stats.wfaction.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.wfaction.timer.period

If stats.wfaction.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a WFActions log.

stats.wfaction.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.wfaction.start.time

If stats.wfaction.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.wfaction.start.time = any positive integer from 0 to 23

The default is 0.

stats.wfaction.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.wfaction.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.thread.log.type

Specifies the logging period for ImageNow Server thread logs.

stats.thread.log.type = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

> **Note:** If you set this setting to 1, you must specify the number of seconds in the stats.thread.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.thread.timer.period

If stats.thread.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a ImageNow Server thread log.

stats.thread.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.thread.start.time

If stats.thread.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.thread.start.time = any positive integer from 0 to 23

The default is 0.

stats.thread.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.thread.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.job.log.type

Specifies the logging period for job logs.

stats.job.log.type = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

Note: If you set this setting to 1, you must specify the number of seconds in the stats.job.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.job.timer.period

If stats.job.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a job log.

stats.job.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.job.start.time

If stats.job.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.job.start.time = any positive integer from 0 to 23

The default is 0.

stats.job.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.job.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

stats.licensing.log.type

Specifies the logging period for licensing logs.

stats.licensing.log.type = 0, 1, 2, 3, or 4

0 = Logging is turned off.

1 = Logging period is user defined.

> **Note:** If you set this setting to 1, you must specify the number of seconds in the stats.licensing.timer.period setting.

2 = Logging period is hourly.

3 = Logging period is every six hours.

4 = Logging period is every 12 hours.

The default is 0.

stats.licensing.timer.period

If stats.licensing.log.type is set to 1, this setting specifies the frequency, in seconds, at which Perceptive Content creates a licensing log.

stats.licensing.timer.period = any positive integer from 5 to 3595

The default is 1800.

stats.licensing.start.time

If stats.licensing.log.type is set to 3 or 4, this setting specifies the starting hour statistics when logs are created for six to 12 hour logs.

stats.licensing.start.time = any positive integer from 0 to 23

The default is 0.

stats.licensing.action.length

Truncates the action string printed to the log to the number of characters specified as the value.

stats.licensing.action.length = any positive integer from 0 to 1000

0 = Show all.

The default is 0.

inserver.ini

The following links provide definitions and sample data for the configuration settings for the different groups of the inserver.ini file.

- Anonymous login
- Business Insight
- Client
- Department
- Experience URL
- Folders
- General
- LearnMode
- Logging
- Network
- OpenID Connect Login Profiles
- Remote
- Timing
- Views

inserver.ini [Anonymous Login] settings

This topic displays in a list the inserver.ini settings under the [Anonymous Login] group.

anonymous.login.enabled

Specifies whether ImageNow Server allows anonymous log on.

anonymous.login.enabled = TRUE or FALSE

The default is FALSE.

number.of.anonymous.users

Specifies how many anonymous users can be logged on to ImageNow Server.

number.of.anonymous.users = any positive integer

The default is 0.

inserver.ini [Business Insight] settings

This topic displays in a list the inserver.ini settings under the [Business Insight] group.

business.insight.authnamespace

Stores the authentication namespace used to connect to Business Insight.

business.insight.authnamespace = any valid namespace

By default, this value matches the Namespace ID value in Business Insight Configuration.

business.insight.address

Stores the URL, including the server, of the Business Insight reporting website set up in your web application server.

business.insight.address = any valid URL for Business Insight

There is no default for this setting.

business.insight.max.output.default

Stores the default number of prior versions of report output that appears when you set the value in Perceptive ContentManagement Console.

business.insight.max.output.default = any positive integer

The default is 5.

inserver.ini [ClientINI] settings

This topic displays in a list the inserver.ini settings under the [ClientINI] group.

client.ini.sync.mode

Specifies whether or not Perceptive Content .ini updates are automatically downloaded to the client. These updates occur during log in.

client.ini.sync.mode = 0, 1, or 2

0 = The client does not download updates.

1 = This setting tells the client to check for and download any updates on log in.

2 = This setting tells the client to download the file every time it logs into the server.

The default is 0.

client.ini.file.path

Specifies the path to the ImageNow.ini file used to update client INI files.

client.ini.file.path = any valid path

The default is $(IMAGENOWDIR6)/etc/clientINI/ImageNow.ini.

client.ini.search.grid.file.path

Specifies the path to the SearchGrid.ini file used to update client INI files.

client.ini.search.grid.file.path = any valid path

The default is $(IMAGENOWDIR6)/etc/clientINI/SearchGrid.ini

inserver.ini [DepartmentsINI] settings

This topic displays the inserver.ini settings in a list under the [DepartmentsINI] group.

department.labeling.enabled

Enables department labeling.

When enabled, a department label that you configure in department settings displays as a prefix for new items you create in Management Console.

department.labeling.enabled = TRUE or FALSE

The default is FALSE.

department.labeling.separator

This setting is only valid when the department.labeling.enabled setting is set to TRUE.

This setting allows you to specify separator characters between the department label and the name of the item in Management Console. The department label displays followed by a space, and then the character.

department.labeling.separator = Any valid character or a space character contained in quotations.

Note: Using the special characters [,] , { , and } is not recommended.

The default is - .

inserver.ini [Experience URL] settings

This topic displays in a list the inserver.ini settings under the [Experience URL] group.

Note:
The inserver.ini configuration file can include multiple [Experience URL] groups. Each [Experience URL] group must have a unique group name. The name must begin with Experience URL and end with a unique value. For example, [Experience URL Default], [Experience URL DrawerA] and [Experience URL DrawerA DocTypeA].

url.filter.type

Each [Experience URL] group must provide a `url.filter.type` key with one of the following values,

`default`, `drawer`, or `doctype`.

Experience URLs are matched in the following order, `doctype`, `drawer` and `default`.

doctype

- Doctype rules are evaluated before drawer rules.
- `drawer.name` and `doctype.name` keys must be provided and the values are case sensitive.
- Doctype is used if the document s drawer and doctype names match.
- `experience.url` must be supplied with a value. The URL specified is expected to be URL encoded and must have the `{{DocumentID}}` keyword in the location that you want to substitute the document s ID.

drawer

- Drawer rules are evaluated after doctype filters.
- `drawer.name` must be provided and the values are case sensitive.
- Drawer is used if the document s drawer name matches the provided drawer.name value and no doctype filter has been specified for the document s drawer and doctype combination.
- `experience.url` must be supplied with a value. The URL specified is expected to be URL encoded and must have the `{{DocumentID}}` keyword in the location that you want to substitute the document s ID.

default

- The default section is required and only one should be specified. If more than one default section is specified, the system will log an error message stating in which section the duplication occurred.
- `experience.url` must be supplied with a value. The URL specified is expected to be URL encoded and must have the `{{DocumentID}}` keyword in the location that you want to substitute the document s ID.

Example

```
[Experience Url Default]

url.filter.type=default

experience.url=https://<serverdomainname>/<webappname>?noheader/#documents
/view/<Admin_Chosen_viewID>/document/
{{DocumentId}}?simplemode=true&showforms=false&showproperties=false

[Experience Url DrawerA]

url.filter.type=drawer

drawer.name=DrawerA
```

```
experience.url=https://<serverdomainname>/<webappname>?noheader/#documents
/view/<Admin_Chosen_viewID>/document/
{{DocumentId}}?simplemode=true&showforms=false&showproperties=false

[Experience Url DrawerB]

url.filter.type=drawer

drawer.name=DrawerB

experience.url=https://<serverdomainname>/<webappname>?noheader/#documents
/view/<Admin_Chosen_viewID>/document/
{{DocumentId}}?simplemode=true&showforms=false&showproperties=false

[Experience Url DrawerB DocTypeA]

url.filter.type=doctype

drawer.name=DrawerB

doctype.name=DocTypeA

experience.url=https://<serverdomainname>/<webappname>?noheader/#documents
/view/<Admin_Chosen_viewID>/document/
{{DocumentId}}?simplemode=true&showforms=false&showproperties=false

[Experience Url DrawerB DocTypeB]

url.filter.type=doctype

drawer.name=DrawerB

doctype.name=DocTypeB

experience.url=https://<serverdomainname>/<webappname>?noheader/#documents
/view/<Admin_Chosen_viewID>/document/
{{DocumentId}}?simplemode=false&showforms=false&showproperties=true
```

inserver.ini [Folders] settings

This topic displays in a list the inserver.ini settings under the [Folders] group.

folders.move.maximum.results

Specifies the maximum number of folders to move.

folders.move.maximum.results = any positive integer

The default is 50.

folders.path.delimiter

Specifies the character used to separate values in the path that displays the folder location.

folders.path.delimiter = any character(s)

Note: To add a space before and after a character, enclose the spaces and delimiter character in quotation marks. For example, suppose you enter `folder.path.delimiter = " \ "` for the folders.path.delimiter setting. Perceptive Content displays the folder path as *<drawer name>* \ *<folder name>.*

There is no default for this setting.

inserver.ini [General] settings

This topic displays in a list the inserver.ini settings under the [General] group.

init.cache.vsl.rules.for.views

Specifies whether ImageNow Server pre-loads server-side cache of VSL statements associated with views and public filters when the service initially starts.

init.cache.vsl.rules.for.views = TRUE or FALSE

TRUE = ImageNow Server pre-loads server side cache.

FALSE = ImageNow Server does not pre-load server side cache.

The default is TRUE.

remove.old.service

Specifies whether ImageNow Server removes old services.

remove.old.service = 1 or 0

1 = ImageNow Server removes services.

0 = ImageNow Server does not remove services.

The default is 0.

client.autotimeout.enabled

Specifies whether ImageNow Server automatically times out the client after the client reaches the client timeout value.

client.autotimeout.enabled = TRUE or FALSE

TRUE = ImageNow Server times out the client.

FALSE = ImageNow Server does not time out the client.

The default is FALSE.

client.autotimeout

If client.autotimeout.enabled is set to TRUE, this setting specifies the number of minutes ImageNow Server waits before timing out the client. This setting applies to ImageNow Client and Interact Desktop Client. ImageNow Server supports a minimum of 30 minutes for ImageNow Client and 2 minutes for Interact Desktop Client.

client.autotimeout = any positive integer

For example, if you set this option to 5 minutes, ImageNow Server logs the ImageNow Client off after 30 minutes of inactivity, and Interact Desktop Client after 2 minutes of inactivity. If you leave the default setting, ImageNow Server logs off both clients after 30 minutes of inactivity.

The default is 30.

client.autotimeout.warning

If client.autotimeout.enabled is set to TRUE, this setting specifies the number of seconds that count down between when the timeout warning is displayed and when the user is logged out. This option should not exceed the client.autotimeout setting. If the client.autotimeout.warning value is greater than the client.autotimeout value, Perceptive Content disables the warning.

Note: This setting is available only for Interact Desktop.

client.autotimeout.warning = any positive integer (min = 10).

0=ImageNow Server does not send a warning

The default is 300.

client.autotimeout.deletelocalcopy

Specifies whether Document Management enables the user to save a local copy of a document when checking it into Perceptive Content.

client.autotimeout.deletelocalcopy = TRUE or FALSE

TRUE = The local copy is always deleted when checking the document in as a new version.

FALSE = The user has the option to delete the local copy when checking the document in as a new version.

The default is FALSE.

client.enable.filetype.checking

Specifies whether the client validates file type before proceeding with document operations.

client.enable.filetype.checking = TRUE or FALSE

The default is TRUE.

client.viewer.render.blacklist.filetypes

Specifies which files types should not be directly rendered in the Perceptive Content client.

client.viewer.render.blacklist.filetypes = any valid file extension, such as XLSX, XLS or PDF

Note:
You must separate multiple file extensions with semicolons.

The default is empty.

disable.pdf.thumbnail.generation

Specifies whether ImageNow Serverenables thumbnail image generation for PDF files.

disable.pdf.thumbnail.generation= TRUE or FALSE

TRUE = The system disables generation of thumbnail images for PDF files.

FALSE = The system enables generation of thumbnail images for PDF files.

The default is TRUE.

thumbnail.max.size

Specifies the maximum pixel size for thumbnail images. Setting the maximum about 500 is not recommended.

thumbnail.max.size = any positive integer

The default is 100.

thumbnail.batch.size

Specifies the number of thumbnail images to retrieve at one time.

Note: This setting is available only for Interact Desktop.

thumbnail.batch.size = any positive integer from 1 to 50

The default is 5.

num.workers

Specifies the number of worker threads in the main pool.

num.workers = any positive integer

The default is 15.

num.async.workers

Specifies the number of worker threads in the asynchronous pool.

num.async.workers = any positive integer

The default is 1.

num.crossnode.cache.workers

Specifies the number of worker threads ImageNow Server dedicates to cross-node cache synchronization.

num.crossnode.cache.workers = any positive integer

The default is 2.

navigation.thumbnails.enabled

Specifies whether or not thumbnails are displayed in the Navigation areas of Interact Desktop.

Note: This setting is available only for Interact Desktop.

navigation.thumbnails.enabled = TRUE or FALSE

The default is TRUE.

inserver.ini [LearnMode] settings

This topic displays in a list the inserver.ini setting sunder the [LearnMode] group.

pretrieve.interval

Specifies, in milliseconds, the polling interval value for LearnMode Pretrieve.

Note: This setting is only available for Interact Desktop.

pretrieve.interval = any positive integer from 0 to 10,000

The default is 1000.

inserver.ini [Logging] settings

This topic displays in a list the inserver.ini settings under the [Logging] group.

socket.level.file

Specifies how ImageNow Server logs socket communication.

socket.level.file = 0, 1, 2, or 3

0 = ImageNow Server does not log communication.

1 = ImageNow Server logs only function names.

2 = ImageNow Server logs all socket transactions.

3 = ImageNow Server logs all socket transactions including SERV_SYNC.

The default is 0.

debug.level.file

Specifies the level ImageNow Server uses to log errors for troubleshooting.

debug.level.file = 0 through 6

Typically, you want to set minimal logging unless you are debugging an issue. If you increase the logging, make sure that you set the logging level back down after you finish debugging. Failure to do so can greatly affect performance and hard disk space.

Note: You can specify unique values for specific users by placing the user name at the beginning of the string. For example, to set logging to 5 for user jsmith, create a string that states: `jsmith.debug.level.file = 5.`

0 = ImageNow Server does not log errors.

1 through 6 = ImageNow Server logs errors. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging with the most information.

The default is 0.

rolling.log.files.enabled

Optional. Enables you to create multiple log files of a size you specify. This setting is useful in large-scale environments where log files tend to be large.

rolling.log.file.enabled = TRUE or FALSE

The default is FALSE.

rolling.log.file.threshold

Optional. When rolling.log.file.enabled is set to TRUE, this setting specifies the size in MB of the log files.

rolling.log.file.threshold = any positive integer

The default is 100.

inserver.ini [Network] settings

This topic displays in a list the inserver.ini settings under the [Network] group.

inowd.port

Specifies the port number of ImageNow Server.

inowd.port = any valid port

The default is 6000.

***<instance name>* inowd.port**

Specifies the port number for a given instance of a server where <*instance name*> is the instance name of the server you want to set the port for. For example, if the instance name for the server is Secondary, this setting would be: `Secondary inowd.port`.

<*instance name*>.inowd.port = any value

There is no default for this setting.

inowd.ip.address

Specifies the IP address of ImageNow Server.

inowd.ip.address = any valid IP address

DEFAULT = ImageNow Server determines its own IP address.

The default is DEFAULT.

remote.hostname.useoverride

Specifies whether ImageNow Server uses the host name in the remote.hostname.override.<*host name*> setting to connect to an agent.

remote.hostname.useoverride = TRUE or FALSE

If ImageNow Server cannot resolve the host name of the agent and remote.hostname.useoverride is set to TRUE, ImageNow Server searches for a replacement host name in the llist of remote.hostname.override.<*hostname*> settings.

If ImageNow Server cannot resolve the hostname of the agent and remote.hostname.useoverride is set to FALSE, ImageNow Server generates an exception error

The default is FALSE.

remote.hostname.override.<*hostname*>

Specifies the host name of the connecting agent ImageNow Server uses when remote.hostname.useoverride is to TRUE.

remote.hostname.override.<*hostname*> = text strings

For example, if ImageNow Server cannot resolve the host name ComputerTwo and remote.hostname.override is set to TRUE, it searches the list of all remote.hostname.override.<*hostname*> settings. When it locates ComputerTwo, it replaces that host name with the set value.

If remote.hostname.useoverride is set to TRUE and no host name is provided for remote.hostname.override.<*host name*>, ImageNow Server generates an exception error.

There is no default for this setting.

inserver.ini [OpenID Connect Login Profiles] settings

This topic displays in a list the inserver.ini settings under the [OpenID Connect Login Profiles] group.

sso.openid.profiles

A comma separated list of OpenID Connect Authentication profiles. Profile names must solely contain alpha numeric characters.

For example, sso.openid.profiles=hylandexperience, defaultWithoutDiscovery.

sso.openid.profiles = any alphanumeric character

sso.openid.profile.<profileName>.client.id

A valid client identifier that is registered with the OpenID Provider.

For example, sso.openid.profile.hylandexperience.client.id=f282592c-e5e4-4b9f-a3fb-022b6c149f04

sso.openid.profile.<profileName>.client.id = any valid client identifier

sso.openid.profile.<profileName>.client.secret

The client secret.

Note:
OpenID client secrets in inserver.ini can be encrypted by running the inserver -encrypt-config command. This command should be ran each time a client secret is updated. Do not manually update the encrypted client secret settings.

For example, sso.openid.profile.hylandexperience.client.secret=HJmUFH3GGRvdrudKyZS0XhGv_Z45DuKhCUk0gJkdnU2

sso.openid.profile.<profileName>.client.secret = any valid string

sso.openid.profile.<profileName>.user.claim

The OpenID Connect user claim is used to map OpenID authenticated end-users to Perceptive Content users. The user claim values should map one-to-one to Perceptive Content usernames. The user claim should be specified as a JSON attribute path. This path should identify a claim in the JSON object returned from the UserInfo endpoint of the OpenID Provider. For more information about the syntax of JSON attribute paths, see Appendix D.

For example, sso.openid.profile.hylandexperience.user.claim=username.

sso.openid.profile.<profileName>.user.claim = any valid JSON attribute path

For more information, see JSON attribute paths.

sso.openid.profile.<profileName>.auto.discovery

Optional. Enable OpenID Connect Discovery. This will auto resolve the endpoints and trusted keys used for ID Token verification.

sso.openid.profile.<profileName>.auto.discovery = TRUE or FALSE

The default is TRUE.

sso.openid.profile.<profileName>.discovery.endpoint

Required if auto-discovery is enabled. The OpenID Provider's openid-configuration endpoint URL.

For example, sso.openid.profile.hylandexperience.discovery.endpoint=https://sample.onbase.com/IdentityProvider/.well-known/openid-configuration.

sso.openid.profile.<profileName>.discovery.endpoint = Any valid URL

sso.openid.profile.<profileName>.issuer.uri

Required if auto-discovery is disabled. The OpenID Provider Issuer URI to be used for validation. This setting is a case sensitive value and is ignored when auto-discovery is enabled.

For example, sso.openid.profile.hylandexperience.issuer.uri=https://sample.onbase.com/IdentityProvider

sso.openid.profile.<profileName>.issuer.uri = any valid uri

sso.openid.profile.<profileName>.token.endpoint

Required if auto-discovery is disabled. The OpenID Provider Token endpoint URL. This setting is ignored when auto-discovery is enabled.

For example, sso.openid.profile.hylandexperience.token.endpoint=https://sample.onbase.com/IdentityProvider/connect/token

sso.openid.profile.<profileName>.token.endpoint = any valid URL

sso.openid.profile.<profileName>.userinfo.endpoint

Required if auto-discovery is disabled. The OpenID Provider UserInfo endpoint URL. This setting is ignored when auto-discovery is enabled.

For example, sso.openid.profile.hylandexperience.userinfo.endpoint=https://sample.onbase.com/IdentityProvider/connect/userinfo.

sso.openid.profile.<profileName>.userinfo.endpoint = any valid URL

sso.openid.profile.<profileName>.discovery.refresh.interval.seconds

Optional. The period of time in seconds that trusted keys are cached from the Open ID Provider JSON web key endpoint. After this time period has elapsed, the cache will be refreshed.

sso.openid.profile.<profileName>.discovery.refresh.interval.seconds = any positive number

The default is 3600.

sso.openid.profile.<profileName>.discovery.minimum.refresh.interval.seconds

Optional. The minimum time period in seconds that must elapse between login profile refresh requests to the Open ID Provider's discovery endpoints. Discovery refresh requests may occur at any time due to a number of possible transient errors.

The default is 60.

sso.openid.profile.<profileName>.pkce.required

Optional. Specifies whether authentication requests require a Proof Key for Code Exchange (PKCE).

num.workers = any positive integer

sso.openid.profile.<profileName>.pkce.required = TRUE or FALSE

The default is TRUE.

sso.openid.profile.<profileName>.scope

Optional. A space separated list of registered scopes. If not specified, an ID Token for all explicitly allowed scopes for the OpenID client will be issued.

For example, sso.openid.profile.hylandexperience.scope=openid

sso.openid.profile.<profileName>.scope = any valid scope

sso.openid.profile.<profileName>.trusted.clients

Optional. A comma separated list of trusted clients. These will be used to validate the ID Token. The profile's client id will always be added as a trusted client.

For example, sso.openid.profile.hylandexperience.trusted.clients=f282592c-e5e4-4b9f-a3fb-022b6c149f04, d48d37b4-c6ac-43a3-9864-60b9bad5c683

sso.openid.profile.<profileName>.trusted.clients = any valid clients

sso.openid.profile.<profileName>.id.token.signed.response.alg

Optional. The token signing algorithm that was specified when registering the client with the OpenID Provider. Only ECDSA and RSA signing algorithms are supported. The default is RS256.

sso.openid.profile.<profileName>.id.token.signed.response.alg = any supported JSON Web Algorithm

The default is RS256.

sso.openid.profile.<profileName>.token.expiration.time.seconds

Optional. Defines the maximum number of seconds from when the ID Token has been issued to when it can be used. If not validated within the time period specified authentication will fail. This policy can be disabled by using a negative value.

sso.openid.profile.<profileName>.token.expiration.time.seconds = any number

The default is 600.

sso.openid.profile.<profileName>.max.age.allowed.skew.seconds

Optional. Additional amount of time in seconds to allow when validating the ID token max age against when the end user authentication occurred.

sso.openid.profile.<profileName>.max.age.allowed.skew.seconds = any positive number

The default is 30.

sso.openid.profile.<profileName>.proxy.url

Optional. Proxy URL that should be used for OpenID Provider HTTP requests.

sso.openid.profile.<profileName>.proxy.url = any valid URL

sso.openid.profile.<profileName>.tls.validate

Optional. Specifies whether to validate TLS certificates on requests made to the OpenID Provider. Must be set to TRUE in a production environment.

sso.openid.profile.<profileName>.tls.validate = TRUE or FALSE

The default is TRUE.

sso.openid.profile.<profileName>.request.timeout.seconds

Optional. Max time in seconds that an OpenID Connect HTTP request is allowed to take.

sso.openid.profile.<profileName>.request.timeout.seconds = any positive number

The default is 15.

inserver.ini [Remote] settings

This topic displays in a list the inserver.ini settings under the [Remote] group.

vsl.extended.operators.enabled

Specifies whether Perceptive Content adds the ends with and contains operators for search grids.

vsl.extended.operators.enable = TRUE or FALSE

TRUE = Ends with and contains appear in the search grid operators list.

FALSE = Ends with and contains do not appear in the search grid operators list.

The default is FALSE.

inserver.ini [Timing] settings

This topic displays in a list the inserver.ini settings under the [Timing] group.

timing.enabled

Specifies whether Client Performance is turned on.

timing.theshold.enabled = TRUE or FALSE

TRUE = Client Performance is enabled and uses the timing.threshold.percentage setting.

FALSE = Client Performance is disabled.

The default is FALSE.

timing.threshold.enabled

When timing.enabled is set to TRUE, this setting specifies if the timing.threshold.percentage setting will be used.

timing.threshold.enabled = TRUE or FALSE

timing.theshold.enabled = TRUE or FALSE

The default is FALSE.

timing.threshold.percentage

When timing.threshold.enabled is set to true, this setting specifies the threshold as a percentage. When the percentage of documents exceeds the specified threshold, the data is included in the report.

timing.threshold.percentage = any positive integer

For example, if timing.threshold.percentage is set to 10 and 10% of the documents exceed the threshold. the event is included in the performance report.

The default is 10.

timing.max.purge.size

Specifies the maximum number of records Client Performance deletes at one time.

timing.max.purge.size = any positive integer

The default is 1000.

timing.cleanup.period

Specifies the number of hours Client Performance waits after completing a purge to check for data to start another purge.

timing.cleanup.period = any positive integer

The default is 6.

timing.state.removal.period

Optional. Specifies, in hours, how often Client Performance searches ImageNow Server for expired reports. Client Performance moves expired reports to the database.

timing.state.removal.period = any positive integer

The default is 4.

timing.purge.delay

Specifies the number of seconds Client Performance waits to delete data when the total number of records to be deleted exceeds the max.purge.size setting.

time.purge.delay = any positive integer

The default is 60.

timing.category.viewer.enabled

Specifies whether Perceptive Content collects data based on a threshold you define for opening the document.

timing.category.viewer.enabled = TRUE or FALSE

The default is TRUE.

timing.category.viewer.report.threshold

Specifies the number of seconds you want to establish as the threshold for opening a document.

Any events that exceed the threshold are included in the Threshold Count column in the performance report.

timing.category.viewer.report.threshold = any positive integer

The default is 5.

timing.category.workflow.enabled

Specifies whether Perceptive Content collects data based on a threshold you define for routing an item forward.

timing.category.forms.enabled = TRUE or FALSE

The default is TRUE.

timing.category.workflow.report.threshold

Specifies the number of seconds you want to establish as the threshold for routing an item forward.

Any events that exceed the threshold are included in the Threshold Count column in the performance report.

timing.category.forms.report.threshold = any positive integer

The default is 5.

timing.category.forms.enabled

Specifies whether Perceptive Content collects data based on a threshold you define for opening a form.

timing.category.forms.enabled = TRUE or FALSE

The default is TRUE.

timing.category.forms.report.threshold

Specifies the number of seconds you want to establish as the threshold for opening a form.

Any events that exceed the threshold are included in the Threshold Count column of the performance report.

timing.category.forms.report.threshold = any positive integer

The default is 5.

timing.detail.purge.enabled

Enables periodic deletion of detailed performance data.

If timing.aggregation.enabled is set to TRUE, Perceptive Content condenses the detailed performance data after this number of hours instead of deleting it.

timing.detail.purge.enabled = TRUE or FALSE

The default is FALSE.

timing.detail.retention.period

Specifies the number of hours after which Perceptive Content deletes detailed performance data.

timing.detail.rentention.period = 0, or a positive integer that is a multiple of 24

The default is 0.

timing.aggregation.enabled

Enables retention of detailed performance data as condensed performance data.

timing.aggregation.enabled = TRUE or FALSE

If set to TRUE, Perceptive Content condenses the detailed performance data after the number of hours set for timing.detail.retention.period.

The default is FALSE.

timing.aggregate.purge.enabled

Enables periodic deletion of condensed performance data.

timing.aggregate.purge.enabled = TRUE or FALSE

The default is FALSE.

timing.aggregate.retention.period

Specifies the number of days after which Perceptive Content deletes condensed performance data.

timing.aggregate.retention.data = an integer between 0 and 9999

The default is 0.

inserver.ini [Views] settings

This topic displays in a list the inserver.ini settings under the [Views] group.

enable.folder.content.view.sorting

Specifies whether the folder content view is turned on.

enable.folder.content.view.sorting = TRUE or FALSE

TRUE = Folder content view results are sorted by the document type ordering specified within the corresponding folder type.

FALSE = Folder content view results are unsorted.

The default is TRUE.

inserverAlarm.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverAlarm.ini file.

Each setting offers two or more options, which are defined in the following groups along with a description. Use this as a guide when customizing the inserverAlarm.ini file.

[General]

remove.old.service

Specifies whether Perceptive Content Server removes old services.

remove.old.service = 1 or 0

1 = Perceptive Content Server removes services.

0 = Perceptive Content Server does not remove services.

The default is 0.

num.workers

Specifies the number of worker threads used when Alarm Agent starts.

num.workers = any positive integer

The default is 5.

[Email]

queue.email.link

Specifies the link type to send in queue alarm emails.

queue.email.link = 0 through 6

0 = Alarm Agent includes a Perceptive Content link.

1 = Not supported.

2 = Alarm Agent includes Perceptive Content link types.

3 = Alarm Agent includes a Perceptive Experience URL link.

4 = Alarm Agent includes Perceptive Content and Perceptive Experience URL links.

5 = Alarm Agent includes Perceptive Experience URL links.

6 = Alarm Agent includes Perceptive Contentand Perceptive Experience URL links.

The default is 0.

debug.level.file

Specifies the verboseness level Alarm Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you set it back down after you finish debugging. Failure to do so can slow performance and consume hard disk space.

debug.level.file = 0 through 6

0 = Alarm Agent does not log errors.

1 through 6 = Alarm Agent logs errors. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

The default is 0.

inserverBatch.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverBatch.ini file.

Each setting offers two or more options, which are defined in the following topics along with a description. Use these topics as a guide when customizing the inserverBatch.ini file

[General]

Changes to settings in the inserverBatch.ini file require a restart of the Perceptive Content Server and any affected agents unless noted otherwise.

pause.between.transactions

Specifies, in milliseconds, how long Batch Agent pauses between pages when processing a batch.

pause.between.transactions = any positive integer

The default is 100.

barcode.fail.to.queue.enabled

Specifies whether Batch Agent can fail a batch with an unverified barcode.

barcode.fail.to.queue.enabled = TRUE or FALSE

TRUE = Batch Agent can fail a batch with unverified barcodes.

FALSE = Batch Agent does not fail unverified barcodes.

The default is FALSE.

submit.to.content.server

Specifies whether Batch Agent submits imported files to Recognition Agent to provide bar code recognition. Recognition Agent requires a separate license.

submit.to.content.server = TRUE or FALSE

TRUE = Batch Agent submits imported files to Recognition Agent.

FALSE = Batch Agent does not submit imported files to Recognition Agent.

The default is FALSE.

remove.old.service

Specifies whether Batch Agent removes old services from the Services list. When you enable this setting and the path and name for services match, Batch Agent removes any existing service registrations.

remove.old.service = 1 or 0

1 = Batch Agent removes old services.

0 = Batch Agent does not remove old services.

The default is 0.

[Batch Logging]

debug.level.file

Specifies the level Batch Agent uses to log errors for troubleshooting.

Typically, you want to set minimal logging unless you are debugging an issue. If you increase the logging level, make sure you reduce the level after you finish debugging. Failure to do so can affect performance and hard disk space.

debug.level.file = 0 through 6

0 = Batch Agent does not log errors.

1 through 6 = Batch Agent logs errors. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, while 6 provides logging that offers the most information.

The default is 0.

[ReadSoft]

perform.readsoft.export

Specifies whether Batch Agent exports files to ReadSoft for optical character recognition.

perform.readsoft.export = TRUE or FALSE

TRUE = Batch Agentexports files to ReadSoft.

FALSE = Batch Agent does not export files to ReadSoft.

The default is FALSE.

export.mode

Specifies which pages to export to ReadSoft.

export.mode = 1 or 2

1 = Only first page.

2 = After every store page.

The default is 1.

selected.batches.only

Specifies whether to process selected batches based on criteria. You set the criteria with the selection.criteria setting.

selected.batches.only = TRUE or FALSE

TRUE = Batch Agent processes selected batches.

FALSE = Batch Agent processes all batches.

The default is FALSE.

selection.criteria

Specifies the criteria for batches, if the selected.batches.only setting is set to TRUE.

selection.criteria = creation.user

There is no default for this setting.

creation.user

Specifies the creation user when selection.criteria is set to creation.user.

creation.user= any valid user names separated by ^

There is no default for this setting.

file.name

Specifies the file name format of exported ReadSoft files.

file.name= any combination of <<drawer>>, <<field1>>, <<field2>>, <<field3>>, <<field4>>, <<field5>>, <<page_number>>, <<docid>>, and <<doctype>>

There is no default for this setting.

export.directory.<*n*>

Specifies the directory to which Batch Agent exports files for ReadSoft. You can specify up to five different directories subsequently numbered.

export.directory.<n>= any valid directory

There is no default for this setting.

failed.export.directory

Specifies the directory to which Batch Agent exports files that failed OCR by ReadSoft.

failed.export.directory = any valid directory

There is no default for this setting.

inserverEM.ini

The following topics provide definitions and sample data for the settings in the inserverEM.ini configuration file. Each topic displays the INI settings for the group that appears in its title, such as [General].

Each setting offers two or more options, which are defined in the following topics along with a description. Use these topics as a guide when customizing the inserverEM.ini file.

[General]

num.workers

Specifies the number of worker threads used when External Messaging Agent starts.

num.workers = any positive integer

The default is 5.

message.pulling.interval

Specifies how often, in seconds, the agent checks and downloads messages from the external message database.

message.pulling.interval = any positive integer

The default is 10.

max.message.per.type

Specifies the maximum number of processed messages to pull each time from the database for each message type.

max.message.per.type = any positive integer

The default is 100.

remove.old.service

Specifies whether External Messaging Agentremoves old services from the Services list. When you enable this setting and the path and name for services match, External Messaging Agentremoves any existing service registrations.

remove.old.service = 1 or 0

1 = External Messaging Agentremoves old services.

0 = External Messaging Agentdoes not remove old services.

The default is 0.

[Expire]

reset.expired.messages

Set to TRUE if there is the potential for multiple External Messaging Agents to work on the same set of records. This allows External Messaging Agent to release a set of records it is processing after the minutes.to.expire timer expires.

reset.expired.messages = TRUE or FALSE

The default is TRUE.

minutes.to.expire

If reset.expired.messages = TRUE, this specifies the number of minutes before External Messaging Agent releases a set of records that has finished processing.

minutes.to.expire = any positive integer

The default is 10.

[Logging]

debug.level.file

Specifies the level External Messaging Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you reset it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

debug.level.file = 0 through 6

0 = External Messaging Agent does not log errors

1 through 6 = External Messaging Agent logs errors. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

The default is 0.

[Purge]

purge.completed.messages

Specifies whether External Messaging Agentremoves messages after successful completion.

purge.completed.messages = TRUE or FALSE

TRUE = Messages with a MSG_STATUS of 3 and an END_TIME of *x* hours are purged after *x* hours have passed.

The default is TRUE.

hours.to.keep.completed.messages

If purge.completed.messages = TRUE, specifies the number of hours before External Messaging Agentpurges completed messages.

hours.to.keep.completed.messages = any positive integer

The default is 48.

purge.errored.messages

Specifies whether External Messaging Agentremoves messages that have been completed with an error. When set to TRUE, messages with an MSG_STATUS of 4 and an END_TIME of *x* hours ago are purged. The hours.to.keep.errored setting specifies the value of *x*.

purge.errored.messages = TRUE or FALSE

The default is TRUE.

hours.to.keep.errored.messages

If purge.completed.messages = TRUE, specifies the number of hours before External Messaging Agentpurges messages that completed with an error.

hours.to.keep.errored.messages = any positive integer

The default is 1200.

number.messages.to.purge

If purge.completed.messages = TRUE, specifies the number of hours before External Messaging Agentpurges messages that completed with an error.

hours.to.keep.errored.messages = any positive integer

The default is 500.

inserverFS.ini

The following topics provide definitions and sample data for the settings in the inserverFS.ini configuration file. Each topic displays the INI settings for the group that appears in its title, such as [General].

Each setting offers two or more options, which are defined in the following topics along with a description. Use these topics as a guide when customizing the inserverFS.ini file.

[General]

The num.transfer.workers, num.osm.replication.works, and max.osm.replication.retries settings previously in inserverFS.ini file now appear in the inserverOSM.ini file during an installation or upgrade. The setting values are not preserved during the transfer, and you must reapply the values.

batch.delete.size

Specifies the number of deleted documents and folders in a batch Perceptive Content deletes permanently at one time. You may need to decrease this value if the CPU is taking too long to remove a large batch of items.

batch.delete.size = any positive integer

The default is 500.

destruction.wait.time

Specifies the number of days a deleted document or folder remains in the recycle bin before it is permanently deleted. If you specify a value of 0, Perceptive Content deletes the document or folder as soon as it is sent to the recycle bin.

destruction.wait.time = any positive integer

The default is 0.

no.work.delay.max.seconds

Specifies how often, in seconds, File System Agent searches for new jobs after the queue is empty.

no.work.delay.max.seconds = 0 through 16

0 = File System Agent continuously checks for new jobs.

1 through 16 = File System Agent waits the specified number of seconds to check for new jobs.

The default is 16.

remove.old.service

Specifies whether ImageNow Server removes old services.

remove.old.service = 1 or 0

1 = ImageNow Server removes services.

0 = ImageNow Server does not remove services.

The default is 0.

inserverImp.ini

The following links provide definitions and sample data for the configuration settings for the different groups of the inserverImp.ini file.

- DOD Record Metadata Mapping
- DOD XML
- File Concatenation
- General
- Key Mapping
- Logging
- Mode COMBO
- Mode DATA CAPTURE
- Mode DOD Record
- Mode Filename

- Mode Index File
- Mode Keymapping
- Mode TIFF Text Combo
- OSM
- Remote
- Serial Number

[DOD Record Metadata Mapping]

field<1-5>

Specifies the mapping of Perceptive Contentrecord properties (associated with the record type) to organizational defined metadata in the <AdditionalInformation> section of the imported XML file.

field<*n*> = any valid XML path

There is no default for this setting.

custom.property<*n*>.name

custom.property<*n*>.value

Specifies the mapping of Perceptive Content custom properties (associated with the record type) to organizational defined metadata in the <AdditionalInformation> section of the imported XML file.

This setting can be set to any valid XML path.

There is no default for this setting.

custom.property<*n*>.namecustom.property<*n*>.value

custom.property<*n*>.name

custom.property<*n*>value

Specifies the mapping of Perceptive Content custom properties (associated with the record type) to organizational defined metadata in the <AdditionalInformation> section of the imported XML file.

This setting can be set to any valid XML path.

There is no default for this setting.

[Mode DOD_XML]

This topic displays in a list the inserverImp.ini settings under the [Mode DOD_XML] group.

xml.file.ext

Specifies that Import Agentshould import XML files that follow DoD 5015.02 STD requirements.

xml.file.ext = any valid XML file extension. Separate multiple extensions with commas.

The default is XML.

[File Concatenation]

This topic displays in a list the inserverImp.ini settings under the [File Concatenation] group.

loop

Specifies the number of times Import Agent checks the file before importing it to ensure that the file is complete.

loop = any positive integer

The default is 10.

[General]

This topic displays in a list the inserverImp.ini settings under the [General] group.

import.mode

Specifies the types of files that Import Agent imports and the method that Import Agent uses to gather document property values and assign them to the new documents.

import.mode = INDEX_FILE, COMBO, KEYMAPPING, TIFF_TEXT_COMBO, FILENAME, DATA_CAPTURE, DOD_RECORD, DOD_XML, CAPTURE_PROFILE

The default is INDEX_FILE.

import.directory.<*n*>

Specifies the directory that Import Agent monitors for import files. You can define an unlimited number of directories by creating new, subsequently named import.directory.<n> settings.

import.directory.<*n*> = any valid directory

The default is *$(IMAGENOWDIR)/import*.

poll.interval

Specifies how often, in seconds, the Import Agent searches for new import files.

Do not change this value without first consulting with Product Support.

poll.interval = any positive integer

The default is 1.

pause.between.transactions

Specifies, in milliseconds, how long Import Agent pauses between pages when processing a batch.

pause.between.transactions = any positive integer

The default is 100.

send.to.queue.<*n*>

Specifies the queue where Import Agent sends imported files. For each import.directory defined, create a subsequently named send.to.queue.<n> settings.

send.to.queue.<n> = any existing queue

There is no default for this setting.

delete.source.objects.after.import

Specifies whether Import Agent deletes the source file or moves it to a specified location after Import Agent imports it.

delete.source.objects.after.import = DELETE or MOVE

DELETE = Import Agent deletes the source file after import.

MOVE = Import Agent moves the file to the directory you specify for import.complete.directory.<*n*> after import.

If you set delete.source.objects.after.import to MOVE, you must set import.failed.directory.<*n*> and import.complete.directory.<*n*>.

The default is MOVE.

import.failed.directory.<*n*>

Specifies the directory where Import Agent stores source files after importing them. If you set delete.source. objects.after.import to MOVE, you must set import.complete.directory.<*n*>. For each import.directory defined, create a subsequently name import.failed.directory.<*n*>.

import.failed.directory.<*n*> = any valid directory

There is no default for this setting.

import.complete.directory.<*n*>

Specifies the directory where Import Agent stores source files after importing them. If you set delete.source. objects.after.import to MOVE, you must set import.complete.directory.<*n*>. For each import.directory defined, create a subsequently name import.failed.directory.<*n*>.

import.complete.directory.<*n*> = any valid directory

There is no default for this setting.

num.directory.workers

Specifies the number of worker threads that monitor the directory specified for import.directory.<n>.

num.directory.workers = any positive integer

The default is 1.

num.import.workers

Specifies the number of worker threads used to import files into Perceptive Content.

num.import.workers = any positive integer

The default is 1.

capture.profile

Specifies a capture profile for the directory Import Agent monitors for the import.directory.<n> setting. Use this setting when you set import.mode to CAPTURE_PROFILE.

There is no default for this setting.

file.encoding

Specifies the type of encoding Import Agent uses, based on UTF-8 or ANSI server types. If you set file.encoding to UTF-8, it is assumed that all files are UTF-8 compatible. If you set file.encoding to ANSI, ANSI files are allowed to run after you upgrade Perceptive Content Server to Unicode.

file.encoding = UTF-8 or ANSI

For Unicode servers, the default is UTF-8.

For ANSI build servers, the default is ANSI.

remove.old.service

Specifies whether Import Agent removes the service if it exists without the instance name.

remove.old.service = 1 or 0

1 = Import Agent removes old services.

0 = Import Agent does not remove old services.

The default is 0.

[Key Mapping]

This topic displays in a list the inserverImp.ini settings under the [Key Mapping] group.

doc.type

Specifies the document type value Import Agentassigns to the Type field.

doc.type = <any valid document type>, DEFAULT, <<date/time>>, <<index provided>>, <<search,<string parament>>>, <<SerialNumber>>, <<tiff_tag>>, <<undefined>>, <<uniqueID>>

The default is DEFAULT.

drawer

Specifies the value Import Agent assigns to the Drawer field.

drawer = <any valid drawer>, <<date/time>>, DEFAULT, <<index provided>>, <<search<string parameter>>>, <<SerialNumber>>, <<tiff_tag>>, <<undefined>>, <<uniqueID>>

The default is DEFAULT.

field<1-5>

Specifies the values Import Agent uses for field1, 2, 3, 4, and 5 and document properties.

field<1-5> = <any valid drawer>, <<date/time>>, DEFAULT, <<index provided>>, <<search<string parameter>>>, <<SerialNumber>>, <<tiff_tag>>, <<undefined>>, <<uniqueID>>

The default is DEFAULT.

inserverImp.ini [Logging] settings

This topic displays in a list the inserverImp.ini settings under the [Logging] group.

debug.level.file

Specifies the verboseness level Import Agent uses to log errors for troubleshooting.

debug.level.file = 0 through 6

0 = Import Agentdoes not log errors.

1 through 6 = Import Agentlogs errors. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, while 6 provides logging with the most information.

The default is 0.

socket.level.file

Specifies whether to log communication between ImageNow Server and Import Agent.

socket.level.file = 1 or 0

1 = Import Agent logs communication withImageNow Server.

0 = Import Agent does not log communication with ImageNow Server.

The default is 0.

[Mode COMBO]

This topic displays in a list the inserverImp.ini settings under the [Mode COMBO] group.

combined.inx.data.file.ext

Specifies the file extension Import Agentuses to find the property values that are contained in the first line of the file.

combined.inx.data.file.ext = any valid file extension. Separate multiple extensions with commas.

The default is CMX.

field.delim

Specifies the character Import Agent uses as the field delimiter in the index file.

field.delim = any character

The default is ^.

[Mode DATA_CAPTURE]

This topic displays in a list the inserverImp.ini settings under the [Mode DATA_CAPTURE] group.

extension.to.capture

Specifies the extension of the files to import when import.mode is set to DATA_CAPTURE.

extension.to.capture = any valid file extension. Separate multiple extensions with commas.

The default is TIFF.

bypass.qa

Specifies whether imported files bypass the BATCH QA process and move directly into the DataCapture process.

bypass.qa = TRUE or FALSE

TRUE = Imported files bypass the QA process.

FALSE = Imported files do not bypass the QA process.

The default is TRUE.

use.previous.keys.when.missing

Specifies which property values to assign if DataCaptureencounters a file from which it cannot extract values.

use.previous.key.when.missing = TRUE or FALSE

TRUE = DataCapture uses the property values from the previously processed document.

FALSE = DataCapture uses the default property values.

The default is FALSE.

capture.template.<*n*>

Specifies which template DataCapture uses to process imported files. Each directory DataCapture monitors can use a different template. For each import.directory defined, create a subsequently named capture.template.<*n*>.If you specify a directory as monitored but do not define a template for that directory, Import Agent stops processing files.

capture.template.<*n*> = any valid template.

There is no default for this setting.

split.multipage.tiffs

Specifies whether Import Agent splits multiple-page TIFF files into one file per page.

split.multpage.tiffs = TRUE or FALSE

TRUE = Import Agent splits multiple-page TIFF files.

FALSE = Import Agent does not split multi-page TIFF files.

The default is FALSE.

scan.user.name

Specifies an identifier that DataCapture requires and that optionally allows non-manager users to access DataCapture results in the batch grid.

scan.user.name = any valid user name

If you leave scan.user.name empty, the import fails.

There is no default for this setting.

[Mode DOD_RECORD]

This topic displays in a list the inserverImp.ini settings under the [Mode DOD_RECORD] group.

manifest.file.ext

Specifies the file extension Import Agent uses to identify the manifest file when import.mode is set to DOD_RECORD.

manifest.file.ext = any valid file extension such as MFT or TXT. Separate multiple extensions with commas.

The default is manifest.

dod.file.retry.attempts

Specifies how many times Import Agent attempts to import a record before considering the import failed.

dod.file.retry.attempts = any positive integer

The default is 1.

dod.file.status.report

Specifies how Import Agent reports the import status of DOD files.

dod.file.status.report = 0, 1, 2

0 = Import Agent does not generate a report.

1 = Import Agent generates a report for failed imports.

2 = Import Agent generates a report for successful and failed imports.

The default is 0.

file.plan.name

Specifies the file plan name that Import Agent uses when importing records to Perceptive Content from an external Records Management application (RMA).

file.plan.name = any defined Perceptive Content file plan

There is no default for this setting.

record.type.name

Specifies the record type name that Import Agent uses when importing records to Perceptive Content from an external Records Management application (RMA).

record.type.name = any defined Perceptive Content record type

There is no default for this setting.

record.folder.type.name

Specifies the record folder type name that Import Agent uses when importing records to Perceptive Content from an external Records Management application (RMA).

record.folder.type.name = any defined Perceptive Content record folder type

There is no default for this setting.

[Mode FILENAME]

This topic displays in a list the inserverImp.ini settings under the [Mode FILENAME] group.

image.file.ext

Specifies the file extension Import Agent uses for image files when import.mode is set to FILENAME.

image.file.ext = any valid file extension. Separate multiple extensions with commas.

The default is PDF.

file.name

Specifies the syntax Import Agent uses to gather values from the file name and assign them to document properties. In the [KEYMAPPING] group, you must enter <<index provided>> for any document properties you specify for file.name.

file.name = any combination of <<drawer>>, <<field1>>, <<field2>>, <<field3>>, <<field4>>, <<field5>>, <<doctype>>

There is no default for this setting.

field.delim

Specifies the character Import Agent uses as the field delimiter in the index file.

field.delim = any character

The default is ^.

split.multipage.tiffs

Specifies whether Import Agent splits multiple-page TIFF files into one file per page.

split.multpage.tiffs = TRUE or FALSE

TRUE = Import Agent splits multiple-page TIFF files.

FALSE = Import Agent does not split multi-page TIFF files.

The default is FALSE.

multi.doc.mode

Specifies whether each page of the imported file is a unique document in Perceptive Content.

multi.doc.mode = TRUE or FALSE

TRUE =Import Agent makes each page of the file a unique Perceptive Content document.

FALSE = Import Agent makes the entire file a single Perceptive Content document.

The default is FALSE.

[Mode INDEX_FILE]

This topic displays in a list the inserverImp.ini settings under the [Mode INDEX_FILE] group.

index.file.ext

Specifies the file extension Import Agentuses to identify the index file when import.mode is set to INDEX_FILE.

index.file.ext = any valid file extension such as INX or TXT. Separate multiple extensions with commas.

The default is INX.

field.delim

Specifies the character Import Agent uses as the field delimiter in the index file.

field.delim = any character

The default is ^.

index.file.status.report

Specifies how Import Agent reports the status of index files as a result of importing.

index.file.status.report = 0, 1, or 2

0 = Import Agent does not generate a report.

1 = Import Agent generates a report for failed imports.

2 = Import Agent generates a report for successful and failed imports.

The default is 0.

index.file.retry.attempts

Specifies how many times Import Agent attempts to import a file before considering it failed.

index.file.retry.attempts = any positive integer

The default is 1.

use.page.num

Specifies whether Import Agent uses page numbers to split files and gathers property values.

use.page.num = TRUE or FALSE

TRUE = Import Agent uses the page number to gather property values from the associated line in the index file. Import Agent splits multiple page TIFF files into one file per page and makes each page a unique document in Perceptive Content. If a line in the index file does not list a page number, Import Agent does not import the page.

FALSE = Import Agent does not use page numbers to split files and assign property values.

The default is 1.

split.multipage.tiffs

Specifies whether Import Agent splits multiple-page TIFF files into one file per page. If you set use.page.num to TRUE, Import Agent ignores this setting.

split.multiple.tiffs = TRUE or FALSE

TRUE = Import Agent splits multiple-page TIFF files.

FALSE = Import Agent does not split multi-page TIFF files.

The default is FALSE.

multi.doc.mode

Specifies whether each page of the imported file is a unique document in Perceptive Content. If you set use.page.num to TRUE, Import Agent ignores this setting.

multi.doc.mode = TRUE or FALSE

TRUE = Import Agent makes each page of the file a unique Perceptive Content document.

FALSE = Import Agent makes the entire file a single Perceptive Content document.

The default is FALSE.

[Mode KEYMAPPING]

image.file.ext

Specifies the file extension Import Agent uses for image files when import. mode is set to KEYMAPPING.

image.file.ext = any valid file extension. Separate multiple extensions with commas.

The default is TIFF.

split.multiple.tiffs

Specifies whether Import Agent splits multiple-page TIFF files into one file per page.

split.multpage.tiffs = TRUE or FALSE

TRUE = Import Agent splits multiple-page TIFF files.

FALSE = Import Agent does not split multi-page TIFF files.

The default is FALSE.

multi.doc.mode

Specifies whether each page of the imported file is a unique document in Perceptive Content.

multi.doc.mode = TRUE or FALSE

TRUE =Import Agent makes each page of the file a unique Perceptive Content document.

FALSE = Import Agent makes the entire file a single Perceptive Content document.

The default is FALSE.

[Mode TIFF_TEXT_COMBO]

This topic displays in a list the inserverImp.ini settings under the [Mode TIFF_TEXT_COMBO] group.

index.file.ext

Specifies whether the file extension Import Agent uses to identify the index file when import.mode is set to TIFF_TEXT_COMBO.

index.file.ext = any valid file extension. Separate multiple extensions with commas.

The default is TXT.

image.file.ext

Specifies the file extension Import Agent uses for image files.

image.file.ext = any valid file extension. Separate multiple extensions with commas.

The default is TIFF.

multi.doc.mode

Specifies whether each page of the imported file is a unique document in Perceptive Content.

multi.doc.mode = TRUE or FALSE

TRUE =Import Agent makes each page of the file a unique Perceptive Content document.

FALSE = Import Agent makes the entire file a single Perceptive Content document.

The default is FALSE.

subsequent.image.use.first.txt

Specifies whether subsequent images in an import use the same index file.

subsequent.image.use.first.txt = TRUE or FALSE

The default is FALSE.

inserverINI.ini [OSM] settings

This topic displays in a list the inserverImp.ini settings under the [OSM] group.

bypass.write.cache

Specifies whether Import Agent writes files directly to the main OSM set when OSM caching is enabled.

bypass.write.cache = TRUE or FALSE

TRUE = Import Agent writes new files to the main OSM set.

FALSE = Import Agent writes new files to the cache OSM set. If a cache OSM is not available, Import Agent writes new files to the main OSM set.

The default is TRUE.

inserverImp.ini [Remote] settings

This topic displays in a list the inserverImp.ini settings under the [Remote] settings

remoted

Specifies whether you installed Import Agent on a different computer than ImageNow Server.

remoted = TRUE or FALSE

TRUE = Import Agent and ImageNow Server are on different computers.

FALSE = Import Agent and ImageNow Server are on the same computer.

The default is FALSE.

heartbeat.interval

Specifies how many seconds Import Agent waits for successful login before terminating the connection.

heartbeat.interval = any positive integer

The default is FALSE.

socket.login.timeout

Specifies how often, in seconds, Import Agent verifies its connection to ImageNow Server.

Do not change this value without first consulting with Perceptive Software Product Support.

socket.login.timeout = any positive integer

The default is 60.

socket.default.timeout

Specifies how many seconds Import Agent waits for APIs.

To override this setting for an individual ImageNow Client, add this setting to the Remote group in imagenow.ini and restart the client.

Do not change this setting without first consulting with Perceptive Software Product Support.

socket.default.timeout = any positive integer

The default is 60.

server.ip.port

Specifies the IP address of ImageNow Server. You can supply multiple IP addresses with a semicolon delimited string. Import Agent attempts to connect to the IP addresses in the order listed until it establishes a successful connection.

server.ip.address = any valid IP address. Separate multiple IP addresses with semicolons.

There is no default for this setting.

server.ip.port

Specifies the port number of ImageNow Server.

server.ip.port = any valid port

There is no default for this setting.

force.server.validation

Specifies whether Import Agent forces the server to validate the user ID and password.

Do not change this value without first consulting with Perceptive Software Product Support.

force.server.validation = 1 or 0

1 = Import Agent forces the server to validate the user ID and password.

0 = Import Agent does not force the server to validate user ID and password

The default is 0.

reconnect.interval

Specifies how long, in seconds, Import Agent will try to reconnect to ImageNow Server after it loses connection.

Do not change this setting without first consulting with Perceptive Software Product Support.

reconnect.interval = any positive integer

The default is 60.

inserverImp.ini [Serial Number] settings

This topic displays in a list the inserverImp.ini settings under the [Serial Number] group.

serial.number.format

Specifies the serial number format Import Agent generates and assigns to each job.

serial.number.format = %d, Text<%d>, <%number of digitsd>, Text<%number of digitsd>, <%0number of digitsd>, Text <%0number of digitsd>

There is no default for this setting.

serial.number.startvalue

Specifies the start value of the serial number.

serial.number.startvalue = any single-digit positive integer

There is no default for this setting.

inserverJob

The following table provides definitions and sample data for the settings in the inserverJob.ini configuration file. This table displays the INI settings under group headings in brackets, such as [Timers], in the order the groups appear in the INI file. Each setting offers two or more options, which are defined in the table below along with a description of each setting and its options. Use this table as a guide when customizing the file.

General

Setting	Default	Description
mq.cleanup.messages.max	25000	Specifies the number of IN_MESSAGE table records Job Agent deletes in a single SQL transaction.
mq.publication.messages.per.worker.max	5000	Specifies the maximum number of messages for which each MQ publication worker threads is responsible. num.workers.mq.publication times (x) mq.pulbication.messages.per.worker.max equals (=) total batch size.
num.workers.mq.publication	1	Specifies the number of workers you need to create to handle MQ publication work.

Timers

Setting	Default	Description
auto.mq.publication.interval.seconds	300	Specifies the number of seconds Job Agent waits

Setting	Default	Description
		between checking for MQ publication work items.
auto.mq.cleanup.interval.seconds	1800	Specifies the number of seconds Job Agent waits between checking for MQ cleanup work items. Changing this value affects the size of the IN_Message table.
auto.suspend.timeout	1200	Specifies the number of seconds Job Agent allows a job to process before suspending it. You can use any positive integer.
auto.destroy.tiemout	1	Specifies the number of hours Job Agent retains a completed job before deleting it. You can use any positive integer.
auto.suspend.interval	1800	Specifies the number of seconds Job Agent waits to start an automatic suspension upon completion of the previous automatic suspension. You can use any positive integer.
auto.resume.interval	600	Specifies the number of seconds Job Agent waits to resume processing jobs after a suspension. You can use any positive integer.
auto.destroy.interval	1800	Specifies the number of seconds Job Agent waits to start an automatic destroy upon completion of the previous automatic destroy. You can use any positive integer.

Logging

Setting	Default	Description
debug.level.file	0	Specifies the level Job Agent uses to log errors for troubleshooting. Typically, you want to set minimal logging unless you are debugging an issue. If you increase the logging, make sure that you set the logging level back down after you finish debugging. Failure to do so can greatly affect performance and hard disk space. Level 0 means that logging is off. Levels 1 through 6 means that logging is on. The higher the number, the more verbose logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information. Tip You can specify unique values for specific users by placing the user name at the beginning of the string. For example, to set logging to 5 for user jsmith, create a string that states: jsmith.debug.level.file = 5.

inserverMonitor.ini [Defaults] settings

This topic displays the inserverMonitor.ini settings under [Defaults].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

defaults.time

Specifies the time of day, based on a 24-hour schedule, that Monitor Agent monitors the even identified

in the Processes group.

defaults.time = any time based on a 24-hour schedule

The default is 20:00.

defaults.day

Specifies the day Monitor Agent monitors the event identified in the Processes group.

defaults.day = EVERYDAY, MONDAY, TUESDAY, WEDNESDAY, THRUSDAY, FRIDAY, SATURDAY, SUNDAY

The default is EVERYDAY.

defaults.dumpdirectory

Specifies the directory Monitor Agent watches for dumps.

defaults.dumpdirectory = any valid directory

The default is $(IMAGENOWDIR)\bin.

defaults.maxattempts

Specifies the maximum number of times Monitor Agent attempts to restart the PAS before identifying it as failed.

defaults.maxattempts = any positive integer

The default is 3.

defaults.archivefiletypes

Specifies the file types Monitor Agent archives.

defaults.archivefiletypes = any file extension

The default is log.

defaults.archivewhichfiles

Specifies which files Monitor Agent archives based on creation date.

defaults.archivewhichfiles = AllLogs, AllBeforeToday

AllLogs is all the logs that are recorded.

AllBeforeToday is all logs recorded before the current date.

The default is AllBeforeToday.

defaults.archivesearchsubdirectories

Specifies whether Monitor Agent searches all sub-directories for more files to archive.

defaults.archivesearchsubdirectories = TRUE, FALSE

TRUE = Monitor Agent searches all sub-directories

FALSE = Monitor Agent does not search sub-directories

The default is TRUE.

defaults.archivedirectory

Specifies the directory Monitor Agent uses to store logs.

defaults.archivedirectory = any valid directory

The default is $(IMAGENOWDIR6)\log

defaults.ignorerequeststrings

Specifies whether to allow actions and events to run on processes that contain strings such as -start , that are run as temporary processes that just query some data or start the actual service.

defaults.ignorerequeststrings = TRUE, FALSE

The default is TRUE.

inserverMonitor.ini [Defines] settings

This topic displays the inserverMonitor.ini settings under [Defines].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

[defined_process]

Specifies the unique name for each process Monitor Agent monitors.

[defined_process] = any unique string

There is no default.

inserverMonitor.ini [EventLog] settings

This topic displays the inserverMonitor.ini settings under [EventLog].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

eventlog.enable

Specifies whether to store information to an external file about events, actions, and status of (PAS) Monitor Agent monitors.

eventlog.enable = TRUE or FALSE

The default is TRUE.

eventlog.outputtiming

If eventlog.enable is set to TRUE, this setting specifies how often, in hours, Monitor Agent logs information to the external file.

eventlog.outputtiming = any positive integer

The default is 6.

inserverMonitor.ini [Logging] settings

This topic displays the inserverMonitor.ini settings under [Logging].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

debug.level.file

Specifies the level Notification Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you rest it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal logging

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

inserverMonitor.ini [Polling] settings

This topic displays the inserverMonitor.ini settings under [Polling].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

polling.interval

Specifies how often, in seconds, Monitor Agent searches for new actions and events.

Note: Do not change this value without first consulting Perceptive Software Product Support.

polling.inteval = any positive integer

The default is 3.

inserverMonitor.ini [Processes] settings

This topic displays the inserverMonitor.ini settings under [Processes].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

[process].event[n].[setting]

Specifies settings for each event that override the threshold values specified in the Defaults group, or specifies more information for each event to use.

These settings are optional.

[process].event[n].[setting] = Time, Day

TimeOfDay setting descriptions

- Time = The time based on 24 hours when the event occurs
- Day = Day of the week the event occurs

There is no default.

[process].event[n].action[n]

Specifies the action Monitor Agent performs when each specific event occurs. Each action for each event must include a unique positive integer.

[process].event[n].action[n] = RestartProcess, Archive

RestartProcess = Monitor Agent restarts the process in response to the event.

Archive = Monitor Agent archives files in response to the event.

There is no default.

[process].event[n].action[n].[setting]

Specifies the setting name and value related to the actions you specified for [process].event[n].action[n] and overrides the global default values or specifies more information for each action to use.

[process].event[n].action[n].[setting] = MaxAttempts, ArchiveWhichFiles, ArchiveDirectory, ArchiveFileType, ArchiveSearchSubDirectories

MaxAttempts = Maximum number of unsuccessful attempts in a row before Monitor Agent considers the action failed.

ArchiveWhichFiles = Files Monitor Agent archives based on creation date, All or AllBeforeToday.

ArchiveDirectory = The directory from which Monitor Agent archives files.

ArchiveFileType = Type of files Monitor Agent archives

ArchiveSearchSubDirectories = Whether Monitor Agent searches sub-directories for more files to archive.

There is no default.

[process].event[n].action[n].failedaction[n]

Specifies an alternative action Monitor Agent performs if action[n] fails.

[process].event[n].action[n].failedaction[n] = RestartProcess, Archive

Refer to [process].event[n].action[n] for description of the options.

There is no default.

[process].event[n].action[n].failedaction[n].[setting]

Specifies settings for failedaction[n].

[process].event[n].action[n].failedaction[n] = MaxAttempts, ArchiveWhichFiles, ArchiveDirectory, ArchiveFileType, ArchiveSearchSubDirectories

Refer to [process].event[n].action[n].[setting] for description of the options.

There is no default.

inserverMonitor.ini [Profiles] settings

This topic displays in a table the inserverMonitor.ini settings under [Profiles].

Use the following sections as a guide when customizing the inserverMonitor.ini file.

profile[n].event[n]

Specifies unique profiles that Monitor Agent uses to perform specific actions in response to events. Profiles are a simplified approach to preform the same actions across multiple processes.

profile[n].event[n] = AbnormalTermination, TimeOfDay, DumpWatch

There is no default.

profile[n].event[n].action[n]

When used in conjunction with profile[n].event[n], this setting specifies the action to perform if the specified event occurs.

profile[n].event[n].action[n] = RestartProcess, Archive

There is no default.

profile[n].event[n].action[n].failedaction[n]

When used in conjunction with profile[n].event[n], this setting specifies the action to perform if the specified event occurs.

profile[n].event[n].action[n].failedaction[n] = RestartProcess, Archive

There is no default.

profile[n].event[n].action[n].[setting_name]

When used in conjunction with profile[n].event[n], this setting specifies the setting name and value related to the action.

profile[n].event[n].action[n].[setting_name] = MaxAttempts, ArchiveWhichFiles, ArchiveDirectory, ArchiveFileType, ArchiveSearchSubDirectories

Refer to [process].event[n].action[n].[setting] for descriptions of the options.

There is no default.

profile[n].event[n].action[n].failedaction[n].[setting_name]

When used in conjunction with profile[n].event[n], this setting specifies the setting name and value related to the action.

profile[n].event[n].action[n].failedaction[n].[setting_name] = MaxAttempts, ArchiveWhichFiles, ArchiveDirectory, ArchiveFileType, ArchiveSearchSubDirectories

Refer to [process].event[n].action[n].[setting] for descriptions of the options.

There is no default.

[process].event[n]

Specifies the program or server Monitor Agent monitors for specific events.

Each event for each process must include a unique positive integer, such as event1 and event2.

[process].event[n] = AbnormalTermination, TimeOfDay, DumpWatch

AbnormalTermination = When PAS stops unexpectedly.

TimeOfDay = When a certain time of day or time of week is passed.

DumpWatch = Watches for dump files created by crashing agents.

There is no default.

inserverNotification.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverNotification.ini file.

Each setting offers two or more options, which are defined in the following groups along with a description. Use this as a guide when customizing the inserverNotification.ini file.

[General]

refresh.settings.interval.minutes

Specifies how often, in minutes, Notification Agent waits between updates.

refresh.settings.interval.minutes = any positive integer

The default is 60.

remove.old.service

Specifies whether ImageNow Server removes old services.

remove.old.service = 1 or 0

1 = ImageNow Server removes services.

0 = ImageNow Server does not remove services.

The default is 0.

[Email]

smtp.server

Specifies the SMTP server Notification Agent uses for email notifications.

smtp.server = any valid IP address or server name of an SMTP server

The default is empty.

smtp.server.port

Specifies the email server port.

smtp.server.port = any valid port

The default is empty.

smtp.from

Specifies the email address to use as the from email address in notification emails sent with this agent.

Note: A reply email address is required.

smtp.from = any email address.

The default is empty.

[Logging]

debug.level.file

Specifies the level Notification Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you rest it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal logging

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

[Workers]

num.workers

Specifies the number of worker threads used to preform background processing.

num.workers = any positive integer

The default is 1.

inserverOSM.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverOSM.ini file.

Each setting offers two or more options, which are defined in the following groups along with a description. Use this as a guide when customizing the inserverOSM.ini file.

[General]

num.transfer.workers

Specifies the number of worker threads for transfer job processing.

num.transfer.workers = any positive integer

The default is 1.

num.osm.replication.workers

Specifies the number of worker threads to process OSM cache replication jobs (asynchronous cache writes).

num.osm.replication.workers = any positive integer

The default is 2.

num.osm.replication.retries

Specifies the total number of allowed attempts to replicate a cached item to the primary device.

num.osm.replication.retries = any positive integer

The default is 3.

num.osm.background.workers

Specifies the number of worker threads to use to process background OSM tasks, such as cleaning up deleted OSM objects.

num.osm.background.workers = any positive integer

The default is 5.

osm.cleanup.interval.seconds

Specifies the time, in seconds, to wait between performing object cleanups on OSM trees.

osm.cleanup.interval.seconds = any positive integer

The default is 30.

max.osm.concurrent.leases

Specifies the maximum number of OSM background-work item types allowed in memory at one time. This is initially set to a low value to balance the workload between multiple OSM agents, but it can be increased for higher throughput.

max.osm.concurrent.leases = any positive integer

The default is 1.

remove.old.service

Specifies whether ImageNow Server removes old services.

remove.old.service = 1 or 0

0 = ImageNow Server removes services.

1 = ImageNow does not remove services.

The default is 0.

osm.phsob.validation.batch.size

Specifies the number of records to process in a single batch.

osm.phsob.validation.batch.size = any positive integer

The default is 10000.

osm.work.wait.interval.milliseconds

Specifies the artificial throttle to the number of records that the system processes.

osm.work.wait.interval.milliseconds = any positive integer

The default is 0.

[Logging]

debug.level.file

Specifies the level OSM Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you reset it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal logging

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

[Verification]

background.validation.enabled

Enables validation of stored objects. This process checks the integrity of files stored by Perceptive Content and can be controlled through the other settings in this section. Run the intool validate-osm-report command to review results of this process.

background.validation.enabled = TRUE or FALSE

The default is FALSE.

Note: When this setting is set to TRUE, the max.osm.concurrent.leases setting should be set to at least one more than the number of OSM trees in your database. For example, if there are four OSM trees, the max.osm.concurrent.leases setting should be set to five or more.

min.verify.interval.weeks

Specifies the minimum amount of time, in weeks, between the revalidation of a phsob.

min.verify.interval.weeks = any positive integer less than the value of max.creation.age.weeks

The default is 52.

max.creation.age.weeks

Specifies the age, in weeks, of the oldest phsobs to validate.

Specifying 0 results in the verification of all phsobs.

max.creation.age.weeks = any integer 0 or greater.

The default is 0.

analyze.pre70.phsobs.enabled

Enables validation of phsobs added prior to version 7.0.

analyze.pre70.phsobs.enabled = TRUE or FALSE

TRUE = Enables the verification of phsobs added to the system prior to version 7.0.

FALSE = Verification is not performed on the phsobs added to the system prior to version 7.0.

The default is FALSE.

inserverRetention.ini [Assign] settings

This topic displays the inserverRetention.ini settings under [Assign].

Use the following sections as a guide when customizing the inserverRetention.ini file.

group.size

Specifies the number of items this agent assigns to a policy at one time.

group.size = any positive integer

The default is 100.

inserverRetention.ini [Cutoff] settings

This topic displays the inserverRetention.ini settings under [Cutoff].

Use the following sections as a guide when customizing the inserverRetention.ini file.

delay.between.cutoff

Specifies the interval, in seconds, the agent runs the cutoff job.

delay.between.cutoff = 60 through 86400

The default is 600.

max.items.to.cutoff

Specifies the maximum number of operations that occur when the agent runs the cutoff job.

Each file plan contains its own cutoff job.

max.items.to.cutoff = 100 through 10000

The default is 2000.

Note: If the number of items to return number set in the odbc.grid.max.fetch.count setting is lower than the number set in the max.items.to.cutoff setting, the odbc.grid.max.fetch.count setting takes precedence and fewer items are returned. For example, if the odbc.grid.max.fetch.count setting is 2000, and the max.items.to.cutoff setting is 5000, 2000 items are returned.

inserverRetention.ini [Deletion] settings

This topic displays the inserverRetention.ini settings under [Deletion].

Use the following sections as a guide when customizing the inserverRetention.ini file.

delete.accession.sets.hours

Specifies, in hours, the time this agent waits to delete accession sets.

delete.accession.sets.hours = any positive integer

The default is 168.

delete.hold.sets.hours

Specifies, in hours, the time this agent waits to delete hold sets.

delete.hold.sets.hours = any positive integer

The default is 168.

delete.offline.transfer.sets.hours

Specifies, in hours, the time this agent waits to delete offline transfer sets.

delete.offline.transfer.sets.hours = any positive integer

The default is 168.

delete.destruction.sets.hours

Specifies, in hours, the time this agent waits to delete destruction sets.

delete.destruction.sets.hours = any positive integer

The default is 168.

delete.offline.move.sets.hours

Specifies, in hours, the time this agent waits to delete offline move sets.

delete.offline.move.sets.hours = any positive integer

The default is 168.

delete.offline.copy.sets.hours

Specifies, in hours, the time this agent waits to delete offline copy sets.

delete.offline.copy.sets.hours = any positive integer

The default is 168.

inserverRetention.ini [Event Hold] settings

This topic displays the inserverRetention.ini settings under [Event Hold].

Use the following sections as a guide when customizing the inserverRetention.ini file.

delay.between.work

Specifies, in seconds, how often Retention Agent waits between searches for modified items.

delay.between.work = 60 - 86400

The default is 600.

max.items.to.route

Specifies the maximum number of modified items the Retention Agent can route out of the hold queue at one time.

max.items.to.route = 1- 50000

The default is 200.

inserverRetention.ini [General] settings

This topic displays the inserverRetention.ini settings under [General].

Use the following sections as a guide when customizing the inserverRetention.ini file.

default.minimum.delay

This setting currently is not supported.

num.workers

Specifies the number of worker threads used to perform background processing.

num.workers = any positive integer

The default is 1.

num.policy.apply.workers

Specifies the number of worker threads Retention Agent uses to perform policy application work.

num.workers = any positive integer

The default is 1.

work.timeout.seconds

Specifies, for active-active installations, the amount of seconds the retention agent may use to process a task before a second agent takes the task.

work.timeout.seconds = any positive integer from 30 to 10000

The default is 180.

remove.old.service

Allows you to remove old services when you upgrade your system.

remove.old.service = 1 or 0

0 = off

1 = on

The default is 0.

inserverRetention.ini [Logging] settings

This topic displays the inserverRetention.ini settings under [Logging].

Use the following sections as a guide when customizing the inserverRetention.ini file.

debug.level.file

Specifies the level Retention Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you rest it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal debugging information

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

inserverRetention.ini [Notification] settings

This topic displays the inserverRetention.ini settings under [Notification].

Use the following sections as a guide when customizing the inserverRetention.ini file.

notify.frequency

Specifies the frequency with which this agent batches and sends email notifications for policies.

notify.frequency = Daily, Weekly, Monthly, Yearly

Daily = The agent sends email notifications once per day.

Weekly = The agent sends email notifications one day per week.

Monthly = The agent sends email notifications one day per month.

Yearly = The agent sends email notifications one day per year.

The default is Weekly.

notify.weekly.day

Specifies the day of each week this agent batches and sends notifications.

This setting is applicable only when you enter Weekly for the notify.frequency setting.

notify.weekly.day = Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

The default is Monday.

notify.monthly.day

Specifies the day of each week this agent batches and sends notifications.

This setting is applicable only when you enter Monthly for the notify.frequency setting.

notify.monthly.day = 1 through 31, Last

The default is 1.

notify.yearly.month

Specifies the name of the month this agent batches and sends notifications.

This setting is applicable only when you enter Yearly for the notify.frequency setting.

notify.yearly.month = any valid month

The default is January.

notify.yearly.day

Specifies the day of the month this agent batches and sends notifications.

This setting is applicable only when you enter Yearly for the notify.frequency setting.

notify.yearly.day = 1 through 31, Last

The default is 1.

due.for.review.group.size

Specifies the maximum number of items that are due for review.

due.for.review.group.size = 1 through 1000

The default is 100.

due.for.review.interval.hours

Specifies the interval, in hours, this agent checks for items due for review.

due.for.review.interval.hours = 1 through 8760

The default is 24.

inserverRetention.ini [PolicyApplyScheduling] settings

This topic displays the inserverRetention.ini settings under [PolicyApplyScheduling].

Use the following sections as a guide when customizing the inserverRetention.ini file.

policy.apply.schedule.mode

Specifies if policy scheduling is on or off. This allows an administrator to set the Retention Agent to run jobs during certain hours of the day, at a specified interval using the settings below.

retention.schedule.mode = TRUE, FALSE

TRUE = Policy scheduling is on.

FALSE = Policy scheduling is off..

The default is FALSE.

policy.apply.schedule.start

Specifies, in hours, when Retention Agent can start removing items associated with destruction retention policies.

retention.schedule.mode = 0 - 23

The default is 22.

Note: The policy.apply.schedule.start mode setting must be set to TRUE for this setting to work.

policy.apply.schedule.duration

Specifies, in hours, the amount of time Retention Agent can take to remove items associated with destruction retention policies.

retention.schedule.mode = 1- 24

The default is 8.

Note: The policy.apply.schedule.start mode setting must be set to TRUE for this setting to work.

policy.apply.schedule.delay

Specifies, in seconds, how often Retention Agent waits to start removing items associated with destruction retention policies.

retention.schedule.mode = 1- 84600

The default is 1.

Note: The policy.apply.schedule.start mode setting must be set to TRUE for this setting to work.

inserverRetention.ini [Remove] settings

This topic displays the inserverRetention.ini settings under [Remove].

Use the following sections as a guide when customizing the inserverRetention.ini file.

group.size

Specifies the number of items this agent removes from a policy at one time when a document type is removed.

group.size = any positive integer

The default is 100.

group.size

Specifies the number of items this agent can route back at one time when an item is released from hold.

group.size = any positive integer

The default is 200.

inserverTask.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverTask.ini file.

Each setting offers two or more options, which are defined in the following groups along with a description. Use this as a guide when customizing the inserverTask.ini file.

[General]

refresh.settings.interval.minutes

Specifies, in minutes, the time this agent waits to refresh all of the settings in this file.

refresh.settings.interval.minutes = any positive integer

The default is 60.

remove.old.service

Specifies whether ImageNow Server removes old services.

remove.old.service = 1 or 0

1 = ImageNow Server does not remove services.

0 = ImageNow Server removes services.

The default is 0.

[Deletion]

delete.tasks.assigned.days

Specifies, in days, the age of assigned tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.assigned.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.returned.days

Specifies, in days, the age of returned tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.returned.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.complete.pending.review.days

Specifies, in days, the age of complete pending tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.complete.pending.review.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.complete.days

Specifies, in days, the age of complete tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.complete.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.cancelled.days

Specifies, in days, the age of canceled tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.cancelled.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.invalid.days

Specifies, in days, the age of invalid tasks the Task Agent deletes. Age calculation begins when a task enters the designated state. In addition to the state, the modification date is also a consideration when deleting tasks.

The Task Agent deletes items in this state only when the modification date is older than the number of days specified in this setting.

delete.tasks.invalid.days = any positive integer

The default is -1.

-1 = Tasks in this state are not deleted.

delete.tasks.job.interval.minutes

Specifies, in minutes, how long the Task Agent waits between delete jobs. Tasks are deleted in batches.

delete.tasks.job.interval.minutes = any positive integer

The default is 5.

[Logging]

debug.level.file

Specifies the level Task Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you reset it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal logging

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

[Workload]

delete.work.load

Specifies the number of tasks to delete in a batch.

delete.work.load = 20 - 250

The default is 20.

inserverWorkflow.ini

The following sections provide definitions and sample data for the configuration settings for the different groups of the inserverWorkflow.ini file.

Each setting offers two or more options, which are defined in the following groups along with a description. Use this as a guide when customizing the inserverWorkflow.ini file.

[General]

connect.uri

Specifies the URI of the Perceptive Connect Runtime instance for integration with Connect ASQs.

connect.timeout

Specifies the duration, in seconds, the system waits before a call to the Perceptive Connect Runtime times out and the workflow item is routed to the failure queue.

The default is 30.

num.workers

Specifies the number of worker threads used to perform background processing.

num.workers = any positive integer

The default is 5.

refresh.queue.interval.seconds

Specifies how often, in seconds, Workflow Agent refreshes queue information, such as inbound and within queue actions, route recall, and archival settings.

refresh.queue.interval.seconds = any positive integer

The default is 600.

refresh.queue.attendee.interval.minutes

Specifies the number of minutes Workflow Agent waits between updates to the attendee count for all queues.

refresh.queue.attendee.interval.minutes = any positive integer

The default is 10.

num.crossnode.cache.workers

Specifies the number of worker threads Workflow Agent dedicates to cross-node cache synchronization.

num.crossnode.cache.workers = any positive integer

The default is 2.

remove.old.service

Allows you to remove old services when you upgrade your system.

remove.old.service = 1 or 0

0 = off

1 = on

The default is 0.

[Logging]

debug.level.file

Specifies the level Workflow Agent uses to log errors for troubleshooting.

Typically, you want minimal logging unless you are debugging an issue. If you increase the logging level, make sure that you reset it after you finish debugging. Failure to do so can slow performance and consume hard disk space.

0 = minimal logging

1 through 6 = logging is on. The higher the number, the more verbose the logging. For example, 1 offers minimal logging, whereas 6 offers logging that offers the most information.

debug.level.file = 0 through 6

The default is 0.

[Workload]

workload.preference

Specifies a preferential order an instance of Workflow Agent uses to process items. An instance setting takes precedence over the global setting.

workload.preference = All, Workflow, Retention

All= The agent processes work in the order it is received.

Workflow = The agent processes workflow queue items before any other work.

Retention = The agent processes retention policy items before any other work. When `workload.preference` is set to this value the system still respects the `retention.schedule.mode`, `retention.schedule.start`, and `retention.schedule.duration` settings.

The default is All.

Note: In an active/active environment where the INI file is shared, the workload.preference setting can be set for a specific instance by prefacing the setting with the instance name using the format `<instance name>.workload.preference=<setting>`.

retention.schedule.mode

Places a time restriction, in hours, when the agent can process retention policy work.

Note: This setting does not affect workflow processing.

Note: The retention.removal.schedule setting is ignored when this setting is enabled.

retention.schedule.mode = Off, Expensive, All

Off = Retention processing runs all of the time

Expensive = The agent processes aging, policy events, and deletion only during specified hours.

All = The agent runs retention policy work only during specified hours.

The default is off.

retention.schedule.start

Specifies the hour the agent can start processing retention policies.

Note: The system does not recognize minute or second formatting.

retention.schedule.start = 0 - 23

The default is 0.

retention.schedule.duration

Specifies, in hours, the amount of time the agent can take to process retention policies.

Note: The system does not recognize minute or second formatting.

retention.schedule.duration = 4 - 24

The default is 4.

retention.removal.schedule.mode

This setting places a time restriction on when Workflow Agent can remove items associated with destruction retention policies.

retention.removal.schedule.mode = Off, On, Weekends, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Off = Workflow Agent runs all of the time.

On = Workflow Agent runs only during specified time schedules.

Weekends = Workflow Agent runs only during specified times on the weekend.

Monday - Sunday = Workflow Agent runs only during specified time on that day.

The default is off.

retention.removal.schedule.start

Specifies the hour formatting on a 24-hour clock.

Note: The system does not recognize minute or second formatting.

retention.removal.schedule.start = 0 - 23

The default is 0.

retention.removal.schedule.duration

Specifies, in hours, the amount of time Workflow Agent can take to remove items associated with destruction retention policies.

retention.removal.schedule.duration = 1 - 24

The default is 0.

retention.event.polling.delay.seconds

Specifies how often, in seconds, Workflow Agent waits before performing retention event queue work.

retention.removal.schedule.duration = Any positive integer.

The default is 120 seconds (2 minutes).

retention.aging.polling.size

The maximum number of retention aging queue events that Workflow Agent can process at one time.

retention.aging.polling.size = Any positive integer.

The default maximum number of retention aging queue events that can be processed at one time is 2000.

retention.delete.polling.delay.seconds

Specifies how often, in seconds, Workflow Agent waits before performing retention delete queue work.

retention.delete.polling.delay.seconds = Any positive integer.

The default is 120 seconds (2 minutes).

retention.delete.polling.size

The maximum number of retention delete queue events that Workflow Agent can process at one time.

retention.delete.polling.size = Any positive integer.

The default maximum number of retention delete queue work that can be processed at one time is 2000.

retention.general.polling.delay.seconds

Specifies how often, in seconds, Workflow Agent waits before performing retention general queue work.

retention.general.polling.delay.seconds = Any positive integer.

The default is 30 seconds.

retention.general.polling.size

The maximum number of retention general queue events that Workflow Agent can process at one time.

retention.general.polling.size = Any positive integer.

The default maximum number of retention general queue events that can be processed at one time is 2000.

retention.mass.event.polling.size

Specifies the number of items per path, that the agent attempts to process at a time.

The minimum number of items per path is 50.

The maximum number of items per path10000.

The default number of items per path is 2000.

retention.mass.event.polling.delay.seconds

Specifies how long the agent waits between processing items.

The minimum duration is 15 seconds.

The maximum duration is 86400 seconds.

The default duration is 120 seconds.

Use command line tools

INTool commands

There are INTool commands for each of the following categories.

- Audit
- Database management
- General
- Installation
- iScript
- License
- Logs
- OSM
- Reasons
- Server
- Uncategorized
- User Administration
- Views
- Workflow

INTool Audit commands

The following INTool commands appear under the Audit category.

import-all-audit-templates

Use the `import-all-audit-templates` command to import all the audit templates that are stored in the *[drive]:\inserver\etc\audit_templates* directory.

While the `import-all-audit-templates`command is importing audit templates, it also reattaches all original users to the templates. If any templates are found to exist in the database that have the same name, an error message is written to the log file and displayed on the INTool command line prompt. This command continues until all templates have been imported even if errors occur.

The name of new templates is the file name without the file extension.

```
intool --cmd import-all-audit-templates
```

import-audit-template

Use the `import-audit-template` command to resolve template name conflicts.

You can specify an audit template file to import. You can also decide the new template name to use when the template is imported.

The `import-audit-template` command also reassigns all original users to the imported template. It displays an error message if the import is not successful.

The following table describes arguments for the `import-audit-template` command.

Argument	Description
`--template-file <file name>`	Specifies which audit template file to import.
`--template-name <name>`	Specifies the name to save for the audit template in the database.

```
intool --cmd --template-file batch_actions.ini --template-name batch_
actions
```

INTool Database Management commands

The following INTool commands appear in the Database Management category.

db-struct

Use the `db-struct` command to display the table structures and key fields in the specified table.

The following table describes arguments for the `db-struct` command.

Argument	Description
`--table-name <name>`	Specifies the name of the database table.

```
intool --cmd db-struct --table-name IN_LM_APP_PLAN
```

db-rec-num

Use the `db-rec-num` command to display the number of records in the specified table.

The following table describes arguments for the `db-rec-num` command.

Argument	Description
`--table-name <name>`	Specifies the name of the database table.

```
intool --cmd db-rec-num --table-name IN_LM_APP_PLAN
```

db-list-tables

Use the `db-list-tables` command to display a list of all Perceptive Content database tables.

```
intool --cmd db-list-tables
```

db-show-execution-plan

Use the `db-show-execution-plan` command to gather and display query execution plans to diagnose scripts that are running too slowly.

The following table describes arguments for the `db-show-execution-plan` command.

Argument	Description
`--query`	Specifies the query
`--queryFile <file>`	Specifies the file containing the queries. The query file must contain one query per line with no replacement variables.
`--queryLogFile <file>`	Specifies the file containing split queries. The query file must contain two lines per query, with one line for the query with replacement variables and another specifying parameter variables.
`--outputFile <path>`	Specifies the path where the plan is saved.

```
intool --cmd db-show-execution-plan --query  SELECT * FROM IN_DOC
```

get-db-version

Use the `get-db-version` command to display the database DDL version.

```
intool --cmd get-db-version
```

db-schema-validation

Use the `db-schema-validation` command to check for irregularities in the database.

Argument	Description
`--ignore-tablespace`	Allows the command to ignore mismatched tablespaces (Oracle) or filegroups (SQL Server) when performing a schema validation.

```
intool --cmd db-schema-validation --ignore-tablespace
```

General Commands

The following INTool commands appear under the General category.

-name

The `-name` command displays the name of the command.

```
intool --cmd -name
```

-description

The `-description` command displays the description of the command.

```
intool --cmd -description
```

-company

The `-company` command displays the company name.

```
intool --cmd -company
```

-version

The `-version` command displays the version.

```
intool --cmd -version
```

-service

The `-service` command specifies service commands.

```
intool --cmd -service
```

-help and -?

The `-help` and`-?` commands displays the command line options.

The following table describes arguments for the `-help` and `-?` commands.

Argument	Description
<command>	Displays the description of the specified command.

```
intool --cmd -help
```

--category

The `--category` command displays a list of command categories or commands under a category.

The following table describes arguments for the `--category` command.

Argument	Description
<category>	Lists the commands under the specified category.

```
intool --cmd --category osm
```

--find <keyword>

The `--find <keyword>` command searches for command names and categories that match the specified keyword. This command displays the results in a list.

The following table describes arguments for the `--find <keyword>` command.

Argument	Description
<category>	Specifies the category to search.

```
intool --cmd --find <keyword> --category osm
```

Installation Commands

The following INTool commands appear under the Installation category.

build-osm

If OSM directories have been removed from the file system, you can use the `build-osm` command to create new, empty OSM directories for each OSM tree record in the database.

This command does not recover any images from previous directories.

```
intool --cmd build-osm
```

add-subob-templ

Use the `add-subob-templ` command to add annotation templates when updating your system in UNIX.

The following table describes arguments for the `add-subob-templ` command.

Argument	Description
`--file <file name>`	Specifies the annotation template file name to add.
`department<department>`	Adds subob templates from a file to the specified department. **Note:** If no department is specified, the Default department is used.

add-users

Use the `add-users` command to add Windows users to ImageNow or to add ImageNow users from a file when you specify the optional file.

The following table describes arguments for the `add-users` command.

Argument	Description
`--file <file name>`	Optional. Specifies the name of the users file.

When you specify a file, each line in the file contains one user. You can format each line with or without the group the user belongs to, using a *<username>**<groupname>* format.

If you do not specify a file, you are prompted to for the user name or base name. For example, after running the `add-users` command, if you enter `test`, `10`, and `5`, the command creates users named test10, test11, test12, test13, test14.

This command does not add UNIX users.

```
intool --cmd add-users --file HRusers.txt
```

create-output-profiles

Use the `create-output-profiles` command to create default output profiles.

The create-output-profiles command creates a set of output profiles for the specified department. Each output profile is named Default and populates each output profile with the default options.

The following table describes arguments for the `create-output-profiles` command.

Argument	Description
`department <department>`	Creates a set of output profiles for the specified department. **Note:** If no department is specified, the Default department is used.

```
intool --cmd create-output-profiles
```

populate-calendar

Use the `populate-calendar` command to populate the ImageNow calendar system for reporting.

```
intool --cmd populate-calendar
```

populate-enumerations

Use the `populate-enumerations` command to populate the ImageNow enumeration tables for reporting.

```
intool --cmd populate-enumerations
```

create-bootstrap-user

Use the `create-bootstrap-user` command to create the initial Perceptive Manager user.

The following table describes arguments for the `create-bootstrap-user` command.

Argument	Description
`--username <user name>`	Specifies the user name for the initial Perceptive Manager user.

For Linux installations, you must run the `create-bootstrap-user` command to create the initial Perceptive Manager user. For Windows installations, the initial Perceptive Manager user is created automatically.

```
intool --cmd create-bootstrap-user --username jdoe
```

iScript Commands

The following INTool commands appear underthe iScript category.

Use the `run-iscript` command to run an iScript file.

The following table describes arguments for the `run-iscript` command.

Argument	Description
`--file <filename>`	Specifies the name of the iScript file.

```
intool --cmd run-iscript --file <file name>
```

License commands

The following INTool commands appear in the License category.

intool --cmd license-check (--type | --seats | --installed) <type>

Verifies the presence of a license.

Argument	Description
`--type <license name>`	Specifies the type of license.
`--seats <license name>`	Returns the number of remaining seat licenses for the specified license name.
`--installed <license name>`	Determines whether the license is installed.

```
intool --cmd license-check --type iScript
```

intool --cmd license-tokens --report [--client-name <client name>][--lictype <license name>]

Runs a license report for token management.

Argument	Description
`--report`	Runs a license token usage report.
`--client-name<client name>`	Optional. The name of your computer or user name.
`--lictype <license name>`	Optional. The name of the license.

```
intool --cmd license-tokens --report
```

intool --cmd license-tokens --release [--client-name <client name>][--lictype <license name>]

Releases Perceptive Content tokens from a machine so that you can use the token on another machine.

Argument	Description
`--release`	Releases the token from the specified machine.
`--client-name<client name>`	Optional. The name of your computer or user name.
`--lictype <license name>`	Optional. The name of the license.

Releases CaptureNow ISIS Level 1 tokens for GUEST1 and Computer2.

```
intool --cmd license-tokens --release --client-name "GUEST1,
Computer2" --lictype "CaptureNow - ISIS Level 1"
```

intool --cmd license-sysfp --file <file name.sysfp>

Retrieve the system fingerprint for the Perceptive Content system. The actual name of the file is supplied by the user who created it.

Argument	Description
`--file <file name.sysfp>`	The name of the system fingerprint file you are retrieving.

Retrieves the system fingerprint and saves the file as perceptive.sysfp.

```
intool --cmd license-sysfp --file perceptive.sysfp
```

intool --cmd license-validate-tokens [--lictype <license name>]

Validate license tokens for the Perceptive Content system.

Argument	Description
`--lictype <license name>`	Optional. The name of the license.

Validates tokens for the Perceptive Web Scanner license.

```
intool --cmd license-validate-tokens --lictype Perceptive Web Scanner
```

intool --cmd release-stale-tokens --lictype <license name> --days <number of days unused>

Releases license tokens that have not been used for a specified number of days.

Argument	Description
`--lictype <license name>`	The name of the license.
`--days <number of days unused>`	The system performs a search for tokens that have not been used in the minimum number of days specified in this argument. The minimum number of days allowed is 30.

Releases all tokens for the CaptureNow- ISIS Level 1 license that have not been used in the last 60 or more days.

```
intool --cmd release-stale-tokens --lictype "CaptureNow - ISIS Level
1" --days 60
```

intool --cmd update-license-allocations

Forces the system to update named license allocations.

```
intool --cmd update-license-allocations
```

intool --cmd set-demo-mode

Configures the demo mode for Perceptive Content. Demo mode can be set to timed or document mode.

Argument	Description
`--mode <mode type>`	Sets the demo mode type. Available types are `timed` and `document`.

Sets the demo mode to `document`.

```
intool --cmd set-demo-mode --mode document
```

Logs commands

The following INTool commands appear under the Logs category.

zip-logs

Use the `zip-logs` command to zip log files.

The following table describes arguments for the `zip-logs` command.

Argument	Description
`--log-name-contains <name fragments>`	Specifies a string of comma-separated name fragment text in the logs files.
`--today`	Only zips today s log files.

Note: Zip logs are placed in the *[drive]:\inserver\log* directory.

```
intool --cmd zip-logs --log-name-contains inserver --today
```

run-system-report

Use the `run-system-report` command to run a combination of system, hardware, and performance reports for diagnostic purposes. These reports are the same reports you can run from the Diagnostic pane in Management Console.

```
intool --cmd run-system-report
```

create-reflect-dataset

Use the `create-reflect-dataset`command to generate a ZIP file of comma-separated workflow process activity data in the *[drive]:\inserver\log\reflect* directory.

The following table describes arguments for the `create-reflect-dataset` command.

Argument	Description
`--process <process>`	Specifies the workflow process and the earliest and latest dates and optional times to include.

Argument	Description
`--duration <integer D, W, or M>`	Specifies the relative interval of days, weeks, or months to include in place of static start and end times and the maximum number of result rows to include.
`--brief`	Generates a file that excludes the case-level attributes.
`--file <file name>`	Specifies the file name. If you want to leave this parameter blank, the file name defaults to `Relect_YYYY_MM_DDTHHMMSSZ.zip`.
`--process-delimiter <character>`	Specifies the character to use when separating the workflow processes, which is useful in instances where your process names include comma characters. If you leave this parameter blank, the character defaults to a comma.

Note: You can import the Case Activity Report file into Perceptive Reflect for processing.

```
intool --cmd create-reflect-dataset --process  AP Workflow  --start
 2012-01-01  --end  2012-12-31  --max-rows 5000 --file  My 2012 Reflect
Report

intool --cmd create-reflect-dataset --process  AP Workflow^HR
Workflow^AR Workflow  --duration 12M --max-rows 5000 --brief--process-
delimiter ^
```

OSM Commands

The following INTool commands appear under the OSM category.

build-osm

If OSM directories have been removed from the file system, you can use the `build-osm` command to create new, empty OSM directories for each OSM tree record in the database.

Note: This command does not recover any images from the previous directories.

```
intool --cmd build-osm
```

fix-next-slot

Use the `fix-next-slot` command to traverse each OSM tree directory and set the right value in the NEXT_SLOT field of each OSM tree record.

Arguments for the `fix-next-slot` command are provided in the following table.

Argument	Description
`--osm-tree <osm tree name>`	Optional. Specifies the name of the OSM tree.
`--slot <next slot>`	Optional. Specifies a quoted digit string that represents the slot.

Note: If you provide the tree name, the system only fixes the record for the specified tree. If you do not provide the tree name, the system fixes all the OSM tree records.

```
intool --cmd fix-next-slot --osm-tree osm 01.00001
intool --cmd fix-next-slot --osm-tree osm 01.00001 --slot
 00000000/00000000/00000000
```

add-osm-set

Use the `add-osm-set` command to add a primary OSM set.

Arguments for the `add-osm-set` command are provided in the following table.

Argument	Description
`--record <record>`	Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

You must know the record definition for the `add-osm-set` command. You can either provide the `--record <record>` argument or omit it and enter the field values at the command line.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd add-osm-set

intool --cmd add-osm-set --record  osm 01^1^1^OSM set for HR files^osm
02^Created for a filter^0^
```

add-osm-set --reference

Use the `add-osm-set --reference` command to add a reference OSM set.

Arguments for the `add-osm-set --reference` command are provided in the following table.

Argument	Description
`--record <record>`	Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set.

You must know the record definition for the `add-osm-set --reference` command. You can either provide the `--record <record>` argument or omit it and enter the field values at the command line.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd add-osm-set --reference

intool --cmd add-osm-set --reference --record  osm 01^1^OSM reference
set for legacy files^^Created to reference existing documents in the
legacy system^
```

add-osm-tree

Use the `add-osm-tree` command to add an FSS or EXT OSM tree.

Arguments for the `add-osm-tree` command are provided in the following table.

Argument	Description
`--type <type>`	Specifies the storage device type, which is FSS (File System Storage) or EXT (External File Storage, used only with OSM plugins).
`--record <record>`	Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

You must know the record definition for the `add-osm-tree` command. You can either provide the `--record <record>` argument or omit it and enter the field values at the command line.

If you don't specify the `--record` argument, you are prompted for all the fields for the OSM tree.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd add-osm-tree --type EXT --record "osm_01.00001^osm_
01^HR^acuostore^"
```

add-osm-filter

Use the `add-osm-filter` command to add an OSM filter.

Arguments for the `add-osm-filter` command are provided in the following table.

Argument	Description
`--osm-set <set name>`	Specifies an OSM set name.
`--type <filter type>`	Represents a DRAWER or DOCTYPE.
`--value <value>`	Specifies the value of a drawer or document type.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

A filter specifies an OSM set in which a document with a certain drawer or document type value is stored. If there are filters on drawer and document type that store data in different locations, and a captured document is assigned document key values for drawer and document type that satisfy the conditions of both filters, the document is stored based on the drawer filter.

You can only add OSM set filters to OSM sets that are either mixed type or document type.

```
intool --cmd add-osm-filter --osm-set osm_01 --type DRAWER --value HR
```

add-osm-cache

Use the `add-osm-cache` command to link two existing OSM sets together.

Arguments for the `add-osm-cache` command are provided in the following table.

Argument	Description
`--permanent-osm-set <set name>`	Specifies the name of the permanent OSM set.
`--cache-osm-set <set name>`	Specifies the name of the cached OSM set.
`--lifetime <minutes>`	Specifies the time in minutes to store the object in the cache.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

When these sets are linked, one OSM set is used for permanent storage and the other OSM set is used as the cache storage.

The default cache lifetime is 1,440 minutes. To change the cache lifetime value, use the `--lifetime` argument.

```
intool --cmd add-osm-cache --permanent-osm-set osm_01 --cache-osm-set
osm_04
```

update-osm-set

Use the `update-osm-set` command to update a specified primary OSM set.

Arguments for the `update-osm-set` command are provided in the following table.

Argument	Description
`--record <record>`	Optional. Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

You must know the record definition for the `update-osm-set` command. You can either provide the `--record <record>` argument or omit it and enter the field values at the command line.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd update-osm-set

intool --cmd update-osm-set --record  osm_01^1^1^Personnel Data^osm_
2^Was formerly HR files^0^osm_01.00001^
```

update-osm-set --reference

Use the `update-osm-set --reference` command to update a specified reference OSM set.

Arguments for the `update-osm-set --reference` command are provided in the following table.

Argument	Description
`--record <record>`	Optional. Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set.

You must know the record definition for the `update-osm-set` command. You can either provide the `--record <record>` argument or omit it and enter the field values at the command line.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd update-osm-set --reference

intool --cmd update-osm-set --reference --record  osm_01^1^OSM reference
 set for legacy files^^Created to reference existing documents in the
legacy system^
```

update-osm-tree

Use the `update-osm-tree` command to update the specified OSM tree.

Arguments for the `update-osm-tree` command are provided in the following table.

Argument	Description
`--type <type>`	Specifies the storage device type, which is FSS (File System Storage) or EXT (External File Storage, used only with OSM plugins).
`--record <record>`	Specifies a quoted string that contains the record fields.
`--delim <character>`	Optional. Specifies a character to use as a delimiter. The default delimiter is ^.

You must know the record definition for to use the `update-osm-tree` command. You can either provide the `--record <record>`argument or omit it and enter the field values at the command line.

You must separate the record values with the ^ character and surround the string with quotation marks. If you want to use a delimiter other than ^, include the `[--delim <character>]` argument, followed by the character in quotation marks.

```
intool --cmd update-osm-tree --type EXT

intool --cmd update-osm-tree --type FSS --record " osm_01.00001^osm_
01^Updated osm tree description^0^0^c:\inserver\osm_
01.00001^^00000000/00000000/00000015^0^0^0^1024^1^1"
```

update-osm-filter

Use the `update-osm-filter` command to change the destination OSM set name for an existing filter that is identified by its type and value.

Arguments for the `update-osm-filter` command are provided in the following table.

Argument	Description
`--osm-set <set name>`	Specifies an OSM set name.
`--type <filter type>`	Represents a DRAWER or DOCTYPE.
`--value <value>`	Specifies the value of a drawer or document type.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

You can only add OSM set filters to OSM sets that are either mixed type or document type.

```
intool --cmd update-osm-filter --osm-set osm_01 --type DRAWER --value HR
```

update-osm-cache

Use the `update-osm-cache` command to change how caching is performed for an OSM set.

Arguments for the `update-osm-cache` command are provided in the following table.

Argument	Description
`--permanent-osm-set<set name>`	Specifies the name of the permanent OSM set.

Argument	Description
`--cache-osm-set <set name>`	Optional. Specifies the name of the cached OSM set.
`--cache-level`	Optional. Specifies the type of caching as disabled, read-only caching, or read-write caching.
`--lifetime <minutes>`	Optional. Specifies the time in minutes to store the object in the cache.

Note: At least one of the optional settings in the table must be set when using the update-osm-cache command.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

When these sets are linked, one OSM set is used for permanent storage and the other OSM set is used as the cache storage.

The default cache lifetime is 1,440 minutes. To change the cache lifetime value, use the `--lifetime` argument.

```
intool --cmd update-osm-cache --permanent-osm-set osm_01 --cache-osm-set
osm_04 --cache-level read-write --lifetime 2880
```

validate-osm-report

Use the `validate-osm-report` command to generate an OSM validation report. The OSM validation report contains a list of all stored objects that are currently in an inconsistent state. The system validates the stored objects when you enable inserverOSM background validation or run the `validate-document` command.

Arguments for the `validate-osm-report` command are provided in the following table.

Argument	Description
`--osm-output <xml file path>`	Specifies the output path for the OSM validation report.
`--email <email address to notify on failure>`	Represents the email address to notify and send the report if there are known validation failures.

```
intool --cmd validate-osm-report --output results.xml --email
test@perceptivesoftware.com
```

Sample command output

```
The following OSM files did not validate:

Status: Object was not found OSM Tree: osm_01.00001 Path:
00000000/00000000/00000000

Status: Object does not match the original OSM Tree: osm_01.00001 Path:
00000000/00000000/00000001
```

Sample report output

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<VerificationResults>
    <VerificationResult>
        <Phsob>
            <id>321Z41Q_00004G1P800000C</id>
            <osmTreeName>osm_01.00001</osmTreeName>
            <state>missing</state>
            <type>fss</type>
            <path>00000000/00000000/00000000</path>
            <verifyTime>2020-01-23T20:16:44Z</verifyTime>
        </Phsob>
    </VerificationResult>
    <VerificationResult>
        <Phsob>
            <id>321Z41Q_00004R1P8000006</id>
            <osmTreeName>osm_01.00001</osmTreeName>
            <state>altered</state>
            <type>fss</type>
            <path>00000000/00000000/00000001</path>
        <verifyTime>2020-01-23T20:17:04Z</verifyTime>
        </Phsob>
    </VerificationResult>
</VerificationResults>
```

validate-document

Use the `validate-document` command to actively check the state of stored objects associated with the latest version of a document. This updates the verification state of stored objects.

Arguments for the `validate-document`command are provided in the following table.

Argument	Description
`--docid`	Specifies the ID of the document to validate.
`--output <xml file path>`	Specifies the output path for the OSM validation report.

```
intool.exe --cmd validate-document --docid 321Z41Q_00004R1P8000001 --
output results.xml
```

Sample report output

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<VerificationResults>
    <VerificationResult>
        <Logob>
            <id>321Z41Q_00004R1P8000005</id>
            <seqNum>1</seqNum>
            <logobType>0</logobType>
        </Logob>
        <Phsob>
            <id>321Z41Q_00004R1P8000006</id>
            <osmTreeName>osm_01.00001</osmTreeName>
            <state>altered</state>
            <type>fss</type>
            <path>00000000/00000000/00000001</path>
            <verifyTime>2020-01-23T20:17:04Z</verifyTime>
            <fileType>tif</fileType>
            <workingName>Demo 02.tif</workingName>
```

```
            </Phsob>
        </VerificationResult>
    </VerificationResults>
```

delete-osm-set

Use the `delete-osm-set` command to delete an OSM set.

Arguments for the `delete-osm-set` command are described in the following table.

Argument	Description
`--osm-set <set name>`	Specifies an OSM set name.

```
intool --cmd delete-osm-set --osm-set osm_03
```

delete-osm-tree

Use the `delete-osm-tree` command to delete an OSM tree.

Argument	Description
`--osm-tree <tree name>`	Specifies the OSM tree to delete.

```
intool --cmd delete-osm-tree --osm-tree osm_01_00001
```

delete-osm-filter

Use the `delete-osm-filter` to delete an OSM filter by filter type and value.

Arguments for the `delete-osm-filter` command are provided in the following table.

Argument	Description
`--type <filter type>`	Represents a DRAWER or DOCTYPE.
`--value <value>`	Specifies the value of a drawer or document type.

The filter value is case-sensitive.

```
intool --cmd delete-osm-filter --type DRAWER --value HR
```

delete-osm-cache

Use the `delete-osm-cache` command to remove the caching link between the permanent and cache OSM sets. Removing the cache link ensures no new objects are added to the cache.

Argument	Description
`--permanent-osm-set <set name>`	Specifies the name of the permanent OSM set.
`--cache-osm-set <set name>`	Specifies the name of the cached OSM set.

```
intool --cmd delete-osm-cache --permanent-osm-set osm_01 --cache-osm-set
osm_04
```

delete-cache-set

Use the `delete-cache-set` command to delete an OSM cache set from both the database and the file system. The command first disables the specified cache and then attempts to delete the cache set and any associated objects still in the cache. If the cache is configured as a write-cache and all objects have not been replicated to the permanent set, the command terminates and intentionally leaves the cache in a disabled state. Once the OSM Agent replicates all objects, you can rerun the command to complete the cache set deletion. The file system directories associated with the cache are then deleted.

Arguments for the `delete-cache-set` command are provided in the following table.

Argument	Description
`--cache-set <cache set name>`	Specifies an OSM cache set name.

```
intool --cmd delete-cache-set --cache-set centera_cache
```

list-osm-sets

Use the `list-osm-sets` command to display a list of all OSM sets, including primary and reference sets.

```
intool --cmd list-osm-sets
```

list-osm-sets --primary

Use the `list-osm-sets --primary` command to display a list of all primary OSM sets.

```
intool --cmd list-osm-sets --primary
```

list-osm-sets --reference

Use the `list-osm-sets --reference` command to display a list of all reference OSM sets.

```
intool --cmd list-osm-sets --reference
```

list-osm-trees

Use the `list-osm-trees` command to display a list of all OSM trees in the specified OSM set.

Arguments for the `list-osm-trees` command are provided in the following table.

Argument	Description
`--osm-set <set name>`	Specifies an OSM set name.

```
intool --cmd list-osm-trees --osm-set osm_01
```

list-osm-filters

Use the `list-osm-filters` to display a list of all OSM filters.

```
intool --cmd list-osm-filters
```

list-osm-caches

Use the `list-osm-caches` command to list all of the existing cache links on the command line.

```
intool --cmd list-osm-caches
```

transfer-doc

Use the `transfer-doc` command to transfer a document to a different OSM set.

Arguments for the `transfer-doc` command are provided in the following table.

Argument	Description
`--docid <id>`	Specifies the document ID.
`--osm-set <set name>`	Specifies an OSM set name.

Note: You cannot add a filter that redirects documents to an OSM set if the set has been designated as a reference set, or a primary set with caching or sub-objects.

You must specify the document by document ID. The system moves all the physical objects and sub objects from the original OSM set to the specified OSM set.

```
intool --cmd transfer-doc -docid 2000000003_00008H3ZMTB0 --osm-set osm_
04
```

cleanup-orphan-erm

Use the `cleanup-orphan-erm` command to clean up OSM records that point to report record that no longer exist.

```
intool --cmd cleanup-orphan-erm
```

add-osm-plugin

Use the `add-osm-plugin` command to add and configure OSM plugins.

After entering the command, you are prompted to enter the plugin name, description, and optional plugin properties.

Alternatively, you can include the name, description, and properties with the command, separated by a delimiter.

Argument	Description
`--record <record>`	Optional. Specifies a delimited string containing the plugin properties.
`--delim <character>`	Optional. Specifies the delimiter used to separate the plugin properties. The default delimiter is ^.

```
intool --cmd add-osm-plugin
```

```
intool --cmd add-osm-plugin --record
name^description^key1^value1^key2^value2
```

delete-osm-plugin

Use the `delete-osm-plugin` command to delete an OSM plugin.

Argument	Description
`--name <name>`	Specifies the plugin name.

```
intool --cmd delete-osm-plugin --name PluginName
```

update-osm-plugin

Use the `update-osm-plugin` command to update OSM plugin configurations.

After entering the command, you are prompted to enter the plugin name, description, and optional plugin properties.

Alternatively, you can include the name, description, and properties with the command, separated by a delimiter.

If a specified plugin property does not already exist, it is created. If the property already exists, it is updated. To delete a plugin property, specify an empty property value.

Argument	Description
`--record <record>`	Optional. Specifies a delimited string containing the plugin properties.
`--delim <character>`	Optional. Specifies the delimiter used to separate the plugin properties. The default delimiter is ^.

```
intool --cmd update-osm-plugin
```

```
intool --cmd update-osm-plugin --record "osmplugin^An OSM Plugin^OSM
Plugin Property^Property value"
```

```
intool --cmd update-osm-plugin --record "osmplugin^An OSM Plugin^OSM
Plugin Property^Updated property value"
```

list-osm-plugins

Use the `list-osm-plugins` command to display a list of OSM plugins.

```
intool --cmd list-osm-plugins
```

Reasons commands

The following INTool commands appear under the Reasons category.

add-digsig-reasons

Use the `add-digsig-reasons`command only when updating your system in UNIX to add digital signature reasons.

The following table describes arguments for the `add-digsig-reasons` command.

Argument	Description
`--file <file name>`	Specifies the name of the digital signature reasons file.

For information on when to run the `add-digsig-reasons` command, refer to the Update Guide for you version of Perceptive Content. For more information about updating your system, contact your Perceptive Software representative.

```
intool --cmd add-digsig-reasons --file PredefinedDigSigReasons.ini
```

add-task-reasons

Use the `add-task-reasons` command to add task reasons from a file.

The following table describes arguments for the `add-task-reasons` command.

Argument	Description
`--file <file name>`	Specifies the file for the task reasons.

```
intool --cmd add-task-reasons --file PredefinedTaskReasons.ini
```

add-ooo-reasons

Use the `add-ooo-reasons` command to add out of office reasons from a file when updating your system in UNIX.

The following table describes arguments for the `add-ooo-reasons` command.

Argument	Description
`--file <file name>`	Specifies the file for the out of office reasons.

For more information on when to run the `add-ooo-reasons` command, refer to the Update Guide for your version of Perceptive Content. For more information about updating your system, contact your Perceptive Software representative.

```
intool --cmd add-ooo-reasons --file PredefinedOutOfOfficeReasons.ini
```

Server commands

The following INTool commands appear in the Server category.

intool --cmd revoke-all-certs

This command removes all trusted certificates from the SSO trust store.

Argument	Description
`--login-profile <name of login profile>`	When specified, this allows for all trusted certificates to be revoked for a specific login profile.

```
intool --cmd revoke-all-certs
intool --cmd revoke-all-certs --login-profile default
```

intool --cmd revoke-cert

This command removes a trusted certificate from the SSO trust store.

Argument	Description
`--login-profile <name of login profile>`	When specified, this allows for a trusted certificates to be revoked for a specific login profile.

```
intool --cmd revoke-cert
intool --cmd revoke-cert --login-profile default
```

intool --cmd import-cert

This command adds a certificate to the SSO trust store.

Argument	Description
`--file <certificate name>`	Specifies the certificate to import.
`--type <type of SSO used with this certificate>`	Imports a trusted certificate into Perceptive Content. Supported values are `pki-sso`, `openid-connect` and `token-auth`.
`--login-profile <name of login`	If the specified type is openid-connect, a login profile

Argument	Description
profile>	must also be specified. This will import a trusted certificate for that specific profile.
`--key-id <key ID value>`	If the specified type is openid-connect, a key ID must also be specified. This value will be validated against the key ID used by your OpenID Provider to sign ID tokens.

```
intool --cmd import-cert --file company1.cer --type pki-sso

intool --cmd import-cert --file company1.cer --type openid-connect --
login-profile default --key-id uniqueKeyId
```

intool --cmd control-logins

This command prevents users from logging into Perceptive Content Server.

Argument	Description
`--enable`	Prevents users from logging in to Perceptive Content Server. Any users who are logged in when this command is enabled are not disconnected; they remain logged in until they disconnect. This command also prevents any agents with a log-in feature from logging in to Perceptive Content Server. The following agents do not require a log in to Perceptive Content Server, so they are the only agents that can access Perceptive Content Server while this command is active. • ACD Agent • Alarm Agent • Auto Update • Batch Agent • BI Authenticator • DataCapture Agent • EOB Agent • ERM Admin Agent

Argument	Description
	• ERM Import Agent • ERM Upload Agent • External Messaging Agent • Fax Agent • ImageNow Forms Server • File System Agent • Forms Processing Agent • Import Agent • INTool • iOrganize Agent • ISIR Agent • Job Agent • LDAP Sync Agent • Mail Agent • Message Agent • Message Queueing Agent • MQSink Agent • Notification Agent • OSM Agent • Output Agent • Recognition Agent • SAP Agent • Task Agent • INUpgradeUtil • Word Agent • Workflow Agent
`--disable`	Disables the command, allowing users to log in to Perceptive Content Server.
`--instance <InstanceName> [--message "<msg>"]`	The running instance of Perceptive Content Server.

```
intool --cmd control-logins --enable --instance Primary --message
"Logging in is temporarily deactivated."
```

Uncategorized commands

The following INTool commands do not appear under a specific category.

export-all-record-objects

Use the `export-all-record-objects` command to export all records in the system.

The following table describes arguments for the `export-all-record-objects` command.

Argument	Description
`--export-dir <export directory name>`	Specifies the directory within the export.file.directory to which the records are exported.

The `export-all-record-objects` command requires a records management license. Upon running the command, export jobs are created and may take several days or weeks to complete depending on the number of records that exist in the system.

```
intool --cmd export-all-record-objects --export-dir DODExportDirectory
```

User Administration commands

The following INTool commands appear under the User Administration category.

add-users

Use the `add-users` command to add Windows users to Perceptive Content or to add Perceptive Content users from a file when you specify the optional file.

Note: To use the `add-users` command, you must be a Perceptive Manager.

The following table contains arguments for the `add-users` command.

Argument	Description
`--file <file name>`	Optional. Specifies the name of the users file.
`--login-name <user name>`	Specifies your user name. Use this argument together with `--login-password` to authenticate your role as a Perceptive Manager.
`--login-password <password>`	Specifies your system password. Use this argument together with `--login-name` to authenticate your role as a Perceptive Manager.

When you specify a file, each line in the file contains one user, which you can format with or without the group to which the user belongs, using a *<user name>\<group name>* format.

When you do not specify a file, you are prompted for the user name or base name. After running the `add-users` command, for example, if you type `test, 10`, and `5` for the number of users to add; when prompted, the command creates users called test10, test11, test12, test13, and test14.

The `add-users`command does not add UNIX users.

```
intool --cmd add-users --login-name pman --login-password ImageNow --
file HRusers.txt

intool --cmd add-users --login-name pman --login-password ImageNow
```

logoff

Use the `logoff` command to log off a user session.

The following table contains arguments for the `logoff` command.

Argument	Description
`--username <user name>`	Specifies the user to log off.

After running the `logoff` command, INTool prompts you to select the appropriate corresponding line number of the user session you want to log off.

Note: Logging off a user session may cause loss of data if the user is in the middle of an operation.

```
intool --cmd logoff --username asmith
```

logoff-expired-sessions

Use the `logoff-expired-sessions` command to log off a user session that has persisted longer than the specified number of minutes. User sessions can be further filtered by client license type.

The following table contains arguments for the `logoff-expired-sessions` command.

Argument	Description
`--max-age <minutes>`	Specifies the maximum duration in minutes a user session can remain logged in to the system.
`--lictype <license type>`	Optional. Specifies the client license types associated with a user session that will be logged off of the system after the maximum duration is passed.

Note: Logging off a user session may cause loss of data if the user is in the middle of an operation.

delete-users

Use the `delete-users` command to delete Perceptive Content or Windows users from the system.

The following table contains arguments for the `delete-users` command.

Argument	Description
`--login-name <user name>`	Specifies your user name. Use this argument together with `--login-password` to authenticate your role as a Perceptive Manager.
`--login-password <password>`	Specifies your system password. Use this argument together with `--login-name` to authenticate your role as a Perceptive Manager.

```
intool --cmd delete-users --login-name pman --login-password ImageNow
```

promote-perceptive-manager

Use the `promote-perceptive-manager` command to promote a user to Perceptive Manager.

Note: To use the `promote-perceptive-manager` command, you must be a Perceptive Manager. If there is no match for the user name entered in the argument, the system alerts you and asks if you want to create a Perceptive Manager with the provided user name.

The following table contains arguments for the `promote-perceptive-manager` command.

Argument	Description
`--username <user name>`	Specifies the user to designate as a Perceptive Manager.
`--login-user <user name>`	Optional. Specifies your user name. Use this argument together with `--login-password` to authenticate your role as a Perceptive Manager.
`--login-password <password>`	Optional. Specifies your system password. Use this argument together with `--login-user` to authenticate your role as a Perceptive Manager.

```
intool --cmd promote-perceptive-manager --username sampleuser1
```

demote-perceptive-manager

Use the `demote-perceptive-manager` command to demote a user from the Perceptive Manager role.

Note: To use the `demote-perceptive-manager` command, you must be a Perceptive Manager.

The following table contains arguments for the `demote-perceptive-manager` command.

Argument	Description
`--username <user name>`	Specifies the user to remove as a Perceptive Manager.
`--login-user <user name>`	Optional. Specifies your user name. Use this argument together with `--login-password` to authenticate your role as a Perceptive Manager.
`--login-password <password>`	Optional. Specifies your system password. Use this argument together with `--login-user` to authenticate your role as a Perceptive Manager.

```
intool --cmd demote-perceptive-manager --username sampleuser2
```

send-message

Use the `send-message` command to send a text message to a user or to all connected Perceptive Content users.

The following table contains arguments for the `send-message` command.

Argument	Description
`--recipient <user name>`	Specifies the name of a single user.
`--broadcast`	Sends the message to all connected Perceptive Content users.
`--message <message>`	Specifies the message to send. Quotation marks are required.

```
intool --cmd send-message --broadcast --message  Log off at 5:00 PM for
system maintenance.
```

expire-digital-ids

Use the `expire-digital-ids` command to immediately expire all active digital IDs. Users are required to enter a new password the next time they apply a digital signature to a document in Perceptive Content.

```
intool --cmd expire-digital-ids
```

create-authentication-token

Use the `create-authentication-token` command to create an authentication token for the specified application.

Note: Prior to running this command, you must set token signing configuration settings in inow.ini.

The following table contains arguments for the `create-authentication-token` command.

Argument	Description
`--lictype`	Specifies the application name. Supported application names are ImageNow Business Insight, ImageNow Forms Server, and Mail Agent.
`--file`	Optional. Specifies a file to which to write the authentication token.

```
intool --cmd create-authentication-token --lictype Mail Agent
```

openidconnect-invalidate-discovery-configuration

Use the `openidconnect-invalidate-discovery-configuration` command to invalidate cached information associated with an OpenID Connect auto discovery profile.

Note: This only affects OpenID Connect authentication profiles that are using auto.discovery.

The following table contains arguments for the `openidconnect-invalidate-discovery-configuration` command.

Argument	Description
`--profile`	Optional. Specifies the profile configured in inserver.ini to validate. If not specified, all cached OpenID Connect profile information is invalidated.

```
#Invalidates configuration for all profiles.

intool --cmd openidconnect-invalidate-discovery-configuration
```

```
#Invalidates configuration for a specific profile.

intool --cmd openidconnect-invalidate-discovery-configuration --profile
default
```

Views Commands

The following INTool commands appear under the Views category.

create-default-view

Use the `create-default-view` command to create the system default views.

The following table describes arguments for the `create-default-views` commands.

Argument	Description
`--doc`	Creates the default document view.
`--folder`	Creates the default folder view.
`--folder-content`	Creates the default folder content view.
`--record`	Creates the default record view.
`--record-folder`	Creates the default record folder view.
`--record-folder-content`	Creates the default record folder content view.
`--task`	Creates the default task view.
`--wf`	Creates the default workflow queue view.
`--replace`	Optional. Replaces the current default view with the system default.
`--noreplace`	Optional. Does not replace the current default view defined.

You can use one of the optional view category arguments to create a single default view. If you don't include this argument, the system creates all default views.

```
intool --cmd create-default-view

intool --cmd create-default-view --doc --replace
```

explain-vsl

Use the `explain-vsl` command to display a list of search constraints, a list of VSL data types, and the first Perceptive Content product release that supported the data type.

The following table describes arguments for the `explain-vsl` command.

Argument	Description
`--view-category doc`	Displays only document search constraints.
`--view-category folder`	Displays only folder search constraints.
`--view-category folder-content`	Displays only folder content search constraints.
`--view-category task`	Displays only task search constraints.
`--view-category wf`	Displays only workflow search constraints.
`--show-types`	Displays a list of the VSL data types, the supported operators, and sample VSL text to use in a call.

```
intool --cmd -explain-vsl
intool --cmd explain-vsl view-category doc --show-types
```

remove-default-user-views

Use the `remove-default-user-views` command to remove the default view settings from all users.

```
intool --cmd remove-default-user-views
```

Workflow commands

The following INTool commands appear under the Workflow category.

reset-item-count

Use the `reset-item-count` command to reset the item count for all queues to the number of items in the specified queue.

The following table describes arguments for the `reset-item-count` command.

Argument	Description
`--zero`	Resets the item count for all queues to zero.
`--q-name <queue>`	Resets the item count for the specified queue.

If this command is executed as a user, only the queues accessible to that user are reset.

```
intool --cmd reset-item-count
intool --cmd reset-item-count --q-name Start
```

unlock-process

Use the `unlock-process` command to remove a user lock from a workflow process.

The following table describes arguments for the `unlock-process` command.

Argument	Description
`--process-name <process>`	Specifies the workflow process you need to unlock

```
intool -cmd unlock-process --process-name approve_expenses
```

reset-item-status

Use the `reset-item-status`command to reset the item from Working to Idle status, or reset the item from Working to Complete status, if run from a Complete queue.

The following table describes arguments for the `reset-item-status` command.

Argument	Description
`--user-name <user name>`	Resets the status for a user in all queues.
`--queue-name <queue>`	Resets the item count for the specified queue.

```
intool --cmd reset-item-status
intool --cmd reset-item-status --user-name jdoe --queue-name Invoices
```

verify-subqueue-names

Use the `verify-subqueue-names`command to view sub queues names that do not meet the supported naming convention: *<sub queue (super queue)>*

The following table describes arguments for the `verify-subqueue-names` command.

Argument	Description
`--preview`	Lists the subqueue names.
`--fix`	Renames all subqueues to the supporting name convention.

```
intool --cmd verify-subqueue-names --fix
```

reset-workflow-views

Use the `reset-workflow-views`command to inherit the properties from a superqueue to a private filter on a subqueue.

The following table describes arguments for the `reset-workflow-views` command.

Argument	Description
`--process-name` *<process name>*	Specifies the name of the workflow process.
`--queue-name`*<queue-name>*	Specifies the workflow queue name.
`--superqueue-name`	Specifies the name of the superqueue.
`--max-rows` *<integer>*	Specifies the maximum number of result rows to include.
`--replace-columns`	Replaces any custom column headings. Using this parameter increases processing time.

```
intool --cmd reset-workflow-views --process-name AP --queue-name
ReviewQueue
```

validate-integration-asq

Use the `validate-integration-asq` command to verify that the parameter map sets in an Integration ASQ are valid for the Envoy service operation defined for that queue.

The following table describes arguments for the `validate-integration-asq` command.

Argument	Description
`--process <process name>`	Validates the parameter map for all of the Integration ASQs in the specified process.
`--queue <queue-name>`	Validates the parameter sets for a specified Integration ASQ.

If you don t provide an argument, Perceptive Content validates all of the Integration ASQs in your system.

```
intool --cmd validate-integration-asq --process AP

intool --cmd validate-integration-asq --queue Admissions
```

INUpgradeUtil commands

The following topics describe INUpgradeUtil commands and the arguments that you can enter with them.

convert-integration-queues

The optional `convert-integration-queues` command converts existing Integration ASQs into Connect ASQs for Perceptive Content 7.2.x compatibility. The use of the `INWfQueue` function to create Integration ASQs is deprecated for Perceptive Content 7.2.1 and future versions. Existing Integration ASQs can be modified but new Integration ASQs cannot be created.

The following are arguments for the`convert-integration-queues` command. One or both of the following arguments are required.

- `--process-name <"Process Name">`
- `--envoy-service-name <"Service Name">`

Example
```
inUpgradeUtil convert-integration-queues --process-name "Human
Resources" --envoy-service-name PeopleSoft
```

remove-fulltext-artifacts

The optional `remove-fulltext-artifacts` command removes fulltext search result artifacts from all documents on the system for Perceptive Content 7.2.x compatibility.

upgrade-server-queries

The `upgrade-server-queries` command upgrades Perceptive Content 6.1.x server queries to the current version of Perceptive Content.

```
inupgradeutil upgrade-server-queries
```

upgrade-privs

The `upgrade-privs` command upgrades Perceptive Content 6.3.x privileges to Perceptive Content 7.0 or higher and adds new privileges that did not exist in previous versions.

The following is an argument for the `upgrade-privs` command.

- `--from <version>`

The `upgrade-privs`command promotes all users who had the owner or manager role in the previous version to the Perceptive Manager role and the Department Manger role for the Default department. This command also grants several privileges enabling user privilege administration or group privilege administration.

```
inpugradeutil upgrade-privs --from <version>
```

upgrade-digsig-reasons

The `upgrade-digsig-reasons` command migrates the IN_SIG_REASON and IN_USR_KEY_REASON records from Perceptive Content 6.1.x to IN_LIST, IN_LIST_ITEMS, and IN_LIST_MEMBER tables in the current version of Perceptive Content.

```
intool upgrade-digsig-reasons
```

upgrade-digsig-version

The `upgrade-digsig-version` command enables the use of digital signatures that were created using certain Unicode versions of ImageNow and Perceptive Content.

The `upgrade-digsig-version` command is required only when updating your system from ImageNow Server 6.x or Perceptive Content Server versions 7.0, 7.1, 7.1.1, or 7.1.2.

upgrade-learn-mode

The `upgrade-learn-mode` upgrades LearnMode applets to LearnMode application plans.

The `upgrade-learn-mode` command is required only when upgrading your system from 6.1.x to 6.2.x or above.

The following are arguments for the `upgrade-learn-mode` command.

- `--convert <AppletName>`
- `--scrub <AppPlanName>`
- `--remove`

```
inupgradeutil upgrade-learn-mode --convert <AppletName> --scrub
<AppPlanName> --remove
```

upgrade-composite-properties

The `upgrade-composite-properties` command upgrades 6.5 composite custom properties.

After the upgrade, you can search for composite custom properties and physical custom properties.

The `upgrade-composite-properties` command is only required when upgrading from 6.5 to 6.5.1 or higher.

```
inupgradeutil upgrade-composite properties
```

update-rules

The `update-rules` command upgrades 6.x routing alarm rules to Perceptive Content 6.4.x or higher.

```
inupgradeutil update-rules
```

import-all-audit-templates

The `import-all-audit-templates` command upgrades legacy audit templates from Perceptive Content 6.1.x to the current version of Perceptive Content 6.5.x or higher.

```
import-all-audit-templates
```

update-license

The `update-license` command upgrades overdraft license usage from 6.5.1 or lower to 6.6 or higher compatibility.

```
inupgradeutil update-license
```

upgrade-views

The `upgrade-views` command upgrades legacy views from 6.6x or lower to 6.7 or higher compatibility.

```
inupgradeutil upgrade-views
```

upgrade-users

The `upgrade-users` command upgrades anonymous user formatting so only one anonymous users is assigned to each purpose.

The `upgrade-users` command upgrades the 6.6 anonymous accounts to 6.7 and later versions.

```
inupgradutil upgrade-users
```

upgrade-timing

The `upgrade-timing` command with the `--purge` argument purges all archived ImageNow Client performance reporting data recorded in versions 6.6 or lower.

The following is an argument for the `upgrade-timing` command.

- `--purge`

```
inupgradeutil upgrade-timing --purge
```

upgrade-outlook-source-profile

The `upgrade-outlook-source-profile` command upgrades Outlook source profiles that describe how Outlook captures an email.

```
inupgradeutil upgrade-outlook-source-profile
```

upgrade-remote-service-files

The `upgrade-remote-service-files` command upgrades remote service file locations from 6.2 and earlier locations.

```
inupgradeutil upgrade-remote-service-files
```

upgrade-audit-templates

The `upgrade-audit-templates` command upgrades 6.7 and 6.8 audit templates for 7.0 compatibility.

```
inupgradeutil upgrade-audit-templates
```

upgrade-custom-properties

The `upgrade-custom-properties` command upgrades 6.7 and 6.8 custom properties for 7.0 compatibility.

```
inupgradeutil upgrade-custom-properties
```

upgrade-policy-queues

The `upgrade-policy-queues` command upgrades retention policy queues for 7.0 compatibility.

```
inupgradeutil upgrade-policy-queues
```

Run INTool commands

Using INTool, you can administer your server by running commands in a command prompt window. To start INTool and view a list of commands, complete the following steps.

1. Click **Start > Run**.
2. In the **Run** dialog box, type `cmd`, and then click **OK**.
3. On the **ImageNow Server** computer, do one of the following actions:
   - In Windows 32-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In Unix, change to the *$(IMAGENOWDIR)/bin* directory.
4. Do one or more of the following steps:
   - To display a list of INTool commands, at the prompt enter `intool`.
   - To view detailed information about a specific INTool command, at the prompt enter `intool --cmd`.

Run INUpgradeUtil commands

To start INUpgradeUtil and view a list of commands, complete the following steps.

Run INUpgradeUtil commands only if you are instructed to do so by Product Support.

1. Click **Start > Run**.
2. In the **Run** dialog box, type `cmd` and then click **OK**.
3. On the **ImageNow Server** computer, do one of the following actions:
   - In Windows 32-bit, open a **Command Prompt** window and change to the*[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In Unix, change to the *$(IMAGENOWDIR)/bin* directory.
4. Do one or more of the following steps:
   - To display a list of INUpgradeUtil commands, at the prompt enter `inupgradeutil`.
   - To view detailed information about a specific INUpgradeUtil command, at the prompt enter `inupgradeutil --cmd-help <command>`.

Use VSL

What is VSL?

Perceptive Content uses Visual Scripting Language (VSL) to create statements you can use in a call.

Like a simple search, a VSL rule consists of three parts:

- A property constraint, such as a document key or a workflow status.
- An operator that compares the property to the value, such as is equal to or starts with.
- A value that defines the statement.

For example, if you want to define a statement that specifies the Invoice document type, the VSL syntax appears as follows. In this example, [doctype] is the property, = is the operator, and Invoice is the value. Using the `explain-vsl INTool` command, you can interpret the VSL statement syntax for the rule you want to create.

```
      [docType] =  Invoice
```

VSL property constraints

The VSL property constraint tables list the search constraint components available for use when running a view in Perceptive Content. You can reference the tables to determine the VSL text that is applicable for specific property constraints in search solutions you may choose to build.

Important VSL constraints and operators may change in future releases. Solutions you build with hard-coded VSL strings may stop working as expected in future upgrades.

Document property constraints

Search constraints are listed in alphabetical order by view constraint syntax for quick reference.

Property Constraint	Constraint Syntax	Data Type
Composite property	{composite property name}.{custom property name}	Same as custom property data type
Custom property	<custom property name>	Same as custom property data type
Physical property	{physical file template}.{physical property name}	Same as physical property data type
Any document key	[anyDocKey]	Text
Approval User	[approvalUser]	User
Version control checkout comments	[checkoutComments]	Text
Version control checkout date	[checkoutDate]	Datetime
Version control checkout	[checkoutUser]	User

Property Constraint	Constraint Syntax	Data Type
user		
Creation date range	[createdWithin]	Number
Creation date	[creationDate]	Datetime
User who captured document	[creationUser]	User
Version control current version number	[currentVersion]	Number
Deletion date	[deletionDate]	Datetime
User who deleted document	[deletionUser]	User
Document ID	[docId]	Text
Document type	[docType]	Text
Drawer value	[drawer]	Text
Field1 value	[field1]	Text
Field2 value	[field2]	Text
Field3 value	[field3]	Text
Field4 value	[field4]	Text
Field5 value	[field5]	Text
ID of the folder the document is in	[folderId]	Text
Whether the document has a physical file reference	[hasPhysicalRef]	Flag
Whether the document has shortcuts in other folders	[hasShortcut]	Flag

Property Constraint	Constraint Syntax	Data Type
Retention hold	[holdName]	Text
Whether the document is checked out in version control	[isCheckedOut]	Flag
Whether the document is in workflow	[isInWf]	Flag
Whether the document is marked private in version control	[isPrivate]	Flag
Whether the document includes a digital signature	[isSigned]	Flag
Whether the document is in version control	[isUnderVersionCtrl]	Flag
Date document was last viewed	[lastViewDate]	Datetime
User who last viewed document	[lastViewUser]	User
Date document was last modified	[modDate]	Datetime
User who last modified document	[modUser]	User
Name of the document	[name]	Text
Date the next document task is due	[nextTaskDue]	Datetime
Document notes	[notes]	Text
Whether the document has a retention hold applied	[onHold]	Flag
Number of document pages	[pages]	Number

Property Constraint	Constraint Syntax	Data Type
User who marked the document private in version control	[privateUser]	User
Digital signature status	[sigStatus]	Status
Number of active tasks	[taskSummaryCountActive]	Number
Number of inactive tasks	[taskSummaryCountInactive]	Number
Status of tasks	[taskSummaryStatus]	Status
Workflow item ID	[wfItemId]	Text
Workflow queue	[wfQueue]	Text
Workflow status	[wfStatus]	Status
User who added document to workflow	[wfUser]	User

Project and folder property constraints

Search constraints are listed in alphabetical order by view constraint syntax for quick reference.

Property Constraint	Constraint Syntax	Data Type
Composite property	{composite property name}.{custom property name}	Same as custom property data type
Custom property	<custom property name>	Same as custom property data type
Creation date range	[createdWithin]	Number
Creation date	[creationDate]	Datetime
User who created the project	[creationUser]	User
Deletion date	[deletionDate]	Datetime

Property Constraint	Constraint Syntax	Data Type
User who deleted the project	[deletionUser]	User
The ID of the folder	[folderId]	Text
Whether the folder is active or inactive	[folderStatus]	Status
The folder's folder type	[folderType]	Text
Whether the project is in workflow	[isInWf]	Flag
Date the project was last modified	[modDate]	Datetime
User who last modified the project	[modUser]	User
Name of the folder	[name]	Text
Date the next task is due	[nextTaskdue]	Datetime
Whether the project has required document types	[requiredDocs]	Flag
Date the project status last changed	[statusDate]	Datetime
User who last changed the project status	[statusUser]	User
Number of active project tasks	[taskSummaryCountActive]	Number
Number of inactive project tasks	[taskSummaryCountInactive]	Number
Status of project task	[taskSummaryStatus]	Status
Workflow item ID	[wfItemId]	Text
Workflow queue	[wfQueue]	Text

Property Constraint	Constraint Syntax	Data Type
Workflow status	[wfStatus]	Status
User who added the project to workflow	[wfUser]	User

Folder content property constraints

Search constraints are listed in alphabetical order by view constraint syntax for quick reference.

Property Constraint	Constraint Syntax	Data Type
Composite property	{composite property name}.{custom property name}	Same as custom property data type
Custom property	<custom property name>	Same as custom property data type
Physical property	{physical file template}.{physical property name}	Same as physical property data type
The date and time the document, folder, or shortcut was added to the folder.	[addedToFolder]	Datetime
The number of days within which the document or folder was added to the folder.	[addedToFolderWithin]	Number
The date the document was checked out.	[checkoutDate]	Datetime
The user name of the user who checked out the document.	[checkoutUser]	User
Whether the content is a document, a folder, a document shortcut, or a folder shortcut.	[contentType]	Status
The number of days within which the content was created	[createdWithin]	Number

Property Constraint	Constraint Syntax	Data Type
The date and time the document, folder, or shortcut was created.	[creationDate]	Datetime
The user who created the document, folder, or shortcut.	[creationUser]	User
The unique ID of the document in the folder.	[docId]	Text
The document type of the document in the folder.	[docType]	Text
The drawer associated with the document, folder, or shortcut.	[drawer]	Text
The Field1 value for the document in the folder.	[field1]	Text
The Field2 value for the document in the folder.	[field2]	Text
The Field3 value for the document in the folder.	[field3]	Text
The Field4 value for the document in the folder.	[field4]	Text
The Field5 value for the document in the folder.	[field5]	Text
The unique ID of the folder.	[folderId]	Text
Whether the folder is active or inactive.	[folderStatus]	Status
The folder type of the folder.	[folderType]	Text
Whether the document in the folder has a physical file reference.	[hasPhysicalRef]	Flag

Property Constraint	Constraint Syntax	Data Type
Whether the folder is in workflow.	[isInWf]	Flag
Whether the document in the folder is marked private.	[isPrivate]	Flag
Whether the document in the folder is added to version control.	[isUnderVersionCtrl]	Flag
The date and time the document or folder was last viewed.	[lastViewDate]	Datetime
The user who last viewed the document or folder.	[lastViewUser]	User
The date and time the document or folder was last modified.	[modDate]	Datetime
The user who last modified the document or folder.	[modUser]	User
Name of the folder, document, or shortcut	[name]	Text
Whether the document in the folder has a direct or inherited retention hold.	[onHold]	Flag
The user who marked the document in the folder private.	[privateUser]	User
Whether the folder includes required document types.	[requiredTypes]	Flag
The status of the digital signature of the document in the folder.	[sigStatus]	Status
The date and time the status of the folder was last changed.	[statusDate]	Datetime

Property Constraint	Constraint Syntax	Data Type
The user who last changed the folder status.	[statusUser]	User
The workflow queue associated with the document or folder.	[wfQueue]	Text
The workflow status of the document or folder.	[wfStatus]	Status
The user who added the document or folder to workflow.	[wfUser]	User

Task property constraints

Search constraints are listed in alphabetical order by view constraint syntax for quick reference.

Property Constraint	Constraint Syntax	Data Type
User who assigned the task	[assignedBy]	User
User to whom the task is assigned	[assignedTo]	User
Date the task was assigned	[assignmentDate]	Datetime
Task comments	[comments]	Text
User who completed the task	[completedBy]	User
Date the task was completed	[completionDate]	Datetime
Task completion method	[completionMethod]	Status
The user who created the task	[createdBy]	User
The date the task was created	[creationDate]	Datetime
Number of days until the task is due	[daysUntilDue]	Number
Document ID	[docId]	Text

Property Constraint	Constraint Syntax	Data Type
Document name	[docName]	Text
Document type	[docType]	Text
Drawer value	[drawer]	Text
Date the task is due	[dueDate]	Datetime
Whether the task is expedited	[expedite]	Flag
Field1 value	[field1]	Text
Field2 value	[field2]	Text
Field3 value	[field3]	Text
Field4 value	[field4]	Text
Field5 value	[field5]	Text
ID of the folder	[folderId]	Text
Name of the folder	[folderName]	Text
The folder's folder type	[folderType]	Text
Whether the task has a due date	[hasDueDate]	Flag
Task instructions	[instructions]	Text
Whether the task creator is also the reviewer	[isCreatorReviewer]	Flag
Whether the task was skipped	[isSkipped]	Flag
Date the task was last modified	[lastModificationDate]	Datetime
User who last modified the task	[modifiedBy]	User
Date the task is obsolete	[obsoleteDate]	Datetime
Whether the task is obsolete	[obsolete]	Flag

Property Constraint	Constraint Syntax	Data Type
Date task was reviewed	[reviewDate]	Datetime
User who reviewed the task	[reviewedBy]	User
Task start date	[startDate]	Datetime
Task status	[status]	Status
Task ID	[taskId]	Text
Task type	[taskType]	Status
Task template name	[templateName]	Text

Workflow property constraints

Search constraints are listed in alphabetical order by view constraint syntax for quick reference.

Property Constraint	Constraint Syntax	Data Type
Composite property	{composite property name}.{custom property name}	Same as custom property data type
Custom property	<custom property name>	Same as custom property data type
Physical property	{physical file template}.{physical property name}	Same as physical property data type
Any document key	[anyDocKey]	Text
Document type	[docType]	Text
Drawer value	[drawer]	Text
Field1 value	[field1]	Text
Field2 value	[field2]	Text
Field3 value	[field3]	Text

Property Constraint	Constraint Syntax	Data Type
Field4 value	[field4]	Text
Field5 value	[field5]	Text
Whether the folder is active or inactive	[folderStatus]	Status
The folder's folder type	[folderType]	Text
Document or folder name	[name]	Text
Whether the folder has required document types	[requiredDocs]	Flag
Document creation date range	[wfDocCreatedWithin]	Number
Document creation date	[wfDocCreationDate]	Datetime
Folder creation date range	[wfFolderCreatedWithin]	Number
Folder creation date	[wfFolderCreationDate]	Datetime
Workflow item creation date range	[wfItemCreatedWithin]	Number
Workflow item creation date	[wfItemCreationDate]	Datetime
Workflow item ID	[wfItemId]	Text
Workflow item type	[wfItemType]	Status
Date item entered workflow queue	[wfQueueStartTime]	Datetime
Workflow queue	[wfQueue]	Text
Date item status last changed	[wfStateStartTime]	Datetime
Workflow status	[wfStatus]	Status
Workflow queue entry date	[wfTimeInQueue]	Number

Property Constraint	Constraint Syntax	Data Type
range		
Workflow status date range	[wfTimeInStatus]	Number
User who added the item to workflow	[wfUser]	User

VSL statement syntax

The VSL statement syntax tables list the supported operators and value components for use when running a view in Perceptive Content. You can reference the tables to determine the VSL text that is applicable for the specific data type used in the Perceptive Content area where you may choose to build a search solution.

Important VSL constraints and operators may change in future releases. Solutions you build with hard-coded VSL strings may stop working as expected when future upgrades are introduced.

Important When you run a statement that uses the **contains**, **does not contain**, **ends with**, or **does not end with** operator, it can slow Perceptive Contentserver performance, depending on the volume of documents.

Text data type

Supported operators	Operator Syntax	Example
is equal to	=	[field1] = 'invoice'
is not equal to	!=	[field1] != 'invoice'
is less than	<	[field1] < 'zyx'
is greater than	>	[field1] > 'abc'
is less than or equal to	<=	[field1] <= 'zyx'
is greater than or equal to	>=	[field1] >= 'abc'
starts with	startswith	[field1] startswith 'a'
does not start with	doesNotStartWith	[field1] doesNotStartWith 'a'
ends with	endswith	[field1] endswith 'a'

Supported operators	Operator Syntax	Example
does not end	doesNotEndWith	[field1]
contains	contains	[field1] contains 'a'
does not contain	doesNotContain	[field1] doesNotContain 'a'
is blank	= $NULL	[field1] = $NULL
is not blank	!= $NULL	[field1] != $NULL
is one of	in	[field1] in 'ab0x07cd' where 0x07 is a placeholder for the seventh character in the ASCII table and ab and cd are the values you want to search for
is not one of	notIn	[field1] notIn 'ab0x07cd' where 0x07 is a placeholder for the seventh character in the ASCII table and ab and cd are the values you want to search for
is between	between	[field1] between 'ab0x07xy' where 0x07 is a placeholder for the seventh character in the ASCII table and ab and xy are the values you want to search for
is not between	notBetween	[field1] notBetween 'ab0x07xy' where 0x07 is a placeholder for the seventh character in the ASCII table and ab and xy are the values you want to search for

Number data type

Supported operators	Operator Syntax	Example
is equal to	=	[pages] = '5'
is not equal to	!=	[pages] != '5'

Supported operators	Operator Syntax	Example
is less than	<	[pages] < '5'
is greater than	>	[pages] > '5'
is less than or equal to	<=	[pages] <= '5'
is greater than or equal to	>=	[pages] >= '5'
is one of	in	[pages] in '10x072' where 0x07 is a placeholder for the seventh character in the ASCII table and 1 and 2 are the values you want to search for
is not one of	notIn	[pages] notIn '10x072' where 0x07 is a placeholder for the seventh character in the ASCII table and 1 and 2 are the values you want to search for
is between	between	[pages] between '10x072' where 0x07 is a placeholder for the seventh character in the ASCII table and 1 and 2 are the values you want to search for
is not between	notBetween	[pages] notBetween '10x072' where 0x07 is a placeholder for the seventh character in the ASCII table and 1 and 2 are the values you want to search for

Datetime data type

Supported operators	Operator Syntax	Example
is equal to	=	[creationDate] = '2010-10-03 20:10:16.123'
is not equal to	!=	[creationDate] != '2010-10-03 20:10:16.123'

Supported operators	Operator Syntax	Example
is less than	<	[creationDate] < '2010-10-03 20:10:16.123'
is greater than	>	[creationDate] > '2010-10-03 20:10:16.123'
is less than or equal to	<=	[creationDate] <= '2010-10-03 20:10:16.123'
is greater than or equal to	>=	[creationDate] >= '2010-10-03 20:10:16.123'
is one of	in	[creationDate] in '2010-10-03 20:10:16.1230x072010-10-09 11.01.05.123' where 0x07 is a placeholder for the seventh character in the ASCII table and 2010-10-03 20:10:16.123 and 2010-10-09 11.01.05.123 are the values you want to search for
is not one of	notIn	[creationDate] notIn '2010-10-03 20:10:16.1230x072010-10-09 11.01.05.123' where 0x07 is a placeholder for the seventh character in the ASCII table and 2010-10-03 20:10:16.123 and 2010-10-09 11.01.05.123 are the values you want to search for
is between	between	[creationDate] between '2010-10-03 20:10:16.1230x072010-10-09 11.01.05.123' where 0x07 is a placeholder for the seventh character in the ASCII table and 2010-10-03 20:10:16.123 and 2010-10-09 11.01.05.123 are the values you want to search for
is not between	notBetween	[creationDate] notBetween '2010-10-03 20:10:16.1230x072010-10-09 11.01.05.123' where 0x07 is a placeholder for the seventh character in

Supported operators	Operator Syntax	Example
		the ASCII table and 2010-10-03 20:10:16.123 and 2010-10-09 11.01.05.123 are the values you want to search for

User data type

Supported operators	Operator Syntax	Example
is equal to	=	[creationUser] = 'jsmith'
is not equal to	!=	[creationUser] != 'jsmith'
starts with	startswith	[creationUser] startswith 'j'
does not start with	doesNotStartWith	[creationUser] doesNotStartWith 'j'
ends with	endswith	[creationUser] endswith 'smith'
is blank	= $NULL	[creationUser] = $NULL
is not blank	!= $NULL	[creationUser] != $NULL
is one of	in	[creationUser] in 'jsmith0x07asmith' where 0x07 is a placeholder for the seventh character in the ASCII table and asmith and jsmith are the values you want to search for
is not one of	notIn	[creationUser] notIn 'asmith0x07jsmith' where 0x07 is a placeholder for the seventh character in the ASCII table and asmith and jsmith are the values you want to search for

Flag data type

Supported operators	Operator Syntax	Example
is equal to	=	[isInWf] = '0' where 0 is false and 1 is true
is not equal to	!=	[isInWf] != '1' where 0 is false and 1 is true

List data type

Supported operators	Operator Syntax	Example
is equal to	=	{List custom property name} = 'Vendor'
is not equal to	!=	{List custom property name} != 'Vendor'
is blank	= $NULL	{List custom property name} = $NULL
is not blank	!= $NULL	{List custom property name} != $NULL
is one of	in	{List custom property name} in 'Tier10x07Tier2' where0x07is a placeholder for the seventh character in the ASCII table andTier1andTier2are the values you want to search for
is not one of	notIn	{List custom property name} notIn 'Tier10x07Tier2' where0x07is a placeholder for the seventh character in the ASCII table andTier1andTier2are the values you want to search for

Status data type

Supported operators	Operator Syntax	Example
is equal to	=	[wfStatus] = '1'
is not equal to	!=	[wfStatus] != '1'
is blank	= $NULL	[wfStatus] = $NULL
is not blank	!= $NULL	[wfStatus] != $NULL

Manage users groups

Manager roles

What is a Perceptive Manager?

A Perceptive Manager is a specialized type of user who can create other users, assign Global privileges to other users, create and configure departments, and promote other users to the Department Manager role.

Perceptive Managers administer two general aspects of the system that are inaccessible to other users. The first is the ability to manage the entire pool of global users. Perceptive Managers create all users in the system, regardless of department. Perceptive Managers can assign user and group privileges in the Global privilege category and remove users from the system. A Perceptive Manager cannot assign his or her own privileges, nor can a Perceptive Manager remove other Perceptive Managers from the system.

A Perceptive Manager also controls the department configuration for the system. Perceptive Managers are the only users that create the departments in the system, modify the department name and displayed information, create and modify department labels, promote a user to the Department Manager role, and demote a user from being a Department Manager.

When you promote a user to the Perceptive Manager role, that user is assigned the security privileges in the Global Manage category automatically, with the exception of the Reports privilege.

By default, Perceptive Managers can migrate components and subcomponents within Perceptive Content between different environments.

The first Perceptive Manager in the system is created during the installation process. You can create subsequent Perceptive Managers with an INTool command. To promote a user to the Perceptive Manager role, you must be a Perceptive Manager. A user can be a Perceptive Manager and a Department Manager simultaneously.

Promote a user to Perceptive Manager

To promote a user to Perceptive Manager, complete the following steps.

Prerequisite To promote a user to Perceptive Manager, you must first be a Perceptive Manager.

1. On the **ImageNow Server** computer, complete one of the following actions.
   - In Windows 32-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following command: `intool --cmd promote-perceptive-manager --username <user name> --login-user <login name> --login-password <login password>`

Note: If there is no match for the user name entered in the argument, the system prompts you to

create a Perceptive Manager user with the provided user name.

3. In Windows, when you receive a confirmation message, close the **Command Prompt** window.

What is a Department Manager?

A Department Manager is a user role with privileges to perform any administrative action in its respective department. Only a Perceptive Manager can promote a user to the Department Manager role.

A Department Manager has access to all forms of content within his or her department other than content protected by access control markings. The Department Manager is automatically granted all privileges in the system for the assigned department other than privileges in the Global privilege category. Department Managers are also the only user role who can share objects defined in Management Console in the manager s department with other departments.

Department Managers assign department-level privileges to users and can determine what types of content to share with other departments. Department Managers can manage, migrate, and share several items in their department, including drawers, groups, application plans, and workflow processes. However, Department Managers cannot administer settings found in the Cross Department Settings area of Management Console without additional privileges. These settings include audit profiles, Business Insight reports, and digital signature certificates.

Department Managers are the only users able to move items between departments on the same system. A move operation requires one Department Manager to send the move package from their department and another Department Manager from the destination department to accept the move package into their department.

A user can be a Department Manager for any number of departments. A Perceptive Manager can be a Department Manager simultaneously. You can have multiple Department Managers for a single department in the system.

Promote a user to Department Manager

Department Managers administer privileges at the department level to users and groups and have the ability to perform any function in Management Console for their own department. To promote a user to the Department Manager role, complete the following steps.

Prerequisite You must be a Perceptive Manager to complete this procedure.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, select **Departments**.
3. In the right pane, complete one of the following steps.

Situation	Steps
Promote a user to Department Manager for a	1. Click the **New** button.

Situation	Steps
new department	2. On the **General** tab, enter text in the required **Name** and **Department Label** boxes for the new department.
Promote a user to Department Manager for an existing department	1. Select the department to modify. 2. Click the **Modify** button.

4. On the **Department Managers** tab, click the **Add** button.
5. In the **Select Users** dialog box, in the **Search for users** box, type all or part of the user name you want to add as a Department Manager and click **Search**.
6. Select the user from the search results list and click **Add**.
7. Click **OK**.

Demote a Department Manager

To demote a user from the Department Manager role, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, select **Departments**.
3. In the right pane, select the Department Manager s department and click the **Modify** button.
4. On the **Department Managers** tab, select the Department Manager you want to demote from the list and click **Remove**.
5. Click **OK**.

Users

About copying security attributes of users and groups

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process.

Security attributes include privilege sets, user or group memberships, access control markings, and audit template assignments.

If you have a user or group that has the same security attributes you need for another user or group you already created, you can copy the security attributes of the source user or group to the destination user or group. The copy process does not create a new user or group.

You can copy attributes within a department or in a cross department setting. You can only copy security attributes for which you have management privileges and to which you have access. You must have Administer User privileges for user privileges you are copying. You must have Administer Group privileges for group privileges you are copying.

You can only copy a group membership to a group in your own department. You cannot copy a group membership to a group that has only been shared with your department.

Import users from a local computer

To import users from a local computer, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, on the **User Profiles** tab, click **Import**.
4. In the **Import Users** page, click **Local Machine** and then click **Next**.
5. In the next page, select the check boxes for the users you want to import and click **Next**.
6. In the next page, select any groups to which you want to add the users and click **Finish**.

Remove a user from a group

To remove a user from a group, complete the following steps.

You cannot remove a user from a group that has been shared to your department. You must remove users from a group in the department where the group resides.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Groups**.
3. In the right pane, in the **Search for groups in this department** box, type all or some of a group name, and then click **Search**.
4. In the **Select a group** list, select a group, and then click **Modify**.
5. In the **Modify Group Properties** dialog box, in the left pane, click **Group Members**.
6. In the right pane, in the **Group Members** list, perform the following substeps.
    1. Select a user and click **Remove**.
    2. To confirm the removal, click **Yes**, and then click **OK**.

Security attribute duplication within a department

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process. The copy process does not create new users or groups. The copy user feature does not copy any user information, such as personal or contact information.

You can copy the following security attributes within a department.

- Access Control Markings
- Annotation Template Privileges
- Application Plan Privileges
- Capture Profile Privileges
- Connection Type Privileges
- Department Privileges
- Document Type Privileges
- Document View Privileges
- Drawer Privileges
- File Plan Privileges
- Folder Type Privileges
- Folder View Privileges
- Forms Privileges
- Group Memberships
- Output Profile Privileges
- Record Category Privileges
- Record Category Type Privileges
- Record Folder Privileges
- Record Folder Type Privileges
- Record Folder View Privileges
- Record Type Privileges
- Record View Privileges
- Retention Hold Privileges
- Source Profile Privileges
- Task Template Privileges
- Workflow Privileges

Rename a user

To modify the user name for a user in the client, complete the following steps. You cannot rename a Perceptive Manager until you demote the user from that role.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, in the **Search for users** box, type all or some of a user name, first name, or last name and click **Search**.
4. In the **Select a user** list, select a user and click **Modify**.
5. In the **Modify User Profile** dialog box, on the **User Account** tab, in the **User Name** field, type the new user name and click **OK**.

Next If your Perceptive Content accounts correspond to a system account, LDAP account, or other SSO option, make sure you update the user name in all required locations. If not, Perceptive Content will not provide the user with access to Perceptive Content functionality. Authenticating users at the system level is required to validate user names and passwords.

Import users from a domain

To import users from a domain, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, on the **User Profiles** tab, click **Import**.
4. In the **Import Users** page, click **Domain** and click **Next**.
5. In the next page, select the check boxes for the users you want to import and click **Next**.
6. In the next page, select any groups you want to add the users to and click **Finish**.

Change a user's active status

To make a user inactive or to reactivate a user, complete the following steps. You cannot change a Perceptive Manager s active status.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, in the **Search for users** box, type all or some of a user name, first or last name, and click **Search**.
4. In the **Select a user** list, select a user and click **Modify**.
5. In the **Modify User Profile** dialog box, in the left pane, select **User Account** if not already selected.
6. In the right pane, select the **Is Active** check box to enable the user to log in to **Perceptive Content** or clear the **Is Active** check box to temporarily prevent the user from logging in.
7. Click **OK**.

Import users from LDAP

To create new Perceptive Content users by importing them from an LDAP server, complete the following steps.

1. **Set up SSL on the ImageNow Client**
2. In the right pane, on the **User Profiles** tab, click **Import**.
3. In the **Import Users** page, select **LDAP** and click **Next**.
4. In the next page, under **LDAP**, do the following substeps:
    1. Type the **Host Name** and **Port** for the LDAP server.
    2. Select the **Connect as Anonymous** check box to allow anonymous logon.

3. Enter the **User Name** and **Password** for the LDAP server.
4. Click **Next**.
5. In the next page, select the user group you want to import from the tree control and click **Next**.
6. In the next page, select the check boxes for the users you want to import and click **Next**.
7. In the next page, select any groups to which you want to add the users and click **Finish**.

Delete a user

You can disable a user by making the user inactive, or you can permanently delete the user. You cannot delete a Perceptive Manager until you demote the user from that role. To delete a user, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, select **Users**.
3. In the right pane, under **Select a user**, select a user and click **Delete**.
4. In the confirmation dialog box, click **Yes**.

Import users from a file

You can import users from a single text file, where the user names are separated by carriage returns. To import users from a file, complete the following steps.

If a user profile with a user name from the text file does not exist in Perceptive Content, the group privileges are assigned to the user profile that is created. However, if a user profile with the user name from the text file already exists in Perceptive Content, then the group privileges are not assigned to the user profile.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, on the **User Profiles** tab, click **Import**.
4. In the **Import Users** page, click **File** and then click **Next**.
5. In the **File Selection** dialog box, navigate to the text file that contains your user list and click **Open**.
6. In the **Import Users** page, complete the following substeps:
    1. In the **Delimiter** list, select the delimiter you want.
    2. Optional. Select the **Ignore first** check box, and in the rows of input file list, select the number of rows you want to ignore.
    3. Click **Next**.
    4. In the next page, select any groups to which you want to add the users and then click **Finish**.

Add a user to a group

To add a user to a group, complete one of the following procedures.

You cannot add a user to a group that has been shared to your department. You must add users to a group in the department where the group resides.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Groups**.
3. In the right pane, select a group and click **Modify**.
4. In the **Modify Group Properties** dialog box, in the left pane, click **Group Members**.
5. In the right pane, under **Group Members**, select one or more users and click **Add**.
6. In the **Select Users** dialog box, type all or some of a user name and click **Search**.
7. Under **Search results**, select a user and click **Add**.
8. Click **OK** until you return to the **Management Console** window.

Security attribute duplication in a cross department setting

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process. The copy process does not create new users or groups. The copy user feature does not copy any user information, such as personal or contact information.

You can copy the following security attributes in a cross department setting.

- Audit Templates
- Batch Users
- BI Privileges
- Capture Privileges
- ERM Search Privileges
- Global Management Privileges
- Interact Search Privileges
- Task View Privileges

Promote a user to Perceptive Manager

To promote a user to Perceptive Manager, complete the following steps.

Prerequisite To promote a user to Perceptive Manager, you must first be a Perceptive Manager.

1. On the **ImageNow Server** computer, complete one of the following actions.
   - In Windows 32-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin* directory.
   - In Windows 64-bit, open a **Command Prompt** window and change to the *[drive:]\inserver\bin64* directory.
   - In UNIX, change to the *$(IMAGENOWDIR)/bin* directory.
2. Enter the following command: `intool --cmd promote-perceptive-manager --username <user name> --login-user <login name> --login-password <login password>`

   Note: If there is no match for the user name entered in the argument, the system prompts you to

create a Perceptive Manager user with the provided user name.

3. In Windows, when you receive a confirmation message, close the **Command Prompt** window.

Groups

Security attribute duplication in a cross department setting

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process. The copy process does not create new users or groups. The copy user feature does not copy any user information, such as personal or contact information.

You can copy the following security attributes in a cross department setting.

- Audit Templates
- Batch Users
- BI Privileges
- Capture Privileges
- ERM Search Privileges
- Global Management Privileges
- Interact Search Privileges
- Task View Privileges

Create a group

To add a new group for users with shared privileges, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Groups**.
3. In the right pane, click **New**.
4. In the **New group** dialog box, in the **Name** field, type a name for the group.
5. Optional. In the **Description** field, type a description for the group.
6. Optional. To prevent the new group from being displayed in any list in **Cross Department Settings**, deselect the **Display this group in Cross Department Settings** check box.

   Note: If you hide the group in Cross Department Settings, you cannot assign the group global settings and instance-level privileges.

7. Type a group name and press `ENTER`.

Delete a group

To delete a user group from Management Console, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Groups**.
3. In the right pane, in the **Search for groups** box, type all or some of a group name, and then click **Search**.
4. In the **Select a group** list, select a group and click **Delete**.
5. In the confirmation dialog box, click **Yes**.

Result Deleting a group does not delete the users assigned to it.

Security attribute duplication within a department

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process. The copy process does not create new users or groups. The copy user feature does not copy any user information, such as personal or contact information.

You can copy the following security attributes within a department.

- Access Control Markings
- Annotation Template Privileges
- Application Plan Privileges
- Capture Profile Privileges
- Connection Type Privileges
- Department Privileges
- Document Type Privileges
- Document View Privileges
- Drawer Privileges
- File Plan Privileges
- Folder Type Privileges
- Folder View Privileges
- Forms Privileges
- Group Memberships
- Output Profile Privileges
- Record Category Privileges
- Record Category Type Privileges
- Record Folder Privileges
- Record Folder Type Privileges
- Record Folder View Privileges

- Record Type Privileges
- Record View Privileges
- Retention Hold Privileges
- Source Profile Privileges
- Task Template Privileges
- Workflow Privileges

What is a group?

Groups streamline the task of assigning standard sets of privileges to large numbers of users and other processes in Perceptive Content.

You can design the Perceptive Content security model by setting up groups and establishing their roles and privileges for security. You can also create different groups for different types of users, and assign both global privileges and department privileges at the group level instead of at the user level. For example, you can create a group and add those users who need access to a particular drawer, or add a privilege to a group of users to only scan but not to copy or move items.

Using groups for the majority of work in assigning privileges cuts down on system administration work and reduces privilege confusion. You can make exceptions for a particular user by denying a privilege at the user level, because the user level privilege overrides the group level privilege. For example, you can deny the Delete privilege for a user at the user level but still allow the user to perform other functions assigned at the group level.

A group can contain multiple users so you can track the actions taken by the users in Perceptive Content for troubleshooting and auditing purposes. You can group queues in Workflow to automate business processes. After an item is saved in Perceptive Content, the item can be routed through any number of queues, which can be grouped by different departments or different desks within a department.

You can add groups of users to task templates for such things as pointer tasks, email notifications, and required signatures.

You can choose to display or hide a group in any Cross Department Settings list. When you hide a group from Cross Department Settings, the system removes any global settings and instance-level privileges that were previously assigned to the group. You cannot assign global settings and instance-level privileges to a hidden group.

As a security measure, if you are a member of a group, you cannot modify that group s assigned privileges and members, and the group does not appear in dialog boxes where you perform these actions in Management Console. We recommend that you use a separate user or manager account to set up groups so you can view all groups simultaneously.

About copying security attributes of users and groups

You can copy the security attributes of users and groups to additional users and groups that you create. This feature can save you time and simplify the security set-up process.

Security attributes include privilege sets, user or group memberships, access control markings, and audit template assignments.

If you have a user or group that has the same security attributes you need for another user or group you already created, you can copy the security attributes of the source user or group to the destination user or group. The copy process does not create a new user or group.

You can copy attributes within a department or in a cross department setting. You can only copy security attributes for which you have management privileges and to which you have access. You must have Administer User privileges for user privileges you are copying. You must have Administer Group privileges for group privileges you are copying.

You can only copy a group membership to a group in your own department. You cannot copy a group membership to a group that has only been shared with your department.

Modify a group

To modify a group s name, description, assigned privileges, or group members, complete the following steps.

Other than modifying group privileges, you cannot modify a group that has been shared to your department. You must modify a group in the department where the group resides.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Groups**.
3. In the right pane, select a group and click **Modify**.
4. In the **Modify Group Properties** dialog box, complete one of the following procedures.

Situation	Steps
Modify group information	1. In the left pane, select the **Group Information** tab. 2. Modify the text in the **Name** and **Description** fields.
Hide the group in Cross Department Settings	1. In the left pane, select the **Group Information** tab. 2. In the right pane, deselect the **Display this group in Cross Department Settings** check box. This action removes any global privileges assigned to the group.
Add or remove group members	1. In the left pane, select the **Group Members** pane. 2. In the right pane, click the **Add** button to add existing users to the group. 3. To remove a user from the group, select a user from the **Group Members** list and click **Remove**.
Assign department level group privileges	1. In the left pane, expand **Privileges** and select a privilege category. 2. In the right pane, modify the privileges as needed.

5. Click **OK**.

Out of Office

What is Out of Office?

You use Out of Office to notify that a user is unavailable to process items.

Your administrator can create and manage reasons for the Out of Office feature, and create, modify, and disable an Out of Office event on behalf of someone else.

> For example, when a user's status is set to out of office using an Out of Office event, items normally routed to the user can be routed to an appropriate alternate queue when a workflow rule that defines the routing is in place.

Your administrator can also designate a delegate who can perform task actions for another user while an out of office event is active.

Create an Out of Office event

To create an Out of Office event, complete the following steps.

1. On the **Perceptive Content** toolbar, on the **Settings** menu, click **Out of Office**.
2. In the **Out of Office New Event** dialog box, specify the following information for your Out of Office event.
   - In the **Begin date** box, specify the date and time you want your Out of Office event to start. The default begin date is the current date and time.
   - In the **End date** box, specify the date and time you want your Out of Office event to end, or leave the box blank if you do not know the end date.

     Note:
     If you leave the box blank, you must disable the event to begin processing items again.

   - In the **Reason** box, select the reason for your Out of Office event.
   - Optional. In the **Delegate User** box, select the user who will serve as the delegate task assignee.
   - Optional. In the **Comments** box, enter any comments about the Out of Office event.
3. Click **OK**.

Create a user's Out of Office event

To create a user s Out of Office event, complete the following steps.

1. In the **Management Console**, in the left pane, click **Users**.
2. In the right pane, click the **User Profiles** tab.
3. In the **Search for users** box, type the name of the user you want to add and then click **Search**.
4. Under **Select a user**, select the appropriate user and then click **Modify**.
5. In the **Modify User Profile** dialog box, click the **Out of Office** pane, and then click **Add**.
6. On the **Out of Office New Event** dialog box, complete the following substeps.

1. In the **Begin date** box, specify the date and time you want your Out of Office event to start. The default begin date is the current date and time.
2. In the **End date** box, specify the date and time you want the users Out of Office event to end or leave the box blank if you do not know the end date.

   Note: If you leave the box blank, you or the user must disable the event to begin processing items again.

3. In the **Reason** box, select the reason for your Out of Office event.
4. Optional. In the **Delegate User** box, select the user who will serve as the delegate task assignee.
5. Optional. In the **Comments** box, enter any comments about the Out of Office event.

7. Click **OK**.

Disable a user's Out of Office event

To disable an ongoing Out of Office event, complete the following steps.

1. In **Management Console**, in the left pane, click **Users**.
2. In the right pane, on the **User Profiles** tab, complete the following substeps:
   1. In the **Search for users** box, type the name of the user you want to find and click **Search**.
   2. Under **Select a user**, select the appropriate user and click **Modify**.
3. In the **Modify User Profile** dialog box, complete the following substeps:
   1. In the left pane, click **Out of Office**.
   2. In the right pane, select the Out of Office event you want to disable and click **Disable**.
4. In the confirmation dialog box, click **Yes**.

Disable an Out of Office event

To disable an Out of Office event, complete the following steps.

1. On the **Perceptive Content** toolbar, click **Settings > Out of Office**.
2. On the **Out of Office - Modify Event** dialog box, click **Disable**, and then click **Yes**.

Modify a reason for Out of Office

To make changes to the text detailing a reason for Out of Office, complete the following steps.

1. In the **Management Console**, in the left pane, click **Out of Office**.
2. In the right pane, click the **Reasons** tab.
3. Select the reason, click **Modify**, and then type the new text.
4. Press ENTER.

View a user's Out of Office event

To open a user's Out of Office event for review, complete the following steps.

1. In the **Management Console**, in the left pane, click **Users**.
2. In the right pane, click the **User Profiles** tab.
3. In the **Search for users** box, type the name of the user you want to add, and then click **Search**.
4. Under **Select a user**, select the appropriate user, and then click **Modify**.
5. In the **Modify User Profile** dialog box, click the **Out of Office** pane.
6. In the right pane, select the out of office event you want to view, and then click **Details**.
7. When you are finished reviewing the out of office event, click **OK**.

Assign privileges

About assigning privileges

Privileges determine whether a group or user has access to a specific action in Perceptive Content.

Perceptive Managers, Department Managers, and users with privileges that enable privilege management can adjust privileges for users and groups. Perceptive Managers can assign any global privilege, while Department Managers assign privileges that only apply in the context of the department they manage.

Managers adjust privileges for users and groups using the following three methods: grant a privilege by allowing it, revoke a privilege by denying it, or choose not to set a privilege assignment at all. A user's effective privileges are always evaluated and displayed at the user level, not at the group level. To determine the effective privileges, Perceptive Content evaluates all of the privilege assignments given to a user and all of the privilege assignments (if any) the user has inherited from groups to which the user is a member. Perceptive Content then determines which privilege assignments get priority over other privilege assignments.

In some cases, you grant privileges to groups of users who need similar privileges. However, certain users may need specific privileges. For example, you can grant a user the ability to delete documents in a specific drawer regardless of the privileges set for groups in which the user is a member. Because this is a privilege granted to a user, it overrides any privileges assigned at the group level.

Users cannot view or modify their own assigned privileges. Users cannot assign privileges to any group for which they are a group member, with the exception of the All Users group. Users also cannot add themselves to a group or remove themselves from a group.

To assign global settings and instance-level privileges to a group in Management Console, the group must be set to display in Cross Department Settings. You cannot assign global settings and instance-level privileges to a hidden group. When you hide a group from Cross Department Settings, the system removes any global settings and instance-level privileges to the group that were previously assigned to the group.

What is the privilege hierarchy?

Perceptive Content evaluates all privilege assignments at the user level.

When user privileges and group privileges are different or when a user belongs to several groups in which the privilege assignments differ, Perceptive Content applies privilege hierarchy rules to resolve the privilege. User privileges are higher priority than group privileges, and deny privileges are higher priority than allow privileges.

The following examples show how the privilege hierarchy works.

User privileges oppose privileges inherited from a group. For example, you grant a user the privilege to delete items. Additionally, the HR group, to which the user belongs, is denied the ability to delete items. As a member of the HR group, this user inherits the deny privilege. While the user can delete items; at the group level, the user cannot delete items. Perceptive Content uses privilege hierarchy rules to determine whether the user can delete an item. Since user level privileges override group level privileges, the user can delete items.

Another area where privilege assignment evaluations occur is at the group level. Group privileges oppose privileges from another group. In this case, the user belongs to two groups. In the HR group, the user is denied the ability to delete items. In the HR_Records group, the user inherits the ability to delete items at the group level. So, one group allows the privilege and another group denies the privilege. Because the deny privilege overrides the allow privilege within the same group level, the user is denied the ability to delete items.

Additional resolutions. When a user is a member of multiple groups where a privilege is allowed or denied in one group and not assigned in any other group, the user's effective privilege is the allowed or denied privilege. In addition, if a privilege is not specifically assigned, the user cannot perform the function.

Remove management privileges

To remove privileges for one or more management functions, complete the following steps.

1. In the **Management Console**, in the left pane, click **Users**.
2. In the right pane, on the **Security** tab, perform one of the following substeps.
    1. In the **Select a user** list, select a user, and then click **Modify**.
    2. In the **Search for users**box, type all or some of a user name, first or last name, and then click **Search**. In the **Select a user** list, select a user, and then click **Modify**. To sort the **Select a user** list in ascending or descending order, click the **Name**, **Last Name**, **First Name**, or **Status** column headers.
3. In the **Security Settings** dialog box, click the **Global Privileges** pane.
4. In the **Privileges** list, perform one of the following substeps.
    1. To remove all management privileges, click the column in front of the **Manage privilege** group until appears in front of the group.
    2. To remove specific management privileges, click the column in front of each privilege in the **Manage group** until appears.

5. Click **OK**.

Assign user access to ERM report documents

To assign user access to ERM report documents, complete the following steps.

This feature assumes that when the report template for each report was created in Perceptive Content ERM Studio, the Report Name index was always mapped to the Perceptive Content Drawer document key.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Drawers**.
3. In the right pane, click **New**. Create a drawer for each report that appears in the **Report Name** list in **ERM** view. The drawer names must match the report names exactly.
4. In the left pane, click **Groups**. In the right pane, click **New**. Create a group for each category of reports that will be viewable by all members of that group. For example, a group called Invoice Reports would grant access to reports that contain invoices. If you want to limit user access to a single report, create a separate group for just that report.
5. For each report group created in the previous step, perform the following substeps.
    1. In the right pane, in the **Select a group** list, select a group and then click **Modify**.
    2. In the **Modify Group Properties** dialog box, in the left pane, expand **Privileges** and click **Drawer Privileges**.
    3. In the **Privileges** list, under **Documents**, to grant the privileges needed to access **ERM** report documents, click the column to the left of **Search** until the **Grant** icon appears.
6. Repeat the previous substeps for any other groups that must have access to **ERM** reports and then click **OK**.
7. In the left pane, under **Select Department**, select **Cross Department Settings**.
8. In the left pane, click **Groups**.
9. In the right pane, complete the following substeps for every group that must have access to ERM reports.
    1. In the right pane, in the **Select a group** list, select a group and then click **Modify**.
    2. In the **Modify Group Properties** dialog box, in the left pane, click **Global Privileges**.
    3. In the right pane, under **Search**, assign every privilege with **ERM** in its title.
    4. Click **OK**.
10. For every user who needs **ERM** report privileges, complete the following substeps.
    1. In the left pane, under **Select Department**, select a department from the list.
    2. In the left pane, click **Users**.
    3. In the right pane, in the **Search for users** box, type all or some of a user name, and then click **Search**. In the **Select a user** list, select a user and then click **Modify**.
    4. In the **Modify User Profile** dialog box, in the left pane, expand **Privileges** and click **Drawer Privileges**.
    5. In the **Privileges** list, under **Documents**, to grant the privileges needed to access **ERM** report

documents, click the column to the left of **Search** until the **Grant** icon appears.

6. Click **OK**.

11. In the left pane, under **Select Department**, select **Cross Department Settings**.
12. In the left pane, click **Users**.
13. In the right pane, complete the following substeps for every user that must have access to **ERM** reports.
    1. In the right pane, in the **Select a user** list, select a group and then click **Modify**.
    2. In the **Modify User Profile** dialog box, in the left pane, click **Global Privileges**.
    3. In the right pane, under **Search**, assign every privilege with **ERM** in its title.
    4. Click **OK**.

Restrict a user from a specific function

Use this procedure to restrict a user from performing a particular function even if the user is made a member of a group that allows that function. For example, if the deny privilege is assigned at the user level for a drawer, and that user is assigned to a group that allows access to the drawer, the user level privilege overrides the group level privilege and prevents the user from inheriting the allow privilege. To restrict a user from performing a specific function in a department, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Users**.
3. In the right pane, in the **Search for users** box, type all or some of a user name and click **Search**.
4. In the **Select a user** list, select a user and click **Modify**.
5. In the **Modify User Profile** dialog box, complete the following substeps.
    1. In the left pane, expand **Privileges** and select the privilege category that applies to the function you want to deny the user.
    2. To deny a privilege, under **Privileges**, click the column in front of the privilege until the **Deny** icon appears.
    3. Optional. To save and display the user's effective privileges so you can verify or modify them before closing this dialog box, click **Apply**.
    4. Click **OK**.

View privileges for a user

Both group privileges and privileges directly assigned to a user determine a user s capabilities in Perceptive Content. To view a user's effective privileges, complete the following steps.

1. In **Management Console**, complete one of the following procedures.

Situation	Steps
View department privileges for a user	1. In the left pane, under **Select Department**, select a department from the list. 2. In the left pane, click **Users**. 3. In the right pane, in the **Search for Users** box, type all or some of a user name, and then click **Search**. 4. In the **Select a user** list, select a user, and then click **Modify**. 5. In the **Modify User Profile** dialog box, in the left pane, expand **Privileges** and click any privilege category. 6. View the effective privileges for that user. 7. Click **OK**.
View global privileges for a user	1. In the left pane, under **Select Department**, select **Cross Department Settings** from the list. 2. In the left pane, click **Users**. 3. In the right pane, in the **Search for users** box, type all or some of a user name, and then click **Search**. 4. In the **Select a user** list, select a group, and then click **Modify**. 5. In the **Modify User Profile** dialog box, in the left pane, select **Global Privileges**. 6. View the effective privileges for that user. 7. Click **OK**.
View department privileges for a group	1. In the left pane, under **Select Department**, select a department from the list. 2. In the left pane, click **Groups**. 3. In the right pane, in the **Search for groups** box, type all or some of a group name, and then click **Search**. 4. In the **Select a group** list, select a group, and then click **Modify**. 5. In the **Modify Group Properties** dialog box, in the left pane, expand **Privileges** and

Situation	Steps
	click any privilege category. 6. View the effective privileges for that group. 7. Click **OK**.
View global privileges for a group	1. In the left pane, under **Select Department**, select **Cross Department Settings** from the list. 2. In the left pane, click **Groups**. 3. In the right pane, in the **Search for groups** box, type all or some of a group name, and then click **Search**. 4. In the **Select a group** list, select a group, and then click **Modify**. 5. In the **Modify Group Properties** dialog box, in the left pane, select **Global Privileges**. 6. View the effective privileges for that group. 7. Click **OK**.

View privileges for a group

To view a group's privileges, complete the following steps.

1. In **Management Console**, complete one of the following procedures.

Situation	Steps
View department privileges for a group	1. In the left pane, under **Select Department**, select a department from the list. 2. In the left pane, click **Groups**. 3. In the right pane, in the **Search for groups** box, type all or some of a group name, and then click **Search**. 4. In the **Select a group** list, select a group, and then click **Modify**. 5. In the **Modify Group Properties** dialog box, in the left pane, expand **Privileges** and click any privilege category. 6. View the effective privileges for that group.

Situation	Steps
	7. Click **OK**.
View global privileges for a group	1. In the left pane, under **Select Department**, select **Cross Department Settings** from the list. 2. In the left pane, click **Groups**. 3. In the right pane, in the **Search for groups** box, type all or some of a group name, and then click **Search**. 4. In the **Select a group** list, select a group, and then click **Modify**. 5. In the **Modify Group Properties** dialog box, in the left pane, select **Global Privileges**. 6. View the effective privileges for that group. 7. Click **OK**.

Create a department

To set up an active department and assign managers to it, complete the following steps.

Prerequisite You can complete this procedure only if you are the owner.

1. In the **Management Console**, on the **Department** menu, click **New**.
2. In the **Department** dialog box, on the **General** tab, in the **Name** box, type the name of the department. For example, `Higher Education`.
3. Optional. In the **Description** box, type some content that describes the purpose of the security group you are creating.
4. Select the **Is Active** box.
5. On the **Managers** tab, click **Add**.
6. On the **Users** tab, perform one of the following actions to search for managers to assign the department.
   - In the **Select a user** list, select a user and then click **Modify**.
   - In the **Search for users** box, type all or some of a user name, first or last name and then click **Search**. In the **Select a user** list, select a user and then click **Modify**.

   Note: To sort the **Select a user** list in ascending or descending order, click the **Name**, **Last Name**, **First Name**, or **Status** column headers.
7. Click **Add** to move the selected managers into the department.
8. Click **OK**, and then click **OK** again when prompted.

Grant management privileges to users

To give users privileges that enable them to perform various management actions in Perceptive Content, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Users**.
3. In the right pane, in the **Search for users** box, type all or some of a user name, first name, or last name and click **Search**.
4. In the **Select a user** list, select a user and click **Modify**.
5. In the **Modify User Profile** dialog box, in the left pane, click **Global Privileges**.
6. In the **Privileges** list, perform one of the following actions.
   - To grant all management privileges, click the column in front of the **Manage** privilege category until appears in front of the group.
   - To grant specific management privileges, click the column in front of each privilege in the **Manage** group until appears.
7. Click **OK**.

Privilege definitions overview

In Perceptive Content, you assign privileges to control the actions that users can perform. Privileges can be assigned at the user or group level. Privileges assigned to a user have higher priority than privileges assigned to a group. Privileges from the categories below have no particular hierarchical relationship among each other beyond the user and group relationship. If two privileges contradict, with one granting access and the other denying, the conflict is resolved in favor of the denying privilege and access is denied. For instance, if a drawer privilege allows access and a document type privilege denies access, then the denying privilege has a higher priority and access is denied. Privileges only affect user abilities in the department where the privilege was assigned, and are assigned at the department level. The exceptions are privileges in the Global privilege category, which affect user abilities throughout the client and are assigned in Cross Department Settings.

For information about specific privileges in privilege categories, view the following help topics.

- Annotation Template Privileges
- Application Plan Privileges
- Category Privileges
- Connection Type Privileges
- Department: Manage
- Department: Administer User Privileges
- Department: Administer Group Privileges
- Document Type: Documents
- Document Type: Explorer/Folder Viewer
- Document Type: Viewer

- Document Type: Document Management
- Drawer: Content
- Drawer: Documents
- Drawer: Folders
- Drawer: Explorer/Folder Viewer
- Drawer: Viewer
- Drawer: Document Management
- Drawer: Batch (Proposed Key)
- File Plan: Content
- File Plan: Records
- File Plan: Record Categories
- File Plan: Record Folders
- File Plan: Explorer/Folder Viewer
- File Plan: Viewer
- Folder Type Privileges
- Form Privileges
- Global: Search
- Global: Capture
- Global: Batch (General)
- Global: Viewer (Unlinked Documents)
- Global: Reports
- Global: Manage
- Global: Administer User Privileges
- Global: Administer Group Privileges
- Hold Privileges
- Record Category Privileges
- Record Category Type Privileges
- Record Folder Privileges
- Record Folder Type Privileges
- Record Type: Records
- Record Type: Explorer/Folder Viewer
- Record Type: Viewer
- Report Security Privileges
- Task Template Privileges
- Workflow: Process
- Workflow: Queue
- Workflow: Application Plan
- Workflow: Route Out Restrictions

Annotation Template Privileges

The following privileges are available for annotation templates and annotations created with templates. These privileges are located in the Security area of an annotation template.

Create

When a user has this privilege, the user can create a new annotation using this template.

Delete

When a user has both this privilege and the **Annotation Template > View** privilege, the user can delete annotation instances created using this template.

Hide

When a user has both this privilege and the **Annotation Template > View** privilege, the user can hide annotation instances created using this template.

Modify

When a user has both this privilege and the **Annotation Template > View** privilege, the user can modify annotation instances created using this template.

View

Allows the user to view annotations instances created using this annotation.

Application Plan Privileges

The following privilege types are available for application plans. These privileges are located in the Security area of an application plan.

Link Documents

Allows the user to create new documents or re-link documents when using this application plan.

Auto Create Folders

Allows the user to automatically create folders when linking a document using this application plan. To automatically create folders, the user must also have access to at least one drawer location for the created folders.

View

Allows the user to run the active screen s view action.

Manage

Allows the user to modify settings for this application plan.

Declare Records

Allows the user to declare a new record or relink a record when using this application plan.

Auto Create Record Folders

Allows the user to automatically create record folders when declaring a record using this application plan.

Category Privileges

The following privilege is available for categories. This privilege is located in the Modify User Profile dialog box or the Modify Group Information dialog box in the Category Privileges pane.

View

Allows the user to view the category and the document types in the category for which the privilege is granted. When the user has both this privilege and the **View > Access** privilege, the user can return documents for this drawer or document type. To open a document, the user must also have the **Documents > Open** privilege for the associated drawer or document type.

Connection Type Privileges

The following privileges are available for Connection Types. These privileges are located in the Modify User Profile dialog box or the Modify Group Information dialog box in the Connection Type Privileges pane.

Apply

Allows the user to apply connections between records.

Remove

Allows the user to remove connections between records.

Department: Administer Group Privileges

The following privileges appear in the Administer Group Privileges category for Department privileges.

Drawer Privileges

Allows the user to grant, deny, or copy privileges in the Drawer privilege category to groups.

Document Type Privileges

Allows the user to grant, deny, or copy privileges in the Document Type privilege category to groups.

Folder Type Privileges

Allows the user to grant, deny, or copy privileges in the Folder Type privilege category to groups.

Workflow Process Privileges

Allows the user to grant, deny, or copy privileges in the Process privilege category to groups.

File Plan Privileges

Allows the user to grant, deny, or copy privileges in the File Plan privilege category to groups.

Record Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Type privilege category to groups.

Record Folder Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Folder Type privilege category to groups.

Record Category Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Category Type privilege category to groups.

Access Control Marking Privileges

Allows the user to grant, deny, or copy access control marking privileges to groups.

Record Container Privileges

Allows the user to grant, deny, or copy record category privileges and record folder privileges to groups in the File Plan Designer.

Connection Type Privileges

Allows the user to grant, deny, or copy privileges in the Connection Type privilege category to groups.

Department: Administer User Privileges

The following privileges appear in the Administer User Privileges category for Department privileges.

Drawer Privileges

Allows the user to grant, deny, or copy privileges in the Drawer privilege category to users.

Document Type Privileges

Allows the user to grant, deny, or copy privileges in the Document Type privilege category to users.

Folder Type Privileges

Allows the user to grant, deny, or copy privileges in the Folder Type privilege category to users.

Workflow Process Privileges

Allows the user to grant, deny, or copy privileges in the Process privilege category to users.

File Plan Privileges

Allows the user to grant, deny, or copy privileges in the File Plan privilege category to users.

Record Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Type privilege category to users.

Record Folder Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Folder Type privilege category to users.

Record Category Type Privileges

Allows the user to grant, deny, or copy privileges in the Record Category Type privilege category to users.

Access Control Marking Privileges

Allows the user to grant, deny, or copy access control marking privileges to users.

Record Container Privileges

Allows the user to grant, deny, or copy record category privileges and record folder privileges to users in the File Plan Designer.

Connection Type Privileges

Allows the user to grant, deny, or copy privileges in the Connection Type privilege category to users.

Department: Manage

The following privileges appear in the Manage category for Department privileges.

Groups

Allows users to create, delete, add users to, or remove users from groups. The ability to assign privileges to groups has dependencies on other Department privileges.

Application Plans

When a user has both this privilege and the **Application Plan > Records > Manage** privilege, the user can create, delete, or modify application plans. When a user creates an application plan, he or she is automatically granted the **Application Plan > Records > Manage** privilege for the plan.

Annotation Templates

Allows users to create, delete, or modify annotation templates. This privilege grants access to the Annotations pane in Management Console.

Drawers

Allows users to create, delete, or modify drawers. This privilege grants access to the Drawers pane in Management Console.

Document Types

Allows users to create, rename, and delete document types. This privilege grants access to the Document Types pane and the Document Type Lists pane in Management Console.

Folder Types

Allows users to create, delete, or modify folder types. This privilege grants access to the Folder Types pane and the Folder Type Lists pane in Management Console. To modify and delete folder types, the user must also have the **Folder Type > Manage** privilege. By default, the **Folder Type > Manage** and **Folder Type > Use** privileges are granted to the creator of the folder type.

Custom Properties

Allows users to create, delete, or modify custom properties. This privilege grants access to the Custom Properties pane in Management Console.

Task Templates

Allows users to create task templates and then modify or delete only those templates. This privilege grants access to the Task Templates pane in Management Console. The user can create new task templates and rename, copy, modify or delete the task templates they created.

Workflow Processes

Allows users to create and modify workflow processes, access all queues, and promote users to Process Manager. This privilege grants access to the Workflow pane in Management Console. To modify workflow processes, you must select the workflow process for the user in the Process Privileges area of the Security Settings window.

Forms

Allows users to create, delete, or modify forms. User can access the Form Designer and the Forms pane in Management Console. User can set privileges for form presentations on an individual basis for both users and groups. User can manage all form components and all forms.

Capture Profiles

Allows users to create, delete, or modify server-side capture profiles. Capture profiles are used for importing items into Perceptive Content.

This privilege grants access to the Capture Profile pane in Management Console.

Source Profiles

Allows users to create, delete, or modify source profiles. Source profiles are used for importing items into Perceptive Content.

This privilege grants access to the Source Profile pane in Management Console.

Output Profiles

Grants users access to the Output Profiles pane in Management Console to modify output profiles.

Document Views

When a user has both this privilege and the **View > Manage** privilege for at least one document view, the user can create, delete, or modify document views and document relationship views. When a user creates a document view, Perceptive Content automatically grants the **View > Manage** privilege.

Folder Views

When a user has both this privilege and the **View > Manage** for at least one folder view, the user can create, delete, or modify folder views and folder relationship views. When a user creates a folder view, Perceptive Content automatically grants the **View > Manage** privilege.

Retention Policies

Grants users access to Retention Policy Designer to create and modify retention policies. The user receives notification emails after retention sets, such as export (accession and offline transfer), destruction, move, and copy sets are complete or if these set types fail.

Retention Holds

Grants users access to the Holds area of Retention Policy Manager and the Export tab in the Sets area of Retention Policy Manager to create, modify, assign, and remove retention holds. Users can search for holds in the explorer grid.

Fax Recipients

Allows users to modify fax recipient information on the Fax Recipients tab in the Output Profiles area of Management Console.

Record Types

Grants users access to the Records pane and the Record Types pane in Management Console to create, modify, and delete record types.

File Plans

Grants users access to the Records pane and the File Plans pane in Management Console. This privilege allows users to create file plans and open File Plan Designer. The user can also view, modify, and delete file plans.

Record Folder Types

Grants users access to the Records pane and the Record Folder Types pane in Management Console to create record folder types. For record folder types that the user creates, the user can also modify and delete record folder types.

Record Category Types

Grants users access to the Records pane and the Record Category Types pane in Management Console to create record category types. For record category types that the user creates, the user can also modify and delete record category types.

Connection Types

Grants users access to the Connection Types pane in Management Console to create, modify, and delete connection types.

Access Control Markings

Grants users access to the Picklists pane in Management Console to create, modify, and delete access control markings and picklists. This privilege grants users all administrative access control marking functionality except for assigning markings.

Record Views

Grants users access to the Record Views pane in Management Console to create, modify, or delete customized record views.

Record Folder Views

Grants users access to the Record Folder Views pane in Management Console to create, modify, or delete customized record folder views.

Document Type: Document Management

The following privileges appear in the Document Management category for Document Type privileges.

Use Version Control

Allows users to add a document to version control, check a document in and out, view a document s history, undo a document s checkout, and get the latest version of a document in version control.

Version control is only available for documents the user can access through the drawer and document type privileges. A user must have this privilege to sign a signature required task type.

Remove from Version Control

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can remove a document from version control.

Undo 3rd Party Check Out

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can reverse a document checked out by another user.

Delete Version History

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can delete the version control history of documents. A document must be removed from version control before a user can delete its history.

Document Type: Documents

The following privileges appear in the Documents category for Document Type privileges.

Open

Allows users to open an accessible document. When a user has both this privilege and the **Drawer > Content > Search** privilege, the user can open documents from a list of document search results in the explorer grid.

Sign

When a user has both this privilege and the **Documents > Open** privilege for the drawer or document type, the user can digitally sign the document in the viewer. A user must have this privilege to complete a signature required task type.

Void Signatures

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can void digital signatures for all users on any accessible signed document in the viewer. Reserve this privilege for highly qualified personnel.

Edit Drawer

When a user has both this privilege and the **Drawer > Content > Create/Append** privilege associated with the destination drawer, the user can move a document to another drawer. Documents that are part of a folder hierarchy can change drawers by moving.

After the user moves a document or folder from its original drawer into a new folder, the user can no longer edit its drawer value from the explorer grid or the viewer. The user must move the document or folder to the desired drawer or folder location.

Edit Type

Allows users to modify the type of a document or folder. When a user has both this privilege and the **View > Access** privilege for at least one document or folder view defined to return results for the drawer, the user can modify this value from the explorer grid.

Edit Keys

Allows users to modify the Field1 through Field5 document keys for accessible documents. Users can perform this action in the explorer grid or in the viewer.

Edit Custom Properties

Allows users to modify custom property values for accessible documents and folders. Users can perform this action in the explorer grid or in the viewer.

Edit Notes

Allows users to create, modify, and delete notes for accessible documents. Users can perform this action in the explorer grid or in the viewer.

Delete

Allows users to delete accessible documents and restore documents they delete. Users can perform this action in the explorer grid.

Merge

Allows users to merge two or more accessible documents into a single document. To perform this action, the user must also have the **Drawer > Content > Create/Append** privilege associated with the target document.

Page Delete

Allows users to delete a page from accessible documents in the viewer. When a user has both this privilege and the **Drawer > Content > Create/Append** privilege associated with the target document, the user can remove pages from a document when copying the document. Users cannot restore deleted pages.

Page Reorder

Allows users to change the order of the pages in an accessible document in the viewer.

Move Page

Allows users to remove a page from one accessible document and add it to another accessible document in the viewer.

Delete Signed Documents

Allows users to delete accessible documents that are digitally signed and to restore documents they delete. Users can perform these actions in the explorer grid.

Move Signature Representations

Allows users to move visual representations of their signatures after the document is saved. Users can perform this action in the viewer.

Delete Signature Representations

Allows users to delete visual representations of their signatures after the document is saved. Users can perform this action in the viewer.

Copy to Clipboard

Allows Interact Desktop users to copy the document page or region to the clipboard for use with Interact Desktop. To perform this action, users must also have the **View > Access** privilege for the associated document view and the **Drawer > Content > Open** privilege for the associated drawer.

Document Type: Explorer/Folder Viewer

The following privileges appear in the Explorer/Folder Viewer category for Document Type privileges.

Print Documents

Allows users to print accessible documents in the explorer grid.

Email ImageNow Link

Allows users to email an Perceptive Content link to a document from the explorer grid. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Email Web Link

Allows users to email a Perceptive Experience link to a document from the explorer grid. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Mail as Attachment

Allows users to email a document from the explorer grid as an attachment. Sender users must have the **Documents > Open** privilege for the associated drawer or document type.

Save Local Copies

Allows users to export a formatted text version of accessible documents in the explorer grid. For documents with annotations, the user must have the **Annotation Template > Hide** privilege.

Fax Document

Allows users to fax accessible documents in the explorer grid.

Launch Associated Application

Allows users to launch an external application, such as Microsoft Windows, to view accessible documents from the explorer grid.

Send Documents to User

Allows users to remotely send accessible documents to another user in the explorer grid.

Sender users must have the **View > Access** privilege for at least one document view and the **Drawer > Content > Search** privilege.

Recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Send to ShareBase

Allows users to send accessible documents to ShareBase in the explorer grid. If the user has the Explorer privilege, they can send the document, even if they do not have the **Documents > Open** privilege for the associated drawer or document.

Document Type: Viewer

The following privileges appear in the Viewer category for Document Type privileges.

Print Document

Allows users to print accessible documents in the viewer.

Email ImageNow Link

Allows users to email an Perceptive Content link to a document from the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Email Web Link

Allows users to email a Perceptive Experience link to a document from the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Mail as Attachment

Allows users to email a document from the viewer as an attachment. Sender users must have the **Documents > Open** privilege for the associated drawer or document type.

Save Local Copies

Allows users to export a formatted text version of accessible documents in the viewer. For documents with annotations, the user must have the **Annotation Template > Hide** privilege.

Fax Document

Allows users to fax accessible documents in the viewer.

Launch Associated Application

Allows users to launch an external application, such as Microsoft Windows, to view accessible documents from the viewer.

Send Document to User

Allows users to remotely send accessible documents to another user in the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document.

Send to ShareBase

Allows users to send accessible documents to ShareBase in the viewer. Users must have the **Documents > Open** privilege for the associated drawer or document.

Drawer: Batch (Proposed Key)

The following privilege appears in the Batch (Proposed Key) category for Drawer privileges.

Process

Allows users to view any batch in which the associated drawer is a proposed key. To process a batch, users must have the following privileges.

- **Global > Batch > QA**
- **Global > Batch > Link**
- **Drawer > Content > Create/Append**
- **Application Plan > Link Documents**

Drawer: Content

The following privileges appear in the Content category for Drawer privileges.

Open

Allows users to open documents and folders in the viewer. When a user has both this privilege and the **Drawer > Content > Search** privilege, the user can open documents and folders from a list of search results in the explorer grid.

To open a folder, you must also have the **Folder Type > Use** privilege.

For any operation you perform in the viewer, you must have this privilege granted.

In Business Insight, users with both this privilege and the **Report > View** privilege can open a document in the viewer from a report hyperlink.

Search

Allows users to search for documents, folders, and shortcuts using accessible views. When a user has both this privilege and the **View > Access** privilege for at least one document or folder view defined to return results for the drawer, the user can modify this value from the explorer grid.

Create/Append

Allows users to create documents, folders, and shortcuts, to copy documents, and to append pages to a document in an accessible drawer. When a user has both this privilege and the **Drawer > Content > Create Shortcuts** privilege, the user can create shortcuts to documents or folders.

Move

When a user has both this privilege and the **Drawer > Content > Create/Append** privilege, the user can move a document, shortcut, or folder to a new folder location.

Rename

Allows users to rename a document, folder, or shortcut in the drawer. When a user has both this privilege and the **View > Access** privilege for at least one document or folder view defined to return results for the drawer, the user can rename a document, folder, or shortcut from the explorer grid.

Delete

Allows users to delete accessible documents and folders from the explorer grid. Users can only restore documents and folders they created. When a user has both this privilege and the **Drawer > Content > Remove Shortcuts** privilege, the user can delete a shortcut to a document or folder.

Edit Custom Properties

Allows users to modify custom property values for accessible documents and folders in the explorer grid or in the viewer.

Edit Drawer

When a user has both this privilege and the **Drawer > Content > Create/Append** privilege associated with the destination folder, the user can move a document or shortcut to a different drawer. After the user moves a document or folder from its original drawer into a new folder, the user can no longer edit its drawer value from the explorer grid or the viewer.

Edit Type

Allows users to modify the type of a document or folder. When a user has both this privilege and the **View > Access** privilege for at least one document or folder view defined to return results for the drawer, the user can modify the document type or folder type from the explorer grid.

Create Shortcuts

Allows users to create shortcuts to a document or folder.

Remove Shortcuts

Allows users to delete shortcuts to a document or folder. Removing a shortcut does not delete the target document or folder.

Drawer: Document Management

The following privileges appear in the Document Management category for Drawer privileges.

Use Version Control

Allows users to add a document to version control, check a document in and out, view a document s history, undo a document s checkout, and get the latest version of a document in version control.

Version control is only available for documents the user can access through the drawer and document type privileges. A user must have this privilege to sign a signature required task type.

Remove from Version Control

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can remove a document from version control.

Undo 3rd Party Check Out

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can reverse a document checked out by another user.

Delete Version History

When a user has both this privilege and the **Drawer > Document Management > Use Version Control** privilege, the user can delete the version control history of documents. A document must be removed from version control before a user can delete its history.

Drawer: Documents

The following privileges appear in the Documents category for Drawer privileges.

Sign

Allows users to digitally sign an accessible document. When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can digitally sign a document in the viewer. A user must have this privilege to complete a signature required task type.

Void Signatures

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can void digital signatures for all users on any accessible signed documents. Reserve this privilege for highly qualified personnel.

Edit Keys

When a user has both this privilege and the **Documents > Open** for the associated drawer or document type, the user can modify the Field1 through Field5 document keys for accessible documents in the explorer grid.

Edit Notes

When a user has both this privilege and the **Documents > Open** for the associated drawer or document type, the user can create, modify, and delete notes for accessible documents in the explorer grid.

Merge

When a user has both this privilege and the **Drawer > Content > Create/Append** privilege associated with the target document, the user can merge two or more accessible documents into a single document.

Page Delete

Allows users to delete a page from accessible documents in the viewer. Users cannot restore deleted pages.

Page Reorder

Allows users to change the order of pages in an accessible document in the viewer.

Move Page

When a user has both this privilege and the **Documents > Open** for the associated drawer or document type, the user can remove a page from one accessible document and add it to another accessible document in the viewer.

Delete Signed Documents

Allows users to delete accessible documents that are digitally signed and to restore documents they delete. Users can perform these actions in the explorer grid.

Move Signature Representations

Allows users to move visual representations of their signatures after the document is saved. Users can perform this action in the viewer.

Delete Signature Representations

Allows users to delete visual representations of their signatures after the document is saved. Users can perform this action in the viewer.

Copy to Clipboard

Allows Interact Desktop users to copy the document page or region to the clipboard for use with Interact Desktop. To perform this action, users must also have the **View > Access** privilege for the associated document view and the **Drawer > Content > Open** privilege for the associated drawer.

Drawer: Explorer/Folder Viewer

The following privileges appear in the Explorer/Folder Viewer category for Drawer privileges.

Print Documents

Allows users to print accessible documents in the explorer grid.

Email ImageNow Link

Allows users to email an Perceptive Content link to a document from the explorer grid. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Email Web Link

Allows users to email a Perceptive Experience link to a document from the explorer grid. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Mail as Attachment

Allows users to email a document from the explorer grid as an attachment. Sender users must have the **Documents > Open** privilege for the associated drawer or document type.

Save Local Copies

Allows users to export a formatted text version of accessible documents in the explorer grid. For documents with annotations, the user must have the **Annotation Template > Hide** privilege.

Fax Document

Allows users to fax accessible documents in the explorer grid.

Launch Associated Application

Allows users to launch an external application, such as Microsoft Windows, to view accessible documents from the explorer grid.

Send Documents to User

Allows users to remotely send accessible documents to another user in the explorer grid.

Sender users must have the **View > Access** privilege for at least one document view and the **Drawer > Content > Search** privilege.

Recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Send to ShareBase

Allows users to send accessible documents to ShareBase in the explorer grid. If the user has the Explorer privilege, they can send the document, even if they do not have the **Documents > Open** privilege for the associated drawer or document

Drawer: Folders

The following privilege appears in the Folders category for Drawer privileges.

Edit Status

Allows users to activate or disable a folder.

Drawer: Viewer

The following privileges appear in the Viewer category for Drawer privileges.

Print Document

Allows users to print accessible documents in the viewer.

Email ImageNow Link

Allows users to email an Perceptive Content link to a document from the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Email Web Link

Allows users to email a Perceptive Experience link to a document from the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document type.

Mail as Attachment

Allows users to email a document from the viewer as an attachment. Sender users must have the **Documents > Open** privilege for the associated drawer or document type.

Save Local Copies

Allows users to export a formatted text version of accessible documents in the viewer. For documents with annotations, the user must have the **Annotation Template > Hide** privilege.

Fax Document

Allows users to fax accessible documents in the viewer.

Launch Associated Application

Allows users to launch an external application, such as Microsoft Windows, to view accessible documents from the viewer.

Send Document to User

Allows users to remotely send accessible documents to another user in the viewer. Sender and recipient users must have the **Documents > Open** privilege for the associated drawer or document.

Send to ShareBase

Allows users to send accessible documents to ShareBase in the viewer. Users must have the **Documents > Open** privilege for the associated drawer or document.

File Plan: Content

The following privileges appear in the Content category for File Plan privileges.

Open

Allows users to open an accessible record, record folder, or record category in a viewer, or open the modify dialog box in File Plan Designer. With this privilege and the **File Plan > Content > Search** privilege, the user can open a record or record folder from a list of search results in the explorer grid.

Search

With this privilege and the **View > Access** privilege for at least one record, record folder, or record category view defined to return results for the file plan, the user can search the contents of the file plan and display search results in a list.

Create/Append

Allows users to create elements in a file plan and append pages to existing records. The following privileges require this privilege as a prerequisite to perform their respective actions.

- **File Plan > Content > Move**
- **File Plan > Records > Merge**

Move

With this privilege and the **File Plan > Content > Create/Append** privilege associated with the destination record folder, the user can move a record or record folder to a new location.

Rename

Allows users to modify the name of an accessible record, record folder, or record category. With this privilege and the **View > Access** privilege for at least one record, record folder, or record category view defined to return results for the file plan, the user can rename elements from the explorer grid.

Delete

Allows users to delete elements in a file plan. With this privilege and the **View > Access** privilege for at least one record view, the user can delete elements from the explorer grid. A user can only restore the specific records, record folders, and record categories that the user deleted.

Edit Custom Properties

Allows users to modify values for the custom properties that are associated with the record, record folder, or record category type.

With this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can modify custom property values from the viewer.

With this privilege and the **View > Access** privilege for at least one record, record folder, or record category view, the user can modify custom property values in the explorer grid.

Edit File Plan

Allows users to change the file plan that is associated with a record, record folder, or record category if the user also has the following privileges associated with the destination file plan.

- **File Plan > Content > Move**
- **File Plan > Content > Create/Append**

The user must also have the **File Plan > Content > Delete** privilege for the source file plan.

After the user moves a record, record folder, or record category from its original file plan into a new file plan, the user can no longer edit its file plan value from the explorer grid or the viewer unless the user has editing privileges for the new file plan.

Edit Type

With this privilege and the **Manage > Record Type** privilege for the destination record type, the user can select a different record, record folder, or record category type for a record or file plan element.

To edit the record, record folder, or record category type from the explorer grid, the user must also have the **View > Access** privilege for at least one record or record folder view defined to return results for the file plan.

Reassign Retention Policy

Allows users to add or remove policies for existing categories. The privilege does not include policy creation. When you grant this privilege to a user, the approval task template privilege for this department is also granted to the user.

Apply Cutoffs

Grants users access to the Cutoffs pane in Management Console to manually change the state of records and record folders to cutoff.

Reverse Cutoffs

Grants access to the Cutoffs pane in Management Console to manually reverse the cutoff state of records or record folders.

Override Closed State

Allows user to add pages to all records and record folders, regardless of the closed state.

Close

Allows users to manually change the record folder state to closed. With this privilege, the user can set a record folder to inherit its closed state from its immediate ancestor.

Reopen

Allows users to manually change the record folder state to open. With this privilege, the user can set a record folder to inherit its open state from its immediate ancestor.

Vital Status

Grants users access to the Vital Records pane in File Plan Designer to apply, modify, review, and remove vital status.

File Plan: Explorer/Folder Viewer

The following privileges appear in the Explorer/Folder Viewer category for File Plan privileges.

Print Record

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can print records from the explorer grid

Save Local Copies

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can export and save one or more of the records from the explorer grid to the local file system.

Launch Associated Application

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can open the current record using the designated application on the local system.

Email ImageNow Link

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can email an Perceptive Content link to a record from the explorer grid.

Email as Attachment

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can email a record from the explorer grid as an attachment.

Fax Record

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can fax a record from the explorer grid.

File Plan: Record Categories

The following privileges appear in the Record Categories section of File Plan privileges.

Modify Properties

When a user has both this privilege and the **Record Category Type > Use** privilege, the user can modify record category properties.

Modify Notifications

When a user has both this privilege and the **Record Category Type > Use** privilege, the user can modify record category notifications.

File Plan: Record Folders

The following privilege appears in the Record Folders section of File Plan privileges.

Edit Status

Allows users to activate or disable a record folder.

File Plan: Records

The following privileges appear in the Records category for File Plans privileges. When a privilege is granted, the user can perform the associated action for records in the file plan.

Edit Properties

Allows users to modify the Field1 through Field5 record keys and record properties. This privilege does not allow the user to modify custom properties or metadata assigned to record pages.

When a user has this privilege, the **View > Access** privilege for at least one record view, and the **File Plan > Content > Search** privilege, the user can modify record properties in the explorer grid.

When a user has both this privilege and the **Records > Open** privilege, the user can modify record properties in the viewer.

Edit Notes

Allows users to modify the record notes.

When a user has both this privilege and the **View > Access** privilege for at least one record view, the user can modify record notes in the explorer grid.

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can modify record notes from the viewer.

Merge

Allows users who have both this privilege and the **File Plan > Content > Create/Append** privilege associated with the target record, to combine two or more records into a single record.

When users also have the **View > Access** privilege for at least one record view, the users can merge records in the explorer grid.

Page Delete

Allows users who have both this privilege and the **Records > Open** privilege for the associated file plan or record type, to delete a page from a record in the viewer. Users cannot restore deleted pages.

Page Reorder

Allows users who have both this privilege and the **Records > Open** privilege for the associated file plan or record type, to modify the order of pages in a record in the viewer.

Move Page

Allows users who have both this privilege and the **Records > Open** privilege for the associated file plan or record type, to remove a page from one record and add that page to another record independent of the file plan. Users can perform this action in the viewer.

Modify Page Properties

Allows users to modify metadata assigned to record pages. When users have both this privilege and the **Records > Open** privilege for the associated file plan or record type, the users can modify page metadata in the viewer.

Copy to Clipboard

Allows Interact Desktop users to copy the record page or region to the clipboard for use with Interact Desktop. To perform this action, users must also have the **View > Access** privilege for the associated record view and the **File Plan > Content > Open** privilege for the associated file plan.

File Plan: Viewer

The following privileges appear in the Viewer category for File Plan privileges.

Print Record

Allows users who have both this privilege and the **Records > Open** privilege for the associated file plan or record type, to print records from the viewer.

Save Local Copies

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can export and save one or more of the records displayed in the viewer to the local file system.

Launch Associated Application

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can open the current record using the designated application on the local system.

Email ImageNow Link

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can email an Perceptive Content link to a record from the viewer.

Email as Attachment

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can email a record from the viewer as an attachment.

Fax Record

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can fax a record from the viewer.

Folder Type Privileges

The following privileges determine the actions users can perform for the folder type. These privileges are located in the Modify User Profile dialog box or the Modify Group Information dialog box, in the Folder Type pane.

Use

Allows users who have both this privilege and the **Drawer > Content > Create/Append** privilege, to use the folder type to create, modify, and search for folders for that folder type. Forms displayed as stand-alone folders require this privilege.

Manage

When a user has both this privilege and the **Global > Manage > Folder Types** privilege, the user can build hierarchies using this folder type. This privilege grants access to the Folder Types tab so the user can modify or remove folder types.

Form Privileges

The following privileges determine the actions users can perform for the form. These privileges are located in the Security area of a form.

Create

Allows users who have both this privilege and the **Form > View** privilege, to use this form to create a data instance for a document. This privilege allows users to enter the initial data in any field of a form and save that data.

Delete

When a user has both this privilege and the **Form > View** privilege, the user can use this form to delete the existing data instance for a document. This privilege allows the user to clear all data fields.

Modify

When a user has both this privilege and the **Form > View** privilege, the user can use this form to modify an existing data instance for a document.

View

Allows users to use this form to view existing data instances for documents. This privilege is granted automatically when you create and publish a form using Form Designer.

Global: Administer Group Privileges

The following privileges appear in the Administer Group Privileges category for Global privileges.

ERM Privileges

Allows users to grant or deny ERM privileges in the Global privilege category to groups.

Capture Privileges

Allows users to grant or deny capture privileges in the Global privilege category to groups.

Interact Search Privileges

Allows users to grant or deny search privileges in the Global privilege category to groups.

Batch Users

Allows users to modify which users batches are visible to selected groups. This grants users access to the Batch Users tab on the Modify Group Information dialog box.

Global: Administer User Privileges

The following privileges appear in the Administer User Privileges category for Global privileges.

ERM Privileges

Allows users to grant or deny ERM privileges in the Global privilege category to users.

Capture Privileges

Allows users to grant or deny capture privileges in the Global privilege category to users.

Interact Search Privileges

Allows users to grant or deny search privileges in the Global privilege category to users.

Batch Users

Allows users to modify which users batches are visible to other users. This grants users access to the Batch Users tab on the Modify User Profile dialog box.

Global: Batch (General)

The following privileges appear in the Batch (General) category for Global privileges.

To process batches with these privileges, you need the **Drawer > Batch (Proposed Key) > Process** privilege.

QA

Allows users to perform QA processing on batches in the viewer.

Link

Allows users to perform link processing on batches in the server.

To link a document, users must also have the **Drawer > Content > Create/Append** privilege.

To link a document using the application plan, users must also have the **Application Plan > Link Documents** privilege.

Delete

Allows users to delete batches.

To delete batches ready for QA requires the **Global > Batch > QA** privilege.

To delete batches ready for linking requires the **Global > Batch > Link** privilege.

Edit Batch Notes

Allows users to modify batch notes.

To modify batch notes on batches ready for QA requires the **Global > Batch > QA** privilege.

To modify batch notes on batches ready for linking requires the **Global > Batch > Link** privilege.

Modify Batch Step or State

Allows users to modify the current batch processing step and the current state for batches.

To modify the step and state of a batch ready for QA requires the **Global > Batch > QA** privilege.

To modify the step and state of batches ready for linking requires the **Global > Batch > Link** privilege.

Resubmit Batch

Allows users to resubmit batches.

To resubmit batches ready for linking requires the **Global > Batch > Link** privilege.

Bypass QA

When a user has both this privilege and the **Global > Batch > QA** privilege, the user can choose to bypass QA processing for batches.

Global: Capture

The following privileges appear in the Capture category for Global privileges.

Batch Mode

Allows users to import documents using Batch Mode. This privilege also enables the Capture button on the Perceptive Content toolbar.

Single Mode

When a user has both this privilege and the **Application Plan > Link Documents** privilege, the user can import documents using Single Mode. This privilege also enables the Capture button on the Perceptive Content toolbar.

Package Mode

When a user has both this privilege and the **Application Plan > Link Documents** privilege, the user can import documents using Package Mode. This privilege also enables the Capture button on the Perceptive Content toolbar.

Global: Manage

The following privileges appear in the Manage category for Global privileges.

LearnMode Options

Allows users to open the LearnMode Options dialog box in the client. To create LearnMode application plans, users must also have the **Global > Manage > Application Plans** privilege.

Server Administrator

Allows users to run administrative and performance tools and to manage the Object Storage Manager, licenses for users and groups, and user sessions.

Basket Groups

Allows users to create, delete, and modify basket groups. Basket groups are required for package scanning.

Package Mode Document Rules

Allows users to create, delete, or modify scan prompt rules for capturing documents in Package Mode.

When users have both this privilege and the **Global > Manage > Basket Groups** privilege, the user can configure Package Mode basket groups.

When users have both this privilege and the **Global > Capture > Basket Groups** privilege, they can capture documents in Package Mode.

Batch Upload Settings

Allows users to modify local batch upload settings.

The Batch Upload Configuration controls whether batch upload is immediate or delayed according to a schedule the user provides.

This privilege enables the Batch Upload: Configure Settings button on the Capture tab, which is accessed through the Options command on the Settings menu of the Perceptive Content toolbar.

Capture Profiles

Allows users to create, delete, or modify client-side capture profiles. Capture profiles are used for scanning or importing documents into Perceptive Content.

For client-side profiles, this privilege enables the Capture button on the Perceptive Content toolbar with the Manage Capture Profiles option and the Manage Profiles button on the Capture pane in the Perceptive Content Options dialog box.

Scanner Profiles

Allows users to create, delete, or modify scanner profiles. A scanner profile contains information about a user s scanning hardware.

Devices

Allows users to create and delete capture devices. A scanning device is required to set up a scanner profile. The scanning device associates the scanning driver with the scanner profile.

Digital ID

Allows users to view, export, void, and expire digital IDs.

Digital IDs are automatically created by the server any time a user, who has the correct privileges, requests to digitally sign a document but does not have a Digital ID.

Digital Signatures

Allows users to set administrative options regarding digital signatures. This includes setting defaults, modifying validity periods, and creating signature and digital ID reasons.

Audit Template Management

Allows users to create, modify, and delete audit templates.

Audit Template Assignment

Allows users to assign audit templates to users and groups.

Reports

Allows users to assign users and privileges to reports and report folders, schedule reports, copy and rename reports, and delete reports and report folders.

A report manager assigns the **Global > Reports > View** privilege in the Global privilege category to user to grant them access to Business Insight in Perceptive Content.

You cannot assign this privilege to a group.

Run iScript Remotely

Allows users to run an iScript on the server remotely.

Task Views

Allows users who have both this privilege and the **View > Manage** privilege to modify task views.

Modify User Profiles

Allows users who have both this privilege and the **Global > Manage > View User Profiles** privilege to modify user profile information.

View User Profiles

Allows users to display but not modify user profiles for users in the system.

Global: Reports

The following privilege appears in the Reports category for Global privileges.

View

Allows users to access the Reports button on the Perceptive Content toolbar.

Users with this privilege can view instances of Business Insight reports to which the users have access in the explorer grid.

For this privilege to appear, Business Insight must be installed on your system.

Global: Search

The following privileges appear in the Search category for Global privileges.

ERM

Allows users to access the ERM Search interface. For this privilege to appear, ERM must be installed on your system.

ERM: Load Local Query

When the user has both this privilege and the **View > Access** privilege for at least one document view, the user can load ERM queries stored locally. To display document results, the user must also have the **Drawer > Content > Search** privilege. For this privilege to appear, ERM must be installed on your system.

ERM: Load Server Query

When the user has both this privilege and the **View > Access** privilege for at least one document view, the user can load ERM queries stored on the server. To display document results, the user must also have the **Drawer > Content > Search** privilege. For this privilege to appear, ERM must be installed on your system.

ERM: Manage Local Queries

When the user has this privilege, the **Global > Search > ERM: Load Local Query** privilege, and the **View > Access** privilege for at least one document view, the user can save, delete, or modify ERM queries stored locally. To display document results, the user must also have the **Drawer > Content > Search** privilege. For this privilege to appear, ERM must be installed on your system.

ERM: Manage Server Queries

When the user has this privilege, the **Global > Search > ERM: Load Local Query** privilege, and the **View > Access** privilege for at least one document view, the user can save, delete, or modify ERM queries stored on the server. To display document results, the user must also have the **Drawer > Content > Search** privilege. For this privilege to appear, ERM must be installed on your system.

Interact for Office Documents

Allows users to search for documents in the Interact for Office client. To display document results, the user must also have the **Drawer > Content > Search** privilege.

Interact for Office Folders

When a user has this privilege, the **Folder Type > Use** privilege, and the **View > Access** privilege for at least one folder view, the user can search for folders in the Interact for Office client. To display the search results, the user must also have the **Drawer > Content > Search** privilege.

Global: Viewer (Unlinked Documents)

The following privileges appear in the Viewer (Unlinked Documents) category for Global privileges.

Print Document

Allows users to print a document from a batch in the viewer.

When a user has both this privilege and the **Global > Batch > QA** privilege, the user can print documents in batches ready for QA.

When a user has both this privilege and the **Global > Batch > Link** privilege, the user can print documents in batches ready for linking.

Email as Attachment

Allows users to email a document from a batch in the viewer as an attachment.

When a user has both this privilege and the **Global > Batch > QA** privilege, the user can mail documents as attachments in batches ready for QA.

When a user has both this privilege and the **Global > Batch > Link** privilege, the user can mail documents as attachments in batches ready for linking.

Save Local Copies

Allows users to export and save one or more of the documents displayed in a batch in the viewer to the local file system.

When a user has both this privilege and the **Global > Batch > QA** privilege, the user can export batches ready for QA.

When a user has both this privilege and the **Global > Batch > Link** privilege, the user can export batches ready for linking.

Launch Associated Application

Allows users to open the current document in a batch using the designated application on the local system, such as Microsoft Word.

When a user has both this privilege and the **Global > Batch > QA** privilege, the user can launch documents in batches ready for QA.

When a user has both this privilege and the **Global > Batch > Link** privilege, the user can launch documents in batches ready for linking.

Hold Privileges

The following privileges are available for retention holds. These privileges are located in the Modify User Profile dialog box or the Modify Group Information dialog box in the Hold Privileges pane.

Apply Document Hold

Allows users to apply this hold directly to items from the explorer grid and the viewer. Users can search for holds they apply in the explorer grid without the **Hold > Search for Documents on Hold** privilege.

Remove Document Hold

Allows users to remove this hold from documents in the explorer grid and the viewer. Users can remove direct holds from the explorer grid with this privilege, but cannot remove inherited holds. Users can search for this hold in the explorer grid without the **Hold > Search for Documents on Hold** privilege.

Search for Documents on Hold

Users can search for this hold in the explorer grid. This search returns items that are under this hold when applied as a direct or an inherited hold.

Workflow: Process

This privilege is located in the Modify User Profile dialog box or the Modify Group Information dialog box in the Process Privileges pane. Using this type of privilege, you can grant access to each workflow process individually.

When you grant Process Privileges, this also grants access to Workflow Designer so the user can modify the selected workflow process.

Workflow: Queue

The following privileges are available for workflow queues.

To set these privileges, you must have the **Global > Manage > Workflow Processes** privilege and process privileges for the associated workflow process. These privileges are located in Workflow Designer, in the

Users area of the Queue Properties dialog box.

You can also designate a user as a queue lead. Queue lead users automatically inherit all privileges for the queue. All queue actions, except adding items, require the **Workflow Queue > Process** privilege.

While creating sub queues in a super queue, assign access by users and groups. Users assigned to a sub queue automatically inherit the **Workflow Queue > Process** privilege for that sub queue.

Add

Allows users to add items to the queue.

Anywhere

Allows users to route items to any queue in the process.

Archive

Allows users to save a copy of a workflow item into the workflow archive.

Delete

Allows users to remove the items from workflow and permanently delete them from Perceptive Content. This privilege overrides the **Document Type > Documents > Delete** and **Drawer > Content > Delete** privileges.

Process

Allows users to process items in the queue.

Remove

Allows users to remove an item from workflow but not from the server. Once an item is removed, it will no longer have any workflow history.

Upstream

Allows users to route items back through the workflow history.

Record Category Privileges

The following privilege types are available for record categories at the instance level. You can set these privileges in the File Plan Designer.

These privileges have no Deny setting so you can only set these privileges to Granted or Unset. These privileges are granted automatically to the user who creates the record category. For all other users, the privileges default to Unset.

You cannot set these privileges for groups that are hidden from Cross Department settings.

File Content

Allows users to create record folders in the record category, to declare records in the record category, and to copy content into the record category. When users have this privilege, they also file content into all record folders within the record category.

Search

Allows users to detect the contents of the record category in the explorer grid. When users have this privilege, the record category and all contained record folders and records appear in the explorer grid.

Record Category Type Privileges

The following privileges determine the actions a user can perform for the record category type. These privileges are located in the Modify User Profile dialog box or the Modify Group Information dialog box, in the Record Category Type pane.

Manage

When a user has both this privilege and the **Global > Manage > Record Category Types** privilege, the user can view and modify instances of this record category type in Management Console and File Plan Designer.

Use

Allows users to perform any operations for this record category type granted to the user by File Plan privileges.

To create or modify record categories, the users must also have the **File Plan > Content > Create/Append** privilege.

Record Folder Privileges

The following privilege types are available for record folders at the instance level. You can set these privileges in the File Plan Designer.

Record folders inherit granted record category privileges. Therefore, if a user has the Search or File Content privileges for a record category that contains a record folder, the user does not need the same privileges for the record folder to perform the privileged action.

The following privileges have no Deny setting so you can only set these privileges to Granted or Unset. These privileges are granted automatically to the user who created the record folder. For all other users, the privileges are Unset by default.

You cannot set these privileges for groups that are hidden from Cross Department settings.

File Content

Allows users to create record folders in the record folder, to declare records in the record folder, and to copy content into the record folder. When users have this privilege, the users can also file content into all record folders within the record folder.

Search

Allows users to detect the contents of the record folder in the explorer grid. When users have this privilege, the record folder and all contained record folders and records appear in the explorer grid.

Record Folder Type Privileges

The following privileges determine the actions a user can perform for the record folder type. These privileges are located in the Modify User Profile dialog box or the Modify Group Information dialog box in the Record Folder Type pane.

Manage

When a user has both this privilege and the **Global > Manage > Record Folder Types** privilege, the user can view and modify instances of this record folder type in Management Console and File Plan Designer.

Use

Allows users to perform any operations for this record folder type granted to the users by File Plan privileges.

To create or modify record folders, the users must also have the **File Plan > Content > Create/Append** privilege.

Record Type: Explorer/Folder Viewer

The following privileges appear in the Explorer/Folder Viewer category for Record Type privileges. When the privilege is granted, the user can perform the associated action in the explorer grid.

Print Record

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can print records from the explorer grid

Save Local Copies

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can export and save one or more of the records from the explorer grid to the local file system.

Launch Associated Application

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can open the current record using the designated application on the local system.

Email ImageNow Link

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can email an Perceptive Content link to a record from the explorer grid.

Email as Attachment

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can email a record from the explorer grid as an attachment.

Fax Record

When a user has this privilege, the **View > Access** privilege, and the **File Plan > Content > Search** privilege, the user can fax a record from the explorer grid.

Record Type: Records

The following privileges appear in the Records category for Record Type privileges.

Open

Allows users to open a record in the viewer. To open a record from a list of record search results in the viewer, the users must also have the **File Plan > Content > Search** privilege.

Edit File Plan

Allows users to change the file plan that is associated with a record. To move a record to a different file plan, the users must also have the following privileges associated with the destination file plan.

- **File Plan > Content > Move**
- **File Plan > Content > Create/Append**

The users must also have the **File Plan > Content > Delete** privilege for the source file plan.

After the users move a record from its original file plan into a new file plan, the users can no longer edit its file plan value from the explorer grid or the viewer unless the users also has the Edit File Plan privilege for the destination file plan.

Edit Type

When the user has both this privilege and the **Global > Manage > Record Types** privilege for the destination record type, the user can select a different record type for a record.

To edit the record type from the explorer grid, the users must also have the **View > Access** privilege for at least one record or record folder view defined to return results for the file plan.

Edit Properties

Allows users to modify the Field1 through Field5 record keys and record properties. This privilege does not allow users to modify custom properties or metadata assigned to record pages.

When a user has this privilege, the **View > Access** privilege for at least one record view, and the **File Plan > Content > Search** privilege, the user can modify record properties in the explorer grid.

When a user has both this privilege and the **Records > Open** privilege, the user can modify record properties in the viewer.

Edit Custom Properties

Allows users to modify values for the custom properties that are associated with the record type.

When a user has both this privilege and the **Records > Open** privilege, the user can modify custom property values in the viewer.

When a user has both this privilege and the **View > Access** privilege, the user can modify custom property values in the explorer grid.

Edit Notes

Allows users to modify the record notes.

When a user has both this privilege and the **View > Access** privilege for at least one record view, the user can modify record notes in the explorer grid.

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can modify record notes from the viewer.

Delete

Allows users to delete records of this type in the file plan.

When a user has both this privilege and the **View > Access** privilege for at least one record view, the user can delete records of this type in the explorer grid.

Merge

When a user has both this privilege and the **File Plan > Content > Create/Append** privilege associated with the target record, the user can combine two or more records into a single record.

When a user also has the **View > Access** privilege for at least one record view, the user can merge records in the explorer grid.

Page Delete

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can delete a page from a record in the viewer. Users cannot restore deleted pages.

Page Reorder

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can modify the order of pages in a record in the viewer.

Move Page

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can remove a page from one record and add that page to another record independent of the file plan. Users can perform this action in the viewer.

Copy to Clipboard

Allows Interact Desktop users to copy the record page or region to the clipboard for use with Interact Desktop. To perform this action, users must also have the **View > Access** privilege for the associated record view and the **File Plan > Content > Open** privilege for the associated file plan.

Modify Page Properties

Allows users to modify metadata assigned to record pages. When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can modify page metadata in the viewer.

Record Type: Viewer

The following privileges appear in the Viewer category for Record Type privileges. When the privilege is granted, the user can perform the associated action in the viewer.

Print Record

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can print records from the viewer.

Save Local Copies

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can export and save one or more of the records displayed in the viewer to the local file system.

Launch Associated Application

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can open the current record using the designated application on the local system.

Email ImageNow Link

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can email an Perceptive Content link to a record from the viewer.

Email as Attachment

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can email a record from the viewer as an attachment.

Fax Record

When a user has both this privilege and the **Records > Open** privilege for the associated file plan or record type, the user can fax a record from the viewer.

Report Security Privileges

The following privileges are associated with Business Insight reports. You can assign report security privileges if you have the Manage Reports privilege. You cannot assign report security privileges to a group. These privileges are located on the Reports pane, in the Report Properties or Folder Properties dialog box, in the Security area of a report or a report folder.

Run

When the user has both this privilege and the **Report > View** privilege, the user can run the report from the explorer grid and save instances of the report for other users to view.

View

Allows users to view a saved instance of a report produced by a run or a schedule in the explorer grid and to email instances of reports to other users.

Workflow: Route Out Restrictions

In the Routes pane of a workflow queue, under Modify Routes Out, on the Restrictions tab, you can restrict users and groups who can route documents out of the queue. If the Route is marked as restricted, this privilege denies the user the ability to route the workflow item down this path.

Restrict Route Out

Restricts users from routing down a specific path. This privilege is compatible with the **Workflow Queue > Process**, **Workflow Queue > Upstream**, or **Workflow Queue > Anywhere** privileges. Users without any of these privileges are unable to route documents out of a queue.

Task Template Privileges

The following privileges are available for task templates. These privileges are located in the Security area of a task template.

Create

Allows users to create new tasks with this template and to modify, reassign, add comments to, return, and cancel tasks they created with this template.

When users have both this privilege and the **Documents > Open** privilege for the associated drawer or document type, they can create tasks for a document.

When a user has this privilege, the **Folder Type > Use** privilege, and the **Drawer > Content > Open** privilege, the user can create tasks for a folder.

Delete

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can delete tasks created with this template.

Manage

When a user has both this privilege and the **Global > Manage > Task Templates** privilege, the user can rename, copy, modify, or delete this task template.

Modify

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can modify, cancel, reassign, add comments to, or return tasks created with this template.

Review

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can review any task created with this task template. The Completion method for the task template must be set to Complete pending review to have tasks routed to reviewers.

View

When a user has both this privilege and the **Documents > Open** privilege for the associated drawer or document type, the user can view tasks created with this template.

A user with this privilege, much like an auditor, can view a task, but cannot make any changes to the task itself. Grant this privilege to a user who has no other task privileges.

Workflow: Application Plan

These queue-specific security settings only apply while the document is in the workflow queue.

Any user who is assigned to the queue with the **Workflow Queue > Process** privilege inherits these privileges. These settings override any privileges set in an application plan or at the user or group level.

These privileges are located in Workflow Designer, in the Applications area of the Queue Properties dialog box, on the Key Attributes tab.

Update Only Empty Key Values

Prevents users from overwriting the existing values in any of the document keys. This includes replacing an existing value with no value.

Without this selected, every key is updated, based on the configuration of the application plan, even if a field is undefined in the application plan. An undefined key overwrites (null) a value stored from the capture profile. This setting applies to all application plans selected for linking.

Modifiable

Allows users to re-link document keys or document properties with values from the business application or manual entry as defined by the application plan. This setting applies to all application plans selected for linking.

Allow Blank

Unless this privilege is granted for the current user, Perceptive Content verifies that any required document keys are created before the document is routed to the next queue. This setting applies to all application plans selected for linking.

Host Entry Validation

Verifies that the learn fields from the business application match the associated index keys before routing to the next queue.

This setting applies only to the application plan selected in the Validation Application Plan list. This setting only applies when one or more Host Validation check boxes are selected.

Manage departments

What is department administration?

Department administration provides the ability to administer multiple departments on a single Perceptive Content instance as if each department existed as a separate instance of Perceptive Content, allowing greater security and specificity for your entire organization. Perceptive Content departments provide the capability to separate the configuration components of Perceptive Content into logical business areas, such as departments of your company or geographic locations.

You can create a department that conveniently pertains to a particular section of your business with no content overlapping with other departments in your business. This setup keeps the department information secure from users in other departments. Departments are an effective way to give administrators access to every feature in Perceptive Content without giving those administrators access to information and features applicable to other departments in your business.

You must be granted at least one management privilege for a department to access that department in Management Console. You can have privileges to access more than one department but you can only access one department at a time in Management Console. When you select a department, every setting or feature you modify in Management Console applies to the selected department only.

The Perceptive Content installation automatically establishes a default department in which to work. Because department administration is an optional feature, you can choose not to create additional departments.

For example, your company has several different departments, including the Human Resources, Finance, Marketing, and Sales departments. Each of the four departments produces content in Perceptive Content that has little or no crossover with the other areas and each department tends to use Perceptive Content for entirely different purposes. To only allow users in each department to see the content and Perceptive Content architecture that pertains to them, you implement a Human Resources Department, Finance Department, Marketing Department, and Sales Department, and move all related content and users to the respective department.

In this scenario, if you want to create a drawer in the Marketing Department that the Sales Department can also use, you can choose to share the drawer. By sharing the drawer with the Sales Department, a Sales manager can now reference the Marketing drawer in the configuration options of the Sales department as if the drawer was in the Sales Manager s own department.

What is a department label?

You can set up a department label unique to your department that appears as a prefix for any future drawers, types, or other content created in Management Console for your department.

A department label ensures that all content types have a unique name in the system.When you create a department label, Perceptive Content automatically prefixes all applicable content names with the specified text. Content types generated automatically by the system also receive department labels. If you share content types prefixed with a department label with another department, the department label remains visible. Therefore, we recommend that you assign a department label to the content types that you do not anticipate sharing with other departments.

For example, if you set up department labels to apply to all created record folder types, and you create Sales - as a department label, then all future record folder types created in your department will have Sales - as a prefix in their title, such as Sales - Misc. Travel Expenses.

What are the cross department settings?

The cross department settings in Management Console exist separately from any one department and include various settings and features that apply to content in any number of departments.

When you access the cross department settings in Management Console, you can manage the following features, which are not available in any other location in Perceptive Content.

- Auditing
- Departments
- Diagnostics
- Digital Signatures
- Out of Office
- Reports
- Users

Several of the capabilities unique to Perceptive Managers are administered in the cross department settings under Department Management and Users. Other users gain access to these settings when they gain privileges to modify any of the settings or features.

You can choose to display or hide a group in any Cross Department Settings list. When you hide a group from Cross Department Settings, the system removes any global settings and instance-level privileges to the group that were previously assigned to the group. You cannot assign global settings and instance-level privileges to a hidden group.

Create a department

A department is a customized subsection of Perceptive Content Management Console that allows for greater security and specificity for a department in your organization. When you install or upgrade Perceptive Content, the server automatically creates a department named Default. To create an additional department or modify an existing department, complete the following steps.

Prerequisite To complete this procedure, you must be a Perceptive Manager.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Departments**.
3. In the right pane, complete one of the following steps.
   - To create a new department, click the **New** button.
   - To modify the name, department label, or description for an existing department, select the department from the **Departments** list and click the **Modify** button.
4. In the resulting dialog box, on the **General** tab, complete the following substeps.
   1. In the **Name** field, enter a unique name for the department.

2. In the **Department Label** field, enter a unique department label for the department. This department label automatically appears at the start of every naming field for a new content type or configuration created in the department.

   Example If you want every future document type created in your department to have the department label Sales - in its name by default, enter `Sales -`in the **Department Label** field.

3. Optional. In the **Description** field, enter a description for the department.

   Note: When you create a department, you can promote another user to the Department Manager role. View the Promote a user to Department Manager topic for instructions.

4. Click **OK**.

Select a department

If the Perceptive Manager grants you access to more than one Perceptive Content department, you can change between multiple departments while remaining on the same Management Console pane. After you switch departments, you continue to work in your newly selected department until you change to another department. To change your active department, complete the following steps.

Prerequisite You must either be a Department Manager for the target department or have at least one privilege for the target department.

1. In **Management Console**, in the left pane, under Select Department, select a department from the list.

Result Perceptive Content changes to the selected department. Any items you create or modify in Perceptive Content are saved to your newly active department. You can complete this procedure again to return to the previous department at any time.

About implementing department privileges

Privileges limit user access to certain views and functionalities within the system. You can modify user privileges and group privileges at both the global level and the department level.

Perceptive Managers are the only users who can assign every global privilege to users and groups. A Department Manager assigns department-level privileges, such as drawer and record privileges. You can grant non-manager users the ability to assign various categories of privileges to users and groups.

A privilege assigned to a user only applies in the context of the department where the privilege was assigned. For example, if a user has the Drawer Manage privilege, the user can only modify drawers in the in the department where that privilege was assigned. The exception to this rule is when you assign global privileges to users, because global privileges enable actions performed in the Cross Department Settings.

The same principles apply to group privileges. Unlike users, however, groups initially exist only in the department where the group was created. However, if you want to use a group in multiple departments, you can share the group.

If a group from another department has been shared with your department, you can assign privileges to that group, but you cannot rename the group or modify its group members. For example, Group A exists in the Sales department. When you share Group A with the HR department, an HR manager can assign privileges for the HR department to Group A. However, the HR manager cannot modify Group A s name or group members.

Manage transfer

What is a department transfer profile?

A department transfer profile is a single file that you edit to contain information about the components you want to transfer from one department to another in a transfer package.

Storing component information as a file allows you to stop the profile creation process at any time without losing information. You can modify the profile at a later time.

What is a department transfer package?

A department transfer package is a file generated by Perceptive Content that contains components you want to transfer from one department to another.

You transfer components from one department to another with a transfer profile and a transfer package.

A transfer package is exported from the originating department and imported into a destination department.

Department transfer components

You can transfer components from one department to another department in Perceptive Content.

You can transfer the following components.

- Address Books
- Annotations
- Application Plans
- Capture Profiles
- Custom Properties
- Cutoff Instructions
- Document Type Categories
- Document Type Lists
- Document Types
- Document Views
- Drawers
- File Plans
- Folder Type Lists
- Folder Types
- Folder Views

- Forms
- Forms-Data Definitions
- Forms-Designs
- Forms-Files
- Forms-Presentations
- Groups
- Output Profiles
- Picklists
- Record Category Types
- Record Connection Types
- Record Folder Types
- Record Folder Views
- Record Types
- Record Views
- Relationship Document Views
- Relationship Folder Views
- Retention Date Periods
- Retention Hold Reasons
- Retention Holds
- Retention Physical File Templates
- Retention Physical Locations
- Retention Physical Properties
- Retention Policies
- Retention Policy Authorities
- Source Profiles
- Task Reason Lists
- Task Templates
- Workflow Alarms
- Workflow Processes
- Workflow Reason Lists
- Workflow Rules

About transferring components to another department

You can transfer components from one department to another in a two-step process. You can only transfer from one department to another department at a time. You must be a Perceptive Content department manager of the originating department to transfer components out of that department. You must be a Perceptive Content department manager of the destination department to receive components transferred into that department.

In the first step of the transfer process, the department manager of the originating department creates a transfer profile that lists every component to permanently transfer to the destination department. Any component that can be shared between departments is eligible for transfer.

In the second step of the transfer process, the department manager of the destination department imports the transferred components as one package. As a result of the transfer, all components in the destination department are shared back to the originating department.

Transfer components between departments

To transfer components from one department to another department, complete the following procedures.

Prerequisite You must be a Perceptive Content department manager of the originating department to transfer components out of that department. You must be a Perceptive Content department manager of the destination department to receive components into that department.

1. In the originating department, create a transfer profile.
2. In the originating department, use the transfer profile to create and export a transfer package.
3. In the destination department, import a transfer package.

Create and export a transfer package

To transfer components from one department to another, complete the following steps.

Prerequisite Create a transfer profile.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **System Management**, then click **Department Transfers**.
3. In the right pane, on the **Department Transfers** tab, click **Export Package**.
4. In the **Export Package** dialog box, next to the **Profile** field, click the ellipsis button.
5. In the **Open** dialog box, navigate to the appropriate location and then select and open the transfer profile you want to use in the transfer package.
6. Next to the **Package** field, click the ellipsis button.
7. In the **Open** dialog box, navigate to the location where you want to create the transfer package.
8. In the **File name** field, type a name for the transfer package.
9. Click **Save**.
10. In the **Export Package** dialog box, click **OK**.

    Perceptive Content exports the transfer package to the location you specified.

Create a transfer profile

To create a department transfer profile, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **System Management**, then click **Department Transfer**.
3. In the right pane, on the **Department Transfer** tab, click **Edit Package Profile**.
4. In the **Department Transfer Profile Editor**, under **General Settings**, select the destination department for the transfer.
5. In the left pane, select one of the listed components and complete any of the following actions.
   - To add a component, from the upper window, select the component you want to add to your migration package and click **Add**.
   - To remove a component, under **Selected**, select the component you want to remove from your migration package and click **Remove**.
6. Click **File > Save As**. In the **Save As** dialog box, type a name for the transfer profile and click **Save**.
7. Close the **Department Transfer Profile Editor**.

Import a transfer package

After you export a transfer package with components from the originating department, you need to import it into the destination department. To import a transfer package, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **System Management** and click **Department Transfer**.
3. In the right pane, on the **Department Transfer** tab, click **Import Package**.
4. In the **Open** dialog box, navigate to the appropriate location and select the transfer package you want to import.
5. Click **Open** to import the package.
6. In the confirmation box, click **OK**.

Create a cross-department migration profile

To create a cross-department migration profile, complete the following steps.

Prerequisite You must be a Perceptive Manager to create a cross-department migration profile.

When creating a cross-department migration profile, the Select a Department list is enabled. You can switch between different departments and view and select items from each department to add them to the migration profile.

1. In **Perceptive Content Management Console**, in the left pane, in the Select Department list, select **Cross Department Settings**.
2. In the left pane, click **Migration**.
3. In the right pane, on the **Migration** tab, click **Edit Package Profile**.

4. In the **Migration Profile Editor** dialog box, for a new profile, click **File > New** to create a profile, or to modify an existing profile, click **File > Open** and choose the profile you want to modify.
5. Optional. To create privileges set for the migration components, in the left pane of the **Migration Profile Editor** dialog box, select **Custom Properties > Migrate user and group privileges with selected objects**.
6. Optional. In the left pane, select one of the listed components and do any of the following actions.
   - To add a component, from the upper window, select the component you want to add to your migration package and click **Add**.
   - To remove a component, under **Selected**, select the component you want to remove from your migration package and click **Remove**.
7. Optional. Click **File > Dependencies** to view dependencies that must be resolved in the target environment.

   The system lists which components it expects to exist in the target system. If they do not exist, the import process fails.
8. Complete one of the following actions.
   - If you are finished editing your migration profile, click **File > Save**.
   - If you want to save a copy of a new migration profile, click **File > Save As** and, in the **Save As** dialog box, type in a name and click **Save**.

Preview a transfer package

To preview a transfer package before importing components from one department to another, complete the following steps.

Prerequisite You must create a transfer profile and export the profile from the originating department to create a transfer package.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **System Management** and click **Department Transfer**.
3. In the right pane, on the **Department Transfer** tab, select **Import Preview**.
4. In the **Open** dialog box, select the transfer package you want to preview and click **Open**.
5. In the confirmation dialog box, click **OK**.

Modify a transfer profile

To modify a department transfer profile, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **System Management** and click **Department Transfer**.
3. In the right pane, on the **Department Transfer** tab, click **Edit Package Profile**.
4. In the **Department Transfer Profile Editor**, click **File > Open**.
5. Choose a transfer profile and click **Open**.
6. In the left pane, select one of the listed components and complete any of the following actions.

- To add a component, from the upper window, select the component you want to add to your migration package and click **Add**.
- To remove a component, under **Selected**, select the component you want to remove from your migration package and click **Remove**.

7. Click **File > Save**.

Share items with departments

What is shared department content?

You can share various items with other departments so users in those departments can access the content types.

When you share items created in your department with another department, users in the target department can access and use the shared items. However, only users from the originating department can modify shared items. You cannot unshare items.

When items have been shared with your department, they will appear in lists in dialog boxes accessible through Management Console. Although you cannot modify most shared items, you can assign privileges from your department to groups that have been shared with your department.

Share an item with another department

You can share an item created in Management Console among multiple departments. To share an item with other departments, complete one of the following procedures.

- Share a capture profile with another department.
- Share a connection type with another department.
- Share a custom property with another department.
- Share a data definition with another department.
- Share a drawer with another department
- Share a document type category with another department
- Share a document type list with another department
- Share a document view with another department
- Share a drawer with another department
- Share a fax recipient with another department
- Share a file plan with another department
- Share a folder type with another department
- Share a folder type list with another department
- Share a group with another department
- Share a picklist with another department
- Share a presentation with another department
- Share a record category type with another department
- Share a record folder type with another department

- Share a record type with another department
- Share a retention date period with another department
- Share a retention hold reason with another department
- Share a retention physical file template with another department
- Share a retention physical location with another department
- Share a retention physical property with anotherdepartment
- Share a retention policy authority with another department
- Share a source profile with another department
- Share a task reason list with another department
- Share a task template with another department
- Share a workflow process with another department
- Share a workflow reason list with another department
- Share a workflow rule with another department
- Share an application plan with another department

Share an application plan with another department

You can enable an application plan to share among multiple departments. To share an application plan with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing an application plan, and have a calculated design and implementation plan in place. Once you share an application plan, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Application Plans** and select an application plan level.
3. On the **Applications** tab, select an application plan and click **Share**.
4. In the **Share <*Application Plan*>** dialog box, select the departments you want to share the application plan with and click **OK**.

Share a capture profile with another department

You can enable a capture profile to share among multiple departments. To share a capture profile with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a capture profile, and have a calculated design and implementation plan in place. Once you share a capture profile, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Capture**.
3. On the **Capture Profile** tab, select a source profile and click **Share**.

4. In the **Share <*Capture Profile*>** dialog box, select the departments you want to share the capture profile with and click **OK**.

Share a source profile with another department

You can enable a source profile to share among multiple departments. To share a source profile with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a source profile, and have a calculated design and implementation plan in place. Once you share a source profile, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Capture**.
3. On the **Source Profile** tab, select a source profile and click **Share**.
4. In the **Share <*Source Profile*>** dialog box, select the departments you want to share the source profile with and click **OK**.

Share a document type category with another department

You can enable a document type category to share among multiple departments. To share a document type category with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a document type category, and have a calculated design and implementation plan in place. After you share a document type category, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Document Types**.
3. On the **Categories** tab, select a document type category and click **Share**.
4. In the **Share <*Document Type Category*>** dialog box, select the departments you want to share the document type category with and then click **OK**.

Share a document type list with another department

You can enable document type lists to share among multiple departments. To share document type lists with other departments, complete the following steps.

When you share a document type with another department, users can view and map all of the custom properties associated with the document type in the Application Plan Designer. **Important:** You should cautiously consider the impact of sharing a document type list, and have a calculated design and implementation plan in place. After you share a document type list, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Document Types**.

3. On the **Document Type Lists** tab, select a document type list and then click **Share**.
4. In the **Share <*Document Type Lists*>** dialog box, select the departments you want to share the document type list with and then click **OK**.

Share a document type with another department

You can enable a document type to share among multiple departments. To share a document type with other departments, complete the following steps.

When you share a document type with another department, users can view and map all of the custom properties associated with the document type in the Application Plan Designer. **Important:** You should cautiously consider the impact of sharing a document type, and have a calculated design and implementation plan in place. After you share a document type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Document Types**.
3. On the **Document Types** tab, select a document type and click **Share**.
4. In the **Share <*Document Types*>** dialog box, select the departments you want to share the document type with and then click **OK**.

Share a document view with another department

You can enable a document view to be shared among multiple departments. To share a document view with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a document view, and have a calculated design and implementation plan in place. After you share a document view, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Views**.
3. In the right pane, select the **Document** tab.
4. In the right pane, select the document view you want to share and then click **Share**.
5. In the **Share *Document View name*** dialog box, check the boxes of the departments with which you want to share the document view and then click **OK**.

Share a drawer with another department

You can enable a drawer to be shared among multiple departments. To share a drawer with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a drawer, and have a calculated design and implementation plan in place. After you share a drawer, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.

2. In the left pane, click **Drawers**.
3. In the right pane, select the drawer you want to share, and then click **Share**.
4. In the **Share *Drawer Name*** dialog box, check the boxes of the departments you want to share the drawer with, and then click **OK**.

Share a folder type list with another department

You can enable a folder type list to share among multiple departments. To share a folder type list with other departments, complete the following steps.

When you share a folder type with another department, users can view and map all of the custom properties associated with the folder type in the Application Plan Designer. **Important:** You should cautiously consider the impact of sharing a folder type list, and have a calculated design and implementation plan in place. After you share a folder type list, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Folder Types**.
3. On the **Folder Type Lists** tab, select a folder type list and click **Share**.
4. In the **Share *<Folder Type Lists>*** dialog box, select the boxes of the departments you want to share the folder type list with and then click **OK**.

Share a folder type with another department

You can enable a folder type to be shared among multiple departments. To share a folder type with other departments, complete the following steps.

When you share a folder type with another department, users can view and map all of the custom properties associated with the folder type in the Application Plan Designer. **Important:** You should cautiously consider the impact of sharing a folder type, and have a calculated design and implementation plan in place. After you share a folder type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Folder Types**.
3. In the right pane, select the folder type you want to share and then click **Share**.
4. In the **Share *<Folder Type name>*** dialog box, check the boxes of the departments with which you want to share the folder type and then click **OK**.

Share a group with another department

You can enable a user group to be shared among multiple departments. To share a group with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a group, and have a calculated design and implementation plan in place. After you share a group, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the

list.

2. In the left pane, click **Groups**.
3. In the right pane, select the group you want to share, and then click **Share**.
4. In the **Share *Group Name*** dialog box, check the boxes of the departments you want to share the group with, and then click **OK**.

Share an item with another department

You can share an item created in Management Console among multiple departments. To share an item with other departments, complete one of the following procedures.

- Share a capture profile with another department.
- Share a connection type with another department.
- Share a custom property with another department.
- Share a data definition with another department.
- Share a drawer with another department
- Share a document type category with another department
- Share a document type list with another department
- Share a document view with another department
- Share a drawer with another department
- Share a fax recipient with another department
- Share a file plan with another department
- Share a folder type with another department
- Share a folder type list with another department
- Share a group with another department
- Share a picklist with another department
- Share a presentation with another department
- Share a record category type with another department
- Share a record folder type with another department
- Share a record type with another department
- Share a retention date period with another department
- Share a retention hold reason with another department
- Share a retention physical file template with another department
- Share a retention physical location with another department
- Share a retention physical property with anotherdepartment
- Share a retention policy authority with another department
- Share a source profile with another department
- Share a task reason list with another department
- Share a task template with another department
- Share a workflow process with another department

- Share a workflow reason list with another department
- Share a workflow rule with another department
- Share an application plan with another department

Share a data definition with another department

To share an existing data definition file for a form, complete the following steps.

Before completing this procedure, you must upload the data definition files. **Important:** You should cautiously consider the impact of sharing a data definition, and have a calculated design and implementation plan in place. Once you share a data definition, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Forms**.
3. In the right pane, click **Manage Form Components**.
4. In the **Manage Form Components** dialog box, in the left pane, click **Data Definitions**.
5. In the right pane, select the XML file and then click **Share**.
6. In the **Share <*Data Definition*>** dialog box, select the boxes of the departments you want to share the data definition with and then click **OK**.

Share a form file with another department

To share an existing shared form file, complete the following steps.

Important: You should cautiously consider the impact of sharing a form file, and have a calculated design and implementation plan in place. Once you share a form file, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Forms**.
3. In the right pane, click **Manage Form Components**.
4. In the **Manage Form Components** dialog box, in the left pane, click **Shared Files**.
5. In the right pane, select the form file and then click **Share**.
6. In the **Share <*Shared Files*>** dialog box, select the boxes of the departments you want to share the form file with and then click **OK**.

Share a form with another department

You can enable forms to share among multiple departments. To share forms with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a form, and have a calculated design and implementation plan in place. Once you share a form, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.

2. In the left pane, click **Forms**.
3. In the right pane, select a form from the list and click **Share**.
4. In the **Share *<Form>*** dialog box, select the departments you want to share the form with and click **OK**.

Share a presentation with another department

To share an existing presentation for a form, complete the following steps.

Before completing this procedure, you must upload the presentation files.**Important:** You should cautiously consider the impact of sharing a presentation, and have a calculated design and implementation plan in place. Once you share a presentation, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Forms**.
3. In the right pane, click **Manage Form Components**.
4. In the **Manage Form Components** dialog box, in the left pane, click **Presentations**.
5. In the right pane, select the presentation and then click **Share**.
6. In the **Share *<Presentation>*** dialog box, select the boxes of the departments you want to share the presentation with and then click **OK**.

Share a fax recipient with another department

You can specify fax recipients to share among multiple departments. To share fax recipients with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a fax recipient, and have a calculated design and implementation plan in place. Once you share a fax recipient, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Output Profiles**.
3. On the **Fax Recipients** tab, select a contact from the list and click **Share**.
4. In the **Share *<Fax Recipients>*** dialog box, select the departments you want to share the fax recipients with and click **OK**.

Share a custom property with another department

To share a custom property with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a custom property, and have a calculated design and implementation plan in place. Once you share a custom property, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Custom Properties**.

3. In the right pane, select the custom property you want to share, and then click **Share**
4. In the **Share <Property Type>** dialog box, check the boxes of the departments you want to share the custom property with, and then click **OK**.

Share a connection type with another department

You can enable Connection types to share among multiple departments. To share Connection types with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a connection type, and have a calculated design and implementation plan in place. Once you share a connection type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Connection Types**.
3. On the **Connection Types** tab, select a connection type and click **Share**.
4. In the **Share <*Connection Types*>** dialog box, select the check boxes of the departments you want to share the Connection types with and then click **OK**.

Share a cutoff instruction with another department

You can enable cutoff instructions to share among multiple departments. To share cutoff instructions with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing cutoff instructions, and have a calculated design and implementation plan in place. Once you share cutoff instructions, you cannot unshare or delete them from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Cutoff Instructions**.
3. On the **Cutoff Instructions** tab, select a cutoff instruction from the list and click **Share**.
4. In the **Share <*Cutoff Instructions*>** dialog box, select the departments you want to share the cutoff instruction with and click **OK**.

Share a file plan with another department

You can enable a file plan to share among multiple departments. To share a file plan with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a file plan, and have a calculated design and implementation plan in place. Once you share a file plan, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **File Plans**.
3. On the **File Plans** tab, select a file plan and click **Share**.

4. In the **Share <*File Plan*>** dialog box, select the departments you want to share the file plan with and then click **OK**.

Share a picklist with another department

You can enable picklists to share among multiple departments. To share picklists with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a picklist, and have a calculated design and implementation plan in place. Once you share a picklist, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Picklists**.
3. In the Picklists pane, select a picklist, and click **Share**.
4. In the **Share <*Picklist*>** dialog box, select the departments you want to share the picklist with and click **OK**.

Share a record category type with another department

You can enable record category types to share among multiple departments. To share record category types with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a record category type, and have a calculated design and implementation plan in place. Once you share a record category type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Record Category Types**.
3. On the **Record Category Types** tab, click **Share**.
4. In the **Share <*Record Category Types*>** dialog box, select the boxes of the departments you want to share the record category types with, and then click **OK**.

Share a record folder type with another department

You can enable record folder types to share among multiple departments. To share record folder types with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a record folder type, and have a calculated design and implementation plan in place. Once you share a record folder type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Record Folder Types**.
3. On the **Record Folder Types** tab, select a record folder type and click **Share**.

4. In the **Share <*Record Folder Types*>** dialog box, select the check boxes of the departments you want to share the record folder types with and then click **OK**.

Share a record type with another department

You can enable record types to share among multiple departments. To share record types with other departments, complete the following steps.

When you share a record type with another department, users can view and map all of the custom properties associated with the record type in the Application Plan Designer. **Important:** You should cautiously consider the impact of sharing a record type, and have a calculated design and implementation plan in place. Once you share a record type, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Records** and click **Record Types**.
3. On the **Record Types** tab, select a record type from the list and click **Share**.
4. In the **Share <*Record Types*>** dialog box, select the departments you want to share the record type with and click **OK**.

Share a retention date period with another department

You can enable a retention date period to share among multiple departments. To share a retention date period with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention date period, and have a calculated design and implementation plan in place. Once you share a retention date period, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Policies**.
3. On the **Date Periods** tab, select a date period and click **Share**.
4. In the **Share <*Retention Date Period*>** dialog box, select the boxes of the departments you want to share the retention date period with and then click **OK**.

Share a retention hold reason with another department

You can enable retention hold reasons to share among multiple departments. To share retention hold reasons with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention hold reason, and have a calculated design and implementation plan in place. Once you share a retention hold reason, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Holds**.

3. On the **Reasons** tab, select a retention hold reason and then click **Share**.
4. In the **Share <*Retention Hold Reason*>** dialog box, select the boxes of the departments you want to share the retention hold reason with and then click **OK**.

Share a retention hold with another department

You can enable a retention hold to share among multiple departments. To share a retention hold with another department, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention hold, and have a calculated design and implementation plan in place. Once you share a retention hold, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Holds**.
3. Select a retention hold and then click **Share**.
4. In the **Share <*Retention Hold* >** dialog box, select the boxes of the departments you want to share the retention hold with and then click **OK**.

Share a retention physical file template with another department

You can enable retention physical file template to share among multiple departments. To share retention physical file template with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention physical file template, and have a calculated design and implementation plan in place. Once you share a retention physical file template, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Physical Locations**.
3. On the **Physical File Templates** tab, select a physical file template, and then click **Share**.
4. In the **Share <*Physical File Templates*>** dialog box, select the boxes of the departments you want to share the physical file template with, and then click **OK**.

Share a retention physical location with another department

You can enable a retention physical location to share among multiple departments. To share a retention physical location with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention physical location, and have a calculated design and implementation plan in place. Once you share a retention physical location, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Physical Locations**.

3. On the **Physical Locations** tab, select a physical location and click **Share**.
4. In the **Share <*Physical Locations*>** dialog box, select the boxes of the departments you want to share the retention physical location with and then click **OK**.

Share a retention physical property with another department

You can enable a retention physical property to share among multiple departments. To share a retention physical property with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention physical property, and have a calculated design and implementation plan in place. Once you share a retention physical property, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Physical Locations**.
3. On the **Physical Properties** tab, select a physical property and click **Share**.
4. In the **Share <*Physical Property*>** dialog box, select the departments you want to share the physical property with and then click **OK**.

Share a retention policy authority with another department

You can enable retention policy authorities to share among multiple departments. To share a retention policy authority with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention policy authority, and have a calculated design and implementation plan in place. Once you share a retention policy authority, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Policies**.
3. On the **Policy authorities** tab, select a policy authority and click **Share**.
4. In the **Share <*Policy authority*>** dialog box, select the check boxes of the departments you want to share the retention policy authority with and click **OK**.

Share a retention policy with another department

You can enable a retention policy to share among multiple departments. To share a retention policy with another department, complete the following steps.

Important: You should cautiously consider the impact of sharing a retention policy, and have a calculated design and implementation plan in place. Once you share a retention policy, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, expand **Retention** and click **Policies**.

3. On the **Policies** tab, select a policy and then click **Share**.
4. In the **Share <*Retention Policy*>** dialog box, select the boxes of the departments you want to share the retention policy with and then click **OK**.

Share a task reason list with another department

You can enable a task reason list to share among multiple departments. To share a task reason list with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a task reason list, and have a calculated design and implementation plan in place. Once you share a task reason list, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Tasks**.
3. In the right pane, in the **Reason Lists** tab, select the task reason list you want to share and then click **Share**.
4. In the **Share <*Reason list name*>** dialog box, check the boxes of the departments with which you want to share the task reason list and then click **OK**.

Share a task template with another department

You can enable a task template to be shared among multiple departments. To share a task template with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a task template, and have a calculated design and implementation plan in place. Once you share a task template, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Tasks**.
3. In the right pane, on the **Templates** tab, select the task template you want to share and then click **Share**.
4. In the **Share <template name>** dialog box, check the boxes of the departments you want to share the task template with and then click **OK**.

Share a workflow alarm with another department

To share a workflow alarm with another department, complete the following steps.

Important: You should cautiously consider the impact of sharing a workflow alarm, and have a calculated design and implementation plan in place. Once you share a workflow alarm, you cannot unshare or delete it from the system.

1. In **Workflow Designer**, double-click the queue containing the alarm.
2. In the **Queue Properties** dialog box, in the left pane, click **Alarms**.

3. In the right pane, select the alarm, and click **Share**.

   Note: If the Share button is disabled, the alarm is not available for the current department.

4. In the **Share <*Alarm*>** dialog box, check the boxes of the departments you want to share the alarm with, and click **OK**.
5. In the **Share <*Alarm*>** confirmation dialog box, click **OK**.

Share a workflow process with another department

You can enable a workflow process to share among multiple departments. To share a workflow process with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a workflow process, and have a calculated design and implementation plan in place. Once you share a workflow process, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Workflow**.
3. In the right pane, select the workflow process you want to share, and then click **Share**.
4. In the **Share <process name>** dialog box, select the departments you want to share the workflow process with, and then click **OK**.

Share a workflow reason list with another department

You can enable a workflow reason list to share among multiple departments. To share a workflow reason list with other departments, complete the following steps.

Important: You should cautiously consider the impact of sharing a workflow reason list, and have a calculated design and implementation plan in place. Once you share a workflow reason list, you cannot unshare or delete it from the system.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Workflow**.
3. In the right pane, in the **Reason Lists** tab, select the workflow reason list you want to share and then click **Share**.
4. In the **Share <*Reason list name*>** dialog box, check the boxes of the departments with which you want to share the workflow reason list and then click **OK**.

Share a workflow rule with another department

To share a workflow routing or alarm rule with another department, complete the following steps.

Important: You should cautiously consider the impact of sharing a workflow rule, and have a calculated design and implementation plan in place. Once you share a workflow rule, you cannot unshare or delete it from the system.

1. In **Workflow Designer**, in the **Tasks** pane, click **Actions**.
2. Click **Manage Actions**.
3. In the **Action Settings** dialog box, on the **Rules** tab, select the rule that you want to share and click **Share**.
4. In the **Share <*Rule*>** dialog box, check the boxes of the departments you want to share the reason list with and then click **OK**.
5. In the **Share <*Rule*>** confirmation dialog box, click **OK**.
6. In the **Actions Settings** dialog box, click **OK**.

Delete a shared item

You can delete a shared item from its source department as long as the shared item is not referenced by any configurations in other departments. To delete a shared item, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select the department where the shared item was created.
2. In the left pane, select an option, such as **Custom Properties** or **Drawers**.
3. In the right pane, select the item you want to delete and click the **Delete** button.
4. In the **Delete** dialog box, click **Yes**.

Manage migration

What is migration?

Migration enables you to create a Perceptive Content test environment with components and subcomponents, such as drawers and departments, for the purpose of testing the new Perceptive Content environment before putting it into production.

When you migrate components, you also must migrate all the associated document types and privilege assignments. For example, when you migrate a drawer that has a defined folder hierarchy, you must also migrate all folder types represented in the drawer's folder hierarchy. To migrate drawers, you must also migrate groups, and vice versa.

You can migrate Record components, including File Plans, Record Category Types, Record Folder Types, and Record Types.

For example, you can first create a workflow process in a test environment and then when you are finished testing, you can migrate the workflow process to your production environment. The environment to which you want to migrate is called the target environment, and the environment you are migrating from is called the source environment.

Migration functionality is enabled for Perceptive Managers and Department Managers by default. However, cross-department migration profiles can only be created by Perceptive Managers. You can disable migration for all users using an INI setting.

Migration components

You can only migrate components between instances of the same version of Perceptive Content. We recommend that you back up your target environment before migrating components.

Components that can be migrated are:

- Application Plans
- Capture and Source Profiles
- Custom Properties
- Document type Lists
- Document Types
- Drawers
- File Plans
- Folder and Document Views
- Folder Type Lists
- Folder Types
- General Settings
- Groups
- Record Category Types
- Record Folder Types
- Record Types
- Workflow Processes

Components and component references

Check these components and component references when you preview a migration package.

Duplicate Components and Component References

The following components can be duplicated in the target environment. Perceptive Content automatically overwrites duplicate components and component references.

- Application plans
- Custom property
- Document type
- Document type list
- File plans
- Folder type
- Folder type list
- Public filter
- Record category types

- Record folder types
- Record types
- View
- Workflow process
- Workflow routing rule
- Workflow alarm

Missing Components and Component References

The following components or component references may be missing in the migration package or target environment.

- Client script
- Custom property
- Custom property list values
- Document type
- Drawers
- File plans
- Folder type
- Form
- Group
- Predefined list
- Reason list
- Record category types
- Record folder types
- Record types
- Sequence
- User
- Workflow alarm
- Workflow routing rule

About migrating views

Views that are customized for items and containers can be migrated along with the other migration components.

When migrating views, if the same item or container view exists on both the source and the target environment, but the target environment includes public filters that do not exist in the source environment, Perceptive Content deletes these public filters as part of the migration process. Private filters are not included in the view migration.

If the source environment includes private filters that you want to migrate to the target environment, ask your view manager to publish the private filters prior to migration. If a view in the source environment includes custom property columns or search conditions, but the custom properties do not exist in the target environment, the import process fails.

About renaming queues

If you rename a queue for a workflow process in a source environment that you previously migrated to a target environment, and you then migrate that same process again, Perceptive Content removes the original queue from the target environment and replaces it with the newly renamed queue.

> For example, suppose you migrate the HR process from a test server to a production server. This process contains the HR Generalist 1 queue. After the migration, you rename the HR Generalist 1 queue to Generalist on the test server, and you migrate the HR process to production again. In this scenario, Perceptive Content removes the HR Generalist 1 queue and all items in this queue on the production server and replaces it with the Generalist queue.

Manage migration profiles

What is a migration profile?

A migration profile is a single file that contains information about the components you want to migrate.

You manage migration using migration profiles and migration packages. Storing this information as a file allows you to stop the creation process without losing information and then modify the profile later. A migration package contains the components you want to migrate.

Migration functionality is enabled for Perceptive Managers by default. You can disable migration for all users using an INI setting.

Create or modify a migration profile

To create or modify a migration profile, complete the following steps.

When creating a department-specific migration profile, the Select Department list on the Migration Profile Editor dialog box displays the same department that was selected in Management Console, and the ability to select a department is disabled. The items displayed on the right-side of the Migration Profile Editor dialog box are the items owned by the selected department.

1. In **Management Console**, in the left pane, click **Migration**.
2. Optional. For a department-specific profile, in the left pane, in the **Select Department** list, select a department and then click **Migration**.
3. In the right pane, on the **Migration** tab, click **Edit Package Profile**.
4. In the **Migration Profile Editor** dialog box, complete any of the following actions.
   - To create a new profile, click **File > New**.
   - To modify an existing profile, click **File > Open** and choose the profile you want to modify.
5. Optional. To create a privileges set for the migration components, in the left pane of the **Migration**

Profile Editor dialog box, select **Custom Properties > Migrate user and group privileges with selected objects**.

6. Optional. In the left pane, select one of the listed components and complete any of the following actions.
   - To add a component, from the upper window, select the component you want to add to your migration package and click **Add**.
   - To remove a component, under **Selected**, select the component you want to remove from your migration package and click **Remove**.
7. Optional. Click **File > Dependencies** to view dependencies that must be resolved in the target environment.

   The system lists which components it expects to exist in the target system. If those components do not exist, the import process fails. Migrating groups with department privileges and Migrate Privileges enabled results in the display of missing references to those departments. Ensure all departments in the list are correct and also exist in the target system.
8. To save the migration profile, complete one of the following actions.
   - If you are finished modifying an existing migration profile, click **File > Save**.
   - If you want to save a copy of a new migration profile, click **File > Save As** and, in the **Save As** dialog box, type a name and click **Save**.

Export a migration package

To move the component settings from your source environment to a target environment, complete the following steps.

Prerequisite To export a migration package, you first need to create a migration profile. You also must have administrative privileges.

The migration package file may contain confidential information. We recommend that you take steps to protect the file so that it can only be readable by the appropriate individuals.

1. In **Management Console**, in the left pane, click **Migration**.
2. In the right pane, on the **Migration** tab, click **Export Package**.
3. In the **Export Package** dialog box, click the ellipsis button next to the **Profile** field.
4. In the **Open** dialog box, navigate to the appropriate location and then select and open the migration profile or profiles you want to use in the migration package.
5. Click the ellipsis button next to the **Package** field.
6. In the **Open** dialog box, navigate to the location where you want to create the migration package.
7. In the **File name** field, type a name for the migration package.
8. Click **Open**.

   Perceptive Content exports the migration package to the location you specified.

Import a migration package

After you export a migration package from your source environment, you need to import it into a target environment. To apply the defined component settings from the migration profiles to your target environment, complete the following steps.

1. Back up your target environment.
2. Preview your migration package to check for and correct any reference errors.
3. In **Management Console**, in the left pane, click **Migration**.
4. In the right pane, on the **Migration** tab, click **Import Package**.
5. In the **Open** dialog box, navigate to the appropriate location and then select the migration package you want to import.
6. Click **Open**.
7. In the confirmation box, click **Yes** to import the migration package.

Preview a migration package

After you export your migration package from your source environment, check for discrepancies between environments before you import your migration package into your target environment. If there are any reference errors between the two environments, you can correct them so the import will be successful. To compare the target and source environments and correct any reference errors, complete the following steps.

Prerequisite You must create a migration profile, add it to a migration package, and export from your source environment.

1. In **Management Console**, in the left pane, click **Migration**.
2. In the right pane, on the **Migration** tab, click **Import Preview**.
3. In the **Open** dialog box, select the migration package you want to preview and click **Open**.
4. Do one of the following actions:
   - In the confirmation box, click **Yes** to import the package.
   - In the confirmation box, click **No** to close the confirmation box.
5. If you clicked Yes, in the **Import Package** dialog box, note the components and component references that must be resolved before importing the migration package, click **Close**, and then do one of the following actions:
   - If there is a duplicate component or component reference, remove it from the migration package or the target environment.
   - If a component or component reference is missing, create it in the target environment or remove it from the migration package.

Run diagnostics

Status Report

What is the ImageNow Server Resource Status report?

The ImageNow Server Resource Status report contains information about the current state of the ImageNow Server resources.

View ImageNow Server Resource Status report

To view the ImageNow Server Resource Status report, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. Click **Status Report**.
3. On the **Diagnostics** tab, in the right pane, click **Status Report**.
   The resource information appears.
4. To update the information, click **Refresh**.

Client Performance

What is ImageNow Client performance reporting?

Perceptive Content Client performance reporting lets you track performance of several key operations in ImageNow Client from the end-user perspective.

Performance reports can track the following operations:

- ImageNowViewer. How long it takes to open an item.
- Perceptive Content Workflow. How long it takes to route an item forward.
- Perceptive Content Form. How long it takes to open a form.
- Perceptive Content Capture. How long it takes to capture either a single item in Single Mode or a set of items in Package Mode.

ImageNow Client stores the recorded information in the content database. The information is first collected as detailed data, but can be optionally averaged and stored as condensed data to save hard drive space.

What is Job Manager?

The Job Manager console lets you view and manage job queues that are set to automatically process items.

If you are waiting for an agent, such as Output Agent or Recognition Agent, to automatically complete a task, you can inspect the corresponding queue to view information about the job. The queue displays information about the current status of each job type, details for each job within a job type, and offers the options to resume or suspend a job. You can also choose to print job details from the Job Manager.

About rating your system performance

The Perceptive Content Experience Index is a tool you can use to rate the performance of your ImageNow Server or ImageNow Client.

This tool rates several necessary components for any computer installed with either ImageNow Client or ImageNow Server, including the performance of the processor, memory, and hard disk. Use the resulting rating to make sure you meet the minimum requirements as described in the Product Technical Specifications or to evaluate your system performance at any time.

The ImageNow Server Experience Index returns a number, ranking the performance from 1 (lowest) to 10 (highest). The rating represents system-specific performance, with any rating less than or equal to 2.9 signifying that your computer does not meet minimum system requirements.

ImageNow Client detailed performance report data

After you configure reporting thresholds, you can export the data as a report. Each instance in the report table represents a single event. The following elements are included in the report.

Data	Description
Server Name	Specifies the name of the Perceptive Content server.
Username	Specifies the user who experienced the event.
Client	Specifies the client used.
Node Name	Specifies the workstation or machine name.
Event Name	Specifies the event, such as EventA.
Event Category	Specifies the category of the event, either Forms, Viewer, or Workflow.
Data Size	Specifies the size of the event data. The unit of measurement depends on the event. Events that download data are typically measured in bytes but may also be measured in megabytes. For example: When measuring the Document Open event, the size of the first page is tracked because it helps interpret the cost associated with the event. Document size is related to the amount of time it takes to download and open the document. If the document is several megabytes, it takes longer to download and render.

Data	Description
Data Cost	Specifies the cost for the event. The unit of measurement is seconds.
Time	Specifies the time and day that the event occurred.
Is Error	Specifies whether an error occurred during the event. A 1 value indicates there was an error.
Param Type	Specifies the parameter type of the event, set by the developer to provide detailed information about the event.
Param Value	Specifies the parameter value of the event, set by the developer to provide detailed information about the event.

Configure an ImageNow Client performance report

ImageNow Client performance reports collect data on the effectiveness of Perceptive Content's performance. After you export the report, you can view the report data. To set up reporting behavior, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Diagnostics**.
3. In the right pane, click **Client Performance**.
4. In the right pane, on the **Configuration** tab, select **Start collecting performance data**.
5. Under **Data Collection Categories**, complete one of the following options.
   - To collect data from specified categories regardless of threshold settings, select **Always collect data for selected categories**.
   - Select **Collect data using category thresholds** to collect only data with a percentage of measurements exceeding the threshold time, specifying the whole number percentage threshold.

   Note: When the percentage of documents exceed the specified threshold, the data is included in the report. For example, setting the percentage threshold to 10% means that if 10% of the data points exceed the threshold, the event appears in the performance report.
6. In the category selection table, do the following substeps.
   1. Select the check box for the category you want to track.
   2. For each selected category, if you are using category thresholds, specify the number of seconds you want to establish as the threshold. Any events that exceed the threshold appear in **Threshold Count** in the performance report.

7. Under **Clean Up Data**, set up cleaning behavior using the following substeps:
    1. Select **Delete** to enable periodic deletion of performance data. In the **After (days)** box, enter the number of days after which you want to delete the performance data.
    2. Select **Condense for storage on delete** to create a separate report that contains averaged condensed records of the performance data when a delete occurs.
    3. Select **Delete condensed performance data** to enable periodic deletion of condensed data. In the **After (days)** box, enter the number of days after which you want to delete the condensed data.

Export a condensed performance report

ImageNow Client stores snapshots of Perceptive Content data over time as condensed performance data. To create a report based on collected condensed performance data, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the right pane, click **Client Performance**.
3. On the **Condensed Export** tab, complete the following substeps.
    1. In the **Export Range** section, specify the date range and time span in hours for the data you want to include in the report.
    2. In the **Averaging Interval** section, select the regular interval of time during which you want data averaged in the report.

    Note: If the total time span is not divisible by the averaging interval, the last interval ends as soon as the selected time span occurs.
4. Click **Export**.
5. In the **Save As** dialog box, specify the file name and location, and then click **Save**.

Export a detailed performance report

To create a report based on detailed performance data, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the right pane, click **Client Performance**.
3. On the **Detailed Export** tab, complete the following substeps.
    1. In the **Export Range** section, specify the time span for the data you want to include in the report.
    2. In the **Application** section, select the client applications you want to include in the report.
    3. In the **Users** section, select the users you want to include in the report.
4. Click **Export**.
5. In the **Save As** dialog box, specify the file name and location and click **Save**.

Logging

What are ImageNow log files?

Perceptive Content log files track events, allowing you to detect and troubleshoot problems in your system.

Any ImageNow Client user can turn on logging and specify the amount of detail that is written to a log file. Separate log files are maintained for each user that is defined in the Management Console. Any action that a user performs on an log file only affects the server activity that is occurring while the user is logged in.

There are two log files. The Controller log tracks activities on the ImageNow Client. The ImageNow Server log tracks activities on the ImageNow Server and can be turned on or off, exported, and deleted by any user with **Global > Manage > Server Administrator** privileges or higher. When an error occurs, you can view details about the error in the appropriate log file and work on resolving the problem. In some instances, you might be asked to send a log file to Technical Services for assistance in resolving an error.

In addition, the user can specify the amount of detail that is written to the ImageNow Server log by setting its level from 1 to 6. The default setting is 0, which means that server logging is turned off. The higher the setting, the more activity detail is written to the log file. Setting the Log Level to 6 results in large log files. Leaving the Log Level set at 6 for an extended period of time can create massive log files that occupy valuable disk space.

Create a log file

Log files track user activities on Perceptive Content, and can be turned on and off, viewed, or deleted by any user on the server. To create a log file for the ImageNow Client or the ImageNow Server, complete one of the following procedures.

1. Use one of the following procedures to create a log file for **Perceptive Content**.

Situation	Steps
Create a controller log file forImageNow Client.	1. Hold down the `SHIFT` key and right-click in the Perceptive Content title bar. 2. Point to **Logging**, and then click **Low**, **Medium**, or **High**.
Create a server log file	1. On the Perceptive Content toolbar, click **Manage**. 2. In the **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list. 3. In the left pane, click **Users**. 4. In the right pane, on the **User Profiles** tab, in the **Search for users** box, type all or some of a user name, first or last name and

Situation	Steps
	then click **Search**. In the **Select a user** list, which you can sort in ascending or descending order by clicking the column headers, select a user and then click **Logging**. 5. In the **Logging** dialog box, select a **Server Log Level** from 1 to 6, depending on the amount of detail you want to be written to the log file. Level 1 writes the least, and Level 6 writes the most. 6. Click **OK**.

Next To stop server logging, set Server Log Level to Default or 0.

Configure logging

You configure logging by making changes in the `[Logging]` section in the *ImageNow.ini* file. To configure logging, complete the following steps.

1. On the **Perceptive Content** toolbar, hold down the `SHIFT` key and right-click in the **Perceptive Content** title bar.
2. Click **Open configuration file**.

   The *ImageNow.ini* file appears.
3. Make the appropriate changes in the `[Logging]` section.

   Note: The `debug.level.file=1` setting means that Controller logging is turned on, and the `debug.level.file=0` setting means that Controller logging is turned off.
4. Save the *ImageNow.ini* file.

Include socket communication in server log

Socket communication, also known as stream level logging, is a separate level of logging from debug that shows what information is passed on the wire between the server and ImageNow Client. To specify whether to include socket communication in the server log file, complete the following steps.

The Log server communication to include socket log file used in this procedure is the equivalent of the `stream.debug.log.level` and `stream.info.log.level` settings.

1. In **ImageNow Client**, hold down the SHIFT key and right-click in the **Perceptive Content** title bar.
2. Click **Logging > Log server communication to include socket log file**.

Delete a controller log file

To delete a controller log file, complete the following steps.

1. On the toolbar, hold down the `SHIFT` key and right-click inside the title area.
2. Click **Delete log file**.

Enable rolling log files

To enable rolling log files, complete the following steps.

1. Open the *inow.ini* file or *inserver.ini* configuration file, located at one of the following directories, depending on your environment:
   - In a 32-bit **Windows** environment, open the configuration file in the *[drive:]\inserver\etc* directory.
   - In a 64-bit **Windows** environment, open the configuration file in the *[drive]:\inserver64\etc* directory.
   - In **UNIX** or **Linux**, open the configuration file in the *$(IMAGENOWDIR)/etc* directory.
2. Under the `[Logging]` group, complete the following substeps.
   1. Set `rolling.log.files.enabled` to `TRUE`.
   2. Set `rolling.log.file.threshold` to a positive integer that represents the maximum log file size in MB. The default is 100.
3. Save and close the configuration file.

Change the Perceptive Content log file directory location

To change the location of the Perceptive Content log file directory from its default location, complete the following steps.

1. Perform one of the following options to open the *inow.ini* configuration file:
   - In **Windows**, navigate to *[drive:]\inserver\etc* and open the *inow.ini* file with a text editor.
   - In **UNIX** or **Linux**, navigate to *$(IMAGENOWDIR)/etc* and open the *inow.ini* file with a text editor.
2. Under the `[Directory Locations]` group, change the `logging.dir` setting to the directory location you want to store log files.
3. Save and close the *inow.ini* file.

   Generated log files are stored in the specified directory, not in *$(IMAGENOWDIR)/log* or *[drive:]\inserver\log*.

Archive log reports

To configure Monitor Agent to archive log files in response to an event, complete the following steps.

1. Navigate to the ***[drive:]\inserver\etc*** folder, and then in a text editor, open the *inserverMonitor.ini* file.
2. To specify the agent for which you want to archive log files, under the [Processes] group, create the following string where <DefinedProcess> is the agent you want to restart, and event<n> is a consecutively numbered event:

Example `<DefinedProcess>.event<n> = TimeOfDay`

3. In the following, **Monitor Agent** performs an action on the day and time you defined in the [Defines] group:

   Example `AlarmAgent.event4 = TimeOfDay`

4. Optional. To override the default time of day or day specified in the [Defaults] group, complete any of the following substeps:
   1. To override the default time of day, create a new string identical to the string you created in step 1 and append .time to the string. Set the value equal to time represented by a 24-hour period. In the following, **Monitor Agent** triggers an event to perform an action at 7:00 AM on the day you defined in the [Defines] group:

      Example `AlarmAgent.event4 = TimeOfDayAlarmAgent.event4.time = 07:00`

   2. To override the default day specified in the [Defaults] group, create a new string identical to the string you created in step 1 and append .day to the string. Set the value equal to the day of the week, or EVERYDAY to include all days. In the following, **Monitor Agent** triggers an event to perform an action every Tuesday at the time you defined in the [Defines] group:

      Example `AlarmAgent.event4 = TimeOfDayAlarmAgent.event4.day = TUESDAY`

5. To specify that **Monitor Agent** archives log reports on the defined or overridden day and time, create the following string where <DefinedProcess> is the agent you want to restart, and event<n> is a consecutively numbered event and action<n> is a consecutively numbered action:

   Example `<DefinedProcess>.event<n>.action<n> = Archive`

   Example In the following, Monitor Agent archives Alarm Agent log files at 1:00 AM every Sunday:`AlarmAgent.event4 = TimeOfDayAlarmAgent.event4.time = 01:00AlarmAgent.event4.day = SUNDAYAlarmAgent.event4.action1 = Archive`

6. Optional. To override the archival behavior specified in the [Defaults] group, complete any of the following substeps:
   1. To override the default archive directory specified in the [Defaults] group, create a new string identical to the string you created in step 3 and append .ArchiveDirectory to the string. Set the value equal to the directory to which you want **Monitor Agent** to archive the files. In the following example, **Monitor Agent** archives log files to c:\logs:

      Example `AlarmAgent.event4.action1.ArchiveDirectory = c:\logs`

   2. To override the default files to archive specified in the [Defaults] group, create a new string identical to the string you created in step 3 and append .Defaults to the string. Set the value equal to AllLogs to archive all logs recorded, or AllBeforeToday to archive logs recorded before the current date. In the following example, **Monitor Agent** archives all logs regardless of log date:

      Example `AlarmAgent.event4.action2.Defaults = AllLogs`

   3. To override the default file type specified in the [Defaults] group, create a new string identical to the string you created in step 3 and append .ArchiveFileType to the string. Set the value equal to the file type you want **Monitor Agent** to use for the log files. In the following example, **Monitor**

Agent uses .txt as the file type:

Example `AlarmAgent.event4.action3.ArchiveFileType = .txt`

4. To override the default inclusion of subdirectories specified in the [Defaults] group, create a new string identical to the string you created in step 3 and append .ArchiveSearchSubDirectories to the string. Set the value equal to TRUE to include subdirectories, or FALSE to exclude subdirectories. In the following example, **Monitor Agent** includes subdirectories when searching for archive files:

   Example `AlarmAgent.event4.action4.ArchiveSearchSubDirectories = TRUE`

7. Save and close the *inserverMonitor.ini* file.

Real Time Telemetry System

What is performance monitoring logging?

Performance monitoring logging captures details of all of the actions taken by each ImageNow Server process (service) and places the information in log files that you generate.

For example, you can monitor actions such as server calls and queries. In addition, you can monitor details about execution plans for SQL queries and use these log files either to analyze and improve communication with the Perceptive Content database or to enhance slow running queries.

The two types of RTTS performance logs are explained in the following examples.

- General action types are logged in the *<servicename>_performancestats_<date>.log* files. Examples are inserver_performancestats_20081009.log or inserverWorkflow_performancestats_20081009.log.
- Specific details about SQL queries are logged in the *<servicename>_QueryStatsDetails_<date>.log* files. Examples are inserver_QueryStatsDetails_20081001_110210.log or inserverWorkflow_QueryStatsDetails_20081001_090302.log.

Configure performance log files

To change settings for performance logging behavior, complete the following steps.

1. On the server computer, navigate to the *[drive:]**inserver*** directory.
2. Open the *inow.ini* file in a text editor.
3. Change the settings as needed in the **[Statistics]** section.
4. Save the file and close it.

   Changes should take effect within 30 seconds.

View performance log files

To view performance log files, complete the following steps.

1. In a window that accepts command prompts, navigate to *[drive:]**inserver\log\performance_stats_logs**.

2. In either a text editor or a spreadsheet application, open the log file you want to view.
3. Optional. If you are using a spreadsheet, you can change the delimiter character used to separate the columns in the log file by changing the value of the **stats.ss.delimiter** setting. The default delimiter character is a tab character.

Performance logging settings

Performance logging settings are located on the ImageNow Server, in *inow.ini* under the [Statistics] section. Use these settings to configure performance logging. If the stats.all.log.type is set to 0, performance logging is disabled. Initially, all settings run hourly. If you want different time periods, you must configure the settings. You can choose to use either the stats settings or the individual category settings, but you cannot use these settings simultaneously. If you turn on individual category settings, those settings override the general stats settings. As an example, you can use the query and server call individual category settings when you want to generate extensive details about SQL queries and execution plans.

Category descriptions

Settings apply to the following categories:

Category	Description
Cache	Timing for the duration of cache lookups or misses.
DataStream	Large I/O timing for waits, transfers, and synchronizing information.
DataStreamElement	Small, elemental timing for specific I/O system calls.
Image	Timing for the duration of image processing. Applies to agents processing thumbnails, image rotations, and image previews.
iScript	Timing for the duration of an iScript.
Job	Timing for the duration of a job server processing a message.
MQ	Timing for the duration of a message queue action.
Query	Timing for the duration of a single SQL query.
ServerCall	Timing for the duration of a single server call.
Storage	Timing for the duration of OSM storage operations.

Category	Description
SubsystemCall	Timing for the duration of a call into a subsystem or third party library. Currently, only LDAP is supported.
Thread	Timing for the duration of thread operations.
WebServices	Timing for the duration of a call into a web services call library.
WFAction	Timing for the duration of a workflow action.

Category settings

To apply a setting to a specific category, replace [Category] in the following sections.

Setting	Value	Default Value	Description	Example
stats.ss.delimiter	Delimiter character	Tab	This is a delimiter character used to separate columns in log files. Useful when imported to a spreadsheet. This setting is commented out by default.	`stats.ss.delimiter=`
stats.all.log.type	0 = Off 1 = User-defined 2 = Hourly 3 = 6 hours 4 = 12 hours	2	The value of this setting determines whether action statistics are logged and how often. Regardless of the value for this setting, the individual category settings override this setting. The stats.all settings are only used when an	`stats.all.log.type=0`

Setting	Value	Default Value	Description	Example
			individual category is turned on. For example, stats.<cat>.log.type is set to 0, where <cat> is a placeholder for a category setting.Individual category settings appear below.	
stats.all.timer.period	An integer representing seconds	1800	This setting is only used when stats.all.log.type is set to 1. The value in this setting defines the length of the logging period. Valid values range from 5 to 3595 seconds.	`stats.all.timer.period=900`
stats.all.start.time	An integer representing the start time hour	0	This setting is only used when stats.all.log.type is set to 3 or stats.all.log.type is set to 4. The value in this setting synchronizes the start time for the logging period. Valid values range from 0 to 23 hours.	`stats.all.start.time=6`
stats.all.action.length	An integer to represent character	0	The length of the string logged to the ACTION column can range from 0 to 1000 characters.	`stats.all.action.length=50`

Setting	Value	Default Value	Description	Example
	length		Any characters beyond this length are truncated in the log file. A value of 0 logs all characters. This setting is only used if the log.type setting is not zero.	
stats.[Category].log.type	0 = Off 1 = User-defined 2 = Hourly 3 = 6 hours 4 = 12 hours	0	The value of this setting determines whether the specified category's action statistics are logged and how often.If this setting is not equal to zero, the individual category settings are used and they override the general settings. To adjust the general settings, use the stats.all settings.	`stats.servercall.log.type=3`
stats.[Category].timer.period	An integer representing seconds	1800	The value in this setting defines the length of the logging period. Valid values range from 5 to 3595 seconds. This setting is only used when stats.[Category].log.type is set to 1.	`stats.servercall.timer.period=900`
stats.[Category].start.time	An integer represen	0	The value in this setting synchronizes the start time for the	`stats.servercall.start.time=6`

Setting	Value	Default Value	Description	Example
	ting the start time hour		logging period. Valid values range from 0 to 23 hours. This setting is only used when stats.[Category].log.type is set to 3 or stats.[Category].log.type is set to 4.	
stats.[Category].action.length	An integer to represent character length	0	The length of the string logged to the ACTION column can range from 0 to 1000 characters. Any characters beyond this length are truncated in the log file. A value of 0 logs all characters. This setting is only used if the log.type setting is not zero.	`stats.servercall.action.length=50`
stats.query.plan.threshold	An integer representing seconds	1.0	The duration of the threshold in seconds to exceed before displaying the execution plan of the query in the query plan log. Valid values can range from 0 to 3599.999. This setting is only used when stats.query.log.type is set to 1.	`stats.query.plan.threshold=2.0`
stats.query.plan.freq	An integer	1	A value of 0 turns this setting off. A	`stats.query.plan.freq=10`

Setting	Value	Default Value	Description	Example
	representing the query plan frequency		number from 1 to 100 determines the logging plan frequency for the stats.query.plan.threshold setting. This setting is only used when stats.query.log.type is set to 1. For example, if the threshold setting value is 30 seconds and this setting is 2, the query plan is logged every 60 seconds.	

Performance log file components

The following chart defines performance log file components and provides examples.

Component/Column Heading	Description	Example
No column heading	Local time is displayed in the first column.	08:08:34.632859(d40)
GMT	The time the statistic was logged in Greenwich Mean Time.	3:00:34 PM
ACTION	The type of action logged.	SELECT * FROM IN_SEQUENCE WITH (ROWLOCK,UPDLOCK) WHERE SEQ_NAME = ? OPTION (FAST 1)
INSTANCE NAME	The instance	Primary

Component/Column Heading	Description	Example
	name of the agent.	
AGENT NAME	The name of the agent that executed the command.	inserver
CATEGORY	The type of action performed by the agent.	query
ROW TYPE	The type of data in this row, such as summary or details.	details
NUM	The number of times the action was performed.	30
TOTAL	The length of time the action took to complete.	0.330924
AVG	The average amount of time actions of that type took to complete.	0.066185
STD DEV	The standard deviation of the minimum and maximum times logged during the timer period.	0.065636
MIN	The time it took to complete the fastest performing action.	0.000496

Component/Column Heading	Description	Example
MAX	The time it took to complete the slowest performing action.	0.159593
MIN USER	The user name of the user who performed the fastest action.	inuser
MAX USER	The user name of the user who performed the slowest action.	test2
MIN TIME	The exact point in time when the fastest action occurred.	1:08:35 PM
MAX TIME	The exact point in time when the slowest action occurred.	1:08:40 PM
ERR	The number of times that type of action in the ACTION column failed, assuming any exceptions were handled correctly.	0
EXC	The number of times that type of action in the ACTION column was interrupted by a thrown exception. This measurement does not affect	5

Component/Column Heading	Description	Example
	overall performance statistics for this action type.	
MIN ARG	The arguments used for the fastest executing query.	`0=<0>Unthreaded`
MAX ARG	The arguments used for the slowest executing query.	`0=<0>0002773NKV7P;1=<0>Unthreaded`

Time Travel Logging

About time travel logging configuration

When configuring time travel logging, consider the following behaviors and guidelines.

- By default, this logging type is on and does not require any configuration.
- Time travel logging parameters are hidden and do not appear in configuration files.
- If needed, you can add time travel logging parameters to the *inow.ini* or to the configuration file for each process on the Perceptive Content system. Time travel logging you set in the *inow.ini* file is set globally.
- Time travel logging you set in a process configuration file overrides default time travel logging.
- You do not have to restart the agent for time travel logging to take effect.
- Additional configuration options allow you to opt out of exception logging based on a category or IDs. Similarly, because logging due to errors is not enabled by default, you can opt in for error logging based on a category or IDs.
- At this time, ID information is unavailable.
- Server call and SQL statement thresholds are also configurable.

About reporting incident conditions

When the Perceptive Contentsystem detects one or more of the following conditions, an incident report is automatically generated:

- `Errors` There is an expected reason for the subsystem failure.
- `Exceptions` There is an unexpected reason for the subsystem failure or an operating system (OS) exception.
- `Slow performing server calls` A server call completes outside the amount of time allowed for the call.
- `Slow performing SQL statements` A SQL statement completes outside of the amount of time allowed for the statement or when a SQL statement times out.

View time travel incident reports

To locate and view time travel incident reports, complete the following steps.

1. Navigate to the *[drive:]****inserver****log*****error_logs***[date]* folder.
2. Open the **inserverBatch_54MW2Y_4b8_07.10.59.875000.log** file with a text editor.

Categories table

The following table describes categories and their types.

Category	Description	Type
54HR0K	The object was not found.	System error as it relates to the object state
54HR69	The object is a duplicate and already exists.	System error as it relates to the object state
54HT7R	The object is in use and cannot be deleted.	System error as it relates to the object state
54HT7U	The object is not in the correct state for this action.	System error as it relates to the object state
54HT7X	The user does not have privileges for this object.	System error as it relates to the object state
54HRRB	A lock related failure occurred.	Generic error
54HRUA	An operation, such as an insert or a hash failed.	System error as it relates to the object state

54HT81	An invalid parameter was provided.	Generic error
54HT85	The requested operation is not supported. For example, an operation may be supported for Windows only.	Generic error
54HT89	Only use this in rare situations.	Core error
54HT8B	A database error occurred.	Core error
54HT8D	A socket communication error occurred.	Core error
54HT8F	A file system error occurred.	Core error
54HT8J	Errors in core system wrappers occurred.	Core error
5HNNG4	A fatal error occurred.	Core error
54HT8M	An error occurred in the OSM system.	Subsystem error
54HT96	A modem error occurred.	Subsystem error
54HT98	The file type database.	Subsystem error
54HT9A	An image processing error occurred.	Subsystem error
54HT9C	A login, authentication or license error occurred.	Subsystem error
54HT9E	An LDAP authentication or replication error occurred.	Subsystem error
54HT9G	An script or xml error occurred	Subsystem error

Condition use cases

Below are examples of use cases for an error, a slow performing server call, and a slow performing SQL statement conditions.

Time travel logging on error

When a client attempts to add a document, the system encounters an Unable to store a document with an empty document id error. This condition invokes the past and captures the events as they occurred before the condition was met. The log shows that the call to getUniqueID returned a valid string, but that the string was then emptied out by another call.

Time travel logging on a slow performing server call

The system completes a call to copy a document. The call is outside the allowed run time of five seconds. The system invokes the past and produces the event log for the entire call. The event log shows that each call to remove a page from the document takes 0.3 seconds. Ultimately, the log file shows that the foreign keys were not properly indexed for the document delete SQL statement.

Time travel logging on a slow performing SQL statement

The system is storing a new document and the insert into the in_instance_prop table takes .4 seconds, which is beyond the time allowed for an SQL statement. Because the slow performing SQL statement condition is met, an event log is generated for the entire server call. To troubleshoot this issue, we store a document of the same type and find that an Oracle instance requires more memory.

Parameters table

The following table defines the parameters for time travel logging for each process on the Perceptive Content system.

Parameter Name	Data Type	Description
ttlogger.enabled	Boolean 1-True, 0-False	Determines if Time Travel Logging (TTL) is on or off.
ttlogger.exception.enabled	Boolean 1-True, 0-False	Determines if TTL will dump to an event log when an exception occurs.
ttlogger.error.enabled	Boolean 1-True, 0-False	Determines if TTL will dump to an event log when an error occurs.
ttlogger.server.call.enabled	Boolean 1-True, 0-False	Determines if TTL will dump when a server call exceeds its threshold.

Parameter Name	Data Type	Description
ttlogger.sql.enabled	Boolean 1-True, 0-False	Determines if TTL will dump when an SQL query exceeds its threshold.
ttlogger.memory.limit	Integer The maximum memory amount is 512 kb.	Determines how much memory TTL can use.
ttlogger.event.limit	Integer The maximum number of events is 1000.	Determines how many events TTL can hold.
ttlogger.error.included	, delimited CINString	Determines what errors will trigger TTL to dump to a file. **Note:** The ttlogger.error.enabled parameter must be set to 0.
ttlogger.exception.excluded	, delimited CINString	Determines what exceptions will trigger TTL to dump to a file. **Note:** The ttlogger.exception.enabled parameter must be set to 1.
ttlogger.server.time.thresh	Floating point By default, this parameter is set to 10 seconds.	If a server call takes longer than this time the TTL will dump to file.
ttlogger.sql.time.thresh	Floating point By default, this parameter is set to 5 seconds.	If an SQL query takes longer than this time, TTL will dump to a file.
ttlogger.future.logging.limit	Integer	This determines the number of events that will be logged after an event that caused the TTL to dump.

Error opt in example

By default, error logging is not enabled. You can opt in to error logging based on categories. To opt in to error logging, add the following parameter to any available configuration file:

```
ttlogger.error.included=54HT7X.
```

Application and OS exception opt out example

To opt out of an application or an OS error, add the following parameter to the configuration file of your choice:

```
ttlogger.exception.excluded=54HT93
```

Controller Log Files

View the Controller Log file

When you enable logging on ImageNow Client, the Controller Log tracks user events. To view the Controller Log file, complete the following steps.

1. Hold down the SHIFT key and right-click in the title bar of the **Perceptive Content** toolbar.
2. Click **View log file**.

Create the Controller Log file

To create the Controller Log file, complete the following steps.

1. Press and hold the SHIFT key and right-click in the **Perceptive Content** title bar.
2. Point to **Logging** and click **Low**, **Medium**, or **High**.

Delete a controller log file

To delete a controller log file, complete the following steps.

1. On the toolbar, hold down the SHIFT key and right-click inside the title area.
2. Click **Delete log file**.

Auditing

What is auditing?

Auditing allows you to troubleshoot issues or track the actions taken in Perceptive Content by specific users or groups.

Perceptive Content stores audit items in log files, the Perceptive Content database, or both. Audit reports are available in the Business Insight Report Library. You can use other third-party tools to view the audit items as well, although Perceptive Software does not provide customer support for those tools.

Create a new audit template overview

The following steps explain how to create a new audit template in Management Console, add audit conditions, and assign the audit template to users and groups.

1. Add an audit template.
2. Add predefined conditions to an audit template.
3. Add client audit conditions to a template.
4. Add server audit conditions to the template.
5. Assign an audit template to users or groups.
6. Enable an audit template.

Add an audit template

To add a new audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, click **New**.
4. In the **New Audit Template** window, in the left pane, click **Properties**.
5. In the right pane, under **General**, type a name and optional description.
6. To activate the audit template after creation, verify that the **Is Active** check box is selected.
7. Click **OK**.

Next For the audit template to be complete, add auditing conditions and assign the template to users and groups.

Add predefined conditions to an audit template

To add predefined conditions to a new audit template, complete the following steps.

1. In the **Audit Template Definition** wizard, in the **Audit Template Conditions** page, click **Add > Predefined**.
2. In the **Predefined Conditions** dialog box, in the **Conditions** list, select the check box for each predefined condition you want to add and then click **OK**.
3. Repeat steps for each predefined audit condition you want to add to the template.

Add client audit conditions to a template

To add client audit conditions to an audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, complete one of the following substeps.

    1. To create a new audit template, click **New**.
    2. To copy an existing audit template, select an audit template and click **Copy**.
    3. To modify an existing audit template, select an audit template and click **Modify**.
4. In the **Audit Template** window, in the left pane, click **Conditions**.
5. Under **Template Conditions**, click **Add > Client**.
6. In the **New Condition** dialog box, in the **Name** box, type a name for this audit condition.
7. In the **Action** list, select the auditing action and click **OK**.

Add server audit conditions to the template

To add server audit conditions to an audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, complete one of the following substeps.
    1. To create a new audit template, click **New**. In the **Audit Template** dialog box, click **Properties**, then type a name for the template and select the **Is Active** check box.
    2. To copy an existing audit template, select an audit template and click **Copy**.
    3. To modify an existing audit template, select an audit template and click **Modify**.
4. In the **Audit Template** window, in the left pane, click **Conditions**.
5. In the right pane, under **Template Conditions**, click **Add > Server**.
6. In the **New Condition** dialog box, in the **Name** box, type a name for this audit condition and complete the following substeps.
    1. In the **Category** list, select the auditing category you want to use for this condition.
    2. In the **Action** list, select the auditing actions you want to use for this condition.
    3. In the **Object** list, select the auditing objects you want to use for this condition.
7. Click **OK**.

Assign an audit template to users or groups

To assign an audit template to users or groups, complete the following steps.

If you want to audit server actions performed by the File System Agent, such as deleting, restoring, or moving a container, you must check the Assign to all agents checkbox when assigning users and groups to the audit template.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list and then complete one of the following procedures.

Situation	Steps
Assign an audit template to a user or group	1. In the left pane, click **Users** or **Groups**. 2. Select a user or group and click **Modify**. 3. In the dialog box, click **Auditing**. 4. In the right pane, under **Audit Templates**, select a template and click **Add** to assign the template for this user or group. 5. Click **Apply**.
Add users or groups when creating or modifying an audit template	1. In the left pane, click **Auditing**. 2. In the right pane, click **New** to create a new audit template, click **Copy** to copy a template, or click **Modify** to modify a template. 3. In the **Audit Template** dialog box, in the left pane, click **User Assignment**. 4. In the right pane, under **Users and Groups**, click **Add**. 5. In the **Select Users and Groups** dialog box, select the users and groups you want to add. 6. Click **OK**.

2. Click **OK**.

Next If the audit template is not active, enable the audit template.

Enable an audit template

To activate an audit template that is already configured, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, select an auditing template and click **Modify**.
4. In the **Audit Template** dialog box, in the left pane, click **Properties**.
5. In the right pane, under **Options**, select the **Is active** check box and click **OK**.

Create an audit authentication template

To create a new audit template that includes a condition to audit failed login attempts or other actions performed by users who are not logged in, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department**

Settings from the list.

2. In the left pane, click **Auditing**.
3. On the **Templates** tab, in the right pane, click **New** to run the **Audit Template Definition** wizard.
4. To provide general information about the auditing template, in the **Audit Template Information** page, type a name and optional description for the audit template and select the **Is active** check box.
5. Click **Next**.
6. To set the audit conditions, in the **Audit Template Conditions** page, complete the following substeps.
    1. Click **Add** and then select **Predefined**.
    2. In the **Predefined Conditions** dialog box, in the **Conditions** list, select **User Login**.
    3. Click **OK**.
    4. In the **Audit Template Conditions** page, click **Next**.
7. To assign the auditing template to a user or group, in the **Audit Template Assignment** page, click **Add**.
8. Click **Finish**.

Copy an audit template

Audit templates describe the user and group actions that you want to log. To create a copy of an audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, select the auditing template you want to copy and then click **Copy**.
4. In the **Copy Audit Template** dialog box, rename the template, then add or remove conditions and modify user assignment as necessary.
5. Click **OK**.

Modify or rename an audit template

You can use audit logs to troubleshoot issues or track the actions taken in Perceptive Content. Audit templates describe the actions that you want to log. To modify or rename an audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the right pane, on the **Templates** tab, select an auditing template and click **Modify**.
3. In the **Audit Template** dialog box, in the left pane, click **Properties**.
4. In the right pane, complete any of the following actions.
    - To rename the template, under **General**, in the **Name** box, type a name for the template.
    - To add or change the description of the template, under **General**, in the **Description** box, type a description for the template.

- To make the template active or inactive, under **Options**, select or clear the **Is active** check box. Make the template inactive if you do not want users to have access to it in the future.

5. In the left pane, click **Conditions**, then in the right pane, add, modify or delete conditions.
6. In the left pane, click **User Assignment**, then in the right pane, add or remove users or groups.
7. Click **OK**.

Delete an audit template

To delete an audit template, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select **Cross Department Settings** from the list.
2. In the left pane, click **Auditing**.
3. In the right pane, on the **Templates** tab, select an auditing template and click **Delete**.
4. In the **Template Delete** dialog box, click **Yes**.

Set the audit log format

You can configure audit logging to create an XML audit log file, populate audit log information in the Perceptive Content database, or both. To configure the audit log format, complete the following steps.

Client auditing with XML files is not fully supported. If you set auditing to use XML, and a client audit entry is logged, the XML file shows only the initial record indicating the audit began; it does not update the record to show the final status of the action.

1. Navigate to the *[drive:]**inserver****etc*** directory and open the *inow.ini* file.
2. Under **[Audit]**, set **audit.format** to one of the following:
   - `1` for XML format.
   - `2` for database format.
   - `3` for both XML and database formats.

   If you want to run audit reports using Business Insight, you must set this value to 2 or 3.
3. To set the verboseness level for user authentication auditing, change the **login.audit.level** setting to one of the following values:
   - `0`. No authentication auditing occurs.
   - `1`. Auditing only occurs on failed authentication attempts.
4. Optional. To audit successful and failed authentication attempts, in **Management Console**, create a new audit template using the predefined condition, **User Login**.
5. Save and close the file.
6. Restart **ImageNow Server**.

   Note: In the log files, the <action.objects>, <source.objects>, and <dest.objects> are repeatable elements. Object types are reported as an attribute of each <audit.object> element.

7. Navigate to the *[drive:]**inserver****audit*** directory.
8. In a text editor, open the XML log file. For example, LoginTrace_20090818.xml.

Audit conditions

The following audit conditions are available for use. You can define client-side, server-side, and predefined conditions.

Available predefined conditions

Predefined Condition	Category	Action	Object
Access Control Marking	Record	All	Access control marking
Add a Digital Signature to a Document	Document	Add	Page version number
Add a Digital Signature to a Record	Record	Add	
Add Annotations to a Document	Document	Add	Document page subobject
Cutoff	Record	Cutoff	All
Document Copy	Document	Copy	Document
Document Create	Document	Create	Document
Document Create via Batch	Batch	Move	Document
Document Delete	Document	Delete	Document
Document Move	Document	Move	Document
Document Page Add	Document	Add	Document page
Document Page Delete	Document	Delete	Document page
Document Restore	Document	Restore	Document
Document Send to Recycle Bin	Document	Send to recycle bin	Document
Document View	Document	Get	Document

Predefined Condition	Category	Action	Object
File Plan	Record	All	File plan
Pick List	Record	All	Pick list
Record Copy	Record	Copy	Record
Record Create	Record	Create	Record
Record Delete	Record	Delete	Record
Record Folder Set Closed State	Record	Set Closed State	Record
Record Move	Record	Move	Record
Record Sent to Recycle Bin	Record	Send to Recycle Bin	Record
Record View	Record	View	Record
Remove Cutoff	Record	Remove cutoff	All
Retention Agent Actions	Retention		
Retention Approval Actions	Retention	Update	Retention approval
Retention Holds	Retention		Retention hold
Retention Policies	Retention		
Search	View	Execute	View
User Login	Server	Verify	User

Available categories, actions, and objects for server-side conditions

The following tables outline the available categories, actions, and objects that can be audited in ImageNow Client and ImageNow Server.

Category

Category Name	Description
All	Choose this option to audit all categories.
Admin	Choose this option to audit actions that an administrator performs. This includes actions performed by a Perceptive Manager, a Department Manager, or a user with management privileges.
Alarm	Choose this option to audit actions that occur to alarms.
Audit	Choose this option to audit auditing.
Batch	Choose this option to audit actions that occur to batches.
Business list	Choose this option to audit actions that occur to business lists.
Capture	Choose this option to audit scanning and capturing activities. This also includes DataCapture forms.
Common	Choose this option to audit any type of common activity, such as logging into ImageNow Client.
Custom property	Choose this option to audit actions performed on custom properties.
Document	Choose this option to audit various types of document actions, such as adding, copying, deleting, or replacing.
Drawer	Choose this option to audit actions performed on drawers and their contents.
Envoy	Choose this option when you want to audit actions that are performed by Envoy.
ERM	Choose this option to audit actions performed using ERM Server.
File	Choose this option to audit actions performed on files.
Folder	Choose this option to audit actions performed on folders and their contents.
Form	Choose this option to audit actions performed on forms.
Form type	Choose this option to audit actions performed on form types.

Category Name	Description
Integration	Choose this option to audit actions performed with business applications, such as SAP.
Job	Choose this option to audit actions performed on jobs.
LearnMode	Choose this option to audit actions performed with LearnMode.
License	Choose this option to audit actions performed involving Perceptive Content and other components licensing.
Record	Choose this option to audit actions performed using File Plan Designer.
Retention	Choose this option to audit actions performed using Retention Policy Manager.
(system)	Choose this option to audit the actions performed by agents in the background, including searching for expired holds and adding documents to a policy.
Security	Choose this option to audit actions that occur regarding security and privileges.
Server	Choose this option to audit ImageNow Server actions.
Shortcut	Choose this option to audit document and folder shortcut actions.
Subobject	Choose this option to audit subobject actions, including annotations.
Task	Choose this option to audit actions that occur to tasks.
Timing	Choose this option to audit timing actions.
View	Choose this option to audit the use of views and filters.
Workflow	Choose this option to audit actions performed using workflow.

Action

Action Name	Description
All	Choose this option to audit all actions for the selected category.

Action Name	Description
Add	Choose this option to audit adding actions for the selected category.
Copy	Choose this option to audit copying actions for the selected category.
Create	Choose this option to audit creation actions for the selected category.
Cutoff	Choose this option to audit cutoff events for the selected category.
Delete	Choose this option to audit deletion actions for the selected category.
Edit properties	Choose this option to audit modifications to a property of an object for the category. This includes changes to drawer and type values, custom property values, and changes to the values in Field1 through Field5.
Execute	Choose this option to audit execute actions for the selected category.
Get	Choose this option to audit retrieval actions for the selected category.
Lock	Choose this option to audit file lock actions for the selected category.
Move	Choose this option to audit moving actions for the selected category. This includes moving objects to a new drawer.
Remove	Choose this option to audit removal actions for the selected category.
Remove cutoff	Choose this option to audit remove cutoff events for the selected category.
Rename	Choose this option audit renaming objects in the selected category.
Replace	Choose this option to audit replacement actions for the selected category.
Restore	Choose this option to audit restore actions from the recycle bin for the selected category.
Search	Choose this option to audit searching actions for the selected category.
Send to recycle bin	Choose this option to audit actions that send documents or folders to the recycle bin for the selected category.
Set closed state	Choose this option to audit record folder closing or opening for the selected category.

Action Name	Description
Share with department	Choose this option to audit sharing of objects with a department.
Transfer	Choose this option to audit transfer actions for the selected category.
Unlock	Choose this option to audit file unlock actions for the selected category.
Update	Choose this option to audit updating actions for the selected category.
Verify	Choose this option to audit verification actions for the selected category.

Object

Object Name	Description
Access control marking	Choose this option to audit access control marking assignments and changes to access control markings.
All	Choose this option to audit all objects for the selected category and action.
Alarm	Choose this option to audit any alarm actions, including create and execute actions for the selected category and action.
Batch	Choose this option to audit all batch objects for the selected category and action.
Batch archive	Choose this option to audit when batch objects are archived for the selected category and action.
Batch attachment	Choose this option to audit when attachments are added to or removed from batch objects for the selected category and action.
Batch page	Choose this option to audit actions that are performed on batch pages of existing batches for the selected category and action.
Batch page recognition zone	Choose this option to audit when OCR recognition zones on batch pages are created, edited, or removed for the selected category and action.
Batch subobject	Choose this option to audit all activities to batch subobjects for the selected category and action.
Business list	Choose this option to audit all activities to business lists for the selected category and action.

Object Name	Description
Business list item	Choose this option to audit all activities to items in business lists for the selected category and action.
Capture batch	Choose this option to audit all activities to Capture batches for the selected category and action.
Capture profile	Choose this option to audit all activities to Capture profiles for the selected category and action.
Capture source	Choose this option to audit all activities to scanning sources for Capture profiles for the selected category and action.
Client search script	Choose this option to audit all activities to client search scripts for the selected category and action.
Connection type	Choose this option to audit all activities on a connection type.
Custom property	Choose this option to audit all activities to custom properties for the selected category and action.
Department	Choose this option to audit all management activities on a department.
Directory	Choose this option to audit all activities to server and client directories for the selected category and action.
Document	Choose this option to audit general activities on documents for the selected category and action.
Document CD form	Choose this option to audit general activities on document CD forms for the selected category and action.
Document digital signature	Choose this option to audit the digital signing of documents for the selected category and action.
Document digital signature reason	Choose this option to audit the creation, modification, or deletion of reasons for digital signatures for the selected category and action.
Document digital signature subobject	Choose this option to audit activities that occur to the subobjects of digital signature on documents for the selected category and action.
Document drawer	Choose this option to monitor changes to the drawer for the selected category and action.

Object Name	Description
Document keywords	Choose this option to monitor changes to the keywords (notes) of a document for the selected category and action.
Document lock	Choose this option to audit every time a document is locked for the selected category and action.
Document page	Choose this option to audit activities that occur to the pages of a document for the selected category and action.
Document page subobject	Choose this option to audit activities that occur to the subobjects of the pages of a document for the selected category and action.
Document property	Choose this option to audit activities that occur to the properties of a document for the selected category and action.
Document subobject	Choose this option to audit activities that occur to document subobjects for the selected category and action.
Document thumbnail	Choose this option to audit activities that occur to document thumbnails for the selected category and action.
Document type	Choose this option to audit activities that occur to document types for the selected category and action.
Document type exam	Choose this option to audit activities that occur to document type exams for the selected category and action.
Document type list	Choose this option to audit activities that occur to document type lists for the selected category and action.
Document version number	Choose this option to audit the version numbers used by version control for a document for the selected category and action. This feature requires a Document Management license.
Drawer	Choose this option to audit actions performed for a drawer or its contents.
Envoy	Choose this option to audit actions that Envoy performs.
Envoy remote service	Choose this option to audit changes to remote services for Envoy.
ERM item	Choose this option to audit changes to items in ERM Server.
ERM report	Choose this option to audit changes to reports in ERM Server.

Object Name	Description
ERM Server document	Choose this option to audit changes to documents in ERM Server.
ERM spool	Choose this option to audit changes to print spools in ERM Server.
External message	Choose this option to monitor messages exchanged between components. HL7 message are included in this object.
Fax	Choose this option to audit when fax activities occur.
File	Choose this option to audit activities that occur to files.
File plan	Choose this option to audit activities performed on file plans.
Folder	Choose this option to audit activities performed on folders.
Folder subobject	Choose this option to audit activities performed on folder subobjects. This object does not apply to the contents of a folder.
Folder type	Choose this option to audit activities performed on folder types.
Folder type list	Choose this option to audit activities performed on folder type lists.
Form	Choose this option to audit changes to Forms.
Form data definition file	Choose this option to audit activities on XML data definition files for Forms.
Form file	Choose this option to audit activities on XML form files in general.
Form presentation file	Choose this option to audit activities on Forms presentation files. Included are XML files, XSL schema files, CSS files, graphics files, and script files.
Form shared file	Choose this option to audit activities to shared files used by Forms. Included are XML files, XSL schema files, CSS files, graphics files, and script files.
Group	Choose this option to audit changes to user groups.
Hosted document	Choose this option to audit changes to business application hosted documents.
Hosted page	Choose this option to audit changes to business application pages of hosted documents.
INI setting	Choose this option to audit changes to properties in INI files on the

Object Name	Description
	ImageNow Server.
iScript sequence object	Choose this option to audit when the sequence object is used by iScript files.
Job	Choose this option to audit activities performed by the embedded agent, Job Agent.
Key pair	Choose this option to audit activities that occur on Digital IDs used to digitally sign documents.
Key pair reason	Choose this option to audit activities that occur on the reasons for Digital IDs which are used to digitally sign documents.
LearnMode application plan	Choose this option to audit activities performed on application plans used by LearnMode.
LearnMode application plan screen	Choose this option to audit activities performed screens for application plans used by LearnMode.
LearnMode Visual Basic script	Choose this option to audit activities that are performed by Visual Basic scripts which are used by LearnMode.
License	Choose this option to audit activities that affect licenses.
License group	Choose this option to audit activities that affect ImageNow license groups.
License token	Choose this option to audit activities that occur to license tokens, such as moving or deleting a license token.
Migration package	Choose this option to audit the activities performed by migration packages.
Migration profile	Choose this option to audit activities performed by migration profiles.
Miscellaneous	Choose this option to audit general activities performed. One example is changes made to database tables.
OSM	Choose this option to audit changes made to the Object Storage Manager.
OSM set	Choose this option to audit changes to Object Storage Manager sets.
OSM set filter	Choose this option to audit changes to Object Storage Manager filters for sets.

Object Name	Description
OSM tree	Choose this option to audit changes to Object Storage Manager trees used by Object Storage Manager.
Out of office event	Choose this option to audit activities triggered by out of office events.
Output profile	Choose this option to audit activities performed using Output profiles.
Page version number	Choose this option to audit when the version number of a page in a document changes.
Physical object	Choose this option to audit activities to physical objects.
Pick list	Choose this option to audit pick list assignments and changes made to pick lists.
Predefined list	Choose this option to audit changes to predefined lists.
Predefined list item	Choose this option to audit changes to the selections available in predefined lists.
Privilege	Choose this option to audit privilege assignments for users and groups.
Record	Choose this option to audit changes to records.
Record type	Choose this option to audit all activities on a record type.
Record category	Choose this option to audit actions performed for a record category or its contents.
Record category type	Choose this option to audit all activities on a record category type.
Record folder	Choose this option to audit actions performed on record folders.
Record folder type	Choose this option to audit actions performed on a record folder type.
Retention action	Choose this option to audit when retention actions occur.
Retention approval	Choose this option to audit when retention approvals occur.
Retention approval set	Choose this option to audit when retention approval sets occur.
Retention approval user	Choose this option to audit activities of retention approval users.

Object Name	Description
Retention authority	Choose this option to audit activities of retention authorities.
Retention hold	Choose this option to audit when holds are placed on retention items.
Retention path	Choose this option to audit when changes occur to retention paths.
Retention phase	Choose this option to audit the phases of retention.
Retention policy	Choose this option to audit changes to retention policies.
Retention policy comment	Choose this option to audit changes to retention policy comments.
Retention set destruction	Choose this option to audit changes to retention policy destruction sets.
Retention set export	Choose this option to audit exports of retention sets.
Rule	Choose this option to audit changes to document and workflow rules.
Shortcut	Choose this option to audit changes to a document or folder shortcut.
Subobject template	Choose this option to audit changes to subobject templates.
Task	Choose this option to audit the activities of tasks.
Task template	Choose this option to audit changes to task templates.
Task script	Choose this option to monitor the scripts used in task templates.
Timing settings	Choose this option to audit timing settings.
Timing statistics	Choose this option to audit timing statistics.
User	Choose this option to audit changes to users.
View	Choose this option to audit changes to views and filters.
Viewer script	Choose this option to audit the buttons and scripts used in the User toolbar.
Workflow item	Choose this option to audit the activities performed by workflow items.
Workflow process	Choose this option to audit the changes made to workflow processes using Workflow Designer.

Object Name	Description
Workflow queue	Choose this option to audit the changes made to workflow queues using Workflow Designer.
Workflow route	Choose this option to audit the changes made to workflow routes using Workflow Designer.
Workflow script	Choose this option to audit the scripts used in Workflow Designer.

Available actions for client-side conditions

Client-side Actions	Description
All	Use this option when you want to audit all of the available actions.
Copy to clipboard	Use this option when you want to audit each time a user copies from a document page using a client.
Email	Use this option when you want to audit each time a user sends an e-mail from a client.
Export	Use this option when you want to audit each time a user exports a document using a client. This includes exporting to a PDF.
Fax	Use this option when you want to audit each time a user faxes a document using a client.
Launch associated application	Use this option when you want to audit each time a user launches an associated application (native application) using a client. For example, Microsoft Word.
Print	Use this option when you want to audit each time a user prints a document or a form from a client.

Sessions

About monitoring user and agent connection

Perceptive Content allows you to monitor an unlimited number of users and agents.

If a user is connected either directly or remotely to your network, Management Console tracks the user s name, license type, time spent online for the session, network address, server instance, and server host. It also displays whether the user is currently online.

You can also track agent sessions. Unlike the user sessions, which only traces remote or active users, agents connected to Perceptive Content appear in Management Console. You can track the same information for agents as you can for users, including the state of the session s connection.

View agent sessions

To display information about the agents that have active sessions with ImageNow Server, complete the following steps.

1. In **Management Console**, in the left pane, click **Diagnostics**.
2. In the right pane, click **Sessions**.

   The list of connected agents appears in the right pane.
3. To sort the **Agent sessions** list in ascending or descending order, click the **Name**, **License Type**, **Time**, or **Address** column headers.
4. To search for a specific agent, in the **Search for agents** box, type all or some of an agent name and click **Search**.

   The Agent sessions list displays the sessions fitting your search criteria.

View user sessions

To display information about the users who have active sessions with ImageNow Server, complete the following steps.

1. In, **Management Console** in the left pane, click **Diagnostics**.
2. In the right pane, click **Sessions**.

   The user sessions information appears in the right pane.
3. To sort the **User sessions** list in ascending or descending order, click the **Name**, **License Type**, **Time**, or **Address** column headers.
4. To search for a specific user, in the **Search for users** box, type all or some of a user name, first or last name, and click **Search**.

   The User sessions list displays the sessions fitting your search criteria.

ImageNow Client API

Manage agents

Fax Agent

Fax an item

If you have a configured fax output profile, you can fax items using the settings defined in the output profile. You can change these settings when faxing or enter them manually. To fax an item, complete the following steps.

1. Open the item.
2. Click **File > Fax**.
3. In the **Fax** dialog box, in **Profile**, select the appropriate output profile for the individual or group you want to fax the item.
4. Optional. Define fax settings for an output profile to change the settings inherited from the output profile.
5. Optional. Define output content settings to change the settings inherited from the output profile.
6. In the **Fax number** box, enter or change the fax number.
7. Under **Notifications**, in the **Email** box, type the email address of the individual or company to where you want to send a notification of a sent fax.

   The email address is remembered and displayed here the next time you send a fax.
8. Click **OK**.

Add a fax number for fax recipients

To add a new fax number to Fax Recipients, complete the following steps.

1. In **Management Console**, in the left pane, click **Output Profiles**.
2. In the right pane, on the **Fax Recipients** tab, click **New**.
3. In the **Fax Recipients** dialog box, enter the contact name and fax number you want and then click **OK**.

> **Note:** In the fax number, formatting is optional. All values except for numbers are ignored.

Retention Agent

What is retention?

Retention functionality allows you to determine whether an item is under a protected phase in a policy, assign physical file references, approve disposition actions, and apply holds.

To track the physical location of an item, you can create a physical file reference.

For example, you can designate a warehouse, shelf number, or box number as a physical location. If a policy creator designates you as an approver, you must approve the path disposition action, such as destruction, offline transfer, or accession, before that action can occur for the items that fall under that path. A hold allows you to preserve a item. When you apply a hold, no changes to that item can occur until you remove that hold or the hold expires.

What is Retention Agent?

The Perceptive Content Retention Agent is responsible for assigning and removing items from a policy, removing retention sets, and exporting from hold sets after they are complete.

Retention Agent provides settings that enable you to assign and remove items. After you activate a policy, the assign setting determines how many items this agent assigns to that policy at one time. If you remove a document type or record type from a policy, Retention Agent uses the remove setting to determine how many items to remove.

After you confirm a retention set, Retention Policy Manager accessions, destroys, or transfers the documents or records in that set from your Perceptive Content system. After the disposition action is complete, Retention Agent uses the deletion setting for each set type, such as accession and offline transfer, to determine when to remove that complete set from Management Console.

About Retention Policies and File Plans

A file plan provides a structure to which you associate retention policies in order to process your records.

You assign an active retention policy to a record category in a file plan. A retention policy is required for every record category. The record folder directly below a record category inherits the policy instructions. The system implements the policy for the top-level folder and all items nested under that folder in the structure.

You cannot associate an individual record or record folder to more than one retention policy. Unlike documents (where you associate document types to a policy), a retention policy for a record is implemented based on a record s location in a file plan. Multiple types can exist in the nested folders under a record category; however, a retention policy for records consumes the items based on that hierarchy rather than a grouping of types.

To view records functionality, you must install a Records Manager license.

Glossary of retention terms

This table lists retention terms and descriptions. To view records functionality, you must install a Records Manager license.

Term	Description
Accession	The transfer of physical and legal custody of documents or records to another owner, such as an archival institution.

Term	Description
Authority	An authority represents the legal, regulatory, statutory, or operational entity, such as the federal government or a legal department, that defines lifecycle requirements.
Destruction	The action or process of destroying physical or electronic documents or records beyond any possible restoration.
Disposition	A final action taken regarding documents and records after they are no longer required for day to day access.
Event	An event triggers the retention period of a policy and is comprised of conditions.
Executed policy	The retention policy that is currently applied.
Hold	A hold defines a period of time in which a document or record cannot be modified, destroyed or transferred, even when its retention period is met.
Offline storage	This storage option means that metadata is stored on your Perceptive Content system and that there is an entry point to its location. This type of storage always requires human intervention. You restore data to where it was staged with offline storage. Physical objects and sub-objects, such as annotations and forms data, are also transferred.
Online transfer	This storage option is instantly accessible by Perceptive Content. Online storage does not require any human intervention. The location of this storage must be accessible by ImageNow Server using a local or mapped network drive.
Path	The location of a document or record during a policy phase.
Path details	The time, event, or time and event based rules you define to determine where a document or record falls within a policy. In addition, you use path details to assign approvers and set the disposition action that

Term	Description
	occurs after the retention period ends.
Permanent	A final disposition action that preserves items indefinitely.
Phase	The particular time in the lifecycle.
Phase start date	The date when all conditions necessary for a phase are met.
Physical file	The hard copy version of an item.
Protected	A document or record that is under a protected phase or policy and therefore, you can make limited modifications, such as applying annotations and digital signatures, to it.
Retention policy	A policy determines the length of time a document or record is retained and describes what to do with the item after the retention period expires.
Retention schedule	A list that describes the length of time you need to retain each document or record type to meet the legal, administrative, and historical requirements of your organization. A retention schedule also includes the final disposition for a type after the retention period is met.
System metadata	This metadata stores special purpose information, which can include who captured, modified, or linked a document or record. This information is automatically-populated and managed in Perceptive Content.
Time period	The rule type you use to set the duration of the retention period when an event rule is also defined for the policy or to create a time based policy.
Unprotected	A document or record that is under an unprotected phase or policy can be modified or deleted by a user with the appropriate privileges.

What is a retention policy?

A retention policy is the definition of how to manage a specific set of documents or records, including how long to keep the items and when to remove them.

To view records functionality, you must install a Records Manager license.

You base retention policies on a phase and a path. A phase is particular time in the item s lifecycle. A path is where the items are located during that time period.

Retention Policy Designer enables you to create a simple or advanced policy. In a simple policy, the Retention Policy Designer streamlines your work by providing the phase and path. When you create an advanced path using Retention Policy Designer, you provide the information for the phase and path instead of letting the designer create these items for you. In addition, you can add multiple phases and paths to an advanced policy. In either type, you can add to the policy by defining rules, selecting approvers, and setting the disposition action for each path.

You can protect items that fall under a simple or advanced policy. You protect the entire simple policy as well as protect the phases in the advanced policy. In addition, you can assign authorities to both policy types.

Create a retention policy

To create a new simple or advanced retention policy, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Policies**.
3. On the **Policies** tab, click **New**.
4. In the **New Policy** dialog box, under **Information**, in the **Name** box, type a policy name, such as the record series name.
5. Optional. In the **Identifier** box, type an identifier, such as the record series code.
6. Optional. In the **Description** box, type a description of the documents or records included under this policy.
7. Optional. To assign a retention authority, such as an agency or regulatory body with which the policy complies, complete the following substeps.
    1. Under **Authorities**, click **Add**.
    2. In the **Select Authorities** dialog box, select the authorities.
    3. Click **OK**.
8. In the **New Policy** dialog box, click **OK**.

View record categories assigned to a policy

You can assign a retention policy to record categories in File Plan Designer. To view a list of the record categories associated with a retention policy, complete the following steps.

1. In **Retention Policy Designer**, click **File > Assign**.
2. Click the **Record Categories** tab.

What is record offline transfer?

Offline transfer is the process of exporting and moving records to an offline physical location.

You define the disposition action of offline transfer in a retention policy in File Plan Designer. The disposition action initiates after the retention period ends.

During the process of offline transfer, the system identifies, transfers and removes the record folders and records within a container identified in the associated retention policy. The system exports the contents of the record category to the output directory. The system retains the metatdata associated with the containers and records.

What are record export sets?

Retention Policy Manager uses export sets to transfer records to a physical location when the path disposition action is accession or offline transfer.

You can export contents of any top-level record folder nested directly under a record category. After the retention period ends, you can configure Perceptive Content to add the contents of the top-level record folder to an export set, so that the system exports all of the record folders and records in a path. After the export set is complete, Perceptive Content exports the set to the physical location defined for the path. The amount of time it takes to create and export a set depends on the number of record folders and records in that set.

When creating an export set, Retention Policy Manager converts all the contents of the top-level record folder that fall under a path into XML files. Each XML file contains record life cycle information, record metadata, and binary contents of a file associated with the record. An XML file can also be created in instances where the record or record folder is empty. In addition to the XML files, the system creates a CSV file, a manifest file, and an XSD file for each export set. The CSV file provides a list of items and information specific to the export set, and the manifest file provides a list of files written as part of the export process. The XSD file provides the schema for the XML representing the connections between records of a given transfer set. This information is available to you when you run an export set report.

In Retention Policy Manager, you can view the status and location of all export sets, run reports, and confirm that Perceptive Content exported the contents of the top-level record folder to the designated physical location. Retention Policy Manager uses the path disposition action to determine what actions to perform on the records and metadata that reside in your Perceptive Content system.

- When the disposition action is offline transfer, the system removes the records and leaves the metadata intact.
- When the disposition action is accession, the system uses the removal method defined for the path to determine whether to remove or retain the records and metadata in your system.

After the system performs the required actions for the records and metadata associated with an export set, Retention Policy Manager uses configuration settings defined in the *inserverRetention.ini* on your ImageNow Server to determine when to remove that export set. If required, you can import the contents of an XML file associated with an export set into the Perceptive Content system using Import Agent.

Physical Locations

About administering physical locations

A physical location stores items that are exported as a result of an offline transfer or accession disposition action within a retention policy.

To view records functionality, you must install a Records Manager license.

To create a physical location, you define a name and output directory. When the disposition action is set to Offline transfer or Accession, you associate a policy with a physical location by selecting the name of the location. Additionally, you can define a notification user or group to send a message when an export, copy, or move set for that physical location is complete.

To create and manage physical locations you must have the Manage Retention Policies privilege unless you are Department Manager. When the retention period duration ends, Retention Policy Manager exports the items to the output directory defined for the selected physical location.

> For example, in a human resources department, you define a name for the output directory, such as HR 2012. After you save the physical location, Retention Policy Manager creates the specified directory, HR 2012, in the export location defined in the inserverOutput.ini file. When you create a physical location, you also associate that location with a physical file template.

Create a physical location

To create a physical location complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Locations** tab, click **New**.
4. To create a physical location, in the **New Physical Location** dialog box, perform the following substeps:
   1. In the **Name** box, type a location name.
   2. Optional. In the **Description** box, type a description for the location.
   3. In the **Output directory** box, type a directory name.

   Retention Policy Manager creates a directory in the export location defined in the inserverOutput.ini file using the name you provide in the **Output directory**. This directory stores the documents or records that are exported as a result of an offline transfer or accession disposition action. To view records functionality, you must install a Records Manager license.
5. To associate a physical file template with the physical location, in the **Physical file template** list, select a template.
6. To send an email notification to a user or group when a physical location set is available, in the **Notification user** section, perform one of the following actions:
   - To notify a user, select **User** and then select a user.
   - To notify a group, select **Group** and then select a group.

Note: A user or group member must have an email address configured in his or her user profile in order to receive an email notification

7. Click **OK**.

Modify or rename a physical location

To update the information for a physical location, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Locations** tab, select the location you want to modify.
4. In the **Modify Physical Location** dialog box, perform one or more of the following actions:
   - To modify the name, in the **Name** box, type a new name.
   - To modify the description, in the **Description** box, type a new description.
   - To modify the output directory, in the **Output directory** box, type a new directory name.
   - To modify the physical file template associated with the physical location, in the **Physical file template** list, select a new template.
5. Click **OK**.

Delete a physical location

To delete a physical location, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Locations** tab, select the location and click **Delete**.
4. In the **Delete Physical Location** message box, click **Yes**.

Physical Properties

Physical property data types

You can choose from the following data types when you create a physical file reference. Based on the date type, you can specify a default value that initially populates the physical file template. All physical file templates can contain NULL (empty) values.

Data Type Name	Data Type	Description	Value Restrictions
Date	Date and time field	A date stored as a string. The displayed date and time format is	Not applicable.

Data Type Name	Data Type	Description	Value Restrictions
		based on the settings chosen when you create the physical file template.	
Flag	Boolean field	This data type is always stored as TRUE (1) or FALSE (0). The values that appear are based on the settings chosen when creating the physical file template.	1 or 0 but you can modify the display strings that represent the 1.
List	Predefined list	This data type creates a group of values that a user can select from a list box for the physical file template.	Not applicable.
Number	Decimal number field	Two display formats are available. Decimal data type display format: number fields that support both positive and negative numbers up to a limited number of digits. Zeros to the right of the decimal are suppressed. Currency data type display format: number fields that display as currency defined using one of the ISO 4217 country codes. The default currency setting matches the local settings of the ImageNow Client computer.	Up to 16 digits. Precision of 15 decimal places.
String	Text field	Text fields that support all printable ASCII	The value can contain up to 128 characters.

Data Type Name	Data Type	Description	Value Restrictions
		characters within the Single Byte character set.	This limit varies depending on your database platform.

Create a physical property overview

To create a physical property, which provides details for a physical location such as a shelf or a box, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Properties** tab, click **New** and then complete any of the following actions.
    1. Create a date physical property.
    2. Create a flag physical property.
    3. Create a list physical property.
    4. Create a number physical property.
    5. Create a string physical property.

Modify or rename a physical property

To modify a property that provides details for a physical location, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Properties** tab, select the physical property and click **Modify**.
4. In the **Modify <*type*> Property** dialog box, do any of the following actions:
    - To modify a date property, change such options as the name or display format.
    - To modify a flag property, change such options as the name or display format.
    - To modify a list property, change such options as the name, default value, or list values.
    - To modify a number property, change such options as the name, default value, or decimal placement.
    - To modify a string property, change such options as the name or default value.
5. Click **OK**.

Copy a physical property

To copy a property that provides details about a physical location, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the

list.

2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Properties** tab, select the physical property and click **Copy**.

   The copy appears in the physical file properties list as
   `Copy of <physical property name>`
   .

Delete a physical property

To delete a property that provides details for a physical location, complete the following steps.

You cannot delete a physical property that is in use.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical Properties** tab, select the physical property you want to delete and then click **Delete**.
4. In the **Delete Physical Property** message box, click **Yes**.

About administering physical file templates

About administering physical file templates

The physical file templates allow you to track a physical location for your items.

You create a physical file template when you want to designate the building, shelf, or box location for your physical items. You define a physical file template using physical property data types, such as strings, numbers, or predefined lists. Physical file templates are also used in destruction sets.

Create a physical file template

To create a physical file template, a group of physical properties that you associate with a physical location, complete the following steps.

Prerequisite Before you can perform this procedure you must create physical properties and have the Global > Manage > Retention Policies privilege.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical File Templates** tab, click **New**.
4. In the **New Physical File Template** dialog box, on the **General** tab, perform the following substeps:
   1. In the **Name** box, type a name.
   2. Optional. In the **Description** box, type a description.
5. On the **Physical Properties** tab, perform the following substeps:
   1. In the **By type** list, select the property type you want to display, such as **Date**, **Number**, or **List**.

To display all physical property types, click **All**.

2. Under **Available**, select from the available list of physical properties and then click **Add**.
3. Optional. Click **Move Up** or **Move Down** to change the order in which the physical properties appear in a physical file reference.

6. Click **OK**.

Copy a physical file template

To copy a physical file template, a group of physical properties that you associate with a physical location, complete the following steps.

Prerequisite This procedure requires the Global > Manage > Retention Policies privilege.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical File Templates** tab, select the physical file template you want to copy and then click **Copy**.

   The copy displays in the physical file template list as `Copy of <physical file template name>`.

Modify or rename a physical file template

To update a physical file template, a group of physical properties that you associate with a physical location, complete the following steps.

If the physical file template is in use, there are certain attributes of the physical file template you cannot change. If you need to change an attribute that is no longer modifiable, you can create a new physical file template for this purpose and discontinue using the existing physical file template.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical File Templates** tab, select the physical file template you want to modify and then click **Modify**.
4. In the **Modify Physical File Template** dialog box, perform one or more of the following actions:
   - To change the name, on the **General** tab, in the Name box, type a new name.
   - To change the description, on the **General** tab, in the **Description** box, type a new description
   - To add a property, on the **Properties** tab, in the **By type** list, select a type. In the **Available** list, select a property and then click **Add**.
   - To remove a property, on the **Properties** tab, in the **Added** list, select a type and then click **Remove**.

Delete a physical file template

To delete a physical file template, a group of physical properties that you associate to a physical location, complete the following steps.

You cannot delete a physical file template that is currently in use.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Physical Locations**.
3. In the right pane, on the **Physical File Templates** tab, select the physical file template you want to delete and then click **Delete**.
4. In the **Delete Physical File Template** message box, click **Yes**.

Holds

What is a retention hold?

A retention hold is a retention functionality that you can apply to documents or records that are under a retention policy to prevent users from modifying, deleting, or transferring the document or record.

You apply holds on a per document or records basis. There are two levels of hold application: direct and inherited.

- `Direct hold`: A hold that you apply to a document or record from ImageNowExplorer, ImageNowViewer or Folder Viewer.
- `Inherited hold`: A hold that you apply to a document or record type for all documents or records of that document or record type.

You manage inherited holds in Retention Policy Manager.

You can apply multiple holds to the same document or record, and the document or record remains on hold until all applied holds are removed.

Export a hold set

You can export copies of documents or records in one or more hold sets. Retention Policy Manager creates a directory in the export location defined in the inserverOutput.ini file using the name you provide in the Output directory box. After the hold set is complete, Retention Policy Manager sends you an email notification. To export hold sets, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Holds** tab, under **Select a hold**, select the hold you want to export and then click **Export**.
4. In the **Export Hold Set** dialog box, complete the following substeps.
    1. Under **General**, from the **Physical location** list, select the physical location to which you want to

export the documents or records.

2. In the **Format** list, select **Original format**, **TIFF**, or **PDF**. If the document or record exists in a format other than TIFF or PDF, when you select TIFF or PDF as the format, **Retention Policy Manager** converts the file to the selected format in the physical location, while maintaining the original format in **Perceptive Content**.
3. If you run **Output Agent** on UNIX, you must select **Original format** to export the hold set.
4. If you choose TIFF or PDF as the format, under **Annotations**, in the **Include** list, select one of the following options.

- **Annotations** to include annotations with the document or record.
- **No Annotations** to remove all annotations from the document or record.

5. Click **OK**.

Create a retention hold in Management Console

To prevent users from modifying a document or record, create a retention hold in Management Console by completing the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Holds** tab, click **New**.
4. In the **New Hold** dialog box, on the **Properties** tab, under **General**, in the **Name** box, type a hold name.
5. Optional. In the **Description** box, type a description.
6. Under **Options**, to activate a hold, verify the **Is Active** check box is selected.
7. To give the user the ability to modify document keys, custom properties, and forms when an item is under a hold, select the **Modify custom properties, keys, and forms** check box.
8. Under **Duration**, to create a permanent hold, select **Indefinite**, or to create a hold that expires, select **Expiration date** and then set the date on which you want the hold to expire. To change the default time, click the hours, minutes, or AM, and then enter the new time.
9. Optional. To add hold reasons, on the **Reasons** tab, under **Available**, select one or more reasons for applying this hold and then click **Add**.
10. Optional. To assign this hold at the document or folder type level, on the **Assignment** tab, in the **Document Type** or **Folder Type** list, select one or more document types or folder types and then click **Add**

    Note: Only documents can be assigned holds at the document type level.

    When you assign a hold at the document type or folder type level, all items indexed with that document type or folder type inherit the hold.
11. On the **Security** tab complete the following substeps.
    1. Click **Add**.
    2. In the **Select User** dialog box, select one or more users and click **OK**.

12. Under **Privileges**, perform one or more of the following actions.

Situation	Steps
Allow a user to apply a direct hold.	• Click the column in front of **Apply Retention Hold**.
Allow a user to remove a direct hold.	• Click the column in front of **Remove Retention Hold**.
Allow a user to search for a hold when applied as a direct or inherited hold.	• Click the column in front of **Search for items on Hold**.

13. Click **OK**.

Rename a hold

To change the name of a hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, under **Select a hold**, select a hold and then click **Rename**.
4. Type a new name in the **Name** box.

Copy a hold

When you apply a retention hold to an item in your system, you cannot modify or delete that item, even after the retention period ends. To create a copy of a hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, under **Select a hold**, select a hold and then click **Copy**.

   The system creates a copy of the selected hold.

Modify a hold

To modify information in a hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. Select a hold, and then click **Modify**.
4. In the **Modify Hold**dialog box, perform one or more of the following actions.

- Optional. Click the **Properties** tab to modify hold settings, such as the hold description or duration.
- Optional. Click the **Reasons** tab to add or remove reasons for applying the hold.
- Optional. Click the **Assignment** tab to add or remove the document or record types to which the hold applies.
- Optional. Click the **Security** tab to modify the security for the hold.
- Optional. Click the **History** tab, select the hold, and click **Details** to view hold history and details. Or, in the **Hold History Details** dialog box, click **Previous** or **Next.**

5. Click **OK**.

Delete a hold

To delete a hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, under **Select a hold**, select a hold and then click **Delete**.
4. In the **Delete Hold** dialog box, click **Yes**.

View hold history

To view the hold history, for example when a user applied a hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Holds** tab, select a hold and click **Modify**.

   In the **Modify Hold** dialog box, on the **History** tab, information about the hold appears, including the user who applied the hold and when the hold was applied.
4. Optional. To view detailed information about an event, select the event, click **Details**, and perform one or more of the following actions when the **Hold History Details** displays.
   - To view an event that occurred before the currently selected event, click **Previous**.
   - To view an event that occurred after the currently selected event, click **Next**.
   - To close the **Hold History Details** dialog box, click **Close**.
5. Click **OK**.

Disable a hold

A hold allows you to preserve a document or record. When a document or record is under a hold, users cannot modify or delete the document or record. You can disable permanent and absolute expiration holds. To disable a retention hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.

3. In the right pane, under **Select a hold**, select a hold and then click **Modify**.
4. In the **Modify Hold** dialog box, on the **Properties** tab, clear the **Active** check box.
5. Click **OK**.

Reasons

Create a retention hold reason

To create a reason for applying a retention hold, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Reasons** tab, click **New**.
4. Type a reason in the **Reason** box.

Modify a hold reason

To change a retention hold reason, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Reasons** tab, click **Modify**.
4. Type a new reason in the **Reason** box.

Delete a hold reason

To delete a retention hold reason, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Holds**.
3. In the right pane, on the **Reasons** tab, click **Delete**.
4. In the **Delete Reason** dialog box, click **Yes**.

Sets

What are retention set notifications?

Retention set notifications provide users the ability to review and confirm sets of documents or records before Retention Policy Manager accesses, destroys, or transfers those documents or records from your Perceptive Content system.

Retention Policy Manager sends an email notification to all certified users for all complete destruction, export, move, copy, and export from hold sets. To receive a set notification, a user must have an email address in the Contact Information area of the User Profile and must have the appropriate privileges. The set type also determines who receives an email notification. In addition, if a notification user or group is defined for the physical location, that user or group receives an email notification after an export, move, or copy set is complete.

All retention set email notifications include information about the set, such as the set type and set ID. You can use the set information to determine which set is ready for confirmation or which set you need to resubmit for further processing.

Retention set types

This table lists the type of sets Retention Policy Manager creates when the path disposition action is set to accession, destruction, or offline transfer and the retention period ends. Depending on the disposition action and whether the items are associated with a physical file reference, Retention Policy Managercan create multiple set types. The disposition action can only occur after you confirm or destroy the set.

Disposition Action	**Set Type (Without Physical File References)**	**Click Confirm To:**	**Set Type (With Physical File References)**	**Click Confirm or Destroy To:**
Accession - delete items and metadata (final)	Export (without physical file references)	Remove items and metadata from the system.	Move, then Export (with physical file references)	Verify that the physical files associated with the move set are in a new location. The system updates the physical file references to reflect the physical location. After you confirm the move set, the system creates an export set. After you confirm the export set, Retention

Disposition Action	Set Type (Without Physical File References)	Click Confirm To:	Set Type (With Physical File References)	Click Confirm or Destroy To:
				Policy Manager removes the items and metadata from the system.
Accession - retain items and metadata (not final)	Export (without physical file references)	N/A Items automatically enter the next phase of the policy.	Copy (with physical file references)	Verify that the physical items were copied so you can accession them. After you verify the copy set, the items enter the next phase of the policy. Because the system retains the items and metadata, you are not prompted to enter the new physical location.
Accession - retain metadata and remove items (not final)	Export (without physical file references)	Update the location of the physical items, remove items, and retain metadata. After you confirm this set, items enter the next phase of the policy.	Move, then Export (with physical file references)	Verify that the physical files associated with the move set are in a new location. The system updates the physical file references to the new physical location. After you confirm the move set, the system creates an export set. When you confirm the export set, the system prompts you to enter the physical location of the

Disposition Action	Set Type (Without Physical File References)	Click Confirm To:	Set Type (With Physical File References)	Click Confirm or Destroy To:
				physical items. After you confirm the export set, the system removes the items and updates the physical file reference with the new physical location. After these actions are complete, the items enter the next phase of the policy.
Destruction (final)	N/A	N/A	Destruction (with physical file references)	Remove items and metadata from the system. Retention Policy Manager prompts you to enter the date the physical items were destroyed and the name of the individual who destroyed them.
Offline transfer (not final)	Export (without physical file references)	Update the location of physical items, remove items, and retain metadata. After you confirm this set, items enter the next phase of the policy.	Move (with physical file references)	Verify that the physical items associated with the move set are in a new location. • If the item is not a record, is associated with physical file references, the system creates a

Disposition Action	Set Type (Without Physical File References)	Click Confirm To:	Set Type (With Physical File References)	Click Confirm or Destroy To:
				move set. • For records or record folders that are associated with physical file references, the system creates a move set with an export set. After you confirm the move set, the items enter the next phase of the policy.

Retention set state definitions

Retention Policy Manager provides sets so you can manage the items you need to destroy, accession, or transfer offline after the retention period ends. Retention Policy Manager also provides export sets when you manually export a hold. Retention Policy Manager displays the current set state so that you know when you can take action on a particular set.

Destruction

What are destruction sets?

Retention Policy Manager creates destruction sets for documents associated with physical file references or records and record folders that are designated for destruction.

When the retention period ends, instead of destroying the documents associated with a physical file reference, records, or record folders that fall under a policy, Retention Policy Manager creates a destruction set for those documents, records, or record folders.

The system can destroy documents that are designated for destruction but do not have associated physical file references when the retention period ends. These documents records do not appear in retention sets.

Retention Policy Manager provides a report for each destruction set. This report lists each document, record, or record folder in the destruction set and any associated physical file reference. You can use the report information to determine the physical documents that you or your storage facility need to destroy.

After the physical documents or records are destroyed, you confirm the destruction set. When you confirm the destruction set, Retention Policy Manager prompts you to confirm the date the physical documents were destroyed, the name of the individual who destroyed them, and the destruction method. After you confirm a destruction set, Retention Policy Manager removes the documents and associated metadata in that set from your Perceptive Content system. Retention Policy Manager uses configuration settings to determine when to remove the destruction set from Management Console.

Confirm a destruction set

To remove the documents or records and metadata associated with a destruction set from your system, complete the following steps.

This task assumes the physical documents or records in the set have been destroyed.

1. In **Management Console**, in the left pane, click **Retention > Sets**.
2. In the right pane, on the **Destruction** tab, select the appropriate set, and then click **Destroy**.
3. In the **Confirm Set Destruction** dialog box, enter the following physical destruction properties:
    1. In the **Date** box, type the date of the destruction or select a date from the calendar control.
    2. In the **Name** box, type the name of the individual who performed the destruction.
    3. In the **Method** box, type a description of the destruction method.
4. Click **OK**.

Generate a destruction report

To create a destruction report in CSV format, complete the following steps.

Prerequisite This procedure requires the Global > Manage > Retention Policies privilege.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Sets**.
3. In the right pane, on the **Destruction** tab, select a retention set and then do the following actions:
    1. Click **Report**.
    2. In the **Save As** dialog box, enter a name for the report and then navigate to the location where you want to save the report.
    3. Click **Save**.
4. To view the report, in Windows Explorer, navigate to the location you chose to save the report. Then, open the CSV file in any application that supports that type of file, including Microsoft Excel or a text editor.

View a destruction set

Viewing a destruction set allows you to view items that are submitted for destruction. This information gives you the opportunity to determine which documents or records you want to destroy. To view a destruction set, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the

list.

2. In the left pane, click **Retention > Sets**.
3. In the right pane, click the **Destruction** tab to view the following information for each set:
   - **Name** contains the name of the destruction set.
   - **Creation Date** contains the date the destruction set was created.
   - **State** contains the state of the destruction set.

Export

What are export sets?

Retention Policy Manager uses export sets to transfer items to a physical location when the path disposition action is accession or offline transfer.

After an item s retention period ends, you can have Perceptive Content add the item to an export set, so that all of the items in a path are exported at the same time instead of exporting one item at a time. After the export set is complete, it is exported to the physical location defined for the path. The amount of time it takes to create and export a set depends on the number of items in that set.

When creating an export set, Retention Policy Manager converts each item that falls under a path to an XML file that meets DoD (Department of Defense) 5015.02 standards. Each XML file contains the item s image file and associated metadata, such as keys and keywords. An XML file can also be created in instances where the item is empty.When an item contains multiple pages, the system creates a separate XML file for each page in that item. In addition to the XML files, the system creates a CSV file for each export set. The CSV file contains information that is specific to the export set. This information is available to you when you run an export set report.

In Retention Policy Manager, you can view the status and location of all export sets, run reports, and confirm that the items were exported to the designated physical location. Retention Policy Manager uses the path disposition action to determine what actions to perform on the items and metadata that reside in your Perceptive Content system.

- When the disposition action is offline transfer, the system removes the pages and leaves the metadata intact.
- If the disposition action is accession, the system uses the removal method defined for the path to determine whether to remove or retain the pages and metadata in your system.

After the system performs the required actions for the pages and metadata associated with an export set, Retention Policy Manager uses configuration settings to determine when to remove that export set. If required, you can bring any XML file associated with an export set back into the Perceptive Content system using Import Agent.

Confirm an export set

To confirm that an export is complete, perform the following steps.

1. In **Management Console**, in the left pane, click **Retention > Sets**.
2. In the right pane, on the **Export** tab, select the appropriate set and then click **Confirm**.

3. In the **Confirm Set Export** dialog box, to update the location of the exported files, enter the new physical reference properties and then click **OK**.

Generate an export set report

To create an export set report in CSV format, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Sets**.
3. In the right pane, on the **Export** tab, select a retention set and then do the following actions:
    1. Click **Report**.
    2. In the **Save As** dialog box, enter a name for the report and then navigate to the location where you want to save the report.
    3. Click **Save**.
4. To view the report, in Windows Explorer, navigate to the location you chose to save the report and open the CSV file in any application that supports that type of file, including Microsoft Excel or a text editor.

Retry an export set request

You can resubmit a request to complete an export set action in order to export a second copy of a set, or if the initial export action is interrupted. If an interruption in the action was due to an error, you can only retry the export after you resolve the error. To retry an export set request, complete one of the following procedures.

An error can interrupt the creation, report creation, export, and removal of export sets.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Sets**.
3. In the right pane, on the **Export** tab, complete one of the following procedures:

Situation	Steps
To export another copy of a set	1. Select a set with the state **Pending relocation confirmation** or **Hold set complete**. 2. Click **Retry**.
To resume an export action that has been interrupted due to an error	1. Select a failed set. 2. Click **Retry**.

View an export set

To view information about a retention set that a user exported or attempted to export, complete the following steps.

You define the path of the export set in *inserverOutput.ini*. The output directory is defined in the physical location.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Sets**.
3. In the right pane, click the **Export** tab to view the following information for each set:
   - **Name** contains the name of the export set.
   - **Creation Date** contains the date the export set was created.
   - **State** contains the state of the export set.
   - **Path** contains the path of the export set shown as *[machine name]\export path\output directory\set name_time stamp*.

Move and Copy

What are move and copy sets?

Move and copy sets allow you to manage the accession or offline transfer of your physical items.

To view records functionality, you must install a Records Manager license.

When items are associated with a physical file reference and the disposition action for the path is accession or offline transfer, the system automatically creates a move or copy set. Each set type contains a CSV file. This file lists the keys for each item and the current physical location.

Retention Policy Manager creates a separate set for each physical file reference and uses the disposition action to determine the set type. When the path disposition action is offline transfer (not final), Retention Policy Manager creates a move set. After a move set is confirmed for this disposition action, the items in that set move to the next phase in the policy.

If the path disposition method is accession, the removal method determines the type of set the system creates. When the method removes the pages, but retains the metadata (not final), the system creates a move set. Retention Policy Manager also creates a move set when the removal method deletes both the items and metadata (final). After a move set is confirmed for removal, the items in that set move to an export set.

When the accession removal method retains the items and metadata (not final), Retention Policy Manager creates a copy set, and the items and metadata remain in the system. After a copy set is confirmed, the items in that set enter the next phase in the retention policy.

Confirm a move or copy set

Move and copy sets contain document or record locations and associated keys, and can be exported to manage the accession or offline transfer of your physical documents or records. To confirm that an export has finished in the desired location, complete the following steps.

1. In **Management Console**, in the left pane, click **Retention > Sets**.
2. In the right pane, on the **Move and Copy** tab, select the appropriate set and click **Confirm**.
3. To update the location of the exported files, in the **Confirm Move Set or Confirm Copy Set** dialog box, enter the new physical reference properties and click **OK**.

Retry a move or copy set report

You can resubmit a request for Perceptive Content to complete a move or copy set report when the initial action is interrupted by an error. The move or copy report set action can only resume after you resolve the error that caused the original action to fail. To retry a move or copy set report, complete the following steps.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. In the left pane, click **Retention > Sets**.
3. In the right pane, on the **Move and Copy** tab, select a failed set and then click **Retry**.

Recognition Agent

What is Recognition Agent?

Recognition Agent is a dedicated, high-volume, server-side agent used to automatically acquire document property values and perform full text recognition during various CaptureNow capture processes.

Recognition Agent offers ICR/OMR/OCR, Barcode, and Forms Identification recognition modules.

- The ICR/OMR/OCR module automatically acquires property values and full text from documents during the batch scanning process.
- The Barcode module is a high-performance barcode solution with robust algorithms for recognizing and decoding 1D, 2D, and postal symbologies. It reads barcodes scanned in grayscale, as well as small or compact barcodes and, with the advanced capability, it scans barcodes that are heavily damaged or skewed.
- The Forms Identification module provides the ability to automatically identify a form without registration or anchor marks.

Licenses for Recognition Agent

A separate license is required for each of the three Recognition Agent modules. The following information describes when you need each license.

Recognition Agent modules

The following licenses are available for Recognition Agent modules.

Recognition Agent - ICR, Recognition Agent - OCR, and Recognition Agent - OMR.

The OCR, ICR, and OMR licenses for the ICR/OMR/OCR module are always required when using Recognition Agent because this module provides the base Recognition Agent functionality.

Barcode

If you need to process barcodes using zonal OCR, advanced barcode options, or iScript (such as when you scan a barcode through a multi-function device and submit it to Recognition Agent through workflow), the license for the Barcode module is required in addition to the licenses for the ICR/OMR/OCR module. CaptureNow, the scanning environment management module, provides basic barcode functionality. When you use CaptureNow to process barcodes, you do not need the Recognition Agent licenses described above. Instead, you need the appropriate CaptureNow licenses.

Recognition Agent - Form Identification

If you need Recognition Agent to automatically identify a form, the license for the Forms Identification module is required in addition to the licenses for the ICR/OMR/OCR module.

Guidelines for enhancing recognition rates

Use the following methods to enhance the ability for Recognition Agent to process files.

- When scanning files to submit to Recognition Agent, configure the scanning profile to scan at a minimum of 300 DPI.
- Use image processing filters, such as Deskew and Despeckle.
- If using Kofax VRS, use the automatic-orientation image processing filter to align the image correctly prior to submitting the file to Recognition Agent.
- If you have the option to change the font used in a file, select Courier 10 point font. Recognition Agent can identify multiple fonts, but Courier 10 point is ideal.
- When possible, submit files to Recognition Agent with printed text instead of hand-written text.

Set Recognition Agent logging

ImageNow Server provides logging specifically for troubleshooting Recognition Agent. Logging set in the *inserverRec.ini* file enables you to audit or troubleshoot Recognition Agent. To specify the level of logging for Recognition Agent, complete the following steps.

1. In the *[drive:]**__*inserver*__*\etc* folder, locate the *inserverRec.ini* file and open it in a text editor.
2. Under `[Logging]`, choose any of the following options.
3. To specify the level of logging for errors, for the `debug.level.file` setting, type one of the following numbers:
   - Type `0` for no logging
   - Type `1` (for the least verbose logging), `2`, `3`, `4`, `5`, or `6` (for more verbose logging)
4. To specify the level of logging for pipe errors, for the `debug.level.pipe` setting, type one of the following numbers:
   - Type `0` for no logging

- Type `1` (for the least verbose logging), `2`, `3`, or `6` (for the most verbose logging)

5. To specify whether to log recognition errors, for the `recognizer.level` setting, type one of the following numbers:
   - Type `0` to not log errors
   - Type `1` (for the least verbose logging), `2`, `3`, or `6` (for more verbose logging)
6. To specify a new location for **Recognition Agent** to store log files, for the `recognizer.path` setting, type a new path. The default path is **Recognition Agent**.
7. Save and close the file.
8. Restart the **Recognition Agent** service.

Forms Identification Module

Enable automatic form identification

The following procedure is a required step in setting up automatic form identification. It requires the Recognition Agent - Form Identification and Recognition Agent - OCR licenses.

1. Use a text editor to modify the *inow.ini* file in the following folder: *[drive:]**inserver**\etc*.
2. To enable automatic form identification, in the [Auto Form] section, change the auto.form.integration setting as shown: `auto.form.integration = TRUE`.

   Note: Be careful not to alter a similar section, [Forms], which contains the statement form.integration=TRUE.

3. Save and close the *inow.ini* file.
4. Optional. If you want to straighten any skewed images as part of automatic form recognition, which can improve form matching, perform the following steps:
   1. Use a text editor to modify the *inserverRec.ini* file in the following folder: *[drive:]**inserver**\etc*.
   2. In the **[Auto Form ID]** section, change the form.enable.deskew setting as shown: form.enable.deskew = TRUE
5. Optional. To improve form matching, also in the **[Auto Form ID]** section of the *inserverRec.ini* file, change the `form.identification.quality` setting as shown: `form.identification.quality=60`

   Note: Valid values are 0-100. The default is 60. Increasing the number may improve your results, but an increase can adversely affect the performance of the identification processor.

6. Save and close the *inserverRec.ini* file.

Set a document type to automatic form identification

To set automatic form identification for a document type, complete the following steps.

1. In the capture profile, on the **Document Keys** tab, double-click **Doc Type**.

   Note: You can create one or more capture profiles that initiate automatic form identification. If the

same ImageNow Client uses automatic form identification with more than one ImageNow Server, create a separate capture profile for each server and do not use the same capture profile with different servers.

2. In the **Key Definition** dialog box, in the **Type** list, leave **Document Type** selected. Automatic form identification requires this **Type** value.
3. In the **Value** list, select the document type that will be assigned to all images that cannot be matched to a master form by automatic form identification.
4. Select the **Enable automatic form identification** check box.
5. In the **Confidence** list, leave **MEDIUM** selected.
6. Optional. If the first captured page matches a master form, **Perceptive Content** can automatically assign the remaining pages in the batch to the corresponding document type, which speeds performance. To choose this option, select the **Accept the entire batch if form matches first scanned page** check box. If this option is enabled, **Perceptive Content** seeks a match on only the first page of that captured batch. If the first page does not return a match, it will not attempt to match any of the remaining pages.

Test automatic form identification

Before making automatic form identification available to your users, make sure that the master forms and confidence levels you have defined are returning a satisfactory number of correctly identified documents.

Prerequisite You must install, license, and configure the Forms Identification module.

1. Use each capture profile you created with the automatic form identification feature to capture a typical set of pages or files.
2. When all documents in a batch have reached the linking step, inspect the **Document Type** column in the batch grid to determine which images were correctly matched to their document types.

   If Perceptive Content correctly assigned document types to a satisfactory number of forms, you can make the capture profiles available to your users.

Troubleshoot automatic form identification

If you experience issues using automatic form identification, try any of the following possible resolutions.

I am unable to match captured images to the correct master forms

Cause	Resolution
Many or all of my captured images are not being matched with master forms.	Inspect your capture profile and make sure the confidence level is set to LOW.
Some of my master forms are very similar, and automatic form identification is matching the	Modify your capture profile and raise the confidence level to MEDIUM and try again. If you still see

Cause	Resolution
captured images to the wrong master form.	mismatches, raise the confidence level to HIGH.
During linking, the item type that was correctly assigned by automatic form identification is overwritten by the value assigned in the application plan.	When linking items captured with automatic form identification, make sure that the application plan you select in the Properties pane is not set up to overwrite proposed key values.

I am unable to log information for automatic form identification

Cause	Resolution
Logging is not enabled.	Enable logging for automatic form identification. Enable logging in the *inserverRec.ini* file using the form.debug.level.file setting.

OCR

What is OCR?

Recognition Agent offers an ICR/OMR/OCR recognition module to automatically acquire property values and full text from documents during the batch scanning process.

The ICR/OMR/OCR module captures information using OCR, OMR, and ICR technologies on a specific zonal location defined on a document. You specify to perform OCR on text in a defined zone during the capture process and assign the gathered text to a document property field. When using the Forms Identification Module, Recognition Agent can also automatically assign data to the Document Type property.

With an OCR zone, you define an area of a document for Recognition Agent to search and then store the search results in an index key. For each zone, you select an OCR filling method to identify the information contained in a zone. In addition, you can assign a script to a capture profile that looks for standard data preceding the data you want to acquire.

> For example, if you want Recognition Agent to gather an ID number from an image, and the image being scanned is standardized to always contain the text "ID : " before the ID number appears, you can indicate in a script for CaptureNow to find the "ID : " value on the page and then acquire the 11 digits following that information. The script adds additional accuracy when regions defined for OCR are extremely close in proximity on the document.

Create an OCR zone for a document property

You can specify to perform OCR on text in a defined zone during the capture process, and assign the gathered text to a document property field. To configure a document property for zonal OCR, complete the following steps.

Prerequisite This procedure requires that the ICR/OMR/OCR Module for Recognition Agent is installed. If the capture profile does not already exist, you must create it before you begin this procedure.

You define this option in a capture profile set to Batch mode. This option is supported for files in the following formats: BMP, PNG, JPEG, TIFF, GIF. It performs a read of the text on a document in TIFF format. This agent cannot acquire data from Word documents or other non-raster file types. You can submit non-raster files to ImageNow Printer to convert them to TIFF format and then submit the converted files to Recognition Agent. When using OCR, a 300 DPI or higher is recommended.

1. On the **Perceptive Content** toolbar, click **Capture > Manage Capture Profiles**.
2. In the **Capture Profiles** dialog box, select the capture profile and click **Modify**.
3. On the **Document Key** tab, double-click a property.
4. In the **Key Definition** dialog box, in the **Type** list, click **OCR Zone**.
5. Click **Settings**.
6. In the **New Zone** dialog box, under **Zone Description**, in the **Name** box, type a name for the new zone.
7. In the **Method** list, select the method you want to use.
8. To specify an **iScript** to apply to the OCR results, in the **Run** list, select a script.
9. Under **Coordinates**, perform the following substeps:
    1. In the **Unit** box, click **Imperial (inches)** or **Metric (cm)**.
    2. In the **Top** box, select or type a number. The number represents the location of your data from the top of a page.
    3. In the **Left** box, select or type a number. This number represents the location of your data from the left most margin of a page.
    4. In the **Width** box, select or type the width of the data you want to acquire.
    5. In the **Height** box, select or type the height of your data.
10. Optional. Under **Verification & Checking**, perform the following substeps:
    1. To specify a minimum level of confidence on OCR results that is acceptable before the **Recognition Agent** returns a failure, select the **OCR Verification Score** check box and enter a number. The default is 63%.
    2. In the **Suspicious Character** box, type a character, such as **#** or **~**, that you want **Recognition Agent** to use in place of characters read by OCR without a high level of confidence as defined in the verification score.
    3. Click **OK**.
11. In the **Key Definition** dialog box, click **OK**.
12. Repeat the previous steps for each property for which you want to define an OCR zone.

OCR zone properties

The following properties are available in the New Zone dialog box for defining an OCR zone for the Field1, Field2, Field3, Field4, and Field5 document properties.

Zone Description

The following properties appear in the Zone Description area.

Name

The name you want to give the OCR Zone.

Method

Specifies which filling method to use for this zone.

Run iScript

Specifies an iScript to apply to the OCR results.

Coordinates

The following properties appear in the Coordinates area.

Height

Set how high in inches or centimeters that the desired information appears on the page.

Left

Set how many inches or centimeters from the left margin of the page that the desired information appears.

Top

Set how many inches or centimeters from the top of the page that the desired information appears.

Unit

Set the unit to inches or centimeters to establish what area of the page you want to acquire.

Width

Set how wide in inches or centimeters that the desired information appears on the page.

Verification and Checking

The following properties appear in the Verification and Checking area.

OCR Verification Score

Specifies the minimum confidence (if any) that is acceptable before the Recognition Agent will return a failure. The default is 63%.

Suspicious Character

Denotes unknown characters with a symbol.

OCR methods

The following table lists the OCR methods available when you configure Perceptive Content to submit documents to Recognition Agent for OCR processing.

Automatically detect format

Specifies that Recognition Agent selects the most suitable recognition method for the zone. This module filling method does not detect hand-printed alphanumeric text.

Barcode

Specifies the page or zone contains a 1D or 2D barcode.

Common numeric fonts

Specifies the page or zone contains printed numeric characters.

Common text fonts

Specifies the page or zone contains common alphanumeric, printed text.

Dot matrix printer text

Specifies the zone contains alphanumeric text printed on a dot-matrix printer.

Handprinted text

Specifies the page or zone contains hand-printed alphanumeric text.

OCR A

Specifies the page or zone contains OCR-A alphanumeric text.

OCR B

Specifies the page or zone contains OCR-B alphanumeric text.

MICR

Specifies the page or zone contains numeric characters printed with special magnetic inks such as those found on personal checks. Recognition Agent supports both E13B and CMC7 formats.

Optical Mark Recognition

Specifies the page or zone contains a possible marking such as a check mark.

Typewriter text

Specifies the page or zone contains printed text.

Output Agent

What is Output Agent?

Output Agent is a server-side process that lets you output documents on a job-by-job basis or in a batch.

When using this agent in a Windows environment, Output Agent can output documents directly to a printer or to a file. You can also output documents in various formats, such as JPEG, TIFF, GIF, BMP and raster PDF, and then print the output files at any time.

Output Agent running on a Windows environment additionally offers the ability to output documents in DICOM format and transmit them to a DICOM server. DICOM is an optional feature of Output Agent and requires an additional license.

You can install Output Agent on Windows and UNIX; however, functional differences between the two environments do exist.

For more details about the features available when Perceptive Content is running in a UNIX environment, refer to the Output Agent for UNIX Installation Guide.

Output Agent outputs copies of documents, called output files. The Perceptive Content documents remain unaltered within the Perceptive Content repository.

Manually create a keyfile

You can manually create and submit a keyfile that specifies the documents you want Output Agent to locate in Perceptive Content and output based on the parameters specified in the inserverOutput.ini file. Depending on your business needs, you can use iScript to automatically generate an Output Agent job or to generate a keyfile. To manually create a keyfile, perform the following steps.

1. Using a text editor, create a file in a temporary location.
2. Using the following guidelines, type a row in the file that defines each document key value you want **Perceptive Content** to search and return matching documents.
   - Use the structure `DRAWER^FIELD1^FIELD2^FIELD3^FIELD4^FIELD5^DOC TYPE^DOCNAME`.
   - Any combination of values can remain blank.
3. Using the file extension specified for the `monitor.extension` setting in the *inserverOutput.ini* file, save and close the file.

   Example The default file extension for the `monitor.extension` setting is TXT.
4. Move the text file to the folder specified for the `monitor.path` setting in the *inserverOutput.ini* file.

   Example The default path is *$(IMAGENOWDIR)/output_agent*.

The following row returns all documents in the AP drawer with a Field2 value of *12345*, regardless of the Field1 value:*AP^^12345*

Output annotations on output files

To configure Output Agent to always include existing annotations on output files, except when iScript disables the layout.annotations.show setting for a job, perform the following steps.

Prerequisite This feature is only available when running Output Agent in a Windows environment.

1. In the *[drive:]**inserver****etc*** folder, locate the *inserverOutput.ini* file and open it in a text editor.
2. Under `[Layout]`, set **layout.annotations.show** to `TRUE`.
   An iScript can override the **layout.annotations.show** setting on a per job basis.
3. Save and close the file.
4. Restart the **Output Agent** service.

Common output file formats

The following table lists the most commonly used file types when configuring Output Agent to export documents. These exported documents are called output files. You specify a file type for output files using the export.file.type setting in the [Export] group of the inserverOutput.ini file.

Output File Type	Value for the export.file.type setting
GIF	2
TIFF	3
Windows BMP	6
JPEG	10
PNG	11
TIFF with JPEG compression	17
TIFF with LZW compression	27
TIFF with G3 compression	29
TIFF with G4 compression	75
TIFF with RLE compression	87
Raster PDF uncompressed	146
Raster PDF with G3 compression	147

Output File Type	Value for the export.file.type setting
Raster PDF with G4 compression	149
Raster PDF with JPEG compression	150

Specify a header for output pages

To configure Output Agent to include a header at the top of each output sheet, complete the following steps.

This feature is only available when running Output Agent in a Windows environment

1. In the *[drive:]**inserver****etc** folder, locate the *inserverOutput.ini* file and open it in a text editor.
2. Under `[Layout]`, for the `layout.header` setting, type the text and output variables that you would like to appear in the header.
3. Save and close the file.
4. Restart the **Output Agent** service.

Troubleshoot item output

If you experience issues outputting an item to email, file, fax, or printer, you can try any of the following possible resolutions.

Output takes longer than expected

Cause	Resolution
The output job submitted is too large for ImageNow Client.	For large and complex output jobs, consider using Output Agent, a server-side process that allows you to output items on a job-by-job basis or in a batch.
Added colors and annotations are slowing the output job.	For best performance, configure your output profiles to convert color images to black and white and only use the color conversion option when needed.

Microsoft Outlook settings are not available when outputting an item to email

Cause	Resolution
Perceptive Content only supports a text-based editor in Outlook.	If you are using Microsoft Word as your default email editor in Outlook, settings such as signature, spell-check, and other editing capabilities may not be available when outputting an item.

Set Output Agent logging

To specify the level of logging for Output Agent, perform the following steps.

1. In the *[drive:]**__*inserver*__*\etc* folder, locate the *inserverOutput.ini* file and open it in a text editor.
2. Under `[Logging]`, to specify the level of logging for errors, for the **debug.level.file** setting, type one of the following options.
   - Type `0` to not log errors.
   - Type `1` through `6` depending on the logging level you want.
   - Type `9` to log the time it takes Output Agent to render files.

   Example Examples of output rendering include drawing annotations and images on an output page, and drawing multiple output pages on a sheet.
3. Repeat the above action for the **debug.level.pipe** setting.
4. To specify whether to log communication between **ImageNow Server** and **Output Agent**, for the **socket.level.file** setting, type one of the following integers.
   - Type `1` to log communication.
   - Type `0` to not log communication.
5. Save and close the file.
6. Restart the **Output Agent** service.

About logging for Output Agent

Output Agent provides logging specifically for troubleshooting output issues.

Log files for Output Agent reside in the [drive]:\inserver\log folder. Log files are named as inserverOutput_ <instance_name>_<date>.log so you can easily identify the file you need. Log files show information about output jobs submitted to Output Agent through iScript and for an output batch submitted to Output Agent through a keyfile.

The Diagnostics feature in Management Console also enables you to monitor Output Agent sessions.

If iScript submits an output job to Output Agent, you can review the status of the job in Job Manager in addition to checking log files for information.

Ooutput Variables

What are output variables?

Output variables specify the different parameters used when generating output files.

You can define one or more variables for Perceptive Content to generate the file name or a header for an output file. You can also provide static text for part of the file name or header.

When exporting items, you can use output variables to specify whether you want to export the item as a single output file, multiple output files (one output file for each file contained in the item), or separate sheets (one output file for each page of the item).

Output variable guidelines

Output variables specify the different parameters Output Agent uses when generating output files.

Guidelines

When using output variables, keep the following guidelines in mind:

- Enclose variables in brackets.
- You can separate static text and variables with underscores such as [DOCID]_Page_Number_ [PAGENUM]) to make the file name or header easier to read.
- You can specify the width of some variables used for file names, such as [%0<a positive integer>PAGENUM]. Defining the width of a variable used to generate a file name helps with file organization when you export multiple documents to a folder.
- Defined file names should not contain the following characters: \ / : * ? " < > |. If any of these characters appear in a file name, Output Agent replaces them with underscores. Defined header names can contain the earlier listed characters.
- When using variables to generate a file name, the entire file path, which includes the file name and extension, cannot exceed the character limit set by your operating system. For example, Windows XP allows a file path up to 255 characters in length.

Available output variables for file names

The following table lists variables you can use to define file names of documents exported by Output Agent, called output files. You specify these variables for the export.filename.format setting in the [Export] group of the *inserverOutput.ini* file.

Exported Document

Variables

Use the following variables to define a name of an exported document.

`[DOCID]`

The Document ID of the exported document

`[DOCNAME]`

The name of the exported document

`[DRAWER], [FIELD1], [FIELD2], [FIELD3], [FIELD4], [FIELD5], or [DOCTYPE]`

The document keys of the exported document

`[DOCNUM]`

A unique value

[%0<a positive integer>DOCNUM]

A unique value while specifying a width for the value.

If you assign the variable `[%03DOCNUM]` and Perceptive Content assigns the exported file as the fifth exported file, the document number included in the exported file name is 005.

Exported Document Page

Variables

Use the following variables to define a name of each page in an exported document.

[ACTUALPAGENUM]

A unique value

[%0<a positive integer>ACTUALPAGENUM]

A unique value while specifying a width for the value.

If you assign the variable `[%03ACTUALPAGENUM]`, a document with 5 pages is exported as 5 files with file names that include the following: 001, 002, 003, 004, and 005.

Exported Document File

Variables

Use the following variables to define the name of each file in an exported document.

[PAGENUM]

A unique value

[%0<a positive integer>PAGENUM]

A unique value while specifying a width for the value.

If you assign the variable `[%03PAGENUM]`, a document that contains the file types PDF, DOC, TIFF, and PNG is exported as 4 files with file names that include the following: 001, 002, 003, and 004.

Exported Sheet/Output Page

Variables

Use the following variables to define the name of an exported sheet, or output page, that contains multiple pages of a document.

[SHEETNUM]

A unique value. You define the number of pages exported per sheet for the `layout.pages.per.sheet` setting in the [Layout] group.

[%0<a positive integer >SHEETNUM]

Unique value while specifying a width for the value.

If you define the export.filename.format setting as `[%03SHEETNUM]`, and you define the layoutpages.per.sheet setting as 4, a document that contains four pages is exported as one sheet with a file name that includes 001.

Available output variables for page headers

The following table lists variables you can use to define a header at the top of each output sheet, or output page, that Output Agent outputs in a file. To specify variables for the header, use the layout.header setting in the [Layout] group of the *inserverOutput.ini* file.

Variables

[DOCID]

Document ID

[DRAWER], [FIELD1], [FIELD2]. [FIELD3]. [FIELD4], [FIELD5], [DOCTYPE]

Document keys. Each document key will be separated with a / .

[PAGE]

Page number

[TOTALPAGES]

Total number of pages

Example

If Output Agent outputs an output file based on a document with the following document keys, and the layou.header setting is set to `[KEYS]`, the following header will appear on each page of the output file: `AP/12345/4341/Acme Corp/33356/Paid/Invoice`

Document Key	Example Configuration	Example Value
Drawer	AP	AP
Field1	Vendor ID	12345

Document Key	Example Configuration	Example Value
Field2	Document ID	4341
Field3	Vendor Name	Acme Corp
Field4	Control Number	3356
Field5	Status	Paid
Doc Type	Invoice	Invoice

Import Agent

What is Import Agent?

The ImageNow Server installation includes Import Agent, which performs bulk importing of electronic files into Perceptive Content. These files become items, such as documents or records.

Import Agent uses an automated import process that requires no user interaction. You can configure Import Agent to poll a particular directory, at a given interval, for a specific file type. If Import Agent finds the designated file type, it attempts to import the file. After Import Agent imports the file, the system treats the file like any other Perceptive Content item.

To use Import Agent to capture files into Perceptive Content, you must select a mode. Each mode provides a distinct method to gather and assign item property values to the imported files. A configuration file, inserverImp.ini, controls all aspects of the import process.

To view records functionality, you must install a Records Manager license.

Import Agent import modes

To use Import Agent to capture documents or records into Perceptive Content, you must select a mode. Each mode provides a distinct method to gather and assign item property values to the imported files. You designate the mode in the Import Agent configuration file, inserverImp.ini. The following sections describe each mode.

INDEX_FILE

Use INDEX_FILE mode to import data objects specified in a separate single-line or multiple-line index file. This is the default import mode.

COMBO

Use COMBO mode to import combined index files and text data objects in ASCII file format. Import Agent gathers property values from the first line of each file and imports the remaining data in the file.

KEYMAPPING

Use KEYMAPPING mode to import TIFF files. Import Agent provides property values based on the TIFF tags that are present in the imported TIFF file.

TIFF_TEXT_COMBO

Use TIFF_TEXT_COMBO mode to import TIFF files. Each TIFF file must have an accompanying text file that contains the text of the TIFF file. Import Agent searches the text to gather property values.

FILENAME

Use FILENAME mode to import files and generate property values based on each file name.

DATA_CAPTURE

Use DATA_CAPTURE mode to import files and submit them to DataCapture. DataCapture performs OCR on the files and assigns property values based on defined templates.

DOD_RECORD

Use DOD_RECORD mode to import XML files into Perceptive Content as records. Import Agent gathers property values from the XML files.

To view records functionality, you must install a Records Manager license.

DOD_XML

Use DOD_XML mode to import XML files into Perceptive Content as documents. Import Agent gathers property values from the XML files.

CAPTURE_PROFILE

Use CAPTURE_PROFILE mode to define a server-based capture profile that imports files as documents or records and assigns property values to the files.

To view records functionality, you must install a Records Manager license.

Configure Import Agent capture profile mode overview

To enable Import Agent to import files as documents or records using Capture Profile mode, you must configure several components. Unlike the other Import Agent modes, Capture Profile mode provides the ability to assign custom property values to an item upon import, and to store a new item in a content model. We recommend that you configure the components in the order listed below. To configure Import Agent Capture profile mode, complete the following steps.

1. Configure Import Agent for an application plan to assign and map metadata to captured content.
2. Create an Import Agent source profile or Create an Import Agent source profile for a record to define which file types to import, the method to gather item property values, and whether to move or delete the

source files after **Import Agent** captures them.

Note: To view records functionality, you must install a Records Manager license.

3. Create an Import Agent capture profile for a document or Create an Import Agent capture profile for a record to identify which application plan and source profile to use when importing files, and to define how to process the resulting items.
4. Configure the *inserverImp.ini* file for Capture Profile mode to specify details such as the import mode and the directory from which to import files.

Configure Import Agent for Capture Profile mode

The *inserverImp.ini* file contains configuration settings for Import Agent. The file is the last component you must configure to enable Import Agent to capture files using Capture Profile mode. To configure the *inserverImp.ini* file for Capture Profile mode, complete the following steps.

1. Stop the **Import Agent** service.
2. Navigate to the *[drive:]**inserver****etc**\inserverImp.ini* file and open it with a text editor.
3. Under **[General]**, perform the following substeps:
    1. For **import.mode**, specify **CAPTURE_PROFILE**.
    2. For **import.directory**, specify a directory for **Import Agent** to monitor for import files. The default is *$(IMAGENOWDIR)/import*.
    3. For **pause.between.transactions**, specify how long, in milliseconds, **Import Agent** pauses between pages when processing a batch. The default is 100.
    4. To move (instead of delete) source files after import, for **import.failed.directory**, specify a directory to move source files that fail to import, and for **import.complete.directory**, specify a directory to move source files that successfully import.

        Note: You define whether to move or delete source files in the Import Agent source profile. When you set the source profile to move source files after import, Import Agent looks to the *inserverImp.ini* file to identify where to move the files.

    5. For **num.directory.workers**, specify the number of worker threads used to monitor the directory specified for the **import.directory** setting. The default is 1.
    6. For **num.import.workers**, specify the number of worker threads used to import files. The default is 1.
    7. For **capture.profile**, specify the name of an active **Import Agent** capture profile.

    Note: Do not change the default value for the **poll.interval** setting without first consulting Product Support. This value specifies how often, in seconds, Import Agent searches for new import files.

4. Under **[File Contention]**, for loop, specify the number of times **Import Agent** checks a file before importing it to ensure the file is complete. The default is 10.
5. To audit or troubleshoot **Import Agent**, under **[Logging]**, perform any of the following options:
    - To log errors, for **debug.level.file**, specify 1 (for the least logging information), 2, 3, 4, 5, or 6 (for

the most logging information). The default is 0, which does not log errors.

- To log communication between ImageNow Server and Import Agent, for **socket.level.file**, specify 1. The default is 0, which does not log communication.

6. If you installed **Import Agent** on a different computer than **ImageNow Server**, under **[Remote]**, perform the following substeps:
   1. For **Remoted**, specify TRUE.
   2. For **hearbeat.interval**, specify how often, in seconds, **Import Agent** verifies its connection. The default is 60.
   3. For **server.ip.address**, specify the IP address of **ImageNow Server**.
   4. For **server.ip.port**, specify the port number of **ImageNow Server**.

   Note: Do not change the default value for the **socket.login.timeout,socket.default.timeout**, or **force.server.validation** setting without first consulting Product Support.

7. To change the serial number format that **Import Agent** generates and assigns to each import job, under **[Serial Number]**, perform the following substeps:
   1. For **serial.number.format**, enclose the default value of **%d** in < > and add text, a specified minimum number of digits, or both.

      Example when you specify <Acme%04d> and the imported job is number 118, Import Agent assigns the serial number Acme0118.

   2. For **serial.number.startvalue**, specify a start value for the serial number. The default is 0.
8. To set whether **Import Agent** writes new files directly to the main OSM set when OSM write caching is enabled, under [OSM], for **bypass.write.cache**, specify one of the following options:
   - TRUE. Writes new files to the main OSM set. TRUE is the default value.
   - FALSE. Writes new files to the cache OSM set. If a cache OSM set is not available, writes new files to the main OSM set.
9. Save and close the *inserverImp.ini* file.
10. Start the **Import Agent** service.

Create an Import Agent capture profile for a document

An Import Agent capture profile stores the settings you define for Import Agent to import files into a document. To create an Import Agent capture profile, complete the following steps.

An Import Agent capture profile is one component required to define an Import Agent Capture Profile mode.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. Click **Capture**.
3. In the right pane, on the **Capture Profile** tab, click **New > Import Agent**.
4. In the **Capture Profile Definition** wizard, on the **Capture Profile Content Type** page, select **Document**.
5. On the **Capture Profile Information** page, complete the following substeps.

1. Type a name and optional description for the capture profile.
2. Verify that the **Profile is active** check box is selected.
3. Click **Next**.

6. On the **Capture Profile Source** page, select one of the following options.
   - **Create a new source profile**.
   - **Select an existing source profile** and then choose a source profile from the list.
7. On the **Capture Profile Options** page, complete the following substeps.
   1. In the **Application plan** list, select the **Import Agent** application plan that you want to associate with this capture profile.
   2. Optional. In the **Workflow process** list, select the workflow process to which you want to route the new documents.
   3. If you selected a workflow process, in the **Workflow queue** list, select the workflow queue to which you want to route the new documents.
   4. Optional. To submit documents to **Recognition Agent** for bar code scanning, select the **Submit to Content Server** check box.
   5. Optional. To add documents to version control, select the **Submit to version control** check box.
   6. Click **Next**.
8. On the **Capture Profile Verification** page, review your capture profile configuration settings and complete one of the following actions.
   - To modify a configuration setting, click **Back** and make any needed changes.
   - To keep the configuration settings, click **Finish**.

Create an Import Agent capture profile for a record

You define an Import Agent capture profile to store the settings that enable Import Agent to import files as records. To create an Import Agent capture profile, complete the following steps.

An Import Agent capture profile is one component required to define an Import Agent Capture Profile mode.

1. In **Management Console**, in the left pane, under **Select Department**, select a department from the list.
2. Click **Capture**.
3. In the right pane, on the **Capture Profile** tab, click **New > Import Agent**.
4. In the **Capture Profile Definition** wizard, on the **Capture Profile Content Type** page, select **Record**.
5. On the **Capture Profile Information** page, complete the following substeps.
   1. Type a name and optional description for the capture profile.
   2. Verify that the **Profile is active** check box is selected.
   3. Click **Next**.
6. On the **Capture Profile Source** page, select one of the following options.
   - **Create a new source profile**.
   - **Select an existing source profile**. Select a source profile from the list.

7. On the **Capture Profile Application Plan** page, select the application plan that you want to associate with this capture profile and click **Next**.
8. On the **Capture Profile Verification** page, review your capture profile configuration settings and complete one of the following actions.
   - To modify a configuration setting, click **Back** and make any necessary changes.
   - To keep the configuration settings, click **Finish**.

Import Agent key mapping options

The following list describes the mapping options available in the [Key Mapping] group in the *inserverImp.ini* file. These options map values to document property fields defined for imported files.

<Any valid document type>

Assign the name of an existing document type in your system.

Example

When doc.type=Invoice, Import Agent assigns the Invoice document type to the new document.

<Any valid drawer>

Assign the name of an existing drawer in your system.

Example

When drawer=Accounts Payable, Import Agent stores the new document in the Accounts Payable drawer.

<<index provided>>

Assign a value specified in the applicable mode group, such as [Mode KEYMAPPING] or [Mode FILENAME].

Example

When field1=<<index provided>> in the [Key Mapping] group, and you configure the [Mode FILENAME] group to locate the field1 value in the file name of an imported file, Import Agent locates the value in the file name and assigns it to the field1 document property.

DEFAULT

Assign the value DEFAULT.

Example

When drawer=DEFAULT, Import Agent stores the new document in the drawer named DEFAULT.

<<date/time>>

Assign the date and time that Import Agent imports the file.

Example

When field3=<<date/time>>, Import Agent assigns the date and time it imported the file to the field3 document property.

<Literal text>

Assign a literal string of text up to 39 characters.

Example

When field3=Acme, Import Agent assigns the literal text "Acme" to the field3 document property.

<<SerialNumber>>

Assign the serial number that Import Agent generates as defined in the [Serial Number] group.

Example

When field3=<<SerialNumber>>, Import Agent assigns the generated serial number to the field3 document property.

<<tiff_tag >>

When import.mode=KEYMAPPING, assign values from a TIFF tag using the following format: <<tiff_tag <tag#> <tag_length> <key_start_position> <key_length>>>

Example

When field1=<<tiff_tag 65329 10 3 5>>, Import Agent locates the specified information in a TIFF tag and assigns it to the field1 document property.

<<search,<string parameter>>>

When import.mode=TIFF_TEXT_COMBO, use Parameter 1 or Parameter 2 to search an index file for values. The fixed_string is case sensitive and must match the string in the text file.

Parameter 1

```
<<search,fixed_string,skip number, extract number>>
```

Import Agent locates the string (fixed_string) and skips y characters while reading x characters. Import Agent does not stop reading a string at an EOL and it removes an EOL from the result string.

y = skip number

x = extract number

Parameter 1 Example

When field1=<<search,"Patient No: ",0,9>>, Import Agent locates the specified information in an index file and assigns it to the field1 document property.

Parameter 2

```
<<search,fixed_string,skipped number,EOL,EOL_ordinal>>
```

Import Agent locates the string (fixed_string) and assigns the first 40 characters of the result string as the property value.

When EOL_ordinal = 1, read to the first line EOL and stop.

When EOL_ordinal = 2, read to the second line EOL and stop.

When EOL_ordinal = 3, read to the third line EOL and stop.

Parameter 2 Example

When field1=<<search,"a",1,EOL,2>>, Import Agent locates the specified information in an index file and assigns it to the field1 document property.

<<undefined>>

Do not assign a value.

Example

When field3=<<undefined>>, Import Agent does not assign a value to the field3 document property.

<<uniqueID>>

Assign the unique ID that generates for each document.

Example

When field3=<<uniqueID>>, Import Agent assigns the document's unique ID to the field3 document property.

Import Agent serial number formats

Import Agent generates and assigns a serial number to each import job. The following table lists the values you can combine to specify a format for the serial number. You specify the format for the serial.number.format setting in the *inserverImp.ini* file.

%d

Assign the standard serial number.

Example

When serial.number.format =%d, and the imported job is number 118, Import Agent assigns the serial number 118.

Text<%d>

Assign a serial number that includes text.

Example

When serial.number.format =Acme<%d>, and the imported job is number 118, Import Agent assigns the serial number Acme118.

When serial.number.format =Acme<%d>Invoice, and the imported job is number 118, Import Agent assigns the serial number Acme118Invoice.

<%number of digitsd>

Assign a serial number that includes the specified minimum number of digits. If the serial number value is shorter than the specified number of digits, Import Agent pads the value with spaces.

Example

When serial.number.format =<%2d>, and the imported job is number 118, Import Agent assigns the serial number 118.

When serial.number.format =<%4d>, and the imported job is number 118, Import Agent assigns the serial number 118.

<%0number of digitsd>

Assign a serial number that includes the specified minimum number of digits. If the serial number value is shorter than the specified number of digits, Import Agent pads the value with zeros.

Example

When serial.number.format =<%04d>, and the imported job is number 118, Import Agent assigns the serial number 0118.

Text<%number of digitsd>

Assign a serial number that includes text and the specified minimum number of digits while padding shorter values with spaces.

Example

When serial.number.format =Acme<%2d>, and the imported job is number 118, Import Agent assigns the serial number Acme118.

When serial.number.format =Acme<%4d>Invoice, and the imported job is number 118, Import Agent assigns the serial number Acme 118Invoice.

Text<%0number of digitsd>

Assign a serial number that includes text and the specified minimum number of digits while padding shorter values with zeros.

Example

When serial.number.format =<Acme%08d>, and the imported job is number 118, Import Agent assigns the serial number Acme00000118.

When serial.number.format =Acme<%04d>Invoice, and the imported job is number 118, Import Agent assigns the serial number Acme0118Invoice.

About running multiple instances of Import Agent

You can install and run more than one instance of Import Agent to increase efficiency when importing a high number of files, as well as to specify unique import settings for different groups of files.

If your organization uses Import Agent to process a high number of files, you can refer to the Import Agent Throughput Best Practices document for guidelines to tune your system for high throughput and efficiency to maximize performance. Based on your requirements and server performance, an additional instance of Import Agent can provide enhanced performance along with optimizing your overall system.

To determine the number of Import Agent instances needed to optimize your processes, you must determine the number of pages you want to import per day and then test the throughput of your existing instance of Import Agent. Add additional instances of Import Agent based on the throughput your system's configuration provides and the number of pages you need to import. You can also contact your Perceptive Software representative to arrange a review by a technical architect.

Install another instance of Import Agent

You can install and run any number of instances of Import Agent on each installation of ImageNow Server. We recommend that you install a new instance of Import Agent in a test environment, test to ensure that other solutions such as server-based printing are not affected, and then migrate the new instance of Import Agent to your production environment. To add another instance of Import Agent to a Windows environment, complete the following steps.

1. Stop all running instances of **Import Agent**. **Import Agent** runs as a Service in Windows.
2. To copy the *EXE* file, complete the following substeps.
    1. Navigate to the *[drive:]**inserver****bin** or *[drive:]**inserver****bin64*** directory.
    2. Create a copy of the *inserverImp.exe* file in the same directory as the original file.
    3. Rename the new file *inserverImp<instance number>.exe*, replacing *<instance number>* with the sequential number of the **Import Agent** instance you want to add.

        Example To add a second instance of Import Agent, name the new file *inserverImp2.exe*.
3. To copy the INI file, complete the following substeps.
    1. Navigate to the *[drive:]**inserver****etc*** directory.
    2. Create a copy of the *inserverImp.ini* file in the same directory as the original file.
    3. Rename the new file *inserverImp<instance number>.ini*, replacing *<instance number>* with the sequential number of the **Import Agent** instance you want to add.

        Example To add a second instance of the Import Agent ini file, name the new file *inserverImp2.ini*.

4. Configure the new *inserverImp<instance number>.ini* file.
4. To install the new instance of **Import Agent**, at the **Command Prompt** window, complete the following substeps.
    1. Navigate to the *\inserver\bin directory*.
    2. Run the following command, where `<instance number>` represents the number of the **Import Agent** instance you want to add: `inserverImp<instance number> -i`
5. Start all instances of **Import Agent**.

Set Import Agent logging

ImageNow Server provides logging specifically for troubleshooting import issues. Logging set in the *inserverImp.ini* file enables you to audit or troubleshoot Import Agent. To specify the level of logging for Import Agent, complete the following steps.

1. In the *[drive:]**__inserver\etc__ folder, locate the *inserverImp.ini* file and open it in a text editor.
2. Under **[Logging]**, choose any of the following options:
    - To specify the level of logging for errors, for the **debug.level.file** setting, type `0`for no logging or `1` (the least logging information), `2`, `3`, `4`, `5`, or `6` (the most logging information).
    - To specify whether to log communication between ImageNow Server and Import Agent, for the *socket.level.file* setting, type `0` to not log communication or `1` to log communication
3. Save and close the file.
4. Restart the **Import Agent** service.

Monitor Agent

What is Monitor Agent?

Monitor Agent enables you to track the status of any Perceptive Contentagent and perform actions based on an event that occurred.

You can use Monitor Agent to help you track the status of agents and perform tasks. By customizing the Monitor Agent configuration file, you can use Monitor Agent to automate certain administrative actions of agents when any of the following events occur:

- An agent terminates abnormally.
- Dump files are created by crashing agents.

An action is an automated process initiated by Monitor Agent in response to an event. When an event occurs, Monitor Agent can perform the following actions in response:

- Restart the process.
- Archive log reports on a schedule or in response to an event.

Additionally, Monitor Agent can perform an action on a defined schedule regardless of any events that may or may not have occurred.

What is a Monitor Agent process?

Monitor Agent processes determine how to manage events that occur to specific agents.

A process is a group of parameters made up of a defined name, one or more events, and one or more actions for each event. You can optionally define your processes to override these thresholds defined in the basic settings and trigger alternate actions in response to a failed action.

To easily reuse a process to monitor several agents, you can define it as part of a Monitor Agent profile.

What is a Monitor Agent profile?

Monitor Agent profiles are a simplified approach to performing the same actions simultaneously across multiple agents in response to a specific event.

A profile is a customized setup of processes, events, and actions used for automating Monitor Agent activity. Profiles are set to activate when specific events occur, such as an abnormal termination or a perceived memory leak. You then choose what actions Monitor Agent should take in response to those events, and the subsequent Monitor Agent processes that should run.

An ideal profile setup would automate Monitor Agent functions in such a way that processes would not have to be manually run in most scenarios.

Monitor Agent process elements

The following list defines the elements you can use when creating a process in Monitor Agent.

Elements

Monitor Agent functionality is supported in Windows and Unix environments except where noted.

`<process>`

The unique name for each process Monitor Agent monitors.

Required?

Yes

`event<n>`

An event ID unique to each process where <n> represents a consecutive positive integer.

Required?

Yes

`<named_event>`

One of the following events to which you want Monitor Agent to respond. You can designate only one event for each event<n> or failedaction<n> element.

Required?

Yes

Event Name	Description
AbnormalTermination	An agent stops unexpectedly. (Windows only)
TimeOfDay	A certain time of day or day of the week has passed.

<setting>

This element enables you to override the thresholds you designated in the [Defaults] group. You can override the following settings:

Required?

No

Event Name	Description
Time	Time, based on a 24-hour clock, when an agent takes place.
Day	Day of the week when an action takes place.

<value>

When you are overriding a setting s threshold, you must specify a value for the setting.

Required?

No, unless using the <setting> element.

<action<n>

An action ID unique to each process where <n> represents a consecutive positive integer.

Required?

Yes

<named_action>

One of the following actions you want Monitor Agent to perform in response to an event or failed action.

Required?

Yes

Action Name	Description
RestartProcess	Monitor Agent restarts the process.
Archive	Monitor Agent archives files.

<failedaction<n>

A failed action ID unique to each process where <n> represents a consecutive positive integer.

Required?

No

The following list demonstrates how to use the elements to create a process:

<process>.event<n> = <named_event>

Defines the event ID and the event name for the process.

Required?

Yes

<process>.event<n>.<setting> = <value>

Overrides the event s threshold with the specified value of the setting defined in the [Defaults] group.

Required?

No

<process>.event<n>.action<n> = <named_action>

Defines the action Monitor Agent performs in response to the event.

Required?

Yes

<process>.event<n>.action<n>.<setting> = <value>

Overrides the action s setting with the specified value of the setting defined in the [Defaults] group.

Required?

No

<process>.event<n>.action<n>.failedaction<n> = <named_action>

Defines the action Monitor Agent performs if the original action fails to complete.

Required?

No

<process>.event<n>.action<n>.failedaction<n>. <setting> = <named_action>

Overrides the action's setting with the specified value of the setting defined in the [Defaults] group.

Required?

No

The following sample process archives the log files on the day and time specified in the *[Defaults]* group of the *inserverMonitor.ini* file. If Alarm Agent is unresponsive for 30 seconds, Monitor Agent will restart Alarm Agent.

```
AlarmAgent.event1 = TimeOfDay

AlarmAgent.event1.action1 = Archive

AlarmAgent.event2 = NonResponsive

AlarmAgent.event2.NonResponsiveTime = 30

AlarmAgent.event2.action1 = RestartProcess
```

Create a Monitor Agent process

You create a process to enable Monitor Agent to perform specific actions in response to one or more events. To create a process, complete the following steps.

Monitor Agent functionality is supported in Windows and Unix environments except where noted.

1. Navigate to the *[drive:]**inserver****etc*** folder and open the *inserverMonitor.ini* file in a text editor.
2. In *inserverMonitor.ini*, under the `[Processes]` group, enter `<process>.event<n>`, where *<process>* is a process name you created in the `[Defines]` group and *<n>* is an event ID represented by a consecutive positive integer.
3. Set the value for the string you created in the preceding step to one of the following events.
   - **AbnormalTermination** An agent stops unexpectedly.
   - **TimeOfDay** A certain time of day or day of the week has passed.
4. Optional. In Windows, to specify a threshold that is different from the thresholds identified in the `[Defaults]` group, append one of the following setting names to the end of the `<process>.event<n>` setting and define the value.
   - **Time** Time, based on a 24-hour clock, when an action takes place.
   - **Day** Day of the week when an action takes place.

5. Complete the following substeps for each action you want to define for each event.
   1. For each event you defined, copy the string and paste the copied string below the original string.
   2. Append `action<n>` to the string you pasted, where <*n*> is an action ID represented by a consecutive positive integer.
6. Set the value for the string you created in the preceding step to one of the following actions.
   - **RestartProcess**Monitor Agent restarts the process.
   - **Archive**Monitor Agent archives files.
7. Optional. To specify an alternate action that **Monitor Agent** follows if the first action fails, complete the following substeps.
   1. Create a new string for the process, event, and action and append `.FailedAction<n>` to the end of the string, where<*n*> is an action ID represented by a consecutive positive integer.
   2. Enter `RestartProcess` or `Archive` as the value for the failed action you created in the preceding step.
8. When you are done creating processes, save and close the *inserverMonitor.ini* file.

Monitor Agent profile elements

The following list defines the elements you can use when creating a profile in Monitor Agent.

Elements

Monitor Agent functionality is supported in Windows and Unix environments except where noted.

profile<n>

A profile ID unique to each process where <n> represents a consecutive positive integer.

Required?

Yes

event<n>

An event ID unique to each process where <n> represents a consecutive positive integer.

Required?

Yes

<named_event>

One of the following events to which you want Monitor Agent to respond. You can designate only one event for each event<n> or failedaction<n> element.

Required?

Yes

Event Name	Description
AbnormalTermination	An agent stops unexpectedly. (Windows only)
TimeOfDay	A certain time of day or day of the week has passed.

<setting>

This element enables you to override the thresholds you designated in the [Defaults] group. You can override the following settings:

Required?

No

Event Name	Description
Time	Time, based on a 24-hour clock, when an agent takes place.
Day	Day of the week when an action takes place.

<value>

When you are overriding a setting s threshold, you must specify a value for the setting.

Required?

No, unless using the <setting> element.

<action<n>>

An action ID unique to each process where <n> represents a consecutive positive integer.

Required?

Yes

<named_action>

One of the following actions you want Monitor Agent to perform in response to an event or failed action.

Required?

Yes

Action Name	Description
RestartProcess	Monitor Agent restarts the process.
Archive	Monitor Agent archives files.

<failedaction<n>>

A failed action ID unique to each process where <n> represents a consecutive positive integer.

Required?

No

The following list demonstrates how to use the elements to create a process:

profile<n>.event<n> = <named_event>

Defines the event ID and the event name for the process.

Required?

Yes

profile<n>.event<n>.<setting> = <value>

Overrides the event s threshold with the specified value of the setting defined in the [Defaults] group.

Required?

No

profile<n>.event<n>.action<n> = <named_action>

Defines the action Monitor Agent performs in response to the event.

Required?

Yes

profile<n>.event<n>.action<n>.<setting> = <value>

Overrides the action s setting with the specified value of the setting defined in the [Defaults] group.

Required?

No

profile<n>.event<n>.action<n>.failedaction<n> = <named_action>

Defines the action Monitor Agent performs if the original action fails to complete.

Required?

No

profile<n>.event<n>.action<n>.failedaction<n>. <setting> = <named_action>

Overrides the action's setting with the specified value of the setting defined in the [Defaults] group.

Required?

No

In the example below, Profile1 responds to two events: Abnormal termination and GDI leak. Based on the profile settings, when a process encounters an abnormal termination (event1), Monitor Agent restarts the process. When the process experiences a GDI leak as defined in the *[Defaults]* group, Monitor Agent runs the program identified in the defaults.program setting defined in the *[Defaults]* group.

```
[Profiles]
profile1.event1 = AbnormalTermination
profile1.event1.action1 = RestartProcess
profile1.event2 = GDILeak
```

In the *[Processes]* group, you can identify Monitor Agent rules you set in the Profile1. To apply a profile to a process, under the *[Processes]* group, enter the process name as you defined in the *[Defines]* group, enter an equal sign (=), then enter the profile ID. In the example below, Monitor Agent manages specific events that happen to Alarm Agent and Batch Agent.

```
[Processes]
AlarmAgent - profile1
BatchAgent = profile1
```

Create a Monitor Agent profile

A profile identifies a process, and a process is a group of parameters made up of a defined name, one or more events, and one or more actions for each event. To create a Monitor Agent profile, complete the following steps for each event you want to define for the profile.

1. Navigate to the *[drive:]***\inserver\etc** folder, and then in a text editor, open the *inserverMonitor.ini* file.
2. In the *inserverMonitor.ini* file, under the `[Profiles]` group, enter `profile<n>.event<n>`, where <*n*> after profile is a profile ID represented by a consecutive positive integer and <*n*> after event is an event ID represented by a consecutive positive integer.

3. Set the value for the string you created in the previous step to one of the following events.
   - **AbnormalTermination** An agent stops unexpectedly.
   - **TimeOfDay** A certain time of day or day of the week has passed.
4. Optional. To specify a threshold that is different from the thresholds identified in the `[Defaults]` group, append one of the following setting names to the end of the `profile<n>.event<n>` setting and define the value.
   - **.Time** Time, based on a 24-hour clock, when an action takes place.
   - **.Day** Day of the week when an action takes place.
5. For each event you defined, copy the string and paste the copied string below the original string.
6. Append `action<n>` to the string you pasted, where <*n*> is an action ID represented by a consecutive positive integer.
7. Set the value for the string you created in the preceding step to one of the following actions.
   - **RestartProcess**Monitor Agent restarts the process.
   - **Archive**Monitor Agent archives files.
8. Optional. To specify an alternate action that **Monitor Agent** follows if the first action fails, create a new string for the profile, event, and action and then append `.FailedAction<n>` to the end of the string, where <*n*> is an action ID represented by a consecutive positive integer.
9. Enter one of the follow actions as the value for the failed action you created in the preceding step.
   - **RestartProcess**Monitor Agent restarts the process.
   - **Archive**Monitor Agent archives files.
10. To activate the profile, under the `[Processes]` group, type the following string, where <*Defined_Process*> is a process you defined in the `[Defines]` group and Profile<*n*> is the profile ID you just created: `<Defined_Process> = Profile<n>`
11. When you are done creating profiles, save and close the *inserverMonitor.ini* file.

Restart non-responsive agents

In Windows, you can configure Monitor Agent to restart an agent when it is unresponsive. To set automatic restart behavior for agents in Monitor Agent, complete the following steps.

1. Navigate to the *[drive:]**__inserver\etc__ directory and open the *inserverMonitor.ini* file in a text editor.
2. To specify the agent you want to restart when it becomes non-responsive, under `[Processes]`, create the following string where <*DefinedProcess*> is the agent you want to restart and `event<n>` is a consecutively numbered event: `<DefinedProcess>.event<n> = NonResponsive`

   Example In the following, Monitor Agent performs an action when Alarm Agent becomes non-responsive: `AlarmAgent.event2 = NonResponsive`
3. Optional. If you want to override the default non-responsive time specified in the `[Defaults]` group, complete the following substeps.
   1. Create a new string identical to the string you created in the previous step.
   2. Append `.NonResponsiveTime` to the string.

3. Set the value equal to the time in seconds you want **Monitor Agent** to wait until it defines the process as non-responsive.

   Example In the following example, Monitor Agent triggers an event to perform an action after Alarm Agent is non-responsive for 30 seconds: `AlarmAgent.event2 = NonResponsiveAlarmAgent.event2.NonResponsiveTime = 30`

4. To specify that **Monitor Agent** restarts an agent after it has been non-responsive, create the following string where `<DefinedProcess>` is the agent you want to restart, `event<n>` is a consecutively numbered event, and `action<n>` is a consecutively numbered action: `<DefinedProcess>.event<n>.action<n> = RestartProcess`

   Example In this example, Monitor Agent restarts Alarm Agent after it has been unresponsive as defined by the defaults.nonresponsivetime settings under the [Defaults] group: `AlarmAgent.event2 = NonResponsiveAlarmAgent.event2.action1 = RestartProcess`

5. Save and close the *inserverMonitor.ini* file.

Restart agents on a defined schedule

You can use Monitor Agent to restart an agent on a schedule you determine to help optimize performance. To specify a day and time to restart the agent, complete the following steps.

1. Navigate to the *[drive:]**__inserver__*\etc* directory and open the *inserverMonitor.ini* file in a text editor.
2. To specify the agent for which you want to schedule restarts, under `[Processes]`, create a *`<DefinedProcess>`*`.event`*`<n>`* `= TimeOfDay` with the following components:

String Component	Represents
`<DefinedProcess>`	The agent you want to restart.
`event`*`<n>`*	A consecutively numbered event

   Example To have Alarm Agent perform an action on the day and time defined in the `[Defines]` group, enter `AlarmAgent.event1 = TimeOfDay`.

3. Optional. To override the default time of day specified in the `[Defaults]` group, complete the following substeps:
   1. Create a new string identical to the string you created in the previous step.
   2. Append `.time` to the string.
   3. Set the value equal to time represented by a 24-hour period.

   Example To have Alarm Agent trigger an event to perform an action at 7:00 AM on the day defined in the `[Defines]` group, enter `AlarmAgent.event1.time = 07:00`.

4. Optional. To override the default day specified in the `[Defaults]` group, do the following substeps:
   1. Create a new string identical to the string you created in the first step.
   2. Append `.day` to the string.

3. Set the value equal to the day of the week, or `EVERYDAY` to include all days.

Example To have Alarm Agent trigger an event to perform an action every Tuesday at the time defined in the `[Defines]` group, enter `AlarmAgent.event1.day = TUESDAY`.

5. To specify that **Monitor Agent** restarts the agent on the defined or overridden day and time, create a *<DefinedProcess>*`.event`*<n>*`.action`*<n>* `= RestartProcess` string with the following components:

String Component	Represents
<DefinedProcess>	• The agent you want to restart.
`event`*<n>*	• A consecutively numbered event.
`action`*<n>*	• A consecutively numbered action.

Example To have Monitor Agent restart Alarm Agent at 7:00 AM every Tuesday, enter `AlarmAgent.event1.action1 = RestartProcess`.

6. Save and close the *inserverMonitor.ini* file.

```
[Processes]
AlarmAgent.event1 = TimeOfDay
AlarmAgent.event1.time = 07:00
AlarmAgent.event1.day = TUESDAY
AlarmAgent.event1.action1 = RestartProcess
```

Restart agents based on a threshold

In Windows, you can configure Monitor Agent to restart an agent when memory, threads, GDI, or handles expand beyond a threshold. To enable an automatic restart when Monitor Agent activity reaches a set threshold, complete the following steps.

1. Navigate to the *[drive:]*`\inserver\etc` directory and open the *inserverMonitor.ini* file in a text editor.
2. To specify the agent you want to restart when it reaches a set threshold, under the `[Processes]` group, create a *<DefinedProcess>*`.event`*<n>* `= <type>Leak` string with the following components:

String Component	Represents
<DefinedProcess>	The process you defined in the `[Defines]` group.

String Component	Represents
`event<n>`	A consecutively numbered event.
`<type>Leak`	• MemoryLeak • ThreadLeak • GDILeak • HandleLeak

Example To have Monitor Agent perform an action when Alarm Agent memory expands beyond a defined threshold, enter `AlarmAgent.event3 = MemoryLeak`.

3. Optional. To override the default amount of memory, thread, GDI, or handle leak specified in the `[Defaults]` group, create a string identical to the string you created in the previous step and append any of the following components:

String Component	Represents
`.memory`	Kilobytes of memory in a memory leak.
`.threads`	The number of threads in a thread leak.
`.GDI`	The number of GDI objects in a GDI leak.
`.handles`	The number of handles in a handle leak.

4. Set the value equal to the maximum allowed by **Monitor Agent** before it considers the amount excessive.

   Example To have Monitor Agent trigger an event to perform an action after Alarm Agent memory expands to 500 KB, enter `AlarmAgent.event3.memory = 500` after `AlarmAgent.event3 = MemoryLeak`

5. To specify that **Monitor Agent** restarts an agent after an activity reaches a set threshold, create a `<DefinedProcess>.event<n>.action<n> = RestartProcess` string with the following components:

String Component	Represents
`<DefinedProcess>`	The agent you want to restart.
`event<n>`	A consecutively numbered event.
`action<n>`	A consecutively numbered action.

Example To have Monitor Agent restart Alarm Agent after the memory expands beyond the threshold defined in the `defaults.memory` settings in the `[Defaults]` group, enter `AlarmAgent.event3.action1 = RestartProcess`.

6. Save and close the *inserverMonitor.ini* file.

```
[Processes]
AlarmAgent.event3 = MemoryLeak
AlarmAgent.event3.memory = 500
```

or

```
[Processes]
AlarmAgent.event3 = MemoryLeak
AlarmAgent.event3.action1 = RestartProcess
```