
Absolute Manage *User Guide*

Windows Admin Version

Absolute[®]Software
www.absolute.com

May 8, 2012

Absolute Manage User Guide 6.1 - Documentation Release 1

This document, as well as the software described in it, is confidential and contains proprietary information protected by non-disclosure agreements. No part of this document may be reproduced in any form or disclosed to any party not bound by a non-disclosure agreement without the express written consent of Absolute Software Corporation.

Absolute Software Corporation reserves the right to revise this document and to periodically make changes in the content hereof without obligation of such revisions or changes unless required to do so by prior agreement.

Information contained herein is believed to be correct, but is provided solely for guidance in product application and not as a warranty of any kind. Absolute Software Corporation assumes no responsibility for use of this information, nor for any infringements of patents or other rights of third parties resulting from the use of this information.

Absolute Software Corporation, Suite 1600, Four Bentall Centre, 1055 Dunsmuir Street PO Box 49211 Vancouver, British Columbia, Canada V7X 1K8.

©2011 Absolute Software Corporation. All rights reserved. Computrace®, Computrace Mobile™ and Absolute are registered trademarks of Absolute Software Corporation. All other trademarks are property of their respective owners. Computrace US Patents #5,715,174, #5,764,892, #5,802,280, #5,896,497, #6,244,758, #6,269,392, #6,300,863, and #6,507,914. Canadian Patents #2,205,370 and #2,284,806. U.K Patents #EP793823, and #GB2338101. German Patent #695 125 34.6-08. Australian patent #699045. Japanese Patent #JP4067035.

Contents

Part 1: Getting Started	1
1 Introduction	2
What does Absolute Manage do?	2
The Absolute Manage system.....	2
Elements of the Absolute Manage system.....	3
How commands work.....	3
How software distribution and license monitoring work	5
How managing mobile devices works	6
Windows Phone	8
Ports used	8
Absolute Manage users	9
Users	9
Administrators.....	9
2 Installation	11
Overview	11
Before you install	11
System requirements	12
Choosing a computer for Absolute Manage Server.....	13
Installing Absolute Manage Server.....	14
Installing Absolute Manage Server on Mac OS X.....	14
Installing Absolute Manage Server on Windows.....	14
After the installation.....	15
Installing Absolute Manage Admin	15
Installing Absolute Manage Admin on Mac OS X.....	15
Installing Absolute Manage Admin on Windows.....	15
Initial configuration of Absolute Manage Server.....	16
Displaying a server's certificate.....	18
Exporting a server certificate	19
Exporting a certificate in Absolute Manage Admin	19
Copying a certificate from the server computer	19
Installing support for reinstalling Windows computers	20
Setting up the Absolute solution.....	20
Setting up the FOG solution.....	22
Setting Absolute Manage Server up for FOG support	23
Installing MDM support	24
Preparation	24
Installing the MDM server	25
Installing the MDM server on Windows	25
Installing the MDM server on Mac OS X.....	25
Importing the SSL key into the certificate	26
Configuring the MDM server	27
Configuring the Exchange server	28
Installing Absolute Manage Agent.....	29
Installation method	30
Installing Absolute Manage Agent manually on Mac OS X.....	30
Installing Absolute Manage Agent manually on Windows.....	30
Installing Absolute Manage Agent using the Agent Deployment Center	33
Prerequisites	34
Overview.....	34
Creating zones in the Agent Deployment Center.....	34
Searching zones	36
Editing zones.....	37
Deleting zones	37
Installing or updating Absolute Manage Agent	38

Enrolling mobile devices.....	39
Enrollment using the MDM server	40
Enrollment using a different web server.....	41
Updating Absolute Manage.....	42
Updating the Agent.....	42
Updating the Software Distribution Center from Absolute Manage 1.x.....	43
Updating the Software Distribution Center.....	43
Choosing distribution points	43
Updating distribution points.....	43
Updating software packages.....	44

Part 2: Using Absolute Manage45

3 Accounts and agent access	46
Overview	46
Administrator accounts	46
Active Directory and Open Directory integration	47
Administrator privileges	47
The relation of agents to servers	47
Agent access	48
Administrator accounts	48
Creating an administrator account from scratch	48
Giving administrator access to an Active Directory account.....	50
Editing administrator accounts.....	51
Disabling and enabling administrator accounts.....	52
Deleting administrator accounts	52
Using administrator accounts.....	53
Logging in	53
Logging out.....	53
Switching accounts	53
Changing your password	54
Assigning servers to agents	54
Assigning inventory servers to agents.....	55
Assigning software distribution or license monitoring servers to agents	57
Appointing administrators to devices	57
Working with appointment groups.....	58
Setting up a standard appointment group.....	58
Setting up a smart appointment group	59
Reusing smart groups.....	60
Editing appointment groups.....	60
Deleting appointment groups	60
Appointing administrators	60
Removing administrators from agents or mobile devices.....	61
Viewing the device to which an administrator is appointed.....	61
Viewing the administrators who are appointed to a device	61
Setting MDM access rights for mobile devices.....	62
Specifying MDM access rights	62
Updating MDM access rights on enrolled iOS devices.....	64
Creating placeholder records for computers	65
Creating placeholder records for computers.....	65
Deleting placeholder records	66
Exporting and importing server settings	66
Exporting server settings on Mac OS X.....	67
Exporting server settings on Windows	67
Importing server settings on Mac OS X.....	67
Importing server settings on Windows	68
4 Gathering and managing information	69
Overview	69

Gathering information	69
Custom information	69
Information storage on the server	69
Displaying information.....	70
Rearranging information.....	70
Custom information	70
Gathering information	70
Configuring automatic information gathering.....	71
Gathering and updating information manually.....	73
Manually gathering computer, font, printer, or startup item information	73
Manually gathering processes information	74
Manually gathering information on installed software	75
Manually requesting information from the server.....	76
Gathering information on files.....	76
Gathering information on registry entries	78
Collecting USGCB SCAP compliance reports	80
Custom information	81
Defining custom information fields	82
Editing custom information fields	85
Deleting custom information fields.....	85
Setting up custom information field mirroring.....	86
Assigning custom information fields	87
Unassigning custom information fields.....	88
Using custom information fields	88
Editing manual custom information fields.....	89
Importing data into custom information fields	90
Exporting and importing custom information field definitions	92
Exporting custom information field definitions	92
Importing custom information field definitions	92
Manually edited information	93
Using client information fields.....	93
Editing client information fields.....	93
Displaying the contents of client information fields	95
Naming client information fields	95
Configuring local access to client information fields	96
Storing and exporting information	97
XML, HTML, and text export.....	98
ODBC export.....	98
Preparing for ODBC export	98
Setting up ODBC export	99
Configuring database backup and maintenance.....	100
Deleting information from the server.....	102
Deleting entire records	102
Deleting associated data for a record	102
Displaying information	103
Opening and configuring browser windows	103
Opening a new browser window.....	103
Configuring the sidebar.....	103
Configuring a browser window	104
Saving configured browser windows.....	104
Working with tabs	104
Adding a tab to a window	104
Renaming a tab	105
Closing tabs	105
Displaying an overview of a single computer.....	105
Configuring the individual computer display	106
Controlling information display from a URL	106
Setting up Google Chrome to support lanrevadmin:// URLs	108
Searching, filtering, and sorting	109
Searching in browser windows	109

Creating groups.....	109
Creating a (standard) group.....	110
Creating a smart group	111
Creating smart groups, alternate technique.....	111
Editing groups.....	112
Deleting groups	112
Saving group definitions.....	112
Transferring groups	112
Exporting groups.....	113
Sorting browser windows	113
Sorting by a column	113
Reversing the sort order	113
Removing sorting.....	114
5 Controlling computers	115
Sending messages	115
Restarting, shutting down, and sleep.....	116
Restarting, shutting down, and putting to sleep	117
Waking up computers.....	118
Scheduling power management events.....	118
Setting up a new schedule.....	118
Assigning existing schedules.....	120
Deleting a schedule	120
Saving schedules	120
Displaying a power usage report.....	120
Remotely controlling computers	122
Supported applications	122
Setting up remote control	122
Initiating remote control.....	124
Launching a remote control session from a URL.....	124
Controlling Time Machine.....	125
Tracking computers	125
Setting up computer tracking.....	126
Starting to track a computer	128
Stopping the tracking of a computer.....	128
Getting information on tracked computers	129
Executing files from your computer	129
Script.....	130
Macintosh application	131
Windows application.....	132
Executing local files.....	132
Terminating processes	133
Working with services.....	134
Stopping a service	135
Starting or restarting a service.....	135
Setting a service's startup status	135
Editing the registry	136
Environment variables	137
Using environment variables.....	137
File-related variables defined by Absolute Manage	137
Registry-related variables defined by Absolute Manage	138
6 Working with mobile devices	140
Sending a message to mobile devices	140
Locking and unlocking mobile devices	141
Erasing mobile devices.....	143
Creating configuration profiles containing variables	143
Defining a variable.....	144
Using variables in configuration profiles.....	145
Installing configuration profiles on mobile devices.....	145

Importing a configuration profile into Absolute Manage	146
Manually installing a configuration profile	147
Failed installations.....	148
Manually removing a configuration profile	148
Installing a configuration profile via a policy.....	149
Making a configuration profile available for optional installation	150
Removing a configuration profile via a policy	151
Conflicting policy settings for configuration profiles	152
Windows Phone and multiple profiles	153
Installing provisioning profiles on iOS devices.....	153
Manually installing a provisioning profile.....	153
Failed installations.....	154
Manually removing a provisioning profile	154
Configuring roaming on mobile devices	155
Preparing iOS devices for software installation	155
Downloading AbsoluteApps from the App Store	156
Installing software on mobile devices	157
Preparing iOS application files.....	158
Importing an application into Absolute Manage.....	159
Making applications available on mobile devices	161
Making apps available via policies.....	161
Making apps available via direct installation.....	162
Uninstalling applications from mobile devices	163
Uninstalling applications from iOS 4 devices	164
Distributing App Store or Google Play (Android Market) apps to mobile users	165
Recommending third-party apps	165
Making volume purchase codes available	167
Deleting codes.....	168
Distributing media to mobile devices	169
Supported media types.....	169
Importing a media file	170
Importing folders of media files	172
Distributing a media file	173
Working with actions	174
Creating a new action	174
Re-executing actions.....	175
Reviewing actions	176
Deleting actions	176
Working with policies	176
Creating a policy.....	177
Adding and removing mobile devices	178
Specifying actions in policies	179
Adding actions to a policy	179
Changing delay or repetition settings.....	180
Removing actions from a policy	180
Specifying applications in policies	181
Specifying configuration profiles in policies	181
Adding a profile	181
Removing a profile	182
Conflicting profile assignments in multiple policies	182
Specifying media in policies	182
Geotracking mobile devices.....	182
Setting passphrases for mobile devices.....	183
Setting a passphrase individually	183
Setting one passphrase for a group of devices	184
Resetting a passphrase.....	185
Enabling geotracking on mobile devices	185
Dealing with lost passphrases	187
Displaying geotracking information	188

Displaying locations numerically	188
Displaying locations on a map.....	188
Naming Android devices	188
7 Working with files	190
Copying and moving files	190
Deleting files	192
Renaming files.....	192
Opening files on administered computers	193
Viewing files from administered computers.....	193
Creating shortcuts for files	195
Creating folders	196
Transferring files to administered computers.....	197
An alternative method of specifying files	199
8 Installing software	200
Creating installer packages	200
Installing software manually	200
Monitoring installed software	201
Overview	201
Prerequisites	201
Structure	201
Setup.....	202
Setting up distribution points.....	202
Distribution point basics	203
Choosing a server as a distribution point.....	203
Specifying the distribution point in the Software Distribution Center.....	204
Editing distribution points	206
Changing the master distribution point.....	206
Removing distribution points	208
Setting up payloads	209
Editing payloads.....	210
Removing payloads.....	210
Setting up software packages	211
Setting options for Adobe CS3 and CS 4	219
Editing software packages	219
Removing software packages	220
Setting up metapackages	220
Editing metapackages.....	227
Removing metapackages.....	227
Setting up computer groups.....	227
Setting up standard computer groups	228
Setting up smart computer groups	229
Editing computer groups	231
Removing computer groups	232
Performing installations	232
Installation process	232
Performing ad hoc installations	233
Automated patch management.....	235
Overview.....	235
Process	235
Finding missing patches	236
Deactivating patch management	236
Reinstalling a Mac OS X computer.....	237
Using a previously specified disk image	241
Reinstalling a Windows computer.....	241
Preparing a disk image using the Absolute server	242
Preparing a disk image using FOG	244
Reinstalling Windows client computers.....	246

9 Monitoring licenses	248
Overview	248
Prerequisites.....	248
Setup.....	248
Prohibited software.....	249
Setting up license specifications	249
Editing license specifications.....	253
Deleting reports	253
Tracking purchasing information.....	254
Entering new purchasing information	254
Editing purchasing information.....	255
Deleting purchasing information	255
Setting up computer groups	256
Configuring agents	256
Configuring agents.....	257
Configuring intervals.....	258
Checking licenses	259
Automatic and manual scans.....	260
Scan results	260
Reports	260
Understanding predefined reports.....	261
Creating custom reports	262
Editing reports	263
Deleting reports	263

Part 3: Reference..... **264**

10 File menu	265
New	265
New Tab.....	265
Open.....	266
Close.....	266
Rename Tab.....	266
Close Tab	266
Save	267
Save As	267
Command window.....	267
Text file.....	268
Export	268
Export Groups.....	269
Import Groups	269
Import Custom Field Data for Desktop Devices	269
Import Custom Field Data for Mobile Devices	271
Print	271
Print Preview.....	271
Print Setup.....	272
Recent Files submenu	272
Exit.....	272
11 Edit menu	273
Undo	273
Cut	273
Copy	273
Paste	273
Delete	274
Select All.....	274
Switch Administrator and Server	274

Change Administrator Password	275
Settings	275
General.....	276
Deployment Center.....	277
Remote Control.....	279
Power Consumption.....	280
12 View menu	281
Toolbar	281
Status Bar	281
Details	281
Select Container.....	281
Configure Columns.....	282
Display All Records.....	282
13 Commands menu	283
Commands menu for desktop computers	283
Commands menu for mobile devices	284
Favorites	284
Command window toolbar	284
Execute	284
Options	285
Targets	286
Save Template.....	287
Show Help.....	287
Agent Settings	287
General.....	288
Servers.....	289
Main list	290
Software Distribution Server	291
License Monitoring Server.....	291
Client Information.....	292
Custom Fields	293
Power Management Settings	293
Send Message	296
Change Operating State	296
Wake Up.....	297
Terminate Process.....	298
Reinstall Mac OS X Computer.....	298
Disk Image	299
Message	301
Reinstall Windows Computer.....	301
Disk Image	302
Message	303
Change Services Operation State	303
Time Machine.....	304
Search Windows Registry	305
Edit Windows Registry	306
Execute Script	307
Execute Macintosh File	309
Executable	310
Message	312
Execute Windows File.....	312
Executable	313
Message	314
Install Software Packages.....	314
Transfer File/Folder	315
Transfer	316
Permissions.....	317

Message	318
Copy File/Folder	318
Create Shortcut	321
Create Folder	322
Delete File/Folder.....	323
Find File	323
Move File/Folder	325
Open File	325
Executable	326
Message	326
Rename File/Folder.....	327
View Text File.....	327
Gather Process Information.....	328
Gather Inventory Information.....	328
Gather Installed Software	329
Gather Compliance Report	331
Run Software Distribution Check.....	332
Run License Monitoring Scan.....	332
Execute Command	332
Command Options	332
Execute Command Now.....	333
Edit Command.....	333
Reapply Command	333
Show/Hide Target List	334
Install Configuration Profile.....	334
Install Provisioning Profile.....	335
Install Application.....	335
Issue Device Lock.....	336
Issue Clear Passcode.....	337
Issue Remote Erase	338
Set Roaming Options.....	338
Send Message to Device.....	339
Update Device Info	339
Track Device.....	339
Get Device Geolocation	341
Reset Tracking Passphrase	341
14 Server menu	342
Synchronize All Tables.....	342
Reload All Tables.....	342
Synchronize Selected Records	343
Reload Selected Records.....	343
Save Distribution and Licensing Info	343
Read Distribution and Licensing Info	343
Save Administrator Info	344
Read Administrator Info	344
Save Custom Information Fields.....	344
Restore Custom Information Fields.....	344
Synchronize Custom Information Fields	344
Save Server Settings.....	345
Restore Server Settings.....	345
Synchronize Server Settings	345
Save All Settings	345
Restore All Settings	345
Create Placeholder Computer Records	346
Change Server Registration.....	347

15 Window menu	349
Cascade.....	349
Tile Horizontally	349
Tile Vertically.....	350
Computers.....	350
Files.....	350
Fonts	350
Processes.....	350
Installed Software	351
Groups	351
Context menu commands.....	352
Missing Operating System Patches	353
Predefined smart groups	353
Context menu	353
Further information	354
Registry Entries	354
Predefined smart groups	354
Context menu	354
Further information	354
Compliance Reports	355
Predefined smart groups	355
Context menu	355
Further information	355
Power Usage Reports.....	355
Predefined smart groups	355
Context menu	356
Main window area	356
Further information	358
Mobile Devices.....	358
Server Center	358
Agent Deployment Center	359
Commands.....	359
Command Templates	360
Context menu	360
Window Reinstallation Tasks.....	361
Context menu	361
Information Items.....	362
Context menu	362
User windows	362
16 Help menu	363
Help Topics	363
Show Release Notes	363
Absolute Manage Support.....	363
Absolute Manage Web Site	363
Acknowledgements.....	363
About Absolute Manage Admin	363
17 Browser windows	365
Toolbar	366
Status bar	366
Table columns	366
Column sidebar	367
Sidebar	367
Categories.....	367
Smart groups	367
Details.....	368
Sidebar context menu	368

New Group	368
New Smart Group.....	369
New Category.....	369
Rename Group.....	370
Rename Category.....	370
Edit Smart Group	370
Remove Group.....	370
Remove Category	371
Remove from Group	371
Table context menu	371
Copy.....	372
Copy "<information item>"	372
New Smart Group from "<information item>"	372
Make Group from Selected Computers.....	372
Show Detail View	373
Synchronize Records	373
Enter Custom Field Data	373
Remove from Server	374
Remove Inventory Data.....	374
Computer Tracking.....	374
Remove from Group	375
Remote Control	375
View in Separate Window	376
Open in External Viewer.....	377
18 Compliance Report window	378
Toolbar	378
Information panel.....	379
Table columns.....	379
Sidebar.....	379
Context menus	380
Copy.....	380
Copy "<information item>"	380
Show Details for This Computer.....	381
Show Details for This Scoring Item	381
New Smart Report Summary Group	381
New Smart Report Item Summary Group	382
New Smart Report Details Group	382
New Category.....	383
Rename Group.....	383
Rename Category.....	383
Edit Smart Group	384
Remove Smart Group	384
Remove Category	384
19 Mobile Devices	385
Toolbar	388
Table columns.....	388
Sidebar.....	389
Built-in.....	389
Assignable Items	389
Policies.....	390
Commands	391
Sidebar context menu.....	391
Mobile Applications	393
New In-house Application Package.....	393
New iOS App Store Application Package.....	394

Application Info tab	395
Volume Purchase Codes tab	396
New Google Play Application Package	397
Duplicate Application Package.....	398
New Smart Group: In-house Application Packages	398
New Smart Group: App Store Application Packages	398
New Smart Group: iOS Provisioning Profiles	398
New Smart Group: Installed Applications.....	398
New Smart Group: Installed Application Statistics.....	399
New Smart Group: Mobile Devices by Installed Software	399
New Smart Group: Installed iOS Provisioning Profiles	399
New Smart Group: Installed iOS Provisioning Profiles Statistics	399
New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles.....	399
Configuration Profiles and Certificates	400
New Configuration Profile	400
New Smart Group: Configuration Profiles	401
New Smart Group: Installed Configuration Profiles.....	401
New Smart Group: Installed Configuration Profiles Statistics	401
New Smart Group: Mobile Devices by Installed Configuration Profiles	402
New Smart Group: Installed Certificates.....	402
New Smart Group: Installed Certificates Statistics	402
New Smart Group: Mobile Devices by Installed Certificates	402
Media	402
New Media File	403
Duplicate Media File.....	404
New Smart Group: Media Files	405
Actions	405
New Send Message to Device Action.....	405
New Send E-mail Action.....	407
New Send SMS (Text Message) Action	409
New Set Roaming Options Action.....	410
New Update Device Info Action	411
New Freeze Device Action	412
New Remove Configuration Profile Action	413
New Demote to Unmanaged Device Action	413
Duplicate Action	414
New Smart Group: Actions.....	414
Policies	414
New Policy.....	415
New Smart Policy: Mobile Devices	415
New Smart Policy: Mobile Devices by Installed Applications.....	415
New Smart Policy: Mobile Devices by Installed Configuration Profiles.....	415
New Group: Mobile Devices	415
New Smart Group: Mobile Devices.....	416
New Smart Group: Command Queue	416
New Smart Group: Command History	416
New Category	416
Rename <item>	416
Edit <item>	416
Remove <item>	416
Table context menu	417
Copy	418
Copy "<information item>"	418
New Smart Mobile Device Group from "<information item>"	419
New Smart Policy from "<information item>"	419

New Smart Application Group from "<information item>"	419
New Smart Configuration Profiles Group from "<information item>"	420
New Smart Provisioning Profiles Group from "<information item>"	420
New Smart Media Files Group from "<information item>"	420
New Command Queue Smart Group from "<information item>"	421
New Command History Smart Group from "<information item>"	421
New Policy with Selected Devices	421
Install Configuration Profile.....	422
Install Provisioning Profile.....	422
Install Application.....	422
Issue Device Lock.....	422
Issue Clear Passcode.....	422
Issue Remote Erase	422
Set Roaming Options.....	422
Send Message to Device.....	422
Set Device Name.....	423
Delete Application	423
Delete Profile.....	423
Update Device Info	424
Show Detail View	424
Synchronize Records	424
Enter Custom Field Data	424
Import Custom Field Data	424
Ignore Devices.....	425
Reset All Ignored Devices	425
Re-execute All Actions for This Device	425
Re-execute This Action for This Device	425
Retry All Failed Profiles.....	425
Remove from Group	426
Remove from Policy.....	426
Track Device.....	426
Get Device Geolocation.....	426
Reset Tracking Passphrase	426
Show Location on Google Maps.....	426
Show Location on Bing Maps.....	426
Set Device Ownership.....	427
Send Re-enrollment Message to Device	427
Update Installed Application Statistics	428
Show Mobile Application Package Details	428
New Mobile Application Package	428
New iOS App Store Application Package	428
New Google Play Application Package	428
Edit Mobile Application Package	428
Duplicate Mobile Application Package	428
Remove Mobile Application Package	429
Show Configuration Profile Details	429
New Configuration Profile.....	429
Edit Configuration Profile	429
Remove Configuration Profile	429
Remove Configuration Profile from Policy	429
Show Provisioning Profile Details	429
Show Media File Details.....	430
Set Availability Time.....	430
New Media File.....	431
Edit Media File	431

Remove Media File.....	431
Show Action Details	431
Duplicate Action	431
Edit Action	432
Remove Action	432
Re-execute This Action for All Devices.....	432
Re-execute This Action for This Policy.....	432
New Send Message Action.....	432
New Send E-mail Action.....	432
New Send SMS (Text Message) Action	432
New Set Roaming Options Action.....	433
New Update Device Info Action	433
New Freeze Device Action	433
New Remove Configuration Profile Action	433
New Demote to Unmanaged Device Action	433
Change Action Schedule	433
Remove Action from Policy	434
Show Policy Members	434
Remove Policy	434
20 Server Center	435
Toolbar	436
Category bar.....	437
Status bar	437
Table columns	437
Sidebar	437
Software Distribution	438
License Monitoring	440
Computer Groups	440
Administration.....	441
Custom Information Fields.....	441
Server	442
Context menus.....	442
Software Distribution.....	443
New Software Package	443
Package	444
Installation Options	446
User Interaction	448
Installation Conditions.....	451
Adobe CS Options.....	451
New Metapackage	453
Metapackage.....	454
Installation Options	455
User Interaction	458
Installation Conditions.....	460
Duplicate Software Package.....	461
New Smart Software Package Group	461
New Payload.....	462
Duplicate Payload	463
New Smart Payload Group	464
New Distribution Point	464
New Smart Distribution Points Group	466
New Disk Image.....	467
New Smart Disk Image Group	468
New Smart Installation Status Group	469
New Missing Software Packages Group	469
License Monitoring.....	470

New License Specification	470
License.....	471
Conditions.....	474
Purchase Tracking.....	474
Purchase	475
Vendor.....	475
Maintenance.....	476
Notes.....	476
New Smart License Specification Group.....	476
New License Status Report.....	477
New Software Usage Report.....	477
New History Report.....	478
New History Summary Report	478
New Missing Software Report	478
Computer Groups	478
New Computer Group	478
New Smart Computer Group.....	479
Remove All Group Members	480
Administrator Setup.....	480
New Administrator.....	481
Remove Administrator from Group.....	484
New Administrator Group.....	484
New Computer Appointment Group.....	485
New Smart Computer Appointment Group	485
New Mobile Devices Appointment Group	486
New Smart Mobile Devices Appointment Group	487
New Smart Administrator Group	488
Refresh	488
Custom Information Fields	489
New Custom Information Field.....	489
Duplicate Custom Information Field	493
Export Selected Fields	493
Import Fields.....	494
Edit <item>	494
Remove <item>.....	494
Retrieve Payloads	495
Retry Package.....	495
Reset Package	495
Install Selected Software Packages.....	496
Repeat Selected Installations	496
Reset Current Server Load	496
Server Settings	497
General.....	497
Server Properties dialog.....	499
Client Info Titles	500
License Monitoring	501
ODBC Connection.....	502
Active Directory	503
MDM.....	504
FOG.....	507
Server Monitor.....	508
21 Agent Deployment Center	510
Toolbar	511
Table columns.....	511
Sidebar.....	512
Sidebar context menu.....	512

New Custom Zone	512
Zone	513
Auto Deployment	514
Server Properties dialog	516
Edit Custom Zone	516
Remove Custom Zone	516
Search Zone	517
Cancel Search	517
Refresh	517
New Smart Group	517
Edit Smart Group	518
Remove Smart Group	518
Import Zones File	518
Table context menu	519
Copy	519
Copy “<information item>”	520
New Smart Group from “<information item>”	520
Install Agent	520
Remove Agent	522
Set Inventory Server	523
Inventory Server Properties dialog	525
Refresh Status	526
22 Commands window	527
Toolbar	527
Table columns	528
Sidebar	528
Context menus	528
Copy	529
Copy “<information item>”	529
New Smart Command Queue Group from “<information item>”	529
New Smart Command History Group from “<information item>”	530
New Smart Command Queue Group	530
New Smart Command History Group	531
Edit Smart Group	531
Remove Smart Group	532
Scheduling Options	532
Execute Command Now	532
Edit Command	532
Reapply Command	532
Remove Command	533
Show Command Result	533
23 Information items	534
Agent Information	534
General	534
Agent Settings	535
Servers	535
Client Information	536
Ungrouped fields	536
Custom Fields	537
Hardware Information	538
System Information	538
CPU Information	538
Battery Information	540
Power Management	541
Power Management Schedules	543
Ungrouped fields	543

Memory Slots	547
Volumes	547
ATA Devices	548
SCSI Devices.....	549
FireWire Devices.....	550
USB Devices	550
PCI Devices.....	551
Displays.....	552
Software Information	553
System Information.....	553
Network Adapters	560
Fonts	561
Printers.....	561
Startup Items	562
Windows Services	562
Installed Software	563
Missing OS Patches	564
Processes.....	565
Files.....	566
Registry Entries.....	569
Computer Tracking	569
Commands	570
Commands.....	570
Command Queue.....	571
Command History.....	571
Server Center	571
Administration	572
Administrators.....	572
Appointments	574
Active Directory Users.....	575
Software Distribution	575
Packages	575
Payloads.....	579
Distribution Points.....	579
Disk Images	580
Installation Status	581
License Monitoring	581
License Specification	581
Purchase Tracking.....	582
License Status	583
License History	584
License History Summary	584
License Status per Agent.....	584
Computer Groups	585
Agent Deployment Center.....	585
Installed Software Statistics	586
Missing OS Patches Statistics	587
Compliance Reports	587
Reports.....	588
Computer Summary.....	588
Item Summary	588
Score Items.....	589
Mobile Device Information	589
Device Information.....	590
Device User Information	598
Installed Applications	599
Installed Configuration Profiles	600
Installed Provisioning Profiles	601
Installed Certificates	601

Installed Application Statistics	602
Installed Configuration Profile Statistics	602
Installed Provisioning Profile Statistics.....	603
Installed Certificate Statistics.....	603
Device Tracking	603
Custom Fields	605
Mobile Application Packages.....	605
Application Packages.....	606
App Store Volume Purchase Codes	607
Mobile Configuration Profile Definitions	608
iOS Provisioning Profile Definitions.....	609
Mobile Media	609
Mobile Actions	610
Mobile Device Policies	611
Device Commands.....	611
EAS Policies	611
Windows Reinstallation Tasks	615
FOG Reinstallation Tasks.....	616
AM Reinstallation Tasks	617
24 Absolute Remote	620
Connection	620
New.....	620
Open	620
Recent Connections.....	621
Close	621
Save As	621
Edit	621
Send Clipboard.....	621
Get Clipboard	621
Settings	622
View	623
Full-Screen Mode	624
Auto-Scrolling	624
Double Size	624
Original Size	624
Half Size	624
Quarter Size	624
Fit to Window	624
Session.....	624
Automatic Clipboard Transfer	625
Don't Limit Color Depth	625
Limit Color to 16 Bit	625
Limit Color to 8 Bit	625
Observe Remote Computer.....	625
Control Remote Computer.....	625
Command.....	625
Window	625
Cascade	626
Help.....	626
About	626
25 Absolute Manage Agent	627
Absolute Manage Agent control panel	627
General.....	627
Client Information.....	628
Software Updates	628
26 Mobile Apps	630
AbsoluteApps	630
AbsoluteApps for iOS.....	630

Applications	631
Updates	631
App Store.....	631
Messages	632
More	632
Profiles	632
About	632
AbsoluteApps for Android	632
Applications	633
Updates	634
Google Play	634
Messages	634
Profiles	634
About	634
AbsoluteSafe	634
Home screen	635
Media display screen	636
Favorites screen.....	637
Updates screen.....	637
Downloads screen	637
Settings screen	638
Index	639

Part 1: Getting Started

The Getting Started part of the manual contains the information you need to get Absolute Manage running:

“Introduction” on page 2 describes the structure and basic concepts of Absolute Manage.

“Installation” on page 11 guides you through the installation of all Absolute Manage components.

Welcome to Absolute Manage, the comprehensive management solution for network administrators.

The following text explains the scope and concepts of Absolute Manage and the different parts of the Absolute Manage system. If you want to get your feet wet right away, you can turn to “Installation” on page 11; however, starting with this section will make it easier for you to set up Absolute Manage in the way best suited to your requirements and to quickly employ it for maximum benefit.

For an overview of Absolute Manage, see:

- “What does Absolute Manage do?” on page 2
- “The Absolute Manage system” on page 2
 - “Elements of the Absolute Manage system” on page 3
 - “How commands work” on page 3
 - “Absolute Manage users” on page 9

What does Absolute Manage do?

Absolute Manage helps you manage the computers and mobile devices in your company:

- Collect a wide range of technical information on the devices for overview reports or in-depths analyses of individual devices.
- Control computers, terminating troublesome processes, executing utility scripts, restarting computers, and much more.
- Manage the configuration and security of mobile devices.
- Automate software installations by just specifying the software that is to be installed on each computer or in a workgroup and letting Absolute Manage do the rest. You can even reinstall the operating system or control the distribution of vendors’ operating system patches.
- Distribute in-house software to mobile devices.
- Configure mobile device settings.
- Locate mobile devices.
- Monitor software installations and usage, to always make sure that you stay within license limits (both installation-based and concurrent use licenses) and to know just what your licensing needs are.

And Absolute Manage does all this without you having to leave your desk at all.

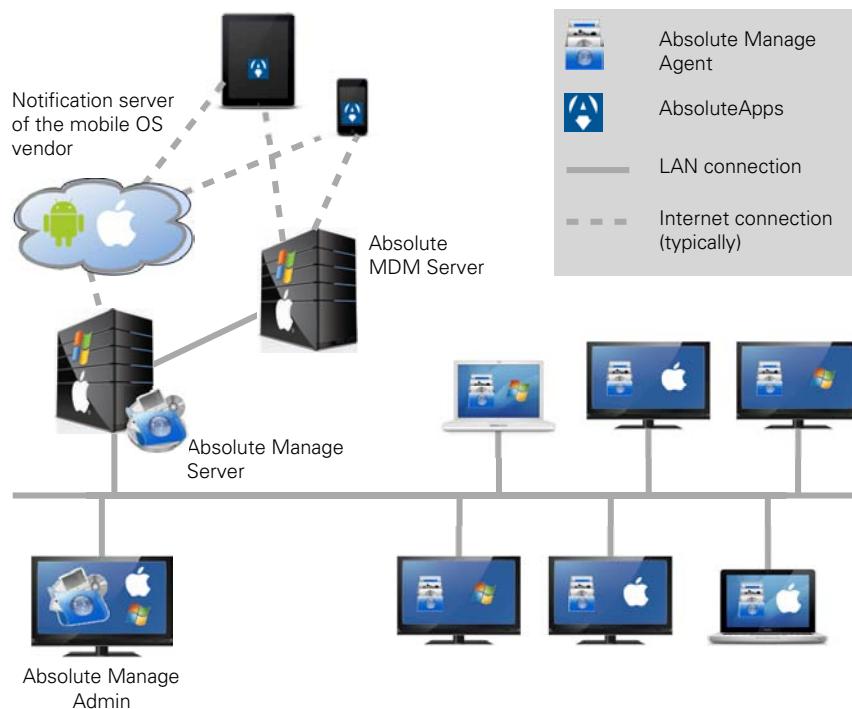
The Absolute Manage system

The Absolute Manage system consists of several different elements that are installed on the computers in the network. There are also different groups of users, as described below.

Elements of the Absolute Manage system

There are several components in the Absolute Manage system:

- An agent is installed on each managed device. Agents receive commands from Absolute Manage and carry them out on the local computer, sending back information when required. There is a minimal local interface to specify some information.
- A central server acts as the hub of the system: On instructions from you, it sends out commands to the agents, collects the information they send back, and stores it in its database. There is usually one server per managed network; multiple servers are possible. Servers have no user interface of their own; they are managed by the admin application. Absolute Manage effortlessly handles hierarchies of servers and specialized servers for, e.g., software distribution.
- An optional MDM server handles the management of mobile devices. It is tightly coupled to the main Absolute Manage Server and controlled from the same admin application.
- The admin application is your command center for the system. You use it both to control the server and – via the server – the agents, and to display the required information. The admin application can be installed on as many computers as desired.

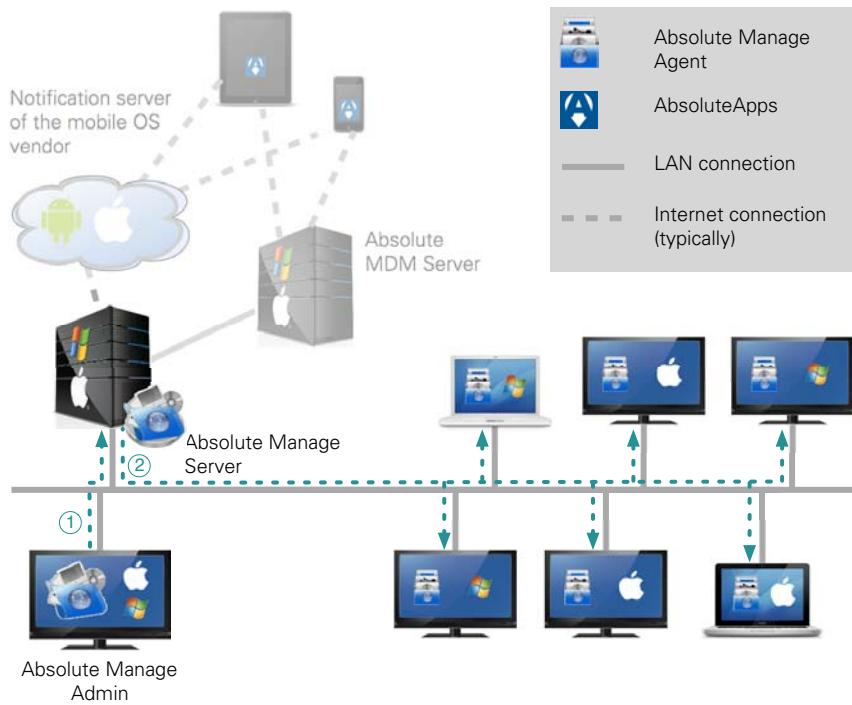


Multiple components can be installed on the same computer.

How commands work

The basic principle of working with Absolute Manage is the same for all commands (except for a software distribution and license monitoring,

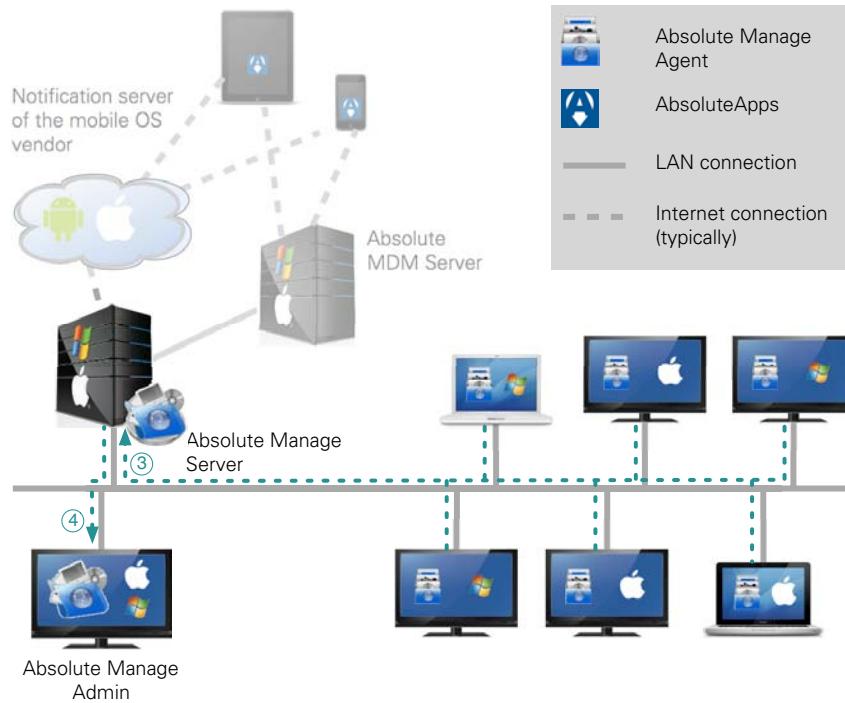
which are described separately in “Installing software” on page 200 and “Monitoring licenses” on page 248, respectively.)



When you issue a command to the Absolute Manage system, the command is transmitted from your admin application to the server (1).

The server checks whether it needs additional information from the agents to complete the command or whether the command involves any agent actions. If neither is the case, the server does not contact the agents.

If, however, the agents need to be involved, the server sends them the appropriate commands (2). Commands may be sent to one, some, or all agents, depending on the command specification from the admin.



The contacted agents perform the appropriate tasks on their computers or collect requested information. They send back the results to the server (3) – either information on the client computer or at least feedback that the set task has been completed.

Any information on the client computers returned by the agents is stored by the server in its database for future reference.

If the original command (1) from the administrator requires the return of information, the server sends the requested information back to the admin (4), processing it first if required.

How software distribution and license monitoring work

Software distribution and license monitoring work in the same basic way described above, in that the admin communicates with the server and the server with the agents.

However, instead of sending commands to the server that are then forwarded to the agents, the admin merely sets up the server as required. Later on, the agents communicate on their own with the server, sending information and, in the case of software distribution, requesting software that is available for them.

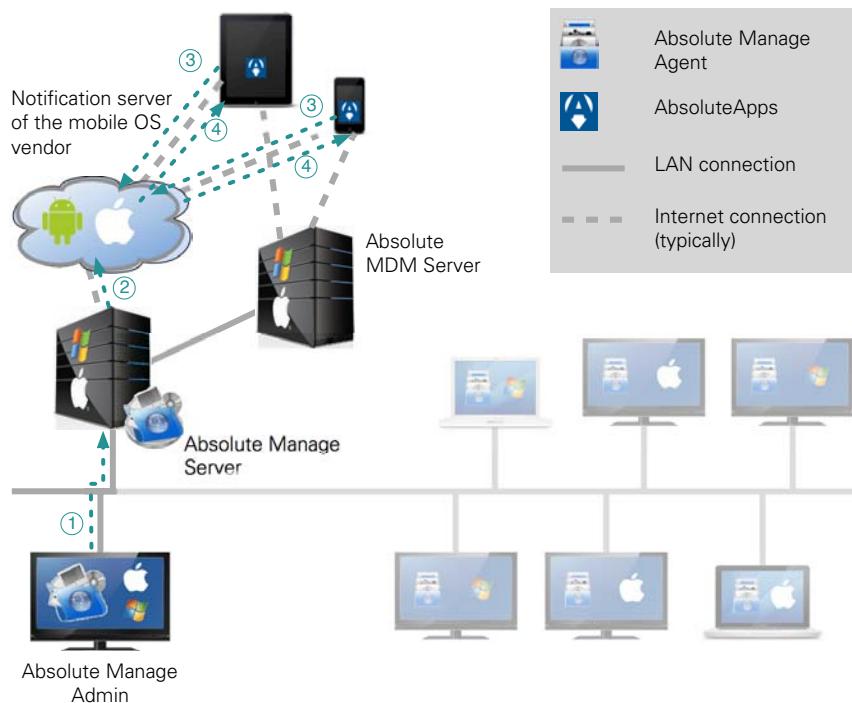
The admin is not involved in these exchanges beyond the initial setup and – if desired – the review of reports and logs.

An explanation of the principles and details of software distribution and license monitoring is available in “Installing software” on page 200 and “Monitoring licenses” on page 248, respectively.

How managing mobile devices works

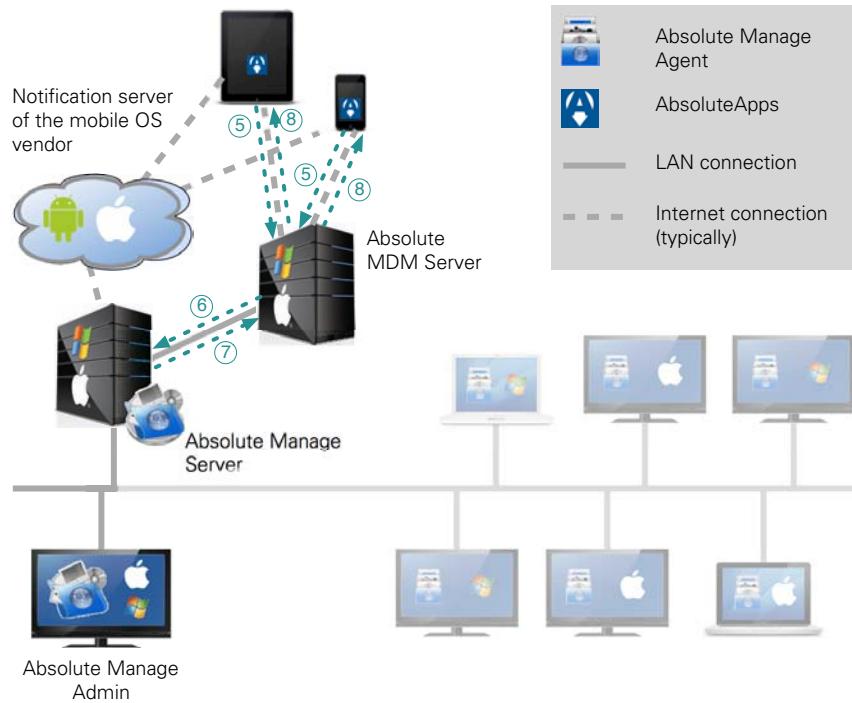
Mobile devices are managed in a similar way as desktop computers. However, there are some differences:

- The Absolute Manage Server cannot contact the mobile devices directly. Instead, contact must be made through a notification server operated by the mobile OS vendor (Apple, Google or Microsoft) and an MDM server. The process for iOS and Android is described below; the one for Windows Phone differs slightly, as described in “Windows Phone” on page 8.

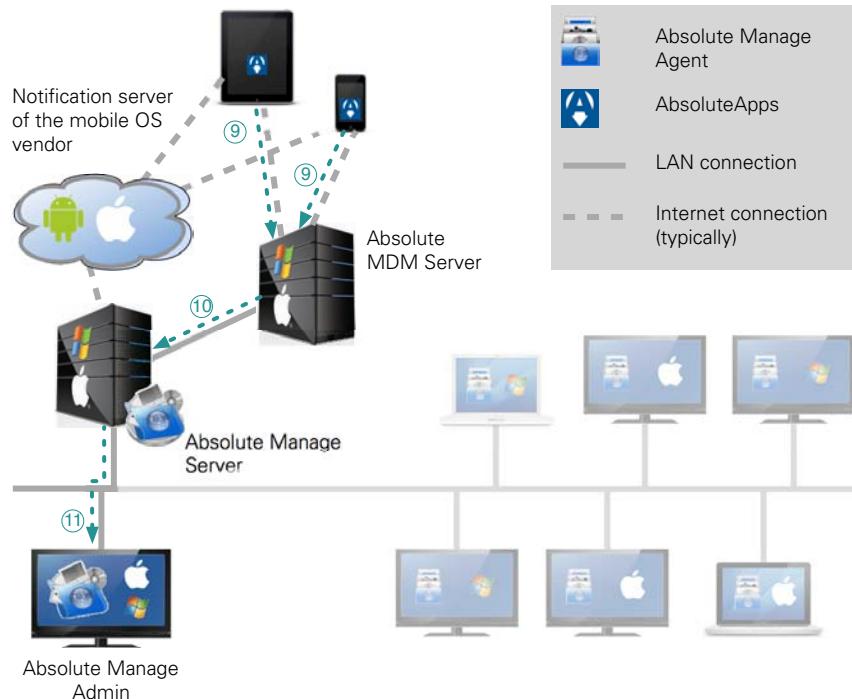


When an admin issues a command that involves mobile devices, it is first sent to Absolute Manage Server(1). If that server determines that the commands require contacting mobile devices, it sends a contact request to OS vendor’s notification server (2), which is regularly contacted by the mobile devices. When a device for which a request is pending next contacts the notification server (3), the contact request is

forwarded to the Absolute Manage client (AbsoluteApps) running on the device (4).



The mobile device contacts the MDM server (5), which forwards the contact notice to the Absolute Manage Server (6). The Absolute Manage Server sends the command required to execute the original admin request (1) to the MDM server (7), which forwards it to the mobile device (8).



If the request requires a response by the device (e.g., returning device status information), the response is sent to the MDM server (9), which forwards it to Absolute Manage Server (10). When the data has arrived on that server, the admin can retrieve it (11).

Windows Phone

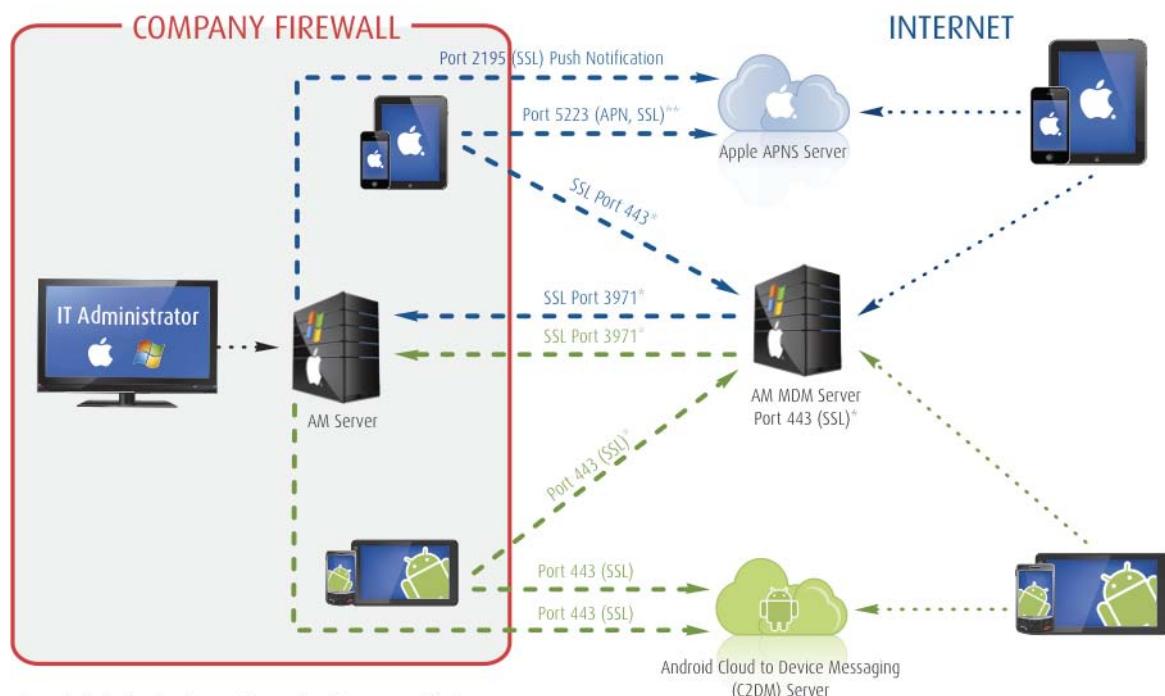
The process for contacting managed Windows Phone devices is largely similar to the process described above, with these differences:

- Instead of a central notification server run by Microsoft, Absolute Manage Server contacts the Exchange server to which the phone is synchronized.
- Except during the initial enrollment process, the Absolute Manage MDM server is bypassed. Instead, the mobile device communicates with the Exchange server, which in turn communicates with Absolute Manage Server.

Ports used

A number of different ports are used in this process:

MDM CONNECTIONS



This is an overview of the ports involved:

- Absolute Manage Server
 - 3971* (also for connections to the administrator application and to local Agents, not shown)
 - 8443* (Mac OS X server only)

- Absolute Manage MDM Server
 - 443*
- Apple push notification server
 - 2195
 - 5223 via ports 80 and 443
- Android cloud-to-device messaging server
 - 443: SSL

An asterisk (*) indicates ports that can be reassigned.

Absolute Manage users

Absolute Manage is used by two groups of people in very different ways:

- ‘Normal’ users – users of the administered devices – have no or very little interaction with Absolute Manage.
- Administrators are the persons who actively use the system to manage remote devices.

Users

Absolute Manage is transparent for users of administered devices. Neither is Absolute Manage activity noticeable for them – except sometimes by its effects, such as new software being available on the device – nor is their active cooperation required for any of Absolute Manage’s actions.

There are some exceptions to this:

- At the discretion of the administrator, users can be notified of some pending actions, such as restarts, that may affect their work. Furthermore, the administrator may give users the option to cancel these actions.
- Users may be given the option to view or edit certain bits of information (so-called client information) locally.
- Apps and media can be made available to users of managed mobile devices to be installed or viewed at their leisure. (Apps can also be installed without requiring any user action.)

Administrators

Administrators use the Absolute Manage Admin application to manage client devices via the Absolute Manage system.

Administrator access requires a password-protected account on the Absolute Manage Server. This ensures both that Absolute Manage cannot be used by unauthorized persons and that an administrator has the same use of Absolute Manage no matter from where he or she accesses the system.

As a general rule, administrators do not have access to all client devices – they can manage only devices to which they have expressly been assigned in the Absolute Manage system. (It is possible to configure individual administrator accounts so that they have access to all devices.)

There are two types of administrators:

- Standard administrators can perform any action that Absolute Manage permits on the client devices to which they have been assigned. Optionally, their access to the assigned devices can be restricted to a specific list of functions.
- Superadministrators have access to all the same functions as standard administrators. In addition, they can create, configure, and delete administrator accounts and assign administrators to computers.

Details of managing administrator accounts are described in “Administrator accounts” on page 48.

Chapter 2 Installation

This chapter describes installing, updating, and uninstalling the components of the Absolute Manage system.

For information on updating from earlier versions, see “Updating Absolute Manage” on page 42.

Overview

Absolute Manage should always be installed in the same order:

1. Server: First the Absolute Manage Server is installed; it is the central element of the Absolute Manage system without which it does not work.
2. Admin: Next, Absolute Manage Admin is installed on at least one administrator workstation. As soon as it is installed, it is used to perform the initial configuration of the server, including entering the authorization code.
3. Agents: Finally, the Absolute Manage Agents are installed. In many cases, this installation can be performed automatically using the Absolute Manage system.

The installation procedures for all components are described below in this order.

Before you install

Before you begin the installation, some preparation is helpful:

1. Check the system requirements (listed below).
2. Decide on a suitable server computer. Some relevant issues are discussed in “Choosing a computer for Absolute Manage Server,” below the system requirements.
3. Decide whether to use the provided Absolute Manage Agent installer or create a custom installer with preconfigured preferences.
4. Decide whether to use Absolute Manage’s Agent Deployment Center to install Absolute Manage Agent centrally on the administered computers.

There must be suitable user accounts for remote installations:

- Mac OS X clients: SSH must be enabled and there must be an account for which you know the password.

- Windows clients: There must be an administrator account for which you know the password.

Note: Installation becomes even easier if the same account name and password can be used on all computers running the same operating system.

System requirements

System requirements for desktop software components:

Component	Mac OS X	Windows
Absolute Manage Server	Mac OS X 10.5.0 or newer	Windows XP SP 2 or newer (Windows XP SP 2, Vista, 7, Server 2003, or Server 2008)
Support for remotely reinstalling Windows computers	An Absolute Manage PXE server or a FOG server in your network. FOG is open-source software running on Linux. The Absolute Manage PXE server has the same requirements as Absolute Manage Server. For the FOG server requirements, see www.fogproject.org . If FOG is used, an ODBC driver capable of connecting to the FOG MySQL server must be installed on the computer on which Absolute Manage Server is running. Any Windows system on which Absolute Manage Server is installed must include .NET 3.5.	
MDM server for managing mobile devices	A computer that can be reached from the Internet by HTTP and HTTPS connections. (This can be a computer on which Absolute Manage Server is running or a separate computer.) An SSL certificate for the computer on which you will be installing the MDM server. The certificate cannot be self-signed. (See step 1 of “Preparation” on page 24 for details.)	Mac OS X 10.5.0 or newer. Property List Editor utility. (This utility is part of the Mac OS X developer software.)
		Windows Server 2003 or 2008 Microsoft Internet Information Services (IIS) 6.0 or newer. The WebDAV Publishing role must not be installed. ASP.NET 2.0 .NET 3.5
MDM for iOS devices (in addition to the general MDM requirements above)	Apple’s iPhone Configuration Utility. This utility is available (for Windows and Mac OS X) from Apple’s support web page.	

Component	Mac OS X	Windows
MDM for Windows Phone devices (in addition to the general MDM requirements above)	(Not available: Windows Phone MDM requires a Windows installation of Absolute Manage Server.)	Exchange Server 2007 or Exchange Server 2010 PowerShell 2.0 or newer
Absolute Manage Admin	Mac OS X 10.5.0 or newer Mac with an Intel processor Screen with a resolution of at least 1024 by 768 pixels For distributing Android apps, a Java runtime (JRE) is required.	Windows XP SP 2 or newer (Windows XP SP 2, Vista, 7, Server 2003, or Server 2008) Screen with a resolution of at least 1024 by 768 pixels For distributing Android apps, a Java runtime (JRE) is required.
InstallEase	Mac OS X 10.4 or newer Xcode 3.2.5 or newer (only for PKG support) Iceberg 1.2.2 or newer (only for Iceberg project support)	Windows XP or newer Microsoft .NET 3.5 SP 1
Absolute Manage Agent	Mac OS X 10.3.9 or newer (Agent 4.0.4 for Mac OS X 10.2 or newer and Agent 4.5.1 for Mac OS X 10.3 or newer; with reduced functionality)	Windows XP or newer (Windows XP, Vista, 7, Server 2003, or Server 2008)

System requirements for mobile components:

Component	iOS	Android	Windows Phone
AbsoluteApps	iOS 4.0 or newer	Android 2.2 or newer	(not available)
AbsoluteFind	iOS 4.0 or newer	(not available)	(not available)
AbsoluteSafe	iOS 4.0 or newer	(not available)	(not available)

All Absolute Manage components also require a working IP network connection. The built-in firewalls of Mac OS X and Windows are fully supported.

Windows and Mac OS X components can be freely mixed between the platforms; e.g., an admin running on Windows can control a server running on Mac OS X to work with agents running on Windows.

Choosing a computer for Absolute Manage Server

Absolute Manage Server does not technically have special requirements beyond the system requirements listed above. However,

some aspects should be considered when choosing a computer on which to install Absolute Manage Server:

- Dedicated server: To maximize operational reliability of the Absolute Manage system, it is helpful to install the server application on a computer that is not used as a workstation (i.e., worked on by a local user).
- Network bandwidth: When Absolute Manage is used to administer a large number of computers, there may be substantial network traffic from and to the server at peak times. In such cases, it is helpful to have as much bandwidth as possible, e.g., by providing a high-bandwidth link to the switch.
- Processor power and disk space: Absolute Manage Server has no special requirements regarding processor power or disk space. Any modern computer should more than suffice. Note, though, that database operations require processor power in proportion to the number of administered computers. Also, the more administrators are active at the same time, the more processor power is required.
- Other server processes: Other server processes running on the same computer as Absolute Manage Server are not normally a problem. However, if they put a strain on resources – in particular processor power and network bandwidth – they may impair the performance of Absolute Manage.

Installing Absolute Manage Server

For the system requirements of Absolute Manage Server, see “System requirements” on page 12.

Installing Absolute Manage Server on Mac OS X

To install Absolute Manage Server on a Mac OS X computer:

1. Copy the Absolute Manage Server installation package to the hard disk of the computer on which you want to install the server.
2. Open the installation package and follow the on-screen instructions.

There is no need to restart the server computer after the installation.

Installing Absolute Manage Server on Windows

To install Absolute Manage Server on a Windows computer:

1. Copy the Absolute Manage Server installation folder to the hard disk of the computer on which you want to install the server.
2. Open the folder and double-click the **Setup** application
3. Follow the on-screen instructions.

After the installation

When you are done installing the server, you should immediately install Absolute Manage Admin and configure the server.

NOTE When you are transferring a server from computer to another (as opposed to setting up a server for the first time), you can import the settings from the existing server, as described in “Exporting and importing server settings” on page 66.

After installing the admin, you can optionally install two additional components:

- Support for remotely reinstalling Windows computers, as described in “Installing support for reinstalling Windows computers” on page 20.
- Support for managing mobile devices (iOS or Android), as described in “Installing MDM support” on page 24.

Installing Absolute Manage Admin

For the system requirements of Absolute Manage Admin, see “System requirements” on page 12.

After you have installed it, you should immediately launch it to authorize and configure Absolute Manage Server.

Installing Absolute Manage Admin on Mac OS X

Copy the Absolute Manage Admin application file to a suitable place on your hard disk (e.g., the **Applications** folder).

If you are planning on managing application packages for Android mobile devices, a Java runtime environment (JRE) is required. Version of Mac OS X up until 10.6.x include an JRE, but newer versions, starting with 10.7 (Lion), do not. At the time of this writing, Apple provides a JRE for installation on Lion at <http://support.apple.com/downloads/#Java>.

NOTE You can also install Absolute Manage Admin on a USB stick to take with you for mobile diagnoses. The application is fully functional when so installed; the only limitation is that it reverts to default **Preferences** dialog settings and window positions when used on a different computer.

Installing Absolute Manage Admin on Windows

To install Absolute Manage Admin on a Windows computer:

1. Copy the Absolute Manage Admin installation folder to the hard disk of your computer.

2. Open the folder and double-click the **Setup** application
3. Follow the on-screen instructions.

Initial configuration of Absolute Manage Server

After you have installed the first copy of Absolute Manage Admin, you should start it immediately to configure the server. (Additional copies of Absolute Manage Admin that you install can simply log in when the server has been configured and accounts been set up.)

This process involves specifying the Absolute Manage Server and then entering registration and initial setup information in a setup wizard:

1. Start Absolute Manage Admin. The **Login** dialog opens:



2. Enter the server address – you can enter the IP number or a DNS name if the server computer has one. The port number should not normally be changed; however, if you have configured the server to use a different port number, enter that number.

Do not enter a name or password.

3. Click **Login**.

You are asked to verify the server identity. For security reasons, Absolute Manage uses SSL certificates to identify all components. When you contact a server for the first time, Absolute Manage Admin asks you to verify that the certificate that it presents indeed belongs to the server you want to contact (instead of, e.g., a malicious server used for a man-in-the-middle attack).

4. Display the server certificate as described in “Displaying a server’s certificate” on page 18.
5. If the fingerprint of the certificate and the unique server identifier match the information in the Absolute Manage Admin’s verification dialog, click **Connect**.

The Absolute Manage Setup wizard opens.

6. Start with entering your and your company's names as well as the serial number and activation key that you have received with your copy of Absolute Manage.

Note: You can run Absolute Manage as a demo by clicking the demo button. In this case, you are limited to ten clients and the software will stop working after 45 days.

7. Specify the ports that the server is to use for communicating with agents and with Absolute Manage Admin.

You can use the same ports for both agents and Absolute Manage Admin. Different ports are recommended when you place an Absolute Manage Server in a demilitarized zone for access from the Internet, as explained in "Setting up computer tracking" on page 126

Absolute Manage Server opens the specified ports in the built-in Mac OS X or Windows firewall on its computer if the firewall is active.

Note: We recommend that you change the ports only when you have a specific need to do so.

8. If you do not want to create administrator accounts on this server but instead want to use existing accounts on another Absolute Manage Server, check **Use administrator accounts from server** and specify the desired server.

Note: If you use accounts from another server, you will not be prompted to create an initial account as described below.

Click the **Set** button to open the SSL certificate for the specified server. (See "Exporting a server certificate" on page 19 for information on creating a certificate file.)

9. Create an initial superadministrator account for yourself.

Note: Details of creating accounts are described in "Administrator accounts" on page 48.

When you finish the wizard, it sets up the server as specified and launches Absolute Manage Admin, opening an empty browser window. Both Absolute Manage Server and Absolute Manage Admin are now installed.

Continue the installation process:

- If you want Absolute Manage to be able to remotely reinstall Windows computers, continue with "Installing support for reinstalling Windows computers," below.
- If support for reinstalling Windows clients is not required but you want to use Absolute Manage to administer mobile devices, continue with "Installing MDM support," below.

- If neither of these capabilities is required, continue with installing Absolute Manage Agent on all computers that are to be administered, as described in “Installing Absolute Manage Agent” on page 29.

Displaying a server’s certificate

To ensure that it communicates only with the intended server, Absolute Manage Admin uses SSL certificates.

When it contacts a server for the first time or when the server’s certificate has changed (for example, after the server was reinstalled), you must verify that the presented certificate does indeed belong to the server it claims to identify.

To verify a certificate, you compare the fingerprint and server unique identifier that Absolute Manage displays with the corresponding values you obtain from the server:

1. The procedure normally begins with Absolute Manage displaying a verification dialog.

Leave the dialog open on the admin workstation.

2. Go to the server computer.

While it is possible to obtain the server certificate information remotely, doing so is less secure than physically accessing the server computer.

3. Depending on the platform, execute a command line instruction:

- On a Mac OS X server, launch the Terminal application and enter this command (on a single line):
"/Library/Application Support/LANrev Server/LANrev Server.app/Contents/MacOS/LANrev Server"
–ShowCertificateFingerprint
- On a Windows server, launch the Command Prompt application and enter this command (on a single line):
"C:\Program Files\Pole Position Software\LANrevServer\LANrev Server.exe" –ShowCertificateFingerprint
(On x64 systems, use "C:\Program Files (x86)\..." instead.)

Note: If you use –ShowCertificate instead of –ShowCertificateFingerprint, additional information is displayed, including the server’s unique identifier. However, this is usually not needed, as the identifier is also part of the certificate and thus covered by the fingerprint verification.

The certificate fingerprint is displayed.

4. Copy or write down the fingerprint and return to the admin workstation.
5. Compare the fingerprint you obtained from the server with the fingerprint displayed by Absolute Manage Admin:

- If the two fingerprints do not match, the server to which Absolute Manage Admin is about to connect is not the server from which you obtained the fingerprint. Make sure that the server address Absolute Manage Admin uses is correct. If the address is correct, there may be an attempt to compromise your Absolute Manage installation by having another server masquerade as your server.
Do not continue the connection! Doing so could severely compromise the security of your network.
- If the two fingerprints match, click the **Connect** button in the verification dialog.

Exporting a server certificate

For security reasons, the individual components of Absolute Manage (servers, administrator applications, and agents) require SSL certificates to verify the identities of other components with which they communicate.

This means that you must specify a certificate for any server that you assign to an agent (e.g., as an inventory server). You can do so either by exporting a certificate from Absolute Manage Admin or by copying the certificate file from the server computer. Both methods are described below.

Exporting a certificate in Absolute Manage Admin

To create the required certificate for a server:

1. Make sure that your admin application is connected to the desired server.

Connecting to a different server is described in “Switching accounts” on page 53.

1. In Absolute Manage Admin, choose **Window > Server Center**.

The **Server Center** window opens.

2. Click the **Server Settings** entry in the sidebar and click the **Save Certificate** button in the lower left of the window.

A standard Save dialog opens.

3. Save the server certificate in a convenient location. You can give it any desired name.

Use this file whenever you are required to provide a certificate for a server that you want to assign to agents.

Copying a certificate from the server computer

After Absolute Manage Server has been launched for the first time (which happens as part of the installation), it saves a copy of its certificate in its application support folder:

- Mac OS X: /Library/Application Support/LANrev Server/Server Certificate.pem
- Windows XP or Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\Server Certificate.pem
- Windows Vista, Windows Server 2008, or Windows 7: C:\ProgramData\Pole Position Software\LANrev Server\Server Certificate.pem

Copy the certificate file from this location to the computer where it is needed.

Installing support for reinstalling Windows computers

Support for remotely reinstalling Windows computers from Absolute Manage Admin requires the installation of additional components.

NOTE Remote reinstallation of Mac OS X computers is supported out-of-the-box by Absolute Manage. If you need to be able to remotely reinstall Mac OS X computers but not Windows computers, you can skip this procedure.

Absolute Manage offers two ways for supporting reinstalling Windows computers: With the included solution for a Windows PXE server by Absolute, or with the popular FOG Linux server solution.

Both are described below in:

- “Setting up the Absolute solution” on page 20
- “Setting up the FOG solution” on page 22

Setting up the Absolute solution

To set up the Absolute support for reinstalling Windows computers:

1. Set up your Absolute Manage servers for software distribution, as described in “Setting up distribution points” on page 202.
2. In Absolute Manage Admin, choose **Window > Server Center** to open the Server Center.
3. Right-click in the sidebar and choose **Software Distribution > New Disk Image** from the context menu to upload the boot disk image.

In the **Disk Image** dialog that opens, specify:

- **Disk image name:** AMWinPE
- **Disk image file:** Click **Select** and choose the AMWinPE.iso file provided by Absolute.
- **Disk image password:** not applicable
- **Distribution point:** Choose the desired option. If you are unsure, choose **Any**.

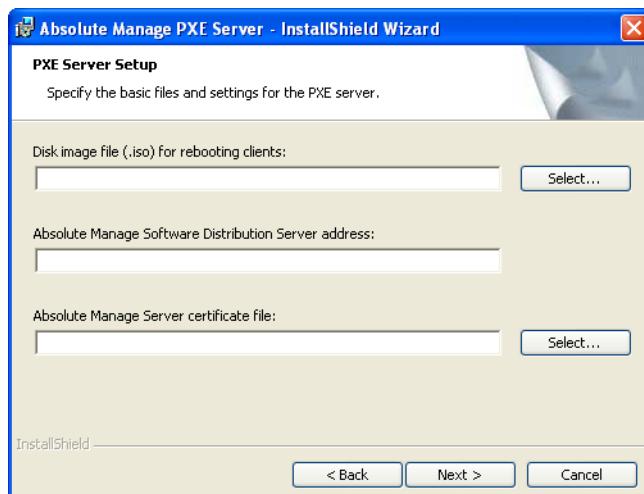
Click **OK** to upload the image.

4. Export the Absolute Manage Server certificate, as described in "Exporting a server certificate" on page 19.
5. Launch the PXE server installer.

This installer is included on the Absolute Manage disk in the "Absolute PC Imaging PXE Server".

Note that the PXE server must not be installed on the computer that is used as the DHCP server.

6. Follow the instructions on screen until you reach the setup screen:



7. Specify this information:

- **Disk image file:** The AMWinPE.iso disk image provided by Absolute. You can download this image from the Resource Center.
Note: This image is (in certain circumstances) required to boot a Windows computer that is about to be reinstalled and is not used as the source for the new installation on the computer. (You specify a different disk image in the Reinstall Windows Computer command dialog.) Do not modify the contents of this image.
- **Absolute Manage Software Distribution Server address:** The IP address or fully qualified DNS name of the Absolute Manage Server in your network on which the disk image is located.
- **Absolute Manage Server certificate file:** The certificate file you have exported in step 4.

8. Click **Next** and continue to follow the on-screen instructions.
9. Configure the DHCP server to allow network booting from the PXE server. (The following instructions apply to a Windows Server 2003 Enterprise Edition; adapt them as necessary for other servers.)

- Open the DHCP server console.
 - Display the scope options.
 - Right-click anywhere in the list of options and choose **Configure Options** from the context menu.
 - Set option “066 Boot Server Host Name” to the IP address of the PXE server you have installed in the previous steps.
 - Set option “067 Bootfile Name” to “pxelinux.0” (without the quotes).
 - Save the changed options and close the server console.
10. Make sure that the client Windows computers are not set to boot from the network.

Absolute Manage now supports remotely reinstalling Windows computers.

Continue the installation process:

- If you want to use Absolute Manage to administer mobile devices, continue with “Installing MDM support”, below.
- Otherwise, continue with installing Absolute Manage Agent on all computers that are to be administered, as described in “Installing Absolute Manage Agent” on page 29.

Setting up the FOG solution

To set up the FOG support for reinstalling Windows computers:

1. Install the FOG server and configure it.

For details, see the FOG documentation. The FOG software and documentation is available from www.fogproject.org.

In particular:

- Configure the FOG server to have a static IP address.
- Configure DHCP to use FOG.

2. Configure MySQL for network access.

For details, see the FOG documentation and MySQL documentation for your platform, as required.

3. If you have installed Absolute Manage Server on a Windows computer, install .NET 3.5, if it is not already present.

Skip this step when you have installed Absolute Manage Server on Mac OS X. Also, you do not need to upgrade any computers running Absolute Manage Admin (but not Server) to .NET 3.5.

4. Make sure that, on the Absolute Manage Server computer, an ODBC driver capable of accessing the MySQL database used by FOG is installed.

If no such driver is present, install it.

Setting Absolute Manage Server up for FOG support

Reinstalling Windows computers requires a one-time setup of Absolute Manage Server to allow it to control the FOG server:

1. In Absolute Manage Admin, open the Server Center, click **Server Settings**, and click the **FOG** tab:

The screenshot shows the 'Server Center' interface with the 'FOG' tab selected. The 'FOG' tab has two main sections: 'MySQL Database' and 'FOG Server'. The 'MySQL Database' section contains fields for 'FOG ODBC driver name', 'FOG MySQL database server address', 'FOG MySQL database name', 'FOG MySQL database username', 'FOG MySQL database password', and 'FOG MySQL database password verification'. The 'FOG Server' section contains fields for 'FOG server URL', 'FOG username', 'FOG password', and 'FOG password verification'.

2. Fill in the required information to access the MySQL database that FOG uses:
 - Enter the name of the ODBC driver on the Absolute Manage Server computer that Absolute Manage is to use to access the MySQL database in **FOG ODBC driver name**.
 - Enter the IP address or DNS name of the MySQL server in **FOG MySQL database server address**.
 - Enter the name of the MySQL database that FOG uses in **FOG MySQL database name**.
 - Enter your access credential for the MySQL database in **FOG MySQL database username**, in **FOG MySQL database password**, and **FOG MySQL database password verification**.
3. Fill in the required information to access the FOG server:
 - In **FOG server URL**, enter the IP address or DNS name of the FOG server and the path of the FOG server management directory, e.g., "http://myfogserver.company.com/fog/management/".
 - Enter your access credential for the MySQL database in **FOG username**, in **FOG password**, and **FOG password verification**.
4. Choose **Server > Save Server Settings**.

You have now configured Absolute Manage to allow reinstallation of administered Windows computers, as described in “Reinstalling a Windows computer” on page 241.

If there are already disk images on the FOG server, you can verify the correctness of the setup by choosing (in Absolute Manage Admin) **Commands > Reinstall Windows Computer**. If Absolute Manage can properly access the FOG server, the disk images are visible in the **Image** pop-up menu.

Absolute Manage now supports remotely reinstalling Windows computers.

Continue the installation process:

- If you want to use Absolute Manage to administer mobile devices, continue with “Installing MDM support”, below.
- Otherwise, continue with installing Absolute Manage Agent on all computers that are to be administered, as described in “Installing Absolute Manage Agent” on page 29.

Installing MDM support

Support for managing mobile devices from Absolute Manage requires the installation and configuration of an MDM (mobile device management) server.

The requirements for the MDM software are listed in “System requirements” on page 12.

There are three installation steps, with a fourth step required only if you plan to manage Windows Phone devices:

- Preparation
- Installing the MDM server
- Configuring the MDM server
- Configuring the Exchange server

Managing a mobile device also requires it to be enrolled in the MDM administration. This is described later in “Enrolling mobile devices” on page 39.

Preparation

1. Obtain an SSL/TLS certificate for the computer on which you will be installing the MDM server.

The certificate must come from a root certification authority (CA) or signed by a CA with authorization from a root CA. In the latter case, you also need the signer certificate of the CA.

The certificate must either be a wildcard certificate for the domain under which the computer on which the MDM server will be installed can be reached from the Internet (e.g., *.mycompany.com) or specific to the server’s DNS name.

2. Set up your firewall to allow connections from your Absolute Manage Server to the notification servers of Apple and Google, respectively:

- gateway.push.apple.com on port 2195 for iOS devices
- android.apis.google.com on port 443 for Android devices

If you do not manage a particular kind of device, you do not need to allow the corresponding connection. (For example, if you do not manage iOS devices, you do not need to allow connections to gateway.push.apple.com.)

Continue with “Installing the MDM server” below.

Installing the MDM server

The installation process differs slightly between Windows and Mac OS X. Both processes are described in separate sections below.

Installing the MDM server on Windows

1. From Absolute Manage Admin, export the certificate of the Absolute Manage Server, as described in “Exporting a server certificate” on page 19.
2. Run the Setup.exe application from the “Absolute MDM Server” folder.

You are guided through the installation.

3. When prompted for the website SSL certificate, choose the certificate described in step 1 of “Preparation”, above.
4. When prompted for the Absolute Manage Server certificate, use the certificate you exported in step 1.

As the DNS address, provide the fully qualified domain name, i.e., the name including the top-level domain. For example, use “mdm.mycompany.com” (instead of just “mdm”).

As explained in “Preparation”, above, this can be the computer on which Absolute Manage Server is running but does not have to be.

After you have installed the MDM server, continue with “Configuring the MDM server”, below.

Installing the MDM server on Mac OS X

1. Run the provided installer package.
2. By default, MDM communications use port 443. If you want to use a different port, edit the “server.port” entry in the /private/etc/lighttpd/lighttpd.conf file.

3. Copy the SSL certificate for the MDM server (see step 1 of “Preparation”) to /etc/lighttpd/certs on the MDM server computer and name it “lighttpd.pem”.

If you have received a certificate that does not contain the SSL private key (e.g., a certificate in .p12 format), you must convert it to include the key, as described in “Importing the SSL key into the certificate”, below.

4. From Absolute Manage Admin, export the certificate of the Absolute Manage Server, as described in “Exporting a server certificate” on page 19.
5. Copy this certificate to /etc/lighttpd/certs on the MDM server computer and name it “AMServerCertificate.pem”.

As explained in “Preparation”, above, this can be the computer on which Absolute Manage Server is running but does not have to be.

6. If the certificate was signed with an intermediate certificate (as opposed to a CA root certificate), append the content of the intermediate certificate to the content of your certificate.

You can do so, e.g., by executing the command
`cat IntermediateCA.pem >> AMServerCertificate.pem`
(This assumes that your intermediate certificate is named IntermediateCA.pem.)

7. On the computer on which the MDM server is installed, open the /Library/Preferences/com.absolute.mdm_server.plist file (using the Property List Editor utility) and enter in the AMServerHostname key the IP address or DNS name of the Absolute Manage Server.
8. On the computer on which the MDM server is installed, run the Start_MDM_Server.command shell script provided on the Absolute Manage installation disk.

This starts the MDM server.

Continue with “Configuring the MDM server”, below.

Importing the SSL key into the certificate

If you have received an SSL certificate that does not contain the SSL private key (e.g., a .p12 certificate), you must convert it. This procedure is not required if you already have a .pem certificate.

1. Import the certificate into the Mac OS X Keychain, e.g., by dragging it into the main window of Keychain.
2. Export the certificate and key to disk in Personal Information Exchange (.p12) format.

3. Convert the resulting file to Privacy Enhanced Mail (.pem) format using the ConvertSSLCertificate.command script provided in the Extras folder on the Absolute Manage installation image.

Configuring the MDM server

The MDM server is configured from Absolute Manage Admin. Configuration is required only for managing iOS devices, not for Android devices.

1. In Absolute Manage Admin, open the Server Center, display the server settings, and click the **MDM** tab.
2. Enter this information:
 - **Profile name:** A descriptive name for the deployment profile. This name will be displayed on iOS devices during the enrollment process.
 - **Profile identifier:** A unique identifier for the profile. It is needed to distinguish it from other profiles you may create on the server.
 - **Description:** A brief explanation of the profile's purpose. It is displayed on the iOS device in the first screen of the enrollment process.
 - **MDM server:** The full DNS name of the server on which you have installed the MDM server.
 - **Port:** The port over which the MDM server communicates. By default, this is 443, but if you have edited the server port in step 2 of "Installing the MDM server", you must specify the custom port here as well.
 - **Microsoft Exchange Server:** If you do not want to set up MDM for Windows Phone devices now, choose **None** and continue with step 3. Otherwise, choose the version of the Exchange server you have installed.
 - **Exchange server:** Enter the IP address or fully qualified DNS name of the Exchange server.
 - **Username:** Enter the username of an account on the Exchange server. Depending on the version of Exchange you are using, the account must have certain privileges. Exchange 2007 accounts must have all of these privileges:
 - View-only administrator
 - Recipient administrator
 - Organization administrator
 - Server administrator
 - Local administrator (for the Exchange server used)Exchange 2010 accounts must have all of these privileges:
 - Server management
 - Organization management
 - Recipient managementIrrespective of the Exchange version, the account you specify must be a member of the Admin group on the computer on which Absolute Manage Server is running.
 - **Password:** The password for the specified account.

3. Click the **Select** button at the upper right of the panel and let the assistant guide you through the creation of a new push notification certificate.

If you already have this certificate, the assistant lets you select it.

4. Choose **Server > Save Server Settings**.
5. Make sure to open the required ports in your firewall. (The following assumes that the MDM server is outside the firewall, as recommended.)

For outgoing connections:

- 443* (This port can be reassigned for contacting the MDM server but not for contacting the Android notification server.)
- 2195 (Not needed if you do not want to mange iOS devices.)
- 5223 (Not needed if you do not want to mange iOS devices.)

For incoming connections:

- 3971*

Functions marked with an asterisk can be reassigned to other ports. If you have done so, open the customized ports in your firewall instead. (Note that you always must open port 443 for outgoing connections if you want to manage Android devices.)

See “Ports used” on page 8 for more information on port usage.

If you plan on managing Windows Phone devices, continue with setting up the Exchange server as described below.

Otherwise, continue with installing Absolute Manage Agent on all computers that are to be administered as described in “Installing Absolute Manage Agent” on page 29.

Configuring the Exchange server

To allow Absolute Manage to administer Windows phone devices, additional setup steps are necessary:

1. If PowerShell 2.0 is not available on the computer on which Absolute Manage Server is running, install it.
2. When you are using Exchange 2007, install the Exchange 2007 Management Tools on the computer on which Absolute Manage Server is running.

If you are using Exchange 2007, you are now done with the setup and can skip to the end of the procedure.

3. If you are using Exchange 2010, continue with this procedure.
Enable access to the PowerShell virtual directory:
 - Open Server Manager for the Exchange server.
 - Click **Roles > Web Server > Internet Information Server**.
 - Click **Sites > Default Web Site**.
 - Click the virtual directory **PowerShell**.
 - Open the authentication settings and set **Windows Authentication** to **Enabled**.
4. Enable the Windows Remote Management (WinRM) service:
 - On the computer running the Exchange server, start PowerShell.
 - Enter `winrm quickconfig`.
 - Accept all proposed settings by pressing Y.
5. Export the SSL certificate of the Exchange server:
 - Open the IIS Manager on the computer on which the Exchange server is running.
 - Click the server's entry and click **Server Certificates**.
 - Open the view pane for the certificate you want to export, click **Details** and click **Copy to File**.
 - Follow the on-screen instructions to export the certificate to a file.
6. Add the Exchange server's SSL certificate to the Absolute Manage server:
 - On the computer running the Absolute Manage server, open the mmc.exe management console.
 - In the console, choose **File > Add/Remove Snap-in**.
 - In the **Add/Remove Snap-in** window, click **Add**.
 - Choose **Certificates** and click **Add**.
 - Choose **Computer Account** and click **Next**.
 - Choose **Local computer** and click **Finish**.
 - Close the **Add Standalone Snap-in** and **Add/Remove Snap-in** windows.
 - In the **Console Root** window, right-click **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** and choose **All Tasks > Import** from the context menu.
 - Follow the steps of the wizard to import the SSL certificate of the Exchange server.

Continue with installing Absolute Manage Agent on all computers that are to be administered as described below.

Installing Absolute Manage Agent

Absolute Manage Agent has the same system requirements as the other Absolute Manage components, as described in "System requirements" on page 12.

Installation method

There are three different methods of installing Absolute Manage Agent:

- Automatically, using the Agent Deployment Center. This is described in “Installing Absolute Manage Agent using the Agent Deployment Center” on page 33.
- For administered Windows computers: Automatically, using a login script. The details of setting this up depend on the specifics of your systems; providing them goes beyond the scope of this manual.
- Manually, executing the installer locally. This is described below. Note that manual installation requires the admin application to run on the same operating system platform as the agents. In other words, if you want to install agents on both Mac OS X and Windows, you need to also install Absolute Manage Admin on both platforms.

In most situations, the automatic methods will be preferable to the manual installation, particularly in cross-platform setups.

Installing Absolute Manage Agent manually on Mac OS X

Installing Absolute Manage Agent manually on a Mac OS X computer requires Absolute Manage Admin for Mac. For details, please see the documentation for Absolute Manage Admin for Mac.

Installing Absolute Manage Agent manually on Windows

To install Absolute Manage Agent manually on a Windows computer:

1. Make the Absolute Manage Agent installer available on the computer on which you want to install – on a server volume accessible from the computer, on a removable medium or by copying to the local hard disk.
2. Open the installation folder.
3. Launch the **Setup** application and follow the onscreen instructions.
4. If Bonjour (ZeroConf) is not installed on the PC, you are at one point asked whether you want to install it.

Bonjour enables the agent to automatically find Absolute Manage Server.

If you install it, you need to restart the computer manually before Bonjour becomes active.

5. If you have installed Bonjour, restart the computer.

A restart is strictly necessary only with Windows 2000, but we recommend that you restart other systems as well after having installed Bonjour.

If you did not install Bonjour, no restart is necessary.

6. Make sure that Windows File & Print Sharing is enabled on the client computer.
7. If you have not already done so, export the certificate for all servers you plan to assign to the agent, as described in “Exporting a server certificate” on page 19.
8. In Absolute Manage Admin on your administrator workstation, choose **Window > Agent Deployment Center**.

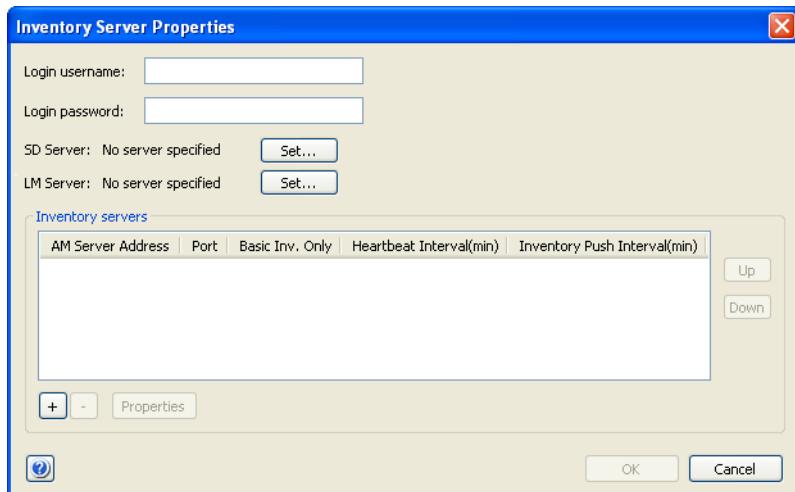
The Agent Deployment Center window opens.

9. Select the computer in which you have installed the agent.

You can select multiple computers together if there is a user account with the same name and password on each of them.

10. Right-click and choose **Set Inventory Server** from the context menu.

The Inventory Server Properties dialog is displayed.

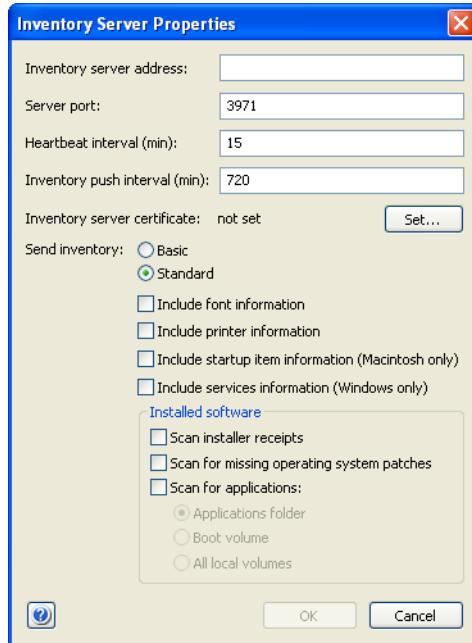


11. Enter the Windows File & Print Sharing username and password required to access the clients.

Note that this means that all selected clients must have Windows File & Print Sharing accounts with the same usernames and passwords. If not all of your clients have such similar accounts, select them in multiple groups, with the clients in each group having similar accounts.

12. If the server you want to assign is not present in the list, click the + button to add it.

13. The **Inventory Server Properties** dialog opens.



14. Enter the DNS name or IP address of your Absolute Admin Server in the **Inventory server address** field.

For most installations, you can leave the other settings at their defaults. More detailed considerations are found in “Assigning inventory servers to agents” on page 55. Recommended values for very large installations are provided in the separate Absolute Manage Optimization Guide.

15. If the **Inventory server certificate** field does not display “valid,” click the **Set** button to select the certificate for the server you are specifying.

Creating a certificate is described in “Exporting a server certificate” on page 19.

Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

16. Click **OK** to create the new server specification.
17. In the **Inventory servers** list, select all servers that you want to use to manage the selected agents.

Optionally, you can also assign software distribution and license monitoring servers at this time, but it is often more efficient to do so later, as described in “Assigning software distribution or license monitoring servers to agents” on page 57.

18. Click **OK** to close the dialog and assign the specified servers to the agents.

When the servers have been successfully assigned, the agent appears in the Computers window of any Absolute Manage Admin that is connected to one of these servers.

Installing Absolute Manage Agent using the Agent Deployment Center

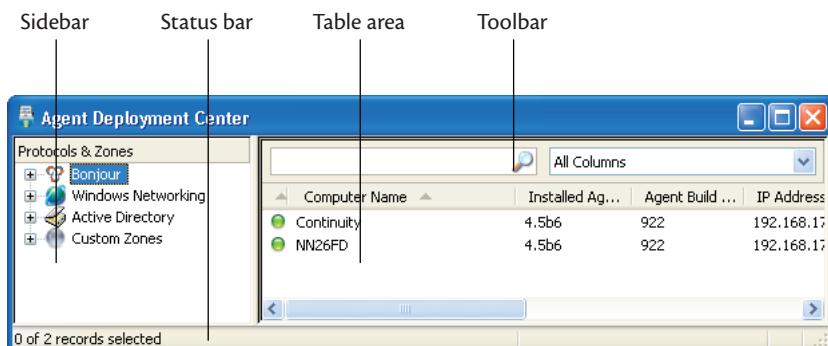
The Agent Deployment Center is an Absolute Manage Admin module that lets you install and update Absolute Manage Agent on computers in your network as well as review the currentness of installed agents.

NOTE Installing agents as described in this procedure is possible only for administrators with the Deploy Agents right. See “New Administrator” on page 481 for details.

The Agent Deployment Center can be used to install agents on computers using the same operating system platform (Mac OS X or Windows) as the administrator application. For agent deployment in mixed networks, you should therefore install at least one Absolute Manage Admin application on each platform.

NOTE In contrast to the other parts of Absolute Manage, the Agent Deployment Center does not work through Absolute Manage Server. Installations are performed directly from Absolute Manage Admin to the client computers; all settings are stored locally on the administrator workstation.

All its functions are controlled from the **Agent Deployment Center** window:



Prerequisites

Installing or updating Absolute Manage Agent via the Agent Deployment Center requires your administrator account to have the **Deploy Agents** permission. (Creating administrator accounts is described in “Administrator accounts” on page 48.)

In addition, every computer on which Absolute Manage Agent is to be installed must have Windows File & Print Sharing enabled and there must be an account that you can use (i.e., for which you know the password).

Overview

To install or update Absolute Manage Agent via the Agent Deployment Center, you perform these steps:

1. Create zones that list all relevant computers.
2. Select the computers on which you want to install or update Absolute Manage Agent, specify the access parameters, and install the agents.

These steps are described below in detail.

You can also specify that agents be installed on all found computers where they are not already present. This is also discussed below.

Creating zones in the Agent Deployment Center

The Agent Deployment Center contains predefined network zones:

- Under **Bonjour**, all Bonjour (ZeroConf) zones defined in your network are automatically listed. In Absolute Manage Admin for Windows, these zones are displayed only when you have installed Bonjour on your workstation.
- Under **Windows Networking** you find the domains and workgroups defined in your network and listed within them the computers.
- Under **Active Directory**, all Active Directory zones defined in your network are automatically listed. This entry is displayed only if there is an Active Directory server in your network.

If these zones do not list all computers that you want to administer or if you want to group the computers differently than they are grouped by the zones, you can define custom zones.

Custom zones are defined by IP address, IP address range, or by DNS name.

NOTE

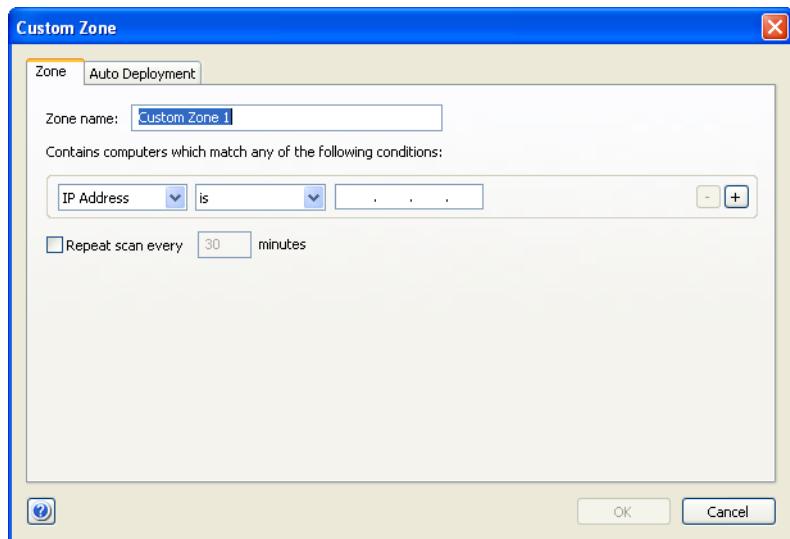
You can also import custom zone definitions from a text file, as described in “Import Zones File” on page 518.

To define a custom zone:

1. Right-click in the **Agent Deployment Center** and choose **New Custom Zone**.

The **Custom Zone** dialog opens.

2. Click the **Zone** tab:



3. Enter a descriptive name for the zone and use the pop-up menus to define conditions for computers that are to be included in the zone.

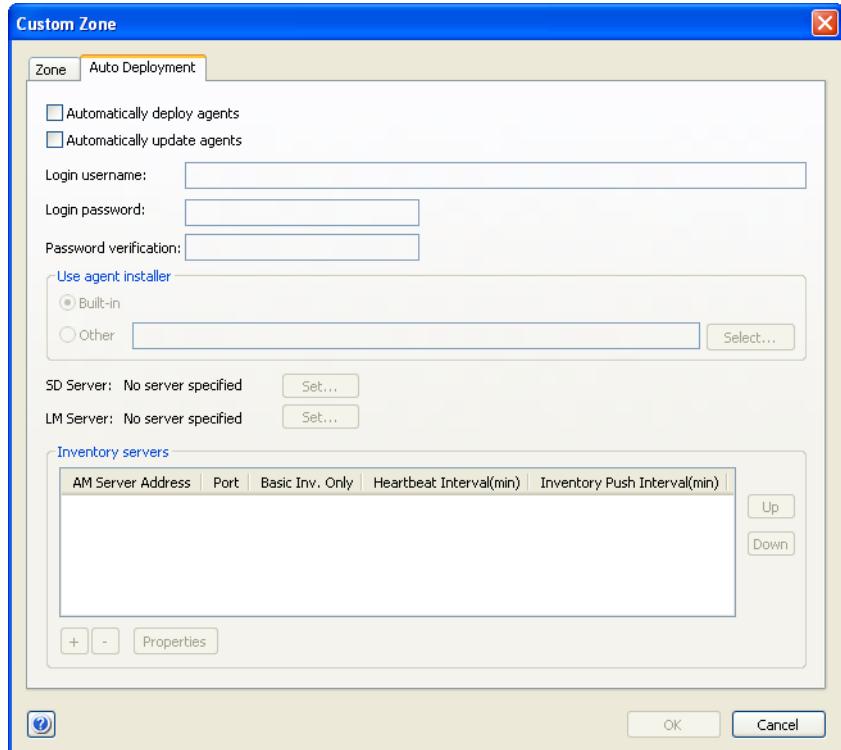
You can specify single IP addresses, ranges of IP addresses, and DNS names.

Using the **+** button, you can create additional conditions. The zone will include any computer that meets at least one of the specified conditions.

Use the **-** button to remove unwanted conditions.

4. If you want Absolute Manage to regularly scan the zone (which is useful with automatic deployment as described below), check **Repeat scan every** and enter the desired interval in minutes.
5. If you do not wish Absolute Manage to automatically install Absolute Manage Agents without further interaction with you, skip to step 7.

Otherwise, click the **Auto Deployment** tab:



6. Fill in the fields as described in step 12 through step 17 of **Installing Absolute Manage Admin on Windows**, above.
7. Click **OK** to create the zone.
8. To save the zone, choose **Save** from the **File** menu.

Saving the zone is optional; however, if you do not do so, it is not available when you next start Absolute Manage Admin.

The new zone appears in the sidebar in the **Custom Zones** section.

If you have specified automatic scanning, Absolute Manage scans the zone for computers. If you have also specified automatic deployment, Absolute Manage Agent will be installed on all computers on which it is not yet present. This requires the computers to have the same operating system as your administrator workstation – Absolute Manage Admin running on Windows can only automatically deploy Absolute Manage Agent for Windows and Absolute Manage Admin for Mac OS X can only deploy Absolute Manage Agent for Mac OS X.

If you have not set the zone for automatic scanning, you will now want to search the zone for devices, as described below.

Searching zones

To search a zone, choose **Search Zone** from the sidebar context menu.

Searching a zone usually takes up to about one second per specified IP address or DNS name.

NOTE

The exact time depends on the server connection timeout set in the **Settings** dialog (see “Settings” on page 275); each IP address where no device is found takes about a tenth of that time. IP addresses where devices are located are scanned much quicker.

You can cancel a search in progress by choosing **Cancel Search** from the zone’s context menu.

The found devices are listed in the table area of the **Agent Deployment Center** window. Colored dots in front of their names indicate their status:

- Green dot: Absolute Manage Agent is current.
- Yellow dot: Absolute Manage Agent is present but outdated.
- Red dot: No Absolute Manage Agent. Installing an agent is possible.
- Grey dot: No Absolute Manage Agent, and no agent can be installed. A common reason is that you are trying to install across platforms (i.e., from the Windows Admin to a Mac client or vice versa), which is not possible with the Agent Deployment Center. Other reasons include: The device is not a computer, or Window File and Printer Sharing is disabled on a Windows client.

On computers that have no agent (■) or an old version (○), you can install the current version, as described below.

If you have specified automatic deployment for the zone (see above), Absolute Manage automatically installs Absolute Manage Agent on all computers that have the same operating system as your administrator workstation and on which no Absolute Manage Agent is present.

Editing zones

To edit a custom zone, select it and choose **Edit Custom Zone** from the sidebar context menu.

Predefined zones cannot be edited.

Deleting zones

To delete a custom zone, select it and choose **Remove Custom Zone** from the sidebar context menu.

Predefined zones cannot be deleted.

Installing or updating Absolute Manage Agent

When the computers on which Absolute Manage Agent is to be installed are listed in the **Agent Deployment Center** window (see above), you can install the agent on them.

NOTE For information on setting a zone up for automatic deployment, see step 5 of the procedure in “**Creating zones in the Agent Deployment Center**” above.

To install or update Absolute Manage Agent:

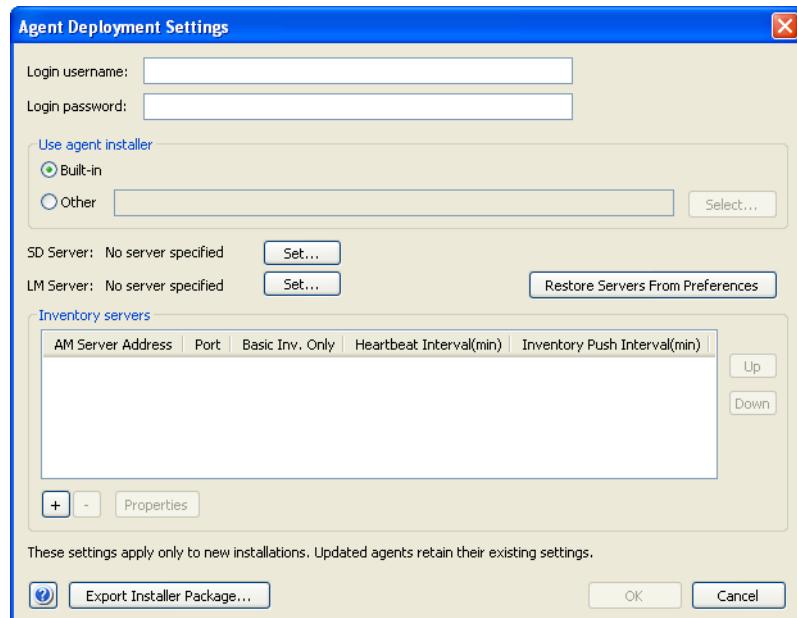
1. In the **Agent Deployment Center** window, select all computers on which you want to update or install the agent. You can select computers that require installations and ones that require updates at the same time.

Make sure to select only Windows computers; to install or update agents on Mac OS X computers, use a Mac OS X computers version of Absolute Manage Admin.

On all Windows computers that you select together, there must be an administrator account with the same name and password.

2. From the sidebar context menu, choose **Install Agent**.

The **Agent Deployment Settings** dialog opens:



3. Fill in the fields as described in step 12 through step 17 of **Installing Absolute Manage Admin on Windows**, above.

4. If you have prepared a custom installer package, click **Other** and then click **Select** to open it.

5. If you want to reuse the installer package for other Agent installations, click Export Installer Package to save the installer along with the specified server settings and required certificates.

You can reuse this package in this dialog by opening it as described in step 4.

6. Click **OK**.

Absolute Manage Admin now installs agents on the selected computers. The progress of the installation is displayed in the Agent Deployment Center's **Connection Status** column. Any errors that occur during an installation are logged in **Documents and Settings\<user>\Local Settings\Temp** (The **Local Settings** folder is normally hidden by the operating system; to view it, you must display hidden objects.)

If the built-in Windows firewall is active on a client computer, installing the agent automatically opens the agent port as specified in the *Settings* dialog (normally port 3970).

Enrolling mobile devices

Mobile devices (Android, iOS – including iPod touches and LAN-only iPads – and Windows Phone) can be administered by Absolute Manage. This requires an MDM (mobile device management) server, into which the devices must be enrolled. This process serves a similar purpose as installing an agent on a desktop computer, but is different in detail.

Only devices meeting the following system software requirements can be enrolled in MDM management:

- iOS 4.0 or newer
- Android 2.2 or newer
- Windows Phone

Enrolling iOS devices requires providing a special configuration profile on a web server and sending a link to this file to all devices you want to include in the mobile device management. This step is not required for enrolling Android devices.

There are two enrollment techniques, both of which are described below:

- Using the MDM server. This is automated to a larger degree and provides access to Active Directory and – if Absolute Manage Server runs on Mac OS X – Open Directory data. This approach requires you to have an Active Directory or Open Directory server, respectively, on which each mobile user has an account.

- Using your own server. This requires more effort on your part and does not provide access to Active Directory or Open Directory data for enrolled users (the Device User Information information item category). However, no Active Directory or Open Directory server is required.

NOTE

Irrespective of the technique used, Android users must enable the installation of content obtained from sources other than the Android Market (Google Play) to be able to complete the enrollment.

Enrollment using the MDM server

1. If you want to enroll Windows Phone devices, make sure that all devices that are to be enrolled are being synchronized via ActiveSync with the Exchange server that you have specified. (See “Configuring the MDM server” on page 27 for details.)
2. Send an e-mail to all users whose mobile devices are to be managed. Include the enrollment URL:
<https://<server address>/Profile/enrollment.mdm>

<server address> is the DNS name of your MDM server, e.g., mdm.mycompany.com.

Make sure to send the e-mail to addresses that these users read on the mobile devices – enrollment is not possible if the e-mail is accessed from another device, such as a desktop or portable computer.

3. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

They will need to enter their Active Directory or Open Directory (depending on which service you use) username and password in the process. If they also enter a domain, Absolute Manage will assume that the account is an Active Directory account; if they do not enter a domain and Absolute Manage Server runs on Mac OS X, the account is assumed to be an Open Directory account.

Android users will need to manually launch the downloaded file (AbsoluteApps.apk), which should be mentioned in the e-mail. If they have not done so before, they will also need to enable the installation of content from sources other than the Android Market (Google Play).

Each device on which users follow this procedure appears in the **Mobile Devices** window in Absolute Manage Admin. You can manage it there using the context menu commands.

For Windows Phone users, the above procedure automatically enrolls all devices linked to the specified Active Directory account.

Enrollment using a different web server

This technique cannot be used for Windows Phone devices.

1. Find the enrollment file. Depending on the target platform (iOS or Android), it is found in different locations:
 - For iOS devices, the file is named MDMEnrollment-Bootstrap.mobileconfig and is found on the Absolute Manage Server, with the exact location depending on the operating system of the server computer:
 - Windows XP or Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\
 - Windows Vista, Windows 7, or Windows Server 2008: C:\ProgramData\Pole Position Software\LANrev Server\
 - Mac OS X: /Library/Application Support/LANrev Server/
 - For Android devices, the enrollment file is the AbsoluteApps.apk app package, which is included with the Absolute Manage installers in the Android folder.
2. Make the enrollment file – MDMEnrollmentBootstrap.mobileconfig or AbsoluteApps.apk – available on a web server.

The file must be accessible with a standard http or https URL.

We recommend that you put it in an area of the web server that requires logging in or provides another form of access control.

3. If you are using an IIS server, use IIS Manager to add the enrollment file's MIME type to the server's **Properties** page:
 - The extension for the iOS file is "mobileconfig" and the file type is "application/x-apple-aspen-config".
 - The extension for the Android file is "apk" and the file type is "application/vnd.android.package-archive".
4. Send an e-mail with the URL of the enrollment file to all users whose mobile devices are to be managed.

Make sure to send the e-mail to addresses that these users read on the mobile devices – enrollment is not possible if the e-mail is accessed from another device, such as a desktop or portable computer.

5. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

Android users will need to manually launch the downloaded file (AbsoluteApps.apk), which should be mentioned in the e-mail. If they have not done so before, they will also need to enable the installation of content from sources other than the Android Market (Google Play).

Each device on which users follow this procedure appears in the **Mobile Devices** window in Absolute Manage Admin. You can manage it there using the context menu commands.

Updating Absolute Manage

When updating Absolute Manage, you should update all components simultaneously. Absolute Manage Server and Absolute Manage Admin must always be the same version, and while older versions of Absolute Manage Agent are supported in principle, some features will be unavailable.

See the installation sections for information on installing the update of Absolute Manage Server and Absolute Manage Admin:

- “Installing Absolute Manage Server” on page 14
- “Installing Absolute Manage Admin” on page 15
- “Installing Absolute Manage Agent” on page 29

Updating the Agent

If you are using the Software Distribution Center, you can use it to update agents extremely easily:

NOTE You must have set up the Software Distribution Center before beginning this procedure, and there must be at least one distribution point.

1. Update Absolute Manage Server and Absolute Manage Admin.
2. Start Absolute Manage Admin and open the **Server Center** window.

You find two automatically generated packages – **Absolute Manage Agent (Mac OS X)** and **Absolute Manage Agent (Windows)** – under **Software Distribution > Software Packages**.

Note: If you have just installed or updated Absolute Manage Server, these packages may take a few minutes to appear in the Software Distribution Center.

3. Drag the packages to the computer groups that contain the clients you wish to update. If you want to update all clients, doing which we highly recommend, drag them to **All Macs** and **All PCs**, respectively.

This updates the agents on all computers in the computer groups to which you have assigned the packages. Unless you later remove the packages from the groups, it also ensures that, in future, new version of Absolute Manage Agent are automatically distributed to these computers. (You are asked for permission first in each case.)

Updating the Software Distribution Center from Absolute Manage 1.x

When you have been using the Software Distribution Center in Absolute Manage 1.x, you must update the server and software package definitions, as described below.

NOTE These updates are not necessary when you have already been using Absolute Manage 2.0 or later.

Updating the Software Distribution Center

Because of a new architecture of the Software Distribution Center in Absolute Manage 2.0 and later, the definitions of distribution points and software packages need to be updated when you have been using version 1.x before. You may also want to consider the choice of computers as distribution points. These issues are described below.

Choosing distribution points

Under the new Software Distribution Center architecture, distribution points do no longer need to be file servers. This means that you can now choose computers on which you cannot or will not run file server software.

We do, however, still recommend that only server computers are used as distribution points, i.e., computers with no local users working on them.

Updating distribution points

To update an existing distribution point to be compatible with the new architecture:

1. Install Absolute Manage Agent on the distribution point, same as you would on any client computer. See “Installing Absolute Manage Agent” on page 29 for details.
2. If file server software on the computer was previously only used for distribution point purposes, you may want to disable it now.
3. In Absolute Manage Admin’s **Server Center** window, double-click the distribution point definition in the **Software Distribution > Distribution Points** category.

The **Distribution Point** window opens. (It is described in detail in “New Distribution Point” on page 464.)

4. Enter the packages root path. This is the local path on the server of the directory in which Absolute Manage is to store software installers. This path may be different on each server.
5. If the distribution point the definition of which you are editing is to be the master server, check the **Is master distribution point** option.

The master distribution point serves as the source of software installers for the other (mirror) distribution points, as discussed in “Structure” on page 201. There must always be exactly one master distribution point.

Because the master distribution point gets traffic from the mirror distribution points in addition to the agents, it should have enough processor power and network bandwidth to not become a bottleneck.

6. Click **OK**.
7. Repeat the process for all other distribution point definitions. Continue with updating the software packages as described below.

Updating software packages

NOTE

Because of limitations of the Windows operating system, Mac OS X software packages must be updated from an Absolute Manage Admin running under Mac OS X.

To update an existing software package to be compatible with the new architecture:

1. Make sure that the software installer (including any auxiliary files it may need) is available in the Windows Explorer on your computer.
2. In Absolute Manage Admin’s **Server Center** window, double-click the software package definition in the **Software Distribution > Software Packages** category.

The **Software Package** window opens. (It is described in detail in “New Software Package” on page 443.)

3. Click the **Select** button and select the software installer.
It does not matter where the installer is located, e.g., it does not need to be on a server.
4. Click **OK**.
5. Repeat the process for all other software package definitions and upload the changes to the Absolute Manage Server using the **Save Distribution and Licensing Info** command from the **Server** menu.

Absolute Manage checks and uploads the installers to the master distribution point. From there, they are automatically and transparently distributed in the background to the mirror servers – you no longer need to manually copy the installers to all distribution points.

Part 2: Using Absolute Manage

The Using Absolute Manage part of the manual describes how to accomplish specific tasks with Absolute Manage:

“Accounts and agent access” on page 46 covers the creation, administration, and appointing of administrator accounts and of agent access privileges.

“Gathering and managing information” on page 69 covers how to collect and display information with Absolute Manage.

“Controlling computers” on page 115 describes performing a range of actions on administered computers from the Absolute Manage Admin console.

“Working with mobile devices” on page 140 covers the management of mobile devices and the software on them through an MDM server.

“Working with files” on page 190 explains copying and manipulating files on administered computers

“Installing software” on page 200 describes using the Software Distribution Center for automated software installations.

“Monitoring licenses” on page 248 covers using the License Monitoring Center to ensure license compliance and finding prohibited software.

Chapter 3 Accounts and agent access

Absolute Manage uses a system of accounts and access rights to control the flow of information and prohibit unauthorized access. Setting them up correctly is necessary to ensure that Absolute Manage gathers and displays all the information you need.

Setting up and configuring these accounts and access rights is explained in this section:

- “Overview” on page 46
- “Administrator accounts” on page 48
- “Using administrator accounts” on page 53
- “Assigning servers to agents” on page 54
- “Appointing administrators to devices” on page 57
- “Setting MDM access rights for mobile devices” on page 62
- “Creating placeholder records for computers” on page 65
- “Exporting and importing server settings” on page 66

Overview

Absolute Manage’s access control centers on two main issues:

- Which administrators can do what in the system?
- Which server can access which agents? This, of course, is only an issue in systems with multiple servers.

This is discussed in more detail below.

Administrator accounts

There are two types of administrator accounts in Absolute Manage, standard accounts and superadministrator accounts.

The two types differ in two respects:

- Superadministrators can create, configure, and delete administrator accounts; normal administrators cannot do this (except for changing their own passwords).
Superadministrators are indicated by yellow icons () in the **Server Center** window’s sidebar.
- Standard administrators can see – and send commands to – only those administered computers to which they have been expressly assigned. Depending on the preference settings, superadministrators may be able to see all computers on which an Absolute Manage Agent is installed.
Standard administrators are indicated by black icons () in the **Server Center** window’s sidebar.

All account information is stored on an Absolute Manage Server, so that an account has the same settings irrespective of the computer from which the administrator is logged in.

Exactly on which server the information is stored on can be configured: By default, each Absolute Manage Server stores its own information. But by entering the address of another server in a server's settings, you can direct it to not keep its own administrator account information but instead use that from the specified server.

Any changes made to the information on the 'parent' server is automatically propagated to all 'child' servers, simplifying account management in large organizations.

Active Directory and Open Directory integration

Absolute Manage automatically takes advantage of Active Directory or Open Directory if either is present in your network. (Using Open Directory requires Absolute Manage Server to run on Mac OS X.) Active Directory or Open Directory users from groups that you specify in the **Server Settings** dialog are listed in the **Server Center** window and can be assigned Absolute Manage administrator privileges. Any changes to the user names or passwords in Active Directory or Open Directory are mirrored in Absolute Manage.

Administrator privileges

All administrators can execute commands targeting the devices to which they have been assigned. Which commands an administrator is permitted to execute can be configured in the Administrator Center; by default, every administrator can execute all commands.

In addition, the program functions to which an administrator has access can also be configured in a finely-grained way. For example, you can prevent an administrator from creating or changing installation packages without restricting other options.

NOTE While these functions can be disabled for superadministrators as well, these administrators can – because of their ability to configure accounts – always re-enable them for their own accounts. Only standard administrators can really be prevented from using these functions.

The relation of agents to servers

Each agent can be accessed only from servers that are explicitly noted in the agent's settings (by IP address or DNS name). That means that other servers are unable both to send commands to these agent's computers or collect information from them.

These servers are called inventory servers. Each agent can have any number of inventory servers, all of which have the same level of access.

In addition, one server can be specified for software distribution and one for license monitoring. Only these servers can access the respective functions of the agents. They can be the same server or

different ones. They may be among the specified inventory servers or may be separate Absolute Manage Servers.

Agent access

As noted above, not all administrators can access all agents. Except for administrators for whom the **Can manage all devices** setting has been enabled, administrators can see information only from administered devices to which they have been expressly assigned.

This makes it possible to, e.g., have administrators that are responsible only for the devices of one team without setting up a separate Absolute Manage Server for this purpose.

Administrator accounts

A person must have an administrator account to be able to access Absolute Manage Admin (and, by extension, the Absolute Manage Server). Accounts are created in Absolute Manage Admin but account information is stored on the Absolute Manage Server.

NOTE You can edit administrator accounts on a particular server only if that server is not set to use another server's account information in the **Server Settings** dialog's **General** tab (see page 497).

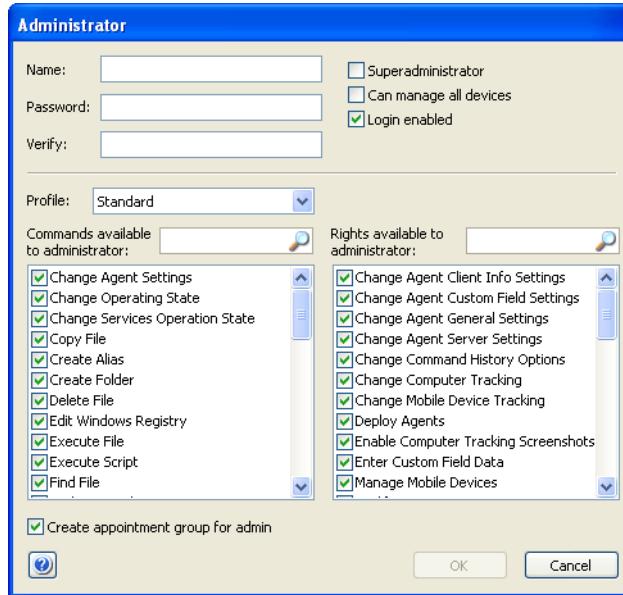
Creating an administrator account from scratch

Administrator accounts can be created from scratch or you can assign administrator rights to an Active Directory or Open Directory user.

To create a new administrator account from scratch:

1. In Absolute Manage Admin, open the **Server Center** window.
2. Choose **Administrator Setup > New Administrator** from the context menu to create a new account.

The **New Administrator** dialog opens:



3. Enter the name for the account and the password. Repeat the password in the **Verify** field.

Both account names and passwords are case-sensitive.

4. Set the desired privileges for the account:

- **Superadministrator:** The administrator has superadministrator privileges. (These privileges are explained in “Administrator accounts” on page 46.) If the option is unchecked, the account is a standard account.
- **Can manage all devices:** If this option is checked, the administrator can access all devices that are managed on the Absolute Manage Server. If the option is unchecked, the administrator can manage only devices to which the account has been expressly assigned.
- **Login enabled:** The account is active. If this option is not checked, the account is disabled.

5. If desired, assign a profile from the **Profile** pop-up menu to the account and proceed with step 9. If you do not assign a profile, continue with the next step.

Assigning a profile sets the commands and rights available to the account. The **Profile** pop-up menu also offers commands to create and delete profiles as well as edit their names.

Note: Profiles are merely presets: You can change the settings for an individual account at any time without affecting the profile, and changing the profile does not affect existing accounts which are based on it.

6. In the commands list, uncheck all commands that you want the administrator not to be able to execute on client devices.

The individual commands are described in “Commands menu” on page 283 and “Mobile Devices” on page 385.

Note: Even if you set up a superadministrator account that cannot execute all commands, a superadministrator can always change his or her own account to regain those rights.

7. In the rights list, uncheck all rights that you want the administrator not to have.

The individual rights are described in “New Administrator” on page 481.

Note: If you uncheck the Manage Mobile Devices right, the administrator is unable to send commands to managed mobile devices, even if the commands themselves are enabled in the administrator account (see step 6).

Note: As with commands, you cannot effectively deny rights to superadministrators.

8. If desired, save the configuration of commands and rights you have created as a profile by choosing **Save As** from the **Profile** pop-up menu.

Creating a profile lets you later quickly create other accounts with the same commands and rights.

9. Check **Create appointment group for admin** if you want to have two groups in the **Server Center** window’s sidebar listing, respectively, all computers and all mobile devices to which this administrator has been assigned.

10. Click **OK** to create the account locally.

11. Create more administrator accounts if desired, as described above, starting with step 2.

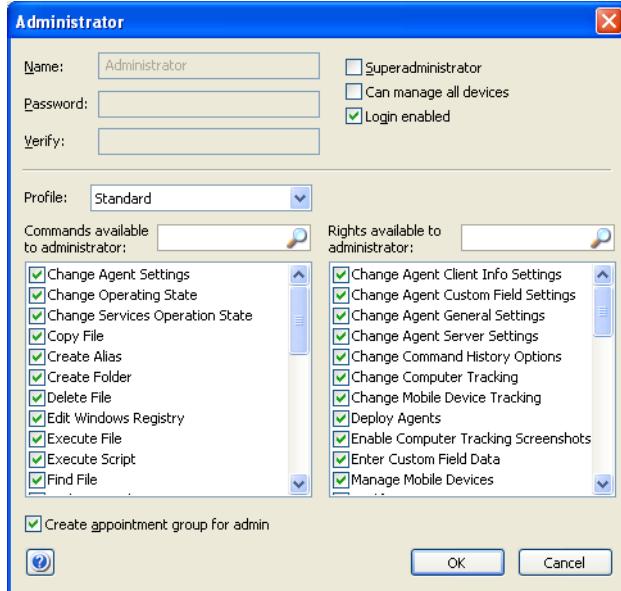
12. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on the Absolute Manage Server.

Giving administrator access to an Active Directory account

If you are connected to an Active Directory server, you can simply assign administrator rights to Active Directory users:

1. Make sure that the Active Directory group containing the Active Directory account in question has been activated in the **Server Settings** dialog’s **Active Directory** pane.
2. In the **Server Center** window, drag the desired users from the **Active Directory** group to the **Administrators** group.

The **Administrator** dialog opens:



3. Set the desired privileges and other options for the account as described above in step 4 and following.

Note: You cannot change from within Absolute Manage the names or passwords of administrator accounts imported from Active Directory.

4. Click **OK** to create the account locally.

The account is not yet saved on the server; this has to be done in a separate step as described below.

5. Create more administrator accounts if desired, as described above.
6. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on the Absolute Manage Server.

Absolute Manage uses Active Directory for this account's log-in process.

Note that when the Active Directory user account from which you have created the administrator account is removed from Active Directory or is moved out of the Active Directory groups that have been specified in server settings, the administrator account will be deleted from Absolute Manage.

Editing administrator accounts

To change the name, password, or access privileges of an existing administrator account:

1. Open the **Server Center** window.

2. Right-click the account that you want to edit and choose **Edit Administrator** from the contextual menu.

In the window's table area – but not in the sidebar – you can also select and edit multiple accounts. Note, however, that editing the names or passwords is not possible in that case.

Editing the names or passwords of accounts based on Active Directory users is never possible from within Absolute Manage.

3. Set the account options as desired, as explained in "Creating an administrator account from scratch", above.
4. Click **OK**.
5. Edit more administrator accounts if desired, as described above.
6. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on the Absolute Manage Server.

NOTE

Administrators can change their own passwords using a different method, as described in "Changing your password" on page 54.

Disabling and enabling administrator accounts

To temporarily disable an administrator account, uncheck the **Login enabled** option for the account in the **Administrator** dialog that you can open using the **Edit Administrator** command.

To re-enable the account, check the option again.

NOTE

At least one superadministrator account must be enabled at all times.

Disabling the account of an administrator who is currently logged in does not log out that user but prevents him or her from logging back in once having logged out.

Deleting administrator accounts

To delete an administrator account, right-click it and choose **Remove Administrator**.

NOTE

At least one enabled superadministrator account must exist at all times.

Deleting the account of an administrator who is currently logged in does not log out that user but prevents him or her from executing commands and from logging back in once having logged out.

Using administrator accounts

Once an administrator account has been set up, it can be used for logging in. Administrators can log in, log out, and change their passwords, as described below.

Logging in

When Absolute Manage Admin is started, it presents a login dialog:



To log in, make sure that the server address and port are correct. Enter your username and password, both of which are case-sensitive, and click **OK**.

NOTE If the administrator account is based on an Active Directory user account, you can use the display name, the account name, or the login name to log in.

You are now logged in and can use Absolute Manage according to the privileges of the specified account.

NOTE There is no way to use Absolute Manage Admin without logging in.

Logging out

There is no way to explicitly log out of Absolute Manage. Logging out is automatic when you exit Absolute Manage Admin; the only other way to log out of your account is to switch to another account, as described below.

Switching accounts

You can at any time switch to another administrator account without having to exit Absolute Manage Admin.

To do so, choose **Switch Administrator and Server** from the **Edit** menu to open the **Login** dialog (see above). Enter the new account name and password.

You can also log in to a different server at the same time.

Changing your password

You can change your password irrespective of whether you are logged into a parent or a child server.

NOTE Passwords can only be changed for accounts that were created in Absolute Manage. Passwords for Active Directory accounts must be changed on the Active Directory server.

To change the password of your own account:

1. Choose **Change Administrator Password** from the **Edit** menu.

The **Change Administrator Password** dialog opens:



2. Enter your current password and your new password. Re-enter the new password in the Password verification field.

Note: Passwords are case-sensitive.

3. Click **OK**.

The new password is effective immediately. If you were logged into a slave server, the password is propagated to the master server (and from there to any other slave servers there may be).

NOTE For changing passwords of other administrator, see “Editing administrator accounts” on page 51. Only superadministrators can change other administrators’ passwords.

Assigning servers to agents

Absolute Manage Agents communicate only with servers that have been expressly assigned to them. This prevents unauthorized access to the administered computers using the considerable capabilities of agents.

Agents can be assigned any running Absolute Manage Server as their inventory server (the main server through which they are managed). They can also be assigned to multiple inventory servers and, if desired, to software distribution and license monitoring servers.

You can assign servers to agents when you install the agents, as described in “Installing Absolute Manage Agent” on page 29. Assigning the servers at any time after the installation is explained below.

Assigning inventory servers to agents

Inventory servers are the ‘normal’ Absolute Manage Servers with which agents communicate to receive commands and send information. Each agent can be configured to communicate with any number of inventory servers.

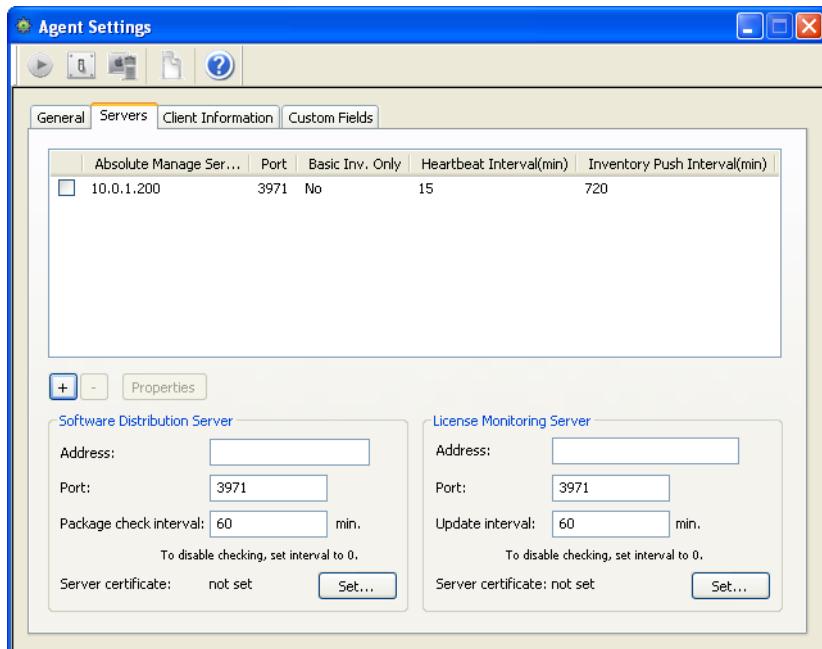
To assign inventory servers to agents:

1. In any browser window, select the computers to which you want to assign servers.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog opens; click the **Servers** tab:



In this dialog pane, you can add and remove inventory servers as well as change the communication settings.

3. To add a server, click the **+** button.

A new line is added to the table of servers and the **Inventory Server Properties** dialog is opened. Enter the IP address or DNS name of the server.

4. If desired, you can edit the other settings for the server:

- The port number is the port on which the server communicates with agents (and the Absolute Manage Admin). This should not normally be changed.
Note: If the built-in Mac OS X or Windows firewall is active on the server computer, the specified port is automatically opened in the firewall.
- The heartbeat interval is the interval in which the agent lets the server know that it is still running.
- The inventory push interval is the interval in which the agents sends changes in the state of its computer – in any information item, except those in the processes, fonts, files, printer, and startup item information.
- If a server is to act only as the software distribution server or license monitoring server for this server, set **Set Inventory** to **Basic**. This prevents unneeded inventory information from being sent to the server from the agent and so both reduces the network load and keeps the server from becoming bogged down by unneeded data. For administered client computers, set it to **Standard**. If desired, check any additional categories, such as **Include font information**, that you want automatically transmitted with every inventory update.

5. If the **Server certificate** field does not display “valid,” click the **Set** button and choose the certificate for the server.

Creating server certificates is described in “Exporting a server certificate” on page 19.

Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

6. Click **OK** to close the **Inventory Server Properties** dialog.
7. If desired, create more servers to add.
8. To remove a server, i.e., to stop agents from communicating with it, select it in the list and click the – button.
9. Before changing the agents’ settings, review the table:
 - All target agents will communicate with checked servers.
 - Only target agents will communicate with unchecked servers that already communicate with them. (I.e., the status of these servers with regard to the target agents will not be changed.)
 - None of the target agents will communicate with servers that are not in the list. (That is, any server not in the list will be removed from all target agents.)
10. Click **Execute**.

The agents are reconfigured according to the command settings.

Assigning software distribution or license monitoring servers to agents

For each agent, there is at most one software distribution server (which it contacts for software installations handled by Absolute Manage) and one license monitoring server (to which it sends reports on licensed software).

If no servers are specified for this function in the initial installation, the main inventory server is set to take on these roles as well. If you configure the servers manually on an agent and leave out the address for the software distribution server and/or the license monitoring server, the respective function is disabled on that agent.

If another setup is intended, you can assign one software distribution server and one license monitoring server to each agent. These servers can be the same or different servers; they may be among the inventory servers assigned to the agent, but need not be.

These servers can be assigned during the installation of the agent, as described in “Installing Absolute Manage Agent” on page 29, or later, as described in “Assigning inventory servers to agents”, above.

If desired, you can at the same time adjust the intervals in which the selected agents are to check for new software and report on installed software, respectively.

Appointing administrators to devices

Only administrators for whose accounts the **Can manage all devices** option is set can access all agents on computers and all mobile devices. All other administrators can only access devices to which they have been expressly assigned. This means that they can send commands only to these computers and mobile devices and display information only from them.

Appointing administrators to devices is done via appointment groups. An appointment group contains either a list of computers or a list of mobile devices. When administrators are added to an appointment group, they get access to all devices in that group. Both administrators and devices may belong to more than one appointment group.

Managing appointment groups and appointing administrators is described in detail in:

- “Working with appointment groups” on page 58
- “Appointing administrators” on page 60

Working with appointment groups

Appointment groups combine a number of devices with one or more administrators, thereby giving these administrators access to the computers.

Setting up a standard appointment group

There are standard appointment groups – where administrators are manually added and removed – and smart appointment groups that automatically include all computers meeting specified criteria.

Managed computers and mobile devices have different appointment groups – you cannot mix the two types of devices in one group.

To set up a standard appointment group:

1. Open the **Server Center** window.
2. From the sidebar context menu, choose **Administrator Setup > New Computer Appointment Group** or **Administrator Setup > New Mobile Devices Appointment Group**, depending on the type of device you want to manage in this group.

The **Administrators Group** dialog opens:



3. Enter the desired name and click **OK**.

The new group appears in the **Server Center** window's sidebar.

4. To add devices to the group, drag them on top of the group icon from a browser window or the **Mobile Devices** window.

To remove devices, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

5. To store the appointment group specification on the Absolute Manage Server, choose **Save Administrator Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new appointment group is lost unless you save the changes at some point before quitting Absolute Manage. Also, other administrators can use the group only after you have saved it to the server.

Setting up a smart appointment group

Smart appointment groups automatically include all computers or mobile devices meeting criteria that you specify when setting up the group.

To create a new smart appointment group:

1. Open the **Server Center** window.
2. From the sidebar context menu, choose **Administrator Setup > New Smart Computer Appointment Group** or **Administrator Setup > New Smart Mobile Devices Appointment Group**, depending on the type of device you want to manage in this group

The **Smart Group** dialog opens:



3. Enter the name for the new appointment group and specify the conditions that devices must meet to be included in the group.

To define a condition, specify an information item in the left-hand text field, choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

With the **+** and **-** buttons, you can add and remove conditions.

4. If you have specified more than one condition, specify through the upper pop-up menu whether devices must meet one or all of the conditions.
5. Click **OK**.

The new group appears in the **Server Center** window's sidebar.

6. To store the appointment group specification on the Absolute Manage Server, choose **Save Administrator Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new appointment group is lost unless you save the changes at some point before quitting Absolute Manage. Also, other administrators can use the group only after you have saved it to the server.

Reusing smart groups

You can drag any custom smart computer group from other browser windows or from within the **Server Center** window to the **Appointments** category in the **Server Center** window's sidebar to create a new computer appointment group with the same specifications as the smart group. In the same way, you can reuse smart mobile device groups from the **Mobile Devices** window.

Editing appointment groups

You can change the names of all appointment groups by double-clicking them in the **Server Center** window's sidebar or by selecting them and choosing **Edit Appointment Group** command from the context menu.

For smart appointment groups, you can also change the selection criteria:

1. Double-click the group in the **Server Center** window's sidebar.
2. The Smart Group dialog opens.
3. Change the selection criteria as described above in **Setting up a smart appointment group**.

Deleting appointment groups

To delete an appointment group, right-click it and choose **Remove Appointment Group** from the context menu.

As described for setting up groups, above, you must update the Absolute Manage Server using the **Save Administrator Info** command for the change to become permanent.

Appointing administrators

To appoint an administrator to a device:

1. Make sure that the **Server Center** window is open.
2. In any browser window, select the computers to which you want to appoint administrators. Or select mobile devices in the **Mobile Devices** window.

*Note: The **Agent Deployment Center** window cannot be used for this purpose.*

3. Drag the selected devices to the appointment group through which it is to be managed.

This appoints all administrators belonging to the group to the selected devices.

Removing administrators from agents or mobile devices

To stop all administrators of an appointment group from managing a device:

1. In the **Server Center** window, select the appointment group to which the device belongs.

All devices in the group are listed in the main part of the **Server Center** window.

2. Right-click the device and choose **Remove from Group** from the context menu.

The administrators in the appointment group can no longer access the removed computer or mobile device.

NOTE If some of the group's administrators also belong to other appointment groups that contain the device in question, they can still administer the device based on their membership in that other group.

To stop an administrator from managing the devices in an appointment group:

1. In the **Server Center** window, expand the appointment group and select the **Assigned Administrators** subcategory.

All administrators that are assigned to the group are listed in the main part of the **Server Center** window.

2. Right-click the administrator and choose **Remove from Group** from the context menu.

The administrator can no longer access the computer or mobile devices in the appointment group (unless he is assigned to another group that also contains some or all of the devices).

Viewing the device to which an administrator is appointed

To see the devices to which an administrator is currently assigned, select the administrator account in question in the **Server Center** window's sidebar.

The device are listed in the table area; computers are listed in the upper half and mobile devices in the bottom half.

Viewing the administrators who are appointed to a device

To see the administrators who are currently appointed to administer a given device, expand the device in the sidebar of a browser window

(such as the **Computers** window or the **Mobile Devices** window) and select its **Administrators** subcategory. The assigned administrators are listed in the main part of the window.

To view the administrators assigned to multiple devices at a glance, add the **Administrator Name** information item to any browser window displaying computer information or the **Mobile Devices** window.

Note that in both cases only administrators are listed who are specifically assigned to the devices. Administrators who can access the device because the **Can manage all devices** setting has been activated for their account are not listed.

Setting MDM access rights for mobile devices

Performing actions on managed mobile devices requires the corresponding access rights to be set when the devices are enrolled. This is done in the **MDM** tab of the server settings.

Should these privileges later be changed, devices must be re-enrolled for the changes to become effective on them.

These procedures are described in:

- “Specifying MDM access rights” on page 62
- “Updating MDM access rights on enrolled iOS devices” on page 64

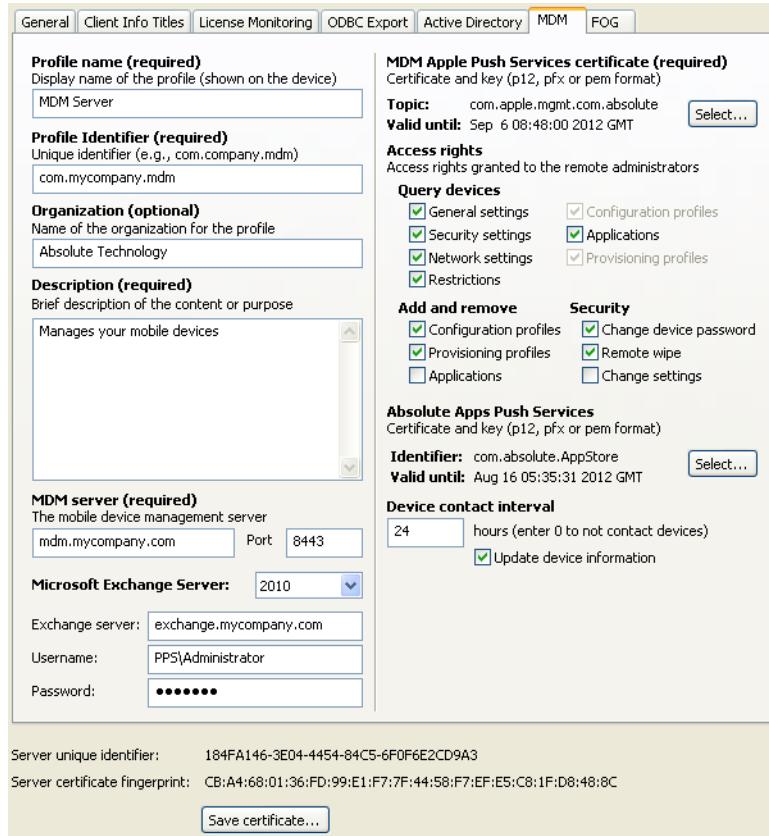
NOTE Setting MDM access rights does not apply to Android devices.

Specifying MDM access rights

To specify the access rights that administrators may have on the mobile devices managed through this Absolute Manage server:

1. Open the **Server Center** window.
2. In the sidebar, click **Server > Server Settings**.
3. In the main part of the window, click the **MDM** tab.

The MDM settings are displayed:



- In the **Access rights** section, check all privileges that you want administrators to be able to have.

The available privileges are described in "MDM" on page 504.

Note that for a particular administrator to have a privilege, the appropriate option must be checked in her or his account setup, as described in "Administrator accounts" on page 48. However, privileges that are unchecked in the **MDM** tab are unavailable to all administrators (including superadministrators), irrespective of their individual account settings.

- Choose **Server > Save Server Settings** to save the changes on the server.
- If there are iOS devices already enrolled on the server, you must re-enroll them to update the access privileges on them. See "Updating MDM access rights on enrolled iOS devices" below, for details.

You have changed the privileges that administrators can have on newly enrolled mobile devices. Privileges on already enrolled iOS devices will be updated once these devices are re-enrolled.

Updating MDM access rights on enrolled iOS devices

Any changes to the MDM access privileges for managed iOS devices (as set in the **MDM** tab of the server settings) require any devices that are already enrolled to be re-enrolled before the changes take effect on them.

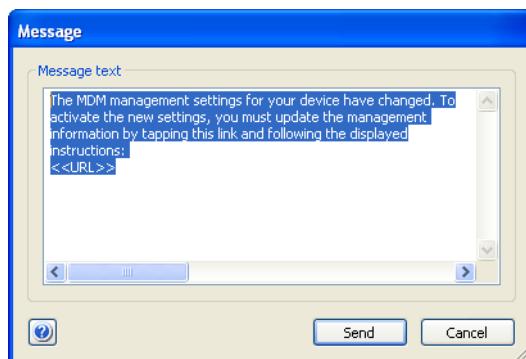
You are prompted to send re-enrollment messages to these devices whenever you change the MDM settings, but you also can do so manually at a later time:

1. In the **Mobile Devices** window, select all devices that need to be re-enrolled.

To quickly find all affected devices, you can create a smart group that collects all devices where the **Mobile Device MDM Profile Up-to-date** has the value "No".

2. Right-click the selected devices and choose **Send Re-enrollment Message to Device** from the context menu.

The **Message** dialog is displayed:



3. Enter a text that you want to send to your users.

Make sure not to delete the URL placeholder; it will automatically be replaced with the actual enrollment URL including the device identifier in the message sent to the users.

If you accidentally delete the placeholder, the URL will be appended to the end of the message.

4. Click **Send** to send the message to all selected devices.

All users will receive the message the next time they contact mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If they are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

When a user taps the URL, the device will be re-enrolled in a process that is similar to the original enrollment process. When that process is finished, the new MDM privileges are in effect on the device.

Creating placeholder records for computers

For the most part, Absolute Manage can only work with computers on which Absolute Manage Agent has been installed. However, a very limited subset of the functionality is also available for computers on which no agent is installed.

To use this capability, you must manually create a placeholder record for each computer in question, as explained below.

Functions available for placeholder records are limited to:

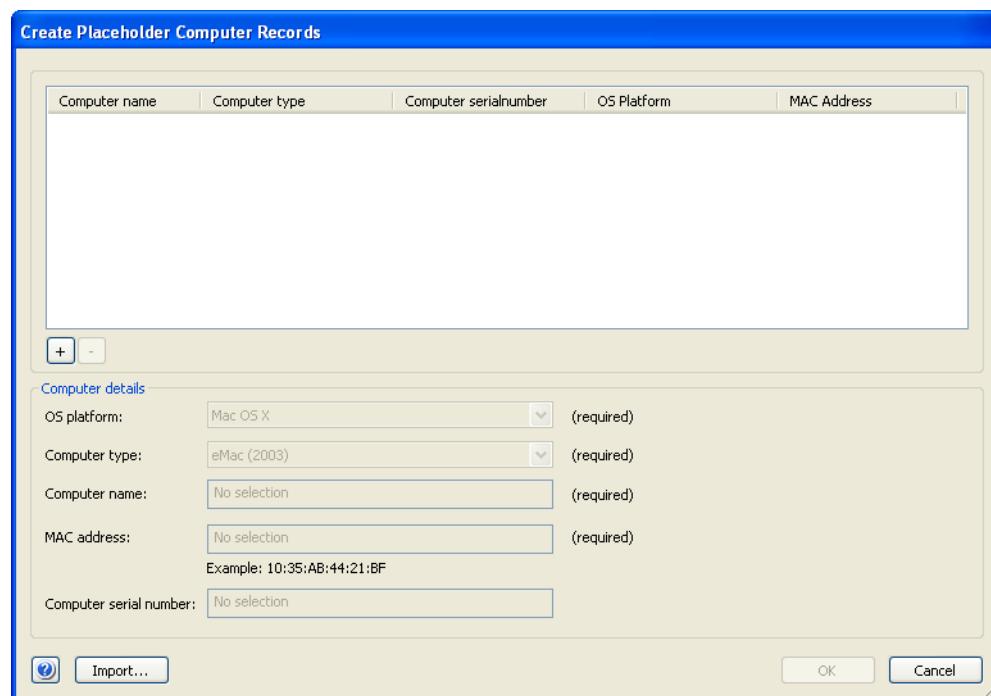
- Displaying them in browser windows. No information is displayed beyond the data that was entered when the placeholder record was created. Display-related functions of browser windows – such as sorting, finding, or exporting – also extend to placeholder records, but functions that actually access the device – such as gathering information – do not.
- The only command that is available for computers represented by placeholder records is **Reinstall Windows Computer**.

Creating placeholder records for computers

To create placeholder records for one or more computers without agents:

1. Choose **Server > Create Placeholder Computer Records**.

The **Add Custom Computers** dialog opens:



2. Click the **+** button.

The entry fields in the dialog become active.

3. Enter the information for the placeholder record you are about to create.

The serial number is optional, all other information is required.

Instead of manually entering the information from each record, you can also click the **Import** button to import the data from a tab-delimited text file. The file format is described in “Create Placeholder Computer Records” on page 346.

4. To create additional placeholder records, repeat step 2 and 3.
5. Click **OK** to save the placeholder records displayed in the dialog.

Deleting placeholder records

To delete existing placeholder records:

1. In any browser window, select the records you want to delete.
2. Right-click the selected records and choose **Remove from Server** from the context menu.

The records are deleted after you have confirmed that you want to do so.

Exporting and importing server settings

If you want to migrate an Absolute Manage Server installation from one computer to another, most of the data, such as the database tables, can be transferred easily by copying the relevant files from the Absolute Manage Server folder. (This folder is found at “/Library/Application Support/LANrev Server” on Mac OS X systems and “Program Files\Pole Position Software\LANrev Server” on Windows systems.)

Transferring custom field definitions and server settings, however, is less straightforward (except between Mac OS X systems, where you can simply copy the “/Library/Preferences/com.poleposition-sw.lanrev_server” file).

There is a command line option that lets you save the server settings and custom field definitions as an XML file and import it into any other server instance. The file is compatible with both the Mac OS X and Windows versions of the server.

Exporting server settings on Mac OS X

To export server settings and custom field definitions from a server installed on Mac OS X:

1. On the computer on which the server is installed, launch Terminal.
2. In the Terminal window, enter this command and press Return:

```
sudo /Library/Application\ Support/LANrev\  
Server/LANrev\ Server.app/Contents/MacOS/LANrev\  
Server --ExportPreferences <export file>.plist
```

<export file> is the path and name of the settings file you want to create.

3. When prompted, enter the password to execute the command with superuser privileges.

The settings file is created with the specified name at the specified location.

Exporting server settings on Windows

To export server settings and custom field definitions from a server installed on Windows:

1. On the computer on which the server is installed, launch cmd.exe with administrator privileges.
2. In the terminal window, browse to the Program Files\Pole Position Software\LANrev Server directory.
3. In the terminal window, enter this command and press Enter:

```
LANrev Server.exe --ExportPreferences <export  
file>.plist
```

<export file> is the path and name of the settings file you want to create.

The settings file is created with the specified name at the specified location.

Importing server settings on Mac OS X

To import server settings and custom field definitions into a server installed on Mac OS X:

1. On the computer on which the server is installed, launch Terminal.
2. In the Terminal window, enter this command and press Return:

```
sudo /Library/Application\ Support/LANrev\  
Server/LANrev\ Server.app/Contents/MacOS/LANrev\  
Server --ImportPreferences <import file>.plist
```

<import file> is the path and name of the settings file you want to import.

3. When prompted, enter the password to execute the command with superuser privileges.

The specified settings file is imported and the existing server settings and custom field definitions are overwritten.

Importing server settings on Windows

To import server settings and custom field definitions into a server installed on Windows:

1. On the computer on which the server is installed, launch cmd.exe with administrator privileges.
2. In the terminal window, browse to the Program Files\Pole Position Software\LANrev Server directory.
3. In the terminal window, enter this command and press Enter:

```
LANrev Server.exe --ImportPreferences <import  
file>.plist
```

<import file> is the path and name of the settings file you want to import.

The specified settings file is imported and the existing server settings and custom field definitions are overwritten.

Absolute Manage helps you manage your network by gathering a wide range of information on the administered computers. This section describes how to use this feature:

- “Overview” on page 69
- “Gathering information” on page 70
- “Custom information” on page 81
- “Manually edited information” on page 93
- “Storing and exporting information” on page 97
- “Displaying information” on page 103
- “Searching, filtering, and sorting” on page 109

Overview

The gathering and managing of information by Absolute Manage centers on the central database integrated in Absolute Manage Server: The server collects information from the agents and stores it in its database. When you want to see specific information, the Absolute Manage admin application queries the server for it and displays it on your workstation.

In principle, the flow of information is very simple: It is gathered by the agents, stored by Absolute Manage Server, and displayed by Absolute Manage Admin.

Gathering information

Information collection by the server is mostly automatic. Some types of information – on processes, fonts, startup items, services and files – are collected on request only to avoid wasting local processing power and network bandwidth.

This is described in more detail in “Gathering information” on page 70.

Custom information

If Absolute Manage’s extensive list of information items does not provide the data you are looking for, you can extend it by creating custom information items.

This is described in detail in “Custom information” on page 81.

Information storage on the server

Absolute Manage Server stores the collected information in an internal relational database. There are a number of tables in this database, among them for storing computer, process, file, font, and Absolute Manage account information. There also exist numerous subtables for information on volumes, memory slots, and other objects that can appear multiple times per computer.

The columns in these tables are called information items; they are the basic unit of information display in Absolute Manage.

Displaying information

Information is displayed by Absolute Manage Admin in so-called browser windows. These windows consist mainly of a table where the columns are information items and the rows represent computers or other objects such as files.

You request particular pieces of information in two basic ways from the server:

- To compare the same information for several administered computers, you put the respective information items into browser windows.
- To view in-depth information on one computer, you select that computer in the sidebar of a browser window.

This is described in more detail in “Displaying information” on page 103.

Rearranging information

You can narrow down and rearrange information in a browser window by searching for text, creating groups of related computers, and sorting browser windows.

This is described in more detail in “Searching, filtering, and sorting” on page 109.

Custom information

Absolute Manage provides ten text fields for storing any kind of information on client computers and retrieve it from there. These fields are intended for information, e.g., inventory numbers, that cannot automatically be determined by the software.

This is described in more detail in “Manually edited information” on page 93.

Gathering information

Gathering information is performed by the Absolute Manage Agents which then forward this information to all inventory servers (i.e., Absolute Manage Servers) that are specified for them.

Some types of information are gathered and forwarded automatically in regular intervals; other types – information on files, processes, fonts, printers, and startup items – are gathered only on request.

In addition, updates for the automatically gathered information can be requested manually in cases where you do not want to wait for the next scheduled update.

This is discussed in detail in:

- “Configuring automatic information gathering” on page 71
- “Gathering and updating information manually” on page 73 (includes gathering information on computers, processes, fonts, printers, and startup items)
- “Gathering information on files” on page 76
- “Gathering information on registry entries” on page 78
- “Collecting USGCB SCAP compliance reports” on page 80

Configuring automatic information gathering

Information on the computers’ hardware and software is gathered automatically by the Absolute Manage Agents and transmitted to the servers. The interval in which these transmissions happen can be configured.

NOTE The Absolute Manage Agents are smart about their transmissions: They send only changed information to the server, not everything they collect.

To configure the update interval:

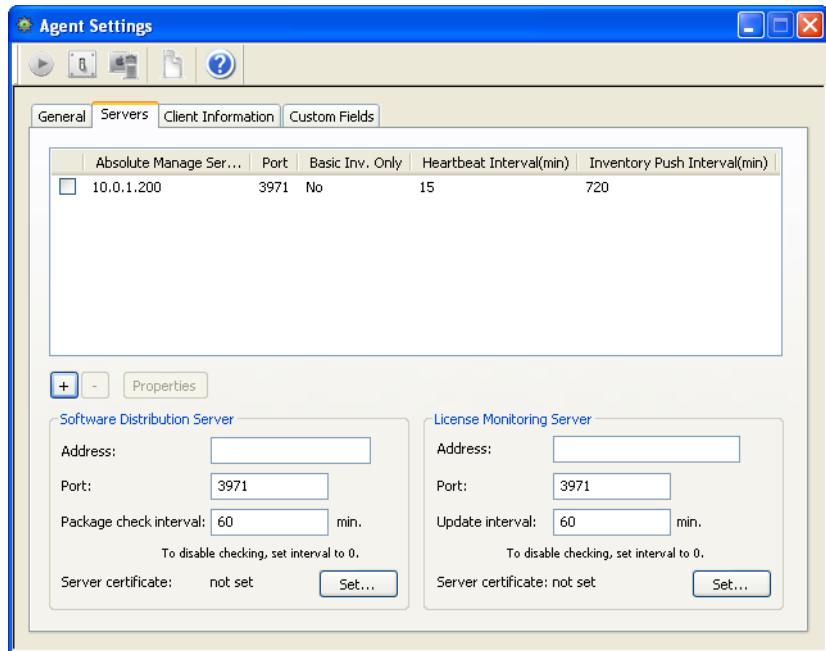
1. In any browser window, select the computers on which you want to configure the update interval.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Agent Settings**.

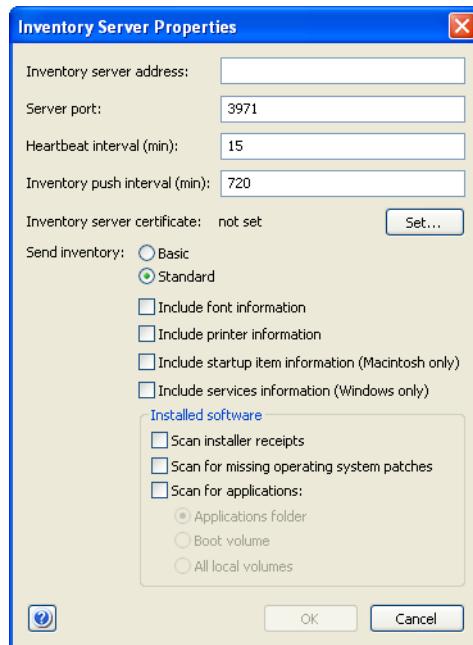
The **Agent Settings** dialog opens.

3. Click the **Servers** tab:



4. Select the desired Absolute Manage Server in the table, and click the **Properties** button.

The **Inventory Server Properties** dialog opens:



5. Enter the desired update interval in minutes.

If several servers are specified in the table – i.e., the selected agents are sending inventory information to several Absolute Manage Servers – the interval can be set separately for each of them.

6. Make sure that the servers you have updated have a checkmark in the table and click **Execute**.

The new interval is set on all target computers.

Gathering and updating information manually

While most information that Absolute Manage provides is gathered automatically, some of it is only provided on request to avoid using up too much network bandwidth. This applies to information on:

- Fonts
- Printers
- Processes
- Startup items
- Installed software (including missing operating system patches)

NOTE While information on files also is collected in a manually triggered procedure, the process is somewhat different, as described in “Gathering information on files” on page 76.

This information can be requested manually, as detailed below. By the same process, information that is normally gathered automatically can be updated before the next automatic update is due.

While the server sends all information it receives to the admin application when required, information can also be manually loaded from the server to Absolute Manage Admin. This is also described below.

Manually gathering computer, font, printer, or startup item information

To collect this information manually:

1. In any browser window, select the computers from which you want to gather the information.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Gather Inventory Information**.

The **Gather Inventory** dialog opens:



3. To cause the agents on the target computers to transmit all computer information (i.e., not just information that has changed) to the server, check **Force full inventory**.

To gather font, printer, startup item, or service information, check the appropriate option.

*Note: Changed computer information is always transmitted when the **Gather Inventory Information** command is executed, even if none of the options in the dialog is checked.*

4. Click **Execute**.

The agents on the target computers collect the requested information and send it to the server, where it is entered in the appropriate tables. The server automatically forwards the information to the admin application if any browser windows display corresponding information items.

Manually gathering processes information

To collect process information manually:

1. In any browser window, select the computers from which you want to gather the information.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Gather Process Information**.

The **Gather Processes** dialog opens.

3. Click **Execute**.

The agents on the target computers collect the process information and send it to the server, where it is entered in the Processes table. The server automatically forwards the information to the admin application if any browser windows display process-related information items.

Manually gathering information on installed software

To collect information on installed software:

1. In any browser window, select the computers from which you want to gather the information.
2. From the **Commands** menu, choose **Gather Installed Software**.

The **Gather Installed Software** dialog opens.



3. Check the desired options:

- **Scan installer receipts:** Absolute Manage checks the target computers for installer receipts and lists the corresponding software. Note that only some installers generate such receipts.
- **Scan for missing operating system patches:** Absolute Manage compares the list of applicable operating system patches that are available in the Software Development Center with the patches that are actually installed on the computer and notes all patches that are missing.
Note: Patches that have been rejected by you or another administrator are not reported as missing.
- **Scan for application:** Absolute Manage scans the specified locations and their subfolders for applications:
 - **Applications folder:** the **Applications** folders (on Mac OS X targets) or the **Program Files** folders (on Windows targets; folder chosen according to the local environment variable settings)
 - **Boot volume:** the entire startup volume
 - **All local volumes:** all volumes currently mounted on the target computer, except server volumes
Note: Scanning entire hard disks can create a huge amount of data. We recommend scanning the boot volume or all local volumes only when really required.

You must check at least one option.

If one method of searching for software is deselected, any software from the target computers that has been previously found by this method is deleted from Absolute Manage's database.

For example, if **Scan installer receipts** is unchecked, Absolute Manage will delete any software on the current target computers that was identified by its installer receipts from the Installed Software table. That software will no longer be displayed in the **Installed Software** window.

4. Click **Execute**.

The agents on the target computers collect the installed software information and send it to the server, where it is entered in the Installed Software table. The server automatically forwards the information to the admin application if any browser windows display related information items.

Note that previously collected installed software information is deleted before the targets are searched: If one method of searching for software is deselected, any software from the target computers that has been previously found by this method is deleted from Absolute Manage's database.

For example, if **Scan installer receipts** is unchecked, Absolute Manage will delete any software on the current target computers that was identified by its installer receipts from the Installed Software table. That software will no longer be displayed in the **Installed Software** window.

Manually requesting information from the server

Absolute Manage Server automatically notifies any connected admin applications when new information arrives and forwards the information that is displayed in browser windows.

If such transmissions are interrupted, e.g., due to abnormal network conditions, you can force a reupdate by choosing **Synchronize All Tables** from the **Server** menu. You can also update just some records by selecting them in any browser window and choosing **Synchronize Selected Records**, which updates all information for the selected computers.

Synchronizing causes the server to send just updated information. When you suspect that some information in Absolute Manage Admin is out of date and is not getting updated through synchronizing, you can choose **Reload All Tables** or **Reload Selected Records**, respectively, to force a complete update of the information stored locally by Absolute Manage Admin.

Gathering information on files

Gathering information on files is different from the other information gathering methods – except gathering information on registry entries – in that it is always done selectively, i.e., not on all files on a target computer but only on those meeting specified conditions.

NOTE Viewing files is not covered in this section; please see “Viewing files from administered computers” on page 193 for information on how to view the contents of a file on an administered computer.

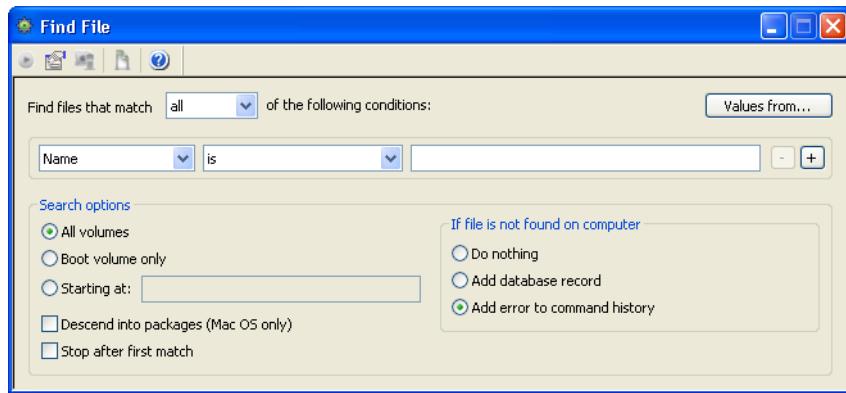
To gather information on files:

1. In any browser window, select the computers from which you want to gather the file information.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Find File**.

The **Find File** dialog opens:



3. Specify the parameters of the files you want to find.

The available parameters are described in "Files" on page 566, except for **Checksum**.

Checksum lets you select files by the MD5 checksums, making sure that files are really the desired version, without changes. Note that the checksum has to be calculated dynamically; doing so for a large number of files requires a huge amount of processing power on the client computer and should therefore be avoided. Always combine the **Checksum** criterion with other criteria that make sure that the checksum needs to be calculated only for a small number of files. Checksums are not available for folders.

When you search for files by version number, make sure to observe the platform conventions:

- On Mac OS X, version numbers have one or two dots, e.g., 2.0, 2.0b1, or 2.0.1.
- On Windows, version numbers have three dots, e.g., 1.2.123.54 or 2.120.43.3.

In general, you should specify the more selective criteria (e.g., name or bundle identifier) first and less selective criteria (e.g., **Is File**) later to speed up the search.

Note: By default, Absolute Manage finds both visible and invisible files. If you wish to find only visible files, specify an additional condition "Is invisible No," making sure to search for files fulfilling "all" conditions (see next step).

4. Choose whether you want to find files that meet at least one of the specified conditions (logical OR) or only files that meet all of them (logical AND).
5. Specify the other options:
 - Whether to search all volumes, just the boot volume, or just a specific folder and its subfolders.
 - Whether to search inside packages on Mac OS X targets.
 - Whether to search just the first matching file on each target computer or all matching files.
6. Specify the behavior when no file matching your specifications is found on a particular target computer:
 - Choose **Do Nothing** to disregard the result. This simply causes neither a record for the non-existing file nor an error to be generated.
 - Choose **Add database record** to create an entry in the file database for the missing file. Entries for missing files are distinguished in particular by having the value "No" in the **File Found** information item.
 - Choose **Add error to command history** to create an entry in the command history noting that the specified file could not be found on the target computer in question.
7. Click **Execute**.

The agents on the target computers search their local hard disks for matching files and send information on them to the server, where it is entered in the Files table. The server automatically forwards the information to the admin application if any browser windows display corresponding information items.

Gathering information on registry entries

Gathering information on registry entries is different from the other information gathering methods – except gathering information on files – in that it is always done selectively, i.e., not on the entire registry contents of target computers but only on those meeting specified conditions.

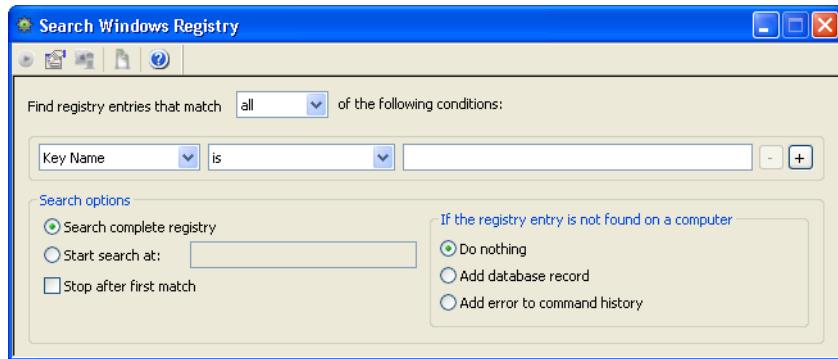
To gather information on registry entries:

1. In any browser window, select the computers from which you want to gather the registry entry information.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Search Windows Registry**.

The **Search Windows Registry** dialog opens:



3. Specify the parameters of the registry entries you want to find.

You can search for keys and values by name or path.

When you specify a path, you can use environment variables, as described in “Environment variables” on page 137.

4. Choose whether you want to find registry entries that meet at least one of the specified conditions (logical OR) or only entries that meet all of them (logical AND).
5. Specify the other options:

- Whether to search the entire registries or just the subset at a specified path.
- Whether to find just the first matching entry on each target computer or all matching entries.
- What to do when no matching registry entry is found on a target computer. You can specify that nothing happens, an error message is inserted in the command history, or a special entry is created in Absolute Manage’s Registry Entries database table.

These special entries specify the registry entry that was searched for and have a value of “No” in the **Registry Entry Found** information item. This allows you, e.g., to easily find all computers missing a particular entry.

6. Click **Execute**.

The agents on the target computers search their local registries for matching entries and send information on them to the server, where it is entered in the Registry Entries table. The server automatically forwards the information to the admin application if any browser windows, e.g., the **Registry Entries** window, display corresponding information items.

Collecting USGCB SCAP compliance reports

Using Absolute Manage, you can execute and collect USGCB SCAP compliance reports on administered computers.

NOTE It is beyond the scope of this manual to discuss the theory, purpose, or use of USGCB SCAP reports. For details on these reports, please consult the relevant section of NIST's website at <http://usgcb.nist.gov/index.html> or other applicable documentation.

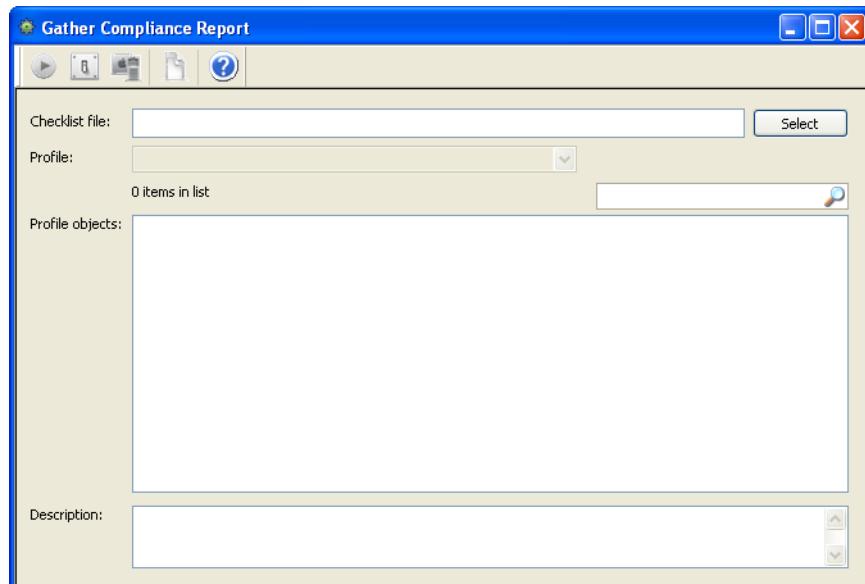
To collect USGCB SCAP reports:

1. In any browser window, select the computers for which you want to collect the compliance reports. Compliance reports can only be collected from Windows clients.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Gather Compliance Report**.

The **Gather Compliance Reports** dialog opens:



3. Click the **Select** button to choose the file containing the report definition or drag the file into the **Checklist file** field from the desktop.
4. From the **Profile** menu, choose the desired profile from the list of profiles available in the chosen report definition file.
5. In the **Profile objects** list, uncheck all options that you do not want to include in the profile.

6. Click **Execute**.

The specified target computers are evaluated according to all chosen report options. The results, along with the calculated scores and the overall pass result, are stored in Absolute Manage's internal Compliance Report database table and can be displayed in the **Compliance Reports** window.

Custom information

In addition to Absolute Manage's extensive list of predefined information items, you can create your own custom information fields to support special requirements. The data for these custom information fields is gathered by the agents and transmitted to the server together with standard inventory information.

Preparing and using custom information fields is a multi-step process:

1. First, you define the fields on the server. Fields can be either manual or dynamic.

Data is entered manually into manual fields or it is imported from text files.

Defining a dynamic field involves specifying scripts or other data sources for Mac OS X and Windows clients that will be evaluated on the administered computers to gather the desired information. The return values are used as the dynamic custom fields' values.

Creating either type of custom information field is described in "Defining custom information fields" on page 82.

2. If desired, you can share custom information fields among multiple Absolute Manage Servers. This is done by setting servers up to not keep their own field definitions but mirroring those of a specified other server.

Details are available in "Setting up custom information field mirroring" on page 86.

3. Then, assign the custom information fields to agents.

Custom information fields can gather information only from agents to which they are assigned.

This is described in "Assigning custom information fields" on page 87.

4. If desired, import data for manual information fields from text files.

This is described in "Importing data into custom information fields" on page 90.

5. Finally, insert the custom information fields in browser windows in the same way as standard information items.

This is described in “Using custom information fields” on page 88.

6. Optionally, you can export or import the definitions of custom information fields.

This is described in “Exporting and importing custom information field definitions” on page 92.

To gather the information for a dynamic custom information item, Absolute Manage evaluates the specified data sources on the assigned administrated computers.

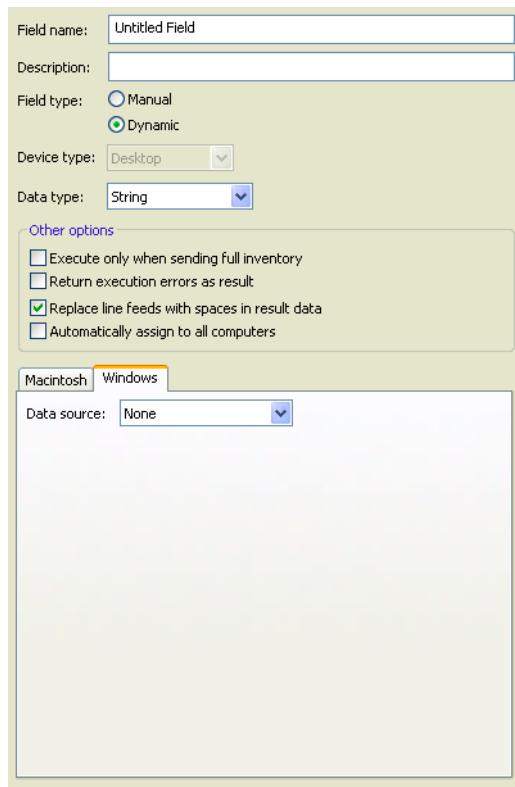
Defining custom information fields

Custom information fields are defined on the Absolute Manage Server, making them available to all administrators.

To define a custom information field:

1. Open the **Server Center** window.
2. Choose **Custom Information Fields > New Custom Information Field** from the context menu.

The **Custom Information Field** dialog is displayed in the main part of the **Server Center** window:



3. Enter a name and a description for the new custom information field.

The description will be displayed as a tooltip for the field.

4. Specify whether the field is to be a manual or a dynamic field:

- Manual fields are for humans to individually enter data into. (Although data can be imported from external text files, as described in “Importing data into custom information fields” on page 90.)
 - Dynamic fields receive their data from automated sources such as scripts or registry entries on the client computers. They behave much like standard information items.
5. Specify whether the custom information field is intended for desktop devices or mobile devices.

Dynamic fields can only be used for desktop devices; custom fields intended for mobile devices must be manual fields.

If you chose **Mobile** as the device type, an additional field is displayed in which you can enter a variable name. This variable can then be used in configuration profiles in the form `$(<variableName>)`.

6. Specify the desired data type of the field:

- **String**: Any unformatted text
- **Number**: Any number. You can choose from several display formats.
- **Boolean**: True or false
- **Date**: A point in time
- **File Version**: A version number according to the conventions of the target platform
- **IP Address**: An IPv4 address (e.g., 192.168.0.1)
- **Enumeration**: A value from a predefined list. Specify the list of possible values using the + and - buttons. (All values are treated as strings.)

Enumeration is not available for dynamic fields; choose **String** instead.

7. If you have specified a manual field, continue with step 13

8. Decide on when the data sources should be evaluated:

- When they are to be executed only when a full inventory report is made, check the **Execute only when sending full inventory** option.

*Note: Full inventory reports are made by the agents when they are first contacted by a server, when they start up, or when they are sent the **Gather Inventory Information** command with the “Force full inventory” option.*

- When the scripts are to be executed every time the inventory is updated, uncheck the option.

Having data sources evaluated only for full inventory reports is especially useful in the case of scripts taking a long time to run, involving user interaction, or gathering information that changes only rarely.

9. If you want execution errors to be returned, check the **Return execution errors as result** option.

This will cause the agents to send any execution errors of a script as if they were the actual results. These values are then stored normally in the custom field.

If the option is unchecked, no values are returned in case of execution errors and the field remains empty.

10. If the entire result is to be stored as a single line of text in the field, check the **Replace line feeds with spaces in result data** option.
11. If you want the custom field to always be available for all client computers (much as built-in information items are), check the **Automatically assign to all computers** option.

If this option is unchecked, you have to assign the field manually to computers, as described in “Assigning custom information fields,” below. This allows you, however, to give each computer only applicable fields, which may be useful if you have a large number of fields that each is relevant only for a subset of the administered computers.

12. Specify the scripts, other programs, or other data sources that are to be executed by choosing the desired option from the **Data Source** pop-up menu.

Data sources are specified separately for Mac OS X and Windows computers; each platform is optional but at least one must be specified.

Because of limitations in the Windows operating system, it is not possible to specify programs with the **Other Executable** type for Mac OS X clients in Absolute Manage Admin for Windows. You can, however, edit custom information fields with this specification in Absolute Manage Admin for Windows as long as you do not change the executable (or change it to one of the script types).

Depending on the type of data source you specify, different options become available. These options are described in “New Custom Information Field” on page 489.

Note: Any executables you specify must be available on your computer – either locally or on a mounted server volume – when you define the field. They do not need to be available later outside

of the Absolute Manage system, as they are stored on the Absolute Manage Server.

The line endings of any specified scripts are automatically converted to the conventions on the target platform during the upload to the Absolute Manage Server. (However, Absolute Manage does not convert line endings in any additional files that are uploaded as a consequence of you checking the **Transfer all files in folder containing the executable** option.)

13. If desired, create additional custom information fields.
14. From the **Server** menu, choose **Save Custom Information Fields** to upload the new field definitions to the Absolute Manage Server.

Absolute Manage Admin uploads the field definition and the specified scripts or executables, if any, to the Absolute Manage Server.

The new custom information fields are available in the **Agent Information > Custom Fields** section of the **Information Items** window.

New dynamic custom information fields are used to actually gather information only if you have checked the **Automatically assign to all computers** option in step 11. Fields for which this option is not checked must be assigned to agents as described in “Assigning custom information fields” below. (This does not apply to manual custom information fields, which are always assigned to all computers.)

Editing custom information fields

To edit a custom information field, proceed as described above but click the field in the sidebar of the **Server Center** window in step 2.

Changes in custom information field definitions are propagated to affected clients (i.e., clients to which the old field definition had been assigned) either upon their next ‘heartbeat’ contact with the Absolute Manage Server, when the **Gather Inventory Information** command is issued from Absolute Manage Admin (your copy or somebody else’s), or when a different custom information field is assigned to that client. Any information gathered for the custom information field before any of these three events occurs will still use the old field definition.

Deleting custom information fields

To delete a custom information field, select it in the sidebar of the **Server Center** window and choose **Delete Custom Information Field** from the context menu.

Setting up custom information field mirroring

You can set up Absolute Manage Servers so that they receive their custom field definitions from a different server.

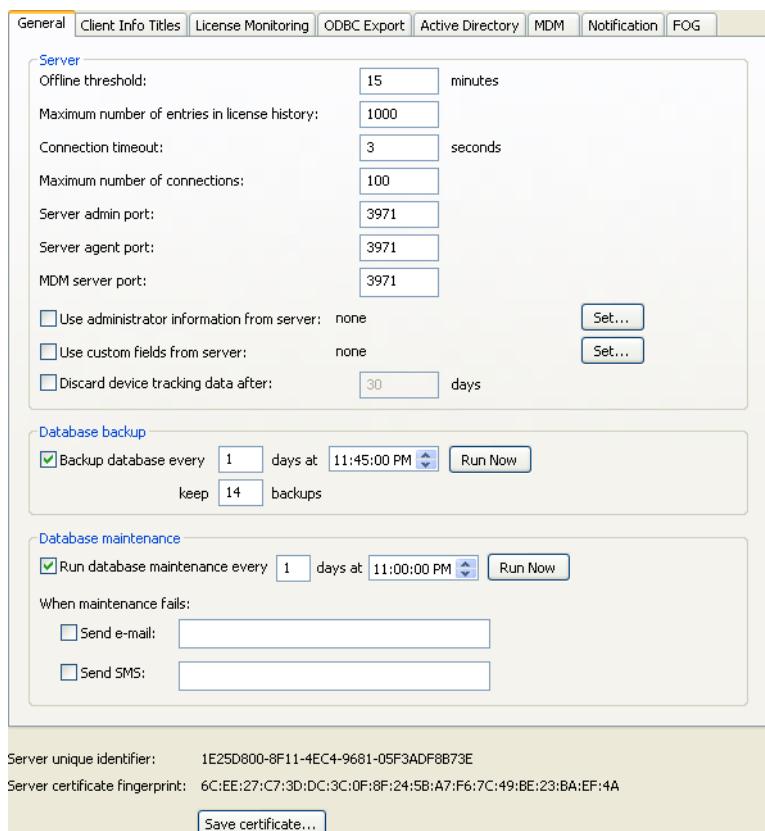
To make a server mirror another server's custom information field definitions:

1. Make sure that you are connected to the server that you want to set up as a mirror.

If you are not, use the Switch Administrator and Server command to connect to it.

2. Open the **Server Center** window.
3. Click the **Server > Server Settings** category in the sidebar.

The **General** pane of the **Server Settings** dialog is displayed in the main part of the **Server Center** window:



4. In the **Use custom fields from server** field, enter the DNS name or IP address of the server that is to be mirrored. If the server communicates over a non-standard admin port, change the port accordingly.

The description will be displayed as a tooltip for the field.

5. From the **Server** menu, choose **Save Server Settings** to upload the new settings to the Absolute Manage Server.

Absolute Manage Admin uploads the settings. This overwrites any custom field definitions that are currently in effect on the server and overwrites them with the definitions from the specified server.

In future, changes on the mirrored server will automatically update this server.

Assigning custom information fields

Absolute Manage gathers information for dynamic custom information fields only from computers to which these fields have been specifically assigned. Only fields with the **Automatically assign to all computers** option checked (and manual custom information fields) are assigned automatically; all other fields have to be assigned manually according to this procedure.

Not assigning fields automatically can have two benefits: First, scripts do not need to be executed on computers for which you are not interested in the information they produce. And second, you can use scripts that may not be compatible with all administered computers sharing a particular platform.

To assign a custom information field to computers:

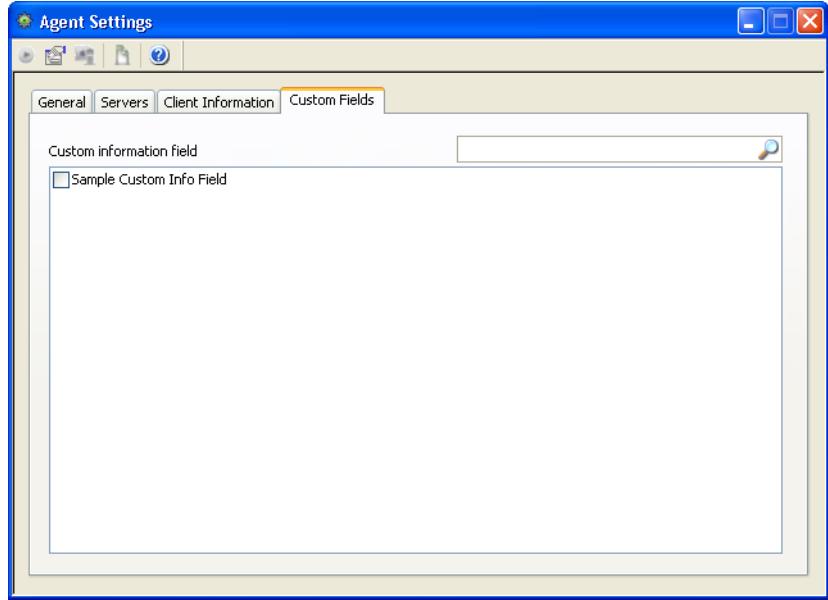
1. Make sure that the custom information field has been defined, as described in "Defining custom information fields" on page 82.
2. In any browser window, select the computers to which you want to assign the field.

Note: For information on specifying groups as targets, see "Targets" on page 286.

3. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog is displayed.

4. Click the **Custom Fields** tab:



5. Check all fields that you want to assign to the target computers and uncheck all fields that you do not want to be assigned to them.

The assignment status of fields with the checkbox in the third state () remains unchanged.

6. Click **Execute**.

The checked fields are assigned to all computers in the target list. From now on, information from these fields is gathered from the target computers (either with each inventory update or only with full inventory reports, as specified in the fields' definitions).

The assigned fields are also displayed when the single computer view of one of the target computers is opened in a browser window as described in "Displaying an overview of a single computer" on page 105.

Unassigning custom information fields

To unassign a custom information field – preventing it from being evaluated on particular client computers – proceed as described above and make sure to uncheck the field in step 5.

Using custom information fields

Custom fields are used like normal information items.

Desktop custom fields are listed in the **Agent Information > Custom Fields** section of the **Information Items** window and can be used in browser windows like standard information items. (This is described in "Displaying information" on page 103.) Remember, however, that dynamic custom fields gather information only from computers to which they have been explicitly assigned, as described in "Assigning custom information fields" on page 87.

Custom fields for mobile devices are listed in the **Mobile Device Information > Custom Fields** section of the **Information Items** window. They are always manual information fields, not dynamic, and so do not need to specifically be assigned to devices.

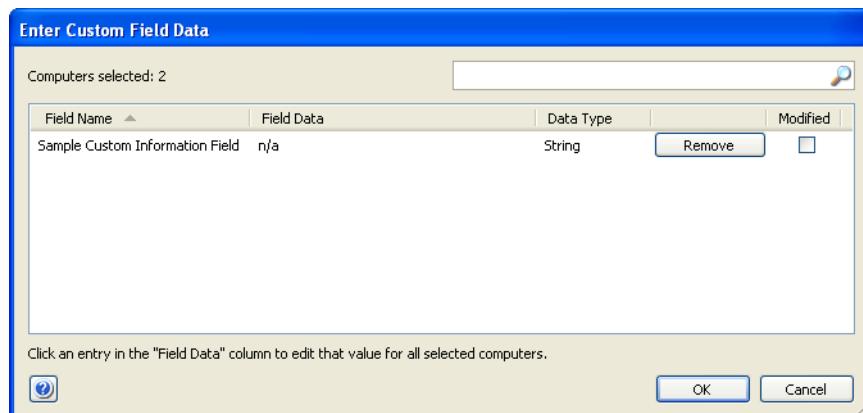
Editing manual custom information fields

You can edit information in manual information fields (but not dynamic information fields) for one or for multiple computers or mobile devices.

To do so:

1. In any browser window or the **Mobile Devices** window, select the computers or mobile devices for which you want to edit the field.
2. Right-click any of the selected computers and choose **Enter Custom Field Data** from the context menu.

The **Edit Custom Field Data** dialog is displayed:



3. If you want to remove the content of a manual custom information field on all selected computers, click the **Remove** button in the row representing that field.
4. If you want to edit the content of a field, click in the **Field Data** column in the row of the field and enter the desired content.
5. Repeat step 3 or step 4 for other fields as desired.
6. Make sure that all fields that you want to modify for all selected computers are checked in the **Modified** column and all others are unchecked.

*Note: The **Modified** column is not displayed if only one computer was selected before the dialog was opened.*

7. When you are done, click **OK**.

Absolute Manage updates the content of the manual custom information fields on the selected computers.

Importing data into custom information fields

You can import data from text files into manual custom information fields.

To import data into custom information fields:

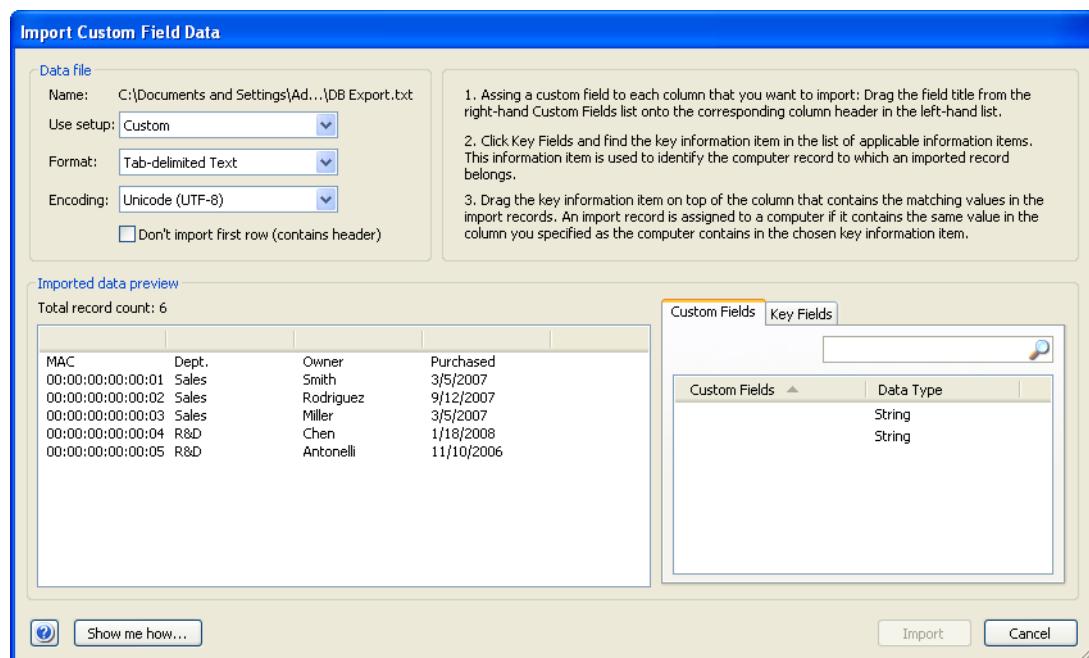
1. From the **File** menu, choose one of two commands, depending on the kind of custom information fields into which you want to import data:
 - To import into custom information fields for desktop devices, choose **Import Custom Field Data for Desktop Devices**.
 - To import into custom information fields for desktop devices, choose **Import Custom Field Data for Mobile Devices**.

The operating system's Open dialog is displayed.

2. Choose the desired text file and click **Open**.

The text files must delimit records with returns and fields within records with tabs, commas, or semicolons. Absolute Manage supports all common text encodings.

When you click **Open**, the **Import Custom Field Data** dialog is displayed:



3. If you have saved a fitting setup, choose it from the **Use setup** pop-up menu.
4. Specify the format and encoding in the respective pop-up menus.

Absolute Manage usually detects these parameters automatically, but you can override it.

5. If the import file contains field names in the first row, check **Don't import first row**.
6. Click the **Custom Fields** tab and drag each custom field into which you want to import data to the column in the import file (displayed in the **Import data preview** section of the dialog) that you want to import into the field.

If you have dragged a field onto the wrong column, you can remove it by right-clicking the column (not the title) and choosing **Remove Field**.

7. Click the **Key Fields** tab and drag the information item that Absolute Manage is to use to assign import records to database records onto the column that Absolute Manage is to use for this purpose.

During the import process, Absolute Manage will, for each import record, take the value from the column that you specified (by dragging the field on top of it) and find the database records that contain the same value in the key field you specified.

The values from the other fields in the import record are then imported into the specified fields (from step 6) of the database record, overwriting any previous content.

It is possible for multiple database records to match the value from the import record, in which case the import values are imported into the fields of all matching database records. (This can be a powerful tool to quickly update many client computer records.)

The specified column in the import file, on the other hand, must be a true key field. That is, no two import records may contain the same value in this column. If they do, no data is imported.

If you have dragged the field onto the wrong column, you can remove it by right-clicking the column (not the title) and choosing **Remove Field**.

8. If you want to reuse the settings you made, save them as a preset using the **Save As** command from the **Use setup** pop-up menu.
9. Click **Import** to perform the import.

Absolute Manage imports the data from the import file into the specified manual custom information fields according to your settings. Any previous content of these fields is overwritten.

Exporting and importing custom information field definitions

You can export the definitions of custom information fields and import them.

Note that you can also export or import all custom field definitions together with the server settings. This is mostly useful when migrating a server from one computer to another. See “Exporting and importing server settings” on page 66 for details.

Exporting custom information field definitions

To export custom information field definitions:

1. In the **Server Center** window, select the custom information fields the definitions of which you want to export.
2. Right-click in the sidebar and choose **Custom Information Fields > Export Selected Fields** from the context menu.

The operating system's Save dialog is displayed.

3. Choose a name and location for field definition file and click **Save**.

Absolute Manage exports the field definitions to the specified file.

You can also drag the fields from the **Server Center** window to the desktop.

Importing custom information field definitions

To import custom information field definitions:

1. In the **Server Center** window, right-click in the sidebar and choose **Custom Information Fields > Import Fields** from the context menu.

The operating system's Open dialog is displayed.

2. Choose the desired field definition file and click **Open**.

You can import files with the “lanrevcfdef” file name extension that have previously been exported from Absolute Manage.

Absolute Manage imports the field definitions from the specified file. If there are any conflicts between the imported fields and existing fields, Absolute Manage informs you of the problem and offers several options to resolve it.

You can also drag the fields from the desktop into the **Server Center** window.

Manually edited information

Absolute Manage provides ten so-called client information fields on each managed computer. These are text fields in which you can manually store arbitrary information, enabling you to note information such as inventory numbers, assigned owners, or maintenance dates.

Information can be edited remotely (from Absolute Manage Admin) and optionally locally (by the user of the managed computer) as well. You can configure whether local access is possible; you can also set the names of the ten fields.

These procedures are described below in:

- **Using client information fields** (page 93)
- **Naming client information fields** (page 95)
- **Configuring local access to client information fields** (page 96)

Using client information fields

Information can be stored in client information fields in two ways:

- By the administrator, using Absolute Manage Admin.
- By the local user, using the Absolute Manage control panel. This access can be prevented, as described below in “Configuring local access to client information fields” on page 96.

Displaying the information is likewise possible for both the administrator and the local user. (It is not possible to prevent the local user from viewing client information fields’ contents.)

Editing client information fields

To edit client information fields remotely:

1. In any browser window, select the computers on which you want to enter information in the client information fields.

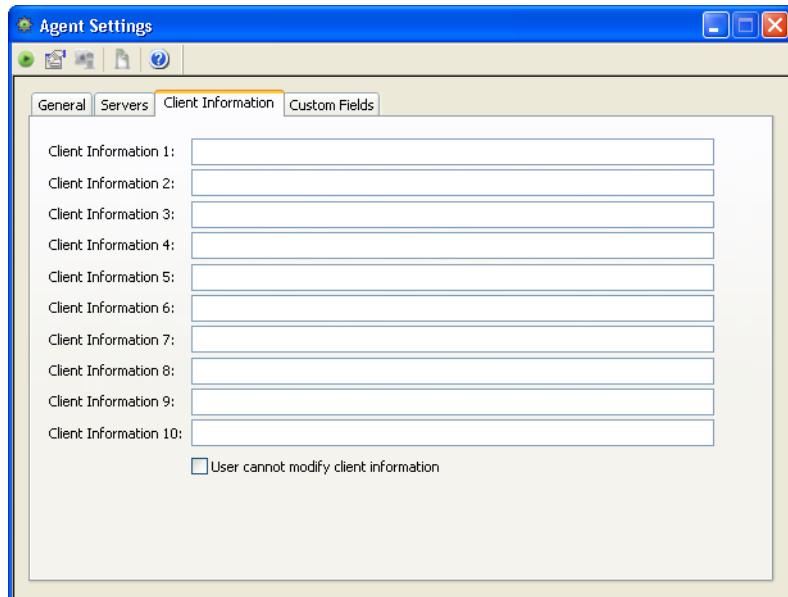
You can select one or more computers.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog opens.

3. Click the **Client Information** tab:



4. Make the desired changes to the fields' contents.

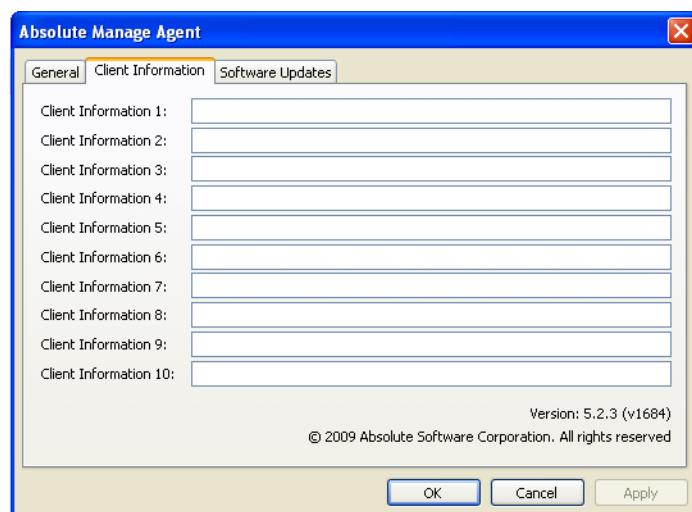
5. Click **Execute**.

The fields' contents are set on all selected computers.

Editing client information fields locally on the administered computer requires the fields to be unlocked for local modification (as described in "Configuring local access to client information fields" on page 96).

To edit client information fields locally:

1. On the administered computer, open the **Absolute Manage Agent** control panel.
2. In the panel, click the **Client Information** tab.



3. Make the desired changes to the fields' contents.
4. Click **OK** to close the control panel.

Displaying the contents of client information fields

The contents of client information fields can be displayed in various ways:

- To display the fields' contents for multiple computers in Absolute Manage Admin, put the information items for the desired fields into any browser window. These information items are always named the same as the fields themselves and are found in the **Agent Information > Agent Settings** category of information items.
- To display the fields' contents for a single computer in Absolute Manage Admin, select that computer in any browser window, open the **Agent Settings** dialog as described above in **Editing client information fields**.
- To display the fields' contents for a single computer on that computer, open the **Absolute Manage Agent** control panel on that computer, as described above in **Editing client information fields**.

Naming client information fields

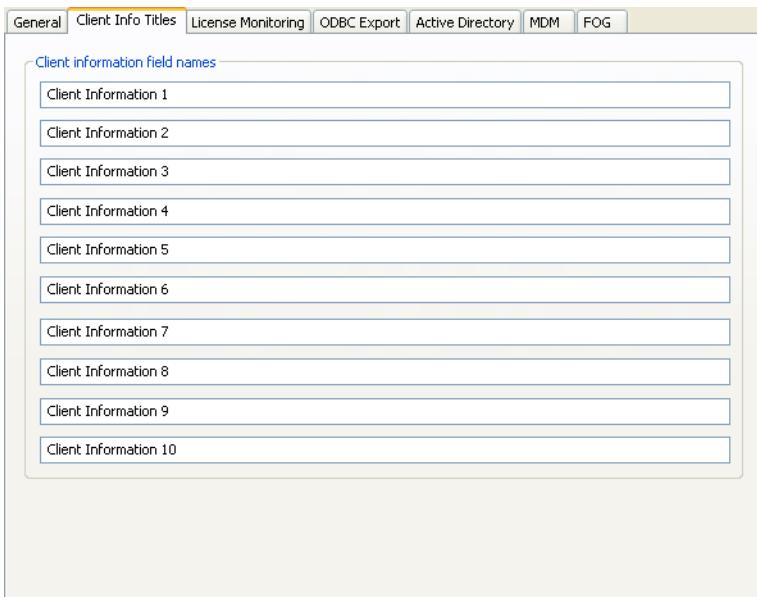
By default, client information fields have generic names. There is no need to rename them to use them; however, you may want to do so to indicate the kind of information that is stored in a field.

To set the name of a client information field:

1. In the **Server Center** window, click the **Server > Server Settings** category.

The **Server Settings** dialog is displayed.

2. Click the **Client Info Titles** tab:



3. Enter the desired names for the ten fields.
4. Click **OK**.

The new names are sent to the server; all agents connected to this server now use these field names.

NOTE

If multiple inventory servers are specified for an agent, it uses the client info titles of the first one in the list in the **Servers** pane of the **Agent Settings** dialog. (For more details, see “Servers” on page 289.)

The information items that display the fields’ contents are also renamed, as noted in “Client Information 1 … 10” on page 536.

Configuring local access to client information fields

By default, local users of administered computers can edit the contents of client information fields through the **Absolute Manage Agent** control panel. If desired, you can prevent them from doing so.

To enable or disable local editing of client information fields:

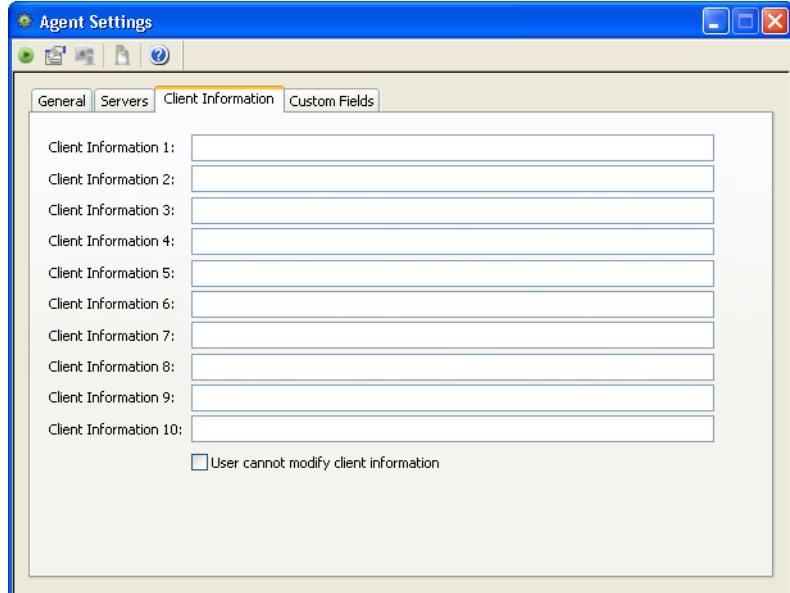
1. In any browser window, select the computers that you want to configure.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog opens.

3. Click the **Client Information** tab:



4. To prevent local users from editing client information fields, check the **User cannot modify client information** option.

To allow local users to edit the fields, uncheck the option.

5. Click **Execute**.

The fields' are locked or unlocked as specified on all selected computers.

Storing and exporting information

The information that Absolute Manage gathers from the managed clients is automatically stored on the Absolute Manage Server without requiring any manual interaction or configuration. (There are, indeed, no configuration options for data storage.)

The gathered software can be made available to other tools by exporting it. There are three principal ways of doing so:

- Manual export to XML, HTML, or text files. This is described in "XML, HTML, and text export" on page 98.
- Periodic automatic export to an ODBC database, as described in "ODBC export" on page 98.
- Periodic automatic export to Microsoft System Management Server (SMS). This requires the Absolute Manage SMS Integration add-on module and is described in that module's documentation.

Absolute Manage also offers backup and maintenance functions:

- Automated database backup and maintenance. This is described in “Configuring database backup and maintenance” on page 100.
- Deleting unneeded information from the server. This is described in “Deleting information from the server” on page 102.

XML, HTML, and text export

You can export information that is being displayed in an Absolute Manage window to a range of common exchange formats:

- HTML
- Comma-separated text (CSV) in two variants
- Tab-delimited text
- XML (using a custom structure)

The process is the same in each case:

1. Make sure that the information you want to export is displayed in a window.

This includes both the desired records (computer, files, etc.) and the desired columns.

2. From the **File** menu, choose **Export**.

The operating system's Save dialog opens.

3. From the dialog's **File Format** pop-up menu, choose the desired format. Specify a name and location for the export file and click **Save**.

The data from the window is exported in the specified format to the specified location.

ODBC export

Absolute Manage Server can automatically export data from its database at specified intervals over an ODBC connection, allowing the target database to be used for a range of applications such as logging, backup, or reporting.

Preparing for ODBC export

To be able to use Absolute Manage's ODBC export feature, you need:

- a database that can be accessed via ODBC
- a compatible ODBC driver
- an account in the database that can create tables and insert data

Please see the documentation of the database or the ODBC driver for details on installing and configuring this software.

NOTE While Absolute Manage is expected to be compatible with a wide range of ODBC software, it has currently only been tested with MySQL and the MyODBC driver. We cannot guarantee compatibility with other databases and drivers.

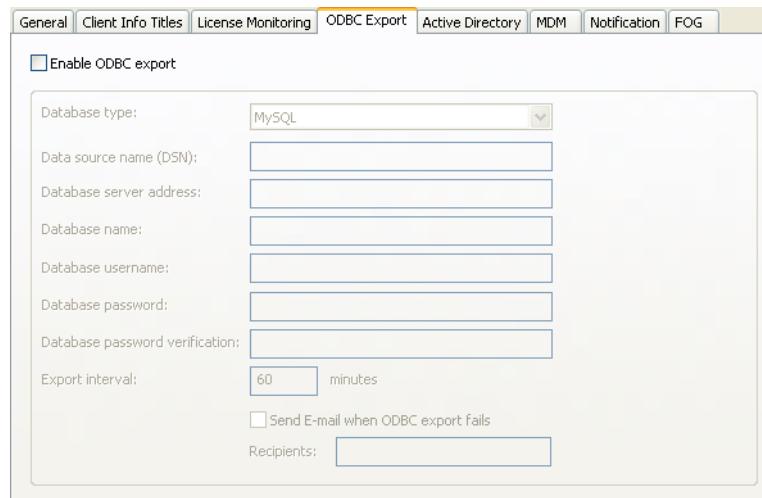
Setting up ODBC export

To set up Absolute Manage for ODBC support, you configure the required access information and desired update interval on the Absolute Manage server:

1. In the **Server Center** window, click the **Server > Server Settings** category.

The **Server Settings** dialog is displayed.

2. Click the dialog's **ODBC Connection** tab.



3. Check **Enable ODBC support** and fill in the fields:

- **Database type:** The kind of database management system connected via ODBC.
- **Data source name (DSN):** The name of the data source as defined in ODBC.
- **Database server address:** The IP address or DNS name of the database server.
- **Database name:** The name of the database on the server in which the information from Absolute Manage is to be stored.
- **Database username:** The database account that Absolute Manage is to use to store the data.
- **Database password:** The password for the database user account.

- **Database password verification:** Repeat the password here to guard against typos.
- **Export interval:** The desired interval in which Absolute Manage export data to the database.
- **Send e-mail when ODBC export fails:** Check this option and enter an e-mail address in the Recipient field to have Absolute Manage send out automatic notifications when the ODBC export could not be completed. You can enter multiple addresses separated by commas.

Note: Apart from the data source name, you can leave all fields empty if the corresponding information is specified in the data source.

4. Click **OK**.

The settings are stored on the server; the export is initiated immediately and in the specified interval from then on.

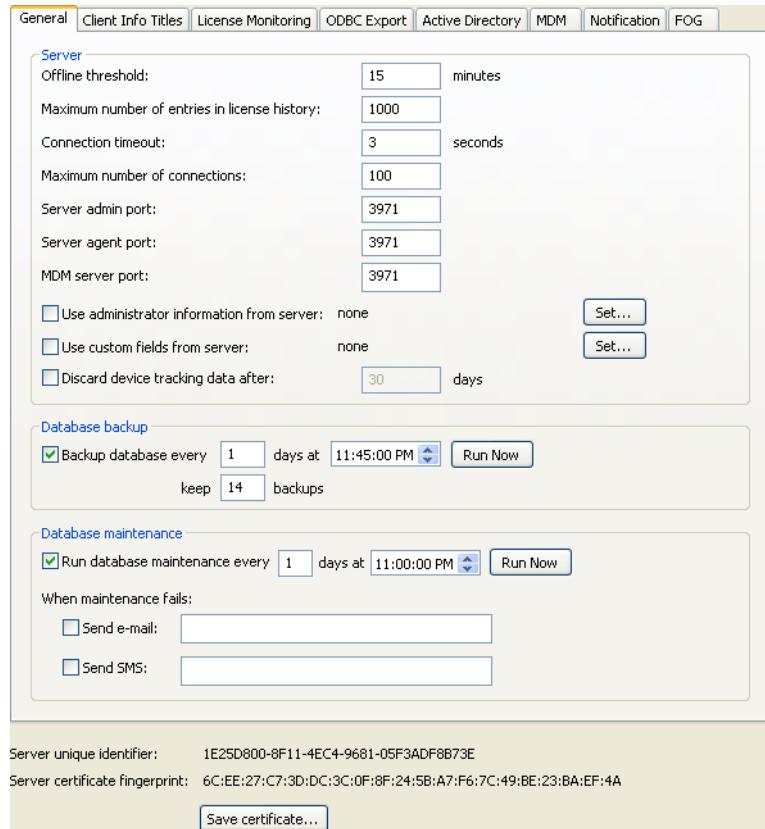
Configuring database backup and maintenance

Absolute Manage lets you configure the database's backup and maintenance options.

To configure the options:

1. In the **Server Center** window, click the **Server > Server Settings** category.

The **Server Settings** dialog is displayed.



2. If you want Absolute Manage to automatically perform database maintenance, check the **Run database maintenance** option and specify the desired interval and time of day.

Database maintenance involves eliminating empty blocks from the database file on disk and performing a full consistency check on the database.

3. If you want Absolute Manage to perform automatic database backups, check the **Backup database** option and specify the desired interval, time of day, and number of backup generations to keep.

The Absolute Manage Server database is located in the **/Library/Application Support/LANrev Server** folder on Mac OS X-based servers and in **C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server** on Windows.

Backups are located in the same folders, in subfolders with the suffix **.dbbackup**, **.dbbackup1**, **.dbbackup2**, etc. for the successive backup generations.

4. If you want to immediately perform the database maintenance or create a database backup, click the appropriate **Run Now** button.

- Choose **Save Server Settings** from the **Server** menu.

Absolute Manage performs the specified operations on the server until the settings are edited again.

Deleting information from the server

Occasionally, you may have collected a significant amount of information that is no longer needed. To prevent this information from taking up space and processing power on the server, you can delete it manually.

Deleting entire records

To delete unneeded records from the Absolute Manage Server:

- In any browser window, select the records that you want to remove from the server.
- Right-click the records and choose **Remove from Server** from the context menu.

A confirmation alert is displayed.

- Click **OK**.

Absolute Manage removes all selected records (along with any associated data, such as inventory information for computer records) from the server. This operation cannot be undone; however, you may recreate the records, e.g., by performing a file search to recreate file records.

Deleting associated data for a record

To delete unneeded information related to computer records:

- In any browser window, select computers for which you want to remove related data.

Note: For information on specifying groups as targets, see "Targets" on page 286.

- Right-click the records and choose **Remove Inventory Data** from the context menu.

The **Remove Inventory Data** dialog is displayed:



3. Check all the types of information that you would like to remove and click OK.

Absolute Manage removes the specified types of associated data for all selected records from the server. This operation cannot be undone; however, you can gather the deleted data anew using the **Gather Inventory Information** command.

Displaying information

When information on administered computers has been found by the Absolute Manage Agents and stored on the Absolute Manage Server, it can be displayed in the administrator application. This is done in browser windows.

Browser windows are, basically, tables in which each row represents a computer or other monitored object (file, font, process, etc.), and each column an information item, i.e., a database table column.

They also let you search for, filter, and sort objects, and provide a way to display an overview of information on a single computer.

NOTE Details on the elements of browser windows are found in “Browser windows” on page 365.

Details on displaying information are available in:

- “Opening and configuring browser windows” on page 103
- “Displaying an overview of a single computer” on page 105
- “Controlling information display from a URL” on page 106
- “Searching, filtering, and sorting” on page 109

Opening and configuring browser windows

Opening a new browser window

To create a new browser window, choose **New** from the **File** menu.

Configuring the sidebar

You can add categories, groups, and smart groups to the sidebar as well as rename and delete them:

- To add a category, choose **New Category** from the sidebar’s context menu.
To rename a category, select it and choose **Rename Category** from the sidebar’s context menu.
To delete a category, select it and choose **Remove Category** from the sidebar’s context menu.
- Adding groups is described in “Creating groups” on page 109. Renaming groups is described in “Editing groups” on page 112. Removing groups is described in “Deleting groups” on page 112.

Configuring a browser window

You configure browser windows by adding, rearranging and removing information items:

- To add an information item, drag it from the **Information Items** window into the table area – this adds the column at the right-hand side of the table – or to the Columns sidebar, where you can insert it at the desired location.
You can also drag columns between Columns sidebars of different browser windows or copy and paste them.
- To rearrange columns, drag their titles in the table area or in the Columns sidebar to the desired location.
To resize columns, drag the right-hand borders in the table title area.
- To remove a column, select its title in the Columns sidebar and click the **Remove** button.

NOTE

If the Columns sidebar is not displayed, you can open it by choosing **Configure Columns** from the **View** menu.

No particular action is required from you to display data in the columns you have added; this is done automatically as long as the data is available on the Absolute Manage Server. Note, however, that some types of data are not collected automatically and must be requested manually, as described in “Gathering information” on page 70.

You can rearrange the groups in the sidebars of most browser windows by dragging them. You can also drag custom smart groups – but not built-in ones such as **Macs only** – between browser windows and the **Server Center** window.

Saving configured browser windows

When you have configured a browser window, you can save it for future reuse using the **Save As** command from the **File** menu. Doing so saves the structure of the window; it does not save the actual data, which are always dynamically loaded from the Absolute Manage Server.

Working with tabs

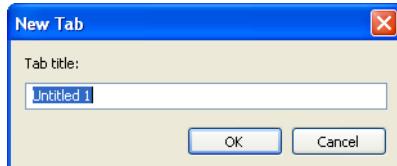
Each Absolute Manage browser window can contain multiple tabs. Absolute Manage tabs are analogous to Web browser tabs: The content of each of them is independent of the others’; the sizes of all tabs in one window are the same; all tabs in one window always move together on the screen.

Adding a tab to a window

To add a new tab to a browser window:

1. From the **File** menu, choose **New Tab**.

The **New Tab** dialog is displayed:



2. Enter the desired name and click **OK**.

The new tab appears in the window.

NOTE Tabs can only be added to browser windows, not to other types of windows.

Renaming a tab

To rename a tab:

1. From the **File** menu, choose **Rename Tab**.

The **Rename Tab** dialog is displayed, which looks similar to the **New Tab** dialog shown above.

2. Edit the name as desired and click **OK**.

The name of the tab is changed.

Closing tabs

To close a tab, either click its close icon  or make it active and choose **Close Tab** from the **File** menu.

Displaying an overview of a single computer

While browser windows normally display a range of information items for a large number of computers, it can also display a complete overview of a single computer.

To display an overview:

1. In the **Groups & Computers** sidebar of any browser window, open a group that contains the desired computer and click on the computer.

A selection of important information items is displayed:



2. To see more detailed information, open the computer in the sidebar to display a range of information item categories. Click the desired category to display the respective information.
3. To revert to the normal tabular display, click on any group in the sidebar.

NOTE

If the “**Double-clicking a computer**” option in the Settings dialog is set to “**Display detail view**”, you can also double-click a computer to view the details.

Configuring the individual computer display

You can configure all displays for individual computer information:

- Add information items to a particular display pane by dragging them there from the **Information Items** window.
- Rearrange information items by dragging them to the desired location in the list.
- Remove information items by selecting them and pressing the Delete key.

Any configuration changes you make in these display panes affect all other computers with the same operating system platform (Windows or Mac OS X).

Saving the browser window (as described in “Saving configured browser windows” on page 104) also saves these configuration changes.

Controlling information display from a URL

In addition to the standard selection of information to display via the graphical user interface, Absolute Manage also lets you specify computers to display via a URL.

You can construct a URL to display information on a particular computer in Absolute Manage using this syntax: `lanrevadmin://showagent?<field>=<value>`.

- `<field>` is the information item by which you want to find the desired computer. It can have any of these values (the value being the first word, with the full name of the information item added in parentheses):

- agentip (**Agent Active IP**)
- agentserial (**Agent Serial Number**)
- computername (**Computer Name**)
- agentname (**Agent Name**)
- computeralias (**Computer Alias**)
- primarymacaddress (**Primary MAC Address**)
- adcomputername (**AD Computer Name**)
- clientinfo1 (**Client Information 1 ... 10**)
- clientinfo2 (**Client Information 1 ... 10**)
- clientinfo3 (**Client Information 1 ... 10**)
- clientinfo4 (**Client Information 1 ... 10**)
- clientinfo5 (**Client Information 1 ... 10**)
- clientinfo6 (**Client Information 1 ... 10**)
- clientinfo7 (**Client Information 1 ... 10**)
- clientinfo8 (**Client Information 1 ... 10**)
- clientinfo9 (**Client Information 1 ... 10**)
- clientinfo10 (**Client Information 1 ... 10**)
- computerservicetag (**Computer Service Tag**)
- currentuseraccount (**Current User Account**)
- currentusername (**Current User Name**)
- customagentname (**Custom Agent Name**)
- mainboardassettag (**Mainboard Asset Tag**)
- mainboardserial (**Mainboard Serial Number**)
- osproductid (**OS Product ID**)
- osserial (**OS Serial Number**)
- securityid (**Security Identifier**)
- systemenclosuretag (**System Enclosure Asset Tag**)
- systemenclosureserial (**System Enclosure Serial Number**)

- <value> is the value to search for.

Calling the URL causes Absolute Manage to search the specified field for the specified value and display a single-computer overview of the found computer.

For example, the URL `lanrevadmin://showagent?computername=My%20Computer` displays the computer with the name "My Computer" in the single-computer overview in Absolute Manage Admin.

Absolute Manage Admin must be installed on the computer on which the URL is called. If it is not running, it is started automatically.

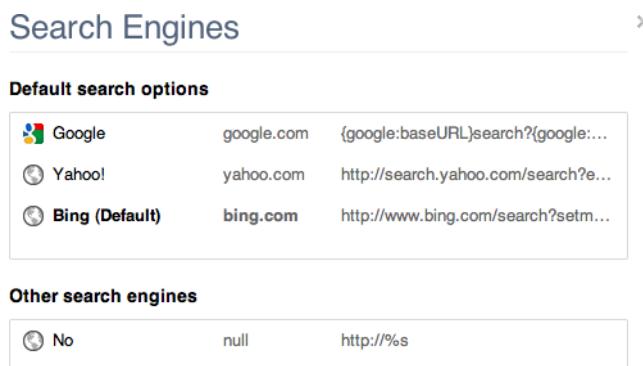
NOTE

With some of the available fields, there may be more than one matching computer. If this happens, Absolute Manage displays the first computer matching the specified criteria.

Setting up Google Chrome to support lanrevadmin:// URLs

In its default setup, Google Chrome does not understand the lanrevadmin:// syntax. To make it compatible with this syntax:

1. In Google Chrome, right-click the address bar and choose **Edit Search Engines**.
The **Search Engines** page is displayed.
2. In the **Other search engines** section, specify a new search engine with these values:
 - **Add a new search engine:** No
 - **Keyword:** null
 - **URL with %s in place of query:** http://%s



3. Press return and close the page.
4. Quit Chrome.
5. Open the “Local State” file with a text editor.

This file is found in different locations, depending on the operating system:

- Mac OS X: /Library/Application Support/Google/Chrome/
- Windows XP or Windows Server 2003: C:\Documents and Settings\<username>\Local Settings\Application Data\Google\Chrome\User Data\
- Windows Vista, Windows Server 2008, or Windows 7: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\

For information on where to find the “Local State” file on other platforms, please see the Chrome help.

6. In the “protocol_handler” section, “excluded_schemes” subsection, add this line (including quotes and comma):

```
"lanrevadmin": false,
```

7. Save and close the file.

You can now use lanrevadmin:// URLs in Chrome like in other browsers.

Searching, filtering, and sorting

Various methods are available to focus on the currently interesting part of the information displayed in browser windows:

- You can search for specific text in a particular column or the entire browser window.
- You can filter computers by creating groups, either according to specified criteria or manually, and restricting the display to just one group.
- You can sort the browser window on any number of columns.

All these methods can be combined to present the information in the browser window.

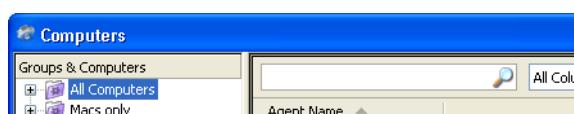
They are described below in:

- “Searching in browser windows” on page 109
- “Creating groups” on page 109
- “Sorting browser windows” on page 113

Searching in browser windows

To search for specific text in browser windows:

1. Enter the text in the search field in the toolbar:



2. Press Enter.

Absolute Manage searches the currently displayed records, hiding all that do not contain the text in the information items in the browser window.

By default, all columns are searched. If you want to search just one particular column, choose that column from the pop-up menu before pressing Enter.

Creating groups

Groups in browser windows are collections of administered computers. They allow you to view a subset of all managed computers with just one click.

There are two kinds of groups:

- (Standard) groups are much like file folders: To include a computer in a group, you add it manually; to take it out again, you manually remove it.

- Smart groups are not so much collections of specific computers but descriptions of what kind of computers you want to include in a group. They are defined by selection criteria and at any time dynamically display those computers that meet the criteria in that instant. Inclusion and exclusion of computers is automatic. For example, you could define a smart group to include all computers with less than 512 MB of memory. When a computer's RAM is updated to more than that amount, Absolute Manage automatically removes it from that group. In standard browser windows, there are three predefined smart groups – for all computers, Mac OS X computers, and Windows computers. In specialized browser windows, e.g., the **Server Center** window, additional or different smart groups may be predefined.

You can use both kinds of groups as command targets by dragging them into the target area of the respective command window. When a command is saved for later execution, the target computers are the members of the groups at execution time, not the computers that were members of the groups when the command was saved.

When smart groups are command targets for repeating commands, Absolute Manage re-evaluates for each repetition which computers belong to the group. In other words, a computer that was a command target because it met the group criteria may not be a target in the next execution because it no longer meets the criteria, and vice versa.

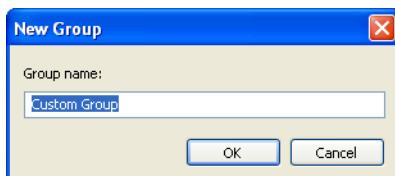
NOTE For performance reasons, the group membership is evaluated periodically, as opposed to constantly. Therefore, computers may fail to be included as a command target if they start meeting the smart group criteria very shortly before the command execution, or they may be included even though they started failing to meet the criteria immediately before command execution.

Creating a (standard) group

To create a manually maintained group:

1. From the context menu in the **Groups and Computers** sidebar in the browser window, choose **New Group**.

The **New Group** dialog opens:



2. Enter the name of the new group and click **OK**.

3. To add computers to the group, drag them from the table (not from other groups in the sidebar) into the group.
4. To remove computers from the group, display the group, right-click the computer, and choose **Remove from Group** from the context menu.

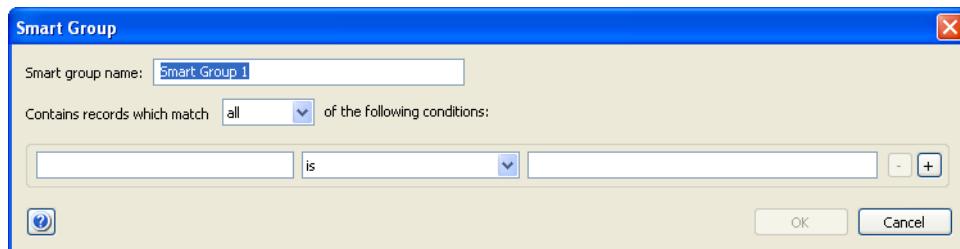
Note: Computers cannot be individually removed from smart groups.

Creating a smart group

To create a smart group:

1. From the context menu in the **Groups and Computers** sidebar in the browser window, choose **New Smart Group**.

The **Smart Group** dialog opens:



2. Enter the name for the new group and define the conditions that computers must meet to be included in the group.

To define a condition, specify an information item in the left-hand text field – you can use any information item listed in the **Information Items** window – choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

With the + and – buttons, you can add and remove conditions.

3. If you have specified more than one condition, specify through the upper pop-up menu whether computers must meet one or all of the conditions.
4. Click **OK**.

Creating smart groups, alternate technique

You can also create smart groups by example. To do so:

1. In any browser window, select records showing the criteria that you want to use for the smart group.

For example, to create a group with all computers with dual-core processors, add the relevant information item – **Cores per**

Processor – to a browser window, if it is not already present. Then, select a computer with the desired value in this column, i.e., 2.

2. Right-click the column in the browser window that you want to use for specifying the smart group and choose **New Smart Group from “<information item>”** from the context menu (where **<information item>** is replaced with the title of the column in which you clicked).

For example, for the smart group for all dual-core processor based computers, click in the **Cores per Processor** column.

3. The **Smart Group** dialog opens with conditions based on your selections already predefined. Proceed as described in the procedure above.

In particular, you can edit the predefined selection conditions, add new ones, or delete them.

Editing groups

To rename a group, select it and choose **Rename Group** from the context menu in the **Groups and Computers** sidebar.

To edit the definition of a smart group, select it and choose **Edit Smart Group** from the context menu in the **Groups and Computers** sidebar.

Adding computers to a standard group and removing them is described above in “Creating a (standard) group” on page 110.

Deleting groups

To delete a group, select it and choose **Remove Group** from the context menu in the **Groups and Computers** sidebar.

Saving group definitions

Groups defined in a browser window are automatically saved when the window is saved. Saving browser windows is described in “Saving configured browser windows” on page 104.

Transferring groups

Groups can be exported and imported by means of the **Export Groups** and **Import Groups** commands.

Export Groups stores all groups and smart groups (but not special categories such as **License Specifications** from the **Server Center** window) from the frontmost window in one file.

Import Groups inserts all groups from the selected file into the frontmost window. Existing groups remain unaffected.

You can directly transfer groups between windows by dragging and dropping them.

Exporting groups

To export selected groups and smart groups from the frontmost window:

1. From the **File** menu, choose **Export Groups**.

A standard Save dialog is displayed.

2. Give the file a name, choose a storage location, and click **Save**.

The definitions of the selected groups and smart groups (but not special categories such as **License Specifications** from the **Server Center** window) from the frontmost window are saved in the file.

Sorting browser windows

Browser windows can be sorted on as many columns as desired.

Sorting by a column

To sort the window by a column, double-click the column's title. The column is made an additional sorting column:

- If this is the first sorting column, the records are sorted by this column.
- If there already are sorting columns, the double-clicked column is added as the next-lower sorting column. This means that all records that sort the same according to the existing columns are sorted by the newly added column.

For example, when sorting by the first column only results in:

1 3 4
1 2 4
1 3 1
2 1 3

Additionally sorting by the second column creates:

1 2 4
1 3 4
1 3 1
2 1 3

A sorting column is indicated by a small triangle in its title (▲).

Reversing the sort order

To reverse the sort order for a column, double-click the column's title again. (The column must already be a sorting column.)

The triangular indicators show the current sort order: If the triangle points upwards, smaller values come first, if it points downwards, larger values come first.

Removing sorting

If you want to stop sorting the table by a particular column, double-click its title with the Ctrl key held down.

You can use Absolute Manage to control administered computers in several ways.

On a basic level, you can restart them, shut them down, wake them up, or put them to sleep, as well as send them messages.

You can also execute various files that are either present locally on the administered computers or on your workstation, and you can terminate processes.

This is discussed in detail in:

- “Sending messages” on page 115
- “Restarting, shutting down, and sleep” on page 116
- “Remotely controlling computers” on page 122
- “Controlling Time Machine” on page 125
- “Tracking computers” on page 125
- “Executing files from your computer” on page 129
- “Executing local files” on page 132
- “Terminating processes” on page 133
- “Working with services” on page 134
- “Editing the registry” on page 136
- “Environment variables” on page 137

Sending messages

You can send messages to administered computers, e.g., to advise employees of upcoming administrative actions.

NOTE While there is no dedicated facility for letting users answer to your messages, you can add a **Cancel** button to message dialogs. Because the agents report which button a user has pressed to dismiss the dialog and this information is noted in the command history, you can use this function to ask simple yes/no questions.

NOTE Sending messages to iOS devices requires a different process, which is described in “Sending a message to mobile devices” on page 140.

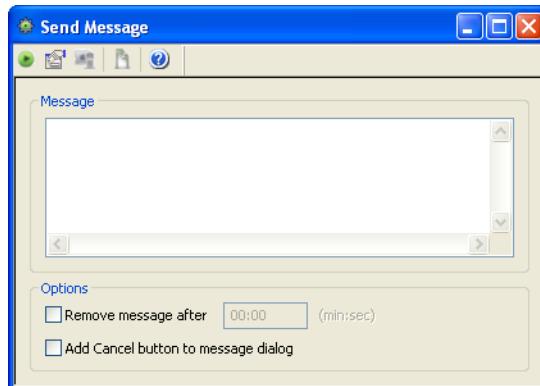
To send a message to administered computers:

1. In any browser window, select the computers to which you want to send the message.

Note: For information on specifying groups as targets, see “Targets” on page 286.

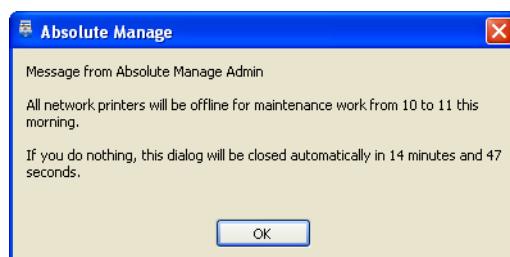
2. From the **Commands** menu, choose **Send Message**.

The **Send Message** dialog opens:



3. Enter the desired message.
4. Set the message options:
 - When you want to make sure that the dialog does not remain on screen indefinitely when there is no user present, specify an interval after which the message is closed automatically.
The dialog is closed as if the user had clicked **OK**. (The timeout is, however, noted in the log.)
 - When you want the users to be able to express non-acceptance, add a **Cancel** button. (There is always an **OK** button.)
5. Click **Execute**.

The message is displayed on the target computers:



If a user dismisses the dialog by clicking on the **Cancel** button (if any), you can see this in the **Command Error Info** column in the **Commands** window.

Restarting, shutting down, and sleep

Absolute Manage can control the operating state of administered computers, i.e., it can restart them, shut them down, put them to sleep, or wake them up.

The process for these commands is very similar; only waking computers up differs slightly.

Using the **Power Management Settings** command, you can also schedule these events, either for a fixed time or for after a certain period of inactivity. This is described in “Scheduling power management events” on page 118.

Restarting, shutting down, and putting to sleep

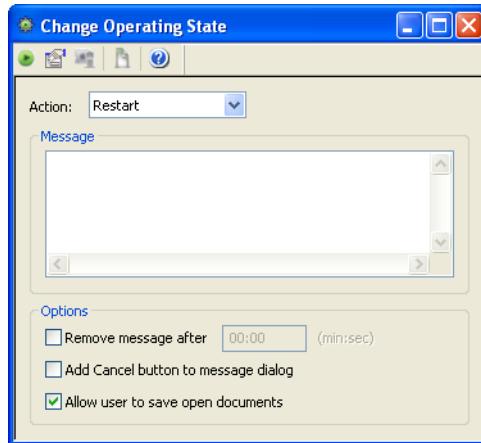
To restart administered computers, shut them down, or put them to sleep:

1. In any browser window, select the computers that you want to control.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Change Operating State**.

The **Change Operating State** dialog opens:



3. Choose the desired action from the pop-up menu.

Note: When you try to put to sleep a Windows computer, Absolute Manage first tries to hibernate it. If that is not supported, it tries to put it into stand-by mode. If the computer does not support this mode either, the command fails with an error log entry.

4. If you want the user to be able to save any changes to open documents, check **Allow user to save open documents**.

If this option is unchecked, restarts and shutdowns are ‘hard’, i.e., any running processes are killed immediately.

5. If desired, enter a message that warns the users. The relevant options are described in “Sending messages” on page 115.

6. Click **Execute**.

Waking up computers

Administered computers can be woken up only if 'Wake on LAN' is enabled on them. How this function is enabled differs between systems. Depending on your system, you will find the required information in the documentation of the operating system, of the computer or motherboard, or of the LAN card.

NOTE Usually, you find the required setting in the **Energy Saver** control panel on Mac OS X computers or the network adapter's hardware properties on Windows systems.

Waking up computers is possible across subnets as long as an Absolute Manage Server or Absolute Manage Agent is running (active) in the target subnet.

To wake up administered computers:

1. In any browser window, select the computers that you want to control.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Wake Up**.

The **Wake Up** dialog opens. It contains no command-specific options.

3. Click **Execute**.

Scheduling power management events

You can set schedules for all power management events. Events can be scheduled to occur at specific times or after a certain period of inactivity.

A report on the effects of the power management is available, as described in "Displaying a power usage report" on page 120.

Setting up a new schedule

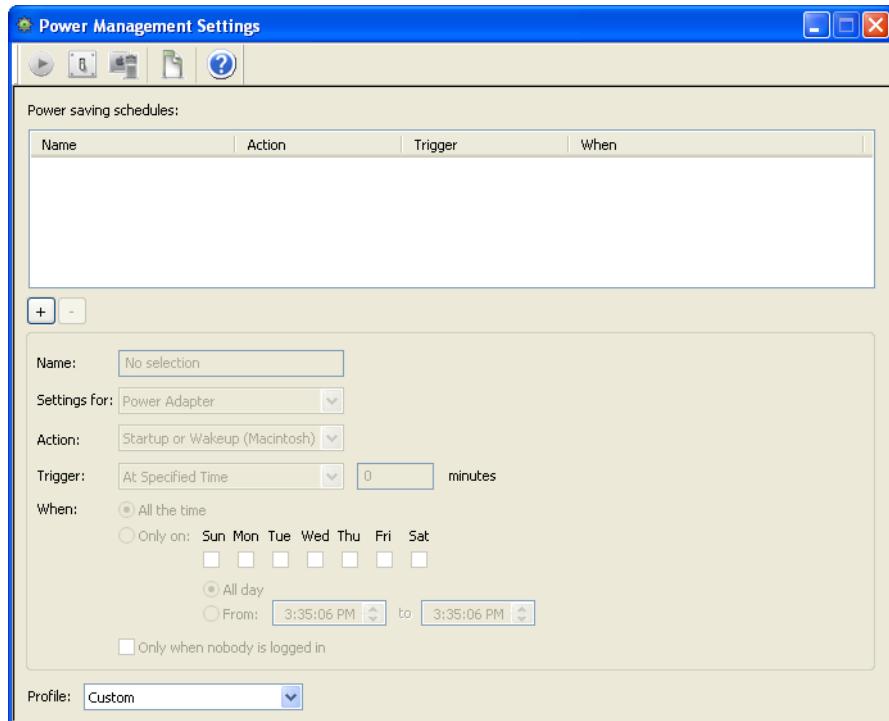
To assign a new schedule to administered computers:

1. In any browser window, select the computers on which you want to set up the schedule.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Power Management Settings**.

The **Power Management Settings** dialog opens.



3. Click the **+** button to create a new schedule.
4. Enter a name for the new schedule in the **Name** field.
5. From the **Settings for** pop-up menu, choose the power modes to which the schedule applies.
6. From the **Action** pop-up menu, choose the event that is to occur when the schedule's trigger fires.

For details on the available options, see “Power Management Settings” on page 293.

7. From the **Trigger** pop-up menu, choose the trigger that initiates the chosen action.

You can choose between a specific time or a certain period of inactivity.

When you have chosen **After Inactivity Of**, specify the interval in minutes.

8. Use the **When** checkboxes and radio buttons to specify the time of the day and days of the week when the schedule is active.

The specified action can occur only on the chosen dates and hours of the day.

9. If desired, add more schedules as described in step 3 through step 8 or delete schedules as described below.

10. Click **Execute**.

All schedules listed in the command dialog are applied to all specified target computers. If any schedules were active on the computers before, they are removed.

Assigning existing schedules

Perform the procedure described in **Setting up a new schedule**, above, but skip step 3 through step 8.

Alternately, you can choose from the **Profile** pop-up menu a profile containing the desired schedules, optionally modify them, and execute the command.

Deleting a schedule

To delete an existing schedule, select it in the **Power saving schedules** list and click the – button.

To remove all schedules from a computer, empty the list and execute the **Power Management Settings** command.

Saving schedules

You can save schedules as profiles that can be easily recalled to be applied to target computers.

To save all schedules currently listed in the **Power saving schedules** list as a profile, choose **Save As** from the **Profile** pop-up menu and enter a name for the profile. The new profile is added to the **Profile** pop-up menu.

To rename a profile, choose it from the **Profile** pop-up menu. Then choose **Rename** from the **Profile** pop-up menu and enter the new name.

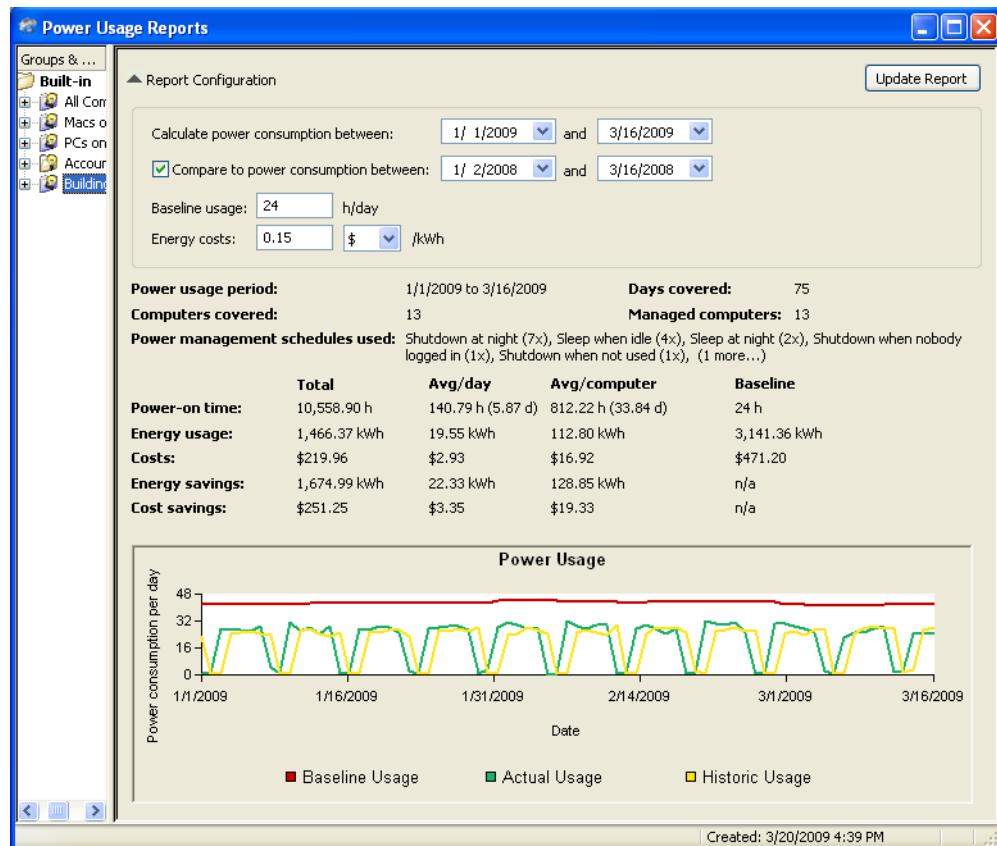
To delete a profile, choose it from the **Profile** pop-up menu. Then choose **Delete** from the **Profile** pop-up menu.

Displaying a power usage report

To display a report on the savings of power and money that have been achieved by using the power management schedules:

1. From the **Window** menu, choose **Power Usage Reports**.

The **Power Usage Reports** window opens:



2. In the window's sidebar, select the computer group on which you want to create a report.
3. Enter the desired report period in the **Calculate power consumption between** fields.
4. Enter the time the computers would have been running without power management schedules in the **Baseline usage** field.

This is the average number of hours that you think a managed computer would have been running during the report period.

5. Enter the amount of money you pay for power in the **Energy costs** field.
6. Click the **Update Report** button.

The actual and baseline values and savings are displayed in the report window and visualized as a graph. Details regarding the displayed information is available in "Power Usage Reports" on page 355.

NOTE The power consumption of the various devices is set in the **Power Consumption** settings pane.

Remotely controlling computers

Absolute Manage lets you view and control the screens of client computers using a wide variety of screen sharing software. All that is required to use this feature is that a controlling application is installed on your computer and a compatible client is available on the target computer.

Supported applications

Absolute Manage supports these screen sharing applications:

- Apple Remote Desktop 3 (guest and host: Mac only)
- DameWare (guest and host: PC only)
- Mac OS X Screen Sharing (guest: any Mac or PC with a VNC client; host: Mac OS X 10.5 and later only)
- MS Remote Assistance (guest and host: PC only)
- PC Anywhere (guest and host: PC only)
- Remote Desktop:
 - CoRD (guest: Mac only; host: PC only)
 - MS Remote Desktop (guest: Mac or PC; host: PC only)
- SSH (guest and host: Mac only)
- Timbuktu (guest and host: Mac or PC)
- Timbuktu secure (guest and host: Mac only)
- VNC:
 - Absolute Remote (guest and host: Mac or PC)
 - Chicken of the VNC (guest: Mac only; host: Mac or PC)
 - JollysFastVNC (guest: Mac only; host: Mac or PC)
 - Real VNC (guest: PC only; host: Mac or PC)
 - Tight VNC (guest: PC only; host: Mac or PC)
 - Ultra VNC (guest: PC only; host: Mac or PC)

Note: VNC is cross-platform; you can combine any of the above VNC implementations as guest and host applications.

NOTE

"Guest" in the above list refers to the platforms on which the software runs as an observer, "host" indicates the platforms that can be observed. For example, using MS Remote Desktop, you can observe or control a PC from a Mac or a PC.

Setting up remote control

To set up initiating remote control from within Absolute Manage:

1. If you want to use an application other than Absolute Remote, install the desired screen sharing software on your administrator workstation.

Absolute Remote is installed automatically as part of Absolute Manage Admin. You can install multiple supported applications.

2. Install compatible client software on all intended target computers if necessary.

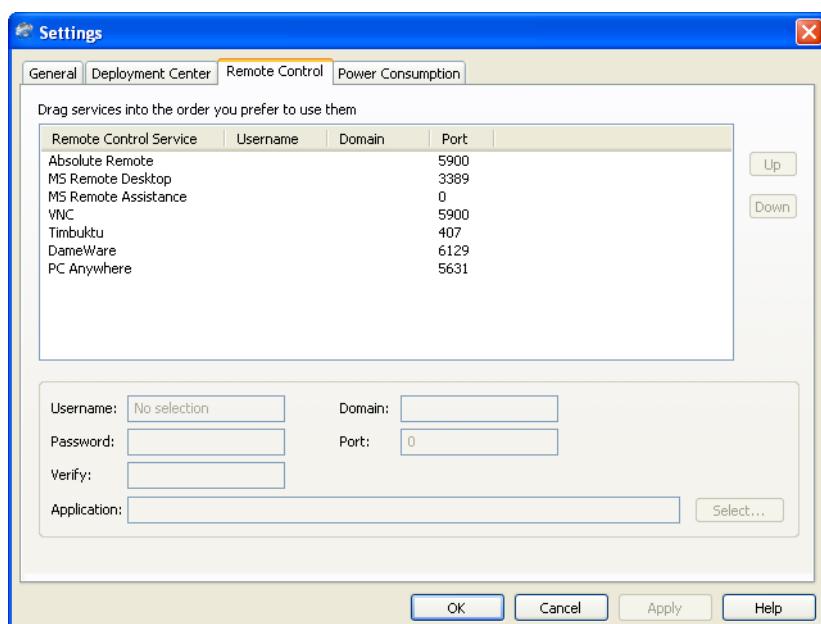
You can use Absolute Manage for doing so; see “Installing software” on page 200 for options.

Using Absolute Remote for viewing a client computer requires the function to be enabled on the client. This is done by checking the **Enable screen sharing** option in the **General** pane of the **Agent Settings** dialog.

In some cases, client software is already part of the operating system. For example, Mac OS X includes a VNC client.

Different client software can be installed on different computers. For example, you can use MS Remote Desktop on some and VNC on others. Absolute Manage automatically selects the correct client, as explained below.

3. To set your preferences, choose **Settings** from the **Edit** menu and click the **Remote Control** pane:



4. Arrange the various supported applications in the list in the order in which you would like to prefer to use them, either by dragging them or by clicking the **Up** and **Down** buttons.

Note: If a remote control connection to a given client is possible with more than one protocol, Absolute Manage uses the one that is highest in the list. For example, if your list looks like the one in the screenshot above and one client could be controlled through both Absolute Remote and MS Remote Desktop, Absolute Manage uses Absolute Remote.

5. For each protocol that you intend to use, select it in the list and enter the default username, password, domain, and port.

Some of this information cannot be specified for all protocols.

6. Choose the application on your computer that you want to use for the selected protocol by clicking the **Select** button.
7. Click **OK**.

Initiating remote control

To remotely control a client computer:

1. In any browser window, select the computer whose screen you want to share.
2. Right-click the selected computer and choose **Remote Control**.

Absolute Manage compiles a list of all suitable protocols (i.e., all supported protocols for which there is a control application on your computer and client software on the target) and chooses the one that is highest in the list of protocols in the **Settings** dialog's **Remote Control** pane.

If Absolute Manage is unable to find suitable client software on the target computer, it displays a dialog (similar to the one described above) in which you can manually specify a protocol and settings to use to connect to the client in question.

3. When a suitable connection setup has been found – either automatically or manually – Absolute Manage prompts the applicable control application on your computer to open a remote control connection to the target. You can then use the applications full capabilities to control the target computer.

Note: For details on the applications capabilities, please see their respective documentation.

Note: Some remote control applications do not accept passwords from other software. When using one of these applications, you need to re-enter the password in the application, even when you have already provided it in Absolute Manage.

Launching a remote control session from a URL

In addition to launching a remote control session via the graphical user interface, Absolute Manage also lets you do so via a URL.

This works just like displaying information for a computer via a URL, as described in "Controlling information display from a URL" on page 106, except that the command is "remotecontrolagent" instead of "showagent".

For example, the URL `lanrevadmin://remotecontrolagent?computername=My%20Computer` launches a remote control session with the computer named "My Computer" as the host.

Controlling Time Machine

Using Absolute Manage, you can control the Time Machine feature of client computers running Mac OS X 10.5 or later. You can:

- Initiate a backup
- Stop a backup
- Activate automatic Time Machine backups
- Deactivate automatic Time Machine backups

To control the operation of Time Machine:

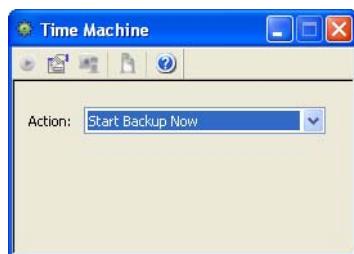
1. In any browser window, select the computers on which you want to control Time Machine.

Only target computers running Mac OS X 10.5 or later will be affected by this procedure.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Time Machine**.

The **Time Machine** dialog opens:



3. Choose the desired action from the pop-up menu.
4. Click **Execute**.

Tracking computers

You can use Absolute Manage to track the current locations of mobile computers.

This capability – called TheftTrack – is largely automatic; it requires minimal configuration and is thereafter available whenever needed.

For information on tracking the locations of mobile devices, see “Geotracking mobile devices” on page 182.

NOTE Absolute Manage’s computer tracking is not a comprehensive theft prevention or retrieval solution and should not be considered as such. (For example, thieves could circumvent it by reformatting the computer’s hard disk.) This feature can, however, be an important part of a larger comprehensive system that you set up.

NOTE Computer tracking can be set and altered only by administrators with the **Change Computer Tracking** right. See “New Administrator” on page 481 for details.

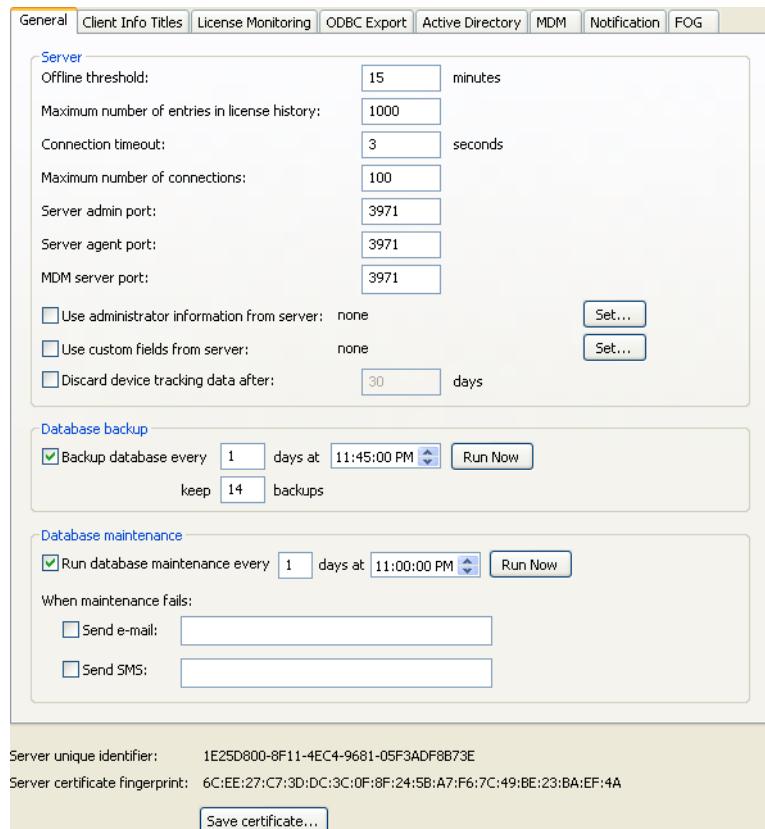
Setting up computer tracking

To set up computer tracking, you must make sure that at least one of your Absolute Manage Servers can be reached from the Internet. As most servers are usually secured behind a firewall, you will often have to take special steps to make this possible.

To set up a server for access from the Internet:

1. In the **Server Center** window, click the **Server > Server Settings** category.

The server settings are displayed in the main part of the window.



*Note: The Server Setting command is available only to administrators with the **Change Server Settings** right. See “New Administrator” on page 481 for details.*

2. In the dialog's **General** tab, set the agent port to a different number than the admin port.
This separation of the ports is necessary so that the admin port can remain inaccessible from the Internet.
3. If you want to keep the data generated while tracking computers for only a limited time, check the **Discard computer tracking data after** option and enter the desired number of days after which Absolute Manage is to delete data.
4. Click **OK** to save the new server settings.
5. In your firewall, open the port that you have specified as Absolute Manage Server's agent port.

You have now set up Absolute Manage Server so that it can receive information from agents even if they are located outside of your organization's network, as long as they are connected to the Internet.

NOTE The Absolute Manage Server will not accept administrative requests over the agent port. Only agent communication is possible over that port. (This does not apply if both ports are identical.)

Starting to track a computer

Absolute Manage does not automatically track all administered computers; rather, you specifically tell it which ones you want to monitor.

To specify that a computer be tracked:

1. In any browser window, select the computer that you want to track.
2. Right-click the computer and choose **Computer Tracking** from the context menu.

The **Computer Tracking** dialog opens:



3. To track the computer, check **Track selected computers**. If you want the computer to transmit screenshots, check that option as well.
4. Click **OK**.

Absolute Manage immediately starts tracking the computer and continues to do so until you disable tracking.

NOTE Tracking can be enabled when the computer is already outside your network but requires one contact between the agent and the Absolute Manage Server to actually begin.

Stopping the tracking of a computer

To stop tracking a computer, open the **Computer Tracking** dialog as described above and uncheck the **Track selected computers** option.

Getting information on tracked computers

You can get information on tracked computers in three ways:

- In a browser window table
To get information on all tracked computers in a table, open a new browser window and add the information items of the **Computer Tracking** category, as described in “Opening and configuring browser windows” on page 103.
Note: The information items are explained in “Computer Tracking” on page 569.
- In the detailed computer view
To get information on an individual computer, open that computer’s detail view as described in “Displaying an overview of a single computer” on page 105 and click the **Computer Tracking** category.
If you have set the tracked computer to take screenshots, they are displayed here as well. The context menu of the screenshot lets you view it in a separate window or the default JPEG viewer of your system or copy it to the clipboard.
- In an exported HTML or XML file
To get information on all tracked computers in an exported file, list all computers which you want to include in the file in a browser window and choose **Export** from the **File** menu. Choose either of the two **TheftTrack Report** options from the **File Format** menu in the Save dialog.

You can use the information displayed by Absolute Manage for taking appropriate steps to physically locate and retrieve the computers.

You can also send commands to the tracked computer (e.g., to execute shell scripts), even if it is located behind a firewall. Commands that you send are queued and executed when the tracked computer sends the next ‘heartbeat’ signal.

Executing files from your computer

Absolute Manage can execute files from an administrator’s computer on administered computers. Because these files can be scripts or application programs, a wide range of tasks can be performed with this feature.

The main limitation is the unavailability of remote input – you cannot enter any parameters while a script or application is running. This means that you need to rely on the cooperation of the local users, use a screen-sharing utility such as VNC, or make sure that no input is required.

To execute a file from your computer on administered computers:

1. In any browser window, select the computers on which you want to execute the file.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose the desired command:

- **Execute Script** to execute a Unix shell script or AppleScript (only on Mac OS X client computers) or a DOS batch file, Visual Basic script, or Powershell script (only on Windows client computers)
- **Execute Macintosh File** to execute a Mac OS X application (only on Mac OS X client computers)
- **Execute Windows File** to execute a Windows application (only on Windows client computers)

The command dialog opens. The individual dialogs are described below.

3. Set the desired options, as described below.

4. Click **Execute**.

The file is copied to the target computers, executed there, and removed when the execution has been completed.

Script

Enter a script text in the **Text** field or select a text file containing a script file.

- If you enter a script text or choose an uncompiled text file, you must make sure that the text conforms to the respective syntax. In the case of AppleScript text entered directly, the **Check Syntax** button can help you.

*Note: When you specify scripts that are intended for other computer platforms than the one you are using, Absolute Manage automatically converts the scripts' line endings to the convention required by the target platform. This does not apply to auxiliary files uploaded by means of the "**Transfer all files in folder containing executable**" option described below.*

- If desired, specify command line options for the script. Absolute Manage provides these options to the script on the target computers according to the respective script architecture's conventions. You can include environment variables in the options, as described in "Environment variables" on page 137.
- By default, any results the scripts return can be viewed in the command history. To have the results be displayed in their own windows upon script completion, check the **Automatically view results** option.

- To view the results from all target computers together in a single window, also check **All results in one window**.
- If the script must be executed with the privileges of an (operating system) administrator, check the **Executable requires administrative privileges** option.
Note: Checking this option does not change the user account in which the script is executed, it merely gives the script more privileges. This is similar to authorizing installer applications by supplying an administrator password.
 - Except for AppleScript scripts, choose the user context in which the script is to be executed – either in the account of whatever user is currently logged in, with a system account, or in a specified account. In the latter case, the specified account must exist on all target computers.
 - Note that scripts that access other applications need these applications to be present on the target computers and have the same names there. If applications are missing or have different names, script execution will fail.
 - If the script relies on additional files that must be transferred to the target computers, put them in the same folder and check the **Transfer all files in folder containing executable** option.

Details on the elements of the command dialog are available in “Execute Script” on page 307.

Macintosh application

Select the desired application using the **Select** button.

Choose the installation volume. Specify the user account, as described above in “Script”.

Specify the execution method – whether to copy the file from your computer or from a server, and in the latter case using which method. If the application is to be copied from a server, provide the necessary access details.

If desired, you can give command line options and a working directory.

NOTE When you copy a Mac OS application from your computer, it must not have a resource fork.

Specify a message, if desired. The details are described in “Sending messages” on page 115.

NOTE If a message has been specified, this is indicated by a dot in the dialog’s **Message** tab.

Details on the elements of the command dialog are available in “Execute Macintosh File” on page 309.

Windows application

Select the desired application using the **Select** button.

Specify the user account in which the application is to be executed. You can choose either the current user, the local system administrator account, or a specific user account. In the latter case, you must specify the password. Also, the account must be available on every target computer – either locally or via the domain – and have the same password everywhere. When you specify a domain username, you must prefix the domain.

If desired, you can give command line options and a working directory.

NOTE When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, Absolute Manage adds the /qn option (/quiet /norestart for MSU files) to run the installer silently. When you add your own options or when another type of installer is selected, you have to provide the command line parameters for a silent installation yourself.

Specify the execution method – whether to copy the file from your computer or from a server, and in the latter case using which method. If the application is to be copied from a server, provide the necessary access details.

Specify a message, if desired. The details are described in “Sending messages” on page 115.

NOTE If a message has been specified, this is indicated by a dot in the dialog's **Message** tab.

Details on the elements of the command dialog are available in “Execute Windows File” on page 312.

Executing local files

Absolute Manage can execute files that are already present on the target computers. This requires the same file to be present on every target computer at the same location.

NOTE Information on copying files to target computers is available in “Transferring files to administered computers” on page 197.

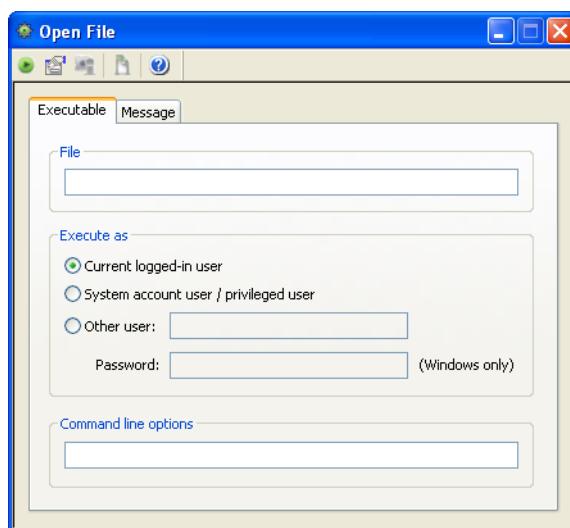
To execute a file that is already on the target computers:

1. In any browser window, select the computers on which you want to execute the file.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Open File**.

The **Open File** dialog opens:



3. Enter the path of the file that you want to execute.

Note: If you select a file in step 1 (instead of computers), the path of that file is pre-entered in the dialog.

4. Specify the user account in which the file is to be executed.

You can specify, the currently active user account, a user with system administrator privileges, or a specific account. In the latter case, you must provide the password for Windows target computers (but not Mac OS X targets).

5. If desired, you can specify command line options, provided the target application supports them

You can include environment variables in the options, as described in "Environment variables" on page 137.

6. Click **Execute**.

Terminating processes

Absolute Manage lets you terminate processes on administered computers.

There are two variants for doing so: 'soft', allowing users to save any changes, and 'hard', instantly killing the processes.

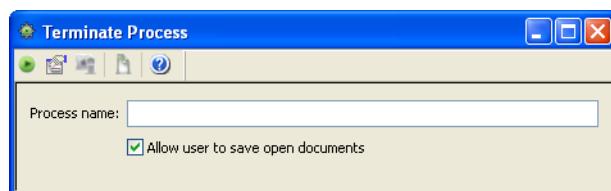
To terminate a process on administered computers:

1. In any browser window, select the computers on which you want to terminate the process.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Terminate Process**.

The **Terminate Process** dialog opens:



3. Enter the name of the process that you want to terminate. The process must have the same name on all target computers.

Note: If you select a process in step 1 (instead of computers), the name of that process is pre-entered in the dialog.

4. Choose a 'soft' or 'hard' termination.

For a 'soft' termination, check **Allow user to save open documents**. In this case, the process is sent a 'terminate' event. The effect is similar to choosing **Exit** in an application. If the process is still operative, users have an opportunity to save any unsaved changes. If the process hangs, it cannot be terminated in this way; you must choose the 'hard' termination.

For a 'hard' termination, uncheck the option. This is equivalent to forcefully killing a process.

5. Click **Execute**.

Working with services

You can use Absolute Manage to start and stop services on administered Windows computers as well as specify their startup status.

Stopping a service

To stop a service on an administered Windows computer:

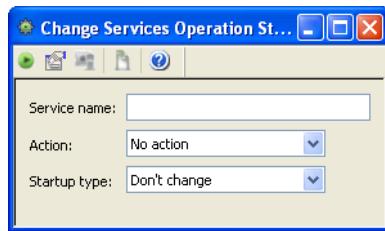
1. In any browser window, select the computers on which you want to terminate the services.

*Note: If the desired service is contained in the server database (the information having been collected with the **Gather Inventory Information** command), you can also select the service in a browser window in which it is displayed. To display services, add information items from the **Windows Services** information items group.*

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Change Services Operation State**.

The **Change Services Operating State** dialog opens:



3. Enter the name of the service that you want to stop (as displayed in the **Service Name** information item. The service must have the same name on all target computers.

Note: If you select a service in step 1 (instead of computers), the name of that service is pre-entered in the dialog.

4. Choose **Stop** from the **Action** pop-up menu.
5. Click **Execute**.

Starting or restarting a service

To start or restart a service, proceed as described in **Stopping a service**, above, but choose **Start** or **Restart**, respectively, from the **Action** pop-up menu.

Setting a service's startup status

To set a services' startup status, proceed as described in **Stopping a service**, above, but make no choice from the **Action** pop-up menu.

Instead, choose an option from the **Startup type** pop-up menu, depending on the desired effect:

- **Automatic:** The service is automatically started whenever the operating system boots.
- **Manual:** The service is not automatically started but may be started by users or other applications.
- **Disabled:** The service cannot be started at all.

Editing the registry

Absolute Manage lets you create, edit, and delete keys and values in the registries of Windows client computers.

NOTE It is easier to work with registry entries that are listed in the Registry Entries table of the Absolute Manage database. Searching for entries to include them in the database is described in “Gathering information on registry entries” on page 78.

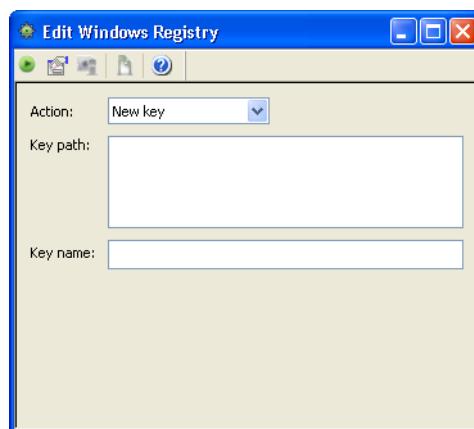
To edit the registry:

1. In any browser window, select the computers on which you want to edit the registry. Or select a registry entry that you want to edit in the **Registry Entries** window or any other browser window displaying registry entries.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Edit Windows Registry**.

The **Edit Windows Registry** dialog opens:



Note: Which fields are displayed in the dialog depends on the chosen action. If you have selected a registry entry before choosing the command, values from that entry are pre-entered into the dialog.

3. Choose the desired action from the **Action** pop-up menu.

Absolute Manage displays the fields appropriate to the action in the dialog.

4. Fill in the fields that are visible:

- **Key path:** Enter the path of the key in which you want to create a new key or value.
- **Key name:** Enter the new key's name.
- **Value path:** Enter the path of the value that you want to change.
- **Value type:** Specify the new data type of the value.
- **Value:** Enter the data that is to be stored in the specified value.
- **Path:** Specify the path of the key or value that you want to rename or delete.
- **New name:** Enter the new name of the specified key or value.

When you specify a path, you can include environment variables, as described in "Environment variables" on page 137.

5. Click **Execute**.

Environment variables

Several commands let you use shell or environment variables. Absolute Manage can use the standard variables of the target system and defines several variables of its own.

Using environment variables

The conventions for using environment variables in command options depend on the target OS platform (i.e., the OS running on the clients you are targeting):

- For Mac OS X targets, enclose the variable in curly braces and prefix it with a dollar sign. For example: "\${HOME}".
- For Windows target, enclose the variable in percent signs. For example: "%USERPROFILE%"

In either case, the entire string must be enclosed in quotes.

File-related variables defined by Absolute Manage

Absolute Manage includes some special environment variables related to file and folder locations:

- LANREV_EXECUTABLE_DIRECTORY: the local folder into which payloads are downloaded during installations
- ProgramFilesx64: On 64-bit Windows systems, the folder in which 64-bit applications are stored (usually C:\Program Files). On other systems, this variable is undefined.

- ProgramFilesx32: On 64-bit Windows systems, the folder in which 32-bit applications are stored (usually C:\Program Files (x86)). On 32-bit Windows systems, the folder in which applications are stored (usually C:\Program Files). On other systems, this variable is undefined.
- ProgramFileSyncNative: On Windows systems, the folder in which system-native applications – that is, 32-bit applications on 32-bit systems and 64-bit applications on 64-bit systems – are stored (usually C:\Program Files). On other systems, this variable is undefined.
- CommonProgramFilesx64: On 64-bit Windows systems, the folder in which common files used by 64-bit applications are stored (usually C:\Program Files\Common Files). On other systems, this variable is undefined.
- CommonProgramFileSyncNative: On Windows systems, the folder in which the common files used by system-native applications – that is, 32-bit applications on 32-bit systems and 64-bit applications on 64-bit systems – are stored (usually C:\Program Files\Common Files). On other systems, this variable is undefined.
- SysDirx32: On Windows systems, the system folder for 32-bit applications. On other systems, this variable is undefined.
- SysDirx64: On 64-bit Windows systems, the system folder for 64-bit applications. On other systems, this variable is undefined.
- SysDirxSystemNative: On Windows systems, the system folder for system-native applications. (For 32-bit system, this is the same as SysDirx32. For 64-bit systems, this is the same as SysDirx64.) On other systems, this variable is undefined.

These variables do not apply to AppleScript scripts. Most of them are not available outside of Absolute Manage, although LANREV_EXECUTABLE_DIRECTORY is available as a command line option for scripts and applications launched by Absolute Manage.

Registry-related variables defined by Absolute Manage

Absolute Manage includes some special environment variables related to registry locations:

- HKLM_Softwarex32 and HKEY_LOCAL_MACHINE_Softwarex32: The registry software hive for 32-bit applications. On 32-bit systems, this is HKEY_LOCAL_MACHINE\Software; on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software\Wow6432Node.
- HKLM_Softwarex64 and HKEY_LOCAL_MACHINE_Softwarex64: The registry software hive for 64-bit applications. On 32-bit systems, this is undefined; on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software.
- HKLM_SoftwareSystemNative and HKEY_LOCAL_MACHINE_SoftwareSystemNative: The registry software hive for the native applications on the system.

On 32-bit systems, this is HKEY_LOCAL_MACHINE\Software;
on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software.

Mobile devices running iOS or Android are administered from Absolute Manage through an MDM (mobile device management) server.

See “Installing MDM support” on page 24 for information on installing the server and “Enrolling mobile devices” on page 39 for information on activating the MDM for a particular mobile device.

Details are described in these sections:

- **Sending a message to mobile devices** (page 140)
- **Locking and unlocking mobile devices** (page 141)
- **Creating configuration profiles containing variables** (page 143)
- **Installing configuration profiles on mobile devices** (page 145)
- **Installing provisioning profiles on iOS devices** (page 153)
- **Configuring roaming on mobile devices** (page 155)
- **Preparing iOS devices for software installation** (page 155)
- **Installing software on mobile devices** (page 157)
- **Distributing App Store or Google Play (Android Market) apps to mobile users** (page 165)
- **Distributing media to mobile devices** (page 169)
- **Working with actions** (page 174)
- **Working with policies** (page 176)
- **Geotracking mobile devices** (page 182)
- **Naming Android devices** (page 188)

Sending a message to mobile devices

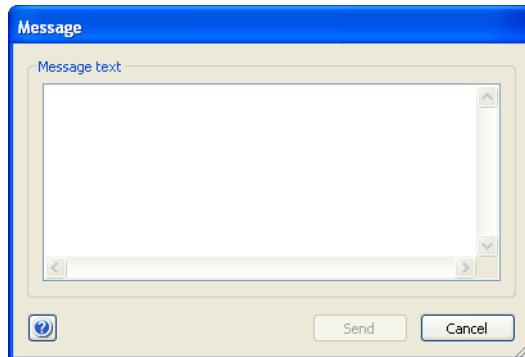
You can send messages from Absolute Manage Admin directly to administered mobile devices (except Windows Phone devices).

Note that this requires the AbsoluteApps application to be installed on the target devices (and having been launched at least once) and push notifications to be enabled on the devices. See “Preparing iOS devices for software installation” on page 155 for information on deploying AbsoluteApps on iOS.

To send a message to mobile devices:

1. In the **Mobile Devices** window, select the devices to which you want to send the message.
2. Right-click the devices and choose **Send Message to Device** from the context menu.

The **Message** dialog opens:



3. Enter the message and click **Send**.

The message is sent to all selected mobile devices. It is displayed the next time they contact mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If they are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.



Locking and unlocking mobile devices

You can remotely lock mobile devices or remove the passcode from the device. These functions are not available for Windows Phone devices.

To lock a mobile device:

1. In the **Mobile Devices** window, select the devices you want to lock.
2. Right-click the devices and choose **Issue Device Lock** from the context menu.

A confirmation dialog is displayed. If any of the selected devices does not have passcode, you are prompted to provide one. This passcode will be set on the locked devices.

3. Click **Lock Device**.

The command is executed on each selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Locking a device is similar to switching it off; to reaccess the device, the user needs to swipe on the start screen and enter the passcode (unless no passcode has been set for the device).

To remove the passcode from a mobile device and optionally setting a new one:

1. In the **Mobile Devices** window, select the devices from which you want to remove the passcode.
2. Right-click the devices and choose **Issue Clear Passcode** from the context menu.

The **Clear Passcode** dialog is displayed:

3. If you want to set a new passcode, enter it in the **New passcode** and **Verification** fields.

Setting new passcodes applies only to Android devices.

Note that, if the configuration profile of the device requires a password, the user is prompted for a new password if you do not specify one.

4. Click **Clear Passcode**.

The command is executed on each selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or

out of range of any accessible network), it will happen once the device has reconnected to a network.

If you have not specified a new passcode and there is no configuration profile on the device that makes a passcode mandatory, the device is now accessible to anybody without requiring a passcode.

Erasing mobile devices

You can remotely erase the entire contents of mobile devices.

IMPORTANT

Note that this action is not reversible and that the erased information cannot be recovered from the mobile device (although recovering the data from a backup, should one exist, might be possible). Erasing devices without the consent of their users may expose you to legal liability.

To erase a mobile device:

1. In the **Mobile Devices** window, select the devices you want to erase.
2. Right-click the devices and choose **Issue Remote Erase** from the context menu.

A confirmation dialog is displayed. For devices with internal SD cards, you can choose to erase these cards as well.

3. Click **Erase Device**.

The next time a selected device contacts the mobile OS vendor's notification server, all of its data is erased. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Erasing the device removes any user data and all applications that were installed by the user. This effectively resets the device to its factory condition.

The erased device can no longer be administered through Absolute Manage until it has been enrolled again or it has been completely restored from a backup that contains the enrollment profile.

Creating configuration profiles containing variables

Absolute Manage supports the use of variables in configuration profiles that you create in the iPhone Configuration Utility.

You can define these variables as custom information fields and apply them by inserting codes into the fields of the configuration profile.

When Absolute Manage applies a configuration profile to an iOS device, it automatically replaces the variable code in the profile with the current value of the variable for that device. This results in two limitations:

- Configuration profiles containing variables must be applied with Absolute Manage; other tools do not support the variables.
- Any changes to the content or definition of a variable after the configuration profile has been applied have no effect on the mobile device. For such changes to affect the device, the profile has to be reapplied after the change has been made.

You can also use information items from the Device User Information category as variables, which is described in “Using variables in configuration profiles” below.

For details on working with variables, see:

- **Defining a variable** (page 144)
- **Using variables in configuration profiles** (page 145)

Defining a variable

To define a variable for use in an iOS configuration profile:

1. Define a custom information field that will serve as the variable, as described in “Defining custom information fields” on page 82.

Specify **Manual** as the field type and **Mobile** as the device type.

Enter the name for the variable in the **Variable name** field. You can enter any name as long as it does not contain spaces, dollar signs (\$), and curly brackets ({}).

Specify the other settings for the field normally.

This field is a normal mobile device custom information field and can be used as such, in addition to being available as a variable for configuration profiles.

2. After you have saved the new custom information fields to the server, fill them in for all mobile devices to which you want to upload configuration profiles with these variables.

Entering information into custom information fields is described in “Using custom information fields” on page 88.

You can also import the variables’ contents from a file, as described in “Importing data into custom information fields” on page 90.

The variables can now be used in configuration files, as described below.

Using variables in configuration profiles

Variables that are to be used in an iOS configuration profile must have been defined as described above.

To use a variable in a configuration profile, create the profile as usual. Wherever you want the variable to appear, enter `$(<variable_name>)`, where `<variable_name>` is the name you have specified in the **Variable name** field when creating the custom information field.

Absolute Manage comes with predefined variables that let you access information items from the Device User Information category, i.e., Active Directory information for the mobile user. (This requires the user to have enrolled through the MDM server, as described in “Enrolling mobile devices” on page 39.)

These variables are available (the name of the corresponding information item is noted in parentheses):

- MDU_DisplayName (Mobile Device User Display Name)
- MDU_FirstName (Mobile Device User First Name)
- MDU_LastName (Mobile Device User Last Name)
- MDU_LogOnName (Mobile Device User Log-on Name)
- MDU_EMail (Mobile Device User E-Mail)
- MDU_PhoneNumber (Mobile Device User Phone Number)
- MDU_Department (Mobile Device User Department)
- MDU_Company (Mobile Device User Company)
- MDU_Street (Mobile Device User Street)
- MDU_City (Mobile Device User City)
- MDU_State (Mobile Device User State)
- MDU_ZIPCode (Mobile Device User ZIP Code)
- MDU_Country (Mobile Device User Country)
- MDU_Office (Mobile Device User Office)
- MDU_OrganizationalUnit (Mobile Device User Organizational Unit)
- MDU_EnrollmentUsername (Mobile Device User Enrollment Username)
- MDU_EnrollmentDomain (Mobile Device User Enrollment Domain)

When the configuration profile is sent to a mobile device through Absolute Manage, Absolute Manage automatically replaces the variable code in the profile with the current content of the corresponding custom information field.

Note that this is not a dynamic link: If you later change the content of the custom information field and want that change to be reflected in the installed configuration profile, you need to reinstall it.

Note, too, that configuration profiles containing variables cannot be installed with other tools than Absolute Manage.

Installing configuration profiles on mobile devices

You can install a configuration profile either manually or via a policy. Using a policy also allows you to make configuration profiles available

to managed mobile devices, but leave it up to the local user of the mobile device whether to install them. (This latter option is not supported for Windows Phone.)

Absolute Manage works with both configuration profiles for devices (including the operating system) and for specific applications that support configuration through profiles.

Details of installing configuration profiles are described:

- **Importing a configuration profile into Absolute Manage** (page 146)
- **Manually installing a configuration profile** (page 147)
- **Manually removing a configuration profile** (page 148)
- **Installing a configuration profile via a policy** (page 149)
- **Making a configuration profile available for optional installation** (page 150)
- **Removing a configuration profile via a policy** (page 151)
- **Conflicting policy settings for configuration profiles** (page 152)

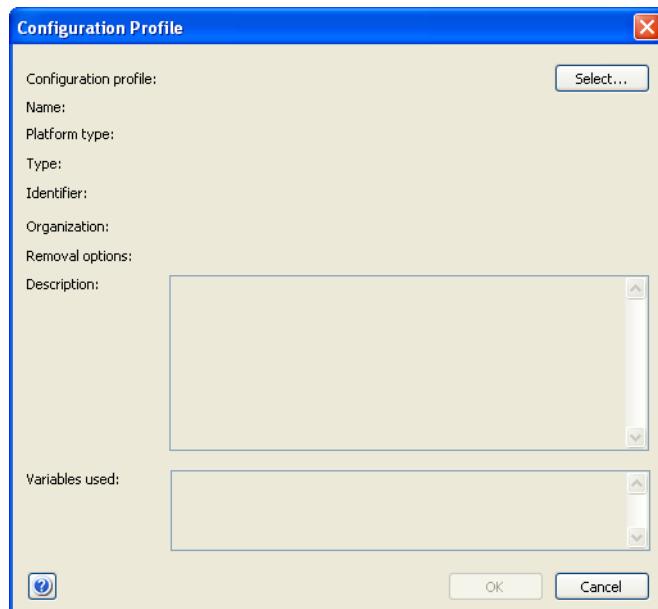
Importing a configuration profile into Absolute Manage

Installing a configuration profile on administered mobile devices requires the profile to be imported into Absolute Manage first.

To import a configuration profile into Absolute Manage:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Configuration Profiles and Certificates > New Configuration Profile** from the context menu.

The **Configuration Profile** dialog opens:



2. Click **Select** and choose the file containing the desired profile.

Configuration profile files for iOS devices can be created in Apple's iPhone Configuration Utility. Configuration profiles for Android and Windows Phone devices must be created manually in the same format. See the separate manuals describing this process for details.

3. Edit the description if desired.
4. Click **OK**.

The profile is imported into Absolute Manage and available for manual or profile-based installation on administered mobile devices.

Manually installing a configuration profile

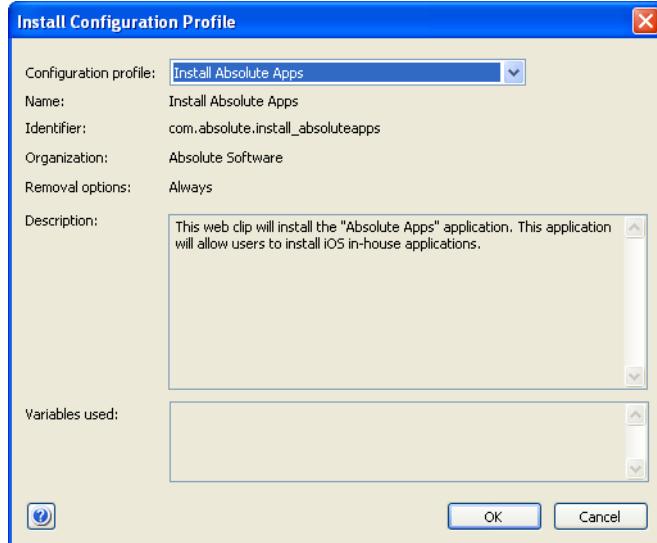
To install a configuration profile on mobile devices:

1. In the **Mobile Devices** window, select the devices on which you want to install the configuration profile.

Make sure to select only devices with a common operating system; all profiles are specific to either a particular operating system and cannot be installed on other operating systems.

2. Right-click the devices and choose **Install Configuration Profile** from the context menu.

The **Install Configuration Profile** dialog opens:



3. From the **Configuration profile** pop-up menu, choose the desired profile.

The menu contains all profiles that have been installed in Absolute Manage, as described in "Importing a configuration profile into Absolute Manage" on page 146. You can also use the **Other** command from the menu to open a configuration profile file from a volume on your computer.

4. Edit the description if desired.
5. Click **OK**.

The profile is sent to all selected mobile devices. It is installed on each selected device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The results vary slightly depending on the type of device:

- iOS and Android devices: The profile is added to the profiles that are installed on the devices.
All configuration profiles that are installed on an iOS or Android device are listed in the **Configuration Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.
- Windows Phone devices: The profile replaces the current profiles of the mailboxes with which the selected devices are synchronized.
Because of the way Exchange ActiveSync works, this applies the profile also to all other devices that are synchronized to the same Exchange mailboxes. (If such other devices are iOS devices, the profile does not replace their current profiles but the profile's settings may override those of any configuration profiles installed on the devices.)
The configuration profile that is currently in effect for a Windows Phone device is listed in the **ActiveSync Policy** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Failed installations

If a configuration profile could not be installed on a device, e.g., because it is not compatible with the device, an error message is generated.

In that case, you can fix all profiles with issues and then reapply them in one step using the **Retry All Failed Profiles** context menu command for the device.

Manually removing a configuration profile

To remove a configuration profile from a mobile device:

1. In the sidebar of the **Mobile Devices** window, expand the device from which you want to remove the configuration profile.
2. For iOS and Android devices, click the **Configuration Profiles** subgroup of the device; for Windows Phone devices, click the **ActiveSync Policy** subgroup.

The configuration profiles that are present on the device are listed in the main part of the window.

3. Select the profile you want to remove and press the Delete key.

You can also right-click the profile and choose **Delete Profile** from the context menu.

The profile is removed from the device the next time it contacts the mobile OS vendors notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

For Windows Phone devices only, the removed profile is replaced with the settings of the default EAS policy specified on the Exchange server.

Installing a configuration profile via a policy

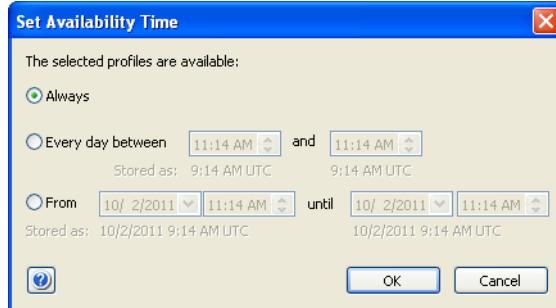
To install a configuration profile on mobile devices automatically:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items > Configuration Profiles** group to one of these subcategories of the **Configuration Profiles** category of the policy via which you want to distribute it:
 - **Auto-install:** The profiles are pushed to the device. They remain on a device even after it is removed from the policy. (After this point, users can remove the profiles manually, however.)
 - **Auto-install, auto-remove:** The profiles are pushed to the device. They are automatically removed from the device when it is removed from the policy.

Note that the actual effect may be different for devices that belong to other policies where the same configuration profile has a different role. See “Conflicting policy settings for configuration profiles” on page 152 for details.

2. If you do not want to restrict the time during which the profile is available, you are done. Only if you want to restrict it, continue.
3. Click the group into which you have put the profile inside the policy in the sidebar so that the configuration profiles contained in it are being displayed in the main part of the window.
4. Right-click the profile and choose **Set Availability Time** from the context menu.

The **Set Availability Time** dialog is displayed:



5. Specify when the profile should be available:

- To make it available for a particular time each day, choose **Every day between** and enter the desired start and end times.
- To make it available for a one-time period, choose **From** and specify the desired start and end times.

For further information, see the description of this dialog in “Set Availability Time” on page 430.

The profile is sent to all devices that belong to the policy the next time each device contacts the mobile OS vendor’s notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If devices are later added to the policy, they are treated the same way. (This may not be the case for devices also belonging to another policy in which the configuration profile is forbidden. See “Conflicting policy settings for configuration profiles” on page 152 for details.)

Profiles are installed on Windows Phone devices automatically, as described above, only if there are no other conflicting automatic profile assignment. If more than one auto-install profile is specified for a Windows Phone device (whether from one policy or from multiple policies), no profile is automatically installed.

Making a configuration profile available for optional installation

To make a profile available on an iOS or Android device but let the user decide whether to install it:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items > Configuration Profiles** group one of these subcategories of the **Configuration Profiles** category of the policy via which you want to distribute it:
 - **On-demand:** The profiles are made available for manual download in AbsoluteApps at the users discretion. They remain on a device even after it is removed from the policy. Users can remove the profiles manually at any time.

- **On-demand, auto-remove:** The profiles are made available for manual download in AbsoluteApps at the users discretion. They are automatically removed from the device when it is removed from the policy.
2. If you do not want to restrict the time during which the profile is available, you are done. If you want to restrict it, specify the desired time as described beginning in step 3 of “Installing a configuration profile via a policy,” above.

The profile is sent to all mobile devices that belong to the policy and is listed there in the **Profiles** section of AbsoluteApps. (This may not be the case for devices also belonging to a different policy with conflicting settings. See “Conflicting policy settings for configuration profiles” on page 152 for details.) If AbsoluteApps is not available on the device, nothing happens. (See “Preparing iOS devices for software installation” on page 155 for information on installing AbsoluteApps.)

The profile is transferred to each device the next time it contacts the mobile OS vendor’s notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If devices are later added to the policy, the profile is made available on them as well.

All configuration profiles that are installed on a device are listed in the subsections of the **Configuration Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Optional installation of profiles is not supported for Windows Phone devices.

Removing a configuration profile via a policy

To remove a configuration profile from mobile devices automatically:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items > Configuration Profiles** group to the **Forbidden Configuration Profiles** folder of the policy via which you want to remove it.
2. If you do not want to restrict the time during which the profile is forbidden, you are done. If you want to forbid it only during a certain time, specify the desired time as described beginning in step 3 of “Installing a configuration profile via a policy,” above.

The next time a device that belongs to the policy contacts the mobile OS vendor’s notification server and is unlocked, the profile is removed from that device. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are

not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

This may not be the case for devices also belonging to a different policy with conflicting settings. See “Conflicting policy settings for configuration profiles” on page 152 for details.

If devices are later added to the policy, the profile is removed from them as well (unless they also belong to a different policy which prevents this).

NOTE Profiles in the “Auto-install, auto-remove” or “On-demand, auto-remove” subcategories of the Configuration Profiles category of a policy are automatically removed from any device that is removed from the policy.

Conflicting policy settings for configuration profiles

It is possible to assign a configuration profile to multiple policies in different roles. For example, it could be auto-installed in one policy and forbidden in another, or on-demand in one policy and auto-installed and auto-removed in another.

This can become an issue if one device is a member of multiple policies and these policies contain the same configuration profile in different categories.

For example, a device could belong to one policy in which the profile is required and another in which it is forbidden. Clearly, there is no way to satisfy both policies’ requirements at the same time.

In cases like this, Absolute Manage uses this hierarchy for the different categories of profiles:

- Auto-install, auto-remove
- Forbidden profiles
- Auto-install
- On-demand, auto-remove
- On-demand

Higher entries have precedence before lower entries. For example, if a configuration profile is auto-installed in one policy to which a device belongs and forbidden in another, the profile is not available on the device because the “forbidden” category has a higher priority than “auto-install”.

This means that, in some instances, an auto-installed and auto-removed profile remains on a device even when the device is removed from the policy in question. This is the case when the device also belongs to another policy in which the profile is either auto-installed or on-demand (and the device does not belong to a policy in which the profile is forbidden).

Windows Phone and multiple profiles

Because only one configuration profile (EAS policy) can be active on a Windows Phone device at any time, Absolute Manage does not install a profile on any Windows Phone devices when the (Absolute Manage) policy or policies to which it belongs specify more than one profile as automatically installed.

Installing provisioning profiles on iOS devices

You can install a provisioning profile manually on an iOS device. While provisioning profiles are normally automatically installed as part of an application, manually installing them may be necessary in special situations.

This is described in:

- **Manually installing a provisioning profile** (page 153)
- **Manually removing a provisioning profile** (page 154)

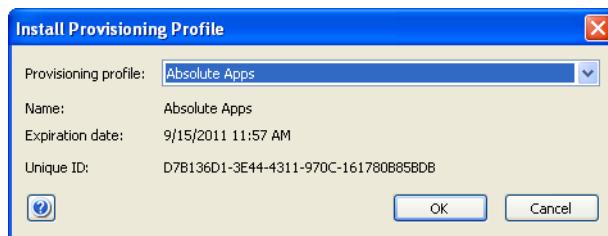
NOTE Android does not support provisioning profiles.

Manually installing a provisioning profile

To install a provisioning profile on iOS devices:

1. In the **Mobile Devices** window, select the devices on which you want to install the configuration profile.
2. Right-click the devices and choose **Install Provisioning Profile** from the context menu.

The **Install Provisioning Profile** dialog opens:



3. From the **Provisioning profile** pop-up menu, choose the desired profile.

The menu contains all profiles that are part of an application package.

If the profile you want to install is not part of an application package, choose **Other** and select the provisioning profile file on your computer.

4. Click **OK**.

The profile is sent to all selected mobile devices. It is installed on each device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

All provisioning profiles that are installed on a device are listed in the **Provisioning Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Failed installations

If a configuration profile could not be installed on a device, e.g., because it is not compatible with the device, an error message is generated.

In that case, you can fix all profiles with issues and then reapply them in one step using the **Retry All Failed Profiles** context menu command for the device.

Manually removing a provisioning profile

To remove a provisioning profile from an iOS device:

1. In the sidebar of the **Mobile Devices** window, expand the device from which you want to remove the provisioning profile.
2. Click the **Provisioning Profiles** subgroup of the device.

The provisioning profiles that are present on the device are listed in the main part of the window.

3. Select the profile you want to remove and press the Delete key.

You can also right-click the profile and choose **Delete Profile** from the context menu.

The profile is removed from the mobile device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Any applications that rely on this profile for authorization can no longer be used on the device after the next time the device (not the app) is restarted.

All provisioning profiles that are installed on a device are listed in the **Provisioning Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Configuring roaming on mobile devices

You can enable and disable data and voice roaming on managed iOS devices.

Note, however, that the local users are not prevented from changing the settings again.

Setting roaming options is not available for Android and iOS 4 devices.

To set the roaming options for managed mobile devices:

1. Select the devices in the **Mobile Devices** window.
2. Right-click the device and choose **Set Roaming Options** from the context menu.
3. In the **Set Roaming Options** dialog, configure the settings as desired.

Settings that are checked will be enabled on the selected devices. Settings that are unchecked will be disabled. Settings in the third neutral state () will be left unchanged.

The options are set on each device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Preparing iOS devices for software installation

Due to the access restrictions for non-Apple software on iOS devices, installing software on such devices through a management system is both limited and requires preparation.

There are two fundamental requirements:

- Any in-house software to be distributed through Absolute Manage must be properly signed with a provisioning profile.
- Software distribution requires the AbsoluteApps app to be installed on iOS 4.x devices, but not iOS 5 and later. However, AbsoluteApps is required for many other functions of Absolute Manage, so we strongly recommend that you always install it.

There are two basic ways to install AbsoluteApps, either as a download from Apple's App Store or as signed in-house software:

- Installing AbsoluteApps as an App Store download is easier but requires each user of a managed iOS device to have a valid

Apple ID. For details, see “Downloading AbsoluteApps from the App Store” on page 156

- Distributing AbsoluteApps as an in-house app is more work but does not put any requirements on your users. This process requires preparing and distributing AbsoluteApps. Contact Absolute Professional Services for details.

NOTE The preparation described in this section is not required for Android or Windows Phone devices.

Downloading AbsoluteApps from the App Store

1. Make sure that every user with a device on which you want to deploy AbsoluteApps has an account with Apple’s App Store.
2. Enroll all iOS devices to which you want to distribute the app in Absolute Manage.

This is described in “Enrolling mobile devices” on page 39.

3. Have all users download and install AbsoluteApps from the App Store.

This can be done either on the mobile device itself or on the computer from which the device is managed through iTunes. In the latter case, the device must be synced with iTunes so that AbsoluteApps is transferred to the device.

4. Configure AbsoluteApps with the internet address and port of your MDM server. There are three ways to do this:

- When AbsoluteApps is first launched, it presents a dialog in which the users can enter this information.



When the user has entered the server address and port in this screen, AbsoluteApps is configured. Skip the remaining steps of this procedure.

- You can configure AbsoluteApps via an app configuration profile. This is documented in the separate guide “Creating App Configuration Profiles”.
 - You can provide this information via a configuration profile, as described below.
5. The **Mobile Devices** window’s **Assignable Items > Configuration Profiles** section contains a profile named “Configure AbsoluteApps”. Install this profile on all iOS devices which have downloaded AbsoluteApps, as described in “Installing configuration profiles on mobile devices” on page 145.
- You can install the profile either manually or via a policy. If you install it via a policy, it is removed automatically once AbsoluteApps has been configured, ensuring that users do not continue to find the icon on their home screens although they already have configured the app.
- The installed configuration profile appears as an icon on the home screens of the iOS devices, like an app. Tapping this profile automatically configures AbsoluteApps, even if the server settings screen is being displayed.
6. Communicate to the users (e.g., by e-mail) that they should tap the configuration profile to configure AbsoluteApps.

Also communicate to the users that they must enable push notifications on their devices for AbsoluteApps to work properly.

When users have performed these steps (installing and configuring the app and enabling push notifications), they have access to all apps you make available to their devices through Absolute Manage. They can also receive messages you send to them from Absolute Manage.

Installing software on mobile devices

You can distribute in-house applications to managed iOS and Android devices. Depending on the operating system running on the mobile device, in most cases you can also distribute application files from an app store.

Distributing software involves up to three steps:

1. First you re-sign the application file using your enterprise provisioning profile.

This step applies only to in-house iOS application files.
2. Then you import the application file into Absolute Manage as a mobile application package.
3. Then you can distribute that package to mobile users.

You can either push-install apps to individual devices or make apps available for user-initiated installation in the AbsoluteApps mobile application, which looks and works similar to Apple's App Store app.

All steps are described below in these sections:

- **Preparing iOS application files** (page 158)
- **Importing an application into Absolute Manage** (page 159)
- **Making applications available on mobile devices** (page 161)
- **Uninstalling applications from mobile devices** (page 163)

Preparing iOS application files

Due to the requirements of iOS, an in-house app must be signed and an enterprise provisioning profile must be attached. In addition, the provisioning profile included with the app bundle by the Xcode development environment must be removed.

NOTE This procedure does not apply to Android or apps from the App Store apps.

Absolute provides a script that handles the required steps automatically; this document describes using the script.

You will need the following:

- A computer running Mac OS X on which Apple's iOS SDK is installed: The provided script requires this operating system and development environment.
Since Absolute Manage itself is not required for this procedure, it often will be easiest to perform it on the development computer that was used to create your in-house apps.
- The PrepareAppForDeployment.sh script included on the Absolute Manage Mac OS X disk
- A valid signing identity, accessible through the Mac OS X Keychain utility, that corresponds to your organization's iOS distribution certificate
- An enterprise distribution provisioning profile that is to be attached to the app. It must correspond to the signing identity.
- The iOS app bundle as created by Xcode

NOTE Instead of using the procedure described below, on Mac OS X 10.6 or later, it is usually easier to use the Configure iOS Apps utility that is included on the Absolute Manage installation disk. See the utility's Help menu for more information.

To prepare an app for distribution with the PrepareAppForDeployment.sh script:

1. Copy the script, the provisioning profile, and the app bundle to convenient locations on your computer.

2. Make sure that the signing identity is available in your keychain.
3. Run the script by entering this command in the terminal:

```
PrepareAppForDeployment.sh --in <app> --out <prepared_app>
--signingidentity <identity> --provisioningprofile
<profile>
```

Where the parameters are:

- *<app>*: The app bundle created by Xcode
- *<prepared_app>*: The location where the script is to create the prepared app it creates as output. Any existing file at this location will be silently overwritten.
You can specify the location of the input file (i.e., *<app>*).
- *<identity>*: The name under which the signing identity is stored in Keychain
- *<profile>*: The distribution provisioning profile that will be used to authorize the app on the iOS devices

For example:

```
PrepareAppForDeployment.sh \
--in "/Users/johndoe/Documents/apps-to-convert/InHouse.app" \
--out "/Users/johndoe/Documents/apps-to-deploy/InHouse.ipa" \
--signingidentity "iPhone Distribution" \
--provisioningprofile "/Users/johndoe/Documents/
In_House_App.mobileprovision"
```

The script extracts the profile from the app bundle, resigns the app using your identity, and saves the resulting new app file at the specified location.

You can now use this app file, together with the specified provisioning profile, to import and distribute the app to iOS devices as described in below.

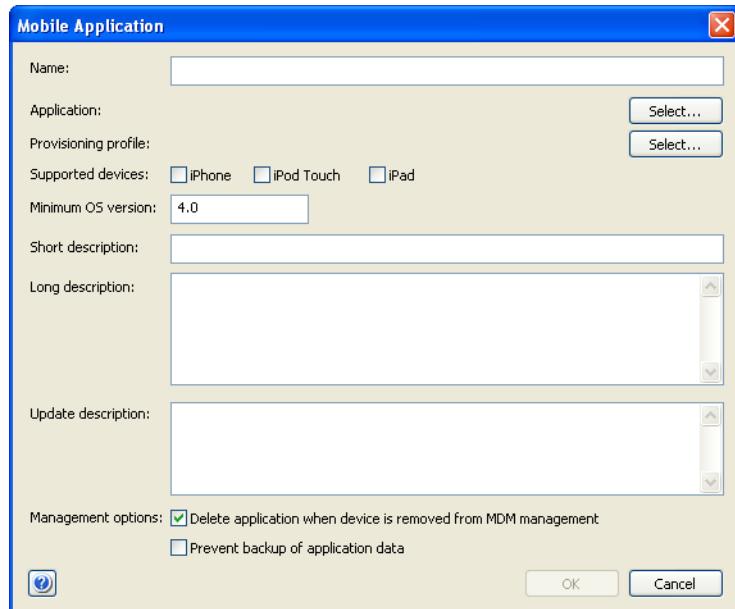
Importing an application into Absolute Manage

An in-house iOS application that you want to import into Absolute manage must have been prepared as described in above. An in-house Android application can be imported as-is.

To import a mobile application into Absolute Manage:

1. In the **Mobile Devices** window, right-click the sidebar and choose **Mobile Applications > New In-house Application Package** from the context menu.

The **Mobile Application** dialog opens:



The dialog is described in “New In-house Application Package” on page 393.

2. Click the upper **Select** button and choose the application file.

This file must have the .ipa extension (for iOS apps) or .apk extension (for Android files), respectively.

Note: Importing Android apps requires a Java runtime environment (JRE) to be installed on your computer.

3. If desired, edit the name for the application package.

This is the name under which the application package is listed in Absolute Manage. It is automatically taken from the application file you have chosen, but you can modify it before saving the package.

4. When importing iOS apps, click the lower **Select** button and choose the provisioning profile. (Skip this step for Android apps.)

The provisioning profile is required for the application to run. It must either be an ad-hoc profile that authorizes the application for a set of specific devices or an in-house provisioning profile that authorizes the application for all iOS devices.

The provisioning profile must be provided by the application’s developer.

5. Fill in the short, long, and update descriptions as desired.
6. If you want the app to remain on managed devices only as long as those devices are under MDM management, check the **Delete**

application when device is removed from MDM management option.

If the option is unchecked, this app remains on devices on which it is installed, even when MDM management of the devices ends.

This option is available only for iOS apps.

7. If you want the data of the application not to be copied in an iTunes or iCloud backup of the device, check the **Prevent backup of application data** option.

If the option is unchecked, the data of the app is backed up normally.

This option is available only for iOS apps.

8. Click **OK** to save the package.

The application package is saved in Absolute Manage and can now be made available in the AbsoluteApps mobile app as described in “Making applications available on mobile devices”, below.

Making applications available on mobile devices

There are two ways for making apps available on managed iOS or Android devices, via policies or via direct installation. Both are described below.

Making apps available via policies

Once you have created an application package as described in above, you can use it to make the application available on devices:

1. Drag the new application package from the **Assignable Items** > **In-house Applications** group to one of the subgroups (except **Forbidden In-house Apps**) of the **In-house Apps** group inside any mobile policy that contains the mobile devices on which you want to make the application available.

The subgroups differ in how the application is installed and removed:

- Auto-install: The app is installed when the device enters the policy. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
- On-demand: The app can be installed manually by the user. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
- Auto-install, Auto-remove: The app is installed when the device enters the policy and removed when it leaves.

- On-demand, Auto-remove: The app can be installed manually by the user. It is removed from the device when it leaves the policy.

Note: For information on on-demand installation on iOS devices, please contact Absolute Support.

On some mobile operating systems, the user may need to confirm the installation or the removal of apps.

Silent installation (no user confirmation required) is supported on:

- Lenovo devices with Persistence
- Some Samsung Galaxy devices

Silent removal is supported on:

- iOS 5.0 or newer (only for apps installed via MDM)
- Lenovo devices with Persistence
- Some Samsung Galaxy devices

The application is displayed in the list of applications inside AbsoluteApps on (for apps installed on demand) or downloaded to (for automatically installed apps) any mobile device belonging to the policy as soon as the device next contacts the mobile OS vendor's push notification server. If it is online via WiFi or a mobile network, this happens quickly, usually within a minute, but if it is not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

You can send messages (see "Sending a message to mobile devices" on page 140) or e-mails to the users of the devices to notify them of the availability of the new application.

Making apps available via direct installation

For a more ad-hoc approach, you can distribute apps directly:

1. In the **Mobile Devices** window, select the mobile devices on which you want to install the app.
2. Choose **Commands > Install Application** from the context menu.

The **Install Application** dialog is displayed.

3. From the **Application** pop-up menu, choose the app you want to install.

You can choose both in-house and third-party App Store or Google Play apps that you have imported. For information on importing commercial apps, see "Recommending third-party apps" on page 165.

4. If desired, edit the long description of the app.

5. Click **OK**.

The application is transferred to each selected device and the users are prompted to install it the next time the device contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

On iOS 4.x devices, the user is prompted to install the application only when AbsoluteApps comes to the front the next time.

If a user declines the installation, the app is not installed on that device.

Note that you cannot install an application on an iOS device that already contains an unmanaged version of the application. (Unmanaged applications are all applications that have been installed by other means than through the MDM system.)

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window. Managed applications available for download are listed in the **Assignable Items** section.

Uninstalling applications from mobile devices

You can directly uninstall applications from devices, with the details varying according to the mobile operating system:

- On iOS 4 devices, direct uninstallation is not available. Instead, you have to remove the provisioning profile, as described below in "Uninstalling applications from iOS 4 devices"
- On iOS 5, only managed applications can be removed, i.e., applications that have been installed through the Absolute Manage MDM system.
- On Android devices, any application can be removed, but the local user must confirm it. If the device supports persistence, no user confirmation is required.

To uninstall applications (other than from iOS 4 devices):

1. In the **Mobile Devices** window, display a list of installed applications.

For example, display the **Applications** category of a managed device or the built-in **All installed applications** smart group.

2. Select the applications that you want to uninstall.
3. Right-click the selected applications and choose **Delete Application** from the context menu.

The next time a device on which one of the selected application is installed contacts the mobile OS vendor's notification server and is

unlocked, any selected application is removed from that device. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

On Android devices, a confirmation alert is displayed before the application is actually removed. If the user does not allow the removal, the application remains on the device.

Uninstalling applications from iOS 4 devices

It is not possible to remotely uninstall applications from devices running iOS 4.x. However, you can disable the ability of an application to run on the device by deleting the provisioning profile.

Note, however, that due to the way iOS handles provisioning profiles, deleting a profile becomes effective only when the device (not the app!) is restarted. In other words, even when you delete the provisioning profile, that app continues to be fully functional until the next device restart.

To disable an application:

1. In the **Mobile Devices** window, drag the application that you want to disable from the **Assignable Items > In-house Applications** group to the **Forbidden In-house Apps** group inside the iOS policy to which the iOS device belongs.

If no such policy exists, you need to create one first, as described in “Working with policies,” below.

The next time a device that belongs to the policy contacts the mobile OS vendor’s notification server, the provisioning profile is removed from that device. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

After the next restart of the device, the application can no longer be used on that device.

Also, the application cannot be installed on any device belonging to the policy.

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Distributing App Store or Google Play (Android Market) apps to mobile users

You can push-install commercial apps to mobile users in a similar way to in-house applications or make them available to users of managed devices to install on demand.

Push-installation works the same way as for in-house applications, as described in “Making apps available via direct installation” on page 162. (Note that you need to import the app first, as described below.)

For iOS apps only, if you have set up a volume purchasing agreement (VPP), you can let mobile users easily purchase apps through this program.

Recommending commercial apps and using VPP codes is described below in these sections:

- **Recommending third-party apps** (page 165)
- **Making volume purchase codes available** (page 167)

Recommending third-party apps

You can create app packages for App Store or Android Market (Google Play) apps that can then be distributed to mobile devices.

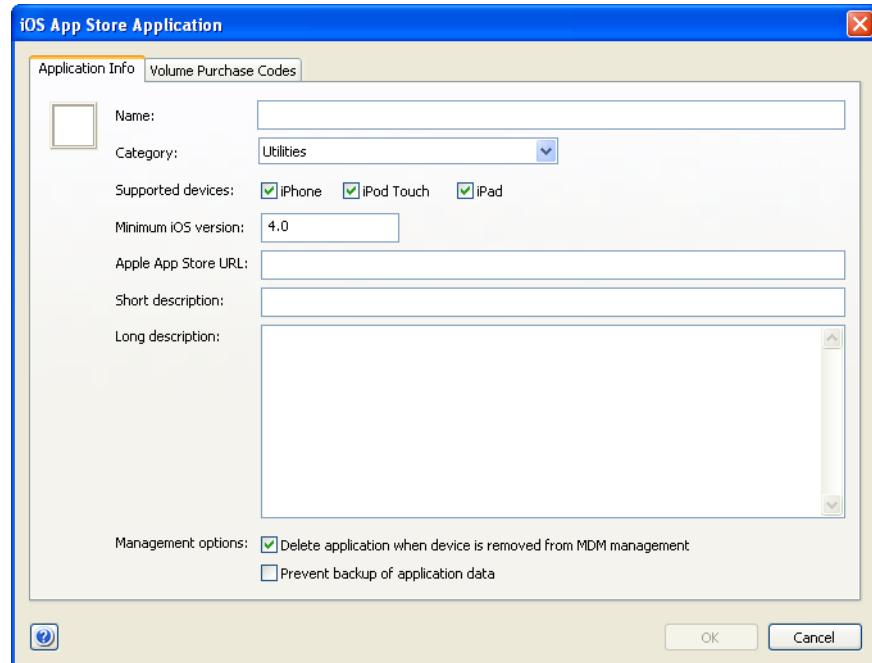
These app packages contain references to the apps, not the actual apps themselves, and appear in the App Store (for iOS apps) or Google Play (for Android apps) sections of AbsoluteApps. Users can install these apps just like any other commercial app.

AbsoluteApps must be installed on all mobile devices to which you want to distribute these app packages. See “Preparing iOS devices for software installation” on page 155 for information on distributing AbsoluteApps to iOS devices and “Enrolling mobile devices” on page 39 for information on distributing it to Android devices.

To create and distribute recommended app packages:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Mobile Applications > New iOS App Store Application Package** or **Mobile Applications > New Google Play Application Package**, depending on the target platform.

Depending on the command chosen, the **iOS App Store Application** dialog (shown below) or the **Google Play Application** dialog opens:



2. Enter the URL of the app's App Store page in the **Apple App Store URL** or **Google Play URL** field, respectively, and press the Tab key or click in another field.

You can obtain the URL by right-clicking the app's icon anywhere in the respective online stores and choosing **Copy Link** from the context menu.

3. If you have volume purchase redemption codes for the app (iOS only), enter them as described in "Making volume purchase codes available" on page 167.
4. Click **OK** to close the dialog and save the new app package.
5. The new app package appears in the **Assignable Items > 3rd Party Applications** group in the **Mobile Devices** window.
6. Drag the app package to the **3rd Party Applications > On-demand** group of a policy containing the devices to which you want to recommend the app.

Policies are described in "Working with policies" on page 176.

The next time a device that belongs to that policy contacts the mobile OS vendor's notification server, the app package information is sent to that device. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not

connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The package appears on the device in the **App Store** section or **Google Play** section, respectively, of AbsoluteApps.

Users can install the app by clicking the **Install** button; if they do so, the app is downloaded from the App Store or Android Market (Google Play) normally.

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window. Recommended applications are listed in the **Assignable Items** section.

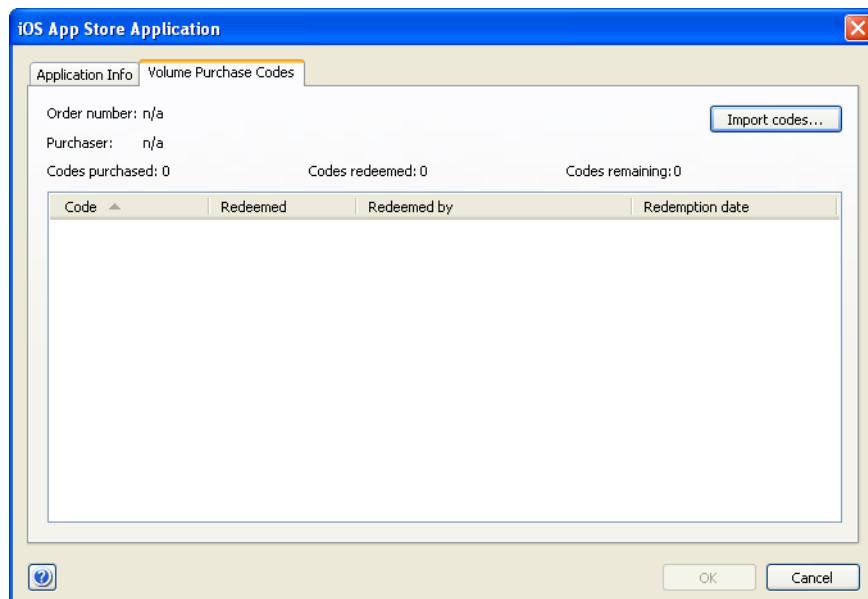
Making volume purchase codes available

Apple's App Store offers a volume purchasing program for apps. If you purchase a block of apps through this program, you receive a list of redemption codes and links.

You can import such code lists into Absolute Manage and allow users of mobile devices to purchase apps through the volume purchasing program without needing to assign them codes individually.

To make volume-purchased apps available to users:

1. Create an app package for the App Store app, as described in "Recommending third-party apps", above, until you reach step 3.
2. Click the Volume Purchase Codes tab to display the corresponding pane:



3. Import the codes in one of these ways:

- Copy and paste:

- Open the Excel file with the codes that you have received from Apple.
- Copy the entire contents or just the rows containing the codes and redemption links.
- Switch to Absolute Manage Admin and click inside the table area.
- Paste the copied codes.
- Exported text file:
 - Open the Excel file with the codes that you have received from Apple.
 - Save the file as a tab-delimited text file.
 - Switch to Absolute Manage Admin and click the **Import Codes** button.
A standard system Open dialog is displayed.
 - Select the exported text file and click **Open**.
- Manually created text file:
 - Create a text file in which each line contains a redemption code, a tab character, and the corresponding redemption link.
 - Save the file as a tab-delimited text file.
 - Switch to Absolute Manage Admin and click the **Import Codes** button.
A standard system Open dialog is displayed.
 - Select the text file and click **Open**.

The codes are added to the table in the dialog.

4. Continue the procedure described in “Recommending third-party apps” with step 4.

All mobile devices to which the package is made available (via the policies to which you assign it) can now purchase the app using the redemption codes.

To redeem a code, the user simply clicks **Install** in AbsoluteApps. Absolute Manage automatically and transparently transmits an unused redemption code and the corresponding link to the App Store. The user of the mobile device does not notice any of this. The used code is automatically marked as redeemed and will not be assigned to another device.

Deleting codes

You can delete redeemed codes – in particular codes that have been redeemed outside of Absolute Manage and thus are still considered available there:

1. In the **Mobile Devices** window, double-click the App Store app package into which the codes have been imported.
2. Click the **Volume Purchase Codes** tab.
3. In the table, select the codes that you want to delete.

4. Press the Delete key.
5. Click **OK** to save the changes and close the dialog.

The codes are removed from the package and are no longer available for redemption inside Absolute Manage.

Distributing media to mobile devices

You can import media files into Absolute Manage and make them available to managed iOS devices through the AbsoluteSafe app.

Media files are distributed through profiles, allowing you fine-grained control over who will and will not have access to a particular file. Furthermore, you can optionally prevent media files from being taken out of AbsoluteSafe.

The files are stored in encrypted form on the device and are not part of any backups of the mobile device to PC (e.g., in iTunes).

To distribute media files, you first import them into Absolute Manage and then assign them to any policies through which you want to distribute them. The details of this are described in:

- **Importing a media file** (page 170)
- **Distributing a media file** (page 173)

Distributing media files to Android or Windows Phone devices is not supported.

Supported media types

You can distribute all kinds of media (i.e., any file from your computer) to managed mobile devices. AbsoluteSafe provides support for viewing a number of popular document, image, video and sound formats right within the app; other media types can be opened in other apps, provided they are available on the mobile device and that you have allowed the media file to leave AbsoluteSafe (see “Importing a media file,” below).

These types of media can be displayed within AbsoluteSafe:

- Web formats
 - HTML (.htm and .html)
 - XML (.xml)
 - XSL (.xsl)
 - Safari web archive (.webarchive)
- PDF (.pdf)
- Text
 - Pages (.pages)
 - RTF (.rtf)
 - RTF directory (.rtfd)
 - Unformatted text (.txt)
 - Word (.doc and .docx)*

- Presentations
 - Keynote (.key)
 - PowerPoint (.ppt and .pptx)*
- Spreadsheets
 - Excel (.xls and .xlsx)*
 - Numbers (.numbers)
- Images
 - BMP (.bmp)
 - GIF (.gif)
 - JPEG (.jpg and .jpeg)
 - PNG (.png)
 - TIFF (.tif and .tiff)
- Audio
 - AAC audio (.m4a)
 - AAC audio books (.m4b and .m4p)
 - AIFF (.aiff, .aif, .aifc, and .cdda)
 - AMR (.amr)
 - MP3 (.mp3 and .swa)
 - MPEG audio (.mpeg, .mpg, .mp3, and .swa)
 - WAVE (.wav and .bwf)
- Video and multimedia
 - 3GP (.3gp and .3gpp)
 - 3GP2 (.3g2 and .3gp2)
 - MPEG-4 (.mp4 and .m4v)
 - QuickTime (.mov, .qt, and .m4v)**
 - AVI (.avi)**

* Microsoft Office files in Office 95 or older formats are not supported.

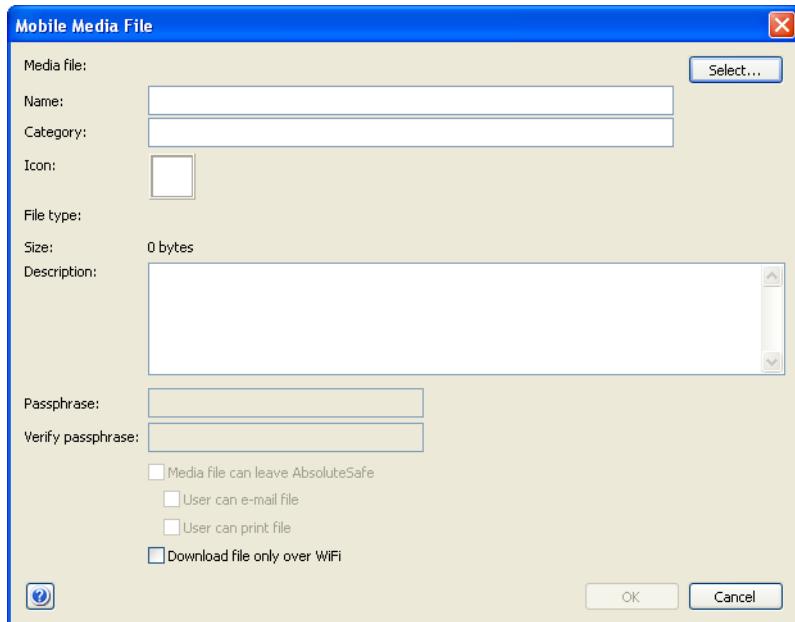
** QuickTime and AVI are container formats that support a wide range of content formats. Some QuickTime and AVI files may not be playable within AbsoluteSafe.

Importing a media file

To be able to assign a media file to a policy and thereby distribute it to managed mobile devices, you first import it into Absolute Manage:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Media > New Media File**.

The **Mobile Media File** dialog is displayed.



2. Click **Select** and choose the desired file or drag the file from the desktop into the **Media file** area.

The **Name**, **Category**, and **Icon** fields are automatically filled based on the file you selected.

You can also select entire folders of media files to batch-import them. If you do, some special considerations apply, as described in "Importing folders of media files," below.

3. Edit the **Name** and **Category** fields if desired. You can also paste a graphic into the **Icon** field that is displayed as the media file's icon on the mobile devices.
4. Enter a description in the **Description** field.

This description will be displayed to mobile users and should give them some indication of the relevance of the file.

5. If desired, set a password for the media file by entering it in the **Passphrase** and **Verify passphrase** fields.

The passphrase must be entered every time the file is displayed in AbsoluteSafe.

If you set a passphrase, you cannot allow the media file to leave AbsoluteSafe. Therefore, you can set a passphrase only for file types that are supported by AbsoluteSafe. (See "Supported media types" on page 169 for a list of supported file types.)

You cannot set a passphrase when **Media file can leave AbsoluteSafe** is enabled.

6. If you want the mobile users to be able to view or edit the media file in apps other than AbsoluteSafe, check **Media file can leave AbsoluteSafe**.

This allows users, e.g., to view the file in a PDF reader, edit in a text editor, or forward it to others by e-mail.

If desired, you can also check **User can e-mail file** and/or **User can print file** to provide buttons with AbsoluteSafe for these two tasks.

You cannot check **Media file can leave AbsoluteSafe** if you have set a password for the file, as described in step 5.

Note: While unchecking this option reliably prevents the file from leaving AbsoluteSafe, the same is not necessarily true for the information contained in the file. For example, a mobile user still could take screenshots of the file and send those to other persons.

7. If the file is large, you may want to check **Download file only over WiFi** so that the user does not have to suffer long downloads or high data charges because the file was downloaded over a mobile data connection, such as 3G (UMTS) or LTE.

This setting requires AbsoluteSafe 1.1 or newer. Earlier versions of AbsoluteSafe ignore it.

8. Click **OK**.

The new media file is added to the **Assignable Items > Media** section of the sidebar and can now be assigned to policies.

Importing folders of media files

Instead of importing individual files, you can import entire folders in one step. The process is the same as described above, with a few changes:

- When you click **Select** in step 2, hold down the Shift key to open the folder selection dialog.
- The names under which the media files are stored in Absolute Manage (the content of the **Name** field) cannot be set individually. Instead Absolute Manage uses the file names, without the file name extensions.
- You can specify a category. If you do, it applies to all files contained in the folder. If you do not specify a category, Absolute Manage automatically assigns a category to each file depending on its file type.
- If you select a folder to import, the displayed file type is always “Batch upload” and no file size is shown.
- Any description and passphrase you specify applies to all files contained in the folder.
- The **Media file can leave AbsoluteSafe** setting you specify applies to all files contained in the selected folder that AbsoluteSafe can display (see “Supported media types” on page 169 for details). Files that AbsoluteSafe cannot display itself are always allowed to leave AbsoluteSafe (irrespective of

the setting you specify) because it would otherwise be impossible for mobile users to view these files.

Distributing a media file

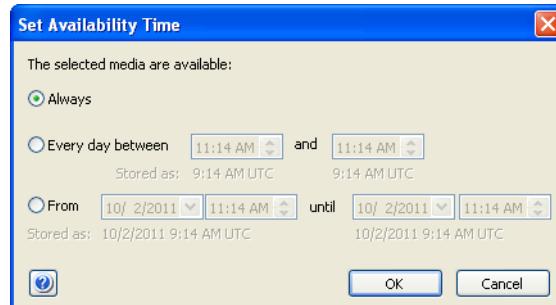
Once you have imported a media file as described in above, you can distribute it to mobile devices via assigning it to a policy:

1. Drag the media file from the **Assignable Items > Media** group to one of the subgroups of the **Media** group inside any mobile policy that contains the mobile devices on which you want to make the application available.

The subgroups differ in how the media file is installed and removed:

- Auto-install: The media file is downloaded when the device enters the policy. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
 - On-demand: The media file can be downloaded manually by the user. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
 - On-demand, auto-remove: The media file can be downloaded manually by the user. It is removed from the device when it leaves the policy.
 - Auto-install, auto-remove: The media file is downloaded when the device enters the policy and removed when it leaves.
2. If you do not want to restrict the time during which the file is available, you are done. Only if you want to restrict it, continue.
 3. Click the **Media** group inside the policy in the sidebar so that the media files that are assigned to the policy are being displayed in the main part of the window.
 4. Right-click the media file and choose **Set Availability Time** from the context menu.

The **Set Availability Time** dialog is displayed:



5. Specify when the file should be available:

- To make it available for a particular time each day, choose **Every day between** and enter the desired start and end times.
- To make it available for a one-time period, choose **From** and specify the desired start and end times.

For further information, see the description of this dialog in “Set Availability Time” on page 430.

6. Click **OK**.

The media file is displayed in the list of files inside AbsoluteSafe on any mobile device belonging to the policy as soon as the device next contacts the mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

You can send messages (see “Sending a message to mobile devices” on page 140) or e-mails to the users of the devices to notify them of the availability of the new file.

All media files that are available to a device are listed in the **Assignable Items** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Working with actions

Actions let you specify what Absolute Manage is to do when a device is added to a smart policy.

Available actions include:

- Sending a message to the device
- Sending a message to an administrator
- Setting roaming options on the device
- Updating the information about the device stored on the server
- Removing MDM or configuration profiles

Actions are defined centrally and stored in the **Actions** group in the **Mobile Devices** window, from where they can be assigned to any desired policies.

Details of working with actions are described below.

Creating a new action

To create a new action:

1. In the sidebar of the **Mobile Devices** window, choose the appropriate command from the **Actions** submenu of the context menu:

- **New Send Message to Device Action** to create an action that sends a message to the device that has joined the smart policy.
- **New Send E-mail Action** to create an action that sends an e-mail to one or more specified addresses (usually those of administrators).
- **New Send SMS (Text Message) Action** to create an action that sends a text message (SMS) to one or more specified phones (usually those of administrators).
- **New Set Roaming Options Action** to create an action that configures data and voice roaming permissions on the device.
- **New Update Device Info Action** to update the information stored on the server for the device. (As if **Update Device Info** has been chosen for the device.)
- **New Freeze Device Action** to create an action that changes the access pass phrase on the device and locks it. (This makes the device inaccessible to the local user.)
- **New Remove Configuration Profile Action** to create an action that removes a configuration profile from the device.
- **New Demote to Unmanaged Device Action** to create an action that removes the MDM profile and, where applicable, the Absolute Manage client software from the device. (This means that the device is no longer managed through Absolute Manage.)

A dialog specific to the action is displayed.

2. Fill in the dialog's fields as desired.

For an explanation of the available fields, see the dialog descriptions in:

- "New Send Message to Device Action" on page 405
- "New Send E-mail Action" on page 407
- "New Send SMS (Text Message) Action" on page 409
- "New Set Roaming Options Action" on page 410
- "New Freeze Device Action" on page 412
- "New Remove Configuration Profile Action" on page 413
- "New Demote to Unmanaged Device Action" on page 413

3. Click **OK** to save the action.

The new action appears in the **Actions** group of the sidebar and can be assigned to policies, as described in "Specifying actions in policies" on page 179.

Re-executing actions

You can re-execute actions on devices in various ways:

- A single action on a single device: Display the device in the sidebar of the **Mobile Devices** window; expand it and click its **Performed Actions** subcategory; right-click the desired action

and choose **Re-execute This Action for This Device** from the context menu.

- A single action on all applicable devices: Display the Actions subcategory of the **Assignable Items** category in the sidebar of the **Mobile Devices** window; right-click the desired action and choose **Re-execute This Action for All Devices** from the context menu.
- A single action on all devices of a policy: Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subcategory; right-click the desired action and choose **Re-execute This Action for This Policy** from the context menu.
- All actions on a single device: Display the device in the sidebar of the **Mobile Devices** window; expand it and click its **Performed Actions** subcategory; right-click anywhere in the window's table area and choose **Re-execute All Actions for This Device** from the context menu.

Any delays and repetitions you have specified for an action also apply when it is re-executed.

Reviewing actions

All actions that have been applied to a device are listed in the Performed Actions subgroup of the device when it is expanded in the sidebar of the **Mobile Devices** window.

Deleting actions

To delete an action from Absolute Manage, right-click it in the sidebar of the **Mobile Devices** window and choose **Remove Action** from the context menu.

This deletes the action, including removing it from all policies to which it is assigned.

For removing actions from individual policies, see “Specifying actions in policies” on page 179.

Working with policies

You can automate certain aspects of mobile device administration by using policies.

A policy is a collection of:

- Mobile devices
- Commercial applications that are recommended for use on these devices
- In-house applications that are either:
 - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
 - Prohibited on these devices

- Automatically installed on devices that are added to the policy and left on devices that are removed from the policy
- Allowed on the devices belonging to the policy
- Allowed on the devices belonging to the policy and deleted from devices that are removed from the policy
- Configuration profiles that are:
 - Mandatory on these devices
 - Available on these devices to be installed by users at their discretion
 - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
 - Forbidden on the devices belonging to the policyConfiguration profiles apply only to managed iOS and Windows Phone devices.
- Media files that are:
 - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
 - Automatically installed on devices that are added to the policy and left on devices that are removed from the policy
 - Allowed on the devices belonging to the policy
 - Allowed on the devices belonging to the policy and deleted from devices that are removed from the policy
- Actions that are performed when mobile devices become members of the policy (smart policies only)

Any changes you make to a policy becomes effective on a device the next time the device contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The details of working with policies are described in:

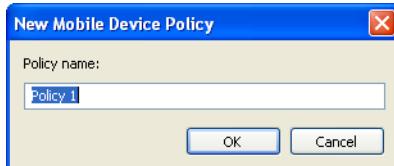
- **Creating a policy** (page 177)
- **Adding and removing mobile devices** (page 178)
- **Specifying actions in policies** (page 179)
- **Specifying applications in policies** (page 181)
- **Specifying configuration profiles in policies** (page 181)
- **Specifying media in policies** (page 182)

Creating a policy

To create a policy to which you manually add devices:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Policies > New Policy**.

The **New Mobile Device Policy** dialog is displayed.



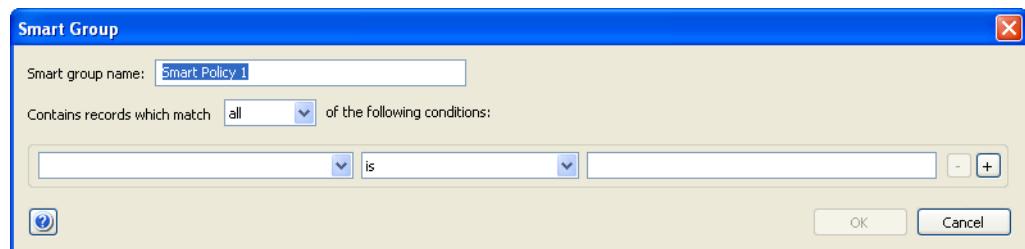
2. Enter the name of the new policy and click **OK**.

The new policy is added to the **Policies** section of the sidebar. It does not contain any devices; you must add them manually as described below in “Adding and removing mobile devices”.

To create a policy to which devices are added automatically according to criteria you specify:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Policies > New Smart Policy**.

The **Smart Group** dialog is displayed.



2. Enter the name of the new policy.
3. Specify the criteria that a mobile device must meet to be included in the group.

For more information on using this kind of dialog, see “Creating a smart group” on page 111.

4. Click **OK**.

The new policy is added to the **Policies** section of the sidebar. It contains all mobile devices that meet the specified criteria. You cannot manually add or remove devices. If a device later meets the criteria, it is automatically added; likewise a device belonging to the policy is automatically removed when it no longer meets the criteria.

Adding and removing mobile devices

Standard policies allow devices to be manually added or removed, but smart policies do not.

To add a mobile device to a policy:

1. In the **Mobile Devices** window, drag the device that you want to add from any group listing devices to the policy to which you want to add it.

The device is now part of the policy and is listed in the main part of the window when you click the policy in the sidebar.

To remove a mobile device from a policy:

1. In the **Mobile Devices** window, select the devices you want to remove.
2. Right-click the devices and choose **Remove from Policy** from the context menu.

The device is now part of the policy and is listed in the main part of the window when you click the policy in the sidebar.

All policies to which a device belongs are listed in the **Policies** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Specifying actions in policies

For each smart policy, you can specify actions that are to be performed when a device is added to the policy.

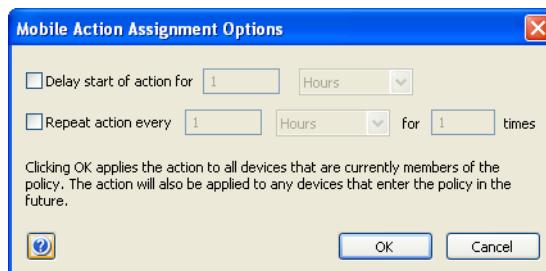
Adding actions to a policy

Any actions you want to specify must already been available in the **Actions** group of the **Mobile Devices** window sidebar. See “Working with actions” on page 174 for information on managing actions.

To specify an action in a policy:

1. In the **Mobile Devices** window, drag the action that you want to add from the **Actions** group in the sidebar of the **Mobile Devices** window to the smart policy to which you want to add it. (Actions cannot be added to standard – non-smart – policies.)

The **Mobile Action Assignment Options** dialog is displayed:



2. Specify whether you want to delay or repeat the action:

- If you check the delay option, the action is not performed immediately when a device becomes a member of the policy, but only after the specified interval has elapsed.
- If you check the repeat option, the action is repeated after the specified interval for the specified number of times.

You can combine both options, for example, to send a message to the device two hours after it has become a member of the policy and then every hour thereafter.

A delayed or repeated action is not executed when the device is no longer a member of the policy.

3. Click **OK**.

The action is added to the policy. It is executed on all devices that are currently a member of the policy and will be executed on each device that enters the policy in the future.

Any delays and repetitions you have specified apply both to existing and future members. The delay for existing members is calculated from the moment when the action is assigned to the policy.

Changing delay or repetition settings

To change the delay or repetition settings for an action in a policy:

1. Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subgroup.

The actions assigned to the policy are displayed in the main part of the **Mobile Devices** window.

2. Right-click the action you want to remove and choose **Change Action Schedule**.
3. Set the delay and repetition as desired.
4. Click **OK**.

The new settings for the action in this policy are saved. They are effective immediately.

Removing actions from a policy

To remove an action from a policy:

1. Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subgroup.

The actions assigned to the policy are displayed in the main part of the **Mobile Devices** window.

2. Right-click the action you want to remove and choose **Remove Action from Policy**.

The action is removed from this policy. Any remaining repetitions or delayed executions are skipped.

For information on removing an action entirely from Absolute Manage (which also removes it from all policies), see “Deleting actions” on page 176.

Specifying applications in policies

In policies, you can specify applications that are available for installation on the mobile devices that belong to the policy, applications that are automatically installed, and applications that are prohibited on these devices.

Doing so is covered in “Making applications available on mobile devices” on page 161 and “Uninstalling applications from mobile devices” on page 163, respectively.

To recommend commercial apps from the Apple App Store or Google Play (Android Market) to users of mobile devices, see “Recommending third-party apps” on page 165.

Specifying configuration profiles in policies

In policies, you can specify configuration profiles that are required on the mobile devices that belong to the policy and configuration profiles that are prohibited on these devices.

Adding a profile

1. To add a configuration profile to a policy:
2. Drag the configuration profile from the **Assignable Items > Configuration Profiles** group to the desired profile group inside the policy:
 - **Auto-install:** These profiles are automatically installed on the devices belonging to the policy.
 - **On-demand:** Users of the devices belonging to the policy can install these profiles if they so desire. The profiles are listed in the **Available** subsection of the **Profiles** section of AbsoluteApps. On-demand profiles are not supported for Windows Phone devices.
 - **Auto-install, auto-remove:** These profiles are automatically installed on any device that is added to the policy and automatically removed from any device that is removed from the policy.
 - **On-demand, auto-remove:** Users of devices belonging to this policy can install these profiles if they so desire. The profiles are automatically removed from any device that is removed from the policy.
 - **Forbidden Configuration Profiles:** These profiles cannot be installed on the devices belonging to the policy.

The next time a device that belongs to the policy contacts the notification server, the configuration profile is installed and activated, made available, or deleted on that device, depending on the category into which you have put it.

Removing a profile

To remove a configuration profile from a policy:

1. Select the configuration profile in the policy.
2. Right-click the profile and choose **Remove Configuration Profile**.

The profile is removed from the policy. There is no immediate effect on the devices that belong to the policy. That is, when you remove a profile from the policy's **Auto-install** list, it is not removed from the devices; and when you remove a profile from the **Forbidden** list, it is not installed on the devices.

However, the restrictions on the mobile devices with respect to the configuration profiles are lifted: A previously required profile may now be deactivated or removed, and a previously prohibited profile may now be installed and activated.

Conflicting profile assignments in multiple policies

It is possible that a device belongs to multiple policies, more than one of which contains the same configuration profile. The profile need not be in the same category in all policies.

See "Conflicting policy settings for configuration profiles" on page 152 for information on how cases are handled this leads to multiple conflicting profile assignments for a device.

Specifying media in policies

In policies, you can specify media that is automatically made available to user on every device that is added to the policy.

Doing so is covered in "Distributing a media file" on page 173.

Geotracking mobile devices

You can record the locations of iOS or Android devices in Absolute Manage, which is especially helpful if the device is lost or stolen.

For similar functions related to administered computers, see "Tracking computers" on page 125.

NOTE For information on geotracking iOS devices, please contact Absolute Support.

Enabling geotracking of mobile devices requires three major steps:

1. AbsoluteApps must be installed on the devices, as described in "Preparing iOS devices for software installation" on page 155 (for iOS devices) and "Enrolling mobile devices" on page 39 (for Android devices), respectively.

2. A passphrase for enabling tracking must be set, as described in “Setting passphrases for mobile devices”, below.
3. Tracking must be enabled for the devices, as described in “Enabling geotracking on mobile devices” on page 185.

Collected mobile device locations can be shown either numerically or on a map, as described in “Displaying geotracking information” on page 188.

NOTE AbsoluteApps must be running on the mobile device for geotracking to work. It does not need to be the front application, but if a user terminates it, geotracking is no longer possible. (A restart is unproblematic, as AbsoluteApps is automatically relaunched when it was running before the restart.) You can usually get a user to reopen AbsoluteApps by sending him or her a message (as described in “Sending a message to mobile devices” on page 140). Viewing the message launches AbsoluteApps.

NOTE While geotracking can often be helpful when recovering a stolen mobile device, it is not a reliable theft recovery system by itself. Among other things, a thief can prevent geotracking by switching the mobile device off or by resetting it to the factory condition (erasing AbsoluteApps in the process).

Setting passphrases for mobile devices

A passphrase must be set on a mobile devices before geotracking can be enabled on it. The passphrase is to ensure the legitimacy of any tracking requests sent to the device.

A passphrase can be set either individually per device, or a group of devices can have the same passphrase.

Setting a passphrase individually

If you want to specify an individual passphrase for a device:

1. Install AbsoluteApps normally on the device, as described in “Preparing iOS devices for software installation” on page 155 (for iOS devices) and “Enrolling mobile devices” on page 39 (for Android devices), respectively.

Note: For information on geotracking iOS devices, please contact Absolute Support.

2. When AbsoluteApps is launched for the first time, the user is first prompted for the server address and then asked to enter a passphrase:



3. Users must enter the same passphrase in both the **Passphrase** and **Confirm** fields before they can click **OK** to use AbsoluteApps.

The passphrase can consist of any number of characters; it is not restricted to digits.

Unless the user tells you this passphrase, you cannot enable tracking. If this passphrase is intended to track the device only in emergency situations – when the device is lost or stolen – it is advisable for the user to write down the passphrase in a safe location

The mobile device now has a passphrase. Geotracking for the device can be enabled when the user provides the passphrase to you, as described in “Enabling geotracking on mobile devices” on page 185.

The passphrase cannot be changed on the device. If users want to change the passphrase, they must contact an administrator who resets the passphrase for them, after which they can enter a new passphrase as described above. See “Resetting a passphrase”, below, for more information.

Setting one passphrase for a group of devices

If you want to specify the same passphrase for a large group or all of your managed devices:

1. After AbsoluteApps has been installed, go to the Absolute Manage support page at www.absolute.com/support and follow the provided link.

As part of the request, you'll need to provide the desired passphrase. You may also need to sign a legal waiver.

Absolute Software will return an encrypted token to you that is based on a combination of your serial number and the passphrase. You will also receive instructions on using this token to modify AbsoluteApps.

2. Follow the instructions provided to set the passphrase on all devices.

Note that this process requires the user to accept the new passphrase on the device.

All mobile devices on which this procedure was performed and on which the users have accepted the change now have the same passphrase. Geotracking for the device can be enabled using this passphrase, as described in "Enabling geotracking on mobile devices" on page 185.

Resetting a passphrase

You can reset the passphrase on a managed mobile device. This removes the current passphrase and requires a new passphrase to be set, either locally by the user as described in "Setting a passphrase individually", above, or remotely by you, as described in "Setting one passphrase for a group of devices", above.

Passphrases can only be reset on one device at a time.

To reset a passphrase:

1. In the **Mobile Devices** window, select the device on which you want to reset the passphrase.
2. Right-click the device and choose **Reset Tracking Passphrase** from the context menu.

A confirmation dialog is displayed.

3. Click **Reset Passphrase**.

The current passphrase is removed from the device and a new one must be set before AbsoluteApps can be used again on that device.

Enabling geotracking on mobile devices

When iOS or Android devices have been properly set up, as described in "Setting passphrases for mobile devices" on page 183, geotracking can be enabled on them.

IMPORTANT

Because the location of a mobile device often is also the location of its user, tracking mobile devices is subject to privacy or data protection laws in many jurisdictions.

Usually, the express consent of the user of the device is required before it may be tracked. In addition, there may be regulations governing how long gathered data may be stored and how and by whom it may be accessed.

Failure to obtain the required consent or observe other applicable legal regulations may expose you to civil and/or criminal liability.

NOTE For information on geotracking iOS devices, please contact Absolute Support.

To enable geotracking on mobile devices:

1. In the **Mobile Devices** window, select all devices on which you want to enable geotracking.
2. Right-click the devices and choose **Track Device** from the context menu.

Note that, if you select multiple devices, all must have the same passphrase.

The **Mobile Device Tracking** dialog is displayed:



3. Check the **Track device** option.
4. Enter the passphrase of the devices in the **Activation passphrase** field.

See “Dealing with lost passphrases,” below, for information on what to do when a passphrase has been lost.

5. Set the desired tracking interval and location accuracy.

Shorter tracking intervals allow for more fine-grained tracking but can create huge amounts of data. For example, tracking 50 devices with an interval of five minutes creates more than five million records per year.

Better location accuracy lets you pinpoint a device’s position with greater precision but is more intrusive of the bearer’s privacy. When the desired accuracy is not technically achievable, location data may have a lower accuracy than specified.

Note that you can change the interval and accuracy at a later time, e.g., when the device is lost or stolen.

6. Click **OK**.

Geotracking is enabled on each device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Dealing with lost passphrases

If tracking is not enabled on a device and the passphrase has been forgotten, there is normally no way to enable tracking when the device is stolen or lost.

(When the device is still available, the situation is easily remedied by resetting the passphrase, as described in "Resetting a passphrase" on page 185.)

To let you enable tracking even in such unfortunate circumstances, Absolute Software can provide you with device-specific code that lets you enable tracking:

1. Go to the Absolute Manage support page at www.absolute.com/support and follow the provided link to enter your request.

As part of the request, you and the (legal) user of the device may need to sign legal waivers.

Absolute Software will send you a special document for Absolute Manage.

2. Send the information shown in the document back to Absolute Software.

You will receive an encrypted device recovery token.

3. Right-click the device in the **Mobile Devices** window, press the Alt key, and choose **Track Device** from the context menu.

The **Mobile Device Tracking** dialog opens in a special mode:



4. Enter the device recovery token in the **Device recovery token** field and click **OK**.

Geotracking is enabled on the selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Displaying geotracking information

You can display collected locations of mobile devices numerically or graphically on a map.

Displaying locations numerically

To display locations numerically, add the information items from the **Mobile Device Information > Device Tracking** category to any group in the **Mobile Devices** window that displays mobile devices.

Displaying locations on a map

To display mobile device locations on a map:

1. In the **Mobile Devices** window, select the location which you want to display.

If you select a device, the last known location will be shown.

2. Right-click the device and choose **Show Location on Google Maps** or **Show Location on Bing Maps** from the context menu.

A new window is opened in your standard web browser, and the location is shown in Google Maps or Bing Maps, respectively.

Naming Android devices

When an Android device is enrolled, Absolute Manage assigns it an automatically generated name. You can, however, assign it a custom name (or rename it at any time).

iOS devices are named on the device itself or in iTunes.

To name an Android device:

1. Select the device in the **Mobile Devices** window.
2. Right-click the device and choose **Set Device Name** from the context menu.
3. In the **New Mobile Device Name** dialog, enter the desired new name and click **OK**.

The device is renamed the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The new name is displayed in the **Mobile Device Name** information item.

Absolute Manage includes a range of functions for working with files on administered computers. You can copy, move, delete, rename, and open files as well as create shortcuts and folders. You can also transfer files from your computer to administered computers.

These functions are described in:

- “Copying and moving files” on page 190
- “Deleting files” on page 192
- “Renaming files” on page 192
- “Opening files on administered computers” on page 193
- “Viewing files from administered computers” on page 193
- “Creating shortcuts for files” on page 195
- “Creating folders” on page 196
- “Transferring files to administered computers” on page 197

Several file-related operations are described elsewhere in this manual:

- Distributing documents and media to managed mobile devices is described in “Distributing media to mobile devices” on page 169.
- Distributing software to administered desktop computers is described in “Installing software” on page 200.
- Distributing software to managed mobile devices is described in “Installing software on mobile devices” on page 157.
- Working with the registries of Windows computers is described in “Editing the registry” on page 136.

NOTE It is easier to work with files that are listed in the Files table of the Absolute Manage database. Searching for files to include them in the database is described in “Gathering information on files” on page 76.

Copying and moving files

Absolute Manage lets you copy or move files on administered computers to a different location on the same computer.

To move or copy files:

1. In any browser window showing files, select the files that you want to copy or move.

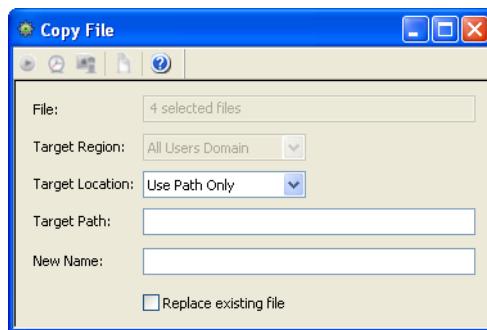
Note: If you would rather specify the computers first or if the file is not available in the Absolute Manage database, there is an alternative method for specifying the command target that is

described in "An alternative method of specifying files" on page 199.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Copy File/Folder** or **Move File/Folder**, depending on the desired action.

The **Copy File** or the **Move File** dialog opens. Both dialogs are very similar; the **Copy File** dialog is shown here:



Note: If you have selected only a single file, the path of that file is displayed in the File field.

3. Choose the target region and location and enter the path where the files are to be copied or moved.

The available target regions and locations are discussed in "Copy File/Folder" on page 318.

4. If you want to give the copied or moved files new names, enter the desired new name.

Note: If you have selected more than one file from the same target computer, trying to rename files will lead to errors.

5. If you want the copied or moved files to replace any files in the target folder that have the same name, check **Replace existing file**.

IMPORTANT

Deleted file cannot be recovered, short of using specialized tools that may or may not be successful.

6. Click **Execute**.

Absolute Manage copies or moves the files as specified. Any errors are noted in the command history.

Deleting files

You can use Absolute Manage to delete files on administered computers.

IMPORTANT

Deleted file cannot be recovered, short of using specialized tools that may or may not be successful.

To delete files:

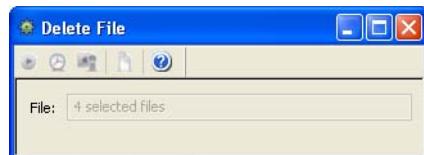
1. In any browser window showing files, select the files that you want to delete.

Note: If you would rather specify the computers first or if the file is not available in the Absolute Manage database, there is an alternative method for specifying the command target that is described in "An alternative method of specifying files" on page 199.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Delete File/Folder**.

The **Delete File** dialog opens:



*Note: If you selected only a single file, the path of that file is displayed in the **File** field.*

3. Click **Execute**.

Absolute Manage deletes all specified files immediately; there is no confirmation, and files are not just moved to the Recycling Bin.

Renaming files

Absolute Manage lets you rename files on administered computers.

To rename files:

1. In any browser window showing files, select the files that you want to rename.

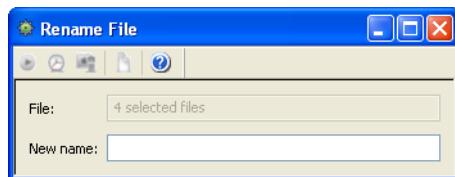
Note: If you would rather specify the computers first or if the file is not available in the Absolute Manage database, there is an alternative method for specifying the command target that is

described in “An alternative method of specifying files” on page 199.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Rename File/Folder**.

The Rename **File** dialog opens:



*Note: If you selected only a single file, the path of that file is displayed in the **File** field.*

3. Enter the new name for the files.

Note: If you have selected more than one file from the same directory on the same computer, trying to rename them will lead to errors.

4. Click **Execute**.

Absolute Manage renames the files.

Opening files on administered computers

You can use Absolute Manage to open files on administered computers locally, i.e., on the computers on which they reside. Since these files can be not only documents but also scripts and applications, this feature provides a way to perform some maintenance tasks.

This is described in “Executing local files” on page 132.

Viewing files from administered computers

Many kinds of files from administered computers can be viewed on administrator workstations. This includes any kind of text file (such as pure text, HTML, or code files) as well as standard types of system logs.

To view a file on one or more administered computers:

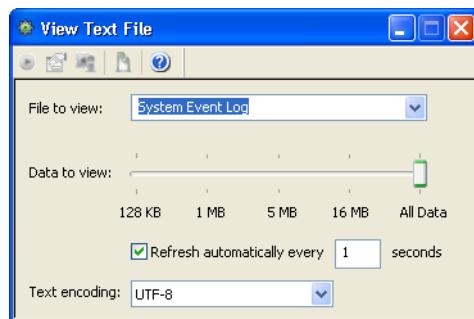
1. In any browser window, select the computers on which you want to view files.

*Note: If you select files in an Absolute Manage browser window before choosing the **View Text File** command, those files are pre-entered into the “File to view” field (see below).*

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **View Text File**.

The **View Text File** dialog opens:



3. To specify the file you want to view, do one of the following:

- Enter the file's full path in the **File to view** field.
For Mac OS X files, you can use the tilde (~) to refer to the current user's home directory.
For files on Windows target computers, you can use variables in the path.
- Choose one of the predefined files from the pop-up menu.

4. If you are specifying a large file and do not want to view all of it, use the Data to view slider to restrict the amount of data from the file that Absolute Manage is to display. Absolute Manage displays the specified amount of data at the end of the file.
5. To automatically refresh the file display in regular intervals, check the **Refresh automatically** option and specify the desired interval.
6. Choose the text encoding of the file you are about to view.

Note: Normally, we recommend that you choose UTF-8, which includes automated line-by-line checking of the actual encoding with conversion performed as required.

7. Click **Execute**.

Absolute Manage displays the content of the file in a new window on your workstation. If you have added multiple computers to the target

list, the files at the specified location on all computers are displayed, each in its own window.

You filter the displayed lines using the filter field at the top of the window. You can also save entire files to disk.

Creating shortcuts for files

Absolute Manage lets you create shortcuts of files (shortcuts on Windows) on administered computers in any location on the same computer.

To create shortcuts of files:

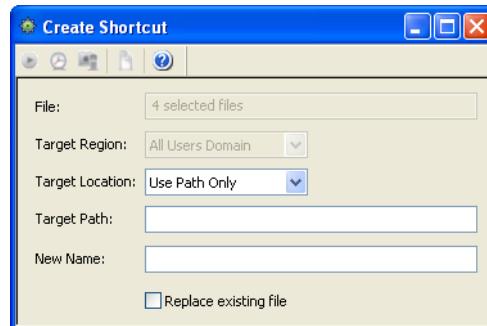
1. In any browser window showing files, select the files of which you want to create shortcuts.

Note: If you would rather specify the computers first or if the file is not available in the Absolute Manage database, there is an alternative method for specifying the command target that is described in "An alternative method of specifying files" on page 199.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Create Shortcut**.

The **Create Shortcut** dialog opens:



*Note: If you had selected only a single file, the path of that file is displayed in the **File** field.*

3. Choose the target region and location and enter the path where the shortcuts are to be created.

The available target regions and locations are discussed in "Copy File/Folder" on page 318.

4. If you want to give the shortcuts names that are different from the default names created by the operating system, enter the desired new name.

Note: If you have selected more than one file from one target computer, trying to name the shortcuts will lead to errors.

5. Click **Execute**.

Absolute Manage creates the shortcuts at the indicated locations on the same computers as the specified files.

Creating folders

Absolute Manage lets you create new folders on administered computers in any desired location.

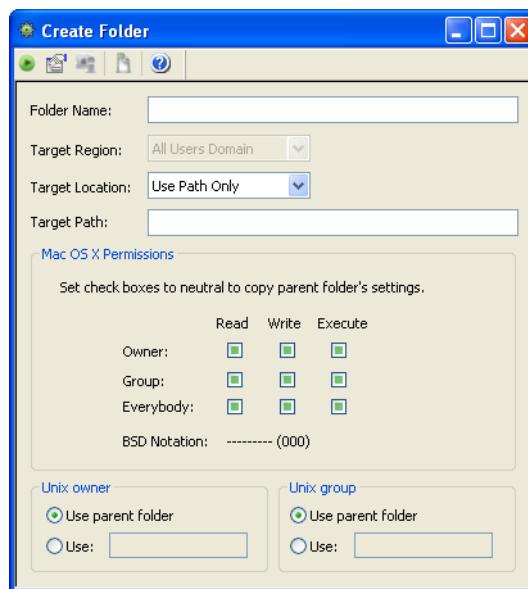
To create folders:

1. In any browser window showing files, select the computers on which you want to create the folders.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Create Folder**.

The **Create Folder** dialog opens:



3. Choose the target region and location and enter the path where the folders are to be created.

The available target regions and locations are discussed in "Copy File/Folder" on page 318.

4. If you create folders on Mac OS X computers, specify their access permissions, owner, and group.

In each case, you can choose between letting the folders inherit these settings from their parent folder or providing an explicit setting.

5. Click **Execute**.

Absolute Manage creates the folders at the indicated locations.

Transferring files to administered computers

You can use Absolute Manage to transfer files from your workstation to any location on administered computers.

This feature is primarily intended to allow you to quickly replace damaged files or provide missing files and perform similar support tasks. While you can use it to perform software installations as well, that is not its main intended application; we recommend that you check out the Software Distribution Center for software distribution, as described in “Installing software” on page 200.

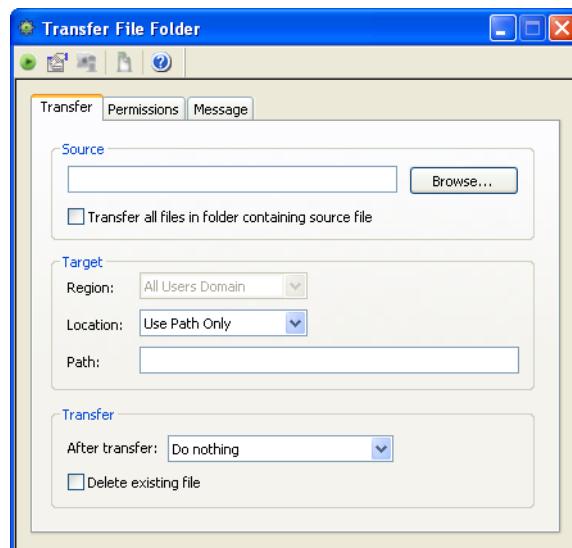
To transfer a file or folder from your workstation to administered computers:

1. In any browser window showing files, select the computers to which you want to transfer the files.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose **Transfer File/Folder**.

The **Transfer File/Folder** dialog opens:



3. Specify the file, folder, or Mac OS X disk image that you want to transfer, either by entering the path in the **Source** field or by clicking the **Select** button and choosing the desired object.

To choose a folder, press the Shift key while clicking **Select**.

4. If you have selected a file, you can check the **Transfer all files in folder containing source file** option to transfer the entire contents of the folder in which the selected file is located to the target computers.

If this option is not checked, only the file itself is transferred.

5. If you have selected a disk image, you can check the **Transfer contents of disk image** option to transfer the contents of the selected disk image file instead of the file itself.

In this case, the target settings in the dialog pane become unavailable; the files from the disk image are always copied to the boot volume at the same paths they have on the disk image.

6. Choose the target region and location and enter the path where the folders are to be created.

The available target regions and locations are discussed in “Copy File/Folder” on page 318.

7. If you copy the file or folder to Mac OS X computers, click the **Permissions** tab to specify the access permissions, owner, and group.



For owner, group, and each permission, you can choose between letting the folders inherit the setting from the source item on your computer or providing an explicit setting. For owner and group, you can also let the item inherit the setting from the enclosing folder on the target computer.

8. If you want to send a message to the user before the transfer begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “Sending messages” on page 115.

If you provide a **Cancel** button in the message dialog, the transfer is aborted on a target computer if a user clicks **Cancel**.

*Note: If a message has been specified, this is indicated by a dot in the dialog's **Message** tab.*

9. Click **Execute**.

Absolute Manage transfers the file or folder to the indicated location on the target computers. Any errors are noted in the command history.

An alternative method of specifying files

The file-manipulating procedures in this chapter all assume that you are specifying the desired files by selecting them in the **Files** window or another browser window displaying files and then adding the target computers (if there is more than one target).

Sometimes, it is easier to start with specifying the computers first and then entering the path of the file. In this case, the file does not need to be in the Files table of the Absolute Manage database, meaning that you do not have to search for it before being able to manipulate it.

NOTE This procedure does not work on multiple files at the same time.

To use this alternative method of working with files:

1. In any browser window, select the computers on which you want to manipulate the files.

Note: For information on specifying groups as targets, see “Targets” on page 286.

2. From the **Commands** menu, choose the desired file-related command.

The command's dialog opens.

3. In the **File** field, enter the path of the file.
4. Proceed with specifying the command options and executing the command, as described in the respective procedures.

While you can use Absolute Manage to manually install software on administered computers (see below), it really shines when you use the Software Distribution Center to automatically distribute software to any number of computers.

The Software Distribution Center can automatically install a specific range of applications on new computers as soon as they are put on the network. Or you can use it to distribute newly introduced or updated applications to specific workgroups or the organization.

NOTE Installing software on administered mobile devices works differently and does not use the Software Distribution Center. See “Installing software on mobile devices” on page 157 for details.

Using the Software Distribution Center is explained in:

- “Overview” on page 201
- “Setting up distribution points” on page 202
- “Setting up payloads” on page 209
- “Setting up software packages” on page 211
- “Setting up metapackages” on page 220
- “Setting up computer groups” on page 227
- “Performing installations” on page 232
- “Performing ad hoc installations” on page 233
- “Automated patch management” on page 235
- “Reinstalling a Mac OS X computer” on page 237
- “Reinstalling a Windows computer” on page 241

Creating installer packages

The Software Distribution Center is designed to work with software installer packages. You can create such packages with the Absolute Manage InstallEase companion tool that is included with Absolute Manage.

See the tool’s documentation for details on its use.

Installing software manually

While the Software Distribution Center is a powerful tool for software rollouts and other repeated installations, it is not always the optimal tool. When you just want to distribute a few files or do a one-off installation, other Absolute Manage functions are usually quicker:

- To copy individual files to one or more administered computers, we recommend using the **Transfer File/Folder** command, as described in “Transferring files to administered computers” on page 197.
- To run an installer application on one or more administered computers (if you do not plan to do so repeatedly), you can use

the **Execute Macintosh File** or **Execute Windows File** commands, depending on the target platform. They are described in “Executing files from your computer” on page 129.

Monitoring installed software

Absolute Manage lets you monitor which software is installed on client computers. This is not done by evaluating the log of software installations through Absolute Manage but by scanning the computers for software and installer receipts. The process is described in “Manually gathering information on installed software” on page 75.

Overview

The Software Distribution Center is a module of the Absolute Manage Server that offers automatic server-based software distribution. It is controlled from the **Server Center** window.

This section explains the basics of the Software Distribution Center structure, setup, and use. It also includes references to detailed instructions.

Prerequisites

Some features of the Software Distribution Center can be used only by administrators whose accounts have certain rights set.

Configuring administrator accounts is described in “Administrator accounts” on page 48.

Structure

The software distribution system has four key components:

- **Distribution points** are servers that host the files to be installed. There can be any number of distribution points, allowing you to place them in a way that minimizes network traffic.
One of the distribution points is defined as the master; all others are mirror servers. The software installers present on the master distribution point are automatically distributed to the mirror servers so that all distribution points always have the same range of software available without requiring any manual maintenance.
There is comparatively little network traffic to the Absolute Manage Server (in its capacity as the Software Distribution Center) as it does not itself distribute the software installers.
- **Payloads** are files or folders that are to be installed. They can be created from local files but are always stored on distribution points.

- **Software packages** are combinations of references to payloads with metadata regarding the target requirements and scheduling of the installation.
Software packages come in two flavors: Standard packages contain payloads, while metapackages contain other software packages (including metapackages).
- **Computer groups** are collections of computers that are to receive the same software.

When these components are set up, the actual installation is almost completely automatic, requiring you only to indicate which software packages are to be installed in which computer groups.

Setup

Setting up the Software Distribution Center consists mainly of defining the key components – distribution points, payloads, software packages, and computer groups. This is done in the Absolute Manage Admin's **Server Center** window, as described in the following sections:

- "Setting up distribution points" on page 202
- "Setting up payloads" on page 209
- "Setting up software packages" on page 211
- "Setting up computer groups" on page 227

Only in some cases do you need to configure agents:

- Where you have assigned more than one Absolute Manage Server to some or all agents. This requires you to specify for each agent which of the Absolute Manage Servers is to act as the software distribution server. This is necessary because, while any number of inventory servers can be assigned to one agent, each agent may have only one software distribution server.
- Where the software distribution server is not the inventory server (i.e., main Absolute Manage Server) assigned to the agent.

In this case, you need to explicitly assign the desired software distribution server to the agent using the **Agent Settings** command. This is described in "Assigning software distribution or license monitoring servers to agents" on page 57.

You can use the same command to specify the interval in which the agent queries the software distribution server for new software.

Setting up distribution points

Distribution points are computers designated to hold software installers for the Software Distribution Center and distribute them to agents.

Distribution point basics

Any Mac OS X or Windows computer can be used as a distribution point. A folder on this computer must be specified in which the software installers will be kept for distribution to clients.

Absolute Manage Agent must be installed on each distribution point. The software distribution server setting must be correctly specified on each of these agents (using the **Servers** tab in the **Agent Settings** dialog): It must point to the main Absolute Manage Server.

One of the distribution points is set to be the master. All payloads are initially uploaded only to this master distribution point by the Absolute Manage Admin. Absolute Manage then distributes the packages transparently in the background to the other distribution points, called mirrors.

Choosing a server as a distribution point

For reasons of reliability and performance we strongly recommend to use only dedicated servers as distribution points, i.e., computers on which only server processes are running and that are not used as workstations by local users.

NOTE Make sure to update the Absolute Manage Agent on a distribution point computer to the latest version (or the same version as that of Absolute Manage Server). Otherwise, you may experience difficulties in distributing software.

There is no problem in principle in letting a distribution point run on the same computer as Absolute Manage Server.

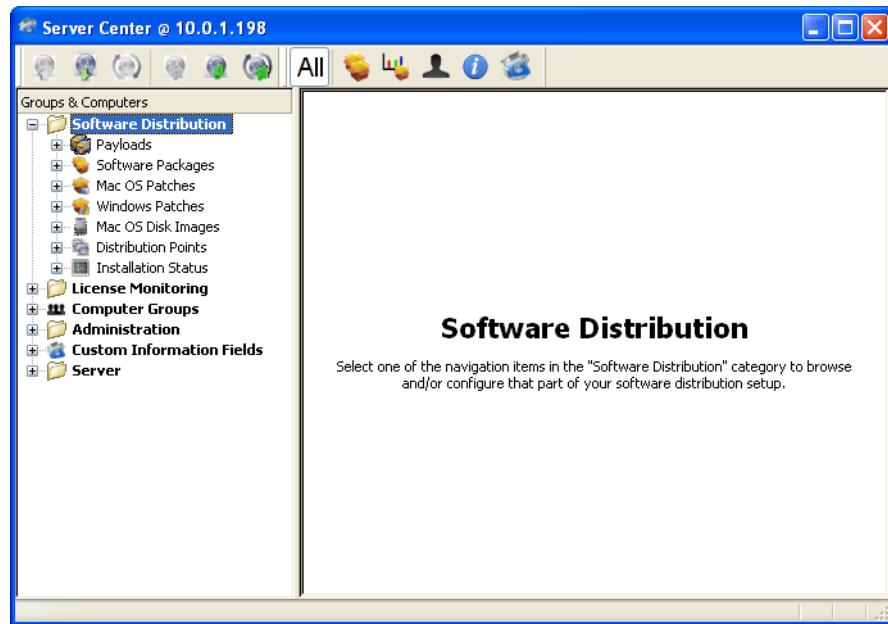
The support of Absolute Manage for multiple distribution points allows you – if the hardware is available – to place distribution points throughout your network, close to the served workstations. Ideally, each network zone would have its own distribution point to minimize interzone traffic.

NOTE As the software distribution server – the central Absolute Manage Server – creates a low amount of traffic, there is no significant performance penalty in having just a single such server.

Specifying the distribution point in the Software Distribution Center

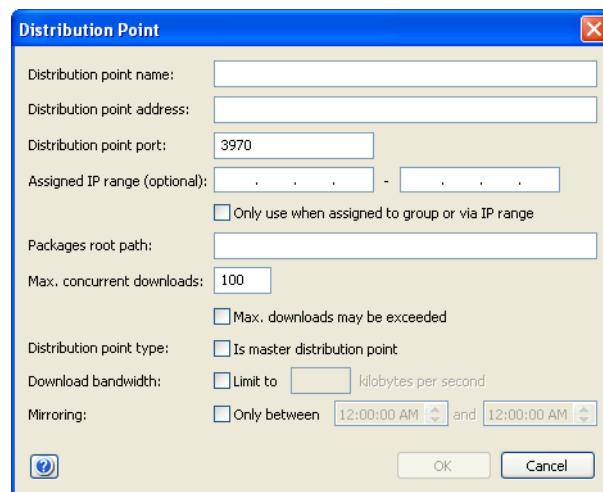
To make the distribution point available in the Software Distribution Center:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.



2. From the sidebar context menu, choose **New Distribution Point**.

The **Distribution Point** dialog opens:



3. Enter the desired name in the **Distribution point name** field.

This name is used only inside the Absolute Manage system; you can choose whatever name you like.

4. Enter the distribution point address – either the IP number or the DNS name – and the port on which the Absolute Manage Agent on the distribution point communicates.

Note: We recommend that you do not change the default port unless you have a specific reason for doing so.

5. In a setup with multiple distribution points, any distribution point can normally serve any agent. If you want to restrict a distribution point to a certain group of clients (e.g., one particular satellite office), specify a range of IP addresses in the **Assigned IP range** fields.

Note: You can also assign a distribution point to a computer group, making it the preferred distribution point for downloads from computers in that group. To assign a distribution point to a group, click the Distribution Points icon in the Server Center window after you have completed specifying the distribution point and drag it to the desired computer group.

6. Enter the path of the folder in which Absolute Manage is to store the software installers on this distribution point.

Note: The contents of this folder is managed entirely by Absolute Manage. Do not manually delete from or add to this folder.

7. Specify the maximum number of concurrent software downloads (agents downloading the software installers) the distribution point will provide.

If you want this limit to be exceedable in cases where an agent wants to download an installer but no distribution point has available download slots, check **Max. downloads may be exceeded**.

If the option is unchecked, the download attempts by the agent will be deferred in situations where no distribution point has download capacity. That means that the software installation on the clients concerned will still happen, only at a later time.

8. If you want this distribution point to be the master distribution point, check the **Is master distribution point** option.

If the option is unchecked, the distribution point will become a mirror that receives all its software installers automatically from the master distribution point.

There must always be exactly one master distribution point. Because the master distribution point must be up and running for the proper functioning of the software distribution and because it receives more traffic than mirror distribution points, we recommend that you designate a reliable computer with high-bandwidth network connections as the master distribution point.

9. If you want to limit how much network bandwidth is used for downloads from this distribution point (both for providing installers to clients and for mirroring to other distribution points), enter the desired limit in **Download bandwidth**.
10. If mirroring is to be limited to a certain time of the day (e.g., after hours), check the **Only between** option and enter the desired interval.

Note: Because of a limitation in the operating system, midnight at the end of the day cannot be specified as "24:00" when using a 24-hour clock. Enter "0:00" instead.

11. Click **OK** to close the dialog.
12. To store the distribution point specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new distribution point becomes available to the Software Distribution Center only after you have done so.

Editing distribution points

To edit an existing distribution point definition:

1. Select the server in the **Server Center** window and choose **Edit Distribution Point** from the sidebar context menu.

The **Distribution Point** dialog opens.
2. Make the desired changes and click **OK**.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Changing the master distribution point

There must always be exactly one master distribution point in the software distribution system. Changing it – designating a different distribution point as the master – therefore requires a specific procedure. The exact steps are different depending on whether the new server has been used as a mirror distribution point before or not.

If the new server already is a mirror distribution point:

1. Make sure that the intended new master distribution point has all the software that the current master distribution point has.

If you have recently made changes to payloads or have created new ones, you may want to compare the total size of the contents of the package root folders on the computers.

2. Edit the existing master distribution point specification as described in **Editing distribution points**, above. Uncheck the **Is master distribution point** option and click **OK**.
3. Edit the specification for the intended new master distribution point in the same way, checking the **Is master distribution point** option.

Absolute Manage displays a dialog informing you of options to transfer the required payloads.

4. Click the **Manually Copy Folder** button.

You do not actually need to copy anything as all required installers are already present on the new master distribution point.

5. From the Server menu, choose **Save Distribution and Licensing Info** to upload the new definitions to the Absolute Manage Server.

The new master distribution point is now active; the previous master distribution point is now a mirror distribution point.

If the new master distribution point has not been used as a distribution point so far:

1. Make sure that the Absolute Manage Agent is installed on the intended new master distribution point.
2. Manually create the package root folder on the intended new master distribution point.
3. Copy the entire contents of the package root folder from the existing master.

Note: There is an alternative process for switching master distribution points in which Absolute Manage Admin re-uploads all the payloads. If you want to follow that process, make sure that the source files for all payloads are available on your computer. Note, however, that all automatically created software patches are lost in this procedure and must be redownloaded from Apple's and Microsoft's servers. Delete all these patches from the Software Distribution System before switching the server.

4. Define the new master distribution point as described in **Specifying the distribution point in the Software Distribution Center**, above. Make sure to check the **Is master distribution point** option.
5. Edit the existing master server specification as described in **Editing distribution points**, above. Uncheck the **Is master distribution point** option and click **OK**.

Absolute Manage displays a dialog informing you of options to transfer the required software installers.

6. Click the **Manually Copy Folder** button.

You do not actually need to copy anything now as you have already done so in step 3, above.

*Note: If you follow the alternative procedure, click the **Re-Upload Payloads** button.*

7. From the **Server** menu, choose **Save Distribution and Licensing Info**.

If you follow the alternative method, Absolute Manage Admin will now attempt to upload the source files for all payloads to the new master distribution point. If this does not succeed for all payloads, Absolute Manage Admin notifies you of the fact and marks all payloads that could not be uploaded as "Source missing" in the **Upload Status** column.

*Note: You may need to add the column to the **Server Center** window to see the information.*

Open each failed payload and respecify the source file. When you are done, choose **Save Distribution and Licensing Info** again.

The new master distribution point is now active; the previous master distribution point is now a mirror. If you have chosen to re-upload payloads, it may take a while before the distribution point is ready, depending on the number and size of the payloads.

Removing distribution points

To remove an existing distribution point definition:

1. Select the distribution point in the **Server Center** window and choose **Remove Distribution Point** from the sidebar context menu.

A confirmation message is displayed.

2. Confirm the decision.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

Until you do this, the distribution point is still available.

NOTE Before you can remove the last remaining distribution point, you must delete all computer groups, payloads, software packages, and disk images in the Software Distribution Center.

Setting up payloads

Payloads are files or folders that are to be installed on the client computers. Payloads are stored on distribution points and referenced in installation packages.

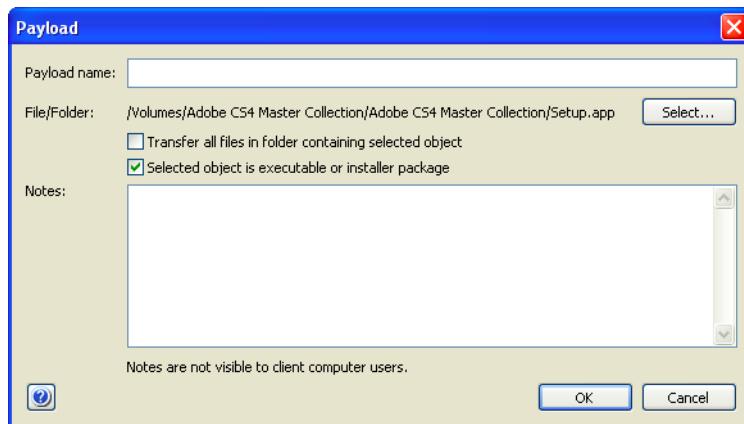
NOTE Due to limitations of the Windows operating system, payloads for Mac OS X clients must be created on administrator computers running Mac OS X.

NOTE Setting up payloads is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 481 for details.

To set up a payload:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. From the sidebar context menu, choose **Software Distribution > New Payload**.

The **Payload** dialog opens:



3. Enter the desired name in the **Payload name** field.

This is the name by which the payload will be known in Absolute Manage; you can choose whatever name you like.

4. Click the **Select** button and specify the file or folder to install.

If you want to create a package for Mac OS X targets, you must do so on a Mac OS X computer.

Note: You can use Absolute Manage InstallEase to create custom installers.

You can specify a disk image (created manually or with Absolute Manage InstallEase) as the file. In that case, any files in the disk image are copied to the same locations on the target hard disk; any missing folders are automatically created by Absolute Manage.

5. If the specified file is not self-contained – i.e., if it requires additional files to be present, as is usually the case for MSI installers – make sure that these files are located in the same folder as the installer and check **Transfer all files in folder containing executable**.
6. If the selected file is an application, a system script, or an installer package, check **Selected object is executable or installer package**.
7. Optionally you can enter a short description of the package in the **Notes** field.
8. Click **OK** to close the dialog.
9. To store the payload on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu. Absolute Manage uploads the payload to the master distribution point, compressing and encrypting it in the process. It also creates a checksum that is verified by agents during installations. When the payload has been successfully uploaded to the master server, its specification is stored on the Absolute Manage Server. Mirroring to any additional distribution points happens automatically in the background.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new software package becomes available to the Software Distribution Center only after you have done so.

Editing payloads

To edit existing payloads:

1. Select the payload in the **Server Center** window and choose **Edit Payload** from the sidebar context menu.

The **Payload** dialog opens.
2. Make the desired changes and click **OK**.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Removing payloads

To remove existing payloads:

1. Select the payloads in the **Server Center** window and choose **Remove Payloads** from the sidebar context menu.

A confirmation message is displayed.

2. Confirm the decision.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

Until you do this, the payloads are still available.

Setting up software packages

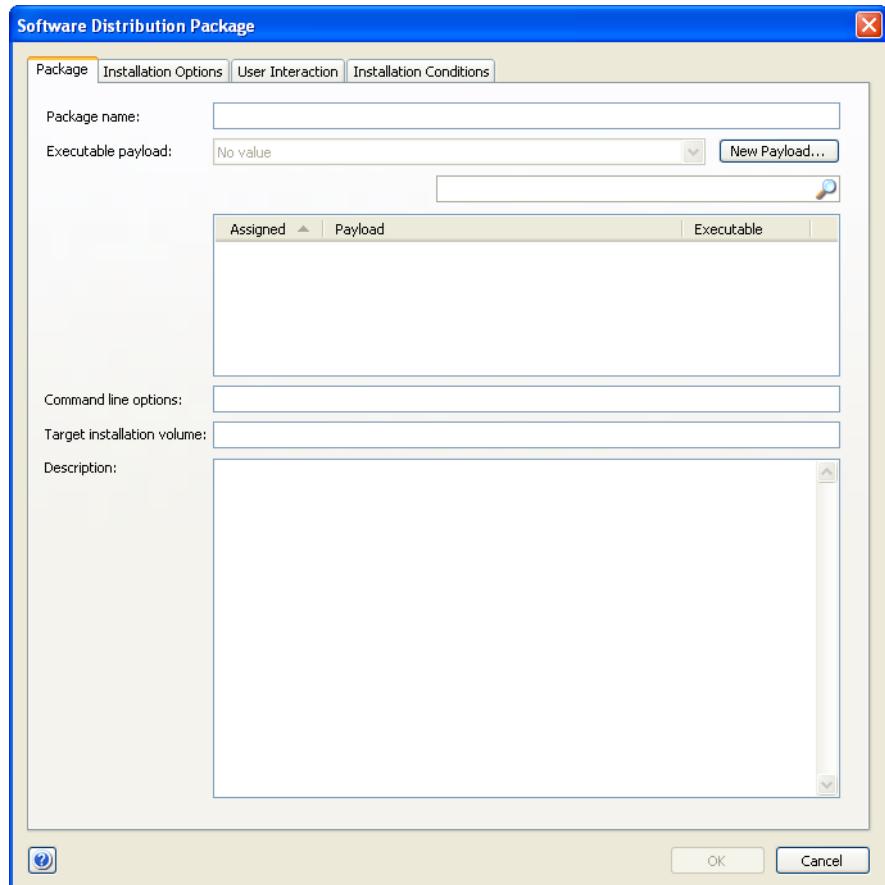
Software packages are combinations of references to payloads on a distribution point and additional metadata. They represent a software installation within the Software Distribution Center.

NOTE Setting up software packages is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 481 for details.

To set up a software package:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. From the sidebar context menu, choose **New Software Package**.

The **Software Distribution Package** dialog opens:



In the **Package** tab, you specify the payloads to be used.

Note: Never use the Absolute Manage Agent updater as the payload in packages you generate. Absolute Manage automatically generates update packages for agents, and you must only use those packages. See "Updating the Agent" on page 42 for details on updating agents.

3. Enter the desired name for the software package in the **Package name** field. Optionally you can also enter a short description of the package in the **Description** field.

This name is used only inside the Absolute Manage system; you can choose whatever name you like.

4. Specify the payloads that are to be included in the package.

All payloads that are available on the distribution points are listed in the dialog pane.

You can add new payloads by clicking the **New Payload** button; proceed as described in "Setting up payloads" on page 209.

You can filter the displayed payload by entering parts of their names in the search field above the list of payloads.

Check all payloads that are to be included in the package.

5. From the **Executable payload** pop-up menu, choose the executable payload of the package.

There must always be exactly one executable payload in each package. This is the payload that is launched by the agent after all payloads have been copied to the target computer.

6. Optionally, you can specify command-line options in the **Command line options** field.

You can include environment variables in the options, as described in "Environment variables" on page 137.

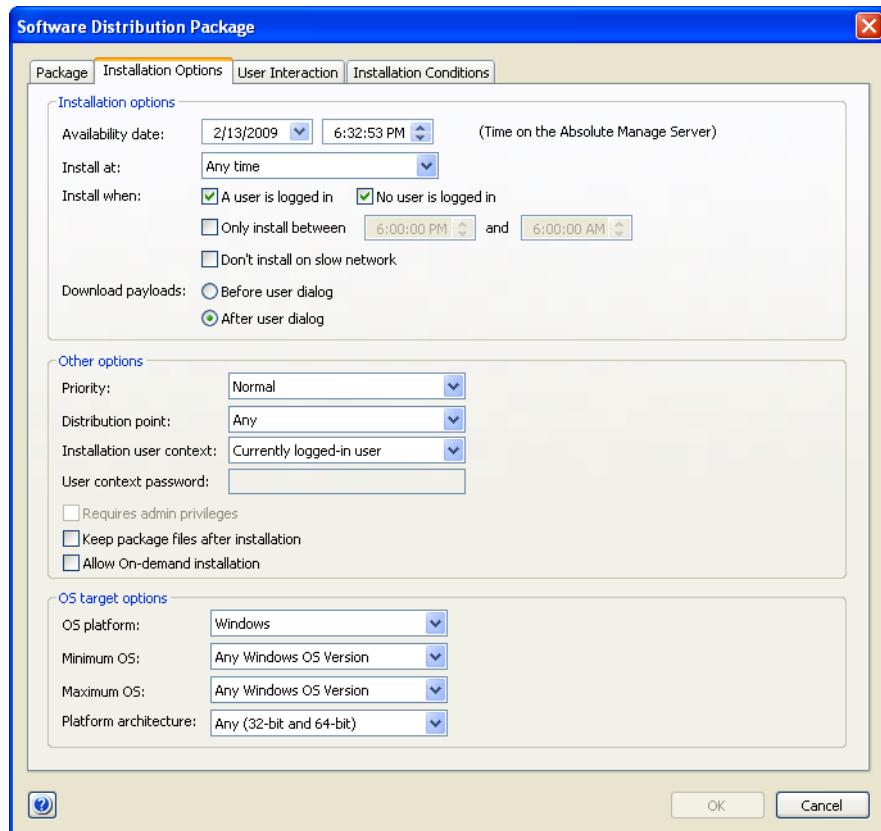
When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, Absolute Manage adds the `/qn` option (`/quiet /norestart` for MSU files) to run the installer silently.

When you add your own options or when another type of installer is selected, you have to provide the command line parameters for a silent installation yourself.

7. For Mac OS X installers, you can specify a desired installation volume in the **Target installation volume** field.

If this field is left empty, the installation will be performed on the boot volume.

To specify requirements and timing options, click the **Installation Options** tab:



8. If you do not want to make the software package available immediately, enter the earliest time when agents can install it in the **Availability date** field.
9. Normally, agents install software packages meant for them as soon as they become available. The **Install at** pop-up menu and **Install when** options lets you modify this behavior:
 - You can instruct the agent to wait until the next startup of the administered computer or user login (choose **Next startup** or **Next login**). The latter is particularly useful when the installer requires a user to be logged in.
 - You can specify that the package can be installed when a user is logged in on the target computer, when no user is logged in, or in both cases.
*Note: It is possible to check both options, which is indeed the default. At least one of the two options must be checked. When the user is allowed to refuse the installation (in the **User Interaction** pane, see below), the package can only be installed when a user is logged in.*
 - You can also specify that installations only happen during certain times, e.g., after hours when the office is not busy (**Only install between**).

10. If the package is to be installed only over fast networks, check **Don't install on slow network**.

A network is considered slow when its nominal data rate is less than 100 Mbit/s.

11. Specify via the **Download payloads** setting when the agent is to download the payloads, before or after a user dialog is displayed.

Downloading the payloads before displaying the dialog makes for snappier responses after the user answers the dialog but may mean unnecessary network traffic if the user refuses the installation. Downloading the payloads after displaying the dialog avoids unnecessary traffic but makes users wait for the download to happen after they have agreed to the installation.

If no user dialog is displayed, the **Download payloads** setting is ignored.

12. Specify a priority if desired. The priority determines the order in which an agent installs packages when several are available simultaneously.

13. If you want to restrict the distribution points from which an agent may download the payloads of this software package to assigned distribution points (from the agent's local subnet or from a computer group to which the agent's computer belongs), choose an option from the **Distribution point** pop-up menu.

If you choose **From assigned distribution point if available**, the agent tries to download the payloads from an assigned distribution point. If no such distribution point is available, it chooses a different one. If you choose **From assigned distribution point only**, the installation fails if there is no assigned distribution point.

14. Specify the user account that is to be used for installations.

Normally, this will be the current local user on each computer. You can specify a different account. For Windows only, you must also specify the account's password in this case. When you specify a Windows domain username, you must prefix it with the domain and \.

You can also specify that the installation be performed in the context of the system user.

If the installation requires administrator privileges on Mac OS X, check the **Requires admin privileges** option.

Note: This latter option does not change the used account; it merely temporarily boosts the privileges available to the installation process.

15. If you want the installation files to remain on the target computers after the installation has finished, check **Keep package files after installation**.

If this option is unchecked, the agents delete the downloaded payloads after the installation is complete.

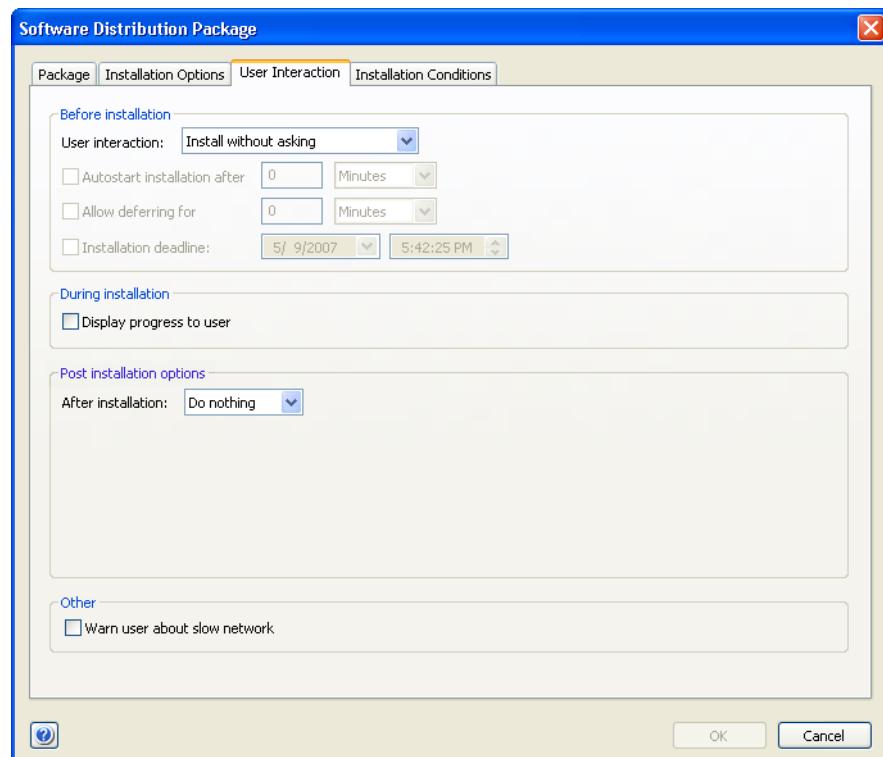
16. If you want the users to start the installation of this package on their own schedule – creating a package for pull installation instead of push installation – check the **Allow on-demand installation** option.

Checking this option disables a number of other options in the **Installation Options** and **User Interaction** panes.

17. Specify the operating system platform – Mac OS X or Windows, optionally restricted to just client or just server systems – and any minimum and/or maximum versions required by the software.

If desired, choose an option from the **Platform architecture** pop-up menu to restrict installation of the package to Intel or PowerPC processors (Mac OS X) or 32-bit or 64-bit systems (Windows), respectively.

18. Click the **User Interaction** tab to specify which information is presented to users and what interaction options they have for the installation:



19. Specify in the **Before installation** pop-up whether the user is to be notified or have the option to postpone or refuse the installation.

Depending on the option chosen, additional settings become available:

You can specify that the installation is automatically started after a certain time if the notification should not be answered by the user.

You can also specify that the installation cannot be postponed for more than a certain interval or beyond a certain date.

Note: If you specify both an interval and a deadline, the earlier of the two resulting dates is effective.

20. If the user is to be informed of the progress of an installation under way, check **Display progress to user**.
21. From the **After installation** pop-up menu, choose the desired action that Absolute Manage Agent is to perform when the installation is complete.

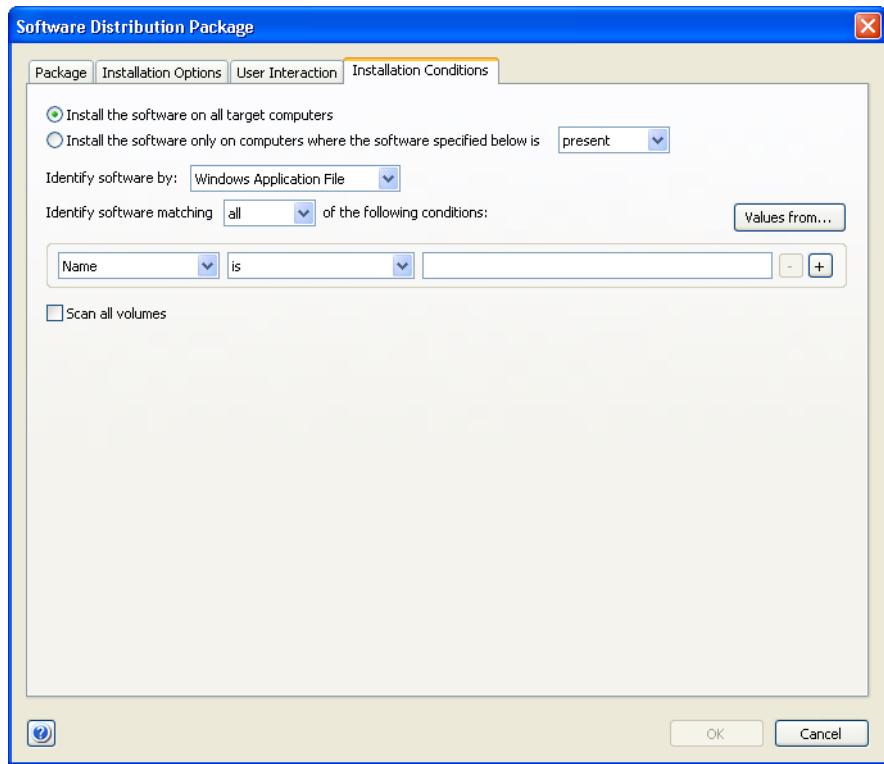
Depending on your choice, additional options may become available.

You can specify an interval after which a notification is automatically closed.

When a restart is to be performed, you can specify that the user is notified in advance. You may give him or her the opportunity to defer the restart, specify that the restart happens automatically after a certain time when the notification is not answered, and have the notification reappear in regular intervals.

22. If desired, check **Warn user about slow network** to inform users when their network connection to the distribution point has a nominal speed of less than 100 Mbit/s.

23. If desired, click the **Installation Conditions** tab to limit the package to be installed only on computers that meet certain prerequisites:



24. To have the software installed on all computers that belong to the computer groups to which the package is assigned, choose **Install the software on all target computers**.

To have it installed only on certain computers, choose **Install the software only on computers where the software specified below is** and specify the appropriate conditions. The available settings are similar to the ones in “Setting up license specifications” on page 249.

25. If an executable payload containing an Adobe CS3 or CS 4 installer or updater is assigned to this software package, you can set additional options as described in **Setting options for Adobe CS3 and CS 4**, below.
26. Click **OK** to close the dialog.

27. To store the software package specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu. Absolute Manage creates the package definition on the Absolute Manage Server.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new software package becomes available to the Software Distribution Center only after you have done so.

Setting options for Adobe CS3 and CS 4

If a software package is assigned a payload containing an Adobe CS3 or CS 4 installer or updater, an additional pane, **Adobe CS Options**, becomes available.

NOTE The settings in this tab are not compatible with Adobe CS 5 or newer. For remotely distributing these versions of Adobe CS, prepare an installer using Adobe Application Manager Enterprise Edition (AAMEE) and use that installer to create a standard software distribution package in Absolute Manage Admin.

To set Adobe CS options:

1. Click the **Adobe CS Options** tab.
2. Click **Use the following settings for installation**.

If you click **Use command line options for installations**, all other settings in this pane are disregarded. If you choose that option, customize the installer's behavior via the command line options in the **Package** pane, as described in step 6 of the previous procedure.

3. Check the desired components for installation or uninstallation in the scrolling list.
4. From the **Action** pop-up menu, choose whether to install or uninstall the software.
5. If desired, enter a serial number in the **Serial number** field.
6. Check the other options as desired.

The options are explained in "Adobe CS Options" on page 451.

Editing software packages

To edit existing software package definitions:

1. Select the packages in the **Server Center** window and choose **Edit Software Package** from the sidebar context menu.

The **Software Distribution Package** dialog opens.

2. Make the desired changes and click **OK**.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Besides changing options for the packages, you can also use this process to specify different payloads, e.g., when a new version has become available.

Removing software packages

To remove existing software package definitions:

1. Select the packages in the **Server Center** window and choose **Remove Software Package** from the sidebar context menu.
A confirmation message is displayed.
2. Confirm the decision.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

Until you do this, the software packages are still available.

Setting up metapackages

Metapackages are combinations of references to software packages and additional metadata. They represent a software installation within the Software Distribution Center.

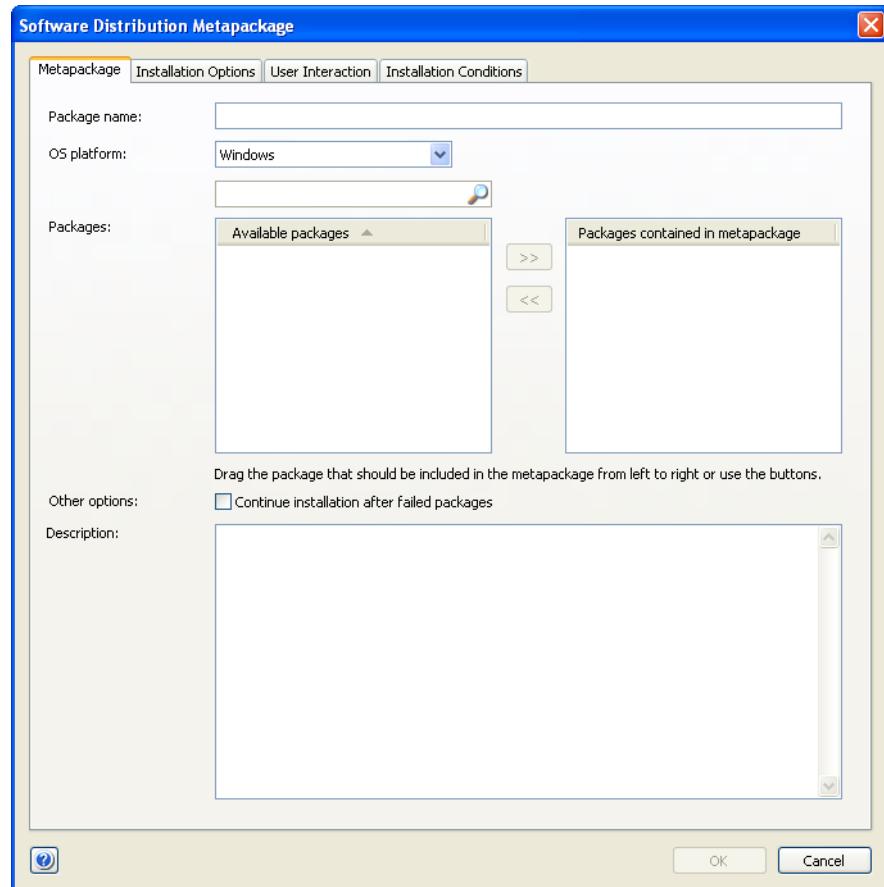
NOTE Setting up metapackages is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 481 for details.

To set up a metapackage:

NOTE The settings you make for the metapackage override any conflicting settings for the software packages and metapackages included in the metapackage.

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. From the sidebar context menu, choose **Software Distribution > New Metapackage**.

The **Metapackage** dialog opens:



In the **Package** tab, you specify the packages to be used.

3. Enter the desired name for the metapackage in the **Package name** field. Optionally you can also enter a short description of the package in the **Description** field.

This name is used only inside the Absolute Manage system; you can choose whatever name you like.

4. Choose the desired target operating system platform from the **OS platform** pop-up menu.
5. Specify the software packages that are to be included in the metapackage.

All packages that are available on the distribution points, including other metapackages, are listed in the dialog pane.

You can filter the displayed packages by entering parts of their names in the search field above the list of packages.

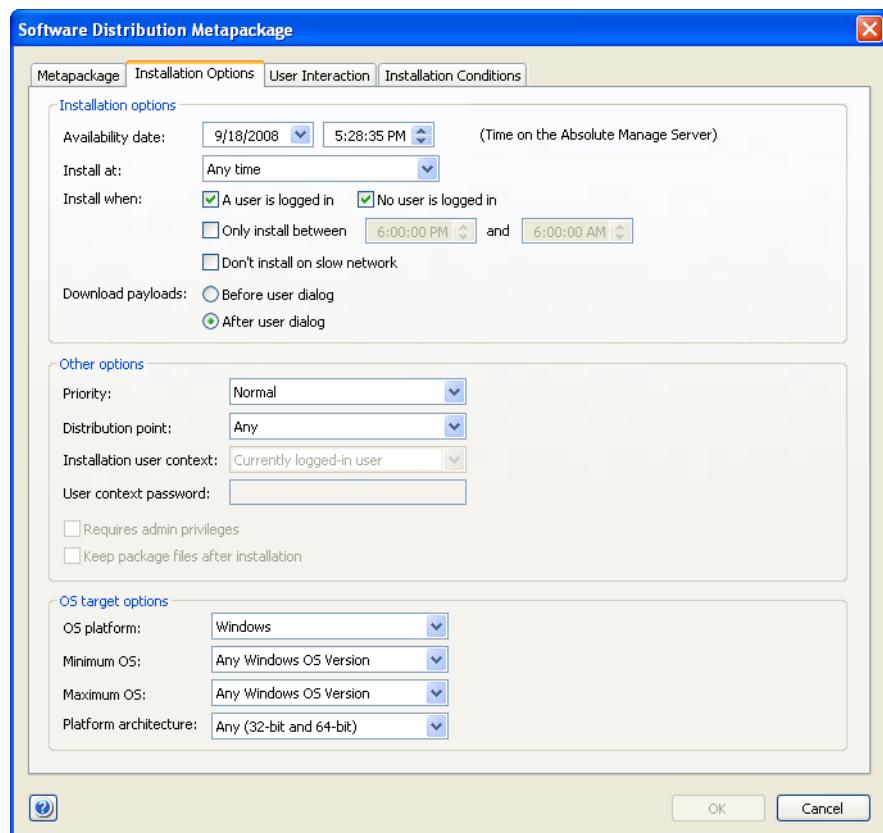
Drag all payloads that are to be included in the metapackage from the left-hand list to the right-hand list.

You can reorder packages in the right-hand list by dragging them higher or lower in the list. Absolute Manage installs packages contained in a metapackage in the order in which they are listed.

6. If you want Absolute Manage to continue installing packages on a client even after the installation of one package fails, check **Continue installation after failed packages**.

If the option is unchecked, a failed package causes the installation of the metapackage to stop.

7. To specify requirements and timing options, click the **Installation Options** tab:



8. If you do not want to make the metapackage available immediately, enter the earliest time when agents can install it in the **Availability date** field.
9. Normally, agents install metapackages meant for them as soon as they become available. The **Install at** pop-up menu and **Install when** options lets you modify this behavior:
 - You can instruct the agent to wait until the next startup of the administered computer or user login (choose **Next startup** or **Next login**). The latter is particularly useful when the installer requires a user to be logged in.

- You can specify that the metapackage can be installed when a user is logged in on the target computer, when no user is logged in, or in both cases.
*Note: It is possible to check both options, which is indeed the default. At least one of the two options must be checked. When the user is allowed to refuse the installation (in the **User Interaction** pane, see below), the package can only be installed when a user is logged in.*
- You can also specify that installations only happen during certain times, e.g., after hours when the office is not busy (**Only install between**).

10. If the package is to be installed only over fast networks, check **Don't install on slow network**.

A network is considered slow when its nominal data rate is less than 100 Mbit/s.

11. Specify via the **Download payloads** setting when the agent is to download the payloads of the contained packages, before or after a user dialog is displayed.

Downloading the payloads before displaying the dialog makes for snappier responses after the user answers the dialog but may mean unnecessary network traffic if the user refuses the installation. Downloading the payloads after displaying the dialog avoids unnecessary traffic but makes users wait for the download to happen after they have agreed to the installation.

If no user dialog is displayed, the **Download payloads** setting is ignored.

12. Specify a priority if desired. The priority determines the order in which an agent installs packages when several are available simultaneously.
13. If you want to restrict the distribution points from which an agent may download the payloads for this metapackage to assigned servers (from the agent's local subnet or from a computer group to which the agent's computer belongs), choose an option from the **Distribution point** pop-up menu.

If you choose **From assigned distribution point if available**, the agent tries to download the payloads from an assigned distribution point. If no such distribution point is available, it chooses a different one. If you choose **From assigned distribution point only**, the installation fails if there is no assigned distribution point.

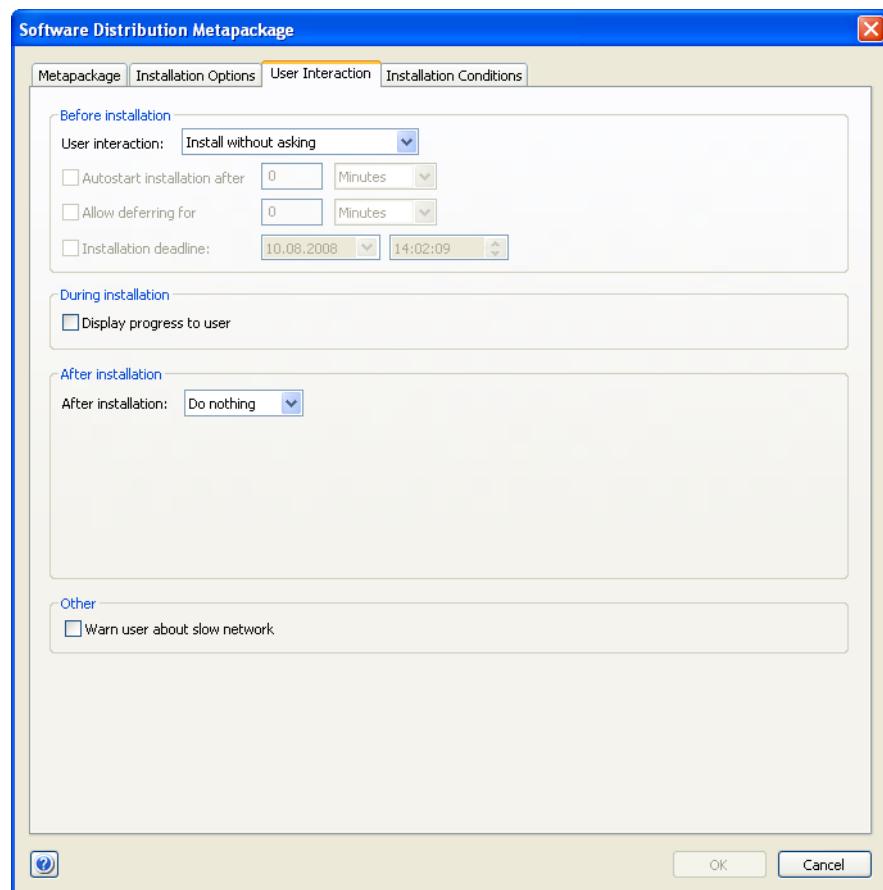
14. The user context cannot be set in a metapackage; it is taken from the individual packages.

Likewise, the software packages determine which payloads are kept after installation and which are deleted.

- Specify the operating system platform – Mac OS X or Windows, optionally restricted to just client or just server systems – and any minimum and/or maximum versions required by the software.

If desired, choose an option from the **Platform architecture** pop-up menu to restrict installation of the package to Intel or PowerPC processors (Mac OS X) or 32-bit or 64-bit systems (Windows), respectively.

- Click the **User Interaction** tab to specify which information is presented to users and what interaction options they have for the installation:



- Specify in the **Before installation** pop-up whether the user is to be notified or have the option to postpone or refuse the installation.

Depending on the option chosen, additional settings become available:

You can specify that the installation is automatically started after a certain time if the notification should not be answered by the user.

You can also specify that the installation cannot be postponed for more than a certain interval or beyond a certain date.

Note: If you specify both an interval and a deadline, the earlier of the two resulting dates is effective.

18. If the user is to be informed of the progress of an installation under way, check **Display progress to user**.
19. From the **After installation** pop-up menu, choose the desired action that Absolute Manage Agent is to perform when the installation is complete.

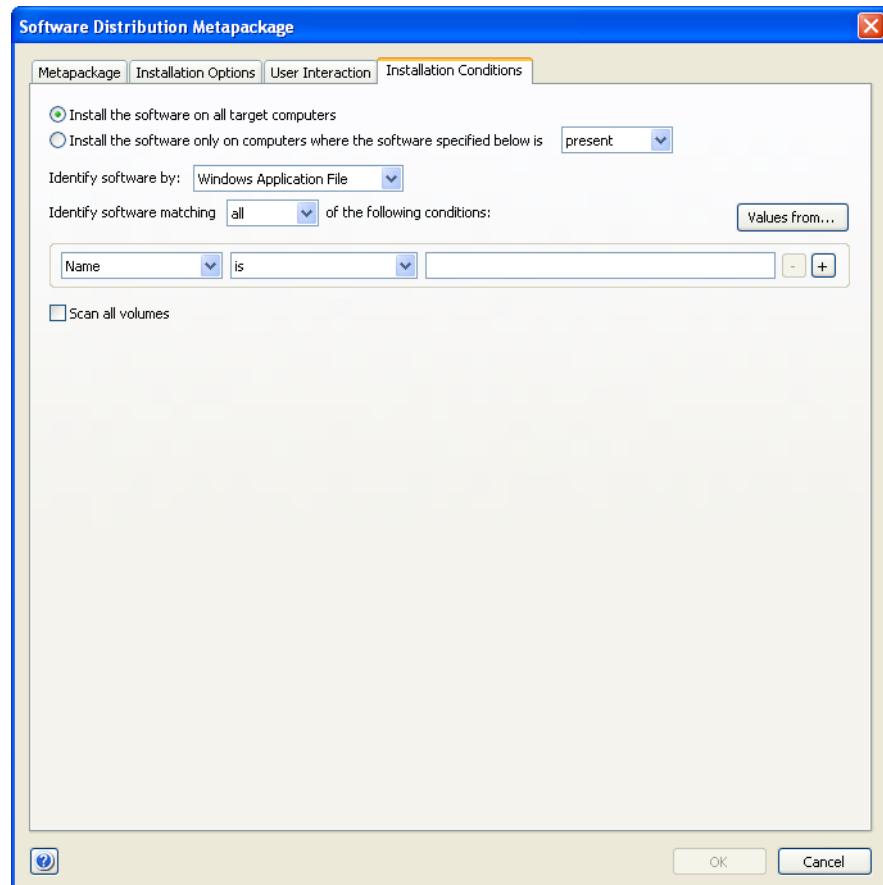
Depending on your choice, additional options may become available:

You can specify an interval after which a notification is automatically closed.

When a restart is to be performed, you can specify that the user is notified in advance. You may give him or her the opportunity to defer the restart, specify that the restart happens automatically after a certain time when the notification is not answered, and have the notification reappear in regular intervals.

20. The **Warn user about slow network** setting is taken from the individual software packages.

21. If desired, click the **Installation Conditions** tab to limit the package to be installed only on computers that meet certain prerequisites:



22. To have the software installed on all computers that belong to the computer groups to which the metapackage is assigned, choose **Install the software on all target computers**.

To have it installed only on certain computers, choose **Install the software only on computers where the software specified below is** and specify the appropriate conditions. The available settings are similar to the ones in “Setting up license specifications” on page 249.

23. Click **OK** to close the dialog.
24. To store the metapackage specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu. Absolute Manage creates the package definition on the Absolute Manage Server.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new metapackage becomes available to the Software Distribution Center only after you have done so.

Editing metapackages

To edit existing metapackage definitions:

1. Select the metapackages in the **Server Center** window and choose **Edit Software Package** from the sidebar context menu.
The **Metapackage** dialog opens.
2. Make the desired changes and click **OK**.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Besides changing options for the metapackages, you can also use this process to specify different contained packages.

Removing metapackages

To remove existing metapackage definitions:

1. Select the metapackages in the **Server Center** window and choose **Remove Software Package** from the sidebar context menu.
A confirmation message is displayed.
2. Confirm the decision.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

Until you do this, the metapackages are still available.

Setting up computer groups

Computer groups are collections of computers that are to be handled the same for software distribution or license monitoring. One computer can belong to multiple computer groups, allowing great flexibility through overlapping groups.

There are standard and smart computer groups:

- Standard computer groups are maintained manually – computers are added and removed by explicit administrator decision. The group is defined by the computers it contains.
- Smart computer groups are maintained automatically. They are defined by one or more criteria and contain all computers meeting those criteria. Absolute Manage automatically adds a computer to a group when it meets the criteria and automatically removes it if it no longer does.

Although standard and smart groups can be used in the same way, they are defined and edited differently, as described below.

NOTE The same computer groups are available for license monitoring and software distribution.

Setting up standard computer groups

Standard computer groups are arbitrary collections of computers that are maintained manually.

NOTE Instead of setting up a standard computer group from scratch as described below, you can also duplicate an existing group by dragging it to the desired category header in the sidebar of the **Server Center** window while holding down the Alt key.

To set up a standard computer group:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. From the sidebar context menu, choose **Computer Groups > New Computer Group**.

The **New Computer Group** dialog opens:



3. Enter the desired name and click **OK**.

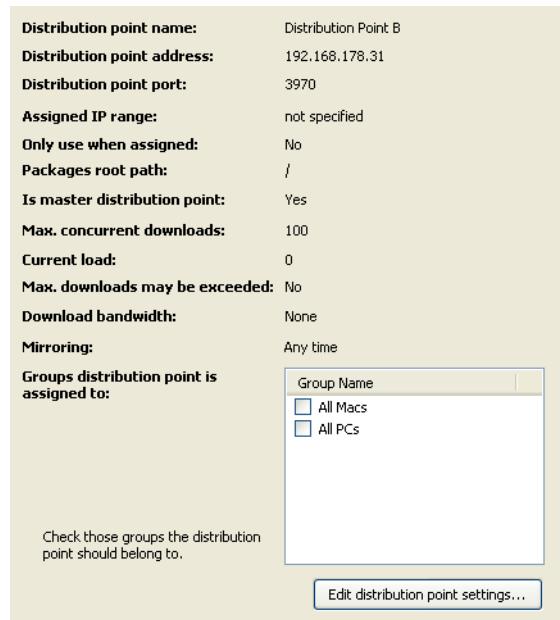
The new group appears in the **Server Center** window's sidebar.

4. To add computers to the group, drag them on top of the group icon from the table area, e.g., from the **Unassigned Computers** default computer group, or from any browser window displaying computers.

To remove computers, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

5. If desired, you can assign distribution points to groups. Computers from a group will prefer these assigned servers for installer downloads.

To assign a distribution point to a group, select the distribution point in the **Server Center** window's sidebar, displaying its details in the window:



Check all groups to which you want to assign the server.

6. To store the computer group specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new computer group becomes available only after you have done so.

Setting up smart computer groups

If any browser window contains a smart group with the desired criteria, you can simply drag it into **Computer Group** entry in the sidebar of the **Server Center** window. Otherwise, you can create the smart computer group from scratch.

NOTE Instead of setting up a smart computer group from scratch as described below, you can also duplicate an existing group by dragging it to the desired category header in the sidebar of the **Server Center** window while holding down the Alt key.

To create a new smart computer group:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the sidebar context menu, choose **Computer Groups > New Smart Computer Group**.

The **Smart Group** dialog opens:



3. Enter the name for the new computer group and define the conditions that computers must meet to be included in the computer group.

To define a condition, specify an information item in the left-hand text field, choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

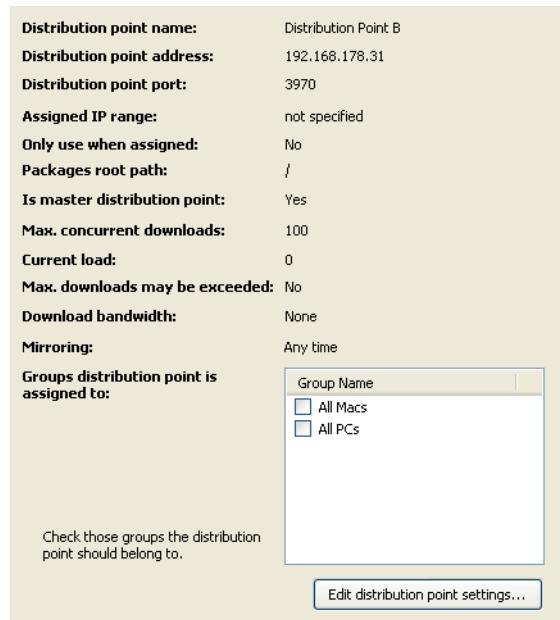
With the **+** and **-** buttons, you can add and remove conditions.

4. If you have specified more than one condition, specify through the upper pop-up menu whether computers must meet one or all of the conditions.
5. Click **OK**.

The new group appears in the **Server Center** window's sidebar.

6. If desired, you can assign distribution points to groups. Computers from a group will prefer these assigned servers for installer downloads.

To assign a distribution point to a group, select the server in the **Server Center** window's sidebar, displaying the server's details in the window:



Check all groups to which you want to assign the server.

7. To store the computer group specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new computer group becomes available only after you have done so.

Editing computer groups

To change the group's name or (for smart computer groups) change its definition, select it in the sidebar and choose **Edit Computer Group** from the sidebar context menu and enter the new name or redefine the group's criteria.

To add computers to a standard (non-smart) group, drag them on top of the group icon from the table area, e.g., from the **Unassigned Computers** default computer group, or from any browser window displaying computers.

To remove computers, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes.

Removing computer groups

To remove an existing computer group definition:

1. Select the group in the **Server Center** window and choose **Remove Computer Group** from the sidebar context menu.
A confirmation message is displayed.
2. Confirm the decision.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes.

Until you do this, the computer group is still available.

Performing installations

Once the software distribution system has been set up as described in the previous sections of this chapter, any installation process is a very simple matter.

To initiate a new installation process:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. Make sure that the software installation package or metapackage has been properly defined.
3. Drag the package from the table area to all computer groups to which the software is to be distributed.

Software installation will begin automatically shortly thereafter. (See below for details.) You can monitor the progress of the individual installation processes in the subgroups of the **Installation Status** subcategory in the sidebar.

The available subgroups are described in “Software Distribution” on page 438.

NOTE

Installations may not begin immediately for a variety of reasons, among them that you have set a later availability date or chosen an option from the software package’s **Installation time** pop-up menu.

Installation process

The actual installation process is completely automatic. It involves these main steps:

- The agents contact their assigned software distribution server to check whether there is new software available for them.

- The server and the contact interval is set in the Agent Settings dialog that is described in “Agent Settings” on page 287.
- The server checks to which computer groups an agent belongs and reviews all software packages and metapackages assigned to those computer groups:
 - Is the software package already available (as per the setting in the package definition)?
 - Does the agent meet the operating system requirements?
 - Are the optional auxiliary requirements from the package definition met (installation time during the day, user logged in, etc.)?
 - Is the package not yet installed on the agent’s computer?
 - If all these questions are answered with “yes”, the Absolute Manage Server notifies the agent of the availability of a new package and provides the location of the payloads on one of the distribution points.
 - The agent downloads the payloads from the distribution point. If the package specifies a user notification or allows the user to postpone or cancel the installation, the agent displays the message before or after downloading the payloads, as specified in the package.
 - The agent executes the executable payload locally according to the specifications in the package.
 - During the installation process, the agent reports the progress to the Absolute Manage Server. When the installation is done, the result is reported – success or failure, and error details in the case of failure.
 - Absolute Manage Admin displays the results in the **Software Distribution > Installation Reports** section of the Server Center.

Performing ad hoc installations

In addition to standard software distribution using distribution groups, Absolute Manage also lets you directly install software packages and metapackages on selected computers.

This is useful if there already are suitable software packages but the group of target computers is not permanent enough to warrant setting up a distribution group.

Ad hoc installations may not be ideal if:

- There is no software package. In this case, one of the methods described in “Installing software manually” on page 200 may be more appropriate.
- You expect to have to install software to the same group of computers more than very occasionally. In this case, we recommend that you set up a distribution group.

Ad hoc installations require payloads, software packages, and distribution points to be set up.

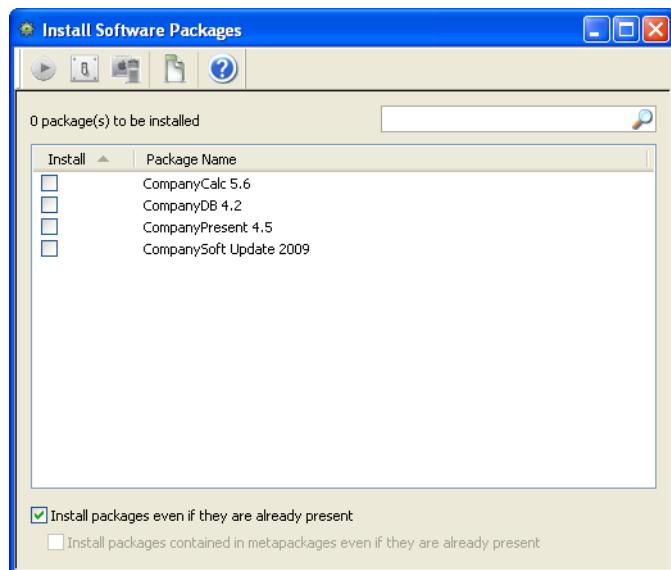
To install software packages ad hoc:

1. In any browser window, select the computers on which you want to install the software packages.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Install Software Packages**.

The **Install Software Packages** dialog opens:



3. Check the packages and metapackages that you want to install.
4. If you want to install selected packages and metapackages on a target computer even if that package has already been installed there, check the **Install packages even if they are already present** option.

If you also want to install all packages contained in selected metapackages regardless of whether they have already been installed, check **Install packages contained in metapackages even if they are already present** as well.

5. Click **Execute**.

Software installation will begin automatically shortly thereafter. Any settings in the packages regarding the installation time are disregarded. Settings regarding user interaction are honored, however.

Absolute Manage Admin displays the installation results in the **Software Distribution > Installation Reports** section of the Server Center

NOTE You can also launch this command by selecting the desired packages in the **Server Center** window, right-clicking them, and choosing **Install Selected Software Packages** from the context menu. In that case, you need to add the target computers to the command window.

Automated patch management

The software distribution system offers automated management of operating system patches and other updates from Apple and Microsoft without any additional setup. The only administrative action required is approval of packages that are made available automatically.

Overview

The automated patch management covers all software updates that Apple and Microsoft make available via the automatic update functions in their operating systems, in particular:

- Free operating system updates and service packs
- Driver patches for Macintosh computers
- Free software updates for application software such as the iLife and iWorks suites or Internet Explorer

You can thus install an operating system in its shipping version (e.g., Mac OS X 10.5) and let all patches automatically be installed, creating a fully up-to-date system with no additional effort.

NOTE For even easier installations of operating systems on computers that already have an Absolute Manage Agent, see “Reinstalling a Windows computer” on page 241.

Process

Automated patch management follows this process:

1. Agents check Apple’s and Microsoft’s servers for any new patches that apply to the computers on which they are running.
2. If such patches are found, the agents check the Software Distribution Center for the presence of the patch.
3. If the patch is not present, it is automatically downloaded and a payload and software package are created from it. This package is placed in the **Unconfirmed Updates** smart group.

4. When patches have been downloaded to the **Unconfirmed Updates** smart group, they must be approved by you before any further processing happens:

Drag them to the **Rejected Updates** group when you do not want them installed. If you want them installed, drag them to all groups containing computers on which the patch is to be installed.

Note: You can reverse the decision to reject a package at any time. (You can also reverse the decision to accept a package, but that obviously does not undo any installations that may already have happened.)

The software package contains information (received from the operating systems' update utilities) about the intended target computers. It is installed on only those client computers where it is –according to this information – actually required.

We therefore recommend that you handle packages that you want to accept in the following way:

- For Mac OS X packages, just drag them to the **All Macs** computer group.
- For Windows packages, create a smart computer group for each major strain of the operating system (e.g., Windows 2003 Server, Windows XP, Windows 7) using the **OS Platform** information item.
Then just drag each accepted patch to the appropriate smart computer group.

5. Software installation from here on follows the same process as for other software packages, as described in "Installation process" on page 232, with only one deviation: Packages are installed only when they apply to the individual computer according to the local Software Update or Windows Update utilities. So, a package that is not needed on a particular client would not be installed, even though it is assigned to a group to which the computer belongs.

Finding missing patches

To find computers that are missing applicable patches (and the missing patches), use the **Missing Operating System Patches** window which automatically lists all computers with missing patches.

You can create smart groups in the **Missing Operating System Patches** window to focus on patches or computers of particular interest.

Deactivating patch management

You can deactivate the patch management for individual agents or completely for the entire Absolute Manage system.

To deactivate it for individual agents, open the Agent Settings dialog for those agents and uncheck the **Include in patch management** option.

To deactivate the patch management completely, switch it off for all agents, as described above.

Reinstalling a Mac OS X computer

Using the software distribution system, Absolute Manage can remotely reinstall the operating system (including additional software, if desired) on client Mac OS X computers.

No manual steps beyond initiating the process are needed, let alone physically visiting the computer. All that is required is that an Absolute Manage Agent is already installed on the computer.

IMPORTANT

This process completely reinstalls a target computer's hard disk. It is in its nature to irrecoverably delete the target volume's previous contents. Before going ahead, you should therefore make absolutely sure that no important data is lost.

Reinstalling Mac OS X client computers requires just a few simple steps:

- Create a disk image with the desired hard disk contents.
- Optionally create a disk image specification in the Software Distribution Center (when you expect to use the image repeatedly).
- Select the target Mac OS X computers, choose **Reinstall Mac OS X Computer**, and specify the disk image to be used.

When you tell Absolute Manage to reinstall a client computer, it stops all processes running on that computer, erases the specified hard disk – optionally preserving user folders and network settings –, copies the disk image's contents to the hard disk, and reboots the computer.

To reinstall a Mac OS X computer:

1. Install on a hard disk volume the operating system.
2. Install and configure the Absolute Manage Agent.

In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

Note: If you do not include Absolute Manage Agent on the disk image, reinstallation is still possible but Absolute Manage will be unable to administer the reinstalled client computers until Absolute Manage Agent is installed on them once more.

3. Install any additional software that you want to be present on the client computers.
4. Create a disk image from the boot volume, e.g., using Apple's Disk Utility, and save it on your computer.

The disk image file must be saved in Apple's .dmg format or any other format that can be mounted on the client computers without requiring additional software.

For performance reasons, we recommend saving the image file as a compressed image, using the appropriate option in Disk Utility.

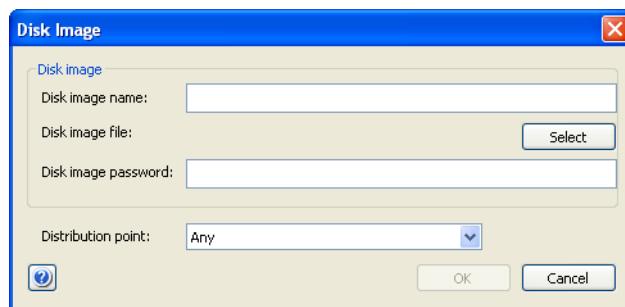
5. If you plan to use the image only once, skip to step 10.

If you plan to reuse the disk image, create a disk image specification as described in the following steps.

*Note: Setting up disk images as described in the next steps is possible only for administrators with the **Modify Disk Image** right. See "New Administrator" on page 481 for details.*

6. Open the **Server Center** window, right-click in the left-hand sidebar, and choose **Software Distribution > New Disk Image** from the context menu.

The **Disk Image** dialog opens:



7. Enter the disk image specification:

- **Disk image name:** The name that you want to give the disk image specification for purposes of identifying it within Absolute Manage.
- **Disk image file:** The file that contains the disk image. Absolute Manage supports Apple's .dmg format as well as any other disk image that can be mounted without additional software on the target computer, e.g., ISO images (.iso) or Active Disk Image images (.adi).
- **Disk image password:** If the image is password-protected, enter the password here.
- **Distribution point:** This option specifies from which distribution points the target computer may download the image:
 - **Any:** The image can be downloaded from any distribution point on which it is found.
 - **From assigned distribution point if available:** The image is downloaded from a distribution point that is assigned to the target computer's subnet or a computer group to which the target computer belongs. If the image is not available on any such distribution point, it is downloaded from another distribution point.

- **From assigned distribution point only:** As above, but if the image is not available, the installation fails.

8. Click **OK** to save the disk image specification.

If desired, create more disk image specifications.

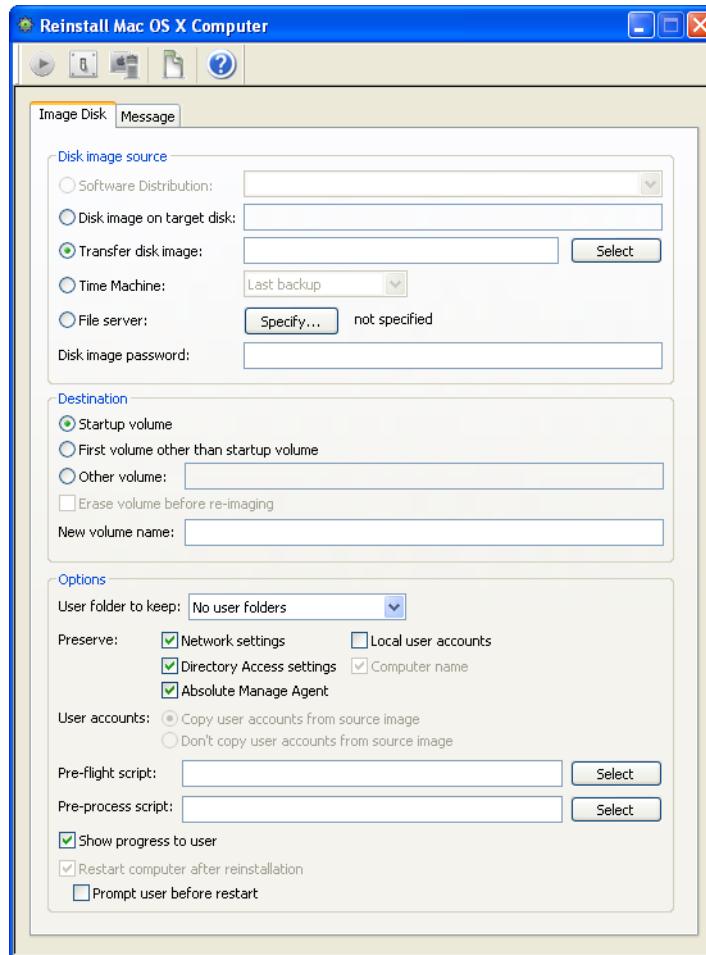
9. From the **Server** menu, choose **Save Distribution and Licensing Info** to store the changes on the server.

You can start using the new disk image through the Software Distribution Center when the upload is complete.

Note: While disk images can be stored in the Software Distribution Center, they cannot be assigned to computer groups as software packages can. Applying a disk images to a clients computer is only possible by explicitly selecting that computer and choosing the Reinstall Mac OS X Computer command.

10. In any browser window, select the Mac OS X computers that you want to reinstall.
11. From the **Commands** menu, choose **Reinstall Mac OS X Computer**.

The **Reinstall Mac OS X Computer** dialog opens:



12. In the **Disk image source** section, specify the disk image that is to be the source of the reinstallation.

The individual options in this dialog are described in “Reinstall Mac OS X Computer” on page 298.

13. In the **Destination** section, specify the volume on which the disk image’s content is to be installed.

IMPORTANT

The option to install on the first volume other than the startup volume is primarily intended to allow you to reinstall the (sole) local volume of a computer that has been booted from a network volume. If there are more than two volumes on a client, there is no way to tell which of the non-startup volumes will be chosen. We strongly recommend against using this option on computers with more than two mounted volumes.

14. In the **Options** section, specify execution options such as scripts to be executed before or after the installation, settings to keep, or user interaction options.

15. If you want to send a message to the user before the installation begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “Sending messages” on page 115.

If you provide a **Cancel** button in the message dialog, the installation is aborted on a target computer if a user clicks **Cancel**.

*Note: If a message has been specified, this is indicated by a dot in the dialog's **Message** tab.*

16. Click **Execute**.

Absolute Manage erases the specified disks of the target Mac OS X computers and copies the software from the disk image. Any errors are noted in the command history.

Using a previously specified disk image

To reinstall a computer using a disk image specification that is already in the Software Distribution Center, proceed as described above but start with step 10.

Reinstalling a Windows computer

Using the software distribution system, Absolute Manage can remotely reinstall the operating system (including additional software, if desired) on client computers, provided an additional server has been set up as described in “Installing support for reinstalling Windows computers” on page 20.

No manual steps beyond initiating the process are needed, let alone physically visiting the computer. All that is required is that an Absolute Manage Agent is already installed on the computer.

Windows computers can be reinstalled, provided that the computer is set to boot from the network first. This is possible even if no agent is installed on them.

IMPORTANT

This process completely reinstalls a target computer’s hard disk. It is in its nature to irrecoverably delete the target volume’s previous contents. Before going ahead, you should therefore make absolutely sure that no important data is lost.

Reinstalling a Windows computer involves these main steps:

1. Create a disk image with the desired hard disk contents and save it on a distribution point.

The details of this step differ depending on which PXE server you use. See the appropriate section for details:

- **Preparing a disk image using the Absolute server** (page 242)
- **Preparing a disk image using FOG** (page 244)

2. Schedule the computer for reinstallation and restart it.

For details, see “Reinstalling Windows client computers” on page 246.

When you tell Absolute Manage to reinstall a client computer, it reboots the computer from the PXE server. It then erases the computer’s boot disk and installs the content of the specified disk image on it. After that, the computer is rebooted from the reinstalled hard disk.

For details, see:

- **Preparing a disk image using the Absolute server** (page 242)
- **Preparing a disk image using FOG** (page 244)
- **Reinstalling Windows client computers** (page 246)

Preparing a disk image using the Absolute server

Preparing disk images using the procedure below requires that an Absolute PXE server is properly set up in your network, as described in “Setting up the Absolute solution” on page 20.

To create a disk image:

1. Install the operating system on a Windows computer.
2. Create an empty file C:\AMFOGImage or C:\AMIImage.
3. Install and configure the Absolute Manage Agent.

In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

Note: If you do not include Absolute Manage Agent on the disk image, reinstallation is still possible but Absolute Manage will be unable to administer the reinstalled client computers until Absolute Manage Agent is installed on them once more. Also, the computer cannot automatically join a domain and the computer name is not set.

4. Install any additional software that you want to be present on the client computers.
5. Stop the LANrev Agent service and delete the registry value “HKLM\Software\Pole Position Software\LANrev Agent\AgentSerialNo”

Note: This is an optional but recommended step that provides a safety measure against duplicate agent IDs. Absolute Manage can reassign new IDs when it detects a duplicate, but deleting the ID

from the registry in the first place makes this process unnecessary.

6. Run the Microsoft Sysprep utility on the computer:

- Windows XP: The utility is found on the Windows installation disk in \Support\Tools\Deploy.cab. Create the directory C:\sysprep, copy Sysprep to it, and execute Sysprep using:

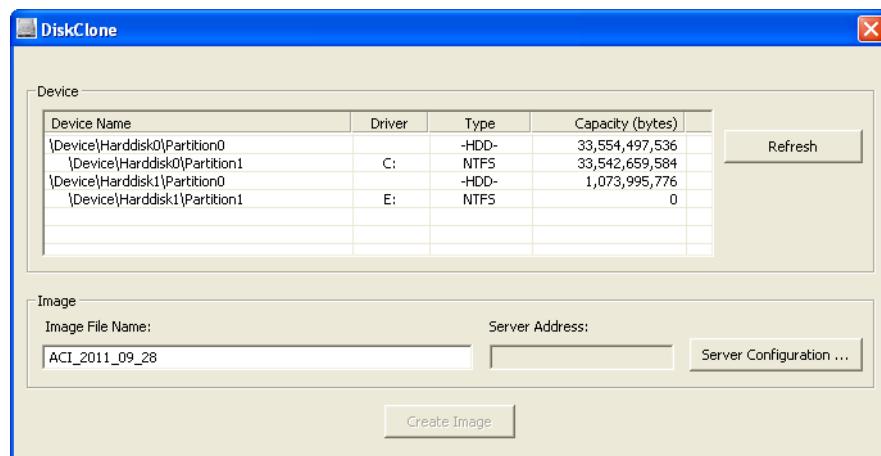
```
C:\sysprep\sysprep.exe -reseal -mini -quiet -noreboot
```

- Windows 7: The utility is installed on the boot disk by default. Execute it with the following command (all in one line):

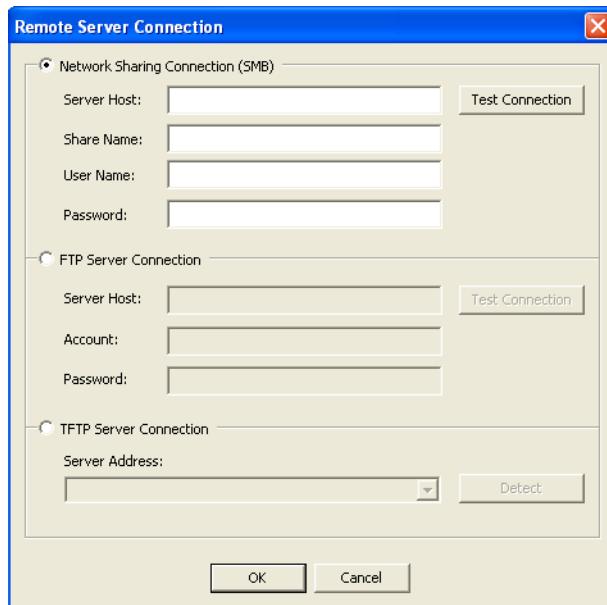
```
C:\windows\system32\sysprep\sysprep.exe  
/generalize /oobe /quiet /quit  
/unattend:C:\windows\system32\sysprep\sysprep.xml
```

See the Sysprep documentation for details, including creating an answer file.

7. Restart the computer, enter the BIOS configuration, and set it to boot from the network.
8. After a short delay, the DiskClone tool is displayed:



9. Click **Server Configuration** to open the **Remote Server Connection** dialog:



10. Enter the address and access information for an SMB share or an FTP server on which you want the image file to be created.

We do not recommend using TFTP because it does not support any kind of authentication.

11. Click **Test Connection** to verify that the connection is working. When it is, click **OK**.

12. In the device list, select the hard disk from which you want to create the installation image.

We recommend that you choose a complete hard disk (a row with "HDD" in the **Type** column), not a partition (a row with a file system name in the **Type** column).

13. Enter the desired name for the image file in the **Image File Name** field.

14. Click **Create Image**.

The disk contents is transferred to the specified server share.

When the transfer is complete, you can use this disk image to reinstall client computers, as described in "Reinstalling Windows client computers" on page 246.

Preparing a disk image using FOG

Preparing disk images using the procedure below requires that an FOG server is properly set up in your network, as described in "Setting up the FOG solution" on page 22.

To create a disk image:

1. Install the operating system on a Windows computer.
2. Create an empty file C:\AMFOGImage
3. Install and configure the Absolute Manage Agent.

In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

Note: If you do not include Absolute Manage Agent on the disk image, reinstallation is still possible but Absolute Manage will be unable to administer the reinstalled client computers until Absolute Manage Agent is installed on them once more. Also, the computer cannot automatically join a domain and the computer name is not set.

4. Install any additional software that you want to be present on the client computers.
5. Stop the LANrev Agent service and delete the registry value "HKLM\Software\Pole Position Software\LANrev Agent\AgentSerialno".

Note: This is an optional but recommended step that provides a safety measure against duplicate agent IDs. Absolute Manage can reassign new IDs when it detects a duplicate, but deleting the ID from the registry in the first place makes this process unnecessary.

6. Run the Microsoft Sysprep utility on the computer:
 - Windows XP: The utility is found on the Windows installation disk in \Support\Tools\Deploy.cab.
Create the directory C:\sysprep, copy Sysprep to it, and execute Sysprep using:

```
C:\sysprep\sysprep.exe -reseal -mini -quiet -noreboot
```

- Windows 7: The utility is installed on the boot disk by default. Execute it with the following command (all in one line):

```
C:\windows\system32\sysprep\sysprep.exe  
/generalize /oobe /quiet /quit  
/unattend:C:\windows\system32\sysprep\sysprep.xml
```

See the Sysprep documentation for details, including creating an answer file.

7. Using FOG, create a disk image of the computer as described in the FOG documentation.

Choose an image type depending on the operating system and partitioning scheme:

- For Windows XP with a single partition, choose **Single Partition (NTFS only, Resizable)**.

- For Windows XP with multiple partitions (e.g., when there is a recovery partition), choose **Multiple Partition Image - Single Disk (Not Resizable)**.
- For Windows 7, choose **Multiple Partition Image - Single Disk (Not Resizable)**.

You can now use this disk image to reinstall client computers, as described below.

Reinstalling Windows client computers

When a PXE server is properly set up (as described in “Installing support for reinstalling Windows computers” on page 20) and a suitable disk image has been created (as described in “Preparing a disk image using the Absolute server” on page 242 and “Preparing a disk image using FOG” on page 244), you can reinstall administered Windows computers:

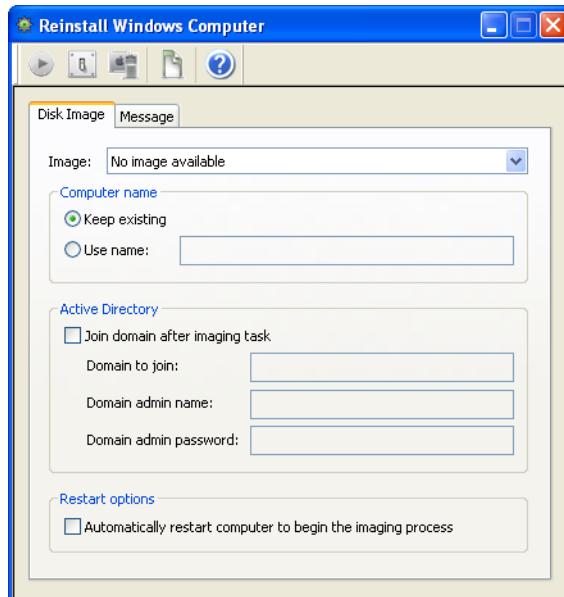
1. In any browser window, choose the computers you want to reinstall.

All selected computers will receive the same disk image.

You can also select computers on which no agent is installed if you have created placeholder records for them, as described in “Creating placeholder records for computers” on page 65.

2. From the **Commands** menu, choose **Reinstall Windows Computer**.

The **Reinstall Windows Computer** dialog opens:



3. From the **Image** pop-up menu, choose the desired disk image to be used for reinstalling the computers.
4. In the Computer name section, specify a new name for the selected computers or choose **Keep existing** to not change them.

5. In the **Active Directory** section, specify whether the reinstalled computers are to join a domain.

If they are to join a domain, provide the name of the domain and administrator credentials for the domain.

6. If you want the reinstallation to proceed automatically when you send the command, check the **Automatically restart computer to begin imaging process** option.

If this option is not checked, the target computers must be restarted manually before they will be reinstalled.

The option has no effect for target computers on which no agent is installed; that is, such computers must always be manually restarted.

7. If you want to send a message to the user before the installation begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “[Sending messages](#)” on page 115.

If you provide a **Cancel** button in the message dialog, the installation is aborted on a target computer if a user clicks **Cancel**.

*Note: If a message has been specified, this is indicated by a dot in the dialog's **Message** tab.*

8. Click **Execute**.

Absolute Manage sends instructions to the PXE server to reinstall the computers after their next restart. If you have checked the **Automatically restart computer to begin imaging process** option, Absolute Manage also instructs the agents to restart the target computers.

Note that the target computers must be set to boot from the network first in order for the reinstallation to be possible.

9. If no agent is installed on the target computers or you have not checked the **Automatically restart computer to begin imaging process** option, restart the target computers manually.

Make sure that they boot from the network first. Many BIOSes allow you to specify the boot order on the fly by pressing the F10 or F12 key during the boot process.

The target computer reboot from the network. The PXE server provides them with the specified disk image and controls the reinstallation process.

The reinstallation task is displayed in the **Window Reinstallation Tasks** window.

Absolute Manage allows you to monitor the installation and use of licensed software on the computers in your network, record purchasing and maintenance agreement details, and create reports on historic usage, ensuring compliance with licensing limits.

You can also specify software that is prohibited in your network and have all instances of this software be reported and optionally terminated automatically.

The various aspects of license monitoring are explained in:

- “Overview” on page 248
- “Setting up license specifications” on page 249
- “Tracking purchasing information” on page 254
- “Setting up computer groups” on page 256
- “Configuring agents” on page 256
- “Checking licenses” on page 259
- “Reports” on page 260

Overview

The License Monitoring Center is a module of the Absolute Manage Server that provides constant automated monitoring of both per-installation and concurrent-use licenses as well as prohibited software. It also provides a repository for information related to license purchases and maintenance agreements.

This section discusses the basics of license monitoring and provides an overview of setting it up.

Prerequisites

Some functions of the License Monitoring Center can be used only by administrators whose accounts have certain rights enabled.

Configuring administrator accounts is described in “Administrator accounts” on page 48.

Setup

Setting up license monitoring involves defining license specifications – which define the software to be monitored and the licensing parameters and optionally include purchasing and maintenance agreement information – and computer groups – groups of computers that are considered together for purposes of license monitoring. This is described in “Setting up license specifications” on page 249 and “Setting up computer groups” on page 256.

Optionally, you can configure on the agents the servers to which they send reports. (If you do not configure this setting, reports are sent to

the default inventory server.) This is described in “Configuring agents” on page 256.

You can also configure the times and intervals for checking for licensed software as well as the intervals for sending information to the server. This is described in “Configuring agents” on page 256.

If everything has been set up, license specifications are assigned to groups. The compliance with these specifications is then monitored and recorded by the Absolute Manage Server. This is described in “Checking licenses” on page 259; the available reports are discussed in “Reports” on page 260.

Prohibited software

If there is software the use of which is prohibited in your network, you can use Absolute Manage to check for the presence of such software. This is done in exactly the same way as license monitoring; all that is required is to mark the software “prohibited” in the license specification.

Setting up license specifications

License specifications combine a definition of an application with information on the available licenses and status (prohibited or not).

License specifications can describe per-use (concurrent) licenses, per-seat (per-installation) licenses, or prohibited software. All three types are defined in the same way; the differences are in step 6 only.

License specifications combine a definition of an application with information on the available licenses and status (prohibited or not).

NOTE License specifications can be created, edited, or deleted only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 481 for details.

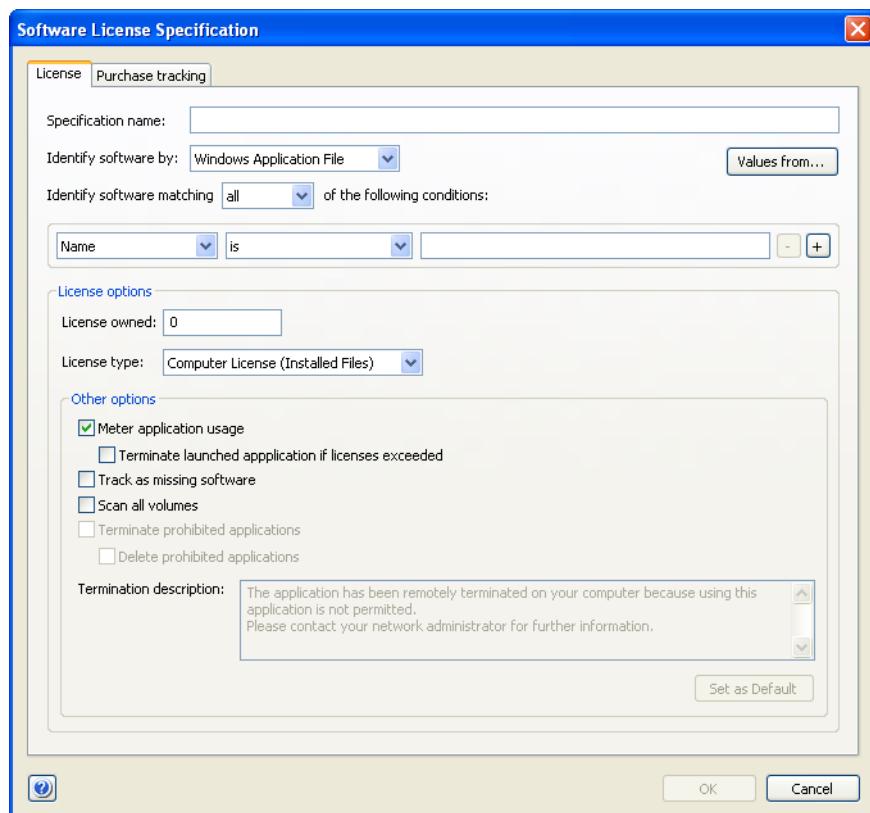
To create a license specification:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.



2. From the sidebar context menu, choose **License Monitoring > New License Specification**.

The **Software License Specification** dialog opens:



3. Enter the desired name in the **Specification name** field.

You can choose any desired name.

4. Choose the type of software that is to be monitored. Your choice in this menu determines, what kind of data Absolute Manage

considers when checking whether the licensed software is installed on an administered computer:

- **Mac OS Application Package:** Mac OS X packages (a folder appearing as a file) are checked.
 - **Mac OS Application File:** Mac OS X files are checked. Files are only considered to match if they are executable applications.
 - **Mac OS File:** Mac OS X files are checked.
 - **Mac OS Installer Receipt:** Installer receipts are checked. Installer receipts are descriptions of installed software in the form of an installer package that some Mac OS X installers create.
 - **Windows Application File:** Windows files are checked. Files are only considered to match if they are executable applications.
 - **Windows File:** Windows files are checked.
 - **Windows Installer Receipt:** The reports on installed software that MSI installers create are checked.
 - **Windows Registry:** The contents of the Windows registry is checked.
5. Specify the conditions that an object must match to be identified as the licensed software.

You can click the **Values from** button to insert default comparison value from a file on your computer.

The available conditions are explained in “Files” on page 566 or “New License Specification” on page 470, depending on the software type selected.

When you specify a path or registry location, you can include environment variables, as described in “Environment variables” on page 137.

*Note: When you specify a license by Windows registry data, you should use the **Key Name** and **Value Name** conditions only when there is no other way to specify the desired software. Checking either condition requires the entire registry to be parsed, which generates significant local processor load on the client computer and also takes a while. If you do require either condition, specify it after any other conditions that may apply because that causes Absolute Manage to apply it only to the part of the registry that meets those other conditions.*

Note: When specifying a file version, make sure to use the right format (three numbers for Mac OS X files, four for Windows files), as described in “Gathering information on files” on page 76.

6. Enter the number of available licenses.

Note that this field is disabled if you have chosen to have Absolute Manage calculate the number of available licenses automatically

from the purchase records, as described in “Tracking purchasing information” on page 254.

7. Choose the type of the license:

- **Computer License (Installed Files):** The license governs how many copies of the software may be installed in your network.
- **Floating License (Running Processes):** The license governs how many copies of the software may be in use at the same time.
- **Site License:** This type is for software that may be used without restriction throughout your network. You can also choose it when you want to use the license specification purely for monitoring purposes.
- **Prohibited Application:** Software that is not allowed in your network. This is not really a license type; however, this setting allows you to use the license-checking mechanism to watch for the presence of undesirable software.

8. Set the other options:

- Check **Meter application usage** if you want Absolute Manage to not only scan the hard disks but also monitor the running processes for the licensed software and store the numbers for later reports.
Note: Only applications on administered computers that have a working network connection to the server are included in the count.
If you want Absolute Manage Agents to automatically terminate any applications launching which exceeds the available license count, check **Terminate launched applications if licenses exceeded**.
When an application is automatically terminated, a message informs the local user about the reason; you can specify the text for this message in the **Termination description** field.
- If you want Absolute Manage Agents to automatically terminate any prohibited application on their computers, check **Terminate prohibited applications**. (This option is available only when you have set the license type to “Prohibited Application.”)
To also delete the offending application, check the **Delete prohibited applications** option.
When an application is automatically terminated, a message informs the local user about the reason; you can specify the text for this message in the **Termination description** field.
- If Absolute Manage is to provide an overview of the computers on which this software is not available, check **Track as missing software**.
Note: Usually, you will want to activate this option only for software that should be installed on all or most of the administered computers. Tracking applications intended

- only for a few computers can clutter up the display of missing applications.*
- If you want Absolute Manage to look for the licensed software on all local volumes of administered computers, check **Scan all volumes**. Otherwise, only the boot volume is scanned.
9. If desired, you can enter details of license purchases and maintenance agreements, as described in “Tracking purchasing information” on page 254.
 10. Click **OK** to close the dialog.

11. To store the license specification on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but the new license specification becomes available to the License Monitoring Center only after you have done so.

Editing license specifications

To edit an existing license specification, select it in the sidebar of the **Server Center** window and choose **Edit License Specification** from the sidebar context menu.

The **Software License Specification** dialog opens that is described above.

After you have completed editing the specification, click **OK** and choose **Save Distribution and Licensing Info** from the **Server** menu to save the changes to the Absolute Manage Server.

Deleting reports

To delete an existing custom report, select it in the sidebar of the **Server Center** window and choose **Remove License Specification** from the sidebar context menu.

The license specification is deleted.

Choose **Save Distribution and Licensing Info** from the **Server** menu to save the changes to the Absolute Manage Server.

Tracking purchasing information

As part of a license specification, you can also record details of purchases of the software in question, including updates and maintenance agreements.

NOTE Purchase tracking information can be entered and edited only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 481 for details.

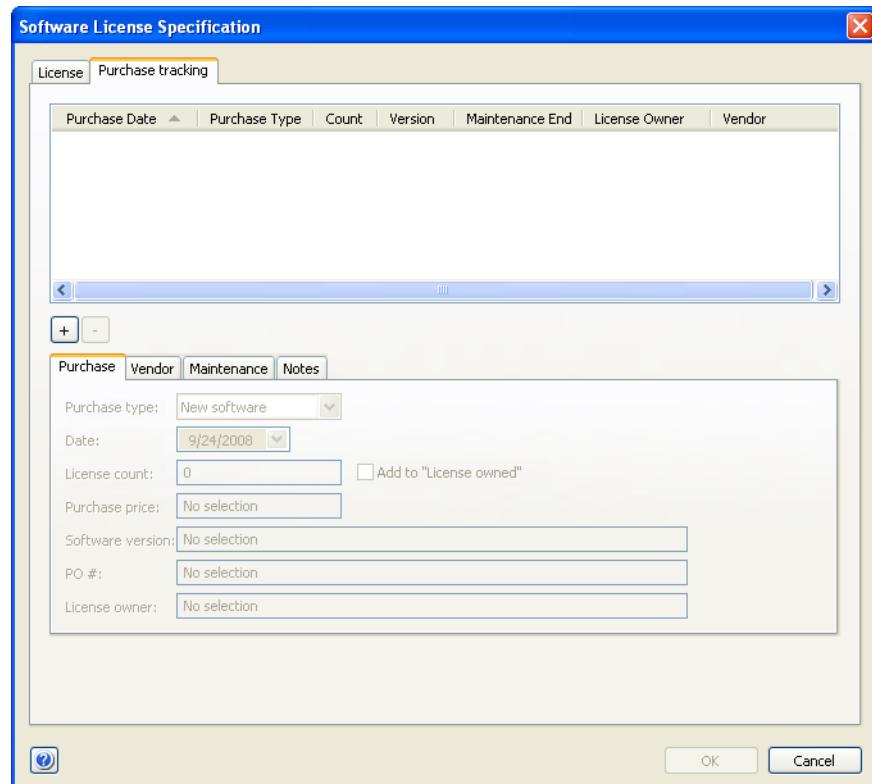
Entering new purchasing information

To enter purchasing or maintenance agreement information for a software:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

The **Software License Specification** dialog opens.

2. Click the dialog’s **Purchase Tracking** tab:



3. To enter details of a new purchase – of any type: new software, software update, maintenance agreement, or maintenance extension – click the **+** button below the list.

4. Enter the information in the four subpanes. These subpanes' fields are described in "Purchase Tracking" on page 474.

Note that checking the **Add to "Licenses owned"** option in the **Purchase** subpane makes Absolute Manage add up all your license purchases to automatically fill the license specification's **Licenses owned** field. Manual entry into that field is disabled in this case.

5. Click **OK** to close the dialog.
6. To store the new information on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

You do not need to save the changes to the Absolute Manage Server immediately (you can perform additional setup steps before doing so), but you must do so before quitting Absolute Manage Admin – otherwise the changes will be lost.

Editing purchasing information

To edit existing information on license purchases or maintenance agreements:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

The **Software License Specification** dialog opens.

2. Click the dialog's **Purchase Tracking** tab.
3. In the list in the upper part of the tab, select the entry that you want to edit.
4. The entry's information is displayed in the subtabs in the lower half of the dialog.
5. Edit the information as desired.
6. Click **OK** to close the dialog.
7. To store the new information on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

Deleting purchasing information

To delete existing information on license purchases or maintenance agreements:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

The **Software License Specification** dialog opens.

2. Click the dialog's **Purchase Tracking** tab.
3. In the list in the upper part of the tab, select the entry that you want to delete.
4. Click the – button below the list.

The selected purchasing or maintenance agreement record is removed.
5. Click **OK** to close the dialog.
6. To store the new information on the Absolute Manage Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

Setting up computer groups

Computer groups are collections of computers that can use the available licenses or that are otherwise to be considered together for software monitoring purposes. One computer can belong to multiple computer groups, allowing great flexibility through overlapping groups.

NOTE Computer groups can be set up only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 481 for details.

The same computer groups are used for license monitoring and software distribution. Creating and maintaining these groups is described in “Setting up computer groups” on page 227.

Configuring agents

The details of license monitoring can be configured individually on each Absolute Manage Agent:

- The intervals in which the agents check the hard disks for licensed software and the times of the day and the week in which they are doing so. (If the License Monitoring Center is configured to monitor running processes for licensed software, it does so constantly.)
- The Absolute Manage Server to which they send license monitoring information and the interval in which they do so.

Configuring the checking intervals and times will often be unnecessary as the defaults serve most organizations well.

Configuring agents

To configure Absolute Manage Agents for license monitoring:

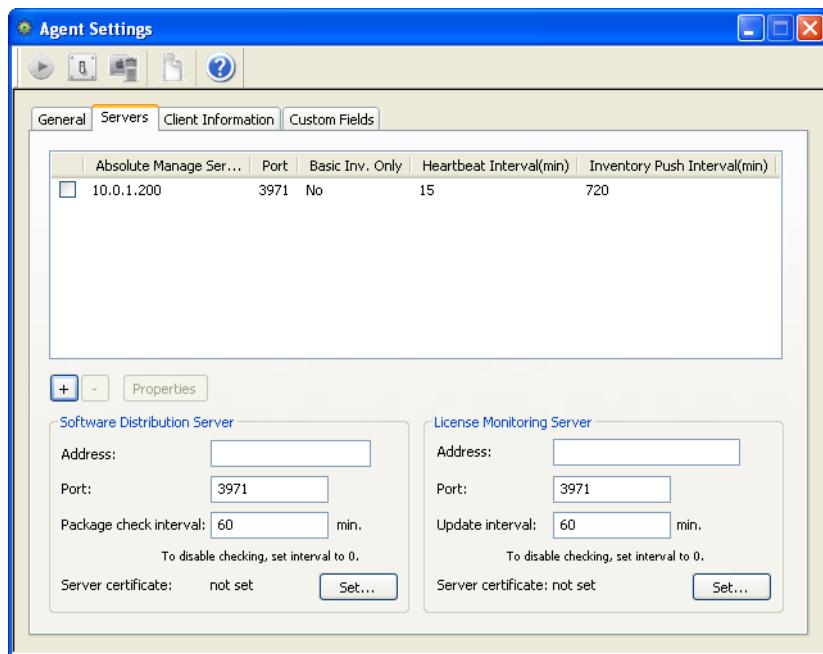
1. In any browser window, select the computers on which you want to configure the agents.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog opens.

3. Click the **Servers** tab:



4. In the **License Monitoring Server** section of the dialog, enter the IP address or DNS name of the Absolute Manage Server that is to be the selected agents' license monitoring contact, the port on which the server listens to traffic from the agents, and the desired interval in which agents check the server for new licensing information.

Note: If you enter an abbreviated DNS name (i.e., a partial name that is completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).

5. If the **Server certificate** field does not display "valid", click the **Set** button and choose the certificate for the server.

Creating server certificates is described in “Exporting a server certificate” on page 19.

Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

6. Click **Execute**.

Configuring intervals

You can configure the interval in which Agents scan the hard disks for installed licensed software and the interval in which they send reports to the server. These intervals are the same for all Agents connected to a particular license monitoring server.

NOTE The interval for scanning for running applications is not set. In contrast to scans of hard disks, such scans consume only negligible processor power and so are always performed frequently – usually about once per minute.

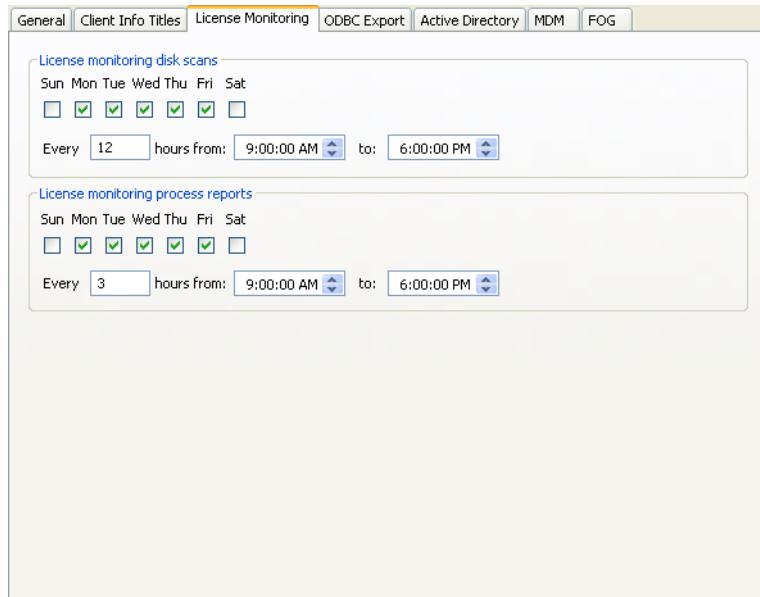
Configuring these intervals and times will often be unnecessary as the defaults serve most organizations well.

To set the intervals:

1. Make sure that you are connected to the license monitoring server that you want to configure.
2. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
3. In the **Server Center** windows sidebar, click **Server**.

The **Server Settings** dialog is displayed in the **Server Center** window.

4. Click the **License Monitoring** tab:



5. In the **Agent License monitoring disk scans** section, specify the days of the week and the period during the day when license scans are to be performed and the interval of such scans.

These settings are provided to avoid sending meaningless data to the server. For example, nothing happens in a normal office at 3 am, so there is no need to monitor license compliance when this has happened at 6 pm and will happen again at 9 am.

Note: Because of a limitation in the operating system, midnight at the end of the day cannot be specified as "24:00" when using a 24-hour clock. Enter "0:00" instead.

6. In the **License monitoring disk scans** section, specify the period during which Agents are to send licensing reports to the server and the interval for sending these reports.

These reports also include results of scans for running software (if any license specifications include such scans), which are performed about once per minute.

7. Click **OK**.

The updated settings are sent to the server with the regular license monitoring updates. (The interval for these updates is specified in the **Servers** tab of the **Agent Settings** command window.)

Checking licenses

Once licenses and computer groups are set up, checking licensing compliance requires assigning licenses to groups.

Absolute Manage Server then automatically transmits the information about what to look for to all relevant Absolute Manage Agents. These agents check their hard disks and, if so configured, running processes according to their individual settings for the specified software and return the results to the server.

Automatic and manual scans

Normally, both the local scans for licensed or prohibited software happen in regular intervals, as specified in the **Agent Settings** dialog. If you want to check for software immediately, outside the normal schedule, you can do so:

1. In any browser window, select the computers on which you want to check for software.

Note: For information on specifying groups as targets, see "Targets" on page 286.

2. From the **Commands** menu, choose **Run License Monitoring Scan**.
3. Click **Execute**.

Absolute Manage Server instructs the agents on the selected computers to scan immediately for all licenses that have been assigned to computer groups to which they belong. The agents send the results to the server immediately after they have completed their scans, irrespective of the schedule set in the **Servers** tab of the **Agent Settings** dialog for doing so.

Scan results

The results of all scans – manual or automatic – are collected by the Absolute Manage Server and presented to connected admins as a series of reports. These reports are discussed below.

Reports

The results of the license monitoring are presented by the Absolute Manage Server in the form of a number of reports.

There are predefined reports; you can also define custom reports that also take the form of groups of database records.

Both predefined and custom reports are described below.

Understanding predefined reports

The predefined reports included with Absolute Manage answer the issues that are most commonly considered in relation with license monitoring:

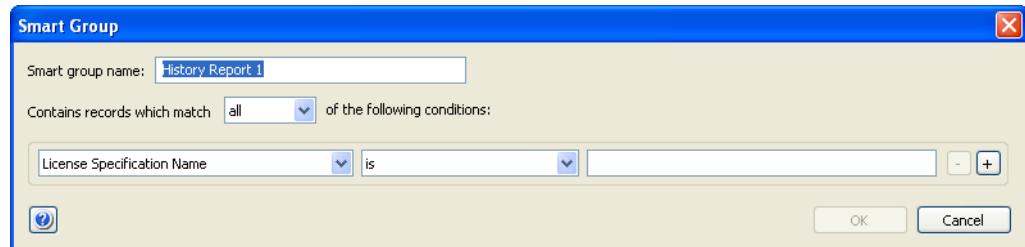
- **Fully compliant:** A list of all software for which the license numbers are observed.
This report includes all license specifications where the total number of copies of the software found in all computer groups to which the specification was assigned does not exceed the number of available licenses.
Note: New licenses may be included in the category even though they are exceeded because not all relevant agents have yet reported on them.
- **Licenses exceeded:** A list of all software that is currently used more often than permitted.
This report includes all license specifications where the total number of copies of the software found in all computer groups to which the specification was assigned is higher than the number of available licenses.
- **Prohibited software:** A list of all copies of prohibited software in the network.
This report includes all pairs of license specifications for prohibited software and computers that have been found, i.e., if software declared prohibited in its license specification has been found on a computer, there is an entry stating the license, the computer, and the number of copies found.
- **Undetermined licenses:** Licenses for which no information has been returned from any agents.
This report includes new licenses for which no agent has yet reported finding or not finding the specified software. If licenses remain in this report for an extended period of time, they may not have been assigned to any computer group.
- **Software usage:** A list of all copies of licensed or prohibited software.
This report includes all pairs of license specifications and computers that have been found, i.e., if the software of a license specification has been found on a computer, there is an entry stating the license, the computer, and the number of copies found.
- **Missing software:** A list of all software that should be installed on a computer but is not.
This report includes all pairs of license specifications and computers that have not been found. Any computer is checked for all licenses that have been assigned to a computer group to which it belongs, except prohibited software.
If any of the software is not found on the computer, an entry in this report is generated stating the license and the computer.
- **History:** A trail of license numbers.
This report includes time-stamped entries of license summaries. Each entry includes the license specification and the number of copies of the specified software found throughout the network.

Creating custom reports

You can create custom reports to complement the predefined ones:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.
2. From the sidebar context menu's **License Monitoring** section, choose one of these commands:
 - **New License Status Report** to create a report on the status of license specifications, similar to the **Fully compliant**, **Licenses exceeded**, or **Prohibited software** reports.
 - **New Software Usage Report** to create a report on the usage of licensed software on individual computers, similar to the **Software usage** report.
 - **New History Report** to create a report on past counts of licensed software, similar to the **History** report.
 - **New History Summary Report** to create a statistical report on the usage levels of licensed software in a selectable period, similar to the **History summary** report.
 - **New Missing Software Report** to create a report on the computers lacking a particular piece of licensed software, similar to the **Missing software** report.

In each case, the **Smart Group** dialog opens:



All five dialogs are similar; they differ only in the contents of the left-hand pop-up menu.

3. Enter a name for the report.
4. Specify the conditions that a license specification, software usage information, or history entry must match to be included in the report.

To do so, choose an information from the left-hand pop-up menu, a relation from the pop-up in the middle, and enter a comparison value in the text field.

You can add and remove conditions using the + and – buttons.

When using multiple conditions, use the top pop-up menu to specify whether records must match all conditions (logical AND) or any condition (logical OR) to be included in the report.

5. Click **OK** to create the report.

Editing reports

To edit an existing custom report, select it in the sidebar of the **Server Center** window and choose **Edit <Report Type>** from the sidebar context menu.

The **Smart Group** dialog opens that is described above.

You cannot edit predefined reports.

Deleting reports

To delete an existing custom report, select it in the sidebar of the **Server Center** window and choose **Remove <Report Type>** from the sidebar context menu.

The report is deleted.

You cannot delete predefined reports.

Part 3: Reference

The Reference part of the manual describes the menus, dialogs, windows, and information items of Absolute Manage. Dialogs and windows are described together with the menu commands that open them. Complex windows are described in their own chapters.

Menus:

- “File menu” on page 265
- “Edit menu” on page 273
- “View menu” on page 281
- “Commands menu” on page 283
- “Server menu” on page 342
- “Window menu” on page 349
- “Help menu” on page 363

Windows:

- “Browser windows” on page 365
- “Compliance Report window” on page 378
- “Mobile Devices” on page 385
- “Server Center” on page 435
- “Agent Deployment Center” on page 510
- “Commands window” on page 527

Information items:

- “Information items” on page 534

External tools and client software:

- “Absolute Remote” on page 620
- “Absolute Manage Agent” on page 627
- “Mobile Apps” on page 630

*Chapter 10**File menu*

The **File** menu contains commands related to working with documents. Absolute Manage offers the usual range of commands in this menu:

- **New** (page 265)
- **New Tab** (page 265)
- **Open** (page 266)
- **Close** (page 266)
- **Rename Tab** (page 266)
- **Close Tab** (page 266)
- **Save** (page 267)
- **Save As** (page 267)
- **Export** (page 268)
- **Export Groups** (page 269)
- **Import Groups** (page 269)
- **Import Custom Field Data for Desktop Devices** (page 269)
- **Import Custom Field Data for Mobile Devices** (page 271)
- **Print** (page 271)
- **Print Preview** (page 271)
- **Print Setup** (page 272)
- **Recent Files submenu** (page 272)
- **Exit** (page 272)

New

The **New** command creates a new browser window.

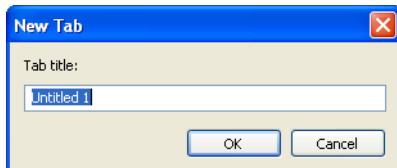
Browser windows display information from the Computers table in Absolute Manage's internal database and can display related information from other tables, e.g., the Fonts or Files table.

A detailed description of browser windows is available in "Browser windows" on page 365.

New Tab

The **New Tab** command creates a new tab in the frontmost window.

Choosing the command opens the **New Tab** dialog:



The command is available only if the frontmost window is a browser window.

Open

The **Open** command lets you open saved Absolute Manage documents.

Choosing the command brings up a standard Open dialog from the operating system. For details on this dialog, please see the Windows documentation.

When you open a document, the browser window structure is recreated as it had been saved. The window is automatically populated with the current data.

A detailed description of browser windows is available in “Browser windows” on page 365.

Close

The **Close** command closes the frontmost window, just like clicking the window’s close box.

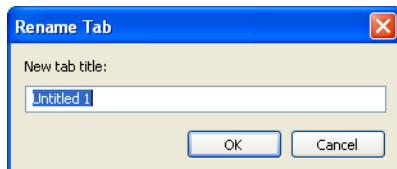
If the window contains unsaved changes, Absolute Manage asks you whether you want to save the changes.

NOTE This excludes changes to the Software Distribution Center and License Monitoring Center. Such changes are automatically saved locally but not sent to the server. They will thus be available to you when you next open Absolute Manage Admin but will not take effect before you manually send them to Absolute Manage Server.

Rename Tab

The **Rename Tab** command lets you rename the active tab.

Choosing the command opens the **Rename Tab** dialog:



The command is available only if the frontmost window contains more than one tab.

Close Tab

The **Close Tab** command closes the active tab.

Choosing the command closes the active tab after displaying a confirmation message.

The command is available only if the frontmost window contains more than one tab.

Save

The **Save** command saves the current state of the frontmost window in a file on disk. If the window is untitled, i.e., if no document has yet been assigned to it, choosing **Save** has the same effect as choosing **Save As** (see below).

When the frontmost window cannot be saved to a file, the **Save** command is disabled.

When the frontmost window is a command window, choosing **Save** opens the **Save Template** dialog that is described in “Command window toolbar” on page 284.

NOTE **Save** is not available for the **Agent Settings** command.

When the frontmost window is the **Agent Deployment Center** window, choosing **Save** saves any changes to custom zones.

Save As

The **Save As** command lets you save the state of the frontmost window under a different name than before.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, please see the Windows documentation.

The saved file contains the window's entire structure information – groups and smart groups, columns, etc. – but none of the actual contents. The contents can be stored in a local file by means of the **Export** command.

NOTE To save the contents of a browser window, use the **Export** command.

When the frontmost window cannot be saved to a file, the **Save As** command is disabled.

Command window

When the frontmost window is a command window, choosing **Save As** opens the **Save Template** dialog that is described in “Command window toolbar” on page 284.

Text file

When the frontmost window is a text file display window, choosing **Save As** lets you save the window's contents as a text file on your computer.

Export

The **Export** command lets you export the contents of the frontmost window as a file.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, please see the Windows documentation.

The command supports these export formats:

- **HTML:** The data is saved as an HTML page.
The data is saved as a single HTML page according to the HTML 4.01 Transitional standard.
- **Text (CSV, UTF-8):** The data is saved as comma-separated values in a text file.
Fields' contents are enclosed in quotes and separated by commas; records are separated by line-feed characters.
The first record contains the column names.
Dates and times are formatted as short dates and times, respectively, according to the system's current region settings.
Numbers are exported 'raw', i.e., without any kind of formatting. Bytes are not converted to megabytes or other multiples.
Text is encoded as UTF-8 (Unicode).
- **Text (CSV):** As **Text (CSV, UTF-8)** but with the current system encoding used instead of UTF-8.
- **Text (localized CSV):** As **Text (CSV)**, but with localized list dividers as separators between fields, e.g., semicolons instead of commas.
- **Text (tab-delimited, UTF-8):** The data is saved as tab-delimited text, encoded as UTF-8.
Fields' contents are separated by tab characters; records are separated by line-feed characters.
The first record contains the column names.
Fields are formatted as in the browser window being exported.
- **TheftTrack Report (HTML):** An HTML file providing an overview of the theft-tracking information on the computers in the window.
- **TheftTrack Report (XML):** The theft-tracking information on the computers in the window in XML format.
- **XML:** The data in the window is saved in XML format for processing in other applications or automated workflows.
The data is saved in a simple structure that contains information about the document, about the columns exported, and the data for the individual records.

Clicking **Save** exports the data from the window.

When the frontmost window cannot be exported, the **Export** command is disabled.

Export Groups

The **Export Groups** command lets you export the selected groups and smart groups of the frontmost window to a file.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, please see the Windows documentation.

The **Export Groups** command is available only if the frontmost window contains groups or smart groups.

Import Groups

The **Import Groups** command lets you import groups and smart groups from a file into the frontmost window.

Choosing the command opens the Open dialog from the operating system. For details on this dialog, please see the Windows documentation.

In the dialog, you can choose any group file that has been previously saved from Absolute Manage. Opening the file adds all groups that are specified in it to the frontmost window.

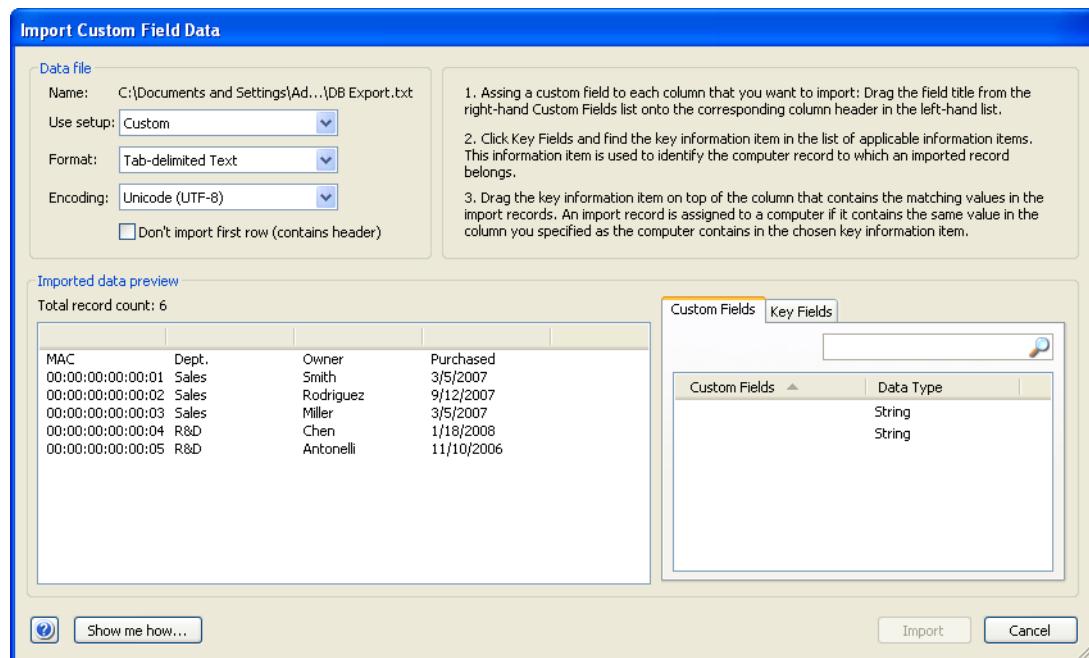
The **Import Groups** command is available only if the frontmost window can contain groups or smart groups.

Import Custom Field Data for Desktop Devices

The **Import Custom Field Data for Desktop Devices** command lets you import data from text files into manual (i.e., non-dynamic) custom information fields that have been defined for desktop devices.

Choosing the command opens the Open dialog from the operating system. (For details on this dialog, please see the Windows documentation.)

When you open a text file in this dialog (in which fields are delimited with tabs, commas, or semicolons and records are delimited with returns), the **Import Custom Field Data** dialog is displayed.



The dialog includes these elements:

- Data file:** The file you have chosen to import.
 - Use setup:** This pop-up menu lets you save particular configurations of this dialog under a name and reopen saved configurations. In addition to all saved setups, it includes these commands:
 - Save As:** Save the current settings in the dialog as a new named setup. All settings from the dialog are saved, except the import file chosen
 - Rename:** Rename the currently chosen setup.
 - Delete:** Delete the currently chosen setup. This does not affect the current settings in the dialog.
 - Data file format:** This menu lets you specify the field delimiter in the import file. Absolute Manage tries to identify the delimiter automatically and presets this menu accordingly.
 - Data file encoding:** The text encoding of the import file. Again, Absolute Manage tries to determine the encoding before displaying the dialog.
 - Don't import first row:** If this option is checked, Absolute Manage starts importing the file with the second row. This is useful if the first row contains the field names.
 - Import data preview:** This table shows the first few lines of the import file according to the current settings in the dialog. It also lets you assign custom information fields to columns in the import file by dragging a field from the **Custom Fields** list to a column.
- Dragging a field from the **Key Fields** list to a column makes that column the column by which import records are matched to Absolute Manage's database records.

- Clicking the small badge  in the column title removes the assigned field.
- **Custom Fields:** This list contains all manual custom information fields for desktop devices that can be assigned to columns of the import file.
Fields are assigned by dragging them on top of columns.
Assigning a field to a column causes that column's data to be imported into the field.
Entering text into the search field filters the list of custom information fields.
 - **Key Fields:** This list contains all information items that can be assigned to columns of the import file.
Fields are assigned by dragging them on top of columns.
Assigning a key field to a column causes Absolute Manage to store the data from each import record in that database record for which the key field matches the assigned column in the import record.
Entering text into the search field filters the list of key fields.
- **Show Me How:** Clicking this button displays a brief tutorial on importing custom information field data.
 - **Cancel:** Clicking this button cancels the import process. No data is imported.
 - **Import:** Clicking this button imports the chosen file according to the specified settings.

Import Custom Field Data for Mobile Devices

The **Import Custom Field Data for Mobile Devices** command lets you import data from text files into manual (i.e., non-dynamic) custom information fields that have been defined for mobile devices.

The command works exactly like **Import Custom Field Data for Desktop Devices**, described above, except that you can choose custom information fields for mobile devices into which to import the data.

Print

The **Print** command will be supported in a future release of Absolute Manage.

Print Preview

The **Print Preview** command will be supported in a future release of Absolute Manage.

Print Setup

The **Print Setup** command will be supported in a future release of Absolute Manage.

Recent Files submenu

The **Recent Files** submenu lists the last eight files that you have opened in Absolute Manage Admin. (The method by which the files were opened – using the **Open** command, by double-clicking, etc. – is immaterial.)

Choosing any file from the submenu opens it.

Exit

The **Exit** command quits Absolute Manage Admin. If there are unsaved changes in any open window, you are prompted to save them.

NOTE This excludes changes to the Software Distribution Center and License Monitoring Center. Such changes are automatically saved locally but not sent to the server. They will thus be available to you when you next open Absolute Manage Admin but will not take effect before you manually send them to Absolute Manage Server.

Chapter 11

Edit menu

The **Edit** menu contains commands related to editing and finding text and objects. Absolute Manage offers the usual range of commands in this menu:

- **Undo** (page 273)
- **Cut** (page 273)
- **Copy** (page 273)
- **Paste** (page 273)
- **Delete** (page 274)
- **Select All** (page 274)
- **Switch Administrator and Server** (page 274)
- **Change Administrator Password** (page 275)
- **Settings** (page 275)

Undo

The **Undo** command reverses the effects of the last action.

Absolute Manage does not currently support the undo function.

Cut

The **Cut** command will be supported in a future release of Absolute Manage.

Copy

The **Copy** command places a copy of the selected text or object on the clipboard.

Besides selected text and objects such as groups, you can also copy selected records. They are converted to text in the clipboard and can be pasted in other applications that accept text.

Paste

The **Paste** command inserts the text or objects on the clipboard into the frontmost window.

The command is dimmed when the clipboard does not contain information that can be pasted at the current location.

Delete

The **Delete** command removes the currently selected text or records.

The command is dimmed when no deletable item is selected.

Select All

The **Select All** command selects all text or records in the current context.

The command is dimmed when the keyboard focus is on an area where there are no selectable objects, e.g., an empty list, or where only one object can be selected at a time, e.g., the **Groups & Machines** list.

Switch Administrator and Server

The **Switch Administrator and Server** command opens the **Login** dialog, letting you log on to a different server, as a different user, or both:



NOTE This dialog is also the login dialog when Absolute Manage is launched, the only difference being that the **Cancel** button is a **Quit** button.

The dialog contains these text fields:

- **Server address:** The IP address or DNS name of the computer on which the desired Absolute Manage Server is running.
- **Server port:** The port number on which the Absolute Manage Server is listening.
The server is preconfigured to use port 3971; we strongly recommend against changing this value unless you experience conflicts.
- **Name:** The username as defined in Absolute Manage's **Administrator Center** window.
- **Password:** The account's password as defined in Absolute Manage's **Administrator Center** window.

If the account is based on an Active Directory user account, you can use the display name, the account name, or the login name to log in.

Note: When you set up a server for the first time, you leave the Password field empty. Details on setting up a server are available in “Initial configuration of Absolute Manage Server” on page 16.

Clicking **Login** terminates the current session and connects you to the specified server and account in a new session.

Change Administrator Password

The **Change Administrator Password** command opens the **Change Administrator Password** dialog that lets you change the password for your Absolute Manage account:



NOTE This command is not available when the currently active account is based on an Active Directory user account.

The dialog contains these fields:

- **Name:** The name of the user account.
- **Old Password:** The existing password.
- **Password:** The new password. A password may contain any Unicode character.
- **Verify:** Retype the new password in this field. If the contents of the **Password** and **Verify** fields do not match, an error message is displayed and the password change is rejected.

Settings

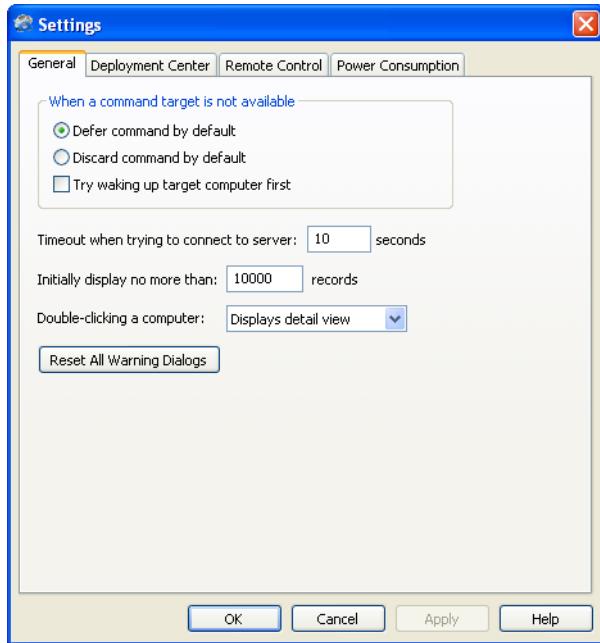
The **Settings** command opens the **Settings** dialog that lets you specify settings for the application:

The **Settings** dialog has four tabs:

- **General**
- **Deployment Center**
- **Remote Control**
- **Power Consumption**

General

The **General** tab of the **Settings** dialog lets you specify various preferences settings for Absolute Manage Admin:



The tab contains these elements:

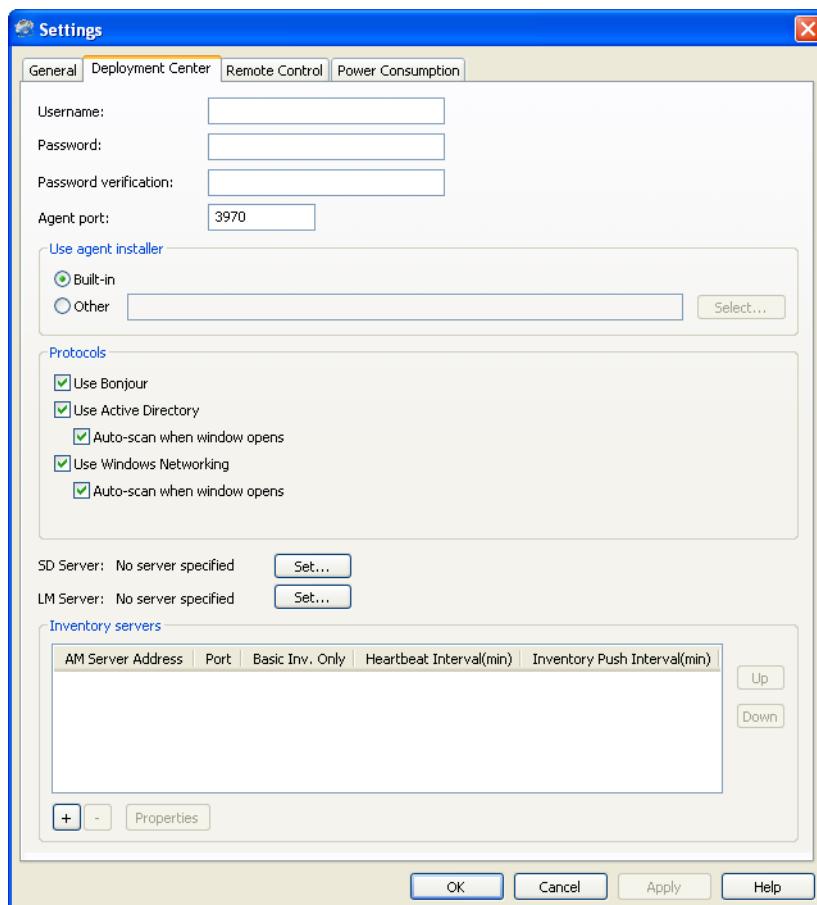
- **Default when a command target is not available:** The default behavior for cases where a target computer for a command is not available when the command is executed.
 - If you choose **Defer command**, the **Defer task if target computer is not available** option in the options dialog is checked for each new command.
 - If you choose **Discard command**, the option in the command options dialog is unchecked by default.
 - If **Try waking up target computer first** is checked, the **Wake up computer if not available** option in the command options dialog is checked by default.
- You can still change the options' settings for each command that you issue.
- **Timeout when trying to connect to server:** The time that Absolute Manage Admin waits for responses from Absolute Manage Server before it considers a connection attempt to have failed.
- **Initially display no more than:** This option lets you limit the number of records that Absolute Manage Admin displays when opening a new browser window or group in a browser window. If a database table on the server contains more records than are displayed by Absolute Manage Admin, there is an indication – “more...” – in the browser window’s status bar. The additional records can be displayed by choosing **Display All Records** from the **View** menu.
- This option is intended primarily for networks with very large database tables.

- **Double-clicking a computer:** The action that Absolute Manage Admin takes when you double-click a computer record in a browser window.
- **Reset All Warning Dialogs:** Some of Absolute Manage's warning alerts offer the option of turning this type of warning off for the future via a „do not show this dialog again“ option. Clicking this button resets all such alerts, showing them again. (Of course, you can turn any of these alerts off again by checking the option once more.)

Deployment Center

The **Deployment Center** tab of the **Settings** dialog lets you specify defaults for installing Absolute Manage Agent on administered computers or removing it.

NOTE You can override all settings when you perform an actual installation using the **Install Agent** command described on page 520 or remove Absolute Manage Agent using the **Remove Agent** command described on page 522.



The tab contains these elements:

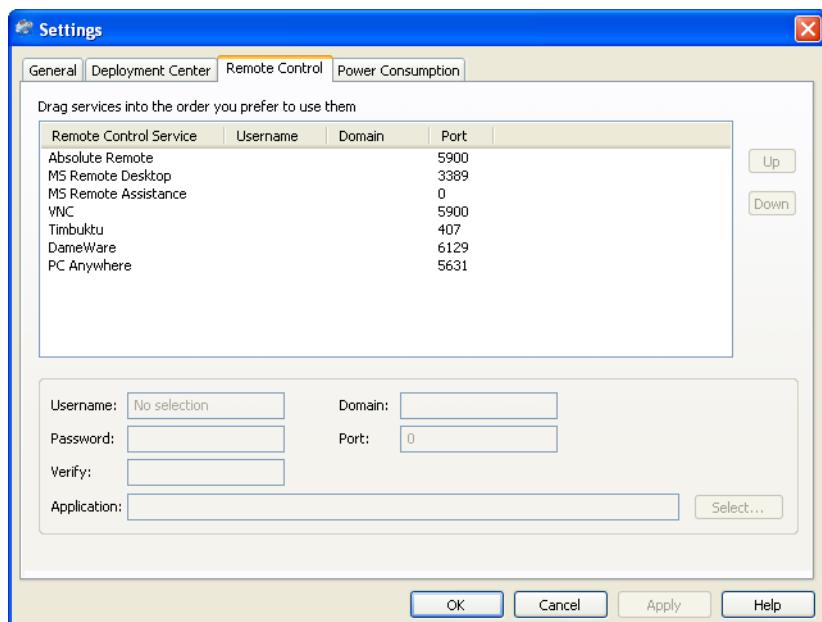
- **Username:** The username that is to be used for NetBIOS login on the selected computers.
- **Password:** The password for the NetBIOS account.

- **Password verification:** Re-enter the password to guard against typos.
- **Agent port:** The TCP port on which the agent is to communicate with the server.
Note: We recommend not to change the port unless you have a specific reason for doing so.
- **Use Agent installer:** Choose whether the installer embedded in Absolute Manage Agent is to be used for installing the Agent or a custom installer that you provide.
You can create a custom installer using the **Export Installer Package** button in the **Agent Deployment Settings** dialog, as described in “Install Agent” on page 520.
- **Select:** Clicking this button lets you select a custom installer.
- **Protocols:** These options let you choose which network protocols Absolute Manage Admin is to use to detect computers on which Absolute Manage Agent could be installed.
For all protocols except Bonjour (ZeroConf), you can specify that Absolute Manage automatically scans the network using that protocol. (With Bonjour, automatic scanning always happens when the protocol is activated.)
- **SD Server:** The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 516.
- **LM Server:** The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 516.
- **Inventory servers:** This table lists all known Absolute Manage inventory servers.
The list contains these columns:
 - **AM Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
 - **Port:** The port over which the server communicates with agents.
 - **Basic Inv. Only:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
 - **Heartbeat Interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See “Server Settings” on page 497 for details.)

- **Inv. Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.) Double-clicking a server displays a dialog for editing its settings. The dialog is described in “Inventory Server Properties dialog” on page 525.
- Clicking the + button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described in “Inventory Server Properties dialog” on page 525. Clicking the – button removes the selected server.

Remote Control

The **Remote Control** tab of the **Preferences** dialog lets you configure the remote control software that Absolute Manage is to use for viewing the screens of client computers.



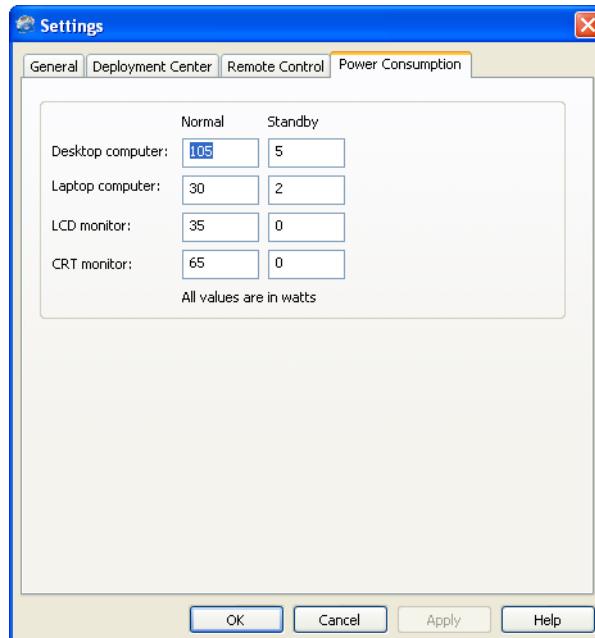
The tab contains these elements. Depending on the selected service, inapplicable fields may be disabled:

- List of supported remote control services: The list contains the remote control services that Absolute Manage supports, along with important parameters.
You can drag the entries to reflect the order of your preference; Absolute Manage always tries from the top of the list before lower ones to remotely control a client.
- **Username:** The user account for the remote control software on the client computers.
- **Password** and **Verify:** The password for the specified account.
Note: Some VNC applications do not support being supplied with a username and password when they are launched; when you are using these applications, you must enter a username and password within the application, even if you have already supplied both in Absolute Manage. This is a limitation of these applications, not of Absolute Manage.

- **Application:** The local application that will be used to connect to the client. If desired, you can specify a different application for the selected service by clicking the **Select** button and choosing the application's executable on the hard disk.
- **Domain:** The Windows networking domain to be used for accessing client computers.
- **Port:** The network port on which to contact the remote control software on the client computers.

Power Consumption

The **Power Consumption** tab of the **Settings** dialog lets you configure the power consumption levels of various types of devices. Absolute Manage uses these rates in calculating the power usage reports.



The tab contains **Normal** and a **Standby** fields for computers (stationary and portable) and monitors (LCD and CRT). They contain the typical amounts of power (measured in watts) that a device of that type consumes in your organization.

Chapter 12

View menu

The **View** menu contains commands related to displaying and configuring toolbars and status bars.

- **Toolbar** (page 281)
 - **Status Bar** (page 281)
 - **Details** (page 281)
 - **Select Container** (page 281)
 - **Configure Columns** (page 282)
 - **Display All Records** (page 282)
-

Toolbar

The **Toolbar** command toggles the display of the toolbar of the frontmost window. It is available only if the frontmost window can have a toolbar.

Status Bar

The **Status Bar** command toggles the display of the status bar at the bottom of the screen.

Details

The **Details** command displays details for a selected computer, software package, or license specification.

Choosing the command for a computer selects it in the browser window's sidebar and displays in the sidebar all information categories that are available for the computer.

Choosing the command for a software package or license specification displays the package's or specification's details in the table area of the browser window.

Select Container

The **Select Container** command selects (in a browser window's sidebar) the container of a selected item.

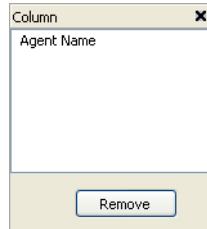
Choosing the command selects the next-higher container (i.e., expandable item) in the browser window's sidebar.

NOTE You can also press Left Arrow on the keyboard for the same effect.

Configure Columns

The **Configure Columns** command lets you add, rearrange, or remove columns from the frontmost window.

Choosing the command displays the Columns sidebar:



The sidebar contains the titles of all columns that appear in the window, in the order in which the columns appear.

Rearranging the column titles in the sidebar rearranges the columns in the window.

Dragging an information item from the **Information Items** window to the sidebar adds a corresponding column to the windows.

Clicking **Remove** removes the selected column from the window.

Clicking the close box in the top right of the sidebar closes it.

Display All Records

The **Display All Records** command loads records from the server into the frontmost window in cases where not all records have been loaded because that would have exceeded the limit set in the **Settings** dialog's **General** tab.

Choosing the command loads all records from the server that are not yet displayed in the frontmost window.

The command is available only if the frontmost window does not display all records (which is indicated in the status bar).

Chapter 13

Commands menu

The **Commands** menu contains commands that let you perform actions related to the managed computers.

There are two different command lists in the menu, one for windows showing information related to desktop computers and another for windows showing information related to mobile devices.

Both versions are listed below.

Commands menu for desktop computers

- **Command window toolbar** (page 284)
- **Agent Settings** (page 287)
- **Power Management Settings** (page 293)
- **Send Message** (page 296)
- **Change Operating State** (page 296)
- **Wake Up** (page 297)
- **Terminate Process** (page 298)
- **Reinstall Mac OS X Computer** (page 298)
- **Reinstall Windows Computer** (page 301)
- **Change Services Operation State** (page 303)
- **Time Machine** (page 304)
- **Search Windows Registry** (page 305)
- **Edit Windows Registry** (page 306)
- **Execute Script** (page 307)
- **Execute Macintosh File** (page 309)
- **Execute Windows File** (page 312)
- **Install Software Packages** (page 314)
- **Transfer File/Folder** (page 315)
- **Copy File/Folder** (page 318)
- **Create Shortcut** (page 321)
- **Create Folder** (page 322)
- **Delete File/Folder** (page 323)
- **Find File** (page 323)
- **Move File/Folder** (page 325)
- **Open File** (page 325)
- **Rename File/Folder** (page 327)
- **View Text File** (page 327)
- **Gather Process Information** (page 328)
- **Gather Inventory Information** (page 328)
- **Gather Installed Software** (page 329)
- **Gather Compliance Report** (page 331)
- **Run Software Distribution Check** (page 332)
- **Run License Monitoring Scan** (page 332)
- **Execute Command** (page 332)
- **Command Options** (page 332)
- **Execute Command Now** (page 333)
- **Edit Command** (page 333)
- **Reapply Command** (page 333)
- **Show/Hide Target List** (page 334)

Commands menu for mobile devices

- [Install Configuration Profile](#) (page 334)
- [Install Provisioning Profile](#) (page 335)
- [Install Application](#) (page 335)
- [Issue Device Lock](#) (page 336)
- [Issue Clear Passcode](#) (page 337)
- [Issue Remote Erase](#) (page 338)
- [Set Roaming Options](#) (page 338)
- [Send Message to Device](#) (page 339)
- [Update Device Info](#) (page 339)
- [Track Device](#) (page 339)
- [Get Device Geolocation](#) (page 341)
- [Reset Tracking Passphrase](#) (page 341)

Favorites

The **Favorites** submenu contains command templates that you want to have quickly available.

The menu contains all command templates that have been saved with the **Include in favorites** option in the **Save Template** dialog or that have been checked in the **Command Templates** window's **Favorites** column.

Command window toolbar

All command windows share a common toolbar. It contains buttons that let you specify options for the timing and scope of the command execution as well as saving command templates and getting help.

The toolbar contains these buttons by default:



These buttons are described in:

- “Execute” on page 284
- “Options” on page 285
- “Targets” on page 286
- “Save Template” on page 287
- “Show Help” on page 287

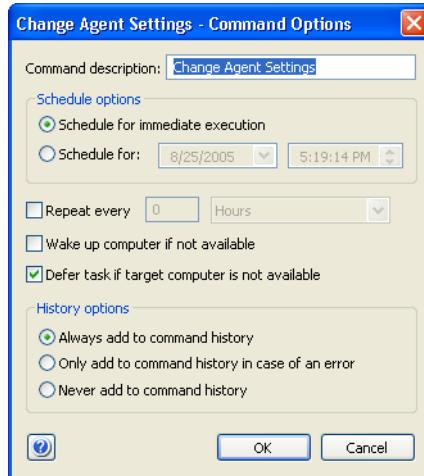
Execute

The **Execute** button executes the command with the currently specified options and closes the command window.

Depending on the scheduling settings (see below), clicking **Execute** executes the command immediately or enters it in the command queue for later execution.

Options

Clicking the **Options** button opens the **Command Options** dialog:



The dialog contains these elements:

- **Command description:** The title under which the command will appear in the **Commands** window.
- **Schedule for immediate execution:** The command will be executed immediately when the **Execute** button in the command window is clicked.
- **Schedule for:** When the **Execute** button in the command window is clicked, the command will not be executed immediately but entered in the command queue to be executed at the specified date.
- **Repeat every:** If this option is checked, the command is executed in the specified intervals after its first execution.
- **Wake up computer if not available:** If this option is checked, Absolute Manage tries to wake up any target computer that is not available before considering it unavailable.
Note: The default for this setting is specified in the Settings dialog.
- **Defer task if target computer is not available:** This option determines what happens with the command if a target computer is not available. If it is checked, the command is entered in the command queue to be executed when the target computer becomes available. If the option is unchecked, the command is considered to have failed and no attempt is made to execute it at a later date.
Note: The default for this setting is specified in the Settings dialog.
- **History options:** These options let you specify in which this command will be entered into the command history:
 - **Always add to command history:** After the command has been completed, it is added to the command history in all cases, no matter the outcome.
 - **Only add to command history in case of an error:** The command is only added to the command history when it could not be executed successfully.

- **Never add to command history:** After the command has been completed, it is removed from the command window. In no case is it added to the command history.

Targets

Clicking the **Targets** button display or hides the **Target Computers** list, toggling its state.



Dragging a computer from a browser window into this list adds it to the target list, causing the command to be executed on that computer as well.

You can include computer groups and smart groups as targets. This has the following effects:

- Specifying a (non-smart) computer group as a target has exactly the same effect as specifying all their members as targets individually.
- The effect of specifying a smart computer group as a target varies according to the type of command execution:
 - When the command is executed immediately or at a specified time or when it is saved as a template and later re-used, all computers that are members of the specified smart group at the moment of execution are the command targets. (That is, it does not matter which computers belong to the smart group at the moment when the command is saved.)
 - When the command is a repeating command, the membership of the smart group is evaluated anew each time the command is executed. All computers that meet the smart group criteria at that time are command targets, and all computers that do not meet these criteria are not targets.

This means that a computer can be sometimes but not always a target of a repeating command with a smart group as its target.

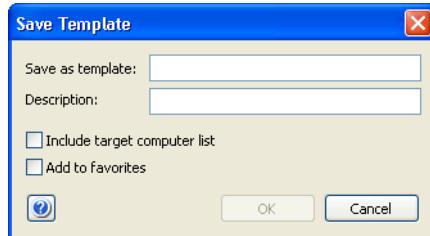
Note: For performance reasons, the membership in the smart groups for purposes of determining targets of repeating commands is evaluated only periodically.

Therefore, computers may be erroneously included in or excluded from the list of targets when their status with respect to the smart group criteria changes very shortly before the execution of the repeating command.

Clicking the **Remove** button removes the selected computers from the target list.

Save Template

Clicking the **Save Template** button opens the **Save Template** dialog:



The dialog lets you save the command in its current state – including all settings – as a template for future reuse. It contains these elements:

- **Save as template:** The name for the command template.
- **Description:** The description for the command template that will be displayed in the **Command Templates** window. When the dialog is opened, this field contains the text from the **Options** dialog's **Command description** field.
- **Include target computer list:** If this option is checked, the current list of target computers for the command is included in the template. If the option is unchecked, the template is saved with an empty target list.
- **Add to favorites:** If this option is checked, the saved template is listed in the **Favorites** submenu.
- **Save:** Clicking the **Save** button stores the command as a command template that can be reused via the **Command Templates** window.

Show Help

Clicking the **Show Help** button displays the help for the command to which the command dialog belongs.

Agent Settings

The **Agent Settings** command lets you specify various settings for the Absolute Manage Agents on the selected computers.

Choosing the command opens the **Agent Settings** dialog. The dialog has four panes:

- **General**
- **Servers**
- **Client Information**
- **Custom Fields**

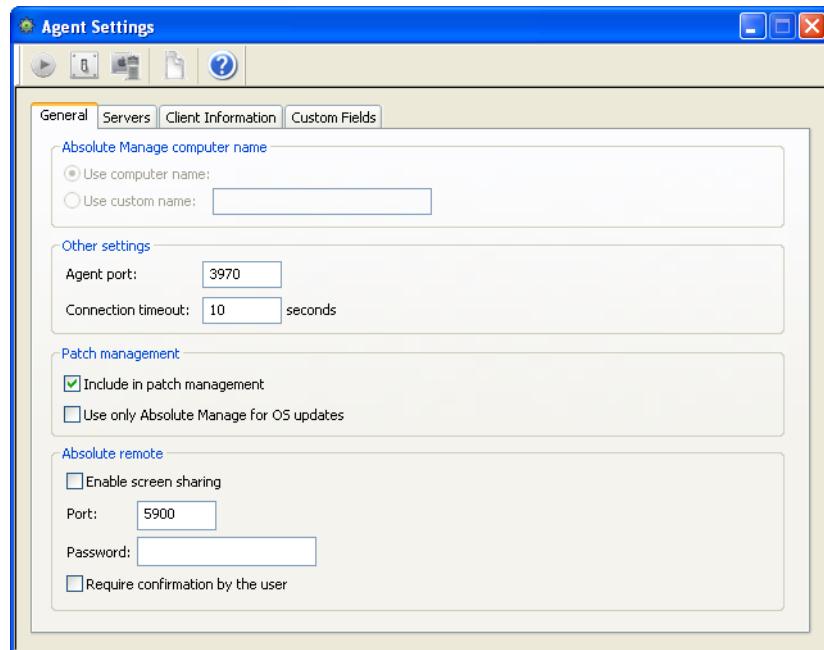
All three are described below.

The toolbar of command windows is described in “Command window toolbar” on page 284. Note, however, that it is not possible to save the **Agent Settings** command as a command template; both the **Save**

Template button in the toolbar and the **Save** command in the **File** menu are disabled.

General

The **General** pane of the **Agent Settings** dialog lets you configure various basic parameters for the agents' operation:



- **Absolute Manage computer name:** The name that is displayed for the computer in the Absolute Manage system. You can choose to use the name specified for the computer in the local operating system or you can specify a custom name that is only used by Absolute Manage. This option is not available when there is more than one computer in the commands target list.
- **Agent port:** The TCP port over which the Agent communicates with the Absolute Manage Server. We recommend that you do not change this port unless there is a specific reason.
- **Connection timeout:** The interval before the Agent considers an attempt to contact a server to have failed. When the attempt was made to send a regular information report (such as the heartbeat or an inventory report), the Agent retries at the next scheduled time. Attempts to download software to be deployed or to report the success of a software installation are repeated at the next opportunity.
- **Include in patch management:** Whether this agent is to use the Software Update Utility (Mac OS X) or Windows Update (Windows) to check for available patches and then install them using the Software Distribution Center. (This is discussed in more detail in "Automated patch management" on page 235.)
- **Use only Absolute Manage for OS Updates:** When this option is checked, the local update mechanism of the operating system – i.e., Software Update for Mac OS X or Windows Update for Windows – is disabled. The agents neither check for

new software via this mechanism nor do they download any updates from Apple's or Microsoft's servers.

All operating system software updates are performed via Absolute Manage's Software Distribution Center.

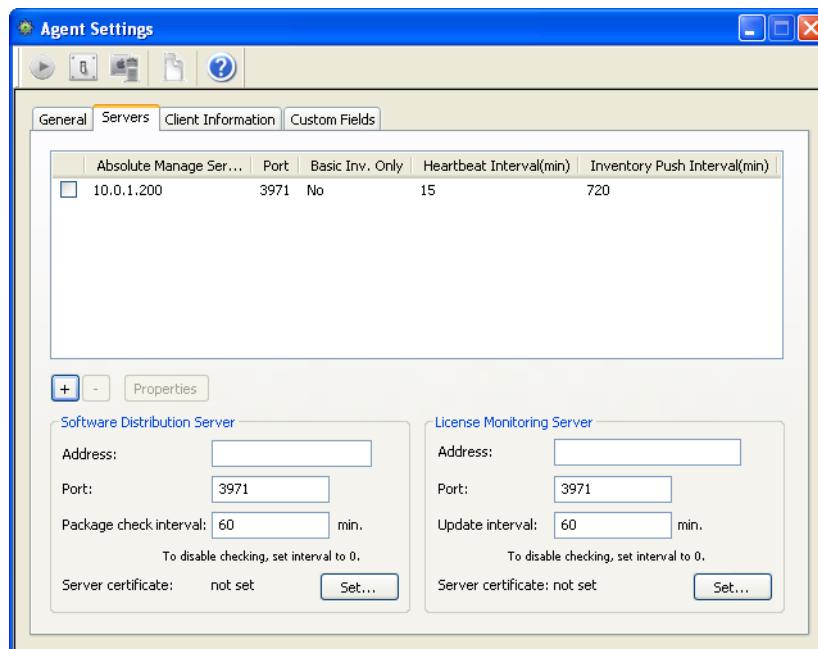
- **Enable screen sharing:** When this option is checked, the computer allows its screen to be shared via the built-in Absolute Remote function of the Agent. (Note that disabling screen sharing here has no effect on third-party screen-sharing software.)
- **Port:** The port over which the Agent accepts screen-sharing requests.
- **Password:** The password required to authorize screen-sharing requests. If this field is left empty, no password is required.
- **Require confirmation by user:** If this option is checked, the local user of the computer has to approve all screen-sharing requests. If it is unchecked, all incoming connection requests are automatically accepted (as long as the correct password, if any, is provided).

When there is more than one target computer, checkboxes are displayed to the right of most options. Only checked options are updated in the Agents.

NOTE The options in this tab can be set only by administrators with the **Change Agent General Settings** right. See "New Administrator" on page 481 for details.

Servers

The **Servers** pane of the **Agent Settings** dialog lets you configure server addresses and communication intervals:



When there is more than one target computer, checkboxes are displayed to the right of all options outside the list. Only checked options are updated in the agents.

Main list

The main list contains the Absolute Manage Servers with which the selected agents can communicate:

- When a server is checked, all agents will be set to communicate with it.
- When a server is unchecked but present in the list, its current state on the agents will not be changed. (That is, agents that were set to communicate with it before will remain to be thus set. Agents who were not set to communicate with this server before will not be set to do so afterwards.)
- A server that is not in the list will be removed from the list of servers to communicate with on all agents; none of the target agents will communicate with this server after the command has been executed.
- A server which contains “Yes” in the **Basic Inv. Only** column will be sent only basic inventory information by the target agents. This useful for eliminating unnecessary network traffic to servers that are to act only as software distribution servers or license monitoring servers.

The list columns contains parameters for the server that you can edit by clicking the **Properties** button, opening the **Inventory Server Properties** dialog (see “Inventory Server Properties dialog” on page 525):

- **Absolute Manage Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
- **Port:** The port over which the server communicates with agents.
- **Basic Inv. Only:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
- **Heartbeat Interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See “Server Settings” on page 497 for details.)
- **Inventory Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

Clicking the **+** button opens a dialog that lets you add a new server to the list. The dialog is described in “Inventory Server Properties dialog” on page 525. Clicking the **-** button removes the selected server.

Software Distribution Server

- **Address:** The IP address or DNS name of the Absolute Manage Server that will be the software distribution server for the selected agents.
Note: Here, too, we recommend using only fully qualified DNS names (or IP numbers).
- **Port:** The port over which the server communicates with agents.
- **Package check interval:** The interval in which the agents are to check the server for new or changed packages.
*Note: The same kind of check can be performed manually from the Absolute Manage Agent control panel’s **Software Updates** pane.*
- The **Server certificate** field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.
- The **Set** button lets you open a saved certificate file to validate the server.
Saving certificate files is described in “Exporting a server certificate” on page 19.

License Monitoring Server

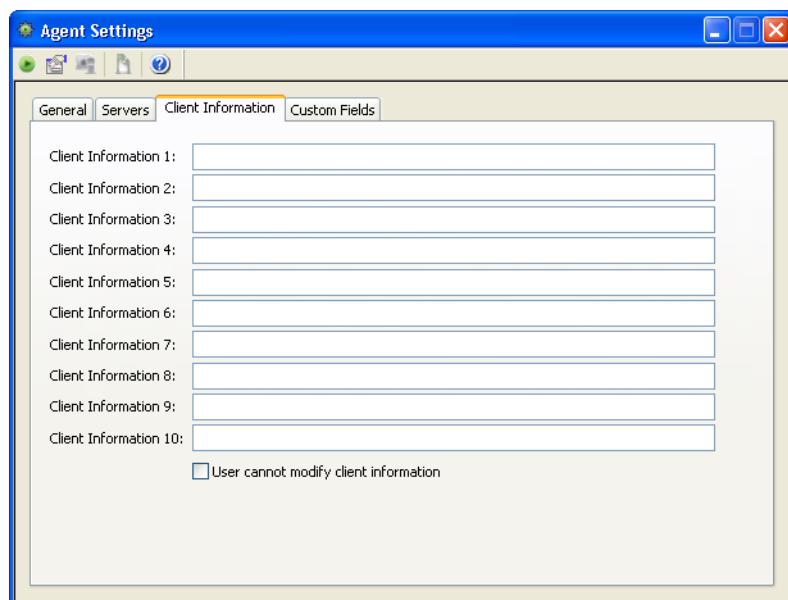
- **Address:** The IP address or DNS name of the Absolute Manage Server that will be the license monitoring server for the selected agents.
Note: Here, too, we recommend using only fully qualified DNS names (or IP numbers).
- **Port:** The port over which the server communicates with agents.
- **Update interval:** The interval in which the agents check the server for changes to the licensing specifications.
- The **Server certificate** field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.
- The **Set** button lets you open a saved certificate file to validate the server.

Saving certificate files is described in “Exporting a server certificate” on page 19.

NOTE The options in this tab can be set only by administrators with the **Change Agent Server Settings** right. See “New Administrator” on page 481 for details.

Client Information

The **Client Information** pane of the **Agent Settings** dialog lets you specify the contents of the ten Client Information fields that allow, e.g., locations or inventory numbers to be stored on the administered computers:



When there is more than one target computer, checkboxes are displayed to the right of all fields. Only checked fields are updated in the agents.

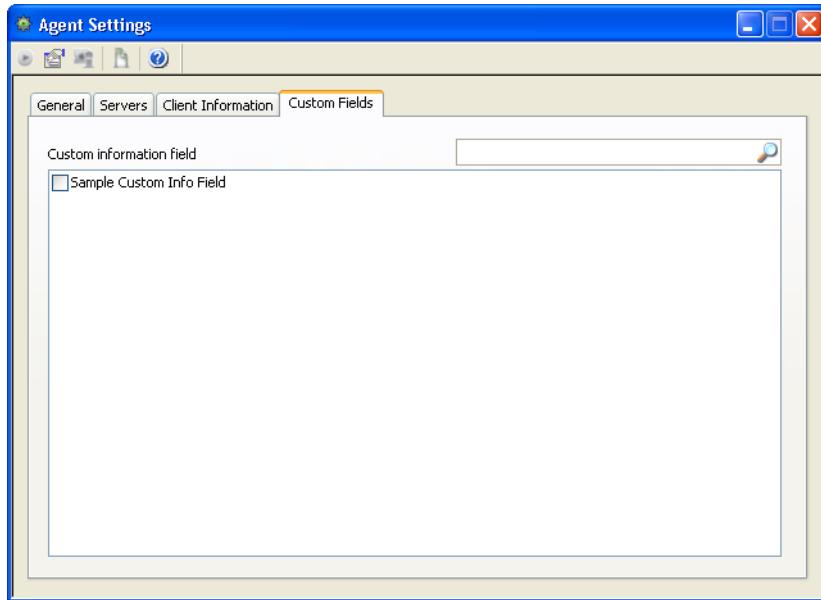
The **User cannot modify client information** option lets you prevent users from changing the fields’ contents locally or allow them to do so.

NOTE The names of the fields can be changed in the **Server Settings** dialog.

NOTE The options in this tab can be set only by administrators with the **Change Agent Client Info Settings** right. See “New Administrator” on page 481 for details.

Custom Fields

The **Custom Fields** pane of the **Agent Settings** dialog lets you assign existing custom information fields to selected agents:



The dialog contains a list displaying all custom information fields that are defined on the Absolute Manage Server.

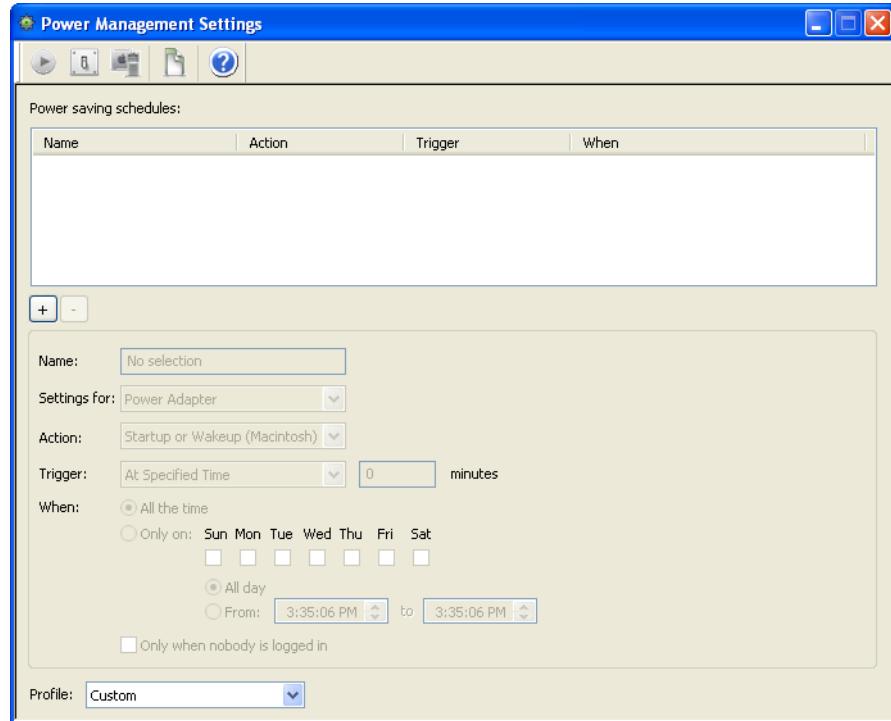
All fields that are checked in the **Use** column are assigned to the target computers; all fields that are not checked are unassigned. The status of fields whose checkbox is in the 'neutral' state () remains unchanged.

NOTE The options in this tab can be set only by administrators with the **Change Custom Info Fields Settings** right. See "New Administrator" on page 481 for details.

Power Management Settings

The **Power Management Settings** command lets you set the target computers' automatic sleep and wake-up settings.

Choosing the command opens the **Power Management Settings** dialog:



The dialog contains these elements:

- **Power saving schedules:** This list contains all schedules that are to be applied to the target computers. You can define any number of schedules; all are applied to the targets and all are active at the same time on these computers. Click the **+** button to create another schedule. Click a schedule in the list to display its settings. You can change the settings of the selected schedule; all changes are saved automatically when you select another schedule. Click the **-** button to delete the selected schedule.
- **Name:** The name of the schedule.
- **Settings for:** The type of power supply to which this schedule applies. The schedule will only be active if the target computer runs on the specified type of power.
- **Action:** What is to happen when the conditions specified in this schedule are met. Available actions include:
 - **Start Up or Wake Up:** The computer is woken from sleep. If it is switched off, it is started. This option applies only to Macintosh clients.
 - **Wake Up:** The computer is woken from sleep. If it is switched off, nothing happens. This option applies only to Macintosh clients.
 - **Sleep:** The computer is put to sleep.
 - **Hibernate:** The computer is put into hibernation. This option applies only to Windows clients.
 - **Restart:** The computer is restarted. This is a 'soft' restart, i.e., the user is prompted to save open documents that

contain unsaved changes. If these prompts are not answered, the restart fails.

- **Restart (Forced):** The computer is restarted. This is a 'hard' restart, i.e., there is no user prompt, all applications are terminated by force, and any unsaved changes in open documents are lost.
- **Shut Down:** The computer is shut down. This is a 'soft' shutdown, i.e., the user is prompted to save open documents that contain unsaved changes. If these prompts are not answered, the shutdown fails.
- **Shut Down (Forced):** The computer is shut down. This is a 'hard' shutdown, i.e., there is no user prompt, all applications are terminated by force, and any unsaved changes in open documents are lost.
- **Log Out:** The active user is logged out. The user is prompted to save open documents that contain unsaved changes. If these prompts are not answered, the logout fails.
- **Display Sleep:** The display is dimmed to blackness.
- **Hard Disk Sleep:** The hard disks are spun down.

Before the **Sleep**, **Hibernate**, **Restart**, **Shut Down**, or **Log Out** actions are performed, an alert is displayed on the target computer that gives the user the chance to cancel the action.

Note: Individual client computers may lack the required hardware or operating system support for some options.

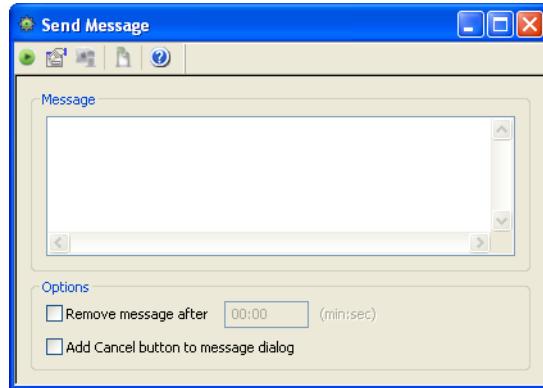
- **Trigger:** The kind of condition by which the action is triggered. You can specify that the action happens at particular times of the day or after a certain period of inactivity.
- **When:** The times of the day and the week when this schedule is to be active. You can either specify that it is active all the time or you can restrict it to certain days and times of the day. The time of the day is the same for all days. Note that the time is specified using a 24 hour clock.
- **Profile:** Using this menu, you can save the current settings for easy later recall.
When the pop-up menu is closed, it displays the currently active profile. If no profile is active, it displays **Custom**.
 - **Save As:** Choosing this command lets you save all schedules currently listed in the list at the top of the command window under a name of your choice. All saved profiles are added to the pop-up menu.
 - **Rename:** Choosing this command lets you edit the name of the currently active profile. The command is unavailable if no profile is active.
 - **Delete:** Choosing this command removes the currently active profile from the **Profile** pop-up menu.
Note: This does not remove the currently shown schedules from the command window.
- **Only when nobody is logged in:** If this option is checked, the schedule applies only as long as no user is logged in on the target computer. If it is unchecked, it applies regardless of whether a user is logged in.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Send Message

The **Send Message** command sends a message to selected client computers.

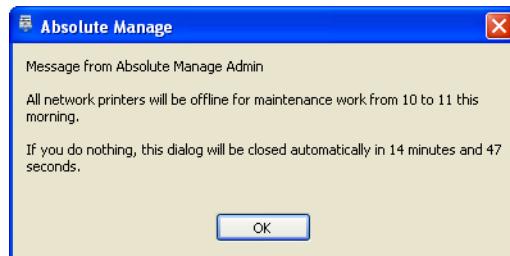
Choosing the command opens the **Send Message** dialog:



The dialog contains these elements:

- **Message**: The text that will appear on the client computers.
- **Remove message after**: If this option is chosen, you can enter a time in minutes and seconds after which the message dialog on the client computer is automatically closed. The dialog is closed as if the user had clicked **OK**. (The timeout is, however, noted in the command history.)
- **Add Cancel button to message dialog**: If this option is checked, the message dialog on the client computer has a **Cancel** button in addition to the **OK** button. You can see in the command history whether a user clicked the **Cancel** button.

When the command is executed, the message appears in a dialog on the screen of each selected target:

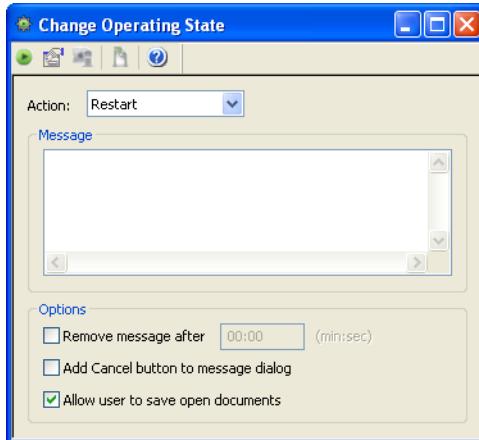


The toolbar of command windows is described in “Command window toolbar” on page 284.

Change Operating State

The **Change Operating State** command restarts, shuts down, or puts to sleep remote computers or logs their users out.

Choosing the command opens the **Change Operating State** dialog:



The dialog contains these elements:

- **Action:** The desired change in the operating states of the target computers.
Note: When you try to put to sleep a Windows computer, Absolute Manage first tries to hibernate it. If that is not supported, it tries to put it into stand-by mode. If the computer does not support this mode either, the command fails with an error log entry.
- **Message:** An optional text that will appear on the target computers before the action is executed. Leave empty to display no message.
- **Remove message after:** If this option is chosen, you can enter a time in minutes and seconds after which the message dialog on the client computer is automatically closed.
- **Add Cancel button to message dialog:** If this option is checked, the message dialog on the client computer has a **Cancel** button in addition to the **OK** button. If a user clicks the **Cancel** button, the action is not executed on that computer.
- **Allow user to save open documents:** If this option is checked, quit events are sent to all running processes, allowing the user to save unsaved changes. If the option is unchecked, all processes are forcefully terminated and unsaved changes are lost.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Wake Up

The **Wake Up** command wakes up remote computers. There are no options for this command, but target computers must support Wake On LAN and the feature must be activated.

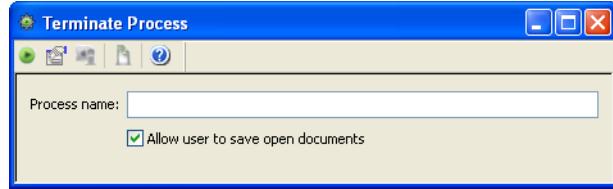
Waking up computers is possible across subnets as long as an Absolute Manage Server or Absolute Manage Agent is running (active) in the target subnet.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Terminate Process

The **Terminate Process** command stops processes running on target computers.

Choosing the command opens the **Terminate Process** dialog:



The dialog contains these elements:

- **Process name:** The name of the process that you want to terminate. You must enter the exact name. If you open the dialog while a process is selected in the frontmost window, the name is pre-entered. If you select more than one process, only the number of processes is shown.
- **Allow user to save open documents:** If this option is checked, quit events are sent to the target processes, allowing the user to save unsaved changes. If the option is unchecked, the processes are forcefully terminated and unsaved changes are lost.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Reinstall Mac OS X Computer

The **Reinstall Mac OS X Computer** command lets you reinstall client computers from a specified disk image or Time Machine backup.

Choosing the command opens the **Reinstall Mac OS X Computer** dialog. The dialog has two panes:

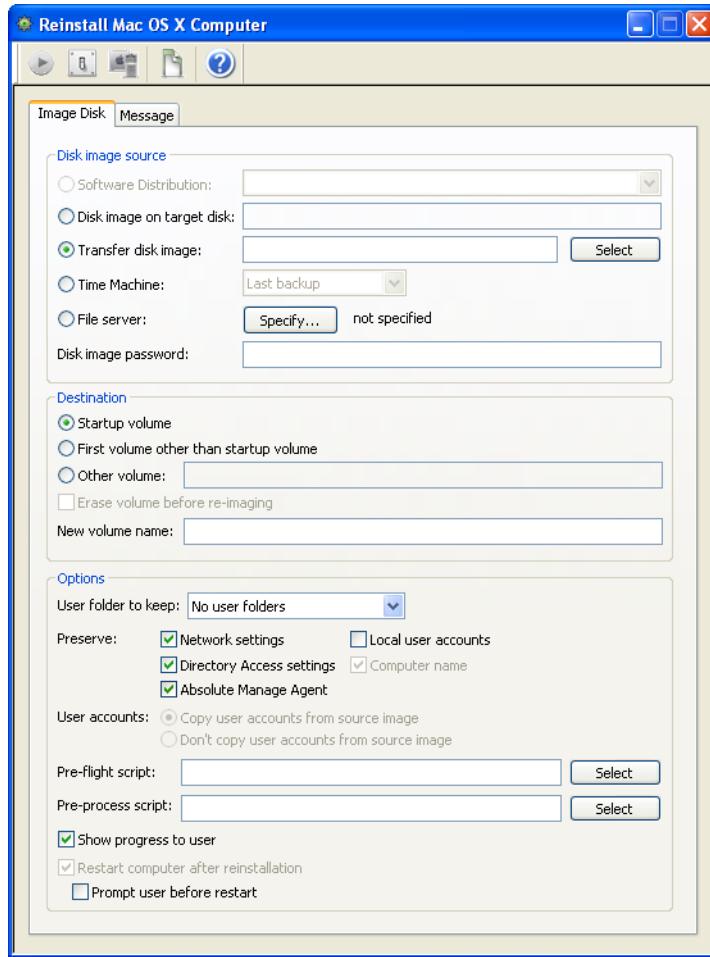
- **Disk Image**
- **Message**

Both are described below.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Disk Image

The **Disk Image** pane of the **Reinstall Mac OS X Computer** dialog lets you choose an image and set options for the reinstallation of the target computers.



The dialog contains the following elements:

- **Software Distribution:** When one of the disk images available in the Software Distribution Center is chosen from the pop-up menu, that image's contents will be written to the boot volumes of the target computers.
- **Disk image on target disk:** Specify the path to a disk image that is already present on the intended target disk.
- **Transfer disk image:** Choosing **Transfer disk image** allows you to select a disk image file on your computer instead of one from the Software Distribution Center. Clicking **Select** opens an **Open** dialog for choosing the image.
- **Time Machine:** If the target computer runs Mac OS X 10.5 or newer and Time Machine is active on it, you can specify that a Time Machine Backup be restored. The pop-up menu lets you specify a date; Absolute Manage restores the last backup prior to that date.
- **File server:** Specify a disk image that is located on a file server. Clicking the **Specify** button opens a dialog in which you specify the server and the location of the disk image on it:

- **Disk image source:** The path of the disk image on the server volume.
- **Server address:** The file server's network address.
- **Server volume:** The volume on which the disk image is located.
- **User:** The user account which Absolute Manage is to use for logging in to the server.
- **Password:** The password for the account.
- **Disk image password:** If the image is password-protected, enter the password here.
- **Re-image:** The volume on which the disk image's contents is to be installed. Options include:
 - **Startup volume:** The selected client's current boot volume.
 - **First volume other than startup volume:** The second volume in the client's volume list, with the startup volume considered the first volume in the list.

IMPORTANT

This option is primarily intended to allow you to reinstall the (sole) local volume of a computer that has been booted from a network volume. If there are more than two volumes on a client, there is no way to tell which of the non-startup volumes will be chosen. We strongly recommend against using this option on computers with more than two mounted volumes.

- **Other volume:** The name of a local volume of the client.
- **New volume name:** The name that the target computers' boot volumes will have after the reinstallation.
- **User folder to keep:** Whether to keep any user folders (i.e., subfolders of the **Users** folder belonging to individual users) during the reinstallation and, if so, which ones:
 - **No user folders:** All user folders will be deleted during the reinstallation.
 - **Folder of current user:** The user folder of the user who is currently logged in will be preserved; all others will be deleted.
 - **All user folders:** All user folders will be preserved.
- **Preserve:** Preserve the target computers' current network settings during the reinstallation:
 - **Network settings:** General network settings.
 - **Directory Access settings:** Settings related to accessing directory services such as Active Directory.
 - **Absolute Manage Agent:** The Absolute Manage Agent with all its settings.
 - **Local user accounts:** Currently existing user accounts on the target computers.
 - **Computer name:** The name of the computer by which it is known in the network.
- **User accounts:** If **Copy user accounts from the source image** is chosen, all user accounts that have been defined on the source image, including their access privileges and data, are copied to the reinstalled computer. If **Don't copy user accounts from the source image** is chosen, no accounts from the source image are added to the preserved accounts (if any) on the target computer.

- **Pre-flight script:** Clicking the **Select** button allows you to specify a shell script that is executed on the target computers after the disk has been mounted but before any files have been copied to the local hard disk.
These parameters are supplied to the script:
 - \$1: the disk image mount point
 - \$2: the name of the specified target volume (*/* for the boot volume)
- **Pre-process script:** Clicking the **Select** button allows you to specify a shell script that is executed on the target computers before the reinstallation.
These parameters are supplied to the script:
 - \$1: the path to the folder where the installation files have been copied
- **Other options:** Additional settings for the reimaging process:
 - **Show progress to user:** A progress bar on the local computer keeps the user informed of the process state.
 - **Restart computer after reinstallation:** If this option is checked, the target computer is rebooted when the installation is complete. When the startup volume is reinstalled, this option cannot be deactivated.
 - **Prompt user before restart:** If this option is checked, a dialog is displayed on the target computer, allowing the user to postpone restarting. This gives local users additional time to save open documents, etc.

Message

The **Message** tab of the **Reinstall Mac OS X Computer** dialog lets you send a message to target computers before their computers are reinstalled. A black dot on the tab  indicates that a message has been specified, even when you select another tab.

The elements of this pane are described in “Send Message” on page 296.

If a **Cancel** button is added to the dialog, any target computer on which the user clicks **Cancel** will not be reinstalled.

Reinstall Windows Computer

The **Reinstall Windows Computer** command lets you reinstall client Windows computers from a specified disk image on the FOG server.

In addition to administered computers with agents you can also specify placeholder records as targets. See “Creating placeholder records for computers” on page 65 for information on how to create placeholder records.

Using the command requires a FOG server or Absolute Manage PXE server in addition to Absolute Manage Server. The required installation procedure is described in “Installing support for reinstalling Windows computers” on page 20.

Choosing the command opens the **Reinstall Windows Computer** dialog. The dialog has two panes:

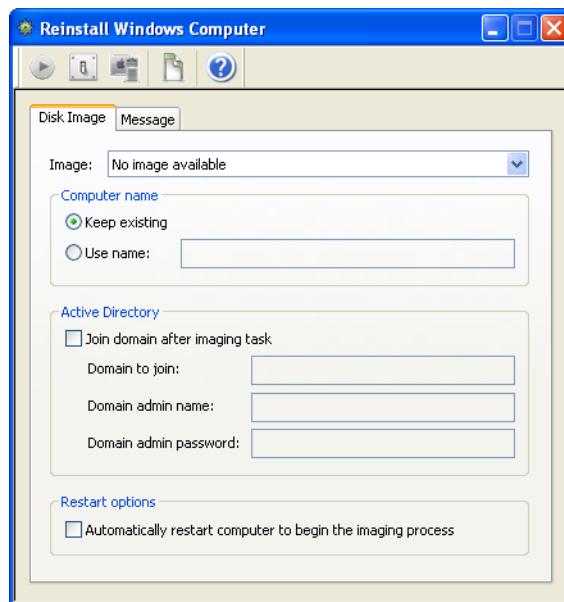
- **Disk Image**
- **Message**

Both are described below.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Disk Image

The **Disk Image** pane of the **Reinstall Windows Computer** dialog lets you choose an image and set options for the reinstallation of the target computers.



The dialog contains the following elements:

- **Image:** This pop-up menu includes all disk images that are stored on the FOG server (if you use FOG) or in Absolute Manage Server under Windows Disk Images (if you use the Absolute Manage PXE server).
- **Computer name:** The name to give the target computer:
 - **Keep existing:** After the reinstallation, the computer has the same name as now.
 - **Use name:** The name is changed to the specified name during reinstallation.
- **Join domain after imaging task:** If this option is checked, the computer joins the specified Active Directory domain after the reinstallation.
- **Domain name:** The name of the Active Directory domain to join.
- **Domain admin name:** The username of an administrator account for the domain controller. You can also enter the UPN (user principal name) for the account.

- **Domain admin password:** The password for the administrator account.
- **Automatically restart computer to begin the imaging process:** If this option is checked, the selected target computers are automatically restarted to begin the reinstallation. This option has no effect on target computers without an agent (i.e., target computers that have been specified by means of placeholder records).

Message

The **Message** tab of the **Reinstall Windows Computer** dialog lets you send a message to target computers before their computers are reinstalled. A black dot on the tab  indicates that a message has been specified, even when you select another tab.

Messages cannot be sent to selected target computers without agents (i.e., computers that are represented by placeholder records).

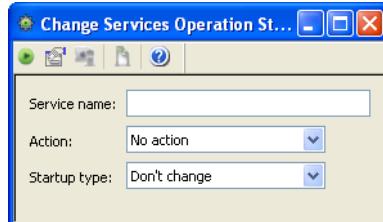
The elements of this pane are described in “Send Message” on page 296.

If a **Cancel** button is added to the dialog, any target computer on which the user clicks **Cancel** will not be reinstalled.

Change Services Operation State

The **Change Services Operation State** command allows you to start or stop services on Windows computers and set their startup states.

Choosing the command opens the **Change Services Operation State** dialog:



The dialog contains these elements:

- **Service name:** The name of the service you wish to affect, as displayed in the **Service Name** information item. If a single service is selected in a browser window when you open the command dialog, its name is pre-entered in the field. If more than one service is selected, the number of services is displayed in the field.
- **Action:** The change to the operating state that you want to affect.
- **Startup type:** The startup status to which you want to set the selected services:

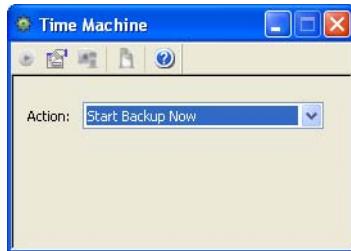
- **Automatic:** The service is automatically started whenever the operating system boots.
- **Manual:** The service is not automatically started but may be started by users or other applications.
- **Disabled:** The service cannot be started at all.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Time Machine

The **Time Machine** command lets you control the operation of Time Machine on target computers. The command can only be used on target computers running Mac OS X 10.5 or later.

Choosing the command opens the **Time Machine** dialog:



The dialog contains these elements:

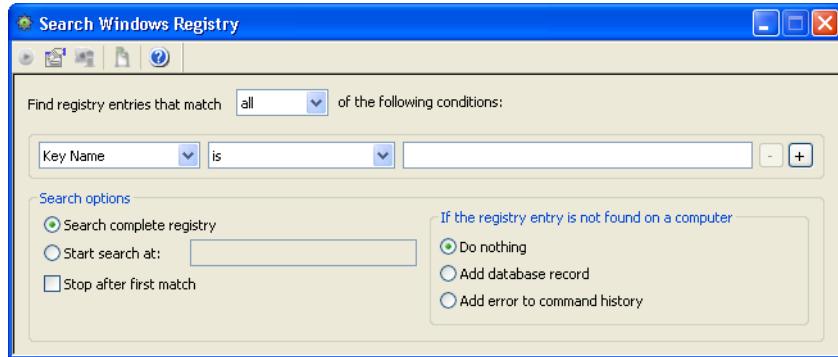
- **Action:** The action that you want Time Machine to perform.
 - **Start Backup Now:** The target computers immediately begin a Time Machine backup.
Note: This command has an effect only on target computers where a Time Machine disk has already been specified.
 - **Stop Running Backup:** Any Time Machine backups in progress on the target computers are immediately stopped.
 - **Enable Automatic Backup:** On all target computers, automatic Time Machine backups are enabled. (This has the same effect as sliding the master switch in the Time Machine control panel to **On**.)
Note: This command has an effect only on target computers where a Time Machine disk has already been specified.
 - **Disable Automatic Backup:** On all target computers, automatic Time Machine backups are disabled. (This has the same effect as sliding the master switch in the Time Machine control panel to **Off**.)

The toolbar of command windows is described in “Command window toolbar” on page 284.

Search Windows Registry

The **Search Windows Registry** command allows you search for keys and values in the registries of administered Windows computers.

Choosing the command opens the **Search Windows Registry** dialog:



The dialog contains these elements:

- **Find registry entries that match:** When **all** is chosen from this pop-up menu, registry entries are found that match all specified conditions (Boolean AND). If **any** is chosen, entries are found that match at least one of the specified conditions (Boolean OR).
- Condition area: The first pop-up menu lets you choose a condition to match registry entries. The second one contains the possible comparison operators. For most conditions, one or two text field lets you specify the value to compare entries against. The **+** and **-** buttons let you add new conditions or remove existing ones.
These search criteria are available:
 - **Key At:** Enter a full path of a key to check whether the key exists (or does not exist) on the target computers.
 - **Value At:** As **Key at**, but for values.
 - **String At:** Enter the full path of a string type value and compare it against a fixed value.
 - **Number At:** As **String at**, but for numbers.
 - **Binary At:** As **Binary at**, but for binary values.
 - **Key Path:** Search for keys by partial paths – all keys are found whose paths contain the search string. The keys' names are not considered part of their paths.
 - **Value Path:** As **Key Path**, but for values.
 - **Key Name:** Search for keys by their names.
 - **Value Name:** As **Key Name**, but for values.
 - **String Value:** Search for string values by their contents.
 - **Number Value:** As **String Value**, but for numbers.
 When you specify a path, you can include environment variables, as described in "Environment variables" on page 137.
- **Search complete registry:** The entire registries of the target computers are searched.

- **Start search at:** When this option is checked and a path in the registry is specified, only keys and values below that path are searched.
- **Stop after first match:** If a matching file has been found on a target computer, the search is stopped on that computer.
- **If the registry entry is not found on a computer:** Specify what Absolute Manage is to do when the registry search returns no hits on a particular target computer:
 - **Do nothing:** No particular action is taken; no entries from this computer appear in the **Registry Entries** window.
 - **Add database record:** A record is created in the Registry Entries database with a value of "No" in the **Registry Entry Found** information item.
 - **Add error to command history:** An error entry, stating that the key could not be found, is added to the **History** section of the **Commands** window.

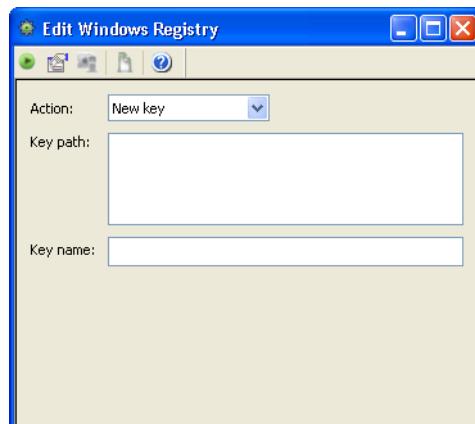
Any found registry entries are added to the Registry Entries database and displayed in the **Registry Entries** window.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Edit Windows Registry

The **Edit Windows Registry** command allows you add, edit or delete keys and values in the registries of administered Windows computers.

Choosing the command opens the **Edit Windows Registry** dialog



The dialog contains these elements:

- **Action:** This pop-up menu lets you specify the desired action that you want to perform in the target computers' registries. These actions are available:
 - **New Key:** Create a new key at a specified path.
 - **New Value:** Create a new value in a specified key.
 - **Change Value:** Alter a value at a specified location.
 - **Delete Key:** Delete a specified key and all its contents.

- **Delete Value:** Delete a specified value.
- **Rename Key:** Change the name of a specified key.
- **Rename Value:** Change the name of a specified value.

Additional elements let you enter key and value specifications and data. Which of them are visible depends on the chosen action. This is a list of all elements; only a subset is visible in each case:

- **Key path:** The path of an existing key in which a new key or value is to be created.
- **Key name:** The name of the new key that you want to create.
- **Value path:** The path of a value that is to be changed.
- **Value type:** The data type of a new value or of a value that is to be changed.
- **Value:** The new data of a value.
- **Path:** The path of a key or value that is to be deleted or renamed.
- **New name:** The new name of a key or value.

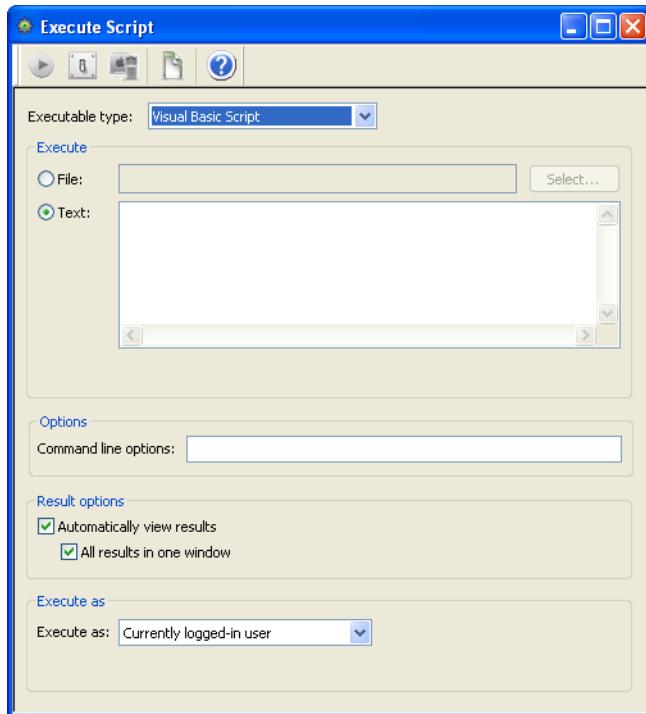
When you specify a path, you can include environment variables, as described in “Environment variables” on page 137.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Execute Script

The **Execute Script** command executes script files on the target computers.

Choosing the command opens the **Execute Script** dialog:



The dialog contains these elements:

- **Executable type:** The type of program that is to run on the clients to gather the information for the field:
 - Unix shell script (Mac OS X targets)
 - AppleScript (Mac OS X targets)
 - DOS batch file (Windows targets)
 - Visual Basic script (Windows targets)
 - PowerShell script (Windows targets)
 Depending on the choice made in this pop-up menu, different fields become available in the dialog pane.
- **File:** The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for all executable types.)
 Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to Absolute Manage Server.
- **Text:** The text of a script can be entered in this field. The entered script is executed on the target computers. (This option is available for all executable types.)
Note: Absolute Manage offers no syntax verification functions for these scripts; we strongly recommend that you test the scripts before entering them here.
- **Transfer all files in folder containing executable:** If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the

script is executed. (This option is available for all executable types.)

Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).

- **Command line options:** Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question). You can include environment variables in the options, as described in “Environment variables” on page 137.
- **Automatically view results:** If this option is checked, the results that the scripts return are automatically displayed in result windows on your computer. (By default, they are just entered in the command history.)
If **All results in one window** is checked, all returned script results are displayed together in a single window. Clicking a computer in the window’s upper half scrolls the lower half to that computer’s results.
If **All results in one window** is unchecked, a separate window is opened for each script result.
- **Executable requires administrative privileges:** If this option is checked, the specified script is executed with administrator privileges on the target computers. (This option is available for the **Unix Shell Script** executable type.)
- **Execute as:** This pop-up menu allows you to specify a user account on the target computers with the privileges of which the script is executed. (This option is available for the **Unix Shell Script**, **DOS Batch File**, **Visual Basic Script**, and **PowerShell** executable types.)

NOTE The result of the script execution, if any, can be displayed via the **Show Command Result** context menu command in the **Commands** window.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Execute Macintosh File

The **Execute Macintosh File** command runs applications from the administrator’s computer on target Mac OS X computers, providing special options for running installer applications.

These file types are supported:

- .pkg and .mpkg files for Apple’s Installer
- Installers based on MindVision’s InstallerVISE engine
- Other installers that contain the installer engine and all required installer files with a single application
- Other applications and AppleScript applets

- Shell scripts and other scripts (text files for which the executable bit is set and which begin with #!)

NOTE You cannot use this command to execute Mac OS files that include a resource fork.

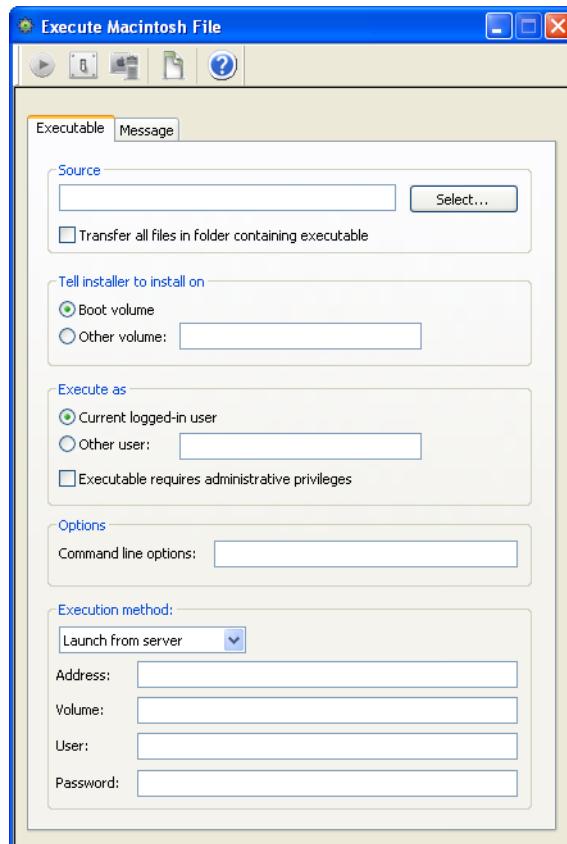
Choosing the command opens the **Execute Macintosh File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 284.

Executable

The **Executable** tab of the **Execute Macintosh File** dialog lets you specify the file to execute and the manner of its execution:



The tab contains these elements:

- **Source:** The file on your computer or on the server that is to be executed.
- **Browse:** Clicking this button opens a dialog in which the file to be executed can be selected.

- **Transfer all files in folder containing executable:** If this option is selected, Absolute Manage transfers not only the executable itself to the target computer but also any other files that are located in the same folder.
- **Tell installer to install on:** The volume where the installer is to install the software.
Note: Specifying a target volume may not be supported by all installers.
- **Execute as:** The user with whose privileges the application is to run.
- **Executable requires administrative privileges:** If this option is checked, the Agents run the script with system administrator privileges.
- **Command line options:** Any text entered in this field is passed as a parameter to the application.
You can include environment variables in the options, as described in “Environment variables” on page 137.
- **Execution method:** How the file is run from a server:
 - **Launch from server:** The specified server volume (see below) is mounted, the file executed, and the server volume unmounted.
 - **Launch using server URL:** The specified file (see URL, below) on a server is executed.
- **Address:** The IP address or DNS name of the server.
SMB server addresses must be prefixed by a double backslash, according to UNC notation.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain), if you use DNS names.
- **Volume:** The volume of the server on which the file is located.
- **User:** The username to use to connect to the server.
- **Password:** The password to use to connect to the server.
- **URL:** The URL of the server volume. The URL is made up of several elements, some of which are optional, in this order:
 - The protocol (`afp` or `smb`), followed by `://`
 - Optionally a username followed by `@`
 - Optionally for AFP servers `,AUTH=` and an authentication type (see below)
 - Optionally `:` and a password
 - The server’s IP address or DNS name
 - Optionally `,` and a port number
 - The path of the server volume to useThe following authentication methods are supported:
 - No User Authent
 - Cleartxt Passwrd
 - Random Exchange
 - 2-Way Random
 - DCAST128
 - DHX2
 - Client Krb v2
 - Microsoft V1.0

These are two sample URLs:

- `afp://username:userpass@server.company.com/volumename/`
- `afp://user:pass;AUTH=Cleartxt Passwrd@server.company.com/volumename/`

Note the space in the **AUTH** parameter in the second example.

Message

The **Message** tab of the **Execute Macintosh File** dialog lets you send a message to target computers before the file is executed. A black dot on the tab  indicates that a message has been specified, even when you select another tab.

The elements of this pane are described in “Send Message” on page 296.

If a **Cancel** button is added to the dialog, the file will not be executed on any target computer on which the user clicks **Cancel**.

Execute Windows File

The **Execute Windows File** command runs applications or .BAT files from the administrator’s computer on target Windows computers.

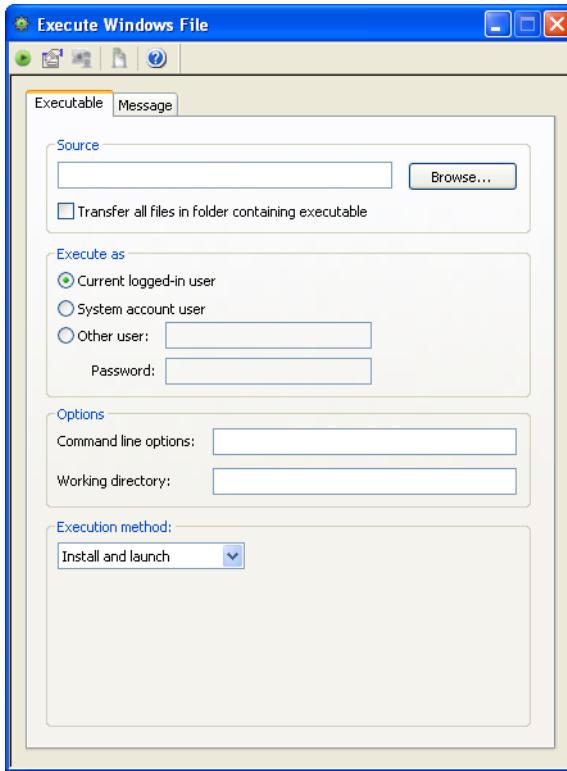
Choosing the command opens the **Execute Windows File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 284.

Executable

The **Executable** tab of the **Execute Windows File** dialog lets you specify the file to execute and the manner of its execution:



The tab contains these elements:

- **Source:** The file on your computer or on the server that is to be executed.
- **Browse:** Clicking this button opens a dialog in which the file to be executed can be selected.
- **Transfer all files in folder containing executable:** If this option is selected, Absolute Manage transfers not only the executable itself to the target computer but also any other files that are located in the same folder.
- **Execute as:** The user with whose privileges the application is to run.
- **Command line options:** The command line options with which the file is launched on the target computer. You can include environment variables in the options, as described in "Environment variables" on page 137.
Note: When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, Absolute Manage adds the /qn option (/quiet /norestart for MSU files) to run the installer silently.
- **Working directory:** The working directory for the file's execution on the target computers.
- **Execution method:** Whether the installer is copied to the target computers or run from a server:
 - **Install and launch:** The specified file is copied to the target computers and run there.

- **Launch from server:** The specified server volume (see below) is mounted, the file executed, and the server volume unmounted.
- **Launch using server URL:** The specified file (see URL, below) on a server is executed.
- **Address:** The IP address or DNS name of the server. SMB server addresses must be prefixed by a double backslash, according to UNC notation.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain), if you enter a DNS name.
- **Volume:** The volume of the server on which the file is located.
- **User:** The username to use to connect to the server. For Windows clients in networks with domains, the username must be specified as **domain\username**.
- **Password:** The password to use to connect to the server.
- **URL:** The URL of the server volume. The URL is made up of several elements, some of which are optional, in this order:
 - The protocol (`smb`), followed by `://`
 - Optionally a username followed by `@`
 - Optionally `:` and a password
 - The server's IP address or DNS name
 - Optionally, `:` and a port number
 - The path of the server volume to use

Message

The **Message** tab of the **Execute Windows File** dialog lets you send a message to target computers before the file is executed. A black dot on the tab  indicates that a message has been specified, even when you select another tab.

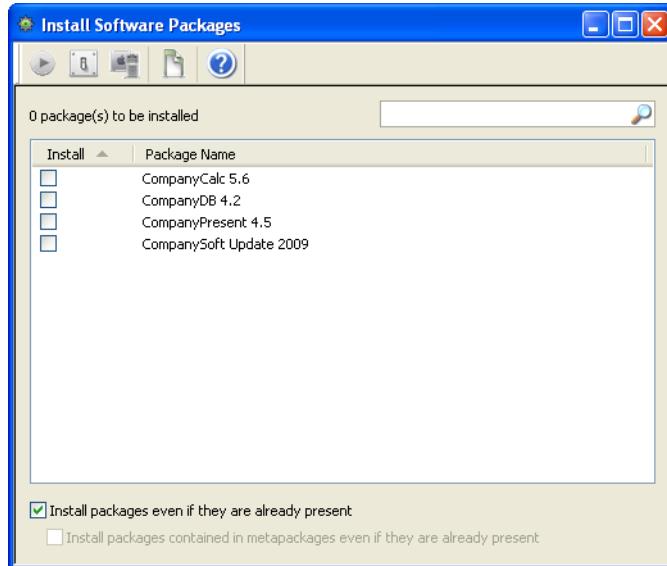
The elements of this pane are described in "Send Message" on page 296.

If a **Cancel** button is added to the dialog, the file will not be executed on any target computer on which the user clicks **Cancel**.

Install Software Packages

The **Install Software Packages** command lets you install a software package or metapackage on target computers without having to create a distribution group.

Choosing the command opens the **Install Software Packages File** dialog:



The dialog contains these elements:

- Search field: Enter part of the name of a software package here to restrict the display to packages with matching names.
- List of packages: Check all packages that you want to install.
- **Install packages even if they are already present**
If this option is checked, packages are installed on the target computers even if they are already present.
If the option is unchecked, the selected packages are installed only on those target computers that do not already have them.
- **Install packages contained in metapackages even if they are already present**
If this option is checked, all packages contained in selected metapackages are installed on the target computers even if they are already present.
If the option is unchecked, packages in the selected metapackages are installed only on those target computers that do not already have them.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Transfer File/Folder

The **Transfer File/Folder** command copies files or folders from your hard disk to those of target computers.

Choosing the command opens the **Transfer File/Folder File** dialog, which has three tabs:

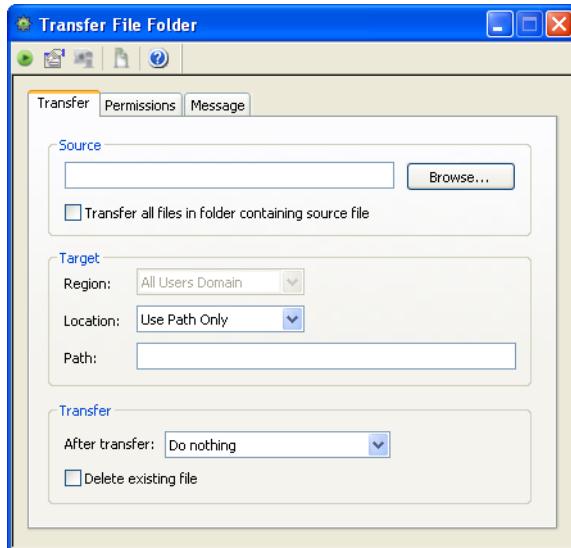
- **Transfer**
- **Permissions**

- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 284.

Transfer

The **Transfer** tab of the **Transfer File/Folder** dialog lets you specify the files or folders to be transferred from your computer:



The tab contains these elements:

- **Source:** The file or folder on your computer or on the server that is to be transferred.
- **Browse:** Clicking this button opens a dialog in which the file to be transferred can be selected.
To choose a folder, press the Shift key while clicking **Select**.
- **Transfer all files in folder containing source file:** If this option is selected, Absolute Manage transfers not only the selected file itself to the target computer but also any other files that are located in the same folder.
- **Transfer contents of disk image:** When a disk image has been selected as the source file, the **Transfer all files in folder containing source file** option becomes this option. Checking it makes Absolute Manage transfer not the disk image itself but its contents to the target computers' boot volumes. In this case, the **Target Region**, **Target Location**, and **Target Path** options are not available; the folder structure from the disk image is mirrored on the boot volumes.
- **Target Region:** The general domain where the files or folders are to be transferred to. The available regions are explained in “Copy File/Folder” on page 318.
- **Target Location:** The specific location within the target region where the files or folders are to be transferred to. The available locations are explained in “Copy File/Folder” on page 318.
- **Target Path:** The path of a folder within the specified target location where the files or folders are to be transferred to (optional).

When **Use Path Only** is chosen as the location, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (E.g., ~/Fonts for the user's fonts folder.) For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in "Environment variables" on page 137.

- **After Transfer:** What Absolute Manage is to do with a file or folder after having transferred it:
 - **Do nothing:** No action is taken beyond transferring the file or folder.
 - **Open file:** Open the file, same as using the **Open File** command (see "Open File" on page 325).
 - **Open file with admin privileges:** Open the file, same as using the **Open File** command. The file is opened with administrator privileges.
- **Delete existing file:** If this option is checked, a file at the target location with the same name as a transferred file or folder is replaced. If the option is unchecked, the transfer fails if a file with the same name already exists.

Permissions

The **Permissions** tab of the **Transfer File/Folder** dialog lets you specify the access permissions for the transferred on Mac OS X target computers:



The tab contains these elements:

- **Mac OS X Permissions:** The access permissions:
 - This permission is set for the transferred file or folder.
 - This permission is set to the same value for the transferred file or folder as for the source file on your computer.
 - This permission is not set for the transferred file or folder.

The permissions are displayed in standard BSD notation below the array for easy verification.
- **Unix owner:** When a file or folder is transferred to a Mac OS X target, its owner can be set. The owner can either be the owner of the parent folder on the target computer, the owner of the source file on your computer, or a specified user of the target computer.

- **Unix group:** When a file or folder is transferred to a Mac OS X target, its group can be set. The group can either be the group of the parent folder on the target computer, the group of the source file on your computer, or a specified group on the target computer.

Message

The **Message** tab of the **Transfer File/Folder** dialog lets you send a message to target computers before the files or folders are transferred. A black dot on the tab  indicates that a message has been specified, even when you select another tab.

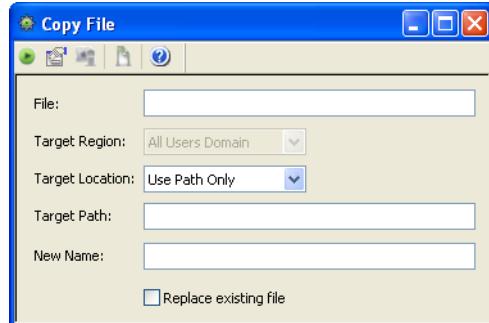
The elements of this pane are described in "Send Message" on page 296.

If a **Cancel** button is added to the dialog, the transfer will not take place to any target computer on which the user clicks **Cancel**.

Copy File/Folder

The **Copy File/Folder** command copies files or folders on the target computers to another location on the same computers.

Choosing the command opens the **Copy File** dialog:



The dialog contains these elements:

- **File:** The path of the file or folder that is to be copied. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
To specify a file or folder manually, enter the entire path, with slashes as path dividers for Mac OS X files and backslashes for Windows files.
For files on Windows targets, you can use environment variables, as described in "Environment variables" on page 137.
- **Target Region:** On Mac OS X target computers, the general domain to which the file or folder is to be copied. These target regions exist:
 - **System Domain:** /System and its subfolders
 - **All Users Domain:** /Library and its subfolders
 - **Current User Domain:** ~/ and its subfolders

- **Classic Domain:** The Mac OS 9 system folder or one of its subfolders. (Requires the Classic environment to be configured on the target computer.)
 - **Network Domain:** The network resources folder defined by NetInfo and its subfolders.
- On Windows targets, only some domains are recognized:
- **System Domain:** The operating system folder and its subfolders
 - **All Users Domain:** The **Users** folder (Vista and later) or **Documents and Settings** folder (XP and earlier) and their subfolders
 - **Current User Domain:** The current user's folder and its subfolders
- **Target Location:** The specific location within the target region where the file or folder will be copied.

Location	Mac OS X	Windows
Use Path Only	The target region is ignored and only the contents of the Target Path field is considered. (Using the contents as an absolute path.)	
Desktop	The desktop of the target computer.	
Top Level	The top level of the specified domain.	
Current User Folder	~/	Current user's folder (in Vista and later usually in Users , in XP and earlier usually in Documents and Settings)
Users	/Users	Users folder (Vista and later) or Documents and Settings folder (XP and earlier)
Applications	/Applications	Program Files folder
Documents	~/Documents	Current user's My Documents folder
Utilities	/Applications/Utilities	n/a
Library	Library folder in the target region.	n/a
Frameworks	Library/Frameworks folder in the target region.	n/a

Location	Mac OS X	Windows
Preferences	Library/ Preferences folder in the target region.	n/a
Preference Panes	Library/ PreferencePanes folder in the target region.	System directory for control panels (usually c:\windows \system32)
Kernel Extensions	Library/Extensions folder in the target region.	Active system folder (usually c:\windows \system32)
Fonts	Library/Fonts folder in the target region.	Windows fonts folder (usually c:\windows\fonts)
Scripting Additions	Library/Scripting- Additions folder in the target region.	n/a
Startup Items	Library/ StartupItems folder in the target region.	Startup program group
Applications Support	Library/Application Support folder in the target region.	Application Data folder
Contextual Menus	Library/Contextual Menu Items folder in the target region.	n/a

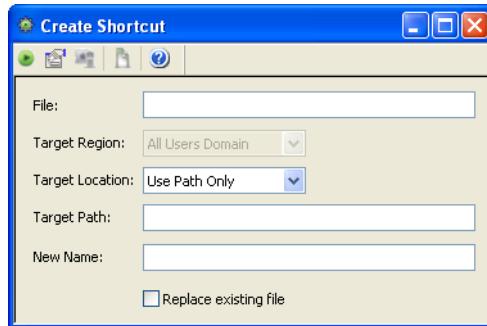
- **Target Path:** The path of a folder within the specified target location where the file or folder is to be copied (optional). When **Use Path Only** is chosen as the location, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (E.g., ~/Fonts for the user's fonts folder.) For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in "Environment variables" on page 137.
- **New Name:** A name for the copied file or folder that is different from the original (optional).
- **Replace existing file:** If this option is checked, a file with the same name as the copied file or folder at the target location is replaced. If the option is unchecked, the copying process fails if a file with the same name already exists.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Create Shortcut

The **Create Shortcut** command creates a shortcut of the selected files or folders on the target computers in a specified location on the same computers. (On Mac OS X targets, an alias is created.)

Choosing the command opens the **Create Shortcut** dialog:



The dialog contains these elements:

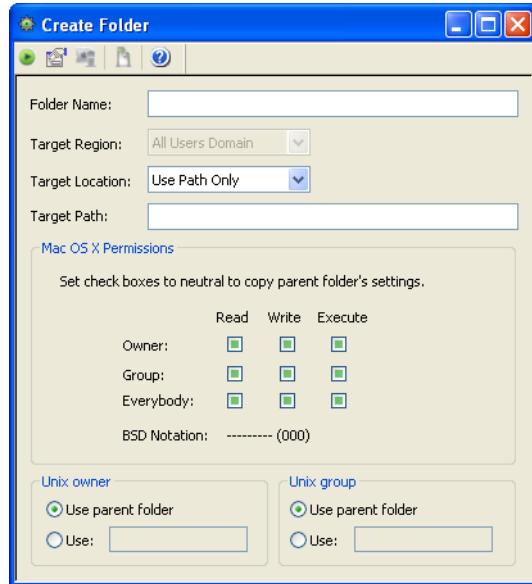
- **File:** The path of the file or folder from which a shortcut is to be created. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
To specify a file or folder manually, enter the entire path, with slashes as path dividers for Mac OS X files and backslashes for Windows files.
For Windows targets, you can use environment variables, as described in "Environment variables" on page 137.
- **Target Region:** The general domain where the shortcut is to be created. The available regions are explained in "Copy File/Folder" on page 318.
- **Target Location:** The specific location within the target region where the shortcut is to be created. The available locations are explained in "Copy File/Folder" on page 318.
- **Target Path:** The path of a folder within the specified target location where the shortcut is to be created (optional).
When **Use Path Only** is chosen as the location, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (E.g., ~/Fonts for the user's fonts folder.)
For Windows targets, you can use environment variables, as described in "Environment variables" on page 137.
- **New Name:** A name for the shortcut that is different from the default name (optional).
- **Replace existing file:** If this option is checked, a file with the same name as the shortcut at the target location is replaced. If the option is unchecked, the process fails if a file with the same name already exists.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Create Folder

The **Create Folder** command creates a folder on the target computers in a specified location.

Choosing the command opens the **Create Folder** dialog:



The dialog contains these elements:

- **Folder Name:** The desired name of the folder.
- **Target Region:** The general domain where the folder is to be created. The available regions are explained in “Copy File/Folder” on page 318.
- **Target Location:** The specific location within the target region where the folder is to be created. The available locations are explained in “Copy File/Folder” on page 318.
- **Target Path:** The path of a folder within the specified target location within which the folder is to be created (optional). Use slashes as path dividers for Mac OS X targets and backslashes for Windows targets.
Note: This is not the path of the folder that is to be created but the path of its parent folder.
When **Use Path Only** is chosen as the location, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (E.g., ~/Fonts for the user’s fonts folder.) For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in “Environment variables” on page 137.
- **Mac OS X Permissions:** When creating folders on Mac OS X target computers, you can specify its permissions:
 - This permission is set for the folder.
 - This permission is set to the same value for the folder as for the parent folder.
 - This permission is not set for the folder.

The permissions are displayed in standard BSD notation below the array for easy verification.

- **Unix owner:** When a folder is created on a Mac OS X target, its owner can be set. The owner can either be the owner of the parent folder or a specified user of the target computer.
- **Unix group:** When a folder is created on a Mac OS X target, its group can be set. The group can either be the group of the parent folder or a specified group on the target computer.

The toolbar of command windows is described in “Command window toolbar” on page 284.

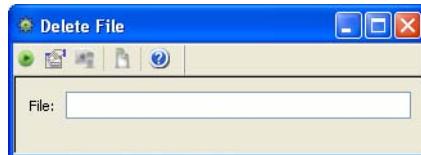
Delete File/Folder

The **Delete File/Folder** removes a file or folder from the target computers.

IMPORTANT

Once executed, this command is not reversible. The selected files and folders are not put into the trash but removed completely. They cannot be recovered, short of using specialized tools.

Choosing the command opens the **Delete File** dialog:



The dialog contains these elements:

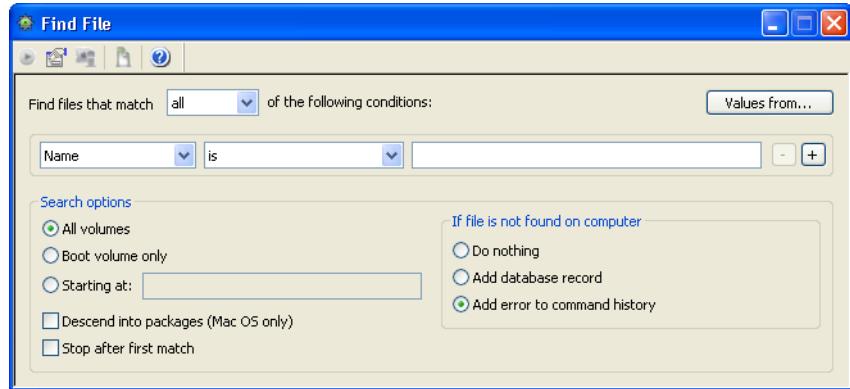
- **File:** The path of the file or folder that is to be deleted. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
To specify a file or folder manually, enter the entire path, with slashes as path dividers for Mac OS X files and backslashes for Windows files.
For Windows targets, you can use environment variables, as described in “Environment variables” on page 137.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Find File

The **Find File** command searches target computers for files and enters found files into the Files table of the Absolute Manage database.

Choosing the command opens the **Find File** dialog:



The dialog contains these elements:

- **Find files that match:** When **all** is chosen from this pop-up menu, files are found that match all specified conditions (Boolean AND). If **any** is chosen, files are found that match at least one of the specified conditions (Boolean OR).
- **Values from:** Clicking this button lets you select a file. All specified conditions are filled with the respective parameters from this file. If you later add new conditions, they initially also contain comparison values from this file.
- Condition area: The first pop-up menu lets you choose a condition to match files. The second one contains the possible comparison operators. For most conditions, a text field lets you specify the value to compare files against. The + and - buttons let you add new conditions or remove existing ones.
The parameters available for specifying conditions are described in “Files” on page 566, except for **Checksum** and **Path**:
 - **Checksum** lets you select files by their MD5 checksums, making sure that files are really the desired version, without alterations. Note that the checksum has to be calculated dynamically; doing so for a large number of files requires a huge amount of processing power on the client computer and should therefore be avoided. Always combine the **Checksum** criterion with other criteria that make sure that the checksum needs to be calculated only for a small number of files.
Checksums are not available for folders.
 - **Path** lets you select files and folders by their paths on the hard disk. It references the **File Path** information item. When this option is chosen, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (For example, ~/Documents for the user’s documents folder.)
For Windows targets, you can use the environment variables when this option is chosen, as described in “Environment variables” on page 137.
- **All volumes:** All volumes of the target computers are searched.

- **Boot volume only:** Only the boot volumes of the target computers are searched.
- **Starting at:** Only the directory specified in the text field and its subdirectories are searched.
You can use Mac OS X' ~/ notation for the user folder and Windows' environment variables as described above for the **Path** criterion.
- **Descend into packages:** If this option is checked, the contents of packages on Mac OS X target computers are included in the search. If it is unchecked, the packages are treated as files and their contents are not searched.
- **Stop after first match:** If a matching file has been found on a target computer, the search is stopped on that computer.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Move File/Folder

The **Move File/Folder** command moves files or folders on the target computers to another location on the same computers.

The command is similar in all respects to the **Copy File/Folder** command (see “Copy File/Folder” on page 318), except that files and folders are moved instead of copied.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Open File

The **Open File** command opens a file on the target computers. The effect is the same as if the file had been double-clicked locally.

The file to be opened must already be present on each target computer. (Compare “Transfer File/Folder” on page 315.)

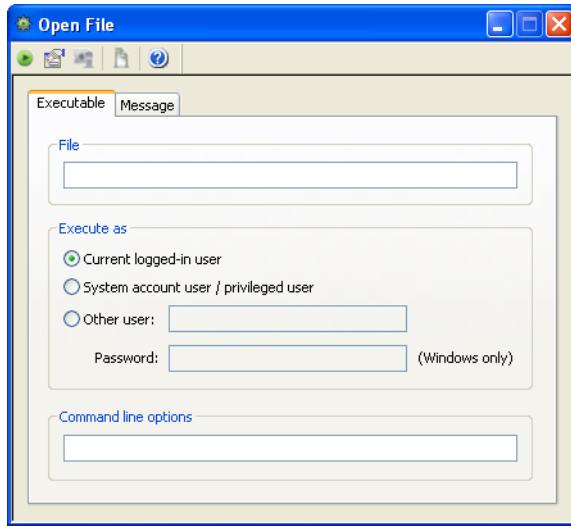
Choosing the command opens the **Open File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 284.

Executable

The **Executable** tab of the **Open File** dialog lets you specify the file to open:



The tab contains these elements:

- **File:** The location of the file on the target computers. If a file is selected in a browser window when you open this command, that file's location is pre-entered. If you select more than one file, only the number of files is shown.
On Windows targets, the PATH variable is automatically evaluated, allowing you to specify just the filename instead of the full path as long as the file is located in a directory that is included in PATH.
You can use other environment variables as well, as described in "Environment variables" on page 137.
- **Currently logged-in user:** The file is opened with the privileges of the current user of the target computer.
- **System account / privileged user:** The file is opened with the privileges of an administrator account.
- **Other user:** The file is opened as if executed by the specified user. For Windows target computers, the password of the user account must also be specified.
For Windows clients in networks with domains, the username must be specified as **domain\username**.
- **Command line options:** Any command-line options you specify here apply only if application files are opened.
You can include environment variables in the options, as described in "Environment variables" on page 137.

Message

The **Message** tab of the **Open File** dialog lets you send a message to target computers before the file is opened.

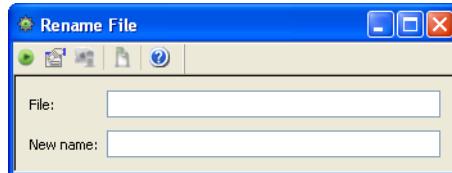
The elements of this pane are described in "Send Message" on page 296.

If a **Cancel** button is added to the dialog, the file will not be opened on any target computer on which the user clicks **Cancel**.

Rename File/Folder

The **Rename File/Folder** command changes the name of files or folders on target computers.

Choosing the command opens the **Rename File** dialog:



The dialog contains these elements:

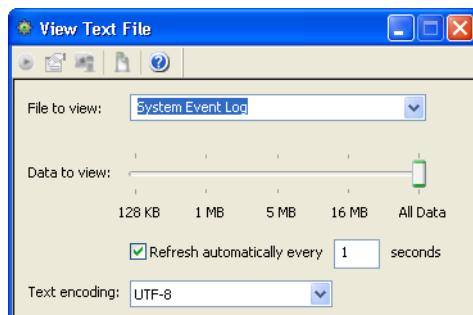
- **File:** The path of the file or folder that is to be deleted. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
To specify a file or folder manually, enter the entire path, with slashes as path dividers for Mac OS X files and backslashes for Windows files.
For Windows targets, you can use environment variables, as described in “Environment variables” on page 137.
- **New name:** The new name of the selected files or folders, without the path.

The toolbar of command windows is described in “Command window toolbar” on page 284.

View Text File

The **View Text File** command displays the contents of files on remote computers – either text files or system log files – on your monitor.

Choosing the command opens the **View Text File** dialog:



The dialog contains these elements:

- **File to view:** The file that you want to display. You specify the file in any of these ways:

- Enter the complete path of the file on the computer, including the file's name and extension (if any).
For Windows targets, you can use environment variables, as described in "Environment variables" on page 137.
When a file has been selected in an Absolute Manage browser window before the **View Text File** command is chosen, that file's path is pre-entered into the **File to view** field.
- Choose one of the predefined files from the pop-up menu.
- **Data to view:** Specify how much of the file's data Absolute Manage is to display.
You may not want to transmit very large files in their entirety across the network. In that case, you can limit the amount Absolute Manage displays (and thus has to transmit). Absolute Manage displays the amount of data you specify from the end of the file.
- **Refresh:** If this option is checked, Absolute Manage automatically continues to fetch the contents of the file in the specified interval.
Note: Fetching large files in short intervals can create significant network loads.
- **Text encoding:** The text encoding system used for the file.

Executing the command opens the specified file on all target computers. If more than one target computer was chosen, Absolute Manage Admin opens multiple windows, one for each target computer.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Gather Process Information

The **Gather Process Information** command makes Absolute Manage Server collect from all target computers information on currently running processes and enter it into the Processes table of its database.

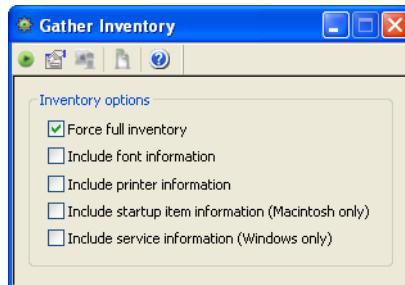
There are no options for this command; neither is there feedback after its execution.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Gather Inventory Information

The **Gather Inventory Information** command makes Absolute Manage Server collect from all target computers information on all of its hardware and software-related information items and enter it into the Computers table of its database.

Choosing the command opens the **Gather Inventory** dialog:



The dialog contains these elements:

- **Force full inventory:** If this option is checked, the server gets from the agents on the target computers all inventory information. If the option is unchecked, only information that has changed since the last transmission is transmitted to the server.
- **Include font information:** If this option is checked, font information is gathered from the target computers. If the option is unchecked, no font information is gathered.
- **Include printer information:** If this option is checked, information on printers is gathered from the target computers. If the option is unchecked, no printer information is gathered.
- **Include startup item information:** If this option is checked, information on startup items is gathered from the target Mac OS X computers. If the option is unchecked, no startup item information is gathered.
- **Include service information:** If this option is checked, information on active services is gathered from the target Windows computers. If the option is unchecked, no services information is gathered.

NOTE The information collected by this command is also collected automatically through regular inventory scans. Use this command when you would like to check the status on some computers immediately or more frequently than allowed for by the inventory push interval set through the **Agent Settings** command.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Gather Installed Software

The **Gather Installed Software** command makes Absolute Manage Server collect from all target computers information on the software installed on these computers and enter it into the Installed Software table of its database.

Choosing the command opens the **Gather Installed Software** dialog:



The dialog contains these elements:

- **Scan installer receipts:** If this option is checked, Absolute Manage scans target computers for installed software by looking for installer receipts. If it is unchecked, all installed software that was found through installer receipts is deleted from the Installed Software table in the Absolute Manage database.
- **Scan for missing operating system patches:** If this option is checked, Absolute Manage scans target computers for operating system patches that are present in the Software Distribution Center and would apply to the target computers but are not installed on them. (Patches that were rejected by an administrator are not considered to be missing.) The results can be viewed in the **Missing Operating System Patches** window.
- **Scan for application:** If this option is checked, Absolute Manage scans target computers for installed software by looking for applications in the specified locations and their subfolders.
 - **Applications folder:** the **Applications** folders (on Mac OS X targets) or the **Program Files** folders (on Windows targets; folder chosen according to the local environment variable settings)
 - **Boot volume:** the entire startup volume
 - **All local volumes:** all volumes currently mounted on the target computer, except server volumes

Note: Scanning entire hard disks can create a huge amount of data. We recommend scanning the boot volume or all local volumes only when really required.

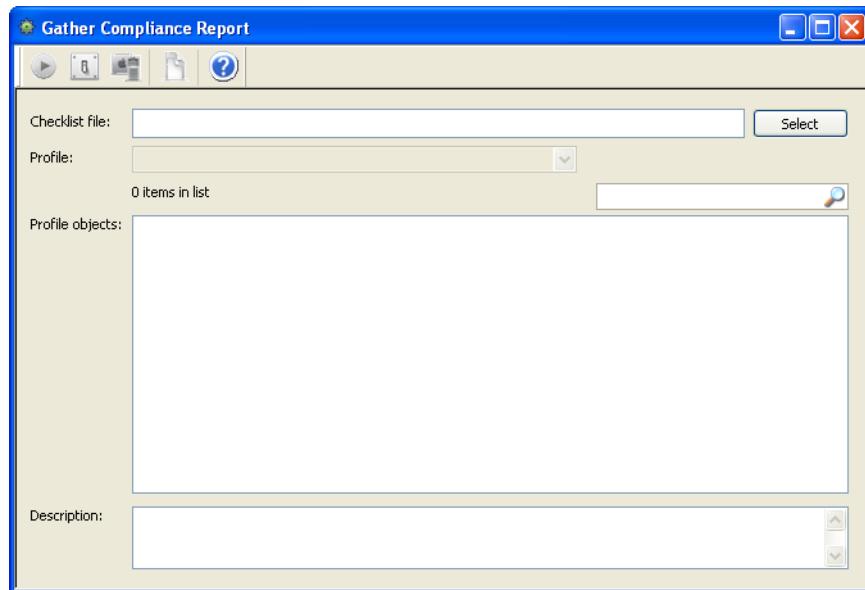
If the **Scan for application** option is unchecked, all installed software that was found through searching the application folders is deleted from the Installed Software table in the Absolute Manage database.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Gather Compliance Report

The **Gather Compliance Report** command makes Absolute Manage Server collect from all Windows target computers information required for FCCP SCAP compliance reports on these computers and enter it into the Compliance Report table of its database.

Choosing the command opens the **Gather Compliance Report** dialog:



The dialog contains these elements:

- **Checklist file:** This is the USGCB file containing the report parameters, an XML file the name of which usually contains "xccdf". Clicking the **Select** button lets you choose a file from your hard disk.
- **Profile:** This pop-up menu lets you choose the desired profile from the profiles contained in the chosen file.
- **Profile Objects:** This list contains the individual options contained in the chosen profile. You can switch them off and on individually. Using the context menu commands, you can also switch on or off multiple selected items together.
Description: The description of the selected object.

The toolbar of command windows is described in "Command window toolbar" on page 284.

Run Software Distribution Check

The **Run Software Distribution Check** causes Absolute Manage Server to check the status of software distribution on the selected target computers. There are no options for this command.

NOTE This check also happens automatically in regular intervals. Use this command when you would like the status to be checked immediately on some computers or more frequently than allowed for by the package check interval set through the **Agent Settings** command.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Run License Monitoring Scan

The **Run License Monitoring Check** causes Absolute Manage Server to check for licensed software on the selected target computers. There are no command-specific options.

NOTE The information collected by this command is also collected automatically through regular license monitoring scans. Use this command when you would like to check the status on some computers immediately or more frequently than allowed for by the license monitoring scan interval set through the **Agent Settings** command.

The toolbar of command windows is described in “Command window toolbar” on page 284.

Execute Command

The **Execute Command** command executes the command in the frontmost window with the current settings. The effect is the same as clicking the **Execute** button.

Execute Command is available only if a command window is the frontmost window.

Command Options

The **Command Options** command lets you change the options for a command.

Command Options is available only if the **Commands** window or a command window is the frontmost window.

Choosing the command opens the **Command Options** dialog described in “Options” on page 285.

Execute Command Now

The **Execute Command Now** command executes the selected command immediately, overriding its scheduling options. A confirmation alert is displayed before the actual execution takes place.

Execute Command Now is available only if the **Commands** window is the frontmost window and a queued (i.e, scheduled or deferred) command is selected.

Edit Command

The **Edit Command** command lets you change the settings for a command in the command queue.

Edit Command is available only if the **Commands** window is the frontmost window and a queued (i.e, scheduled or deferred) command is selected.

Choosing **Edit Command** displays a message asking you to choose between editing the command setting only for the selected target or for all targets for which the command was originally given.

When you have made your choice, the original command dialog will be opened, displaying the current settings. The target list contains all or one of the original targets, as per your choice.

After you have modified the command settings as desired, clicking the **Execute** button executes the command or re-enters it into the command queue in its edited form, depending on the scheduling options you have specified.

Reapply Command

The **Reapply Command** command lets you execute a command again that has already been executed, successfully or failing. You can change the command settings before re-executing the command.

Reapply Command is available only if the **Commands** window is the frontmost window.

Using **Reapply Command** is similar to using **Edit Command**, described above.

Show/Hide Target List

The **Show/Hide Target List** command toggles the target list of a command between visible and hidden. Choosing the command has the same effect as clicking the **Targets** button in a command window.

The target list is explained in “Command window toolbar” on page 284.

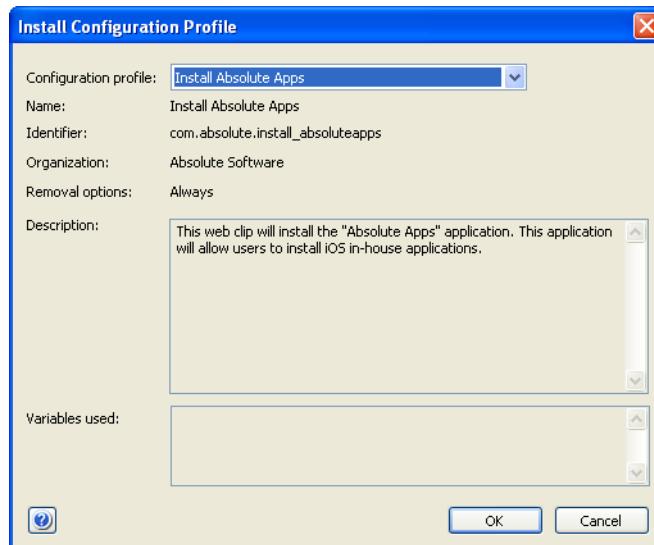
Show/Hide Target List is available only if a command window is the frontmost window.

Install Configuration Profile

Choosing this command displays the **Install Configuration Profile** dialog in which you can choose a configuration profile file to install on the selected devices.

The effect of the command is slightly different depending on the platform of the selected devices (configuration profiles are not supported for Android devices):

- For iOS devices, the profile is added to the profiles already installed on the device (if any).
- For Windows Phone devices, the selected profile replaces the current EAS policy on the device.



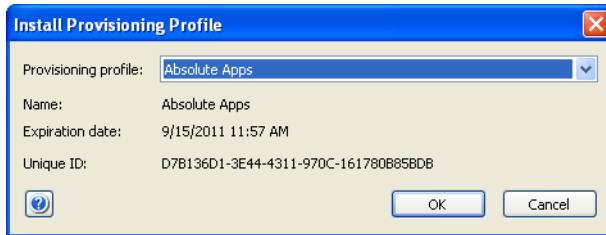
The dialog contains these elements:

- **Configuration profile:** The configuration profile you want to install. The pop-up menu contains all profiles that are available in Absolute Manage. You can choose **Other** from this menu to open a configuration profile file that has not yet been imported into Absolute Manage.

- **Name:** The name of the profile.
- **Identifier:** The identifier of the profile.
- **Organization:** The organization of the profile.
- **Removal options:** Whether the local user of the mobile device can remove the profile and whether a passcode is required for doing so.
- **Description:** A description of the profile. This description is displayed to the user of the managed mobile device. You can edit it before assigning the profile.

Install Provisioning Profile

Choosing this command displays the **Install Provisioning Profile** dialog in which you can choose a provisioning profile file to install on the selected iOS devices. (Provisioning profiles are not supported for Android and Windows Phone devices.)



The dialog contains these elements:

- **Provisioning profile:** The provisioning profile you want to install. The pop-up menu contains all profiles that are available in Absolute Manage. You can choose **Other** from this menu to open a provisioning profile file that has not yet been imported into Absolute Manage.
- **Name:** The name of the profile.
- **Expiration date:** The date on which the provisioning profile becomes invalid.
- **Unique ID:** The globally unique identifier for the profile.

Install Application

Choosing this command displays the **Install Application** dialog in which you can choose an in-house or recommended app to install on

the selected iOS or Android devices. (Installing applications on Windows Phone devices is not supported.)



The dialog contains these elements:

- **Application:** The in-house app you want to install. The pop-up menu contains all apps for the operating system of the selected devices that are available in Absolute Manage.
- **Bundle identifier:** The bundle identifier of the chosen application.
- **Version:** The version of the chosen application.
- **Build number:** The build number of the chosen application.
- **Minimum OS version:** The minimum version of the mobile OS required by the chosen application.
- **Supported devices:** The types of device on which the app can be used.
This information is displayed only for iOS devices.
- **Short description:** The short description of the application that it was given when it was imported into Absolute Manage.
- **Long description:** The long description of the application that it was given when it was imported into Absolute Manage. You can edit this description before installing the app.

Clicking **OK** in this dialog transfers the app to the selected mobile devices upon the next contact and presents their users with a prompt to install the app. If a user declines, the app is not installed on that device.

Note that you cannot install an application on an iOS device that already contains an unmanaged version of the application. (Unmanaged applications are all applications that have been installed by other means than through the MDM system.)

Issue Device Lock

Choosing this command locks the selected devices as if they had been switched off. Unlocking them requires entering the passcode locally (assuming that a passcode has been set on the device).

The device is locked as soon as it next contacts the mobile OS vendor's notification server.

A confirmation dialog is displayed before the command is executed. If any of the devices does not currently have a passcode, you are prompted to provide a passcode for it:

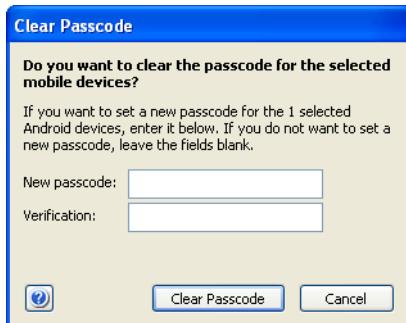


This command does not apply to Windows Phone devices.

Issue Clear Passcode

Choosing this command removes any passcode on the device so that it can be accessed without authentication and optionally lets you set a new passcode.

Choosing the command opens the **Clear Passcode** dialog:



The dialog contains these elements:

- **New passcode:** The new passcode that you want to set on the device after clearing the current one. Leave this field empty to not specify a new passcode.
Setting a new passcode is possible only on Android devices.
- **Verification:** Repeat the passcode to guard against typos.

Clicking **Clear Passcode** removes the passcode as soon as the device next contacts the mobile OS vendor's notification server. The new passcode, if any, depends on several factors:

- If you have specified a new passcode, that new passcode is set on the device.

- If the configuration profile on the device specifies that a passcode is required, the user immediately has to create a new passcode.
- If neither is the case, the device is left without a passcode.

This command does not apply to Windows Phone devices.

Issue Remote Erase

Choosing this command erases all information on the selected mobile devices and returns them to their factory settings.

A confirmation dialog is displayed before the command is executed. For devices with SD cards, it gives you the choice of erasing just the internal storage or the SD card as well.

The device is erased as soon as it next contacts the mobile OS vendor's notification server.

IMPORTANT

Note that this action is not reversible and that the erased information cannot be recovered from the mobile device (although recovering the data from a backup, should one exist, might be possible). Erasing devices without the consent of their users may expose you to legal liability.

Also, the erased device can no longer be administered through Absolute Manage until it has been enrolled again.

Set Roaming Options

Choosing this command opens the **Set Roaming Options** dialog in which you can activate and deactivate voice and data roaming for selected mobile devices:



The dialog contains these elements:

- **Enable voice roaming:** If this option is checked, voice roaming will be enabled on the mobile device. If it is unchecked, voice roaming will be disabled. (If it is in the third state, no change will be made.)
Note that some mobile communications companies prevent access to this setting. If that is the case for the selected devices, this option is disabled.

- **Enable data roaming:** If this option is checked, data roaming will be enabled on the mobile devices. If it is unchecked, voice roaming will be disabled. (If it is in the third state, no change will be made.)

Note that local users of the mobile devices will still be able to change the settings you make in this dialog.

Roaming options can only be set for iOS devices running iOS 5 or newer.

Send Message to Device

Choosing this command lets you send a message to all selected mobile devices, provided that the AbsoluteApps application is installed on them. (This command does not support Windows Phone devices.)

The message is sent as soon as the device next contacts the mobile OS vendor's notification server.

Update Device Info

Choosing this command queries the device and updates the information about it in the Absolute Manage database.

Track Device

This command lets you enable and disable geotracking for mobile devices and set tracking details. It is not available when multiple devices are selected. (This command does not support Windows Phone devices.)

IMPORTANT

Because the location of a mobile device often is also the location of its user, tracking mobile devices is governed by privacy or data protection laws in many jurisdictions.

Usually, the express consent of the user of the device is required before it may be tracked. In addition, there may be regulations governing how long gathered data may be stored and how and by whom it may be accessed.

Failure to obtain the required consent or observe other applicable legal regulations may expose you to civil and/or criminal liability.

NOTE

For information on geotracking iOS devices, please contact Absolute Support.

Choosing the command opens the **Mobile Device Tracking** dialog:



The dialog contains these elements:

- **Track device:** Checking this option enables tracking of the selected device, unchecking it disables it.
Note that tracking can be enabled only for devices on which AbsoluteApps is installed. Deploying AbsoluteApps is described in “Preparing iOS devices for software installation” on page 155.
- **Activation passphrase:** The pin needed to access the selected mobile device.
This pin is specified when AbsoluteApps is launched for the first time on a mobile device or centrally after the deployment of AbsoluteApps. See “Setting passphrases for mobile devices” on page 183 for details.
- **Tracking interval:** The interval in which a location record for the device is recorded.
If the device has no contact with the MDM server at the scheduled time, it caches its locations and transmits it when it next has contact.
If a device has no location information at the scheduled time, e.g., because it has no GPS contact and is not in range of a known WiFi network, no location record is created.
Specifying short tracking intervals can lead to very large numbers of tracking records and should therefore be carefully considered. For example, tracking 50 devices with an interval of five minutes creates more than five million records per year.
- **Location accuracy:** The maximum accuracy with which the device position is recorded.
Lower accuracies mean that a device cannot be located as precisely but better preserves the privacy of the user.

If the Alt key is pressed while choosing the **Track Device** command, a slightly different version of the dialog is displayed that allows you to enable geotracking on a device for which you do not have the passphrase. See “Dealing with lost passphrases” on page 187 for details.

For more information on geotracking, see “Geotracking mobile devices” on page 182.

Get Device Geolocation

This command queries the selected device for its current location and enters it in the Absolute Manage database. (This command does not support Windows Phone devices.)

If geotracking is not currently activated on the device, you must enter the activation passphrase. You can query the locations of devices only if AbsoluteApps is installed on them.

For more information on geotracking, see “Geotracking mobile devices” on page 182.

Reset Tracking Passphrase

Choosing this command removes the current passphrase from the selected mobile device. (This command does not support Windows Phone devices.)

When you choose this command, a confirmation dialog is displayed. Confirming your command removes the passphrase currently in effect on the mobile device and requires a new passphrase to be set (either locally or remotely) before AbsoluteApps can be used again on the device.

See “Setting passphrases for mobile devices” on page 183 for details.

Chapter 14

Server menu

The **Server** menu contains commands that let you configure the Absolute Manage Server's settings and exchange information with it.

All commands affect only the server where you are currently logged in.

- **Synchronize All Tables** (page 342)
- **Reload All Tables** (page 342)
- **Synchronize Selected Records** (page 343)
- **Reload Selected Records** (page 343)
- **Save Distribution and Licensing Info** (page 343)
- **Read Distribution and Licensing Info** (page 343)
- **Save Administrator Info** (page 344)
- **Read Administrator Info** (page 344)
- **Save Custom Information Fields** (page 344)
- **Restore Custom Information Fields** (page 344)
- **Synchronize Custom Information Fields** (page 344)
- **Save Server Settings** (page 345)
- **Restore Server Settings** (page 345)
- **Synchronize Server Settings** (page 345)
- **Save All Settings** (page 345)
- **Restore All Settings** (page 345)
- **Create Placeholder Computer Records** (page 346)
- **Change Server Registration** (page 347)

Synchronize All Tables

The **Synchronize All Tables** command downloads all updated information from the server to which you are connected.

Choosing the command prompts the server to send all information that the local copies of the database tables do not yet contain or contain in an outdated form.

This command makes sure that your copy of Absolute Manage Admin has access to up-to-date information.

Reload All Tables

The **Reload All Tables** command downloads all information from the server to which you are connected.

Choosing the command prompts the server to send all information in the database tables, irrespective of whether it is already present in the local copies of the tables.

This command makes sure that the tables in your copy of Absolute Manage Admin contain the same information as the tables in the Absolute Manage Server database, even if they previously have been out of sync.

Synchronize Selected Records

The **Synchronize Selected Records** command downloads updated information for the selected computers from the server to which you are connected.

Choosing the command prompts the server to send all information on the selected records that the local copies of the database tables do not yet contain or contain in an outdated form.

This command makes sure that the information that is displayed in the selected records is up to date.

Reload Selected Records

The **Reload Selected Records** command downloads all information for the selected records from the server to which you are connected.

Choosing the command prompts the server to send all information on the selected computers that is contained in the database tables, irrespective of whether it is already present in the local copies of the tables.

This command makes sure that the records in your copy of Absolute Manage Admin contain the same information as the records in the Absolute Manage Server database, even if they previously have been out of sync.

Save Distribution and Licensing Info

The **Save Distribution and Licensing Info** command writes the current settings for license monitoring and software distribution to the Absolute Manage Server to which you are connected.

Choosing the command updates the information on groups, packages, licenses, and distribution points on the Absolute Manage Server to include any changes you have made locally.

Read Distribution and Licensing Info

The **Read Distribution and Licensing Info** command downloads the current settings for license monitoring and software distribution from the Absolute Manage Server to which you are connected.

Choosing the command updates the local information on groups, packages, licenses, and distribution points to be identical to that on the Absolute Manage Server.

Save Administrator Info

The **Save Administrator Info** command writes the current administrator account settings to the Absolute Manage Server to which you are connected.

Choosing the command updates the information on administrator accounts on the Absolute Manage Server to include any changes you have made locally.

Read Administrator Info

The **Read Administrator Info** command downloads the current administrator account settings from the Absolute Manage Server to which you are connected.

Choosing the command updates the local information on administrator accounts to be identical to that on the Absolute Manage Server.

Save Custom Information Fields

The **Save Custom Information Fields** command writes the current custom information field definitions to the Absolute Manage Server to which you are connected.

Choosing the command updates the information on custom information fields on the Absolute Manage Server to include any changes you have made locally.

Restore Custom Information Fields

The **Restore Custom Information Fields** command downloads the current information field definitions from the Absolute Manage Server to which you are connected.

Choosing the command updates the local information on custom information fields to be identical to that on the Absolute Manage Server.

Synchronize Custom Information Fields

The **Synchronize Custom Information Fields** command synchronizes the current custom information field definitions on your local computer with that of the Absolute Manage Server to which you are connected. If there are conflicts, a message informs you of the fact.

Choosing the command updates the information on custom information fields on the Absolute Manage Server to include any changes you have made locally.

Save Server Settings

The **Save Server Settings** command writes the current server settings to the Absolute Manage Server to which you are connected.

Choosing the command updates the server settings on the Absolute Manage Server to include any changes you have made locally.

Restore Server Settings

The **Restore Server Settings** command downloads the current server settings from the Absolute Manage Server to which you are connected.

Choosing the command updates the local information on settings to be identical to that on the Absolute Manage Server.

Synchronize Server Settings

The **Synchronize Server Settings** command synchronizes the current server settings on your local computer with that of the Absolute Manage Server to which you are connected. If there are conflicts, a message informs you of the fact.

Choosing the command updates the server settings on the Absolute Manage Server to include any changes you have made locally.

Save All Settings

The **Save All Settings** command writes all current settings from the Server Center to the Absolute Manage Server to which you are connected.

Choosing the command updates the settings on the Absolute Manage Server to include any changes you have made locally. It is the equivalent of choosing all of these commands individually:

- **Save Distribution and Licensing Info**
- **Save Administrator Info**
- **Save Custom Information Fields**
- **Save Server Settings**

Restore All Settings

The **Restore All Settings** command downloads all current settings for the Server Center from the Absolute Manage Server to which you are connected.

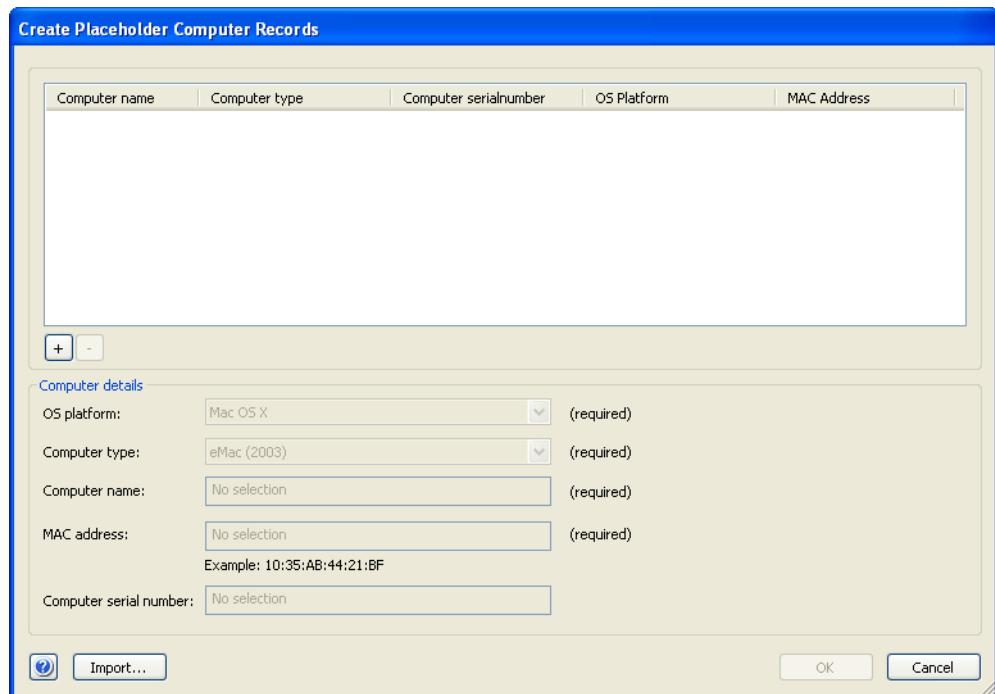
Choosing the command updates the local information in the Server Center to be identical to that on the Absolute Manage Server. It is the equivalent of choosing all of these commands individually:

- **Read Distribution and Licensing Info**
- **Read Administrator Info**
- **Restore Custom Information Fields**
- **Restore Server Settings**

Create Placeholder Computer Records

The **Create Placeholder Computer Records** lets you create dummy records for use in reinstalling Windows computers on which no Absolute Manage Agent is yet installed.

Choosing the command opens the **Create Placeholder Computer Records** dialog:



The dialog contains these elements:

- The list at the top contains all custom computer records that you have specified since opening the dialog. The list does not contain records that you have specified in earlier uses of this dialog.
- The + button lets you create a new record. Clicking the button creates a new entry in the list and activates the entry fields below the list.
- Clicking the - button deletes the currently selected records from the list.

- **OS platform:** The flavor of operating system used on the computer. This information appears in the **OS Platform** column of browser windows.
- **Computer type:** The make of the computer that is being specified. This information appears in the **Computer Type** column of browser windows.
- **Computer name:** A descriptive name for the computer. This information appears in the **Agent Name** column of browser windows.
- **MAC address:** The MAC address of the network interface of the specified computer. This information appears in the **Primary MAC Address** column of browser windows.
- **Computer serial number:** The serial number of the computer. This information is optional; if provided, it appears in the **Computer Serial Number** column of browser windows.
- **Import:** Clicking this button displays a standard Open dialog in which you can select a tab-delimited text file that contains the information for the placeholder records you want to create. The file must contain one line for each record, with this information (in this order, separated by tabs):
 - OS platform: "Mac OS X" or "Windows"
 - Computer type: The type as displayed in the Computer Type information item
 - Computer name: The name as displayed in the Computer Name information item
 - MAC address: The MAC address of the computer' main network interface
 - Computer serial number: The serial number as displayed in the Computer Serial Number information item. This information is optional.
- **OK:** Clicking the **OK** button creates dummy computer records in the Absolute Manage database. These records appear in browser windows but can be used only as targets for the **Reinstall Windows Computer** command.

Change Server Registration

The **Change Server Registration** command opens the **Registration** dialog that lets you change the registration specifications for the server, e.g., to increase the number of users:



The dialog contains these fields::

- **Name:** Your name.
- **Company:** The name of your company.
- **Serial number:** The serial number of your copy of Absolute Manage.
- **Activation key:** The Absolute Manage activation key that you have received.
- **Demo:** Clicking this button starts Absolute Manage Server in demo mode. In demo mode, Absolute Manage can be used for 45 days to administer up to ten computers and up to ten mobile devices.

Note: The demo mode is only available when the server has not yet been registered.

NOTE The **Change Server Registration** command can be used only by administrators with the **Change Server Settings** right. See “New Administrator” on page 481 for details.

The **Window** menu contains commands related to working with windows. There are commands for arranging windows, commands to open a range of predefined windows, and commands for opening user-created windows:

- **Cascade** (page 349)
- **Tile Horizontally** (page 349)
- **Tile Vertically** (page 350)
- **Computers** (page 350)
- **Files** (page 350)
- **Fonts** (page 350)
- **Processes** (page 350)
- **Installed Software** (page 351)
- **Missing Operating System Patches** (page 353)
- **Registry Entries** (page 354)
- **Compliance Reports** (page 355)
- **Power Usage Reports** (page 355)
- **Mobile Devices** (page 358)
- **Server Center** (page 358)
- **Agent Deployment Center** (page 359)
- **Commands** (page 359)
- **Command Templates** (page 360)
- **Window Reinstallation Tasks** (page 361)
- **Information Items** (page 362)
- **User windows** (page 362)

The frontmost window is indicated by a checkmark .

Cascade

The **Cascade** command rearranges the open windows, making them all the same size and staggering them across the screen.

Tile Horizontally

The **Tile Horizontally** command rearranges the open windows, making them all the same size and putting them row-like on top of each other so that together they cover the entire screen.

Horizontally tiled windows are the width of the screen, unless there are so many that tiling them all on top of each other would make them too low. In that case, they are tiled in multiple columns.

Tile Vertically

The **Tile Vertically** command rearranges the open windows, making them all the same size and putting them column-like beside each other so that together they cover the entire screen.

Vertically tiled windows are the height of the screen, unless there are so many that tiling them all beside each other would make them too narrow. In that case, they are tiled in multiple rows.

Computers

The **Computers** command opens the **Computers** window.

The **Computers** window is a predefined browser window that displays the contents of the Computers table of the Absolute Manage database, i.e., all administered client computers.

Browser windows are described in “Browser windows” on page 365. The columns in the **Computers** window are described in “Information items” on page 534.

Files

The **Files** command opens the **Files** window.

The **Files** window is a predefined browser window that displays the contents of the Files table of the Absolute Manage database, i.e., all files that have been searched for on client computers.

Browser windows are described in “Browser windows” on page 365. The columns in the **Files** window are described in “Files” on page 566.

Fonts

The **Fonts** command opens the **Fonts** window.

The **Fonts** window is a predefined browser window that displays the contents of the Fonts table of the Absolute Manage database, i.e., all fonts that have been found to be installed on client computers.

Browser windows are described in “Browser windows” on page 365. The columns in the **Fonts** window are described in “Fonts” on page 561.

Processes

The **Processes** command opens the **Processes** window.

The **Processes** window is a predefined browser window that displays the contents of the Processes table of the Absolute Manage database, i.e., all processes that have been found to be running on client computers.

Browser windows are described in “Browser windows” on page 365. The columns in the **Processes** window are described in “Processes” on page 565.

Installed Software

The **Installed Software** command opens the **Installed Software** window.

The **Installed Software** window is a predefined browser window that displays the contents of the Installed Software table of the Absolute Manage database, i.e., all software that has been found to be installed on client computers by means of the **Gather Installed Software** command described on page 329.

NOTE The **Gather Installed Software** command may not find all software on client computers. Software outside the Applications or Program Files folders the installation of which has not generated an installer receipt is not listed in this window.

Browser windows are described in “Browser windows” on page 365. The columns in the **Processes** window are described in “Processes” on page 565.

The **Installed Software** window contains some additional groups and context menu items that are not present in standard browser windows. These are described below.

Groups

There are a number of predefined smart groups in the **Installed Software** window:

- **Mac Software:** All installed software – both installer receipts and the contents of the **Applications** folder – that has been found on Mac OS X clients.
- **Mac Installer Receipts:** Installed software that has been found on Mac OS X clients by checking installer receipts.
- **Mac Applications:** Installed software that has been found on Mac OS X clients by searching the specified folders on client computers.
- **Apple Software:** Software from Apple Computer, Inc., that has been found on Mac OS X clients.
- **Non-Apple Software:** Software that has been found on Mac OS X clients and that has not been created by Apple Computer, Inc.
- **PC Software:** All installed software – both installer receipts and the contents of the **Program Files** folder – that has been found on Windows clients.

- **PC Installer Receipts:** Installed software that has been found on Windows clients by checking installer receipts.
- **PC Applications:** Installed software that has been found on Windows clients by searching the specified folders on client computers.
- **PC Hotfixes:** Any installed patches from Microsoft were found on client computers and are marked as hotfixes.
- **Mac Installer Receipt Statistics:** Summary information on the kinds and numbers of all installed software that has been found on client Mac OS X computers by scanning installer receipts.
- **Mac Application Statistics:** Summary information on the kinds and numbers of all installed software that has been found on client Mac OS X computers by searching the **Applications** folders.
- **PC Installer Receipt Statistics:** Summary information on the kinds and numbers of all installed software that has been found on client Windows computers by scanning installer receipts.
- **PC Application Statistics:** Summary information on the kinds and numbers of all installed software that has been found on client Windows computers by searching the **Program Files** folders.

Context menu commands

In addition to some commands found in other browser windows, the context menu of the **Installed Software** window contains some unique commands:

- **New Smart Group: Installed Software:** This command opens a dialog in which you can define a new smart group for the contents of the Installed Software table (i.e., the contents of the **Installed Software** window).
- **New Smart Group: Installed Software Statistics:** This command opens a dialog in which you can define a new smart group for statistics information on installed software.
- **New Smart Group: Computers by Installed Software:** This command opens a dialog in which you can define a new smart group for computers based on software that is installed on it or software that is not installed on it.

You can choose:

- Whether to list computers that match some or all of the specified software
- Whether to list computers that have or do not have the software
- Which method to use to decide whether the software is installed

Smart groups defined by this command list only computers running the operating system family specified by the matching method. For example, if you specify software matching by PC installer receipt, the resulting group contains only Windows client computers. Even if the group contains computers

missing the specified software, Mac OS X client computers – who by definition miss the specified software – are not listed.

NOTE Creating smart groups is described in “Creating a smart group” on page 111.

Missing Operating System Patches

The **Missing Operating System Patches** command opens the **Missing Operating System Patches** window.

The **Missing Operating System Patches** window is a predefined browser window that displays patches that are known to Absolute Manage but are not installed on applicable computers.

The data displayed in this window is collected using the **Gather Installed Software** command.

NOTE Patches that were rejected by an administrator are not considered to be missing patches. Furthermore, only client computers that are part of the automated patch management are considered.

The **Missing Operating System Patches** window has slightly different predefined smart groups and context menu than other browser windows, as described below.

Predefined smart groups

The **Missing Operating System Patches** window contains four default smart groups:

- **Missing Mac OS Patches:** Patches missing on Mac OS X computers.
- **Missing Microsoft Patches:** Patches missing on Windows computers.
- **Missing Mac OS Patches Statistics:** An overview of all patches that are missing on at least one client Mac OS X computer and the total number of computers on which each of these patches is missing.
- **Missing Microsoft Patches Statistics:** Same as **Missing Mac OS Patches Statistics** but for Windows computers.

Context menu

The context menu contains these commands:

- **New Missing Mac OS Patches Smart Group:** Creates a new smart group for missing Mac OS X patches.
- **New Missing Microsoft Patches Smart Group:** Creates a new smart group for missing Windows patches.

- **New Missing Mac OS Patches Statistics Smart Group:** Creates a new smart group for summary information on missing patches on Mac OS X computers.
- **New Missing Windows Patches Statistics Smart Group:** Creates a new smart group for summary information on missing patches on Windows computers.

The dialog for defining smart groups is described in “New Smart Group” on page 369.

Computer- and file-related commands in the table context menu are described in “Commands menu” on page 283.

For the remaining three commands (**Rename Group**, **Edit Smart Group**, and **Remove Group**), please see the description of browser windows in “Browser windows” on page 365.

Further information

Browser windows in general are described in “Browser windows” on page 365. The columns in the **Missing Operating System Patches** window are described in “Missing OS Patches” on page 564.

Details of Absolute Manage’s patch management are described in “Automated patch management” on page 235.

Registry Entries

The **Registry Entries** command opens the **Registry Entries** window.

The **Registry Entries** window is a predefined browser window that displays registry entries which have been found by the **Search Windows Registry** command.

Predefined smart groups

The usual **Macs only** and **All Computers** smart groups are not present in the **Registry Entries** because registries are found only on PCs.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 365.

Further information

Browser windows in general are described in “Browser windows” on page 365. The columns in the **Registry Entries** window are described in “Registry Entries” on page 569.

Compliance Reports

The **Compliance Reports** command opens the **Compliance Reports** window.

The **Compliance Reports** window is a predefined browser window that displays compliance reports which have been created by means of the **Gather Compliance Report** command.

Double-clicking any report opens the **Compliance Report** window for that report. See “Compliance Report window” on page 378 for details.

Predefined smart groups

The only predefined smart group is the **All Reports** group.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 365. (The **New Smart Compliance Report Group** command is similar to the **New Smart Group** command.)

The context menu in the main window area contains an additional command, **Show Report Details**. Choosing this command opens the **Compliance Report** window for that report, just like double-clicking the report.

Further information

Browser windows in general are described in “Browser windows” on page 365. The columns in the **Compliance Reports** window are described in “Compliance Reports” on page 587.

Power Usage Reports

The **Power Usage Reports** command opens the **Power Usage Reports** window.

The **Power Usage Reports** window is a special window that displays summary information on power savings achieved by using Absolute Manage's power management features.

Predefined smart groups

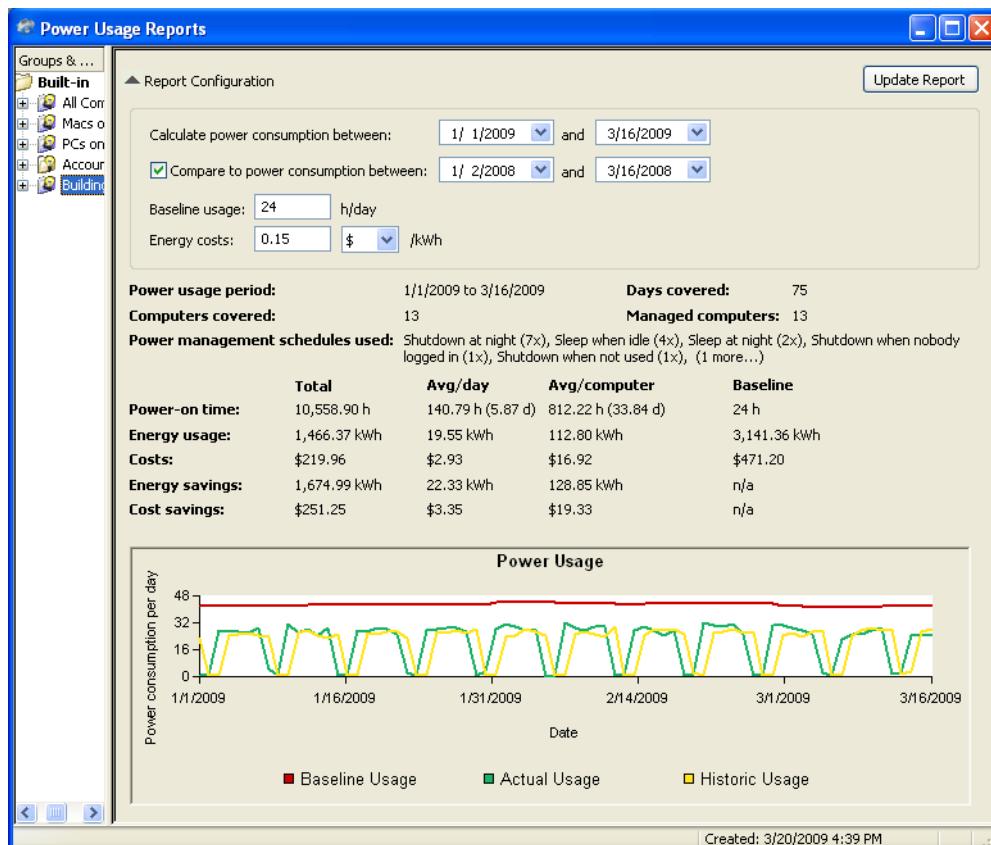
The predefined smart groups are similar to the ones in standard browser windows, as described in “Sidebar” on page 367. Reports are created for the selected groups.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 365.

Main window area

The main area of the compliance report window contains a configuration section, a statistics section, and a graphical display of the power consumption.



In the configuration section:

- **Update Report:** Clicking this button recalculates the displayed statistics and the graph based on the current configuration settings for the selected computer group.
- **Calculate power consumption between:** The power consumption between the dates you specify here (inclusive) is displayed both in the statistics section and the graph.
- **Compare to power consumption between:** If this option is checked, the historic power consumption in the specified period is displayed in the graph for comparison purposes. This period is exactly as long as the primary period chosen above.
- **Baseline usage:** This is the number of hours per day that an administered computer is considered to be running without the Absolute Manage power management. In effect, this number provides the value from which your savings are calculated.

- **Energy costs:** The price you pay for a kilowatt-hour of electricity. Enter a value and a currency; some common currencies can be chosen from the pop-up menu.

In the statistics section:

- **Report period:** The days for which the statistics are provided. Note that this may differ from the dates in the configuration section if you have changed the period and not yet clicked the **Update Report** button.
- **Days covered:** The number of days in the report period.
- **Computers covered:** The number of computers that have been included in the report.
- **Managed computers:** The number of computers to which power management schedules are currently being applied.
- **Power management schedules used:** A list of power management schedules that are being applied to the managed computers.
- **Power-on time:** The time the computers included in the report have been running. Reported values include:
 - **Total:** the sum over all computers and report days
 - **Avg/day:** the daily average for all computers
 - **Avg/computer:** the average per computer over the entire report period
 - **Baseline:** the comparison value over all computers and days if no power management had happened
- **Energy usage:** The power consumption of the computers in the report. The consumption is calculated using these typical values:
 - Desktop computer: 105 W operational, 5 W sleep
 - Laptop computer: 30 W operational, 2 W sleep
 - LCD monitor: 35 W operational, 0 W sleep
 - CRT monitor: 65 W operational, 0 W sleepSee **Power-on time**, above for explanations of the individual values.
- **Costs:** The costs of the consumed power. See **Power-on time**, above for explanations of the individual values.
- **Energy savings:** The power saved when compared to the baseline level. See **Power-on time**, above for explanations of the individual values.
- **Cost saving:** The money saved when compared to the baseline level. See **Power-on time**, above for explanations of the individual values.

The graph provides a visual overview of the power that has been used during the report period. It contains three data series:

- Baseline usage: The amount of power that would have been consumed without the power management schedules. (Based on the number of hours that is specified in the **Baseline usage** field.)

- Actual usage: The amount of power that was consumed during each displayed interval.
- Historic usage: The power usage during the specified comparison period.

NOTE Both the actual and the baseline power consumption is calculated based on the values in the **Power Consumption** settings pane.

Further information

Absolute Manage's power management functions are described in "Scheduling power management events" on page 118.

Mobile Devices

The **Mobile Devices** command opens the **Mobile Devices** window that integrates all aspects of working with administered mobile devices, such as iPhones and iPads.

The **Mobile Devices** window is much like a browser window. However, in contrast to a normal browser window, it displays information from one of several database tables grouped into multiple categories, depending on which smart group or other sidebar entry is selected.

The items and context menu commands of the **Mobile Devices** window are described in "Mobile Devices" on page 385.

Browser windows in general are described in "Browser windows" on page 365. The columns in the **Mobile Devices** window are described in "Mobile Device Information" on page 589.

Server Center

The **Server Center** command opens the **Server Center** window that integrates all aspects of configuring software distribution, license monitoring, and administrator accounts, and server monitoring.

The **Server Center** window is much like a browser window. However, in contrast to a normal browser window, it displays information from one of several database tables grouped into multiple categories, depending on which smart group or other sidebar entry is selected.

The items and context menu commands of the **Server Center** window are described in "Server Center" on page 435.

Browser windows in general are described in "Browser windows" on page 365. The columns in the **Server Center** window are described in "Server Center" on page 571.

Agent Deployment Center

The **Agent Deployment Center** command opens the **Agent Deployment Center** window that integrates all aspects of centrally installing and updating Absolute Manage Agent on administered computers.

The **Agent Deployment Center** window is much like a browser window. However, in contrast to a normal browser window, it displays information on devices in the network – computers and other devices.

The items and context menu commands of the **Agent Deployment Center** window are described in “Agent Deployment Center” on page 510.

Browser windows in general are described in “Browser windows” on page 365. The columns in the **Agent Deployment Center** window are described in “Agent Deployment Center” on page 585.

NOTE The Agent Deployment Center can be used only by administrators with the **Deploy Agents** right. See “New Administrator” on page 481 for details.

Commands

The **Commands** command opens the **Commands** window that displays all pending and currently executing commands as well as the command history and lets you edit and reschedule commands. You can also issue new commands by selecting the desired target computers and choosing the desired option from the **Commands** menu.

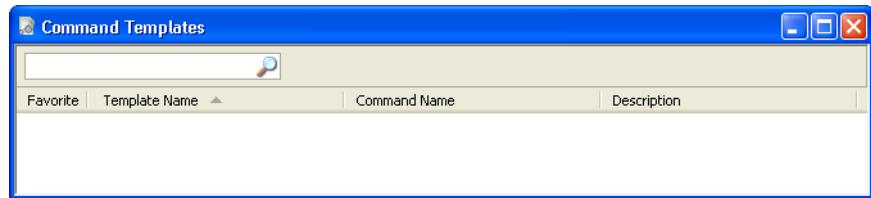
The **Commands** window is much like a browser window. However, in contrast to a normal browser window, it displays information items from the **Commands** category (described in “Commands” on page 570).

The items and context menu commands of the **Commands** window are described in “Commands window” on page 527.

Browser windows in general are described in “Browser windows” on page 365.

Command Templates

The **Command Templates** command opens the **Command Templates** window that lists all commands that have been saved as templates.



The window contains these elements:

- **Search Templates:** This field lets you quickly restrict the display to command templates that contain the search text. Clicking the magnifying glass icon at the right of the field executes the search.
- **Favorite:** Command templates checked in this column appear in the **Favorites** submenu of the **Commands** menu.
- **Template Name:** The name under which the template has been saved. You can click this field of a selected command template to edit the name.
- **Command:** The command that is executed by the template.
- **Description:** The description of the command template that you have entered when saving the template. You can click this field of a selected command template to edit the description.

Context menu

The window's context menu contains these commands:

- **Use Template:** Choosing this command opens the selected templates, displaying the respective commands' command dialogs. You can edit all the options in these dialogs, including the target list, before clicking the **Execute** button to actually issue the command.
- **Remove Template:** Choosing this command deletes the selected templates from the Command Templates window. If the template was included in the **Favorites** submenu, it is removed there as well.

Window Reinstallation Tasks

The **Windows Reinstallation Tasks** command opens the **Windows Reinstallation Tasks** window that lists all Windows reinstallation commands that have been sent to an Absolute PXE server or a FOG server.



The window lists all issued reinstallation tasks for Windows target computers (i.e., tasks started with the **Reinstall Windows Computer** command).

It may also include tasks executed by a FOG server that have not come from Absolute Manage, e.g., because they were entered through the FOG web interface.

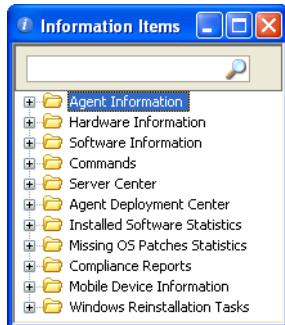
Context menu

The window's context menu contains these commands (in addition to standard commands for all browser windows described in "Sidebar context menu" on page 368 and "Table context menu" on page 371, respectively):

- **Show Computer Detail View:** This command is similar to the **Show Detail View** command standard to all browser windows.
Choosing this command displays the selected computer's detail information in the **Computers** window.
- **Synchronize Records:** Clicking this button updates the displayed information with current data from the PXE server.

Information Items

The **Information Items** command opens the **Information Items** window that lists all information items.



The window contains these elements:

- The text field lets you quickly restrict the display to information items the name of which contains the search text. Clicking the magnifying glass icon at the right of the field executes the search.
- A hierarchical list of information items, grouped by category.

Dragging an information item to a browser window adds a column displaying the information item to the window.

Context menu

The **Information Items** window's context menu contains these commands:

- **Copy**: This command copies the name of the current information item. It has the same effect as the **Copy** command from the **Edit** menu.
- **Edit Custom Field**: This command is available only for custom information items. Choosing it lets you edit the selected custom information item in the **Custom Information Field** dialog. A custom information item can also be edited by double-clicking in the **Information Items** window.

User windows

The bottom part of the menu contains all browser windows and command dialogs that you have opened. If no such window has yet been opened, this section is not displayed.

Chapter 16

Help menu

The **Help** menu lets you access the Absolute Manage online help and copyright information:

- **Help Topics** (page 363)
- **Show Release Notes** (page 363)
- **Absolute Manage Support** (page 363)
- **Absolute Manage Web Site** (page 363)
- **Acknowledgements** (page 363)
- **About Absolute Manage Admin** (page 363)

Help Topics

The **Help Topics** command opens Absolute Manage Admin's online help.

Show Release Notes

The **Show Release Notes** command opens the release notes for the installed release of Absolute Manage in a PDF reader.

The release notes can only be displayed when a PDF reader – such as Adobe Reader – is installed on your computer.

Absolute Manage Support

The **Absolute Manage Support** command opens the main support page from Absolute Manage's Web site in your default Web browser.

Absolute Manage Web Site

The **Absolute Manage Web Site** command opens the main Absolute Manage Web page in your default Web browser.

Acknowledgements

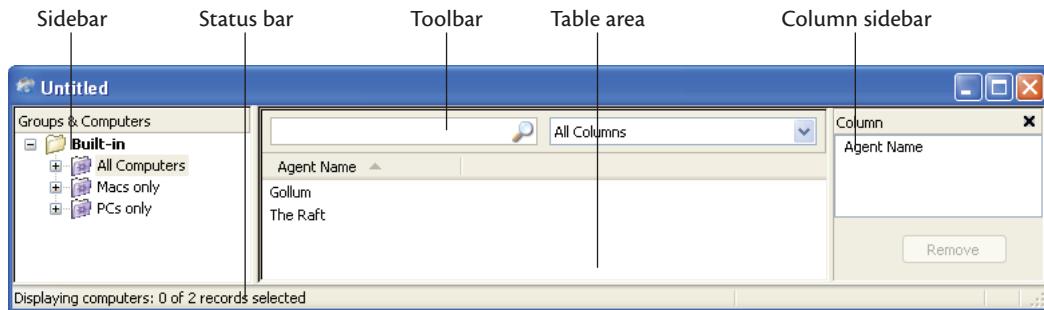
The **Acknowledgements** command opens a window displaying the acknowledgements for code incorporated into Absolute Manage and other contributions.

About Absolute Manage Admin

The **About Absolute Manage Admin** command opens the **About Absolute Manage Admin** dialog. The dialog contains information on

the application version, developer credits, registration information, and copyright information. It also displays the server to which the Absolute Manage Admin application is currently connected.

Browser windows display the contents of Absolute Manage's internal database in a configurable table view.



Browser windows contain these elements:

- **Toolbar** (page 366)
- **Status bar** (page 366)
- **Table columns** (page 366)
- **Column sidebar** (page 367)
- **Sidebar** (page 367)
- **Sidebar context menu** (page 368)
 - **New Group** (page 368)
 - **New Smart Group** (page 369)
 - **New Category** (page 369)
 - **Rename Group** (page 370)
 - **Edit Smart Group** (page 370)
 - **Remove Group** (page 370)
 - **Remove Category** (page 371)
 - **Remove from Group** (page 371)
- **Table context menu** (page 371)
 - **Copy** (page 372)
 - **Copy "<information item>"** (page 372)
 - **New Smart Group from "<information item>"** (page 372)
 - **Make Group from Selected Computers** (page 372)
 - **Show Detail View** (page 373)
 - **Synchronize Records** (page 373)
 - **Enter Custom Field Data** (page 373)
 - **Remove from Server** (page 374)
 - **Remove Inventory Data** (page 374)
 - **Computer Tracking** (page 374)
 - **Remove from Group** (page 375)
 - **Remote Control** (page 375)
 - **View in Separate Window** (page 376)
 - **Open in External Viewer** (page 377)

Toolbar

Browser windows have toolbars that let you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Status bar

Browser windows have status bars displaying information on the state of the window.

The status bar displays the number of records currently shown in the window. It also shows the kind of information displayed:



If the window does not display all records from the server database table (because the number of records exceeds the initial display limit set in the **Settings** dialog's **General** pane), this is indicated with the addition "(more...)" after the record count in the status bar. If data on an individual computer is displayed (as described in "Sidebar" on page 367), the status bar also indicates how old the currently shown information is.

Table columns

The columns displayed in browser windows are completely configurable:

The columns display information items from the **Agent Information**, **Hardware Information**, **Software Information**, **Command History**, and **License Status per Agent** categories. Information items are described in "Information items" on page 534.

Columns can be dragged around in the window to be rearranged. Dragging an item from the **Information Items** window into a browser window creates a new column at the right of the table.

Deleting columns is possible in the **Columns** sidebar, in addition to rearranging and adding columns. This is described below.

Double-clicking a column title in the browser window sorts the table by that column or, if the column is already a sort column, reverses the sort order. If there already are sorting columns, double-clicking a new column makes it a subsorting column. Double-clicking while holding down the Alt key unsorts a column.

If individual computers are selected in the sidebar (see below), the columns are hidden and information on the selected computer is displayed.

Column sidebar

Browser windows contains a Column sidebar for rearranging the columns in the window.

It is opened by choosing **Configure Columns** from the **View** menu.

The sidebar contains the titles of all columns that are displayed in the browser window.

The order of the column titles is the same as that of the columns in the table in the window. Dragging a column title to another location in the sidebar repositions the column in the window.

Dragging an information item into the sidebar adds a corresponding column to the window. You can also drag columns from one Columns sidebar to another or transfer them by copying and pasting.

Clicking the Remove button deletes the selected columns from the window.

Sidebar

Browser windows contains a sidebar with a number of categories and predefined smart groups to which more can be added.

Categories

New browser windows contain the **Built-in** category. (Predefined windows may contain other or additional categories.) More categories can be added using the **New Category** context menu command.

Categories group other categories, groups, and smart groups very much like folders in a file system.

Smart groups

- **All Computers:** All computers listed in the Computers table in the Absolute Manage database.
- **Macs only:** All Mac OS X computers contained in the database.
- **PCs only:** All Windows computers contained in the database.

Additional smart groups and groups can be added using the **New Group** and **New Smart Group** commands in the action context menu.

NOTE Smart groups are defined by selection criteria, dynamically displaying computers that match the criteria at the moment. Groups are folder-like, containing the computers that have been put into them manually.

You can rearrange smart groups by dragging them to the desired place in the list.

Details

The smart groups can be expanded to reveal the computers contained in them. A computer can be clicked to reveal basic information on that computer in the table area.

Expanding a computer displays a range of categories in the sidebar. Clicking on of the categories displays information from that category for the respective computer in the table area.

Details can be displayed in the same way for computers in user-created groups and smart groups.

Sidebar context menu

The sidebar context menu of browser windows contains commands for managing groups and smart groups.

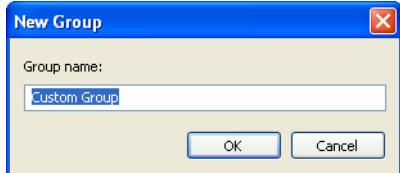
The commands are described in detail in the following sections.

- “New Group” on page 368
- “New Smart Group” on page 369
- “New Category” on page 369
- “Rename Group” on page 370
- “Rename Category” on page 370
- “Edit Smart Group” on page 370
- “Remove Group” on page 370
- “Remove Category” on page 371
- “Remove from Group” on page 371

New Group

The **New Group** command creates a new (non-smart) group.

Choosing the command opens the **New Group** dialog:

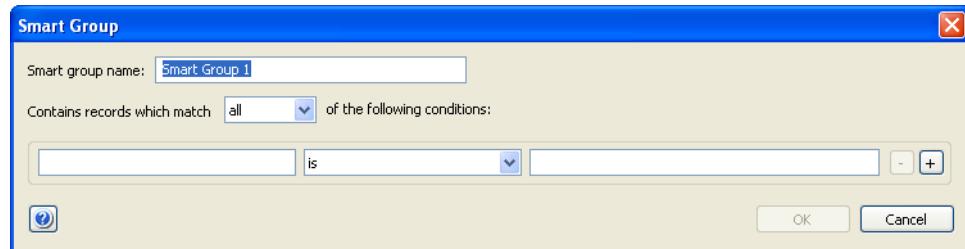


The dialog contains a field for naming the new group.

New Smart Group

The **New Smart Group** command creates a new smart group.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

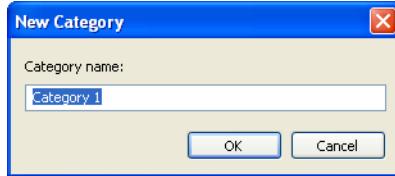
- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you specify an information item on which records are to be matched.
 - The pop-up menu in the middle contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Category

The **New Category** command creates a new category in the browser window's sidebar.

Rename Group

Choosing the command opens the **New Category** dialog:



The dialog contains a field for editing the name of the category.

Rename Group

The **Rename Group** command renames an existing smart or non-smart group.

Choosing the command opens the **Rename Group** dialog:



The dialog contains a field for editing the name of the group.

If a category is selected, this command is renamed **Rename Category**.

Rename Category

If a category in the sidebar is selected, the **Rename Group** command is renamed **Rename Category**.

Choosing the command is similar to choosing **Rename Group**; see there for details.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the **Smart Group** dialog, described in **New Smart Group**, above.

Remove Group

The **Remove Group** command deletes the selected smart or non-smart groups.

Choosing the command deletes the selected groups. A confirmation alert is displayed first. The computers listed in the groups is not deleted from the database.

If a category is selected, this command is renamed **Remove Category**.

Remove Category

If a category in the sidebar is selected, the **Remove Group** command is renamed **Remove Category**.

Choosing the command is similar to choosing **Remove Group**; see there for details.

Remove from Group

The **Remove from Group** command deletes the selected computers from the displayed group.

It is not available when a smart group is being displayed.

Table context menu

The table context menu of browser windows contains commands from the **Commands** menu. In addition, it contains a number of specific commands:

- “Copy” on page 372
- “Copy “<information item>”” on page 372
- “New Smart Group from “<information item>”” on page 372
- “Make Group from Selected Computers” on page 372
- “Show Detail View” on page 373
- “Synchronize Records” on page 373
- “Remove from Server” on page 374
- “Remove Inventory Data” on page 374
- “Computer Tracking” on page 374
- “Remove from Group” on page 375
- “Remote Control” on page 375
- “View in Separate Window” on page 376
- “Open in External Viewer” on page 377

For information on the rest of the commands in the table context menu, see “Commands menu” on page 283. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

In the **Computer Tracking** section of a computer's detail view, you can use **Copy** to copy a screenshot.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 343.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (e.g., **Copy “Computer Type”**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Group from “<information item>”

The **New Smart Group from “<information item>”** command lets you create a smart group with pre-filled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

Make Group from Selected Computers

The **Make Group from Selected Computers** command lets you create a smart group with pre-filled criteria.

Choosing the command creates a new group from the selected computers. A dialog is displayed in which you must give the group a name; when you close the dialog, the group is added to the sidebar.

Show Detail View

The **Show Detail View** command displays the detailed information for the currently selected computer.

It has the same effect as the **Details** command described on page 281.

Synchronize Records

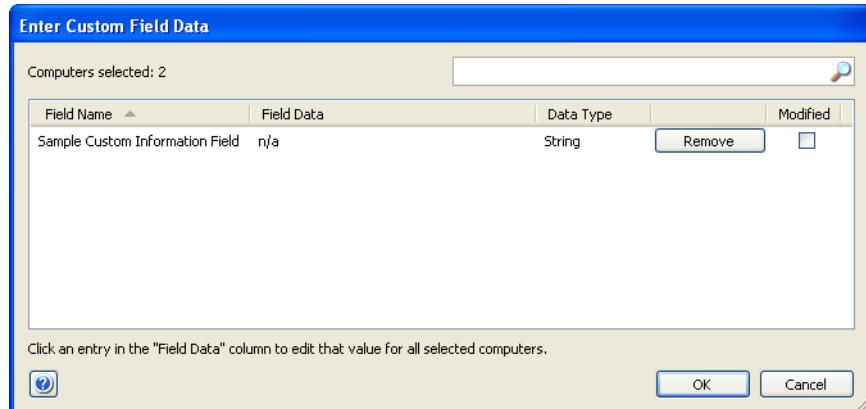
The **Synchronize Records** command downloads updated information for the selected records from the server to which you are connected.

It has the same effect as the **Synchronize Selected Records** command described on page 343.

Enter Custom Field Data

The **Enter Custom Field Data** command lets you edit the content of manual custom information fields for multiple computers in one step.

Choosing the command opens the **Enter Custom Field Data** dialog:



The dialog contains a list of available manual custom information fields.

Clicking one of the fields' **Field Data** column lets you edit the content of that field for all selected computers.

Clicking the **Remove** button removes the field content from all selected computers.

Only fields that are checked in the **Modified** column are modified when you click **OK**.

NOTE The **Modified** column is not displayed if only one computer was selected before the dialog was opened.

Remove from Server

The **Remove from Server** command deletes the selected records from the server. A confirmation alert is displayed first.

NOTE If a computer is deleted from the server, it may be automatically reappear at a later time if it is still present in the network and Absolute Manage Agent is running on it.

NOTE The **Remove from Server** command can be used for computer records only by administrators with the **Remove Computer Records** right. See “New Administrator” on page 481 for details.

Remove Inventory Data

The **Remove Inventory Data** command lets you remove data related to the selected computers from Absolute Manage’s databases. It is useful for deleting extensive information that was needed only for a specific purpose, speeding up Absolute Manage processes.

Choosing the command opens the **Remove Inventory Data** dialog:



The checkboxes allow you to specify the data to be deleted.

Clicking **OK** deletes all data on the server of the marked types which relate to the selected computers.

NOTE The **Remove Inventory Data** command can be used for computer records only by administrators with the **Remove Inventory Data** right. See “New Administrator” on page 481 for details.

Computer Tracking

The **Computer Tracking** command lets you activate or deactivate tracking for the selected computers and specify tracking options.

Choosing the command opens the **Computer Tracking** dialog:



The dialog contains these options:

- **Track selected computers:** Check this option to activate tracking the computers; uncheck it to stop tracking them.
- **Take screenshots:** If this option is checked, the tracked computers take screenshots and transmit them to the Absolute Manage Server whenever they send a 'heartbeat' (e.g., when the network connection is changed, when a user logs in or out, when the computer is woken up, or in regular intervals otherwise).

NOTE The **Computer Tracking** command is available only to administrators with the **Change Computer Tracking** right. See "New Administrator" on page 481 for details.

Remove from Group

The **Remove from Group** command deletes the selected computers from the displayed group or computer group.

It is not available when a smart group is being displayed.

Remote Control

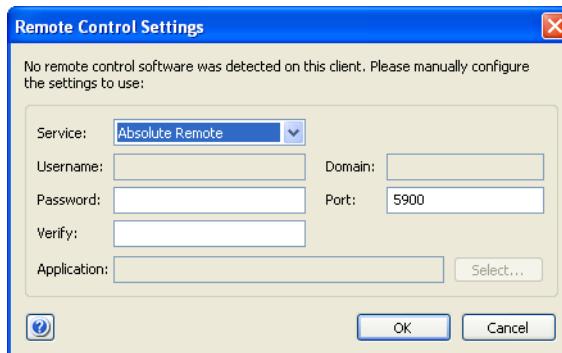
The **Remote Control** command lets you remotely control the selected client computers using screen sharing software.

Choosing the command launches a local remote control software – such as Absolute Remote, Timbuktu, Mac OS X Screen Sharing, MS Remote Desktop, or a VNC application – and connects it to the selected client computer.

Details of the process are described in "Remotely controlling computers" on page 122.

A screen sharing client for the application must be available on the remote computer. If Absolute Manage does not detect any such client

or if you hold down the Shift key while choosing the command, the **Remote Control Settings** dialog opens:



The dialog contains these elements. Fields that do not apply to the chosen service are disabled:

- **Service:** The desired protocol to use for remotely controlling the target computer.
- **Username:** The user account for the remote control software on the client computers.
- **Password** and **Verify:** The password for the specified account.
Note: Some VNC applications do not support being supplied with a username and password when they are launched; when you are using these applications, you must enter a username and password within the application, even if you have already supplied both in Absolute Manage. This is a limitation of these applications, not of Absolute Manage.
- **Application:** The local application that will be used to connect to the client. If "n/a" is displayed, no application for the selected protocol was found.
- **Select:** Click this button to choose the desired application to use.
- **Domain:** The Windows networking domain to be used for accessing client computers.
Note: Some VNC applications do not support domains.
- **Port:** The network port on which to contact the remote control software on the client computers.

View in Separate Window

The **View in Separate Window** command opens the selected image in its own window.

The command is available only in the context menu for a screenshot in the **Computer Tracking** section of a computer's detail view.

Open in External Viewer

The **Open in External Viewer** command opens the selected image in the default application for viewing JPEG files, as configured on your computer.

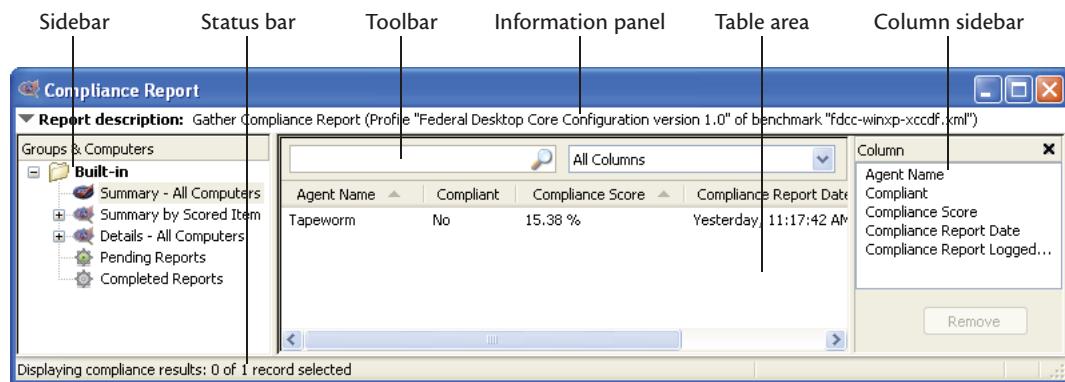
The command is available only in the context menu for a screenshot in the **Computer Tracking** section of a computer's detail view.

Chapter 18

Compliance Report window

The **Compliance Report** window displays the details of an USGCB SCAP compliance report: The tested computers, their individual results and compliance results, item-by-item breakdowns, and summaries by item across all computers.

The window is opened by double-clicking a report in the **Compliance Reports** window.



The elements of a **Compliance Report** window are described below:

- **Toolbar** (page 378)
- **Information panel** (page 379)
- **Table columns** (page 379)
- **Sidebar** (page 379)
- **Context menus** (page 380)
 - **Copy** (page 380)
 - **Copy “<information item>”** (page 380)
 - **Show Details for This Computer** (page 381)
 - **Show Details for This Scoring Item** (page 381)
 - **New Smart Report Summary Group** (page 381)
 - **New Smart Report Item Summary Group** (page 382)
 - **New Smart Report Details Group** (page 382)
 - **New Category** (page 383)
 - **Rename Group** (page 383)
 - **Rename Category** (page 383)
 - **Edit Smart Group** (page 384)
 - **Remove Smart Group** (page 384)
 - **Remove Category** (page 384)

Toolbar

The **Compliance Report** window toolbar lets you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to commands that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Information panel

The information panel at the top of a **Compliance Report** window displays information on the report itself.

Clicking the triangle ▾ at the left of the panel left expands and collapses it.

In its collapsed state, it displays the name of the report as well as the profile and the benchmark file used.

In its expanded state, it displays additional information on the report. These information items are described in “Reports” on page 588.

Table columns

The columns displayed in a **Compliance Report** window are described in “Compliance Reports” on page 587.

Sidebar

The **Compliance Report** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

- **Summary – All Computers:** Summary information on all computers for which the report has been completed.
- **Summary by Scored Item:** Summary information on all score items, showing how the compliance for each item was across all tested computers.
Expand the category and click any score item to display the individual results of each computer.
- **Details – All Computers:** Detailed information for one computer on each score item.
Expand the category and click the desired computer in the sidebar to display its details.
- **Pending Reports:** All reports that are in the process of being collected.
- **Completed Reports:** All reports that have been completely gathered.

Any additional smart groups that you define are displayed below these groups.

Context menus

The context menus of a **Compliance Report** window contains commands for managing reports and smart groups.

The commands are described in detail in the following sections.

- “Copy” on page 380
- “Copy “<information item>” on page 380
- “Show Details for This Computer” on page 381
- “Show Details for This Scoring Item” on page 381
- “New Smart Report Summary Group” on page 381
- “New Smart Report Item Summary Group” on page 382
- “New Smart Report Details Group” on page 382
- “New Category” on page 383
- “Rename Group” on page 383
- “Rename Category” on page 383
- “Edit Smart Group” on page 384
- “Remove Smart Group” on page 384
- “Remove Category” on page 384

For information on the rest of the commands in the table context menu, see “Commands menu” on page 283. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 273.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (e.g., **Copy “Command Name”**).

If multiple records are selected, the contents of the information item from all of them are copied.

Show Details for This Computer

The **Show Details for This Computer** command displays the detailed report scores for the computer on which you click.

Using this command is the same as selecting the computer in the sidebar under **Details – All Computers**.

Show Details for This Scoring Item

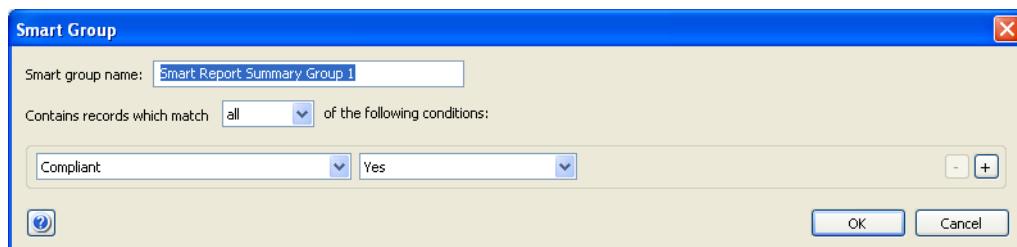
The **Show Details for This Scoring Item** command displays the detailed report scores for the scoring item on which you click.

Using this command is the same as selecting the scoring item in the sidebar under **Summary by Scored Item**.

New Smart Report Summary Group

The **New Smart Report Summary Group** command lets you create a smart group that displays all report summaries meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



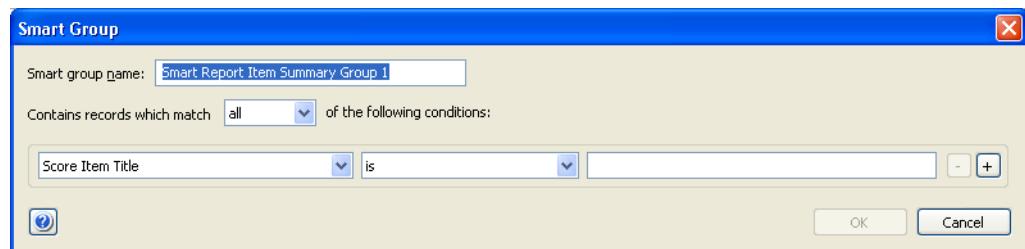
The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in "Computer Summary" on page 588.
 - The second pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Smart Report Item Summary Group

The **New Smart Report Item Summary Group** command lets you create a smart group that displays all score item summaries meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



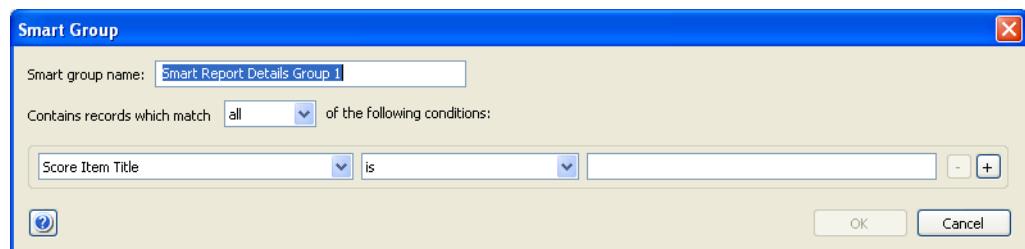
The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in "Item Summary" on page 588.
 - The second pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Smart Report Details Group

The **New Smart Report Details Group** command lets you create a smart group that displays all report details on individual computers meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Score Items” on page 589.
 - The second pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The + and – buttons let you add new conditions or remove existing ones.

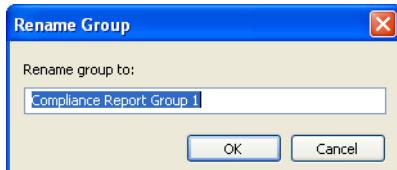
New Category

The **New Category** command creates a new category in the window’s sidebar.

Rename Group

The **Rename Group** command renames an existing smart group.

Choosing the command opens the **Rename Group** dialog:



The dialog contains a field for editing the name of the group.

If a category is selected, this command is renamed **Rename Category**.

Rename Category

If a category in the sidebar is selected, the **Rename Group** command is renamed **Rename Category**.

Choosing the command is similar to choosing **Rename Group**; see there for details.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the specification dialog for the type of smart group that is selected. For details, see the command for creating that type of smart group:

- “New Smart Report Summary Group” on page 381
- “New Smart Report Item Summary Group” on page 382
- “New Smart Report Details Group” on page 382

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Remove Category

If a category in the sidebar is selected, the **Remove Smart Group** command is renamed **Remove Category**.

Choosing the command is similar to choosing **Remove Smart Group**; see there for details.

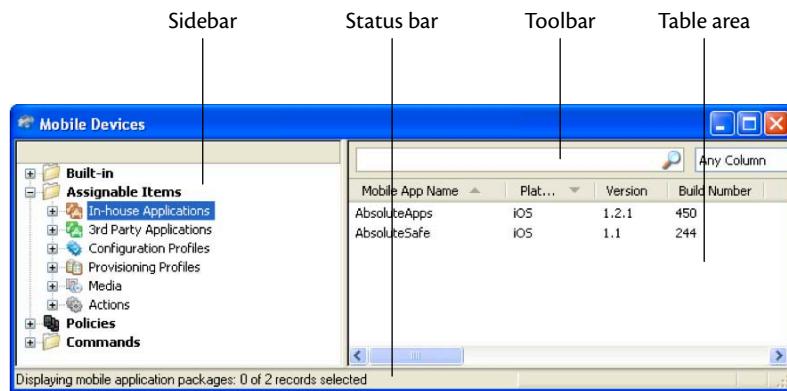
Chapter 19

Mobile Devices

The **Mobile Devices** window displays information on mobile devices enrolled in the MDM server that is specified in the server settings. (See “MDM” on page 504 for more information.) It also displays limited information on iOS devices that are managed through a copy of iTunes installed on any administered computer.

NOTE Administrators can see in this window only information about devices to which they have been assigned, unless the **Can manage all devices** option has been activated for their account.

The window is opened by choosing the **Mobile Devices** command from the **Window** menu.



The elements of the **Mobile Devices** window are described below:

- **Toolbar** (page 388)
- **Table columns** (page 388)
- **Sidebar** (page 389)
- **Sidebar context menu** (page 391)
 - **Mobile Applications** (page 393)
 - **New In-house Application Package** (page 393)
 - **New iOS App Store Application Package** (page 394)
 - **New Google Play Application Package** (page 397)
 - **Duplicate Application Package** (page 398)
 - **New Smart Group: In-house Application Packages** (page 398)
 - **New Smart Group: App Store Application Packages** (page 398)
 - **New Smart Group: iOS Provisioning Profiles** (page 398)
 - **New Smart Group: Installed Applications** (page 398)
 - **New Smart Group: Installed Application Statistics** (page 399)
 - **New Smart Group: Mobile Devices by Installed Software** (page 399)

-
-
- **New Smart Group: Installed iOS Provisioning Profiles** (page 399)
 - **New Smart Group: Installed iOS Provisioning Profiles Statistics** (page 399)
 - **New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles** (page 399)
 - **Configuration Profiles and Certificates** (page 400)
 - **New Configuration Profile** (page 400)
 - **New Smart Group: Configuration Profiles** (page 401)
 - **New Smart Group: Installed Configuration Profiles** (page 401)
 - **New Smart Group: Installed Configuration Profiles Statistics** (page 401)
 - **New Smart Group: Mobile Devices by Installed Configuration Profiles** (page 402)
 - **New Smart Group: Installed Certificates** (page 402)
 - **New Smart Group: Installed Certificates Statistics** (page 402)
 - **New Smart Group: Mobile Devices by Installed Certificates** (page 402)
 - **Media** (page 402)
 - **New Media File** (page 403)
 - **Duplicate Media File** (page 404)
 - **New Smart Group: Media Files** (page 405)
 - **Actions** (page 405)
 - **New Send Message to Device Action** (page 405)
 - **New Send E-mail Action** (page 407)
 - **New Send SMS (Text Message) Action** (page 409)
 - **New Set Roaming Options Action** (page 410)
 - **New Update Device Info Action** (page 411)
 - **New Freeze Device Action** (page 412)
 - **New Remove Configuration Profile Action** (page 413)
 - **New Demote to Unmanaged Device Action** (page 413)
 - **Duplicate Action** (page 414)
 - **New Smart Group: Actions** (page 414)
 - **Policies** (page 414)
 - **New Policy** (page 415)
 - **New Smart Policy: Mobile Devices** (page 415)
 - **New Smart Policy: Mobile Devices by Installed Applications** (page 415)
 - **New Smart Policy: Mobile Devices by Installed Configuration Profiles** (page 415)
 - **New Group: Mobile Devices** (page 415)
 - **New Smart Group: Mobile Devices** (page 416)
 - **New Smart Group: Command Queue** (page 416)
 - **New Smart Group: Command History** (page 416)
 - **New Category** (page 416)
 - **Rename <item>** (page 416)
 - **Edit <item>** (page 416)
 - **Remove <item>** (page 416)
 - **Table context menu** (page 417)
 - **Copy** (page 418)
 - **Copy "<information item>"** (page 418)

- **New Smart Mobile Device Group from “<information item>”** (page 419)
- **New Smart Policy from “<information item>”** (page 419)
- **New Smart Application Group from “<information item>”** (page 419)
- **New Smart Configuration Profiles Group from “<information item>”** (page 420)
- **New Smart Provisioning Profiles Group from “<information item>”** (page 420)
- **New Smart Media Files Group from “<information item>”** (page 420)
- **New Command Queue Smart Group from “<information item>”** (page 421)
- **New Command History Smart Group from “<information item>”** (page 421)
- **New Policy with Selected Devices** (page 421)
- **Install Configuration Profile** (page 422)
- **Install Provisioning Profile** (page 422)
- **Install Application** (page 422)
- **Issue Device Lock** (page 422)
- **Issue Clear Passcode** (page 422)
- **Issue Remote Erase** (page 422)
- **Set Roaming Options** (page 422)
- **Send Message to Device** (page 422)
- **Set Device Name** (page 423)
- **Delete Application** (page 423)
- **Delete Profile** (page 423)
- **Update Device Info** (page 424)
- **Show Detail View** (page 424)
- **Synchronize Records** (page 424)
- **Enter Custom Field Data** (page 424)
- **Import Custom Field Data** (page 424)
- **Ignore Devices** (page 425)
- **Reset All Ignored Devices** (page 425)
- **Re-execute All Actions for This Device** (page 425)
- **Re-execute This Action for This Device** (page 425)
- **Retry All Failed Profiles** (page 425)
- **Remove from Group** (page 426)
- **Remove from Policy** (page 426)
- **Track Device** (page 426)
- **Get Device Geolocation** (page 426)
- **Reset Tracking Passphrase** (page 426)
- **Show Location on Google Maps** (page 426)
- **Show Location on Bing Maps** (page 426)
- **Set Device Ownership** (page 427)
- **Send Re-enrollment Message to Device** (page 427)
- **Update Installed Application Statistics** (page 428)
- **Show Mobile Application Package Details** (page 428)
- **New Mobile Application Package** (page 428)
- **New iOS App Store Application Package** (page 428)
- **New Google Play Application Package** (page 428)
- **Edit Mobile Application Package** (page 428)
- **Duplicate Mobile Application Package** (page 428)
- **Remove Mobile Application Package** (page 429)

- [Show Configuration Profile Details](#) (page 429)
- [New Configuration Profile](#) (page 429)
- [Edit Configuration Profile](#) (page 429)
- [Remove Configuration Profile](#) (page 429)
- [Remove Configuration Profile](#) (page 429)
- [Show Provisioning Profile Details](#) (page 429)
- [Show Media File Details](#) (page 430)
- [Set Availability Time](#) (page 430)
- [New Media File](#) (page 431)
- [Edit Media File](#) (page 431)
- [Remove Media File](#) (page 431)
- [Show Action Details](#) (page 431)
- [Duplicate Action](#) (page 431)
- [Edit Action](#) (page 432)
- [Remove Action](#) (page 432)
- [Re-execute This Action for All Devices](#) (page 432)
- [Re-execute This Action for This Policy](#) (page 432)
- [New Send Message Action](#) (page 432)
- [New Send E-mail Action](#) (page 432)
- [New Send SMS \(Text Message\) Action](#) (page 432)
- [New Set Roaming Options Action](#) (page 433)
- [New Freeze Device Action](#) (page 433)
- [New Remove Configuration Profile Action](#) (page 433)
- [New Demote to Unmanaged Device Action](#) (page 433)
- [Change Action Schedule](#) (page 433)
- [Remove Action from Policy](#) (page 434)
- [Show Policy Members](#) (page 434)
- [Remove Policy](#) (page 434)

Toolbar

The **Mobile Devices** window toolbar lets you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to commands that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Table columns

The columns displayed in a **Mobile Devices** window are described in “Mobile Device Information” on page 589.

Sidebar

The **Mobile Devices** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

Built-in

- **All mobile devices:** All found managed mobile devices. Devices that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iOS devices:** All found mobile devices running iOS. Any devices that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPhones:** All found iPhones. Any iPhones that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPads:** All found iPads. Any iPads that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPod touch devices:** All found iPod touch devices. Any iPods that have been removed with the **Ignore Devices** context menu command are not listed.
- **All Android devices:** All found mobile devices running Android.
- **All Android phones:** All found mobile phones running Android.
- **All Android tablets:** All found tablets running Android.
- **All Windows Phone devices:** All found mobile devices running Windows Phone.
- **All installed applications:** All applications that were found on the listed devices. No applications from devices that have been removed with the **Ignore Devices** context menu command are listed.
- **All installed provisioning profiles:** All provisioning profiles that were found on the listed devices.
- **All installed configuration profiles:** All configuration profiles that were found on the listed devices.
- **All installed certificates:** All certificates that were found on the listed devices.
- **Installed software statistics:** Summary information on the applications that were found on the mobile devices. No applications from devices that have been removed with the **Ignore Devices** context menu command are included in the summary.
These statistics are not automatically updated. To update them, choose **Update Installed Application Statistics** from the context menu.

Assignable Items

- **In-house Applications:** All packages for in-house iOS and Android apps that have been created in Absolute Manage.
- **3rd Party Applications:** All packages for recommended apps that have been created in Absolute Manage.

- **Configuration Profiles:** All configuration profiles that have been imported into Absolute Manage. This includes EAS policies for Windows Phone.
- **Provisioning Profiles:** All provisioning profiles that have been assigned to applications inside Absolute Manage.
- **Media:** All mobile media files that have been specified in Absolute Manage.

Policies

All policies that have been created in Absolute Manage. Each policy has a number of categories:

- **In-house Apps:** Apps developed by your organization:
 - **Auto-install:** Apps that are mandatory on the devices belonging to the policy.
 - **On-demand:** Apps that are available for installation in AbsoluteApps on the devices belonging to the policy.
 - **Auto-install, Auto-remove:** Apps that are automatically installed on devices that are added to the policy and uninstalled from devices that are removed from the policy (unless the devices belong to another policy in which the app is automatically installed).
 - **On-demand, Auto-remove:** Apps that are available for installation in AbsoluteApps on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the app is automatically installed).
 - **Forbidden In-house Apps:** Apps that may not be installed on the devices belonging to the policy.
- **3rd Party Applications:** Apps from an app store:
 - **On-demand:** Apps that have been recommended for use on the devices belonging to the policy.
- **Configuration Profiles:** Apps developed by your organization. There are several subcategories:
 - **Auto-install:** Configuration profiles that are mandatory on the devices belonging to the policy.
 - **On-demand:** Configuration profiles that users of the devices belonging to the policy can install if desired.
 - **Auto-install, Auto-remove:** Configuration profiles that are automatically installed on devices that are added to the policy and uninstalled from devices that are removed from the policy (unless the devices belong to another policy in which the profile is automatically installed).
 - **Forbidden:** Configuration profiles that must not be installed on the devices belonging to the policy.
- **Media:** Media files that are automatically transferred to mobile devices belonging to this policy.
 - **Auto-install:** Media files that are automatically downloaded to devices that are added to the policy. They are not automatically removed when the device leaves the policy.
 - **On-demand:** Media files that are available for installation in AbsoluteApps on the devices belonging to the policy. They

- are not automatically removed when the device leaves the policy.
- **Auto-install, Auto-remove:** Media files that are automatically downloaded to devices that are added to the policy and deleted from devices that are removed from the policy (unless the devices belong to another policy in which the media files are automatically downloaded).
- **On-demand, Auto-remove:** Media files that are available for installation in AbsoluteApps on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the media files are automatically downloaded).

Commands

- **Queued Commands:** Commands issued to managed mobile devices that have not yet been reported as completed.
- **Command History:** Commands issued to managed mobile devices that have been completed, successfully or unsuccessfully.

Any additional smart groups that you define are displayed below these groups.

Sidebar context menu

The context menus of the sidebar of the **Mobile Devices** window contains commands for grouping devices as well as working with applications, profiles, certificates, and policies.

The commands are described in detail in the following sections.

- “Mobile Applications” on page 393
 - “New In-house Application Package” on page 393
 - “New iOS App Store Application Package” on page 394
 - “New Google Play Application Package” on page 397
 - “Duplicate Application Package” on page 398
 - “New Smart Group: In-house Application Packages” on page 398
 - “New Smart Group: App Store Application Packages” on page 398
 - “New Smart Group: iOS Provisioning Profiles” on page 398
 - “New Smart Group: Installed Applications” on page 398
 - “New Smart Group: Installed Application Statistics” on page 399
 - “New Smart Group: Mobile Devices by Installed Software” on page 399
 - “New Smart Group: Installed iOS Provisioning Profiles” on page 399
 - “New Smart Group: Installed iOS Provisioning Profiles Statistics” on page 399
 - “New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles” on page 399

- “Configuration Profiles and Certificates” on page 400
 - “New Configuration Profile” on page 400
 - “New Smart Group: Configuration Profiles” on page 401
 - “New Smart Group: Installed Configuration Profiles” on page 401
 - “New Smart Group: Installed Configuration Profiles Statistics” on page 401
 - “New Smart Group: Mobile Devices by Installed Configuration Profiles” on page 402
 - “New Smart Group: Installed Certificates” on page 402
 - “New Smart Group: Installed Certificates Statistics” on page 402
 - “New Smart Group: Mobile Devices by Installed Certificates” on page 402
- “Media” on page 402
 - “New Media File” on page 403
 - “Duplicate Media File” on page 404
 - “New Smart Group: Media Files” on page 405
- “Actions” on page 405
 - “New Send Message to Device Action” on page 405
 - “New Send E-mail Action” on page 407
 - “New Send SMS (Text Message) Action” on page 409
 - “New Set Roaming Options Action” on page 410
 - “New Update Device Info Action” on page 411
 - “New Freeze Device Action” on page 412
 - “New Remove Configuration Profile Action” on page 413
 - “New Demote to Unmanaged Device Action” on page 413
 - “Duplicate Action” on page 414
 - “New Smart Group: Actions” on page 414
- “Policies” on page 414
 - “New Policy” on page 415
 - “New Smart Policy: Mobile Devices” on page 415
 - “New Smart Policy: Mobile Devices by Installed Applications” on page 415
 - “New Smart Policy: Mobile Devices by Installed Configuration Profiles” on page 415
- “New Group: Mobile Devices” on page 415
- “New Smart Group: Mobile Devices” on page 416
- “New Smart Group: Command Queue” on page 416
- “New Smart Group: Command History” on page 416
- “New Category” on page 416
- “Rename <item>” on page 416
- “Edit <item>” on page 416
- “Remove <item>” on page 416

For information on the rest of the commands in the table context menu, see “Commands menu” on page 283. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

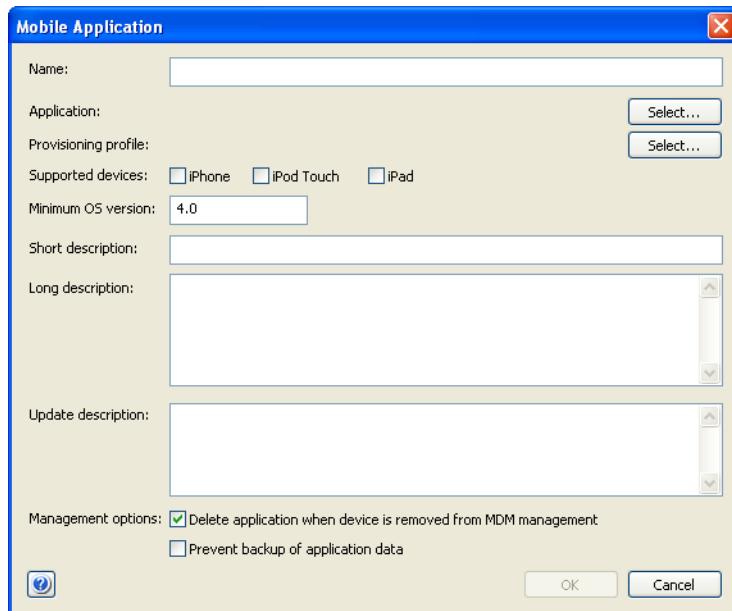
Mobile Applications

The Mobile Applications submenu contains commands for working with application packages and provisioning profiles:

- “New In-house Application Package” on page 393
- “New iOS App Store Application Package” on page 394
- “New Google Play Application Package” on page 397
- “Duplicate Application Package” on page 398
- “New Smart Group: In-house Application Packages” on page 398
- “New Smart Group: App Store Application Packages” on page 398
- “New Smart Group: iOS Provisioning Profiles” on page 398
- “New Smart Group: Installed Applications” on page 398
- “New Smart Group: Installed Application Statistics” on page 399
- “New Smart Group: Mobile Devices by Installed Software” on page 399
- “New Smart Group: Installed iOS Provisioning Profiles” on page 399
- “New Smart Group: Installed iOS Provisioning Profiles Statistics” on page 399
- “New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles” on page 399

New In-house Application Package

This command opens the **Mobile Application** dialog in which you can specify a new iOS application package.



The dialog contains these elements:

- **Name:** The name for the package. This name is displayed in AbsoluteApps.
- **Application:** The application file, which must have the .ipa extension. Clicking the **Select** button lets you select the file on your computer.
Note: Because of a limitation in Windows Vista, Windows 7, and Windows Server 2008, you cannot select files on network shares when running Absolute Manage Admin on these operating system. Copy the file to a local volume before selecting it.
- **Provisioning profile:** The provisioning profile authorizing the application for deployment on the intended mobile device. The provisioning profile is provided by the application developer. Clicking the **Select** button lets you select the file on your computer containing the profile.
Provisioning profiles do not apply to Android apps.
- **Supported devices:** The devices on which this app can be used. Check all devices that support this app.
This option applies only to iOS apps.
- **Short description:** A brief description of the application. This description is displayed in AbsoluteApps.
- **Long description:** A more extensive description of the application. This description is displayed in AbsoluteApps.
- **Update description:** A description of the changes in the application compared to the previous version. This description is displayed in AbsoluteApps. It should only be filled in when the application package contains an application for which an earlier version exists.
- **Delete application when device is removed from MDM management:** If this option is checked, the app will automatically be deleted from any device on which it is installed when that device is no longer under MDM management. If the option is unchecked, removing a device from management leaves the app untouched on it.
This option applies only to iOS apps.
- **Prevent backup of application data:** If this option is checked, any data belonging to this app that is stored on the device is not included in iTunes or iCloud backups of the device. If the option is unchecked, the application data is backed up normally.
This option applies only to iOS apps.

New iOS App Store Application Package

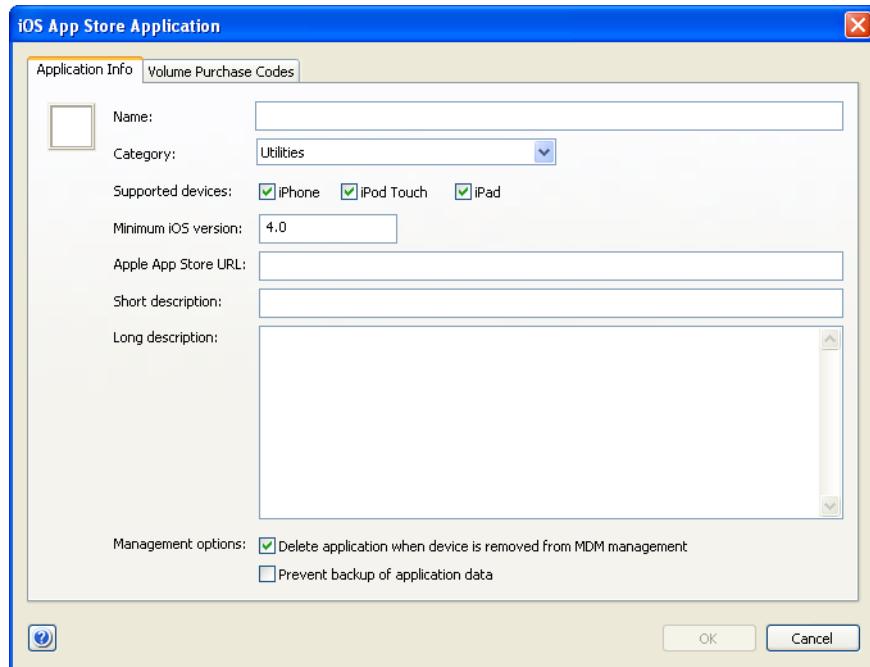
This command opens the **iOS App Store Application** dialog in which you can specify a new application package for an application from the App Store.

The dialog includes two tabs:

- **Application Info tab** (page 395)
- **Volume Purchase Codes tab** (page 396)

Application Info tab

The **Application Info** tab lets you specify the app and its important parameters.



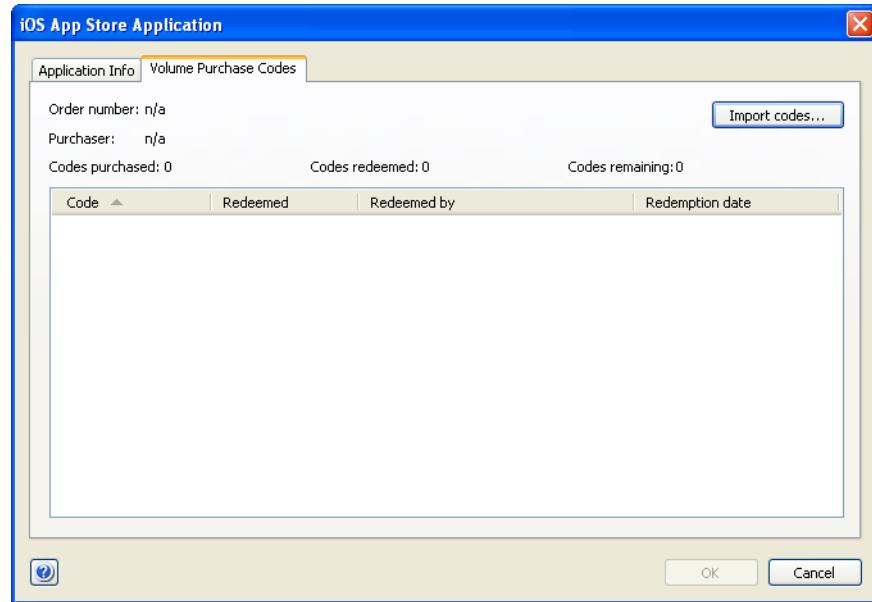
The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the App Store URL is specified but you can paste in a custom graphic.
- **Name:** The name for the package. This name is displayed in AbsoluteApps.
- **Category:** The App Store category to which the app belongs.
- **Platform:** The iOS hardware platforms on which the app can run.
- **Minimum iOS version:** The minimum version of iOS required to run this app.
- **Apple App Store URL:** The URL of the App Store page for this app.
You can obtain the URL by right-clicking the app's icon anywhere in Apple's App Store and choosing **Copy Link** from the context menu.
- **Short description:** A brief description of the application. This description is displayed in AbsoluteApps.
- **Long description:** A more extensive description of the application. This description is displayed in AbsoluteApps.
- **Delete application when device is removed from MDM management:** If this option is checked, the app will automatically be deleted from any device on which it is installed when that device is no longer under MDM management. If the option is unchecked, removing a device from management leaves the app untouched on it.
- **Prevent backup of application data:** If this option is checked, any data belonging to this app that is stored on the device is

not included in iTunes or iCloud backups of the device. If the option is unchecked, the application data is backed up normally.

Volume Purchase Codes tab

The **Volume Purchase Code** tab lets you import and manage available App Store volume purchase program redemption codes.



The dialog contains these elements:

- **Order number:** The order number for the redemption code purchase.
- **Purchaser:** The user through whose App Store account the codes were purchased.
- **Codes purchased:** The total number of redemption codes purchased for this app.
- **Codes redeemed:** The number of codes for this app that have already been redeemed.
- **Codes remaining:** The number of redemption codes for this app that have not yet been redeemed.
Codes purchased is always the sum of codes redeemed and codes remaining.
- **Import Codes:** Clicking this button let you import redemption codes into the app package definition. It opens a standard Open dialog where you can choose a text file in one of the following formats:
 - A file exported from the Excel file with the purchased code you received from Apple.
To create this file, open the Excel file and save it as tab-delimited text. Files of this type must begin with two asterisks (**).
 - A standard tab-delimited text file.

Files of this type contain in each line a redemption code followed by a tab and the redemption link. This kind of file must not begin with a double asterisk.

The codes in the imported file are appended to the list of codes in the dialog.

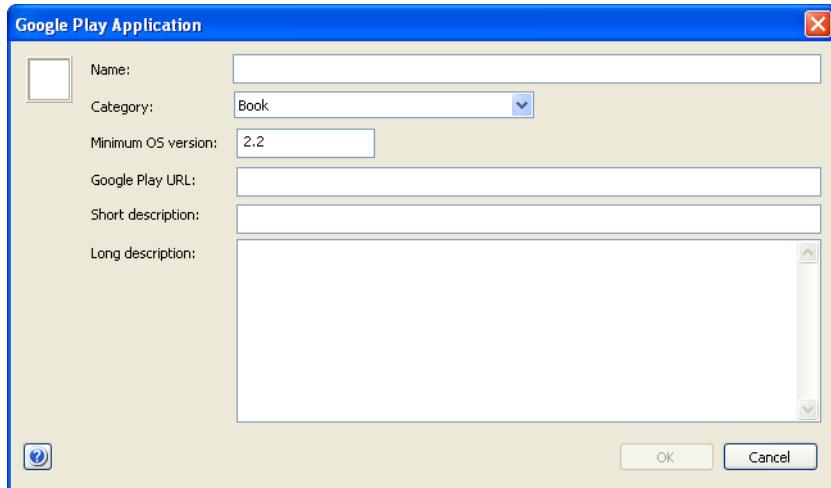
The list that takes up the main part of the dialog lists all redemption code for this app package. It contains these columns:

- **Code:** The redemption code.
- **Redeemed:** Whether this code has already been redeemed.
- **Redeemed by:** The device on which this code was redeemed.
- **Redemption date:** The date on which the code was redeemed.

Pasting text that conforms to the two supported import file formats into the list enters the codes just as if they had been imported.

New Google Play Application Package

This command opens the **Google Play Application** dialog in which you can specify a new application package for an application from the Android Market (Google Play).



The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the Google Play URL is specified but you can paste in a custom graphic.
- **Name:** The name for the package. This name is displayed in AbsoluteApps.
- **Category:** The Google Play category to which the app belongs.
- **Minimum OS version:** The minimum version of Android required to run this app.
- **Google Play URL:** The URL of the Google Play page for this app.

You can obtain the URL by right-clicking the app's icon anywhere in Google Play and choosing **Copy Link** from the context menu.

- **Short description:** A brief description of the application. This description is displayed in AbsoluteApps.
- **Long description:** A more extensive description of the application. This description is displayed in AbsoluteApps.

Duplicate Application Package

This command opens the selected mobile application package in the **Mobile Application** dialog with a new name. You can edit the settings as desired and save the duplicate.

See "New In-house Application Package" on page 393 for details of the dialog.

New Smart Group: In-house Application Packages

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile in-house application packages defined in Absolute Manage.

For details, see "New Smart Group" on page 369.

New Smart Group: App Store Application Packages

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for App Store and Android Market (Google Play) application packages defined in Absolute Manage.

For details, see "New Smart Group" on page 369.

New Smart Group: iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for provisioning profiles that are present on administered iOS devices.

For details, see "New Smart Group" on page 369.

New Smart Group: Installed Applications

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for applications installed on managed mobile devices.

For details, see "New Smart Group" on page 369.

New Smart Group: Installed Application Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for installed application statistics.

For details, see “New Smart Group” on page 369.

New Smart Group: Mobile Devices by Installed Software

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that lists mobile devices based on what software is or is not installed on them.

For details, see “New Smart Group” on page 369.

New Smart Group: Installed iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for provisioning profiles that are present on administered mobile devices.

For details, see “New Smart Group” on page 369.

New Smart Group: Installed iOS Provisioning Profiles Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for installed provisioning profile statistics.

For details, see “New Smart Group” on page 369.

New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for iOS devices based on which provisioning profiles are or are not installed on them.

For details, see “New Smart Group” on page 369.

Configuration Profiles and Certificates

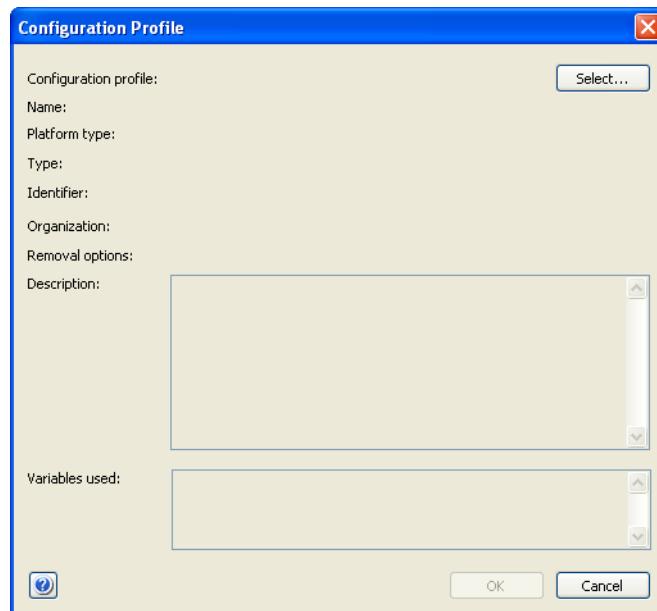
The Mobile Applications submenu contains commands for working with configuration profiles:

- “New Configuration Profile” on page 400
- “New Smart Group: Configuration Profiles” on page 401
- “New Smart Group: Installed Configuration Profiles” on page 401
- “New Smart Group: Installed Configuration Profiles Statistics” on page 401
- “New Smart Group: Mobile Devices by Installed Configuration Profiles” on page 402
- “New Smart Group: Installed Certificates” on page 402
- “New Smart Group: Installed Certificates Statistics” on page 402
- “New Smart Group: Mobile Devices by Installed Certificates” on page 402

New Configuration Profile

This command opens the **Configuration Profile** dialog in which you can specify a new configuration profile.

The **Configuration Profile** dialog lets you import a configuration profile into Absolute Manage that can then be distributed to administered mobile devices.



The dialog contains these elements:

- **Configuration profile:** The file containing the configuration profile. Clicking the **Select** button lets you select the file on your computer.

Configuration profiles are created in Apple's iPhone Configuration Utility.

- **Name:** The name of the profile. The name is automatically read from the profile and cannot be changed in Absolute Manage.
- **Platform type:** The operating system to which the profile applies. The type is automatically detected and cannot be changed in Absolute Manage.
- **Type:** The kind of profile – device or app profile.
- **Identifier:** The identifier of the profile. The identifier is automatically read from the profile and cannot be changed in Absolute Manage.
- **Organization:** The organization of the profile. The identifier is automatically read from the profile and cannot be changed in Absolute Manage.
- **Removal options:** Whether the local user of the mobile device can remove the profile and whether a passcode is required for doing so.
- **Description:** A description of the profile. This description is displayed to the user of the managed mobile device.
- **Variables used:** The variables used in this profile that will be replaced with actual values during the installation. (See "Creating configuration profiles containing variables" on page 143 for information on using variables in profiles.)

New Smart Group: Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for configuration profiles defined in Absolute Manage.

For details, see "New Smart Group" on page 369.

New Smart Group: Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for configuration profiles installed on managed mobile devices.

For details, see "New Smart Group" on page 369.

New Smart Group: Installed Configuration Profiles Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for statistics on configuration profiles installed on administered mobile devices.

For details, see "New Smart Group" on page 369.

New Smart Group: Mobile Devices by Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices based on the configuration profiles that are or are not installed on them.

For details, see “New Smart Group” on page 369.

New Smart Group: Installed Certificates

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for certificates installed on managed mobile devices.

For details, see “New Smart Group” on page 369.

New Smart Group: Installed Certificates Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for statistics on certificates installed on administered mobile devices.

For details, see “New Smart Group” on page 369.

New Smart Group: Mobile Devices by Installed Certificates

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices based on which certificates are or are not installed on them.

For details, see “New Smart Group” on page 369.

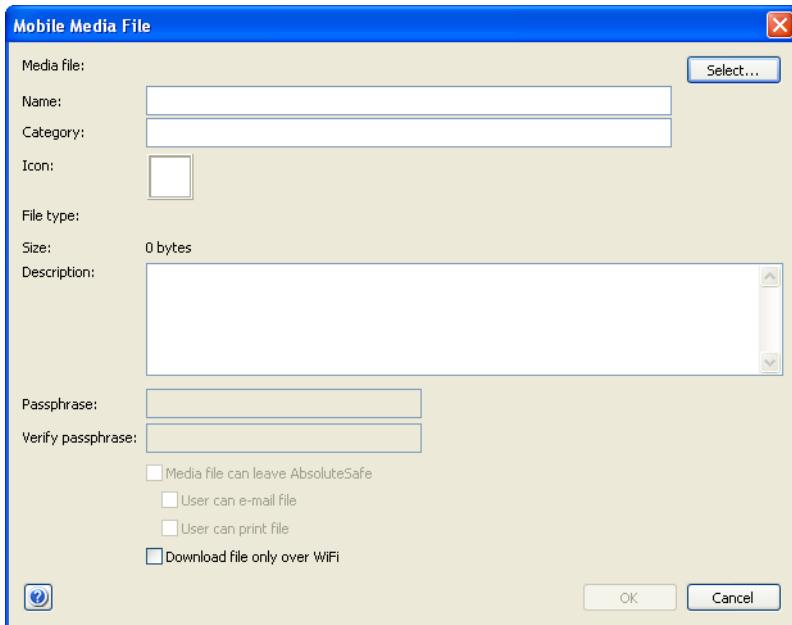
Media

The **Media** submenu contains commands for working with media objects:

- “New Media File” on page 403
- “Duplicate Media File” on page 404
- “New Smart Group: Media Files” on page 405

New Media File

This command opens the **Mobile Media File** dialog in which you can specify a media file that is to be made available to managed mobile devices:



The dialog contains these elements:

- **Media file:** The file you want to make available. Clicking the **Select** button lets you choose a file. (Holding down the Shift key while clicking **Select** lets you choose a folder of media files.) You can also drag a file or folder from the desktop into this area to choose it.
- **Name:** The name under which the file appears on managed mobile devices. This field is deactivated when a folder is selected; the name is in that case automatically set from the filename.
- **Category:** The category in which it is displayed by AbsoluteSafe on the managed device. This field is prepopulated by Absolute Managed based on the kind of file selected, but you can enter any desired category name. If the category does not yet exist, AbsoluteSafe will create it. If you have selected a folder (instead of a single file), you can leave the category free to have Absolute Manage automatically assign a category to each file depending on its file type or enter a category that is applied to all files contained in the folder.
- **Icon:** The icon that is displayed for the media file on the managed mobile devices. The icon is automatically created based on the type of the selected file, but you can also paste any graphic into this field.
- **File type:** The type of the selected file. If you have selected a folder instead of a single file, "Batch upload" is displayed.

- **Size:** The file size in bytes.
- **Description:** A description of the file for the mobile users. This description is displayed in AbsoluteSafe.
- **Passphrase:** When you enter text into this field, the media file is only displayed when the user enters the same text on the mobile device.
- **Verify passphrase:** Repeat the passphrase to guard against typos.
- **Media file can leave AbsoluteSafe:** If you check this option, users of mobile devices can open the file in an app other than AbsoluteSafe, for example, to view it in a PDF reader or to mail it to somebody else.

Two other options become available:

- **User can e-mail file:** If this option is checked, a button for sending this file by e-mail appears in AbsoluteSafe.
- **User can print file:** If this option is checked, a button for printing this file appears in AbsoluteSafe.

If this option is unchecked, mobile users can view the file only in AbsoluteSafe.

If you have selected an entire folder of files (instead of a single file), this setting does not apply to files that cannot be displayed in AbsoluteSafe (see “Supported media types” on page 169 for a complete list): These files are always allowed to leave AbsoluteSafe because otherwise there would be no way for the mobile users to view them.

Note: While unchecking this option reliably prevents the file from leaving AbsoluteSafe, the same is not necessarily true for the information contained in the file. For example, a mobile user still could take screenshots of the file and send those to other persons.

- **Download file only over WiFi:** If you check this option, AbsoluteSafe will download the file only if the mobile device is on a WiFi-connection, not when it is connected over a mobile data connection such as 3G (UMTS) or LTE.

This setting is ignored by versions of AbsoluteSafe earlier than 1.1.

Clicking **OK** saves the media file in Absolute Manage. It can then be assigned to a policy to make it available to mobile users.

Duplicate Media File

This command creates a duplicate of the selected media file record, removes the media file from it, and opens the **Mobile Media File** dialog.

In the dialog, the **Category**, **Description**, and **Media file can leave AbsoluteSafe** settings are preserved. You can select a new media file to fill the other fields and enter a new name for the duplicated media file object.

For a description of the **Mobile Media File** dialog, see above.

New Smart Group: Media Files

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile media files.

For details, see “New Smart Group” on page 369.

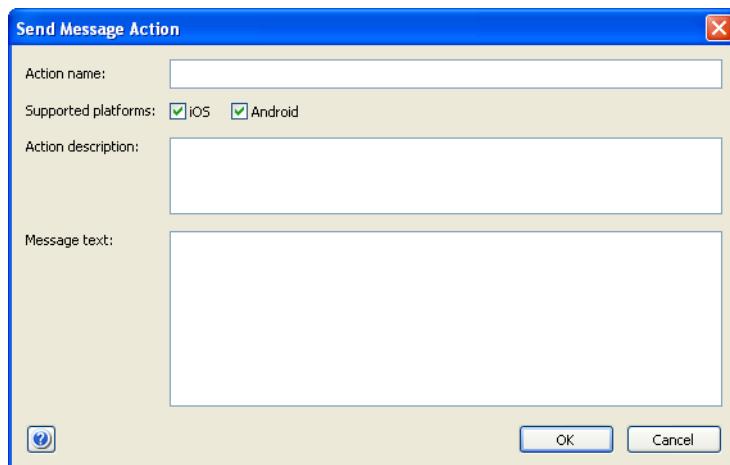
Actions

The **Actions** submenu contains commands for working with actions that can be assigned to smart policies:

- “New Send Message to Device Action” on page 405
- “New Send E-mail Action” on page 407
- “New Send SMS (Text Message) Action” on page 409
- “New Set Roaming Options Action” on page 410
- “New Update Device Info Action” on page 411
- “New Freeze Device Action” on page 412
- “New Remove Configuration Profile Action” on page 413
- “New Demote to Unmanaged Device Action” on page 413
- “Duplicate Action” on page 414
- “New Smart Group: Actions” on page 414

New Send Message to Device Action

This command opens the **Send Message Action** dialog in which you can specify a message that is to be sent to mobile devices that become members of a policy:



The dialog contains these elements:

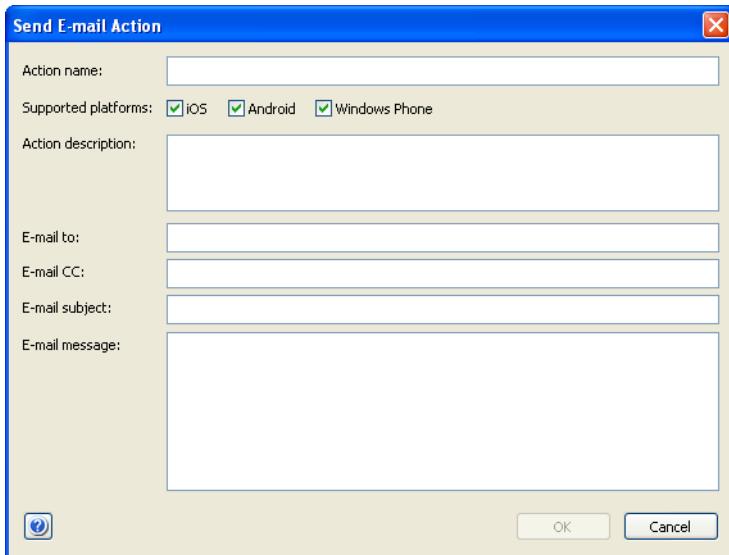
- **Action name:** The name under which the action is stored in Absolute Manage.
- **Supported platforms:** The mobile device platforms to which you want the action to apply.

- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **Message text:** The text that is sent to managed mobile devices that trigger the action. The message appears on-screen on the mobile device.
You can use these variables in the message text, which Absolute Manage replaces with the actual information for the device when the message is sent:
 - MD_CurrentCarrierNetwork: Content of the Mobile Device Current Carrier Network information item
 - MD_DeviceModel: Content of the Mobile Device Model item
 - MD_DeviceName: Content of the Mobile Device Name information item
 - MD_HomeCarrierNetwork: Content of the Mobile Device Home Network information item
 - MD_IMEI: Content of the Mobile Device IMEI/MEID information item
 - MD_PhoneNumber: Content of the Mobile Device Phone Number information item
 - MD_SerialNumber: Content of the Mobile Device Serial Number information item
 - MD_LastMDMHeartbeat: Content of the Mobile Device Last Contact information item
 - MD_WifiIPAddress: Content of the Mobile Device WiFi IP Address information item
 - MD_CellIPAddress: Content of the Mobile Device Cell IP Address information item
 - MD_IPAddress: Content of the Mobile Device Public IP Address information item
 - MD_Model: Content of the Mobile Device Model Number information item
 - MD_OSVersion: Content of the Mobile Device OS Version information item
 - MD_WifiMACAddress: Content of the Mobile Device WiFi MAC Address information item
 - MD_IsJailbroken: Content of the Mobile Device Jailbroken information item
 - MD_PasscodePresent: Content of the Mobile Device Passcode Present information item
 - MD_IsRoaming: Content of the Mobile Device Is Roaming information item
 - MD_DataRoamingEnabled: Content of the Mobile Device Data Roaming Enabled information item
 - MD_VoiceRoamingEnabled: Content of the Mobile Device Voice Roaming Enabled information item

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Send E-mail Action

This command opens the **Send E-mail Action** dialog in which you can specify an e-mail that is to be sent when mobile devices become members of a policy:



The dialog contains these elements:

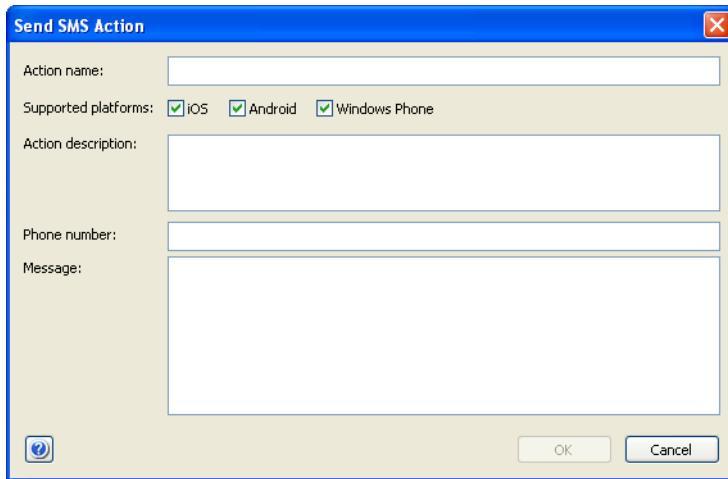
- **Action name:** The name under which the action is stored in Absolute Manage.
- **Supported platforms:** The mobile device platforms to which you want the action to apply. (Actions cannot be applied to Windows Phone devices.)
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **E-mail to:** The e-mail address to which the e-mail is to be sent.
- **E-mail cc:** The e-mail addresses to which the e-mail is to be copied, if any.
- **E-mail subject:** The subject of the e-mail.
- **E-mail message:** The body of the e-mail.
You can use these variables in the e-mail text, which Absolute Manage replaces with the actual information for the device when the message is sent:
 - MD_CurrentCarrierNetwork: Content of the Mobile Device Current Carrier Network information item
 - MD_DeviceModel: Content of the Mobile Device Model item
 - MD_DeviceName: Content of the Mobile Device Name information item
 - MD_HomeCarrierNetwork: Content of the Mobile Device Home Network information item
 - MD_IMEI: Content of the Mobile Device IMEI/MEID information item

- MD_PhoneNumber: Content of the Mobile Device Phone Number information item
- MD_SerialNumber: Content of the Mobile Device Serial Number information item
- MD_LastMDMHeartbeat: Content of the Mobile Device Last Contact information item
- MD_WifiIPAddress: Content of the Mobile Device WiFi IP Address information item
- MD_CellIPAddress: Content of the Mobile Device Cell IP Address information item
- MD_IPAddress: Content of the Mobile Device Public IP Address information item
- MD_Model: Content of the Mobile Device Model Number information item
- MD_OSVersion: Content of the Mobile Device OS Version information item
- MD_WifiMACAddress: Content of the Mobile Device WiFi MAC Address information item
- MD_IsJailbroken: Content of the Mobile Device Jailbroken information item
- MD_PasscodePresent: Content of the Mobile Device Passcode Present information item
- MD_IsRoaming: Content of the Mobile Device Is Roaming information item
- MD_DataRoamingEnabled: Content of the Mobile Device Data Roaming Enabled information item
- MD_VoiceRoamingEnabled: Content of the Mobile Device Voice Roaming Enabled information item

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Send SMS (Text Message) Action

This command opens the **Send SMS Action** dialog in which you can specify an SMS text message that is to be sent when mobile devices become members of a policy:



The dialog contains these elements:

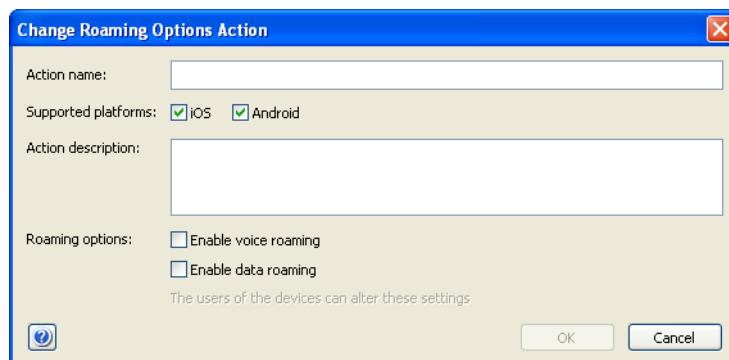
- **Action name:** The name under which the action is stored in Absolute Manage.
- **Supported platforms:** The mobile device platforms to which you want the action to apply. (Actions cannot be applied to Windows Phone devices.)
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **Phone number:** The telephone number to which the SMS text message is to be sent. When you enter multiple phone numbers separated by commas, the text message is sent to all of them.
- **Message:** The message that is going to be sent. The message may be up to 140 characters long.
You can use these variables in the message text, which Absolute Manage replaces with the actual information for the device when the message is sent:
 - MD_CurrentCarrierNetwork: Content of the Mobile Device Current Carrier Network information item
 - MD_DeviceModel: Content of the Mobile Device Model information item
 - MD_DeviceName: Content of the Mobile Device Name information item
 - MD_HomeCarrierNetwork: Content of the Mobile Device Home Network information item
 - MD_IMEI: Content of the Mobile Device IMEI/MEID information item
 - MD_PhoneNumber: Content of the Mobile Device Phone Number information item

- MD_SerialNumber: Content of the Mobile Device Serial Number information item
- MD_LastMDMHeartbeat: Content of the Mobile Device Last Contact information item
- MD_WifiIPAddress: Content of the Mobile Device WiFi IP Address information item
- MD_CellIPAddress: Content of the Mobile Device Cell IP Address information item
- MD_IPAddress: Content of the Mobile Device Public IP Address information item
- MD_Model: Content of the Mobile Device Model Number information item
- MD_OSVersions: Content of the Mobile Device OS Version information item
- MD_WifiMACAddress: Content of the Mobile Device WiFi MAC Address information item
- MD_IsJailbroken: Content of the Mobile Device Jailbroken information item
- MD_PasscodePresent: Content of the Mobile Device Passcode Present information item
- MD_IsRoaming: Content of the Mobile Device Is Roaming information item
- MD_DataRoamingEnabled: Content of the Mobile Device Data Roaming Enabled information item
- MD_VoiceRoamingEnabled: Content of the Mobile Device Voice Roaming Enabled information item

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Set Roaming Options Action

This command opens the **Change Roaming Options Action** dialog in which you can specify roaming options that are to be applied to mobile devices that become members of a policy:



The dialog contains these elements:

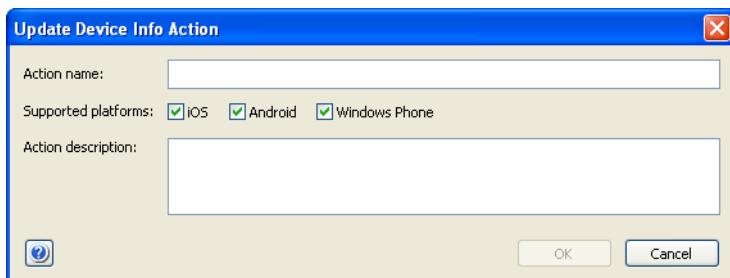
- **Action name:** The name under which the action is stored in Absolute Manage.

- **Supported platforms:** The mobile device platforms to which you want the action to apply.
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **Roaming options:** Whether to enable or disable voice and data roaming, respectively, on managed mobile devices entering a policy. Checking an option enables the respective kind of roaming on all devices, unchecking the option, disables the kind of roaming, and setting the option to the third state () leaves the roaming setting unchanged. Note that the local users of the managed mobile devices can change the roaming settings at any time.

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Update Device Info Action

This command opens the **Update Device Info Action** dialog in which you can specify that the information stored on the Absolute Manage Server for a device is updated when it becomes the member of a smart policy:



The dialog contains these elements:

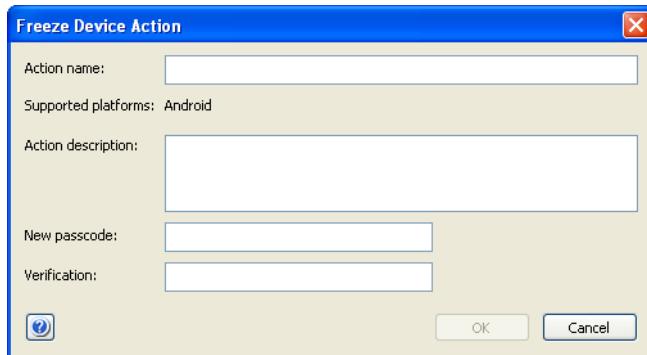
- **Action name:** The name under which the action is stored in Absolute Manage.
- **Supported platforms:** The mobile device platforms to which you want the action to apply.
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, Absolute Manage updates all information on the device that is stored on the server. This is similar to applying the **Update Device Info** command to the device.

New Freeze Device Action

This command opens the **Freeze Device** dialog in which you can specify that a device is locked and given a new passcode when it becomes the member of a smart policy:



The dialog contains these elements:

- **Action name:** The name under which the action is stored in Absolute Manage.
- **Supported platforms:** The mobile device platforms to which you want the action to apply.
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **New passcode:** The new passcode for the device. This replaces any existing passcode that there may be on the device.
- **Verification:** Repeat the new passcode.

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

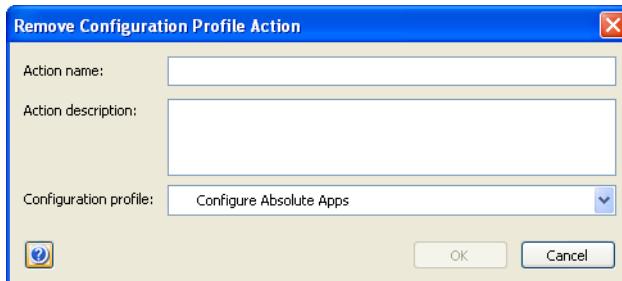
When the action is applied to a device, the device will be locked so that it is no longer accessible. At the same time the passcode is changed so that the user of the device must contact you to regain access to it.

NOTE

It may be possible to circumvent the lock by resetting the device to its factory state. However, this usually deletes all data on the device.

New Remove Configuration Profile Action

This command opens the **Remove Configuration Profile** dialog in which you can specify a configuration profile that is to be removed from a mobile device when it becomes a member of a policy:



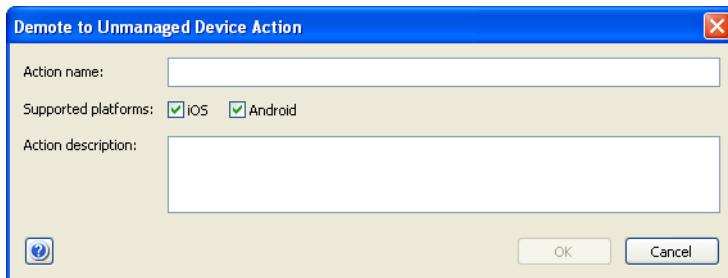
The dialog contains these elements:

- **Action name:** The name under which the action is stored in Absolute Manage.
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.
- **Configuration profile:** A list of all available configuration profiles. The chosen profile will be removed from the target devices when the action is triggered.

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Demote to Unmanaged Device Action

This command opens the **Demote to Unmanaged Device Action** dialog in which you can specify that a device is removed from MDM management when it becomes the member of a smart policy:



The dialog contains these elements:

- **Action name:** The name under which the action is stored in Absolute Manage.

- **Supported platforms:** The mobile device platforms to which you want the action to apply.
- **Action description:** A descriptive text explaining the purpose of the action. The text is displayed in Absolute Manage Admin and is intended for your own reference and that of other administrators.

Clicking **OK** saves the action in Absolute Manage. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, Absolute Manage removes the device from MDM management. This action cannot be reversed inside Absolute Manage; the device must first be enrolled anew.

Duplicate Action

This command duplicates the selected action and opens the dialog for editing it. Which dialog it opens depends on the type of the duplicated action. See “Actions” on page 405 for an overview of the available dialogs.

New Smart Group: Actions

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that includes all actions meeting the specified criteria. See “Working with actions” on page 174 for more information on actions.

For details on the **Smart Group** dialog, see “New Smart Group” on page 369.

Policies

The **Policies** submenu contains commands for working with configuration profiles:

- “New Policy” on page 415
- “New Smart Policy: Mobile Devices” on page 415
- “New Smart Policy: Mobile Devices by Installed Applications” on page 415
- “New Smart Policy: Mobile Devices by Installed Configuration Profiles” on page 415

New Policy

This command opens the **New Mobile Device Policy** dialog in which you can specify a name for a new policy.

A policy groups administered mobile with permitted and prohibited applications as well as required and prohibited configuration profiles. See “Working with policies” on page 176 for more information.

New Smart Policy: Mobile Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy that includes all mobile devices meeting the specified criteria. See “Working with policies” on page 176 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 369.

New Smart Policy: Mobile Devices by Installed Applications

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy in which you can specify mobile devices by applications that are installed or not installed on them. See “Working with policies” on page 176 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 369.

New Smart Policy: Mobile Devices by Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy in which you can specify mobile devices by configuration profiles that are installed or not installed on them. See “Working with policies” on page 176 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 369.

New Group: Mobile Devices

This command is the **New Group** command standard to all browser windows. It creates a group for mobile devices.

New Smart Group: Mobile Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices.

For details, see “New Smart Group” on page 369.

New Smart Group: Command Queue

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for entries in the command queue.

For details, see “New Smart Group” on page 369.

New Smart Group: Command History

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for entries in the command history.

For details, see “New Smart Group” on page 369.

New Category

This command is the **New Category** command standard to all browser windows.

For details, see “New Category” on page 369.

Rename <item>

This command lets you edit the name of the selected item in the sidebar of the **Mobile Devices** window.

Edit <item>

This command lets you edit the selected items from the **Mobile Devices** window. The items are opened in the dialog in which they were created; see these dialogs’ descriptions for details.

Remove <item>

This command lets you remove the selected items from the Mobile Devices window. Not all objects can be removed.

Table context menu

The context menus for the table area of the **Mobile Devices** window contains commands for working with the items displayed and controlling mobile devices.

Depending on the content displayed in the table area, different commands are included in the context menu.

These commands may appear:

- “Copy” on page 418
- “Copy “<information item>”” on page 418
- “New Smart Mobile Device Group from “<information item>”” on page 419
- “New Smart Policy from “<information item>”” on page 419
- “New Smart Application Group from “<information item>”” on page 419
- “New Smart Configuration Profiles Group from “<information item>”” on page 420
- “New Smart Provisioning Profiles Group from “<information item>”” on page 420
- “New Smart Media Files Group from “<information item>”” on page 420
- “New Command Queue Smart Group from “<information item>”” on page 421
- “New Command History Smart Group from “<information item>”” on page 421
- “New Policy with Selected Devices” on page 421
- “Install Configuration Profile” on page 422
- “Install Provisioning Profile” on page 422
- “Install Application” on page 422
- “Issue Device Lock” on page 422
- “Issue Clear Passcode” on page 422
- “Issue Remote Erase” on page 422
- “Set Roaming Options” on page 422
- “Send Message to Device” on page 422
- “Set Device Name” on page 423
- “Delete Application” on page 423
- “Delete Profile” on page 423
- “Update Device Info” on page 424
- “Show Detail View” on page 424
- “Synchronize Records” on page 424
- “Enter Custom Field Data” on page 424
- “Import Custom Field Data” on page 424
- “Ignore Devices” on page 425
- “Reset All Ignored Devices” on page 425
- “Re-execute All Actions for This Device” on page 425
- “Re-execute This Action for This Device” on page 425
- “Retry All Failed Profiles” on page 425
- “Remove from Group” on page 426
- “Remove from Policy” on page 426
- “Track Device” on page 426
- “Get Device Geolocation” on page 426

- “Reset Tracking Passphrase” on page 426
- “Show Location on Google Maps” on page 426
- “Show Location on Bing Maps” on page 426
- “Set Device Ownership” on page 427
- “Send Re-enrollment Message to Device” on page 427
- “Update Installed Application Statistics” on page 428
- “Show Mobile Application Package Details” on page 428
- “New Mobile Application Package” on page 428
- “New iOS App Store Application Package” on page 428
- “New Google Play Application Package” on page 428
- “Edit Mobile Application Package” on page 428
- “Duplicate Mobile Application Package” on page 428
- “Remove Mobile Application Package” on page 429
- “Show Configuration Profile Details” on page 429
- “New Configuration Profile” on page 429
- “Edit Configuration Profile” on page 429
- “Remove Configuration Profile” on page 429
- “Remove Configuration Profile from Policy” on page 429
- “Show Provisioning Profile Details” on page 429
- “Show Media File Details” on page 430
- “Set Availability Time” on page 430
- “New Media File” on page 431
- “Edit Media File” on page 431
- “Remove Media File” on page 431
- “Show Action Details” on page 431
- “Duplicate Action” on page 431
- “Edit Action” on page 432
- “Remove Action” on page 432
- “Re-execute This Action for All Devices” on page 432
- “Re-execute This Action for This Policy” on page 432
- “New Send Message Action” on page 432
- “New Send E-mail Action” on page 432
- “New Send SMS (Text Message) Action” on page 432
- “New Set Roaming Options Action” on page 433
- “New Freeze Device Action” on page 433
- “New Remove Configuration Profile Action” on page 433
- “New Demote to Unmanaged Device Action” on page 433
- “Change Action Schedule” on page 433
- “Remove Action from Policy” on page 434
- “Show Policy Members” on page 434
- “Remove Policy” on page 434

Copy

This command is the **Copy** command from the **Edit** menu.

For details, see “Copy” on page 273.

Copy “<information item>”

This command is the **Copy “<information item>”** command standard to all browser windows.

For details, see “Copy “<information item>”” on page 372.

New Smart Mobile Device Group from “<information item>”

This command is the **New Smart Group from “<information item>”** command standard to all browser windows.

For details, see “New Smart Group from “<information item>”” on page 372.

New Smart Policy from “<information item>”

Choosing this command lets you create a mobile device policy with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart policy.

For details on the dialog, see “New Smart Group” on page 369. For more information on policies, see “Working with policies” on page 176.

New Smart Application Group from “<information item>”

Choosing this command lets you create a smart group for application packages with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Smart Configuration Profiles Group from “<information item>”

Choosing this command lets you create a smart group for configuration profiles with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Smart Provisioning Profiles Group from “<information item>”

Choosing this command lets you create a smart group for provisioning profiles with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Smart Media Files Group from “<information item>”

Choosing this command lets you create a smart group for media files with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Command Queue Smart Group from “<information item>”

Choosing this command lets you create a smart group for command queue entries with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Command History Smart Group from “<information item>”

Choosing this command lets you create a smart group for command history entries with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 369.

New Policy with Selected Devices

Choosing this command lets you create a new policy that already contains the selected mobile devices.

Choosing the command opens the **New Mobile Device Policy** dialog in which you can specify the name for the new policy.

Install Configuration Profile

This is the same command as **Install Configuration Profile** on page 334.

Install Provisioning Profile

This is the same command as **Install Provisioning Profile** on page 335.

Install Application

This is the same command as **Install Application** on page 335.

Issue Device Lock

This is the same command as **Issue Device Lock** on page 336.

Issue Clear Passcode

This is the same command as **Issue Clear Passcode** on page 337.

Issue Remote Erase

This is the same command as **Issue Remote Erase** on page 338.

Set Roaming Options

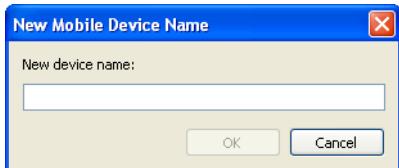
This is the same command as **Set Roaming Options** on page 338.

Send Message to Device

This is the same command as **Send Message to Device** on page 339.

Set Device Name

Choosing this command opens the **New Mobile Device Name** dialog in which you can assign a name to a selected Android device:



The dialog contains this element:

- **New device name:** The name in this field will be assigned to the device.

This command applies only to Android devices.

Delete Application

Choosing this command removes the selected applications from the mobile devices on which they are installed.

This command can be used only to delete installed applications, such as when the list of applications on a particular device or the list of all applications are displayed.

Which applications can be removed depends on the mobile OS:

- iOS 4.x: No applications can be removed.
- iOS 5.0 and later: Managed applications can be removed, i.e., applications that have been installed through the MDM system. No user confirmation is required.
- Android: Any application can be removed. The local user must confirm the removal, except on devices that support persistence.
- Windows Phone: Deleting applications is not supported.

Delete Profile

Choosing this command removes the selected configuration or provisioning profiles from the mobile devices on which they are installed.

This command can be used only to delete installed profiles, such as when the list of configuration profiles on a particular device or the list of all installed provisioning profiles are displayed.

Applying this command to a Windows Phone device removes its current EAS policy. This means that the default EAS policy specified on the Exchange server is applied to the device.

This command cannot be used to remove profiles from iOS 4 devices.

Update Device Info

This is the same command as **Update Device Info** on page 339.

Show Detail View

This command is the **Show Detail View** command standard to all browser windows. These commands are also similar:

- **Show Mobile Application Package Details**
- **Show Configuration Profile Details**
- **Show Provisioning Profile Details**
- **Show Media File Details**
- **Show Action Details**

These commands have the same effect as the **Details** command described on page 281.

Synchronize Records

This command is the **Synchronize Records** command standard to all browser windows.

It has the same effect as the **Synchronize Selected Records** command described on page 343.

Enter Custom Field Data

The **Enter Custom Field Data** command lets you edit the content of manual custom information fields for multiple mobile devices in one step.

The command is similar to the **Enter Custom Field Data** command of browser windows, described on page 373.

Import Custom Field Data

The **Import Custom Field Data** command lets you import data from text files into manual (i.e., non-dynamic) custom information fields that have been defined for mobile devices.

The command is the same as the **Import Custom Field Data for Mobile Devices** command, described on page 271.

Ignore Devices

Choosing this command removes the selected iOS devices from the **Mobile Devices** window. Ignored devices and the applications, on them are not listed in any of the groups in the window.

This command applies only to iOS devices found because they are connected to administered computers. It does not apply to mobile devices managed through an MDM server.

Devices will be redisplayed the next time that their agents send inventory information to the server.

Reset All Ignored Devices

Choosing this command ‘unignores’ all devices that have previously been removed from the **Mobile Devices** window using the **Ignore Devices** command described above.

Re-execute All Actions for This Device

Choosing this command treats the selected device as if it was just entering all the smart policies to which it belongs. All actions specified in these policies for new devices are re-executed for this device. Any delays and repetitions specified for the actions still apply.

Re-execute This Action for This Device

Choosing this command re-executes the selected action on the displayed device. Any delays and repetitions specified for the actions still apply.

Retry All Failed Profiles

Choosing this command tries to install configuration and provisioning profiles on the selected device that failed during an earlier installation attempt. It tries to reinstall all profiles that are assigned to any policy to which the device belongs and that are not yet present on the device.

This command is intended to make it easier to install profiles that could not be installed in an earlier attempt, e.g., because they were incompatible with a device. In that case, you can fix all profiles that generated error messages and then choose **Retry All Failed Profiles** from the context menu for the device.

Remove from Group

Remove from Group

This command is the **Remove from Group** command standard to all browser windows. It is not available when a smart group is being displayed.

For details, see “Remove from Group” on page 375.

Remove from Policy

This command is similar to the **Remove from Group** command standard to all browser windows. Choosing it removes the selected devices from the policy. It is not available when a smart policy is being displayed.

Track Device

This is the same command as **Track Device** on page 339.

Get Device Geolocation

This is the same command as **Get Device Geolocation** on page 341.

Reset Tracking Passphrase

This is the same command as **Reset Tracking Passphrase** on page 341.

Show Location on Google Maps

This command displays the location of a tracked mobile device in Google Maps.

Choosing the command opens a new window in your default web browser and displays the selected location in Google Maps. If a device (instead of a recorded location of a device) is selected before choosing the command, the last known location is displayed.

This command does not support Windows Phone devices.

Show Location on Bing Maps

This command displays the location of a tracked mobile device in Bing Maps.

Choosing the command opens a new window in your default web browser and displays the selected locations in Bing Maps. If a device (instead of a recorded location of a device) is selected before choosing the command, the last known location is displayed.

This command does not support Windows Phone devices.

Set Device Ownership

Choosing this command opens the **Set Device Ownership** dialog. Using it, you can specify whether the selected device is a company-owned device or the personal device of the user:

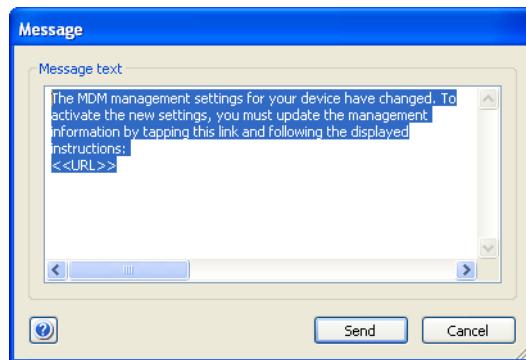


The dialog contains these elements:

- **Device is company device:** Choosing this option indicates that the device belongs to your company or organization.
- **Device is owned by user:** Choosing this option indicates that the device is privately owned by the user.

Send Re-enrollment Message to Device

Choosing this command opens the **Message** dialog. Using it, you can prompt users of managed mobile devices to re-enroll their devices, which is necessary when you have changed the MDM privileges in the **MDM** tab of the server settings:



The dialog contains this element:

- **Message text:** The text in this field will be sent to the users of the managed devices. The URL placeholder will be replaced by an individualized enrollment URL in the actual message.

Update Installed Application Statistics

This command applies only to iOS devices.

Update Installed Application Statistics

Choosing this command updates the summary information displayed in the Installed Software Statistics smart group (see “Sidebar” on page 389) to reflect the current information available on the inventory server.

This command is available only when the **Installed Software Statistics** smart group is displayed.

Show Mobile Application Package Details

This command displays the details on the selected mobile application package in the main part of the window. Choosing it is the same as clicking on the package in the sidebar of the **Mobile Devices** window.

New Mobile Application Package

This command is the same command as **New In-house Application Package**, described on page 393.

New iOS App Store Application Package

This command is the same command as **New iOS App Store Application Package**, described on page 394.

New Google Play Application Package

This command is the same command as **New Google Play Application Package**, described on page 397.

Edit Mobile Application Package

This command lets you edit the selected application package in the **Mobile Application** dialog.

See “New In-house Application Package” on page 393 for details.

Duplicate Mobile Application Package

This is the same command as **Duplicate Application Package**, described on page 398.

Remove Mobile Application Package

This command removes the selected application packages from Absolute Manage. Choosing the command when a policy is displayed removes the application only from the policy.

Show Configuration Profile Details

This command displays the details on the selected configuration profile in the main part of the window. Choosing it is the same as clicking on the profile in the sidebar of the **Mobile Devices** window.

New Configuration Profile

This is the same command as **New Configuration Profile**, described on page 400.

Edit Configuration Profile

This command lets you edit the selected application package in the **iOS Configuration Profile** dialog.

See “New Configuration Profile” on page 400 for details.

Remove Configuration Profile

This command removes the selected configuration profile from Absolute Manage.

Remove Configuration Profile from Policy

This command removes the selected configuration profile from the currently displayed policy.

Show Provisioning Profile Details

This command displays the details on the selected provisioning profile in the main part of the window. Choosing it is the same as clicking on the profile in the sidebar of the **Mobile Devices** window.

Show Media File Details

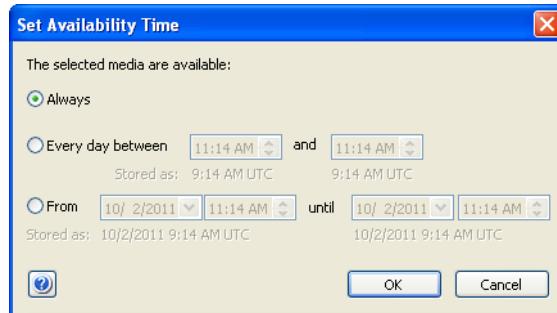
This command displays the details on the selected media file in the main part of the window. Choosing it is the same as clicking on the media file in the sidebar of the **Mobile Devices** window.

Set Availability Time

This command lets you restrict the availability of a media file or configuration profile within a policy. (It is not available when you display the media files or profiles in a subgroup of **Assignable Items**.)

The availability time set in this dialog is always specific to the policy to which the media file or profile is assigned. It does not affect the same media file or profile in other policies; and if the media file or profile is moved to a different policy, the availability time is reset.

Choosing **Set Availability Time** opens the **Set Availability Time** dialog:



The dialog contains these elements:

- **Always:** If this option is chosen, the media file is available to the members of this policy at any time.
- **Every day between:** If this option is chosen, the media file is available to the members of this policy only during a certain time of the day (for example, during office hours). The specified times refer to the local time of the Absolute Manage server. Note that you can set the start time to be later than the end time. In that case, the availability is from the beginning of the day to the end time and from the start time to the end of the day. (Think of this as a wrap-around interval crossing midnight.) For example, a start time of 9:00 and an end time of 8:00 would result in the profile being available from midnight to 8:00 and from 9:00 to midnight.

- **From:** If this option is chosen, the media file is available to the members of this policy only for the specified interval, not before or after.

NOTE Times are entered by you as local times and stored as UTC (Coordinated Universal Time, similar to GMT or Greenwich Mean Time). This means that you have to take into account any time differences between the server and mobile clients. You also have to manually compensate for daylight saving time (DST), if desired, because DST does not apply to UTC.

New Media File

This is the same command as **New Media File**, described on page 403.

Edit Media File

This command lets you edit the selected media file in the **Mobile Media File** dialog.

See “New Media File” on page 403 for details.

Remove Media File

This command removes the selected media file from Absolute Manage.

Show Action Details

This command displays the details on the selected action in the main part of the window. Choosing it is the same as clicking on the action in the **Actions** group in the sidebar of the **Mobile Devices** window.

Duplicate Action

This command opens the selected action in the appropriate **New ... Action** dialog with a new name. You can edit the settings as desired and save the duplicate.

The various action editing dialogs are described in “Actions” on page 405.

Edit Action

This command lets you edit the selected action in the appropriate **New ... Action** dialog.

The various action editing dialogs are described in “Actions” on page 405.

Remove Action

This command removes the selected action from Absolute Manage. This also removes it from any policy to which it has been assigned.

If you want to remove an action only from the policy the actions of which you are displaying, use the **Remove Action from Policy** command, described on page 434.

Re-execute This Action for All Devices

Choosing this command treats the selected action as if it has just been assigned to all the smart policies to which it is assigned. It is re-executed on all devices belonging to these policies. Any delays and repetitions specified for the action still apply.

Re-execute This Action for This Policy

Choosing this command treats the selected action as if it has just been assigned to the displayed policy. It is re-executed on all devices belonging to the policy. Any delays and repetitions specified for the action still apply.

New Send Message Action

This is the same command as **New Send Message to Device Action**, described on page 405.

New Send E-mail Action

This is the same command as **New Send E-mail Action**, described on page 407.

New Send SMS (Text Message) Action

This is the same command as **New Send SMS (Text Message) Action**, described on page 409.

New Set Roaming Options Action

This is the same command as **New Set Roaming Options Action**, described on page 410.

New Update Device Info Action

This is the same command as **New Update Device Info Action**, described on page 410.

New Freeze Device Action

This is the same command as **New Freeze Device Action**, described on page 412.

New Remove Configuration Profile Action

This is the same command as **New Remove Configuration Profile Action**, described on page 413.

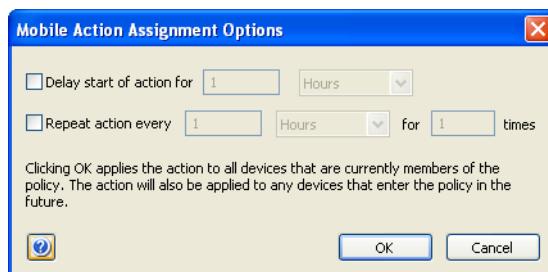
New Demote to Unmanaged Device Action

This is the same command as **New Demote to Unmanaged Device Action**, described on page 413.

Change Action Schedule

This command lets you change the delay and repetition settings for a particular action in a policy.

Choosing **Change Action Schedule** opens the **Mobile Action Assignment Options** dialog:



The dialog contains these elements:

- **Delay start of action for:** If this option is chosen, the action will not be performed immediately when a device enters the policy but the specified interval later.

- **Repeat action every:** If this option is chosen, the action is performed repeatedly on the device in the specified interval for the specified number of times. The initial execution is counted as the first repetition, so if you specify that the action is to be repeated two times, the initial action will be executed plus one more execution.

Remove Action from Policy

This command removes the selected action from the policy the actions of which you are displaying.

Show Policy Members

This command displays the devices that belong to a policy in the main part of the window. Choosing it is the same as clicking on the policy in the sidebar of the **Mobile Devices** window.

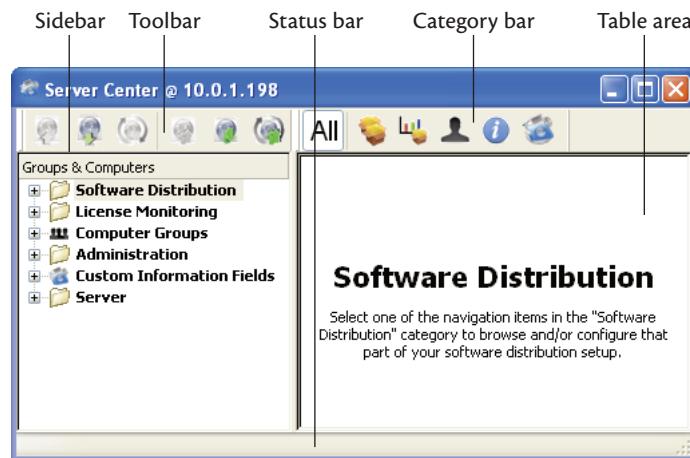
Remove Policy

This command removes the selected policy from Absolute Manage.

Chapter 20

Server Center

The Server Center is a module of the Absolute Manage system that lets you easily manage the software distribution and license monitoring capabilities of the software. You can also manage administrator accounts, configure custom information fields, and set server options. All these functions are controlled via the **Server Center** window in Absolute Manage Admin.



The elements of the **Server Center** window are described below:

- **Toolbar** (page 436)
- **Category bar** (page 437)
- **Status bar** (page 437)
- **Table columns** (page 437)
- **Sidebar** (page 437)
- **Context menus** (page 442)
 - **Software Distribution** (page 443)
 - **New Software Package** (page 443)
 - **New Metapackage** (page 453)
 - **Duplicate Software Package** (page 461)
 - **New Smart Software Package Group** (page 461)
 - **New Payload** (page 462)
 - **Duplicate Payload** (page 463)
 - **New Smart Payload Group** (page 464)
 - **New Distribution Point** (page 464)
 - **New Smart Distribution Points Group** (page 466)
 - **New Disk Image** (page 467)
 - **New Smart Disk Image Group** (page 468)
 - **New Smart Installation Status Group** (page 469)
 - **New Missing Software Packages Group** (page 469)
 - **License Monitoring** (page 470)
 - **New License Specification** (page 470)
 - **New Smart License Specification Group** (page 476)
 - **New License Status Report** (page 477)
 - **New Software Usage Report** (page 477)
 - **New History Report** (page 478)
 - **New History Summary Report** (page 478)

- **New Missing Software Report** (page 478)
- **Computer Groups** (page 478)
 - **New Computer Group** (page 478)
 - **New Smart Computer Group** (page 479)
 - **Remove All Group Members** (page 480)
- **Administrator Setup** (page 480)
 - **New Administrator** (page 481)
 - **Remove Administrator from Group** (page 484)
 - **New Administrator Group** (page 484)
 - **New Computer Appointment Group** (page 485)
 - **New Smart Computer Appointment Group** (page 485)
 - **New Mobile Devices Appointment Group** (page 486)
 - **New Smart Mobile Devices Appointment Group** (page 487)
 - **New Smart Administrator Group** (page 488)
 - **Refresh** (page 488)
- **Custom Information Fields** (page 489)
 - **New Custom Information Field** (page 489)
 - **Duplicate Custom Information Field** (page 493)
 - **Export Selected Fields** (page 493)
 - **Import Fields** (page 494)
- **Edit <item>** (page 494)
- **Remove <item>** (page 494)
- **Retrieve Payloads** (page 495)
- **Retry Package** (page 495)
- **Reset Package** (page 495)
- **Install Selected Software Packages** (page 496)
- **Repeat Selected Installations** (page 496)
- **Reset Current Server Load** (page 496)
- **Server Settings** (page 497)
- **Server Monitor** (page 508)

Toolbar

The **Server Center** window toolbar lets you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Category bar

The **Server Center** window contains a category bar that lets you restrict the display in the window to one or a few of the categories listed in the sidebar.



Clicking each category toggles its display on or off. If all categories are off in the category bar, all categories are displayed. You can activate display of each category independently of the others, for example, displaying custom information fields together with the server setup.

NOTE Clicking a category with the Shift key held down restricts the display in the window to that category.

Computer groups are displayed if either **Software Distribution** or **License Monitoring** is activated; they cannot be displayed or hidden on its own.

Status bar

The **Server Center** window has a status bar displaying information on the state of the Server Center.

The status bar displays the number of records currently shown in the window. In addition, it displays note icons when the settings in the window have been modified locally and the changes have not yet saved to the server:



Table columns

The columns displayed in the **Server Center** change depending on the object selected in the sidebar.

The columns display information items applicable to the category selected in the sidebar or a custom information view similar to a dialog. Columns can be configured as for other browser windows. (Configuring columns is described in “Opening and configuring browser windows” on page 103.)

Sidebar

The **Server Center** window contains a sidebar with a number of categories and smart groups custom-made for using the Server

Center's functions. The smart groups are divided into several categories; there are also settings categories.

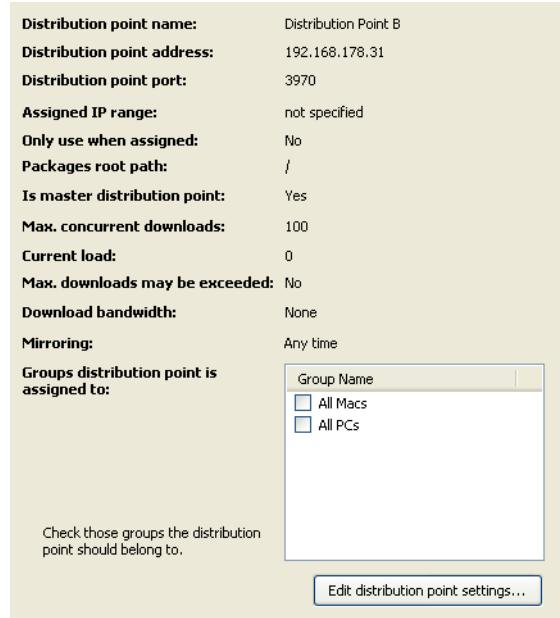
Software Distribution

This category contains several subcategories:

- **Payloads:** All installers and installer help support files that have been defined for software distribution.
Clicking a payload displays the payload's details in the main window area. Double-clicking a payload displays the **Payload** dialog.
- **Software Packages:** All software packages and metapackages that have been defined for software distribution.
Clicking a package or metapackage displays its settings in the main window area. You can check groups to assign the package to these groups. Holding down the Alt and Ctrl keys checks or unchecks all groups in the list.
Double-clicking a metapackage opens the **Software Distribution Metapackage** dialog. Double-clicking a software package opens the **Software Distribution Package** dialog.
Clicking a payload displays the file contained in the payload.
Double-clicking a payload file displays the **Payload** dialog.
- **Mac OS Patches:** All software packages that have automatically been created by the operating system patch management for Mac OS X clients. (Details are available in "Automated patch management" on page 235.)
 - **Accepted Patches:** Automatically created patch software packages that have been accepted by an administrator.
 - **Rejected Patches:** Automatically created patch software packages that an administrator has decided should not be installed on client Mac OS X computers.
 - **Unconfirmed Patches:** Automatically created patch software packages that no administrator has yet decided on.
Within these categories, patches are further grouped according to the version of Mac OS X to which they apply.
Some patches may apply to more than one version. In this case, they are listed in all applicable subgroups. Deleting the patch from any of those groups deletes it from all others as well.
Clicking a patch displays its details in the **Server Center** window's table area. Double-clicking a patch opens it in an editing dialog similar to the one described in **New Software Package** (page 443).
- **Windows Patches:** All software packages that have automatically been created by the operating system patch management for Windows clients. (Details are available in "Automated patch management" on page 235.)
The subcategories are the same as for **Mac OS Patches**, described above. Patches for Windows are also subgrouped according to the Windows version for which they are intended.
- **Mac OS Disk Images:** All disk images for Mac OS clients that have been defined for software distribution.

Clicking a disk image displays its details in the main window area. Double-clicking it opens the **Disk Image** dialog.

- **Windows Disk Images:** All disk images for Windows clients that have been defined for software distribution.
 - **Distribution Points:** All distribution points that have been defined for software distribution.
- Clicking a distribution point displays its settings and an editable list of groups to which it is assigned:



Checking a group assigns the distribution point to it, unchecking the group unassigns the distribution point. When a distribution point is assigned to a group, computers from that group download installers preferably from that distribution point.

Note: Holding down the Alt and Ctrl keys while clicking a checkbox in the list of assigned groups checks or unchecks all groups in the list.

Double-clicking a distribution point displays its settings in the **Distribution Point** dialog.

- **Installation Status:** This is a collection of smart groups that contain installation processes by their states:
 - **General log:** All installation processes, whether scheduled, under way, or completed.
 - **Installations in Progress:** Installation processes that have begun but are not yet completed.
 - **Successful Installations:** Installation processes that have been completed with the successful installation of the software.
 - **Failed Installations:** Installation processes that have been terminated without successfully installing the software.
 - **Deferred Installations:** Installation processes that were scheduled for a time in the past but had to be deferred because the target computer could not be contacted.
 - **Refused Installations:** Installation processes that failed because the user of the target computer declined the installation.

Clicking any subcategory displays all installation processes that are part of the category.

License Monitoring

- **License Specifications:** All license specifications that have been defined for license monitoring.
Clicking a license specification displays its details in the main window area. Double-clicking it opens the **License Specification** dialog.
- **License Purchases:** All license specifications for which license purchases that have been entered.
Clicking a license specification here displays the specification's purchasing details in the main window area. Double-clicking it opens the **License Specification** dialog.
- **Reports:** This is a collection of smart groups that contain license specifications by their states and other reports:
 - Selecting the **Reports** group itself displays all license specifications, regardless of status.
 - **Fully compliant:** All software licenses that are not exceeded.
 - **Licenses exceeded:** All software licenses that are used more often than the number of licenses in the license specification allows.
 - **Prohibited software:** All found software instances that are prohibited according to its license specifications. Each agent has one entry per type of prohibited software that was detected on it.
 - **Undetermined licenses:** All license specifications that have been defined and saved to the Absolute Manage Server, but which no agent has yet checked for.
 - **Software usage:** All found software instances on all agents. Each agent has one entry per licensed software that was detected on it.
 - **Missing software:** License specifications that are assigned to a computer group but not present on all computers of each group to which they have been assigned. There is one entry per missing software per agent.
 - **History:** List of all license monitoring counts. Each count is timestamped. There is one entry for each license specification per reporting date.
 - **History summary:** A statistical overview of the license usage in the past.

Clicking any of the subcategories displays the items that belong to it.

Computer Groups

This category contains all computer groups that have been defined. It also creates a few predefined smart groups:

- **All Macs:** All administered computers running Mac OS X.

- **Assigned Packages:** All packages that are assigned to the group.
Clicking the subcategory displays all assigned packages.
- **Assigned License Specifications:** All license specifications that are assigned to the group.
Clicking the subcategory displays all assigned license specifications.
- **Assigned Distribution Points:** All distribution points that are assigned to the group. Assigning distribution points to a group tells the Absolute Manage Agents in the group to prefer these distribution points for installer downloads.
Clicking the subcategory displays all assigned distribution points.
- **All PCs:** All administered computers running Windows.
This smart group contains the same subgroups as **All Macs**, described above.
- **Unassigned Computers:** All administered computers that are not part of any computer group.
Clicking the category displays all unassigned computers.

Administration

- **Active Directory:** All Active Directory accounts from the Active Directory groups that have been specified in the **Server Settings** dialog's **Active Directory** subpane.
- **Administrators:** All administrator accounts that have been defined in Absolute Manage Server and all manually managed administrator groups.
Clicking an administrator displays all agents to which it has been assigned in the main window area.
Double-clicking an administrator displays its settings in the **Administrators** dialog.
- **Appointments:** All standard and smart appointment groups. Any devices that have not been added to any appointment group are contained in the **Unmanaged Computers** and **Unmanaged Mobile Devices** groups.
Clicking an appointment group displays the devices that are part of it. Double-clicking a standard appointment group lets you edit its name; double-clicking a smart appointment group lets you edit its definition.
Clicking the **Assigned Admins** category within an appointment group displays the administrators that are part of the group.

The **Administration** category also contains all smart administrator groups that have been defined.

Clicking a smart administrator group displays all administrators who belong to it; double-clicking the group opens its definition.

Custom Information Fields

This category contains all custom information fields that have been defined.

Clicking a custom information field displays its settings in the main window area.

Server

This category groups the server-related information.

- **Server Settings:** Clicking this subcategory displays the server settings in a dialog-like format in the main part of the **Server Center** window.
This is described in “Server Settings” on page 497.
- **Server Monitor:** Clicking this subcategory displays a monitoring pane in which important server statistics are displayed.
This is described in “Server Monitor” on page 508.

Context menus

The context menus of the **Server Center** window contain commands for managing all elements of the center.

The commands are described in detail in the following sections.

- **Software Distribution** (page 443)
 - **New Software Package** (page 443)
 - **New Metapackage** (page 453)
 - **Duplicate Software Package** (page 461)
 - **New Smart Software Package Group** (page 461)
 - **New Payload** (page 462)
 - **Duplicate Payload** (page 463)
 - **New Smart Payload Group** (page 464)
 - **New Distribution Point** (page 464)
 - **New Smart Distribution Points Group** (page 466)
 - **New Disk Image** (page 467)
 - **New Smart Disk Image Group** (page 468)
 - **New Smart Installation Status Group** (page 469)
 - **New Missing Software Packages Group** (page 469)
- **License Monitoring** (page 470)
 - **New License Specification** (page 470)
 - **New Smart License Specification Group** (page 476)
 - **New License Status Report** (page 477)
 - **New Software Usage Report** (page 477)
 - **New History Report** (page 478)
 - **New History Summary Report** (page 478)
 - **New Missing Software Report** (page 478)
- **Computer Groups** (page 478)
 - **New Computer Group** (page 478)
 - **New Smart Computer Group** (page 479)
 - **Remove All Group Members** (page 480)
- **Administrator Setup** (page 480)
 - **New Administrator** (page 481)
 - **Remove Administrator from Group** (page 484)
 - **New Administrator Group** (page 484)
 - **New Computer Appointment Group** (page 485)

- **New Smart Computer Appointment Group** (page 485)
- **New Mobile Devices Appointment Group** (page 486)
- **New Smart Mobile Devices Appointment Group** (page 487)
- **New Smart Administrator Group** (page 488)
- **Refresh** (page 488)
- **Custom Information Fields** (page 489)
 - **New Custom Information Field** (page 489)
 - **Duplicate Custom Information Field** (page 493)
- **Edit <item>** (page 494)
- **Remove <item>** (page 494)
- **Retrieve Payloads** (page 495)
- **Retry Package** (page 495)
- **Reset Package** (page 495)
- **Install Selected Software Packages** (page 496)
- **Repeat Selected Installations** (page 496)
- **Reset Current Server Load** (page 496)

When one or more administered computers are selected in the window, other commands are displayed in the table context menu that are described in “Commands menu” on page 283. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Software Distribution

The **Software Distribution** submenu contains commands for managing software distribution functions:

- **New Software Package** (page 443)
- **New Metapackage** (page 453)
- **Duplicate Software Package** (page 461)
- **New Smart Software Package Group** (page 461)
- **New Payload** (page 462)
- **Duplicate Payload** (page 463)
- **New Smart Payload Group** (page 464)
- **New Distribution Point** (page 464)
- **New Smart Distribution Points Group** (page 466)
- **New Disk Image** (page 467)
- **New Smart Disk Image Group** (page 468)
- **New Smart Installation Status Group** (page 469)
- **New Missing Software Packages Group** (page 469)

New Software Package

The **New Software Package** command creates a new software package.

Choosing the command opens the **Software Distribution Package** dialog. The dialog has four panes:

- **Package**

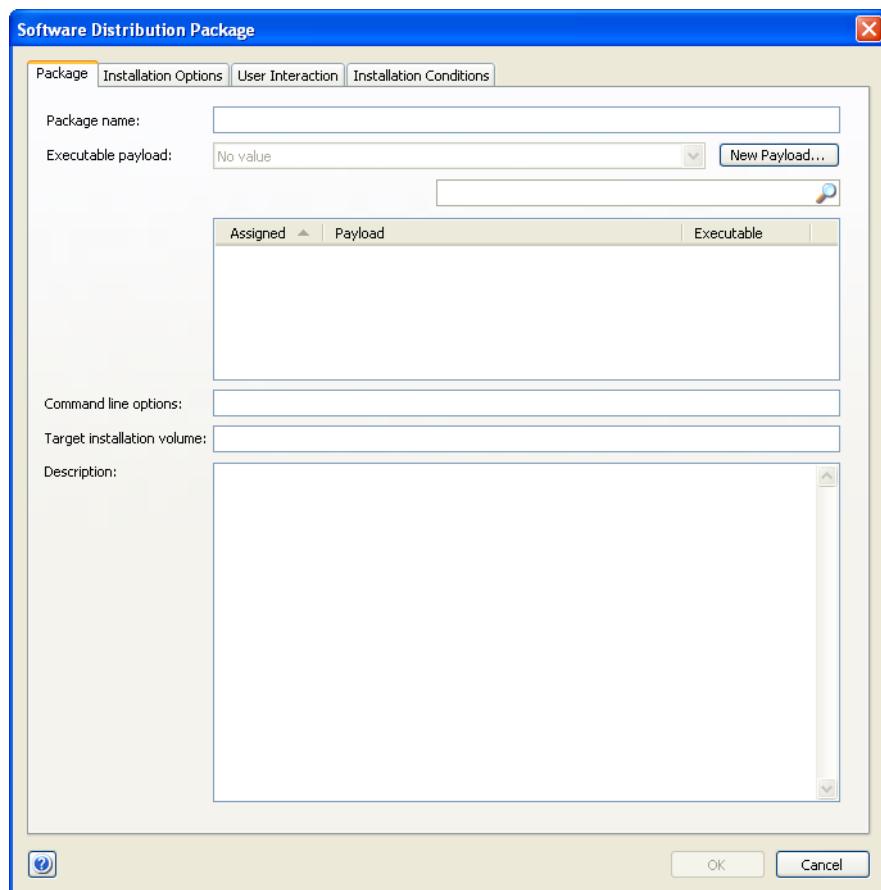
- **Installation Options**
- **User Interaction**
- **Installation Conditions**
- **Adobe CS Options**

All four are described below.

NOTE The **New Software Package** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

Package

The **Package** pane of the **Software Distribution Package** dialog lets you specify basic settings for the software package:



The pane contains these elements:

- **Package Name:** The name of the software package.
- **Executable Payload:** The payload that will be launched on the client computers to install this package.
A package can have any number of payloads; however, there must be exactly one executable payload. Executable payloads

can be applications (in particular, installers) or, for Mac OS X target computers, shell scripts.

Note: Non-executable payloads can, e.g., be configuration files for the installer (the executable payload). Including a configuration file as the non-executable payload allows you to perform different installations without needing multiple copies of the executable.

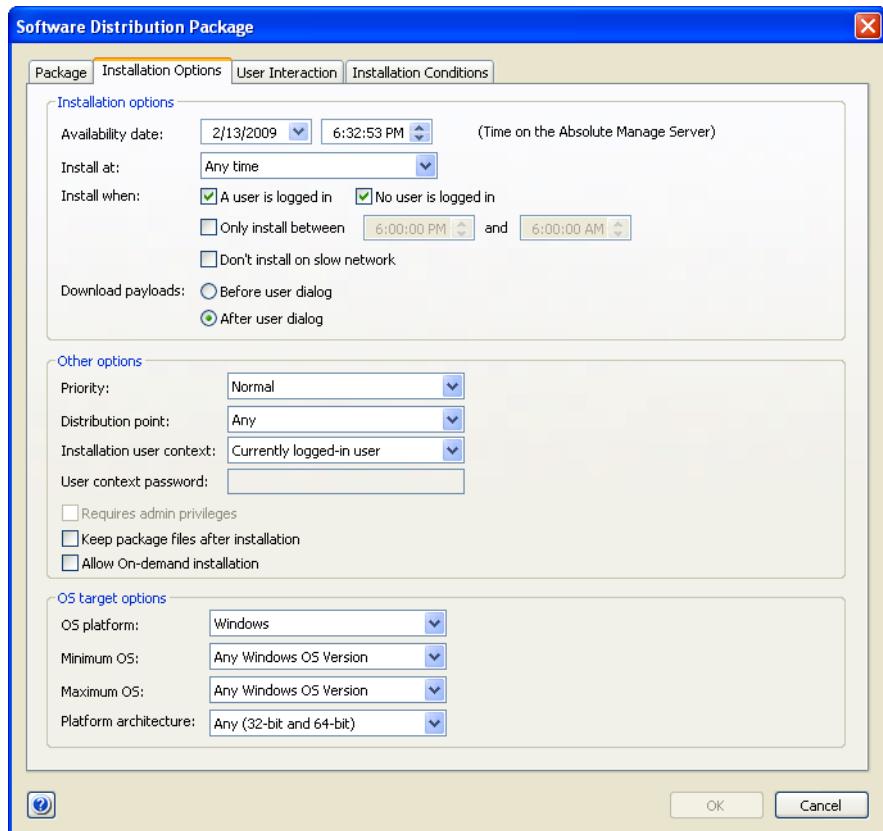
You can choose the executable from the pop-up menu. The menu contains all payloads checked in the list of payloads. Clicking the **New Payload** button opens the **Payload** dialog, letting you define a new payload on the fly.

The search field lets you filter the list of available payloads.

- **Command line options:** Options for the execution of the payload. (Optional.)
You can include environment variables in the options, as described in “Environment variables” on page 137.
Note: When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, Absolute Manage adds the /qn option (/quiet /norestart for MSU files) to run the installer silently.
- **Target installation volume:** The volume of the target computers on which the software is to be installed; relevant for Mac OS X only. When this is empty, the software is installed on the boot volume.
- **Description:** A description of the software contained in the package. This text is displayed if the local user is asked for confirmation.

Installation Options

The **Installation Options** pane of the **Software Distribution Package** dialog lets you specify various options for the installation of the package:



The pane contains these elements:

- **Availability date:** The earliest date when this package may be used for software installations on administered computers.
- **Install at:** Whether to install the package anytime or just on particular occasions.
- **Install when:** These options let you further specify conditions that must be met for the installation to proceed:
 - **A user is logged in:** If this option is checked, the package will be installed when a user is logged in on the target computer.
 - **No user is logged in:** If this option is checked, the package will be installed when no user is logged in on the target computer (and the computer is running).

Note: Both these options can be checked at the same time, in which case the package is installed irrespective of whether a user is logged in. It is not possible to uncheck both options.

*Note, too, that certain settings in the **User Interaction** pane force the settings of these options, in which case they are disabled.*

- **Only install between:** This option lets you restrict the installation of the package to a certain period of the day, e.g., after hours.

- **Don't install on slow network:** If this option is checked, installations take place only when the network connection between the client and the distribution point has a nominal transfer rate of at least 100 Mbit/s.
- **Download payloads:** This setting specifies when the Agent downloads a payload, before displaying a user dialog or after. Downloading the payload before displaying the dialog makes the installation feel more responsive to the user. Downloading the payload after the dialog avoids unnecessary downloads when the user cancels the installation.
The setting has no effect when there is no user interaction during the installation.
- **Priority:** The priority of this package. When more than one package is available for installation on a client, packages with higher priorities are installed first.
- **Distribution point:** An optional restriction on the distribution point from which the installer is transferred to the client:
 - **Any:** No restriction.
 - **From assigned distribution point if available:** When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, another distribution point is used.
 - **From assigned distribution point only:** When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, the installation fails.An assigned distribution point is a distribution point that either includes the agent's IP address in the range of IP addresses it is set to serve (see "New Distribution Point" on page 464 for details) or that has been assigned to a computer group of which the target computer is a member.
If no IP range has been specified in a distribution point definition, it is considered to be assigned to all clients in the same subnet. (The server's subnet mask is used to determine the extent of the subnet.)
- **Installation user context:** The user name of the account that is to be used for running the installer.
The **Currently logged-in user** option runs the installation in the user context of the user who is logged in on the client computer at installation time.
The **System account user** option runs the installation from the system user account.
- **User context password:** The password for the account to be used. This is not required for installations on Mac OS X.
- **Requires admin privileges:** This option applies only to installations on Mac OS X. If it is checked, the installer is authorized to run with administrator privileges.
Note: This does not change the user account from which the package is installed; it merely increases the available privileges for the installation, if necessary.
- **Other options:** Miscellaneous settings.
 - **Keep package files after installation:** If this option is checked, Absolute Manage does not delete the installation files after the installation is complete.

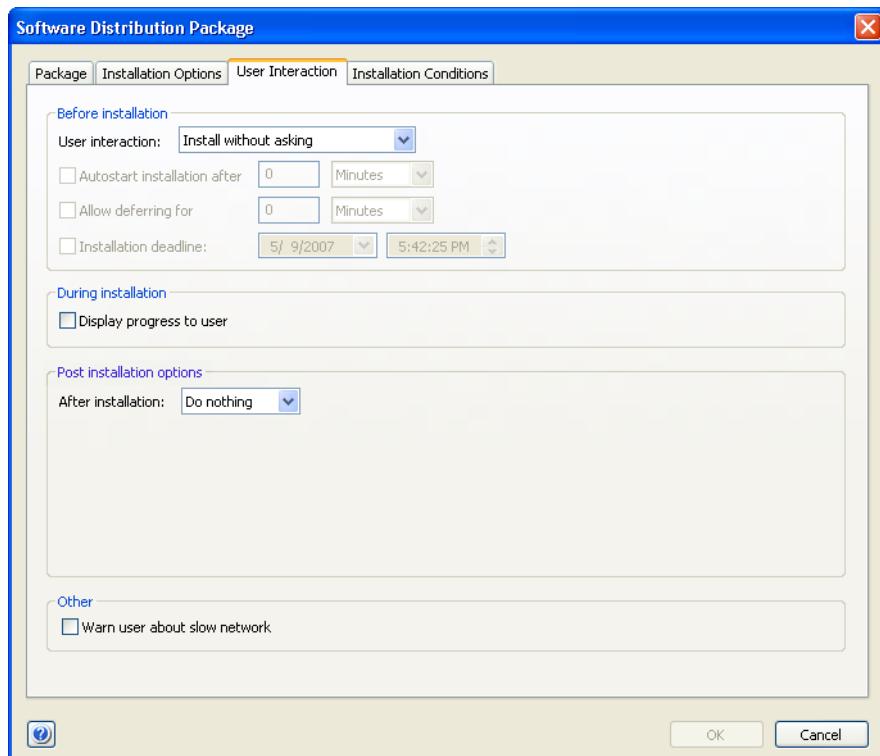
- **Allow on-demand installation:** If this option is checked, this package appears when the user manually queries the software distribution server for new packages. Checking this option disables a number of other options in the **Installation Options** and **User Interaction** panes.

- **OS Platform:** The operating systems on which the package may be installed.
- **Minimum OS:** The lowest version of the operating system on which the package may be installed.
- **Maximum OS:** The highest version of the operating system on which the package may be installed.
- **Platform architecture:** This option lets you restrict the installation to only Intel or PowerPC-based computers under Mac OS X. Under Windows, you can restrict installations to 32-bit or 64-bit versions of the OS.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

User Interaction

The **User Interaction** pane of the **Software Distribution Package** dialog lets you specify the information users are given during the installation process and the actions they can perform:



The pane contains these elements:

- **Before installation:** The way in which the user may influence the installation:

- **Install without asking:** The user is not informed of the installation.
- **Inform user before installation:** The user is informed of the installation before the fact but cannot affect it.
- **Allow to reschedule:** The user can postpone the installation but not disallow it altogether.
- **Allow to refuse:** The user may altogether refuse to have this package installed on his or her computer.
- **Autostart installation after:** This option is only active when a **Before installation** option other than **Install without asking** is chosen. It lets you specify a time after which the installation starts automatically when the user does not respond to the installation notification.
- **Allow deferring for:** This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the maximum time for which users can postpone the installation.
- **Installation deadline:** This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the latest time when the installation must begin.

NOTE

When you specify both a maximum deferring interval and an installation deadline, both are active. This means that the earlier of the two resulting dates becomes effective: If the deadline is reached, the installation is forced (unless the user has canceled it altogether), even if the interval has not yet expired. And if the interval expires, the installation begins even if the deadline has not yet been reached.

- **Display progress bar to the user:** If this option is checked, the users of the target computers are informed of the installation progress by a progress bar. If the option is unchecked, there is no feedback on the progress.
- **After installation:** The action that Absolute Manage Agent performs on the target computer after the installation is complete:
 - **Do nothing:** No action is performed.
 - **Notify user:** A message informing the user of the completed installation is displayed.
An additional option becomes available:
 - **Automatically close notification after:** This option lets you specify a time after which Absolute Manage Agent automatically closes the notification alert.
 - **Restart:** The computer is automatically restarted without a notification displayed first. Processes are sent termination messages, allowing data in open documents to be saved first.
Additional options become available:
 - **Show notification:** Checking this option causes Absolute Manage Agent to display a notification of the pending restart. The restart happens after the user has responded to the notification.
 - **Restart after no more than:** This option is available only when **Show notification** has been checked. It lets you set an interval after which the restart is

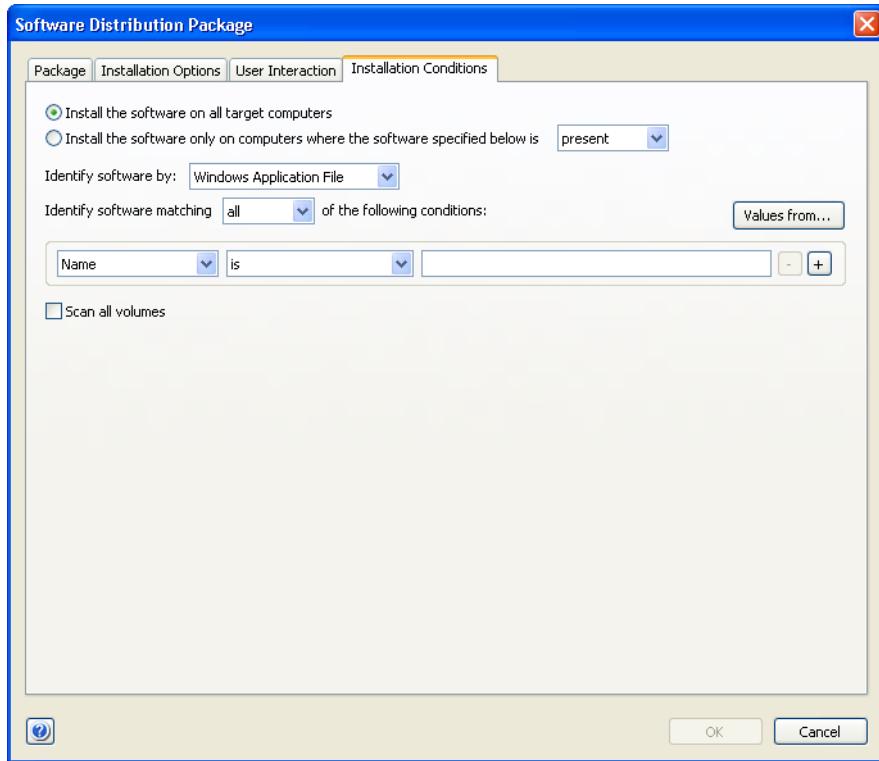
performed even when the user does not respond to the notification.

- **Allow user to postpone restart:** This option is available only when **Show notification** has been checked. It lets you give the user the option to defer the restart to a later date.
- **Show dialog again every:** This option is available only when **Allow user to postpone restart** has been checked. It lets you make Absolute Manage display the restart notification dialog at regular intervals, reminding the user that a restart is still required. If an interval has been specified in the **Restart after no more than** option (see above), it applies to these reminders as well.
 - **Force restart:** As **Restart**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost. The same options as for **Restart** become available.
 - **Shut down:** As **Restart**, above, but the target computer is shut down instead of restarted. The same options as for **Restart** become available.
 - **Force shutdown:** As **Shutdown**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost. The same options as for **Restart** become available.
- **Warn about slow network:** If this option is checked, the user of a target computer is warned before installations when the network connection between the client and the distribution point has a nominal transfer rate of less than 100 Mbit/s. The warning is not displayed if the software package is set to install without asking the user.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

Installation Conditions

The **Installation Conditions** pane of the **Software Distribution Package** dialog lets you specify that a package be installed only on client computers that meet certain criteria:



The pane contains these elements:

- **Install the software on all target computers:** The package will be installed on all computers in the computer groups to which it is assigned.
- **Install the software only on computers where the software specified below is:** Choose whether the package is to be installed only on computers that already have certain software (choose **present**) or on computers that lack specified software (choose **not present**).

The rest of the elements are similar to the corresponding ones in the **New License Specification** dialog discussed on page 470.

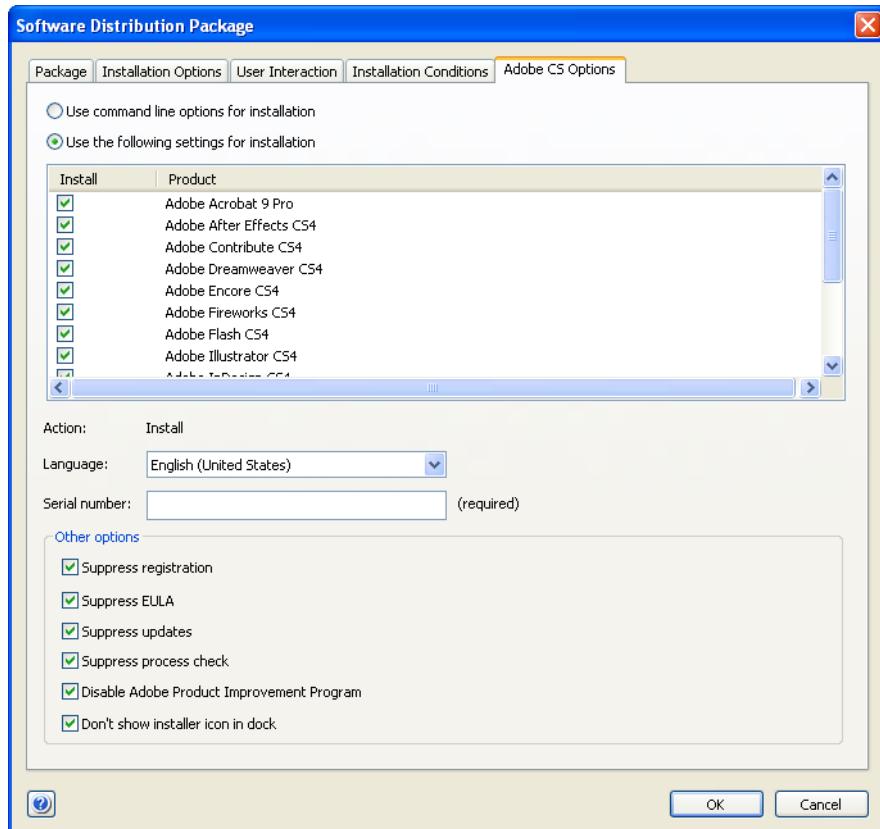
NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

Adobe CS Options

The **Adobe CS Options** pane of the **Software Distribution Package** dialog lets you set special options for installing, uninstalling or updating the Adobe Creative Suite. The tab is only available when a payload

containing an Adobe CS3 or CS4 installer or updater is assigned to the software package.

NOTE The settings in this tab are not compatible with Adobe CS 5 or newer. For remotely distributing these versions of Adobe CS, prepare an installer using Adobe Application Manager Enterprise Edition (AAMEE) and use that installer to create a standard software distribution package in Absolute Manage Admin.



The pane contains these elements:

- **Use command line options for installation:** If you choose this option, you can specify the installer behavior by supplying command line options in the **Package** pane. If you choose this option, all other settings in the dialog are ignored.
- **Use the following settings for installation:** If you choose this option, you can check the components that you want to be installed by this package in the scrolling list. You can also set additional options through the other checkboxes and radio buttons. The exact content of the list depends on which Adobe CS installer you are using.
- **Action:** Displays whether this package installs or uninstalls software. (You made this choice when creating the payload.)
- **Language:** The desired user interface language for the installed software.

- **Serial number:** Enter the serial number for the package here. Depending on the specific Adobe software you are installing the serial number is either optional or mandatory; this is indicated beside the field.
If you do not enter an optional serial number, the serial number will have to be entered individually for each installed copy when it is first launched.
- **Other options:** These settings let you disable various optional functions of the installer:
 - **Suppress registration :** If this option is checked, local users are not prompted to register their copy of Adobe CS.
 - **Suppress EULA:** If this option is checked, the license agreement is not displayed when Adobe CS is first started on the target computer.
 - **Suppress updates:** If this option is checked, the installed copies of Adobe CS will not check Adobe's servers for available updates.
 - **Suppress process check:** If this option is checked, the installer does not check for certain running applications. If the option is unchecked, the installer refuses to run on a target computer on which any of these applications is running.
 - **Disable Adobe Product Improvement Program:** If this option is checked, the Adobe Product Improvement Program (a tool that collects data and sends it to Adobe) is disabled.
 - **Don't show installer icon in dock:** If this option is checked, the Adobe CS installer does not show up in the dock of target Macintosh computers.

If the assigned payload contains an Adobe CS updater (instead of an installer), only some of the options in the dialog are available.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Distribution and Licensing Info" command (described on page 343).

New Metapackage

The **New Metapackage** command creates a new metapackage.

Choosing the command opens the **Metapackage** dialog. The dialog has four panes:

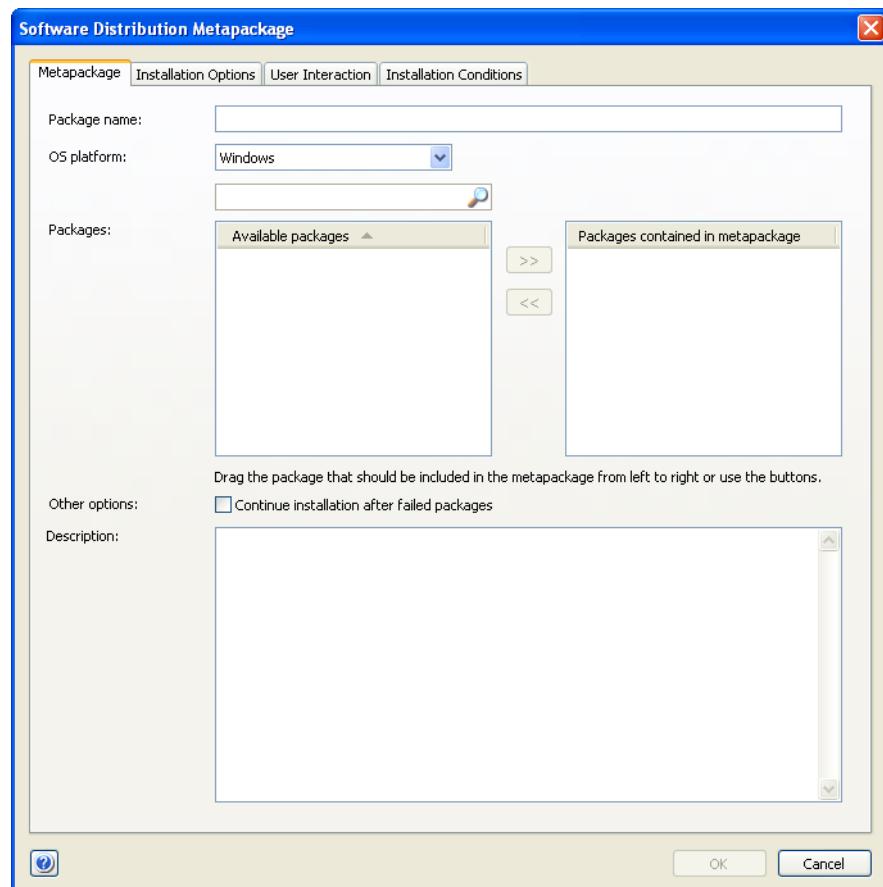
- **Metapackage**
- **Installation Options**
- **User Interaction**
- **Installation Conditions**

All four are described below.

NOTE The **New Metapackage** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

Metapackage

The **Package** pane of the **Metapackage** dialog lets you specify basic settings for the metapackage:



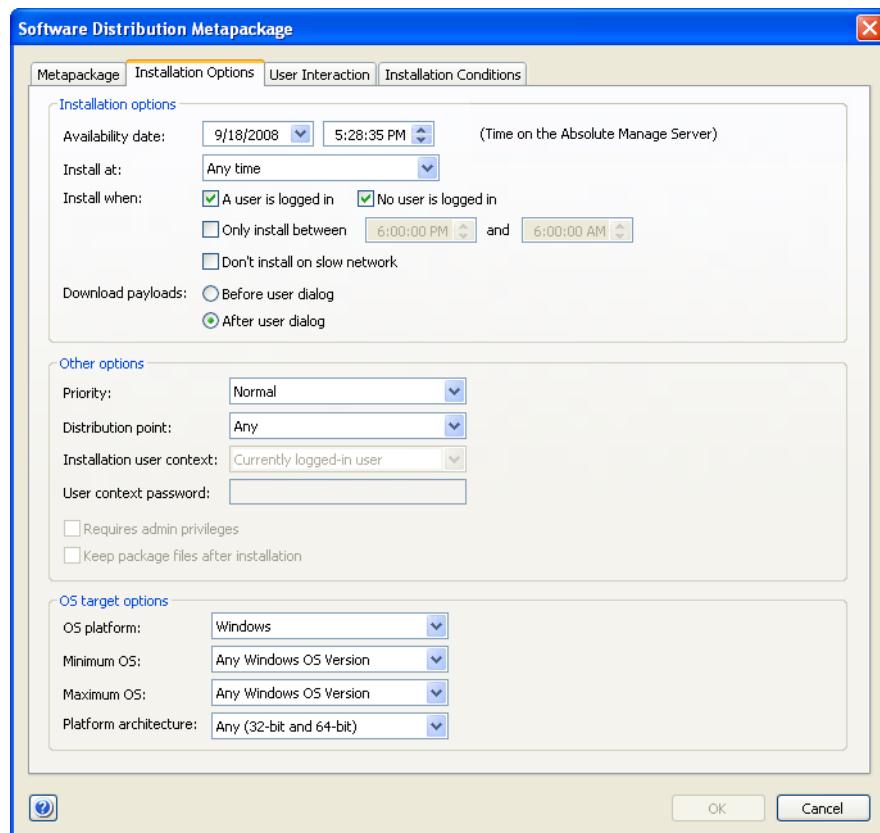
The pane contains these elements:

- **Package Name:** The name of the metapackage.
- **OS Platform:** The operating systems on which the metapackage may be installed. The chosen platform determines which packages are displayed in the pane.
- **Packages:** These two lists display the available packages and the packages contained in the metapackage. Dragging a package to the right list adds it to the package; dragging it back to the left list removes it. Dragging packages within the right list changes their installation order: Packages are installed in the order listed, from top to bottom. Entering text in the filter field above the lists filters the list of available packages.

- **Continue installation after failed packages:** If this option is checked, Absolute Manage will skip over any failed packages and install the rest of the packages in the metapackage. If the option is unchecked, the installation of a metapackage is stopped when a package contained in it fails to install.
- **Description:** A description of the software contained in the metapackage. This text is displayed if the local user is asked for confirmation.

Installation Options

The **Installation Options** pane of the **Metapackage** dialog lets you specify various options for the installation of the package:



NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Availability date:** The earliest date when this metapackage may be used for software installations on administered computers.
- **Install at:** Whether to install the metapackage anytime or just on particular occasions.
- **Install when:** These options let you further specify conditions that must be met for the installation to proceed:

- **A user is logged in:** If this option is checked, the metapackage will be installed when a user is logged in on the target computer.
- **No user is logged in:** If this option is checked, the metapackage will be installed when no user is logged in on the target computer (and the computer is running).

*Note: Both these options can be checked at the same time, in which case the metapackage is installed irrespective of whether a user is logged in. It is not possible to uncheck both options. Note, too, that certain settings in the **User Interaction** pane force the settings of these options, in which case they are disabled.*

- **Only install between:** This option lets you restrict the installation of the metapackage to a certain period of the day, e.g., after hours.
- **Don't install on slow network:** If this option is checked, installations take place only when the network connection between the client and the distribution point has a nominal transfer rate of at least 100 Mbit/s.
- **Download payloads:** This setting specifies when the Agent downloads a payload, before displaying a user dialog or after. Downloading the payload before displaying the dialog makes the installation feel more responsive to the user. Downloading the payload after the dialog avoids unnecessary downloads when the user cancels the installation.
The setting has no effect when there is no user interaction during the installation.
- **Priority:** The priority of this metapackage. When more than one metapackage or standard package is available for installation on a client, packages with higher priorities are installed first.
- **Distribution point:** An optional restriction on the distribution point from which the installer is transferred to the client:
 - **Any:** No restriction.
 - **From assigned distribution point if available:** When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, another distribution point is used.
 - **From assigned distribution point only:** When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, the installation fails.An assigned distribution point is a distribution point that either includes the agent's IP address in the range of IP addresses it is set to serve (see "New Distribution Point" on page 464 for details) or that has been assigned to a computer group of which the target computer is a member.
If no IP range has been specified in a distribution point definition, it is considered to be assigned to all clients in the same subnet. (The server's subnet mask is used to determine the extent of the subnet.)
- **Installation user context:** This option is not available for metapackages; all packages are installed with their individual user contexts.

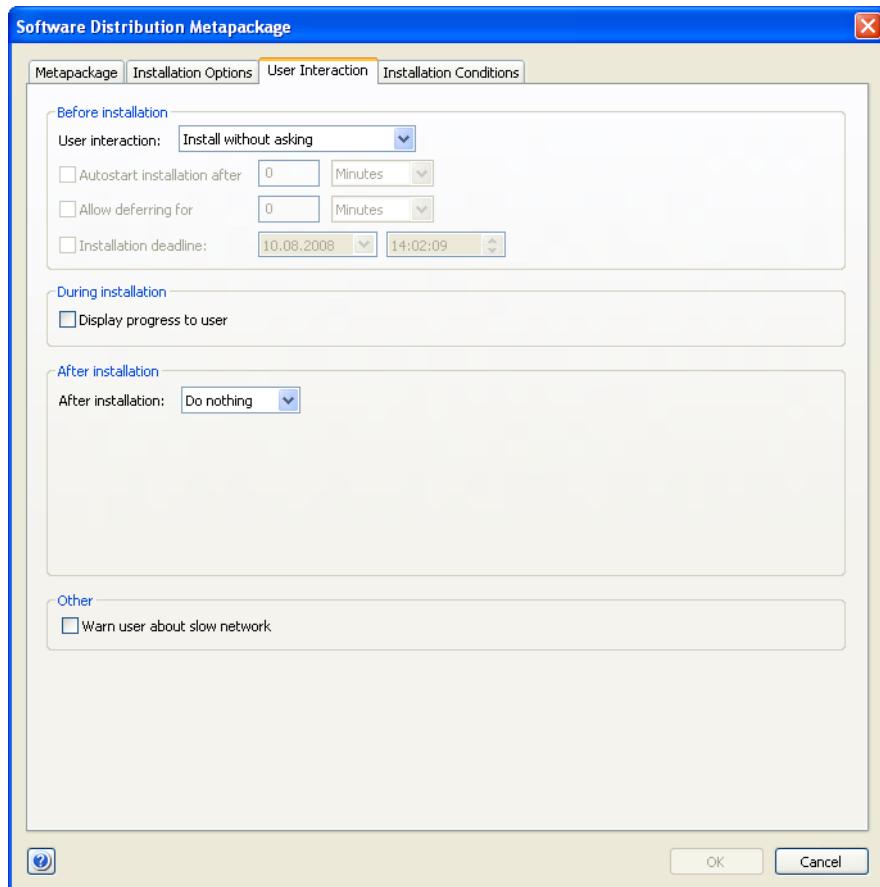
- **User context password:** This option is not available for metapackages; all packages are installed with their individual user passwords (if any).
- **Requires admin privileges:** This option is not available for metapackages; all packages are installed with their individual settings.
- **Other options:** Miscellaneous settings.
 - **Keep package files after installation:** This option is not available for metapackages; all packages are installed with their individual settings.
- **OS Platform:** The operating systems on which the metapackage may be installed.
- **Minimum OS:** The lowest version of the operating system on which the metapackage may be installed.
- **Maximum OS:** The highest version of the operating system on which the metapackage may be installed.
- **Platform architecture:** This option lets you restrict the installation to only Intel or PowerPC-based computers under Mac OS X. Under Windows, you can restrict installations to 32-bit or 64-bit versions of the OS.

NOTE

Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

User Interaction

The **User Interaction** pane of the **Metapackage** dialog lets you specify the information users are given during the installation process and the actions they can perform:



NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Before installation:** The way in which the user may influence the installation:
 - **Install without asking:** The user is not informed of the installation.
 - **Inform user before installation:** The user is informed of the installation before the fact but cannot affect it.
 - **Allow to reschedule:** The user can postpone the installation but not disallow it altogether.
 - **Allow to refuse:** The user may altogether refuse to have this metapackage installed on his or her computer.
- **Autostart installation after:** This option is only active when a **Before installation** option other than **Install without asking** is chosen. It lets you specify a time after which the installation starts automatically when the user does not respond to the installation notification.

- **Allow deferring for:** This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the maximum time for which users can postpone the installation.
- **Installation deadline:** This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the latest time when the installation must begin.

NOTE When you specify both a maximum deferring interval and an installation deadline, both are active. This means that the earlier of the two resulting dates becomes effective: If the deadline is reached, the installation is forced (unless the user has canceled it altogether), even if the interval has not yet expired. And if the interval expires, the installation begins even if the deadline has not yet been reached.

- **Display progress bar to the user:** If this option is checked, the users of the target computers are informed of the installation progress by a progress bar. If the option is unchecked, there is no feedback on the progress.
- **After installation:** The action that Absolute Manage Agent performs on the target computer after the installation is complete:
 - **Do nothing:** No action is performed.
 - **Notify user:** A message informing the user of the completed installation is displayed.
An additional option becomes available:
 - **Automatically close notification after:** This option lets you specify a time after which Absolute Manage Agent automatically closes the notification alert.
 - **Restart:** The computer is automatically restarted without a notification displayed first. Processes are sent termination messages, allowing data in open documents to be saved first.
Additional options become available:
 - **Show notification:** Checking this option causes Absolute Manage Agent to display a notification of the pending restart. The restart happens after the user has responded to the notification.
 - **Restart after no more than:** This option is available only when **Show notification** has been checked. It lets you set an interval after which the restart is performed even when the user does not respond to the notification.
 - **Allow user to postpone restart:** This option is available only when **Show notification** has been checked. It lets you give the user the option to defer the restart to a later date.
 - **Show dialog again every:** This option is available only when **Allow user to postpone restart** has been checked. It lets you make Absolute Manage display the restart notification dialog at regular intervals, reminding the user that a restart is still required. If an interval has been specified in the **Restart after no**

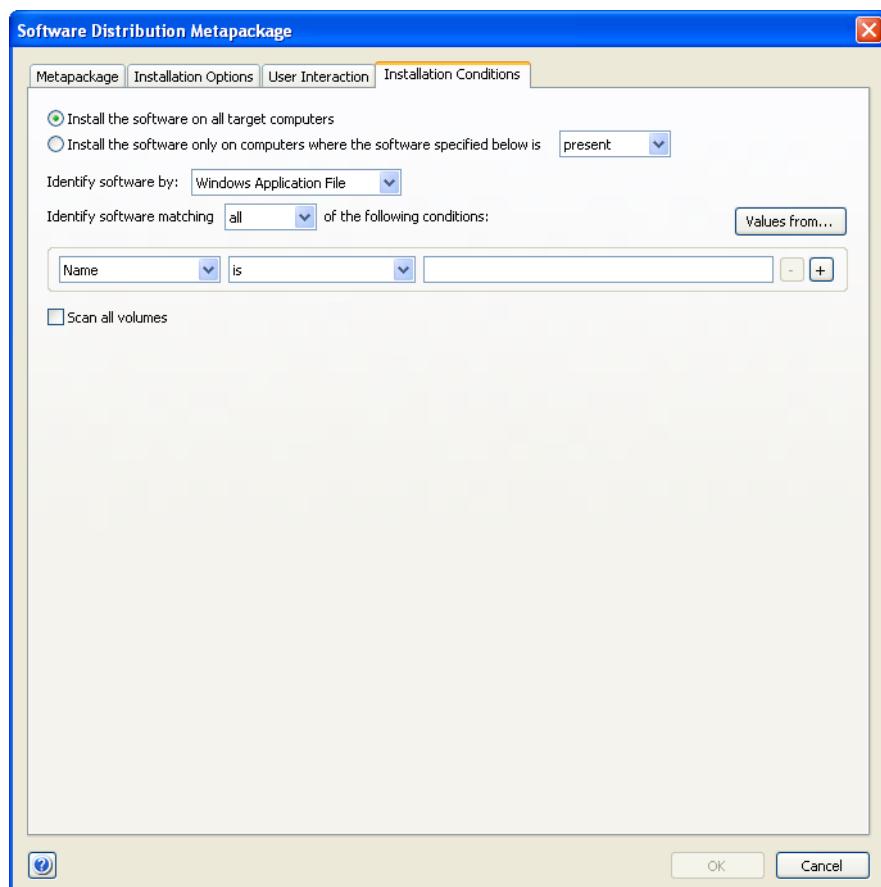
more than option (see above), it applies to these reminders as well.

- **Force restart:** As **Restart**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost. The same options as for **Restart** become available.
- **Warn about slow network:** If this option is checked, the user of a target computer is warned before installations when the network connection between the client and the distribution point has a nominal transfer rate of less than 100 Mbit/s. The warning is not displayed if the metapackage is set to install without asking the user.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

Installation Conditions

The **Installation Conditions** pane of the **Metapackage** dialog lets you specify that a metapackage be installed only on client computers that meet certain criteria:



NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Install the software on all target computers:** The metapackage will be installed on all computers in the computer groups to which it is assigned.
- **Install the software only on computers where the software specified below is:** Choose whether the metapackage is to be installed only on computers that already have certain software (choose **present**) or on computers that lack specified software (choose **not present**).

The rest of the elements are similar to the corresponding ones in the **Software License Specification** dialog discussed on page 470.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

Duplicate Software Package

The **Duplicate Software Package** command lets you create a new software distribution package or metapackage based on an existing one.

Depending on which type of package is selected, choosing the command opens the **Software Distribution Package** dialog that is described in “New Software Package” on page 443 or the Metapackage dialog described in “New Metapackage” on page 453, with the selected package’s settings displayed. If you click **OK** in that dialog, a new package is created.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

NOTE The **Duplicate Software Package** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

New Smart Software Package Group

The **New Smart Software Package Group** command creates a new smart group for software packages and metapackages.

Choosing the command opens the **Smart Group** dialog:



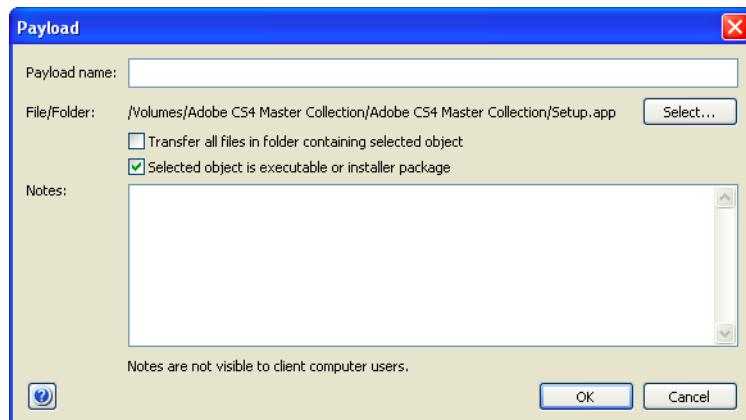
The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Packages** subcategory of the **Software Distribution** category (see page 575).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Payload

The **New Payload** command lets you create a new payload specification for use in software distribution packages.

Choosing the command opens the **Payload** dialog:



The dialog contains these elements:

Payload name: The name by which the payload is displayed in Absolute Manage. You can enter any name desired.

File/Folder: The file or folder that forms this payload. Clicking the **Select** button lets you select a file or folder.

Transfer all files in folder containing selected object: If this option is checked, all files that are located in the same folder as the payload file are transferred as part of this payload. If the option is unchecked, only the file itself is transferred.

Selected object is executable or installer package: If this option is checked, this payload is considered executable by Absolute Manage. Each software distribution package must contain exactly one executable payload.

Notes: Here you can enter explanations and remarks for yourself or other administrators. The text in this field is not visible to users of client computers.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 273.

NOTE The **New Payload** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

Duplicate Payload

The **Duplicate Payload** command lets you create a new payload based on an existing one.

Choosing the command opens the **Payload** dialog that is described in “New Payload” on page 462. If you click **OK** in that dialog, a new package is created.

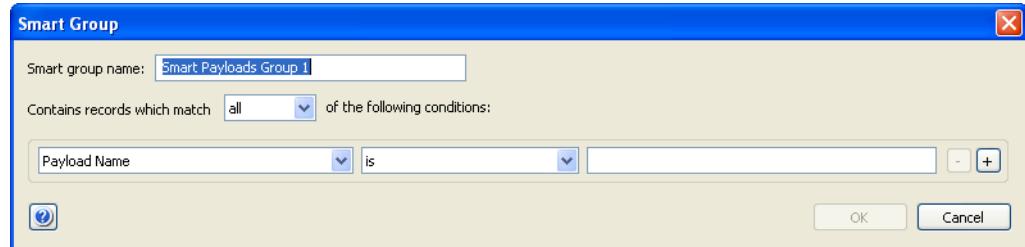
NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

NOTE The **Duplicate Payload** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

New Smart Payload Group

The **New Smart Payload Group** command creates a new smart group for payloads.

Choosing the command opens the **Smart Group** dialog:



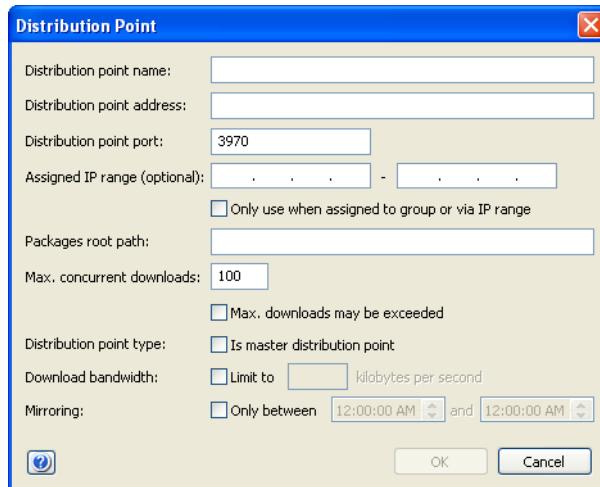
The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Packages** subcategory of the **Software Distribution** category (see page 575).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Distribution Point

The **New Distribution Point** command creates a new distribution point on which software installers are stored.

Choosing the command opens the **Distribution Point** dialog:



The dialog contains these elements:

- **Distribution point name:** The name by which the distribution point is to be known inside Absolute Manage.
- **Distribution point address:** The distribution point's IP address or DNS name.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain), if you enter a DNS name.
- **Distribution point port:** The port on which the Absolute Manage Agent installed on the distribution point communicates.
- **Assigned IP range (optional):** These fields can be used to assign the distribution point to computers within a particular IP range. The lower limit of the range must be specified in the left-hand field, the upper limit in the right-hand field.
This setting is used when a package is set to be provided from assigned distribution points, as described in **Distribution Point** in "Installation Options" on page 446.
- **Only use when assigned to group or via IP range:** Checking this option causes the distribution point to serve only client computers to which it has been expressly assigned in one of two ways:
 - Because the computers' IP addresses lie in the specified range
 - Because the distribution point has been assigned to a computer group to which the computers belong
- **Packages root path:** The path on the distribution point of the folder in which Absolute Manage is to store the software installers.
- **Max. concurrent downloads:** The number of download processes that may be under way at the same time.

- **Max. downloads may be exceeded:** This option governs the distribution point's behavior when all available distribution points are operating at capacity and an additional agent request for an installer download comes in:
 - If the option is checked, the installer is provided to the agent even though the specified maximum number of downloads is already in progress, because no other distribution point has available capacity.
 - If the option is unchecked, the agent's request is turned down and the agent must repeat it later.
- **Is master distribution point:** If this option is checked, the distribution point is the master distribution point from which all other distribution points receive their software installers. If it is unchecked, the distribution point is a mirror that receives its installers from the master.
There must always be exactly one master distribution point.
- **Download bandwidth:** This option lets you limit the network bandwidth employed for both providing installers to agents and mirroring installers between distribution points.
- **Only between:** This option lets you restrict mirroring of installers to or from this distribution point to a certain time of the day. Outside of the specified interval, no mirroring involving this distribution point happens.

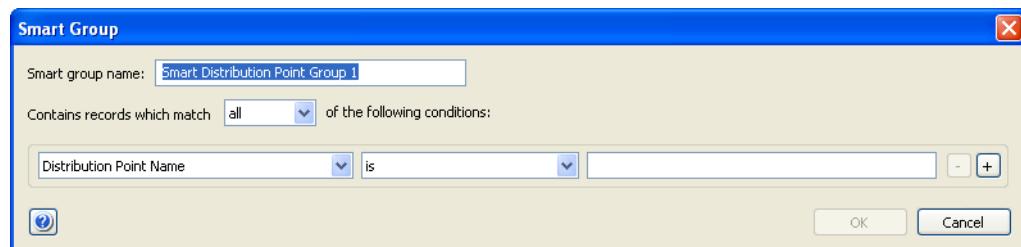
NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

NOTE The **New Distribution Point** command can be used only by administrators with the **Modify Distribution Points** right. See “New Administrator” on page 481 for details.

New Smart Distribution Points Group

The **New Smart Distribution Points Group** command creates a new smart group for distribution points.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

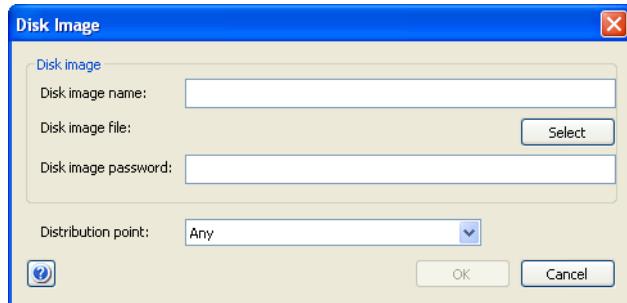
- **Smart Group Name:** The name for the smart group.

- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you enter an information item on which records are to be matched. You can use any information item from the **Distribution Points** subcategory of the **Software Distribution** category (see page 579).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Disk Image

The **New Disk Image** command creates a new disk image specification for reinstalling client computers.

Choosing the command opens the **Disk Image** dialog:



The dialog contains these elements:

- **Disk image name:** The name that you want to give the disk image specification for purposes of identifying it within Absolute Manage.
- **Disk image file:** The file that contains the disk image. Absolute Manage supports Apple's .dmg format as well as any other disk image that can be mounted without additional software on the target computer, such ISO images (.iso) and Active Disk Image images (.adi).
- **Disk image password:** If the specified disk image is password-protected, enter the password here.
- **Distribution point:** This option specifies from which distribution points the target computer may download the image:
 - **Any:** The image can be downloaded from any distribution point on which it is found.
 - **From assigned distribution point if available:** The image is downloaded from a distribution point that is assigned to

the target computer's subnet or to its computer group. If the image is not available on any such distribution point, it is downloaded from another distribution point.

- **From assigned distribution point only:** As above, but if the image is not available, the installation fails.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Distribution and Licensing Info" command (described on page 343).

NOTE The **New Disk Image** command can be used only by administrators with the **Modify Disk Images** right. See "New Administrator" on page 481 for details.

New Smart Disk Image Group

The **New Smart Disk Image Group** command creates a new smart group for disk image specifications.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Disk Images** subcategory of the **Software Distribution** category (see page 580).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

New Smart Installation Status Group

The **New Smart Installation Status Group** command creates a new smart group for installations according to their status.

Choosing the command opens the **Smart Group** dialog:



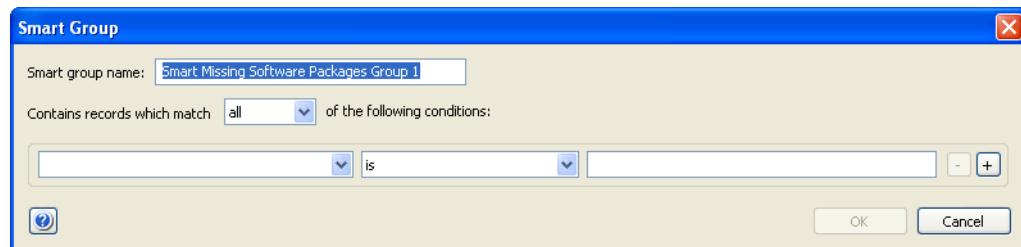
The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Installation Status** subcategory of the **Software Distribution** category (see page 581).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The + and - buttons let you add new conditions or remove existing ones.

New Missing Software Packages Group

The **New Missing Software Packages Group** command creates a new smart group that lists all software packages which are assigned to computers but not installed on them.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Installation Status** subcategory of the **Software Distribution** category (see page 581).
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

License Monitoring

The **License Monitoring** submenu contains commands for managing software distribution functions:

- **New License Specification** (page 470)
- **New Smart License Specification Group** (page 476)
- **New License Status Report** (page 477)
- **New Software Usage Report** (page 477)
- **New History Report** (page 478)
- **New History Summary Report** (page 478)
- **New Missing Software Report** (page 478)

New License Specification

The **New License Specification** command creates a new license specification.

Choosing the command opens the **Software License Specification** dialog, which has two panes:

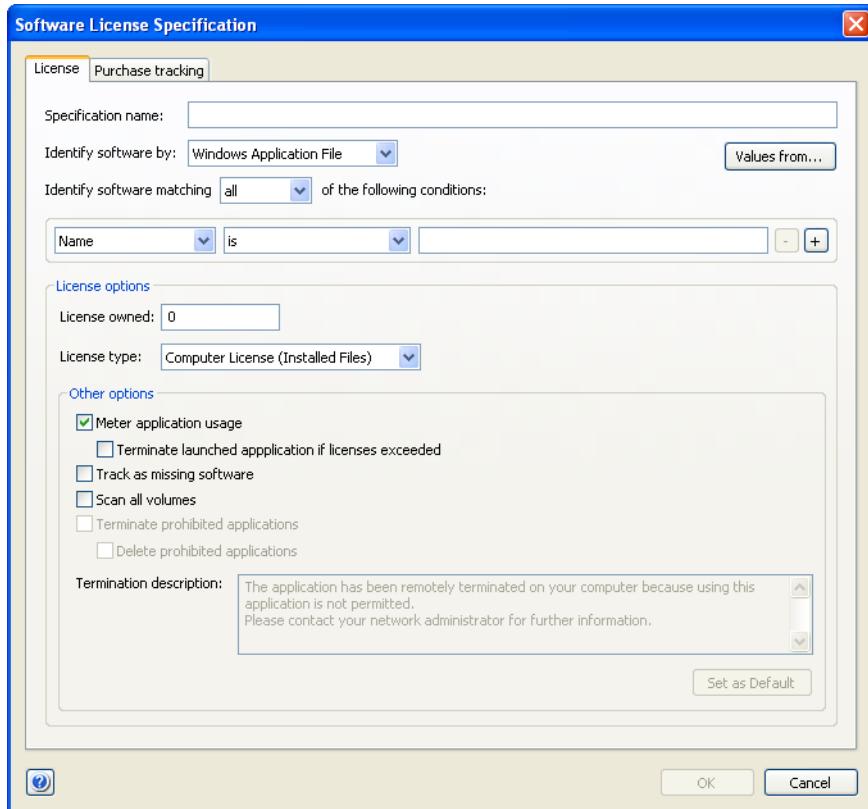
- **License**
- **Purchase Tracking**

Both are described below.

NOTE The **New License Specification** command can be used only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 481 for details.

License

The **License** pane of the **Software License Specification** dialog lets you enter the details of the software license:



The pane contains these elements:

- **Specification Name:** The name of the license specification.
- **Identify software by:** How the software is to be identified that is described by this license:
 - **Mac OS Application Package:** a Mac OS X package (a folder appearing as a file).
 - **Mac OS Application File:** a Mac OS X file. Files are only considered to match if they are executable applications.
 - **Mac OS File:** a Mac OS X file.
 - **Mac OS Installer Receipt:** a description of the installed software in the form of an installer package that some Mac OS X installers create.
 - **Windows Application File:** a Windows file. Files are only considered to match if they are executable applications.
 - **Windows File:** a Windows file.
 - **Windows Installer Receipt:** a report on the installed software created by MSI installers.
 - **Windows Installed Software:** software installed on the administered computer.
 - **Windows Registry:** specified contents of the Windows registry.
- **Identify software matching:** When **all** is chosen from this pop-up menu, software is found that matches all specified conditions (Boolean AND). If **any** is chosen, software is found

that matches at least one of the specified conditions (Boolean OR).

- **Values from:** Clicking this button lets you select a file. All specified conditions are filled with the corresponding parameters from this file. If you later add new conditions, they initially also contain comparison values from this file.
- Condition area: The first pop-up menu lets you choose a condition to match software. The second one contains the possible comparison operators. For most conditions, a text field lets you specify the value to compare files against. The + and – buttons let you add new conditions or remove existing ones.

The parameters available for specifying conditions are described in “Files” on page 566, except for **Path** and the conditions available when **Windows Registry** is selected as the software type. These additional conditions are described in “Conditions” on page 474.

- **Path:** Lets you select files and folders by their paths on the hard disk. It references the **File Path** information item. When this option is chosen, you can specify the user folder on Mac OS X targets and its subfolders using the ~/ notation. (For example, ~/Documents for the user’s documents folder.)
For Windows targets, you can use the environment variables when this option is chosen, as described in “Environment variables” on page 137.
- **Original File Name:** The original file name of a Windows file, as displayed in its properties in the Windows Explorer.
- **Internal Name:** The internal name of a Windows file, as displayed in its properties in the Windows Explorer.

*Note: When you specify a license by Windows registry data, you should use the **Key Name** and **Value Name** conditions only when there is no other way to specify the desired software. Checking either condition requires the entire registry to be parsed, which generates significant local processor load on the client computer. If you do require either condition, specify it after any other conditions that may apply because that causes Absolute Manage to apply it only to the part of the registry that meets those other conditions.*

Note: When specifying a file version, make sure to use the right format (three numbers for Mac OS X files, four for Windows files), as described in “Gathering information on files” on page 76.

- **Licenses owned:** The number of licenses that are available for use.
You can either enter these licenses manually or have Absolute Manage calculate them automatically as the sum of your license purchases. In the latter case, you must create purchase records in the dialog’s **Purchase Tracking** pane for all licenses you have purchased of this software.
- **License type:**
 - **Computer License (Installed Files):** The license governs how many copies of the software may be installed in your network.

- **Floating License (Running Processes):** The license governs how many copies of the software may be in use at the same time.
- **Site License:** This type indicates software that may be used without restriction throughout your network. Choose it when you want to use the license specification for monitoring purposes.
- **Prohibited Application:** Using this software is not allowed in your network. (This is not really a license type but allows you to check for the presence of undesirable software.)
- **Meter application usage:** If this option is checked, the running processes on the client computers are checked for the licensed software.

Note: Only applications on administered computers that have a working network connection to the server are included in the count.

Note: The computers' hard disks are always checked for installed packages, whether this option is activated or not.

 - **Terminate launched application if licenses exceeded:** If a user launches the specified application and all licenses are already in use, Absolute Manage immediately terminates the application again, displaying the message from the **Termination description** field (see below) on the administered computer.
- **Track as missing software:** Absolute Manage lists this software as missing when it is not installed on a client computer.
- **Scan all volumes:** If this option is checked, all local volumes of administered computers are scanned for this software. If it is unchecked, only boot volumes are scanned.
- **Terminate prohibited applications:** If this option is checked, Absolute Manage automatically terminates any found applications that you have assigned the **Prohibited Application** license type. Absolute Manage displays the message from the **Termination description** field (see below) on the administered computer
This option is available only for Mac OS application packages and files and Windows application files. It requires that the **Meter application usage** option is also checked.
 - **Delete prohibited applications:** If this option is checked, the prohibited application is deleted from the client computer in addition to being terminated.
- **Termination description:** This is the message displayed on client computers when Absolute Manage terminates an application because licenses are exceeded or the application is prohibited.

To insert a line break, type Ctrl-Enter.

Clicking the **Set as Default** button makes the current text in the field the default for any licenses you create from now on.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Distribution and Licensing Info" command (described on page 343).

Conditions

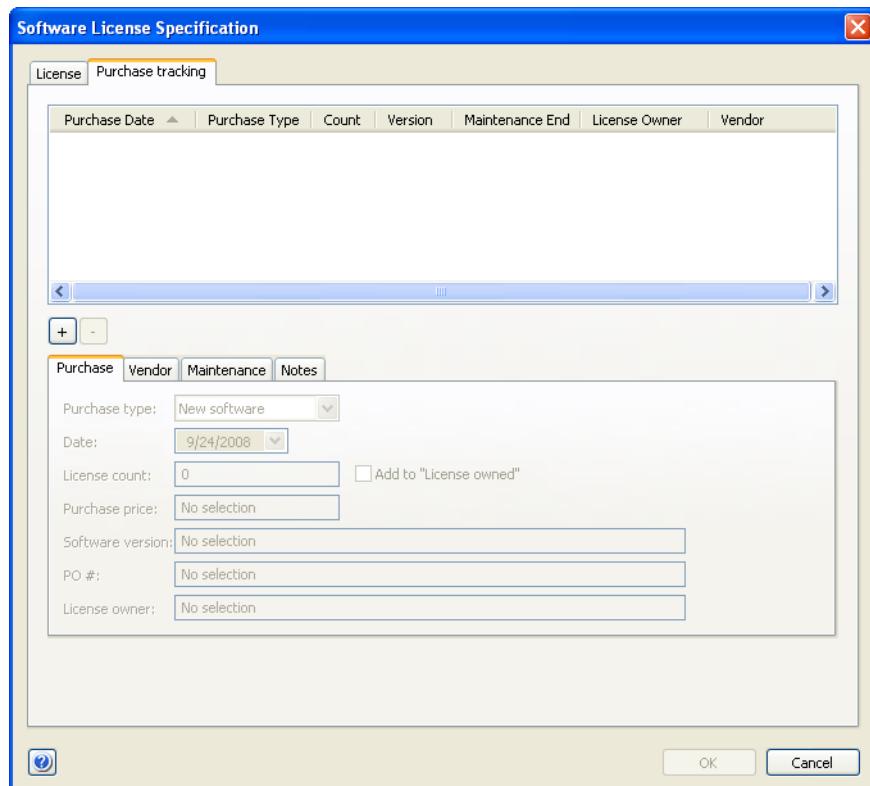
Most of the conditions available for specifying how to determine the presence of licensed software are information items that are described in "Files" on page 566. There are, however, some additional conditions:

- **Path** lets you select files and folders by their paths on the hard disk. It references the **File Path** information item.
- **Path of Key** is the path of a key in the Windows registry.
- **Path of Value** is the path of a value in the Windows registry.
- **String at Path** is the value at the supplied path, interpreted as a string.
- **Number at Path** is the value at the supplied path, interpreted as a number.
- **Key Name** is a key with the specified name anywhere in the registry.
- **Value Name** is a value with the specified name anywhere in the registry.

*Note: Searching for either **Key Name** or **Value Name** creates significant processor loads on the clients. Use these options only when there is no other way to identify the presence of the software.*

Purchase Tracking

The **Purchase Tracking** pane of the **Software License Specification** dialog lets you view, create, and maintain records of any purchases and maintenance contracts associated with the specified license:



The pane contains a list of recorded purchases in the upper half and four subpanes – described below – that display full information on the selected purchase.

The **+** button lets you add a new purchase. When a single existing purchase is selected, holding down the Ctrl key while clicking the button duplicates the purchase. The **-** button lets you delete the selected purchase from the list.

Purchase

The **Purchase** subpane lets you record the basic information about a license purchase:

- The **Purchase type** pop-up menu lets you specify the type of purchase you are recording.
- In the **Date** field, the date of the purchase can be entered.
- The **License count** field includes the number of licenses that were bought in the recorded purchase.
- If the **Add to “Licenses owned”** option is checked, the total number of licenses in the **License** pane’s **Licenses owned** field is automatically calculated from all purchases with this option checked.
The option is only available when the purchase type is “New Software.”
- The **Purchase price** field lets you record the price of the licenses.
- The **Software version** field contains the version of the software that was bought.
- The **PO #** field lets you specify a purchase order or other internal reference number for the recorded purchase.
- The **License owner** field lets you specify an employee or department that is internally in your organization considered to be the owner of the licenses acquired in the recorded purchase.

Vendor

The **Vendor** subpane lets you record information about the vendor from whom the license was purchased:

- The **Name** field contains the company’s name.
- The **Reference #** allows you to specify an internal supplier reference number or a similar key for the vendor’s company.
- The **Contact** field contains your contact person at the vendor’s company.
- The **Support** field contains a phone number, e-mail address or other contact information for technical support regarding the purchased licenses.

Maintenance

The **Maintenance** subpane lets you specify the maintenance purchased:

- Check the **Maintenance purchased from** option if maintenance has been purchased, either together with software licenses or in a separate agreement. Specify the duration in the two date fields.
- The **Maintenance price** field lets you enter the price of the maintenance contract.
- The **Reference #** field contains a contract number or similar identifying information for the maintenance agreement.

Notes

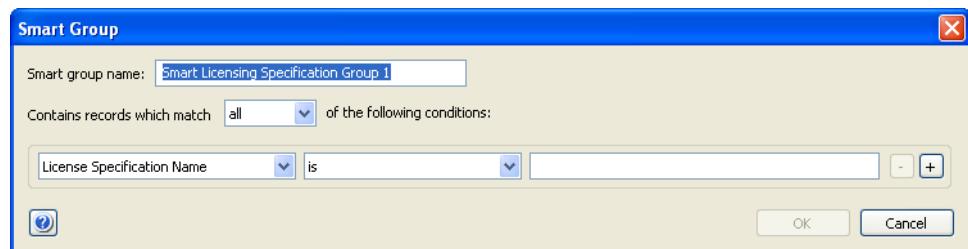
The **Notes** subpane lets you enter any additional information regarding the purchased licenses.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

New Smart License Specification Group

The **New Smart License Specification Group** command creates a new smart group for license specifications.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

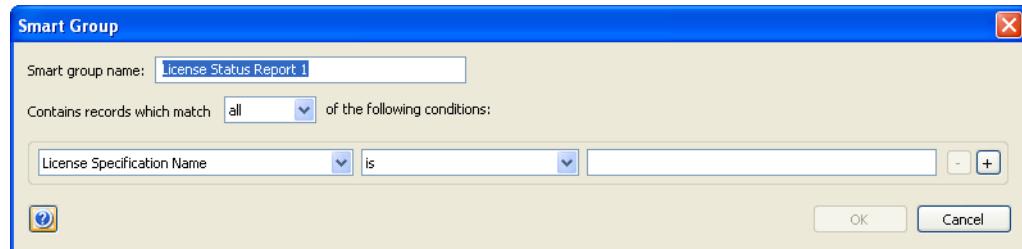
- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
 - The pop-up menu in the middle contains the possible comparison operators.

- The right-hand text field lets you specify the value to compare record values against.
- The + and – buttons let you add new conditions or remove existing ones.

New License Status Report

The **New License Status Report** command creates a new licensing report smart group listing license specifications. The report created in this way is similar to the **Fully compliant**, **Licenses exceeded**, or **Prohibited software** reports.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the licensing report.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
 - The pop-up menu in the middle contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The + and – buttons let you add new conditions or remove existing ones.

New Software Usage Report

The **New Software Usage Report** command creates a new licensing report smart group listing the state of individual computers regarding individual licensed applications. The report created in this way is similar to the **Software usage** or **Missing software** reports.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 464.

New History Report

The **New History Report** command creates a new licensing report smart group listing license history snapshots.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 464.

New History Summary Report

The **New History Summary Report** command creates a new statistical report on the maximum, minimum, and average usage of the specified licenses.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 464.

New Missing Software Report

The **New Missing Software Report** command creates a new report smart group listing missing software that meets the specified criteria.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 464.

Computer Groups

The **Computer Groups** submenu contains commands for managing computer groups for both software distribution and license monitoring:

- **New Computer Group** (page 478)
- **New Smart Computer Group** (page 479)
- **Remove All Group Members** (page 480)

New Computer Group

The **New Computer Group** command creates a new computer group.

Choosing the command opens the **New Computer Group** dialog:



The **New computer group name** field lets you specify the name for the new group.

Clicking **OK** creates the group.

Computers, software packages, and license specifications can be assigned to the computer group by dragging them on top of the category.

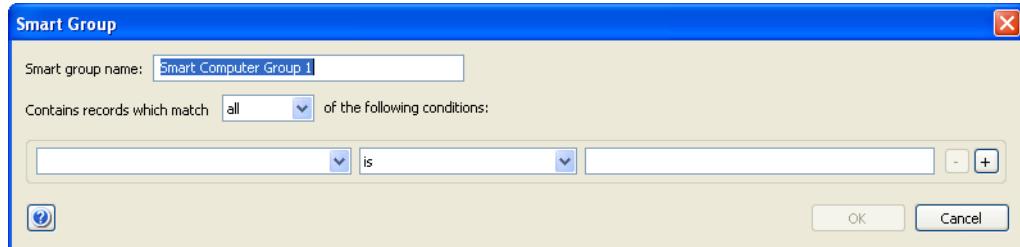
NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Distribution and Licensing Info" command (described on page 343).

NOTE The **New Computer Group** command can be used only by administrators with the **Modify Computer Groups** right. See "New Administrator" on page 481 for details.

New Smart Computer Group

The **New Smart Computer Group** command creates a new smart computer group.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

NOTE The **New Smart Computer Group** command can be used only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 481 for details.

Remove All Group Members

The **Remove All Group Members** command removes selected computers from a computer group.

Choosing the command removes the selected computers from the computer group in which they were selected. A confirmation alert is displayed first. The computers remain in the database and they also remain in any other computer groups of which they may be members.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Distribution and Licensing Info” command (described on page 343).

NOTE The **Remove All Group Members** command can be used only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 481 for details.

Administrator Setup

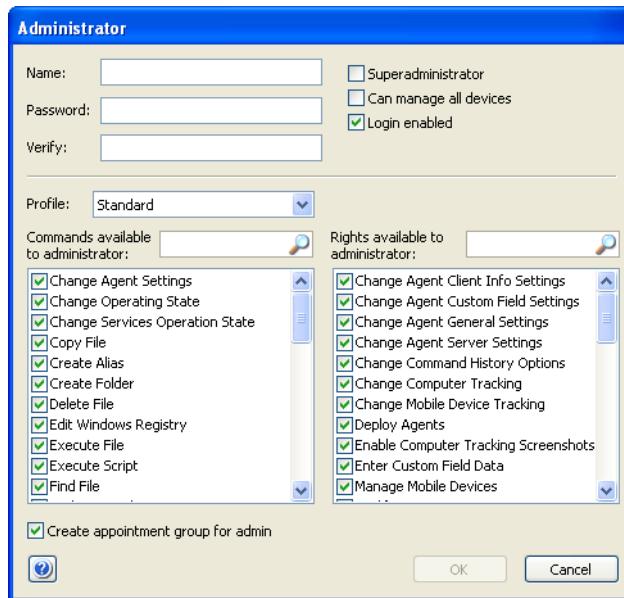
The **Administrator Setup** submenu contains commands for managing administrator accounts as well as administrator and appointment groups:

- **New Administrator** (page 481)
- **Remove Administrator from Group** (page 484)
- **New Administrator Group** (page 484)
- **New Computer Appointment Group** (page 485)
- **New Smart Computer Appointment Group** (page 485)
- **New Mobile Devices Appointment Group** (page 486)
- **New Smart Mobile Devices Appointment Group** (page 487)
- **New Smart Administrator Group** (page 488)
- **Refresh** (page 488)

New Administrator

The **New Administrator** command opens the dialog for creating a new administrator account on the currently connected Absolute Manage Server.

Choosing the command opens the **Administrator** dialog:



The dialog contains these elements:

- **Name:** The log-in name of the account.
- **Password:** The password. A password may contain any Unicode character.
- **Verify:** Whenever the password is changed, you need to retype the new password in this field. If the contents of the **Password** and **Verify** fields do not match, an error message is displayed and the password change is rejected.
- **Superadministrator:** When this option is checked, the account has superadministrator privileges, when it is not, it has normal privileges. (Details on administrator privileges are available in “Initial configuration of Absolute Manage Server” on page 16.)
- **Can manage all devices:** If this option is checked, the administrator can access all computers and mobile devices that are managed on the Absolute Manage Server. If the option is unchecked, the administrator can manage only devices to which the account has been expressly assigned.
- **Login enabled:** The account is active. If the option is unchecked, the account is temporarily suspended; the user cannot access Absolute Manage Admin.
- **Profile:** Using this pop-up menu, account settings can be saved as a profile and profiles applied to the account.
 - Profile names: In the upper section of the pop-up menu, all existing profiles are listed. Choosing a profile from the

menu applies its settings to the current administrator account.

Note: Profiles are merely presets: Changing a profile-based account does not affect the profile and vice versa.

- **Commands available to administrator:** The administrator can use all commands checked in this list.
The individual options in the list correspond to commands from the **Commands** menu.
Note: Any commands related to mobile devices also require the Manage Mobile Devices right (see below) to be enabled for the administrator to be able to use them.
Note: Holding down the Alt and Ctrl keys while clicking a checkbox in this list checks or unchecks all options in the list.
- **Create appointment group for admin:** If this option is checked, Absolute Manage automatically creates two appointment groups in the Server Center's sidebar, one for computers and one for mobile devices. The groups list, respectively, all computers and mobile devices to which the administrator has been assigned and offers a convenient way to assign him or her to additional devices.
- **Rights available to administrator:** The administrator can perform all actions checked in this list. These are the available rights and the corresponding access options in Absolute Manage Admin:
 - **Change Agent Client Info Settings:** Set options in the **Client Information** tab of the **Agent Settings** command window.
 - **Change Agent Custom Field Settings:** Set options in the **Custom Fields** tab of the **Agent Settings** command window.
 - **Change Agent General Settings:** Set options in the **General** tab of the **Agent Settings** command window.
 - **Change Agent Server Settings:** Set options in the **Servers** tab of the **Agent Settings** command window.
 - **Change Command History Options:** Specify in a command window's **Command Options** dialog under which conditions the command will be listed in the command history.
If an administrator does not have this right, all of his or her commands will be issued with the **Always add to command history** setting.
 - **Change Computer Tracking:** Set and edit computer tracking options using the **Computer Tracking** context menu command from a browser window.
 - **Change Mobile Device Tracking:** Set and edit mobile device tracking options.
 - **Deploy Agents:** Use the Agent Deployment Center.
 - **Enable Computer Tracking Screenshots:** Enable the **Take screenshots** option in the **Computer Tracking** dialog.
 - **Enter Custom Field Data:** Enter and edit information in Manual type custom information fields (i.e., fields that are not calculated automatically by Absolute Manage).
 - **Manage Mobile Devices:** Issue commands to mobile devices managed from Absolute Manage through an MDM server.

This right is a “master switch” for the administrator account. It is required for the administrator to be able to send commands to mobile devices at all, but any specific commands he or she is to be able to send must also be checked in the **Commands available to administrator** list, (see above).

- **Modify Computer Groups:** Create, edit, or delete computer groups in the Server Center.
- **Modify Custom Information Fields:** Create, edit, and delete custom information field definitions on the server.
- **Modify Disk Images:** Create, edit, or delete disk images for reinstalling computers in the Server Center.
- **Modify Distribution Points:** Create, edit, or delete distribution point definitions in the Server Center.
- **Modify Mobile Device Configuration Profiles:** Import or delete configuration profiles for mobile devices in the Server Center.
- **Modify License Specifications:** Create, edit, or delete license specifications in the Server Center.
- **Modify Mobile Actions:** Create, edit, or delete actions that can be applied to mobile devices entering a smart policy.
- **Modify Mobile Applications:** Create, edit, or delete application packages for installation on administered mobile devices.
- **Modify Mobile Device Policies:** Create, edit, or delete policies for administered mobile devices.
- **Modify Mobile Media:** Create, edit, or delete media files to be distributed to administered mobile devices.
- **Modify Server Settings:** View and change server options in the Server Center or via the **Change Server Registration** command.
- **Modify Software Packages:** Create, edit, or delete software packages in the Server Center.
- **Remote Control:** Open a screen-sharing connection to an administered computer using the **Remote Control** command.
- **Remove Computer Records:** Delete a computer from a browser window, e.g., using the **Remove from Server** command.
- **Remove History Commands:** Delete entries from the **History** group in the **Commands** window.
- **Remove Inventory Data:** Delete inventory data, e.g., using the **Remove Inventory Data** command.
- **Remove License Reports:** Delete log entries from the **License Monitoring > Reports** group in the Server Center.
- **Remove Mobile Device History Commands:** Delete entries from the **Commands** group in the **Mobile Devices** window.
- **Remove Mobile Device Records:** Delete a mobile device from the **Mobile Devices** window.
- **Remove SD Log Entries:** Delete log entries from the **Software Distribution > Installation Status** group in the Server Center.

- **Reset Software Packages:** Use the **Reset Package** context menu command in the Server Center.
- **Retry Software Packages:** Use the **Retry Package** context menu command in the Server Center.
- **View Administrator Settings:** See administrator-related information in the Server Center.
- **View Commands Window:** Open the **Commands** window and view its contents.
- **View Computer Tracking Data:** See the contents of information items from the **Computer Tracking** category.
- **View Computer Tracking Screenshots:** See the screenshots taken as part of the computer tracking.
- **View Custom Information Fields:** See the contents of custom information fields.
- **View License Monitoring Settings:** Open the **License Monitoring** category in the Server Center and view its contents.
- **View Mobile Device Tracking Data:** See the collected geolocation data of tracked mobile devices.
- **View Server Status:** Open the **Server Monitor** category in the Server Center and view its contents.
- **View Software Distribution Settings:** Open the **Software Distribution** category in the Server Center and view its contents.

Note: Holding down the Alt and Ctrl keys while clicking a checkbox in this list checks or unchecks all options in the list.

Remove Administrator from Group

The **Remove Administrator from Group** command removes selected administrators from an administrator group.

Choosing the command removes the selected administrators from the administrator group in which they were selected. A confirmation alert is displayed first. The administrators remain in the database and they also remain in any other administrator groups of which they may be members.

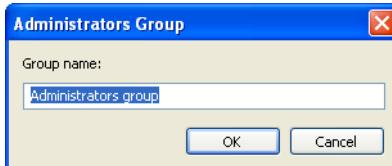
NOTE

Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the “Save Administrator Info” command (described on page 344).

New Administrator Group

The **New Administrator Group** command creates a new (non-smart) group for administrator accounts.

Choosing the command opens the **Administrators Group** dialog:



The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Administrator Info" command (described on page 344).

New Computer Appointment Group

The **New Computer Appointment Group** command creates a new (non-smart) appointment group for computers.

Choosing the command opens the **New Appointment Group** dialog:



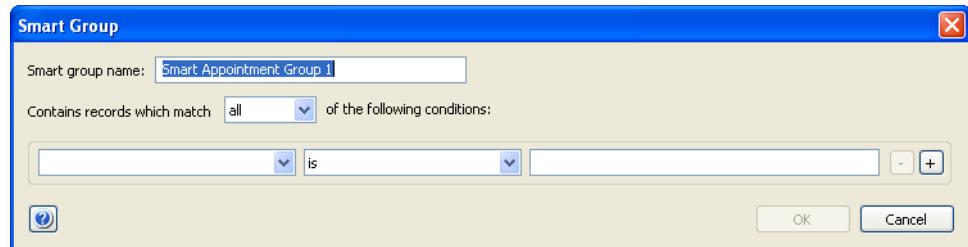
The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Administrator Info" command (described on page 344).

New Smart Computer Appointment Group

The **New Smart Computer Appointment Group** command creates a new appointment group that automatically includes all computers meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Administrator Info" command (described on page 344).

New Mobile Devices Appointment Group

The **New Mobile Devices Appointment Group** command creates a new (non-smart) appointment group for managed mobile devices.

Choosing the command opens the **New Appointment Group** dialog:



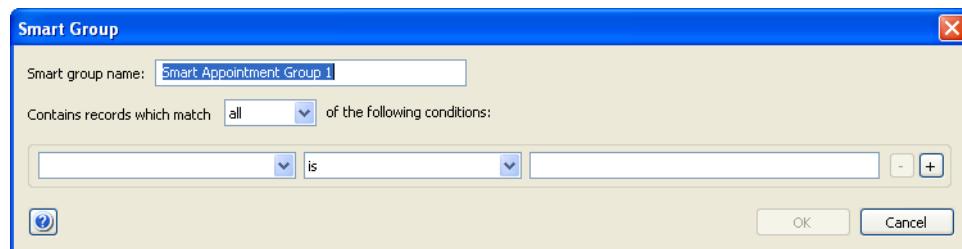
The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Administrator Info" command (described on page 344).

New Smart Mobile Devices Appointment Group

The **New Smart Mobile Devices Appointment Group** command creates a new appointment group that automatically includes all mobile devices meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you enter an information item on which records are to be matched. You can use any information items for mobile devices.
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The + and - buttons let you add new conditions or remove existing ones.

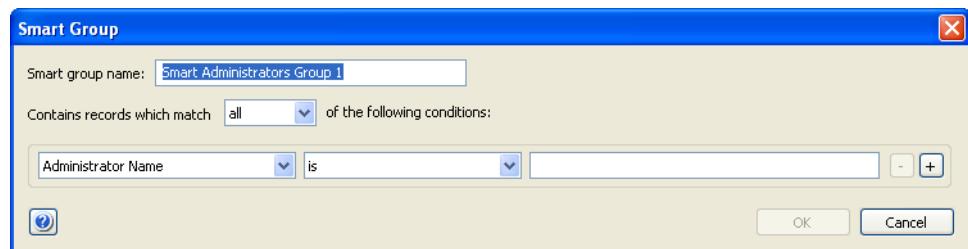
Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the "Save Administrator Info" command (described on page 344).

New Smart Administrator Group

The **New Smart Administrator Group** command creates a new administrator group that automatically includes all administrators meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server using the “Save Administrator Info” command (described on page 344).

Refresh

The **Refresh** command updates the information displayed in the **Active Directory** section with the current information from the Active Directory servers.

This command is only available when the **Active Directory** category or one of its subcategories is selected.

Custom Information Fields

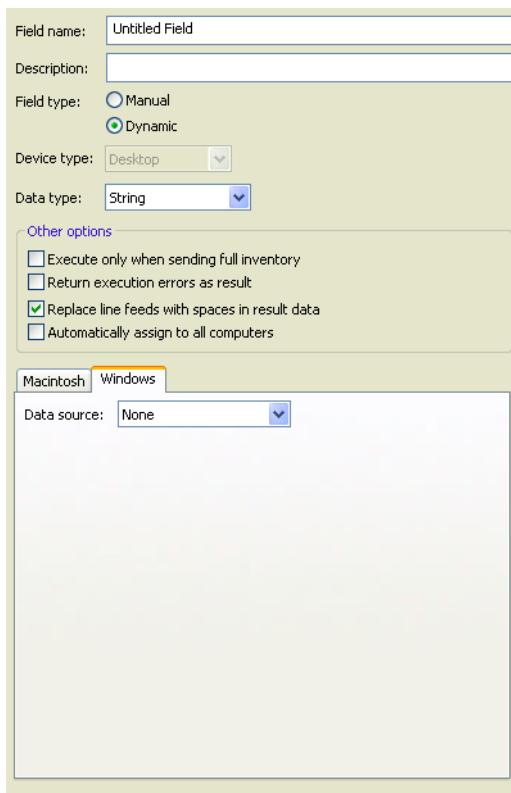
The **Custom Information Fields** submenu contains commands for creating custom information fields:

- **New Custom Information Field** (page 489)
- **Duplicate Custom Information Field** (page 493)

New Custom Information Field

The **New Custom Information Field** command creates a new custom information field.

Choosing the command displays the setup fields for the newly created field in the Server Center's main area:



The dialog contains these elements:

- **Field name:** The name of the custom information field under which it appears in the **Information Items** window.
- **Description:** An optional description of the field which is displayed as a tooltip in the **Information Items** window.
- **Data type:** The type of data that the field contains. Available types include:
 - **String:** Any unformatted text
 - **Number:** Any number. You can choose from several display formats.

- **Boolean:** True or false
- **Date:** A point in time
- **File Version:** A version number according to the conventions of the target platform
- **IP Address:** An IPv4 address (e.g., 192.168.0.1)
- **Enumeration:** A value from a predefined list. You must specify the list of possible values. (All values are treated as strings.)

Specifying the proper data type especially helps with sorting the records as expected.

- **Field type:** There are two types of custom information fields:
 - **Manual:** Information in the field is entered manually by you or other administrators.
 - **Dynamic:** Information in the field is automatically calculated by Absolute Manage.
- **Execute only when sending full inventory:** If this option is checked, the specified scripts are executed only when a full inventory is requested from the agent. (At the first contact, when the agent starts up, or later whenever the **Gather Inventory Information** command is issued with the **Force full inventory** option.)
If the option is unchecked, the script is executed also when the inventory is incrementally updated.
This option applies only to dynamic fields.
- **Return execution errors as result:** If this option is checked, any error information that is created during an unsuccessful execution of the specified scripts is returned and entered into the field.
If the option is unchecked, the field remains empty when the script encounters an execution error.
This option applies only to dynamic fields.
- **Replace line feeds with spaces in result data:** If this option is checked, Absolute Manage replaces all linebreaks in the results returned by the script with spaces, turning the result into a single line of text.
This option applies only to dynamic fields.
- **Automatically assign to all computers:** If this option is checked, the custom information field is automatically assigned to all client computers. If it is unchecked, it must be assigned manually to any client computer to which it is to apply.
This option applies only to dynamic fields.
- **Macintosh:** This tab lets you the program that is to gather the information for the custom information field on Mac OS X clients. The program must return the desired information as its result.
If an action has been defined for the Macintosh platform, a diamond is displayed on the tab.
This option applies only to dynamic fields.
It contains these elements:
 - **Data source:** The type of program or setting that Absolute Manage is to use on the clients to gather the information for the field.
Depending on the choice in this pop-up menu, different fields become available in the dialog pane.

- **File:** The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to Absolute Manage Server.
- **Executable:** The field is similar to **File**, described above. (This option is available for the **Other Executable** data source.)
- **Text:** The text of a script can be entered in this field. The entered script is executed on the target computers. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
Note: Absolute Manage offers no syntax verification or debugging functions for these scripts; we strongly recommend that you test the scripts before entering them here.
- **Command line options:** Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question). You can include environment variables in the options, as described in “Environment variables” on page 137.
This option is available for the **Unix Shell Script** and **Other Executable** data sources.
- **Transfer all files in folder containing executable:** If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the script is executed. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).
- **Execute as:** This pop-up menu allows you to specify a user account on the target computers with the privileges of which the script is executed. (This option is available for the **Unix Shell Script** and **Other Executable** data sources.)
- **Executable requires administrative privileges:** If this option is checked, the specified script is executed with administrator privileges on the target computers. (This option is available for the **Unix Shell Script** data source.)
- **Location:** The place where the desired plist preferences file is located. (This option is available for the **Property List Value** data source.)
*Note: The **Current Host** setting refers to preferences stored in **~/Library/ByHost/**.*
- **Domain:** The domain name used as an identifier for the plist file. This is the same as the file name without the .plist extension. (This option is available for the **Property List Value** data source when the **User Preferences** or **System Wide Preferences** location has been chosen.)
*Note: For example, the domain for the Dock’s preferences would be **com.apple.dock**.*

- **Full Path:** The full path to the desired plist file. (This option is available for the **Property List Value** data source when the **Full Path** location has been chosen.)
- **Key:** The top-level key in the plist file the value of which Absolute Manage returns as the custom field's contents. (This option is available for the **Property List Value** data source.)

Note: If you require value from the second or lower levels of a plist file, you have to extract them with a custom script.
- **Windows:** This tab lets you the program that is to gather the information for the custom information field on Windows clients. The program must return the desired information as its result.

If an action has been defined for the Macintosh platform, a diamond is displayed on the tab.

The tab contains these elements:

 - **Data source:** The type of program or setting that Absolute Manage is to use on the clients to gather the information for the field.

Depending on the choice in this pop-up menu, different fields become available in the dialog pane.
 - **File:** The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for the **Visual Basic Script**, **DOS Batch File**, and **PowerShell** data sources.)

Note: Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to Absolute Manage Server.
 - **Executable:** The field is similar to **File**, described above. (This option is available for the **Other Executable** data source.)
 - **Text:** The text of a script can be entered in this field. The entered script is executed on the target computers. (This option is available for the **Visual Basic Script**, **DOS Batch File**, and **PowerShell** data sources.)

Note: Absolute Manage offers no syntax verification or debugging functions for these scripts; we strongly recommend that you test the scripts before entering them here.
 - **Command line options:** Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question). You can include environment variables in the options, as described in "Environment variables" on page 137.

This option is available for the **Visual Basic Script**, **DOS Batch File**, **PowerShell**, and **Other Executable** data sources.
 - **Transfer all files in folder containing executable:** If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the script is executed. (This option is available for

the **Visual Basic Script, DOS Batch File, PowerShell, and Other Executable** data sources.)

Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).

- **Execute as:** This pop-up menu allows you to specify a user account on the target computers with the privileges of which the script is executed. (This option is available for all data sources.)
- **Registry Path:** The full path in the registry of the desired value. (This option is available for the **Registry Value** data source.)
All values are returned as strings, irrespective of the data type of the registry value.
You can include environment variables in the options, as described in “Environment variables” on page 137.

NOTE The **New Custom Information Field** command can be used only by administrators with the **Modify Custom Information Fields** right. See “New Administrator” on page 481 for details.

Duplicate Custom Information Field

The **Duplicate Custom Information Field** command lets you create a new custom information field based on an existing one.

Choosing the command displays the Custom Information Field dialog that is described in “New Custom Information Field” on page 489.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server, e.g., using the **Save Custom Information Fields** command (described on page 344).

NOTE The **Duplicate Custom Information Field** command can be used only by administrators with the **Modify Custom Information Fields** right. See “New Administrator” on page 481 for details.

Export Selected Fields

The **Export Selected Fields** command lets you export the definitions for the selected custom information fields to a file.

Choosing the command displays a standard Save dialog where you can specify the name and location for the file.

The command is not available when an external script file or other executable is specified in the definition on the field. (In other words, the command can be used for manual custom information fields and

for dynamic fields that are defined using inline scripts, property list values, or registry values.)

NOTE

Exported field definitions are stored in a simple XML file with the extension ".lanrevcfdef". They are intended to be imported into another copy of Absolute Manage Admin using the **Import Fields** command (see below).

Import Fields

The **Import Fields** command lets you import definitions for custom information fields that have previously been exported from Absolute Manage.

Choosing the command displays a standard Open dialog.

Edit <item>

The **Edit <item>** commands lets you edit existing items in the Server Center.

The actual name of the command reflects the selected item. If no item or an item that cannot be edited is selected, the command is not available.

Choosing any of the command opens the appropriate dialog. See the descriptions of the corresponding commands for details:

- **Edit Administrator: New Administrator**
- **Edit Administrator Group: New Administrator Group**
- **Edit Appointment Group: New Computer Appointment Group**
- **Edit Custom Information Field: New Custom Information Field**
- **Edit Disk Image: New Disk Image**
- **Edit License Specification: New License Specification**
- **Edit Payload: New Payload**
- **Edit Smart Group: New Smart Software Package Group** (or another smart group command)
- **Edit Software Package: New Software Package**
- **Edit Distribution Point: New Distribution Point**

Remove <item>

The **Remove <item>** commands lets you delete existing items in the Server Center.

The actual name of the command reflects the selected item. If no item or an item that cannot be deleted is selected, the command is not available.

Choosing any of the commands deletes the selected item.

NOTE Any changes become effective only when you commit them to the Absolute Manage Server using the appropriate command from the Server menu.

NOTE Using the commands may require specific rights in your administrator account. See “New Administrator” on page 481 for details.

Retrieve Payloads

The **Retrieve Payloads** command lets you download payloads from the distribution point to your local computer.

Choosing the command displays a standard Save dialog in which you can choose a location to which to download the payload file.

NOTE The **Retrieve Payloads** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 481 for details.

Retry Package

The **Retry Package** command causes Absolute Manage Server to re-attempt to install a failed software installation. This command is available only in the context menu of the content area and only when software packages, patches, or the **Installation Status** group or one of its subgroups are displayed.

Choosing this command makes the Absolute Manage Server retry the installation on all computers where it failed before. It does not re-attempt deferred or refused installations.

NOTE The **Retry Package** command can be used only by administrators with the **Retry Software Packages** right. See “New Administrator” on page 481 for details.

Reset Package

The **Reset Package** command causes Absolute Manage Server to treat the selected package as not yet having been installed on any

target computer. This command is available only in the context menu of the content area and only when software packages, patches, or the **Installation Status** group or one of its subgroups are displayed.

Choosing this command causes Absolute Manage Server to install the package on all computers in the distribution groups to which it is assigned, just as if the package was newly created, and irrespective of whether the package has already been installed on a computer or its installation been refused or deferred.

NOTE The **Reset Package** command can be used only by administrators with the **Reset Software Packages** right. See “New Administrator” on page 481 for details.

Install Selected Software Packages

The **Install Selected Software Packages** command is identical to the **Install Software Packages** command described on page 314, the only difference being that the software packages or metapackages on which you right-click are already selected in the command window.

Repeat Selected Installations

The **Repeat Selected Installations** command becomes available if one or more software installation entries in one of the smart groups in the **Installation Status** section is selected.

Choosing this command causes Absolute Manage to reset the installation status of the selected packages with respect to the selected computers, treating them as if they never had been installed. The packages will be installed on the computers according to their settings.

Reset Current Server Load

The **Reset Current Server Load** command causes Absolute Manage Server to reset the count of current connections for the selected distribution point to zero. This does not interrupt any actual connections; it merely changes the bookkeeping information. This command is available only in the context menu of the content area and only when distribution points are displayed.

This command is intended as a troubleshooting tool when the distribution point – perhaps as the consequence of a power outage or other crash – seems to count connections as open that have long since been closed.

Server Settings

The **Server Settings** category lets you view and specify basic settings for the connected Absolute Manage Server and set the names of client information fields.

Choosing the command displays the **Server Settings** dialog in the main area of the **Server Center** window. It has five panes:

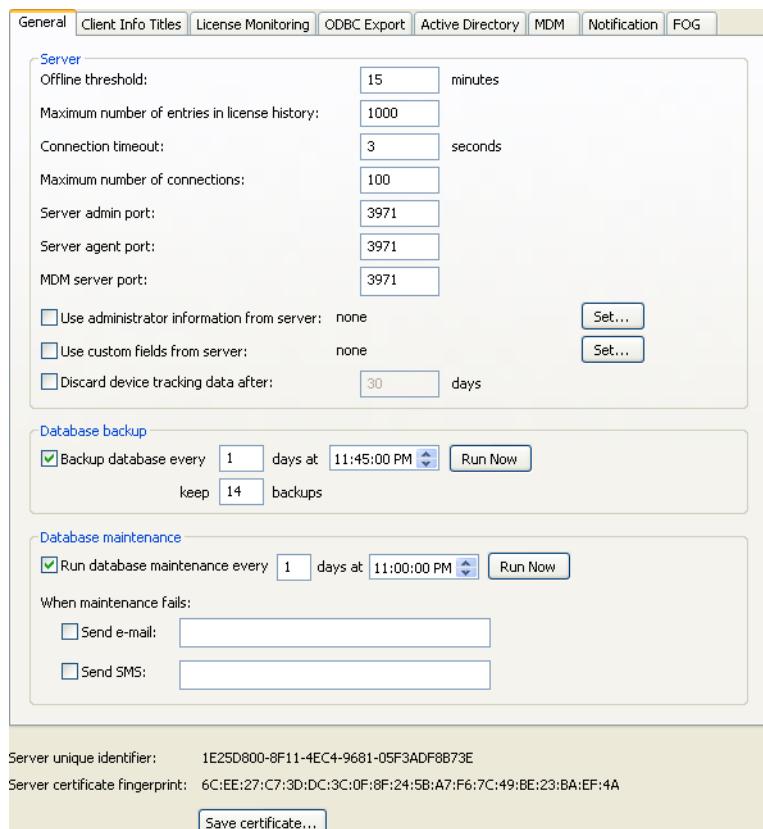
- **General** (page 497)
- **Client Info Titles** (page 500)
- **License Monitoring** (page 501)
- **ODBC Connection** (page 502)
- **Active Directory** (page 503)
- **MDM** (page 504)
- **FOG** (page 507)

NOTE

The **Server Settings** command can be used only by administrators with the **Change Server Settings** right. See “New Administrator” on page 481 for details.

General

The **General** pane lets you specify the basic server parameters.



The **General** pane contains these options:

- **Offline threshold:** The interval in which an agent must contact the server. If the server is not contacted by an agent for this time, it considers the agent's computer to be offline.
*Note: This interval should be no shorter than the **Heartbeat Interval** setting for the agents. (See "Servers" on page 289 for details.)*
- **Maximum number of entries in licensing history:** The maximum number of entries displayed in license history reports. If more entries are generated, only the newest entries are displayed.
Note: A license history entry records the entire licensing state at a given time, much like a snapshot in a backup history.
- **Connection timeout:** The time after which the server considers an attempt to establish a connection with an Absolute Manage Agent or Admin to have failed.
- **Maximum number of connections:** How many simultaneous connections to agents or admins will this server allow at most?
- **Server admin port:** The port over which the server communicates with Absolute Manage Admins.
- **Server agent port:** The port over which the server communicates with Absolute Manage Agents.
- **MDM server port:** The port over which the MDM server communicates.
Note: The three ports may be the same or different.
- **Use administrator information from server:** By default, each Absolute Manage Server contains its own administrator information (accounts, privileges, etc.). When another server is specified here, it instead dynamically gets the information from that server.
Clicking the **Set** button opens the **Server Properties** dialog where you can specify the server. The dialog is described below.
- **Use custom fields from server:** By default, each Absolute Manage Server contains its own custom field definitions. When another server is specified here, it instead dynamically gets the information from that server.
Clicking the **Set** button opens the **Server Properties** dialog where you can specify the server. The dialog is described below.
- **Discard computer tracking data after:** If this option is checked, Absolute Manage deletes data collected while tracking administered computers after the specified number of days.
Clicking the **Set** button opens the **Server Properties** dialog where you can specify the server. The dialog is described below.
- **Backup database every:** This option lets you specify the interval in which the Absolute Manage server's internal database is backed up as well as the number of backup generations that are kept.
Clicking the **Run Now** button performs the backup immediately.
Backup files are stored in the same directory as the database file itself.

- **Run database maintenance every:** This option lets you specify the interval in which the Absolute Manage server's internal database is maintained. Maintenance includes compacting the database file and checking it for possible corruption. If corruption is detected, Absolute Manage tries to correct the problem automatically. It informs you whether it appears to have succeeded or not. Clicking the **Run Now** button immediately creates a backup. Checking **Send e-mail** makes Absolute Manage send an e-mail to the specified address whenever database maintenance is not successful. You can have the e-mails sent to multiple addresses by separating them with commas. Checking **Send SMS** makes Absolute Manage send a text message (SMS) to the specified phone number whenever database maintenance is not successful. You can enter multiple phone numbers separated by commas to send messages to all of them.
- **Server unique identifier:** The unique identifier of the displayed server. You can use this information to verify that you are connected to the correct server.
- **Server certificate fingerprint:** The fingerprint of the SSL certificate with which the displayed server identifies itself. You can use this information to verify that you are connected to the correct server.
- **Save Certificate:** Clicking this button lets you save the server's certificate for use in identifying the server when you assign it to clients.

Server Properties dialog

The **Server Properties** dialog lets you specify a server that supplies administrator account information or custom field information to the server being configured.



The dialog contains these elements:

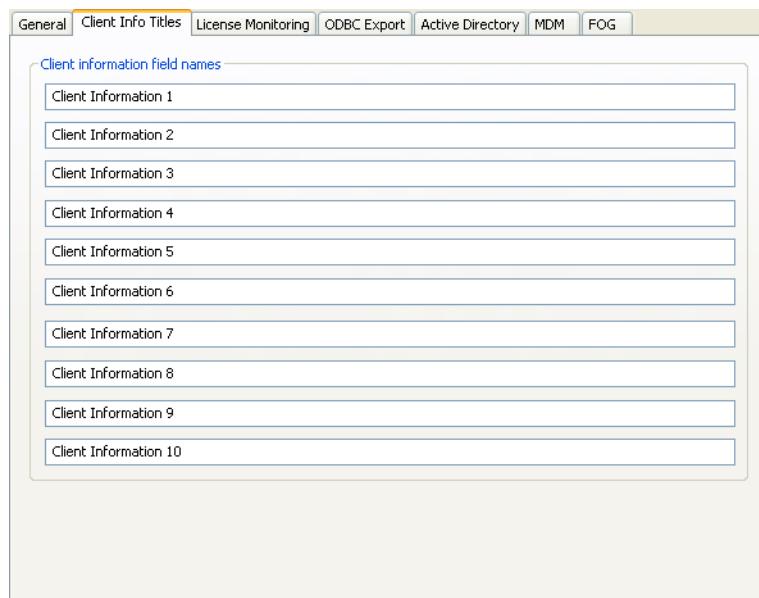
- **Server address:** The DNS name or IP address of the desired server.
- **Server port:** The port over which the specified server communicates with agents.
- **Server certificate:** This field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved. Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of the **Save Certificate** button in the **Server Settings** section of

the Server Center, as described in “Exporting a server certificate” on page 19.)

Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

Client Info Titles

The **Client Info Titles** pane of the **Server Settings** dialog contains the names of the ten client information fields in which you can store custom information on the clients.



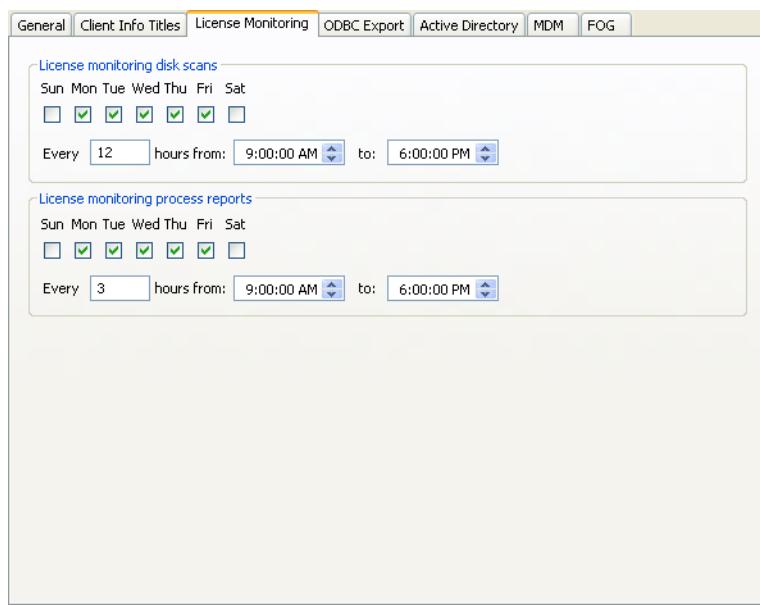
Editing one of the titles automatically changes the name of that client information field on all agents connected to the server.

NOTE

If multiple inventory servers are specified for an agent, it uses the client info titles of the first one in the list in the **Servers** pane of the **Agent Settings** dialog. (For more details, see “Servers” on page 289.)

License Monitoring

The **License Monitoring** tab of the **Server Settings** dialog lets you specify the schedules for the agents' license monitoring activities.



In the **Licensing monitoring disk scans** section, you can specify when and how often the Agent should scan the disk for licensed software. The Agent scans at all checked days of the week during the specified hours in the specified interval.

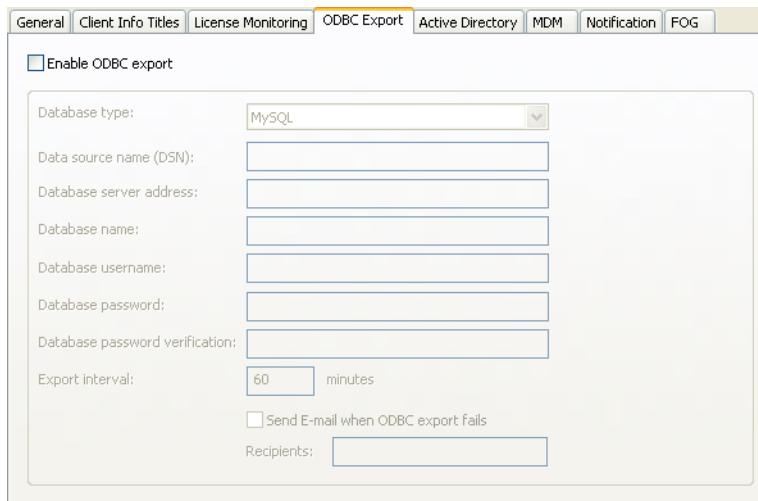
In the **Licensing monitoring process reports** section, you specify when and how often the Agent sends reports on licensed software to the server. Since these reports include both installed software and running software (if there are license specifications that are configured accordingly), it can make sense to send reports more often than disk scans are performed.

Any changes you make here are pushed to the Agents according to the license monitoring update interval settings. (The setting is specified in the **Servers** tab of the **Agent Settings** command window.)

ODBC Connection

The **ODBC Connection** tab lets you activate and configure link via ODBC to a database into which all data from Absolute Manage's internal database is exported at regular intervals.

NOTE This is a one-way link; no changes to the data in the target database are ever re-imported into Absolute Manage's internal database.



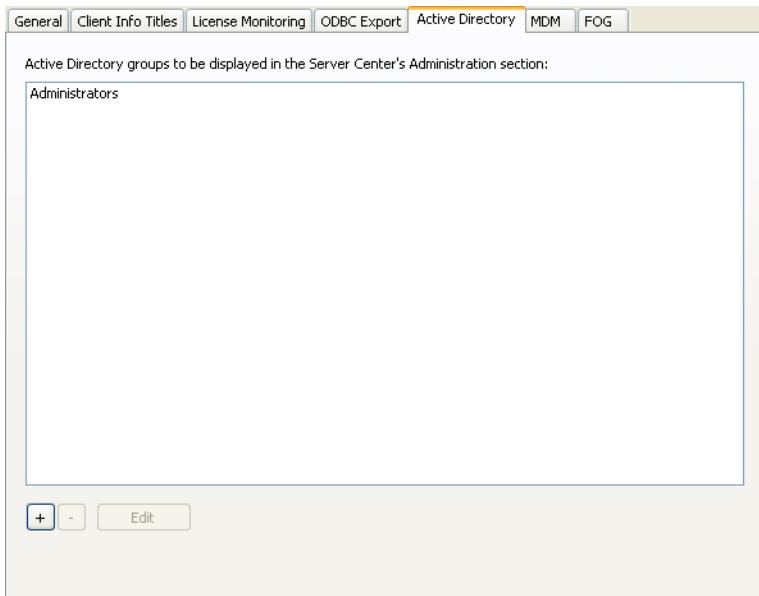
The **ODBC Connection** pane contains the options listed below. Note that all the database specifications (i.e., all options except **Enable ODBC export** and **Data source name**) can be omitted if they are already contained in the specified ODBC data source.

- **Enable ODBC export:** This is the master switch that activates or deactivates the automatic ODBC export.
- **Database type:** The type of the database that is connected via ODBC.
- **Data source name:** The ODBC data source that represents the database.
- **Database server address:** The DNS name or IP address of the server on which the database is hosted.
- **Database name:** A login name for the database. The corresponding account must have sufficient privileges to create tables and write data.
- **Database password and Database password verification:** The password for the specified database user account.
- **Export interval:** The interval in which Absolute Manage is to export data to the database.
- **Send e-mail when ODBC export fails:** If this option is checked, a notification e-mail is sent to the specified addresses. Separate multiple addresses with commas.

Active Directory

The **Active Directory** tab of the **Server Settings** dialog lets you specify the Active Directory groups the accounts in which Absolute Manage makes available for creating administrator accounts.

NOTE The accounts in the specified groups are not automatically made administrator accounts in Absolute Manage; they are merely available in the **Server Center** window's sidebar for this purpose. Account from groups not specified here are not available.



The tab contains these elements:

- List of groups: The list contains all groups you have so far specified.
- +: This button lets you add groups to the list. Clicking the button opens a dialog in which you enter the group's name.
- -: Clicking this button removes the selected group from the list.

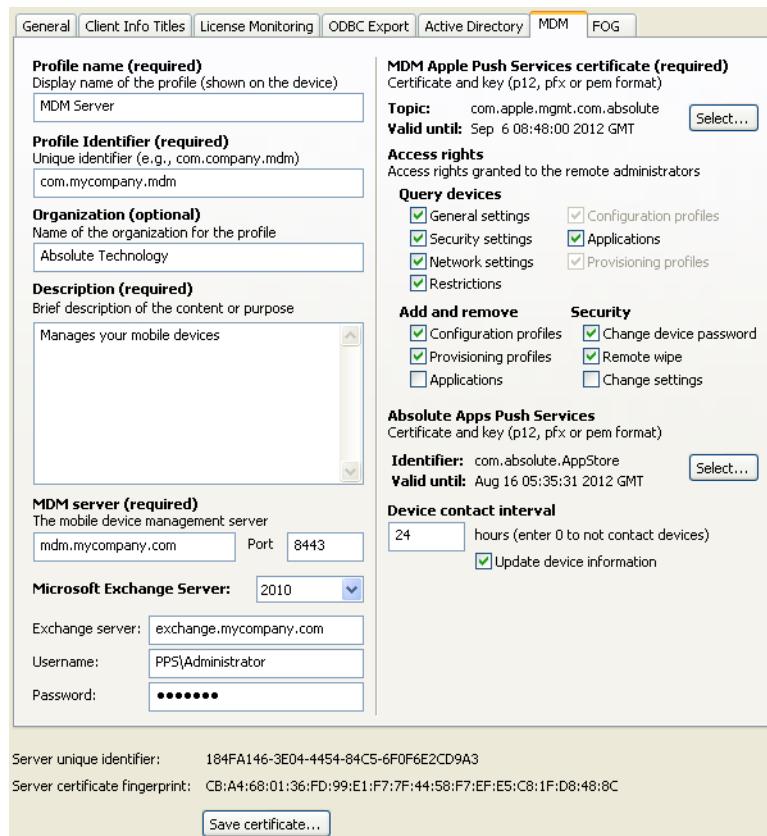
Double-clicking a group in the list opens a dialog that lets you change that group's name.

NOTE If an Active Directory account from one of the specified groups is moved out of the group, it will be deleted as an Absolute Manage administrator account.

MDM

The **MDM** tab of the **Server Settings** dialog lets you specify the settings required to manage mobile devices through Absolute Manage.

NOTE Any change in the Access rights section of this dialog has no effect on currently enrolled devices until they are re-enrolled (as described in “Enrolling mobile devices” on page 39).



The tab contains these elements:

- **Profile name:** A descriptive name for the deployment profile. The name will be displayed on the mobile device during the enrollment process.
- **Profile identifier:** A unique identifier for the deployment profile.
- **Organization:** The name of your organization. This information is optional.
- **Description:** A brief description of the purpose of the deployment profile. Users of mobile devices will see this description during the enrollment process.
- **MDM server:** The full DNS name of the mobile device management server into which the profile enrolls the mobile device. Also include the port over which the MDM server communicates.
- **Microsoft Exchange Server:** Choose the version of the Exchange server you want to use for Windows Phone MDM.

If you do not want to manage Windows Phone devices, choose **None**. (This disables the following three items.)

- **Exchange Server:** Enter in this field the Internet address for the Exchange server you want to use.
- **Username:** Enter the username of an account on the Exchange server. Depending on the version of Exchange you are using, the account must have certain privileges.
Exchange 2007 accounts must have all of these privileges:
 - View-only administrator
 - Recipient administrator
 - Organization administrator
 - Server administrator
 - Local administrator (for the Exchange server used)Exchange 2010 accounts must have all of these privileges:
 - Server management
 - Organization management
 - Recipient managementIrrespective of the Exchange version, the account you specify must be a member of the Admin group on the computer on which Absolute Manage Server is running.
- **Password:** Enter in this field the password name of the specified account.
- **MDM Push Services certificate:** Clicking the **Select** button lets you create or select a certificate for validating the MDM server to the mobile devices.
Clicking the button opens an assistant in which you can either select an existing certificate (must be located as a file on your computer) or create a new one.
Creating a new certificate requires you to enter your name and company information which is then saved as a certificate request and uploaded to an Apple server. You download the certificate from the same server as a file and select it.
- **Query devices for:** These checkboxes determine the information from the managed mobile devices that administrators can view:
 - **General settings:** Administrators can view the general settings of an administered mobile device.
 - **Security settings:** Administrators can view the security-related settings of an administered mobile device.
 - **Network settings:** Administrators can view the network settings of an administered mobile device.
 - **Restrictions:** Administrators can view the restrictions in effect on an administered mobile device.
 - **Configuration profiles:** Administrators can view the configuration profiles installed on an administered mobile device. This setting can only be changed when **Configuration profiles** is unchecked in the **Add and remove** section (see below).
 - **Applications:** Administrators can view the applications that are installed on the mobile device. This includes both applications from the iTunes store and in-house applications.
 - **Provisioning profiles:** Administrators can view the provisioning profiles installed on an administered mobile device. This setting can only be changed when

Provisioning profiles is unchecked in the **Add and remove** section (see below).

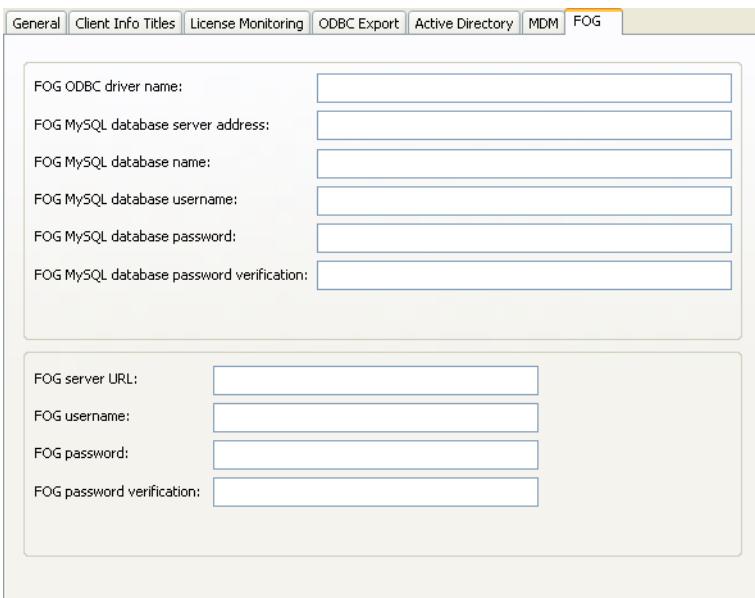
- **Add and remove:** These checkboxes determine the which kind of profiles administrators can delete from the device or add to it:
 - **Configuration profiles:** The administrators can add or delete configuration profiles. Only administrators with the Modify Mobiel Device Configuration Profiles privilege can do so.
 - **Provisioning profiles:** The administrators can add or delete provisioning profiles. Only administrators with the Modify Mobile Applications privilege can do so.
 - **Applications:** The administrators can install apps on the device using the **Install Application** command and delete them using **Delete Application**. This feature is not available for devices running iOS 4.x.
- **Security:** These checkboxes determine the which kind of security-related operation the administrators with the Manage Mobile Devices privilege can perform on the mobile device:
 - **Change device password:** The administrators can set a new password for the device.
 - **Remote wipe:** The administrators can remotely erase the entire contents of the mobile device.
This resets the device to its factory condition. Note that this also removes the MDM settings from the device, so that it is no longer possible to access it from Absolute Manage.
 - **Change settings:** The administrators can remotely change certain settings on the mobile device, such as roaming options. In contrast to specifying these settings via profiles, the settings are changed directly and can be changed back by the user of the managed device.
- **AbsoluteApps Push Services certificate:** The certificate needed for the server to inform devices of new and updated in-house applications available in the AbsoluteApps app and send them messages.
This certificate is needed only when you plan to distribute in-house apps to iOS devices. If you will not do so, specifying this certificate provides no benefits.
You can obtain an app push services certificate from Apple's iPhone Provision Portal.
- **Device contact interval:** The interval in which the MDM server sends a request to managed mobile devices to contact the server and updates its status.
These contact requests are sent through Apple's notification servers and are subject to a timeout on these servers; i.e., when there is no contact to the mobile device for a certain time, the contact request is removed without having been delivered to the device. The length of the timeout is unknown but believed to be a few days. We therefore recommend to set the contact interval no higher than 48 hours to ensure that the timeout period does not cause contact requests to fail, e.g., for devices that are switched off for long periods of time.
- **Update device information:** If this option is checked, the information about the device stored in the Absolute Manage

database is updated each time the device contacts the MDM server. (This information includes data on hardware, operating system, network used, and installed software.)

If the option is off, the information stored on the device is never updated.

FOG

The **FOG** tab of the **Server Settings** dialog lets you specify the settings for reinstalling administered computers with the **Reinstall Windows Computer** command.



The tab contains these elements:

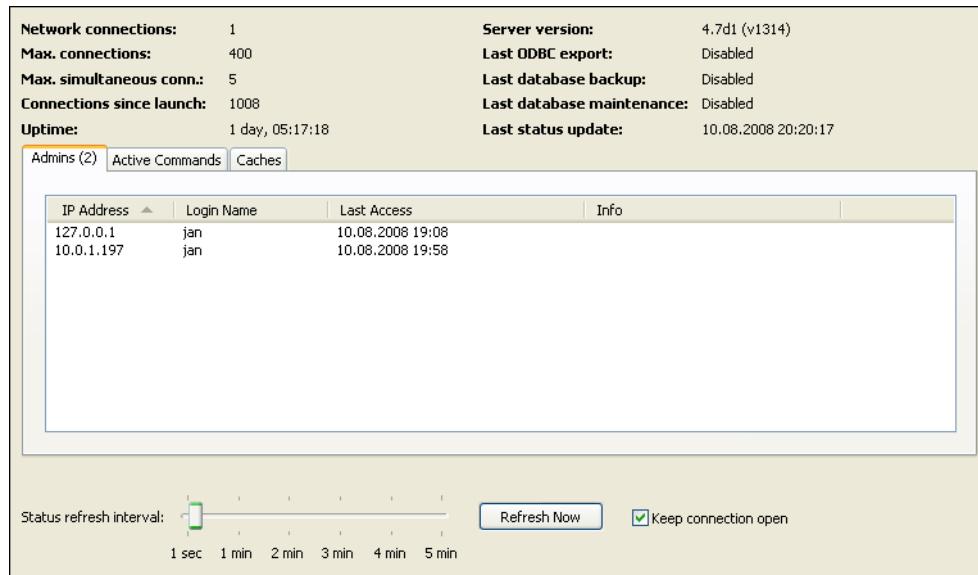
- **FOG ODBC driver name:** The name of the ODBC driver which the Absolute Manage Server computer is to access the MySQL database of the FOG server.
- **FOG MySQL database server address:** The IP address or DNS name of the computer on which the FOG MySQL database server is running.
- **FOG MySQL database name:** The name of the MySQL database used by the FOG software.
- **FOG MySQL database username:** The account name that Absolute Manage Server is to use to access the FOG MySQL database.
- **FOG MySQL database password:** The password for the account.
- **FOG MySQL database password verification:** The password for the account repeated, to guard against typos.
- **FOG server URL:** The IP address or DNS name of the computer on which the FOG server (i.e., the FOG software itself, not the MySQL database server it is using) is running and the path of the FOG management directory on that computer. For example: <http://myfogserver.company.com/fog/> management/.
- **FOG username:** The account name that Absolute Manage Server is to use to access the FOG server.

- **FOG password:** The password for the account.
- **FOG password verification:** The password for the account repeated, to guard against typos.

Server Monitor

The **Server Monitor** category in the **Server Center** window lets you view current server activities.

Selecting the category displays a range of information in the main area of the **Server Center** window:



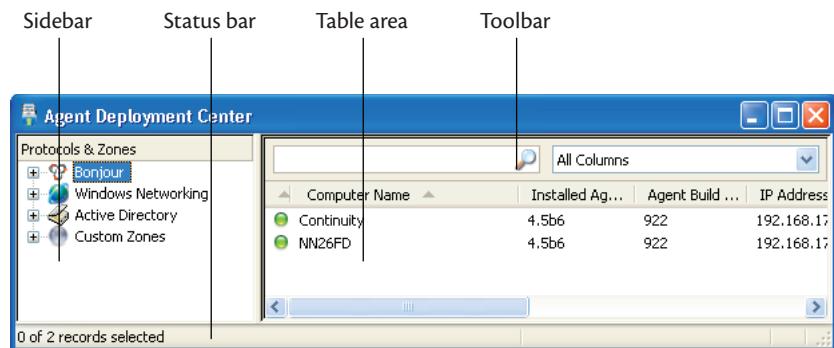
The monitor contains these elements:

- **Network connections:** The number of active network connections of the server.
- **Max. connections:** The maximum number of connections that is configured on this server. (This is the total number of connections; the **Maximum number of connections** field in the Absolute Manage Server's **Server Settings** dialog specifies only the number of outgoing agent connections.)
- **Max. simultaneous conn.:** The maximum number of simultaneous network connections on this server since it was last launched.
- **Connections since launch:** The total number of network connections on this server since it was last launched.
- **Uptime:** The amount of time that has elapsed since the last time the server was launched.
- **Server version:** The version number of the server.
- **Last ODBC export:** The time when the last ODBC export was performed. If ODBC exports are not activated, "Disabled" is displayed.
- **Last database export:** The time when the last database backup was performed. If database backups are not activated, "Disabled" is displayed.

- **Last database maintenance:** The time when the database maintenance was performed. If database maintenance is not activated, “Disabled” is displayed.
- **Last status update:** The time when the information displayed in the server monitor was last updated.
- **Admins:** The number of administrators who have been logged in on this server since the last time the server was restarted (including administrators who are currently logged in). Clicking this tab displays an overview of these admins.
- **Active commands:** The number of commands that are currently being executed on the server. Clicking this tab displays a list of the commands.
- **Caches:** Clicking this tab displays a breakdown of the requests by type as well as the maximum numbers of agent request or inventory requests that were cached at the same.
- **Status Refresh Interval:** The interval for automatic updates of the information displayed in the server monitor.
- **Refresh Now:** Clicking this button updates the the information displayed in the server monitor irrespective of the refresh interval.
- **Keep connection open:** If this option is checked, the connection to the server is not closed after the data has been refreshed. This helps reduce network overhead in case of frequent updates.

The Agent Deployment Center is a module of the Absolute Manage system that lets you install and update agents on supported computers in the network without having to physically visit these computers. It is controlled from the **Agent Deployment Center** window in Absolute Manage Admin.

NOTE The Agent Deployment Center can be used only by administrators with the **Deploy Agents** right. See “New Administrator” on page 481 for details.



The elements of the **Agent Deployment Center** window are described below:

- **Toolbar** (page 511)
- **Table columns** (page 511)
- **Sidebar** (page 512)
 - **Sidebar context menu** (page 512)
 - **New Custom Zone** (page 512)
 - **Edit Custom Zone** (page 516)
 - **Remove Custom Zone** (page 516)
 - **Search Zone** (page 517)
 - **Cancel Search** (page 517)
 - **Refresh** (page 517)
 - **New Smart Group** (page 517)
 - **Edit Smart Group** (page 518)
 - **Remove Smart Group** (page 518)
 - **Import Zones File** (page 518)
 - **Table context menu** (page 519)
 - **Copy** (page 519)
 - **Copy “<information item>”** (page 520)
 - **New Smart Group from “<information item>”** (page 520)
 - **Install Agent** (page 520)
 - **Remove Agent** (page 522)
 - **Set Inventory Server** (page 523)
 - **Refresh Status** (page 526)

Toolbar

The **Agent Deployment Center** window toolbar lets you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Table columns

The main table in the **Agent Deployment Center** window displays network devices found in the zones that have been searched. The columns in the table display information items that are mostly described in “Agent Deployment Center” on page 585.

In addition, to the named columns displaying information items, the first column indicates the status of the device:

- A green dot indicates that the current version of Absolute Manage Agent is installed on the computer.
- A yellow dot indicates that an outdated version of Absolute Manage Agent is installed on the computer.
- A red dot indicates that Absolute Manage Agent is not installed on the computer but could be installed.
- A grey dot indicates a device that does not support Absolute Manage Agent, i.e., one of the following:
 - A computer with an incompatible operating system (i.e., Mac OS X when you are installing from a Mac OS X Windows Admin)
 - A non-computer device (such as a router or printer)
 - A computer that could support Absolute Manage Agent but on which the required connection protocol (Window File and Printer Sharing for the Windows Admin) is disabled.

Sidebar

The **Agent Deployment Center** window contains a sidebar with predefined and custom zones reflecting the network structure:

- **Bonjour**: All Bonjour (previously known as Rendezvous, an implementation of ZeroConfig) zones.
- **Windows Networking**: All Windows networking domains and groups defined in your network and the computers contained in them.
- **Active Directory**: All Active Directory zones in your network. If there are no Active Directory servers in your network, this sidebar entry is missing.
- **Custom zones**: All zones that you have defined.

Clicking on any zone displays the network devices that have been found in that zone.

Sidebar context menu

The context menu of the **Agent Deployment Center** window's sidebar contains commands for managing custom zones.

The commands are described in detail in the following sections.

- “New Custom Zone” on page 512
- “Edit Custom Zone” on page 516
- “Remove Custom Zone” on page 516
- “Search Zone” on page 517
- “Cancel Search” on page 517
- “Refresh” on page 517
- “New Smart Group” on page 517
- “Edit Smart Group” on page 518
- “Remove Smart Group” on page 518
- “Import Zones File” on page 518

New Custom Zone

The **New Custom Zone** command creates a new zone in the **Custom Zones** section and lets you specify automatic scanning of this zone for computers and installation of agents on them.

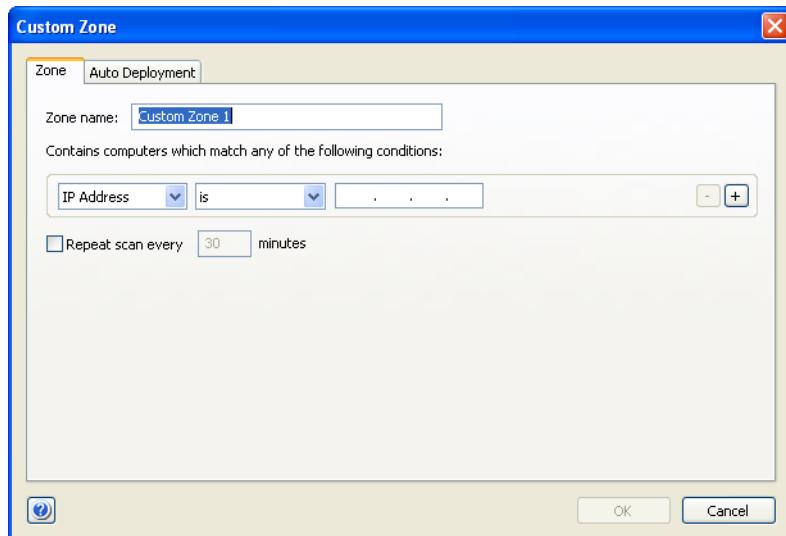
Choosing the command opens the **Custom Zone** dialog, which has two panes:

- **Zone**
- **Auto Deployment**

Both are described below.

Zone

The **Zone** pane of the **Custom Zones** dialog lets you define a virtual network zone that Absolute Manage uses to search for computers and for deploying agents:

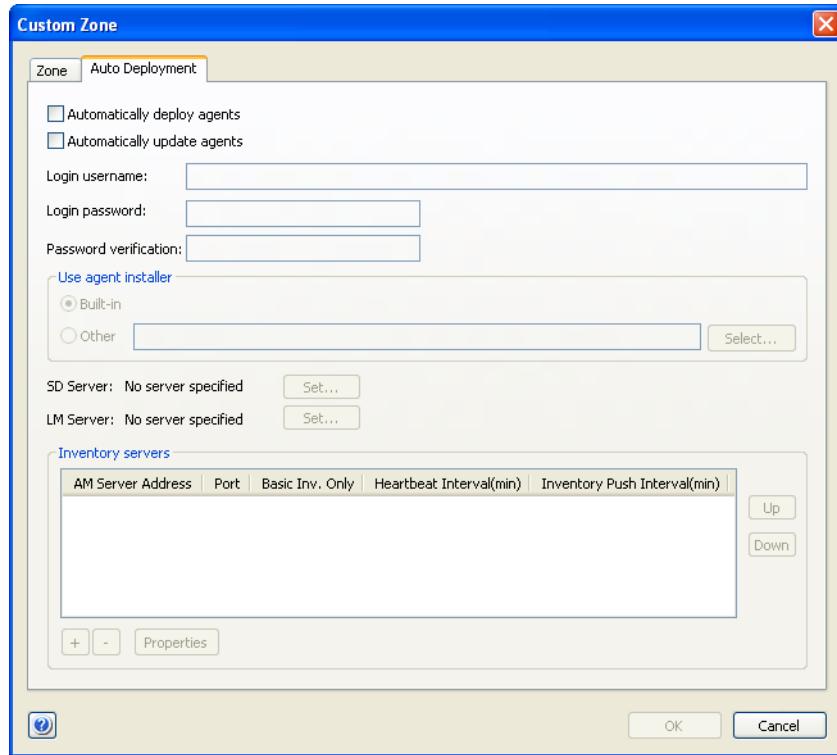


The pane contains these elements:

- **Zone Name:** The name under which your custom zone will be displayed.
- Condition area: Choose between including computers in zones by IP address or by host name. For IP addresses, you can choose between single addresses or address ranges by means of the second pop-up menu. The text field lets you enter the address or name to look for. The + and - buttons let you add new conditions or remove existing ones. A zone includes all computers that match any of the specified conditions (Boolean OR).
- **Repeat scan every:** Check this option and enter a number of minutes to have Absolute Manage scan this zone automatically for new computers in the specified interval.
Note: This setting is particularly useful in combination with automatic deployment of agents, as described below.

Auto Deployment

The **Auto Deployment** pane of the **Custom Zones** dialog lets you specify whether and how to automatically install agents on computers found in the zone on which no agent is present:



NOTE

Automatic installation is possible only on computers running the same operating system as your administrator workstation. That is, if you are running Absolute Manage Admin on Mac OS X, you can automatically deploy only to client computers running Mac OS X. And from Absolute Manage Admin for Windows, automatic deployment is only possible to computers running Windows.

The pane contains these elements:

- **Automatically deploy agents:** If this option is checked, Absolute Manage automatically installs Absolute Manage Agents on computers found in this zone that do not already have them.
- **Automatically update agents:** If this option is checked, Absolute Manage automatically updates any Absolute Manage Agents found on computers in this zone when they are outdated.
- **Login username:** The username that is to be used for NetBios login on the selected computers. The account names (as well as the passwords) are case-sensitive. You must use the abbreviated username.
If you are using network domains for your Windows computers, you must prefix the account name with the domain name. (No prefix is required when you are using workgroups.)
- **Login password:** The password for the NetBios account.

- **Password verification:** Re-enter the password to guard against typos.
- **Use Agent installer:** Choose **Built-in** if the installer embedded in Absolute Manage Agent is to be used for installing the Agent. Choose **Other** to specify a custom installer using the **Select** button.
- **SD Server:** The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described below in “Server Properties dialog” on page 516.
- **SM Server:** The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 516.
- **Inventory servers:** This table lists all known Absolute Manage inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.
The list contains these columns:
 - **AM Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
 - **Port:** The port over which the server communicates with agents.
 - **Basic Inv. Only:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
 - **Heartbeat Interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See “Server Settings” on page 497 for details.)
 - **Inv. Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)
Double-clicking a server displays a dialog for editing its settings. The dialog is described in “Inventory Server Properties dialog” on page 525.
- Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server’s setting; the dialog is described in “Inventory Server Properties dialog” on page 525. Clicking the **-** button removes the selected server.

Server Properties dialog

The **Server Properties** dialog lets you specify a software distribution or license monitoring server.



The dialog contains these elements:

- **Server address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
- **Server port:** The port over which the server communicates with agents.
- **Interval:** The interval in which the agents are to check the software distribution server for new installation packages or check the license monitoring server for changes to the license specifications, respectively.
- Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of the **Save Certificate** button in the **Server Settings** section of the Server Center, as described in "Exporting a server certificate" on page 19.)
The certificate is required for specifying the server.

Edit Custom Zone

The **Edit Custom Zone** command lets you edit an existing custom zone.

Choosing the command opens the **Custom Zone** dialog that is described in "New Custom Zone" on page 512.

Remove Custom Zone

The **Remove Custom Zone** command deletes a custom zone.

Choosing the command deletes the selected custom zones. A confirmation alert is displayed first.

Search Zone

The **Search Zone** command searches the selected zone for network devices.

Choosing the command makes Absolute Manage admin scan the network range specified in the zone for client computers.

While a zone scan is in progress, the command changes to **Cancel Search**, described below.

NOTE It takes approximately a tenth of the server connection timeout set in the **Settings** dialog (see “Settings” on page 275) to scan one IP address when there is no device present at that address; i.e., about a second at the default timeout of ten seconds. When a device is present, scanning is usually faster.

Cancel Search

The **Cancel Search** command terminates the current scan of the selected zone.

This command replaces the **Search Zone** command, described above, while a zone scan is under way.

Refresh

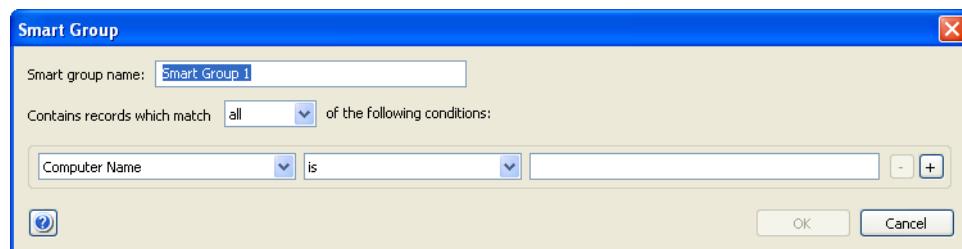
The **Refresh** command recreates the Windows Networking domains and workgroups and redispays the computers within them.

This command is only available when the **Windows Networking** category is right-clicked.

New Smart Group

The **New Smart Group** command creates a new smart group for found network devices.

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
 - The pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The **+** and **-** buttons let you add new conditions or remove existing ones.

NOTE Devices may appear multiple times in smart groups when they were found using more than one method (e.g., through Bonjour and by scanning an IP range.)

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the **Smart Group** dialog described in “New Smart Group” on page 517.

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Import Zones File

The **Import Zones File** command lets you import zones definitions from a text file.

Choosing the command adds the zones specified in the text file to the currently existing zones. To avoid ending up with duplicate zones, you may need to delete existing zones before importing the file.

Files may include the following specifications:

- Zone names are standard text on a line by themselves.
Zone names must contain at least one character.
The specification of what is to be included in the zone follows in the lines below the zone name. Anything up to the next zone name is considered to belong to the zone's definition.
Available specifications include single addresses, address ranges, subnets, and named domains, as described below.
- An IP address indicates a single computer to include in the zone.
Example: 10.7.23.123
- Two IP addresses divided by a hyphen indicate an address range.
Example: 10.7.33.1 - 10.7.33.127
- An IP address and a network mask connected by an ampersand indicate a subnet.
Example: 10.7.23.123 & 255.255.0.0
- Text included in quotation marks is considered a domain.
Example: "poleposition-sw.com"
- Text following a semicolon (;), number sign (#), or two slashes (//) up to the end of the line is considered a comment and is ignored.
Example: // This is a comment

Table context menu

The context menu of the **Agent Deployment Center** window's table area contains commands for installing and uninstalling Absolute Manage Agent and refreshing the display.

The commands are described in detail in the following sections.

- “Copy” on page 519
- “Copy “<information item>”” on page 520
- “New Smart Group from “<information item>”” on page 520
- “Install Agent” on page 520
- “Remove Agent” on page 522
- “Set Inventory Server” on page 523
- “Refresh Status” on page 526

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 273.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (e.g., **Copy “Inventory Server”**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Group from “<information item>”

The **New Smart Group from “<information item>”** command lets you create a smart group with pre-filled criteria.

Choosing the command opens the **Search Zone** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

Install Agent

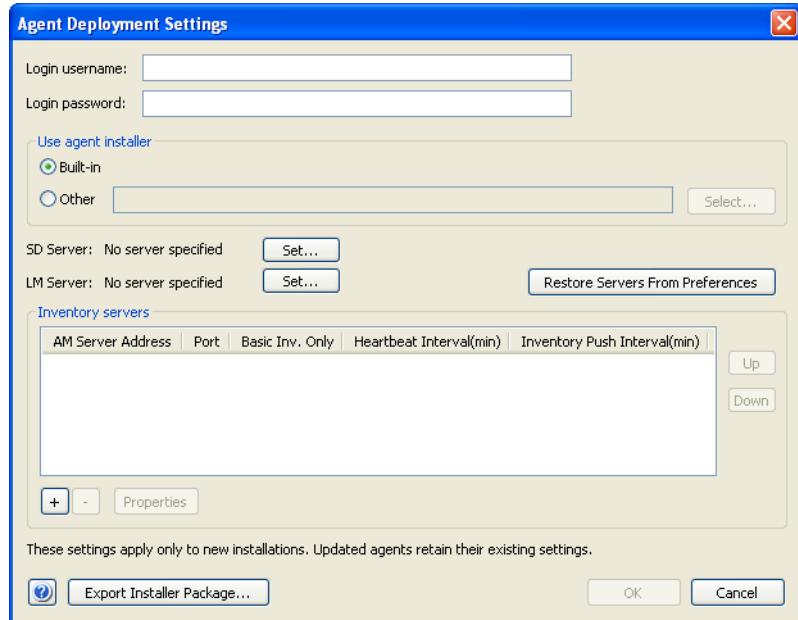
The **Install Agent** command installs Absolute Manage Agent on the selected computers. If an older version of Absolute Manage Agent is already present on the computer, it is updated.

You can install Absolute Manage Agents only on the same platform on which your copy of Absolute Manage Admin is running, i.e., you cannot deploy Windows agents from Mac OS X or vice versa.

The command is available only if Absolute Manage Agent can be installed on the selected computer.

NOTE Windows File & Print Sharing must be active on the target computers for this installation to work.

Choosing the command opens the **Agent Deployment Settings** dialog:



The dialog contains these elements:

- **Login username:** The username that is to be used for NetBIOS login on the selected computers. The username must include the domain to which the target computers belong. You can omit the domain name only when the computer does not belong to a domain.
- **Login password:** The password for the NetBIOS account.
- **Use Agent installer:** Choose whether the installer embedded in Absolute Manage Agent is to be used for installing the Agent or a custom installer that you provide.
- **Select:** Clicking this button lets you select a custom installer.
- **SD Server:** The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in "Server Properties dialog" on page 516.
- **SM Server:** The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in "Server Properties dialog" on page 516.
- **Restore Servers from Preferences:** Clicking this button selects the inventory servers that have been specified in the **Deployment Center Deployment Center** pane of the **Preferences Settings** dialog.
- **Inventory servers:** This table lists all known Absolute Manage inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.
The list contains these columns:
 - **AM Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To

avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).

- **Port:** The port over which the server communicates with agents.
- **Basic Inv. Only:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
- **Heartbeat Interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See "Server Settings" on page 497 for details.)
- **Inv. Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

Double-clicking a server displays a dialog for editing its settings. The dialog is described in "Inventory Server Properties dialog" on page 525.

- Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described in "Inventory Server Properties dialog" on page 525. Clicking the **-** button removes the selected server.
- **Export Installer Package:** Clicking this button lets you save a custom installer package that includes both the server settings you have specified in this dialog as well as the required certificates.

You can use this installer package in the **Use agent installer** section of this dialog.

Except for the servers to assign, the presets in all fields are specified in the **Settings** dialog (see page 275).

NOTE

If the built-in Windows firewall is active on a client computer, installing the Absolute Manage Agent automatically opens the agent port as specified in the **Settings** dialog (usually port 3970).

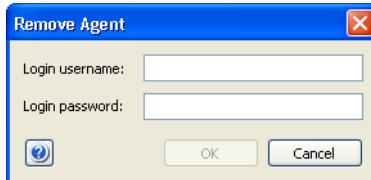
Remove Agent

The **Remove Agent** command removes Absolute Manage Agent from the selected computers.

You can remove Absolute Manage Agents only from the same platform on which your copy of Absolute Manage Admin is running, i.e., you cannot remove Windows agents from an admin running on Mac OS X or vice versa.

The command is available only if Absolute Manage Agent is installed on the selected computer. It is not available if no Absolute Manage Agent is present or if SSH is disabled on the target computer.

Choosing the command opens the **Remove Agent** dialog:



The dialog contains these elements:

- **Login username:** The username that is to be used for NetBIOS login on the selected computers.
- **Login password:** The password for the NetBIOS account.
- **Password verification:** Re-enter the password to guard against typos.

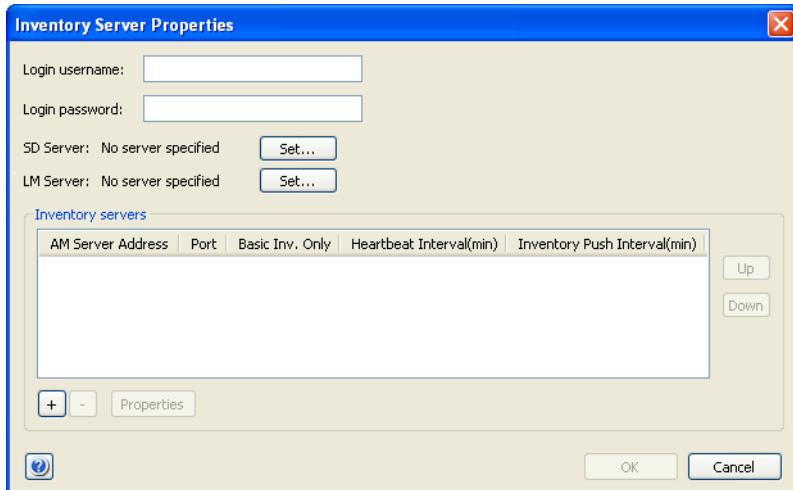
The presets in all fields are specified in the Settings dialog (see page 275).

Set Inventory Server

The **Set Inventory Server** command assigns Absolute Manage Servers to selected computers.

The command is available only if Absolute Manage Agent is installed on a selected computer. It is not available if no Absolute Manage Agent is present or if the selected computer does not run Windows.

Choosing the command opens the **Inventory Server Properties** dialog:



The dialog contains these elements:

- **Login username:** The Windows File & Print Sharing username for connecting to the client.
- **Login password:** The password for the specified Windows File & Print Sharing account.
- **SD Server:** The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 516.
- **LM Server:** The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 516.
- **Inventory servers:** This table lists all known Absolute Manage inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.

The list contains these columns:

- **AM Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
- **Port:** The port over which the server communicates with agents.
- **Basic Inv. Only:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
- **Heartbeat Interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See “Server Settings” on page 497 for details.)
- **Inv. Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

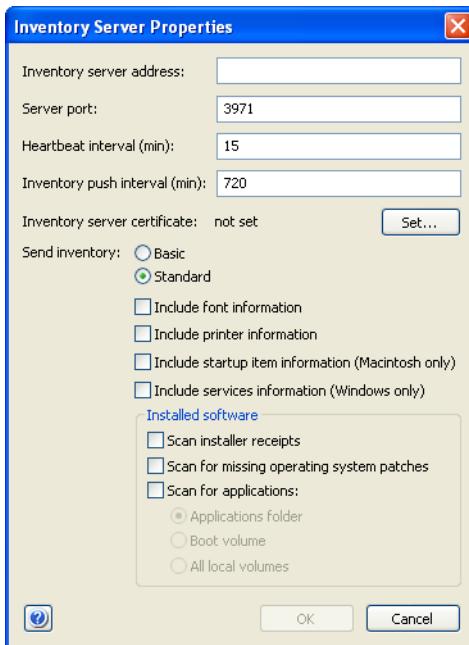
Double-clicking a server displays a dialog for editing its settings. The dialog is described below.

Clicking the **Up** button moves the selected entry up in the list, clicking the **Down** button moves it down.

Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server’s setting; the dialog is described below. Clicking the **-** button removes the selected server.

Inventory Server Properties dialog

The **Inventory Server Properties** dialog lets you specify details about how an agent interacts with an inventory server.



The dialog contains these elements:

- **Inventory Server Address:** The IP address or DNS name of the server.
Note: If you enter an abbreviated DNS name (i.e., one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (i.e., ones that include the full domain).
- **Server Port:** The port over which the server communicates with agents.
- **Heartbeat interval:** The interval in which the agents are to contact the server to let it know that they are still available.
Note: This interval should not be longer than the Agent Offline Threshold setting of the Absolute Manage Server. (See "Server Settings" on page 497 for details.)
- **Inventory Push Interval:** The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)
- **Inventory server certificate:** This field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.
Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of

the **Save Certificate** button in the **Server Settings** section of the Server Center, as described in “Exporting a server certificate” on page 19.)

- **Send inventory:** This lets you specify the amount of inventory information the agent sends by default:
 - **Basic:** If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this sever. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
 - **Standard:** If this option is checked, the agents send the usual complete range of information to the server. We recommend that you use this option for administered clients.
 - **Include font information:** The agent automatically includes information on installed fonts when sending inventory information to the server.
 - **Include printer information:** The agent automatically includes information on connected printers when sending inventory information to the server.
 - **Include startup item information:** The agent automatically includes information on installed startup items when sending inventory information to the server.
 - **Include service information:** The agent automatically includes information on running services when sending inventory information to the server.
 - **Scan installer receipts:** The agent automatically scans the installer receipts on the computer when it is requested to determine the installed software.
 - **Scan for missing operating system patches:** The agent automatically scans the computer for available operating system patches that are not installed when it is requested to determine the installed software.
 - **Scan for application:** You can specify the default location where the agent looks for installed applications when requested to do so.

Refresh Status

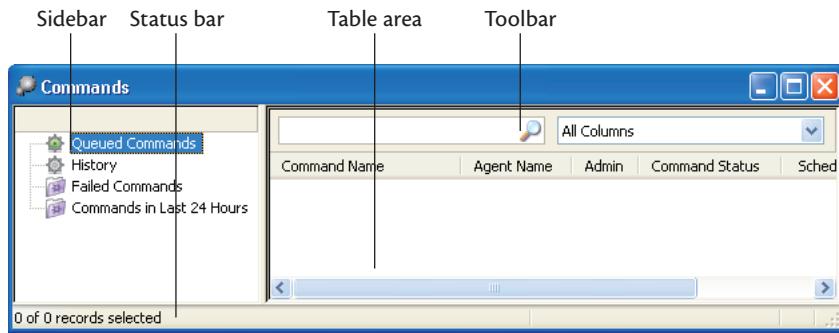
The **Refresh Status** command updates the displayed information for the selected network devices.

Choosing the command causes Absolute Manage Admin to query the device and update the displayed information.

Chapter 22

Commands window

The **Commands** window lists all commands that are pending, that are being executed, that have been executed and those that have failed. It lets you reschedule and edit these commands or re-execute completed commands.



The elements of the **Commands Center** window are described below:

- **Toolbar** (page 527)
- **Table columns** (page 528)
- **Sidebar** (page 528)
- **Context menus** (page 528)
 - **Copy** (page 529)
 - **Copy “<information item>”** (page 529)
 - **New Smart Command Queue Group from “<information item>”** (page 529)
 - **New Smart Command History Group from “<information item>”** (page 530)
 - **New Smart Command Queue Group** (page 530)
 - **New Smart Command History Group** (page 531)
 - **Edit Smart Group** (page 531)
 - **Remove Smart Group** (page 532)
 - **Scheduling Options** (page 532)
 - **Execute Command Now** (page 532)
 - **Edit Command** (page 532)
 - **Reapply Command** (page 532)
 - **Remove Command** (page 533)
 - **Show Command Result** (page 533)

Toolbar

The **Commands** window toolbar lets you quickly restrict the display to records that contain the search text entered in the toolbar. The pop-up menu lets you specify whether all columns should be searched or just one particular column.



The text field lets you quickly restrict the display to commands that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Clicking the magnifying glass icon at the right of the field executes the search.

Table columns

The columns displayed in the **Commands** window are described in “Commands” on page 570.

Sidebar

The **Commands** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

- **Queued Commands:** All commands that are pending execution, either because they have been scheduled for a future date or because they have been deferred.
- **History:** All commands that have already been completed, successfully or unsuccessfully. Because the history includes the results for each command (in the **Command Result Error** and **Command Error Info** columns), it also provides a command log.
- **Failed Commands:** All commands that Absolute Manage has attempted to execute but that have failed. (Does not include deferred commands, i.e., commands that could not yet be executed because the target computer is unavailable.)
- **Commands in Last 24 hours:** All commands that have been completed, successfully or unsuccessfully, in the last 24 hours.

Any additional smart groups that you define are displayed below these groups.

Context menus

The context menus of the **Commands** window contains commands for managing commands and smart groups.

The commands are described in detail in the following sections.

- “Copy” on page 529
- “Copy “<information item>”” on page 529
- “New Smart Command Queue Group from “<information item>”” on page 529
- “New Smart Command History Group from “<information item>”” on page 530
- “New Smart Command Queue Group” on page 530
- “New Smart Command History Group” on page 531
- “Edit Smart Group” on page 531

- “Remove Smart Group” on page 532
- “Scheduling Options” on page 532
- “Execute Command Now” on page 532
- “Edit Command” on page 532
- “Reapply Command” on page 532
- “Remove Command” on page 533
- “Show Command Result” on page 533

For information on the rest of the commands in the table context menu, see “Commands menu” on page 283. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 273.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (e.g., **Copy “Command Name”**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Command Queue Group from “<information item>”

The **New Smart Command Queue Group from “<information item>”** command lets you create a smart group with prefilled criteria.

Choosing the command opens the **New Smart Command Queue Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

New Smart Command History Group from “<information item>”

The **New Smart Command History Group from “<information item>”** command lets you create a smart group with pre-filled criteria.

Choosing the command opens the **New Smart Command History Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

New Smart Command Queue Group

The **New Smart Command Queue Group** command creates a new smart group for pending or running commands (i.e., commands that have not yet finished executing).

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

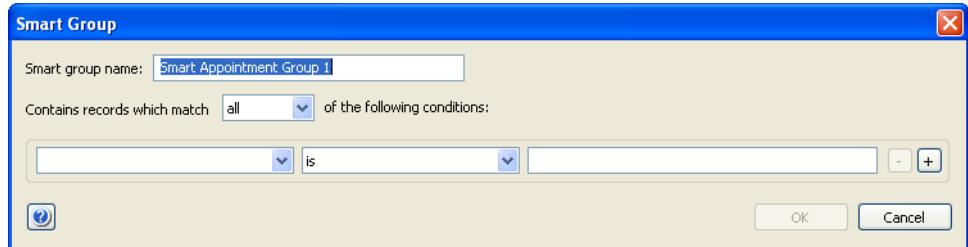
- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Commands” on page 570, “General” on page 534, and “Administration” on page 572.
 - The second pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.

- The + and – buttons let you add new conditions or remove existing ones.

New Smart Command History Group

The **New Smart Command History Group** command creates a new smart group for completed commands (i.e., commands that have been executed successfully or with a failure).

Choosing the command opens the **Smart Group** dialog:



The dialog contains these elements:

- **Smart Group Name:** The name for the smart group.
- **Contains records which match:** When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
 - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in "Commands" on page 570, "General" on page 534, and "Administration" on page 572.
 - The second pop-up menu contains the possible comparison operators.
 - The right-hand text field lets you specify the value to compare record values against.
 - The + and – buttons let you add new conditions or remove existing ones.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the specification dialog for the type of smart group that is selected. For details, see the command for creating that type of smart group:

- "New Smart Command Queue Group" on page 530
- "New Smart Command History Group" on page 531

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Scheduling Options

The **Scheduling Options** command lets you reschedule a pending command. It is not available for commands that are already executing or have been completed.

Choosing the command opens the **Scheduling Options** dialog that is described in “Options” on page 285, although the **Command description** field is not available.

Execute Command Now

The **Execute Command Now** command lets you execute a pending command immediately. It is not available for commands that are already executing or have been completed.

Choosing the command immediately executes all chosen commands, regardless of their scheduling settings. A confirmation message is displayed first.

Edit Command

The **Edit Command** command lets you change the settings of a command that has not yet been executed. It is not available for commands that are already executing or have been completed.

Choosing the command opens the selected command’s command dialog, as described in “Commands menu” on page 283.

Reapply Command

The **Reapply Command** command lets you execute a command again. A new copy of the command is created in the command queue.

Choosing the command opens the selected command’s command dialog, as described in “Commands menu” on page 283.

Remove Command

The **Remove Command** command deletes a command from the command table. If the command is pending, it will not be executed. A confirmation message is displayed first.

NOTE In the command history, the **Remove Command** command can be used only by administrators with the **Remove History Entry** right. See “New Administrator” on page 481 for details.

Show Command Result

The **Show Command Result** command displays the results of script commands executed on administered computers. It applies only to instances of the **Execute Script** commands that have already been completed.

Choosing the command opens an editable text window displaying the result that has been returned by the executed script. You can save the result using the **Save As** command.

Absolute Manage can display numerous aspects of the client computer's state and configuration. It does so in information items, which are analogous to database fields.

This chapter contains a complete listing of all information items, sorted by subject matter.

NOTE If you are looking for an information item by name, please use the **Index**.

Information items cover these areas:

- “Agent Information” on page 534
- “Hardware Information” on page 538
- “Software Information” on page 553
- “Commands” on page 570
- “Server Center” on page 571
- “Agent Deployment Center” on page 585
- “Installed Software Statistics” on page 586
- “Missing OS Patches Statistics” on page 587
- “Compliance Reports” on page 587
- “Mobile Device Information” on page 589
- “Windows Reinstallation Tasks” on page 615

Agent Information

Information items in the **Agent Information** section contain information on the Agent properties and settings. There are three subcategories:

- **General** (page 534)
- **Agent Settings** (page 535)
- **Custom Fields** (page 537)

General

The **General** category contains information items related to the version and identifying information of Absolute Manage Agent.

Agent Name The name under which the computer on which Absolute Manage Agent is installed is displayed in Absolute Manage.

NOTE If **Use Custom Agent Name** is “Yes” this information item is the same as **Custom Agent Name**. If **Use Custom Agent Name** is “No”, it is the same as **Computer Name**.

Agent Version The version number of the Absolute Manage Agent.

Agent Build Number	The build number of the Absolute Manage Agent.
Agent Serial Number	The unique serial number of the Absolute Manage Agent.
Agent Active IP	The IP address that the Absolute Manage Agent used for the last communication with the server. (This is the IP address of the computer, on which Absolute Manage Agent is installed, or one of its IP addresses if it has multiple network adapters.)
Computer Online	Whether the computer has sent its last scheduled heartbeat signal. (In the Computers window, this information is indicated by a green or red dot in front of the computer's row.)
Computer Online (Icon)	A graphical information on whether the computer has sent its last scheduled heartbeat signal: A green dot indicates that it has; a red dot, that it has not. (This is the same as the online status column in the Computers window.)
Last Heartbeat	The time when the last heartbeat signal has been received from this agent.

NOTE The heartbeat is a regular signal by the agent indicating that it is still running.

Record Creation Date	The time when the record for this computer was created in the server.
-----------------------------	---

Agent Settings

The **Agent Settings** category contains information items related to the current settings of Absolute Manage Agents.

Servers

The **Servers** subcategory contains information about server-related settings of Absolute Manage Agents. If an agent communicates with multiple servers, one row per server is generated for each agent.

Server Address	The address of all Absolute Manage Servers with which the Absolute Manage agent is set to communicate, not including any servers that are software distribution or license monitoring servers for the agent but not inventory servers.
-----------------------	--

Server Port	The port on the Absolute Manage Server with which the Absolute Manage Agent communicates.
--------------------	---

Server Unique ID	The unique ID of the Absolute Manage Server with which the Absolute Manage Agent communicates. The ID stays constant even when the server's network address changes.
-------------------------	--

Heartbeat Interval	The interval, in minutes, in which the Absolute Manage Agent contacts the server to let it know that its computer is still running.
---------------------------	---

Inventory Push Interval	The interval, in minutes, in which the Absolute Manage Agent transmit any changes to the state or parameters of its computer to the server.
Basic Inventory Only	Whether this server has been configured in the Agent Settings to request only basic inventory information from this agent.

Client Information

The **Client Information** subcategory contains information about user-definable information stored on administered computers.

Client Information 1 ... 10	The first through tenth of the information fields for user-definable information. The contents of these fields can be any text, as specified by administrators or local users.
------------------------------------	--

NOTE The actual fields may have names that differ from those of these information items, when you have edited the field names in the **Server Settings** dialog.

Client Info Locked	Whether the client information fields are locked on this computer. If fields are locked, only administrators can edit their contents, not local users.
---------------------------	--

Ungrouped fields

Custom Agent Name	A custom name for this computer just for use within the Absolute Manage system, as specified in the Agent Settings dialog's General tab.
--------------------------	--

Use Custom Agent Name	Whether the custom agent name (see above) is to be used to indicate the computer within the Absolute Manage system.
------------------------------	---

SD Server Address	The IP address or DNS name of the software distribution server specified for this computer.
--------------------------	---

SD Server Port	The port on the software distribution server that is specified for this computer.
-----------------------	---

SD Server Unique ID	The unique ID of the software distribution server assigned to this agent. The ID stays constant even when the server's network address changes.
----------------------------	---

SD Server Check Interval	The interval, in minutes, in which the Absolute Manage Agent is set to check the software distribution server for new installation packages.
---------------------------------	--

LM Server Address	The IP address or DNS name of the license monitoring server specified for this computer.
--------------------------	--

LM Server Port	The port on the license monitoring server that is specified for this computer.
-----------------------	--

LM Server Unique ID	The unique ID of the license monitoring server assigned to this agent. The ID stays constant even when the server's network address changes.
LM Server Check Interval	The interval, in minutes, in which the Absolute Manage Agent checks for changes to the license specifications on the license monitoring server.
Agent Port	The local port on which the agent can be reached by the server.
Connect Timeout	The time, in seconds, which the agent waits for responses from the server before it considers a connection attempt to have failed.
Included in Patch Management	Whether this agent is set to check for operating system and software patches from Apple or Microsoft and install them using Absolute Manage's software distribution feature.
Use Only Absolute Manage for OS Updates	This information item displays "True" if the Use only Absolute Manage for OS updates option in the Agent Settings dialog is checked for the agent, i.e., if the client computer receives operating system updates only through Absolute Manage's patch management and not through Software Update (Mac OS X) or Windows Update (Windows), respectively.
Absolute Remote Enabled	Is the screen-sharing function that is built into the Agent enabled on this computer?
Absolute Remote Port	The port over which the Agent accepts screen-sharing connections.
Absolute Remote User Confirmation Required	Whether screen-sharing requests must be accepted by the user before the Agent establishes the connection.
Computer Is Tracked	Is this computer currently being monitored via Absolute Manage's computer tracking feature?

Custom Fields

The **Custom Fields** category contains all custom information fields for desktop devices that have been defined on the currently connected server.

The exact contents of this category and the functions of the individual fields depend entirely on the specific local configuration of the site and cannot be described further here.

NOTE Double-clicking a custom information item in the **Information Items** window lets you edit its specifications.

Hardware Information

Information items in the **Hardware Information** section contain information on the client computer hardware. There are nine subcategories:

- **System Information** (page 538)
- **Memory Slots** (page 547)
- **Volumes** (page 547)
- **ATA Devices** (page 548)
- **SCSI Devices** (page 549)
- **FireWire Devices** (page 550)
- **USB Devices** (page 550)
- **PCI Devices** (page 551)
- **Displays** (page 552)

System Information

The **System Information** category contains information on the computer itself (as opposed to installed and peripheral devices.)

CPU Information

The **CPU Information** subcategory contains processor-related information.

Physical Cores	The total number of main processor cores installed in the computer.
----------------	---

NOTE	Due to a limitation in Windows, Absolute Manage cannot report physical cores that have been disabled during the boot process or in Task Manager.
-------------	--

Active Cores	The number of currently enabled main processor cores in the computer.
--------------	---

This number may be lower than **Physical Cores**, above, when individual cores are disabled, e.g., to lower power consumption.

NOTE	Due to a limitation in Windows, Absolute Manage cannot report processors that have been disabled in Task Manager.
-------------	---

Physical Processors	The number of physical main processors installed in the computer.
---------------------	---

Only physically discrete processors are counted; a processor supporting hyperthreading or multiple cores is counted as one processor.

NOTE	Due to a limitation in Windows, Absolute Manage cannot report processors that have been disabled during the boot process or in Task Manager.
-------------	--

Cores per Processor	How many cores does the main processor have?
Processor Speed	The processor's clock rate.
Processor Type	The main processor's series and version.
Processor Vendor	The main processor's manufacturer.
Processor Is 64-bit	Is the main processor a 64-bit processor.
Processor ID String	Intel-compatible processors only: The processor type string as reported by the operating system.
Processor Architecture	A string briefly describing the basic processor type (Intel, AMD, or PowerPC) and data word size (32 bit or 64 bit).
Processor L1 Data Cache	The size of the processor's level 1 cache for data.
Processor L1 Instruction Cache	The size of the processor's level 1 cache for instructions.
Processor L2 Data Cache	The size of the processor's level 2 cache for data.
Processor L2 Instruction Cache	The size of the processor's level 2 cache for instructions.
Processor L3 Cache	The size of the processor's level 3 cache.
Bus Speed	The clock speed the processor's front-side bus.
Processor Family	The family ID of the main processor, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers.
Processor Model	The model ID of the main processor within its family, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers
Processor Stepping	The stepping ID of the main processor within its model, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers
Processor Has MMX	Does the processor support the MMX instruction set?
Processor Has 3DNow	Does the processor support the 3DNow instruction set?
Processor Has SSE	Does the processor support the SSE instruction set?
Processor Has SSE2	Does the processor support the SSE2 instruction set?

Hardware Information

Processor Has SSE3 Does the processor support the SSE3 instruction set?

Processor Supports Hyperthreading Does the processor support hyperthreading?

Processor Hyperthreading Enabled Is hyperthreading currently enabled?

NOTE Due to a limitation in Windows, Absolute Manage may misreport hyperthreading to be off when processors have been disabled in Task Manager.

Battery Information

The **Battery Information** subcategory contains information related to the batteries of administered laptops.

AC Charger Connected Laptops only: Is the laptop's AC power adapter currently providing mains power?

AC Charger Charging Laptops only: Is the laptop's AC power adapter currently charging the laptop's battery?

Battery Installed Laptops only: Is a battery currently present in this laptop?

Battery Fully Charged Laptops only: Is the laptop's battery currently reported by the computer as being fully charged?

Original Battery Capacity Laptops only: The rated original capacity of the battery in mAh (milliampere-hours).

Maximum Battery Capacity Laptops only: The current maximum capacity of the battery in mAh (milliampere-hours), as reported by the laptop's power management.

Remaining Battery Capacity Laptops only: The currently remaining power in the battery in mAh (milliampere-hours), as reported by the laptop's power management.

Battery % of Original Capacity Laptops only: The battery's current maximum capacity as a percentage of its original rated capacity.

Battery Load Cycles Laptops only: The total number of load cycles of this battery, as reported by the laptop's power management.

Battery Type Windows laptops only: The basic type of the laptop's battery (e.g., "Lithium Ion").

Battery Manufacturer Laptops only: The manufacturer of the battery. (This information is not available for PowerPC-based Macs.)

Battery Manufacturing Date Laptops only: The date when the battery was manufactured. (This information is not available for PowerPC-based Macs.)

Battery Device Name	Laptops only: The device name of the battery as provided by the operating system.
Battery Serial Number	Laptops only: The serial number of the battery. (This information is not available for PowerPC-based Macs.)
Battery Temperature	Laptops only: The current temperature of the battery in degrees Celsius.
<h2>Power Management</h2>	
	The Power Management subcategory contains information related to the power management settings and capabilities of administered computers.
Power-on Avg/Day	The average number of hours that the computer has been powered up per day. (The average is calculated for the entire period during which Absolute Manage has monitored this computer.)
Power-on Avg/Week	The average number of hours that the computer has been powered up per week. (The average is calculated for the entire period during which Absolute Manage has monitored this computer.)
Power-on Avg/Month	The average number of hours that the computer has been powered up per month. (The average is calculated for the entire period during which Absolute Manage has monitored this computer. A month is considered to have 30 days.)
Power-on Avg/Year	The average number of hours that the computer has been powered up per year. (The average is calculated for the entire period during which Absolute Manage has monitored this computer. A year is considered to have 365 days.)
Power-on Yesterday	The average number of hours that the computer has been powered up yesterday. (This information is only available if Absolute Manage has started monitoring this computer before yesterday.)
Power-on Last 7 Days	The average number of hours that the computer has been powered up during the last seven calendar days. (This information is only available if Absolute Manage has started monitoring this computer more than seven days ago.)
Power-on Last 30 Days	The average number of hours that the computer has been powered up during the last 30 calendar days. (This information is only available if Absolute Manage has started monitoring this computer more than 30 days ago.)
Power-on Last 365 Days	The average number of hours that the computer has been powered up during the last 365 calendar days. (This information is only available if Absolute Manage has started monitoring this computer more than 365 days ago.)

Power-on Tracking Start	The date when Absolute Manage has started tracking this computer's power management.
System Sleep Timer	The number of minutes of inactivity before the administered computer is set to go to sleep.
System Hibernate Timer	Windows only: The number of minutes of inactivity before the administered computer is set to go into hibernation.
Disk Sleep Timer	The number of minutes of inactivity before the administered computer is set to spin down the hard disks.
Display Sleep Timer	The number of minutes of inactivity before the administered computer is set to turn off the display.
Action on Power Button	The action the administered computer performs when the power button is pressed. This does not apply to Macintosh laptops.
Action on Clamshell Close	Windows only: The action the administered computer performs when the clamshell case is closed. This applies only to laptops.
Action on Sleep Button	Windows only: The action the administered computer performs when the sleep button is pressed.
Wake on AC Change	Is the administered computer set to wake up when the power adapter is connected or disconnected? This applies only to laptops.
Wake on Clamshell Open	Is the administered computer set to wake up when its clamshell case is opened? This applies only to laptops.
Automatic Restart on Power Loss	Is the administered computer set to restart automatically after being affected by a power outage?
Display Sleep Uses Dim	Does the administered computer reduce the screen brightness after a certain period of inactivity, but before going to sleep?
Display Reduces Brightness	Is the display brightness automatically reduced when the computer is on battery power?
TTYs Keep Awake	Mac only: Do activities on remote terminal connections count as activities to reset the sleep timer?
Hibernation Mode	The kind of hibernation the computer enters when it goes to sleep.
UPS Installed	Is a UPS (uninterruptible power supply) connected to the administered computer?

NOTE

Absolute Manage only detects a UPS when it has properly registered with the operating system.

Sudden Motion Sensor	Mac only: Is the administered computer equipped with a sudden motion sensor?
-----------------------------	--

Power Management Schedules

The **Power Management Schedules** subcategory contains information on the power management schedules that have been set up in Absolute Manage for the administered computers.

PM Schedule Name	The name of the power management schedule.
PM Settings For	The type of power supply (e.g., battery or power adapter) to which the schedule applies.
PM Action	The scheduled action.
PM Trigger	The trigger for the action.
PM Inactivity Timer	The inactivity period in minutes after the specified action is to be performed.
PM Time	The time at which the specified action is to be performed.
PM Only When No User Logged In	Is this scheduled to be performed only when no user is logged in?
PM Schedule Count	The number of the power management schedule rules applied to a computer. If no power management is active on the computer, the value is 0. Note that this information does not apply to power management schedule records (as do the other information items in this subcategory) but to computer records.

Ungrouped fields

Physical Memory	The amount of actual RAM installed in the computer.
Computer Type	For PCs, "PC Compatible" is displayed. For Macs, the exact model is displayed.
Boot ROM Information	The information string from the computer's boot ROM. The exact contents and formatting of this string depends on the ROM vendor.
Primary MAC Address	The MAC address of the computer's current primary network connection.
Date & Time	The date and time of the computer's internal clock. This information is current as of the last 'heartbeat' contact from the agent with the Absolute Manage Server. It is not updated in real time.

You can find out the difference between the client's local clock and the server's clock by comparing the **Date & Time** and **Last Heartbeat** information items: Both display the same point in time but the first is measured by the client's clock and the second as measured by the server's.

Computer Production Date Macs only: The date when the computer was manufactured.

Computer Production Factory Macs only: The site where the computer was manufactured.

Computer Serial Number The serial number of the computer.

NOTE Some Windows computers may not have a serial number.

Computer Boot Time The date and time when the computer was last booted.

Computer Uptime The time since the computer was last booted, in hours and minutes.
This information is current as of the last inventory update. To find out the uptime now, trigger an inventory update using the **Gather Inventory Information** command.

Computer Age Macs only: The age of the computer, i.e., the time that has elapsed since its production.

SMC Version Intel-based Macs only: The version number of the computer's SMC firmware.

Apple Product Name Macs only: The official product name Apple uses for this type of Macintosh.

NOTE The content of this information item, same as with the other "Apple ..." information items listed below, is downloaded from an Apple server, based on the client computer's serial number. It is therefore available only if the client computer had a working Internet connection at least once after Absolute Manage Agent has been installed on it. All "Apple ..." information items listed below are updated every ten days as long as the client computer can reach Apple's server.

Apple Purchase Date Macs only: The date when the Macintosh was purchased, according to Apple's files.

NOTE See the note for Apple Product Name, above.

Computer Warranty Info	The computer's current warranty status.
NOTE	This information is retrieved from a server of the computer's vendor and faces restrictions similar to those noted under "Apple Product Name," above. In addition, not all vendors provide this information.
Computer Warranty End	The date when the warranty for the computer will end. A value of "n/a" indicates either that no information is available or that the warranty has expired.
NOTE	This information is retrieved from a server of the computer's vendor and faces restrictions similar to those noted under "Apple Product Name," above. In addition, not all vendors provide this information.
Unique Computer ID	Macs only: A UUID given the computer by Apple that uniquely identifies it.
BIOS Date	Windows only: The creation date of the computer's BIOS, as stored in the BIOS.
BIOS Vendor	Windows only: The creator of the computer's BIOS.
BIOS Version	Windows only: The version number of the computer's BIOS.
SMBIOS Version	Windows only: The version number of the computer's System Management BIOS.
Mainboard Manufacturer	Windows only: The vendor of the mainboard used in the computer.
Mainboard Product Name	Windows only: The mainboard's name as specified by its vendor.
Mainboard Serial Number	Windows only: The mainboard's serial number.
Mainboard Type	Windows only: The type of the mainboard used in the computer, as specified by its vendor.
Mainboard Version	Windows only: The version number of the mainboard used in the computer.
Mainboard Asset Tag	Windows only: The asset tag of the computer's main board.
System Enclosure Manufacturer	Windows only: The vendor of the computer's case.
System Enclosure Serial Number	Windows only: The serial number of the computer's case.

System Enclosure Type	Windows only: The type of the computer's case.
System Enclosure Version	Windows only: The version number of the computer's case.
System Enclosure Asset Tag	Windows only: The asset tag of the computer's case.
Computer Manufacturer	Windows only: The producer of the computer system.
Computer Version	Windows only: The version number of the computer system.
Computer Model	Windows only: The model name of the computer system.
Computer Service Tag	Windows only: The service tag of the computer system.
Computer Express Service Tag (Dell)	Dell systems only: The express service tag of the computer system.
Swap Space Total	The size of the swap space that is currently reserved on the hard disk.
Swap Space Used	The current amount of data that has been swapped to disk.
Swap Space Free	The amount of swap space that has been reserved but is currently unused.
Swap Space Encrypted	Macs only: Whether encryption for the swap file has been enabled.
Memory Slots	The number of slots for RAM on the computer's motherboard.
Memory Module Count	The number of RAM modules installed in the computer.
Volume Count	The number of volumes that are mounted on the computer.
ATA Device Count	The number of ATA devices that are connected to the computer and powered on.
SCSI Device Count	The number of SCSI devices that are connected to the computer and powered on.
FireWire Device Count	The number of FireWire devices that are connected to the computer and powered on.
USB Device Count	The number of USB devices that are connected to the computer.
PCI Device Count	The number of PCI cards that are installed in the computer.
Display Count	The number of display devices that are connected to the computer and have been recognized by it.

Memory Slots	The Memory Slots category contains information items related to individual memory slots.
Memory Slot Name	The label of the memory slot.
Memory Size	The RAM size of the memory module installed in the slot.
Memory Speed	Macs only: The clock rate with which the memory module is accessed.
Memory Type	The general type of memory installed in the memory slot, such as SDRAM, DDR SDRAM, etc.
Volumes	The Volumes category contains information items related to individual volumes mounted on the administered computer.
Volume Name	The name of the volume. (On Windows computers, this may be empty.)
Size	The formatted capacity of the volume. (Total space, whether free or used.)
Format	The file system with which the volume is formatted – NTFS, FAT32, Mac OS Extended, etc. (See also Journaled , below.)
Volume Type	The general type of volume – hard disk, removable, or server.
NOTE	On Windows client computers, it is possible to recognize CD-ROMs and RAM disks. This information is not available on Mac OS X clients where these media are listed just as “removable”.
Free Space	The unused capacity of the volume in absolute terms.
Free Space %	The unused capacity of the volume as a percentage of the total formatted capacity.
Drive Letter	Windows only: The drive letter that is currently assigned to the volume.
Volume Serial Number	Windows only: The serial number of the volume.
Object Count	Macs only: The total number of objects – files and folders, visible and invisible – on the volume. This information is not available for server volumes.
Folder Count	Macs only: The total number of directories – both visible and invisible – on the volume. This information is not available for server volumes.
Creation Date	Macs only: The date and time when the volume was last formatted.
Modification Date	Macs only: The date and time when the volume was last modified.

Backup Date	Macs only: The date and time when the volume was last backed up. If no backup has yet been made, the date is "n/a".
NOTE	Not all backup applications set this date when they back up a volume.
Checked Date	Macs only: The date when the hard disk was last checked by a hard disk utility.
NOTE	Not all such utilities set this date when they check a volume.
Boot Volume	Is this the volume from which the computer has booted?
Compressed	Windows only: Is the data on this volume compressed by the operating system?
Journalized	Macs only: Is this volume journaled?
Case-sensitive	Are file names on this volume case-sensitive? (I.e., would "File.txt" and "file.txt" considered to be two different names?)
Locked by Hardware	Macs only: Is this volume write-protected through a hardware setting?
Locked by Software	Macs only: Is this volume write-protected through a software setting?
NOTE	Due to a limitation in the Mac OS, volumes that are write-protected by hardware, such as CD-ROMs, may be displayed as being write-protected by software.
Unix Mount Point	Macs only: The mount point of the volume on the computer.
ATA Devices	The ATA Devices category contains information items related to individual ATA devices connected to the administered computer. Only devices that are powered on are listed.
ATA Bus Number	The number of the ATA bus on which the device is located.
ATA Unit Number	The unit number of the ATA device on its bus.
ATA Manufacturer	The company who has manufactured this ATA device.
ATA Model	The model number of the ATA device, as specified by the manufacturer.
ATA Device Type	The general type of the ATA device, such as hard disk, CD-ROM/DVD-ROM, etc.

ATA Serial Number The serial number of the ATA device, as specified by the manufacturer.

NOTE Not all ATA devices have serial numbers.

ATA SMART Status The status of the SMART hard disk monitoring system for the ATA device.

NOTE This information is available only for hard disks.

ATA Revision The revision (version) number of the ATA device, as specified by the manufacturer.

ATA Protocol The type of ATA protocol used by the computer to communicate with this device.

ATA Capacity The formatted capacity of the ATA device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

ATA Socket Type Macs only: The type of interface by which the ATA device is connected to the computer.

ATA Bay Name Macs only: The name of the drive bay in which the ATA device is located.

SCSI Devices

The **SCSI Devices** category contains information items related to individual SCSI devices connected to the administered computer. Only devices that are powered on are listed.

SCSI Bus Number The number of the SCSI bus on which the device is located.

SCSI Unit Number The SCSI ID of the device.

SCSI Manufacturer The company who has manufactured this SCSI device.

SCSI Model The model number of the SCSI device, as specified by the manufacturer.

SCSI Device Type The general type of the SCSI device, such as hard disk, CD-ROM/DVD-ROM, etc.

SCSI Revision The revision (version) number of the SCSI device, as specified by the manufacturer.

SCSI Capacity The formatted capacity of the SCSI device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

SCSI Transfer Width The width, in bits, of the SCSI bus over which the device is connected.

FireWire Devices

The **FireWire Devices** category contains information items related to individual FireWire devices connected to the administered computer. Only devices that are powered on are listed.

FireWire Manufacturer The company who has manufactured this FireWire device.

FireWire Model The model number of the FireWire device, as specified by the manufacturer.

FireWire Firmware Revision Macs only: The revision (version) number of the FireWire device's firmware, as specified by the manufacturer.

FireWire Software Version Macs only: The version of the core FireWire software that is integrated in the firmware.

FireWire Speed Macs only: The maximum speed of the FireWire bus over which the device is connected.

FireWire Capacity The formatted capacity of the FireWire device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

FireWire Vendor ID The ID number for the vendor of the FireWire device.

FireWire Model ID The ID that the device's vendor has assigned to this type of model.

USB Devices

The **USB Devices** category contains information items related to individual USB devices connected to the administered computer.

USB Vendor The company who has manufactured this USB device.

USB Model The model name of the USB device, as specified by the manufacturer.

USB Serial Number The serial number of the USB device, as assigned by the manufacturer.

NOTE Many USB devices do not have serial numbers.

USB Max. Power	The highest power draw, measured in mA (milliampere), that this device can have.
NOTE	This value is taken from the device's firmware. Depending on how accurately the manufacturer specifies this value, the actual peak consumption may exceed this value.
USB Device Speed	The maximum connection speed that the USB device supports.
NOTE	The device may not actually be able to transfer data at this rated speed.
USB Capacity	Macs only: The nominal data capacity of a USB device. If the device does not store data, its capacity is given as "n/a".
NOTE	Some data storage devices do not properly announce their capacity, in which case the information item also contains "n/a".
USB Vendor ID	Macs only: The ID number for the vendor of the USB device.
USB Product ID	Macs only: The ID that the device's vendor has assigned to this type of model.
USB Product Version	The version of the USB product, as specified by the manufacturer.
USB Device Protocol	An identifier for the protocol that the USB device uses to communicate with its driver. The meaning of the identifier depends on the USB device.
USB Device Class	The general type of the USB device, e.g. hub or mouse.
USB Device Subclass	An identifier to distinguish different subtypes of one type of USB device.
PCI Devices	The PCI Devices category contains information items related to individual PCI cards installed in the administered computer.
PCI Name	The name of the PCI device, as specified by the manufacturer.
PCI Type	The general type of the PCI device, e.g., "display" (graphics card).
PCI Slot	Macs only: The label of the PCI slot in which the device is installed.
PCI ROM Revision	Macs only: The revision (version) of the PCI device's firmware, as specified by the manufacturer.
PCI Device ID	The ID number for the PCI device model.
PCI Vendor ID	The ID number for the vendor of the PCI device.

PCI Revision ID	The revision of the PCI device's firmware.
Displays	The Displays category contains information items related to individual displays connected to the administered computer. Only displays that have been recognized by the computer are listed.
Display Type	The general type of the display.
NOTE	This information item may display "CRT" for LCD displays connected to an analog interface.
Display Vendor	The manufacturer of the display.
Display Product Name	The model name of the display.
Display Manufacture Date	The date on which the display was produced.
Display Serial Number	The serial number of the display.
Resolution	The current horizontal and vertical size of the display, in pixels.
NOTE	This information item displays the current setting. It does not, e.g., display the natural resolution of an LCD display if it is set to a different resolution.
Depth	The color depth to which the display is set, expressed as bits per pixel.
Refresh Rate	The screen refresh rate to which the display is currently set.
Main Display	Is this the computer's main display? (On Mac OS X computers, the main display is the one containing the menu bar; on Windows computers it is the one with the Start menu.)
Mirror	Macs only: Is this display currently being mirrored?
Display Online	Whether the frame buffer is connected to a monitor.
Display Is Built-in	Whether the display is an internal display, i.e., built into the computer.
Quartz Extreme	Macs only: Is Quartz Extreme active for this display?
VRAM Size	The amount of video RAM being used for this display.
Display Serial Number (internal)	Macs only: The internal serial number of the display device. This is usually, but not always, the same number as Display Serial Number, above.
Display Model ID	Macs only: The ID number for the display model.

Video Card Model	The model name of the video card to which the display is connected.
------------------	---

Software Information

Information items in the **Hardware Information** section contain information on the operating systems on the client computers, their network settings, processes, and files. There are seven subcategories:

- **System Information** (page 553)
- **Network Adapters** (page 560)
- **Fonts** (page 561)
- **Printers** (page 561)
- **Startup Items** (page 562)
- **Windows Services** (page 562)
- **Installed Software** (page 563)
- **Missing OS Patches** (page 564)
- **Processes** (page 565)
- **Files** (page 566)
- **Registry Entries** (page 569)
- **Computer Tracking** (page 569)

System Information

The **System Information** category contains information on the operating system and its settings.

Computer Name	The name of the computer, as defined in the operating system.
Current User Name	The full name of the user who is currently logged in on the computer. If no user is logged in, an empty string is displayed. (For example, "Jane Doe".)
Current User Account	The name of the current user's account under which he or she is logged in. (For example, "janedoe" on a Mac or "COMPUTER/JaneDoe" on Windows.)
Current User Is Admin	Whether the currently logged-in user has administrator rights on the computer.
Last User Account	The name of the account under which the current user is logged in on the computer. If no user is logged in, the name of the account of the last user who was logged in is displayed.
Last User Name	The full name of the user who is currently logged in on the computer. If no user is logged in, the name of the user who was last logged in is displayed.
Idle Time	The time for which the client computer had been idle when its information was last updated on the Absolute Manage Server.
OS Platform	The general type and flavor of the operating system, e.g., Windows XP Professional or Mac OS X.

Software Information

OS Version	The operating system's version number.
OS Build Number	The build number of the operating system.
OS Service Pack	Windows only: The latest operating system service pack installed on the computer.
OS Language	The user interface language of the operating system. For single-language operating systems like standard Windows XP installation, this is the installed language. For operating systems that can change the interface language dynamically, like Mac OS X or Windows Vista, this is the currently chosen language.
OS Installation Date	Windows only: The date when this copy of the operating system was installed.
OS Activated	Windows only: Whether this copy has already been activated. This information item does not apply to Windows 2000.
OS Activation Grace Period	Windows only: The end of the grace period before which the operating system must be activated. This information item does not apply to Windows 2000.
OS Serial Number	Windows only: The serial number of this copy of the operating system.
OS Product ID	Windows only: The serial number of the individual copy of the operating system on this computer.
	This is the ID number that is displayed in the System control panel's General tab.
OS Is Volume-Licensed	Windows only: Whether this copy of the operating system has been activated as part of a volume license. This information item applies to the same operating systems as the OS Activated information item described above.
Security Identifier	Windows only: The unique ID that Windows generates for use with Active Directory and other security-related purposes.
Virtual Machine	Windows only: The type of virtual machine inside which the agent is running. Absolute Manage can currently identify Parallels, Virtual PC, and VMware. If the agent is not running inside a virtual machine, "native" is reported.
AD Computer Name	The name of the computer as specified in Active Directory.
AD Computer Organizational Unit	The name of the Active Directory organizational unit to which the computer belongs.
AD Computer Organizational Unit Path	The path of the Active Directory organizational unit to which the computer belongs.

AD User Organizational Unit	The name of the Active Directory organizational unit to which the computer's current user belongs.
AD User Organizational Unit Path	The path of the Active Directory organizational unit to which the computer's current user belongs.
AD User Is Member Of	The Active Directory groups to which the computer's current user belongs. Multiple groups are separated by commas.
AD Computer Is Member Of	The Active Directory groups to which the computer belongs. Multiple groups are separated by commas.
Computer Is Behind NAT	Is there a NAT router between the computer and the Absolute Manage Server?
NOTE	This information item indicates whether the client has a NAT connection as viewed from the Absolute Manage Server, not as viewed from the Internet.
Darwin Version	Macs only: The version of Darwin that is part of the operating system.
Daylight-Saving Time	Is daylight-saving time in effect on the computer?
GMT Delta	The difference between UTC (Universal Time, commonly known as GMT) and the computer's clock.
Defender Installed	Windows only: Is Windows Defender installed on this computer?
Defender Enabled	Windows only: Is Windows Defender currently enabled on this computer?
Defender Real-Time Protection	Windows only: Is Windows Defender's real-time protection enabled on this computer?
Defender Auto Scan Enabled	Windows only: Is Windows Defender' automatic scanning feature enabled on this computer?
Defender Engine Version	Windows only: The version number of the Windows Defender software.
Defender Definition Version	Windows only: The version number of the malware definitions used by Windows Defender.
Disk Encryption Product	The name of the disk encryption software, if any, used on the administered computer.
Disk Encryption Version	The version of the disk encryption software used.

Disk Encryption Status	The state of the disk encryption on the administered computer as reported by disk encryption software.
Disk Encryption Algorithm	The encryption algorithm used by disk encryption software, as reported by the software.
Disk Encryption Key Size	The length, in bits, of the encryption key used, as reported by the software.
Fast User Switching Enabled	Is fast switching between user accounts (i.e., without having to close all applications and logging out before using a different account) enabled on this computer?
Firewall Enabled	Is the operating system's built-in firewall enabled on this computer?
Personal File Sharing	Macs only: Is Personal File Sharing enabled on the computer?
Windows File Sharing	Macs only: Is file sharing for Windows enabled active on the computer?
Personal Web Sharing	Macs only: Is Personal Web Sharing enabled on the computer?
Remote Login	Macs only: Is remote login enabled on the computer?
FTP Access	Macs only: Is FTP access enabled on the computer?
Remote Apple Events	Macs only: Is the Remote Apple Events service enabled on the computer?
Printer Sharing	Macs only: Is Printer Sharing enabled on the computer?
Remote Management	Macs only: Is Apple Remote Desktop remote management access (apart from screen sharing) enabled?
Remote Desktop Screen Sharing	Is screen sharing via Apple Remote Desktop or Microsoft Remote Desktop, respectively, enabled on the computer?
Timbuktu Access	Can this computer be remotely controlled via Timbuktu?
VNC Access	Can this computer be remotely controlled via VNC?
PC Anywhere Access	Can this computer be remotely controlled via PC Anywhere?
DameWare Access	Can this computer be remotely controlled via DameWare?
Allow Remote Assistance	Windows only: Is Remote Assistance enabled on this computer?
Allow Remote Control via Assistance	Windows only: Is controlling this computer via Remote Assistance enabled?
Wake on LAN Enabled	Macs only: Is Wake on LAN (waking from sleep on administrative network access) enabled on the computer?

Wake on LAN Supported	Macs only: Does this computer support Wake on LAN?
OS Update Utility Enabled	Is the local update utility of the operating system (i.e., Software Update on Macs and Windows Update on Windows computers) enabled on this client?
Time Machine Auto Backup Enabled	Macs only, Mac OS X 10.5 or later: Whether Time Machine is currently set to make automatic backups. (This is equivalent to the master switch in the Time Machine control panel to be set to On .)
Time Machine Status	Macs only, Mac OS X 10.5 or later: The status – idle or performing a backup – of Time Machine on this computer.
Time Machine Backup Disk	Macs only, Mac OS X 10.5 or later: The name of the volume to which Time Machine is currently set to back up.
Time Machine Latest Backup	Macs only, Mac OS X 10.5 or later: The time when the most recent Time Machine backup was performed.
Time Machine Oldest Backup	Macs only, Mac OS X 10.5 or later: The time when the first Time Machine backup was performed.
Time Machine Snapshot Count	Macs only, Mac OS X 10.5 or later: The number of snapshots in the Time Machine backup on this computer.
<hr/> NOTE This is not the number of snapshots that Time Machine has taken but only the number of those that are currently retained. For example, Time Machine takes hourly backups but after a day or so discards all of a day's backups except for one.	
Time Machine Disk Size	Macs only, Mac OS X 10.5 or later: The formatted capacity of the Time Machine backup disk.
Time Machine Disk Free	Macs only, Mac OS X 10.5 or later: The current unused capacity of the Time Machine backup disk.
Inventory Received	The time when the most recent contact regarding inventory information was made with this agent. (Note that the contact may also have been a notification by the agent that nothing has changed since the last contact.).
Inventory Updated	The time when the most recent update of the inventory information for this computer was performed on the Absolute Manage Server.
Font Info Updated	The time when the most recent update of the installed font information for this computer was performed on the Absolute Manage Server.
Printer Info Updated	The time when the most recent update of the printer information for this computer was performed on the Absolute Manage Server.

Startup Item Info Updated	Macs only: The time when the most recent update of the startup item information for this computer was performed on the Absolute Manage Server.
Installed Software Info Updated	The time when the most recent update of the installed software information for this computer was performed on the Absolute Manage Server.
Missing Patches Info Updated	The time when the most recent update of the missing patches information for this computer was performed on the Absolute Manage Server.
Windows Services Info Updated	Windows only: The time when the most recent update of the Windows services information for this computer was performed on the Absolute Manage Server.
Computer Tracking Info Updated	The time when the most recent update of the computer tracking information for this computer was performed on the Absolute Manage Server.
Process Info Updated	The time when the most recent update of the process information for this computer was performed on the Absolute Manage Server.
Custom Info Items Updated	The time when the most recent update of the custom information items for this computer was performed on the Absolute Manage Server.
Network Adapter Count	The number of active network adapters currently of the computer.
Font Count	The number of fonts installed on the computer that are included in the Fonts table in the Absolute Manage database.
Printer Count	The number of printers defined on the computer that are included in the Printers table in the Absolute Manage database.

NOTE Collecting or updating font information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include font information” checked.

NOTE Collecting or updating printer information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include printer information” checked.

Startup Item Count	Macs only: The number of startup items on the computer that are included in the Startup Item table in the Absolute Manage database.
--------------------	---

NOTE Collecting or updating startup item information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include startup item information” checked.

Windows Service Count	Windows only: The number of services from this computer that are included in the Absolute Manage database.
-----------------------	--

NOTE Collecting or updating service information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include service information” checked.

Installed Software Count	The number of installed software items from this computer that are included in the Installed Software table in the Absolute Manage database.
--------------------------	--

NOTE Collecting or updating installed software information is not automatic but has to be explicitly triggered by the **Gather Installed Software** command.

Missing OS Patches Count	The number of operating system software patches missing from this computer.
--------------------------	---

NOTE Collecting or updating information about installed (or missing) patches is not automatic but has to be explicitly triggered by the **Gather Installed Software** command.

Process Count	The number of processes running on the computer that are included in the Processes table in the Absolute Manage database.
---------------	---

NOTE Collecting or updating process information is not automatic but has to be explicitly triggered by the **Gather Process Information** command.

File Count	The number of files located on the computer that are included in the Files table in the Absolute Manage database.
------------	---

NOTE Collecting or updating file information is not automatic but has to be explicitly triggered by the **Find File** command. Only files found by this command are stored in the Absolute Manage database, not all files on searched target computers.

Network Adapters	The Network Adapters category contains information on the active network adapters of a computer. (Active adapters are those currently assigned an IP address.)
Adapter Name	The label of the network adapter, e.g., Ethernet or AirPort.
Adapter IP Address	The IP address assigned to the network adapter.
Adapter Subnet Mask	The subnet mask assigned to the network adapter.
Adapter MAC Address	The MAC address of the network adapter.
Router Address	The IP address of the router assigned to the network adapter.
DHCP Server Address	The IP address of the DHCP server, if any, that currently supplies the IP address to the network adapter.
DNS Servers	The IP addresses of all DNS servers which the network adapter is set to contact to resolve names into IP addresses. If multiple DNS servers are specified, their IP addresses are separated by commas.
Search Domains	Macs only: The default search domains specified for the network adapter. If multiple domains are specified, they are separated by commas.
Configuration Type	The way in which the network adapter has been configured, e.g., DHCP or manually.
TCP Implementation	Macs only: The general type of TCP stack in use on the network adapter.
Primary Interface	Is this the network adapter currently being used as the main IP interface of this computer?
Device Name	The logical name of the network adapter.
Link Status	Whether the network link on this network adapter is up or down.
Adapter Speed	The nominal data rate on this network adapter's current connection.
Full Duplex	Macs only: Is the network adapter currently operating in full duplex mode (as opposed to half duplex)?.
MTU	Macs only: The MTU (maximum transmission unit) size that is currently specified on the network adapter.
Adapter Vendor	The manufacturer of this network adapter.
Hardware	The hardware category of the network adapter.
Scope ID	Windows only: The scope ID that is set for this network adapter.

DNS Suffix	Windows only: The TCP domain that is currently assigned to this network adapter.
Host	Windows only: The name that is displayed for this computer in the network connected to this network adapter.
WINS Resolution	Windows only: The mode for resolving WINS (Windows Internet Name Service) addresses specified for this network adapter.
WINS Server	Windows only: The servers specified on this network adapter for resolving WINS addresses.
Enable DNS for WINS Resolution	Windows only: Can this computer use DNS in addition to WINS to resolve network addresses in the network connected to this adapter?
Enable LMHOST Lookup	Windows only: Can this computer use the LMHOST file to resolve network addresses in the network connected to this adapter?

Fonts

The **Fonts** category contains information on the fonts installed on a computer.

NOTE The information items in this category do not list all fonts on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include font information”

Font Name	The name of the font.
Font Type	The general font format, such as bitmap, TrueType, PostScript, etc.
Sizes	The type sizes in which this font is available. This is relevant only for bitmap fonts; for vector fonts, “All Sizes” is displayed.

Printers

The **Printers** category contains information on the printers defined on a computer.

NOTE The information items in this category do not list all printers on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include printer information”

Printer Name	The name under which the printer is defined.
Printer Model	A description of the make and model of the printer.
Location	The location of the printer, as specified in the printer definition. If the user did not specify a location, some drivers provide default location information.

Printer Host Name	If the printer is connected to a print server, this is the network name or address of the server. Otherwise, the localhost is displayed.
Printer State	Macs only: The current state of the printer.
Default	Is this the default printer on the administered computer?
Remote	Is this the printer connected via a print server?
PostScript	Macs only: Does this printer support PostScript (Adobe PostScript or an emulation)?
Driver Version	Macs only: The version number of the printer driver used for this printer. This information is not available for all printer drivers.
URI	Macs only: The uniform resource identifier of the printer.
Printer ID	The locally unique ID that the operating system assigns to the printer.

Startup Items

The **Startup Items** category contains information on the startup items specified on a computer. This category applies only to administered Mac OS X computers.

NOTE The information items in this category do not list all startup items on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include startup item information”.

Startup Item Name	Macs only: The file name of the startup item.
Provides	Macs only: The name of the service that the startup item offers.
Startup Item Description	Macs only: A brief description of the startup item, supplied by the startup item’s developer in the file.
Path	Macs only: The path of the startup item’s file.
Uses	Macs only: any other services that this startup item requires.

Windows Services

The **Windows Services** category contains information on the services available on a computer. This category applies only to administered Windows computers.

NOTE The information items in this category do not list all services on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include service information”.

Service Name	Windows only: The internal name of the service.
---------------------	---

Service Display Name	Windows only: The name of the service as it is displayed to the user.
Service Description	Windows only: A brief description of the service, supplied by the service's developer in the file.
Service Status	Windows only: The current operating state of the service (started or stopped).
Service Startup Type	Windows only: The startup type currently set for the service (automatic, manual, or disabled).
Service Log On As	Windows only: The user account in which the service is running.
Service Executable Path	Windows only: The location on the client's hard disk of the service's executable file.
Installed Software	The Installed Software category contains information on installed software that has been found by the Gather Installed Software command.
NOTE For summary information on installed software, see "Installed Software Statistics" on page 586.	
Inst. Software Name	The name of the software.
Inst. Software Company	Windows only: The name of the company that produced the software.
Inst. Software Version String	The full version information for the software.
Inst. Software Version Number	The version number of the software. This may be "n/a" if no valid version number can be extracted from the version string (see above).
Inst. Software Size	The size of the installed software on the disk.
Inst. Software Installation Date	The date when the software has been installed on the client computer.
Inst. Software Info	Macs only: Additional information from the software's version information file.
Inst. Software File Architecture	Macs only: The instruction architecture used by the code contained in a file. This information is not available for installed software that has been found using installer receipts.
	The range of possible values is the same as for the File Architecture information item described on page 567.
Uninstallable	Windows only: Is there an uninstallation entry for the software on the client computer?

Software Information

Is Hotfix	Windows only: Is this software marked as a hotfix?
Identification Type	The method by which Absolute Manage has found this software.
Install Location	The path of the software on the client computer. This information is not available for software that has been identified by its installer receipt.
Inst. Software Product ID	For Mac OS X software this is the software's bundle identifier. For Windows software, it is the ID noted in the registry.
Registered Company	Windows only: The company to which this product has been registered. (Which usually will be the name of your company or organization.)
Registered Owner	Windows only: The person to which this product has been registered.
Installed By	Windows only: The name of the user account under which the software has been installed.
Uninstall String	Windows only: The command string that will be used by the installer for removing the software. (If and when it is so directed by a user.)
Installer Receipt ID	The identifier of the installer receipt by which the software was identified. This information is available only for software that has been found through its installer receipt.

Missing OS Patches

The **Missing OS Patches** category contains information on operating system patches that are missing on client computers.

NOTE The information items in this category list only those missing operating system patches that have been collected by means of the **Gather Installed Software** command.

Missing Patch Name	The name of the missing patch.
Missing Patch Version	The version number of the missing patch.
Missing Patch Release Date	Windows only: The date when Microsoft released this patch.
Missing Patch Install Deadline	Windows only: The date recommended by Microsoft by which this patch should be installed.
Missing Patch Is Mandatory	Windows only: Whether Microsoft has marked this patch as mandatory.
Missing Patch Action	Windows only: Whether this patch includes an install or an uninstall action.
Missing Patch Is Beta	Windows only: Is this patch marked as beta-level software?

Missing Patch Superseded by Package Windows only: Whether a later patch is available that supersedes this patch.

Missing Patch Language Windows only: The operating system language for which this patch is intended.

Processes

The **Processes** category contains information on the processes running on a computer.

NOTE The information items in this category do not list all processes on administered computers but only those that have explicitly been collected by means of the **Gather Process Information** command.

Process Name The name of the process. The names of zombie processes on Mac OS X are enclosed in parentheses.

Process File Type Macs only: The file type code of the file from which the process has been launched.

NOTE Not all files on Mac OS X computers have file type codes.

Process File Creator Macs only: The file creator code of the file from which the process has been launched.

NOTE Not all files on Mac OS X computers have file creator codes.

Process ID The ID number of the process.

User ID The ID of the user account from which the process was launched.

Username The name of the user account from which the process was launched.

Session ID Windows only: The ID of the session to which the process belongs. This applies only to PCs with multiple users.

Process Executable Path The path to the file from which the process has been launched.

NOTE Not all processes are launched from files.

Process Architecture Macs only: The instruction architecture used by the process, Intel or PowerPC.

Group ID Macs only: The ID of the group to which the user account belongs from which the process was launched.

Group Name	Macs only: The name of the group to which the user account belongs from which the process was launched.
Parent Process ID	The ID number of the process that has launched this process.
Parent Process Name	The name of the process that has launched this process.
Real User ID	Macs only: The process' real user ID, i.e., the ID of the user who launched the process.
Real Username	Macs only: The process' real username, i.e., the account name of the user who launched the process.
Real Group ID	Macs only: The process' real group ID, i.e., the ID of the group to which the user belongs who launched the process.
Real Group Name	Macs only: The process' real group name, i.e., the name of the group to which the user belongs who launched the process.
Launch Date	The date and time when the process was launched.
Background Only	Macs only: Is this process an interfaceless background process?
Virtual Memory	Windows only: The amount of virtual memory that has been allocated to the process.
Threads	Windows only: The number of threads of which this process consists.
Page Faults	Windows only: The number of page faults that this process has generated since it has been launched.
Process Priority	Windows only: The priority that the process has on the computer, from 0 through 31. Higher numbers denote higher priorities.

Files

The **Files** category contains information on the files and folders that have been found on a computer.

NOTE The information items in this category do not list all files and folders on administered computers but only those that have explicitly been searched for by means of the **Find File** command.

File Name	The name of the file, including any extensions.
File Path	The path of the file, including the file name.
File Type	Macs only: The type code of the file.

NOTE Not all files on Mac OS X computers have file type codes.

File Creator	Macs only: The creator code of the file.
NOTE	Not all files on Mac OS X computers have creator codes.
File Bundle Identifier	Macs only: The unique identifying string for the file bundle, if any. (For example: com.apple.systempreferences.)
NOTE	Not all files on Mac OS X computers have file creator codes.
File Size	The amount of data in the file.
File Creation Date	The date and time when the file was first created.
File Modification Date	The date and time when the file was last modified.
File Access Date	The date and time when the file was last opened.
File Backup Date	Macs only: The date and time when the file was last backed up.
NOTE	Some backup utilities may not set this date when backing up a file.
File Version	The version number of the file, as stored in the file.
NOTE	When you use the File Version information item in specifications for smart groups and for other comparison purposes, Absolute Manage uses the comparison string to determine the operating system platform you target: If the version number you specify to compare the information item's contents with has fewer than three dots, it is considered a Mac OS X version. With three dots, Absolute Manage assumes it to be a version of a Windows file. It is not possible to specify a search condition that works on both platforms.
File Version String	Macs only: A textual description of the file version that is available for some files. This information item can sometimes help to differentiate between two different versions with the same version number or provide version information when no proper version number is available.
File Build Number	The build number of the file, as stored in the file.
File Architecture	Macs only: The instruction architecture used by the code contained in a file. This information is available only for executable files. These values are supported:
	<ul style="list-style-type: none">• Universal (Intel, PowerPC)• Universal (Intel, PowerPC/64bit)

- Universal (Intel, PowerPC, PowerPC/64bit)
- Universal (PowerPC, PowerPC/64bit)
- Intel
- PowerPC
- PowerPC/64bit
- PowerPC (CFM)
- Shell Script
- Classic
- Unknown

Unix Permissions	Macs only: The read, write and execute permissions set for the file, in both letter and numeric notation.
Unix Owner	Macs only: The user account who is the file's owner.
Unix Group	Macs only: The user group to which the file is assigned.
Is Alias	Is this file a shortcut (or, on Mac OS X, an alias)?
Is Application	Is this file an application file (including Mac OS X application packages)?
Is Classic App	Macs only: Is this file an application file that must run in the Classic environment?
Is File	Is this a file (as opposed to a package or a folder)?
Is Hard Link	Macs only: Is this a Unix hard link file?
Is Invisible	Is this file marked as being invisible?
Is Locked	Macs only: Is this file read-only?
Is Open	Macs only: Is this file currently open?
Is Package	Macs only: Is this file a Mac OS X package (a folder looking like a file)?
Is Stationery	Macs only: Is this file marked as stationery?
Is Symbolic Link	Macs only: Is this a Unix symbolic link file?
Is Scriptable	Macs only: Is this file an application that can be controlled through AppleScript?
Has Custom Icon	Macs only: Does this file have a custom icon (an icon for this file only, as opposed to an icon for all files of this type)?
File Found	Has this file been found during the last update of file information for this computer?
File Record Modification Date	The last time that this file record was modified.

Registry Entries

The **Registry Entries** category contains information on the registry entries that have been found client computers.

NOTE

The information items in this category do not list all registry entries on administered computers but only those that have explicitly been searched for by means of the **Search Windows Registry** command.

Registry Name Windows only: The name of the found registry entry.

Registry Value Type Windows only: The data type of the found registry value. For registry keys, this is "n/a".

Registry Value Windows only: The data of the found registry value. For registry keys, this is "n/a".

Full Registry Path Windows only: The path of the found registry entry in the registry.

Registry Value Number Windows only: The data of the found registry value if the value has the type Number.

Registry Value String Windows only: The data of the found registry value if the value has the type String.

Registry Value Binary Windows only: The data of the found registry value if the value has the type Binary.

Registry Entry Found Windows only: Whether the specified registry entry was actually found on the target computer. When searching registries, it is possible to specify that an entry with the value "No" in the **Registry Entry Found** information item is added for a computer on which the specified entry was not found.

Registry Record Modification Date Windows only: The date and time when this registry record in the Absolute Manage database was last updated.

Computer Tracking

The **Computer Tracking** category contains information on tracked client computers.

Tracked Computer Time Stamp The date and time (according to the Absolute Manage Server's clock) of the last contact with the tracked computer.

Tracked Computer Address The IP address that the tracked computer currently has in the local network in which it is located.

Tracked Computer Router Address The IP address of the router that the tracked computer is currently using.

Tracked Computer Public Address The IP address that the tracked computer currently has in the Internet.

Tracked Computer GMT Delta	The current time difference between the tracked computer's internal clock and universal time (GMT).
Tracked Computer Current User Name	The name of the current user who is active on the tracked computer. (See "Current User Name" on page 553.)
Tracked Computer Current User Account	The full name of the account that is currently active on the tracked computer. (See "Current User Account" on page 553.)
Tracked Computer Resolved Address	The DNS name that the tracked computer currently has in the local network in which it is located.
Tracked Computer Resolved Router Address	The DNS name of the router that the tracked computer is currently using.
Tracked Computer Resolved Public Address	The DNS name that the tracked computer currently has in the Internet.
Tracked Computer Time	The date and time (according to the tracked computer's local clock) of the last contact with the tracked computer.

Commands

Information items in the **Commands** section contain information on related to commands that you have issued to the clients. There are three subcategories:

- **Commands** (page 570)
- **Command Queue** (page 571)
- **Command History** (page 571)

Commands

The **Commands** category contains information item related to commands sent from Absolute Manage Admin to administered computers. They can be used only in the **Commands** window.

Command Name	The name of the command. This is the menu item in the Commands menu with which the command is initiated.
Command Description	The description of the command, as entered in the Command description field in the command scheduling dialog. If the command has no individual description, a default description is displayed.
Is Repeating Command	Whether this command has been marked as a repeating command in its Options dialog.
Interval	The interval in which the command is specified to be executed.
Interval Unit	The unit for the execution interval (see Interval , above).

Creation Time	The date and time when the command was entered in the command queue (when the Execute button in the command window was clicked).
Command Queue	The Command Queue category contains information items related to commands sent from Absolute Manage Admin to administered computers that have not yet been completed. They can be used only in the Queued Commands view of the Commands window and other smart groups in that window that display queued (not yet completed) commands.
Scheduled Time	The date and time when the command is scheduled to be executed. In the case of deferred commands, this time may lie in the past.
Command Status	The current execution status of the command – scheduled, deferred, or executing.
Command History	The Command History category contains information item related to commands sent from Absolute Manage Admin to administered computers that have been completed. They can be used only in the History , Failed Commands , and Commands in Last 24 Hours views of the Commands window as well as in other smart groups in that window that display completed commands.
Start Time	The date and time when the execution of the command has started.
Finish Time	The date and time when the execution of the command was completed.
Command History Status	The success or otherwise of the command execution.
Command Result Error	The error that was generated by the command. If the command was executed successfully, this is “No error”.
Command Error Info	Additional information on the nature of the error that is available for some errors.

Server Center

Information items in the **Server Center** section contain information on software distribution, license monitoring, and administrator accounts. There are three subcategories:

- **Administration** (page 572)
- **Software Distribution** (page 575)
- **License Monitoring** (page 581)
- **Computer Groups** (page 585)

Administration

Information items in the **Administrators** category contain information on the administrators assigned to computers. There are three subcategories:

- **Administrators** (page 572)
- **Appointments** (page 574)
- **Active Directory Users** (page 575)

Administrators

The **Administrators** category contains information about administrator accounts. They can be used only in the **Server Center** window.

Administrator Name	The account name of this administrator account.
	This information item can also be added to tables that list managed computer or mobile devices. In that case, it lists the administrators that are appointed to manage the devices.
Is Superadmin	Does this administrator account have superadministrator privileges?
Can Manage All Devices	Is it possible to manage all administered computers and mobile devices from this administrator account, even those to which the account is not expressly assigned?
Account Enabled	Can users currently log in to this administrator account? (That is, is the account currently enabled?)
Deploy Agents	Can Absolute Manage Agents be installed and other Agent Deployment Center functions be used by this administrator account?
View Software Distribution Settings	Can the software distribution settings be displayed using this administrator account?
View License Monitoring Settings	Can the license monitoring settings be displayed using this administrator account?
View Administrator Settings	Can the administrator settings be displayed using this administrator account?
View Custom Information Fields	Can custom information field definitions be displayed using this administrator account?
View Server Status	Can the server status be displayed using this administrator account?
View Commands Window	Can the Commands window be opened using this administrator account?
View Computer Tracking Data	Can computer tracking information be displayed using this administrator account?
View Computer Tracking Screenshots	Can screenshots taken as part of the computer tracking be displayed using this administrator account?

Modify Server Settings	Can server settings be modified using this administrator account?
Modify Custom Information Fields	Can custom information field definitions be modified using this administrator account?
Enter Custom Field Data	Can the contents of custom information fields be edited using this administrator account?
Modify Software Packages	Can software packages be edited using this administrator account?
Modify Disk Images	Can disk images for the Software Distribution Center be edited using this administrator account?
Modify Computer Groups	Can computer groups be edited using this administrator account?
Modify Distribution Points	Can distribution point specifications be edited using this administrator account?
Reset Software Packages	Can software packages be reset (as per the Reset Package command) using this administrator account?
Retry Software Packages	Can software packages be retried (as per the Retry Package command) using this administrator account?
Remove SD Log Entries	Can software distribution log entries be deleted using this administrator account?
Modify License Specifications	Can license specifications be edited using this administrator account?
Remove License Reports	Can entries in the reports in the License Monitoring Center be deleted using this administrator account?
Remove History Commands	Can entries in the command history be deleted using this administrator account?
Change Command History Options	Can the options for recording a command in the command history (in the command's Options dialog) be edited using this administrator account?
Remove Computer Records	Can computer records be deleted from browser windows using this administrator account?
Remove Inventory Data	Can inventory data for computers be deleted using this administrator account?
Change Computer Tracking	Can computer tracking settings be edited from this administrator account?
Enable Computer Tracking Screenshots	Can making screenshots as part of the computer tracking be enabled from this administrator account?

Remote Control	Can remote controlling of administered computers be initiated from this administrator account?
Manage Mobile Devices	Can this administrator change settings for managed mobile devices and send commands to them?
Modify Mobile Applications	Can this administrator create and edit mobile application packages?
Modify Mobile Configuration Profiles	Can this administrator create and edit configuration profiles for mobile devices?
Modify Mobile Media	Can this administrator create and edit media files for mobile devices?
Modify Mobile Actions	Can this administrator create and edit actions for assignment to smart policy groups?
Modify Mobile Device Policies	Can this administrator create and edit policies and smart policies for mobile devices?
Remove Mobile Device Records	Can this administrator remove records for mobile devices from the Absolute Manage database?
Remove Mobile Device History Commands	Can this administrator remove entries in the mobile device command history?
View Mobile Device Tracking Data	Can this administrator see the geolocation information of managed mobile devices?
Change Mobile Device Tracking	Can this administrator enable and disable mobile device tracking?
Change Agent General Settings	Can settings in the General pane of the Agent Settings dialog be edited from this administrator account?
Change Agent Server Settings	Can settings in the Servers pane of the Agent Settings dialog be edited from this administrator account?
Change Agent Client Info Settings	Can settings in the Client Information pane of the Agent Settings dialog be edited from this administrator account?
Change Agent Custom Field Settings	Can settings in the Custom Fields pane of the Agent Settings dialog be edited from this administrator account?
Is AD User	Is this an Active Directory user account? (As opposed to a user account that has been created in Absolute Manage.)

Appointments

The **Appointments** category contains information about appointment groups. They can be used only in the **Server Center** window.

Appointment Group Name	The name of this appointment group.
Active Directory Users	
	The Active Directory Users category contains information about Active Directory accounts that are being made available for use as Absolute Manage administrator accounts. These information items can be used only in the Server Center window.
AD Display Name	The displayed account name of this Active Directory account.
AD Account Name	The internal account name of this Active Directory account.
AD Login Name	The name with which users can log into this Active Directory account.
AD Account Disabled	Is this account currently disabled in Active Directory?
Software Distribution	Information items in the Software Distribution category contain information on the elements of the software distribution system. There are six subcategories: <ul style="list-style-type: none"> • Packages (page 575) • Payloads (page 579) • Distribution Points (page 579) • Disk Images (page 580) • Installation Status (page 581)
Packages	
	The Packages category contains information about software packages and metapackages. They can be used only in the Server Center window, for smart groups displaying software packages.
Package Name	The name of the software package.
Executable Payload	The name of the payload in the package that has been specified as being executable.
Is Metapackage	Is this package a metapackage?
Executable Size	The size of the installer specified in the package.
Executable Options	The command-line options to use for the specified installer.
Target Installation Volume	The name of the volume, if any, of the target computers on which the software is to be installed.
Continue Installation After Failure	Whether the installation of this metapackage is to continue even if there is a failure installing one of the contained packages. (This information item applies only to metapackages, not standard packages.)

Package Description	The description of the software package that has been entered in the Software Package dialog.
Availability Date	The earliest time when this package can be used for installations, as specified in the package.
Install At	The general occasion on which this package is to be installed – at any time, after the next restart, or after the next login.
Install When User Is Logged In	Is this package to be installed when a user is logged in at install time?
Install When No User Is Logged In	Is this package to be installed when no user is logged in at install time?
Install Time Start	If the package may be installed only during a certain time of the day, this is the beginning of the specified interval.
NOTE The content of this information item is disregarded when any Install Time Option other than “Between” has been chosen.	
Install Time End	If the package may be installed only during a certain time of the day, this is the end of the specified interval.
NOTE The content of this information item is disregarded when any Install Time Option other than “Between” has been chosen.	
Priority	The installation priority of the package.
Distribution Point Selection	Which distribution point may be used for installing this software package – any, preferably servers from the target computer’s local zone, or exclusively servers from the local zone?
Installation Context	The user context in which this package is to be installed.
Installation Context User	The user account which is to be the context in which this package is to be installed. This information item is relevant only when the installation context is “Other user.”
Requires Admin Privileges	Does the installation of this software package require administrator privileges on the target computer?
Keep Package File After Installation	Will leave Absolute Manage Agent the downloaded installation files on the target computer’s hard disk instead of deleting it?
Allow On-Demand Installation	Is the package available for pull-installation by the user (instead of the standard push-installation)?
Don’t Install on Slow Network	Is this software package set to install only when there is at least a 100 Mbit/s connection to the target computer?

Payload Download Time	When Absolute Manage is to download the payload to the client computers, before or after displaying any user dialogs.
Target OS Platform	The operating system family – Mac OS X or Windows – for which this software package is intended.
Minimum OS	The earliest version of the operating system that supports the software package.
Maximum OS	The latest version of the operating system that supports the software package.
Platform Architecture	The processor architecture (processor type and bit width) required by the installed software as specified in the software package's specification.
User Interaction	The type of involvement by the local users of target computers allowed by the package.
Auto Start Installation	The number of minutes after which the installation from the package is started automatically on a client if the notification dialog has not been answered by the user.
Allow to Defer For	The number of minutes for which the local user of a target computer can defer this installation.
NOTE If the interval is specified in the package in a unit other than minutes, it is converted to minutes in this information item.	
Installation Deadline	The latest date by which the installation of the package must start.
Display Installation Progress	Whether Absolute Manage Agent is to display the progress of this package's installation.
Action after Installation	Which action, if any, is the agent to take after completing the installation?
Close Install Notification After	The time in minutes after Absolute Manage Agent automatically closes the notification dialog on the target computer if the local user does not acknowledge it.
Restart Notification	Whether Absolute Manage Agent is to display a notification before it restarts the computer after having installed this package.
Allow to Postpone Restart	Whether the local user of the target computer can postpone the restart after the end of the installation.
Repeat Restart Notification	The interval in which Absolute Manage Agent is to display a restart notification while the local user of the target computer keeps postponing the restart.

Warn About Slow Network	Is the local user of the target computer to be warned before the installation of this software package is the network connection is slower than 100 Mbit/s?
Has Installation Condition	Whether any conditions have been specified for the package that must be met before installation commences. See “Installation Conditions” on page 451 for details.
Is Mac OS Software Update	Whether this package is a software update from Apple that has automatically been turned into a software package by the Software Distribution Center.
Is Windows Software Update	Whether this package is a software update from Microsoft that has automatically been turned into a software package by the Software Distribution Center.
Software Patch Version	The version number of this software update. This information applies only to software packages created via the automated patch management.
Software Patch Recommended	Macs only: Whether Apple recommends installing this software update. (This is equivalent to the update being checkmarked in the Software Update utility.) This information applies only to software packages created via the automated patch management.
Supported Operating Systems	The operating system versions or subtypes for which this patch is intended (e.g., Mac OS X 10.4 or Windows XP).
Patch Release Date	Windows only: The date when Microsoft released this patch.
Patch Install Deadline	Windows only: The date recommended by Microsoft by which this patch should be installed.
Patch Is Mandatory	Windows only: Whether Microsoft has marked this patch as mandatory.
Patch Action	Windows only: Whether this patch includes an install or an uninstall action.
Patch Is Beta	Windows only: Is this patch marked as beta-level software?
Patch Can Be Uninstalled	Windows only: Whether this patch can be uninstalled using the Add/Remove Software control panel.
Superseded by Package	Windows only: Whether a later patch is available that supersedes this patch.
Patch Language	Windows only: The operating system language for which this patch is intended.

Requires Exclusive Install	Windows only: Whether this patch must be installed by itself, i.e., not in one installation process together with other patches.
-----------------------------------	--

NOTE	Absolute Manage automatically handles such needs for exclusiveness; you do not need to do anything about it.
-------------	--

Requires Exclusive Uninstall	Windows only: Whether this patch must be uninstalled by itself, i.e., not in one uninstallation process together with other patches.
-------------------------------------	--

Payloads

The **Payloads** category contains information about payloads. They can be used only in the **Server Center** window, for smart groups displaying payloads.

Payload Name	The name of the payload, as specified in the Payload dialog.
Executable Name	The name of the file contained in the payload.
Payload Size	The download size of the payload contents.
Upload Status	The current status of the process of uploading the payload to the distribution point.
Is Executable	Whether the payload has been marked as being executable in the Payload dialog.
Transfer All Files in Folder	Whether the software package is set to transfer all files from the specified installer's folder for installations.
Executable Source	The path on your disk of the file contained in the payload.
Payload Unique ID	An ID for identifying the payload. The ID is guaranteed to be unique in this installation of Absolute Manage.
Payload Notes	The notes that have been entered for this payload.

Distribution Points

The **Distribution Points** category contains information about distribution points. They can be used only in the **Server Center** window, for smart groups displaying distribution points.

Distribution Point Name	The name of the distribution point, as specified in the Server Center.
Address	The network address of the distribution point.
Port	The network port used by the Absolute Manage Agent on this distribution point.

Distribution Point Unique ID	The unique ID of the distribution point, which stays constant even if it is renamed.
Distribution Point Certificate Fingerprint	The fingerprint of the certificate validating the identity of the distribution point.
IP Range Start	If the distribution point is set to provide software packages only to a specific range of IP addresses, this is the lower limit of that range.
IP Range End	If the distribution point is set to provide software packages only to a specific range of IP addresses, this is the upper limit of that range.
Only Use Distribution Point When Assigned	Is this distribution point set to serve only client computers to which it has explicitly assigned (by way of computer groups or IP ranges)?
Max. Downloads	The maximum number of concurrent downloads that this distribution point is to support.
Current Load	The number of concurrent downloads currently in progress on this distribution point.
Allow More than Max. Downloads	Is this distribution point to support more than the specified maximum number of concurrent downloads if no other distribution points with free capacity are available?
Is Master Distribution Point	Is this distribution point set to be the master distribution point?
Distribution Point OS Platform	The operating system platform installed on the computer on the distribution point is running.
Packages Root Path	The path to the folder containing the software installers on this distribution point.
Download Bandwidth	The limit to the download bandwidth that has been specified for this distribution point. If no limit has been set, "n/a" is displayed.
Mirroring From	The start time of the mirroring interval specified for this server. If no mirroring time limit has been specified, "n/a" is displayed.
Mirroring Until	The end time of the mirroring interval specified for this server. If no mirroring time limit has been specified, "n/a" is displayed.
Disk Images	
The Disk Images category contains information about disk image specifications. They can be used only in the Server Center window, for smart groups displaying disk images.	
Disk Image Name	The name of the disk image specification.
Disk Image Size	The size of the selected disk image file.

Disk Image Upload Status	Whether the disk image file is available on the distribution points.
Disk Image File	The path of the selected disk image file.
Disk Image Distribution Point	The setting of the Distribution point option in the disk image specification (which specifies from which distribution points the image may be downloaded).

Installation Status

The **Installation Status** category contains information about the status of installation processes initiated by the software distribution system.

Installation Status	The current status of the software installation.
Deferred Until	If the software installation is deferred, the time when the next installation attempt will be made.
Installation Result Error	The result of a completed installation.
Add. Status Information	Additional status information that is available for some errors.
Installation Log Date	The date and time when the log entry was made.

License Monitoring

Information items in the **License Monitoring** category contain information on the elements of the license monitoring system. There are five subcategories:

- **License Specification** (page 581)
- **Purchase Tracking** (page 582)
- **License Status** (page 583)
- **License History** (page 584)
- **License History Summary** (page 584)
- **License Status per Agent** (page 584)

License Specification

The **License Specification** category contains information items related to license specifications. They can be used only in the **Server Center** window.

License Specification Name	The name of the license specification.
Software Identified By	How the software to which the license applies is to be identified.
Licenses Owned	The number of available licenses for this software.

License Type	The type of license – by installation, by concurrent use, or prohibited software.
Scan All Volumes	Whether all volumes of a target computer are to be scanned for the licensed software (Yes) or just the boot volume (No).
Meter App Usage	Whether, in addition to the installed software, the running processes are to be checked as well for the licensed software.
Terminate App If License Exceeded	Whether Absolute Manage Agents are to terminate local copies of the software specified by this license if the number of floating licenses is exceeded.
Terminate Prohibited Apps	Whether Absolute Manage Agents are to forcefully terminate local copies of the software specified by this license.
Delete Prohibited Apps	Whether Absolute Manage Agents are to delete local copies of the software specified by this license.
Track as Missing Software	Whether the specified software is to be listed as missing when it is not found on a computer.

Purchase Tracking

The **Purchase Tracking** category contains information items related to purchase tracking data. They can be used only in the **Server Center** window; most of them correspond to items in the **Purchase Tracking** tab of the **License Specification** dialog.

Purchase Type	The kind of purchase.
Purchase Date	The date when the purchase happened.
Purchase Count	The number of licenses purchased.
Purchase Price	The price of the license purchase.
Purchase Software Version	The version of the software that was purchased.
Purchase Order Number	The order number of the purchase.
Purchase License Owner	The person or department who owns the purchased licenses.
Purchase Vendor Name	The vendor of the licenses.
Purchase Vendor Reference	A reference number for the purchase from the vendor's company.

Purchase Vendor Contact	The contact person for the purchase at the vendor's company.
Purchase Vendor Support	Contact information for technical support related to this purchase.
Purchase Maintenance Available	Has maintenance been purchased with these licenses?
Purchase Maintenance Begin	The start date of the purchased maintenance period, if any.
Purchase Maintenance End	The end date of the purchased maintenance period, if any.
Purchase Maintenance Price	The price of the maintenance purchase.
Purchase Maintenance Reference	The contract number or similar identification reference for the maintenance agreement, if any.
Purchase Notes	Any additional notes that have been entered for the purchase record.
<h3>License Status</h3>	
The License Status category contains information items related to the status of licenses. They can be used only in the Server Center window.	
Total Install Count	The number of client computers on which the licensed software is installed.
Total Running Count	The number of client computers on which the licensed software is currently running.
Total Usage Time	The overall time, in minutes, that the licensed software has been used on administered computers.
Total Launches	The total number of times that the licensed software has been started on administered computers.
Last Launch Date	The last date and time that the licensed software has been started on an administered computer.
License Status	The current status of this license – whether the use is within legal limits or exceeds them.
License Status Log Date	The timestamp for the license status – the exact date and time when the status was registered.

License History

The **License History** category contains information items related to historical license monitoring data. They can be used only in the **Server Center** window.

Total Install Count The number of client computers on which the licensed software was installed when this license metering was taken.

Total Running Count The number of client computers on which the licensed software was running when this license metering was taken.

Historic License Status The status of this license – whether the use was within legal limits or exceeded them – at the time specified by the **Status Timestamp** information item.

Status Timestamp The date and time when this license metering was taken.

License History Summary

The **License History Summary** category contains information items that provide statistical information about the license history. They can be used only in the **Server Center** window.

Min. Install Count The smallest number of client computers with the licensed software installed that has been encountered in the license history.

Avg. Install Count The average number of client computers with the licensed software installed throughout the license history.

Max. Install Count The largest number of client computers with the licensed software installed that has been encountered in the license history.

Min. Running Count The smallest number of client computers running the licensed software that has been encountered in the license history.

Avg. Running Count The average number of client computers running the licensed software throughout the license history.

Max. Running Count The largest number of client computers running the licensed software that has been encountered in the license history.

First Status Timestamp The date and time when this licensed software was first found.

Latest Status Timestamp The date and time when this licensed software was most recently found.

License Status per Agent

The **License Status perAgent** category contains information items related to the license status of individual computers.

Install Count	The number of times the licensed software is currently installed on this computer.
Running Count	The number of times the licensed software is currently running on this computer.
Usage Time	The overall time, in minutes, that the licensed software has been used on this computer.
Number of Launches	The total number of times that the licensed software has been started on this computer.
Last Launch Date	The last date and time that the licensed software has been started on an administered computer.
Report Date	The date and time when the status of this license specification on this client computer was reported.
Computer Groups	<p>The Computer Groups category contains an information item related to the computer groups defined in the Server Center window.</p> <p>You can use this information item in the Server Center window when the Computer Groups category is selected and in any browser window displaying computer information.</p>
Computer Group	The name of a computer group. If used in a browser window listing computers, the information item displays the name of a computer group to which the computer belongs.

Agent Deployment Center

Information items in the **Agent Deployment Center** section contain information on devices in the network, on Absolute Manage Agents installed on them, and on Absolute Manage Agent installation or update processes. These information items can be used only in the **Agent Deployment Center** window.

Computer Name	The name or IP address of a found network device, depending on the type of zone.
Connection Status	The status of an installation in progress, if any. If no installation is in progress, the status is “idle”.
IP Address	The IP address of a found network device.
DNS Name	The DNS name of a found network device as specified on the local DNS server.
Agent Port	The port on which an installed Absolute Manage Agent is set to communicate.

Agent Status	The status of the detected device with regard to the Absolute Manage Agent installed on it – whether it is up to date, outdated, or missing. Devices on which no agent can be installed display “n/a”.
Installed Agent Version	The version number of the Absolute Manage Agent installed on the computer.
Installed Agent Build Number	The build number of the Absolute Manage Agent installed on the computer.
Inventory Server	The inventory server that an installed Absolute Manage Agent is set to use. If several inventory servers are specified, only the first is listed.
SSH Port	The port that the SSH service on the device uses.
Access Status	The possibility of accessing the computer using SSH.
Protocol	The way in which the network device has been detected.
Deployment Result	The result of the last installation or update of Absolute Manage Agent on this device from the Agent Deployment Center.
Deployment Result Message	Additional information that is available for some errors.

Installed Software Statistics

The **Installed Software Statistics** category contains summary information on installed software that has been found by the **Gather Installed Software** command.

NOTE For information on individual installed software items on client computers, see “Installed Software” on page 563.

Inst. Software Stat Name	The name of the installed software being summarized.
Inst. Software Stat Count	The number of computers on which the installed software has been found.
Inst. Software Stat Company	Windows only: The name of the company that produced the software.
Inst. Software Stat Size	The size of the installed software on the disk.
Inst. Software Stat Info	Macs only: Additional information from the software’s version information file.
Inst. Software Stat Uninstallable	Windows only: Is there an uninstallation entry for the software on the client computer?

Inst. Software Stat Is Hotfix	Windows only: Is this software marked as a hotfix?
Inst. Software Stat Identification Type	The method by which Absolute Manage has found this software?
Inst. Software Stat Installer Receipt ID	The identifier of the installer receipt by which the software was identified. This information is available only for software that has been found through its installer receipt.

Missing OS Patches Statistics

The **Missing OS Patches Statistics** category contains summary information on which operating system patches are missing on how many applicable computers. This information is collected by the **Gather Installed Software** command.

These information items can be used in the statistics categories of the **Missing Operating System Patches** window.

Missing Patch Stat Name	The name of the missing patch being summarized.
Missing Patch Stat Version	The version number of the missing patch being summarized.
Missing Patch Stat Count	The number of computers on which the patch has been found to be missing.
Missing Patch Stat Release Date	Windows only: The date when the patch being summarized was released by Microsoft.
Missing Patch Stat Install Deadline	Windows only: The date by which the patch being summarized should be installed, according to Microsoft's recommendation.
Missing Patch Stat Superseded by Package	Windows only: Is a later patch available that supersedes the patch being summarized?
Missing Patch Stat Language	Windows only: The language for which the patch being summarized is intended.

Compliance Reports

The **Compliance Reports** category contains information from the compliance reports that Absolute Manage has gathered on administered computers. This information is collected by the **Gather Compliance Report** command.

These information items can be used in the **Compliance Reports** window.

There are four subcategories:

- **Reports** (page 588)
- **Computer Summary** (page 588)
- **Item Summary** (page 588)
- **Score Items** (page 589)

Reports

The **Reports** category contains information on the report parameters.

Profile Name The name of the profile on which the report is based.

Compliance Check Start Date The date and time when Absolute Manage began gathering the report.

Compliance Check Finish Date The date and time when Absolute Manage completed gathering the report.

Benchmark File The report definition file chosen as the basis for this report.

Report Description The description of the report from the chosen report definition file.

Computer Summary

The **Computer Summary** category contains information on the overall results of the tested computer.

Compliant Whether the computer was found to be compliant, according to the rules in the report.

Compliance Score The compliance score the computer achieved in the report.

Compliance Report Date The date when the report was last changed in Absolute Manage Admin. This may be later than the date when the report was created.

Compliance Report Logged-In User The name of the user account that was active on the administered computer when the report was compiled.

Item Summary

The **Item Summary** category contains summary information on the score items included in the report.

Max. Achieved Score The maximum score that any of the tested computers achieved for this item.

Average Achieved Score The average score achieved by all tested computers for this item.

Min. Achieved Score The minimum score that any of the tested computers achieved for this item.

Max. Item Score The maximum score that can be achieved for this item.

Compliance Count	The number of computers that met the compliance criteria for this item.
Error Count	The number of computers for which the compliance testing for this item returned an error.
Failure Count	The number of computers that were found to not meet the compliance criteria of this item.
Scored Computer Count	The number of computers that were scored using this report.
Scoring States	A list of all individual scoring states that the tested computers achieved for this item.

Score Items

Score Item Title	The Score Items category contains information on the individual score item results of each computer.
Score	The score the computer achieved in this score item.
Score State	The pass or fail state of the report item for this computer.
Max. Score	The maximum possible score to be achieved in this score item.
Score Item Index Path	The path of the individual score item in the report.
Score Item Weight	The weight of the individual score item within the report.
Score Item Description	The description of the individual score item, as noted in the report file.
XCCDF Item Identifier	The unique identifier of this score item.

Mobile Device Information

The **Mobile Device Information** category contains information about mobile devices managed by Absolute Manage through an MDM server.

This information is collected automatically for managed mobile devices on which AbsoluteApps is installed (first upon enrollment and then at each regular contact specified by the iOS contact interval setting of the MDM server). It can be manually updated through the **Update Device Info** command.

There are a number of subcategories:

- **Device Information** (page 590)
- **Device User Information** (page 598)
- **Installed Applications** (page 599)

- **Installed Configuration Profiles** (page 600)
- **Installed Provisioning Profiles** (page 601)
- **Installed Certificates** (page 601)
- **Installed Application Statistics** (page 602)
- **Installed Configuration Profile Statistics** (page 602)
- **Installed Provisioning Profile Statistics** (page 603)
- **Installed Certificate Statistics** (page 603)
- **Device Tracking** (page 603)
- **Custom Fields** (page 605)
- **Mobile Application Packages** (page 605)
- **Application Packages** (page 606)
- **App Store Volume Purchase Codes** (page 607)
- **Mobile Configuration Profile Definitions** (page 608)
- **iOS Provisioning Profile Definitions** (page 609)
- **Mobile Media** (page 609)
- **Mobile Actions** (page 610)
- **Mobile Device Policies** (page 611)
- **Device Commands** (page 611)
- **EAS Policies** (page 611)

Device Information

The **Device Information** category contains information on the managed mobile devices themselves.

Mobile Device Name	The name of the connected mobile device. For iOS devices, this is the name that was given to the device in iTunes or the device settings. For Android devices, the name is assigned by Absolute Manage and can be changed as described in “Naming Android devices” on page 188.
Mobile Device Model	The type of the connected mobile device.
Mobile Device Model Number	iOS and Android devices only: The model number the device vendor uses to identify the mobile device in its ordering system.
Mobile Device OS Version	The version number of the operating system installed on the mobile device.
Mobile Device OS Build Number	The build number of the operating system version installed on the mobile device.
Mobile Device OS Platform	The operating system family used on this device.
Mobile Device Serial Number	iOS and Android devices only: The serial number of the mobile device.
Mobile Device Phone Number	The telephone number currently assigned to the mobile device, if any.
Mobile Device Last Contact	The time when the last communication from the mobile device was received by the MDM server.

Mobile Device Ownership	Whether the device belongs to the company or the user. (This information can be changed with the Set Device Ownership context menu command.)
Mobile Device IMEI/ MEID	The IMEI (GSM) or MEID (CDMA) telephone identification number of the connected mobile device, if any.
Mobile Device Identifier (UDID)	The target identifier (a unique internal ID) of the connected mobile device.
Mobile Device Capacity	iOS and Android devices only: The storage capacity of the mobile device, excluding space required by the operating system. This capacity is usually a few gigabytes below the nominal capacity. (For example, a 32 GB iPhone may have a capacity of 29.33 GB.) For iOS devices, this number is the same as the capacity displayed in iTunes.
Mobile Device Available Capacity	iOS and Android devices only: The free storage on the mobile device. For iOS devices, this number is the same as the free space displayed in iTunes.
Mobile Device Bluetooth MAC Address	iOS and Android devices only: The MAC address of the mobile device's Bluetooth connection.
Mobile Device WiFi MAC Address	iOS and Android devices only: The MAC address of the mobile device's WiFi connection.
Mobile Device GPS Capable	iOS and Android devices only: Whether the mobile device can locate itself by GPS signals. Note that devices which are not GPS capable may still be able to locate themselves by other means, such as known locations of cell towers or WiFi networks in range. However, these location methods are usually less accurate than GPS location.
Mobile Device Production Date	iOS devices only: The date when the mobile device was manufactured.
NOTE	The content of this information item, same as with the next four information items listed below, is downloaded from an Apple server, based on the device's serial number. It is therefore available only if the iOS device had a working Internet connection at least once after being enrolled in the MDM management. The information is updated every ten days as long as the device continues to have an Internet connection to the Apple server.
Mobile Device Purchase Date	iOS devices only: The date when the iOS device was purchased, according to Apple's files.
NOTE	See the note for Mobile Device Production Date, above.

Mobile Device Age	iOS devices only: The age of the mobile device, i.e., the time that has elapsed since its production.
NOTE	See the note for Mobile Device Production Date, above.
Mobile Device Warranty Info	iOS devices only: The iOS device's current warranty status.
NOTE	See the note for Mobile Device Production Date, above.
Mobile Device Warranty End	iOS devices only: The date when the warranty for the iOS device will end. A value of "n/a" indicates either that no information is available or that the warranty has expired.
NOTE	See the note for Mobile Device Production Date, above.
Mobile Device Public IP Address	iOS and Android devices only: The public IPv4 address over which the mobile device was communicating with Absolute Manage at the time of its last contact. This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet.
Mobile Device Public IP Address (v6)	iOS and Android devices only: The public IPv6 address over which the mobile device was communicating with Absolute Manage at the time of its last contact. This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet.
Mobile Device Cell IP Address	iOS and Android devices only: The IP address of the mobile device in the mobile (cellular) network it is currently using (if any).
Mobile Device WiFi IP Address	iOS and Android devices only: The IPv4 address of the mobile device in the WiFi network it was using at the time of its last contact (if any).
Mobile Device WiFi IP Address (v6)	iOS and Android devices only: The IPv4 address of the mobile device in the WiFi network it was using at the time of its last contact (if any).
Mobile Device WiFi Network	iOS and Android devices only: The name of the WiFi network (if any) to which the mobile device was connected at the time of its last contact.
Mobile Device Is Tablet	iOS and Android devices only: Whether the mobile device is a tablet or not.
Mobile Device Display Resolution	iOS and Android devices only: The screen size of the mobile device, measured in pixels.

Mobile Device Battery Level	iOS and Android devices only: The remaining charge level of the mobile device's battery, expressed as a percentage.
Mobile Device Status	The management status of the device: <ul style="list-style-type: none">• Unmanaged: This device is not part of the MDM.• Managed and offline: The device is part of the MDM system but has not responded to the last contact request.• Managed and online: The device is part of the MDM system and has responded to the last contact request.
Mobile Device Managed	Whether the device is managed: The information item contains "true" if the device is managed and online or managed and offline; it contains "false" if the device is unmanaged (see above).
Mobile Device Jailbroken	iOS and Android devices only: Whether the device has been jailbroken, that is, whether it contains modified firmware.
Mobile Device Supports Persistence	Android devices only: Whether the device supports persistence, i.e., lets the Absolute Manage client software remain on the device even after removal attempts and factory resets.
Mobile Device Modem Firmware Version	iOS and Android devices only: The version number of the modem firmware in the mobile device, if any.
Mobile Device Hardware Encryption	iOS and Android devices only: The kind of hardware encryption (block level or file level) available on the device.
Mobile Device Passcode Compliant	iOS and Android devices only: The passcode on the device complies with all applicable requirements, including those of Exchange when applicable.
Mobile Device Passcode Compliant with Profiles	iOS and Android devices only: The passcode on the device complies with all active profiles.
Mobile Device Passcode Present	iOS and Android devices only: A passcode (PIN to wake up the device) is set on the mobile device.
Mobile Device Is Roaming	iOS and Android devices only: Whether the mobile device is currently roaming (connected to a mobile network other than that of the standard provider).
Mobile Device Data Roaming Enabled	iOS and Android devices only: Whether the mobile device is set to allow data roaming (exchanging data over mobile networks other than that of the standard provider).

Mobile Device Voice Roaming Enabled	iOS devices only: Whether the mobile device is set to allow voice roaming (initiating or receiving voice calls over mobile networks other than that of the standard provider).
Mobile Device Home Network	iOS and Android devices only: The standard mobile network of the mobile device.
Mobile Device Cellular Technology	iOS and Android devices only: The basic cellular technology that the mobile device is currently using to communicate, such as GSM or CDMA.
Mobile Device Current Carrier Network	The mobile network into which the mobile device was booked at the time of the last contact.
Mobile Device Carrier Settings Version	iOS and Android devices only: The version number of the carrier settings in the iOS device. Carrier settings include the name of the various available networks and other information. They are provided by Apple and can be updated independently of the iOS software.
Mobile Device Home Mobile Country Code	iOS and Android devices only: The mobile country code of the standard mobile network of the mobile device.
Mobile Device Home Mobile Network Code	iOS and Android devices only: The mobile network code of the standard mobile network of the mobile device.
Mobile Device Current Mobile Country Code	iOS and Android devices only: The mobile country code of the mobile network into which the iOS device was booked at the time of the last contact.
Mobile Device Current Mobile Network Code	iOS and Android devices only: The mobile network code of the mobile network into which the iOS device was booked at the time of the last contact.
Mobile Device SIM ICC Identifier	iOS and Android devices only: The mobile country code of the SIM installed in the mobile device.
Mobile Device Board	iOS and Android devices only: The name or type code of the motherboard of the mobile device. Many motherboards used in mobile devices do not have an accessible name or type code.
Mobile Device Brand	iOS and Android devices only: The brand name of the mobile device as noted in its firmware. This brand is not necessarily the manufacturer; see “Mobile Device Manufacturer”, below. (For example, the brand may also be the carrier who sold the phone.)
Mobile Device CPU Name	iOS and Android devices only: The type of the CPU used in the mobile device.

Mobile Device CPU Speed	iOS and Android devices only: The clock rate of the CPU used in the mobile device.
Mobile Device Info	Android devices only: Additional information about the mobile device as provided by its manufacturer.
Mobile Device IMEISV	Android devices only: The revision number of the software installed on the mobile device, as noted in the device's IMEI.
Mobile Device Internal Storage Available	Android devices only: The amount of internal storage for application data in the mobile device that is currently free. Note that some devices partition the built-in storage and declare some to be USB storage. In this case, the internal storage shown by this information item is much smaller than the actual built-in storage. (See "Mobile Device SD Card 1 Available," below.)
Mobile Device Internal Storage Total	Android devices only: The total amount of internal storage for application data available in the mobile device. Note that some devices partition the built-in storage and declare some to be USB storage. In this case, the internal storage shown by this information item is much smaller than the actual built-in storage. (See "Mobile Device SD Card 1 Total," below.)
Mobile Device Kernel Version	Android devices only: The version information for the operating system kernel active in the mobile device.
Mobile Device Manufacturer	The company which produced the mobile device. This is not necessarily the same company under the brand name of which the device was sold; see "Mobile Device Brand," above.
Mobile Device Network Type	Android devices only: The base technology of the cellular network to which the mobile device is connected. Possible values are "none", "EDGE", "GPRS", or "UMTS".
Mobile Device Product Name	Android devices only: The product name of the mobile device, as noted in the device's firmware. This name is usually not the same as the product name printed on the case.
Mobile Device SD Card 1 Available	Android devices only: The amount of storage that is currently free on the first SD card in the mobile device. Note that some devices partition the built-in storage and declare some to be USB storage. In this case, some of the internal storage is shown as SD card 1.
Mobile Device SD Card 1 Total	Android devices only: The amount of storage available on the first SD card in the mobile device.

	Note that some devices partition the built-in storage and declare some of it to be USB storage. In this case, some of the internal storage is shown as SD card 1.
Mobile Device SD Card 2 Available	Android devices only: The amount of storage that is currently free on the second SD card in the mobile device.
Mobile Device SD Card 2 Total	Android devices only: The amount of storage available on the second SD card in the mobile device.
Mobile Device System Cache Available	Android devices only: The amount of cache memory that is currently free on the mobile device.
Mobile Device System Cache Total	Android devices only: The total amount of cache memory on the mobile device.
Mobile Device System Memory Available	Android devices only: The amount of RAM in the mobile device that is currently free.
Mobile Device System Memory Total	Android devices only: The amount of RAM installed in the mobile device.
Mobile Device System Storage Available	Android devices only: The amount of storage memory, excluding SD cards, that is currently free on the mobile device.
Mobile Device System Storage Total	Android devices only: The total amount of storage memory, excluding SD cards, on the mobile device.
Mobile Device AbsoluteApps Version	iOS and Android devices only: The version number of the copy of AbsoluteApps that is installed on the managed mobile device.
Mobile Device AbsoluteApps Build Number	iOS and Android devices only: The build number of the copy of AbsoluteApps that is installed on the managed mobile device.
Mobile Device AbsoluteApps Supports Tracking	iOS and Android devices only: Whether the copy of AbsoluteApps installed on the device supports geotracking.
Mobile Device Record Creation Date	The time when the record for this mobile device was created in the server.
Mobile Device MDM Profile Up-to-date	iOS devices only: Whether the MDM access privileges that are set in the MDM profile on the managed device are the same as those currently set on the server. For information on updating MDM profiles, see “Updating MDM access rights on enrolled iOS devices” on page 64.
Mobile Device OS Language	The language to which the operating system on this mobile device is set.
Mobile Device GUID	The GUID (UUID) of the mobile device.

Mobile Device Identity	The identifier of the mobile device on the Exchange server.
Mobile Device Enable Outbound SMS	Whether the device is set to allow the user to send SMS messages.
Mobile Device Last Policy Update Time	The date and time when the EAS policy of the device was last modified.
Mobile Device Remote Wipe Supported	Does this device allow its contents to be remotely wiped by an administrator?
Mobile Device Wipe Ack Time	The time at which the Exchange server received the acknowledgement for the most recent wipe of the mobile device.
Mobile Device Wipe Request Time	The time at which the remote wipe setting was enabled on the mobile device.
Mobile Device Wipe Sent Time	The time at which the Exchange server sent the most recent wipe command to the mobile device.
Mobile Device Last Device Wipe Requestor	The Exchange user who initiated the most recent remote wipe of the mobile device. If the device has since again been paired to the Exchange server, this information may be lost.
Mobile Device Number of Folders Synced	The number of folders on this device that are synchronized to the Exchange server.
Mobile Device Access State	The access status that the device currently has with respect to the Exchange server. The normal status is "Allowed," which grants normal access. "Quarantined" or "blocked" indicates, respectively, limited or prohibited access. For details, see the Exchange documentation.
Mobile Device Access State Reason	A brief indication of the reason for the current access status. For details, see the Exchange documentation.
Mobile Device Remote Wipe Status	The status of the device regarding remote wipes, if any. The normal status for a mobile device with no wipes pending or underway is "DeviceOk".
Mobile Device Remote Wipe Status Note	Additional information regarding the Mobile Device Remote Wipe Status (see above). Additional information is not always available.
Mobile Device Information Last Change	The most recent time at which the information stored on the server for the mobile device changed. Note that this is not necessarily the time on which the corresponding property of the device changed, just the time when the mobile client software informed the MDM server of the change.
	Certain changes that frequently occur are not considered for this information, such as changes of the battery level, free storage, or roaming status.

Mobile Device Installed Software Last Change	The most recent time at which the information stored on the server for the software installed on the mobile device changed. Note that this is not necessarily the time on which an app was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.
Mobile Device Installed Configuration Profiles Last Change	The most recent time at which the information stored on the server for the configuration profiles installed on the mobile device changed. Note that this is not necessarily the time on which a profile was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.
Mobile Device Installed Certificates Last Change	The most recent time at which the information stored on the server for the certificates installed on the mobile device changed. Note that this is not necessarily the time on which a certificate was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.
Mobile Device Installed Provisioning Profiles Last Change	The most recent time at which the information stored on the server for the provisioning profiles installed on the mobile device changed. Note that this is not necessarily the time on which a profile was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Device User Information

Mobile Device User Display Name	The user's display name as stored in Active Directory or Open Directory.
Mobile Device User First Name	The user's first name as stored in Active Directory or Open Directory.
Mobile Device User Last Name	The user's last name as stored in Active Directory or Open Directory.
Mobile Device User Log-on Name	The account name with which the user can log into Active Directory or Open Directory.
Mobile Device User E-Mail	The user's e-mail address as stored in Active Directory or Open Directory.
Mobile Device User Phone Number	The user's phone number as stored in Active Director or Open Directory.y

Information items

Mobile Device User Department	The user's department as stored in Active Directory or Open Directory.
Mobile Device User Company	The name of the user's company as stored in Active Directory or Open Directory.
Mobile Device User Street	The user's street address as stored in Active Directory or Open Directory.
Mobile Device User City	The user's city as stored in Active Directory or Open Directory.
Mobile Device User State	The user's state as stored in Active Directory or Open Directory.
Mobile Device User ZIP Code	The user's postal code as stored in Active Directory or Open Directory.
Mobile Device User Country	The user's country as stored in Active Directory or Open Directory.
Mobile Device User Office	The user's office as stored in Active Directory or Open Directory.
Mobile Device User Organizational Unit Path	The name of the Active Directory or Open Directory organizational unit to which the mobile device's current user belongs
Mobile Device User Organizational Unit	The path of the Active Directory or Open Directory organizational unit to which the mobile device's current user belongs
Mobile Device User Is Member Of	The Active Directory or Open Directory groups to which the mobile device's current user belongs. Multiple groups are separated by commas.
Mobile Device User Enrollment Username	The username that the user entered when enrolling this device into the MDM server.
Mobile Device User Enrollment Domain	The domain that the user entered when enrolling this device into the MDM server.
Installed Applications	<p>The Installed Applications category contains information on the applications that are installed on a mobile device.</p> <p>The information items in this category apply only to iOS and Android devices.</p>
NOTE	Applications that are included with the device firmware, such as Camera or Mail on iOS devices, are not listed.
Mobile Device Installed App Name	The name of the application.

Mobile Device Installed App Version	The short version number of the application.
Mobile Device Installed App Build Number	The build number of the application.
NOTE	Not all applications have build numbers.
Mobile Device Installed App Version String	The version string of the application.
Mobile Device Installed App Bundle Identifier	The string that uniquely identifies the application's bundle.
Mobile Device Installed App Size	The amount of storage that the application takes up on the mobile device.
Mobile Device Installed App Data Size	iOS devices only: The amount of storage that the data of the application takes up on the mobile device.
Mobile Device Installed App Data Directory	Android devices only: The directory on the mobile device in which the app stores its data.
Mobile Device Managed App Status	iOS devices only: The status of this app on the specific managed device (e.g., "Managed" or "Needs redemption code").
	This information is not supported for apps on devices running iOS 4.x.
Mobile Device Managed App Prevent Data Backup	iOS devices only: Whether backing up of the apps data (through standard system backups) is prevented on this device.
Mobile Device Managed App Bound to MDM	iOS devices only: Whether the app will be automatically removed from this device once the device is no longer enrolled in an MDM management server.
Installed Configuration Profiles	The Installed Configuration Profiles category contains information about configuration profiles that are installed on administered mobile devices.
	These information items can be used in the Mobile Devices window.
Mobile Device Installed Profile Name	The name of the configuration profile.
Mobile Device Installed Profile Description	The optional description string of the profile.

Information items

Mobile Device Installed Profile Organization	The optional name of the organization which has provided the profile.
Mobile Device Installed Profile Identifier	The identifying string of the profile.
Mobile Device Installed Profile UUID	The unique identifier of the profile.
Mobile Device Installed Profile Version	The version of the profile installed on the mobile device.
Mobile Device Installed Profile Encrypted	Whether the profile is encrypted.
Mobile Device Installed Profile Managed	Whether the profile is managed by the MDM system.
Mobile Device Installed Profile Allow Removal	Whether the profile can be removed remotely.
Mobile Device Installed Profile Type	The type of profile – device profile or app profile. Device profiles contain settings for the hardware or operating system, app profiles contain settings for individual apps.

Installed Provisioning Profiles

The **Installed Provisioning Profiles** category contains information about the provisioning profiles that are installed on administered iOS devices.

These information items can be used in the **Mobile Devices** window. They apply only to iOS devices.

iOS Installed Provisioning Profile Name	The name of the provisioning profile.
iOS Installed Provisioning Profile Expiry Date	The date until which the provisioning profile is valid.
iOS Installed Provisioning Profile UUID	The unique identifier of the provisioning profile.

Installed Certificates

The **Installed Certificates** category contains information on the certificates which are installed on the administered mobile devices.

These information items can be used in the **Mobile Devices** window. They apply only to iOS devices.

Mobile Device Installed Certificate Name	The name of the certificate.
Mobile Device Installed Certificate Is Identity	Whether the certificate is the identity certificate of the device.

Installed Application Statistics

NOTE As with the information items in the Installed Applications category, applications that are included in the device firmware are not listed. Also, applications on ignored devices (see “Ignore Devices” on page 425) are not included in the statistics.

These information items can be used in the Installed Software Statistics smart group in the **Mobile Devices** window. They apply only to iOS and Android devices.

Mobile Device Inst. App Name	The name of the application being summarized.
Mobile Device Inst. App Count	The number of copies of the application being summarized that were found across all mobile devices.
Mobile Device Inst. App Bundle Identifier	The string that uniquely identifies the bundle of the application being summarized.

Installed Configuration Profile Statistics

The **Installed Configuration Profile Statistics** category contains summary information on the configuration profiles installed on the managed mobile devices.

These information items can be used in groups in the **Mobile Devices** window that provide configuration profile statistics

Mobile Device Inst. Profile Name	The name of the configuration profile being summarized.
Mobile Device Inst. Profile Count	The number of copies of the configuration profile being summarized that were found across all managed mobile devices.
Mobile Device Inst. Profile Managed Count	The number of found copies of the configuration profile that are managed.
Mobile Device Inst. Profile Description	The description of the configuration profile being summarized.

Information items

Mobile Device Inst. Profile Identifier	The (locally) unique identifier of the configuration profile being summarized.
Mobile Device Inst. Profile Organization	The organization which has issued the configuration profile being summarized.
Mobile Device Inst. Profile UUID	The globally unique identifier of the configuration profile being summarized.
Installed Provisioning Profile Statistics	<p>The Installed Provisioning Profile Statistics category contains summary information on the provisioning profiles installed on the managed iOS devices.</p> <p>These information items can be used in groups in the Mobile Devices window that provide provisioning profile statistics. They apply only to iOS devices.</p>
iOS Inst. Prov. Profile Name	The name of the provisioning profile being summarized.
iOS Inst. Prov. Profile Count	The number of copies of the provisioning profile being summarized that were found across all managed mobile devices.
iOS Inst. Prov. Profile Max Expiry Date	The latest expiry date found in any of the copies of the provisioning profile being summarized.
iOS Inst. Prov. Profile Min Expiry Date	The earliest expiry date found in any of the copies of the provisioning profile being summarized.
iOS Inst. Prov. Profile UUID	The globally unique identifier of the configuration profile being summarized.
Installed Certificate Statistics	<p>The Installed Certificate Statistics category contains summary information on the certificates installed on the managed iOS devices.</p> <p>These information items can be used in groups in the Mobile Devices window that provide certificate statistics. They apply only to iOS devices.</p>
Mobile Device Inst. Certificate Name	The name of the certificate being summarized.
Mobile Device Inst. Certificate Count	The number of copies of the certificate being summarized that were found across all managed mobile devices.
Mobile Device Inst. Certificate Identity Count	The number of copies of the certificate being summarized that are used as identity certificates on managed mobile devices.
Device Tracking	The Device Tracking category contains geotracking information on tracked mobile devices.

These information items can be used in groups in the **Mobile Devices** window that list mobile devices. They apply only to iOS and Android devices.

Mobile Device Tracking Enabled	Whether the geolocation of this device is being tracked.
Mobile Device Tracking Interval	The interval in which the geolocation of this device is recorded.
Mobile Device Tracking Accuracy	The tracking accuracy set for this device. Note that the actual accuracy of a particular location record (see the Mobile Device Location Accuracy information item, below) may be lower than this setting when the desired accuracy is not technically possible at the time of recording the location.
Mobile Device Tracking Time	The time when the location of the device was determined.
Mobile Device Location Latitude	The latitude at which the device was located.
Mobile Device Location Longitude	The longitude at which the device was located.
Mobile Device Location Accuracy	The maximum possible distance from the true position with which the device was located.
Mobile Device Location Cell IP Address	The IP address of the mobile device in the mobile (cellular) network it is currently using (if any). This information is reported only when it changes; otherwise, the information item contains "n/a".
Mobile Device Location Public IP Address	The public IP address over which the mobile device is communicating with Absolute Manage. This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet. This information is reported only when it changes; otherwise, the information item contains "n/a".
Mobile Device Location WiFi IP Address	The IPv4 address of the mobile device in the WiFi network it is currently using (if any). This information is reported only when it changes; otherwise, the information item contains "n/a".
Mobile Device Location WiFi IP Address (v6)	The IPv6 address of the mobile device in the WiFi network it is currently using (if any). This information is reported only when it changes; otherwise, the information item contains "n/a".

Mobile Device Location Battery Level

The remaining charge level of the mobile device's battery at the time the location was recorded, expressed as a percentage.

Mobile Device Location Battery State

The state of the mobile device's battery when the location was recorded:

- On Battery (Discharging): The device is running on battery power.
- On Power (Charging): The device is running on mains power.
- Full: The battery is full

Custom Fields

The **Custom Fields** category contains all custom information fields for mobile devices that have been defined on the currently connected server.

The exact contents of this category and the functions of the individual fields depend entirely on the specific local configuration of the site and cannot be described further here.

NOTE Double-clicking a custom information item in the **Information Items** window lets you edit its specifications.

Mobile Application Packages

The **Mobile Application Packages** category contains information on the mobile application packages which have been created in Absolute Manage.

These information items can be used in the **Mobile Devices** window, in the **In-house Applications** group as well as the **In-house Applications** groups of policies. They apply only to iOS and Android devices.

Mobile App Name

The name of the application package.

Mobile App Version

The version number of the application contained in the package.

Mobile App Build Number

The build number of the application contained in the package.

Mobile App OS Platform

The operating system for which the application contained in the package was written.

Mobile App Size

The size the app code requires on the mobile device after installation.

Mobile App Is Universal

iOS devices only: Whether this app runs on all three iOS hardware platforms – iPhone, iPad, and iPod touch.

Mobile App Supported Devices

iOS devices only: A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) on which this app runs.

Mobile App Min OS Version

The minimum version of the mobile operating system that this app requires to run.

Mobile App Bundle Identifier	The unique identifier of the application package.
Mobile App Short Description	The short description of the application package.
Mobile App Long Description	The long description of the application package.
Mobile App Update Description	The update description of the application package.
Mobile App Prevent Data Backup	The application data of this app is not included in standard device backups via iTunes. This is always false for Android apps.
Mobile App Remove When MDM Is Removed	iOS devices only: This application will be automatically removed from the device when the device is no longer managed through an MDM system (i.e., when the MDM profile is deleted from the device). This is always false for Android apps.
Mobile App Assignment Rule	Whether the app is installed automatically or on-demand and removed automatically or manually.
Application Packages	
The Application Packages category contains information on the mobile applications that an administrator has specified as recommended apps in Absolute Manage.	
These information items can be used in the Mobile Devices window, in the App Store Applications group and the 3rd Party Applications groups of policies. They apply only to iOS and Android devices.	
App Name	The name of the application package.
App Category	The category of the application package, as specified by the administrator.
App Min OS Version	The minimum version of the operating system required to use the app.
App OS Platform	The mobile operating system on which this app runs.
App Short Description	The short description of the app.
App Long Description	The long description of the app.
App URL	The URL of the app's page in the App Store.
App Supported Devices	iOS devices only: A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) on which this app runs.

App Is Universal	iOS devices only: Whether this app runs on all three iOS hardware platforms – iPhone, iPad, and iPod touch.
App Prevent Data Backup	iOS devices only: Whether the data of this app on the device is prevented from being included in system backups. This is always false for Android apps.
App Remove When MDM Is Removed	iOS devices only: Whether this app will be automatically deleted from devices that are no longer enrolled on an MDM server. This is always false for Android apps.
App Store VPP Codes Purchased	iOS apps only: The total number of App Store volume purchase program codes that have been imported for this app.
App Store VPP Codes Redeemed	iOS apps only: The number of App Store volume purchase program codes that have already been used to install a copy of this app on an administered mobile device.
App Store VPP Codes Remaining	iOS apps only: The remaining number of App Store volume purchase program codes that are available for installing this app on an administered mobile device.
App Store VPP Order Number	iOS apps only: The order number under which the App Store volume purchase program codes were bought.
App Store VPP Purchaser	iOS apps only: The App Store user through whose account the App Store volume purchase program codes were bought.
App Assignment Rule	Whether the app is installed automatically or on-demand and removed automatically or manually.
App Store Volume Purchase Codes	
The App Store Volume Purchase Codes category contains information about individual purchase codes from the App Store volume purchase program.	
These information items can be used in the Mobile Devices window, in the App Store Applications group and the 3rd Party Applications groups of policies.	
ASVPP Redemption Code	The actual purchase code that must be entered.
ASVPP Code Redeemed	Whether the code has already been redeemed.
ASVPP Redemption Date	The date when the code has been redeemed. If the code has not yet been redeemed, this information item contains "n/a".

Mobile Configuration Profile Definitions	The Mobile Configuration Profile Definitions category contains information on the configuration profiles with have been imported into Absolute Manage.
	These information items can be used in the Mobile Devices window, in the Assignable Items > Configuration Profiles group.
Mobile Profile Name	The name of the configuration profile.
Mobile Platform Type	The mobile OS platform to which this configuration profile applies.
Mobile Profile Type	The type of profile – device profile or app profile. Device profiles contain settings for the hardware or operating system, app profiles contain settings for individual apps.
Mobile Profile Description	The description of the configuration profile.
Mobile Profile Organization	The organization which has issued the configuration profile.
Mobile Profile Identifier	The unique identifier of the configuration profile, as entered by the creator of the profile.
Mobile Profile UUID	The automatically created globally unique ID of the configuration profile.
Mobile Profile Allow Removal	Whether the profile may be removed from the iOS device by the user. Possible values include, "Never", "Always", and "With authentication".
Mobile Profile Variables Used	A comma-separated list of variables that are used in this configuration profile. See "Creating configuration profiles containing variables" on page 143 for more information on variables in configuration profiles.
Assigned Mobile Profile Availability	Whether the profile is always available on the devices to which it was assigned or only at certain times.
Assigned Mobile Profile Availability Start Time	The time when the profile becomes available on the devices to which it was assigned.
Assigned Mobile Profile Availability End Time	The time when the profile stops being available on the devices to which it was assigned.
Assigned Mobile Profile Assignment Rule	Whether the profile is installed automatically or on-demand and removed automatically or manually.

iOS Provisioning Profile Definitions

The **iOS Provisioning Profile Definitions** category contains information on the provisioning profiles with have been found on administered iOS devices.

These information items can be used in the **Mobile Devices** window, in the **Assignable Items > Provisioning Profiles** group.

iOS Provisioning Profile Name

The name of the provisioning profile.

iOS Provisioning Profile Expiry Date

The date until which the provisioning profile is valid.

iOS Provisioning Profile UUID

The automatically created globally unique ID of the provisioning profile.

Mobile Media

The **Mobile Media** category contains information on mobile media files that are managed by Absolute Manage.

These information items can be used in the **Mobile Devices** window, in the **Assignable Items > Media** group.

Media Name

The name of the mobile media file, as specified in the **Mobile Media File** dialog. (See also “Media File Name” below.)

Media Description

The description of the mobile media file, as entered in the **Mobile Media File** dialog.

Media File Size

The size (in bytes) of the mobile media file on disk.

Media Type

The file type of the mobile media file.

Media Category

The content category to which the mobile media file has been assigned in the **Mobile Media File** dialog.

Media File Can Leave AbsoluteSafe

Whether the mobile users are permitted to take this file out of AbsoluteSafe, either to view or edit it in another app or to forward it to other devices.

Media File Can Be E-Mailed

Whether the mobile media file can be sent from within AbsoluteSafe to the system mail program for e-mailing to another device.

Media File Can Be Printed

Whether the mobile media file can be printed from within AbsoluteSafe.

Media File Is WiFi-Only

Whether the mobile media file is downloaded only when the device is connected over WiFi.

Media File Last Modified

The date when the mobile media file object (as opposed to the file that it specifies) was last edited.

Media File Name	The name of the file specified in the mobile media file object. (See also Media Name, above.)
Media Unique Identifier	The unique internal modifier of the mobile media file within Absolute Manage.
Assigned Media Availability	Whether the media file is always available on the devices to which it was assigned or only at certain times.
Assigned Media Availability Start Time	The time when the media file becomes available on the devices to which it was assigned.
Assigned Media Availability End Time	The time when the media file stops being available on the devices to which it was assigned.
Assigned Media Assignment Rule	Whether the media file is installed automatically or on-demand and removed automatically or manually.
Mobile Actions	<p>The Mobile Actions category contains information on the actions which have been defined for assignment to smart policies.</p> <p>These information items can be used in the Mobile Devices window, in views where actions are displayed.</p>
Mobile Action Name	The name of the action.
Mobile Action Description	The description of the action, as entered by the administrator.
Mobile Action Type	The type of the action, e.g., send message or freeze device.
Mobile Action Supported Platforms	The mobile operating systems on which this action can be performed.
Mobile Action Unique Identifier	The unique identifier of the action.
Mobile Action Device Execution Time	<p>The last time the action was executed on this device.</p> <p>This information item can only be used in views displaying the actions that have been performed on a particular device.</p>
Mobile Action Policy Initial Delay	<p>The delay between a device entering this policy and the first execution of the action on that device.</p> <p>This information item can only be used in views displaying the actions assigned to a particular policy.</p>
Mobile Action Policy Repeat Count	<p>The number of times that the action is specified to be executed on devices belonging to this smart policy.</p> <p>This information item can only be used in views displaying the actions assigned to a particular policy.</p>

Mobile Action Policy Repeat Interval	The interval between repeated executions of the action on devices belonging to this smart policy. This information item can only be used in views displaying the actions assigned to a particular policy.
Mobile Device Policies	The Mobile Device Policies category contains information on the mobile device policies which have been created in Absolute Manage. These information items can be used in the Mobile Devices window, in the Policies section.
Policy Name	The name of the policy.
Is Smart Policy	Whether this policy is a smart policy, i.e., a policy in which mobile devices are included automatically according to rules set in the policy.s
Device Commands	The Device Commands category contains information on commands issued to managed mobile devices. These information items can be used in the Mobile Devices window, in the Commands section.
Mobile Device Command Type	The command that was sent to the mobile device.
Mobile Device Command Status	The current status of the command.
Mobile Device Command Time Issued	The date and time when the command was sent by Absolute Manage Admin to Absolute Manage Server. Note that this time is not necessarily the time when the mobile device received the command, as commands are forwarded to the device only when it contacts the push notification server. This can take some time, even days, if the device is, e.g., switched off or overseas with roaming disabled.
Mobile Device Command Error	The error, if any, of the command execution that was returned.
Mobile Device Command Error Info	A verbose explanation of the returned error.
Mobile Device Command Finish Time	The time when the execution of the command finished on the mobile device.
EAS Policies	The EAS Policies category contains information on the Exchange ActiveSync policy settings which are active on administered Windows Phone devices. These information items can be used in the Mobile Devices window.

	All information items in this category apply only to Windows Phone devices.
EAS Allow Bluetooth	Whether and to which degree the EAS policy active on this device allow Bluetooth to be used on it: <ul style="list-style-type: none">• Allow: The user can access all Bluetooth capabilities.• HandsFreeOnly: The user can use Bluetooth headsets, but all other devices are blocked.• Disable: The user cannot access any Bluetooth functions of this device.
EAS Allow Browser	Whether the EAS policy active on this device allows Microsoft Pocket Internet Explorer to be used on it. Note that this setting does not affect third-party browsers.
EAS Allow Camera	Whether the EAS policy active on this device allows the camera (if any) of it to be used.
EAS Allow Consumer E-mail	Whether the EAS policy active on this device allows the user of it to configure a personal e-mail account.
EAS Allow Desktop Sync	Whether the EAS policy active on this device allows it to be synchronized with a desktop computer via direct cable connection.
EAS Allow External Device Management	Whether the EAS policy active on this device allows it to access the Exchange server even if it is being managed by an external device management program. Note that Absolute Manage is not considered "external" for purposes of this setting, because it works through the Exchange server.
EAS Allow HTML E-mail	Whether the EAS policy active on this device allows HTML e-mails on it.
EAS Allow Internet Sharing	Whether the EAS policy active on this device allows it to be used as an internet modem for other devices (tethering).
EAS Allow IrDA	Whether the EAS policy active on this device allows it to accept infrared connections.
EAS Allow Mobile OTA Update	Whether the EAS policy active on this device allows it to see certain available updates. Not all Windows Phone devices may support this restriction.
EAS Allow Non-Provisionable Devices	Whether the EAS policy active on this device allows non-provisionable devices to synchronize with the Exchange server. Non-provisionable devices are devices that cannot enforce all of the restrictions specified in the EAS policy.
EAS Allow POP/IMAP E-mail	Whether the EAS policy active on this device allows the user to configure a POP or IMAP e-mail account on it.

EAS Allow Remote Desktop	Whether the EAS policy active on this device allows it to view the screens of other devices using a remote desktop connection.
EAS Allow Simple Device Password	Whether the EAS policy active on this device allows the user to set a device password with a recognizable pattern (e.g., 1111 or 1234) on it.
EAS Allow S/MIME Encryption Algorithm Negotiation	Whether the EAS policy active on this device allows the messaging application to negotiate a different encryption algorithm in cases where a receiver does not support the specified algorithm.
EAS Allow S/MIME Software Certificates	Whether the EAS policy active on this device allows S/MIME software certificates.
EAS Allow Storage Card	Whether the EAS policy active on this device allows access to information on storage cards in the device.
EAS Allow Text Messaging	Whether the EAS policy active on this device allows its user to send text messages.
EAS Allow Unsigned Applications	Whether the EAS policy active on this device allows unsigned applications to be installed on it.
EAS Allow Unsigned Installation Packages	Whether the EAS policy active on this device allows unsigned installation packages to be run on it.
EAS Allow WiFi	Whether the EAS policy active on this device allows wireless Internet access on it.
EAS Alphanumeric Device Password Required	Whether the EAS policy active on this device requires the device password to be alphanumeric.
EAS Allowed Applications	A list of applications that are marked as approved for this device by the EAS policy active on it.
EAS Attachments Enabled	Whether the EAS policy active on this device allows the user to download e-mail attachments.
EAS Policy Creation Date	The date when the EAS policy active on this device was created.
EAS Device Encryption Enabled	Whether the EAS policy active on this device enables the encryption of the device.
EAS Device Password Enabled	Whether the EAS policy active on this device requires the user to set a password for the device.
EAS Device Password Expiration	The maximum time the EAS policy active on the device allows the same password to be used before it must be changed. The time has the format dd.hh.mm:ss, e.g., "04.17:30:00". If no maximum time is specified, "unlimited" is displayed.

EAS Device Password History	How many previously used password the EAS policy active on this device requires the device to store. The device will not let the user specify a new password that is the same as one of the stored passwords.
EAS Device Policy Refresh Interval	The interval in which the Exchange server sends the EAS policy to this mobile device, as specified in the EAS policy active on the device. The interval has the format dd.hh.mm:ss, e.g., "04.17.30:00". If no interval is specified, "unlimited" is displayed.
EAS IRM Enabled	Whether the EAS policy active on this device enables information rights management.
EAS Is Default Policy	Whether the EAS policy active on this device is the default mailbox policy.
EAS Maximum Attachment Size	The maximum size of e-mail attachments in kilobytes that the EAS policy active on this device allows to be downloaded.
EAS Maximum Calendar Age Filter	The maximum range of calendar entries that the EAS policy active on this device specifies to be synchronized.
EAS Maximum Device Password Failed Attempts	The maximum number of incorrect password entries that the EAS policy active on this device allows before refusing additional attempts.
EAS Maximum E-mail Age Filter	The maximum age of e-mails that are synchronized to this device by the EAS policy active on it. E-mails that are older than the specified time are not synchronized.
EAS Maximum E-mail Body Truncation Size	The maximum size in kilobytes of plain-text e-mail bodies (i.e., not counting attachments or headers) that the EAS policy active on this device synchronizes in their entirety. E-mails bodies larger than this size are truncated.
EAS Maximum E-mail HTML Body Truncation Size	The maximum size in kilobytes of HTML e-mail bodies (i.e., not counting attachments or headers) that the EAS policy active on this device synchronizes in their entirety. E-mails bodies larger than this size are truncated.
EAS Maximum Inactivity Before Device Lock	The interval of inactivity before this device locks itself that the EAS policy active on it specifies. The interval has the format hh.mm:ss, e.g., "06.20:00". If no interval is specified, "unlimited" is displayed.
EAS Minimum Device Password Complex Characters	The minimum number of non-letter characters that the EAS policy active on the device requires the device password to include.
EAS Minimum Device Password Length	The minimum number of characters that the EAS policy active on the device requires the device password to include in total.
EAS Mobile OTA Update Mode	The kinds of updates that the EAS policy active on the device allows the device to see. Not all Windows Phone devices may support this restriction.

EAS Policy Modification Date	The date when the EAS policy active on this device was last modified.
EAS Policy Name	The name of the EAS policy active on this device.
EAS Password Recovery Enabled	Whether the EAS policy active on this device allows the recovery password to be stored on an Exchange server.
EAS Require Device Encryption	Whether the EAS policy active on this device requires the device to be encrypted.
EAS Require Encrypted S/MIME Messages	Whether the EAS policy active on this device requires S/MIME messages to be encrypted.
EAS Require Encryption S/MIME Algorithm	The algorithm that the EAS policy active on this device specifies for encrypting an S/MIME message.
EAS Require Manual Sync When Roaming	Whether the EAS policy active on this device disables automatic synchronization with the Exchange server while the device is roaming.
EAS Require Signed S/MIME Algorithm	The algorithm that the EAS policy active on this device specifies for signing an S/MIME message.
EAS Require Signed S/MIME Messages	Whether the EAS policy active on this device requires S/MIME messages to be signed.
EAS Require Storage Card Encryption	Whether the EAS policy active on this device requires any storage card used in the device to be encrypted.
EAS Blocked Applications	A list of applications on the mobile device that are prevented from running by the EAS policy active on the device.
EAS UNC Access Enabled	Whether the EAS policy active on this device allows it to access Windows file shares.
EAS WSS Access Enabled	Whether the EAS policy active on this device allows it to access SharePoint services.

Windows Reinstallation Tasks

The **Windows Reinstallation Tasks** category contains information on reinstallation processes for Windows computers that have been dispatched to Absolute's PXE server or to a FOG server.

These information items can be used in the **Window Reinstallation Tasks** window.

There are two subcategories:

- **FOG Reinstallation Tasks** (page 616)
- **AM Reinstallation Tasks** (page 617)

FOG Reinstallation Tasks	The FOG Reinstallation Tasks category contains information on reinstallation tasks handled by a FOG server.
	These information items can be used in the Window Reinstallation Tasks window, in the FOG Reinstallation Tasks section.
FOG Host Name	The name of the computer that is being reinstalled.
FOG Image Name	The name of the image on the FOG server that is being used for the reinstallation.
FOG Image Size	The size of the image on the FOG server that is being used for the reinstallation.
FOG Image Creation Date	The date when the image on the FOG server that is being used for the reinstallation was created.
FOG Image Created By	The username of the administrator who created the image on the FOG server that is being used for the reinstallation.
FOG Task Name	The name that has been set for the FOG task. Absolute Manage does not set task names, so this information items always displays "n/a", but FOG tasks enter from other sources, e.g., through the web interface, may have names.
FOG Task State	The current processing state of the reinstallation task, e.g., "in progress". Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing Synchronize Records from the context menu.
FOG Task Type	The type of the FOG task displayed. Tasks initiated by Absolute Manage always have the type "Push image" but tasks from other sources, e.g., FOG's web interface, may have different types.
FOG Task Creation Date	The date and time when the FOG server received the command to execute the task.
FOG Task Data Copied	The amount of data that has been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing Synchronize Records from the context menu.
FOG Task Data Total	The total amount of data that needs to be copied to the target computer.
FOG Task Percent Complete	The ratio of the total data that has already been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing Synchronize Records from the context menu.
FOG Task Time Elapsed	The length of time that the reinstallation process has been taken so far. Note that this information is updated only periodically. You can refresh

AM Reinstallation Tasks

Reinstallation Task State

the information by right-clicking and choosing **Synchronize Records** from the context menu.

For completed reinstallations, the total amount of time they have taken is displayed.

Reinstallation Task Percent Complete

The **AM Reinstallation Tasks** category contains information on reinstallation tasks handled by a Absolute Manage Server with the support of an Absolute Manage PXE server.

These information items can be used in the **Window Reinstallation Tasks** window, in the **AM Reinstallation Tasks** section.

Reinstallation Task Info

The current processing state of the reinstallation task, e.g., "In progress."

Reinstallation Task Data Total

The ratio of the total data that has already been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

Reinstallation Task Data Copied

Diagnostic info on the reinstallation task, if any.

The total amount of data that needs to be copied to the target computer.

Reinstallation Task Last Update

The amount of data that has so far been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

The last time that information about this task was received from the updater process.

In effect, this is the record modification date for the reinstallation task description and the date at which all variable fields (like Reinstallation Task Data Copied) were updated.

Reinstallation Task Join AD Domain

Whether the computer being reinstalled will automatically join an Active Directory domain afterwards.

This information item corresponds to the **Join domain after imaging task** option in the **Reinstall Windows Computer** dialog.

Reinstallation Task Domain to Join

The name of the Active Directory domain (if any) that the computer being reinstalled will join after the reinstallation is complete.

This information item corresponds to the **Domain to join** field in the **Reinstall Windows Computer** dialog.

Reinstallation Task Hostname Action

What will done about the hostname of the reinstalled computer.

This information item corresponds to the **Computer name** option in the **Reinstall Windows Computer** dialog.

Reinstallation Task
Hostname to Set The new hostname of the reinstalled computer (if it is not set to keep the previous hostname).

This information item corresponds to the **Use name** field in the **Reinstall Windows Computer** dialog.

Chapter 24

Absolute Remote

Absolute Remote is a VNC viewer application that is part of Absolute Manage. It is compatible with any VNC-compliant host software on remote computers;.

Absolute Remote is automatically installed with Absolute Manage and usually launched from within it with the **Remote Control** context menu command.

The menus and commands of Absolute Remote are described in these sections:

- “Connection” on page 620
- “Edit” on page 621
- “View” on page 623
- “Session” on page 624
- “Command” on page 625
- “Window” on page 625
- “Help” on page 626

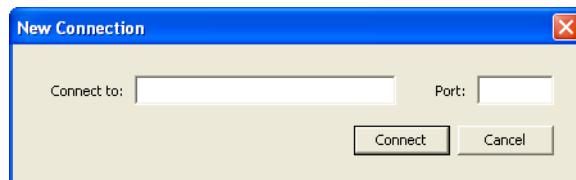
Connection

The **Connection** menu contains commands for opening and closing connections:

- **New** (page 620)
- **Open** (page 620)
- **Recent Connections** (page 621)
- **Close** (page 621)
- **Save As** (page 621)

New

The **New** command opens the **New Connection** dialog:



The dialog contains these elements:

- **Connect to:** The DNS name or IP address of the computer to which you want to connect.
- **Port:** The port of the remote computer to which you want to connect. This is usually 5900.

Open

The **Open** command opens a standard Open dialog in which you can choose a saved connection document.

Clicking **Open** causes Absolute Remote to connect to the remote computer specified in the connection document with the saved settings.

Recent Connections

The **Recent Connections** submenu contains the most recent connections that you have established in Absolute Remote.

Choosing a connection from the submenu opens it with the same settings it had when you closed it.

Choosing **Clear Menu** removes all recent connections from the submenu.

Close

The **Close** command closes the frontmost window and the connection to the computer displayed in it.

Save As

The **Save As** command opens a standard Save dialog in which you can save the current connection to disk as a document.

Clicking **Save** saves the address of the target computer and the current connection settings in a connection document.

Edit

The **Edit** menu contains commands for manually transferring the clipboard content to or from the remote computer.

- **Send Clipboard** (page 621)
- **Get Clipboard** (page 621)
- **Settings** (page 622)

Send Clipboard

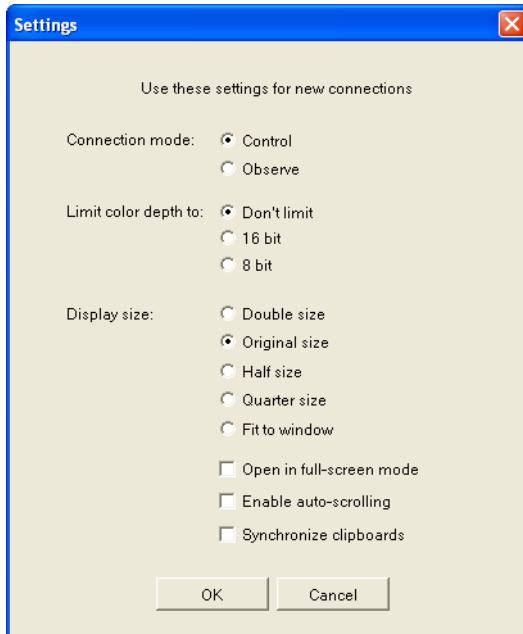
The **Send Clipboard** command transfers the content of your clipboard to the clipboard of the remote computer displayed in the frontmost window.

Get Clipboard

The **Get Clipboard** command transfers the content of the clipboard of the remote computer displayed in the frontmost window to your clipboard.

Settings

The **Preferences** command opens the **Preferences** dialog that lets you specify settings for the application:



The dialog contains settings for specifying the defaults for a new connection:

- **Connection mode:** Choose how a new connection accesses remote computers:
 - **Control:** You can see the screen, use the mouse, and input text.
 - **Observe:** You can just see the screen but not control the computer through the remote link.
- **Limit color depth to:** The maximum color depth that the representation of the remote screen on your computer may have. If you specify **Don't limit**, the full screen depth of the remote **computer is used**.
- **Display size:** The initial enlargement or reduction used to display the remote computer screen. If you choose **Fit to window**, the maximum size is used that fully fits in the Absolute Remote window. Resizing that window changes the display enlargement factor.
- **Open in full-screen mode:** If this option is checked, the window for a new connection takes up your whole screen.
- **Enable auto-scrolling:** If this option is checked, the display of the remote screen in the Absolute Remote window automatically scrolls when the mouse pointer nears the edge of the window.
- **Synchronize clipboards:** If this option is checked, the clipboard of the remote computer and your clipboard are automatically synchronized in a new connection.

View

The **View** menu contains commands for setting the size of the remote display:

- **Full-Screen Mode** (page 624)
- **Auto-Scrolling** (page 624)
- **Double Size** (page 624)
- **Original Size** (page 624)
- **Half Size** (page 624)
- **Quarter Size** (page 624)
- **Fit to Window** (page 624)

Full-Screen Mode

The **Full-Screen Mode** command expands the frontmost window to fill the entire screen.

To return the display to windowed mode, move the mouse to the middle of the upper screen border and click the Window icon on the tab that appears.

Auto-Scrolling

The **Auto-Scrolling** command toggles the auto-scrolling mode of the frontmost window.

In auto-scrolling mode, the display scrolls automatically when the mouse pointer nears the edge of the window. This setting has no effect when the entire remote screen is visible in the window.

Double Size

The **Double Size** command enlarges the display in the frontmost window to 200%. (Each remote pixel is displayed as two by two local pixels.)

Original Size

The **Original Size** command zooms the display in the frontmost window to 100%. (Each remote pixel is displayed as one local pixel.)

Half Size

The **Half Size** command reduces the display in the frontmost window to 50%. (Two by two remote pixels are displayed as one local pixel.)

Quarter Size

The **Quarter Size** command reduces the display in the frontmost window to 25%. (Four by four remote pixels are displayed as one local pixel.)

Fit to Window

The **Fit to Window** command enlarges or reduces the display in the frontmost window to the maximum size that still fits in the window.

If the window is subsequently resized, the zooming of the remote screen is automatically adapted.

Session

The **Session** menu contains commands for configuring the running session:

- **Automatic Clipboard Transfer** (page 625)
- **Don't Limit Color Depth** (page 625)
- **Limit Color to 16 Bit** (page 625)
- **Limit Color to 8 Bit** (page 625)
- **Observe Remote Computer** (page 625)
- **Control Remote Computer** (page 625)

Automatic Clipboard Transfer

The **Automatic Clipboard Transfer** command toggles the synchronization of the local clipboard and the clipboard of the computer displayed in the frontmost window.

If the clipboards are synchronized, each change to one of them is automatically applied to the other as well. If they are not synchronized, they normally have different content (which can be transferred between them manually with the **Send Clipboard** and **Get Clipboard** commands).

Don't Limit Color Depth

The **Don't Limit Color Depth** command sets the frontmost window to display the same color depth as the remote computer does locally.

Limit Color to 16 Bit

The **Limit Color to 16 Bit** command sets the frontmost window to a color depth of 16 bit per pixel or the same color depth as the remote computer uses locally, whichever is lower.

Limit Color to 8 Bit

The **Limit Color to 8 Bit** command sets the frontmost window to a color depth of 8 bit per pixel or the same color depth as the remote computer uses locally, whichever is lower.

Observe Remote Computer

The **Observe Remote Computer** command sets the mode of the session displayed in the frontmost window to Observe. You can only see the remote screen but not perform any actions on it.

Control Remote Computer

The **Control Remote Computer** command sets the mode of the session displayed in the frontmost window to Control. You can both see the remote screen and perform any actions on it by controlling the remote mouse and the keyboard input.

Command

The **Command** menu contains commands for sending keyboard combinations to remote computers.

Choosing any of the commands from this menu is the same as pressing the corresponding keys locally on the remote computer that is displayed in the frontmost window.

Window

The **Window** menu contains the Cascade command and a list of open windows:

- **Cascade** (page 626)

Cascade

The **Cascade** command rearranges the open windows, making them all the same size and staggering them across the screen.

Help

The **Help** menu contains the **About** command:

- **About** (page 626)

About

The **About** command opens the application's About dialog. The dialog contains information on the application version and copyright information.

Absolute Manage Agent is the client software of Absolute Manage that is installed on every administered computer. It works mostly behind the scenes, acting on instructions received from the Absolute Manage Server, but has some user-accessible elements.

Absolute Manage Agent control panel

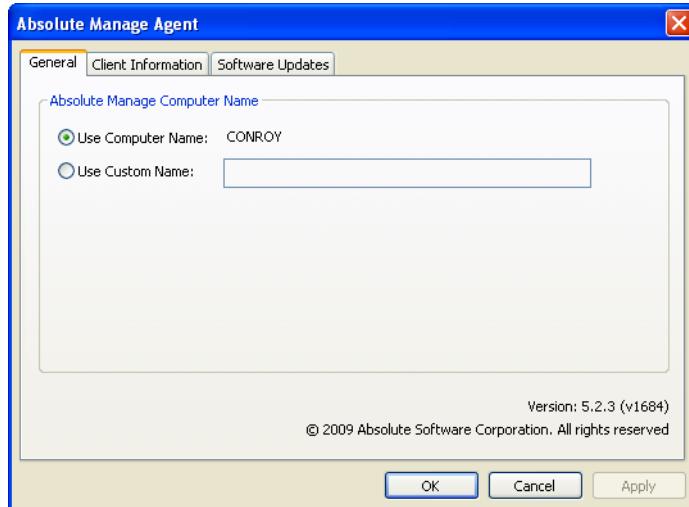
The Absolute Manage control panel is located in the **System Preferences** on Mac OS X clients and the **Control Panel** on Windows systems.

It has three panes:

- **General**
- **Client Information**
- **Software Updates**

General

The General pane lets local users set the name under which their computer appears in Absolute Manage:

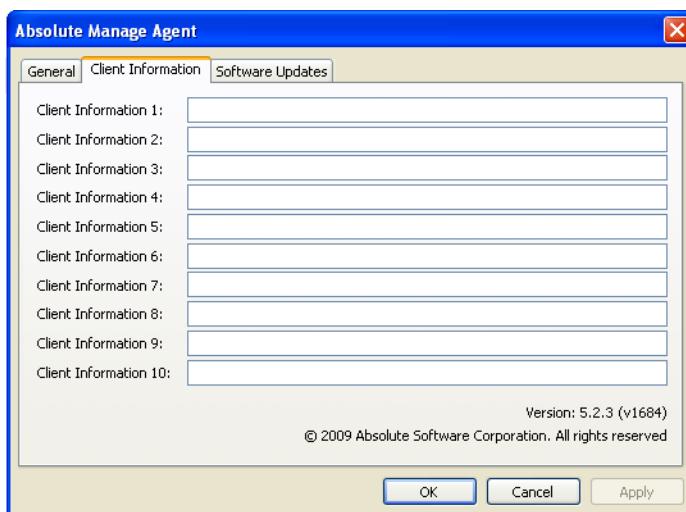


The pane contains this element:

- **Absolute Manage Computer Name:** The name that is displayed for the computer in the Absolute Manage system. You can choose to use the name specified for the computer in the local operating system or you can specify a custom name that is only used by Absolute Manage.
*Note: This setting is available to administrators in the **Agent Settings** dialog's **General** pane.*

Client Information

The **Client Information** pane lets local users specify information in up to ten fields:

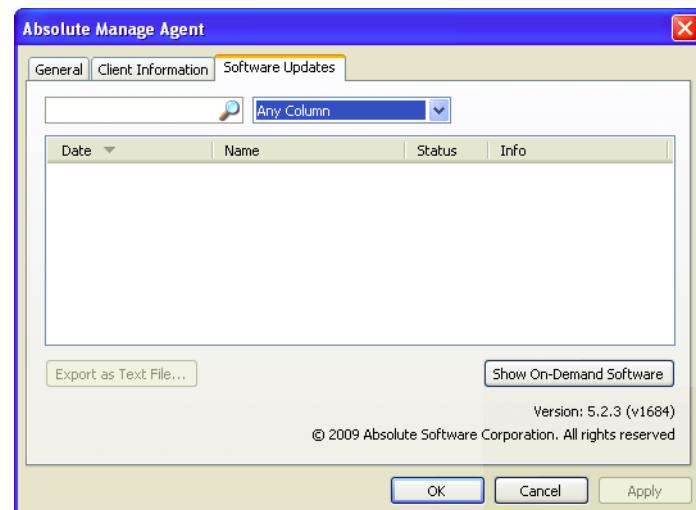


The pane contains these elements:

- **Client Information n:** All ten fields can contain custom text information that the user by default can freely edit. The names of the fields may be set on the server through the **Client Info Titles** pane of Absolute Manage Admin's **Server Settings** dialog. If a field is renamed, its label in the Absolute Manage Agent control panel changes accordingly. The fields can be locked against changes by local users in the **Agent Settings** dialog's **Client Information** pane. In that pane, administrators can also edit the fields' contents.

Software Updates

The **Software Updates** pane lists all software updates that have been installed on the computer using Absolute Manage's software distribution and patch management systems and allows local users to check for new updates:



The pane contains these elements:

- Filter field: When text is entered into this field, the display is restricted to only those software installations whose descriptions contain that string. Optionally, the filtering can be restricted to a single column, in which case only software installations containing the string in the specified column are displayed.
- Table: The table lists all software installations that have been made on this computer by means of Absolute Manage's software distribution and patch management systems. In addition to successful software package or patch installations, the table also lists failed and refused installations as well as deferred installations and installations in progress. Columns can be rearranged by dragging their titles. Clicking a title sorts the table by that column; if the title of the current sorting column is clicked, the sort order is reversed.
- **Export as Text File:** Clicking this button allows the local user to export the table's currently displayed contents as a tab-delimited text file.
- **Show On-Demand Software:** Clicking this button causes the Agent to contact its designated software distribution server for any new software packages that are marked as on-demand downloads. It displays all found packages in the **Absolute Manage Software Distribution** window.
- **Get New Software:** If you hold down the Shift key and click, the **Show On-Demand Software** button changes to **Get New Software**. Clicking this button causes the Agent to contact its designated software distribution server for new software packages, downloading any found packages according to the packages' settings.

*Note: This is the same kind of check as that invoked by the **Run Software Distribution Check** command.*

Chapter 26

Mobile Apps

Absolute Manage comes with two mobile apps, AbsoluteApps and AbsoluteSafe, that let users of managed mobile devices access distributed software and apps, and that provide reporting, messaging, and other functions to administrators.

The apps are described in these sections:

- “AbsoluteApps” on page 630
 - “AbsoluteApps for iOS” on page 630
 - “AbsoluteApps for Android” on page 632
- “AbsoluteSafe” on page 634

AbsoluteApps

AbsoluteApps is the client app for mobile devices that ties them into Absolute Manage:

- It enables administrators to provide software to mobile device users.
- It reports on the state and properties of the mobile device.
- It allows the location of the device to be tracked.
- It provides a channel for direct distribution of messages for Absolute Manager administrators to mobile device users.

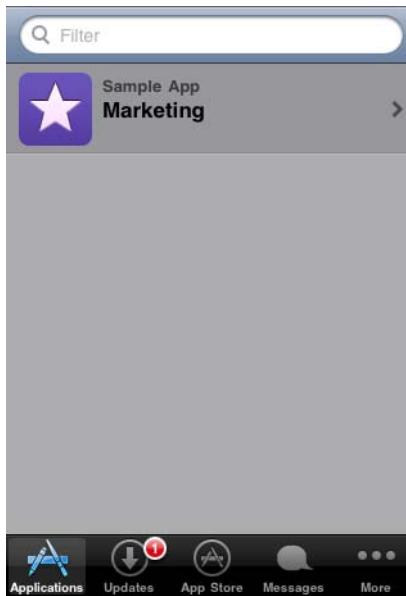
AbsoluteApps is available for iOS and Android:

- “AbsoluteApps for iOS” on page 630
- “AbsoluteApps for Android” on page 632

AbsoluteApps for iOS

The installation of AbsoluteApps is described in “Preparing iOS devices for software installation” on page 155.

AbsoluteApps is structured in multiple sections, which are described below.



Applications

The Applications section lists all applications that have been made available to the mobile device and that are not yet installed on it. (For information on making apps available, see “Installing software on mobile devices” on page 157.)

Tapping one of the listed applications displays details about it. Tapping the **Install** button in this detail view installs the application on the mobile device.

The **Filter** field at the top of the applications screen allows you to enter a string to filter the displayed apps: Only apps that contain the specified string in their names are displayed.

Updates

The Updates section lists all available updates for apps that have been installed on this device via AbsoluteApps.

Tapping an update displays details on it. Tapping the **Update** button in the details view installs the update on the mobile device.

Tapping the **Update All** button in the main Updates section installs all available updates.

App Store

The App Store section is similar to the Applications section but lists recommended apps from Apple’s App Store instead of in-house applications. This includes apps covered by volume purchases.

Messages

The Messages section contains all messages that have been sent from Absolute Manage to this mobile device.

Tapping the **Clear** button removes all messages.

More

The **More** button opens a screen where additional sections are listed.

Tapping the **Edit** button lets you configure which sections are listed on the main screen. To add a section to the main screen, drag it to the desired position in the button bar at the bottom of the edit screen. Tap **Done** to return to the More screen.

Profiles

The Profiles section lists all configuration profiles that are available for installation on the iOS device.

Tapping a profile displays its description and allows you to install it by tapping the **Install** button.

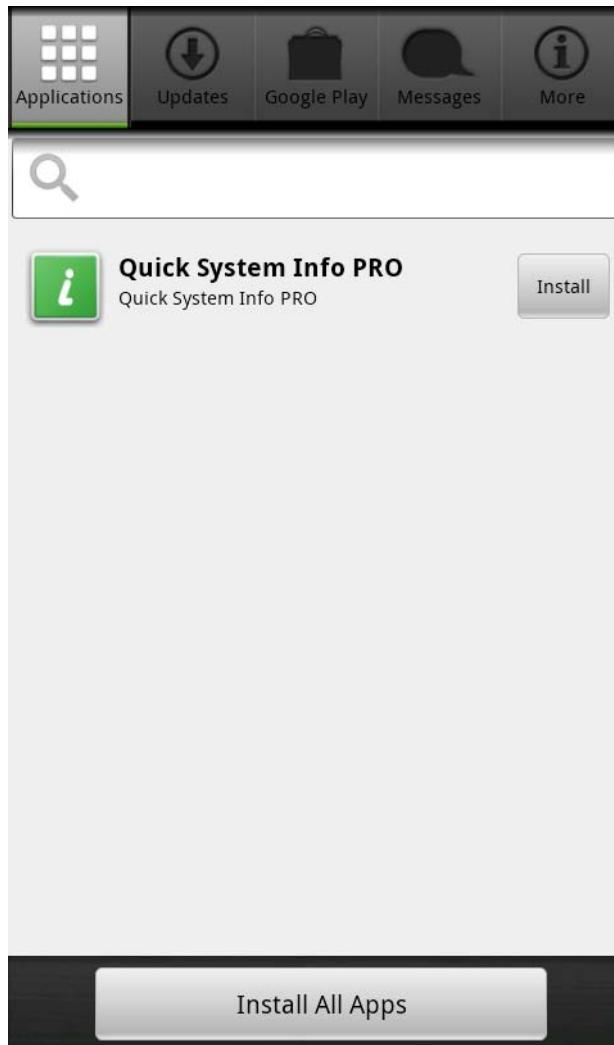
About

The About section displays version and copyright information for AbsoluteApps.

AbsoluteApps for Android

The installation of AbsoluteApps for Android is described in “Enrolling mobile devices” on page 39.

AbsoluteApps is structured in multiple sections, which are described below.



Applications

The Applications section lists all applications that have been made available to the mobile device and that are not yet installed on it. (For information on making apps available, see “Installing software on mobile devices” on page 157.)

Tapping one of the listed applications displays details about it. Tapping the **Install** button installs the application on the mobile device.

Tapping the **Install All Apps** button installs all displayed apps.

The filter field at the top of the applications screen allows you to enter a string to filter the displayed apps: Only apps that contain the specified string in their names are displayed.

Updates

The Updates section lists all available updates for apps that have been installed on this device via AbsoluteApps.

Tapping an update displays details on it. Tapping the **Update** button installs the update on the mobile device.

Tapping the **Update All Apps** button in the main Updates section installs all available updates.

Google Play

The Google Play section is similar to the Applications section but lists recommended apps from Google Play (Android Market) instead of in-house applications.

Messages

The Messages section contains all messages that have been sent from Absolute Manage to this mobile device.

Tapping the **Clear Selected** button removes the selected messages; tapping **Clear All** removes all messages.

Profiles

The Profiles section contains two tabs:

- The Installed tab lists all configuration profiles that are installed on the device.
Tapping a profile lists its details and shows a **Remove** button.
Tapping that button deletes the profile from the device.
- The Available tab lists all profiles that have been made available for optional installation on this device but aren't yet installed.
Clicking the **Install** button beside a profile installs it.

About

The About section displays version and copyright information for AbsoluteApps.

AbsoluteSafe

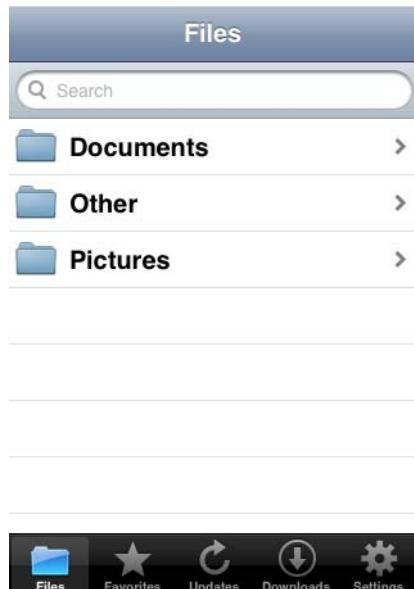
AbsoluteApps is the client app for mobile devices that lets administrators distribute media to mobile users:

- Media can be distributed selectively based on policies.
- Access to media can be restricted to specific periods of time.
- Media can be displayed in the app. For each document, administrators can allow or prohibit transfer to other apps on the mobile device.
- The app supports text, images, video, and audio documents.

AbsoluteSafe can be downloaded from Apple's App Store like any normal app. To make it easier for mobile users, you can specify AbsoluteSafe as a recommended app, as described in "Recommending third-party apps" on page 165. For your convenience, Absolute Manage ships with AbsoluteSafe predefined (see the **Mobile Devices** window, **Assignable Items > 3rd Party Applications**).

For the file types that AbsoluteSafe can display, see "Distributing media to mobile devices" on page 169.

Home screen



The home screen lists the available media, automatically sorted in folders according to the categories specified for the media files.

Tapping a folder displays the files it contains; tapping a file displays it. See "Media display screen," below, for details.

In the folders, files that you have already downloaded are displayed with solid icons; files that have not yet been downloaded have translucent icons. Files that have been downloaded but for which a newer version is available have a small plus sign overlaid over their icons:

A newer version of this document is available.

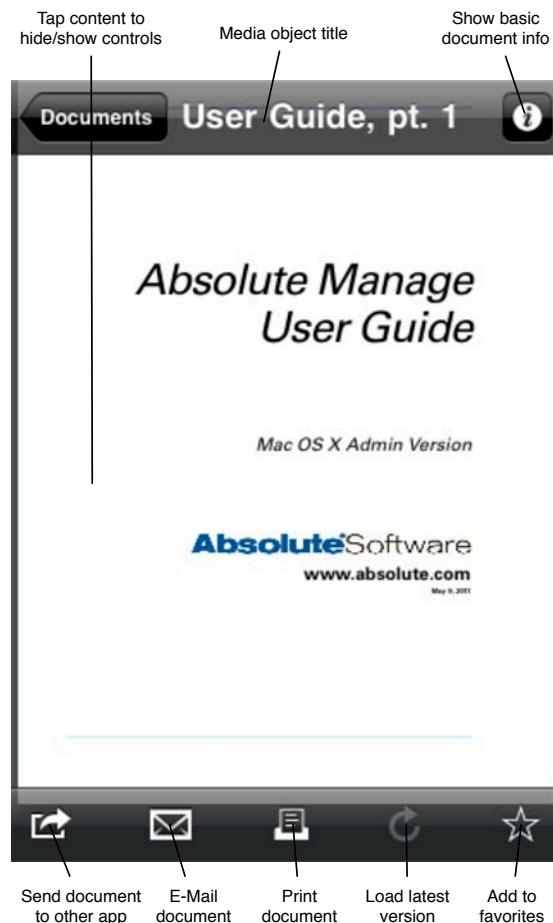
	Requirements Rev 3	
	User Guide, pt. 1	
	User Guide, pt. 2	

This document has not been loaded yet.

This document has already been loaded.

The search field at the top of the home screen lets you enter part of the name of a file you are looking for. If a string is entered in this field, all files containing the string as part of their names are listed.

Media display screen



The media display screen shows the content of supported file types. For unsupported file types, only the basic document information is shown.

You can click the main area to hide or show the controls. The controls let you:

- Show the basic document information, such as type and size, as well as the description entered by the administrator.
- Send the document to another app that supports this document type. This button is available only if the document may leave AbsoluteSafe.
- E-mail the document using Mail. This button is available only if e-mailing was enabled for the document by the administrator.
- Print the document to a compatible printer. This button is available only if printing was enabled for the document by the administrator.

- Update the document to the latest version made available by the administrator. This button is available only if a newer version of the document is available.
- Mark the document as a favorite. If the star is hollow, the document is not yet a favorite and tapping the star makes it one. If the star is filled, the document is a favorite, and tapping the star removes that status.

Favorites screen

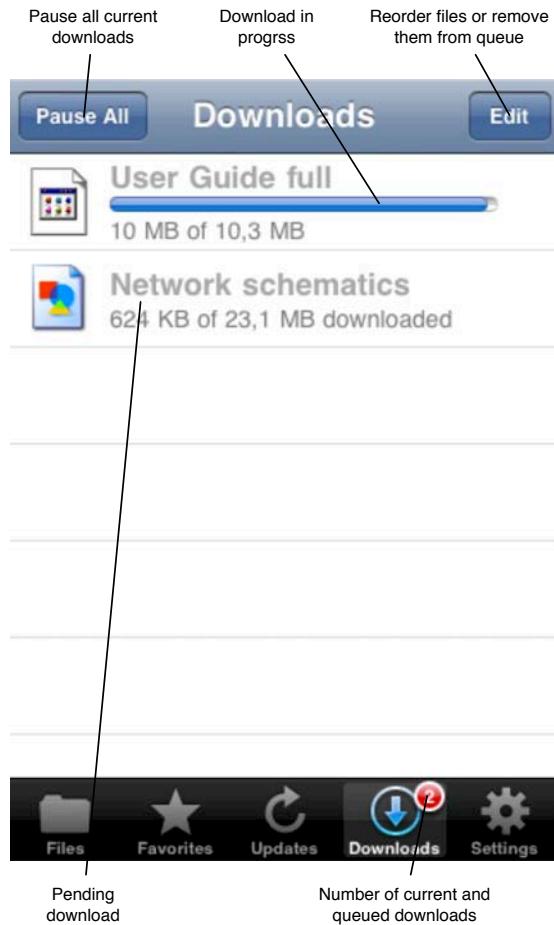
The **Favorites** screen lists all files you have marked as a favorite (see “Media display screen” above). It is otherwise like the home screen.

Updates screen

The **Updates** screen lists all files for which newer versions are available for download.

Downloads screen

The **Downloads** screen lists all downloads in progress:



Clicking the **Edit** button lets you reorder the downloads and remove individual ones.

Settings screen



The **Settings** screen:

- Displays the amount of memory used by AbsoluteSafe.
- Lets you delete all downloaded files to free up memory.
- Displays the MDM server to which you are connected.
- Lets you connect to a different MDM server.
- Displays version and copyright information.

Tapping **Remove Downloaded Files** deletes all downloaded files from your device. You can, however, redownload all files as desired.

Tapping the **Change** button lets you connect to a different MDM server.

Index

A

About (menu command)
in Absolute Remote 626
About Absolute Manage Admin (menu command) 364
Absolute Manage
 administrators explained 9
 elements of Absolute Manage explained 3
 feature overview 2
 installing 11–44
 introduction to 2–10
 running as a demo 17
 superadministrators explained 9, 10
 system overview 2–10
 system requirements 12
 updating 42
 user types explained 9
Absolute Manage Admin
 basic function 3
 changing passwords 54
 installing 15
 logging in 53
 logging out 53
Absolute Manage Agent
 access 46
 assigning license monitoring servers to 57
 assigning servers to 54
 assigning software distribution servers to 57
 basic function 3
 installing 29
 automatically 35
 on mobile devices 39
 using the Agent Deployment Center 33
Absolute Manage Agents
 configuring for license monitoring 256
 description 627–629
 information items 534–537
Absolute Manage apps 630–638
Absolute Manage InstallEase 200
Absolute Manage Server
 assigning to agents 54
 backup 100
 basic function 3
 choosing a computer 14
 configuring for license monitoring 258
 creating certificates 19
 deleting information 102
 initial configuration 16
 installing 14
 maintenance 100
 settings, exporting and importing 66
Absolute Manage SMS Integration 97
Absolute Manage Support (menu command) 363
Absolute Manage Web Site (menu command) 363
Absolute Remote 620–626
Absolute Remote Enabled (information item) 537
Absolute Remote Port (information item) 537
Absolute Remote User Confirmation Required (information item) 537
AbsoluteApps 155, 630–634
 Android 632
 iOS 630
AbsoluteSafe 634–638
AC Charger Charging (information item) 540

AC Charger Connected (information item) 540
access regulations 46–68
 overview 46
Access Status (information item) 586
Account Enabled (information item) 572
accounts *see also administrators, accounts*
Acknowledgements (menu command) 363
Action after Installation (information item) 577
Action on Clamshell Close (information item) 542
Action on Power Button (information item) 542
Action on Sleep Button (information item) 542
actions
 creating 174
 deleting 174, 176
 explained 174
 re-executing 175
 reviewing 176
 specifying in policies 179
Active Cores (information item) 538
Active Directory
 creating administrator accounts from 50
 zones 34
Active Directory integration 47
Active Directory Users (information item category) 575
AD Account Disabled (information item) 575
AD Account Name (information item) 575
AD Computer Is Member Of (information item) 555
AD Computer Name (information item) 554
AD Computer Organizational Unit (information item) 554
AD Computer Organizational Unit Path (information item) 554
AD Display Name (information item) 575
AD Login Name (information item) 575
AD User Is Member Of (information item) 555
AD User Organizational Unit (information item) 555
AD User Organizational Unit Path (information item) 555
Adapter AMC Address (information item) 560
Adapter IP Address (information item) 560
Adapter Name (information item) 560
Adapter Speed (information item) 560
Adapter Subnet Mask (information item) 560
Adapter Vendor (information item) 560
Add. Status Information (information item) 581
Address (information item) 579
admin application *see Absolute Manage Admin*
administered computers *see computers*
administering
 mobile devices 140–189
Administration (information item category) 572–575
Administrator Name (information item) 572
administrators
 account types 46
 accounts 48
 creating 48
 deleting 52
 disabling 52
 editing 51
 enabling 52
 from Active Directory users 50
 overview 46
 switching 53
 appointing to devices 57
 changing passwords 54

administrators
explained 9
information items 572–575
logging in 53
logging out 53
privileges 47
removing from devices 61
unappointing 61
viewing assignments 61
Administrators (information item category) 572
Adobe CS, installation options 219
Agent Active IP (information item) 535
Agent Build Number (information item) 535
Agent Deployment Center 510–526
automatic deployment 35
columns 511
context menu 512, 519
creating zones 34
deleting zones 37
editing zones 37
information items 511
installing Absolute Manage Agent with 33–39
predefined zones 34
searching zones 36
toolbar 511
zone definition files 518
zones 512
Agent Deployment Center (information item category) 585–586
Agent Deployment Center (menu command) 359
Agent Deployment Settings (dialog) 521
Agent Information (information item category) 534–537
Agent Name (information item) 534
Agent Port (information item) 537, 585
Agent Serial Number (information item) 535
Agent Settings (information item category) 535
Agent Settings (menu command) 287
Agent Status (information item) 586
Agent Version (information item) 534
agents see *Absolute Manage Agent*
aliases, creating 195
Allow More than Max. Downloads (information item)
580
Allow On-Demand Installation (information item) 576
Allow Remote Assistance (information item) 556
Allow Remote Control via Assistance (information item) 556
Allow to Defer For (information item) 577
Allow to Postpone Restart (information item) 577
AM Reinstallation Tasks (information item category)
617
Android devices
enrolling 39
installing Android Market (Google Play) apps 165
installing the Agent 39
naming 188
Android Market
distributing apps from 165
recommending apps from 165
Android MDM *see MDM*
Android, AbsoluteApps for 632
App Assignment Rule (information item) 607
App Category (information item) 606
App Is Universal (information item) 607
App Long Description (information item) 606
App Min OS Version (information item) 606
App Name (information item) 606
App OS Platform (information item) 606
App Prevent Data Backup (information item) 607
App Remove When MDM Is Removed (information item) 607
App Short Description (information item) 606
App Store
distributing apps from 165
recommending apps from 165
volume purchasing program 167
App Store Application Packages (information item category) 606
App Store Volume Purchase Codes (information item category) 607
App Store volume purchasing program 167
App Store VPP Codes Purchased (information item)
607
App Store VPP Codes Redeemed (information item)
607
App Store VPP Order Number (information item) 607
App Supported Devices (information item) 606
App URL (information item) 606
Apple Product Name (information item) 544
Apple Purchase Date (information item) 544
Apple Remote Desktop, remote control with 122
AppleScript, executing on administered computers
130
applications
executing on administered computers 131
appointing administrators 57
appointment group
removing devices 61
Appointment Group Name (information item) 575
appointment groups
adding devices
automatically 59
manually 58
deleting 60
editing 60
explained 57
setting up 58, 59
Appointments (information item category) 574
Assigned Media Assignment Rule (information item)
610
Assigned Media Availability (information item) 610
Assigned Media Availability End Time (information item) 610
Assigned Media Availability Start Time (information item) 610
Assigned Mobile Profile Assignment Rule (information item) 608
Assigned Mobile Profile Availability (information item)
608
Assigned Mobile Profile Availability End Time (information item) 608
Assigned Mobile Profile Availability Start Time (information item) 608
ASVPP Code Redeemed (information item) 607
ASVPP Redemption Code (information item) 607
ASVPP Redemption Date (information item) 607
ATA Bay Name (information item) 549
ATA Bus Number (information item) 548
ATA Capacity (information item) 549
ATA Device Count (information item) 546
ATA Device Type (information item) 548
ATA Devices (information item category) 548
ATA Manufacturer (information item) 548
ATA Model (information item) 548
ATA Protocol (information item) 549
ATA Revision (information item) 549
ATA Serial Number (information item) 549
ATA SMART Status (information item) 549
ATA Socket Type (information item) 549
ATA Unit Number (information item) 548
Auto Start Installation (information item) 577

-
- automated patch management 235
Automatic Clipboard Transfer (menu command) 625
Automatic Restart on Power Loss (information item)
 542
Auto-Scrolling (menu command) 624
Availability Date (information item) 576
Average Achieved Score (information item) 588
Avg. Install Count (information item) 584
Avg. Running Count (information item) 584
- B**
- Background Only (information item) 566
backing up
 clients, using Time Machine 125
 databases 100
 server database 498
Backup Date (information item) 548
Basic Inventory Only (information item) 536
batch files *see DOS batch files*
Battery % of Original Capacity (information item) 540
Battery Device Name (information item) 541
Battery Fully Charged (information item) 540
Battery Information (information item category) 540
Battery Installed (information item) 540
Battery Load Cycles (information item) 540
Battery Manufacturer (information item) 540
Battery Manufacturing Date (information item) 540
Battery Serial Number (information item) 541
Battery Temperature (information item) 541
Battery Type (information item) 540
Benchmark File (information item) 588
BIOS Date (information item) 545
BIOS Vendor (information item) 545
BIOS Version (information item) 545
Bonjour zones 34
Boot ROM Information (information item) 543
Boot Volume (information item) 548
browser windows
 adding columns 104
 Column sidebar 367
 columns 366
 configuring 104
 configuring single-computer display 106
 configuring the sidebar 103
 context menu
 sidebar 368
 table 371
 defined 70
 description 365–377
 explained 103
 filtering 109
 groups
 adding computers 111
 creating 110
 creating smart groups 111
 deleting 112
 editing 112
 removing computers 111
 information items 366
 new 103
 rearranging columns 104
 removing columns 104
 saving 104
 searching in 109
 single-computer view 105
 smart groups 367
 sorting 113
status bar 366
tabs 104
toolbar 366
Bus Speed (information item) 539
- C**
- Can Manage All Devices (information item) 572
Cancel Search (menu command) 517
Cascade (menu command) 349
 in Absolute Remote 626
Case-sensitive (information item) 548
categories, explained 367
category bar 437
certificates *see SSL certificates*
Change Action Schedule (menu command) 433
Change Administrator Password (menu command)
 275
Change Agent Client Info Settings (information item)
 574
Change Agent Custom Field Settings (information item)
 574
Change Agent General Settings (information item)
 574
Change Agent Server Settings (information item) 574
Change Command History Options (information item)
 573
Change Computer Tracking (information item) 573
Change Mobile Device Tracking (information item)
 574
Change Operating State (menu command) 296
Change Roaming Options Action (dialog) 410
Change Server Registration (menu command) 347
Change Services Operation State (menu command)
 303
Checked Date (information item) 548
Clear Passcode (dialog) 337
Client Info Locked (information item) 536
Client Information (information item category) 536
Client Information (information item) 536
client information fields 93
 configuring local access 96
 editing 93
 renaming 95
 viewing 95
Close (menu command) 266
 in Absolute Remote 621
Close Install Notification After (information item) 577
Close Tab (menu command) 266
collecting information *see information, gathering*
Column sidebar
 browser windows 367
columns
 adding to browser windows 104
 arranging 104
 removing 104
 resizing 104
 searching in 109
Command (menu), in Absolute Remote 625
Command Description (information item) 570
Command Error Info (information item) 571
command history 528
Command History (information item category) 571
Command History Status (information item) 571
Command Name (information item) 570
Command Options (dialog) 285
Command Options (menu command) 332
Command Queue (information item category) 571
Command Result Error (information item) 571
Command Status (information item) 571
Command Templates (menu command) 360
Command Templates (window) 360

command windows, toolbar 284
commands
 devices involved 4
 information items 570–571
 log *see command history*
Commands (information item category) 570–571
Commands (information item subcategory) 570
Commands (menu command) 359
Commands (menu) 283–341
Commands (window) 527–533
 columns 528
 context menu 528
 information items 528
 smart groups 528
 toolbar 527
Compliance Check Finish Date (information item) 588
Compliance Check Start Date (information item) 588
Compliance Count (information item) 589
Compliance Report (window) 378–384
 columns 379
 context menu 380
 information items 379
 information panel 379
 smart groups 379
Compliance Report Date (information item) 588
Compliance Report Logged-In User (information item)
 588
compliance reports 80
Compliance Reports (information item category) 587–
 589
Compliance Reports (menu command) 355
Compliance Reports (window) 355
 toolbar 378
Compliance Score (information item) 588
Compliant (information item) 588
Compressed (information item) 548
Computer Age (information item) 544
Computer Boot Time (information item) 544
Computer Express Service Tag (Dell) (information
 item) 546
Computer Group (information item) 585
computer groups
 adding and removing computers 231
 assigning distribution points 228, 230
 assigning software packages 232, 233
 duplicating 228, 229
 editing 231
 explained 202
 removing 232
 setting up 227
Computer Groups (information item category) 585
Computer Is Behind NAT (information item) 555
Computer Is Tracked (information item) 537
Computer Manufacturer (information item) 546
Computer Model (information item) 546
Computer Name (information item) 553, 585
Computer Online (Icon) (information item) 535
Computer Online (information item) 535
Computer Production Date (information item) 544
Computer Production Factory (information item) 544
Computer Serial Number (information item) 544
Computer Service Tag (information item) 546
Computer Summary (information item category) 588
Computer Tracking (information item category) 569
Computer Tracking (menu command) 374
Computer Tracking Info Updated (information item)
 558
Computer Type (information item) 543
Computer Uptime (information item) 544
Computer Version (information item) 546
Computer Warranty End (information item) 545
Computer Warranty Info (information item) 545
computers
 adding to appointment groups
 automatically 59
 manually 58
 appointing administrators 57
 backing up 125
 controlling 115–139
 executing applications 131
 executing files
 from admin computer 129
 local files 132
 executing scripts 130
 installing
 Mac OS X 237
 Windows 241
 putting to sleep 117
 remotely controlling 122
 restarting 117
 screen sharing 122
 shutting down 117
 single-computer information 105
 tracking 125
 viewing appointed administrators 62
 waking up 118
Computers (menu command) 350
Computers (window) 350
Configuration Profile (dialog) 400
configuration profiles
 Active Directory data in 145
 conflicting policies 152
 importing 146
 installing 146
 automatically 149
 manually 147
 optionally 150
 removing
 automatically 151
 manually 148
 variables in 143
Configuration Type (information item) 560
Configure Columns (menu command) 282
Connect Timeout (information item) 537
Connection (menu) 620
Connection Status (information item) 585
Continue Installation After Failure (information item)
 575
Control Remote Computer (menu command) 625
controlling
 computers 115–139
 Time Machine 125
Copy (menu command) 273
 Agent Deployment Center 519
 browser windows 372
 Commands window 529
 Compliance Report window 380
Copy "" (menu command)
 Agent Deployment Center 520
 browser windows 372
 Commands window 529
 Compliance Report window 380
Copy File/Folder (menu command) 318
copying files 190
Cores per Processor (information item) 539
CPU Information (information item category) 538
Create Folder (menu command) 322
Create Placeholder Computer Records (menu com-
 mand) 346
Create Shortcut (menu command) 321

-
- Creation Date (information item) 547
 Creation Time (information item) 571
 CSV, export format 268
 Current Load (information item) 580
 Current User Account (information item) 553
 Current User Is Admin (information item) 553
 Current User Name (information item) 553
 Custom Agent Name (information item) 536
 Custom Fields (information item category)
 for desktop devices 537
 for mobile devices 605
 Custom Info Items Updated (information item) 558
 custom information
 custom information fields 81
 custom information *see also client information fields*
 custom information fields
 assigning 87
 defining 82
 deleting 85
 editing 85
 editing manual fields 89
 exporting 66, 92
 importing 66, 92
 importing data 90, 269, 271
 mirroring 86
 unassigning 88
 using 88
 Custom Zone (dialog) 512
 Cut (menu command) 273
- D**
- DameWare Access (information item) 556
 DameWare, remote control with 122
 Darwin Version (information item) 555
 databases
 backup 100
 exporting to 98
 maintenance 100
 Date & Time (information item) 543
 Daylight-Saving Time (information item) 555
 Default (information item) 562
 Defender Auto Scan Enabled (information item) 555
 Defender Definition Version (information item) 555
 Defender Enabled (information item) 555
 Defender Engine Version (information item) 555
 Defender Installed (information item) 555
 Defender Real-Time Protection (information item) 555
 Deferred Until (information item) 581
 Delete (menu command) 274
 Delete Application (menu command) 423
 Delete File (dialog) 323
 Delete File/Folder (menu command) 323
 Delete Profile (menu command) 423
 Delete Prohibited Apps (information item) 582
 deleting files 192
 deleting information 102
 demo of Absolute Manage 17
 Demote to Unmanaged Device Action (dialog) 413
 Deploy Agents (information item) 572
 Deployment Center
 preferences 277
 Deployment Result (information item) 586
 Deployment Result Message (information item) 586
 Depth (information item) 552
 Details (menu command) 281
 Device Information (information item category) 590
 Device Name (information item) 560
 Device Tracking (information item category) 603
 Device User Information (information item category)
 598
 DHCP Server Address (information item) 560
- Disk Encryption Algorithm (information item) 556
 Disk Encryption Key Size (information item) 556
 Disk Encryption Product (information item) 555
 Disk Encryption Status (information item) 556
 Disk Encryption Version (information item) 555
 Disk Image (dialog) 467
 Disk Image Distribution Point (information item) 581
 Disk Image File (information item) 581
 Disk Image Name (information item) 580
 Disk Image Size (information item) 580
 Disk Image Upload Status (information item) 581
 disk images
 creating Mac OS X images 237
 creating Windows images
 using Absolute PXE 242
 using FOG 244
 reusing Mac OS X images 241
 Disk Images (information item category) 580
 Disk Sleep Timer (information item) 542
 Display All Records (menu command) 282
 Display Count (information item) 546
 Display Installation Progress (information item) 577
 Display Is Built-in (information item) 552
 Display Manufacture Date (information item) 552
 Display Model ID (information item) 552
 Display Online (information item) 552
 Display Product Name (information item) 552
 Display Reduces Brightness (information item) 542
 Display Serial Number (information item) 552
 Display Serial Number (internal) (information item)
 552
 Display Sleep Timer (information item) 542
 Display Sleep Uses Dim (information item) 542
 Display Type (information item) 552
 Display Vendor (information item) 552
 displaying information 103
 Displays (information item category) 552
 distributing iOS software *see software, installing*
 Distribution Point (dialog) 465
 Distribution Point Certificate Fingerprint (information item) 580
 Distribution Point Name (information item) 579
 Distribution Point OS Platform (information item) 580
 Distribution Point Selection (information item) 576
 Distribution Point Unique ID (information item) 580
 distribution points
 assigning to computer groups 228, 230
 considerations for designating 203
 editing 206
 explained 201
 master server explained 203
 mirror server explained 203
 removing 208
 setting up 202
 switching the master server 206
 updating 43
- Distribution Points (information item category) 579
 DNS Name (information item) 585
 DNS Servers (information item) 560
 DNS Suffix (information item) 561
 Don't Install on Slow Network (information item) 576
 Don't Limit Color Depth (menu command) 625
 DOS batch files, executing on administered computers 130
 Double Size (menu command) 624
 Download Bandwidth (information item) 580
 Drive Letter (information item) 547
 Driver Version (information item) 562
 Duplicate Action (menu command) 414, 431
 Duplicate Application Package (menu command) 398
 Duplicate Custom Information Field (menu command) 493

Duplicate Media File (menu command) 404
Duplicate Mobile Application Package (menu command) 428
Duplicate Payload (menu command) 463
Duplicate Software Package (menu command) 461

E

EAS Allow Bluetooth (information item) 612
EAS Allow Browser (information item) 612
EAS Allow Camera (information item) 612
EAS Allow Consumer E-mail (information item) 612
EAS Allow Desktop Sync (information item) 612
EAS Allow External Device Management (information item) 612
EAS Allow HTML E-mail (information item) 612
EAS Allow Internet Sharing (information item) 612
EAS Allow IrDA (information item) 612
EAS Allow Mobile OTA Update (information item) 612
EAS Allow Non-Provisionable Devices (information item) 612
EAS Allow POP/IMAP E-mail (information item) 612
EAS Allow Remote Desktop (information item) 613
EAS Allow S/MIME Encryption Algorithm Negotiation (information item) 613
EAS Allow S/MIME Software Certificates (information item) 613
EAS Allow Simple Device Password (information item) 613
EAS Allow Storage Card (information item) 613
EAS Allow Text Messaging (information item) 613
EAS Allow Unsigned Installation Packages (information item) 613
EAS Allow WiFi (information item) 613
EAS Allowed Applications (information item) 613
EAS Alphanumeric Device Password Required (information item) 613
EAS Attachments Enabled (information item) 613
EAS Blocked Applications (information item) 615
EAS Device Encryption Enabled (information item) 613
EAS Device Password Enabled (information item) 613
EAS Device Password Expiration (information item) 613
EAS Device Password History (information item) 614
EAS Device Policy Refresh Interval (information item) 614
EAS IRM Enabled (information item) 614
EAS Is Default Policy (information item) 614
EAS Maximum Attachment Size (information item) 614
EAS Maximum Calendar Age Filter (information item) 614
EAS Maximum Device Password Failed Attempts (information item) 614
EAS Maximum E-mail Age Filter (information item) 614
EAS Maximum E-mail Body Truncation Size (information item) 614
EAS Maximum E-mail HTML Body Truncation Size (information item) 614
EAS Maximum Inactivity Before Device Lock (information item) 614
EAS Minimum Device Password Complex Characters (information item) 614
EAS Minimum Device Password Length (information item) 614
EAS Mobile OTA Update Mode (information item) 614
EAS Password Recovery Enabled (information item) 615
EAS Policies (information item category) 611
EAS Policy Creation Date (information item) 613
EAS Policy Modification Date (information item) 615
EAS Policy Name (information item) 615

EAS Require Device Encryption (information item) 615
EAS Require Encrypted S/MIME Messages (information item) 615
EAS Require Encryption S/MIME Algorithm (information item) 615
EAS Require Manual Sync When Roaming (information item) 615
EAS Require Signed S/MIME Messages (information item) 615
EAS Require Storage Card Encryption (information item) 615
EAS UNC Access Enabled (information item) 615
EAS WSS Access Enabled (information item) 615
Edit (menu) 273–280
 in Absolute Remote 621
Edit Action (menu command) 416, 432
Edit Administrator (menu command) 494
Edit Administrator Group (menu command) 494
Edit Appointment Group (menu command) 494
Edit Command (menu command) 333, 532
Edit Configuration Profile (menu command) 416, 429
Edit Custom Field (menu command) 362
Edit Custom Information Field (menu command) 494
Edit Custom Zone (menu command) 516
Edit Disk Image (menu command) 494
Edit Distribution Point (menu command) 494
Edit Group (menu command) 416
Edit iOS Provisioning Profile (menu command) 416
Edit Item (menu command) 494
Edit License Specification (menu command) 494
Edit Media File (menu command) 416, 431
Edit Mobile Application Package (menu command) 416, 428
Edit Payload (menu command) 494
Edit Policy (menu command) 416
Edit Smart Group (menu command) 370, 384, 494, 518, 531
Edit Software Package (menu command) 494
Edit Windows Registry (menu command) 306
Enable Computer Tracking Screenshots (information item) 573
Enable DNS for WINS Resolution (information item) 561
Enable LMHOST Lookup (information item) 561
enrolling mobile devices 39
Enter Custom Field Data (menu command) 373
 Mobile Devices window 424
Enter Custom Fields Data (information item) 573
environment variables 137
 for files 137
 for the registry 138
erasing mobile devices 143
Error Count (information item) 589
Exchange server, configuring 28
Executable Name (information item) 579
Executable Options (information item) 575, 576
Executable Payload (information item) 575
Executable Size (information item) 575
Executable Source (information item) 579
Execute Command (menu command) 332
Execute Command Now (menu command) 333, 532
Execute Macintosh File (menu command) 309
Execute Script (menu command) 307
Execute Windows File (menu command) 312
executing
 applications 131
 files on administered computers
 from admin computer 129
 local files 132
 scripts 130
Exit (menu command) 272

-
- Export (menu command) 268
 Export Groups (menu command) 269
 Export Selected Fields (menu command) 493
 exporting
 custom information fields 66, 92
 export formats 268
 groups 269
 HTML 98, 268
 information 97
 ODBC 98
 smart groups 269
 text 98
 to databases 98
 XML 98, 268
- F**
- Failure Count (information item) 589
 Fast User Switching Enabled (information item) 556
 Favorite Commands (submenu)
 browser windows 371, 380, 529
 Server Center 443
 Favorites (submenu) 284
 configuring 360
 FDCC *see USGCB*
 feature overview 2
 File (menu) 265–272
 File Access Date (information item) 567
 File Architecture (information item) 567
 File Backup Date (information item) 567
 File Build Number (information item) 567
 File Bundle Identifier (information item) 567
 File Count (information item) 559
 File Creation Date (information item) 567
 File Creator (information item) 567
 File Found (information item) 568
 File Modification Date (information item) 567
 File Name (information item) 566
 File Path (information item) 566
 File Record Modification Date (information item) 568
 file servers
 see also distribution points
 File Size (information item) 567
 File Version (information item) 567
 File Version String (information item) 567
 files
 copying 190
 creating aliases 195
 creating shortcuts 195
 deleting 192
 executing on administered computers
 from admin computer 129
 local files 132
 gathering information 76
 moving 190
 opening 193
 renaming 192
 searching for 76
 transferring to administered computers 197
 viewing 193
 working with 190–199
 Files (information item category) 566
 Files (menu command) 350
 Files (window) 350
 files *see also media*
 filtering browser windows 109
 Find File (menu command) 323
 fingerprints of SSL certificates, displaying 18
 Finish Time (information item) 571
 Firewall Enabled (information item) 556
 FireWire Capacity (information item) 550
 FireWire Device Count (information item) 546
 FireWire Devices (information item category) 550
 FireWire Firmware Revision (information item) 550
 FireWire Manufacturer (information item) 550
 FireWire Model (information item) 550
 FireWire Model ID (information item) 550
 FireWire Software Version (information item) 550
 FireWire Speed (information item) 550
 FireWire Vendor ID (information item) 550
 First Status Timestamp (information item) 584
 FOG Host Name (information item) 616
 FOG Image Created By (information item) 616
 FOG Image Creation Date (information item) 616
 FOG Image Name (information item) 616
 FOG Image Size (information item) 616
 FOG Reinstallation Tasks (information item category)
 616
 FOG Task Creation Date (information item) 616
 FOG Task Data Copied (information item) 616
 FOG Task Data Total (information item) 616
 FOG Task Name (information item) 616
 FOG Task Percent Complete (information item) 616
 FOG Task State (information item) 616
 FOG Task Time Elapsed (information item) 617
 FOG Task Type (information item) 616
 Folder Count (information item) 547
 folders
 creating 196
 Font Count (information item) 558
 Font Info Updated (information item) 557
 Font Name (information item) 561
 Font Type (information item) 561
 Fonts (information item category) 561
 Fonts (menu command) 350
 Fonts (window) 350
 fonts, gathering information on 73
 Free Space % (information item) 547
 Free Space (information item) 547
 Freeze Device Action (dialog) 412
 FTP Access (information item) 556
 Full Duplex (information item) 560
 Full Registry Path (information item) 569
 Full-Screen Mode (menu command) 624
- G**
- Gather Compliance Report (menu command) 331
 Gather Installed Software (dialog) 330
 Gather Installed Software (menu command) 329
 Gather Inventory (dialog) 329
 Gather Inventory Information (menu command) 328
 Gather Process Information (menu command) 328
 gathering information *see information, gathering*
 General (information item category) 534
 geolocation *see geotracking*
 geotracking 182
 displaying information 188
 enabling on mobile devices 185
 resetting passphrases 185
 setting passphrases 183
 Get Clipboard (menu command) 621
 Get Device Geolocation (menu command) 341
 GMT Delta (information item) 555
 Google Play Application (dialog) 397
 Google Play *see Android Market*
 Group ID (information item) 565
 Group Name (information item) 566
 groups
 adding computers 111
 as command targets 110
 creating 110
 deleting 112
 editing 112

-
- groups*
 exporting 269
 importing 269
 removing computers 111
 saving 112
- H**
- Half Size (menu command) 624
 Hardware (information item) 560
 Hardware Information (information item category) 538–553
 Has Custom Icon (information item) 568
 Has Installation Condition (information item) 578
 Heartbeat Interval
 explained 290
 information item 535
 Help (menu) 363–364
 in Absolute Remote 626
 Help Topics (menu command) 363
 Hibernation Mode (information item) 542
 Historic License Status (information item) 584
 history report 478
 history summary report 478
 Host (information item) 561
 HTML
 export format 268
 exporting 98, 268
- I**
- Identification Type (information item) 564
 Idle Time (information item) 553
 Ignore Devices (menu command) 425
 Import Custom Field Data (menu command)
 Mobile Devices window 424
 Import Custom Field Data for Desktop Devices (menu command) 269
 Import Custom Field Data for Mobile Devices (menu command) 271
 Import Fields (menu command) 494
 Import Groups (menu command) 269
 Import Zones File (menu command) 518
 importing
 custom information field data 90
 custom information fields 66, 92
 importing groups 269
 importing text information 269, 271
 Included in Patch Management (information item) 537
 information
 client information fields 93
 compliance reports 80
 custom information 81
 see also client information fields
 deleting 102
 displaying 103
 displaying via URL 106
 exporting 97
 files 76
 fonts 73
 gathering 69–114
 automatically 71
 manually 73
 installed software 75
 managing 69–114
 manually edited information 93
 on single computers 105
 printers 73
 processes 74
 registry 78
 startup items 73
 storing 97
 USGCB SCAP reports 80
 information items
 adding to browser windows 104
 Administration 572–575
 Agent Deployment Center 585–586
 Agent Information 534–537
 Commands 570–571
 custom information fields 81
 defined 70
 Hardware Information 538–553
 License Monitoring 581–585
 searching in 109
 Server Center 571–585
 Software Distribution 575–581
 Software Information 553–570
 Information Items (menu command) 362
 Information Items (window) 362
 information panel 379
 Inst. Software Company (information item) 563
 Inst. Software File Architecture (information item) 563
 Inst. Software Info (information item) 563
 Inst. Software Installation Date (information item) 563
 Inst. Software Name (information item) 563
 Inst. Software Product ID (information item) 564
 Inst. Software Size (information item) 563
 Inst. Software Stat Company (information item) 586
 Inst. Software Stat Count (information item) 586
 Inst. Software Stat Identification Type (information item) 587
 Inst. Software Stat Info (information item) 586
 Inst. Software Stat Installer Receipt ID (information item) 587
 Inst. Software Stat Is Hotfix (information item) 587
 Inst. Software Stat Name (information item) 586
 Inst. Software Stat Size (information item) 586
 Inst. Software Stat Uninstallable (information item) 586
 Inst. Software Version Number (information item) 563
 Inst. Software Version String (information item) 563
 Install Agent (menu command) 520
 Install Application (dialog) 336
 Install Application (menu command) 336
 Install At (information item) 576
 Install Configuration Profile (dialog) 334
 Install Configuration Profile (menu command) 334
 Install Count (information item) 585
 Install Location (information item) 564
 Install Provisioning Profile (dialog) 335
 Install Provisioning Profile (menu command) 335
 Install Selected Software Packages (menu command) 496
 Install Software Packages (menu command) 314
 Install Time End (information item) 576
 Install Time Start (information item) 576
 Install When No User Is Logged In (information item) 576
 Install When User Is Logged In (information item) 576
 Installation Context (information item) 576
 Installation Context User (information item) 576
 Installation Deadline (information item) 577
 Installation Result Error (information item) 581
 Installation Status (information item category) 581
 Installed Agent Build Number (information item) 586
 Installed Agent Version (information item) 586
 Installed Application Statistics (information item category) 602
 Installed Applications (information item category) 599
 Installed Certificate Statistics (information item category) 603

-
- Installed Certificates (information item category) 601
Installed Configuration Profile Statistics (information item category) 602
Installed Configuration Profiles (information item category) 600
Installed Provisioning Profile Statistics (information item category) 603
Installed Provisioning Profiles (information item category) 601
installed software
 gathering information 75
Installed Software (information item category) 563
Installed Software (menu command) 351
Installed Software (window) 351
Installed Software Count (information item) 559
Installed Software Info Updated (information item) 558
Installed Software Statistics (information item category) 586–587
installer packages, creating 200
Installer Receipt ID (information item) 564
installing
 Absolute Manage 11–44
 preparation 11
 Absolute Manage Admin 15
 Absolute Manage Agent 29
 automatically 35
 manually on Mac OS X 30
 manually on Windows 30
 using the Agent Deployment Center 33
 Absolute Manage Server 14
 choosing a computer 14
 initial configuration 16
 configuration profiles 146
 MDM 24
 provisioning profiles 153
 software 200–247
 ad hoc 233
 App Store apps 165
 configuring agents 202
 manually 200
 on mobile devices 157
 overview 201
 performing installations 232
 preparing iOS devices 155
 setup 202
 Windows reinstallation support 20
 see also *reinstalling*
Interval (information item) 570
Interval Unit (information item) 570
introduction to Absolute Manage 2–10
Inventory Push Interval (information item) 536
Inventory Received (information item) 557
Inventory Server (information item) 586
Inventory Server Properties (dialog) 290, 523, 525
inventory servers explained 55
Inventory Updated (information item) 557
iOS
 AbsoluteApps for 630
 iOS App Store Application (dialog) 394
 iOS devices
 disabling software 164
 enrolling 39
 geotracking 182
 installing App Store apps 165
 installing provisioning profiles 153
 installing the Agent 39
 MDM access rights 62
 policies 176
 preparing for software installation 155
 preparing software 158
 re-enrolling 64
 removing software 164
 updating MDM privileges 64
iOS devices *see also* *mobile devices*
iOS Inst. Prov. Profile Count (information item) 603
iOS Inst. Prov. Profile Max Expiry Date (information item) 603
iOS Inst. Prov. Profile Min Expiry Date (information item) 603
iOS Inst. Prov. Profile Name (information item) 603
iOS Inst. Prov. Profile UUID (information item) 603
iOS Installed Provisioning Profile Expiry Date (information item) 601
iOS Installed Provisioning Profile Name (information item) 601
iOS Installed Provisioning Profile UUID (information item) 601
iOS MDM *see* *MDM*
iOS policies *see* *policies*
iOS Provisioning Profile Definitions (information item category) 609
iOS Provisioning Profile Expiry Date (information item) 609
iOS Provisioning Profile Name (information item) 609
iOS Provisioning Profile UUID (information item) 609
IP Address (information item) 585
IP Range End (information item) 580
IP Range Start (information item) 580
Is AD User (information item) 574
Is Alias (information item) 568
Is Application (information item) 568
Is Classic App (information item) 568
Is Executable (information item) 579
Is File (information item) 568
Is Hard Link (information item) 568
Is Hotfix (information item) 564
Is Invisible (information item) 568
Is Locked (information item) 568
Is Mac OS Software Update (information item) 578
Is Master Distribution Point (information item) 580
Is Metapackage (information item) 575
Is Open (information item) 568
Is Package (information item) 568
Is Repeating Command (information item) 570
Is Scriptable (information item) 568
Is Smart Policy (information item) 611
Is Stationery (information item) 568
Is Superadmin (information item) 572
Is Symbolic Link (information item) 568
Is Windows Software Update (information item) 578
Issue Clear Passcode (menu command) 337
Issue Device Lock (menu command) 336
Issue Remote Erase (menu command) 338
Item Summary (information item category) 588
- J**
- Journalized (information item) 548
- K**
- Keep Package File After Installation (information item) 576
keys in the registry, working with 136
- L**
- laptops
 tracking 125
Last Heartbeat (information item) 535
Last Launch Date (information item) 583, 585
Last User Account (information item) 553

Last User Name (information item) 553
Latest Status Timestamp (information item) 584
Launch Date (information item) 566
License History (information item category) 584
License History Summary (information item category) 584
License Monitoring (information item category) 581–585
License Monitoring Center
 checking licenses 259
 computer groups 256
 configuring agents 256
 configuring servers 258
 license specifications 249
 maintenance agreement information 254
 purchase information 254
 reports 260
license monitoring servers
 assigning to agents 57
License Specification (information item category) 581
License Specification Name (information item) 581
license specifications, setting up 249
License Status (information item category) 583
License Status (information item) 583
License Status Log Date (information item) 583
License Status per Agent (information item category) 584
licenses
 checking 259
 maintenance agreement information 254
 monitoring 248–263
 overview 248
 purchase information 254
Licenses Owned (information item) 581
Licenses Type (information item) 582
Limit Color to 16 Bit (menu command) 625
Limit Color to 8 Bit (menu command) 625
Link Status (information item) 560
LM Server Address (information item) 536
LM Server Check Interval (information item) 537
LM Server Port (information item) 536
LM Server Unique ID (information item) 537
Local OS Updating Disabled (information item) 537
Locate My Mobile Device *see geotracking*
locating mobile devices *see geotracking*
Location (information item) 561
Lock Device (dialog) 336
Locked by Hardware (information item) 548
Locked by Software (information item) 548
locking mobile devices 141
log *see command history*
logging in 53
logging out 53
Login (dialog) 274

M

Mac OS X Screen Sharing, remote control with 122
Mac OS X patch management 235
Main Display (information item) 552
Mainboard Asset Tag (information item) 545
Mainboard Manufacturer (information item) 545
Mainboard Product Name (information item) 545
Mainboard Serial Number (information item) 545
Mainboard Type (information item) 545
Mainboard Version (information item) 545
maintaining
 databases 100
 server database 499
maintenance agreement information, recording 254
Make Group from Selected Computers (menu command) 372

Manage Mobile Devices (information item) 574
master distribution points
 explained 203
 switching 206
Max. Achieved Score (information item) 588
Max. Downloads (information item) 580
Max. Install Count (information item) 584
Max. Item Score (information item) 588
Max. Running Count (information item) 584
Max. Score (information item) 589
Maximum Battery Capacity (information item) 540
Maximum OS (information item) 577
MDM
 iOS access rights 62
MDM Server, basic function 3
MDM, installing support for 24
media
 distributing 169
 importing 170
 making available to mobile devices 173
 specifying in policies 182
 supported file types 169
Media Category (information item) 609
Media Description (information item) 609
Media File Can Be E-Mailed (information item) 609
Media File Can Be Printed (information item) 609
Media File Can Leave AbsoluteSafe (information item) 609
Media File Is WiFi-Only (information item) 609
Media File Last Modified (information item) 609
Media File Name (information item) 610
Media File Size (information item) 609
media files *see media*
Media Name (information item) 609
Media Type (information item) 609
Media Unique Identifier (information item) 610
Memory Module Count (information item) 546
Memory Size (information item) 547
Memory Slot Name (information item) 547
Memory Slots (information item category) 547
Memory Slots (information item) 546
Memory Speed (information item) 547
Memory Type (information item) 547
messages, sending 115
 to mobile devices 140
Metapackage (dialog) 453
metapackages
 conflicting settings 220
 editing 227
 removing 227
 setting up 220
Meter App Usage (information item) 582
Microsoft SMS 97
Min. Achieved Score (information item) 588
Min. Install Count (information item) 584
Min. Running Count (information item) 584
Minimum OS (information item) 577
Mirror (information item) 552
mirror distribution points, explained 203
mirroring custom information fields 86
Mirroring From (information item) 580
Mirroring Until (information item) 580
Missing Operating System Patches (menu command) 353
Missing Operating System Patches (window) 353
Missing OS Patches (information item category) 564
Missing OS Patches Count (information item) 559
Missing OS Patches Statistics (information item category) 587
Missing Patch Action (information item) 564
Missing Patch Install Deadline (information item) 564
Missing Patch Is Beta (information item) 564

-
- Missing Patch Is Mandatory (information item) 564
Missing Patch Language (information item) 565
Missing Patch Name (information item) 564
Missing Patch Release Date (information item) 564
Missing Patch Stat Count (information item) 587
Missing Patch Stat Deadline (information item) 587
Missing Patch Stat Language (information item) 587
Missing Patch Stat Name (information item) 587
Missing Patch Stat Release Date (information item) 587
Missing Patch Stat Superseded by Package (information item) 587
Missing Patch Stat Version (information item) 587
Missing Patch Superseded by Package (information item) 565
Missing Patch Version (information item) 564
Missing Patches Info Updated (information item) 558
missing software report 478
Mobile Action Assignment Options (dialog) 433
Mobile Action Description (information item) 610
Mobile Action Device Execution Time (information item) 610
Mobile Action Name (information item) 610
Mobile Action Policy Initial Delay (information item) 610
Mobile Action Policy Repeat Count (information item) 610
Mobile Action Policy Repeat Interval (information item) 611
Mobile Action Supported Platforms (information item) 610
Mobile Action Type (information item) 610
Mobile Action Unique Identifier (information item) 610
Mobile Actions (information item category) 610
Mobile App Assignment Rule (information item) 606
Mobile App Build Number (information item) 605
Mobile App Bundle Identifier (information item) 606
Mobile App Is Universal (information item) 605
Mobile App Long Description (information item) 606
Mobile App Min OS Version (information item) 605
Mobile App Name (information item) 605
Mobile App OS Platform (information item) 605
Mobile App Prevent Data Backup (information item) 606
Mobile App Remove When MDM Is Removed (information item) 606
Mobile App Short Description (information item) 606
Mobile App Size (information item) 605
Mobile App Supported Devices (information item) 605
Mobile App Update Description (information item) 606
Mobile App Version (information item) 605
Mobile Application (dialog) 393
Mobile Application Packages (information item category) 605
Mobile Configuration Profile Definitions (information item category) 608
Mobile Device AbsoluteApps Build Number (information item) 596
Mobile Device AbsoluteApps Supports Tracking (information item) 596
Mobile Device AbsoluteApps Version (information item) 596
Mobile Device Access State (information item) 597
Mobile Device Access State Reason (information item) 597
Mobile Device Age (information item) 592
Mobile Device Available Capacity (information item) 591
Mobile Device Battery Level (information item) 593
Mobile Device Bluetooth MAC Address (information item) 591
Mobile Device Board (information item) 594
Mobile Device Brand (information item) 594
Mobile Device Capacity (information item) 591
Mobile Device Carrier Settings Version (information item) 594
Mobile Device Cell IP Address (information item) 592
Mobile Device Cellular Technology (information item) 594
Mobile Device Command Error (information item) 611
Mobile Device Command Error Info (information item) 611
Mobile Device Command Finish Time (information item) 611
Mobile Device Command Status (information item) 611
Mobile Device Command Time Issued (information item) 611
Mobile Device Command Type (information item) 611
Mobile Device Commands (information item category) 611
Mobile Device CPU Name (information item) 594
Mobile Device CPU Speed (information item) 595
Mobile Device Current Carrier Network (information item) 594
Mobile Device Current Mobile Country Code (information item) 594
Mobile Device Current Mobile Network Code (information item) 594
Mobile Device Data Roaming Enabled (information item) 593
Mobile Device Display Resolution (information item) 592
Mobile Device Enable Outbound SMS (information item) 597
Mobile Device GPS Capable (information item) 591
Mobile Device GUID (information item) 596
Mobile Device Hardware Encryption (information item) 593
Mobile Device Home Mobile Country Code (information item) 594
Mobile Device Home Mobile Network Code (information item) 594
Mobile Device Home Network (information item) 594
Mobile Device Identifier (UDID) (information item) 591
Mobile Device Identity (information item) 597
Mobile Device IMEI/MEID (information item) 591
Mobile Device IMEISV (information item) 595
Mobile Device Info (information item) 595
Mobile Device Information (information item category) 589–611
Mobile Device Inst. App Bundle Identifier (information item) 602
Mobile Device Inst. App Count (information item) 602
Mobile Device Inst. App Name (information item) 602
Mobile Device Inst. Certificate Count (information item) 603
Mobile Device Inst. Certificate Identity Count (information item) 603
Mobile Device Inst. Certificate Name (information item) 603
Mobile Device Inst. Profile Count (information item) 602
Mobile Device Inst. Profile Description (information item) 602
Mobile Device Inst. Profile Identifier (information item) 603
Mobile Device Inst. Profile Managed Count (information item) 602
Mobile Device Inst. Profile Name (information item) 602

-
- Mobile Device Inst. Profile Organization (information item) 603
Mobile Device Inst. Profile UUID (information item) 603
Mobile Device Installed App Build Number (information item) 600
Mobile Device Installed App Bundle Identifier (information item) 600
Mobile Device Installed App Data Directory (information item) 600
Mobile Device Installed App Data Size (information item) 600
Mobile Device Installed App Name (information item) 599
Mobile Device Installed App Size (information item) 600
Mobile Device Installed App Version (information item) 600
Mobile Device Installed App Version String (information item) 600
Mobile Device Installed Certificate Is Identity (information item) 602
Mobile Device Installed Certificate Name (information item) 602
Mobile Device Installed Certificates Last Change (information item) 598
Mobile Device Installed Configuration Profiles Last Change (information item) 598
Mobile Device Installed Profile Allow Removal (information item) 601
Mobile Device Installed Profile Description (information item) 600
Mobile Device Installed Profile Encrypted (information item) 601
Mobile Device Installed Profile Identifier (information item) 601
Mobile Device Installed Profile Managed (information item) 601
Mobile Device Installed Profile Name (information item) 600
Mobile Device Installed Profile Organization (information item) 601
Mobile Device Installed Profile Type (information item) 601
Mobile Device Installed Profile UUID (information item) 601
Mobile Device Installed Profile Version (information item) 601
Mobile Device Installed Provisioning Profiles Last Change (information item) 598
Mobile Device Installed Software Last Change (information item) 598
Mobile Device Internal Storage Available (information item) 595
Mobile Device Internal Storage Total (information item) 595
Mobile Device Is Roaming (information item) 593
Mobile Device Jailbroken (information item) 593
Mobile Device Kernel Version (information item) 595
Mobile Device Last Contact (information item) 590
Mobile Device Last Device Wipe Requestor (information item) 597
Mobile Device Last Policy Update Time (information item) 597
Mobile Device Location Accuracy (information item) 604
Mobile Device Location Battery Level (information item) 605
Mobile Device Location Battery State (information item) 605
Mobile Device Location Cell IP Address (information item) 604
Mobile Device Location Latitude (information item) 604
Mobile Device Location Longitude (information item) 604
Mobile Device Location Public IP Address (information item) 604
Mobile Device Location WiFi IP Address (information item) 604
Mobile Device Location WiFi IP Address (v6) (information item) 604
Mobile Device Managed (information item) 593
Mobile Device Managed App Bound to MDM (information item) 600
Mobile Device Managed App Prevent Data Backup (information item) 600
Mobile Device Managed App Status (information item) 600
mobile device management *see MDM*
Mobile Device Manufacturer (information item) 595
Mobile Device MDM Profile Up-to-date (information item) 596
Mobile Device Model (information item) 590
Mobile Device Model Number (information item) 590
Mobile Device Modem Firmware Version (information item) 593
Mobile Device Name (information item) 590
Mobile Device Network Type (information item) 595
Mobile Device Number of Folders Synced (information item) 597
Mobile Device OS Language (information item) 596
Mobile Device OS Number (information item) 590
Mobile Device OS Version (information item) 590
Mobile Device Ownership (information item) 591
Mobile Device Passcode Compliant (information item) 593
Mobile Device Passcode Compliant with Profiles (information item) 593
Mobile Device Passcode Present (information item) 593
Mobile Device Phone Number (information item) 590
Mobile Device Policies (information item category) 611
mobile device policies *see policies*
Mobile Device Product Name (information item) 595
Mobile Device Production Date (information item) 591
Mobile Device Public IP Address (information item) 592
Mobile Device Public IP Address (v6) (information item) 592
Mobile Device Purchase Date (information item) 591
Mobile Device Record Creation Date (information item) 596
Mobile Device Remote Wipe Supported (information item) 597
Mobile Device SD Card 1 Available (information item) 595
Mobile Device SD Card 1 Total (information item) 595
Mobile Device SD Card 2 Available (information item) 596
Mobile Device SD Card 2 Total (information item) 596
Mobile Device Serial Number (information item) 590
Mobile Device SIM ICC Identifier (information item) 594
Mobile Device Status (information item) 593, 597
Mobile Device Status Note (information item) 597
Mobile Device Supports Persistence (information item) 593
Mobile Device System Cache Available (information item) 596
Mobile Device System Cache Total (information item) 596
Mobile Device System Memory Available (information item) 596

-
- Mobile Device System Memory Total (information item) 596
Mobile Device System Storage Available (information item) 596
Mobile Device System Storage Total (information item) 596
Mobile Device Tracking (dialog) 339
Mobile Device Tracking Accuracy (information item) 604
Mobile Device Tracking Enabled (information item) 604
Mobile Device Tracking Interval (information item) 604
Mobile Device Tracking Time (information item) 604
Mobile Device User City (information item) 599
Mobile Device User Company (information item) 599
Mobile Device User Country (information item) 599
Mobile Device User Department (information item) 599
Mobile Device User Display Name (information item) 598
Mobile Device User E-Mail (information item) 598
Mobile Device User Enrollment Domain (information item) 599
Mobile Device User Enrollment Username (information item) 599
Mobile Device User First Name (information item) 598
Mobile Device User Is Member Of (information item) 599
Mobile Device User Last Name (information item) 598
Mobile Device User Log-on Name (information item) 598
Mobile Device User Office (information item) 599
Mobile Device User Organizational Unit (information item) 599
Mobile Device User Organizational Unit Path (information item) 599
Mobile Device User Phone Number (information item) 598
Mobile Device User State (information item) 599
Mobile Device User Street (information item) 599
Mobile Device User ZIP Code (information item) 599
Mobile Device Voice Roaming Enabled (information item) 594
Mobile Device Warranty End (information item) 592
Mobile Device Warranty Info (information item) 592
Mobile Device WiFi IP Address (information item) 592
Mobile Device WiFi IP Address (v6) (information item) 592
Mobile Device WiFi MAC Address (information item) 591
Mobile Device WiFi Network (information item) 592
Mobile Device Wipe Ack Time (information item) 597
Mobile Device Wipe Request Time (information item) 597
Mobile Device Wipe Sent Time (information item) 597
mobile devices 630–638
 adding to appointment groups
 automatically 59
 manually 58
 administering 140–189
 appointing administrators 57
 configuration profiles with variables 143
 enabling geotracking 185
 enrolling 39
 erasing 143
 installing commercial apps 165
 installing configuration profiles 146
 installing provisioning profiles 153
 installing software 157
installing the Agent 39
locking and unlocking 141
making media available 173
making software available 161
sending messages 140
server contact interval 506
showing location 188
viewing appointed administrators 62
Mobile Devices (menu command) 358
Mobile Devices (window) 385–434
 columns 388
 information items 388
 sidebar context menu 391, 417
 smart groups 389
 toolbar 388
Mobile Media (information item category) 609
Mobile Platform Type (information item) 608
Mobile Profile Allow Removal (information item) 608
Mobile Profile Description (information item) 608
Mobile Profile Identifier (information item) 608
Mobile Profile Name (information item) 608
Mobile Profile Organization (information item) 608
Mobile Profile Type (information item) 608
Mobile Profile UUID (information item) 608
Mobile Profile Variables Used (information item) 608
Modification Date (information item) 547
Modify Computer Groups (information item) 573
Modify Custom Information Fields (information item) 573
Modify Disk Images (information item) 573
Modify Distribution Points (information item) 573
Modify License Specifications (information item) 573
Modify Mobile Actions (information item) 574
Modify Mobile Applications (information item) 574
Modify Mobile Configuration Profiles (information item) 574
Modify Mobile Device Policies (information item) 574
Modify Mobile Media (information item) 574
Modify Server Settings (information item) 573
Modify Software Packages (information item) 573
monitoring licenses, overview 248
Move File/Folder (menu command) 325
moving files 190
MS Remote Assistance, remote control with 122
MS Remote Desktop, remote control with 122
MTU (information item) 560
- ## N
- naming
 Android devices 188
 files 192
Network Adapter Count (information item) 558
Network Adapters (information item category) 560
New (menu command) 265
 in Absolute Remote 620
New Administrator (menu command) 481
New Administrator Group (menu command) 484
New Category (menu command) 369, 383
New Command History Smart Group from “” (menu command) 421
New Command Queue Smart Group from “” (menu command) 421
New Computer Appointment Group (menu command) 485
New Computer Group (menu command) 478
New Configuration Profile (menu command) 400, 429
New Connection (dialog) 620
New Custom Information Field (menu command) 489
New Custom Zone (menu command) 512
New Demote to Unmanaged Device Action (menu command) 413, 433

-
- New Disk Image (menu command) 467
 New Distribution Point (menu command) 464
 New Freeze Device Action (menu command) 412, 433
 New Google Play Application Package (menu command) 397, 428
 New Group
 Mobile Devices (menu command) 415
 New Group (menu command) 368
 New History Report (menu command) 478
 New History Summary Report (menu command) 478
 New In-house Application Package (menu command) 393
 New iOS App Store Application Package (menu command) 394, 428
 New License Specification (menu command) 470
 New License Status Report (menu command) 477
 New Media File (menu command) 403, 431
 New Metapackage (menu command) 453
 New Missing Mac OS Patches Smart Group (menu command) 353
 New Missing Mac OS Patches Statistics Smart Group (menu command) 354
 New Missing Microsoft Patches Smart Group (menu command) 353
 New Missing Software Packages Group (menu command) 469
 New Missing Software Report (menu command) 478
 New Missing Windows Patches Statistics Smart Group (menu command) 354
 New Mobile Application Package (menu command) 428
 New Mobile Devices Appointment Group (menu command) 486
 New Payload (menu command) 462
 New Policy (menu command) 415
 New Policy with Selected Devices (menu command) 421
 New Remove Configuration Profile Action (menu command) 413, 433
 New Send E-mail Action (menu command) 407, 432
 New Send Message Action (menu command) 432
 New Send Message to Device Action (menu command) 405
 New Send SMS (Text Message) Action (menu command) 409, 432
 New Set Roaming Options Action (menu command) 410, 433
 New Smart Administrator Group (menu command) 488
 New Smart Application Group from "" (menu command) 419
 New Smart Command History Group (menu command) 531
 New Smart Command History Group from "" (menu command) 530
 New Smart Command Queue Group (menu command) 530
 New Smart Command Queue Group from "" (menu command) 529
 New Smart Computer Appointment Group (menu command) 485
 New Smart Computer Group (menu command) 479
 New Smart Configuration Profiles Group from "" (menu command) 420
 New Smart Disk Image Group (menu command) 468
 New Smart Distribution Points Group (menu command) 466
 New Smart Group
 Actions (menu command) 414
 App Store Application Packages (menu command) 398
 Command History (menu command) 416
 Command Queue (menu command) 416
 Computers by Installed Software (menu command) 352
 Configuration Profiles (menu command) 401
 In-house Application Packages (menu command) 398
 Installed Application Statistics (menu command) 399
 Installed Applications (menu command) 398
 Installed Certificates (menu command) 402
 Installed Certificates Statistics (menu command) 402
 Installed Configuration Profiles (menu command) 401
 Installed Configuration Profiles Statistics (menu command) 401
 Installed iOS Provisioning Profiles (menu command) 399
 Installed iOS Provisioning Profiles Statistics (menu command) 399
 Installed Software (menu command) 352
 Installed Software Statistics (menu command) 352
 iOS Provisioning Profiles (menu command) 398
 Media Files (menu command) 405
 Mobile Devices (menu command) 416
 Mobile Devices by Installed Certificates (menu command) 402
 Mobile Devices by Installed Configuration Profiles (menu command) 402
 Mobile Devices by Installed iOS Provisioning Profiles (menu command) 399
 Mobile Devices by Installed Software (menu command) 399
 New Smart Group (menu command) 369, 517
 New Smart Group from "" (menu command)
 Agent Deployment Center 520
 browser windows 372
 New Smart Installation Status Group (menu command) 469
 New Smart License Specification Group (menu command) 476
 New Smart Media Files Group from "" (menu command) 420
 New Smart Mobile Device Group from "" (menu command) 419
 New Smart Mobile Devices Appointment Group (menu command) 487
 New Smart Payload Group (menu command) 464
 New Smart Policy
 Mobile Devices (menu command) 415
 Mobile Devices by Installed Applications (menu command) 415
 Mobile Devices by Installed Configuration Profiles (menu command) 415
 New Smart Policy from "" (menu command) 419
 New Smart Provisioning Profiles Group from "" (menu command) 420
 New Smart Report Details Group (menu command) 382
 New Smart Report Item Summary Group (menu command) 382
 New Smart Report Summary Group (menu command) 381
 New Smart Software Package Group (menu command) 461
 New Software Package (menu command) 443
 New Software Usage Report (menu command) 477
 New Tab (menu command) 265
 New Update Device Info Action (menu command) 411

Number of Launches (information item) 585

O

Object Count (information item) 547
Observe Remote Computer (menu command) 625
ODBC, exporting to 98
Only Use Distribution Point When Assigned (information item) 580
Open (menu command) 266
 in Absolute Remote 620
Open Directory integration 47
Open File (menu command) 325
Open in External Viewer (menu command) 377
opening files 193
Original Battery Capacity (information item) 540
Original Size (menu command) 624
OS Activated (information item) 554
OS Activation Grace Period (information item) 554
OS Build Number (information item) 554
OS Installation Date (information item) 554
OS Is Volume-Licensed (information item) 554
OS Language (information item) 554
OS Platform (information item) 553
OS Product ID (information item) 554
OS Serial Number (information item) 554
OS Service Pack (information item) 554
OS Update Utility Enabled (information item) 557
OS Version (information item) 554

P

Package Name (information item) 575
Packages (information item category) 575
Packages Root Path (information item) 580
Page Faults (information item) 566
Parent Process ID (information item) 566
Parent Process Name (information item) 566
passphrases
 resetting 185
 setting 183
passwords, changing 54
Paste (menu command) 273
Patch Action (information item) 578
Patch Can Be Uninstalled (information item) 578
Patch Install Deadline (information item) 578
Patch Is Beta (information item) 578
Patch Is Mandatory (information item) 578
Patch Language (information item) 578
patch management 235
Patch Release Date (information item) 578
Path (information item) 562
Payload Download Time (information item) 577
Payload Name (information item) 579
Payload Notes (information item) 579
Payload Size (information item) 579
Payload Unique ID (information item) 579
payloads
 editing 210
 removing 210
 setting up 209
PC Anywhere Access (information item) 556
PC Anywhere, remote control with 122
PCI Device Count (information item) 546
PCI Device ID (information item) 551
PCI Devices (information item category) 551
PCI Name (information item) 551
PCI Revision ID (information item) 552
PCI ROM Revision (information item) 551
PCI Slot (information item) 551
PCI Type (information item) 551
PCI Vendor ID (information item) 551
Personal File Sharing (information item) 556
Personal Web Sharing (information item) 556

Physical Cores (information item) 538
Physical Memory (information item) 543
Physical Processors (information item) 538
placeholder records
 creating 65
 deleting 66
 explained 65
Platform Architecture (information item) 577
PM Action (information item) 543
PM Inactivity Timer (information item) 543
PM Only When No User Logged In (information item) 543
PM Schedule Count (information item) 543
PM Schedule Name (information item) 543
PM Settings For (information item) 543
PM Time (information item) 543
PM Trigger (information item) 543
policies
 adding and removing mobile devices 178
 conflicting settings for configuration profiles 152
 creating 177
 explained 176
 specifying actions 179
 specifying applications 181
 specifying configuration profiles 181
 specifying media 182
Policy Name (information item) 611
Port (information item) 579
position of mobile devices 182
positions of mobile devices *see geotracking*
PostScript (information item) 562
Power Management (information item category) 541
power management schedules 118
 creating 118
Power Management Schedules (information item category) 543
Power Management Settings (menu command) 293
power usage reports 120
Power Usage Reports (menu command) 355
Power Usage Reports (window) 355
Power-on Avg/Day (information item) 541
Power-on Avg/Month (information item) 541
Power-on Avg/Week (information item) 541
Power-on Avg/Year (information item) 541
Power-on Last 30 Days (information item) 541
Power-on Last 365 Days (information item) 541
Power-on Last 7 Days (information item) 541
Power-on Tracking Start (information item) 542
Power-on Yesterday (information item) 541
PowerShell scripts, executing on administered computers 130
Primary Interface (information item) 560
Primary MAC Address (information item) 543
Print (menu command) 271
Print Preview (menu command) 271
Print Setup (menu command) 272
Printer Count (information item) 558
Printer Host Name (information item) 562
Printer ID (information item) 562
Printer Info Updated (information item) 557
Printer Model (information item) 561
Printer Name (information item) 561
Printer Sharing (information item) 556
Printer State (information item) 562
Printers (information item category) 561
printers, gathering information 73
Priority (information item) 576
Process Architecture (information item) 565
Process Count (information item) 559
Process Executable Path (information item) 565
Process File Creator (information item) 565
Process File Type (information item) 565

-
- Process ID (information item) 565
Process Info Updated (information item) 558
Process Name (information item) 565
Process Priority (information item) 566
processes
 gathering information 74
 terminating 133
Processes (information item category) 565
Processes (menu command) 350
Processes (window) 350
Processor Architecture (information item) 539
Processor Family (information item) 539
Processor Has 3DNow (information item) 539
Processor Has MMX (information item) 539
Processor Has SSE (information item) 539
Processor Has SSE2 (information item) 539
Processor Has SSE3 (information item) 540
Processor Hyperthreading Enabled (information item) 540
Processor ID String (information item) 539
Processor Is 64-bit (information item) 539
Processor L1 Data Cache (information item) 539
Processor L1 Instruction Cache (information item) 539
Processor L2 Data Cache (information item) 539
Processor L2 Instruction Cache (information item) 539
Processor L3 Cache (information item) 539
Processor Model (information item) 539
Processor Speed (information item) 539
Processor Stepping (information item) 539
Processor Supports Hyperthreading (information item) 540
Processor Type (information item) 539
Processor Vendor (information item) 539
Profile Name (information item) 588
prohibited software, monitoring 249
Protocol (information item) 586
Provides (information item) 562
provisioning profiles
 installing 153
 removing 154
Purchase Count (information item) 582
Purchase Date (information item) 582
purchase information, recording 254
Purchase License Owner (information item) 582
Purchase Maintenance Available (information item) 583
Purchase Maintenance Begin (information item) 583
Purchase Maintenance End (information item) 583
Purchase Maintenance Price (information item) 583
Purchase Maintenance Reference (information item) 583
Purchase Notes (information item) 583
Purchase Order Number (information item) 582
Purchase Price (information item) 582
Purchase Software Version (information item) 582
Purchase Tracking (information item category) 582
Purchase Type (information item) 582
Purchase Vendor Contact (information item) 583
Purchase Vendor Name (information item) 582
Purchase Vendor Reference (information item) 582
Purchase Vendor Support (information item) 583
putting to sleep administered computers 117
- Q**
- Quarter Size (menu command) 624
Quartz Extreme (information item) 552
- R**
- RAM, information items 547
Read Administrator Info (menu command) 344
Read Distribution and Licensing Info (menu command) 343
- Real Group ID (information item) 566
Real User ID (information item) 566
Real Username (information item) 566
Reapply Command (menu command) 333, 532
Recent Connections (submenu) 621
Recent Files (submenu) 272
Record Creation Date (information item) 535
re-enrolling iOS devices 64
Re-execute All Actions for This Device (menu command) 425
Re-execute This Action for All Devices (menu command) 432
Re-execute This Action for This Device (menu command) 425
Re-execute This Action for This Policy (menu command) 432
Refresh (menu command) 488, 517
Refresh Rate (information item) 552
Refresh Status (menu command) 526
Registered Company (information item) 564
Registered Owner (information item) 564
Registration (dialog) 347
registry
 gathering information 78
 searching for entries 78
Registry Entries (information item category) 569
Registry Entries (menu command) 354
Registry Entries (window) 354
Registry Entry Found (information item) 569
Registry Name (information item) 569
Registry Record Modification Date (information item) 569
Registry Value (information item) 569
Registry Value Binary (information item) 569
Registry Value Number (information item) 569
Registry Value String (information item) 569
Registry Value Type (information item) 569
registry, editing 136
Reinstall Mac OS X Computer (menu command) 298
Reinstall Windows Computer (menu command) 301
Reinstallation Task Data Copied (information item) 617
Reinstallation Task Data Total (information item) 617
Reinstallation Task Domain to Join (information item) 617
Reinstallation Task Hostname to Set (information item) 617, 618
Reinstallation Task Info (information item) 617
Reinstallation Task Join AD Domain (information item) 617
Reinstallation Task Last Update (information item) 617
Reinstallation Task Percent Complete (information item) 617
Reinstallation Task State (information item) 617
reinstalling
 Mac OS X 237
 Windows 241
Reinstalling Windows computers
 installing support for 20
Reload All Tables (menu command) 342
Reload Selected Records (menu command) 343
Remaining Battery Capacity (information item) 540
Remote (information item) 562
Remote Apple Events (information item) 556
Remote Control (information item) 574
Remote Control (menu command) 375
Remote Desktop Screen Sharing (information item) 556
Remote Desktop, remote control with 122
Remote Login (information item) 556
Remote Management (information item) 556
remotely controlling computers 122
 via URLs 124

Remove Action (menu command) 416, 432
Remove Action from Policy (menu command) 434
Remove Administrator (menu command) 494
Remove Administrator from Group (menu command) 484
Remove Administrator Group (menu command) 494
Remove Agent (menu command) 522
Remove All Group Members (menu command) 480
Remove Appointment Group (menu command) 494
Remove Category (menu command) 371, 384, 416
Remove Command (menu command) 533
Remove Computer Records (information item) 573
Remove Configuration Profile (menu command) 416, 429
Remove Configuration Profile Action (dialog) 413
Remove Configuration Profile from Policy (menu command) 429
Remove Custom Information Field (menu command) 494
Remove Custom Zone (menu command) 516
Remove Disk Image (menu command) 494
Remove Distribution Point (menu command) 494
Remove form Policy (menu command) 426
Remove from Group (menu command) 371, 375
Remove from Server (menu command) 374
Remove Group (menu command) 370, 416
Remove History Commands (information item) 573
Remove Inventory Data (information item) 573
Remove Inventory Data (menu command) 374
Remove iOS Provisioning Profile (menu command) 416
Remove Item (menu command) 494
Remove License Reports (information item) 573
Remove License Specification (menu command) 494
Remove Media File (menu command) 416, 431
Remove Mobile Application Package (menu command) 416, 429
Remove Mobile Device History Commands (information item) 574
Remove Mobile Device Records (information item) 574
Remove Payload (menu command) 494
Remove Policy (menu command) 416, 434
Remove SD Log Entries (information item) 573
Remove Smart Group (menu command) 384, 494, 518, 532
Remove Software Package (menu command) 494
Remove Template (menu command) 360
removing
 configuration profiles
 automatically 151
 manually 148
 provisioning profiles 154
 software (iOS) 164
Rename Action (menu command) 416
Rename Category (menu command) 370, 383
Rename Configuration Profile (menu command) 416
Rename File (dialog) 327
Rename File/Folder (menu command) 327
Rename Group (menu command) 370, 383, 416
Rename iOS Provisioning Profile (menu command) 416
Rename Media File (menu command) 416
Rename Mobile Application Package (menu command) 416
Rename Policy (menu command) 416
Rename Tab (menu command) 266
renaming files 192
Repeat Restart Notification (information item) 577
Repeat Selected Installations (menu command) 496
Report Date (information item) 585
Report Description (information item) 588
Reports (information item category) 588
reports on licensed software 260
Requires Admin Privileges (information item) 576
Requires Exclusive Install (information item) 579
Requires Exclusive Uninstall (information item) 579
Reset All Ignored Devices (menu command) 425
Reset Current Server Load (menu command) 496
Reset Package (menu command) 496
Reset Software Packages (information item) 573
Reset Tracking Passphrase (menu command) 341
Resolution (information item) 552
Restart Notification (information item) 577
restarting administered computers 117
Restore All Settings (menu command) 345
Restore Custom Information Fields (menu command) 344
Restore Server Settings (menu command) 345
Retrieve Payloads (menu command) 495
Retry All Failed Profiles (menu command) 425
Retry Package (menu command) 495
Retry Software Packages (information item) 573
roaming options, setting 155
Router Address (information item) 560
Run License Monitoring Scan (menu command) 332
Run Software Distribution Check (menu command) 332
Running Count (information item) 585

S

Save (menu command) 267
Save Administrator Info (menu command) 344
Save All Settings (menu command) 345
Save As (menu command) 267
 in Absolute Remote 621
Save Custom Information Fields (menu command) 344
Save Distribution and Licensing Info (menu command) 343
Save Server Settings (menu command) 345
Save Template (dialog) 287
Scan All Volumes (information item) 582
Scheduled Time (information item) 571
Scheduling Options (menu command) 532
scheduling power management events 118
Scope ID (information item) 560
Score (information item) 589
Score Item Description (information item) 589
Score Item Index Path (information item) 589
Score Item Title (information item) 589
Score Item Weight (information item) 589
Score Items (information item category) 589
Score State (information item) 589
Scored Computer Count (information item) 589
Scoring States (information item) 589
screen sharing 122
scripts
 executing on administered computers 130
 in custom information fields 84
SCSI Bus Number (information item) 549
SCSI Capacity (information item) 549
SCSI Device Count (information item) 546
SCSI Device Type (information item) 549
SCSI Devices (information item category) 549
SCSI Manufacturer (information item) 549
SCSI Model (information item) 549
SCSI Revision (information item) 549
SCSI Transfer Width (information item) 550
SCSI Unit Number (information item) 549
SD Server Address (information item) 536
SD Server Check Interval (information item) 536
SD Server Port (information item) 536
SD Server Unique ID (information item) 536
Search Domains (information item) 560
Search Windows Registry (menu command) 305

Search Zone (menu command) 517
searching
 files 76
 for network devices 36
 in browser windows 109
 in columns 109
 registry 78
 zones in the Agent Deployment Center 36
Security Identifier (information item) 554
Select All (menu command) 274
Select Container (menu command) 281
Send Clipboard (menu command) 621
Send E-mail Action (dialog) 407
Send Message (menu command) 296
Send Message Action (dialog) 405
Send Message to Device (menu command) 339
Send Re-enrollment Message to Device (menu command) 427
Send SMS Action (dialog) 409
sending messages 115
 to mobile devices 140
Server (menu) 342–348
Server Address (information item) 535
Server Center 435–509
 category bar 437
 columns 437
 computer groups 227
 context menu 442
 information items 437
 smart groups 438
 status bar 437
 toolbar 436
Server Center (information item category) 571–585
Server Center (menu command) 358
Server Monitor (category) 508
Server Port (information item) 535
Server Properties (dialog) 516
Server Settings (category) 497
Server Unique ID (information item) 535
servers
 mirroring custom information fields 86
servers *see Absolute Manage Server*
Servers (information item category) 535
Service Description (information item) 563
Service Display Name (information item) 563
Service Executable Path (information item) 563
Service Log On As (information item) 563
Service Name (information item) 562
Service Startup Type (information item) 563
Service Status (information item) 563
services
 starting 135
 startup status 134
 stopping 135
Session (menu) 624
Session ID (information item) 565
Set Availability Time (menu command) 430
Set Device Name (menu command) 423
Set Device Ownership (menu command) 427
Set Inventory Server (menu command) 523
Set Roaming Options (menu command) 338
Settings (menu command) 275
 in Absolute Remote 622
shell scripts, executing on administered computers 130
shell variables *see environment variables*
shortcuts, creating 195
Show Action Details (menu command) 431
Show Command Result (menu command) 533
Show Computer Detail View (menu command) 361
Show Configuration Profile Details (menu command) 429
Show Detail View (menu command) 373, 424
Show Details for This Computer (menu command) 381
Show Details for This Scoring Item (menu command) 381
Show Location on Bing Maps (menu command) 426
Show Location on Google Maps (menu command) 426
Show Media File Details (menu command) 430
Show Mobile Application Package Details (menu command) 428
Show Policy Members (menu command) 434
Show Provisioning Profile Details (menu command) 429
Show Release Notes (menu command) 363
Show Report Details (menu command) 355
Show Status Bar (menu command) 281
Show/Hide Target List (menu command) 334
shutting down administered computers 117
Size (information item) 547
Sizes (information item) 561
sleep
 putting to sleep administered computers 117
 waking up administered computers 118
Smart Group (dialog) 369
 Agent Deployment Center 517
 command history 531
 command queue 530
 compliance report details 382
 compliance report summary 381
 compliance score item summary 382
 distribution points 466
 installation status 469
 license history 478
 license history summary 478
 license specifications 476
 license status 477
 missing software 478
 missing software packages 469
 payloads 464
 software packages 462, 468
 software usage 477
smart groups
 browser windows 367
 Commands window 528
 Compliance Report window 379
 creating 111
 deleting 112
 editing 112
 exporting 269
 importing 269
 Mobile Devices window 389
 saving 112
 Server Center 438
SMBIOS Version (information item) 545
SMC Version (information item) 544
software
 App Store volume purchasing program 167
 importing into Absolute Manage 159
 information on installed software 75

software
installing 200–247
ad hoc 233
App Store apps 165
configuring agents 202
manually 200
on mobile devices 157
overview 201
performing installations 233
preparing iOS devices 155
setup 202
making available to mobile devices 161
monitoring prohibited software 249
preparing for iOS devices 158
recommending commercial apps 165
removing (iOS) 164
Software Distribution (information item category) 575–581
Software Distribution Center 200–247
distribution points 202
metapackages 220
patch management 235
payloads 209
performing ad hoc installations 233
performing installations 232
reinstalling Mac OS X computers 237
reinstalling Windows computers 241
software packages 211
updating 43
Software Distribution Package (dialog) 443
software distribution servers
assigning to agents 57
Software Identified By (information item) 581
Software Information (information item category) 553–570
Software License Specification (dialog) 470
software packages
ad hoc installations 233
Adobe CS 219
assigning to computer groups 232
conflicting settings 220
editing 219
explained 202
removing 220
setting up 211
updating 44
Software Patch Recommended (information item) 578
Software Patch Version (information item) 578
sort order 113
sorting browser windows 113
sorting columns 113
SSH Port (information item) 586
SSL certificates
displaying 18
exporting 19, 499
staging servers *see distribution points*
Start Time (information item) 571
starting services 135
Startup Item Count (information item) 559
Startup Item Description (information item) 562
Startup Item Info Updated (information item) 558
Startup Item Name (information item) 562
startup items
gathering information 73
Startup Items (information item category) 562
startup status of services 134
status bar
browser windows 366
Server Center 437
Status Timestamp (information item) 584
stolen computers, tracking 125
stopping services 135
storing information 97
Sudden Motion Sensor (information item) 543
superadministrators explained 10, 46
Superseded by Package (information item) 578
Supported Operating Systems (information item) 578
Swap Space Free (information item) 546
Swap Space Total (information item) 546
Swap Space Used (information item) 546
Switch Administrator and Server (menu command) 274
switching administrator accounts 53
Synchronize All Tables (menu command) 342
Synchronize Custom Information Fields (menu command) 344
Synchronize Records (menu command) 373
in the Windows Reinstallation Tasks window 361
Synchronize Selected Records (menu command) 343
Synchronize Server Settings (menu command) 345
System Enclosure Asset Tag (information item) 546
System Enclosure Manufacturer (information item) 545
System Enclosure Serial Number (information item) 545
System Enclosure Type (information item) 546
System Enclosure Version (information item) 546
System Hibernate Timer (information item) 542
System Information (information item category)
hardware 538
software 553
System Management Server 97
system overview 2–10
system requirements of Absolute Manage 12
System Sleep Timer (information item) 542

T

tab-delimited text, export format 268
tabs
closing 105
new 104
renaming 105
Target Installation Volume (information item) 575
Target OS Platform (information item) 577
TCP Implementation (information item) 560
Terminate App If License Exceeded (information item) 582
Terminate Process (menu command) 298
Terminate Prohibited Apps (information item) 582
terminating
processes 133
services 135
text
export format 268
exporting 98, 268
text file display window 195
TheftTrack 125
Threads (information item) 566
Tile Horizontally (menu command) 349
Tile Vertically (menu command) 350
Timbuktu Access (information item) 556
Timbuktu, remote control with 122
Time Machine (menu command) 304
Time Machine Auto Backup Enabled (information item) 557
Time Machine Backup Disk (information item) 557
Time Machine Disk Free (information item) 557
Time Machine Disk Size (information item) 557

Time Machine Latest Backup (information item) 557
Time Machine Oldest Backup (information item) 557
Time Machine Snapshot Count (information item) 557
Time Machine Status (information item) 557
Time Machine, controlling 125
toolbar
 Agent Deployment Center 511
 browser windows 366
 command windows 284
 Commands window 527
 Compliance Reports window 378
 Mobile Devices window 388
 Server Center 436
Toolbar (menu command) 281
Total Install Count (information item) 583, 584
Total Launces (information item) 583
Total Running Count (information item) 583, 584
Total Usage Time (information item) 583
Track as Missing Software (information item) 582
Track Device (menu command) 339
Tracked Computer Address (information item) 569
Tracked Computer Current User Account (information item) 570
Tracked Computer Current User Name (information item) 570
Tracked Computer GMT Delta (information item) 570
Tracked Computer Public Address (information item) 569
Tracked Computer Resolved Address (information item) 570
Tracked Computer Resolved Public Address (information item) 570
Tracked Computer Resolved Router Address (information item) 570
Tracked Computer Router Address (information item) 569
Tracked Computer Time (information item) 570
Tracked Computer Time Stamp (information item) 569
tracking
 computers 125
 license purchases 254
Transfer All Files in Folder (information item) 579
Transfer File/Folder (menu command) 315
transferring files to administered computers 197
TTYs Keep Awake (information item) 542

U

unappointing administrators 61
Undo (menu command) 273
Uninstall String (information item) 564
Uninstallable (information item) 563
Unique Computer ID (information item) 545
Unix Group (information item) 568
Unix Mount Point (information item) 548
Unix Owner (information item) 568
Unix Permissions (information item) 568
Unix shell scripts *see shell scripts*
unlocking mobile devices 141
unsorting browser windows 114
Update Device Info (menu command) 339
Update Device Info Action (dialog) 411
Update Installed Application Statistics (menu command) 428
updating
 Absolute Manage 42
 distribution points 43
 Software Distribution Center 43
 software packages 44
Upload Status (information item) 579
UPS Installed (information item) 542
URI (information item) 562

URLs
 displaying information 106
 launching remote control sessions 124
Usage Time (information item) 585
USB Device Class (information item) 551
USB Device Count (information item) 546
USB Device Protocol (information item) 551
USB Device Speed (information item) 551
USB Device Subclass (information item) 551
USB Devices (information item category) 550
USB Max. Power (information item) 551
USB Model (information item) 550
USB Product ID (information item) 551
USB Product Version (information item) 551
USB Vendor (information item) 550
USB Vendor ID (information item) 551
Use Custom Agent Name (information item) 536
Use Template (menu command) 360
User ID (information item) 565
user information fields *see client information fields*
User Interaction (information item) 577
Username (information item) 565
users, Absolute Manage user types explained 9
Uses (information item) 562
USGCB SCAP reports 80

V

values in the registry, working with 136
variables
 environment variables 137
 environment variables for files 137
 environment variables for the registry 138
 in configuration profiles 143
 defining 144
 using 145
Video Card Model (information item) 553
View (menu) 281–282
 in Absolute Remote 623
View Administrator Settings (information item) 572
View Commands Window (information item) 572
View Computer Tracking Data (information item) 572
View Computer Tracking Screenshots (information item) 572
View Custom Information Fields (information item) 572
View in Separate Window (menu command) 376
View License Monitoring Settings (information item) 572
View Mobile Device Tracking Data (information item) 574
View Server Status (information item) 572
View Software Distribution Settings (information item) 572
View Text File (dialog) 327
View Text File (menu command) 327
viewing files 193
Virtual Memory (information item) 566
Visual Basic scripts, executing on administered computers 130
VNC Access (information item) 556
VNC, remote control with 122
Volume Count (information item) 546
Volume Name (information item) 547
Volume Serial Number (information item) 547
Volume Type (information item) 547
Volumes (information item category) 547
VRAM Size (information item) 552

W

Wake on AC Change (information item) 542
Wake on Clamshell Open (information item) 542
Wake on LAN Enabled (information item) 556

Wake on LAN Supported (information item) 557
Wake Up (menu command) 297
waking up administered computers 118
Warn About Slow Network (information item) 578
warning messages, suppressing and reactivating 277
Window (menu) 349–362
 in Absolute Remote 625
Windows Networking zones 34
Windows Reinstallation Tasks (information item category) 615–618
Windows Reinstallation Tasks (menu command) 361
Windows Reinstallation Tasks (window) 361
Windows Service Count (information item) 559
Windows Services (information item category) 562
Windows Services Info Updated (information item)
 558
WINS Resolution (information item) 561
WINS Server (information item) 561

X

XCCDF Item Identifier (information item) 589
XML
 export format 268
 exporting 98, 268

Z

zone definition files 518
zones, in the Agent Deployment Center 512
 creating 34
 deleting 37
 editing 37
 searching 36